
CHALMERS

GÖTEBORGS UNIVERSITET

# Artins förmodan: $p$-adiska tal, ändliga kroppar och ekvationer utan heltalslösningar

*Examensarbete för kandidatexamen i matematik vid Göteborgs universitet*
*Kandidatarbete inom civilingenjörsutbildningen vid Chalmers*

Alexander Karlsson
Markus Klyver
Kajsa Wahl

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2019

# Artins förmodan: $p$-adiska tal, ändliga kroppar och ekvationer utan heltalslösningar

*Examensarbete för kandidatexamen i matematik vid Göteborgs universitet*
Alexander Karlsson Kajsa Wahl

*Kandidatarbete i matematik inom civilingenjörsprogrammet Teknisk matematik vid Chalmers*
Markus Klyver

Handledare: Julia Brandes
Examinator: Ulla Dinger och Maria Roginskaya

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2019

# Populärvetenskaplig presentation

Att hitta heltalslösningar till ekvationer har länge varit av intresse inom matematiken. Redan på 200-talet arbetade den grekiske matematikern Diofantos med just detta. Diofantos skrev en bok, Arithmetica, som behandlar 130 olika ekvationer och deras heltalslösningar. Ekvationer där endast heltalslösningar efterfrågas har blivit uppkallade efter Diofantos och kallas numera diofantiska ekvationer. Till exempel kan polynomekvationer betraktas som diofantiska om man begränsar sig till att söka lösningar bland heltalen.

Ett exempel på en känd polynomekvation är $a^2+b^2 = c^2$ från Pythagoras sats om rätvinkliga trianglar. Ekvationen kan ses som en diofantisk ekvation om vi bara intresserar oss för heltalslösningarna. Sådana lösningar kallas för pythagoreiska tripplar. Ett exempel på en pythagoreisk trippel är $3, 4$ och $5$, eftersom $3^2 + 4^2 = 5^2$.

En annan känd polynomekvation är $x^n + y^n = z^n$, som är ekvationen i Fermats sista sats. Satsen säger att ekvationen inte har några positiva heltalslösningar då $n$ är större än två. Om $n$ är lika med två får vi precis ekvationen i Pythagoras sats, vilken har oändligt många heltalslösningar. Fermat skrev sin sista sats i ett exemplar av Diofantos Arithmetica och därefter skrev han "Jag har ett i sanning underbart bevis för detta påstående, men marginalen är alltför trång för att rymma detsamma." (Originalet på latin: "Cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet").

Att avgöra vilka diofantiska ekvationer som har lösningar är fortfarande ett öppet matematiskt problem. Matematikern David Hilbert formulerade år 1900 en lista på 23 matematiska problem där det tionde problemet löd "Existerar det en algoritm som kan avgöra om en diofantisk polynomekvation har en lösning?" Den ryske matematikern Matijasevitj [13] lyckades bevisa att en sådan algoritm inte existerar, och därmed är studerandet av diofantiska ekvationer fortfarande relevant. På 30-talet formulerade matematikern Emil Artin en förmodan kring när en viss sorts ekvationer, nämligen homogena polynomekvationer, har lösningar. Att ett polynom är homogent innebär att varje term i polynomet har samma grad. Exempelvis är ekvationen $a^2 + b^2 = c^2$ från Pythagoras sats en homogen polynomekvation eftersom varje term är av grad två. En homogen polynomekvation av grad större än noll har alltid nollan som lösning, i exemplet ovan ser vi att om $a, b$ och $c$ är lika med noll är ekvationen uppfylld.

Vi ska undersöka nödvändiga villkor för att en diofantisk homogen polynomekvation ska ha nollskilda lösningar. Ofta har ekvationer implicita delbarhetsvillkor. Till exempel gäller det i Fermats ekvation att $x$, $y$ och $z$ inte alla kan vara udda eftersom vänsterledet då skulle bli jämnt medan högerledet skulle bli udda, och då gäller inte likheten. Liknande hinder till att lösningar existerar kan finnas även om vi testar delbarhet med ett annat tal än två och ibland innebär det att ekvationen inte har några lösningar alls. Artin förmodade att om variabelantalet i en homogen polynomekvation är tillräckligt stort så finns det inte några delbarhetsrelaterade skäl till varför en ekvation saknar nollskilda lösningar.

Artins förmodan ligger till grund för det här arbetet. Förmodan är i allmänhet falsk, men stämmer ändå i många fall och vi ska i det här arbetet bygga upp teorin för att motivera formuleringen av Artins förmodan.

**Sammanfattning**

Artins förmodan om homogena polynomekvationer ligger till grund för den här uppsatsen. Förmodan är falsk i allmänhet men stämmer i många fall. Ett av våra mål är att motivera varför förmodan är formulerad som den är. Utöver det presenterar vi ett motbevis till förmodan samt bevisar förmodan i ett specifikt fall. Vi konstruerar de $p$-adiska talen då förmodan är formulerad i termer av $p$-adiska tal och vi presenterar teori om ändliga kroppar då teorin behövs i motiveringen av förmodan, motbeviset och i beviset av det specifika fallet.

**Abstract**

This paper is based on Artin's conjecture concerning homogeneous polynomial equations. The conjecture is false in general but it is still true in many cases. One of our goals is to motivate why the conjecture is formulated the way it is. Moreover, we present a counterproof to the conjecture and we prove the conjecture in one specific case. We construct the $p$-adic numbers as the conjecture is expressed in terms of $p$-adic numbers and we introduce theory on finite fields, as it is needed in the motivation of the conjecture, the counterproof and in the proof of the specific case.

# Innehåll

# Förord

Vi vill tacka vår handledare Julia Brandes för all hjälp och för det stöd vi fått under arbetets gång. Som grupp har vi träffats tillsammans med handledaren en gång i veckan för att uppdatera varandra kring vad som har gjorts, ställa de frågor som behövts ställas, planera den kommande veckan och för att ta viktiga beslut.

Under arbetets gång har vi fört en gemensam dagbok där vi antecknat vad som sagts på möten och vilka beslut som tagits. Utöver det har varje enskild persons arbete loggats i en tidslogg där vi skrivit hur många timmar vi arbetat samt vad vi har gjort. I stora drag har Alexander och Kajsa varit huvudansvariga för att motivera Artins förmodan, samt att ge motbevis och bevis till Artins förmodan medan Markus har varit huvudansvarig för teorin som behandlar de $p$-adiska talen.

Alexander fick från början ansvar för att tillsammans med Markus läsa om $p$-adiska tal och förstå Hensels lemma. Han har sedan tillsammans med Kajsa funderat över motiveringen till Artins förmodan, Terjanians motbevis och läst Lewis bevis. De avsnitt i rapporten som huvudsakligen är skrivna av Alexander är den populärvetenskapliga presentationen, kapitel $1, 4, 5, 6$, avsnitt 2.1 samt avsnitt A och B i Appendix.

Kajsa har haft huvudansvar för att dagboken ska bli uppdaterad varje vecka. Hon fick från början även ansvar för att sätta sig in i kroppsutvidgningar och förstå normfunktionen. Vidare har hon tillsammans med Alexander funderat över motiveringen till Artins förmodan, Terjanians motbevis och läst Lewis bevis. De avsnitt i rapporten som huvudsakligen är skrivna av Kajsa är den populärvetenskapliga presentationen, sammanfattningen, förordet, kapitel $1, 3, 4, 5, 6$ och avsnitt A i Appendix.

Markus har varit huvudansvarig för kandidatrapportens utformning i LaTeX och för att uppdatera kontinuerligt mot SVN. Markus fick från början även ansvar för att tillsammans med Alexander läsa om $p$-adiska tal och förstå Hensels lemma. Vidare har Markus varit ansvarig för teorin som behandlat $\mathbb{Q}_p$ och för att bevisa de satser som behövts för att arbetet inte ska ha luckor. De avsnitt i rapporten som huvudsakligen är skrivna av Markus är kapitel 2 och Appendix.

# 1 Inledning

På 1930-talet formulerade Emil Artin en förmodan om villkoren för existensen av icke-triviala lösningar till homogena polynomekvationer [1]. Det här arbetet syftar till att undersöka motiveringen bakom Artins förmodan.

För att avgöra om en polynomekvation saknar heltalslösningar kan man undersöka om den saknar reella lösningar, då $\mathbb{R}$ som bekant är en komplettering av $\mathbb{Q}$ och därmed har heltalen som delmängd. Det finns ibland uppenbara anledningar till att ekvationer saknar icke-triviala lösningar, exempelvis saknar $x^2 + y^2 = 0$ icke-triviala lösningar bland de reella talen eftersom $x^2 \geq 0$ för alla $x$.

På liknande sätt kan delbarhets- och kongruensegenskaper säga något om heltalslösningar till en ekvation. Om en ekvation har en heltalslösning har den även en lösning modulo $p^n$, för alla primtal $p$ och alla positiva heltal $n$. För att utesluta att det existerar en icke-trivial lösning kan vi därför betrakta ekvationen modulo $p^n$. Om endast nollan uppfyller ekvationen modulo $p^n$ för alla tal $n$ är enbart nollan en lösning även till den ursprungliga ekvationen, eftersom det enda talet som är oändligt delbart med $p$ är noll. De så kallade $p$-adiska talen $\mathbb{Q}_p$ "sammanfattar" $\mathbb{Z}/p^n\mathbb{Z}$, för alla $n$ och för varje $p$, och är precis som $\mathbb{R}$ kompletteringar av $\mathbb{Q}$. Mängden $\mathbb{Q}_p$ karakteriserar alltså alla delbarhetsvillkor, för ekvationen i fråga, som har med $p$ att göra. Det existerar inte heller några kompletteringar av $\mathbb{Q}$ utöver $\mathbb{R}$ och $\mathbb{Q}_p$ enligt Ostrowskis sats, vilken vi presenterar i kapitel 2. Då $\mathbb{Q}_p$ är kompletteringar av $\mathbb{Q}$ är heltalen en delmängd även till de $p$-adiska talen, så om det inte förekommer en lösning i $\mathbb{Q}_p$ gör det inte heller det i $\mathbb{Z}$. Artins förmodan är formulerad i termer av $p$-adiska tal.

**Artins förmodan:** Låt $F(x_1, \ldots, x_n)$ vara ett homogent polynom av grad $d$ med koefficienter i $\mathbb{Q}_p$. Ekvationen $F(x_1, \ldots, x_n) = 0$ har en icke-trivial lösning i $\mathbb{Q}_p$ om $n$ är större än $d^2$.

Artins förmodan är falsk i allmänhet. Terjanian [18] motbevisade Artins förmodan genom att konstruera ett polynom i 18 variabler av grad fyra över $\mathbb{Q}_2$ som enbart har den triviala lösningen i $\mathbb{Q}_2$. Lewis och Montgomery [12] visade att det för oändligt många grader $d$ finns ett primtal $p$ och ett homogent polynom över $\mathbb{Z}$ av grad $d$ som enbart har den triviala lösningen i $\mathbb{Q}_p$, fastän variabelantalet är större än

$$\exp\left(\frac{d}{(\log d)(\log\log d)^{1+\varepsilon}}\right),$$

för något $\varepsilon > 0$.

Förmodan stämmer emellertid i vissa fall, och det är ett öppet matematiskt problem under vilka ytterligare antaganden förmodan stämmer. Hasse [8] visade att Artins förmodan stämmer för kvadratiska homogena polynom. Lewis [11] samt Demyanov [5] har oberoende bevisat Artins förmodan då graden av det homogena polynomet är tre.

Syftet med vårt arbete är att undersöka motivationen bakom Artins förmodan samt att återge en version av Terjanians motbevis och huvuddragen av Lewis bevis för kubiska homogena polynom. För att undersöka motivationen bakom Artins förmodan utreder vi varför Artin förmodade att det krävs ett variabelantal på $d^2 + 1$ för att en icke-trivial lösning alltid ska existera till ett homogent polynom av grad $d$. Vårt mål är således att konstruera homogena polynomekvationer av grad $d$ i $d^2$ variabler som enbart har den triviala lösningen, genom att använda en liknande metod som Mordell [14]. Genom att systematiskt konstruera sådana polynom för alla grader och för alla primtal motiveras förmodan.

För att nå våra mål presenterar vi först den teori som krävs. Vi börjar med att konstruera de $p$-adiska talen och vidare introducera kroppsutvidgningar och teori kring ändliga kroppar. Vi ska speciellt betrakta en funktion som kallas norm från en kroppsutvidgning till dess ursprungliga kropp, vilken är fundamental i den systematiska konstruktionen av de homogena polynomekvationerna. Efter presentationen av ovanstående teori redogör vi för den systematiska konstruktionen av de homogena polynomekvationerna samt bevisar och motbevisar Artins förmodan i de två fall som tidigare nämnts.

# 2 De $p$-adiska talen

Syftet med det här kapitlet är att utöka $\mathbb{Q}$ till de $p$-adiska talen $\mathbb{Q}_p$ som är en fullständig kropp som ej sammanfaller med $\mathbb{R}$, för varje primtal $p$. I det första avsnittet introducerar vi den $p$-adiska valueringen samt det $p$-adiska absolutvärdet. Avsnitt 2.2 lägger grunden för den algebraiska konstruktionen av de $p$-adiska talen och i avsnitt 2.3 konstruerar vi dem. Teorin i det här kapitlet återfinns bland annat i Gouvêa [6] och Greenberg [7].

## 2.1 Valueringar och absolutvärden

Målet med det här avsnittet är att lägga grunden för konstruktionen av de $p$-adiska talen. Vi börjar med att definiera vad en valuering är.

**Definition 2.1.** Låt $K$ vara en kropp. Funktionen $v$ är en valuering på $K$ om den för alla $x, y \in K$ uppfyller

(i) $v(xy) = v(x) + v(y)$,

(ii) $v(x+y) \geq \min\{v(x), v(y)\}$,

(iii) $v(x) = \infty$ om och endast om $x = 0$.

Om $\mathrm{Im}(v) \subseteq \mathbb{Z} \cup \{\infty\}$ säger vi att $v$ är en diskret valuering.

Vidare definierar vi den $p$-adiska valueringen vilken används både i definitionen av det $p$-adiska absolutvärdet samt i konstruktionen av de $p$-adiska talen.

**Definition 2.2.** Fixera ett primtal $p$. Den $p$-adiska valueringen $v_p(n)$ för ett nollskilt heltal $n$ definieras som en funktion $v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}$ på följande sätt:

Låt $v_p(n)$ vara det unika positiva heltal $k$ som satisfierar $n = p^k m$ för ett heltal $m$ där $p$ och $m$ är relativt prima. Vi utökar $v_p(n)$ till hela $\mathbb{Q} \setminus \{0\}$ genom

$$v_p(x) = v_p(a) - v_p(b)$$

där $x = \frac{a}{b}$ är ett rationellt tal, där $b \neq 0$.

För $x = 0$ låter vi $v_p(0) := \infty$. Vi har därmed utökat $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$.

Notera att för ett heltal $n$ är $v_p(n)$ lika med antalet gånger $n$ är delbart med $p$.

**Lemma 2.3.** Funktionen $v_p$ är en valuering på $\mathbb{Q}$.

*Bevis.* Antag först att $x$ och $y$ är heltal. Låt $x = p^n x'$ och $y = p^m y'$ där $p$ inte delar $x'$ och $y'$. Då gäller att

$$v_p(xy) = v_p(p^{n+m} x'y') = n + m = v_p(x) + v_p(y).$$

Antag nu att $n \leq m$. Då gäller att

$$v_p(x+y) = v_p(p^n(x' + p^{m-n}y')) \geq n = \min\{v_p(x), v_p(y)\}.$$

Detta bevisar både (i) och (ii) när $x$ och $y$ är heltal.

När $x, y \in \mathbb{Q}$ inte är heltal kan vi sätta $x = \dfrac{a}{b}$ och $y = \dfrac{c}{d}$. Valueringen kan beräknas som

$$v_p(xy) = v_p\left(\frac{ac}{bd}\right) = v_p(ac) - v_p(bd) = v_p(a) - v_p(b) + v_p(c) - v_p(d) = v_p(x) + v_p(y).$$

Alltså gäller (i) för alla $x, y \in \mathbb{Q}$. På liknande sätt visas även (ii) i det rationella fallet, här har vi

$$\begin{aligned} v_p(x+y) &= v_p\left(\frac{ad+bc}{bd}\right) \\ &= v_p(ad+bc) - v_p(bd) \\ &\geq \min\{v_p(ad),\, v_p(bc)\} - v_p(bd) \\ &= \min\{v_p(x),\, v_p(y)\}. \end{aligned}$$

Slutligen följer (iii) från definitionen av $v_p$. □

**Lemma 2.4.** Den $p$-adiska valueringen är väldefinierad.

*Bevis.* Det som ska visas är att den $p$-adiska valueringen är oberoende av representationen av det rationella talet $\frac{a}{b}$. Antag därför att $\frac{a}{b} = \frac{c}{d}$, vilket är ekvivalent med att $ad = cb$. Vi har att

$$0 = v_p(ad) - v_p(cb) = v_p(a) + v_p(d) - v_p(c) - v_p(b) = v_p\left(\frac{a}{b}\right) - v_p\left(\frac{c}{d}\right)$$

Alltså är $v_p\left(\frac{a}{b}\right) = v_p\left(\frac{c}{d}\right)$, så $v_p$ är väldefinierad. □

Som vi nu visat är den $p$-adiska valueringen en väldefinierad valuering på $\mathbb{Q}$. Vi använder valueringen för att definiera det $p$-adiska absolutvärdet men innan vi gör det påminner vi om vad ett absolutvärde är, samt introducerar begreppet *icke-arkimediskt* absolutvärde.

**Definition 2.5.** Låt $K$ vara en kropp och $\mathbb{R}_{\geq 0}$ de icke-negativa reella talen. Ett *absolutvärde* på $K$ är en funktion $|\cdot| : K \to \mathbb{R}_{\geq 0}$ sådan att för alla $x, y \in K$, så är

1. $|x| \geq 0$ och $|x| = 0$ om och endast om $x = 0$,
2. $|x||y| = |xy|$,
3. $|x + y| \leq |x| + |y|$.

Om $|\cdot|$ dessutom uppfyller att

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

sägs absolutvärdet vara *icke-arkimediskt*. Ett absolutvärde som inte är icke-arkimediskt sägs vara *arkimediskt*.

*Anmärkning* 2.6. Olikheten $|x + y| \leq \max(|x|, |y|)$ är känd som den ultrametriska olikheten, och kan ses som en starkare version av triangelolikheten. En tolkning av den ultrametriska olikheten är att alla trianglar är likbenta.

Speciellt är det vanliga absolutbeloppet ett absolutvärde på $\mathbb{Q}$. Absolutvärdet

$$|x| = \begin{cases} 1 \text{ då } x \neq 0 \\ 0 \text{ då } x = 0 \end{cases}$$

definierar det triviala absolutvärdet. Låt oss nu definiera det $p$-adiska absolutvärdet.

**Definition 2.7.** Det $p$-adiska absolutvärdet av rationella tal $x \neq 0$ definieras för ett primtal $p$ som $|x|_p := p^{-v_p(x)}$ och $|0|_p := 0$.

*Anmärkning* 2.8. Vi noterar att $|\cdot|_p$ för nollskilda element i $\mathbb{Q}$ bara kan anta värden på formen $p^{-k}$ för $k \in \mathbb{Z}$.

**Sats 2.9.** Det $p$-adiska absolutvärdet $|\cdot|_p$ är ett väldefinierat icke-arkimediskt absolutvärde på $\mathbb{Q}$.

*Bevis.* Absolutvärdet är väldefinierat eftersom valueringen är väldefinierad, enligt lemma 2.4. Vi behöver verifiera de fyra kraven i definitionen av ett icke-arkimediskt absolutvärde.

Eftersom $p > 0$ och $|x|_p = p^{-v_p(x)}$ har vi att $|x|_p \geq 0, \forall x \in \mathbb{Q}$ och per definition är $|x|_p = 0$ om och endast om $x = 0$.

Enligt lemma 2.3 har vi att $v_p(xy) = v_p(x) + v_p(y)$, så

$$|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p.$$

Vidare är $|x+y|_p \leq |x|_p + |y|_p$, ty

$$|x+y|_p = p^{-v_p(x+y)} \leq p^{-\min\{v_p(x),v_p(y)\}} \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p.$$

Alltså är $|\cdot|_p$ ett icke-arkimediskt absolutvärde på $\mathbb{Q}$. □

**Exempel 2.10.** För att få en uppfattning om hur det $p$-adiska absolutvärdet fungerar ger vi några exempel nedan.

$|25|_5 = 5^{-2}$, ty $v_5(25) = 2$.

$\left|\frac{1}{18}\right|_3 = 3^2$, ty $v_3\left(\frac{1}{18}\right) = v_3(1) - v_3(18) = 0 - 2 = -2$.

$\left|\frac{12}{13}\right|_3 = 3^{-1}$, ty $v_3\left(\frac{12}{13}\right) = v_3(12) - v_3(13) = 1 - 0 = 1$.

Notera att tal som med det vanliga absolutbeloppet betraktas som "stora" men som innehåller många faktorer av $p$ är "små" med avseende på det $p$-adiska absolutvärdet.

**Sats 2.11. (Ostrowskis sats)** Varje icke-trivialt absolutvärde på $\mathbb{Q}$ är ekvivalent med något av $|\cdot|_p$ eller det vanliga absolutbeloppet.

*Bevis.* Se Gouvêa [6, sats 3.1.3]. □

Ostrowskis sats medför alltså att det inte finns några fler kompletteringar av $\mathbb{Q}$ än $\mathbb{R}$ och $\mathbb{Q}_p$, för varje $p$. Kom ihåg att vi dock får olika kompletteringar $\mathbb{Q}_p$ för olika $p$. Exempelvis är $\mathbb{Q}_5$ och $\mathbb{Q}_{11}$ två olika kompletteringar av $\mathbb{Q}$.

## 2.2 Diskreta valueringsringar

För att konstruera de $p$-adiska talen behövs ytterligare teori om diskreta valueringsringar och deras fullständiga utökning, vilket vi presenterar i det här avsnittet. Hittills har vi enbart betraktat den $p$-adiska valueringen på $\mathbb{Q}$. Generellt kan vi dock betrakta ett godtyckligt integritetsområde $R$ med en valuering $v$.

**Definition 2.12.** Om $R$ är ett integritetsområde med diskret valuering $v$ säger vi att $R$ utgör en diskret valueringsring.

**Exempel 2.13.** Betrakta en kropp $K$ och tillhörande ring $K[[x]]$ av formella potensserier $\sum_k a_k x^k$ över $K$. Definiera nu $v(x) := n$ om

$$a_0 = \ldots = a_{n-1} = 0 \text{ och } a_n \neq 0.$$

Vi ser att en sådan funktion $v : K[[x]] \to \mathbb{R}_{\geq 0}$ uppfyller kraven för en valuering i definition 2.1, och vi ser att $K[[x]]$ är en diskret valueringsring med valuering $v$.

Med den $p$-adiska valueringen är $v_p(p) = 1$. Element vars $p$-adiska valuering är 1, kallas för uniformiseringselement. Begreppet kan generaliseras till godtyckliga valueringsringar.

**Definition 2.14.** Låt $K$ vara en diskret valueringsring med valuering $v$. Ett element $\pi \in K$ med $v(\pi) = 1$ benämner vi som ett uniformiseringselement.

*Anmärkning* 2.15. Vi kan se diskreta valueringsringar som principiala integritetsområden, med ett unikt maximalt ideal, som inte utgör kroppar. Om $R$ är en diskret valueringsring med ett maximalt ideal $(p)$ för något irreducibelt element $p \in R$, kan vi definiera en funktion $v : R \to \mathbb{Z} \cup \{\infty\}$ med $v(0) = \infty$ och $v(a)$ som det största heltalet $n$ sådant att $a \in (p^n)$. Det är enkelt att kontrollera att $v$ utgör en valuering på $R$.

Vi definierar nu vad som menas med en komplettering av en valueringsring, för att senare kunna definiera de $p$-adiska talen.

**Definition 2.16.** Låt $R_1, R_2, R_3, \ldots$ vara ringar och $K = R_0$ en kropp med homomorfierna $\varphi_1, \varphi_2, \varphi_3, \ldots$ där

$$K = R_0 \xleftarrow{\varphi_1} R_1 \xleftarrow{\varphi_2} R_2 \xleftarrow{\varphi_3} \cdots \xleftarrow{\varphi_k} R_n \xleftarrow{\varphi_{k+1}} \cdots . \tag{1}$$

Betrakta den direkta produkten $R = \prod_{k=0}^{\infty} R_k$ av ringarna $R_0, R_1, R_2, \ldots, R_n, \ldots$ vars element nu är givna av oändliga följder.

Delringen $\hat{R}$ som definieras som alla element $x = (x_1, x_2, x_3, \ldots) \in \prod_{k=0}^{\infty} R_k$ för vilka

$$\varphi_k(x_k) = x_{k-1} \quad \forall k \geq 1 \tag{2}$$

säger vi vara den fullständiga kompletteringen av $R$. Vidare inför vi notationen $\hat{R} = \varprojlim R_k$ för den fullständiga kompletteringen $\hat{R}$ av $\mathbb{R}_k$ med avseende på homomorfierna $\varphi_k$.

## 2.3 Algebraisk konstruktion av de $p$-adiska talen

I det här avsnittet presenterar vi en algebraisk konstruktion av de $p$-adiska talen $\mathbb{Q}_p$, eftersom Artins förmodan är formulerad i termer av $\mathbb{Q}_p$. Vi konstruerar först de $p$-adiska heltalen $\mathbb{Z}_p$ och definierar sedan $\mathbb{Q}_p$ som bråkkroppen av $\mathbb{Z}_p$.

*Anmärkning* 2.17. Vi betecknar de $p$-adiska heltalen med $\mathbb{Z}_p$ vilket ej är att förväxla med $\mathbb{Z}/p\mathbb{Z}$ som är heltalen modulo $p$.

Betrakta uppsättningen i ekvation (1) där vi hade

$$K = R_0 \xleftarrow{\varphi_1} R_1 \xleftarrow{\varphi_2} R_2 \xleftarrow{\varphi_3} \cdots \xleftarrow{\varphi_n} R_n \xleftarrow{\varphi_{n+1}} \cdots .$$

Låt nu $p$ vara ett primtal och sätt $R_k = \mathbb{Z}/p^{k+1}\mathbb{Z}$.

Tag nu projektionsavbildningen

$$\begin{aligned} \varphi_k : \mathbb{Z}/p^{k+1}\mathbb{Z} &\to \mathbb{Z}/p^k\mathbb{Z} \\ a_{k+1} &\mapsto a_k \end{aligned}$$

för en följd $\{a_j\}_j \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$.

**Definition 2.18.** Vi definierar de $p$-adiska heltalen, $\mathbb{Z}_p$, som den fullständiga kompletteringen av $\prod_{k=1}^{\infty} \mathbb{Z}/p^k\mathbb{Z}$ med avseende på $\varphi_k$,

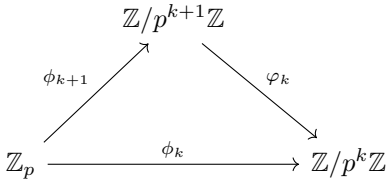
$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\varphi_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\varphi_2} \mathbb{Z}/p^3\mathbb{Z} \cdots \xleftarrow{\varphi_k} \mathbb{Z}/p^{k+1}\mathbb{Z} \xleftarrow{\varphi_{k+1}} \cdots .$$

Vi skriver $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z}$.

*Anmärkning* 2.19. Om vi betecknar funktionerna som avbildar $x \in \mathbb{Z}_p$ enligt

$$\phi_k : x \mapsto a_k \mod p^k$$

för $x \in \mathbb{Z}_p$ kan vi med denna notation se att $\mathbb{Z}_p$ definieras precis så att vi får de kommutativa diagrammen




för varje heltal $n \geq 1$.

Eftersom $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ utgör ett integritetsområde[1] är följande definition av de $p$-adiska talen naturlig att göra.

**Definition 2.20. (Definition av de $p$-adiska talen)** De $p$-adiska talen $\mathbb{Q}_p$ definieras som $\mathbb{Z}_p[\frac{1}{p}]$, vilket är kroppen av alla bråk i $\mathbb{Z}_p$.

*Anmärkning* 2.21. Varje $p$-adiskt tal $x \in \mathbb{Q}_p$ kan skrivas på formen

$$x = \sum_{k=-m_0}^{\infty} a_k p^k$$

för något $m_0 \geq 0$ och koefficienter $0 \leq a_k \leq p-1$. Representationen av $p$-adiska tal visas i sats D.15 i Appendix.

*Anmärkning* 2.22. För $x \in \mathbb{Z}_p$ gäller att $|x|_p \leq 1$. Vi utökar absolutvärdet till $\mathbb{Z}_p$ i sats D.1 i Appendix.

[1] Se sats D.8 i Appendix.

*Anmärkning* 2.23. En alternativ analytisk konstruktion av de $p$-adiska talen återfinns i Appendix, avsnitt B. I avsnitt E i Appendix bevisar vi att de två olika konstruktionerna ger upphov till isomorfa kroppar.

Att definiera de $p$-adiska heltalen som ett bakåtgränsvärde kallas ibland för att betrakta det projektiva kategoriteoretiska gränsvärdet. De $p$-adiska talen kan uppfattas både som potensserier och som ett projektivt gränsvärde, vilket vi visar i avsnitt D i Appendix. För att betona vikten av båda synsättten ger vi nu några konkretiserande exempel.

**Exempel 2.24.** Heltalet $-1$ kan skrivas som $-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \ldots$ med konvergens i den $p$-adiska metriken.[2]

**Exempel 2.25.** Antag att $p = 2$. Talet 75 kan skrivas som

$$75 = 1 \cdot 1 + 1 \cdot 2 + 1 \cdot 2^3 + 1 \cdot 2^6.$$

Genom att betrakta $\mathbb{Z}_p$ som ett projektivt gränsvärde kan vi istället skriva

$$75 = ([1]_2, [3]_4, [3]_8, [11]_{16}, [11]_{32}, [75]_{64}, [75]_{128}, \ldots)$$

som följd i $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ där $[a]_{p^i}$ betecknar ekvivalensklassen $[a]_{p^i} \in \mathbb{Z}/p^i\mathbb{Z}$.

Med synsättet av $\mathbb{Z}_p$ som projektivt gränsvärde blir det lätt att skriva ned ett explicit uttryck för -75,

$$-75 = (-[1]_2, -[3]_4, -[3]_8, -[11]_{16}, -[11]_{32}, -[75]_{64}, -[75]_{128}, \ldots).$$

**Exempel 2.26.** Hittills har vi enbart betraktat $p$-adiska utvecklingar av heltal. Den 7-adiska utvecklingen av $\frac{-5}{6}$ är

$$\frac{-5}{6} = \frac{5}{1-7} = 5(1 + 7 + 7^2 + 7^3 + \ldots).$$

Vi vill nu ge några insikter om likheterna och skillnaderna mellan de reella talen $\mathbb{R}$ och de $p$-adiska talen $\mathbb{Q}_p$. Kroppen $\mathbb{R}$ av reella tal karakteriseras av att varje Dedekindfullständig totalt ordnad kropp är isomorf med $\mathbb{R}$. Isomorfin är unik och bevarar ordningen [17, kap. 30]. Karakteriseringen av $\mathbb{R}$ ger en abstrakt syn av de reella talen. En allmän karakterisering av $\mathbb{Q}_p$ kan göras genom följande representationsatssats:

**Sats 2.27. (Karakterisering av $\mathbb{Q}_p$)**

För varje primtal $p$ finns det unik kropp, som vi väljer att kalla $\mathbb{Q}_p$, med ett icke-arkimediskt absolutvärde sådant att

(i) $\mathbb{Q}_p$ har en delkropp isomorf med $\mathbb{Q}$,

(ii) absolutvärdet inducerat på $\mathbb{Q}$ via inklusionen enligt (i) är det $p$-adiska absolutvärdet $|\cdot|_p$,

(iii) $\mathbb{Q}$ ligger tätt i $\mathbb{Q}_p$ med avseende på $|\cdot|_p$,

(iv) $\mathbb{Q}_p$ är cauchyfullständigt med avseende på $|\cdot|_p$.

Kroppen $\mathbb{Q}_p$ är unik upp till en unik ringisomorfi som bevarar absolutvärden.

*Bevis.* Se exempelvis Gouvêa [6, sats 3.2.13]. □

[2] Se exempel D.12 i Appendix.

# 3 Kroppsutvidgningar

Det här kapitlet behandlar kroppsutvidgningar. Vi förklarar hur kroppar kan utvidgas, definierar begreppet splittringskropp, presenterar teori om ändliga kroppar och slutligen betraktar vi en funktion från en kroppsutvidgning till dess ursprungliga kropp som kallas för norm. Särskilt normfunktionen är central i konstruktionen av homogena polynom. Vi vill i senare kapitel använda teorin för att systematiskt konstruera homogena polynom av valfri grad $d$ i $d^2$ variabler med enbart det triviala nollstället. Teorin vi presenterar i det här kapitlet återfinns bland annat i Cohn [3] och Lang [10].

## 3.1 Grundläggande teori om kroppsutvidgningar

Den intuitiva bilden av kroppsutvidgningar är att vi önskar "lägga till" element i den kropp vi betraktar, så att alla kroppsaxiom fortfarande uppfylls. För att förstå oss på kroppsutvidgningar betraktar vi ett känt exempel, nämligen hur vi får de komplexa talen från de reella talen. Polynomet $x^2 + 1$ har inga nollställen i $\mathbb{R}$. Om vi låter $i$ vara en rot till $x^2 + 1$ erhåller vi de komplexa talen från $\mathbb{R}$ genom att utöka $\mathbb{R}$ till en ny kropp som inkluderar $i$.

Vi börjar med att påminna om några relevanta begrepp. Om $K$ är en *delkropp* till en kropp $E$ betraktas $E$ som en kroppsutvidgning av $K$, vanligt skrivet $E/K$. (Notera att $E/K$ här inte betecknar en kvotring och att risken för att förväxla dessa notationer inte är särskilt stor eftersom vi pratar om kroppar, och kroppar har inga kvotringar förutom de triviala.) Kroppen $E$ betraktas som ett vektorrum[3] över $K$ och beroende på dimensionen av vektorrummet säger vi att utvidgningen är ändlig eller oändlig. Dimensionen av vektorrummet $E$ över $K$ benämns *graden* av $E$ över $K$, och betecknas med $[E : K]$.

Om $E/K$ är en ändlig kroppsutvidgning av grad $n$ finns det en bas $u_1, \ldots, u_n \in E$ för $E$ över $K$. Varje element $a \in E$ kan då uttryckas som en unik linjärkombination av baselementen

$$a = \sum_{i=1}^{n} \alpha_i u_i,$$

där $\alpha_i \in K$.

När vi utvidgar en kropp genom att "lägga till" element så att kroppsaxiomen fortfarande är uppfyllda säger vi att vi *adjungerar* element. Låt $K$ vara en kropp, $E$ en kroppsutvidgning av $K$ och $\alpha_1, \alpha_2, \ldots, \alpha_n$ element i $E \setminus K$. Den minsta delkroppen av $E$ innehållande såväl $K$ som $\alpha_1, \ldots, \alpha_n$ betecknas $K(\alpha_1, \ldots, \alpha_n)$. Välj $\beta_1, \ldots, \beta_m$ bland $\alpha_1, \ldots, \alpha_n$ sådana att $1, \beta_1, \ldots, \beta_m$ är $K$-linjärt oberoende. Då är $K(\alpha_1, \ldots, \alpha_n) = K(\beta_1, \ldots, \beta_m)$ och graden $[K(\beta_1, \ldots, \beta_m) : K] = m + 1$. Elementen i $K(\beta_1, \ldots, \beta_m)$ är bråk $\frac{f(\beta_1, \ldots, \beta_m)}{g(\beta_1, \ldots, \beta_m)}$, där $f, g$ är polynom i $m$ variabler med koefficienter i $K$ och där $g(\beta_1, \ldots, \beta_m) \neq 0$. När vi utvidgar $\mathbb{R}$ till $\mathbb{C}$ adjungerar vi ett icke-reellt element för att få hela $\mathbb{C}$, så $[\mathbb{C} : \mathbb{R}] = 2$.

## 3.2 Splittringskroppar

Låt $f$ vara ett polynom över en kropp $K$. Vi vet att $f$ inte alltid har rötter i $K$, till exempel saknar $f$ rötter i $\mathbb{R}$ om $f(x) = x^2 + 1$. Däremot visar vi i det här avsnittet att vi alltid kan hitta en rot till ett polynom över en kropp i en kroppsutvidgning av den ursprungliga kroppen.

**Sats 3.1.** Låt $K$ vara en kropp. Beteckna idealet som genereras av $f \in K[x]$ med $(f(x))$. Då gäller det att $K[x]/(f(x))$ är en kropp om och endast om $f(x)$ är irreducibelt i $K[x]$.

[3] Se definition A.1 i Appendix.

*Bevis.* Antag att $f(x)$ är irreducibelt och låt $I = (f(x))$. Antag att $g(x) + I \neq I$, det vill säga att $g(x) \notin I$, vilket är ekvivalent med att $f(x)$ inte delar $g(x)$. Då är den största gemensamma delaren av $f(x)$ och $g(x)$ ett och därmed finns polynom $h(x), l(x) \in K[x]$ sådana att

$$1 = \gcd(f(x), g(x)) = f(x)h(x) + g(x)l(x).$$

Vidare är $1 - g(x)l(x) = f(x)h(x) \in I$ och $g(x)l(x) + I = 1 + I$, vilket innebär att $(l(x) + I)(g(x) + I) = 1 + I$. Elementet $g(x) + I$ är alltså inverterbart med inversen $l(x) + I$.

Antag nu att $K[x]/I$ är en kropp, att $f(x)$ inte är irreducibelt och att graden av $f(x)$ är större än noll. Vi vill nu härleda en motsägelse. Antagandet innebär att $f(x) = a(x)b(x)$ där $a(x), b(x) \in K[x]$ är av grad större eller lika med ett. Då är $a(x)b(x) + I = I$ och därmed $(a(x) + I)(b(x) + I) = I$ vilket medför att $a(x) + I$ är en nolldelare i $K[x]/I$. Alltså är $K[x]/I$ inte en kropp, vilket motsäger antagandet. Således är satsen bevisad. □

**Sats 3.2.** Låt $K$ vara en kropp och $f(x) \in K[x]$ ett irreducibelt polynom. Då existerar en kropp $L \supseteq K$ sådan att $f$ har ett nollställe i $L$.

*Bevis.* Låt $(f(x)) = I$ och $L = K[x]/I$. Vi vet att $L$ är en kropp och att den innehåller en delkropp som är isomorf med $K$. Låt $f(x) = a_0 + a_1x + \ldots + a_nx^n$ och låt $\alpha$ beteckna elementet $I + x \in L$. Då är

$$\begin{aligned} f(\alpha) &= a_0 + a_1(I + x) + \ldots + a_n(I + x)^n \\ &= I + (a_0 + a_1x + \ldots + a_nx^n) \\ &= I + f(x) \\ &= I \end{aligned}$$

vilket är noll i $L$. □

**Korollarium 3.3.** Låt $f$ vara ett icke-konstant polynom över en kropp $K$. Det finns då en utvidgning $E/K$ där $f$ har en rot.

*Bevis.* Om $f(x)$ är irreducibelt över K ger sats 3.2 att $f(x)$ har en rot i $K[x]/(f(x))$. Om $f(x)$ inte är irreducibelt så har det någon irreducibel faktor $g(x) \in K[x]$ och $f(x) = g(x)h(x)$ för något $h(x) \in K[x]$. Enligt sats 3.2 har $g(x)$ ett nollställe $\alpha$ i $K[x]/(g(x))$, vilket även är ett nollställe till $f(x)$ eftersom $f(\alpha) = g(\alpha)h(\alpha) = 0 \cdot h(\alpha) = 0$. □

Polynomet $x^2 + 1$ är irreducibelt i $\mathbb{R}[x]$, vilket motiverar den algebraiska konstruktionen av de komplexa talen eftersom $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$. Vi ser i korollarium 3.3 att det alltid finns en kroppsutvidgning där ett polynom över en kropp har en rot. Om varje icke-konstant polynom över en kropp $K$ har en rot i $K$ sägs $K$ vara algebraiskt sluten. Algebrans fundamentalsats säger att varje icke-konstant polynom över $\mathbb{C}$ har en rot i $\mathbb{C}$ och därmed är $\mathbb{C}$ algebraiskt sluten. Därmed kan varje icke-konstant polynom över $\mathbb{C}$ skrivas som en produkt av linjära faktorer. Efter den här diskussionen gör vi följande definition.

**Definition 3.4.** Låt $f$ vara ett polynom över en kropp $K$. Antag att $f$ i någon utvidgning $E/K$ kan skrivas som en produkt av linjära faktorer

$$f = a_0(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n), \quad \alpha_1, \ldots, \alpha_n \in E, \quad a_0 \in K, \quad a_0 \neq 0.$$

Vi säger då att $f$ *splittar* över E.

Om $f$ splittar över $E$ men inte över någon mindre utvidgning $E' \subset E$ kallas $E$ splittringskroppen för $f$ över $K$.

*Anmärkning* 3.5. Kroppen $K(\beta_1, \ldots, \beta_m)$ är splittringskroppen för $f$ över $K$ om $E$ är en utvidgning av $K$ och $f = a_0(x - \beta_1)(x - \beta_2)\cdots(x - \beta_m)$ över $E$.

**Exempel 3.6.** De komplexa talen är splittringskroppen över $\mathbb{R}$ för alla polynom över $\mathbb{R}$ med icke-reella rötter eftersom de polynomen kan skrivas som en produkt av linjära faktorer i $\mathbb{C}$.

Notera att ett polynom $f(x) \in K[x]$ alltid har en splittringskropp, nämligen kroppen som genereras av polynomets rötter i en algebraiskt sluten utvidgning av $K$.

## 3.3 Ändliga kroppar

En kropp $K$ som innehar ett ändligt antal element kallas för en ändlig kropp eller en Galoiskropp. Det vanligaste exemplet av ändliga kroppar är $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, där $p$ är något primtal, men det finns fler kroppar av ändlig ordning. Vi ska nu betrakta ändliga kroppar av icke-primtalsordning.

**Sats 3.7.** Ett $k$-dimensionellt vektorrum $V$ över $\mathbb{F}_p$ har $p^k$ element, där $p$ är ett primtal.

*Bevis.* Låt $u_1, \ldots, u_k$ vara en bas för $V$. Då kan varje element $a \in V$ skrivas som en unik linjärkombination på formen $a = \sum_{i=1}^{k} \alpha_i u_i$ där $\alpha_i \in \mathbb{F}_p$. Eftersom varje koefficient kan anta $p$ olika värden får vi att antalet element i $V$ är $p^k$. □

**Definition 3.8.** En kropps *karakteristik* är det minsta positiva heltal $n$ för vilket

$$\sum_{k=1}^{n} 1 = 0.$$

Om summan aldrig blir noll definierar vi karakteristiken till att vara noll.

**Exempel 3.9.** De reella talen har karakteristik noll, ty $\sum_{k=1}^{n} 1 \neq 0$ för alla $n > 0$.

**Sats 3.10.** Karakteristiken av en ändlig kropp är $p$, för något primtal $p$.

*Bevis.* Det är klart att karakteristiken av en ändlig kropp inte är noll, ty om den vore noll skulle ettan ha oändlig ordning. En ändlig grupp, och därmed ändlig kropp, innehar dock inga element av oändlig ordning. Antag nu att karakteristiken inte vore $p$ utan något sammansatt tal $n = ab$. Vi har då att $n \cdot 1 = 0$, så $ab \cdot 1 = 0 = (a \cdot 1)(b \cdot 1) = 0$ men eftersom vi är i en kropp som inte har någon nolldelare är antingen $a \cdot 1 = 0$ eller $b \cdot 1 = 0$, vilket är en motsägelse. En ändlig kropp har alltså ett primtal som karakteristik. □

**Definition 3.11.** En *primkropp* är en kropp som inte innehåller någon äkta delkropp.

**Sats 3.12.** Varje kropp innehåller en unik primkropp.

*Bevis.* Antag att $K$ är en kropp. Låt $E$ vara snittet av alla delkroppar till $K$. Vi vill nu visa att $E$ är en unik primkropp i $K$. För det första ligger 0 och 1 i $E$, eftersom de finns i varje delkropp, så $E$ är icketom. Vidare, om $a, b \in E$ så ligger $a, b \in L$ för varje delkropp $L$ till $K$, vilket gör att även $a + b, a - b, ab$ och $a/b$, det sista givet att $b \neq 0$, ligger i varje $L$ och därmed i $E$. $E$ är alltså en kropp.

Om $L$ skulle vara en äkta delkropp till $E$ skulle $L$ vara en delkropp till $K$ också. Detta motsäger att $E$ är snittet av alla delkroppar till $K$, eftersom snittet ligger i varje delkropp. Alltså är $E$ en primkropp.

Slutligen, antag att $E'$ är en annan primkropp i $K$. Vi får då av konstruktionen av $E$ att $E \subseteq E'$ men eftersom $E'$ är en primkropp måste $E' = E$. □

**Sats 3.13.** Låt $F$ vara en ändlig kropp av karakteristik $p$. Då är primkroppen $E$ i $F$ isomorf med $\mathbb{F}_p$.

*Bevis.* Definiera $\phi : \mathbb{Z} \to F$ där $\phi(n) = n \cdot 1_F$. Eftersom $F$ har karakteristik $p$ är $\ker \phi = p\mathbb{Z}$. Den fundamentala homomorfisatsen för grupper ger då att bilden av $\phi$ är isomorf med $\mathbb{F}_p$, vilket är en primkropp och från sats 3.12 får vi då att $\mathbb{F}_p$ är den unika primkroppen i $F$. □

Låt $F$ vara en ändlig kropp. Från de tre föregående satserna följer det att karakteristiken av $F$ är $p$, där $p$ är ett primtal, och primkroppen i $F$ är isomorf med $\mathbb{F}_p$. Eftersom $F$ är en ändlig kropp är även graden av utvidgningen av $F$ över $\mathbb{F}_p$ ändlig, vilket gör att $F$ är ett ändligtdimensionellt vektorrum över $\mathbb{F}_p$, säg av grad $k$. Enligt sats 3.7 vet vi att antalet element i $F$ är $p^k$. Antalet element i en ändlig kropp är alltså en primpotens, $p^k$, där $p$ är kroppens karakteristik.

**Lemma 3.14.** I en ändlig kropp $F$ av ordning $q = p^k$ uppfyller varje element $a \in F$ ekvationen $a^q = a$.

*Bevis.* Om $a = 0$ är $a^q = a$, antag därför att $a \neq 0$. Alla nollskilda element i $F$ bildar en multiplikativ grupp, $F^\times$, av ordning $q - 1$. För en ändlig grupp $G$ gäller, enligt Lagranges sats, att $a^{|G|} = 1_G$ för alla $a \in G$, så vi får att alla $a \in F^\times$ uppfyller $a^{q-1} = 1$, och om vi multiplicerar med $a$ får vi precis $a^q = a$. □

Lemma 3.14 visar att samtliga element i $F$ är rötter till polynomet $x^q - x$. Vi vet också att polynomet som mest kan ha $q$ rötter i någon kropp, vilket medför att varje element är en distinkt rot. Vi kan alltså skriva

$$x^q - x = (x - a_1)(x - a_2) \cdots (x - a_q), \quad a_1, \ldots, a_q \in F.$$

En ändlig kropp $F$ av ordning $q = p^k$ är alltså splittringskroppen för $x^q - x$ över $\mathbb{F}_p$. Vi ser att $F$ är bestämd av sin ordning upp till isomorfi. Alltså, för något heltal $q$ finns det högst en kropp av ordning $q$, där $q$ är en primpotens. Omvänt gäller att om $q = p^k$, där $p$ är ett primtal, existerar det en kropp av ordning $q$, nämligen splittringskroppen för $x^q - x$ över $\mathbb{F}_p$.

För att visa att splittringskroppen av $x^q - x$ över $\mathbb{F}_p$ består av exakt de $q$ elementen som är rötter till $x^q - x$ betraktar vi följande beräkningar. Låt $a$ och $b$ beteckna två rötter, då gäller det att

$$(a + b)^q - (a + b) = a^q + b^q - a - b = 0$$

eftersom binomialsatsen medför att varje binomialkoefficient förutom första och sista är en multipel av $p$ i en kropp av karakteristik $p$, så $a + b$ är också en rot. Dessutom är

$$(ab)^q - ab = a^q b^q - ab = ab - ab = 0$$

så även $ab$ är en rot. Om $b \neq 0$ så gäller det att

$$(b^{-1})^q - b^{-1} = (b^q)^{-1} - b^{-1} = 0$$

så $b^{-1}$ är en rot. Vidare har vi att

$$(-b)^q - (-b) = (-1)^q b^q + b.$$

Om $p$ är udda så är $(-1)^q = -1$, där $q = p^k$, och $-b$ är en rot. Om $p$ är jämnt är $-b \equiv b \bmod 2$ också en rot eftersom $-1 \equiv 1 \bmod 2$. Slutligen konstaterar vi även att 0 och 1 alltid är rötter till polynomet och därmed en del av splittringskroppen.

För att explicit konstruera ändliga kroppar av icke-primtalsordning, säg $q = p^k$, utgår vi från en kropp $F$ med ordning $p$, där $p$ är ett primtal. Först väljer vi ett irreducibelt polynom, $f \in F[X]$

av grad $k$. Därefter bildar vi kvotringen $F[x]/(f(x))$. Då får vi en kropp av ordning $q$, som brukar betecknas $\mathbb{F}_q$.

Vi visar med ett exempel:

**Exempel 3.15.** Polynomet $x^2 + x + 1$ är irreducibelt i $\mathbb{F}_2[x]$. Vi får därmed kroppen av ordning $4 = 2^2$ genom att bilda kvotringen

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1).$$

Låt $\alpha$ beteckna en rot till $x^2 + x + 1$. Elementen i $\mathbb{F}_4$ är då $\{0, 1, \alpha, \alpha + 1\}$. Eftersom det i $\mathbb{F}_4$ gäller att $\alpha^2 + \alpha + 1 = 0$, vilket är ekvivalent med att $\alpha^2 = -\alpha - 1 = \alpha + 1$, erhåller vi följande additions- och multiplikationstabeller:

| $\oplus$ | $0$ | $1$ | $\alpha$ | $1+\alpha$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\alpha$ | $1+\alpha$ |
| $1$ | $1$ | $0$ | $1+\alpha$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $1+\alpha$ | $0$ | $1$ |
| $1+\alpha$ | $1+\alpha$ | $\alpha$ | $1$ | $0$ |

Tabell 1: Additionstabell för kroppen $\mathbb{F}_4$.

| $\otimes$ | $0$ | $1$ | $\alpha$ | $1+\alpha$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\alpha$ | $1+\alpha$ |
| $\alpha$ | $0$ | $\alpha$ | $1+\alpha$ | $1$ |
| $1+\alpha$ | $0$ | $1+\alpha$ | $1$ | $\alpha$ |

Tabell 2: Multiplikationstabell för kroppen $\mathbb{F}_4$.

## 3.4 Norm

I det här avsnittet ska vi betrakta en funktion $N_{L/K} : L \to K$, där $L/K$ är en ändlig kroppsutvidgning, som kallas för *norm*. Teorin i det här avsnittet återfinns bland annat i Conrad [4].

**Definition 3.16.** Låt $V$ vara ett $n$-dimensionellt vektorrum över kroppen $K$ och låt $\varphi : V \to V$ vara en endomorfi. För en bas $\mathcal{B} = \{e_1, ..., e_n\}$ till $V$ låt $\varphi(e_j) = \sum_{i=1}^{n} a_{ij} e_i$, där $a_{ij} \in K$. Matrisen $[\varphi] := (a_{ij})$ sägs vara representationsmatrisen för $\varphi$ med avseende på basen $\mathcal{B}$.

*Anmärkning* 3.17. Om vi väljer en annan bas för $V$ ändras i allmänhet representationsmatrisen, men den är similär med den första matrisen och similära matriser har samma determinant.

Låt nu $L/K$ vara en ändlig kroppsutvidgning. Det finns då för varje element $\beta \in L$ en K-linjär avbildning $m_\beta : L \to L$ där $m_\beta(x) = \beta x$, för $x \in L$. Genom att välja en bas för $L$ som vektorrum över $K$ kan vi skapa en representationsmatris till $m_\beta$, vilken betecknas $[m_\beta]$.

**Exempel 3.18.** Låt $K = \mathbb{R}, L = \mathbb{C}$ och låt $\{1, i\}$ vara en bas för $\mathbb{C}$ över $\mathbb{R}$. Låt $\beta = a + bi$ där $a, b \in \mathbb{R}$. Multiplicerar vi nu $\beta$ med baselementen får vi

$$\beta \cdot 1 = a \cdot 1 + bi \cdot 1$$

$$\beta \cdot i = -b \cdot 1 + a \cdot i.$$

Representationsmatrisen blir då

$$[m_\beta] = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

**Exempel 3.19.** Låt $K = \mathbb{F}_2$ och $L = \mathbb{F}_4$ som i exempel 3.15. Låt vidare $\{1, \alpha\}$ vara en bas för $\mathbb{F}_4$ över $\mathbb{F}_2$. Låt $\gamma = a + b\alpha$ där $a, b \in \mathbb{F}_2$. Eftersom $\alpha^2 = \alpha + 1$ i $\mathbb{F}_4$ får vi, när vi multiplicerar $\gamma$ med baselementen,

$$\gamma \cdot 1 = a \cdot 1 + b\alpha \cdot 1,$$

och

$$\begin{aligned} \gamma \cdot \alpha &= a \cdot \alpha + b\alpha \cdot \alpha \\ &= a \cdot \alpha + b \cdot \alpha^2 \\ &= a \cdot \alpha + b \cdot (\alpha + 1) \\ &= b + (a + b) \cdot \alpha. \end{aligned}$$

Representationsmatrisen blir då

$$[m_\gamma] = \begin{pmatrix} a & b \\ b & a + b \end{pmatrix}.$$

**Definition 3.20.** *Normen* för $\beta$ från $L$ till $K$ är determinanten av en representationsmatris för den $K$-linjära avbildningen $m_\beta$:

$$N_{L/K}(\beta) = \det([m_\beta]) \in K.$$

**Exempel 3.21.** Betraktar vi exempel 3.18 ser vi att normen för $\beta = a + bi$ är

$$N_{L/K}(\beta) = \det([m_\beta]) = a^2 + b^2.$$

**Exempel 3.22.** Betraktar vi exempel 3.19 ser vi att normen för $\gamma = a + b\alpha$ är

$$N_{L/K}(\gamma) = \det([m_\gamma]) = a^2 + ab - b^2.$$

**Sats 3.23.** Det gäller att $N_{L/K}(\beta) = 0$ om och endast om $\beta = 0$.

*Bevis.* Om $\beta = 0$ är $[m_\beta]$ nollmatrisen och därmed är $\det([m_\beta]) = 0$.

Om $L$ är en kroppsutvidgning av $K$ med $[L : K] = n$ så gäller det att $L$ och $K^n$ är isomorfa som vektorrum. Dessutom är multiplikation med $\beta \neq 0$ en isomorfi från $L$ till $L$. Vi ska visa att då $\beta \neq 0$ är $\det([m_\beta]) \neq 0$. Antag att $\beta \neq 0$. Betrakta det kommutativa diagrammet

$$\begin{array}{ccc} L & \xrightarrow{m_\beta} & L \\ {\scriptstyle \gamma_1}\uparrow & & \downarrow{\scriptstyle \gamma_2} \\ K^n & \xrightarrow{[m_\beta]} & K^n \end{array}$$

där $\gamma_1$ och $\gamma_2$ är isomorfier. Eftersom $m_\beta$ är en isomorfi är sammansättningen $\gamma_2 \circ m_\beta \circ \gamma_1$ en isomorfi från $K^n$ till $K^n$. Sammansättningen motsvarar den linjära avbildningen $[m_\beta]$, vilken endast är en isomorfi då $\det([m_\beta]) \neq 0$. Alltså, $\beta \neq 0$ medför att $\det([m_\beta]) \neq 0$.

□

# 4 Motivering av Artins förmodan

Vi ska i det här kapitlet med hjälp av teorin vi nu har presenterat härleda ett systematiskt sätt att konstruera homogena polynom av valfri grad $d$ i $d^2$ variabler med enbart det triviala nollstället på ett liknande sätt som Mordell [14]. På så vis motiverar vi formuleringen av Artins förmodan.

Vi börjar med att definiera vad som menas med ett homogent polynom av grad $d$ och påminner om Artins förmodan.

**Definition 4.1.** Låt $K$ vara en kropp. Ett homogent polynom i $n$ variabler av grad $d$ över $K$ är en linjärkombination av monom av grad $d$, alltså

$$F(x_1, x_2, \ldots, x_n) = \sum_{k=1}^{m} c_k \prod_{j=1}^{n} x_j^{r_{k,j}}, \quad c_k \in K \text{ och } r_{k,j} \in \mathbb{Z}$$

med homogenitetskravet

$$\sum_{j=1}^{n} r_{k,j} = d \quad \forall k.$$

**Exempel 4.2.** Polynomet $5x^2y^3z - 3x^5y + 2xyz^4$ är homogent, eftersom summan av potenserna i varje term är lika. Polynomet $3x^2y^4 - 6xyz^5$ är *inte* homogent eftersom summan av potenserna i varje term är olika.

**Artins förmodan:** Låt $F(x_1, \ldots, x_n)$ vara ett homogent polynom av grad $d$ med koefficienter i $\mathbb{Q}_p$. Ekvationen $F(x_1, \ldots, x_n) = 0$ har en icke-trivial lösning i $\mathbb{Q}_p$ om $n$ är större än $d^2$.

För att konstruera homogena polynom med enbart det triviala nollstället i $\mathbb{Z}_p$ (och därmed även i $\mathbb{Q}_p$) ska vi använda oss av normen i definition 3.20. Låt oss börja med att betrakta ett konkret exempel då $p = 2$.

**Exempel 4.3.** Vi betraktar den ändliga kroppen $\mathbb{F}_4$ som är en utvidgning av $\mathbb{Z}/2\mathbb{Z}$ vilket diskuterades i exempel 3.15. Polynomet $a^2 + ab - b^2$ som fås av normen i exempel 3.22 har bara det triviala nollstället i $\mathbb{Z}/2\mathbb{Z}$. Låt nu $f(a, b) = a^2 + ab - b^2$ och låt $F(a, b, c, d) = f(a, b) + 2f(c, d)$. Då gäller det att $F$ är ett homogent polynom av grad två i fyra variabler som vi ska se enbart har den triviala lösningen i $\mathbb{Z}_2$. Vi betraktar polynomet $F$ över $\mathbb{Z}/2^n\mathbb{Z}$ med successivt växande $n$.

Antag att $F(a, b, c, d) = 0$. Det gäller att $F(a, b, c, d) \equiv f(a, b) \mod 2$. Enligt sats 3.23 gäller det att $f(a, b) \equiv 0 \mod 2$ om och endast om $a \equiv 0 \mod 2$ och $b \equiv 0 \mod 2$. Då är alltså $a = 2a'$ och $b = 2b'$ för några $a', b'$. Det följer att

$$f(a, b) = (2a')^2 + (2a')(2b') - (2b')^2 = 4a'^2 + 4a'b' - 4b'^2.$$

Således är $f(a, b) = 4f(a', b')$.

Betrakta nu $F(a, b, c, d) = 4f(a', b') + 2f(c, d)$ modulo $2^2$. Det gäller att $4f(a', b') + 2f(c, d) \equiv 0 \mod 4$ är ekvivalent med att $f(c, d) \equiv 0 \mod 2$. På samma sätt som tidigare får vi att $c \equiv d \equiv 0 \mod 2$ och att $f(c, d) = 4f(c', d')$, där $2c' = c$ och $2d' = d$.

Vi forsätter på samma sätt ad infinitum och erhåller då att $a \equiv b \equiv c \equiv d \equiv 0 \mod 2^n$, för alla $n$. Då den triviala lösningen är den enda lösningen i $\mathbb{Z}/2^n\mathbb{Z}$ för alla $n$ så är det även den enda lösningen i $\mathbb{Z}_2$. Vi har alltså konstruerat ett homogent polynom av grad två i fyra variabler som enbart har den triviala lösningen.

Låt oss nu generalisera föregående exempel. Eftersom det existerar en kroppsutvidgning av $\mathbb{Z}/p\mathbb{Z}$ av varje grad $d > 1$, för alla $p$, konstruerar vi polynom över $\mathbb{Z}/p\mathbb{Z}$ av varje grad $d$ med $d^2$ variabler som bara har det triviala nollstället med samma metod som i exempel 4.3. Mer explicit låter vi $f(\mathbf{x}_1)$, där $\mathbf{x}_1 = (x_{1,1}, \ldots, x_{1,d})$, beteckna det polynom vi får av att beräkna normen av ett element $(x_{1,1}, \ldots, x_{1,d}) \in \mathbb{F}_{p^d}$, där $\mathbb{F}_{p^d}$ är en kroppsutvidgning av $\mathbb{F}_p$. Polynomet är homogent och har enligt sats 3.23 enbart det triviala nollstället i $\mathbb{Z}/p\mathbb{Z}$. Låt nu

$$F(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d) = f(\mathbf{x}_1) + p \cdot f(\mathbf{x}_2) + \cdots + p^{d-1} \cdot f(\mathbf{x}_d), \tag{3}$$

Då är $F$ ett homogent polynom av grad $d$ i $d^2$ variabler.

Vi ska härleda en motsägelse och för att göra det antar vi att det finns en icke-trivial lösning till $F(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d) = 0$ i $\mathbb{Z}_p$. Om alla $x_{i,j}$ är delbara med $p$ är $x_{i,j} = p \cdot y_{i,j}$ för något $y_{i,j}$ och $F(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d) = p^d F(\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_d)$. Om alla $y_{i,j}$ är delbara med $p$ kan vi upprepa föregående argument och till slut kommer vi ha en lösning där någon koordinat inte är delbar med $p$, eftersom enbart noll är oändligt delbar med $p$. Det existerar alltså en lösning där något $x_{i,j}$ inte är delbart med $p$.

Vi har således enligt vårt antagande en icke-trivial lösning till $F(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d) = 0$ där någon koordinat inte är delbar med $p$. Det gäller att $F(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d) \equiv f(\mathbf{x}_1) \mod p$. Emellertid vet vi från sats 3.23 att $f(\mathbf{x}_1) \equiv 0 \mod p$ om och endast om $x_{1,1} \equiv x_{1,2} \equiv \ldots \equiv x_{1,d} \equiv 0 \mod p$, så $x_{1,i} = p \cdot y_{1,i}$ för några $y_{1,i}$. Således är $f(\mathbf{x}_1) = p^d f(\mathbf{y}_1)$ eftersom f är ett homogent polynom av grad $d$.

Betrakta nu ekvationen $p^d f(\mathbf{y}_1) + p \cdot f(\mathbf{x}_2) + \cdots + p^{d-1} \cdot f(\mathbf{x}_d) \equiv 0 \mod p^2$ vilken är ekvivalent med $p^{d-1} f(\mathbf{y}_1) + f(\mathbf{x}_2) + \cdots + p^{d-2} \cdot f(\mathbf{x}_d) \equiv 0 \mod p$. Då är alltså $f(\mathbf{x}_2) \equiv 0 \mod p$ och enligt sats 3.23 gäller det att $x_{2,1} \equiv x_{2,2} \equiv \ldots \equiv x_{2,d} \equiv 0 \mod p$, så $x_{2,i} = p \cdot y_{2,i}$ för några $y_{2,i}$. Således är $f(\mathbf{x}_2) = p^d f(\mathbf{y}_2)$.

Fortsätter vi så här får vi att $x_{1,1} \equiv x_{1,2} \equiv \ldots \equiv x_{1,d} \equiv x_{2,1} \equiv \ldots \equiv x_{2,d} \equiv \ldots \equiv x_{d,d} \equiv 0 \mod p$ och erhåller en motsägelse eftersom vi har antagit att någon koordinat ej är delbar med $p$. Alltså finns det ingen icke-trivial lösning till $F(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d) = 0$.

Precis som i exempel 4.3 är $F(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d)$ alltså ett homogent polynom i $d^2$ variabler av grad $d$ som endast har det triviala nollstället i $\mathbb{Z}_p$.

Det existerar således polynom av varje grad $d$ i $d^2$ variabler med enbart det triviala nollstället, polynomet i ekvation (3) är ett sådant. Det är därmed klart att antagandet i Artins förmodan om att variabelantalet ska vara strikt större än $d^2$ är nödvändigt för att det garanterat ska existera en icke-trivial lösning.

# 5 Ett motexempel till Artins förmodan

Precis som vi nämnde i inledningen motbevisade Terjanian [18] Artins förmodan genom att konstruera ett homogent polynom i 18 variabler av grad fyra. Vi ska i det här kapitlet återge och förklara Terjanians motbevis.

Om vi låter

$$G(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3^4 - (x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2) - x_1x_2x_3(x_1 + x_2 + x_3)$$

och sätter

$$\begin{aligned} F(x_1, \ldots, x_{18}) = {} & G(x_1, x_2, x_3) + G(x_4, x_5, x_6) + G(x_7, x_8, x_9) \\ & + 4G(x_{10}, x_{11}, x_{12}) + 4G(x_{13}, x_{14}, x_{15}) + 4G(x_{16}, x_{17}, x_{18}), \end{aligned}$$

så är $F$ ett homogent polynom i 18 variabler av grad fyra som vi ska visa enbart har den triviala lösningen i $\mathbb{Q}_2$. För att visa det använder vi en liknande metod som i föregående kapitel.

Eftersom $\mathbb{Z}/4\mathbb{Z}$ är ändlig observerar vi efter beräkningar att

$$G(x_1, x_2, x_3) \equiv 1 \bmod 4 \text{ eller så är } G(x_1, x_2, x_3) \equiv 0 \bmod 4.$$

Dessutom gäller det att

$$G(x_1, x_2, x_3) \equiv 0 \bmod 4 \text{ om och endast om } x_1 \equiv x_2 \equiv x_3 \equiv 0 \bmod 2.$$

Eftersom $G(x_1, x_2, x_3)$ antingen är kongruent med 0 eller 1 modulo 4 är summan $G(x_1, x_2, x_3) + G(x_4, x_5, x_6) + G(x_7, x_8, x_9)$ bara kongruent med noll modulo fyra om varje term för sig är kongruent med noll. Det följer därför att $G(x_1, x_2, x_3) + G(x_4, x_5, x_6) + G(x_7, x_8, x_9) \equiv 0 \bmod 4$ om och endast om $x_1 \equiv \ldots \equiv x_9 \equiv 0 \bmod 2$.

Alltså kan varje $x_i$ skrivas som $2y_i$ för något $y_i$, där $i = 1, \ldots, 9$. Det gäller då att

$$G(x_1, x_2, x_3) + G(x_4, x_5, x_6) + G(x_7, x_8, x_9) = 16(G(y_1, y_2, y_3) + G(y_4, y_5, y_6) + G(y_7, y_8, y_9)).$$

Om vi nu betraktar ekvationen

$$\begin{aligned} & 16(G(y_1, y_2, y_3) + G(y_4, y_5, y_6) + G(y_7, y_8, y_9)) \\ & +4(G(x_{10}, x_{11}, x_{12}) + G(x_{13}, x_{14}, x_{15}) + G(x_{16}, x_{17}, x_{18})) \equiv 0 \bmod 16 \end{aligned}$$

och använder samma metod som i föregående kapitel får vi att $x_{10} \equiv \ldots \equiv x_{18} \equiv 0 \bmod 2$. Vi fortsätter på samma sätt och får då att $x_i$ är oändligt delbar med 2 för alla $i$. Därmed följer det att $F(x_1, \ldots, x_{18}) = 0$ om och endast om $x_1 = \ldots = x_{18} = 0$. Således är $F$ ett homogent polynom i 18 variabler av grad fyra med enbart den triviala lösningen, vilket motsäger Artins förmodan.

# 6 Bevis av Artins förmodan för kubiska homogena polynom

I det här kapitlet presenterar vi ett bevis av Artins förmodan för kubiska homogena polynom, vilket är ett av huvudmålen med arbetet. Närmare bestämt ska vi bevisa följande sats:

**Sats 6.1.** Varje kubisk homogen polynomekvation i $n$ variabler med koefficienter i $\mathbb{Q}_p$ har en icke-trivial lösning i $\mathbb{Q}_p$ då $n \geq 10$.

Lewis [11] formulerar satsen mer allmänt, men vi återger huvuddragen av Lewis bevis i specialfallet ovan. Hädanefter betecknar $F(X)$ ett kubiskt homogent polynom med koefficienter i $\mathbb{Z}_p$.

## 6.1 Inför beviset

I det här avsnittet presenterar vi teori som vi i nästa avsnitt använder i beviset av satsen.

Vi börjar med att betrakta $\mathbb{Z}_p^n = \prod_{k=1}^{n} \mathbb{Z}_p$ och formulerar två definitioner.

**Definition 6.2.** En vektor $X \in \mathbb{Z}_p^n$ sägs vara primitiv om minst en koordinat i $X$ är inverterbar.

*Anmärkning* 6.3. De inverterbara elementen i $\mathbb{Z}_p$ är alla tal $x$ sådana att $|x|_p = 1$, alltså alla $x$ som inte delas av $p$, se korollarium C.4 i Appendix.

**Definition 6.4.** För $X = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ är $||X||_{\max} := \max_i\{|x_i|_p\}$, där $i = 1, \ldots, n$.

Antag nu att $F(X) = 0$ endast har den triviala lösningen i $\mathbb{Q}_p$. Välj $m \in \mathbb{Z}$ sådant att det är det minsta positiva heltal för vilket $F(A) \not\equiv 0 \bmod p^m$ för alla primitiva vektorer $A$. Ett sådant $m$ existerar, vilket vi nu ska visa.

Antag att det inte existerar ett sådant $m$. Då finns det en följd av vektorer $\{A_i\}$, för $i = 1, 2, \ldots$, sådana att $F(A_i) \equiv 0 \bmod p^i$ för alla $i$. Vi visar i sats D.28 i Appendix att $\mathbb{Z}_p$ är kompakt och därmed existerar det en konvergent delföljd till $\{A_i\}$. Säg att delföljden konvergerar mot vektorn $A$. Eftersom någon koordinat i varje $A_i$ inte är delbar med $p$ så är $||A_i||_{\max} = 1$ för alla $i$. Om $A$ inte är primitiv så är $||A_i - A||_{\max} \geq 1 - \frac{1}{p}$ och därmed konvergerar delföljden inte mot $A$. Således är $A$ en primitiv vektor. Vi har då att $F(A) = 0$, vilket är en motsägelse till att $F(X) = 0$ endast har den triviala lösningen.

Vi ska nu välja en bas till $\mathbb{Z}_p^n$ på ett specifikt sätt. Betrakta en godtycklig bas $\{E_1, \ldots, E_n\}$ till $\mathbb{Z}_p^n$. Låt $N_i$ beteckna antalet basvektorer $E_k$ med de två egenskaperna

$$F(E_k) \equiv 0 \bmod p^i, \qquad F(E_k) \not\equiv 0 \bmod p^{i+1}. \tag{4}$$

Eftersom basvektorerna är primitiva behöver vi bara ta hänsyn till värden på $i$ som är mindre än $m$, på grund av hur vi har valt $m$.

Utav alla möjliga baser till $\mathbb{Z}_p^n$ väljer vi en bas där följande regel gäller:

$$\begin{aligned} &\text{(i) } N_{m-1} \text{ är maximal.} \\ &\text{(ii) Efter att vi har valt } N_{m-1} \text{ enligt (i) är } N_{m-2} \text{ maximal.} \\ &\text{(iii) Efter att vi har valt } N_{m-1} \text{ och } N_{m-2} \text{ enligt (ii) är } N_{m-3} \text{ maximal.} \\ &\quad\vdots \end{aligned} \tag{5}$$

Alltså, vi väljer först ut så många linjärt oberoende basvektorer som möjligt som uppfyller (4) då $i = m-1$. För de här basvektorerna, $E_k$, gäller det även att $F(E_k) \equiv 0 \mod p^{m-2}$, men eftersom de inte uppfyller $F(E_k) \not\equiv 0 \mod p^{m-1}$ räknas de inte igen i steg (ii). Däremot kan det finnas andra basvektorer som uppfyller (4) då $i = m-2$ vilka räknas i steg (ii). Vi fortsätter sedan på samma sätt tills $n$ basvektorer är valda.

Från vår definition av $N_i$ och konstanten $m$ följer det alltså att

$$N_0 + N_1 + \cdots + N_{m-1} = n, \qquad N_{m-1} \geq 1, \qquad N_i \geq 0, \text{ för alla } i. \tag{6}$$

För basen vi nu har valt betecknar vi basvektorerna $E_k$ med egenskaperna i (4) med $E_\mu^{(i)}$ där $\mu = 1, 2, \ldots, N_i$. Vi har alltså

$$F(E_\mu^{(i)}) \equiv 0 \mod p^i, \qquad F(E_\mu^{(i)}) \not\equiv 0 \mod p^{i+1},$$
$$i = 0, 1, \ldots, m-1, \qquad \mu = 1, 2, \ldots, N_i.$$

Från linjär algebra är det känt att givet en bas $\{E_1, \ldots, E_n\}$ kan vektorn $V$ skrivas som

$$V = \sum_{i=1}^{n} v_i E_i.$$

Låt nu $x_\mu^{(i)}$ beteckna koordinaten som är koefficienten till $E_\mu^{(i)}$.

Vi formulerar nu två lemman samt Chevalleys sats som är viktiga för det kommande beviset.

**Lemma 6.5.** Låt $F(X)$ vara ett kubiskt homogent polynom med koefficienter i $\mathbb{Z}_p$. Antag att $F(X) = 0$ bara har den triviala lösningen i $\mathbb{Q}_p$. Låt $q$ vara antingen $0, 1$ eller $2$. Låt $s \in \mathbb{Z}_{\geq 0}$ och sätt

$$\begin{aligned} x_\mu^{(3j+q)} &= p^{s-j} y_\mu^{(3j+q)} && \text{om } 0 \leq j \leq s, \\ x_\mu^{(3j+q)} &= y^{(3j+q)} && \text{om } j > s, \\ x_\mu^{i} &= 0 && \text{om } i \not\equiv q \mod 3 \end{aligned} \tag{7}$$

(I) Då blir $F(X)$ ett polynom i $Y$ där alla koefficienter är delbara med $p^{3s+q}$, och kan alltså skrivas

$$F(X) = p^{3s+q} H(Y).$$

(II) Om $X_1$ och $X_2$ är två vektorer vars koordinater kan skrivas på formen (7) där $y_\mu$ är ett $p$-adiskt heltal, och om de båda har samma $y_\mu^{(3j+q)}$, där $0 \leq j \leq s$, så är

$$F(X_1) \equiv F(X_2) \mod p^{3s+q+1}.$$

*Bevis.* För bevis, se lemma 3 i Lewis [11]. □

En variabel sägs *förekomma explicit* i ett polynom $F(X)$ om den finns i någon av termerna i $F(X)$ som har en nollskild koefficient. Vidare säger vi att en lösning $X$ är singulär om $F(X) = 0$ och $\frac{\partial F(X)}{\partial x_i} = 0$ för alla $i$.

**Lemma 6.6.** Låt $F(X)$ vara ett kubiskt homogent polynom med koefficienter i en ändlig kropp $\mathbb{F}$ sådant att $F(X) = 0$ som mest har singulära lösningar i $\mathbb{F}$. Då förekommer antingen variabeln $x_i$ inte explicit i $F(X)$ eller så har termen $x_i^3$ en nollskild koefficient i $F(X)$.

*Bevis.* För bevis, se lemma 2 i Lewis [11]. □

**Sats 6.7 (Chevalleys sats).** Låt $\mathbb{F}$ vara en ändlig kropp med karakteristik $p$. Om $f(x_1, \ldots, x_n)$ är ett polynom av grad $d$ över $\mathbb{F}$ och $n > d$ så gäller det att antalet nollställen till $f(x_1, \ldots, x_n)$ i $\mathbb{F}$ är en multipel av $p$. Speciellt gäller det att om $f(x_1, \ldots, x_n)$ är ett homogent polynom så har $f(x_1, \ldots, x_n)$ minst en icke-trivial lösning i $\mathbb{F}$.

*Bevis.* Se Ireland och Rosen [9, s. 143]. □

## 6.2 Bevis

Efter föregående avsnitt är vi nu redo att ge beviset.

**Sats 6.1.** Varje kubisk homogen polynomekvation i $n$ variabler med koefficienter i $\mathbb{Q}_p$ har en icke-trivial lösning i $\mathbb{Q}_p$ då $n \geq 10$.

*Bevis.* För att visa satsen gör vi ett kontrapositivt bevis. Vi ska alltså visa att om $F(X) = F(x_1, \ldots, x_n) = 0$ endast har den triviala lösningen i $\mathbb{Q}_p$ så är $n \leq 9$. Antag därför att $F(X) = 0$ endast har den triviala lösningen i $\mathbb{Q}_p$. Välj nu en bas enligt (5). Vi ska visa att[4]

$$\begin{aligned} \mathcal{N}_0 &= N_0 + N_3 + N_6 + \cdots \leq 3, \\ \mathcal{N}_1 &= N_1 + N_4 + N_7 + \cdots \leq 3, \\ \mathcal{N}_2 &= N_2 + N_5 + N_8 + \cdots \leq 3. \end{aligned} \tag{8}$$

Ty om (8) är sann, så medför (6) att $n \leq 9$ och således är satsen bevisad.

Antag att $\mathcal{N}_q \geq 4$ för något $q = 0, 1, 2$. Eftersom $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ (se korollarium D.24) är en ändlig kropp med karakteristik $p$ kan vi använda oss av lemma 6.6 och Chevalleys sats. Lemma 6.6 ger att antingen har $x_i^3$ nollskild koefficient eller så förekommer $x_i$ inte explicit i $F(X)$. Om $x_i$ inte förekommer explicit så kan vi alltid hitta en primitiv vektor $Y$ sådan att $H(Y) \equiv 0 \mod p$, där $H(Y)$ är det homogena polynomet i (I) i lemma 6.5, nämligen en av vektorerna där alla koordinater utom den $i$:te är noll. I fallet då alla $x_i$ förekommer explicit får vi från Chevalleys sats att det finns en primitiv vektor $Y$ sådan att $H(Y) \equiv 0 \mod p$.

Använd nu transformationen (7) på den primitiva vektorn $Y$ som löser ekvationen, med $s = \lfloor \frac{1}{3}(m - q - 1) \rfloor$. Vi får då en vektor $X \in \mathbb{Z}_p^n$ som, då $k = \lfloor \frac{1}{3}(m - q - 1) \rfloor$, uppfyller följande villkor:

(A) Varje $x_\mu^{(3j+q)}$, där $0 \leq j \leq k$ är delbart med $p^{k-j}$, men något $x_\mu^{(3j+q)}$ är inte delbart med $p^{k-j+1}$.

(B) $x_\mu^{(3j+q)} = 0$ om $j > k$.

(C) $x_\mu^i = 0$ om $i \not\equiv q \bmod 3$.

(D) $F(X) \equiv 0 \bmod p^{3k+q+1}$.

Att varje $x_\mu^{(3j+q)}$ är delbart med $p^{k-j}$ i villkor (A) följer av transformationen (7). Att något $x_\mu^{(3j+q)}$ inte är delbart med $p^{k-j+1}$ följer av att $Y$ är primitiv. Vektorn $X$ uppfyller villkor (B) på grund av transformationen (7) och (II) i lemma 6.5. Villkor (C) följer direkt av transformationen (7) och villkor (D) följer av att $H(Y) \equiv 0 \bmod p$ och (I) i lemma 6.5.

Existensen av en sådan vektor $X$ är dock en motsägelse till valet av basen, vilket vi nu ska visa.

För att visa motsägelsen börjar vi med att anta att ett sådant $X$ existerar. Om någon av $x_\mu^{(3k+q)}$ inte är delbar med $p$ så kan vi byta $E_\mu^{(3k+q)}$ mot $X$ och fortfarande ha en bas. Villkoret att alla $x_\mu^{(3k+q)}$ inte är delbara med $p$ krävs, ty annars är $X$ ej primitiv och kan därmed inte vara en basvektor. Vidare har vi fortfarande en bas, ty säg att vi har en vektor $v$ i något vektorrum där $\{b_1, \ldots, b_n\}$ är en bas. Då kan $v$ skrivas som en linjärkombination, säg $v = v_1 b_1 + \ldots + v_n b_n$, där vi kan anta att $v_1 \neq 0$. Då gäller även att $\{v, b_2, \ldots, b_n\}$ är en bas, ty om de var linjärt beroende skulle $v$ vara en linjärkombination av $b_2, \ldots, b_n$ men det medför att $v_1 = 0$ vilket är en motsägelse. Om $v_1$ är inverterbar kan vi dessutom skriva $b_1$ som en linjärkombination av $v, b_2, \ldots, b_n$ och därmed spänner de hela rummet. I vårt fall är något $x_\mu^{(3k+q)}$ inte delbart med $p$ och därmed inverterbart i $\mathbb{Z}_p$, så när vi byter $E_\mu^{(3k+q)}$ mot $X$ erhåller vi en ny bas.

Å ena sidan uppfyller $X$ att $F(X) \equiv 0 \bmod p^{3k+q+1}$ enligt villkor (D). Å andra sidan, enligt definitionen av basen i (4), är $F(E_\mu^{(3k+q)}) \not\equiv 0 \bmod p^{3k+q+1}$. Alltså, när vi ersätter $E_\mu^{(3k+q)}$ med $X$ så ersätter vi en vektor som räknas i $N_{3k+q}$ med en som räknas i $N_{3k+q+\lambda}$, för något $\lambda > 0$.

[4]Notera att det inte är oändliga summor, $N_i$ är bara definierad upp till $i = m - 1$.

Med andra ord, värdet för $N_{3k+q+\lambda}$ blir större än vad det var tidigare. De andra $N_{3k+q+\lambda}$ förblir oförändrade. Att någon $N_{3k+q+\lambda}$ blir större än tidigare är dock en motsägelse mot valet av basen enligt (5) eftersom vi hela tiden väljer $N_i$ maximal med start vid $i = m-1$. Eftersom vi får en motsägelse vet vi att alla $x_\mu^{(3k+q)}$ är delbara med $p$ och alltså är $\frac{1}{p}X = X_1$ en vektor i $\mathbb{Z}_p^n$.

Villkoren (A), (C) och (D) uppfylls även av $X_1$ om vi byter $k$ mot $k-1$. Villkoret (B) behöver inte vara uppfyllt av $X_1$ eftersom $x_\mu^{(3k+q)}$ inte nödvändigtvis är 0. Låt därför $X_2$ vara vektorn som erhålls från $X_1$ genom att sätta $x_\mu^{(3k+q)} = 0$. Eftersom $X_1$ och $X_2$ uppfyller förutsättningarna i påstående (II) i lemma 6.5 med $s = k-1$ medför lemmat att

$$F(X_1) \equiv F(X_2) \bmod p^{3(k-1)+q+1}.$$

Dessutom är $F(X_1) \equiv 0 \bmod p^{3(k-1)+q+1}$ enligt villkor (D) så $X_2$ uppfyller villkoren (A)-(D) med $k$ utbytt mot $k-1$. Upprepad användning av den här metoden visar att det finns någon vektor $X'$ i $\mathbb{Z}_p^n$ som uppfyller (A)-(D) med $k = 0$. Då $k = 0$ kräver villkor (A) att något $x_\mu^{(q)}$ i $X'$ inte är delbart med $p$ och precis som tidigare leder det här till en motsägelse till valet av basen.

Det följer därför att om $F(X) = 0$ endast har den triviala lösningen så är $\mathcal{N}_q \leq 3$ för $q = 0, 1, 2$. Vi får då av (6) att $N_0 + \cdots + N_{m-1} \leq 9$ och satsen är bevisad. □

# Appendix

Vi presenterar här ytterligare teori om de $p$-adiska talen samt påminner om några definitioner och satser som används utan att formellt formuleras i rapporten. Som nämndes i kapitel 2 ger vi här en analytiskt konstruktion av de $p$-adiska talen. Vidare presenterar vi Hensels lemma, visar att $p$-adiska tal kan skrivas som oändliga summor och bevisar att den analytiska och den algebraiska konstruktionen av de $p$-adiska talen ger upphov till isomorfa ringar. Teorin i det här kapitlet återfinns bland annat i Gouvêa [6], Greenberg [7] och Reid [15].

# A Vektorrum och heltalsringar

Vi har tidigare betraktat vektorrum över kroppar och diskuterat valueringsringar i samband med den algebraiska konstruktionen av de $p$-adiska talen, varför vi nu ger de formella definitionerna. Vi börjar med att ge definitionen av ett vektorrum.

**Definition A.1.** Låt $K$ vara en kropp. Ett vektorrum $V$ över $K$ är en icke-tom mängd med två operationer – addition och skalärmultiplikation med element i $K$ – som uppfyller att

1. $V$ är en kommutativ grupp under addition
2. $a(v + w) = av + aw$
3. $(a + b)v = av + bv$
4. $a(bv) = (ab)v$
5. $1v = v$

där $a, b \in K$ och $v, w \in V$.

Vi definierar vidare heltalsringar, valueringsideal och restklasskroppar.

**Definition A.2.** Låt $K$ vara en kropp och $|\cdot|$ ett icke-arkimediskt absolutvärde på $K$. Delringen

$$\mathcal{O} = \{x \in K : |x| \leq 1\} \subseteq K$$

kallas heltalsringen till $K$ med avseende på $|\cdot|$.

Idealet

$$\mathfrak{p} = \{x \in K : |x| < 1\} \subseteq \mathcal{O}$$

kallas valueringsidealet till $K$ med avseende på $|\cdot|$.

Kvotringen $\Bbbk = \mathcal{O}/\mathfrak{p}$ kallas restklasskroppen med avseende på absolutvärdet $|\cdot|$.

*Anmärkning* A.3. Då vi önskar specificera vilken kropp som avses skriver vi $\mathcal{O}_K$, $\mathfrak{p}_K$ och $\Bbbk_K$.

*Anmärkning* A.4. Vissa författare använder notationen

$$\begin{aligned}\mathfrak{o} &= \{x \in K : |x| \leq 1\},\\ \mathfrak{m} &= \{x \in K| : |x| < 1\},\\ \mathfrak{u} &= \mathfrak{o} \setminus \mathfrak{m} = \{x \in K : |x| = 1\}.\end{aligned}$$

Det är förväntat att många algebraiska egenskaper hos absolutvärdet avspeglas i egenskaper hos heltalsringen. Eftersom vi mestadels är intresserade av det $p$-adiska absolutvärdet, låt oss beräkna heltalsringen, valueringsidealet och restklasskroppen till $\mathbb{Q}$ och $\mathbb{Q}_p$ med avseende på $|\cdot|_p$.

**Sats A.5.** Vi har att

$$\begin{aligned} \mathcal{O}_{\mathbb{Q}_p} &= \mathbb{Z}_p & \mathcal{O}_{\mathbb{Q}} &= \mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\} \\ \mathfrak{p}_{\mathbb{Q}_p} &= p\mathbb{Z}_p & \mathfrak{p}_{\mathbb{Q}} &= p\mathbb{Z}_{(p)} \\ \Bbbk_{\mathbb{Q}_p} &= \mathbb{F}_p & \Bbbk_{\mathbb{Q}} &= \mathbb{F}_p. \end{aligned}$$

*Bevis.* Satsen följer från definition A.2 genom att sätta in $\mathbb{Q}$ och $\mathbb{Q}_p$ i definitionen. □

# B Analytisk konstruktion av de $p$-adiska talen

Vi ska i det här avsnittet konstruera de $p$-adiska talen analytiskt. Vi gör konstruktionen genom att använda cauchyföljder, analogt med konstruktionen av $\mathbb{R}$. Vi påminner först om vad som menas med ett metriskt rum samt en cauchyföljd i ett metriskt rum.

**Definition B.1.** Ett metriskt rum är en tupel $(X, d)$ med en mängd $X$ och en funktion $d : X \times X \to \mathbb{R}_{\geq 0}$ sådant att för alla $x, y, z \in X$, så är

1. $d(x, y) \geq 0$,
2. $d(x, y) = d(y, x)$ och $d(x, y) = 0$ om och endast om $x = y$,
3. $d(x, z) \leq d(x, y) + d(y, z)$.

Om varje cauchyföljd i $X$ konvergerar till ett element i $X$ sägs $(X, d)$ utgöra ett fullständigt metriskt rum med avseende på metriken $d$.

Vi väljer att skriva det metriska rummet som $X$, utan att glömma den bakomliggande strukturen.

Det går att se en cauchyföljd som en följd $\{x_n\}_n \subset X$ sådan att $d(x_n, x_m)$ går mot 0 då $n, m \to \infty$. Eller mer formellt:

**Definition B.2.** En cauchyföljd i ett metriskt rum $X$ är en följd $\{x_n\} \subset X$ sådan att för alla $\varepsilon > 0$ existerar ett $N > 0$ sådant att $d(x_n, x_m) < \varepsilon$ för alla $n, m > N$.

**Sats B.3.** Låt $K$ vara en kropp med ett absolutvärde $|\cdot|$. Den kanoniska definitionen $d(x, y) := |x - y|$ inducerar då en metrik på $K$ och $K$ kan då utökas till ett metriskt rum.

*Bevis.* Vi verifierar axiomen för en metrik. Observera först att $d(x, y) = |x - y| \geq 0$ och $d(x, y) = 0$ om och endast om $x - y = 0$. Det senare är ekvivalent med att $d(x, y) = 0$ om och endast om $x = y$. Funktionen $d$ är således strikt positivt definit.

Vidare är $d(x, y) = d(y, x)$ eftersom $d(x, y) = |x - y| = |-(y - x)| = |-1||y - x| = |y - x| = d(y, x)$.

Det återstår nu att visa att $d$ uppfyller triangelolikheten. Tag godtyckliga element $x, y, z \in K$. Vi uppskattar sedan

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

Alltså är $d$ en metrik på kroppen $K$. □

*Anmärkning* B.4. Om $d(x, y) = |x - y|_p$ erhålls den $p$-adiska metriken på $\mathbb{Q}$.

Betrakta nu det $p$-adiska absolutvärdet på $\mathbb{Q}$ och korresponderande metrik. Definiera mängden

$$\mathcal{C}_p := \{\{x_n\}_n : \{x_n\}_n \text{ är en cauchyföljd med avseende på } |\cdot|_p\}$$

och mängden av alla följder i $\mathcal{C}_p$ som konvergerar mot noll

$$\mathcal{N}_p = \{\{x_n\}_n \in \mathcal{C}_p : x_n \to 0 \text{ med avseende på } |\cdot|_p\}.$$

**Sats B.5.** Mängden $\mathcal{C}_p$ med operationerna $(x_n) + (y_n) := (x_n + y_n)$ och $(x_n) \cdot (y_n) := (x_n y_n)$ är en kommutativ ring med en multiplikativ identitet.

*Bevis.* Vi behöver verifiera att $(x_n + y_n)$ och $(x_n y_n)$ är cauchyföljder. Låt $(x_n)$ och $(y_n)$ vara cauchyföljder med $|x_n - x_m| < \varepsilon$ och $|y_n - y_m| < \varepsilon$ för alla $n, m > N$ där $N > 0$. Då gäller

$$|x_n + y_n - (x_m + y_m)| = |x_n - x_m + y_n - y_m| \leq |x_n - x_m| + |y_n - y_m|.$$

Eftersom det antogs att $(x_n)$ och $(y_n)$ båda var cauchyföjder får vi nu att

$$|x_n - x_m| + |y_n - y_m| < 2\varepsilon$$

för alla $n, m \geq N$, så $(x_n + y_n)$ är en cauchyföljd.

På samma sätt verifieras slutenheten under multiplikation. Betrakta uppskattningen

$$|x_n y_n - x_m y_m| = |x_n(y_n - y_m) + y_m(x_n - x_m)| \leq |x_n||y_n - y_m| + |y_m||x_n - x_m|$$

där $|x_n|, |y_n|$ är begränsade och $|x_n - x_m| < \varepsilon, |y_n - y_m| < \varepsilon$ for $n, m \geq N$ för något heltal $N$. Vi ser att högerledet kan göras godtyckligt litet genom att välja $N > 0$ tillräckligt stort, varvid $(x_n) \cdot (y_n)$ utgör en cauchyföljd i $\mathcal{C}_p$.

Kommutativiteten ärvs från motsvarande egenskap hos $\mathbb{Q}$ och den multiplikativa identiteten är den konstanta sekvensen av ettor. □

*Anmärkning* B.6. Mängden $\mathcal{N}_p$ är ett ideal i $\mathcal{C}_p$.

*Anmärkning* B.7. Genom att identifiera $q \in \mathbb{Q}$ med den konstanta följden $(q, q, q, \ldots)$ ser vi att $\mathbb{Q}$ är en delmängd i $\mathcal{C}_p$ . Vidare kan vi observera att $\mathcal{C}_p$ har nolldelare, ty

$$(0, p, 0, p^2, 0, \ldots) \cdot (p, 0, p^2, 0, p^3, \ldots) = (0, 0, 0, 0, \ldots).$$

Vi ska utöka $\mathbb{Q}$ till en fullständig kropp och följande lemma används för att bevisa att $\mathcal{N}_p$ är ett maximalt ideal i $\mathcal{C}_p$.

**Lemma B.8.** En följd $\{x_n\}_n$ är en cauchyföljd med avseende på ett icke-arkimediskt absolutvärde $|\cdot|$ om och endast om $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.

*Bevis.* Antag att $\{x_n\}_n$ är en cauchyföljd. Implikationen åt höger följer då omedelbart.

För att bevisa implikationen åt andra hållet, antag att $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$ och låt $m = n + r > n$. Då får vi

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \ldots - x_n| \\ &\leq \max\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \ldots, |x_{n+1} - x_n|\} \end{aligned}$$

eftersom $|\cdot|$ är icke-arkimediskt, så $|x_m - x_n| \to 0$ om $|x_{n+1} - x_n| \to 0$. □

*Anmärkning* B.9. Lemma B.8 gäller inte för arkimediska absolutvärden. Låt $|\cdot|$ vara det vanliga absolutbeloppet. Exempelvis uppfyller då partialsummorna av den harmoniska serien $x_n = \sum_{k=1}^{n} \frac{1}{k}$ att $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$, men serien $\sum_{k=1}^{\infty} \frac{1}{k}$ är divergent.

*Anmärkning* B.10. Lemma B.8 medför även att följder $\{x_n\}_n$ på formen $x_n = \sum_{k=0}^{n} a^k p^k$, där $0 \leq a_k \leq p-1$ är cauchyföljder i $\mathbb{Q}_p$.

De $p$-adiska talen definieras analytiskt genom att bilda kvotringen $\mathcal{C}_p/\mathcal{N}_p$. I de kommande satserna visar vi därför att om $R$ är en kommutativ ring med multiplikativ identitet och $I$ är ett maximalt ideal så är $R/I$ en kropp. Dessutom visar vi att $\mathcal{N}_p$ är ett maximalt ideal.

**Sats B.11.** Ett ideal $M \subseteq A$, där $A$ är en kommutativ ring med en multiplikativ identitet, är maximalt om och endast om $A/M$ är en kropp.

*Bevis.* Antag först att $A/M$ är en kropp och att $I$ är ett ideal som har $M$ som äkta delmängd. Betrakta ett element $a \in I, a \notin M$. Då är $a + M \neq M$. Eftersom $A/M$ är en kropp så existerar något $b \in A$ sådant att $(a + M) \cdot (b + M) = 1 + M$.

Därmed är $m = ab - 1 \in M$ Men det medför att $1 \in I$, ty $ab - m = 1$ och $ab \in I$ och $m \in M \subset I$. Vi observerar att $I = A$, och alltså är $M$ maximal.

Antag nu omvändningen, alltså att $M$ är ett maximalt ideal. Låt $x + M$ vara ett nollskilt element i $A/M$. Vi vill visa att det existerar $b + M \in A/M$ sådant att $(x + M) \cdot (b + M) = 1 + M$.

Låt $M' = \{xa + m : a \in A, m \in M\}$. Vi ser att $M'$ är ett ideal i $A$ och $M' \supsetneq M$ eftersom $x \in M'$, men $x \notin M$. Alltså måste $M' = A$ eftersom $M$ är maximal. Speciellt har vi $1 \in M'$, vilket betyder att $1 = xa + m$ för något $a \in A, m \in M$.

Då $M$ är ett ideal är $1 - xa \in M$, och således är $(a + M) \cdot (x + M) = 1 + M$. □

**Sats B.12.** $\mathcal{N}_p$ är ett maximalt ideal i $\mathcal{C}_p$.

*Bevis.* Välj $\{x_n\} \in \mathcal{C}_p \setminus \mathcal{N}_p$ och låt $I$ vara idealet som genereras av $(x_n)$ och $\mathcal{N}_p$. Eftersom $(x_n)$ inte går mot 0 så finns det $c > 0$ och heltal $N$ så att $\forall n \geq N \ |x_n| \geq c$. Nu låter vi $\{y_n\}$ vara en följd sådan att $y_n = 0$ om $n < N$ och $y_n = \frac{1}{x_n}$ om $n \geq N$.

Följden $\{y_n\}$ är en cauchyföljd eftersom för $n \geq N$ är

$$|y_{n+1} - y_n| = \left| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right| = \left| \frac{x_n - x_{n+1}}{x_{n+1} x_n} \right| \leq \frac{|x_n - x_{n+1}|}{c^2}$$

som går mot 0. Enligt föregående lemma är $\{y_n\}$ då en cauchyföljd eftersom $|\cdot|$ är icke-arkimediskt.

Vidare ser vi att $x_n y_n = 0$ då $n < N$ och $x_n y_n = 1$ då $n \geq N$. Låt $(1, 1, \ldots)$ beteckna den konstanta följden av ettor. Med denna notation får vi att $(1, 1, \ldots) - (x_n) \cdot (y_n)$ går mot 0. Därmed är $(1, 1, \ldots) - (x_n) \cdot (y_n) \in \mathcal{N}_p$.

Men det betyder att $(1, 1, \ldots)$ kan skrivas som en multipel av $(x_n)$, adderat med ett element $(n_p) \in \mathcal{N}_p$. Alltså måste $(1, 1, \ldots) \in I$, vilket medför att $I = \mathcal{C}_p$ och $\mathcal{N}_p$ är maximal i $\mathcal{C}_p$. □

Eftersom $\mathcal{N}_p$ utgör ett maximalt ideal av $\mathcal{C}_p$ enligt sats B.12 gör vi nu följande definition

**Definition B.13.** De $p$-adiska talen definieras som $\mathbb{Q}_p := \mathcal{C}_p/\mathcal{N}_p$.

Konstruktionen återfinns bland annat i Gouvêa [6, s. 43–56]. De $p$-adiska talen $\mathbb{Q}_p$ blir alltså en kropp eftersom $\mathcal{C}_p$ är en kommutativ ring med en multiplikativ identitet och $\mathcal{N}_p$ är ett maximalt ideal.

Vi frågar oss nu om $\mathbb{Q}_p$ verkligen är en komplettering av de rationella talen. De rationella talen $\mathbb{Q}$ är inte cauchyfullständiga med avseende på $|\cdot|_p$, vilket bevisas i sats C.6. Däremot är $\mathbb{Q}_p$ cauchyfullständigt av konstruktion, så $\mathbb{Q}_p$ är faktiskt en komplettering av $\mathbb{Q}$.

Vidare kan vi identifiera varje rationellt tal $r \in \mathbb{Q}$ med ekvivalensklassen till den konstanta följden $(r, r, \ldots)$ och vi får inklusionen $\mathbb{Q} \subset \mathbb{Q}_p$.

**Definition B.14.** Mängden $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ kallas för de $p$-adiska heltalen.

*Anmärkning* B.15. Notera att definitionen av $\mathbb{Z}_p$ kräver ett absolutvärde på $\mathbb{Q}_p$. Den $p$-adiska metriken i anmärkning B.4 är bara definierad på $\mathbb{Q}$. Den naturliga utökningen av $|\cdot|_p$ definieras senare i definition D.1. I fortsättningen kommer vi att anta det $p$-adiska absolutvärdet på $\mathbb{Q}_p$ om inget annat sägs.

*Anmärkning* B.16. Bråkkroppen av $\mathbb{Z}_p$ är precis $\mathbb{Q}_p$.

# C Hensels lemma

De polynom vi har studerat har varit definierade på den $p$-adiska kompletteringen av $\mathbb{Q}$ eller $\mathbb{Z}$. Vi ska nu betrakta ett enkelt sätt att avgöra huruvida ett polynom över $\mathbb{Z}_p$ har rötter eller inte. Hensels lemma kan ses som en konstruktiv algoritm för att hitta en rot genom iterering.

**Sats C.1. (Hensels lemma i en variabel)**

Låt $F(x) = a_0 + a_1 x + \ldots + a_n x^n$ vara ett polynom över $\mathbb{Z}_p$. Antag att det finns ett $p$-adiskt heltal $\alpha_1$ sådant att

$$F(\alpha_1) \equiv 0 \bmod p$$
$$F'(\alpha_1) \not\equiv 0 \bmod p.$$

Då existerar ett unikt $p$-adiskt heltal $\alpha$ sådant att $\alpha \equiv \alpha_1 \bmod p$ och $F(\alpha) = 0$.

*Anmärkning* C.2. Hensels lemma kan även formuleras för polynom i flera variabler.

För beviset behöver vi definiera den formella derivatan av ett polynom över en kropp $K$.

**Definition C.3.** Låt $K$ vara en kropp och

$$F(x) = \sum_{k=1}^{n} c_k (x - a)^k$$

ett polynom över $K$. Den formella derivatan av $F$, betecknad $F'$, definieras som

$$F'(x) := \sum_{k=1}^{n-1} k c_k (x - a)^{k-1}$$

med konventionen $x^0 := 1$.

*Bevis av sats C.1 (Hensels lemma i en variabel).* Beviset går ut på att konstruera en cauchyföljd $\{\alpha_n\}_n \to \alpha$ av $p$-adiska heltal som konvergerar till roten $\alpha$. En följd som uppfyller

(i) $F(\alpha_n) \equiv 0$ i $\mathbb{Z}/p^n\mathbb{Z}$

(ii) $\alpha_n \equiv \alpha_{n+1}$ i $\mathbb{Z}/p^n\mathbb{Z}$

kommer vara en cauchyföljd, samt uppfylla både $F(\alpha) \equiv 0$ och $\alpha \equiv \alpha_1 \mod p$ av konstruktion. Å andra sidan kommer en rot $\alpha$ bestämma en sådan följd $\{\alpha_n\}_n$. Det gäller alltså bara att bestämma $\alpha$ för att bevisa satsen.

Vi kan resonera på följande sätt: definiera

$$\alpha_2 := \alpha_1 + b_1 p$$

för något $b_1 \in \mathbb{Z}_p$ och betrakta den formella taylorutvecklingen av $F$ till den första ordningen i punkten $\alpha_2$,

$$F(\alpha_2) = F(\alpha_1 + b_1 p) = F(\alpha_1) + F'(\alpha_1) b_1 p + \xi(p^n) \tag{9}$$

där $\xi(p^n)$ är resttermer i $p^n$. Utvecklingen kan betraktas som utvecklingar av de binom som fås vid insättning av $\alpha_2$, enligt

$$F(\alpha_1 + b_1 p) = a_0 + a_1(\alpha_1 + b_1 p) + \ldots + a_n(\alpha_1 + b_1 p)^n.$$

Varje term $(\alpha_1 + b_1 p)^k = x^k + (x^k)' b_1 p + p^2 \xi(p^k)$ ger upphov till en ändlig restterm $\xi(p^k)$. Eftersom den formella derivatan är linjär, ges utvecklingen i (9). Resttermerna försvinner om vi väljer att betrakta uttrycket $\bmod p^2$,

$$F(\alpha_2) \equiv F(\alpha_1) + F'(\alpha) b_1 p \mod p^2.$$

Eftersom vi vet att $F(\alpha_1) \equiv 0 \mod p$, måste $F(\alpha_1) = px$ för något $x$. Ekvationen kan därmedelst skrivas som

$$px + F'(\alpha_1) b_1 p \equiv 0 \mod p^2$$

och efter division med $p$ ges

$$x F'(\alpha_1) b_1 \equiv 0 \mod p.$$

Men eftersom $p$ inte delar $F'(\alpha)$ kan vi skriva

$$b_1 \equiv -x(F'(\alpha_1))^{-1}.$$

Vi inser dessutom att vi kan konstruera hela följden $\{\alpha_n\}_n$ på samma sätt genom att sätta $\alpha_3 = \alpha_2 + b_2 p$, $\alpha_4 = \alpha\alpha_3 + b_3 p$, ... och detta bevisar satsen. □

**Korollarium C.4.** Alla $x \in \mathbb{Z}_p$ sådana att $|x|_p = 1$ är inverterbara i $\mathbb{Z}_p$.

*Bevis.* Låt $f(x) = ax - 1$, där $a \in \mathbb{Z}_p$ och $|a|_p = 1$. Då gäller det att $a \not\equiv 0 \mod p$ och därmed finns det $a'$ så att $aa' \equiv 1 \mod p$. Alltså är $f(a') \equiv 0 \mod p$ och $f'(a') = a \not\equiv 0 \mod p$. Då finns det, enligt Hensels lemma, ett $p$-adiskt heltal $\alpha$ sådant att $f(\alpha) = 0$ vilket betyder att $a\alpha = 1$. Således är alla $x \in \mathbb{Z}_p$ med $|x|_p = 1$ inverterbara. □

Låt oss nu betrakta en enkel tillämpning av Hensels lemma.

**Exempel C.5.** Vi söker en motsvarighet till $\sqrt[3]{2}$ i $\mathbb{Z}_5$. Med andra ord låter vi $p = 5$. Vi observerar att ett sådant tal är ett nollställe till polynomet $f(x) = x^3 - 2 \in \mathbb{Z}_5[x]$. Vi har att $f(3) \equiv 0 \bmod 5$ och $f'(3) \not\equiv 0 \bmod 5$. Det finns då, enligt Hensels lemma, en unik kubrot till 2 i $\mathbb{Z}_5$ som är kongruent med $3 \mod 5$. En explicit räkning ger att kubroten är på formen $3 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + \cdots$.

Hensels lemma beskriver en fundamental egenskap hos de $p$-adiska talen. Vi ska nu använda lemmat för att bevisa att $\mathbb{Q}$ inte är cauchyfullständigt med avseende på $|\cdot|_p$.

**Sats C.6.** De rationella talen $\mathbb{Q}$ är inte cauchyfullständiga med avseende på $|\cdot|_p$.

*Bevis.* Fixera ett primtal $p$. Tag ett strikt positivt heltal $b$ som inte har $p$ i sin primtalsfaktorisering och där $b \geq \dfrac{p+1}{2}$. Exempelvis är $b = p+1$ ett sådant tal, eftersom $p$ inte kan förekomma i primtalsfaktoriseringen av $b$ och $b = p+1 > p > 0$.

Sätt nu $a = b^k + p$ där $k \geq 2$ och inte heller innehåller $p$ i sin primtalsfaktorisering. Polynomet $f(x) = x^k - a$ uppfyller då

$$f(b) \equiv 0 \mod p$$

eftersom genom räkning gäller

$$\begin{aligned} f(b) &= b^k - \left(b^k + p\right) \\ &= \left(b^k - b^k\right) - p \\ &= -p \\ &\equiv 0 \mod p. \end{aligned}$$

Vidare uppfyller derivatan $f'(b) = kb^{k-1} \not\equiv 0$ av Euklides lemma. Enligt Hensels lemma finns det då en följd heltal $\{x_n\}_n$ sådant att

$$f(x_n) \equiv 0 \mod p^n \ \forall n$$

$$x_{n+1} \equiv x_n \mod p^n \ \forall n.$$

Eftersom $f(x_n) = x_n^k - a \equiv 0 \mod p^n$ måste $p$ dela $x_n^k - a$. Av definition av det $p$-adiska absolutvärdet har vi då

$$|x_n^k - a|_p \leq \frac{1}{p^n}$$

och därmed gäller

$$\lim_{n\to\infty} |x_n^k - a|_p \leq \lim_{n\to\infty} \frac{1}{p^n} = 0,$$

så vi har gränsvärdet $\lim\limits_{n\to\infty} x_n^k = a$.

Men också: enligt kongruensen $x_{n+1} \equiv x_n \mod p^n$ delar talet $p^n$ då $x_{n+1} - x_{n+1}$. Precis på samma sätt som här ovan kan vi göra den snarlika räkningen

$$\lim_{n\to\infty} |x_{n+1} - x_n|_p \leq \lim_{n\to\infty} \frac{1}{p^n} = 0.$$

Av lemma B.8 måste $\{x_n\}_n$ då vara en cauchyföljd i $\mathbb{Q}$.

Härifån vill vi nu söka en motsägelse. Om nu vi antar $\lim\limits_{n\to\infty} x_n := c \in \mathbb{Z}$ måste $c^k = a$ eftersom $\lim\limits_{n\to\infty} x_n^k = c^k$. Alltså måste $c$ antingen vara ett heltal eller icke-rationellt. Vårt mål är att visa att $c$ inte kan vara ett heltal, vilket skulle tvinga följden $\{x_n\}_n$ att konvergera mot ett icke-rationellt element i $\mathbb{Q}_p \setminus \mathbb{Q}$. För motsägelse kan vi alltså anta att $c^k = a$ för något heltal $c \in \mathbb{Z}$.

Vi får två fall: ett där $k$ är udda, och ett där $k$ är jämnt. Om $k$ är udda är $a = |c|^k$. Är $k = 2m$ däremot jämnt är $a = c^{2m} = \left(c^2\right)^m = \left(|c|^2\right)^m = |c|^{2m} = |c|^k$. I båda fallen är alltså $|c|$ ett positivt heltal med $a = |c|^k$.

Sätt $d = |c|$. Då är $d^k = b^k + p$ av definition. Alltså är

$$p = d^k - b^k = (d-b)\left(d^{k-1} + d^{k-2}b + d^{k-3}b^2 + \cdots + cb^{k-2} + b^{k-1}\right) = (d-b)y,$$

där vi definierar $y := \left(d^{k-1} + d^{k-2}b + d^{k-3}b^2 + \cdots + cb^{k-2} + b^{k-1}\right)$. Vidare är

$$\begin{aligned} y = d^{k-1} + d^{k-2}b + d^{k-3}b^2 + \cdots + db^{k-2} + b^{k-1} &\geq d^{k-1} + b^{k-1} \\ &\geq d + b \geq 2. \end{aligned}$$

Vi såg att både $d-b$ och $y$ var faktorer av $p$, som är ett primtal. Primtal har bara faktorerna 1 och $p$, så vi måste ha $y=p$ och $d-b=1$. Detta eftersom om $c=1$ skulle vi haft $a=1$, men $a=b^k+p>2$. Det senare fallet är alltså omöjligt. Av att $y=p$ har vi

$$\begin{aligned} p &= d^{k-1}+d^{k-2}b+d^{k-3}b^2+\cdots+db^{k-2}+b^{k-1} \\ &\geq d^{k-1}+b^{k-1}\geq d+b. \end{aligned}$$

Likheten $d-b=1$ ger $d=b+1$, men

$$d+b=2b+1>2b>p.$$

Nu har vi både $d+b=1$ och $d+b>p\geq 2$, och därav en motsägelse.

Därmed måste $c$ vara icke-rationellt och kan inte vara ett heltal. Vår följd $\{x_n\}_n$ måste alltså ha ett icke-rationellt gränsvärde och konvergerar således inte i $\mathbb{Q}$. De rationella talen är med andra ord inte cauchyfullständiga med avseende på $|\cdot|_p$. □

# D Representation av $p$-adiska tal som oändliga summor

Vi ska i det här avsnittet motivera att ett $p$-adiskt tal kan skrivas på den allmänna formen

$$\sum_{k\in\mathbb{Z}} a_k p^k.$$

Konvergerar summan? I sådana fall, i vilken mening ska konvergensen uppfattas? För att summan inte enbart ska betraktas som en symbolisk sådan, ska vi nu se hur konvergens av en $p$-adisk utveckling kan definieras. Vi väljer att betrakta den analytiska konstruktionen av $\mathbb{Q}_p$, eftersom den faller sig naturlig för att formellt definiera $p$-adiska utvecklingar. Enligt konstruktionen i definition B.13 kan vi identifiera de rationella talen med ekvivalensklasser till konstanta rationella följder. Det vill säga, funktionen

$$\begin{aligned} \theta : \mathbb{Q} &\to \mathrm{Im}(\theta)\subset\mathbb{Q}_p \\ q &\mapsto [(q,q,q,\ldots)] \end{aligned}$$

för $q\in\mathbb{Q}$ utgör en ringisomorfi. Detta motiverar att beteckna talet $[(q,q,q,\ldots)]\in\mathbb{Q}_p$ med $q$. Vi vill nu definiera ett konvergensbegrepp på $\mathbb{Q}_p$ för att se hur $p$-adiska tal kan representeras.

Det går att utöka den $p$-adiska metriken i anmärkning B.4, som är definierad på $\mathbb{Q}$, till $\mathbb{Q}_p$. Utökningen av den $p$-adiska metriken formulerar vi som en definition.

**Definition D.1.** Tag ett tal $x\in\mathbb{Q}_p$ och låt $\{x_n\}_n$ vara en representant för $x$. Vi definierar då

$$|x|_p := \lim_{n\to\infty}|x_n|_p.$$

**Sats D.2.** Gränsvärdet i definition D.1 är väldefinierat och med andra ord oberoende av representant av ekvivalensklassen för $x\in\mathbb{Q}_p$.

*Bevis.* Tag en representant $\{x_n\}_n$ för $x\in\mathbb{Q}_p$. Följden $\{|x_n|_p\}_n$ utgör en cauchyföljd i $\mathbb{R}$, ty $\{x_n\}_n\in\mathcal{C}_p$. Detta medför att för två representanter $\{x_n\}_n$ och $\{y_n\}_n$ för $x\in\mathbb{Q}_p$ måste både gränsvärdena $\lim_{n\to\infty}|x_n|_p$ och $\lim_{n\to\infty}|y_n|_p$ existera och vara lika med varandra, det vill säga

$$\lim_{n\to\infty}|x_n|_p=\lim_{n\to\infty}|y_n|_p.$$

Gränsvärdet är då oberoende av representant av ekvivalensklassen för $x\in\mathbb{Q}_p$. □

Många egenskaper hos absolutvärdet på $\mathbb{Q}$ gäller även för absolutvärdet på $\mathbb{Q}_p$. Först och främst bevaras egenskapen att utökningen i definition D.1 är ett absolutvärde. En viktig egenskap som bevaras är att det utökade absolutvärdet är icke-arkimediskt:

**Sats D.3.** Absolutvärdet på $\mathbb{Q}_p$ är ett icke-arkimediskt absolutvärde.

*Bevis.* För att bevisa satsen gäller det att verifiera axiomen (1)-(4) i definition 2.5. Antag att $x \in \mathbb{Q}_p$ och välj en representant $\{x_n\}_n$ för $x$. Vi ser att $\lim_{n\to\infty} |x_n|_p = 0$ om och endast om $\{|x_n|_p\}_n$ ligger i samma ekvivalensklass som den konstanta följden $(0, 0, 0, \ldots)$ av nollor. Vidare är ett gränsvärde av en icke-negativ följd alltid icke-negativt. Absolutvärdet på $\mathbb{Q}_p$ är därför strikt positivt definit och uppfyller axiom (1).

Tag nu $y \in \mathbb{Q}_p$ och välj på samma sätt en representant $\{y_n\}_n$ för $y$. Då kan vi betrakta gränsvärdet

$$|xy|_p = \lim_{n\to\infty} |x_n y_n|_p = \lim_{n\to\infty} |x_n|_p |y_n|_p = |x|_p |y|_p.$$

Detta verifierar axiom (2).

På samma sätt kan vi också betrakta gränsvärdet

$$|x + y|_p = \lim_{n\to\infty} |x_n + y_n|_p \leq \lim_{n\to\infty} |x_n|_p + \lim_{n\to\infty} |y_n|_p = |x|_p + |y|_p$$

som gäller enligt triangelolikheten för rationella tal. Vi har då visat att absolutvärdet på gränsvärdet $\mathbb{Q}_p$ uppfyller axiom (3).

Vi konkluderar därmed att absolutvärdet på $\mathbb{Q}_p$ verkligen är ett absolutvärde. Slutligen vill vi visa att det är icke-arkimediskt. Men detta följer från att absolutvärdet på $\mathbb{Q}$ är icke-arkimediskt, ty

$$|x + y|_p = \lim_{n\to\infty} |x_n + y_n|_p \leq \lim_{n\to\infty} \max\{|x_n|_p, |y_n|_p\} = \max\{|x|_p, |y|_p\}$$

eftersom max är en kontinuerlig funktion.

Absolutvärdet på $\mathbb{Q}_p$ är därför icke-arkimediskt, och vi har bevisat satsen. □

*Anmärkning* D.4. Vi ser att definitionen utökar det $p$-adiska absolutvärdet till $\mathbb{Q}_p$ och enligt sats B.3 inducerar detta en metrik $d : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{R}_{\geq 0}$ på $\mathbb{Q}_p$.

*Anmärkning* D.5. Eftersom absolutvärdet på $\mathbb{Q}_p$ är en utökning av absolutvärdet på $\mathbb{Q}$ är även den $p$-adiska metriken på $\mathbb{Q}_p$ en utökning av den $p$-adiska metriken på $\mathbb{Q}$.

*Anmärkning* D.6. De $p$-adiska talen är cauchyfullständiga med avseende på $|\cdot|_p$.

*Anmärkning* D.7. I anmärkning 2.8 noterade vi att det $p$-adiska absolutvärdet på $\mathbb{Q}$ enbart kunde anta diskreta värden. Med definition D.1 ser vi att det utökade absolutvärdet $|\cdot|_p$ på $\mathbb{Q}_p$ bara kan anta värden på formen $p^{-k}$ med $k \in \mathbb{Z}$ för nollskilda element i $\mathbb{Q}_p$. Observationen låter oss utöka valueringen på $\mathbb{Q}$ till en valuering på $\mathbb{Q}_p$ genom att definiera

$$v(x) := \frac{\log\left(|x|_p^{-1}\right)}{\log p}, \quad x \in \mathbb{Q}_p \setminus \{0\}$$

och $v(0) := \infty$. Notera att valueringen definieras precis så att $|x|_p = p^{-v_p(x)}$.

När vi definierade de $p$-adiska talen $\mathbb{Q}_p$ som en bråkkropp behövde vi att $\mathbb{Z}_p$ var ett integritetsområde. Låt oss nu bevisa påståendet.

**Sats D.8.** De $p$-adiska heltalen $\mathbb{Z}_p$ är ett integritetsområde.

*Bevis.* Tag $a, b \neq 0$ i $\mathbb{Z}_p$. Då är $v_p(ab) = v_p(a) + v_p(b) < \infty$, så $ab \neq 0$. □

För att kunna visa att alla $p$-adiska tal kan skrivas som oändliga summor behöver vi definiera vad som menas med konvergens i $\mathbb{Q}_p$.

**Definition D.9.** Vi definierar öppna bollar som $B_r(x) := \{y \in \mathbb{Q}_p : d(x,y) < r\}$.

Vi ger den självklara definitionen för konvergens i $\mathbb{Q}_p$:

**Definition D.10.** En följd $\{x_k\}_{k=1}^{\infty}$ av $p$-adiska tal $x_k \in \mathbb{Q}_p$ sägs konvergera med avseende på det $p$-adiska absolutvärdet när $k \to \infty$ om och endast om $|x - x_k|_p \to 0$ för något $x \in \mathbb{Q}_p$ och vi skriver $x_k \to x$. Följden $\{x_k\}_{k=1}^{\infty}$ sägs divergera om den inte konvergerar.

*Anmärkning* D.11. Gränsvärden i metriska rum är unika [16, sats 3.2b], och därför är även gränsvärden i $\mathbb{Q}_p$ unika.

**Exempel D.12.** Serieutvecklingen $-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \ldots$ i exempel 2.24 konvergerar eftersom $|p|_p = \frac{1}{p} < 1$. Dessutom är $|-1|_p = 1$.

**Exempel D.13.** Den geometriska serien

$$\sum_{k \geq 0} r^k$$

konvergerar för alla element $r$ i valueringsidealet till $\mathbb{Q}_p$. Beviset är helt analogt med det reella fallet. Vi skriver

$$1 + r + r^2 + r^3 + \cdots := \lim_{n \to \infty} \left(1 + r + r^2 + \cdots + r^n\right) = \lim_{n \to \infty} \frac{1 - r^{n+1}}{1 - r}.$$

I det $p$-adiska absolutvärdet gäller

$$\lim_{n \to \infty} |r^{n+1}|_p = \lim_{n \to \infty} |r|_p^{n+1} = 0$$

om och endast om $|r|_p < 1$. Exempel 2.26 är ett exempel på en geometrisk serie som konvergerar i $\mathbb{Z}_7$.

Formeln gäller dessutom för alla valueringsringar, och konvergensen beror inte på huruvida absolutvärdet är arkimediskt eller icke-arkimediskt.

**Exempel D.14.** Vi betonar igen att stora tal kan ha ett litet $p$-adiskt absolutvärde och att vi därför ska vara försiktiga med gränsvärden i $\mathbb{Q}_p$. Följden $\left\{\frac{1}{1+p^k}\right\}_{k=1}^{\infty}$ konvergerar *inte* mot 0 i $\mathbb{Q}_p$. Istället har vi

$$\left|\frac{1}{1+p^k} - 1\right|_p = \left|\frac{p^k}{1+p^k}\right|_p = \frac{|p|_p^k}{|1+p^k|_p} = p^{-k} \to 0.$$

Den sista likheten följer av att $v_p(1+p^k) = 0$, eftersom $1 + p^k = 1 \mod p$. Följden konvergerar därför istället mot 1 i $\mathbb{Q}_p$.

Vi är nu redo att presentera delkapitlets huvudsats om decimalutvecklingar i $\mathbb{Q}_p$:

**Sats D.15. (Formen på element i $\mathbb{Q}_p$ och $\mathbb{Z}_p$)**

Alla $p$-adiska tal $x \in \mathbb{Q}_p$ kan skrivas på formen

$$x = \sum_{k=-m_0}^{\infty} a_k p^k$$

för något $m_0 \geq 0$.

Vidare är $m_0 = 0$ för de $p$-adiska heltalen $y \in \mathbb{Z}_p$, och dessa kan med andra ord skrivas på formen

$$y = \sum_{k=0}^{\infty} a_k p^k.$$

För att bevisa satsen visar vi först följande lemma:

**Lemma D.16.** De rationella talen $\mathbb{Q}$ ligger tätt i $\mathbb{Q}_p$, vilket betyder att varje boll på formen $B_r(x)$ för $x \in \mathbb{Q}$ innehåller element i $\mathbb{Q}$.

*Anmärkning* D.17. Heuristiskt kan vi betrakta egenskapen som att element i $\mathbb{Q}_p$ kan approximeras "godtyckligt bra" med element i $\mathbb{Q}$. Exempelvis ligger $\mathbb{Q}$ även tätt i $\mathbb{R}$, eftersom varje reellt tal har en godtycklig bra rationell approximation.

*Bevis av lemma D.16.* Vi vill visa att $\mathbb{Q}$ ligger tätt i $\mathbb{Q}_p$ med avseende på den $p$-adiska topologin. Låt därför $\varepsilon > 0$ och betrakta bollen $B_\varepsilon(x)$ för något element $x \in \mathbb{Q}_p$. Kan vi visa att det finns ett rationellt $q \in \mathbb{Q}$ som tillhör bollen $B_\varepsilon(x)$ är vi klara.

Vi väljer nu att betrakta den analytiska definitionen av $\mathbb{Q}_p$, där varje element är en ekvivalensklass av rationella cauchyföljder. Tag en representant $\{x_n\}_n$ för $x \in \mathbb{Q}_p$ och låt $0 < \delta < \varepsilon$. Eftersom $\{x_n\}_n$ är en cauchyföljd kan vi ta $N$ sådant att $|x_n - x_m|_p < \delta$ sånär $n, m \geq N$. Vi påstår då att den konstanta följden $(x_N, x_N, x_N, \ldots) \in B_\varepsilon(x)$. För att se detta kan vi beräkna absolutvärdet

$$|(x_1, x_2, x_3, \ldots) - (x_N, x_N, x_N, \ldots)|_p = \lim_{n\to\infty} |x_n - x_N|_p \leq \delta < \varepsilon$$

enligt definition D.1. Således ligger följden $(x_N, x_N, x_N, \ldots)$ i bollen $B_\varepsilon(x)$, vilket skulle visas. □

*Anmärkning* D.18. På samma sätt bevisas att $\mathbb{Z}$ ligger tätt i $\mathbb{Z}_p$.

*Bevis av sats D.15.* Vi börjar med att karaktärisera elementen i $\mathbb{Z}_p$. Tag $x \in \mathbb{Z}_p$. Av lemma D.16 ligger $\mathbb{Q}$ tätt i $\mathbb{Q}_p$. Det är alltså klart att vi kan välja $\dfrac{a}{b} \in \mathbb{Q}$ sådant att

$$\left|x - \frac{a}{b}\right|_p \leq p^{-n} < 1$$

där $n \geq 1$. Vi påstår dock något starkare; att $\dfrac{a}{b}$ kan väljas som ett *heltal* i $\mathbb{Z}$, vilket vi nu ska visa. För $\dfrac{a}{b}$ gäller

$$\left|\frac{a}{b}\right|_p = \left|x - \left(x - \frac{a}{b}\right)\right|_p \leq \max\left\{|x|_p, \left|x - \frac{a}{b}\right|_p\right\} \leq 1.$$

Alltså kan inte $p$ dela $b$, och vi har då att $bb' \equiv 1 \mod p^n$ för något $b'$. Härav följer att

$$\left|x - \frac{a}{b}\right|_p = |x - ab'|_p \leq p^{-n}$$

med $ab' \in \mathbb{Z}$. Bråket $\dfrac{a}{b}$ kan ersättas med $ab' \in \mathbb{Z}$ eftersom $\dfrac{a}{b} \equiv ab' \mod p^n$. Vidare kan vi då välja $0 \leq \alpha_n \leq p^n - 1$ sådant att $\alpha \equiv ab' \mod p^n$. Detta medför att

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

Det går då hitta en unik följd heltal $\{\alpha_n\}_n$ med

(i) $0 \leq \alpha_n < p^n$

(ii) $\alpha_{n+1} \equiv \alpha_n \mod p^n$

som konvergerar till $x$ eftersom $|x - \alpha_n|_p \leq p^{-n}$. Å andra sidan är en följd som uppfyller (i) och (ii) en cauchyföljd enligt lemma B.8 och konvergerar i $\mathbb{Z}$ eftersom alla $\alpha_n$ ligger i $\mathbb{Z}$.

Därför kan vi skriva

$$x = \sum_{k \geq 0} a_k p^k$$

med $0 \leq a_k \leq p - 1$. Kofficientera $a_k$ relaterar till följden $\{\alpha_n\}_n$ genom att $\alpha_n = \sum_{k=0}^{n-1} a_k p^k$ och $\alpha_n \in \mathbb{Z}/p^n\mathbb{Z}$. Vi har därför visat satsen för $\mathbb{Z}_p$.

För ett element $y \in \mathbb{Q}_p$ kan vi bara notera att

$$y = \frac{x}{p^m}$$

för något $x \in \mathbb{Z}_p$, eftersom $\mathbb{Q}_p$ enligt definition 2.20 kunde definieras som kroppen av alla bråk $\mathbb{Z}_p[\frac{1}{p}]$ i $\mathbb{Z}_p$. Direkt insättning ger

$$y = \frac{1}{p^m} \sum_{k \geq 0} a_k p^k = \sum_{k \geq 0} a_k \frac{p^k}{p^m} = \sum_{k \geq 0} a_k p^{k-m} = \sum_{k \geq -m} a_{k-m} p^k.$$

Genom att sätta $m_0 = m \geq 0$ och en omnumrering av koefficienter följer satsen. □

*Anmärkning* D.19. För att skriva ut operationerna på $\mathbb{Q}_p$ explicit, tag två element $x = \sum_{k \in \mathbb{Z}} a_k p^k$ och $y = \sum_{k \in \mathbb{Z}} b_k p^k$, båda sådana att $x, y \in \mathbb{Q}_p$. Då är summan

$$x + y = \sum_{k \in \mathbb{Z}} (a_k + b_k) p^k$$

och produkten

$$xy = \sum_{k \in \mathbb{Z}} c_k p^k \quad \text{där} \quad c_k = \sum_{n \in \mathbb{Z}} b_n a_{k-n},$$

vilket känns igen från komplex analys som Cauchys produktformel för formella Laurentserier.

**Korollarium D.20.** För varje $x \in \mathbb{Z}_p$ finns det ett unikt $0 \leq \alpha_n \leq p^n - 1$ sådant att $x \equiv \alpha_n \mod p^n$.

*Bevis.* Påståendet säger bara att $\mathbb{Z}$ ligger tätt i $\mathbb{Z}_p$. Beviset är analogt med beviset till sats D.15. □

*Anmärkning* D.21. Från de $p$-adiska utvecklingarna i sats D.15 ser vi att kardinaliteten hos $\mathbb{Z}_p$ och $\mathbb{Q}_p$ är $|\mathbb{Z}_p| = |\mathbb{Q}_p| = \mathfrak{c} = 2^{\aleph_0}$.

*Anmärkning* D.22. Vi ser att $p$-adiska utvecklingar i $\mathbb{Q}_p$ är unika. Vi har med andra ord inte en situation liknande den i de reella talen $\mathbb{R}$ där $0.999... = 1$.

**Lemma D.23.** Idealet $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$ är ett maximalt ideal i $\mathbb{Z}_p$.

*Bevis.* För att underlätta beviset använder vi valueringen $v_p$ istället för absolutvärdet $|\cdot|_p$. Att $|x|_p \leq 1$ är ekvivalent med att $v_p(x) \geq 0$. Antag att $I \subseteq \mathbb{Z}_p$ är ett ideal sådant att $a \in I$ och $v_p(a) = 0$, alltså $a$ ligger inte i $p\mathbb{Z}_p$. Då gäller att

$$0 = v_p(1) = v_p(aa^{-1}) = v_p(a) + v_p(a^{-1}) = v_p(a^{-1})$$

Att $v_p(a^{-1}) = 0$ medför att $a^{-1} \in \mathbb{Z}_p$ och därmed är $aa^{-1} = 1 \in I$. Alltså gäller det att varje ideal $I$, som inte är en delmängd i $p\mathbb{Z}_p$, är hela $\mathbb{Z}_p$. □

**Korollarium D.24.** Ringarna $\mathbb{Z}_p/p^m\mathbb{Z}_p$ och $\mathbb{Z}/p^m\mathbb{Z}$ är isomorfa. Speciellt är $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

*Bevis.* Vi börjar med att visa att de nollskilda idealen i $\mathbb{Z}_p$ är precis idealen $p^m\mathbb{Z}$ för $m = 0, 1, 2, \ldots$. Speciellt är $p\mathbb{Z}_p$ det enda maximala idealet i $\mathbb{Z}_p$. Att idealet $p\mathbb{Z}_p$ är maximalt i $\mathbb{Z}_p$ visar vi i lemma D.23.

Tag därför ett nollskilt ideal $I$ i $\mathbb{Z}_p$, och välj $\alpha \in I$ sådan att $|\alpha|_p \leq |a|_p$ för alla $a \in I$. Då är $|\alpha|_p = p^{-m}$ enligt anmärkning D.7. Definiera $\mathbb{Z}_p^* := \mathcal{O}_{\mathbb{Q}_p} \setminus \mathfrak{p}_{\mathbb{Q}_p} = \{x \in \mathbb{Q}_p : |x|_p = 1\}$. Då kommer $p^{-m}\alpha \in \mathbb{Z}_p^*$, och $p^m \in I$. Men för $a \in I$ gäller $|ap^{-m}|_p \leq 1$, så $a \in p^m\mathbb{Z}$. Idealet $I \subset p^m\mathbb{Z}$ måste då vara maximalt, och $I = p^m\mathbb{Z}$.

Homomorfin

$$\begin{aligned} \theta : \mathbb{Z}/p^m\mathbb{Z} &\to \mathbb{Z}_p/p^m\mathbb{Z}_p \\ [a]_{p^m} \in \mathbb{Z}/p^m\mathbb{Z} &\mapsto [a]_{p^m} \in \mathbb{Z}_p/p^m\mathbb{Z}_p \end{aligned}$$

är injektiv eftersom $p^m\mathbb{Z} \cap \mathbb{Z} = p^m\mathbb{Z}$. Den är också surjektiv, av korollarium D.20. Det är klart att den bevarar addition och multiplikation från definitionen. Detta bevisar att $\theta$ är en ringisomorfi, och alltså är $\mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^m\mathbb{Z}$. Eftersom $p\mathbb{Z}_p$ är maximalt kommer $\mathbb{Z}_p/p\mathbb{Z}_p$ vara en kropp med $p$ element, så $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. Med andra ord är följden

$$0 \to \mathbb{Z}_p \xrightarrow{p^m} \mathbb{Z}_p \xrightarrow{\phi_m} \mathbb{Z}/p^m\mathbb{Z} \to 0$$

exakt, där avbildningen $p^m$ är elementvis multiplikation med $p^m$ och $\phi_m$ homomorfierna i anmärkning 2.19. □

För att fullständigt abstrahera resultatet i sats D.15 formulerar vi motsvarande sats för diskreta valueringsringar.

**Sats D.25.** Låt $R$ vara en diskret valueringsring och låt $K$ utgöra kroppen av alla bråk i $R$. Beteckna restklasskroppen $\Bbbk = \mathcal{O}/\mathfrak{p}$. Om $A$ nu utgör en mängd av representanter för sidoklasserna i $\mathfrak{p} \subseteq \mathcal{O}$ och om $\pi$ är ett uniformiseringelement i $K$ kan varje element $a \in R$ skrivas på formen

$$a = \sum_{k=0}^{\infty} a_k \pi^k.$$

Vidare kan alla element $x \in K$ skrivas som

$$x = \sum_{k=-m_0}^{\infty} b_k \pi^k$$

där $m_0 \geq 0$ Vi har att $a_k, b_k \in A$ för alla $k$.

*Bevis.* Beviset för satsen är helt analogt beviset för sats D.15, inklusive lemmat. □

Vi har redan sett i sats D.23 att $\mathfrak{p}_{\mathbb{Q}_p} = \mathbb{Z}_p$ är en lokal ring med maximalt ideal $\mathfrak{p}_{\mathbb{Q}_p} = p\mathbb{Z}_p$. Vi generaliserar detta till allmänna kroppar med valueringar.

**Sats D.26.** Låt $K$ vara en kropp och $|\cdot|$ ett icke-arkimediskt absolutvärde på $K$. Då är $\mathcal{O}$ en maximal delring till $K$ och $\mathfrak{p} \subset \mathcal{O}$ är ett maximalt ideal i $\mathcal{O}$. Dessutom är alla element $x \in \mathcal{O} \setminus \mathfrak{p}$ inverterbara.

*Bevis.* Det är klart att $\mathcal{O}$ är en delring. Vi vill nu argumentera med motsägelse att $\mathcal{O}$ är maximal. Antag att $\mathcal{O}'$ är en delring med $\mathcal{O} \subset \mathcal{O}'$. Då finns det per definition ett element $\alpha \in \mathcal{O}'$ med $|\alpha| > 1$. Tag slutna bollar $\overline{B_{|\alpha|^k}(0)} \subseteq \mathcal{O}'$. Då ser vi att $K = \bigcup_{k \geq 1} \overline{B_{|\alpha|^k}(0)} = \mathcal{O}'$. Detta är en motsägelse, så $\mathcal{O}$ måste vara maximal.

Vill vi vidare visa att ett godtyckligt element $x \in \mathcal{O} \setminus \mathfrak{p}$ är inverterbart. Notera först att alla icke-nollskilda element i en kropp är inverterbara. Eftersom $|x| = 1$ kan inte $x = 0$, och $x$ måste då vara inverterbart. Vidare är det en trivial observation att $|x^{-1}| = 1$, eftersom $|xx^{-1}| = |1| = 1$. Argumentet visar även att $\mathfrak{p}$ är ett maximalt ideal i $\mathcal{O}$, ty ett $\mathcal{O}$-ideal $\mathfrak{p}'$ med $\mathfrak{p} \subset \mathfrak{p}'$ innehåller ett identitetselement $\beta^{-1}\beta$, $\beta \in \mathfrak{p}' \setminus \mathfrak{p}$. Detta skulle medföra $\mathfrak{p}' = \mathcal{O}$, och $\mathfrak{p}$ måste vara maximal. □

*Anmärkning* D.27. Beviset återfinns i [2, sats 2.4.1].

Vi avslutar avsnittet med att visa att $\mathbb{Z}_p$ är en kompakt mängd.

**Sats D.28.** Mängden $\mathbb{Z}_p$ är kompakt.

*Bevis.* Vi visar att $\mathbb{Z}_p$ är följdkompakt vilket medför att $\mathbb{Z}_p$ är kompakt eftersom $\mathbb{Z}_p$ är ett metriskt rum [16, sats 3.6]. Låt $\{\alpha_n\}_n$ vara en följd i $\mathbb{Z}_p$. Enligt sats D.15 kan $\alpha_n$ då skrivas som

$$\alpha_n = \sum_{i=0}^{\infty} a_i^{(n)} p^i$$

med $0 \leq a_k^{(n)} \leq p-1$. Det finns då något $b_0$ så att $0 \leq b_0 \leq p-1$ och så att $a_0^{(n)} = b_0$ för oändligt många $n$. Samlingen av alla $\alpha_n$ med $b_0$ som första koefficient blir en delföljd till $\{\alpha_n\}$, kalla den $\{\alpha_{0,n}\}$. Vi upprepar nu konstruktionen av $\{\alpha_{0,n}\}$ och får på så sätt en följd av delföljder $\{\alpha_{k,n}\}$ och ett $p$-adiskt heltal

$$b = \sum_{i=0}^{\infty} b_i^{(n)} p^i.$$

Det gäller då att, för varje $k$, är de första $k+1$ termerna i följden $\{\alpha_{k,n}\}$ samma som i $b$. Då är $\{\alpha_{k,k}\}$ en delföljd till $\{\alpha_n\}$ som konvergerar mot $b$. □

# E Den analytiska och algebraiska definitionen av de $p$-adiska talen är isomorfa

När vi konstruerade de $p$-adiska talen algebraiskt nämnde vi att den algebraiska konstruktionen och den analytiska konstruktionen ger upphov till isomorfa kroppar. Vi ger nu en explicit isomorfi mellan de olika strukturera.

**Sats E.1.** Strukturerna i definition B.13 och definition 2.20 är isomorfa som kroppar.

*Bevis.* Det räcker med att visa att ringarna av $p$-adiska heltal, definierade i definition B.14 och definition 2.18, är isomorfa som ringar.

Inför beteckningarna

$$\mathbb{Z}_p^{\text{analytisk}} = \left\{ x \in \mathbb{Q}_p^{\text{analytisk}} := \mathcal{C}_p/\mathcal{N}_p : |x|_p \leq 1 \right\}$$

och

$$\mathbb{Z}_p^{\text{algebraisk}} = \varprojlim \mathbb{Z}/p^k\mathbb{Z} = \left\{ \{a_j\}_j \in \prod_{k=1}^{\infty} \mathbb{Z}/p^k\mathbb{Z} : \varphi_k(a_k) = a_{k-1} \ \ \forall k \geq 1 \right\}$$

där $\varphi_k$ är homomorfin i ekvation (2).

Av den analytiska definitionen och sats D.15 måste alltså de $p$-adiska heltalen $\mathbb{Z}_p^{\text{analytisk}}$ utgöras av alla element i $x \in \mathbb{Q}_p$ på formen

$$x = \sum_{k \geq 0} a_k p^k \tag{10}$$

där $0 \leq a_k \leq p-1$ för alla $k \geq 0$.

Eftersom alla $p$-adiska heltal kan representeras på formen given i ekvation (10) betraktar vi likheterna

$$\begin{cases} x & \equiv a_0 \mod p \\ x & \equiv a_0 p + a_1 \mod p^2 \\ x & \equiv a_0 + a_1 p + a_2 p^2 \mod p^3 \\ x & \equiv a_0 + a_1 p + a_2 p^2 + a_3 p^3 \mod p^4 \\ & \vdots \end{cases}$$

och generellt gäller

$$x \equiv \sum_{k=0}^{n} a_k p^k \mod p^{n+1}.$$

En funktion

$$\begin{aligned} \theta : \mathbb{Z}_p^{\text{analytisk}} &\to \mathbb{Z}_p^{\text{algebraisk}} \\ x = \sum_{k\geq 0} a_k p^k &\mapsto (a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots) \end{aligned}$$

är därför en lämplig ansats för en homomorfi. Vi visar att denna funktion är väldefinierad genom att först notera att $y = (y_1, y_2, y_3, \ldots) = (a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots)$ ligger i den direkta produkten $\prod_{k=1}^{\infty} \mathbb{Z}/p^k\mathbb{Z}$. Om vi nu tar homomorfin $\varphi_k(y_k) := y_{k-1}$ ger en direkt beräkning att

$$\varphi_k(y_{k+1}) = \varphi_k\left(\sum_{j=0}^{k} a_j p^j\right) = \sum_{j=0}^{k-1} a_j p^j = y_k,$$

och vi har då verifierat att $\theta : \mathbb{Z}_p^{\text{analytisk}} \to \mathbb{Z}_p^{\text{algebraisk}}$ verkligen antar värden i målmängden. För att visa att $\theta$ är en ringhomomorfi behöver vi även visa att $\theta$ bevarar addition och multiplikation mellan element. Tag därför två element $\alpha = (\alpha_1, \alpha_2, \alpha_3, \ldots)$ och $\beta = (\beta_1, \beta_2, \beta_3, \ldots)$ i $\mathbb{Z}_p$ godtyckligt. Då är

$$\theta(\alpha) + \theta(\beta) = \theta((\alpha_0 + \beta_0), (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)p, \ldots)) = \theta(\alpha + \beta)$$

och

$$\begin{aligned} \theta(\alpha) \cdot \theta(\beta) &= \theta(\alpha_0, \alpha_1, \alpha_2, \ldots) \cdot \theta(\beta_0, \beta_1, \beta_2, \ldots) \\ &= (\alpha_0, \alpha_0 + \alpha_1 p, \alpha_0 + \alpha_1 p, \ldots) \cdot (\beta_0, \beta_0 + \beta_1 p, \beta_0 + \beta_1 p, \ldots). \end{aligned}$$

Genom att komponentvis skriva

$$\left(\sum_{i=0}^{j} \alpha_i p^i\right) \cdot \left(\sum_{i=0}^{j} \beta_i p^i\right) \equiv \sum_{k=0}^{j+1} \left(\sum_{n=0}^{k} \beta_n \alpha_{k-n}\right) p^k \mod p^{j+1}.$$

ser vi att kongruensen ovan bara är faltningsidentiteten i anmärkning D.19, nu av finita summor, där vi har observerat att $c_m p^m \equiv 0 \mod p^{j+1}$ för alla $m \geq j+1$. Vi kommer med andra ord att ha

$$\begin{aligned} \alpha_1\beta_1 p^2 &\equiv 0 \mod p^2 \\ (\alpha_1\beta_2 + \alpha_2\beta_1)p^3 &\equiv 0 \mod p^3 \\ (\alpha_2\beta_2)p^4 &\equiv 0 \mod p^3 \\ \vdots \quad & \quad \vdots \quad \quad \vdots \end{aligned}$$

och alla dessa termer är alltså lika med noll.

Från hur multiplikation på $\mathbb{Z}_p$ är definierad (se anmärkning D.19) är

$$\begin{aligned}\theta(\alpha)\cdot\theta(\beta) &= (\alpha_0, \alpha_0+\alpha_1 p, \alpha_0+\alpha_1 p, \ldots)\cdot(\beta_0, \beta_0+\beta_1 p, \beta_0+\beta_1 p, \ldots)\\ &= (\alpha_0\beta_0, \alpha_0\beta_0 + (\alpha_1\beta_0+\alpha_0\beta_1)p + \cancel{\alpha_1\beta_1 p^2},\\ &\quad \alpha_0\beta_0 + (\alpha_1\beta_0+\alpha_0\beta_1)p + (\alpha_0\beta_2+\alpha_1\beta_1+\alpha_1\beta_0)p^2 +\\ &\quad \cancel{(\alpha_1\beta_2+\alpha_2\beta_1)p^3} + \cancel{(\alpha_2\beta_2)p^4}, \ldots)\\ &= \theta\left(\sum_{k=0}^{\infty}\left(\sum_{n=0}^{k}\beta_n\alpha_{k-n}\right)p^k\right) = \theta(\alpha\cdot\beta).\end{aligned}$$

Därför är $\theta$ en ringhomomorfi.

Slutligen vill vi se att $\theta$ är en bijektion. Av definition måste $\theta$ vara injektiv. Att $\theta$ även är surjektiv följer från att $\mathbb{Z}_p^{\text{algebraisk}}$ utgör precis de följer i $\prod_{k=1}^{\infty}\mathbb{Z}/p^k\mathbb{Z}$ som uppfyller $\varphi_k(a_k) = a_{k-1}$. □

# Referenser


[1] E. Artin. *The Collected Papers of Emil Artin*. Reading, Mass: Addison-Wesley Pub. Co., 1965. ISBN: 978-1-4614-5798-5.

[2] Gilles Bellot. "Introduction to $p$-adic numbers – an overview of ultrametric spaces and $p$-adic numbers". Examensarb. Aug. 2015. URL: https://bell0bytes.eu/content/images/mathematics/algnum/p-adic.pdf.

[3] P.M. Cohn. *Algebra Vol. 2*. Chichester, UK: John Wiley & Sons Ltd., 1977. ISBN: 0-471-01823-6.

[4] K. Conrad. *Trace and Norm*. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/tracenorm.pdf (hämtad 2019-05-03).

[5] V.B. Dem'yanov. "On cubic forms in discretely normed fields". I: *Doklady Akademii Nauk SSSR, n. Ser.* 74 (jan. 1950).

[6] F.Q. Gouvêa. *p-adic numbers: an introduction*. Berlin New York: Springer-Verlag, 1993. ISBN: 978-3-540-62911-5.

[7] M.J. Greenberg. *Lectures on forms in many variables*. New York: W.A. Benjamin, Inc., 1969. ISBN: 9784871877305.

[8] H. Hasse. "Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper". I: *Journal Fur Die Reine Und Angewandte Mathematik - J REINE ANGEW MATH* 1924 (jan. 1924), s. 113–130. DOI: 10.1515/crll.1924.153.113.

[9] K. Ireland och M. Rosen. *A Classical Introduction to Modern Number Theory*. New York, NY: Springer-Verlag New York, 1990. ISBN: 978-0-387-97329-6.

[10] S. Lang. *Algebra*. Reading, Massachusetts, USA: Addison-Wesley Publishing Company, Inc. third edition, 1999. ISBN: 0-201-55540-9.

[11] D. J. Lewis. "Cubic Homogeneous Polynomials Over $p$-Adic Number Fields". I: *Annals of Mathematics* 56.3 (1952), s. 473–478. ISSN: 0003486X. URL: http://www.jstor.org/stable/1969655.

[12] D. J. Lewis och Hugh L. Montgomery. "On zeros of $p$-adic forms." I: *Michigan Math. J.* 30.1 (1983), s. 83–87. DOI: 10.1307/mmj/1029002790. URL: https://doi.org/10.1307/mmj/1029002790.

[13] Yu. V. Matiyasevich. "The Diophantineness of enumerable sets". I: *Dokl. Akad. Nauk SSSR* 191.2 (1970), s. 279–282.

[14] L. J. Mordell. "A Remark on Indeterminate Equations in Several Variables". I: *J. London Math. Soc.* 12.2 (1937), s. 127–129. DOI: 10.1112/jlms/s1-12.1.127. URL: https://doi.org/10.1112/jlms/s1-12.1.127.

[15] M. Reid. *Undergraduate Commutative Algebra*. Cambridge, UK: Cambridge University Press, 1995. ISBN: 0-521-45889-7.

[16] W. Rudin. *Principles of mathematical analysis*. New York: McGraw-Hill, 1976. ISBN: 9780070856134.

[17] M. Spivak. *Calculus*. Berkeley, CA: Publish or Perish, Inc., 1994. ISBN: 0-914098-89-6.

[18] G. Terjanian. "Un contre-exemple à une conjecture d'Artin". I: *C. R. Acad. Sci. Paris Sér* A-B 262 (1966), A612.