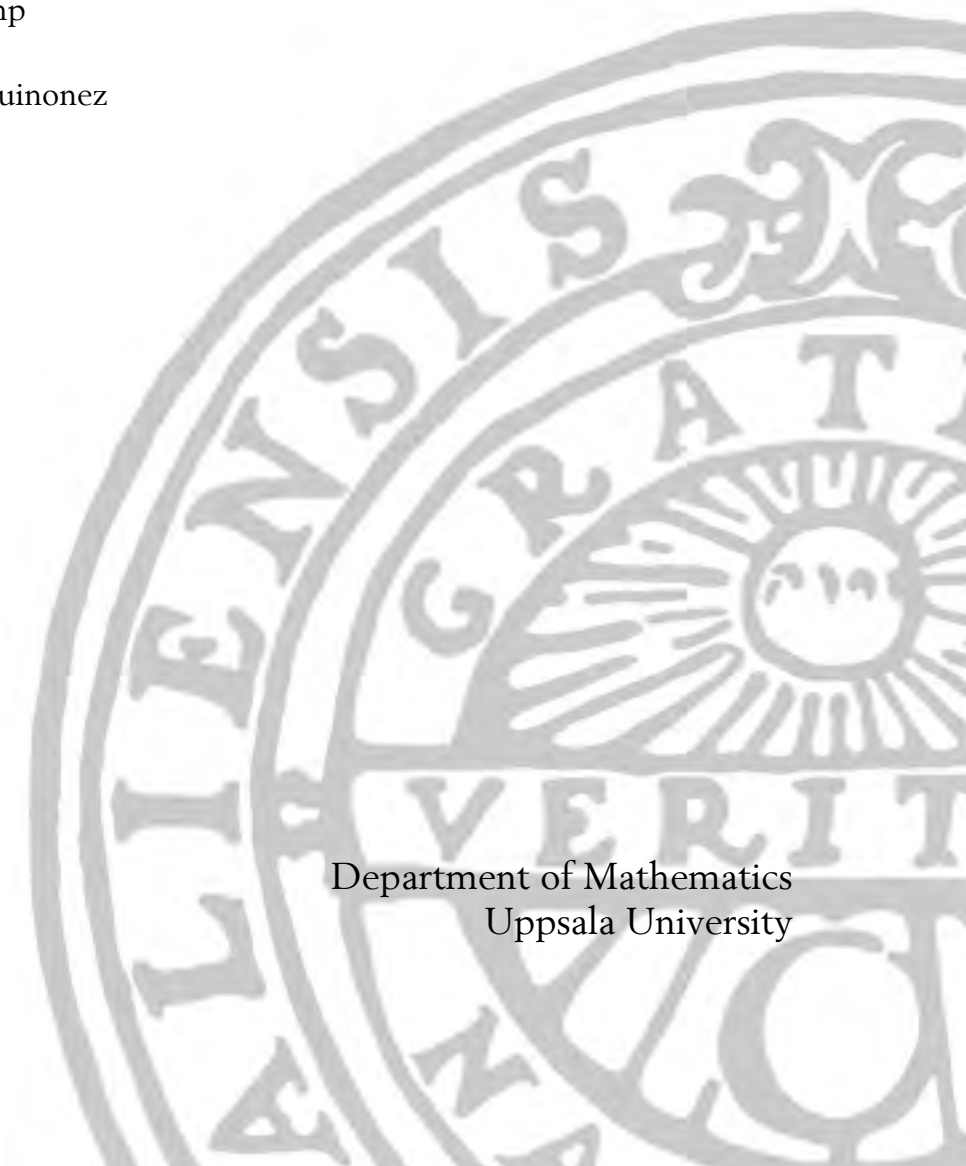
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2016:1

Om den kompletta tillslutningen av de p-adiska talen

Mårten Nilsson

Examensarbete i matematik, 15 hp
Handledare: Martin Herschend
Examinator: Veronica Crispin Quinonez
Februari 2016



Department of Mathematics
Uppsala University

Om den kompletta tillslutningen av de p-adiska talen

Författare: Mårten Nilsson Handledare: Martin Herschend

12 februari 2016

Sammanfattning

Denna kandidatuppsats i matematik behandlar konstruktionen av två talkroppar, de p-adiska talen samt de komplexa p-adiska talen, för varje primtal p. Kapitel 1 tjänar som en introduktion till de förstnämnda. Kapitel 2 behandlar processen "komplettering", som används vid de p-adiska talens formella konstruktion, samt i en klassisk konstruktion av de reella talen. Kapitel 3 innehåller den nödvändiga teorin för processen "tillslutning", som bland annat kan användas på de reella talen för att konstruera de komplexa talen. I kapitel 4 använder vi denna teori för att tillsluta de p-adiska talen. Efter detta noteras att resultatet tyvärr inte äger egenskapen "komplett", så vi utnyttjar teorin i kapitel 2 för att åtgärda detta. Slutligen konstaterar vi att resultatet av denna »sväng-om« - komplettering, tillslutning, komplettering - faktiskt är en algebraiskt sluten mängd, »den kompletta tillslutningen av de p-adiska talen«!

Innehåll

Kapitel 1

De p-adiska talen

1.1 Introduktion

I detta kapitel introduceras de p-adiska talen. För detaljer se [Koblitz, 1984]. De *p-adiska talen* är, på samma sätt som de reella talen, en klass av kroppar som innehåller de rationella talen; med andra ord utgör de, för varje primtal p, en *utvidgning* av dessa. Informellt är de en mängd av uttryck på formen

$$c_{-m} \cdot p^{-m} + ... + c_{-1} \cdot p^{-1} + c_0 + c_1 \cdot p^1 + ...,$$

där $0 \leq c_k < p$, varpå strukturen hos kropp är definierad. I analogi med de reella talen, där decimalutvecklingen tillåts fortsätta infinitivt, tillåter varje p-adiskt talsystem ovanstående utveckling.

De p-adiska talen kan konstrueras på flera sätt, och vilken av dessa som förefaller mest "naturlig" kan i hög grad hävdas bero på sammanhanget. T ex kan de p-adiska heltalen identifieras som de oändliga följder av heltal $\{a_i\}$ som uppfyller

$$\begin{aligned} &(1)\ 0 \leq a_i < p^i \\ &(2)\ a_i \equiv a_{i+1} \pmod{p^i}, \end{aligned}$$

vilka är av principiellt intresse i studiet av ekvationer i restklasser. De p-adiska talen kan sedan konstrueras utifrån denna ring. Andra isomorfa konstruktioner låter sig naturligt definieras i andra sammanhang, t ex utifrån vad man vill ha för egenskaper hos sin kroppsutvidgning.

1.2 Ett vägskäl som ger upphov till en analogi till $\mathbb{R}$

För en redogörelse av en annan situation där de p-adiska talen naturligt uppkommer, kan man till en början fråga sig vilka egenskaper man skulle vilja ha i en eventuell utvidgning av de rationella talen. En idé kan vara att titta på vad som finns hos den mest kända av kroppsutvidgningar, de reella talen. En sådan egenskap, som återfinns hos de rationella talen såväl som hos de reella talen, är

existensen av ett *absolutbelopp:*

$$|x| = \begin{cases} x & \text{om } x > 0, \\ -x & \text{annars,} \end{cases}$$

Egenskaperna hos denna funktion kan vi generalisera till begreppet *multiplikativ norm*. Detta definierar vi som en funktion $|\cdot|_* : K \to \mathbb{R}^+$ på en kropp K så att

(1) $|x|_* = 0$ om och endast om $x = 0$,
(2) $|x \cdot y|_* = |x|_* \cdot |y|_*$
(3) $|x + y|_* \leq |x|_* + |y|_*$.

Två vanliga sätt att benämna $|x|_*$ är att kalla det elementets *reellvärdiga evaluering* eller kort och gott elementets »absolutbelopp«.

Värt att påpeka är att i händelse av att en multiplikativ norm finns definierad, så kan man på ett naturligt sätt tala om avstånd genom att definiera en metrik såsom $d(x, y) = |x - y|_*$. Med en metrik kan man i sin tur *komplettera* en mängd. Detaljerna i detta kommer att diskuteras senare, men kort kan nämnas att detta är nyckelsteget i en vanlig konstruktion av de reella talen, vilket i samma veva skänker dem egenskapen av att vara *kompletta*.

Så, *om* vi kan hitta en alternativ, multiplikativ norm på de rationella talen, skulle vi kunna komplettera dessa med avseende på den metrik den normen inducerar. *Om* vi sedan »kan ta absolutbeloppet« av de nya tal som kompletteringen medför, skulle vi alltså ha en komplett kropputvidgning som precis som de reella talen äger egenskapen »absolutbelopp«. Finns det då några alternativa, multiplikativa normer?

Det visar sig att så är fallet. Exempelvis har vi den *triviala normen*,

$$|x|_0 = \begin{cases} 0 & \text{om } x = 0, \\ 1 & \text{annars.} \end{cases}$$

På $\mathbb{Q}$ kan man också, till följd av aritmetikens fundamentalsats, definiera en klass av mindre uppenbara, multiplikativa normer. Dessa är för varje primtal p den s k *p-adiska normen*,

$$|x|_p = \begin{cases} p^{-n} & \text{om } x = p^n \cdot \frac{a}{b}, p \not| ab, \\ 0 & \text{om } x = 0. \end{cases}$$

Dessa uppfyller de tre kraven ovan för en multiplikativ norm.

Bevis. (1) gäller per definition. Om $x = 0$ eller $y = 0$, gäller också (2) och (3) trivialt, så anta att $x = \frac{p^n \cdot a}{b}, y = \frac{p^m \cdot c}{d}$, där p inte delar a, b, c, d. Då har vi

$$|x \cdot y|_p = p^{-(m+n)} = p^{-m} \cdot p^{-n} = |x|_p \cdot |y|_p,$$

så (2). Anta nu att $n \leq m$. Då gäller

$$|x + y|_p = |p^n \frac{(ad + p^{m-n}bc)}{bd}|_p = |p^n|_p \cdot |ad + p^{m-n}bc|_p \cdot |\frac{1}{bd}|_p \leq p^{-n} = |x|_p,$$

då $|\frac{1}{bd}|_p = 1$ och $|ad + p^{m-n}bc|_p \leq 1$ då $ad + p^{m-n}bc$ är ett heltal. Motsvarande resonemang gäller om $m \leq n$, vilka tillsammans ger

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

vilket uppenbart är som mest $|x|_p + |y|_p$ (3). □

Det är lätt att kontrollera att t ex $\sqrt{|\cdot|}$ fortfarande är en multiplikativ norm, däremot är så inte fallet för $|\cdot|^2$ (då $2^2 = |2|^2 = |1+1|^2 \not\leq |1|^2 + |1|^2 = 2$). Alltså tycks vi i viss mån kunna konstruera nya »absolutbelopp«, som fortfarande uppfyller uppsatta kriterier, genom att upphöja någon av de tre ovanstående typerna med vissa reella tal. Finns det då några andra multiplikativa normer än dessa? Ett fantastiskt resultat från 1916 visar att så inte är fallet:

Ostrowskis sats. *Alla icke-triviala, multiplikativa normer $|\cdot|_*$ på $\mathbb{Q}$ kan antingen skrivas $|\cdot|_* = |\cdot|_p^t$, eller $|\cdot|_* = |\cdot|^t$, där $t > 0$ är ett reellt tal.*

Bevis. Detta bevis är hämtat ur [Koblitz, 1984]. Notera att $|\frac{m}{n}|_* = |m|_* \cdot |\frac{1}{n}|_*$ och $1 = |1|_* = |n|_* \cdot |\frac{1}{n}|_*$ ger $|\frac{m}{n}|_* = \frac{|m|_*}{|n|_*}$, samt att $|-1|_* = 1$, då $1 = |1|_* = |-1|_*|-1|_*$ och $|-1|_* > 0$. Därför räcker det med att kontrollera vad en multiplikativ norm gör med naturliga tal. Vi kan dela upp presumptiva normer i två fall: antingen finns det ett naturligt tal n med »absolutbelopp« större än 1, eller så gör det inte det. Vi kommer att se att det första fallet medför att $|\cdot|_*$ kan skrivas $|\cdot|^t$, den andra fallet att normen kan skrivas $|\cdot|_p^t$.

Fall I: $\exists n \in \mathbb{N} : |n|_* > 1$. Då finns det ett minsta sådant n, n_0. Då $|1|_* = 1$ måste $n_0 > 1$, och således kan vi skriva $|n_0|_* = n_0^t$, där t är ett positivt, reellt tal. Notera att alla naturliga tal n kan skrivas i bas n_0,

$$n = a_0 + a_1 \cdot n_0^1 + ... + a_s \cdot n_0^s, 0 \leq a_i < n_0,\ a_s \neq 0.$$

Detta innebär att

$$|n|_* \leq |a_0|_* + |a_1 \cdot n_0^1|_* + ... + |a_s \cdot n_0^s|_* = |a_0|_* + |a_1|_* \cdot n_0^{1t} + ... + |a_s|_* \cdot n_0^{st}.$$

Då $a_i < n_0$, och n_0 är det minsta tal n så att $|n|_* > 1$, måste $|a_i|_* \leq 1$, och vi kan skriva

$$|n|_* \leq 1 + n_0^t + ... + n_0^{st} = n_0^{st}(n_0^{-st} + ... + 1),$$

och vidare

$$|n|_* \leq n_0^{st}(n_0^{-st} + ... + 1) \leq n_0^{st} \sum_{i=0}^{\infty} \frac{1}{n_0^{it}} = n_0^{st} \cdot C \leq n^t \cdot C,$$

där de sista två stegen utnyttjar att summan är geometrisk med termerna $\to 0$, och $n \geq n_0^s$, på grund av att $n = a_0 + a_1 \cdot n_0^1 + ... + a_s \cdot n_0^s$.
Detta innebär att vi för $n = 1, 2, 3...$ har

$$\begin{aligned} & |n|_* \leq n^t \cdot C \\ \implies\ & |n^N|_* = |n|_*^N \leq n^{Nt} \cdot C \\ \implies\ & |n|_* = (|n|_*^N)^{\frac{1}{N}} \leq (n^{Nt} \cdot C)^{\frac{1}{N}} = n^t \cdot C^{\frac{1}{N}} \end{aligned}$$

för *alla* $N \in \mathbb{N}$. Genom att låta $N \to \infty$ har vi sedan $|n|_* \leq n^t$.

Det återstår att visa att $|n|_* \geq n^t$. Notera n skrivet i bas n_0 medför att $n_0^{s+1} > n \geq n_0^s$. Ett smärre omflyttning i $|n_0^{s+1}|_* = |n + n_0^{s+1} - n|_* \leq |n|_* + |n_0^{s+1} - n|_*$ ger

$$\begin{aligned} |n|_* &\geq |n_0^{s+1}|_* - |n_0^{s+1} - n|_* \\ &\geq n_0^{(s+1)t} - (n_0^{s+1} - n)^t, \end{aligned}$$

där vi använder att $|n_0^{s+1}|_* = |n_0|_*^{s+1}$, $|n_0| = n_0^t$ i den första termen, och att $|n|_* \leq n^t$ i den andra. Därefter ger $n \geq n_0^s$ att

$$\begin{aligned} |n|_* &\geq n_0^{(s+1)t} - (n_0^{s+1} - n_0^s)^t \\ &= n_0^{(s+1)t}(1 - (1 - \frac{1}{n_0})^t) \\ &\geq C' n^t, \end{aligned}$$

där C' endast beror på de fixerade talen N_0, t. Eftersom detta håller för alla n, håller det också för n^N. Genom att dra N:e roten på bägge sidor har vi sedan $|n|_* \geq n^t$, och således $|n|_* = n^t$. För ett rationellt tal $x = \pm\frac{p}{q}$ innebär detta att $|x|_* = |\pm 1|_* \cdot \frac{|p|_*}{|q|_*} = 1 \cdot \frac{p^t}{q^t} = (\frac{p}{q})^t = x^t$.

Fall II: $\forall n \in \mathbb{N} : |n|_* \leq 1$. Låt på motsvarande sätt n_0 vara det minsta n så att $|n|_* < 1$ (n_0 måste existera, för annars är $|...|_*$ den triviala normen). Vi kan direkt dra slutsatsen att n_0 är ett primtal, för om $n_0 = n_1 \cdot n_2$ med $n_1, n_2 < n_0$ så måste $|n_0|_* = |n_1|_*|n_2|_* = 1 \cdot 1 = 1$, vilket är en motsägelse. Fortsättningsvis benämner vi därför $n_0 = p$. Låt nu $q \neq p$ vara ett annat primtal. Anta att $|q|_* < 1$. Då har vi, för något stort N, $|q^N|_* = |q|_*^N < \frac{1}{2}$. Vi har också, för något stort M, $|p^M|_* = |p|_*^M < \frac{1}{2}$. Eftersom p^M, q^N är relativt prima kan vi skriva $mp^M + nq^N = 1$, där m, n är heltal (Euklides algoritm). Detta medför att

$$\begin{aligned} 1 = |1|_* = |mp^M + nq^N|_* &\leq |mp^M|_* + |nq^N|_* = |m|_*|p^M|_* + |n|_*|q^N|_* \\ &\leq |p^M|_* + |q^N|_* < \frac{1}{2} + \frac{1}{2} = 1, \end{aligned}$$

också en motsägelse - således måste $|q|_* = 1$. Detta implicerar i sin tur att för $x = p_1^{a_1} \cdot ... \cdot p_s^{a_s}$, där p_i är ett primtal och a_j är heltal, att $|x|_* = |p_1^{a_1}|_* \cdot ... \cdot |p_s^{a_s}|_* = 1 \cdot ... \cdot 1 \cdot |p_k^{a_k}|_* \cdot 1 \cdot ... \cdot 1$ (precis då $p_k = p$). Genom att skriva $|p|_* = p^{-t}$ (t>0) har vi sedan

$$|x|_* = |p_k^{a_k}|_* = |p_k|_*^{a_k} = (p^{-t})^{a_k} = (p^{-a_k})^t = (|x|_p)^t,$$

så i detta fall kan vi fånga $|\cdot|_*$ på formen $|\cdot|_p^t$. □

Det visar sig (se avsnitt 1.4) att om två normer förhåller sig $|\cdot|_1 = |\cdot|_2^t$ kommer de att ge upphov till samma komplettering. Det visar sig också att en komplettering med avseende på den triviala normen inte ger några nya tal överhuvudtaget; detta innebär att komplettering med avseende på någon av de p-adiska normerna är *de enda kompletteringar av* $\mathbb{Q}$ *varpå ett »absolutbelopp« potentiellt finns definierat* (förutom $\mathbb{R}$). Vi ska se att så är fallet.

1.3 Komplettera $\mathbb{Q}$: $\mathbb{R}$ i en handviftning

Ett central koncept när man talar om kompletteringar är begreppet *Cauchy-följd*. Formellt säger vi att en följd $(a_i) = (a_1, a_2...)$ av element i ett metriskt rum är *Cauchy-riktig*[1] om $\forall\epsilon\ \exists N\ \forall m, n \geq N : d(a_m, a_n) < \epsilon$. Med andra ord

[1] Detta begrepp har jag valt att införa då den engelska benämningen *Cauchy* inte fungerar särskilt väl som adjektiv i det svenska språket.

kommer elementen slutligen godtyckligt nära varandra. *Vad* de kommer godtyckligt nära till är dock inte självklart, och begreppet är inte liktydigt med en konvergent följd. Med avseende på det vanliga avståndet $|x-y|$ är t ex följden $(3, 3.1, 3.14, 3.141, ...)$ av rationella tal Cauchy-riktig, men då den kommer godtyckligt nära π och inte något rationellt tal, konvergerar den inte i $\mathbb{Q}$. Om alla Cauchy-riktiga följder i en mängd *konvergerar till ett element i mängden* säger vi att vi mängden är *komplett*; detta är en av de mest utmärkande egenskaperna hos de reella talen.

Att fullständigt bereda väg för hur man konstruktivt går från ett metriskt rum till ett komplett sådant kräver en djuplodad analys (se avsnitt 2.1), men inuitivt kan vi, som i exemplet ovan, se att vi med Cauchy-följder av rationella tal kan »peka på något nytt« - i synnerhet då på talet π, men i allmänhet på alla reella tal. Om två Cauchy-följder $(a_i), (b_i)$ skulle peka på samma tal kan man förvänta sig att $|a_t - b_t| \to 0$ när $t \to \infty$, och det visar sig att denna förväntan duger gott till att definiera en ekvivalensrelation på mängden av Cauchy-följder. På så sätt har man med dessa ekvivalensklasser lyckats etablera en 1-1-korrespondens med det vi vanligen uppfattar som reella tal. Faktum är att denna korrespondens t.o.m. kan tjäna som *definition* för dessa. Vad beträffar absolutbelopp kan man definiera detta på en Cauchy-följd (a_i) genom $\lim_{t\to\infty} |a_t|$. Att detta tal är detsamma för alla Cauchy-följder i en ekvivalensklass är lätt att visa. Om (b_i) tillhör samma ekvivalensklass har vi nämligen

$$|a_i| = |a_i - b_i + b_i| \leq |a_i - b_i| + |b_i|$$
$$|b_i| = |b_i - a_i + a_i| \leq |b_i - a_i| + |a_i|,$$

och då $|b_t - a_t| = |a_t - b_t| \to 0$ när $t \to \infty$ måste $\lim_{t\to\infty} |a_t| = \lim_{t\to\infty} |b_t|$. De andra två egenskaperna vi förväntar oss hos de reella talen - att de är kompletta samt att strukturen hos en kropp fortsätter att gälla - visar sig gälla generellt i kompletteringar av kroppar, vilket behandlas i detalj i avsnitt 2.3.

1.4 p-adisk komplettering av de rationella talen

Ovanstående konstruktion av de reella talen är i högsta grad beroende på valet av absolutbelopp och metriken som denna inducerar. Vad händer om vi, helt analogt, skulle välja någon av andra normerna på $\mathbb{Q}$ som står tillbuds istället?

Den metrik som den triviala normen inducerar medför att en följd endast är Cauchy-riktig om $\exists N : \ a_m = a_n \ \forall m, n > N$, vilka ju tillhör samma ekvivalensklass som den konstanta följden $(a_N, a_N, ...)$. Mängden av dessa har vi redan identifierat som $\mathbb{Q}$, och således är de rationella talen redan kompletta och en komplettering bidrar med intet nytt.

Det visar sig också, att om en följd är Cauchy-riktig med avseende på en metrik $|x-y|_*$, så är den också det för alla metriker på formen $|x-y|_*^t$, där t reellt. Detta inses enklast genom att för varje $\epsilon_1 > 0$ ta $\epsilon_2 = \epsilon_1^t$, eftersom vi då för varje Cauchy-följd (a_i) har

$$|a_m - a_n|_* < \epsilon_2 = \epsilon_1^t \iff |a_m - a_n|_*^t < \epsilon_1$$

för tillräckligt stora m, n. Detta tillsammans med Ostrowskis (i sammanhanget uttömmande) sats innebär att vi inte har många kandidater kvar.

En Cauchy-riktig följd med avseende på en av p-adiska metrikerna uppfyller $\forall\epsilon\ \exists N\ \forall m,n \geq N : |a_m - a_n|_p < \epsilon$. På motsvarande sätt som i den reella konstruktionen betraktar vi två följder $(a_i), (b_i)$ som ekvivalenta om $|a_t - b_t|_p \to 0$ när $t \to \infty$, och vi skriver $(a_i) \sim (b_i)$. Vi definierar återigen normen av en ekvivalensklass genom ett välja en representant (a_i) och beräkna

$$|(a_i)|_p = \lim_{t\to\infty} |a_t|_p.$$

Förutsatt att gränsvärdet är väldefinierat är detta detsamma för samtliga följder i en ekvivalensklass enligt samma resonemang som i avsnitt 1.3. Att gränsvärdet existerar kan visas på följande sätt. Vi kan anta $(a_i) \not\sim (0)$. För alla tillräckligt små ϵ finns då oändligt många k så att $|a_k|_p > \epsilon$. I synnerhet kan vi, eftersom $\exists N\ \forall m,n \geq N : |a_m - a_n|_p < \epsilon$, välja ett $k_N > N$ så $\forall m > N : |a_{k_N} - a_m|_p < \epsilon$. Detta medför att

$$\epsilon < |a_{k_N}|_p = |a_m + a_{k_N} - a_m|_p \leq \max\left(|a_m - a_{k_N}|_p, |a_m|_p\right) = |a_m|_p,$$

men

$$|a_m|_p = |a_m + a_{k_N} - a_{k_N}|_p \leq \max\left(|a_m - a_{k_N}|_p, |a_{k_N}|_p\right) = |a_{k_N}|_p$$

så $|a_{k_N}|_p = |a_m|_p$ för alla $m > N$, och alltså måste $|(a_i)|_p = \lim_{t\to\infty} |a_t|_p = |a_{k_N}|_p$. Mängderna av dessa p-adiskt Cauchy-riktiga följder i $\mathbb{Q}$ utgör alltså alternativa kompletteringar av $\mathbb{Q}$ där en multiplikativ norm *för alla element* fortfarande finns definierad. Hur knyter då dessa abstrakta objekt an till den informella definitionen av p-adiska tal i avsnitt 1.1? Kopplingen ges i följande sats:

Sats. *Varje ekvivalensklass a där $|a|_p \leq 1$ innehåller exakt en representant $\{a_i\}$ så att*

$$(1)\ 0 \leq a_i < p^i$$
$$(2)\ a_i \equiv a_{i+1} \pmod{p^i},$$

där $i = 1, 2, 3, ...$

Bevis. Detta bevis är hämtat från [Koblitz, 1984]. Vi börjar med att visa att (a_i) är unik. Antag därför att det finns en annan följd $(a_i'), a_{i_0} \neq a_{i_0}'$, som uppfyller (1), (2). (1) implicerar då att $a_{i_0}' \not\equiv a_{i_0} \bmod p^{i_0}$, och (2) medför $a_i' \not\equiv a_i \bmod p^{i_0}$ för alla $i \geq i_0$. $a_i' - a_i \not\equiv 0 \bmod p^{i_0}$ innebär att talet $a_i' - a_i$ innehåller som mest p^{i_0-1}, så

$$|a_i' - a_i|_p > \frac{1}{p^{i_0}}$$

för alla $i \geq i_0$, så $(a_i), (a_i')$ kan inte tillhöra samma ekvivalensklass.

Det återstår att visa att vi i varje ekvivalensklass kan hitta en följd som uppfyller (1), (2). För detta ändamål formulerar vi följande lemma:

Lemma. *Om x är ett rationellt tal så att $|x|_p \leq 1$, existerar det för alla i ett heltal $0 \leq \alpha \leq p^i - 1$ så att $|\alpha - x|_p \leq p^{-i}$.*

Bevis. Skriv $x = \frac{a}{b}$. Då b, p är relativt prima, kan vi skriva $mb + np^i = 1$. Det p-adiska avståndet från x till am blir då

$$|am - x|_p = |am - \frac{a}{b}|_p \leq |\frac{a}{b}|_p |mb - 1|_p \leq |mp - 1|_p = |np^i|_p = \frac{|n|_p}{p^i} \leq \frac{1}{p^i}.$$

Eftersom vi för varje heltal s har

$$|am - x + sp^i|_p \leq \max\left(|am - x|_p, |sp^i|_p\right) \leq \frac{1}{p^i}$$

kan vi sedan förskjuta am med sp^i tills vi funnit ett heltal $\alpha = am + sp^i$ i $\{0, 1, ..., p^i - 1\}$. □

Låt (b_i) nu vara en godtycklig Cauchy-följd med $|(b_i)|_p \leq 1$. Från denna vill vi konstruera en ekvivalent Cauchy-riktig följd $\{a_i\}$ som uppfyller (1), (2). Om vi låter $N(j)$ beteckna det tal så att $|b_i - b_{i'}|_p \leq p^{-j}$ när $i, i' \geq N(j)$ (att (b_i) är Cauchy-riktig tillåter oss göra detta), och antar att $N(j) \geq j$, kan vi med lemmat hitta (a_j) med $0 \leq a_j < p^j$ så att

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

Detta är möjligt eftersom kravet $|b_i|_p \leq 1$ uppfylls för alla $i \geq N(1)$, då

$$|b_i|_p \leq \max\left(|b_{i'}|_p, |b_i - b_{i'}|_p\right)$$

och $|b_{i'}|_p \to 1$ när $i' \to \infty$ ($|b_i - b_{i'}|_p \leq 1$ följer ur N:s konstruktion). Denna följd (a_i) uppfyller uppenbarligen (1), och kvar återstår att visa ekvivalens samt att (2) uppfylls. Ekvivalens har vi då vi givet något j och $i \geq N(j)$ kan skriva

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

men

$$\begin{aligned}
|a_i - a_j|_p &= |a_i - b_{N(i)} - (a_j - b_{N(i)})|_p \leq \max\left(|a_i - b_{N(i)}|_p, |a_j - b_{N(i)}|_p\right) \\
&= \max\left(|a_i - b_{N(i)}|_p, |a_j - b_{N(j)} - (b_{N(i)} - b_{N(j)})|_p\right) \\
&\leq \max\left(|a_i - b_{N(i)}|_p, |a_j - b_{N(j)}|_p, |(b_{N(i)} - b_{N(j)})|_p\right) \\
&\leq \max\left(\frac{1}{p^i}, \frac{1}{p^j}, \frac{1}{p^j}\right) = \frac{1}{p^j},
\end{aligned}$$

så $|a_i - b_i|_p \to 0$ när $i \to \infty$. Egenskap (2), det vill säga att $a_i \equiv a_{i+1} \bmod p^i$, följer ur ett specialfall av ovanstående,

$$|a_{i+1} - a_i|_p \leq \max\left(\frac{1}{p^{i+1}}, \frac{1}{p^i}, \frac{1}{p^i}\right) = \frac{1}{p^i},$$

eftersom $a_{i+1} - a_i$ i sådana fall åtminstone är delbart med p^i, vilket innebär att $a_i - a_{i+1} \equiv 0 \bmod p^i \iff a_i \equiv a_{i+1} \bmod p^i$. □

Med detta i bagaget ska vi nu visa hur ett uttryck $b_0 + b1 \cdot p^1 + ...$ precis motsvarar en följd (a_i), och därigenom precis en ekvivalensklass $a = [(a_i)]$. Betrakta sekvensen $(a_1, a_2, ...) = (b_0, b_0 + b_1 \cdot p^1, ...)$, där $0 \leq b_k < p$. Egenskap (2) håller uppenbarligen, eftersom $\forall j \geq i : a_j - a_i = b_{i+1} \cdot p^{i+1} + ... + b_j \cdot p^j \equiv 0 \mod p^i$. Då varje a_i dessutom kan ses som ett i siffror långt, positivt tal i basen p följer det också att $0 \leq a_i < p^i$ (1). Elementen i denna följd utgör delsummorna i uttrycket $b_0 + b_1 \cdot p^1 + ...$, och eftersom dessa bildar en p-adiskt Cauchy-riktig följd är denna summa *per definition* ett element i $\mathbb{Q}_p$; faktum är att vi precist identifierar a med denna oändliga summa. Detta är egentligen helt analogt med oändliga summor i de reella talen, som också formellt definieras som Cauchy-följder av delsummor.

Hur gör vi då om vår ekvivalensklass a inte uppfyller $|a|_p \leq 1$? I synnerhet har vi då $|a|_p = p^m$, och i sådana fall kan vi konstruera $a' = a \cdot p^m$ som uppfyller $|a|_p \leq 1$ och lämpar sig för satsen ovan. Detta innebär att alla p-adiska tal kan skrivas som en summa av rationella tal:

$$a = b_0 \cdot p^{-m} + ... + b_{m-1} \cdot p^{-1} + b_m + b_{m+1} \cdot p^1 + ...,$$

eller om $b_n = c_{n-m}$,

$$a = c_{-m} \cdot p^{-m} + ... + c_{-1} \cdot p^{-1} + c_0 + c_1 \cdot p^1 + ...$$

för att exakt återge den informella definition som gavs i avsnitt 1.1. Det är dock inte trivialt huruvida en kroppstruktur fortfarande föreligger i denna komplettering, och för detta ändamål ska vi i kapitel 2 betrakta ämnet ur ett mer generellt perspektiv.

1.5 Polynomiella ekvationer i $\mathbb{Q}_p$

Slutligen ska vi kort diskutera polynomiella ekvationer i $\mathbb{Q}_p$. För en mer detaljerad framställning (som bland annat behandlar den p-adiska varianten av Newtons metod), se [Koblitz, 1984]. I detta sammanhang kommer det faktum att vi alltid kan finna en representant

$$a = b_0 \cdot p^{-m} + ... + b_{m-1} \cdot p^{-1} + b_m + b_{m+1} \cdot p^1 + ...$$

väl till pass. För att inse detta kan vi till en början notera att ovanstående uttryck har som konsekvens att

$$p^m \cdot a \equiv b_0 + b_1 \cdot p + ... + b_{i-1} \cdot p^{i-1} \pmod{p^i},$$

för alla naturliga tal i. I synnerhet bör det fall då $|a|_p \leq 1$ uppmärksammas, eftersom m då är lika med noll, och a då i varje restklass kan hanteras som vilket heltal som helst.

Bektrakta nu ekvationen $P(x) = 0$, där P är ett polynom med koefficienter i $\mathbb{Q}_p$. Genom att multiplicera med den största normen bland P:s koefficienter kan vi omvandla detta uttryck till $Q(x) = 0$, där Q nu istället är ett polynom med koefficienter vars p-adisk normer är mindre eller lika med 1. Detta innebär att vi kan skriva

$$Q(x) \equiv Q_i(x) \pmod{p^i},$$

där varje Q_i är ett polynom med heltalskoefficienter. Antag nu att det finns något p-adiskt tal s som uppfyller $Q(s) = 0$. Vi får två fall. Om det skulle förhålla sig så att $|s|_p \leq 1$, skulle den obekanta i varje restklass kunna hanteras som ett heltal. Med andra ord skulle problemet reduceras till att för varje i lösa $Q_i(x) \equiv 0 \pmod{p^i}$, och rent konkret skulle $i = 1$ generera den första »p-adiska siffran«, vilken induktivt sedan skulle kunna användas för att bestämma nästkommande siffra genom att lösa Q:s nollställen i nästa restklass. I det andra fallet, om $|s|_p > 1$, är detta förfarande självfallet inte möjligt. För att undkomma detta, skriv $Q(x) = a_0 + a_1x + ... + a_nx^n$. Ekvationen $Q(x) = 0$ ger då att

$$\begin{aligned} a_1x + ... + a_nx^n &= -a_0 \\ |a_1x + ... + a_nx^n|_p &= |a_0|_p = p^{-m}, \end{aligned}$$

där V.L. $\leq \max\left(|a_lx^l|_p\right)_{l\in\{1,...,n\}} = |a_j|_p|x^j|_p = p^{-k}|x|_p^j$, så

$$\begin{aligned} p^{-m} &\leq p^{-k}|x|_p^j \\ |x|_p^{-j} &\leq p^{m-k} \\ |x|_p &\leq p^{\frac{k-m}{j}} = \left(\frac{|a_0|_p}{|a_j|_p}\right)^{\frac{1}{j}}. \end{aligned}$$

Alltså: Om a_0 inte är p-adiskt större än någon av de andra koefficienter i polynomet, skulle man kunna garantera att Q endast har lösningar s som uppfyller $|s|_p \leq 1$. Ett exempel på ett sådant polynom är $R(x) = Q(|a_0|_p \cdot x)$, och R:s nollställen går således att finna med metoden skisserad ovan. Dessa lösningar skiljer sig bara från vårt första polynom P:s nollställen med faktorn $|a_0|_p$, så på detta vis kan vi alltid finna en lösning till $P(x) = 0$ förutsatt att en sådan existerar.

Detta är dock inte alltid fallet. Ett exempel är ekvationen $x^2 - 2 = 0$ i $\mathbb{Q}_5$, eftersom denna - trots att kravet $|a_0|_5 \leq |a_2|_5$ uppfylls - inte har någon lösning i mod 5. I allmänhet kan vi för varje p hitta polynom utan lösningar i $\mathbb{Q}_p$. De p-adiska talkropparna är alltså, i likhet med till exempel $\mathbb{R}$, *inte* algebraiskt slutna. För en generell diskussion med mål att åtgärda detta, se kapitel 3. I kapitel 4 ägnar vi oss åt att tillämpa denna teori till att från varje $\mathbb{Q}_p$ konstruera talkroppen Ω_p, som dels är algebraiskt sluten samt komplett, och dessutom har $\mathbb{Q}_p$ som delkropp.

Kapitel 2

Om komplettering

2.1 Ett generellt sätt att utvidga ett metriskt rum

Som vi såg i kapitel 1 kan de rationella talen ses som en delmängd av ekvivalensklasser av Cauchy-riktiga följder, om elementen i $\mathbb{Q}$ identifieras som de ekvivalensklasser som innehåller konstanta följder. Det finns ingenting som hindrar oss från att utföra motsvarande konstruktion på ett godtyckligt metriskt rum X, eftersom varken Cauchy-riktiga följder eller ekvivalensrelationen på dessa ($x \sim y \iff \lim_{n\to\infty} d(x_n, y_n) = 0$) kräver något annat än att avståndet mellan två element finns definierat. På så sätt kan man i generella ordalag tala om *kompletteringen* $\overline{X}$ av ett metriskt rum X,

$$\overline{X} = \{[(x_n)] : (x_n) \text{ Cauchy-riktig följd i } X\}.$$

Vad kan vi säga om denna mängd? Går det att utvidga metriken på X, så att $\overline{X}$ också är ett metriskt rum? Är $\overline{X}$ *komplett*, det vill säga: konvergerar varje Cauchy-riktig följd i $\overline{X}$ till ett element i $\overline{X}$? Terminologin ger en fingervisning om att så är fallet, vilket fångas i följande sats:

Sats. *För alla element $\bar{x}, \bar{y} \in \overline{X}$ definierar*

$$\bar{d}(\bar{x}, \bar{y}) = \lim_{n\to\infty} d(x_n, y_n)$$

en metrik. Med avseende på denna är $\overline{X}$ komplett.

Bevis. Detta bevis är huvudsakligen från [Nironi, 2007], så när på en del detaljer. Vi börjar med att visa att gränsvärdet ovan existerar. Tag två Cauchy-riktiga följder $(x_i), (y_j)$. Då existerar något N så att $d(x_N, x_n), d(y_N, y_n) < \epsilon$ om $n \geq N$, och

$$\begin{aligned}
\lim_{n\to\infty} d(x_n, y_n) &\leq \lim_{n\to\infty} (d(x_N, x_n) + d(x_N, y_n)) \\
&\leq d(x_N, y_N) + \lim_{n\to\infty} (d(x_N, x_n) + d(y_N, y_n)) \\
&< d(x_N, y_N) + 2\epsilon,
\end{aligned}$$

vilket visar att gränsvärdet konvergerar. Antag nu att $x \sim x', y \sim y'$. Eftersom

$$d(x_n, y_n) \leq d(x_n, x'_n) + d(x'_n, y'_n) + d(y'_n, y_n)$$
$$d(x'_n, y'_n) \leq d(x'_n, x_n) + d(x_n, y_n) + d(y_n, y'_n)$$

måste

$$|d(x_n, y_n) - d(x'_n, y'_n)| \leq d(x_n, x'_n) + d(y'_n, y_n),$$

men detta uttryck går mot 0 när $n \to \infty$. Detta innebär att $\lim_{n\to\infty} d(x_n, y_n) = \lim_{n\to\infty} d(x'_n, y'_n)$, så $\bar{d}$ är väldefinierad.

För att visa att $\bar{d}$ är en metrik erinrar vi oss att $\bar{d}$ i sådana fall måste uppfylla

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

Eftersom $\bar{x} \sim \bar{y} \leftrightarrow \lim_{n\to\infty} d(x_n, y_n) = 0$ gäller per definition (1). Egenskap (2) ärvs då

$$\bar{d}(\bar{x}, \bar{y}) = \lim_{n\to\infty} d(x_n, y_n) = \lim_{n\to\infty} d(y_n, x_n) = \bar{d}(\bar{y}, \bar{x}),$$

och (3) följer då

$$d(x_n, y_n) \leq d(x_n, z_n) + d(z_n, y_n)$$
$$\lim_{n\to\infty} d(x_n, y_n) \leq \lim_{n\to\infty} d(x_n, z_n) + \lim_{n\to\infty} d(z_n, y_n)$$
$$\bar{d}(\bar{x}, \bar{y}) \leq d(\bar{x}, \bar{z}) + d(\bar{z}, \bar{y}).$$

För att visa att $\overline{X}$ är komplett preciserar vi först vår utsaga att X motsvaras av de ekvivalensklasser i $\overline{X}$ som innehåller en konstant följd. Vi skriver

$$\varphi : X \to \overline{X}, x \mapsto [(x, x, x....)]$$

och noterar att

$$\bar{d}(\varphi(x), \varphi(y)) = \lim_{n\to\infty} d(x, y) = d(x, y),$$

så φ utgör en isometri från X till $\overline{X}$. Bilden av denna avbildning äger två egenskaper så pass viktiga, att de med fördel kan summeras i ett lemma.

Lemma.

1. *I varje omgivning kring ett element i $\overline{X}$ kan vi hitta ett element i bilden $\varphi(X)$ ($\varphi(X)$ är* tät *i $\overline{X}$),*
2. *Varje Cauchy-riktig följd i $\varphi(X)$ konvergerar till ett element i $\overline{X}$.*

Bevis. Tag $\bar{x} = [(x_i)] \in \overline{X}$. Eftersom (x_i) är Cauchy-riktig kan vi $\forall \epsilon > 0$ hitta ett N så att $d(x_m, x_N) < \frac{\epsilon}{2}$, $\forall m \geq N$. Detta innebär att avståndet från $\bar{x}$ till elementet $[(x_N, x_N, ...)] \in \overline{X}$ blir

$$\bar{d}(\bar{x}, [(x_N, x_N, ...)]) = \lim_{n\to\infty} (x_n, x_N) \leq \frac{\epsilon}{2} < \epsilon,$$

så $\varphi(X)$ är tät i $\overline{X}$.

För att visa att varje Cauchy-riktig följd $\{\varphi(x_1), \varphi(x_2), ...\}$ i $\varphi(X)$ konvergerar till ett element i $\overline{X}$, skriver vi $\hat{x}_i = |(x_i, x_i, ...)|$ och noterar att

$$\bar{d}(\hat{x}_m, \hat{x}_n) = d(x_m, x_n),$$

så i sådana fall är följden $(x_1, x_2...)$ Cauchy-riktig i X. Detta innebär att det för varje ϵ existerar ett N så att

$$d(x_k, x_N) < \frac{\epsilon}{2}, \ \forall k \geq N.$$

Om vi nu skriver $\bar{x} = [(x_1, x_2...)]$ implicerar detta för varje ϵ att

$$\bar{d}(\bar{x}, \hat{x}_k) = \lim_{n\to\infty} d(x_n, x_N) \leq \frac{\epsilon}{2} < \epsilon,$$

för alla $k \geq N$. Således kommer följden godtyckligt nära $\bar{x}$, och lemmat är visat. □

Tag nu en Cauchy-riktig följd $(\bar{x}_1, \bar{x}_2, ...)$ med element i $\overline{X}$. Enligt lemmat är $\varphi(X)$ är tät i $\overline{X}$, så för varje ϵ kan vi välja $\hat{x}_i \in \varphi(X)$ så att $\hat{x}_i \in B_{\frac{\epsilon}{3}}(\bar{x}_i)$. Två element i $(\hat{x}_1, \hat{x}_2, ...)$ uppfyller för tillräckligt stora m, n

$$\begin{aligned}\bar{d}(\hat{x}_m, \hat{x}_n) &\leq \bar{d}(\hat{x}_m, \bar{x}_m) + \bar{d}(\bar{x}_m, \hat{x}_n) \leq d(\hat{x}_m, \bar{x}_m) + \bar{d}(\bar{x}_m, \bar{x}_n) + \bar{d}(\bar{x}_n, \hat{x}_n) \\ &< \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon,\end{aligned}$$

så dessutom garanterar lemmat att $(\hat{x}_1, \hat{x}_2, ..)$ konvergerar mot något $\bar{x} \in \overline{X}$. Alltså, för tillräckligt stora n gäller

$$\bar{d}(\bar{x}_n, \hat{x}_n) < \frac{\epsilon}{3}$$

och

$$\bar{d}(\bar{x}, \hat{x}_n) < \frac{2\epsilon}{3},$$

vilka tillsammans med triangelolikheten ger att

$$\bar{d}(\bar{x}, \bar{x}_n) \leq \bar{d}(\bar{x}, \hat{x}_n) + \bar{d}(\bar{x}_n, \hat{x}_n) < \frac{2\epsilon}{3} + \frac{\epsilon}{3} = \epsilon.$$

Detta visar att varje Cauchy-följd $(\bar{x}_1, \bar{x}_2, ...)$ i $\overline{X}$ konvergerar mot något $\bar{x}$ i $\overline{X}$, och således är $\overline{X}$ komplett. □

Från ett godtyckligt metriskt rum X kan vi alltså alltid konstruera ett annat, komplett metriskt rum $\overline{X}$. Med detta kan vi sedan konstruera en komplett utvidgning (E, d_E) till (X, d) på följande vis: Sätt $E = X \cup (\overline{X} \setminus \varphi(X))$, och definiera en bijektion $\vartheta : E \to \overline{X}$ genom

$$\vartheta(x) = \begin{cases} \varphi(x) & \text{om } x \in X \\ x & \text{annars.} \end{cases}$$

Om $d_E(x, y) = \bar{d}(\vartheta(x), \vartheta(y))$ är $(\overline{X}, \bar{d}), (E, d_E)$ isometriska, så (E, d_E) är komplett, och om d_E begränsas till delmängden $X \subset {}^1E$ sammanfaller denna dessutom med d. Med hjälp av denna *kirurgi* kan man således alltid utvidga ett

[1] Symbolen "$\subset$" är här synonym med *delmängd av*. För att beteckna strikt delmängd kommer "$\subsetneq$" att användas.

metriskt rum till ett komplett sådant, så att de egenskaper rummet besitter kvarstår i det utvidgade rummet. I detta skede är vi mogna att ställa oss frågan: Kan detta kompletteringförfarande bevara någonting mer, om vi utgår från ett metriskt rum med ytterligare algebraisk struktur? Med tanke på att texten utgår från $\mathbb{Q}$, är förstås komplettering av kroppar av särskilt intresse.

2.2 Förutsättningar för att komplettera en kropp

Låt oss utgå från en generell kropp K, varpå en metrik av något slag finns definierad. Med tillvägagångssättet i 2.1 kan vi då konstruera dennas komplettering $\widehat{K}$[2]. Då $x \mapsto [(x, x, ...)]$, och således $x+y \mapsto [(x+y, x+y, ...)]$, $xy \mapsto [(xy, xy, ...)]$, kan det tyckas naturligt att utvidga kroppens två operationer till

$$+ : \widehat{K} \times \widehat{K} \to \hat{K}, \quad ([(x_i)], [(y_i)]) \mapsto [(x_i + y_i)]$$
$$\bullet : \widehat{K} \times \widehat{K} \to \hat{K}, \quad ([(x_i)], [(y_i)]) \mapsto [(x_i \cdot y_i)].$$

För våra syften måste vi dock vara säkra på två saker: För det första måste vi kunna garantera att dessa funktioner, givet två Cauchy-följder som invärde, alltid producerar en Cauchy-riktig följd som utvärde. För det andra måste det gälla att den ekvivalensklass som motsvarar "summan" respektive "produkten" ovan inte beror på vilket par av representanter vi väljer i $([(x_i)], [(y_i)])$.

Detta är ingalunda någonting som varje metrik uppfyller. Tag till exempel $(\mathbb{Q}, d)$, där $d(x, y) = |\arctan(x) - \arctan(y)|$. I händelse av att någon läsare behöver övertygas om att detta faktiskt är en metrik kan det påpekas att detta direkt följer från att vi redan konstaterat detta för $|\cdot - \cdot|_*$ (visas i 2.3), samt det faktum att arctan är injektiv. Med avseende på denna metrik har vi $(x_i) = (1, 1, 3, 3, 5, 5, ...)$ samt $(y_i) = (0, -1, -2, -3, ...)$ som exempel på Cauchy-riktiga följder och således element i någon ekvivalensklass i $\widehat{K}$. I summan av dessa följder, $(1, 0, 1, 0, ...)$, förblir dock avståndet mellan två efter varandra följande element $|\arctan(1) - \arctan(0)| = \frac{\pi}{4}$. Detta innebär att följdens termer inte kommer godtyckligt nära varandra, och att följden således inte är Cauchy-riktig.

2.3 Kompletteringar av kroppar med absolutbelopp

I en kropp K utrustad med en multiplikativ norm $|\cdot|_*$ har vi som följd också för alla x, y i K en metrik $d(x, y) = |x - y|_*$, eftersom

$$d(x, y) = |x - y|_* = 0 \text{ om och endast om } x = y, \tag{1}$$
$$d(x, y) = |x - y|_* = |y - x|_* = d(y, x), \tag{2}$$
$$d(x, y) = |x - y|_* = |x - z + z - y|_* \leq |x - z|_* + |z - y|_* = d(x, z) + d(z, y). \tag{3}$$

Resonemang i 2.1 garanterar vidare att

$$\hat{d}(\hat{x}, \hat{y}) = \lim_{n \to \infty} |x_n - y_n|_*$$

[2]Observera att vi i kroppssammanhang skriver $\widehat{K}$ istället för $\overline{K}$ för att beteckna en komplettering, då den senare är reserverad som beteckning för en kropps s k tillslutning (se avsnitt 3.4).

existerar och är väldefinierad. I synnerhet gäller detta $\hat{d}(\hat{x}, 0)$, vilket innebär att vi kan definiera

$$|\hat{x}|_* := \lim_{n\to\infty} |x_n|_*.$$

Det visar att detta, givet att operationerna i 2.2 är väldefinierade, faktiskt är utgör ett absolutbelopp på $\widehat{K}$, eftersom samtliga krav i avsnitt 1.2,

(1) "$|x|_* = 0 \iff x = 0$"**:**

$$|\hat{x}|_* = 0 = \hat{d}(\hat{x}, \hat{0}) = 0 \text{ om och endast om } \hat{x} = \hat{0},$$

(2) "$|x \cdot y|_* = |x|_* \cdot |y|_*$"**:**

$$\begin{aligned} |\hat{x} \bullet \hat{y}|_* &= \lim_{n\to\infty} |x_n \cdot y_n|_* = \lim_{n\to\infty} (|x_n|_* \cdot |y_n|_*) \\ &= \lim_{n\to\infty} (|x_n|_*) \cdot \lim_{n\to\infty} (|y_n|_*) = |\hat{x}|_* \cdot |\hat{y}|_*, \end{aligned}$$

(3) "$|x + y|_* \leq |x|_* + |y|_*$"**:**

$$\begin{aligned} |\hat{x} + \hat{y}|_* &= \lim_{n\to\infty} |x_n + y_n|_* \leq \lim_{n\to\infty} (|x_n|_* + |y_n|_*) \\ &= \lim_{n\to\infty} (|x_n|_*) + \lim_{n\to\infty} (|y_n|_*) = |\hat{x}|_* + |\hat{y}|_* \end{aligned}$$

då uppfylls.

Med antagandet att vår metrik är norminducerad ska vi åter betrakta situationen i 2.2. Denna visar sig vara så hanterbar att ingenting mer krävs för att garantera att kroppstrukturen bibehålls, vilket vi summerar i följande sats:

Sats. *Låt K vara en kropp varpå en multiplikativ norm finns definierad. Då är dennas komplettering med avseende på den norminducerade metriken också en kropp, med*

$$\begin{aligned} + &: \hat{K} \times \hat{K} \to \hat{K}, \quad ([(x_i)], [(y_i)]) \mapsto [(x_i + y_i)] \\ \bullet &: \hat{K} \times \hat{K} \to \hat{K}, \quad ([(x_i)], [(y_i)]) \mapsto [(x_i \cdot y_i)]. \end{aligned}$$

Bevis. Vi erinrar oss att vi dels måste kontrollera att två Cauchy-följder som invärde ger upphov till en Cauchy-riktig följd som utvärde, samt att vi alltid hamnar i samma ekvivalensklass oavsett val av representanter som invärden. Med detta i åtanke börjar vi med att visa att additionen uppför sig väl. Tag för varje ϵ_{x+y}, $\epsilon = \frac{\epsilon_{x+y}}{2}$ och ett N så att $\forall m, n \geq N : \ |x_m - x_n|_*, |y_m - y_n|_* < \epsilon$. Då gäller

$$\begin{aligned} |x_m + y_m - (x_n + y_n)|_* = |x_m - x_n + y_m - y_n)|_* &\leq |x_m - x_n|_* + |y_m - y_n|_* \\ &< \frac{\epsilon_{x+y}}{2} + \frac{\epsilon_{x+y}}{2} = \epsilon_{x+y}. \end{aligned}$$

För att visa att $\hat{x} + \hat{y}$ inte beror på valet av representanter, tag godtyckliga $(x_i), (x_i') \in \hat{x}, (y_i), (y_i') \in \hat{y}$. För dessa gäller

$$|x_n + y_n - (x_n' + y_n')|_* = |x_n - x_n' + y_n - y_n')|_* \leq |x_n - x_n'|_* + |y_n - y_n'|_*,$$

vilket ju går mot 0 när $n \to \infty$, och sålunda hamnar vi i alltid samma ekvivalensklass, oavsett val av representanter i $\hat{x}, \hat{y}$.

För att övertyga oss om att också $\hat{x} \cdot \hat{y}$ är en väldefinierad ekvivalensklass av Cauchy-riktiga följder går vi till väga på samma sätt. Vi visar först att $(x_i \cdot y_i)$ är Cauchy-riktig. Tag L så att $x_i, y_i < L$ för alla i, och tag vidare något N, så att $\forall\ m, n \geq N:\ |x_m - x_n|_*, |y_m - x_n|_* < \frac{\epsilon_{xy}}{2L}$. Då gäller

$$\begin{aligned} |x_m \cdot y_m - x_n \cdot y_n|_* &= |x_m \cdot y_m - x_m \cdot y_n + x_m \cdot y_n - x_n \cdot y_n|_* \\ &\leq |x_m(y_m - y_n)|_* + |y_n(x_m - x_n)|_* \\ &\leq L(|y_m - y_n|_* + |x_m - x_n|_*) < L(\frac{\epsilon_{xy}}{2L} + \frac{\epsilon_{xy}}{2L}) = \epsilon_{xy}, \end{aligned}$$

så $(x_i \cdot y_i)$ är Cauchy-riktig. Denna produkt hamnar också i samma ekvivalensklass oavsett val av Cauchy-följd i $\hat{x}, \hat{y}$ eftersom

$$\begin{aligned} |x_n \cdot y_n - x'_n \cdot y'_n| &\leq |x_n(y_n - y'_n)|_* + |y'_n(x_n - x'_n)|_* \\ &\leq |x_n|_*|(y_n - y'_n)|_* + |y'_n|_*|(x_n - x'_n)|_*, \end{aligned}$$

som ju också går mot 0 när $n \to \infty$.

Således har vi för alla $\hat{x}, \hat{y} \in \widehat{K}$ att $\hat{x} + \hat{y}, \hat{x} \cdot \hat{y} \in \widehat{K}$, och $\widehat{K}$ är en kommutativ ring. Faktum är att detta även gäller för mängden av Cauchy-följder i K. För att visa implikationen $\hat{x} \in \widehat{K} \setminus \hat{0} \implies \hat{x}^{-1} \in \widehat{K}$, och att $\widehat{K}$ därmed är en kropp, ska vi dock dra nytta av den ekvivalensrelation vi definierat.

Notera först att det för alla Cauchy-följder i en ekvivalensklass gäller

$$|\hat{x}|_* - \epsilon < |x_m|_* < |\hat{x}|_* + \epsilon,$$

för tillräckligt stora m (notera att vi här åberopar det faktum att $|\hat{x}|_*$ alltid existerar). Följdaktligen måste, om $\hat{x} \neq 0$, samtliga Cauchy-följder i $\hat{x}$ endast innehålla ett ändligt antal icke-nollskilda element. Detta innebär i sin tur att vi från en sådan följd (x_i) kan definiera

$$x'_i = \begin{cases} x_i & \text{om } i \geq N, \\ 1 & \text{annars,} \end{cases}$$

och $(x'_i) \sim (x_i)$ då $|x'_i - x_i|_* = 0$ om $i \geq N$, och således också ett element i $\hat{x}$. Denna följd lämpar sig ypperligt att invertera »element per element«,

$$x_i^{-1} = \frac{1}{x'_i} = \begin{cases} \frac{1}{x_i} & \text{om } i \geq N, \\ 1 & \text{annars,} \end{cases}$$

och på så sätt bilda $[(x_i^{-1})]$, en klar kandidat som invers till $\hat{x}$ förutsatt att följden är Cauchy-riktig, eftersom vi då skulle ha $[(x_i^{-1})] \bullet [(x'_i)] = [(1, 1, ...)] = \hat{1} \in \widehat{K}$. För detta ändamål, notera först att det existerar ett N, så att $\forall m, n \geq N:\ |x'_m - x'_n|_* < \frac{\epsilon_{x'^{-1}}|\hat{x}|_*^2}{4}$. Låt vidare N vara så pass stort att $|x_m|_* > \frac{|\hat{x}|_*}{2}$. Då har vi

$$|\frac{1}{x'_m} - \frac{1}{x'_n}|_* = |\frac{x'_n - x'_m}{x'_m \cdot x'_n}|_* < \frac{4|x'_n - x'_m|_*}{|\hat{x}|_*{}^2} < \epsilon_{x'^{-1}},$$

så $\hat{x}^{-1}$ ligger faktiskt i $\widehat{K}$, och satsen gäller. □

Denna sats kommer visa sig ovärderlig, eftersom vi närsom en kropp inte är komplett enkelt kan konstruera en kropp som är det. Analogt med 2.1 har vi åter

$$\varphi : K \to \hat{K}, x \mapsto [(x, x, x....)],$$

som utöver att vara en isometri nu också uppfyller

$$\varphi(x+y) = [(x+y, x+y, x+y....)] = [(x, x, x....)] + [(y, y, y....)] = \varphi(x) + \varphi(y)$$
$$\varphi(x \cdot y) = [(x \cdot y, x \cdot y, x \cdot y....)] = [(x, x, x....)] \bullet [(y, y, y....)] = \varphi(x) \bullet \varphi(y)$$

och alltså är en ringisomorfism mellan K och bilden av φ. Detta tillsammans med det faktum att K är en kropp implicerar att K är isomorf med en underkropp av $\widehat{K}$, så $\widehat{K}$ kan också ses som en kroppsutvidgning av K. Mer precist kan vi återigen med kirurgi (jämför avsnitt 2.1) konstruera $E = K \cup (\widehat{K}/\varphi(K))$, varpå bijektionen $\vartheta : E \to \overline{X}$, definierad genom

$$\vartheta(k) = \begin{cases} \varphi(x) & \text{om } x \in K \\ x & \text{annars.} \end{cases}$$

åter möjliggör överföring av struktur hos kompletteringen till E. Konkret kan addition, multiplikation samt absolutbelopp i E definieras genom

$$x +_E y = \vartheta^{-1}(\vartheta(x) + \vartheta(y))$$
$$x \cdot_E y = \vartheta^{-1}(\vartheta(x) \bullet \vartheta(y))$$
$$|x|_E = |\vartheta(x)|_*,$$

vilket explicit visar att $\hat{K}$ alltid kan ses som kroppsutvidgning av K sånär som på isomorfi.

Kapitel 3

Om tillslutning

3.1 Introduktion

Som vi såg i avsnitt 1.5 finns det polynom utan nollställen i $\mathbb{Q}_p$. För att råda bot på detta tillkortakommande ska vi nu helt enkelt undersöka möjligheten att *lägga till dessa* till varje talkropp $\mathbb{Q}_p$. På så sätt skulle man kunna bilda kropp, som då åtminstone innehåller lösningar till alla polynom med koefficienter i $\mathbb{Q}_p$. Detta för tankarna till det förhållande som föreligger mellan $\mathbb{R}$ och $\mathbb{C}$, även om den situationen visar sig vara ytterst sällsam. För att komma till $\mathbb{C}$ räcker det nämligen för det första att lägga till ett element, i, för att alla polynom med koefficienter i $\mathbb{R}$ ska ha en lösning; dessutom visar det sig därefter att alla polynom med koefficienter i $\mathbb{C}$ redan *har* sina lösningar i $\mathbb{C}$, och att kroppen $\mathbb{C}$ således är *algebraiskt sluten*. Går det att hitta en motsvarande utvidgning till varje $\mathbb{Q}_p$, $\overline{\mathbb{Q}_p}$, så att varje polynom i $\overline{\mathbb{Q}_p}$ har sina nollställen i $\overline{\mathbb{Q}_p}$? För att ta reda på detta ska vi studera möjligheterna till detta för kroppar i allmänhet.

3.2 Enkla algebraiska kroppsutvidgningar

Vi börjar med att studera fallet då vi till K adderar ett element α, som uppfyller $P(\alpha) = 0$ för något polynom P i $K[X]$. Detta kallas för en *enkel utvidgning med ett algebraiskt element*. För att kunna angripa detta ämne på ett smidigt sätt ska vi först gå igenom behövliga begrepp och satser ur den abstrakta algebran. För fler detaljer, se [Grillet, 2007]. Som konvention antar vi att alla ringar är kommutativa med multiplikativa enhetselement.

En första viktig notation är $R[X]$, som benämner *ringen av polynom med koefficienter i ringen* R. I denna ring är additionen samt multiplikationen precis som man kan tänka sig,

$$\sum_{i=0}^{n} a_i X^i + \sum_{k=0}^{m} b_i X^i = \sum_{l=1}^{\max\{m,n\}} (a_l + b_l) X^l$$

$$\sum_{i=0}^{n} a_i X^i \cdot \sum_{k=0}^{m} b_i X^i = \sum_{l=1}^{m \cdot n} \sum_{i+j=l} a_i b_j X^l.$$

I synnerhet kommer förstås polynomringen $K[X]$, där koefficienterna är element i kroppen K, att vara särskilt intressant. Ett viktigt påpekande är att det också är möjligt att bilda polynom med flera »obekanta«. Ta till exempel $K[X, Y]$, mängden av alla polynom med två obekanta och med koefficienter i K. Det går till och med bra att tala om polynomringen $K[(X_i)_{i\in I}]$, där I är en godtycklig indexmängd. Detta beror på att vi i konstruerandet av element i polynomringen ändå bara använder oss av ett ändligt antal av dessa. Resultatet blir därför åter ett polynom, och antalet obekanta i polynomet sammanfaller med hur många element i $(X_i)_{i\in I}$ vi väljer att ta.

Ett annat centralt begrepp i ringteorin är *ideal*. Dessa är delmängder av en ring R som dels är additivt slutna, och dels är slutna under multiplikation med valfritt element i ringen, det vill säga

1. $\forall x, y \in \mathfrak{a} \implies x + y \in \mathfrak{a}$, samt
2. $\forall r \in R, x \in \mathfrak{a} \implies r \cdot x \in \mathfrak{a}$.

Ett ideal kallas *äkta* om det är strikt mindre än hela mängden R.

Det är kutym att beteckna ideal i frakturstil. I första hand kommer minusklerna $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$... att användas, men även majusklerna $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$... kommer komma till användning för att undvika missförstånd i de situationer då ideal i två olika ringar diskuteras.

Både polynomringar och ideal figurerar i följande viktiga sats:

Satsen om nollskilda ideal i $K[X]$. *Alla nollskilda ideal i $K[X]$ genereras av ett unikt moniskt polynom.*

Bevis. Detta bevis är taget från [Grillet, 2007]. Låt $\mathfrak{a} \neq 0$ vara ett ideal i $K[X]$. I $\mathfrak{a}$ måste det då finnas ett moniskt polynom $f \neq 0$ med den lägsta graden bland polynomen i $\mathfrak{a}$. Vidare har vi att det ideal som genereras av f är en delmängd av $\mathfrak{a}$. Å andra sidan, för något godtyckligt $g \in \mathfrak{a}$, måste $g = fq + r$ för några $q, f \in K[X]$, där grad $r <$ grad f. Men då måste $r = g - fq \in \mathfrak{a}$ och $r = 0$, eftersom f ju har lägsta graden bland de nollskilda polynomen i $\mathfrak{a}$. Således måste $g = fq$ ligga i idealet genererat av f, och eftersom g var godtyckligt måste hela $\mathfrak{a}$ genereras av f.

Antag nu att $\mathfrak{a}$ genereras av två moniska polynom f, h. Då måste $h = g \cdot q_1$ och $h = g \cdot q_2$ för några $q_1, q_2 \in K[X]$, och q_1, q_2 vara konstanta. Faktum är att de till och med måste vara lika med 1 då polynomen är moniska, så $f = h$ och detta polynom är således unikt. □

Ett ideal $\mathfrak{a}$ i ring R kan användas till att konstruera en ny ring. Detta är den så kallade *kvotringen* $R/\mathfrak{a}$, definierad genom

$$R/\mathfrak{a} = \{x + \mathfrak{a} : x \in R\},$$

där

$$x + \mathfrak{a} = \{x + a : a \in \mathfrak{a}\}$$

och med operationerna

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$$
$$(x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = (x \cdot y) + \mathfrak{a}.$$

Det går till och med att konstruera kroppar från ringar, vilket kommer utnyttjas flitigt på kommande sidor. Hur man ska gå till väga framgår från följande sats:

Satsen om maximala ideal. *Om $\mathfrak{a}$ är ett ideal i ett kommutativ ring, är $R/\mathfrak{a}$ en kropp om och endast om $\mathfrak{a}$ är ett äkta ideal som inte är en delmängd av något annat ideal än sig själv och hela ringen R. Idealet $\mathfrak{a}$ kallas då* maximalt*.*

Bevis. De kritiska stegen i detta bevis är tagna från [Grillet, 2007]. Först visar vi

$$R \text{ kropp} \iff R \text{ har inga äkta nollskilda ideal.}$$

"$\Rightarrow$": Tag något element $x \neq 0$ i något ideal $\mathfrak{c}$. Då x har en invers i R, måste också $1 \in \mathfrak{c}$; således måste $\mathfrak{c} = R$ och idealet är inte äkta.
"$\Leftarrow$": Om R inte har något äkta nollskilt ideal måste vi för alla $x \neq 0$ ha $1 \in Rx = R$, så x har en invers och R måste då vara en kropp.

Antag nu att vi funnit något ideal $\mathfrak{a}$ så att $R/\mathfrak{a}$ inte har några äkta ideal. Med den sedvanliga epimorfismen,

$$\begin{aligned} \pi : R &\to R/\mathfrak{a} \\ x &\mapsto x + \mathfrak{a} \end{aligned}$$

får vi för varje ideal $a \subset \mathfrak{c} \subset R$ en mängd

$$\mathfrak{A} = \pi(\mathfrak{c}) = \{x + \mathfrak{a} \in R/\mathfrak{a} : x \in \mathfrak{c}\}.$$

Då denna mängd är additivt sluten samt sluten med avseende på multiplikation med godtyckligt element i $R/\mathfrak{a}$, är detta ett ideal i $R/\mathfrak{a}$. Eftersom vi antagit att det inte finns några äkta sådana, blir slutsatsen att $\pi(\mathfrak{c})$ antingen måste vara 0 eller $R/\mathfrak{a}$. Detta implicerar i sin tur att $\mathfrak{c} \in \{\mathfrak{a}, R\}$, och således är $\mathfrak{a}$ ett maximalt ideal i R.

Vi har nu etablerat att om $R/\mathfrak{a}$ är en kropp, så är $\mathfrak{a}$ maximalt. För det omvända, notera att det faktum att $\mathfrak{a}$ är ett maximalt ideal i R innebär att det inte existerar något ideal $\mathfrak{b}$ så att $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$. Antag nu att $\mathfrak{A}$ är ett ideal i $R/\mathfrak{a}$. Då har vi

$$\mathfrak{c} = \pi^{-1}(\mathfrak{A}) = \{x \in R : x + \mathfrak{a} \in \mathfrak{A}\}.$$

Denna mängd är additivt sluten samt sluten med avseende på multiplikation med godtyckligt element i R, och med detta ett ideal i R. Eftersom $\mathfrak{a} \subset \mathfrak{c} \subset R$ följer det att $\mathfrak{c}$ antingen måste vara $\mathfrak{a}$ eller R. Från detta följer vidare att $\mathfrak{A} \in \{0, R/\mathfrak{a}\}$, det vill säga att det inte finns något nollskilt äkta ideal i $R/\mathfrak{a}$. Alltså,

$$R/\mathfrak{a} \text{ har inga äkta ideal} \iff \mathfrak{a} \text{ är ett maximalt ideal i } R,$$

och satsen följer. □

Låt nu $K \subset E$ vara en kroppsutvidgning. För ett element $\alpha \in E$, låt $K(\alpha)$ beteckna den minsta kropp så att $K \cup \{\alpha\} \subset K(\alpha)$, och på motsvarande sätt för en delmängd $S \subset E$, låt $K(S)$ beteckna den minsta delkropp så att $K \cup S \subset K(S)$. I analogi med beteckningen för polynomringar låter vi $K[\alpha]$ beteckna ringen av alla ändliga summor och produkter av element i $K \cup \{\alpha\}$.

Ett annat sätt är att låta $q(X) \in K[X]$ vara ett irreducibelt polynom, och $\mathfrak{a} = K[X] \cdot q(X)$. Då $\mathfrak{a}$ är maximalt är $E = K[X]/\mathfrak{a}$ en kropp, och

$K \subset E$ eftersom K kan identifieras med de konstanta polynomen. Faktum är att $E = K(\alpha)$, med $\alpha = x + \mathfrak{a}$. Detta förhållande illustreras i följande sats:

Sats. *Om $p(\alpha) = 0$ för något icke-konstant $p \in K[X]$ existerar det ett irreducibelt polynom q så att $q(\alpha) = 0$. Då gäller $p(\alpha) = 0$ om och endast om q delar p, och $K[\alpha] = K(\alpha) \cong K[X]/(q)$. Dessutom är $1, \alpha, ..., \alpha^{n-1}$ en bas i $K(\alpha)$ över K, där n är graden hos q.* I detta fall kallas α *algebraisk över K.*

Bevis. Också idéerna i detta bevis härrör från [Grillet, 2007]. Låt $\Psi : K[x] \to K(\alpha)$ vara den s k *evauleringshomomorfismen* $f \mapsto f(\alpha)$. Då har vi Im $\psi = K[\alpha]$, och för två element $f, g \in$ Ker ψ, som ju är icke-tom då $\psi(p) = 0$, gäller

$$\begin{aligned} 0 = \psi(f) + \psi(g) = \psi(f + g) \qquad &\implies f + g \qquad \in \text{Ker } \psi \\ 0 = \psi(f) = \psi(K[\alpha])\psi(f) = \psi(K[\alpha] \cdot f) \qquad &\implies K[\alpha] \cdot f \qquad \in \text{Ker } \psi. \end{aligned}$$

Ker ψ är således ett ideal, genererat av något moniskt polynom q enligt satsen om nollskilda ideal i $K[X]$. Således måste $p \in$ Ker ψ om och endast om p delas av q, och $K[\alpha] \cong K[X]/$ Ker $\psi = K[X]/(q)$. Skriv nu $q = gh$. Eftersom

$$gh \in \text{ Ker } \psi \implies g \in \text{ Ker } \psi \text{ eller } h \in \text{ Ker } \psi,$$

har vi att q uppfyller $q|gh \implies q|g$ eller $q|h$. Antag att $q|g$. Då måste g, q dela varandra, vilket innebär h är en enhet. Således är q *irreducibelt.*

Antag nu att $K[X] \cdot q$ är en delmängd av något ideal $\mathfrak{a} = K[X] \cdot k$. Då gäller $q = kl$ för något l, och någon av k, l måste vara en enhet. Om k är en enhet är $\mathfrak{a} = K[X]$, och om l är en enhet måste $\mathfrak{a} = K[X] \cdot q$, så idealet genererat av q är maximalt. Satsen om maximala ideal ger då att $K[X]/(q)$ är en kropp, så $K[\alpha] = K(\alpha) \cong K[X]/(q)$.

Vi ska slutligen visa att $1, \alpha, ..., \alpha^{n-1}$ är en bas i $K(\alpha)$ över K. Låt $n =$ grad $q > 0$. För varje $f \in K[x]$ har vi $f = qg + r$, där grad $r <$ grad q. Särskilt har vi $f(\alpha) = r(\alpha)$. Detta betyder att varje $f(\alpha)$ i $K[\alpha]$ kan skrivas som en linjär kombination av $1, \alpha, ..., \alpha^{n-1}$ med koefficienter i K. Vidare har vi att om $r(\alpha) = 0$ så måste q dela r, men grad $r <$ grad q, så i sådana fall måste $r = 0$. Om $a_0, ...a_{n-1} \in K$ är koefficienterna i r har vi alltså

$$r(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} = 0 \implies a_0 = a_1 = ... = a_{n-1} = 0,$$

vilket precis motsvarar att $1, \alpha, ..., \alpha^{n-1}$ är *linjärt oberoende.* □

Denna sats har två omedelbara konsekvenser: För varje polynom p kan vi finna en kroppsutvidgning E med något element α som uppfyller $p(\alpha) = 0$. Dessutom kan $K(\alpha)$ ses som ett vektorrum över K, där dimensionen n, hädanefter betecknat $[K(\alpha) : K]$, är densamma som graden hos q. Detta koncept är mycket viktigt och kan faktiskt utvidgas till kroppsutvidgningar i allmänhet, även det då förstås inte är givet att $[E : K] < \infty$. Är så fallet säger vi att E är *ändlig* över K.

3.3 Om större algebraiska utvidgningar

När man i allmänhet talar om en *algebraisk utvidgning* till K, åsyftas en kropp $K \subset E$ vari samtliga element $\alpha \in E$ är algebraiska över K. Alla ändliga utvidgningar är algebraiska, för om $[E : K] = n$ måste nämligen för varje element

$b \in E$ $1, b, b^2, ..., b^n$ vara linjärt beroende och

$$k_0 + k_1 b + k_2 b^2 + ... + k_n b^n = 0$$

med någon nollskild koefficient. Ett annat behagligt faktum är att om E, F är två ändliga utvidgningar så att $K \subset E \subset F$, gäller $[F : K] = [F : E][E : K] = m \cdot n$. Detta följer helt enkelt från att vi i F över E kan skriva

$$x = \sum_{i=1}^{m} e_i \cdot F_i = \sum_{i=1}^{m} (\sum_{j=1}^{n} k_{i,j} E_j) \cdot F_i)$$

där $E_1, ..., E_n$ är en bas i E över K, och $F_1, ..., F_m$ är en bas i F över E. Om $x = 0$ så måste $\forall i : e_i = 0$, och då gäller $\forall i, j : k_{i,j} = 0$. Därför måste $E_j \cdot F_i$ vara basvektorer i F över K, och eftersom det av dessa finns $m \cdot n$ stycken har vi att $[F : K] = m \cdot n = [F : E][E : K]$.

Med dessa faktum samt resultat från 3.2 i vår arsenal ska vi bevisa ett antal satser rörande algebraiska utvidgningar i allmänhet.

Sats. *Om alla $\alpha \in S$ är algebraiska över K, så är $K(S)$ algebraisk över K.*

Bevis. Det är en god idé att först etablera följande lemma:

Lemma. *Om $E = K(\alpha_1, ..., \alpha_n)$, där samtliga α_i är algebraiska över K, är E ändlig (och därmed algebraisk) över K.*

Bevis. Detta bevis är hämtat från [Grillet, 2007]. Vi visar detta med induktion. Om $n = 0$ är $E = K$ och således ändlig över K. Anta nu som induktionssteg att $[F : K] < \infty$, där $F = K(\alpha_1, ..., \alpha_{n-1})$. Eftersom nu det existerar något nollskilt polynom f så att $f(\alpha_n) = 0$, så är $E = F(\alpha)$ en enkel algebraisk utvidgning och $[E : F] < \infty$. Men i sådana fall är $[E : K] = [E : F][F : K]$ också ändligt, och lemmat gäller. □

Notera nu att varje x i $K(S)$ kan likställas med ett ändligt uttryck innehållande ändligt många element ur K, och i synnerhet ändligt många element i $\alpha_1, .., \alpha_n$ från S. Detta innebär att varje x återfinns i en mindre kropp $K(\alpha_1, .., \alpha_n)$, varefter lemmat ger att varje x är algebraiskt över K. □

För en kedja av kroppar $K \subset E \subset F$, där F är algebraisk över K, har vi förstås att F också är algebraisk över E (eftersom $K \subset E$). Dessutom har vi då också att E är algebraisk över K (eftersom $E \subset F$), så

F är algebraisk över $K \implies F$ är algebraisk över E och E är algebraisk över K.

Detta är i själva verket en ekvivalens, och den andra riktningen har fått ett särskilt namn:

Tornegenskapen. *Låt $K \subset E \subset F$ vara kroppar. Om F är algebraisk över E och E är algebraisk över K, måste F vara algebraisk över K.*

Bevis. Varje α i F är ett nollställe till något irreducibelt polynom

$$f(X) = a_0 + a_1 X + ...a_n X^n \in E[X],$$

och således också algebraiskt över $K(a_0, ..., a_n)$. Eftersom som nu $[K : K(a_0, ..., a_n)]$, $[K(a_0, ..., a_n) : K(a_0, ..., a_n, \alpha)]$ båda är ändliga måste

$$[K : K(a_0, ..., a_n, \alpha)] = [K : K(a_0, ..., a_n)] \cdot [K(a_0, ..., a_n) : K(a_0, ..., a_n, \alpha)] < \infty,$$

och α är algebraiskt över K, för alla $\alpha \in F$. □

Som avslutning ska vi nu ta oss an problemet att att hitta en utvidgning som innehåller samtliga nollställen till någon given kropps polynomring.

Sats. *Varje kropp K har en algebraisk utvidgning som innehåller en rot till varje icke-konstant polynom i $K[X]$.*

Bevis. Detta bevis kommer från [Grillet, 2007]. Notera först att vi etablerat (se avsnitt 3.2) att vi givet ett ickekonstant polynom $p \in K[X]$ kan konstruera en utvidgning vari p har en rot. Induktivt kan vi på samma sätt för ett ändligt antal ickekonstanta polynom $f_1, ..., f_n \in K[X]$ konstruera en utvidgning vari samtliga f_i har en rot. Denna utvidgning är dessutom är algebraisk över K, enligt sats i avsnitt 3.3. Skriv nu familjen av *alla* ickekonstanta polynom $(f_i)_{i \in I}$, och betrakta polynomringen $K[(X_i)_{i \in I}]$ (notera att indexmängden är densamma). I denna ring genererar mängden av samtliga $f_i(X_i)$ ett ideal $\mathfrak{a}$. Detta ideal $\mathfrak{a}$ är ett äkta ideal, det vill säga $\mathfrak{a} \neq K[(X_i)_{i \in I}]$. I annat fall måste $1 \in \mathfrak{a}$, och

$$1 = \sum_{j \in J} u_j f_j(X_j)$$

där $u_j \in K[(X_i)_{i \in I}]$ och J är en ändlig mängd. Låt nu E beteckna en algebraisk utvidgning över K vari samtliga f_j har en rot α_j, och låt $\varphi : K[(X_i)_{i \in I}] \to E$ vara evauleringsmorfismen

$$\varphi(f(X_{i_1}, ..., X_{i_n})) = f(\alpha_{i_1}, ..., \alpha_{i_n}), \text{ där } \alpha_{i_k} = \begin{cases} \alpha_j & \text{om } i_k = j \in J, \\ 0 & \text{annars.} \end{cases}$$

Med denna kan vi skriva

$$1 = \varphi(1) = \varphi(\sum_{j \in J} u_j f_j(X_j)) = \sum_{j \in J} \varphi(u_j)\varphi(f_j(X_j)) = 0,$$

vilket förstås är en motsägelse, och således är $\mathfrak{a}$ ett äkta ideal.

Enligt det s k *Krulls teorem* (se [Cohn, 2005] för bevis av detta) existerar det ett maximalt ideal $\mathfrak{m}$ i $K[(X_i)_{i \in I}]$ innehållande $\mathfrak{a}$. Satsen om maximala ideal i avsnitt 3.2 säger då att $K[(X_i)_{i \in I}]/\mathfrak{m} = F$ är en kropp. En delkropp av denna är isomorf med K genom morfismen $x \mapsto x + \mathfrak{m}$, så F kan ses en utvidgning av K. Dessutom uppfyller varje element $\alpha_i = X_i + \mathfrak{m} \in F$ att $f_i(\alpha_i) = 0$, så varje polynom i K har sin lösning i F.

Det återstår att visa att F är algebraisk över K. De två morfismerna

$$\pi : K[(X_i)_{i \in I}] \to K[(X_i)_{i \in I}]/\mathfrak{m}, f((X_i)_{i \in I}) \mapsto f((X_i)_{i \in I}) + \mathfrak{m}$$
$$\varphi : K[(X_i)_{i \in I}] \to K[(X_i)_{i \in I}]/\mathfrak{m}, f((X_i)_{i \in I}) \mapsto f((\alpha_i)_{i \in I})$$

måste sammanfalla eftersom båda projicerar samtliga X_i på α_i och alla $x \in K$ på $x + \mathfrak{m}$. Således måste $f((X_i)_{i \in I}) + \mathfrak{m} = f((\alpha_i)_{i \in I})$ och vi kan skriva $F = K[(\alpha_i)_{i \in I}] = K((\alpha_i)_{i \in I})$. Eftersom samtliga α_i är algebraiska över K måste sålunda hela F vara algebraisk över K enligt sats ovan. □

Nu är vi väl rustade att möta den verkliga besten.

3.4 Algebraisk tillslutning

All matematik i detta avsnitt kommer från [Grillet, 2007]. En kropp L kallas *algebraiskt sluten* om följande tre påståenden uppfylls:

1. Den enda algebraiska utvidgningen av L är L självt.
2. I $L[X]$ har alla irreducibla polynom grad 1.
3. Alla icke-konstanta polynom i $L[X]$ har en lösning i L.

Dessa är i själva verket ekvivalenta. Från sats i 3.2 vet till exempel att varje irreducibelt polynom q inducerar en kroppsutvidgning $L[X]/q \cong L(\alpha)$, och att $[L(\alpha), L] = \text{grad } q$. Om nu den enda algebraiska utvidgningen av L är L självt måste sålunda grad $q = 1$ gälla för alla irreducibla polynom ($1 \implies 2$). Men då måste också alla icke-konstanta polynom i $L[X]$ ha lösningar i L, eftersom de kan skrivas som en produkt av irreducibla polynom ($2 \implies 3$). Anta nu att α är algebraiskt över L. Då finns något irreducibelt polynom q så att $q(\alpha) = 0$. Om nu alla polynom har en lösning i L, måste $q(X) = X - r$. Men då ger $q(\alpha) = \alpha - r = 0$ att $\alpha = r \in L$ ($3 \implies 1$).

Att finna algebraiskt sluten utvidgning till en given kropp K kallas för att *tillsluta* K. Detta går alltid att göra:

Sats. *Varje kropp K har en algebraisk kroppsutvidgning $\overline{K}$ som är algebraiskt sluten.*

Bevis. Man kan med den sista satsen i 3.3 bilda ett väldigt högt torn

$$K = E_0 \subset E_1 \subset ... \subset E_n \subset ...$$

av kroppsutvidgningar, där E_{n+1} är en algebraisk kroppsutvidgning till E_n som innehåller alla nollställen till samtliga polynom i E_n. Betrakta nu mängden $\overline{K} = \bigcup_{i \in I} E_i$. Om man tar två godtyckliga element x_1, x_2 i denna mängd, kommer de med all säkerhet vara hemmahörande i några delkroppar, säg $x_1, \in E_i, x_2, \in E_j$. Dessa delkroppar kommer i sin tur att vara delmängder av någon tredje kropp E_k. Således ligger också produkten, inverserna samt summan av x_1, x_2 i $E_k \subset \overline{K}$, och $\overline{K}$ är en kropp.

På motsvarande sätt måste $\overline{K}$ vara algebraiskt sluten, eftersom koefficienterna i varje $f \in \overline{K}[X]$ alla ligger i något E_n; en rot finns då per definition i $E_{n+1} \subset \overline{K}$.

Slutligen har vi för varje $x \in \overline{K}$ att $\exists n : x \in E_n$. Eftersom E_n är algebraisk över K enligt tornegenskapen, måste x vara algebraisk över K, och således är $\overline{K}$ en algebraisk utvidgning av K. □

I viss mening slukar en algebraiskt sluten kropp alla algebraiska utvidgningar man kan göra på dess delkroppar:

Sats. *Alla homomorfismer från en kropp K till en algebraiskt sluten kropp kan utvidgas till varje algebraisk utvidgning av K. I synnerhet finns det en homomorfism till varje annan algebraiskt sluten utvidgning av K; i detta fall är homomorfismen dessutom bijektiv.*

Bevis. Låt E vara en algebraisk utvidgning av K och φ vara en homomorfism från K till en algebraiskt sluten kropp L. Vi undersöker först fallet om E är en enkel utvidgning. Då är $E = K(\alpha)$ och problemet reduceras till vad α ska skickas till. Eftersom α är ett algebraiskt element vet vi att det finns ett irreducibelt polynom q så att $q(\alpha) = 0$. Om varje koefficient k_i i q ersätts med $\varphi(k_i)$ får vi ett motsvarande polynom ${}^{\varphi}q$ i L. Vi har

$$q(\alpha) = \sum_{i=0}^{n} k_i \alpha^i = 0$$

$$\implies 0 = \varphi(0) = \varphi(q(\alpha)) = \sum_{i=0}^{n} \varphi(k_i)\varphi(\alpha)^i = {}^{\varphi}q(\varphi(\alpha)),$$

så $\varphi(\alpha)$ är en lösning till ${}^{\varphi}q$ i L. Eftersom nu kroppen L är algebraiskt sluten, måste det existera åtminstone en rot i L, kanske flera, och genom att låta α skickas på någon av dessa har vi fått en utvidgning av φ till $K(\alpha)$.

I det generella fallet måste ett urvalsekvivalent lemma åberopas.

Zorns lemma. *När X är en icke-tom, partiellt ordnad mängd, och varje icke-tom kedja i X har en övre gräns i X, måste X ha ett maximalt element.*

Förklaring. Ett bevis av detta lemma kräver en del mängdlära och utelämnas därför (går dock att finna i [Grillet, 2007], A.2 - A.4). Däremot kan det vara på sin plats att förklara de begrepp som ingår i denna sats:

En *partiellt ordnad mängd* är en mängd X med en binär relation $\leqq$, som är reflexiv ($x \leqq x$), transitiv ($x \leqq y, y \leqq z \implies x \leqq z$) samt antisymmetrisk ($x \leqq y, y \leqq x \implies x = y$). Två element i X behöver inte stå i relation till varandra över huvudtaget.

En *kedja* är en delmängd $C \subset X$ så att åtminstone ett av uttrycken $x \leqq y, y \leqq x$ håller för alla element $x, y \in C$. En "övre gräns" för C är ett element b i X så att $x \leqq b$ för alla $x \in C$. □

Låt nu $\mathcal{S}$ vara mängden av alla ordnade par (F, ψ), där F är en underkropp till E, $K \subset F \subset E$, och $\psi : F \to L$ är en homomorfism som utvidgar φ (alltså: $\psi(x) = \varphi(x)$ för alla $x \in K$). Till exempel så är $(K, \varphi) \in \mathcal{S}$. Ordna nu $\mathcal{S}$ partiellt genom $(F, \psi) \leqq (G, \chi)$ om och endast om F är en underkropp till G och χ utvidgar ψ. Låt nu $\mathcal{C} = (F_i, \psi_i)_{i \in I}$ vara en icketom kedja i $\mathcal{S}$. Från dessa kan vi bilda kroppen $F = \bigcup_{i \in I} F_i \subset E$. För att inse att detta är en kropp, ta två godtyckliga element $x_1, x_2 \in F$. Då dessa är hemmahörande i några delkroppar, säg $x_1, \in F_{i_1}, x_2, \in F_{i_2}$, och dessa delkroppar i sin tur är delmängder av någon tredje kropp F_{i_3}, måste produkten, inverserna och summan av x_1, x_2 ligga i F_{i_3}. Men $F_{i_3} \subset F$, så i sådana fall ligger de också i F. Dessutom gäller $F_{i_3} \subset E$, så varje element i F ligger också i E, och F är en underkropp till E.

Vidare är en morfism $\psi : F \to L$ definierad för alla $x \in F$ genom $\psi(x) = \psi_i(x)$ närsom $x \in F_i$. Denna utvidgar φ, så $(F, \psi) \in \mathcal{S}$, och dessutom är (F, ψ) är en övre gräns för $\mathcal{C}$, eftersom det för alla i gäller $(F_i, \psi_i) \leqq (F, \psi)$.

Enligt Zorns lemma måste det nu finnas ett maximalt element (M, μ) i $\mathcal{S}$. Om $M \neq E$, så är varje $\alpha \in E \backslash M$ algebraiskt över M, eftersom E är en algebraisk utvidgning av $K \subset M$. Men i sådana fall kan μ utvidgas till den enkla utvidgningen $M(\alpha)$, vilket motsäger det faktum att M är maximalt. Således

måste $M = E$, och en befintlig morfism $\varphi : K \to L$ kan utvidgas till $\mu : E \to L$.

Som ett specialfall av detta har vi en morfism $\mu : \overline{K} \to L$, vilket innebär att $\overline{K} \cong \text{Im } \mu \subset L$. Men i sådana fall är bilden Im μ också algebraiskt sluten, och den enda algebraiska utvidgningen av Im μ är Im μ självt. Således måste Im $\mu = L$, och $\overline{K} \cong L$. □

En algebraiskt sluten utvidgning är alltså unik upp till isomorfier där ursprungsmängden K »lämnas orörd«, eller med mer exakt terminologi *unik upp till K-isomorfi*. Därför kan dessa i grund och botten ses som samma objekt, som vi hädanefter benämner *K:s algebraiska tillslutning*.

3.5 Multiplikativa normer i algebraiska utvidgningar

Vi ska nu diskutera möjligheten att utvidga en befintlig norm på en kropp K till en algebraisk utvidgning E. Detta kräver ingående teori i det generella fallet, men med relativt små medel går det att konstatera ett par viktiga faktum.

Till en början ska det nämnas att vi fortsättningsvis kommer att begränsa oss till de fall då K som metriskt rum är *lokalt kompakt*. Detta innebär att det i varje punkt x finns en omgivning som kan inneslutas i en mängd vari varje följd av element har en konvergent delföljd. Samtliga tre typer av kompletteringar av $\mathbb{Q}$ (se avsnitt 1.2) faller under denna kategori:

1. $\mathbb{Q}$ med den triviala normen är lokalt kompakt. Tag kring x valfri omgivning med radius mindre än 1. Varje följd av element består då av en konstant följd $(x, x, x...)$ och konvergerar därför.

2. $\mathbb{R}$ är lokalt kompakt. Detta följer från Heine-Borels teorem (se [Rudin, 1976]).

3. $\mathbb{Q}_p$ är lokalt kompakt. Detta resonemang kommer from [Koblitz, 1984]. Vi kan t ex ta mängden

$$x + \mathbb{Z}_p := \{y : |y - x|_p \leq 1\}$$

som är isometrisk med de p-adiska heltalen $\mathbb{Z}_p$ genom $z \mapsto z - x$. Varje följd i $\mathbb{Z}_p$ sedan har en konvergent delföljd via följande diagonalargument: Tag först en delföljd där den första p-adiska siffran är densamma. Från denna kan sedan en delföljd där den andra p-adiska siffran också är densamma bildas, och på så vis bildas en oändlig lista av följder där den $i : te$ raden innehåller p-adiska tal där de i första siffrorna är gemensamma. Bilda från dessa följder sedan en ny följd, där det första elementet är det första elementet i den första följden, det andra elementet det andra elementet i den andra följden, och så vidare (helt enkelt de element som utgör listans diagonal). Denna följd är Cauchy-riktig, och konvergerar således.

Med detta antagande kan man visa följande sats:

Sats. *Antag att V är kropp som kan skrivas som ett vektorrum av ändlig dimension över en lokalt kompakt kropp K utrustad med icke-trivial norm $|\cdot|_*$. Då finns det som mest en norm $|\cdot|_V$ som utvidgar $|\cdot|_*$ till V, det vill säga $|x|_* = |x|_V$ för alla element x i K.*

Bevis. Detta bevis kommer ifrån [Koblitz, 1984], dock med ytterligare detaljer tillagda. Idéen till beviset ligger i att visa att två icke-triviala multiplikativa normer $|\cdot|_1, |\cdot|_2$ måste förhålla sig

$$|\cdot|_2 \leq d_1|\cdot|_1$$
$$|\cdot|_1 \leq d_2|\cdot|_2,$$

där $d_1, d_2 > 0$. Om det nu skulle något x så att $|x|_1 \neq |x|_2$, säg $|x|_1 < |x|_2$, måste det för tillräckligt stora N gälla att $d_1|x^N|_1 < |x^N|_2$, vilket är en motsägelse.

Det visar sig att ovanstående olikheter även gäller för vektornormer i allmänhet, och eftersom en multiplikativ norm på V samtidigt är en vektornorm, om elementen i K ses som skalärer, skulle ett bevis av detta faktum implicera ovanstående. Med detta som målsättning börjar vi med att leta efter vektornormer på V. Låt $v_1, v_2, ..., v_n$ vara en bas i V, och definiera vektornormen

$$|a_1v_1 + ... + a_nv_n|_{\sup} = \max_{1\leq i\leq n}(|a_i|_*).$$

Detta är en vektornorm eftersom vi givet $x = a_1v_1 + ... + a_nv_n, y = b_1v_1 + ... + b_nv_n \in V, c \in K$ har

(1) "$|x|_{\sup} = 0 \iff x = \bar{0}$":

$$|x|_{\sup} = \max_{1\leq i\leq n}(|a_i|_*) = 0 \iff |a_1|_* = ... = |a_n|_* = 0 \iff x = \bar{0}.$$

(2) "$|c \cdot x|_{\sup} = |c|_* \cdot |x|_{\sup}$":

$$|c \cdot x|_{\sup} = \max_{1\leq i\leq n}(|c \cdot a_i|_*) = |c|_* \max_{1\leq i\leq n}(|a_i|_*) = |c|_* \cdot |x|_{\sup}.$$

(3) "$|x + y|_{\sup} \leq |x|_{\sup} + |y|_{\sup}$":

$$\begin{aligned} |x + y|_{\sup} &= \max_{1\leq i\leq n}(|a_i + b_i|_*) \leq \max_{1\leq i\leq n}(|a_i|_* + |b_i|_*) \\ &\leq \max_{1\leq i\leq n}(|a_i|_*) + \max_{1\leq j\leq n}(|b_j|_*) = |x|_{\sup} + |y|_{\sup}. \end{aligned}$$

Låt nu $|\cdot|_V$ vara någon annan vektornorm på V. Då har vi

$$|x|_V \leq |a_1|_*|v_1|_V + ... + |a_n|_*|v_n|_V \leq n \max_{1\leq i\leq n}(|a_i|_*) \max_{1\leq j\leq n}(|v_j|_V) = c_1|x|_{\sup}.$$

Kvar återstår att visa att

$$|x|_{\sup} \leq c_2|x|_V,$$

eftersom detta skulle implicera att

$$|x|_1 \leq c_1|x|_{\sup} \leq d_2|x|_2.$$

För detta ändamål behöver vi först följande lemma:

Lemma. *Om K är lokalt kompakt, och V är ett vektorrum över K av ändlig dimension, så är V lokalt kompakt med avseende på $|\cdot|_{sup}$.*

Bevis. Notera först att varje följd (x_i) i V inducerar n stycken följder i K om man betraktar varje x_i koordinatvis. Låt nu $x = a_1v_1 + ... + a_nv_n$ vara en godtycklig punkt i V. Eftersom nu K är lokalt kompakt, finns det för varje a_j ett $\epsilon_j > 0$ så att mängden

$$\{b \in K : |a_j - b|_* \leq \epsilon_j\}$$

är kompakt i K. Låt nu $\epsilon = \min_{1 \leq j \leq n} \epsilon_j$, och definiera en disk

$$D = \{v \in V : |x - v|_{\sup} \leq \epsilon\}.$$

Tag nu en följd (x_i) i D, och (a_{1_i}) i K bestående av x_i:s första koefficienter. Eftersom nu

$$|a_1 - a_{1_i}|_* \leq \max_{1 \leq j \leq n} (|a_j - a_{j_i}|_*) = \epsilon \leq \epsilon_1$$

är detta en följd av element ur en kompakt mängd, och det finns någon delföljd $(a_{1_{i_j}})$ som konvergerar. På så vis har vi funnit en ny följd i D, (x_{i_j}), där den första koefficienten konvergerar. Med denna följd kan vi i sin tur bilda ny delföljd genom att ta den andra koefficienten i varje x_{i_j}. Återigen finns här en konvergent delföljd, vilket producerar ännu en ny delföljd i V, $(x_{i_{j_k}})$, där de två första koefficienterna nu konvergerar. Genom att utföra denna procedur i n steg kan vi således hitta en delföljd i (x_i) som konvergerar, så D är kompakt, och således är V lokalt kompakt. □

Betrakta nu mängden

$$U = \{x \in V : |x|_{\sup} = 1\}.$$

För det första är detta en kompakt mängd med avseende på $|\cdot|_{\sup}$: Att V är lokalt kompakt är ekvivalent med att det finns något $\epsilon > 0 \in \mathbb{R}$ så att

$$A = \{x \in V : |x|_{\sup} \leq \epsilon\}$$

är kompakt. Eftersom $|\cdot|_*$ är icke-trivial existerar det något element a med $|a|_* \notin \{0, 1\}$. Med hjälp av (eventuellt negativa) potenser får vi sedan att $\exists c \in K \setminus \{0\} : |c|_* \leq \epsilon$. Mängden

$$B = \{x \in V : |x|_{\sup} \leq |c|_*\}$$

är då också kompakt: Tag en följd i B, som från A:s kompakthet har en delföljd som konvergerar mot ett element $a \in A$. Denna är Cauchy-riktig, så $\forall \delta \ \exists N, \forall m \geq N : |a - x_m| < \delta$, men

$$|a|_* = |a + x_m - x_m|_* \leq |a - x_m|_* + |x_m|_* \leq |c|_* + \delta,$$

så $|a|_* \leq |c|_*$ och B är kompakt. Omskalning genererar sedan mängden

$$\{y \in V : |y|_{\sup} \leq 1\},$$

som då också är kompakt. På motsvarande sätt har vi i synnerhet att

$$\{y \in V_i : |y|_{\sup} \leq 1\},$$

där V_i är det $n-1$-dimensionella underrum som spänns upp av vektorna v_1, ..., v_{i-1}, v_{i+1}, ..., v_n, är kompakt. Om denna mängd förskjuts med vektorn v_i får vi precis mängden

$$U_i = \{y : y \in U \text{ och } y\text{:s } v_i\text{-komponent lika med } 1\}.$$

Med unionen av dessa mängder i respektive $n-1$-dimensionella underrum kan vi sedan skriva

$$U = \bigcup_{1\leq i\leq n} U_i = \bigcup_{1\leq i\leq n} \{y + v_i : y \in \text{span}(v_1, ..., v_{i-1}, v_{i+1}, ...v_n), |y|_{\text{sup}} \leq 1\},$$

och eftersom en ändlig union av kompakta mängder är kompakt, måste U vara kompakt. Detta innebär att varje följd i U har en delföljd som konvergerar till något $x \in U$.

För det andra finns det något ϵ så att det för alla $x \in U$ gäller $|x|_V \geq \epsilon$. Detta visas med ett motsägelsebevis: Om så inte är fallet existerar det en sekvens (x_i) i U så att $|x_i|_V \to 0$. Att U är kompakt innebär då att det finns någon delföljd (x_{i_j}) som konvergerar till något x i U. Vi har

$$|x|_V \leq |x - x_{i_j}|_V + |x_{i_j}|_V \leq c_1|x - x_{i_j}|_{\text{sup}} + |x_{i_j}|_V,$$

vilket går mot noll när $j \to \infty$. Alltså, $|x|_V = 0 \implies x = 0 \in U$. Motsägelse!

Tag nu ett godtyckligt $x \in V$, $|x|_{\text{sup}} = |a|_*$. Då har vi $\frac{x}{a} \in U$, $|\frac{x}{a}|_V \geq \epsilon$, och

$$\begin{aligned} |\frac{x}{a}|_V \geq \epsilon = \epsilon|\frac{x}{a}|_{\text{sup}} &\iff \\ |\frac{x}{a}|_{\text{sup}} \leq \frac{1}{\epsilon}|\frac{x}{a}|_V &\iff \\ |x|_{\text{sup}} \leq c_2|x|_V, & \end{aligned}$$

vilket slutför beviset. □

Så, om vi kan hitta en utvidgning, så är den unik. Vi ska nu ta fram en kandidat till detta, och nöjer oss därför med att studera ändliga kroppsutvidgningar. Vi börjar med det enklaste fallet $E = K(\alpha)$, där α är ett algebraiskt element över K. Vi erinrar oss (se avsnitt 3.2) att detta innebär att α är ett nollställe till något polynom $a_n + a_{n-1}X + ... + a_1X^{n-1} + X^n$. Även här kommer perspektivet att se E som ett vektorrum över K bära frukt, eftersom vi då kan *se multiplikation av ett element som en linjär avbildning.* I basen $1, \alpha, ..., \alpha^{n-1}$ motsvaras t ex multiplikation med α av matrisen

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & 0 & \cdots & 0 & -a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & -a_2 \\ 0 & 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}$$

vilket lätt inses med hjälp av sambandet $\alpha^n = -a_1\alpha^{n-1} - ... - a_{n-1}\alpha - a_n$. Särskilt är determinanten av denna matris av intresse eftersom denna inte beror på val av bas i $K(\alpha)$. Denna, som vanligen betecknas $N_{K(\alpha)/K}(\alpha)$, kan skrivas

$$N_{K(\alpha)/K}(\alpha) = (-1)^n a_n.$$

För ett generellt element x i en ändlig utvidgning E kan $N_{E/K}(x)$ definieras på motsvarande sätt, och med denna kan vi faktiskt finna ett uttryck för den utvidgade normen i termer av den gamla, förutsatt att någon sådan existerar.

Sats. *Om K är en kropp utrustad med en icke-trivial multiplikativ norm $|\cdot|_*$ samt är lokalt kompakt med avseende på denna, och E är en ändlig utvidgning av K, finns det som mest en multiplikativ norm $|\cdot|_E$ på E som utvidgar $|\cdot|_*$. I sådana fall ges denna för ett element $x \in E$ av*

$$|\cdot|_E = \sqrt[[E:K]]{|N_{E/K}(x)|_*}.$$

Bevis. Följande resonemang kommer från [Bachman, 1964]. Sätt $n = [E : K]$. Vi vet från föregående sats att en eventuell multiplikativ norm på E är unik, så vi benämner även denna fortsättningsvis $|\cdot|_*$. Antag att $|x|_* < 1$. Då gäller $|x|_*^r \to 0$, och $|x^r|_* \to 0$. Eftersom nu

$$|x^r|_{\sup} \leq c|x^r|_*$$

har vi likaledes att $|x^r|_{\sup} \to 0$. Låt nu $x_1, ..., x_n$ vara en bas i E över K. Då kan vi skriva

$$x^r = a_{r1}x_1 + ... + a_{rn}x_n,$$

och

$$\lim_{r\to\infty} |a_{ri}|_* = 0 \quad i = 1, ..., n.$$

Skriver vi x^r som matriser innebär detta att gränsvärdet när $r \to \infty$ är nollmatrisen, och att $N_{E/K}(x^r) \to 0$. Från detta faktum, samt att determinanter är multiplikativa, har vi

$$\lim_{r\to\infty} |N_{E/K}(x^r)|_* = \lim_{r\to\infty} |N_{E/K}(x)|_*^r = 0.$$

Slutsatsen blir att om $|x|_* < 1$, så måste $|N_{E/K}(x)|_* < 1$. Om $|x|_* > 1$, så måste $|\frac{1}{x}|_* < 1$, och då har vi

$$|N_{E/K}(\frac{1}{x})|_* = |N_{E/K}(x^{-1})|_* = |N_{E/K}(x)|_*^{-1} = \frac{1}{|N_{E/K}(x)|_*} < 1,$$

så $|N_{E/K}(x)|_* > 1$. Detta innebär att om $|N_{E/K}(x)|_* = 1$, så $|x|_* = 1$. Eftersom $N_{E/K}(x) \in K$ motsvarar matrisen för $N_{E/K}(N_{E/K}(x))$ att multiplicera samtliga basvektorer med $N_{E/K}(x) \in K$. I synnerhet

$$N_{E/K}(N_{E/K}(x)) = \begin{vmatrix} N_{E/K}(x) & 0 & \cdots \\ 0 & \ddots & 0 \\ \vdots & 0 & N_{E/K}(x) \end{vmatrix} = N_{E/K}(x)^n.$$

Antag nu att $x \neq 0$, och låt $y = \frac{N_{E/K}(x)}{x^n}$. Då är

$$|N_{E/K}(y)|_* = |\frac{N_{E/K}(N_{E/K}(x))}{N_{E/K}(x^n)}|_* = |\frac{N_{E/K}(x)^n}{N_{E/K}(x)^n}|_* = 1,$$

vilket då implicerar att $|y|_* = 1$. Men då har vi för alla nollskilda element x i E

$$\begin{aligned} 1 = |\frac{N_{E/K}(x)}{x^n}|_* &\iff \\ |x^n|_* = |N_{E/K}(x)|_* &\iff \\ |x|_* = \sqrt[n]{|N_{E/K}(x)|_*}&, \end{aligned}$$

vilket skulle visas. □

Antag nu att $|\cdot|_*$ kan utvidgas till någon algebraisk utvidgning E, och att $\alpha \in E$ är nollställe till något polynom $a_n + a_{n-1}X + ... + a_1X^{n-1} + X^n$. Då ger satsen direkt att

$$|\alpha|_* = \sqrt[[E:K]]{|N_{E/K}(\alpha)|_*},$$

men eftersom $K(\alpha) \subset E$, kan vi också betrakta $|\cdot|_*$ begränsad till denna mindre kropp. Eftersom $[K(\alpha) : K] = n$ får vi då med dessa satser att normen av α kan skrivas

$$|\alpha|_* = \sqrt[n]{|N_{K(\alpha)/K}(\alpha)|_*} = \sqrt[n]{|(-1)^n a_n|_*} = \sqrt[n]{|a_n|_*}.$$

Eftersom normen är unik om den existerar enligt sats, kan motsvarande göras för samtliga element i E. Konkret betyder detta att normen av α alltid kan beräknas med hjälp av det irreducibla polynom som α satisfierar. I nästa kapitel ska vi se att detta faktiskt är en norm för alla algebraiska utvidgningar av $\mathbb{Q}_p$.

Kapitel 4

Den kompletta tillslutningen av $\mathbb{Q}_p$

4.1 Normutvidgning till $\overline{\mathbb{Q}_p}$

Låt oss kort resumera vad vi hitintills åstadkommit. I kapitel 2 har vi lagt konstruktionen av kropparna av p-adiska tal på en stadig grund. Vi har visat att en aritmetik finns och är väldefinierad, samt att en multiplikativ norm existerar för samtliga element som går att konstruera i denna. I kapitel 3 har vi sedan undersökt möjligheten att konstruera en kroppsutvidgning där samtliga polynom har en rot. Resonemang i 3.4 visar att en sådan alltid går att konstruera. Låt oss i p-adiska fallet beteckna denna kropp med symbolen $\overline{\mathbb{Q}_p}$. Förstås är det önskvärt att även på denna kropp finna en multiplikativ norm. Antag att en sådan norm existerar. För ett element $\alpha \in \overline{\mathbb{Q}_p}$ måste då också denna norm vara definierad i kroppen $\mathbb{Q}_p(\alpha)$. Från det faktum att α är algebraiskt över $\mathbb{Q}_p$ (följer från tornegenskapen) konstaterade vi i avsnitt 3.5 att detta möjliggjorde ett konkret sätt att beräkna normen av α. Å andra sidan »slukar« en tillslutning alla möjliga algebraiska utvidgningar (sats i avsnitt 3.4), så på samma sätt kan normen av $\alpha \in \overline{\mathbb{Q}_p}$ beräknas med hjälp av

$$|\alpha|_* = \sqrt[[E:\mathbb{Q}_p]]{|N_{E/\mathbb{Q}_p}(\alpha)|_p}$$

där $E \subset \overline{\mathbb{Q}_p}$ är *valfri* ändlig utvidgning av $\mathbb{Q}_p$ som innehåller α. Vi skall nu visa att detta faktiskt är en norm.

Sats. *Låt E vara en ändlig utvidgning av $\mathbb{Q}_p$. Då existerar en norm på E som utvidgar $|\cdot|_p$ på $\mathbb{Q}_p$.*

Bevis. Vi visar först att vår kandidat ovan utvidgar $|\cdot|_p$. Eftersom matrisen för multiplikation med ett element $\beta \in \mathbb{Q}_p$ motsvaras av en diagonaliserad matris med β längs diagonalen, har vi

$$|\beta|_* = \sqrt[[E:\mathbb{Q}_p]]{|N_{E/\mathbb{Q}_p}(\beta)|_p} = \sqrt[[E:\mathbb{Q}_p]]{|\beta^{[E:\mathbb{Q}_p]}|_p} = |\beta|_p,$$

så $|\cdot|_*$ utvidgar $|\cdot|_p$. Vi ska nu visa att $|\cdot|_*$ uppfyller

$$\begin{aligned}&(1)\ |x|_* = 0 \text{ om och endast om } x = 0,\\ &(2)\ |x\cdot y|_* = |x|_*\cdot|y|_*\\ &(3)\ |x+y|_* \leq \max(|x|_*, |y|_*).\end{aligned}$$

Om $|x|_* = 0$, måste

$$|N_{E/\mathbb{Q}_p}(x)|_p = 0 \implies N_{E/\mathbb{Q}_p}(x) = 0,$$

men då motsvarar multiplikation med x en icke-inverterbar matris, och x kan inte vara en enhet. Eftersom E är en kropp måste därför $x = 0$. Den omvända inriktningen följer från att $|\cdot|_*$ utvidgar $|\cdot|_p$. Gällande den multiplikativa egenskapen har vi

$$\begin{aligned}|x\cdot y|_* &= \sqrt[[E:\mathbb{Q}_p]]{|N_{E/\mathbb{Q}_p}(x\cdot y)|_p} = \sqrt[[E:\mathbb{Q}_p]]{|N_{E/\mathbb{Q}_p}(x)\cdot N_{E/\mathbb{Q}_p}(y)|_p}\\ &= \sqrt[[E:\mathbb{Q}_p]]{|N_{E/\mathbb{Q}_p}(x)|_p}\cdot \sqrt[[E:\mathbb{Q}_p]]{|N_{E/\mathbb{Q}_p}(y)|_p} = |x|_*\cdot|y|_*.\end{aligned}$$

Den additiva egenskapen är betydligt svårare att visa. Följande resonemang kommer från [Koblitz, 1984]. Antag utan förlust av allmängiltighet att $|x|_p$ är den större av $|x|_p, |y|_p$. Om $\gamma = \frac{y}{x}$, måste då $|\gamma|_p \leq 1$. Genom att dela med $|x|_p$ kan vi reducera (3) till $|1+\gamma|_p \leq 1$. Således följer satsen om vi kan visa detta för alla $\gamma \in E$ med $|\gamma|_p \leq 1$.

Notera nu att vi kan definiera $|\gamma|_*, |1+\gamma|_*$ med kroppen $\mathbb{Q}_p(\gamma) = \mathbb{Q}_p(1+\gamma)$ enligt

$$\begin{aligned}|\gamma|_* &= \sqrt[[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]]{|N_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(\gamma)|_p}\\ |1+\gamma|_* &= \sqrt[[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]]{|N_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(1+\gamma)|_p},\end{aligned}$$

och således räcker det att kontrollera detta i $\mathbb{Q}_p(\gamma)$. Sätt därför $K = \mathbb{Q}_p(\gamma)$, $n = [K : \mathbb{Q}_p]$ och låt $\{1, \gamma, ..., \gamma^{n-1}\}$ vara en bas i K. Låt $|\cdot|_{\text{sup}}$ vara supnormen med avseende på denna bas (se avsnitt 3.5). Alltså, för ett element $\alpha = \sum_{i=0}^{n-1} a_i\gamma^i$,

$$|\alpha|_{\text{sup}} := \max_{0\leq i\leq n}(a_i).$$

Definiera på motsvarande sätt för en $n\times n$-matris A med element i $\mathbb{Q}_p$

$$|A|_{\text{sup}} := \max_{0\leq i,j\leq n}(a_{ij}).$$

Alla linjära avbildningar från K till K motsvaras i basen ovan av en matris med element i $\mathbb{Q}_p$. Låt nu A motsvara multiplikation med γ. Då motsvarar A^i multiplikation med γ^i, och $I + A$ multiplikation med $1+\gamma$. Den bärande delen i det fortsatta beviset är att visa att följden $(|A^i|_{\text{sup}})$ är begränsad. Antag att så är fallet. Eftersom $\det A$ består av en rad termer med n stycken faktorer av A:s element, och $|\cdot|_p$ uppfyller den (3) ovan, har vi

$$|\det A|_p \leq (\max_{0\leq i,j\leq n}|a_{ij}|_p)^n = |A|_{sup}^n.$$

Från detta gäller

$$|1+\gamma|_*^N = |\det(1+A)^N|_p^{\frac{1}{n}} \leq |(1+A)^N|_{\sup}$$
$$\leq \max_{0\leq i\leq N} |\binom{N}{i} A^i|_{\sup} \leq \max_{0\leq i\leq N} |A^i|_{\sup} \leq C,$$

om $(|A^i|_{\sup})$ är begränsad. Således har vi

$$|1+\gamma|_* \leq \sqrt[N]{C},$$

och genom att låta $N \to \infty$ får vi således $|1+\gamma|_* \leq 1$, och satsen följer.

Kvar återstår alltså att visa att följden $(|A^i|_{\sup})$ är begränsad. Detta visas med ett motsägelsebevis. Om så inte är fallet kan vi nämligen finna en följden $i_j, j = 1, 2, ...$ så att $|A^{i_j}|_{\sup} > j$. Låt $b_j := |A^{i_j}|_{\sup}$, och låt $\beta_j \in \mathbb{Q}_p$ vara det *element* i A^{i_j} så att $|\beta_j|_p = b_j$. Definiera matrisen

$$B_j := \frac{A^{i_j}}{\beta_j}.$$

Uppenbarligen gäller $|B_j|_{\sup} = 1$. Eftersom nu matriser med element i $\mathbb{Q}_p$ kan ses som element i ett n^2-dimensionellt vektorrum över $\mathbb{Q}_p$, har vi från beviset av den första satsen i avsnitt 3.5 att

$$\{M \in \mathbb{Q}_p^{n\times n} : |M|_{\sup} = 1\}$$

är en kompakt mängd. Eftersom nu B_j är element i denna mängd måste det finnas en följd (B_{j_k}) som konvergerar till någon matris B. Men det $B_j = \det A^{i_j}/\beta_j^n$, så

$$|\det B_j|_p < \frac{|\det A^{i_j}|_p}{j^n} = \frac{|N_{K/\mathbb{Q}_p}(\gamma^{i_j})|_p}{j^n}$$
$$= \frac{|\gamma|_*^{[K:\mathbb{Q}_p]\cdot i_j}}{j^n} \leq \frac{1}{j^n},$$

vilket implicerar att

$$\det B = \lim_{k\to\infty} \det B_{j_k} = 0$$

eftersom varje element i B är gränsvärdet av motsvarande element i B_{j_k} enligt definitionen av sup-normen. Från den linjära algebran har vi att $\det B = 0$ innebär att det måste finnas något nollskilt element l i K så att $Bl = 0$. Om vi kan visa att detta har som följd att B är lika med nollmatrisen har sålunda funnit vår motsägelse, eftersom detta är oförenligt med att $|B|_{sup} = 1$.

Notera att $l, \gamma l, ..., \gamma^{n-1} l$ är en annan möjlig bas i K. Därför räcker det med att visa att $B\gamma^i l = 0$ för varje i, eftersom B multiplicerat med varje element skrivet i denna bas då måste vara lika med noll. Vi har

$$B\gamma^i l = BA^i l = A^i Bl = A^i \cdot 0 = 0,$$

eftersom B är gränsvärdet av matriser på formen $B_j = A^{i_j}/\beta_j$, vilka uppenbarligen kommuterar med varje A^i. Således har vi funnit vår motsägelse, och $(|A^i|_{\sup})$ måste vara begränsad. □

Eftersom nu $|\cdot|_*$ faktiskt existerar på hela $\overline{\mathbb{Q}_p}$ och är unik betecknar vi hädanefter den multiplikativa normen på $\overline{\mathbb{Q}_p}$ med $|\cdot|_p$.

4.2 En p-adisk analog till de komplexa talen

Så $\overline{\mathbb{Q}_p}$ är en algebraiskt sluten kropp varpå en multiplikativ norm finns definierad. Är detta då en p-adisk analog till de komplexa talen? Detta är förstås när det kommer till kritan en definitionsfråga, men i ett avseende är denna kropp tyvärr ovärdig en sådan titel:

Sats. *Kroppen $\overline{\mathbb{Q}_p}$ är inte komplett.*

Bevis. Se [Koblitz, 1984]. □

För att råda bot på detta kompletterar vi ännu en gång. Eftersom $\overline{\mathbb{Q}_p}$ är en kropp varpå en multiplikativ norm finns definierad, garanterar resultat i avsnitt 2.3 att detta är möjligt. På vis har vi kommit fram till den enorma kroppen Ω_p[1]. Om denna kan man konstatera:

Sats. *Kroppen Ω_p är algebraiskt sluten.*

Bevis. Detta bevis kommer från [Koblitz, 1984]. Låt $f(X) = X^n + a_n X^{n-1} + ... + a_2 X + a_1, a_i \in \Omega_p$. Vi måste visa att f har en rot i Ω_p. För varje $i = 1, ..., n$, låt $(a_{i,j})$ vara en följd av element i $\overline{\mathbb{Q}_p}$ som konvergerar till a_i. Låt $g_j(X) = X^n + a_{n,j}X^{n-1} + ... + a_{2,j}X + a_{1,j}$, och beteckna nollställena till g_j med $r_{1,j}, ..., r_{n,j}$. Om dessa kan vi konstatera,

Lemma. *Det existerar en konstant C så att $|r_{i,j}|_p \leq C$ för alla $i, j \in \mathbb{N}$.*

Bevis. Vi introducerar först en vektornorm på vektorrummet av polynom av grad n i $\overline{\mathbb{Q}_p}[X]$,

$$|g| = \max_i(|a_i|_p).$$

Detta är en norm enligt beviset till första satsen i avsnitt 3.5. Med denna ser vi att

$$\begin{aligned} g_j(r_{i,j}) = r_{i,j}^n + a_{n,j}r_{i,j}^{n-1} + ... + a_{2,j}r_{i,j} + a_{1,j} = 0 \implies \\ |r_{i,j}|_p^n = |a_{n,j}r_{i,j}^{n-1} + ... + a_{2,j}r_{i,j} + a_{1,j}|_p \\ \leq \max(|g_j(X)|_p|r_{i,j}|_p^{n-1}, |g_j(X)|_p) \leq |g_j(X)|_p^n + |g_j(X)|_p. \end{aligned}$$

Den sista olikheten gäller då vi antingen har att $|r_{i,j}|_p^n \leq |g_j(X)|_p|r_{i,j}|_p^{n-1}$, från vilket gäller att $|r_{i,j}|_p^n \leq |g_j(X)|_p^n$, eller att $|r_{i,j}|_p^n \leq |g_j(X)|_p$. I vilket fall är $|r_{i,j}|_p^n$ uppåt begränsad av summan av dessa. Eftersom nu $\forall\epsilon\ \exists N : \forall m \geq N |g_m(X) - f(X)|_p < \epsilon$ har vi

$$|g_m(X)|_p = |g_m(X) - f(X) + f(x)|_p < \epsilon + |f(x)|_p,$$

vilket kan användas till att finna en begränsning för alla j,

$$|g_j(X)|_p < \epsilon + |f(x)|_p + \max_{1 \leq i < N} |g_i(X)|_p = k.$$

I synnerhet har vi $|r_{i,j}|_p^n \leq k^n + k$, och $|r_{i,j}|_p$ är uppåt begränsad. □

[1] En annan beteckning för denna kropp är $\mathbb{C}_p$, utläst »de komplexa p-adiska talen«, just för att betona analogin till $\mathbb{R}$ och dennas kompletta tillslutning $\mathbb{C}$.

Vi ska nu visa att vi kan finna ett nollställe $r_{i_j,j}$ (med $1 \leq i_j \leq n$) till g_j för $j = 1, 2, 3...$ så att $(r_{i_j,j})$ är en Cauchy-riktig följd. Om vi lyckas med detta är vi klara: Eftersom Ω_p är komplett existerar $r \in \Omega_p$ så att

$$r = \lim_{j\to\infty} r_{i_j,j}.$$

Men

$$f(r) = \lim_{j\to\infty} f(r_{i_j,j}) = \lim_{j\to\infty} g_j(r_{i_j,j}) = 0,$$

så i sådana fall har f en rot, och Ω_p är algebraiskt sluten.

För att visa att det går att finna en sådan Cauchy-riktig följd antar vi först att vi känner $r_{i_j,j}$; från denna ska vi så småningom välja $r_{i_{j+1},j+1}$. Vi definierar $\delta_j = |g_j - g_{j+1}| = \max_{1\leq i\leq n}(|a_{i,j} - a_{i,j+1}|_p)$ (vilket går mot noll när $j \to \infty$) och $A_j = \max(1, |r_{i_j,j}|_p^n)$. Från lemmat följer det att det existerar en konstant A så att $A_j \leq A$ för alla j, och från det faktum att $g_{j+1} \in \overline{Q_p}[X]$ kan skrivas som en produkt av linjära polynom (se avsnitt 3.4) har vi sedan

$$\prod_i |r_{i_j,j} - r_{i,j+1}|_p = |g_{j+1}(r_{i_j,j})|_p = |g_{j+1}(r_{i_j,j}) - g_j(r_{i_j,j})|_p \leq \delta_j A_j \leq \delta_j A.$$

Detta implicerar att någon faktor uppfyller $|r_{i_j,j} - r_{i,j+1}|_p \leq \sqrt[n]{\delta_j A}$. Låt nu $r_{i_{j+1},j+1}$ vara någon sådan rot. På så vis har vi funnit en följd av rötter $(r_{i_j,j})$ där avståndet mellan två element krymper allt eftersom följden växer. I p-adisk metrik är detta tillräckligt för att följden ska vara Cauchy-riktig: Om (a_i) är en följd som uppfyller $\forall\epsilon\ \exists N\ \forall k \geq N :\ |a_{k+1} - a_k|_p < \epsilon$, har vi, om $m > n \geq N$,

$$|a_m - a_n|_p \leq |a_m - a_{m-1} + a_{m-1} - ... + a_{i+1} - a_i|_p \leq \max_{m>i\geq n} \{|a_{i+1} - a_i|_p\} < \epsilon,$$

vilket precis motsvarar definitionen av en Cauchy-följd. I synnerhet innebär detta att vår följd av rötter $(r_{i_j,j})$ är Cauchy-riktig, och satsen följer. □

För de p-adiska talen har vi i och med detta funnit en »komplex utvidgning«, det vill säga en utvidgning som både är komplett och algebraiskt sluten. Epitetet är alltså denna gång välförtjänt.

På ett liknande sätt som att $\mathbb{C}$ med hjälp av både analytiska och algebraiska metoder kan användas för utsagor om de reella talen, kan Ω_p röja hemligheter om $\mathbb{Q}_p$. Kropparna kan till och med användas i studiet av de sedvanliga komplexa talen, med hjälp av isomorfismer dem emellan. För vidare läsning rekommenderas senare delen av [Hamburg, 2004], samt det sista kapitlet i [Koblitz, 1984].

Litteraturförteckning

[Bachman, 1964] Bachman, G. (1964). *Introduction to p-Adic Numbers and Valuation Theory*. Academic Press Inc.

[Cohn, 2005] Cohn, P. M. (2005). *Basic Algebra: Groups, Rings and Fields*. Springer Science + Business Media.

[Grillet, 2007] Grillet, P. A. (2007). *Abstract Algebra*. Springer Science + Business Media.

[Hamburg, 2004] Hamburg, M. (2004). Construction of c_p and extension of p-adic valuations to c. `http://wstein.org/129/projects/hamburg/Project.pdf`. Hämtad 2015-12-31.

[Koblitz, 1984] Koblitz, N. (1984). *p-adic Numbers, p-adic Analysis, and Zeta-functions*. Springer-Verlag.

[Nironi, 2007] Nironi, F. (2007). Completion of a metric space. `http://www.math.columbia.edu/~nironi/completion.pdf`. Hämtad 2015-11-05.

[Rudin, 1976] Rudin, W. (1976). *Principles of Mathematical Analysis*. McGraw-Hill, Inc.