Der Satz von Skolem, Mahler, Lech - Ein Ergebnis über die Nullstellen linearer Rekursionsfolgen

Diplomarbeit
zur Erlangung des akademischen Grades
Magistra der Naturwissenschaften
an der formal- und naturwissenschaftlichen Fakultät
der Universität Wien

eingereicht von Ilse Fischer

Begutachter: o.Univ.Prof.Dr. Johann Cigler

Wien, im September 1997

Inhaltsverzeichnis

Kapitel 1

Einführung

1.1 Worum geht es?

Unter einer linearen, homogenen Rekursionsfolge (in dieser Arbeit kurz Rekurrenz genannt) versteht man eine Folge $(a_n)_{n\geq 0}$ über einem Körper K, für die es $s_1, s_2, ...s_m \in K$ gibt, nicht alle Null, sodaß

$$a_n = s_1 a_{n-1} + s_2 a_{n-2} + ... + s_m a_{n-m} \tag{1.1}$$

für $n \geq m$ erfüllt ist.
Eine Rekurrenz ist durch ihre 'Anfangsbedingungen' $a_0, a_1, ...a_{m-1}$ und die Koeffizienten ihrer 'Rekurrenzrelation' $s_1, s_2, ...s_m$ eindeutig bestimmt. Jedes Element a_n der Folge mit $n \geq m$ läßt sich mit Hilfe von (1.1) rekursiv aus den m vorhergehenden Folgengliedern berechnen. Beispiele für solche Folgen sind daher leicht konstruiert:

Beispiele

(1) Die Fibonaccizahlen sind eine sehr bekannte Rekurrenz:
$(f_n)_{n\geq 0} = (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, ...)$
Bildungsgesetz: $f_n = f_{n-1} + f_{n-2}$ für $n \geq 2$.

(2) $(a_n)_{n\geq 0} = (8, 0, 9, 0, 8, 0, 4, 0, 0, 0, 16, 0, 128, 0, 576, 0, 2048, 0, 6400, 0, 18432, 0, 50176, ...)$
Diese Rekurrenz genügt einer Rekurrenzrelation, die man nicht sofort errät: $a_n = 6a_{n-2} - 12a_{n-4} + 8a_{n-6}$

(3) $(b_n)_{n\geq 0} = (0, 3, 9, 0, -81, -243, 0, 3^7, 3^8, 0, -3^{10}, -3^{11}, 0, ...)$
$b_n = -3b_{n-1} + 9b_{n-2} - 54b_{n-3}$

(4) $(c_n)_{n\geq 0} = (0, 0, 1, 0, 3, 0, 8, 0, 21, 0, 55, 0, 144, 0, 377, 0, 987, ...)$
$c_n = 3c_{n-2} - c_{n-4}$

(5) Jede periodische Folge ist eine Rekurrenz: Es seien $d_0, d_1, ...d_{m-1} \in K$. Dann ist die Folge $(d_n)_{n\geq 0}$ mit dem Bildungsgesetz $d_n = d_{n-m}$ für $n \geq m$ eine Rekurrenz mit Periode $d_0, d_1, ...d_{m-1}$.

In dieser Arbeit beschäftigte ich mich mit folgendem schönen

Satz von Skolem, Mahler, Lech
Es sei $(a_n)_{n\geq 0}$ eine Rekurrenz über einem Körper K mit char(K)=0. Dann ist die Menge aller Indizes n mit $a_n = 0$ die Vereinigung einer endlichen Menge und endlich vieler arithmetischer Progressionen.
(Unter einer arithmetischen Progression verstehen wir hier eine Menge der Form $r + d\mathbb{N}$, wobei $r, d \in \mathbb{N}$ und $r < d$.)

Für $K = \mathbb{Q}$ wurde dieser Satz 1933 erstmals von Skolem in [19] veröffentlicht. Im Jahre 1935 bewies Mahler ihn in [10] für algebraische Erweiterung von $\mathbb{Q}$ und 1953 gelang Lech schließlich der Beweis für beliebige Erweiterungen von $\mathbb{Q}$, also für jeden Körper der Charakteristik 0 (siehe [9]).
Mit Hilfe eines Einbettungssatzes für Körper (der in Kapitel 3 vorgestellt wird, [4]) wurde der Beweis des Satzes von Cassels 1976 vereinfacht.

Wir wollen den Satz zunächst anhand der fünf Beispiele veranschaulichen und überprüfen:

(1) Die 'Nullstellenmenge' der Fibonaccifolge $\{n \in \mathbb{N} | f_n = 0\} = \{0\}$ ist endlich. Für diese Folge ist der Satz von Skolem-Mahler-Lech daher leicht nachgewiesen.

(2) Man wird vermuten, daß $\{n \in \mathbb{N} | a_n = 0\} = (1 + 2\mathbb{N}) \cup \{8\}$, d.h. die Nullstellenmenge ist in diesem Fall die Vereinigung einer einelementigen Menge und einer arithmetischen Progression.

(3) Ebenso vermutet man wahrscheinlich $\{n \in \mathbb{N} | b_n = 0\} = 3\mathbb{N}$ und

(4) $\{n \in \mathbb{N} | c_n = 0\} = (2\mathbb{N}) \cup \{0\}$.

(5) Es sei $R = \{r \in \{0, 1, ...m-1\} | d_r = 0\}$. Dann ist $\{n \in \mathbb{N} | d_n = 0\} = \bigcup\limits_{r \in R} (r + m\mathbb{N})$.

(Im nächsten Abschnitt werden wir die Vermutungen für die Beispiele (2),(3) und (4) beweisen.)

1.2 Äquivalenz Rekurrenzen $\leftrightarrow$ Exponentialpolynome

Die Folge $(a_n)_{n\geq 0}$ sei wieder eine Rekurrenz über einem beliebigen Körper K, die der Rekurrenzrelation (1.1) genügt. Es gibt eine Möglichkeit, für a_n eine explizite Formel anzugeben, die sich mit Hilfe der Anfangsbedingungen $a_0, a_1, ...a_{m-1}$ und der Koeffizienten $s_1, s_2 ... s_m$ der Rekurrenzrelation bestimmen läßt.

Dazu berechnen wir zunächst die erzeugende Funktion $\sum\limits_{n=0}^{\infty} a_n X^n =: F(X)$ von $(a_n)_{n\geq 0}$:
Multipliziere die Gleichung $a_n = s_1 a_{n-1} + ... + s_m a_{n-m}$ mit X^n und summiere über alle $n \geq m$

$$\Rightarrow \quad \sum_{n=m}^{\infty} a_n X^n = X s_1 \sum_{n=m}^{\infty} a_{n-1} X^{n-1} + ... + X^m s_m \sum_{n=m}^{\infty} a_{n-m} X^{n-m}.$$

Es folgt:

$$F(X) - a_0 - a_1X - ... - a_{m-1}X^{m-1} =$$
$$= Xs_1(F(X) - a_0 - a_1X - ... - a_{m-2}X^{m-2}) + ... + X^m s_m F(X)$$

Das ist eine lineare Gleichung in $F(X)$. Mit ihrer Hilfe können wir die erzeugende Funktion berechnen:

$$F(X) =$$
$$\frac{a_0 + a_1X + ... + a_{m-1}X^{m-1} + Xs_1(-a_0 - a_1X - ... - a_{m-2}X^{m-2}) + ... + X^{m-1}s_{m-1}(-a_0)}{1 - s_1X - ... - s_mX^m}$$

$F(X)$ ist eine rationale Funktion. Der Nenner (=: $s(X)$) hat den Grad m, der Zähler (=: $r(X)$) einen Grad $\leq m-1$. (Ich nehme o.B.d.A $s_m \neq 0$ an.)
Man sieht also, daß Rekurrenzen als Taylor-Koeffizienten von rationalen Funktionen auftreten, wobei der Grad des Zählers echt kleiner als der Grad des Nenners ist ($\Leftrightarrow \lim\limits_{x\to\infty} F(x) = 0$, d.h. '$F(X)$ verschwindet in ∞').

Es sei $L \supseteq K$ der Zerfällungskörper des Polynoms $s(X)$. Wegen $s(0) \neq 0$ kann man $s(X)$ über L folgendermaßen in Linearfaktoren zerlegen:

$$s(X) = \prod_{i=1}^{k}(1 - \alpha_i X)^{n_i},$$

wobei $\alpha_i \in L$, $n_i \in \mathbb{N}$, $\sum\limits_{i=1}^{k} n_i = m$ und $\alpha_i \neq \alpha_j$ für $i \neq j$.

Wenn man bei $\frac{r(X)}{s(X)}$ eine Partialbruchzerlegung durchführt, erhält man

$$\frac{r(X)}{s(X)} = \sum_{i=1}^{k}\sum_{j=1}^{n_i}\frac{r_{ij}}{(1-\alpha_i X)^j},$$

wobei r_{ij} Koeffizienten in L sind. (An dieser Stelle geht $deg(r) < deg(s)$ ein.)
Mit Hilfe der bekannten Identität

$$\left(\frac{1}{1-Y}\right)^{-j} = \sum_{h=0}^{\infty}\binom{h+j-1}{j-1}Y^h$$

erhalten wir

$$\begin{aligned} F(X) &= \sum_{i=1}^{k}\sum_{j=1}^{n_i}\frac{r_{ij}}{(1-\alpha_i X)^j} = \\ &= \sum_{i=1}^{k}\sum_{j=1}^{n_i} r_{ij}\left(\sum_{h=0}^{\infty}\binom{h+j-1}{j-1}\alpha_i^h X^h\right) = \sum_{h=0}^{\infty}\left(\sum_{i=1}^{k}\sum_{j=1}^{n_i} r_{ij}\binom{h+j-1}{j-1}\alpha_i^h\right)X^h. \end{aligned}$$

Der Koeffizientenvergleich ergibt

$$a_h = \sum_{i=1}^{k}\left(\sum_{j=1}^{n_i} r_{ij}\binom{h+j-1}{j-1}\right)\alpha_i^h.$$

Der Binomialkoeffizient $\binom{h+j-1}{j-1}$ kann als Polynom in h mit Grad $j-1$ aufgefaßt werden. Setze $A_i(h) = \sum_{j=1}^{n_i} r_{ij}\binom{h+j-1}{j-1}$. Dann ist $A_i(h)$ ein Polynom in h dessen Grad $\leq n_i - 1$ ist.

$\Rightarrow a_h = \sum_{i=1}^{k} A_i(h)\alpha_i^h$. Das ist also die versprochene explizite Darstellung der Rekurrenz.

Umgekehrt definiert aber auch jedes andere 'Exponentialpolynom'

$$\sum_{i=1}^{k} B_i(n)\beta_i^n =: b_n$$

eine Rekurrenz:

Es seien $B_i(X)$ beliebige Polynome über L. Setze $n_i = deg(B_i) + 1$, $m = \sum_{i=1}^{k} n_i$ (=: Ordnung des Exponentialpolynoms) und $s(X) := \prod_{i=1}^{k}(1-\beta_i X)^{n_i} = 1 - s_1 X - \ldots - s_m X^m$.

Ich behaupte, daß dann die Folge $(b_n)_{n\geq 0}$ der Rekurrenzrelation

$$b_n = s_1 b_{n-1} + \ldots + s_m b_{n-m} \quad n \geq m$$

genügt.

Um das zu sehen, definieren wir auf der Menge aller Folgen über L den Shift-Operator $E : f(h) \mapsto f(h+1)$. Er erfüllt folgende Eigenschaften:

(1) $E^n(f)(h) = f(n+h)$

(2) $E(f+g) = E(f) + E(g)$

(3) Es sei $\alpha, \beta \in L$. Dann gilt:

$$(E-\alpha)(E-\beta) = E^2 - (\alpha+\beta)E + \alpha\beta = (E-\beta)(E-\alpha)$$

Es folgt

$$(E-\alpha_i)(B_i(h)\beta_i^h) = B_i(h+1)\beta_i^{h+1} - B_i(h)\beta_i^{h+1} = (\Delta B_i(h))\beta_i^{h+1},$$

wobei $\Delta B_i(h) = B_i(h+1) - B_i(h)$ ein Polynom ist, dessen Grad kleiner als der von $B_i(h)$ ist. Aus $deg(B_i) = n_i - 1$ folgt daher:

$$(E-\beta_i)^{n_i}(B_i(h)\beta_i^h) \equiv 0$$

Wir setzen $P = \prod_{i=1}^{k}(E-\beta_i)^{n_i}$. Wegen Eigenschaft (3) müssen wir in diesem Produkt nicht auf die Reihenfolge der Faktoren $E - \beta_i$ achten:

$$\Rightarrow P(b_h) = P\left(\sum_{j=1}^{k} B_j(h)\beta_j^h\right) \overset{(2)}{=} \sum_{j=1}^{k} P(B_i(h)\beta_i^h) =$$

$$= \sum_{j=1}^{k}\left(\prod_{i\neq j}(E-\beta_i)^{n_i}\right)(E-\beta_j)^{n_j}(B_j(h)\beta_j^h) = 0$$

und daher

$$\begin{aligned} 0 = P(b_h) &= (E^n - s_1 E^{n-1} - ... - s_m) b_h = \\ &= b_{h+n} - s_1 b_{h+n-1} - ... - s_m b_h. \end{aligned}$$

Man sieht, daß eine ein-eindeutige Korrespondenz zwischen Rekurrenzen, rationalen Funktionen, die in ∞ verschwinden, und Exponentialpolynomen besteht. Der Satz von Skolem-Mahler-Lech ist daher auch einer über rationale Funktionen und über Exponentialpolynome.

Beispiele Wie nützlich diese Darstellung durch Exponentialpolynome ist, werde ich nun anhand von Beispiel (2),(3) und (4) demonstrieren. Mit ihrer Hilfe lassen sich nämlich unsere Vermutungen bezüglich der Nullstellenmengen beweisen.

ad 2) Das 'charakteristische Polynom' (=Nenner der erzeugenden Funktion) von $(a_n)_{n\geq 0}$ lautet

$$s_a(X) = 1 - 6X^2 + 12X^4 - 8X^6.$$

Nach Bestimmung der Nullstellen von $s_a(X)$ erhält man die Zerlegung

$$s_a(X) = (1 - \sqrt{2}X)^3 (1 + \sqrt{2}X)^3.$$

Es folgt die Existenz von zwei Polynomen $p(X), q(X) \in \mathbb{Q}[\sqrt{2}]$ mit $deg(p), deg(q) \leq 2$ und

$$a_n = (\sqrt{2})^n p(n) + (-\sqrt{2})^n q(n)$$

Diese Polynome könnte man, wie oben gezeigt, mit Hilfe der erzeugenden Funktion von $(a_n)_{n\geq 0}$ berechnen. Da wir aus obiger Ableitung schon den maximalen Grad der Polynome $p(X)$ und $q(X)$ kennen, können wir aber auch so vorgehen: Wir setzen die Polynome

$$p(X) = p_0 + p_1 X + p_2 X^2 \text{ und } q(X) = q_0 + q_1 X + q_2 X^2$$

unbekannt an. Mit Hilfe der 'Anfangfsbedingungen'

$$a_0 = 8, a_1 = 0, a_2 = 9, a_3 = 0, a_4 = 8, a_5 = 0$$

ergibt sich folgendes lineares Gleichungssystem in $p_0, p_1, p_2, q_0, q_1, q_2$:

$$\begin{aligned} 8 &= p_0 + q_0 \\ 0 &= \sqrt{2}(p_0 + p_1 + p_2 - q_0 - q_1 - q_2) \\ 9 &= 2(p_0 + p_1 2 + p_2 4 + q_0 + q_1 2 + q_2 4) \\ 0 &= 2\sqrt{2}(p_0 + p_1 3 + p_2 9 - q_0 - q_1 3 - q_2 9) \\ 8 &= 4(p_0 + p_1 4 + p_2 16 + q_0 + q_1 4 + q_2 16) \\ 0 &= 4\sqrt{2}(p_0 + p_1 5 + p_2 25 - q_0 - q_1 5 - q_2 25) \end{aligned}$$

Wenn man dieses Gleichungssystem löst, erhält man $p_0 = q_0 = 0, p_1 = q_1 = -1, p_2 = q_2 = \frac{1}{16}$ und damit

$$a_n = (\sqrt{2})^n \left(4 - n + \frac{n^2}{16}\right)(1 + (-1)^n) \quad \forall n \in \mathbb{N}.$$

Da $a_n = 0 \Leftrightarrow (4 - n + \frac{n^2}{16} = 0 \vee 1 + (-1)^n = 0)$, folgt

$$\{n \in \mathbb{N} | a_n = 0\} = \{8\} \cup (1 + 2\mathbb{N}).$$

ad 3) Aus der Zerlegung des charakteristischen Polynoms von $(b_n)_{n \geq 0}$

$$s_b(X) = 1 + 3X - 9X^2 + 54X^3 = (1 + 6X)\left(1 - 3\frac{1+\sqrt{3}i}{2}X\right)\left(1 - 3\frac{1-\sqrt{3}i}{2}X\right)$$

folgt der Ansatz

$$b_n = r(-6)^n + s\left(3\frac{1+\sqrt{3}i}{2}\right)^n + t\left(3\frac{1-\sqrt{3}i}{2}\right)^n$$

$(r, s, t \in \mathbb{C})$. Gemeinsam mit den Anfangsbedingungen $b_0 = 0, b_1 = 3, b_2 = 9$ erhält man ein Gleichungssystem in r, s und t:

$$\begin{aligned}
0 &= r + s + t \\
3 &= r(-6) + s\left(3\frac{1+\sqrt{3}i}{2}\right) + t\left(3\frac{1-\sqrt{3}i}{2}\right) \\
9 &= r(-6)^2 + s\left(3\frac{1+\sqrt{3}i}{2}\right)^2 + t\left(3\frac{1-\sqrt{3}i}{2}\right)^2
\end{aligned}$$

Die Lösung dieses Gleichungssystems ist $r = 0$, $s = -\frac{\sqrt{3}}{3}i$ und $t = \frac{\sqrt{3}}{3}i$. Das ergibt

$$\begin{aligned}
b_n &= \left(3\frac{1+\sqrt{3}i}{2}\right)^n \left(-\frac{\sqrt{3}}{3}i\right) + \left(3\frac{1-\sqrt{3}i}{2}\right)^n \left(\frac{\sqrt{3}}{3}i\right) = \\
&= 3^n \left(\frac{\sqrt{3}}{3}i\right) \cdot \left(-\left(\frac{1+\sqrt{3}i}{2}\right)^n + \left(\frac{1-\sqrt{3}i}{2}\right)^n\right).
\end{aligned}$$

Da $b_n = 0 \Leftrightarrow$

$$\begin{aligned}
&\Leftrightarrow \quad 0 = -\left(\frac{1+\sqrt{3}i}{2}\right)^n + \left(\frac{1-\sqrt{3}i}{2}\right)^n = -\left(\frac{1+\sqrt{3}i}{2}\right)^n + \left(\left(\frac{1+\sqrt{3}i}{2}\right)^5\right)^n \Leftrightarrow \\
&\Leftrightarrow \quad \left(\left(\frac{1+\sqrt{3}i}{2}\right)^4\right)^n = 1 \Leftrightarrow 3|n \text{ (weil } \left(\tfrac{1+\sqrt{3}i}{2}\right)^4 \text{ primitive 3-te Einheitswurzel ist)}
\end{aligned}$$

folgt die Behauptung.

ad 4)

$$\begin{aligned}
s_c(X) &= 1-3X^2+X^4= \\
&= \left(1-\frac{1+\sqrt{5}}{2}X\right)\left(1-\frac{1-\sqrt{5}}{2}X\right)\left(1+\frac{1+\sqrt{5}}{2}X\right)\left(1+\frac{1-\sqrt{5}}{2}X\right) \\
\ldots \Rightarrow c_n &= \left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n+\left(-\frac{1+\sqrt{5}}{2}\right)^n-\left(-\frac{1-\sqrt{5}}{2}\right)^n\right)\frac{1}{2\sqrt{5}}= \\
&= (1+(-1)^n)\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)\frac{1}{2\sqrt{5}} \\
&\Rightarrow \quad \{n\in\mathbb{N}|c_n=0\}=(1+2\mathbb{N})\cup\{0\}.
\end{aligned}$$

Nachdem wir den Satz von Skolem-Mahler-Lech für unsere Beispiele aus Abschnitt 1.1 gezeigt haben, wollen wir ihn hier auch noch für einen anderen einfachen Spezialfall beweisen:

Es sei $(a_n)_{n\geq 0}$ wieder eine beliebige Rekurrenz, die der Rekurrenzrelation (1.1) genügt. Diese Rekurrenzrelation und daher erst recht ihre Länge m ist nicht eindeutig bestimmt. Ist aber $m\in\mathbb{N}$ minimal, sodaß $s_1, s_2, \ldots s_m \in K$ existieren, die (1.1) erfüllen, dann nennt man m die Ordnung der Rekurrenz $(a_n)_{n\geq 0}$. (Sie stimmt übrigens mit der Ordnung des entsprechenden Exponentialpolynoms überein.) Die Ordnung beschreibt also in gewisser Weise die Komplexität der Rekurrenz.
Man kann den Satz von Skolem-Mahler-Lech für Rekurrenzen der Ordnung 1 und 2 leicht zeigen:

Ordnung 1 Es sei $(a_n)_{n\geq 0}$ eine Rekurrenz über K, mit

$$a_n = s_1 a_{n-1} \text{ für } n\geq 1.$$

Dann gilt $a_n = s_1^n a_0$. Ist daher $a_{n_0}=0$ für ein $n_0\in\mathbb{N}$, so ist entweder $s_1=0$ oder $a_0=0$, und daher $a_n=0 \quad \forall n\in\mathbb{N}$.

Ordnung 2 Es sei $(a_n)_{n\geq 0}$ eine Rekurrenz über K, mit

$$a_n = s_1 a_{n-1} + s_2 a_{n-2} \text{ für } n\geq 2.$$

Wir unterscheiden zwei Fälle:

(1) Wenn das charakteristische Polynom $1-s_1X-s_2X^2$ zwei verschiedene Nullstellen α,β in seinem Zerfällungskörper L hat, so gibt es $a, b\in L$ mit

$$a_n = a\alpha^n + b\beta^n \quad \forall n\in\mathbb{N}.$$

Es folgt $\alpha,\beta,a,b\neq 0$, denn andernfalls wäre $(a_n)_{n\geq 0}$ eine Rekurrenz der Ordnung 1. Angenommen es gäbe zwei verschiedene natürliche Zahlen $n_1<n_2$ mit $a_{n_1}=a_{n_2}$=0. Dann ist

$$-\frac{a}{b}=\left(\frac{\beta}{\alpha}\right)^{n_i}$$

für $i = 1, 2$. Dividiert man die erste dieser beiden Gleichungen durch die zweite, so erhält man

$$\left(\frac{\beta}{\alpha}\right)^{n_2 - n_1} = 1.$$

Der Bruch $\frac{\beta}{\alpha}$ ist daher eine Einheitswurzel. Es sei $d \in \{1, 2, 3, ...\}$ minimal mit

$$\left(\frac{\beta}{\alpha}\right)^{d} = 1$$

und $r \in \mathbb{N}$ minimal mit $a_r = 0$. Dann ist $\{n \in \mathbb{N} | a_n = 0\} = r + d\mathbb{N}$, wie man leicht zeigt. (Es ist $r < d$, weil sonst $a_{r-d} = 0$ folgen würde und das ein Widerspruch zur Wahl von r ist.) Solche Rekurrenzen haben daher entweder keine oder eine Nullstelle oder sie haben unendlich viele, die eine arithmetische Progression bilden.

(2) Übrig bleibt der Fall, daß das charakteristische Polynom der Rekurrenz eine doppelte Nullstelle $\alpha \in L \setminus \{0\}$ hat. Dann gibt es $a_1, a_2 \in L$ mit $a_2 \neq 0$ und

$$a_n = (a_2 \cdot n + a_1)\alpha^n.$$

Ist $\frac{-a_1}{a_2}$ ein natürliche Zahl, so ist sie das einzige Element der Menge $\{n \in \mathbb{N} | a_n = 0\}$. Andernfalls kann so eine Rekurrenz überhaupt keine Nullstellen haben.

Nun könnte man meinen, daß man für Rekurrenzen höherer Ordnung den Satz auf ähnliche Weise mit Hilfe von Exponentialpolynomen beweisen kann. Ganz so einfach ist es aber nicht: Mit dem eben gezeigten haben wir den Satz für Rekurrenzen der Ordnung 1 und 2 in Körpern mit beliebiger Charakteristik bewiesen. In der Formulierung des Satzes wurde der Fall $\mathrm{char}(K) > 0$ aber ausgenommen. Im nächsten Kapitel werde ich für jedes prime p einen Körper F mit $\mathrm{char}(F) = p$ und eine Rekurrenz über F der Ordnung 3 angeben, deren Nullstellenmenge nicht diese schöne Struktur hat. Das impliziert dann, daß man den Satz von Skolem-Mahler-Lech für Rekurrenzen, deren Ordnung größer als 2 ist, nicht mehr so einfach durch ein paar algebraische Umformungen des Exponentialpolynoms zeigen kann.
(Für Rekurrenzen, deren Ordnung größer als 3 ist, kann man das natürlich nur vermuten. Diese Vermutung ist jedoch sehr naheliegend, da solche Rekurrenzen ja nur noch komplizierter als jene der Ordnung 3 sind.)

1.3 Rekurrenzen über Körpern mit positiver Charakteristik

In diesem Abschnitt sei p eine beliebige, aber feste Primzahl und $k = \mathbb{F}_p(X)$ der Quotientenkörper des Polynomringes $\mathbb{F}_p[X]$ (X eine Unbestimmte).
Ich definiere eine Folge $(u_n)_{n \geq 0}$ über k:

$$u_n = (X+1)^n - X^n - 1$$

Die Folge $(u_n)_{n\geq 0}$ ist eine Rekurrenz, da $(X+1)^n - X^n - 1 = (X+1)^n - X^n - 1^n$ ein Exponentialpolynom ist. Berechnet man die Koeffizienten des charakteristischen Polynoms $(1-(X+1)Y)(1-XY)(1-Y)$ von $(u_n)_{n\geq 0}$, so erhält man die Rekurrenzrelation

$$u_n = (2+X)u_{n-1} - (X^2+3X+1)u_{n-2} + (X^2+X)u_{n-3} \quad n \geq 3.$$

Ich behaupte, daß

$$\{n \in \mathbb{N} | u_n = 0\} = \{1, p, p^2, p^3, p^4, p^5, ...\} = \{p^i | i \in \mathbb{N}\}$$

und daher nicht Vereinigung einer endlichen Menge und endlich vieler arithmetischer Progressionen ist.

Es gilt

$$\begin{aligned} 0 = (X+1)^n - X^n - 1 &= \sum_{k=0}^{n} \binom{n}{k} X^{n-k} - X^n - 1 = \sum_{k=1}^{n-1} \binom{n}{k} X^{n-k} \Leftrightarrow \\ &\Leftrightarrow \binom{n}{k} \equiv 0 \quad mod\, p \quad \forall k \in \{1, ...n-1\} \end{aligned}$$

Es genügt daher die Äquivalenz

$$\binom{n}{k} \equiv 0 \quad mod\, p \quad \forall k \in \{1, ...n-1\} \quad \Leftrightarrow \quad n = p^m \text{ für ein } m \in \mathbb{N} \qquad (*)$$

zu zeigen. Dafür benötigen wir folgenden

Hilfssatz 1.1 *Satz von Lucas (1878)*

Es seien $r, s \in \mathbb{N}$ beliebig und $n \in \mathbb{N}$, sodaß $r < p^n$ und $s < p^n$. Nach dem Satz über die p-adische Darstellung natürlicher Zahlen gibt es $r_i, s_i \in \{0, 1, ...p-1\}$ für $i = 0, 1, ...n-1$ mit $r = r_0 + r_1 p + ... + r_n p^{n-1}$ und $s = s_0 + s_1 p + ... + s_n p^{n-1}$. Dann gilt

$$\binom{s}{r} \equiv \binom{s_{n-1}}{r_{n-1}} \binom{s_{n-2}}{r_{n-2}} ... \binom{s_0}{r_0} \quad mod\, p.$$

Beweis: Betrachte $(1+X)^s \in \mathbb{F}_p[X]$.

$$\begin{aligned} & \sum_{k=0}^{\infty} \binom{s_{n-1}p^{n-1} + ... + s_1 p + s_0}{k} X^k = (1+X)^{s_{n-1}p^{n-1}+...+s_1p+s_0} \equiv \\ \equiv\ & (1+X^{p^{n-1}})^{s_{n-1}} \cdot ... \cdot (1+X^p)^{s_1} (1+X)^{s_0} = \\ =\ & \sum_{i_{n-1}=0}^{\infty} \binom{s_{n-1}}{i_{n-1}} (X^{p^{n-1}})^{i_{n-1}} \cdot ... \cdot \sum_{i_1=0}^{\infty} \binom{s_1}{i_1} (X^p)^{i_1} \sum_{i_0=0}^{\infty} \binom{s_0}{i_0} X^{i_0} = \\ =\ & \sum_{i_{n-1},...i_1,i_0 \geq 0} \binom{s_{n-1}}{i_{n-1}} \cdot ... \cdot \binom{s_1}{i_1} \binom{s_0}{i_0} X^{i_{n-1}p^{n-1}+...+i_1p+i_0} \end{aligned}$$

(in $\mathbb{F}_p[X]$, da $(1+X)^p \equiv (1+X^p) \ \ mod\, p)$
Der Koeffizientenvergleich bei $r = r_{n-1}p^{n-1} + ... + r_1 p + r_0$ und die Tatsache, daß die p-adische Darstellung von r eindeutig ist, ergibt die Behauptung. □

Wir wollen nun (*) zeigen:
Zuerst nehmen wir $n = p^m$ für ein $m \in \mathbb{N}$ an. Es sei $k \in \{1, 2, ...p^m - 1\}$. Dann gibt es $k_i \in \{0, 1, ...p-1\}$ für $i = 0, 1, ...m-1$ mit $k = k_0 + k_1 p + ... + k_{m-1}p^{m-1}$. Da $k \neq 0$ ist $k_{i_0} \neq 0$ für ein i_0. Es ist daher $\binom{0}{k_{i_0}} \equiv 0 \ \ mod\, p$. Das, gemeinsam mit dem Hilfssatz, ergibt

$$\binom{p^m}{k} \equiv \binom{1}{0}\binom{0}{k_{m-1}}...\binom{0}{k_{i_0}}...\binom{0}{k_0} \equiv 0 \ \ mod\, p$$

und damit haben wir eine Richtung von (*) gezeigt.

Es sei umgekehrt n keine Potenz von p. Dann gibt es zwei natürliche Zahlen m und $l \neq 1$, $p \not| l$, sodaß $n = p^m l$. Wiederum aus dem Hilfssatz folgt:

$$\binom{p^m l}{p^m} \equiv \binom{l_{k-1}}{0}\binom{l_{k-2}}{0} \cdot ... \cdot \binom{l_1}{0}\binom{l_0}{1}\binom{0}{0} \cdot ... \cdot \binom{0}{0} \equiv \binom{l}{1} \not\equiv 0 \ \ mod\, p$$

wenn $l = l_{k-1}p^{k-1} + ... + l_0$ die p-adische Darstellung von l ist (Daraus ergibt sich nämlich die p-adische Darstellung von $p^m l = l_{k-1}p^{m+k-1} + ... + l_0 p^m$.).
Somit haben wir (*) vollständig gezeigt und damit die Aussage über die Nullstellenmenge von $(u_n)_{n\geq 0}$.
(Dieses Beispiel stammt übrigens von Lech [9].)

Dieses Beispiel lehrt uns, daß der Satz von Skolem-Mahler-Lech für Rekurrenzen über Körper mit positiver Charakteristik, die ein Element enthalten, welches transzendent über dem Primkörper ist, im allgemeinen nicht erfüllt ist. Nun stellt sich die Frage, wie es mit den restlichen Körpern von positiver Charakteristik aussieht, d.h. mit den Körpern F, wo jedes Element algebraisch über dem Primkörper ist: Es sei $(a_n)_{n\geq 0}$ eine Rekurrenz über F, die der Rekurrenzrelation (1.1) genügt und $p = $char$(F)$. Da $a_n \in \mathbb{F}_p[a_0, a1, ...a_{m-1}, s_1, s_2, ...s_m]$ für $n \in \mathbb{N}$ können wir o.B.d.A. annehmen, daß F endlich erzeugt über $\mathbb{F}_p$ ist und daher, wegen der Voraussetzung, daß F nur algebraische Elemente enthält, endlich ist. Wir zeigen die Existenz einer natürlichen Zahl $\Pi \in \{1, 2, 3, ...\}$ mit

$$a_n = a_{n+\Pi} \quad \forall n \in \mathbb{N}.$$

(d.h. $(a_n)_{n\geq 0}$ ist periodisch und insbesondere ist daher die Nullstellenmenge dieser Rekurrenz die Vereinigung endlich vieler arithmetischer Progressionen zum Modul Π.)
Wieder können wir o.B.d.A. annehmen, daß $s_m \neq 0$. Setze $c = |F|$. Betrachte die $c^m + 1$ m-tupel

$$(a_0, a_1, ...a_{m-1})$$

$$(a_1, a_2, ...a_m)$$

$$...$$

$$(a_{c^m}, a_{c^m+1}, ...a_{c^m+m-1})$$

Da es genau c^m verschiedene m-tupel über F gibt, folgt aus dem Dirichletschen Schubfachprinzip die Existenz zweier natürlicher Zahlen $n_1 < n_2$ mit $n_1, n_2 \in \{0, 1, ...c^m\}$ und

$$(a_{n_1}, ...a_{n_1+m-1}) = (a_{n_2}, ...a_{n_2+m-1}).$$

Setze $\Pi = n_2 - n_1$. Mit Hilfe der Rekurrenzrelation zeigt man induktiv relativ leicht, daß

$$a_n = a_{n+\Pi} \text{ für } n \geq n_1$$

und unter Benützung von $s_m \neq 0$ folgt schließlich

$$a_n = a_{n+\Pi} \quad \forall n \in \mathbb{N}.$$

(vgl. Hilfssatz 5.1)
Somit erhalten wir eine zweite große Klasse von Rekurrenzen (neben denen der Ordnung 1 und 2) über Körper mit positiver Charakteristik, deren Nullstellenmenge diese schöne Struktur hat.

Damit ist das Thema 'Rekurrenzen über Körpern mit positiver Charakteristik' für uns endgültig abgeschlossen und wir wenden uns nun ganz den Rekurrenzen über Körpern mit Charakteristik 0 zu.

1.4 Wie geht es weiter ?

Unser Ziel ist es, den Satz von Skolem-Mahler-Lech allgemein zu beweisen. Das wird in Kapitel 2, 3 und 4 geschehen. Der Umfang dieser drei Kapitel läßt schon vermuten, daß der Beweis nicht ganz einfach ist. Der Hauptgrund für diesen Umfang ist, daß man einige neue Begriffe benötigt. Hat man diese Begriffe einmal verstanden, so finde ich den Beweis relativ einfach, da er in dieser neuen 'Begriffswelt' hauptsächlich Analogien zu wohlvertrauten Dingen verwendet.
(Für mein Verständis besteht in der Mathematik natürlich vieles aus Analogien zu schon bekannten Dingen. Oft sind diese Analogien aber nicht sofort erkennbar, manchmal wird sie auch nur die/der wirklich sehen, die/der sie gefunden und durch sie etwas bewiesen hat. Das Schöne bei unserem Beweis ist, daß diese Analogien besonders offensichtlich sind.)
Etwas konkreter: Der Beweis funktioniert, indem man die Rekurrenzen in einen anderen Körper verlegt, nämlich in $\mathbb{Q}_p$, den Körper der p-adischen Zahlen. Aus diesem Grund besteht das ganze zweite Kapitel aus der Konstruktion dieses Körpers und einer Einführung in die einfachsten Elemente der dazugehörenden Theorie. Im dritten Kapitel passiert dann die Verlegung der Rekurrenzen in diesen Körper. Im vierten Kapitel können wir schließlich alle in $\mathbb{Q}_p$ zur Verfügung stehenden Hilfsmittel verwenden, um den Satz zu beweisen. Die erwähnten Analogien betreffen hauptsächlich Sätze über Potenzreihen aus der reellen oder komplexen Analysis. So wird zum Beispiel ein Analogon zum Identitätssatz für Potenzreihen ein besonders wichtiges Hilfsmittel sein.

Kapitel 2

Der Körper der p-adischen Zahlen

2.1 Über Zifferndarstellungen

Studiert man Darstellungsweisen der natürlichen Zahlen in anderen Kulturkreisen, so bekommt man leicht den Eindruck, daß das Dezimalsystem eine der grundlegendsten Errungenschaften 'unserer Mathematik' ist. Wer schon einmal probiert hat, im römischen Ziffernsystem zu multiplizieren, weiß wovon die Rede ist.
Die Leistung des Dezimalsystems liegt für uns vordergründig in den einfachen Schemen für die vier Grundrechnungsarten, die durch dieses System ermöglicht werden: Im Prinizip muß man die Grundrechnungsarten nur für die Ziffern $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ auswendig lernen, um beliebig große (natürliche, rationale oder reelle) Zahlen addieren, subtrahieren, multiplizieren und dividieren zu können. Das folgende Kapitel und damit letztendlich auch der ganze Beweis des Satzes von Skolem-Mahler-Lech zeigen aber, daß der Einfluß der Dezimaldarstellung auf die Mathematik an dieser Stelle beim bloßen Rechnen nicht endet.

Die Dezimaldarstellung der natürlichen Zahlen beruht auf dem folgenden

Satz 2.1 *Es sei $g \in \{2, 3, 4, ...\}$.*
Für jede natürliche Zahl n existiert eine eindeutig bestimmte Folge $(a_i)_{i\geq 0}$, mit $a_i \in \{0, 1, ...g-1\}$, $a_i = 0$ für fast alle i und $n = \sum\limits_{i=0}^{\infty} a_i g^i$.

Nun hätte man auch gerne eine Darstellung dieser Art für rationale Zahlen.
Üblicherweise geht man da folgendermaßen vor: Man läßt auch negative Potenzen von g zu. Ist nun r eine postive rationale Zahl, so kann man die Existenz einer Folge $(a_i)_{i\in\mathbb{Z}}$ ($a_i \in \{0, 1, ...g-1\}$, $a_i = 0$ für große i) mit $r = \sum\limits_{i\in\mathbb{Z}} a_i g^i$ zeigen, wobei die Reihe bezüglich des gewöhnlichen Absolutbetrages konvergiert. Um eine Reihenentwicklung von $-r$ zu definieren, setzt man vor die Reihenentwicklung von r ein Vorzeichen '-' : $-r = -\sum\limits_{i\in\mathbb{Z}} a_i g^i$. Die Folge $(a_i)_{i\in\mathbb{Z}}$ ist eindeutig bestimmt, wenn man zusätzlich voraussetzt, daß $a_i \neq g-1$ für unendlich

viele i.
Für $g = 10$ erhält man die gewohnte Dezimaldarstellung der rationalen Zahlen.

Es geht aber auch anders: Ist $g = p$ eine Primzahl, dann kann man auf $\mathbb{Q}$ einen Absolutbetrag $|.|_p$ definieren, sodaß folgender Satz gilt:

Satz 2.2 *Es sei $r \in \mathbb{Q}$. Dann gibt es eine eindeutig bestimmte Folge $(a_i)_{i\in\mathbb{Z}}$ ($a_i \in \{0, 1, ...p-1\}$, $a_i = 0$ für kleine i) mit $r = \sum\limits_{i\in\mathbb{Z}} a_i p^i$, wobei die Summe bezüglich $|.|_p$ konvergiert.*
Man nennt diese Reihendarstellung die p-adische (Reihen-)Darstellung der rationalen Zahl r.

Hier wird die Ausdehnung der Zifferndarstellung auf $\mathbb{Q}$ ermöglicht, in dem man – im Gegensatz zur Dezimaldarstellung – beliebig große Potenzen von p zuläßt.
Ich bemerke außerdem, daß im Unterschied zur ersten Möglichkeit die Folge $(a_i)_{i\in\mathbb{Z}}$ ohne zusätzliche Bedingung eindeutig bestimmt ist und daß auch nicht die Einführung eines Vorzeichens nötig ist (mit dem Nachteil, daß man negative Zahlen an ihrer p-adischen Darstellung nicht sofort erkennt.).
Im nächsten Abschnitt definieren wir den Absolutbetrag $|.|_p$ auf $\mathbb{Q}$ und beweisen Satz 2.

2.2 Der p-adische Absolutbetrag

Definition 2.1 *Der p-adische Absolutbetrag $|.|_p : \mathbb{Q} \to \mathbb{R}^+$ ist wie folgt definiert: Ist $r \in \mathbb{Q} \setminus \{0\}$, so gibt es eindeutig bestimmte $u, v, \sigma \in \mathbb{Z}$ ($v > 0, ggt(u, v) = 1, p \not| uv$) mit $r = p^\sigma \frac{u}{v}$. Setze $|r|_p = p^{-\sigma}$ und $|0|_p = 0$.*

Eine rationale Zahl ist also 'klein' bezüglich des p-adischen Absolutbetrages, wenn ihr (gekürzter) Zähler durch eine 'hohe' Potenz von p teilbar ist.

Diese Abbildung nennt man p-adischen *Absolutbetrag*, da sie folgende 3 Eigenschaften erfüllt:

(1) $|r|_p = 0 \iff r = 0$

(2) $|rs|_p = |r|_p|s|_p \quad \forall r, s \in \mathbb{Q}$

(3) $|r + s|_p \leq max\{|r|_p, |s|_p\} \quad \forall r, s \in \mathbb{Q}$

Beweis:

(1) klar

(2) Ist $rs = 0$, dann ist entweder $r = 0$ oder $s = 0$ und daher $|r|_p|s|_p = 0 = |rs|_p$.
Ist dagegen $rs \neq 0$, so gibt es $u, v, w, x, \sigma, \tau \in \mathbb{Z}$ mit $p \not| uvwx$ und $r = p^\sigma \frac{u}{v}$ bzw. $s = p^\tau \frac{w}{x}$. Es folgt:

$$|rs|_p = \left| p^{\sigma+\tau} \frac{uw}{vx} \right|_p = p^{-(\sigma+\tau)} = p^{-\sigma} p^{-\tau} = |r|_p|s|_p$$

(3) Ist $r = 0$ oder $s = 0$, so ist die Aussage klar.
Es sei also wieder $r = p^\sigma \frac{u}{v}$ und $s = p^\tau \frac{w}{x}$ mit $u, v, w, x, \sigma, \tau \in \mathbb{Z}$ und $p \not| uvwx$. Wir nehmen o.B.d.A. $\tau \geq \sigma$ an. Dann ist

$$r + s = \frac{p^\sigma (ux + p^{\tau-\sigma} vw)}{vx}.$$

Aus $ux + p^{\tau-\sigma} wv \in \mathbb{Z}$ folgt $|ux + p^{\tau-\sigma} vw|_p \leq 1$ und gemeinsam mit (2) ergibt das

$$|r + s|_p \leq \left| \frac{p^\sigma}{vx} \right|_p = p^{-\sigma}$$

Abbildungen φ, die von einem Körper (wie in unserem Fall $\mathbb{Q}$) in die positiven reellen Zahlen führen, die Eigenschaften (1),(2) erfüllen und statt (3) möglicherweise nur die schwächere Dreiecksungleichung $\varphi(a + b) \leq \varphi(a) + \varphi(b)$, nennt man Bewertungen. Der herkömmliche Absolutbetrag ist auch eine Bewertung auf $\mathbb{Q}$, und, wie man zeigen kann (Satz von Ostrowski), abgesehen von den eben definierten, im wesentlichen die einzige auf $\mathbb{Q}$ (d.h bis auf äquivalente und die triviale).
Bewertungen eines Körpers K sind die Normen des Vektorraumes K über K. Sie induzieren daher Metriken auf K. Damit sollte auch klar sein, was Begriffe wie Konvergenz, Stetigkeit, Cauchyfolge und Vollständigkeit in $\mathbb{Q}$ bezüglich $|.|_p$ bedeuten.

Wir können nun den Satz über die 'Zifferndarstellung' rationaler Zahlen bezüglich $|.|_p$ beweisen:

Beweis von Satz 2.2: Zuerst zeigen wir die *Existenz* der Darstellung: Es sei $r = \frac{a}{b}$ $(a, b \in \mathbb{Z}, b \neq 0)$.
Wir nehmen zunächst $p \not| b$ an. Dann ist $b \ mod\, p$ in $\mathbb{Z}/p\mathbb{Z}$ invertierbar und es existiert daher ein $a_0 \in \{0, 1, ...p - 1\}$ mit $a_0 \equiv \frac{a}{b} \ mod\, p$. Es folgt $p|(ba_0 - a)$ und weiter, wegen $p \not| b$, $|a_0 - \frac{a}{b}|_p \leq \frac{1}{p}$.
Genauso ist $b \ mod\, p^2$ in $\mathbb{Z}/p^2\mathbb{Z}$ invertierbar. Es gibt daher ein $b_1 \in \{0, 1, ...p^2 - 1\}$ mit $b_1 \equiv \frac{a}{b} \ mod\, p^2$. Mit anderen Worten: $|b_1 - \frac{a}{b}|_p \leq \frac{1}{p^2}$. Wegen $a_0 \equiv \frac{a}{b} \equiv b_1 \ mod\, p$ gibt es ein $a_1 \in \{0, 1, ...p - 1\}$ mit $a_0 + a_1 p = b_1$.
Als nächstes betrachtet man $\frac{a}{b} \ mod\, p^3$ und stellt analog fest, daß ein $a_2 \in \{0, 1, ...p - 1\}$ existiert mit $|a_0 + a_1 p + a_2 p^2 - \frac{a}{b}|_p \leq \frac{1}{p^3}$ u.s.w.
Auf diese Weise erhält man eine Folge $(a_n)_{n \geq 0}$ mit

$$\left| \sum_{n=0}^{N-1} a_n p^n - \frac{a}{b} \right|_p \leq \frac{1}{p^N}$$

Es folgt: $\sum_{n=0}^{\infty} a_n p^n = \frac{a}{b}$, wobei die Reihe bezüglich $|.|_p$ gegen $\frac{a}{b}$ konvergiert.
Wenn aber $p|b$, dann sei $\sigma \in \mathbb{N}$ maximal mit $p^\sigma|b$. Setze $b' = \frac{b}{p^\sigma}$. Nach dem eben gezeigtem gibt es eine Folge $(a'_n)_{n\geq 0}$ $(a'_n \in \{0, 1, ...p-1\})$ mit $\sum_{n=0}^{\infty} a'_n p^n = \frac{a}{b'}$. Multipliziert man diese Gleichung mit $p^{-\sigma}$, so erhält man $\sum_{n=0}^{\infty} a'_n p^{n-\sigma} = \frac{a}{b}$ und damit die p-adischen Reihendarstellung einer beliebigen rationaler Zahlen $\frac{a}{b}$.

Eindeutigkeit: Angenommen es gäbe zwei verschiedene Folgen $(x_n)_{n\in\mathbb{Z}}$, $(y_n)_{n\in\mathbb{Z}}$ $(x_n, y_n \in \{0, 1...p-1\}$, $x_n = y_n = 0$ für kleine $n)$ mit $\sum_{n\in\mathbb{Z}} x_n p^n = \sum_{n\in\mathbb{Z}} y_n p^n$. Dann gibt es ein minimales $N_0 \in \mathbb{Z}$ mit $x_{N_0} \neq y_{N_0}$. Es folgt $(x_{N_0} - y_{N_0})p^{N_0} + \sum_{n=N_0+1}^{\infty} (x_n - y_n)p^n = 0$, d.h.

$$((x_{N_0} - y_{N_0})p^{N_0} + \sum_{n=N_0+1}^{N} (x_n - y_n)p^n)_{N\geq N_0}$$

ist eine Nullfolge bezüglich $|.|_p$. Dann müßte aber auch die Folge der Beträge

$$(|(x_{N_0} - y_{N_0})p^{N_0} + \sum_{n=N_0+1}^{N} (x_n - y_n)p^n|_p)_{N\geq N_0}$$

eine Nullfolge sein (diesmal bezüglich $|.|$). Das ist aber nicht der Fall

$$\begin{aligned} (x_{N_0} - y_{N_0})p^{N_0} &+ \sum_{n=N_0+1}^{N} (x_n - y_n)p^n \in p^{N_0}\mathbb{N} \setminus p^{N_0+1}\mathbb{N} \Rightarrow \\ |(x_{N_0} - y_{N_0})p^{N_0} &+ \sum_{n=N_0+1}^{N} (x_n - y_n)p^n|_p = p^{N_0} \quad \forall N \geq N_0. \quad \square \end{aligned}$$

Bemerkung Wie im Beweis dieses Satzes werde ich in Zukunft statt $|\alpha - \beta|_p \leq \frac{1}{p^i}$ $(i \geq 1)$ häufig $\alpha \equiv \beta \mod p^i$ schreiben. Das ist eine Kongruenzrelation auf $\mathbb{Q}$, die die Kongruenzrelation $a \equiv b \mod p^i \iff p^i|a-b$ auf $\mathbb{Z}$ fortsetzt.

Beispiele Mit Hilfe der Formel

$$\frac{-1}{p^d - 1} = \lim_{n\to\infty} \frac{(p^d)^n - 1}{p^d - 1} = \sum_{i=0}^{\infty} (p^d)^i \quad (d \in \mathbb{N})$$

(wobei 'lim' hier bezüglich des p-adischen Absolutbetrages zu verstehen ist; im p-adischen ist nämlich $\|p^d\|_p < 1$, also ist die rechte Seite der Formel eine konvergente geometrische Reihe) erhält man relativ einfach die p-adischen Entwicklungen folgender rationaler Zahlen:

(1) Die 2-adische Entwicklung von -1:

$$-1 = \frac{-1}{2-1} = \lim_{n\to\infty} \frac{2^n - 1}{2-1} = 1 + 1 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + ...$$

(2) Die 2-adische Entwicklung von $\frac{1}{3}$:

$$\frac{1}{3} = 1 + \frac{-2}{2^2-1} = 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 0 \cdot 2^6 + ...$$

(3) Die 3-adische Entwicklung von $\frac{5}{24}$:

$$\frac{5}{24} = \frac{1}{3}\left(1 + \frac{-3}{3^2-1}\right) = 1 \cdot 3^{-1} + 1 + 0 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 1 \cdot 3^4 + 0 \cdot 3^5 + ...$$

(4) Die 7-adische Entwicklung von $\frac{48}{57}$:

$$\begin{aligned} \frac{48}{57} &= 1 + \frac{-9}{57} = 1 + \frac{-54}{342} = 1 + \frac{-(5+7^2)}{7^3-1} = \\ &= 6 + 0 \cdot 7 + 1 \cdot 7^2 + 5 \cdot 7^3 + 0 \cdot 7^4 + 1 \cdot 7^5 + 5 \cdot 7^6 + ... \end{aligned}$$

(Man hätte die Existenz der p-adischen Reihendarstellung in Satz 2.2 auch mit Hilfe der in den Beispielen angedeuteten Methode beweisen können. Sie ist konstruktiver als die im Beweis verwendete, da man durch sie gleich die gesamte Reihenentwicklung erhält. Allerdings erfordert sie ein wenig Übung und ist daher am Anfang nicht so naheliegend, wie die im Beweis verwendete.)

Die Dezimalbruchentwicklung einer rationalen Zahl wird schließlich periodisch und umgekehrt stellt jeder periodische Dezimalbruch eine rationale Zahl dar. Das Analoge gilt für die p-adische Entwicklung einer rationalen Zahl:

Satz 2.3

(1) Es sei $r \in \mathbb{Q}$ und $(a_i)_{i\in\mathbb{Z}}$ eine Folge ($a_i \in \{0, 1, ...p-1\}$, $a_i = 0$ für kleine i) mit $r = \sum\limits_{i\in\mathbb{Z}} a_i p^i$. Dann gibt es ein $M \in \mathbb{N}$, sodaß die Folge $(a_n)_{n\geq M}$ periodisch ist.

(2) Ist umgekehrt $(b_i)_{i\in\mathbb{Z}}$ ($b_i \in \{0, 1, ...p-1\}$, $b_i = 0$ für kleine i) eine Folge und $M \in \mathbb{N}$, sodaß $(b_n)_{n\geq M}$ periodisch ist. Dann gibt es ein $s \in \mathbb{Q}$ mit $\sum\limits_{i\in\mathbb{Z}} b_i p^i = s$.

Beweis:
(1) Es sei $r = \frac{a}{b}$ $(a, b \in \mathbb{Z}, b \neq 0)$. Ich setze

$$A_N = a_N + a_{N+1}p + a_{N+2}p^2 + ... = \frac{r - \sum\limits_{i=-\infty}^{N-1} a_i p^i}{p^N}$$

für $N \in \mathbb{Z}$. Die N-te 'Ziffer' a_N der Reihenentwicklung von r erfüllt $|A_N - a_N|_p \leq \frac{1}{p}$ ($\Leftrightarrow$ $A_N \equiv a_n \ \ mod\, p$) und ist durch diese Ungleichung sogar eindeutig bestimmt (d.h. kennt man A_N, so kann man daraus a_N berechnen). Zusammen mit der Rekursionsformel $A_{n+1} = \frac{A_n - a_n}{p}$ zeigt das, daß a_n für $n \geq N$ nur von A_N abhängt (in dem eben beschriebenen Sinn).

Es folgt: Wenn $A_{N_1} = A_{N_2}$, dann ist $a_{N_1+n} = a_{N_2+n}$ für $n \geq 0$.
Um daraus die Periodizität der Folge ab einer gewissen Stelle M zu schließen, müssen wir nur mehr die Existenz zweier verschiedener natürlicher Zahlen N_1 und N_2 zeigen, mit $A_{N_1} = A_{N_2}$.
Nach dem Dirichletschen Schubfachprinzip genügt es dazu nachzuweisen, daß A_N für $N \in \mathbb{N}$ nur endlich viele Werte annimmt. Für $N \in \mathbb{N}$ ist $\sum\limits_{i=-\infty}^{N-1} a_i p^i$ eine positive rationale Zahl, die kleiner als $\sum\limits_{i=-\infty}^{N-1} (p-1)p^i = p^N$ ist. Die Ungleichungskette

$$-\left|\frac{r}{p}\right| - 1 \leq \frac{-|r| - |p^N|}{p^N} \leq A_N \leq \frac{|r| + |p^N|}{p^N} \leq \left|\frac{r}{p}\right| + 1 \quad (N \in \mathbb{N})$$

ergibt, daß A_N $(N \in \mathbb{N})$ beschränkt bezüglich $|.|$ ist. Da A_N eine rationale Zahl ist, dessen Nenner b teilt, folgt die Behauptung (in einem beschränkten Intervall gibt es nur endlich viele rationale Zahlen deren Nenner b teilt).

(2) Es sei $d > 0$, sodaß $b_{n+d} = b_n$ für $n \geq M$. Da $\sum\limits_{i<M} b_i p^i$ eine endliche Summe ist und daher eine rationale Zahl ist, reicht es zu zeigen, daß $\sum\limits_{i \geq M}^{\infty} b_i p^i$ (in $\mathbb{Q}$) konvergiert.
Da die Folge $\left(\sum\limits_{i=M}^{n} b_i p^i\right)_{n \geq M}$ eine Cauchyfolge bezüglich $|.|_p$ ist (siehe Beginn des nächsten Abschnitts), genügt es sogar nur die Konvergenz einer Teilfolge zu zeigen. Wir machen das für die Teilfolge

$$s_n = \sum_{i=M}^{M+nd-1} b_i p^i.$$

Wegen der d-Periodizität der Folge $(b_n)_{n \geq M}$ gilt die Formel

$$s_n = s_1 + s_1 p^d + s_1 p^{2d} + \ldots + s_1 p^{(n-1)d} = s_1 \frac{1 - p^{dn}}{1 - p^d}$$

für $n = 1, 2, 3, \ldots$. Da $|p^{dn}| \to 0$ bei $n \to \infty$, folgt $\lim\limits_{n \to \infty} s_n = \frac{s_1}{p^d - 1} \in \mathbb{Q}$. $\square$

2.3 Konstruktion von $\mathbb{Q}_p$

Die rationalen Zahlen sind bezüglich des p-adische Absolutbetrages nicht vollständig: Ich haben bereits erwähnt, daß $\left(\sum\limits_{i=-\infty}^{N} a_i p^i\right)_{N \geq 0}$ eine Cauchyfolge ist, wenn $a_i \in \{0, 1, \ldots p-1\}$ und $a_i = 0$ für kleine i:

$$\left|\sum_{i=-\infty}^{M} a_i p^i - \sum_{i=-\infty}^{N} a_i p^i\right|_p = \left|\sum_{i=N+1}^{M} a_i p^i\right|_p \leq \frac{1}{p^{N+1}} \quad (N \leq M)$$

In Satz 2.3 haben wir bewiesen, daß so eine Cauchyfolge genau dann konvergiert, wenn $(a_i)_{i \in \mathbb{Z}}$ schließlich periodisch ist. Es gibt daher Cauchyfolgen dieser Form, die nicht konvergieren.

Man könnte auch anders argumentieren: Jeder solchen Folge $(a_i)_{i\in\mathbb{Z}}$ wird auf diese Weise eine Cauchyfolge zugeordnet. Cauchyfolgen zu zwei verschiedenen Folgen haben positiven Abstand (siehe Beweis der Eindeutigkeit von Satz 2.2). Aus der Abzählbarkeit von $\mathbb{Q}$ und der Überabzählbarkeit der Menge dieser Folgen, ergibt sich die Existenz von (überabzählbarvielen) Cauchyfolgen, die nicht konvergieren.

Für unsere Zwecke wäre aber ein vollständiger, p-adisch-bewerteter Körper, der $\mathbb{Q}$ enthält, nützlich. Es genügt uns der kleinste Körper mit dieser Eigenschaft. Was das heißen soll, erklärt die folgende Definition:

Definition 2.2 *Es sei K ein Körper und $\gamma : K \to \mathbb{R}^+$ eine Bewertung auf K.*
Ein Körper $L \supseteq K$ gemeinsam mit einer Bewertung $\Gamma : L \to \mathbb{R}^+$ heißt Vervollständigung von K bezüglich γ, wenn

(1) $\Gamma|_K = \gamma$,

(2) L vollständig bezüglich Γ ist,

(3) L der Abschluß von K bezüglich Γ ist, d.h. K dicht in L liegt.

Der folgende Satz zeigt, daß man für jeden bewerteten Körper (K,γ) eine solche Vervollständigung abstrakt definieren kann. Sie ist sogar eindeutig bestimmt:

Satz 2.4 *Zu jedem bewerteten Körper existiert eine Vervollständigung im Sinne von Definition 2.2.*
Zwei verschiedene Vervollständigungen desselben bewerteten Körpers sind isometrisch-isomorph.

Beweisskizze Ich werde den Beweis des Satzes nur in groben Zügen skizzieren, weil ich einerseits denke, daß das verwendete Prinzip sehr bekannt ist, und andererseits die vielen kleinen Details, die ich auslasse, relativ leicht zu zeigen sind.

Existenz: Es sei K_c die Menge der Cauchyfolgen über K. K_c ist ein Ring bezüglich 'komponentenweiser' Addition und Multiplikation. Die Menge aller Nullfolgen ($=: N$) über K ist ein maximales Ideal in K_c, wie man leicht zeigt. Es folgt, daß $K_c/N =: L$ ein Körper ist.
Man kann sich K in L durch den Monomorphismus $\varphi : K \to L$, wobei $\varphi(\alpha) = (\alpha)_{i\geq 0} + N$, eingebettet vorstellen.
Die Bewertung $\Gamma : L \mapsto \mathbb{R}^+$ auf L sei definiert durch $\Gamma((a_i)_{i\geq 0} + N) := \lim\limits_{i\to\infty} \gamma(a_i)$. Mit dieser Definition läßt sich zeigen, daß (L,Γ) eine Vervollständigung von (K,γ) ist. (Insbesondere gilt: Ist $(a_n)_{n\geq 0}$ eine Cauchyfolge in K, so konvergiert $(\varphi(a_n))_{n\geq 0} = (a_n + N)_{n\geq 0}$ gegen $(a_n)_{n\geq 0} + N$.)
Im folgenden stellen wir uns K als Teilkörper von L vor.

Eindeutigkeit: Es sei (M, Δ) eine zweite Vervollständigung von (K, γ) und $\psi : K \to M$ der isometrische Monomorphismus, der die Interpretation $K \subseteq M$ zuläßt.
Ich erweitere diesen Monomorphismus folgendermaßen zu eine Abbildung $\Psi : L \to M$: Da K dicht in L ist, gibt es für $\alpha \in L$ eine Folge $(a_i)_{i \geq 0}$ in K, mit $\lim_{i \to \infty} a_i = \alpha$. Wegen ihrer Konvergenz ist diese Folge insbesondere eine Cauchyfolge und weil ψ eine Isometrie ist, gilt dasselbe für die Folge $(\psi(a_i))_{i \geq 0}$. Das, gemeinsam mit der Vollständigkeit von M, ergibt, daß $(\psi(a_i))_{i \geq 0}$ gegen ein Element $\Psi(\alpha) \in M$ konvergiert.
Es ist leicht einzusehen, daß die so definierte Abbildung $\Psi : L \to M$ ein isometrischer ($\Rightarrow$ injektiver) Homomorphismus ist.
Es bleibt zu zeigen, daß Ψ auch surjektiv ist: Da $\overline{\Psi(L)} \supseteq \overline{\psi(K)} = M$ ($\psi(K)$ liegt dicht in M, wegen Eigenschaft (3) in Definition 2.2) genügt es zu zeigen, daß $\Psi(L)$ abgeschlossen ist (Das gelingt, weil L vollständig und Ψ Isometrie ist.). $\square$

Nach Satz 2.4 existiert also eine Vervollständigung von $(\mathbb{Q}, |.|_p)$. Wir bezeichnen sie mit $(\mathbb{Q}_p, \|.\|_p)$ und nennen die Elemente des Körpers $\mathbb{Q}_p$ die p-adischen Zahlen.
Da $\mathbb{Q}$ dicht in $\mathbb{Q}_p$ ist, erfüllt der erweiterte p-adische Absolutbetrag $\|.\|_p$ auch Eigenschaft (3), die ich zu Beginn des Kapitels für $|.|_p$ gezeigt habe. (Eigenschaft (1) und (2) folgen schon aus der Tatsache, daß $\|.\|_p$ eine Bewertung ist.)

Bemerkenswert ist außerdem, daß sich der Bildbereich des p-adischen Absolutbetrages bei der Vervollständigung nicht vergrößert:

$$\{\|z\|_p | z \in \mathbb{Q}_p\} = \overline{\{|z|_p | z \in \mathbb{Q}\}} = \overline{\{p^n | n \in \mathbb{Z}\} \cup \{0\}} = \{p^n | n \in \mathbb{Z}\} \cup \{0\}$$

(Hier sind die Abschlüsse in $\mathbb{R}$ bezüglich des gewöhnlichen Absolutbetrages gemeint.)
Bei der Vervollständigung von $\mathbb{Q}$ zu $\mathbb{R}$ vergrößert sich der Bildbereich des gewöhnlichen Absoltubetrages nämlich schon: Aus $\{|x| | x \in \mathbb{Q}\} = \mathbb{Q}^+$ wird $\{|x| | x \in \mathbb{R}\} = \mathbb{R}^+$.

2.4 Fortsetzung der p-adischen Zifferndarstellung auf $\mathbb{Q}_p$

Wir wissen, daß $\mathbb{R}$ die Vervollständigung von $\mathbb{Q}$ bezüglich des gewöhnlichen Absolutbetrages im Sinne von Definition 2.2 ist.
Unabhängig davon haben wir aber auch eine etwas konkretere Vorstellung von $\mathbb{R}$: Man kann die reellen Zahlen auch als die Menge aller Ausdrücke der Form

$$...a_2 a_1 a_0, a_{-1} a_{-2} a_3 ...$$

($a_i \in \{0, 1...9\}$, $a_i = 0$ für große i) sehen (modulo Ausdrücke der Form $0, 0...0\bar{9}$ und natürlich in Verbindung mit der bekannten Addition und Multiplikation).
Für die p-adischen Zahlen gilt wieder ähnliches: Es besteht eine eineindeutige Beziehung zwischen den Äquivalenzklassen von $\mathbb{Q}_p$ und Cauchyfolgen der Form $\left(\sum_{i=-\infty}^{N} b_i p^i\right)_{N \geq 0}$ ($b_i \in \{0, 1, ...p-1\}$ und $b_i = 0$ für kleine i). Das zeigen wir mit folgendem

Hilfssatz 2.1 *Jede Äquivalenzklasse $\alpha \in \mathbb{Q}_p$ mit $\|\alpha\|_p \leq 1$ enthält eine repräsentative Cauchyfolge $(s_i)_{i\geq 1}$ natürlicher Zahlen mit folgenden zwei Eigenschaften:*

(1) $0 \leq s_i < p^i$ *für* $i = 1, 2, 3, ...$

(2) $s_i \equiv s_{i+1} \mod p^i$ *für* $i = 1, 2, 3, ...$

Beweis: Aus der Konstruktion von $\mathbb{Q}_p$ ergibt sich die Existenz einer Cauchyfolge rationaler Zahlen $(a_i)_{i\geq 1}$, die in der Äquivalenzklasse α liegt. Wir müssen eine Folge $(s_i)_{i\geq 1}$ finden, die Eigenschaft (1) und (2) erfüllt und für die $(a_i - s_i)_{i\geq 1}$ eine Nullfolge bezüglich $|.|_p$ ist.
Da $(a_i)_{i\geq 1}$ eine Cauchyfolge ist, gibt es für $i = 1, 2, 3, ...$ eine natürliche Zahl $N(i)$ mit $|a_j - a_k|_p \leq \frac{1}{p^i}$ für $j, k \geq N(i)$. O.B.d.A können wir annehmen, daß $i \mapsto N(i)$ monoton steigend ist und $N(i) \geq i \quad \forall i$.
Es folgt $|a_i|_p \leq 1$, wenn $i \geq N(1)$, da für $k \geq N(1)$

$$|a_i|_p = |a_k + a_i - a_k|_p \leq \max\{|a_k|_p, |a_i - a_k|_p\} \leq \max\{|a_k|_p, \frac{1}{p}\}$$

und $|a_k|_p \to \|\alpha\|_p \leq 1$ für $i \to \infty$. Gemeinsam mit der Tatsache, daß $i \mapsto N(i)$ monoton steigend ist, ergibt das, daß $a_{N(i)}$ eine rationale Zahl ist, deren Nenner nicht durch p teilbar ist. Es gibt daher natürliche Zahlen $s_i \in \{0, 1, ...p^i - 1\}$ mit

$$|s_i - a_{N(i)}|_p \leq \frac{1}{p^i}$$

für $i = 1, 2, 3...$.
Ich behaupte, daß $(s_i)_{i\geq 1}$ die gewünschte Folge ist.
Aus

$$|s_{i+1} - s_i|_p = |s_{i+1} - a_{N(i+1)} + a_{N(i+1)} - a_{N(i)} + a_{N(i)} - s_i|_p \quad \leq$$
$$\leq \max\{|s_{i+1} - a_{N(i+1)}|_p, |a_{N(i+1)} - a_{N(i)}|_p, |s_i - a_{N(i)}|_p\} \leq \max\{\frac{1}{p^{i+1}}, \frac{1}{p^i}, \frac{1}{p^i}\} \quad = \quad \frac{1}{p^i}$$

folgt $s_{i+1} \equiv s_i \mod p^i$.
Es sei $j \in \mathbb{N}$ und $i \geq N(j)$. Dann gilt

$$|s_i - a_i|_p = |s_i - s_j + s_j - a_{N(j)} + a_{N(j)} - a_i|_p \quad \leq$$
$$\leq \max\{|s_i - s_j|_p, |s_j - a_{N(j)}|_p, |a_{N(j)} - a_i|_p\} \overset{i\geq N(j)\geq j}{\leq} \max\{\frac{1}{p^j}, \frac{1}{p^j}, \frac{1}{p^j}\} \quad = \quad \frac{1}{p^j},$$

also $|s_i - a_i|_p \to 0$ wenn $i \to \infty$ (Es ist $|s_i - s_j|_p \leq \frac{1}{p^j}$ wegen $s_i \equiv s_{i-1} \equiv ... \equiv s_j \mod p^j$) . □

Es seien α und $(s_i)_{i\geq 1}$ wie im Hilfssatz. Laut Konstruktion von $\mathbb{Q}_p$ konvergiert $(s_i)_{i\geq 1}$ gegen α.
Wähle $j \in \mathbb{N}$ beliebig. Wegen Eigenschaft (1) der Folge $(s_i)_{i\geq 1}$ gibt es $a_0, a_1, ...a_{j-1} \in \{0, 1, ...p - 1\}$ mit $s_j = a_0 + a_1 p + ... + a_{j-1}p^{j-1}$. Aus (2) folgt die Existenz einer ganzen Zahl a_j mit $s_{j+1} = a_0 + a_1 p + ... + a_j p^j$. Wiederum wegen (1) ist $a_j \in \{0, 1, ...p - 1\}$.

Auf diese Weise erhält man eine Folge $(a_i)_{i\geq 0}$ $(a_i \in \{0,1,...p-1\})$ mit $s_i = a_0 + a_1 p + ... + a_{i-1}p^{i-1}$ für $i \in \mathbb{N}$. Es folgt $\sum\limits_{i=0}^{\infty} a_i p^i = \alpha$ und wir erhalten die gewünschte Zifferndarstellung für den Fall $\|\alpha\|_p \leq 1$.

Ist $\|\alpha\|_p \geq 1$, so ist $\|p^m \alpha\|_p \leq 1$ für ein $m \in \mathbb{N}$ (da $\|p^m\|_p \to 0$ bei $m \to \infty$). Es gibt dann eine Folge $(a_i)_{i\geq 0}$ $(a_i \in \{0,1,...p-1\})$ sodaß $\sum\limits_{i=0}^{\infty} a_i p^i = \alpha p^m$. Es folgt $\sum\limits_{i=0}^{\infty} a_i p^{i-m} = \alpha$.
Damit erhalten wir die p-adische Reihendarstellung für beliebiges $\alpha \in \mathbb{Q}_p$, d.h. wir haben die Existenz einer Folge $(b_i)_{i\in\mathbb{Z}}$ $(b_i \in \{0,1,...p-1\}$, $b_i = 0$ für kleine $i)$ gezeigt, mit $\sum\limits_{i\in\mathbb{Z}} b_i p^i = \alpha$.
Daß diese Folge sogar eindeutig bestimmt ist, sieht man im Beweis von Satz 2.2 (Eindeutigkeit).
Aus dieser 'Zifferndarstellung' kann man auch den p-adischen Absolutbetrag von α berechnen: Es sei $n_0 \in \mathbb{Z}$ minimal, sodaß $b_{n_0} \neq 0$. Dann ist $\|\alpha\|_p = \frac{1}{p^{n_0}}$. Existiert kein solches n_0, dann ist $\alpha = 0$ und daher $\|\alpha\|_p = 0$.

Umgekehrt ist $\left(\sum\limits_{i=-\infty}^{n} b_i p^i\right)_{n\geq 0}$ für jede solche Folge $(b_i)_{i\in\mathbb{Z}}$ eine Cauchyfolge und wegen der Vollständigkeit von $\mathbb{Q}_p$ gibt es daher ein $\beta \in \mathbb{Q}_p$ mit $\sum\limits_{i\in\mathbb{Z}} b_i p^i = \beta$. Damit ist die ein-eindeutige Korrespondenz zwischen den p-adischen Zahlen β und den Folgen $(b_i)_{i\in\mathbb{Z}}$ vollständig gezeigt.

2.5 Das Auflösen algebraischer Gleichungen in $\mathbb{Q}_p$

In diesem Abschnitt werden wir einiges über die algebraischen Eigenschaften des Körpers $\mathbb{Q}_p$ erfahren.
Wir werden sehen, daß man eine algebraische Gleichung

$$a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 = 0 \quad (a_i \in \mathbb{Q}_p)$$

näherungsweise lösen kann, und zwar mit einem (sehr einfachem) Verfahren, daß der Intervallschachtelung in $\mathbb{R}$ oder auch dem Newtonverfahren ähnelt.
Mit Hilfe dieser Überlegungen werden wir zeigen können, daß $\mathbb{Q}$ nicht algebraisch abgeschlossen ist und daß die Körper $\mathbb{Q}_{p_1}$ und $\mathbb{Q}_{p_2}$ nicht (algebraisch) isomorph sind, wenn p_1 und p_2 zwei verschiedene Primzahlen sind. Das sind aber nur zwei kleine, für den weiteren Verlauf unwichtige Anwendungen dieses Verfahrens (bzw. von Satz 2.6, der aus dem Verfahren resultieren wird), die uns zeigen sollen, wie nützlich es trotz seiner Einfachheit ist. Satz 2.6 hingegen wird in Kapitel 3, bei der Verlagerung der Rekurrenzen nach $\mathbb{Q}_p$, entscheidend in den Beweis des Satzes von Skolem-Mahler-Lech eingehen.

Eigentlich werden wir algebraische Gleichungen nur in und über einer Teilmenge von $\mathbb{Q}_p$ auflösen, nämlich in $\mathbb{Z}_p := \{z \in \mathbb{Q}_p \mid \|z\|_p \leq 1\}$ der abgeschlossenen Einheitskugel. Das sind genau jene p-adischen Zahlen, in deren Reihenentwicklung keine negative Potenz von p auftritt und man nennt sie daher ganze p-adische Zahlen. Sie bilden, etwas überraschend wenn man an die Einheitskugel in $\mathbb{C}$ denkt, einen Integritätsbereich:

Es seien $a, b \in \mathbb{Z}_p$, dann ist $\|a-b\|_p \leq \max\{\|a\|_p, \|b\|_p\} \leq 1$ und daher liegt die Differenz $a-b$ in $\mathbb{Z}_p$. Genauso ist das Produkt $a \cdot b$ eine ganze p-adische Zahl, da wegen der Multiplikativität des p-adischen Absolutbetrages $\|a \cdot b\|_p = \|a\|_p \cdot \|b\|_p \leq 1$ ist.
Der Name und das Symbol legen schon nahe, daß $\mathbb{Z}_p$ für $\mathbb{Q}_p$ das ist, was $\mathbb{Z}$ für $\mathbb{Q}$ ist. Neben der Analogie bei der Zifferndarstellung (aus der übrigens auch folgt, daß $\mathbb{Z}_p$ der Abschluß von $\mathbb{Z}$ in $\mathbb{Q}_p$ ist) werden wir in diesem Abschnitt sehen, daß man auf $\mathbb{Z}_p$ auch eine Projektion '*mod* p^n' mit Bildbereich $\mathbb{Z}/p^n\mathbb{Z}$ definieren kann. Außerdem ist $\mathbb{Q}_p$ der Quotientenkörper von $\mathbb{Z}_p$ – genau wie $\mathbb{Q}$ der von $\mathbb{Z}$ ist: Es sei $r \in \mathbb{Q}_p$. Dann gibt es ein $m \in \mathbb{N}$ mit $p^m r \in \mathbb{Z}_p$. Wegen $p^m \in \mathbb{Z}_p$ folgt die Behauptung.
Die ganzen p-adischen Zahlen werden im folgenden eine wichtige Rolle spielen.

Der nächste Satz zeigt uns, daß es genügt Polynome über $\mathbb{Z}_p$ und deren Nullstellen in $\mathbb{Z}_p$ zu betrachten:

Satz 2.5 *Es sei $p(X)$ ein Polynom über $\mathbb{Q}_p$. Dann gibt es eine natürliche Zahl k und ein Polynom $q(X)$ mit Koeffizienten in $\mathbb{Z}_p$, sodaß die Lösungen von $q(X) = 0$ in $\mathbb{Z}_p$ multipliziert mit dem Faktor p^{-k} genau die Lösungen von $p(X) = 0$ in $\mathbb{Q}_p$ sind.*

Beweis: Der Beweis des Satzes ist konstruktiv, d.h. es wird gezeigt wie sich k und $q(X)$ tatsächlich berechnen lassen.
Es sei $p(X) = p_0 + p_1X + ... + p_nX^n$ und $p_n \neq 0$. Zunächst zeigen wir, daß die Lösungen von $p(X) = 0$ beschränkt sind: Es sei $r \in \mathbb{Q}_p \setminus \mathbb{Z}_p$ eine Lösung. Dann gilt

$$\|p_n r^n\|_p = \| - p_0 - p_1 r - ... - p_{n-1} r^{n-1}\|_p \leq$$

$$\leq \max_{i\in\{0,1,...n-1\}} \|p_i r^i\|_p \overset{\|r\|>1}{\leq} \left(\max_{i\in\{0,1,...n-1\}} \|p_i\|_p \right) \|r\|_p^{n-1}$$

und daher

$$\|r\|_p \leq \frac{\max_{i\in\{0,1,...n-1\}} \|p_i\|_p}{\|p_n\|_p}.$$

Aus diesem Grund gibt es eine (berechenbare) natürliche Zahl k, sodaß $\|x\|_p \leq p^k$ für alle $x \in \mathbb{Q}_p$ mit $p(x) = 0$. (Die reine Existenz einer solchen Zahl k würde einfacher aus der Tatsache folgen, daß jedes Polynom über einem Körper nur endlich viele Nullstellen hat.)
Nun konstruieren wir das Polynom $q(X)$: Es sei zunächst $\overline{q}(X) = p(p^{-k}X)$. Dann sind die Nullstellen x von $p(X)$ mit $\|x\|_p \leq p^k$ (das sind laut Konstruktion von k alle Nullstellen) genau die Nullstellen von $\overline{q}(X)$ in $\mathbb{Z}_p$ multipliziert mit p^{-k}.
Schließlich sei $m \in \mathbb{N}$ so gewählt, daß die Koeffizienten von $p^m \cdot \overline{q}(X)$ in $\mathbb{Z}_p$ liegen. Das Polynom $q(X) := p^m \cdot \overline{q}(X)$ leistet das Gewünschte. □

Wir nehmen nun an, daß $a(X) = a_0 + a_1X + ... + a_mX^m$ ein Polynom mit Koeffizienten in $\mathbb{Z}_p$ ist. Wie gesagt wollen wir ein Verfahren angeben, mit dessen Hilfe man die Nullstellen von $a(X)$ in $\mathbb{Z}_p$ näherungsweise berechnen kann.
Der Grund, wieso wir uns auf $\mathbb{Z}_p$ beschränken, ist, daß wir für $n = 1, 2, 3, ...$ die Projektionen

$$\alpha_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}, \quad \alpha_n(z_0 + z_1p + z_2p^2 + ...) = z_0 + z_1p + ... + z_{n-1}p^{n-1} + p^n\mathbb{Z}$$

benötigen. Etwas salopper ausgedrückt: Wir wollen die Zahlen $mod\, p^n$ betrachten können. Der Homomorphismus α_n induziert einen weiteren Homomorphismus

$$\beta_n : \mathbb{Z}_p[X] \to (\mathbb{Z}/p^n\mathbb{Z})[X],$$

den wir ebenfalls verwenden werden. Um nicht unnötig Verwirrung zu stiften, werde ich aber statt $\beta_n(a)(\alpha_n(z))$, wobei $z \in \mathbb{Z}_p$, lieber $a(z) \;\; mod\, p^n$ schreiben bzw. $a(X) \;\; mod\, p^n$ für $\beta_n(a)(X)$, wenn X eine Unbestimmte ist.

Beschreibung des Verfahrens:

Zunächst beachten wir: Ist $deg(a) = n$, dann gibt es Polynome $a_1(X), a_2(X), ...a_n(X)$ über $\mathbb{Z}_p$ mit

$$a(X+Y) = a(X) + Y \cdot a_1(X) + Y^2 \cdot a_2(X) + ... + Y^n \cdot a_n(X).$$

Man sieht relativ leicht, daß $a_i(X) = \frac{a^{(i)}(X)}{i!}$ und daher insbesondere $a_1(X) = a'(X)$. (Taylorsche Lehrsatz)

Zu Beginn berechnet man alle $z_0 \in \{0, 1, ...p-1\}$ mit $a(z_0) \equiv 0 \;\; mod\, p$. Jede Lösung von $a(z) = 0$ in $\mathbb{Z}_p$ beginnt dann ihre Reihendarstellung mit einem dieser z_0, da aus $a(z_0 + z_1 p + z_2 p^2 + ...) = 0$ unter Anwendung des Homomorphismus α_1 die Kongruenz $a(z_0) \equiv 0 \;\; mod\, p$ folgt. Gibt es also kein solches z_0, so weiß man bereits, daß die Gleichung in $\mathbb{Z}_p$ überhaupt keine Lösung hat.

Existieren hingegen ein oder auch mehrere solche z_0 , so fragt man sich im nächsten Schritt, ob diese Lösungen $mod\, p^2$ 'fortsetzbar' sind, d.h. ob es $z_1 \in \{0, 1, ...p-1\}$ gibt, mit $a(z_0 + z_1 p) \equiv 0 \;\; mod\, p^2$. Es gilt

$$\begin{aligned} a(z_0 + z_1 p) &= a(z_0) + z_1 p \cdot a_1(z_0) + (z_1 p)^2 \cdot a_2(z_0) + ... \equiv \\ &\equiv a(z_0) + z_1 p \cdot a'(z_0) \;\; mod\, p^2. \end{aligned}$$

Diese Rechnung zeigt, daß z_1 Lösung der linearen Kongruenz

$$\frac{a(z_0)}{p} + z_1 \cdot a'(z_0) \equiv 0 \;\; mod\, p$$

ist ($a(z_0) \equiv 0 \;\; mod\, p \Rightarrow \frac{a(z_0)}{p} \in \mathbb{Z}_p$).
Ist nun $a'(z_0) \not\equiv 0 \;\; mod\, p$, so existiert genau ein solches z_1.
Ist dagegen $a'(z_0) \equiv 0 \;\; mod\, p$, so betrachtet man die beiden Unterfälle $\frac{a(z_0)}{p} \equiv 0 \;\; mod\, p$ und $\frac{a(z_0)}{p} \not\equiv 0 \;\; mod\, p$. Im ersten Fall ist jedes $z_1 \in \{0, 1, ...p-1\}$ eine Fortsetzung, im zweiten Fall keines und das Verfahren bricht ab.

Es sei also z_1 eine solche 'Fortsetzung $mod\, p^2$'. Im nächsten Schritt wollen wir die Näherungslösung $z_0 + z_1 p \quad mod\, p^3$ fortsetzen, d.h. wir wollen alle $z_2 \in \{0, 1, ...p-1\}$ bestimmen mit $a(z_0 + z_1 p + z_2 p^2) \equiv 0 \;\; mod\, p^3$.

Das funktioniert ganz analog zur Fortsetzung $mod\, p^2$:

$$\begin{aligned}
a(z_0 + z_1 p + z_2 p^2) &= \\
&= a(z_0 + z_1 p) + z_2 p^2 \cdot a_1(z_0 + z_1 p) + (z_2 p^2)^2 \cdot a_2(z_0 + z_1 p) + \ldots \equiv \\
&\equiv a(z_0 + z_1 p) + z_2 p^2 a'(z_0 + z_1 p) \;\; mod\, p^3 \equiv \\
&\equiv a(z_0 + z_1 p) + z_2 p^2 a'(z_0) \;\; mod\, p^3
\end{aligned}$$

Es folgt, daß z_2 wieder Lösung einer linearen Gleichung in $\mathbb{Z}/p\mathbb{Z}$ ist:

$$\frac{a(z_0 + z_1 p)}{p^2} + z_2 \cdot a'(z_0) \equiv 0 \;\; mod\, p.$$

Ist $a'(z_0) \not\equiv 0 \;\; mod\, p$, so gibt es genau ein solches z_2; ist dagegen $a'(z_0) \equiv 0 \;\; mod\, p$, so ist im Falle $\frac{a(z_0+z_1p)}{p^2} \equiv 0 \;\; mod\, p$ (d.h. wenn $z_0 + z_1 p$ schon Lösung $mod\, p^3$ ist) jedes $z_2 \in \{0, 1, \ldots p-1\}$ Lösung – anderenfalls keines.

Als nächstes untersucht man die Fortsetzbarkeit der erhaltenen Näherungslösungen $mod\, p^4$ u.s.w. ...

Auf dieses Weise erhält man Folgen $(z_n)_{n\geq 0}$ mit $z_n \in \{0, 1, \ldots p-1\}$, sodaß

$$a\left(\sum_{n=0}^{N-1} z_n p^n\right) \equiv 0 \;\; mod\, p^N \quad N = 1, 2, 3, \ldots$$

Es folgt

$$a\left(\sum_{n=0}^{\infty} z_n p^n\right) \equiv 0 \;\; mod\, p^N \quad N = 1, 2, 3, \ldots$$

und daher

$$\left\| a\left(\sum_{n=0}^{\infty} z_n p^n\right) \right\|_p \leq \frac{1}{p^N} \quad N = 1, 2, 3 \ldots \Rightarrow \left\| a\left(\sum_{n=0}^{\infty} z_n p^n\right) \right\|_p = 0$$

d.h. $\sum\limits_{n=0}^{\infty} z_n p^n$ ist Nullstelle des Polynoms $a(X)$.

Es ist klar, daß man durch dieses Verfahren jede Folge $(z_n)_{n\geq 0}$ mit dieser Eigenschaft erhält, und da jede ganze p-adische Zahl eine Reihendarstellung der Form $\sum\limits_{n=0}^{\infty} z_n p^n$ hat, gewinnt man so, wenn man nur unendlich lange rechnet, jede ganze p-adische Nullstelle von $a(X)$. $\square$

Mit Hilfe dieses Verfahrens kann man also Schritt für Schritt die p-adische 'Zifferndarstellung' der Nullstellen von $a(X)$ in $\mathbb{Z}_p$ berechen, genauso wie man das in $\mathbb{R}$ bei der Intervallschachtelung macht.

Die Schwäche des p-adische Verfahrens im Vergleich zur Intervallschachtelung ist, daß es im allgemeinen nicht entscheidet, ob überhaupt eine Nullstelle existiert, d.h. es kann passieren, daß man durch $(n-1)$-maliges Fortsetzen zu einer 'Lösung $mod\, p^n$' gelangt, die aber $mod\, p^{n+1}$ keine Fortsetzung mehr hat (in $\mathbb{R}$ ermöglicht der Zwischenwertsatz ein einfaches Kriterium für die Existenz von Nullstellen. Er ist die Grundlage für die Intervallschachtelung.).

Ist aber $a'(z_0) \not\equiv 0 \;\; mod\, p$ (und $a(z_0) \equiv 0 \;\; mod\, p$), so kann man mit Hilfe des beschriebenen Verfahrens schon eine Aussage über die Existenz einer Lösung von $a(z) = 0$ mit $z \equiv z_0 \;\; mod\, p$ treffen. Es gibt dann nämlich immer genau eine solche Lösung.

Dieses Ergebnis fassen wir im folgenden Satz zusammen:

Satz 2.6 (Henselsches Lemma) *(1) Es sei $a(X) \in \mathbb{Z}_p[X]$, $z_0 \in \mathbb{Z}_p$ mit $a(z_0) \equiv 0 \mod p$ und $a'(z_0) \not\equiv 0 \mod p$. Dann existiert genau ein $z \in \mathbb{Z}_p$ mit $a(z) = 0$ und $z \equiv z_0 \mod p$.*

(2) Wenn $a(X) \mod p$ nur einfache Nullstellen besitzt, dann gibt es zu jedem $z_0 \in \mathbb{Z}_p$ mit $a(z_0) \equiv 0 \mod p$ genau ein $z \in \mathbb{Z}_p$ mit $a(z) = 0$ und $z \equiv z_0 \mod p$.
Insbesondere hat dann $a(X)$ in $\mathbb{Z}_p$ genauso viele Nullstellen wie $a(X) \mod p$ im Körper $\mathbb{Z}/p\mathbb{Z}$.

Beweis: ad 1) Die 'Ziffern' der p-adische Reihendarstellung $\sum\limits_{n=0}^{\infty} z_n p^n$ von z lassen sich rekursiv mit Hilfe folgender linearen Kongruenzen über $\mathbb{Z}/p\mathbb{Z}$ berechnen:

$$\frac{a(z_0 + z_1 p + ... + z_{n-1}p^{n-1})}{p^n} + z_n a'(z_0) \equiv 0 \mod p \quad n = 1, 2, 3, ...$$

Diesen Algorithmus kann man auch als Newton-Algorithmus sehen: Beim Newton-Vefahren in $\mathbb{R}$ geht man von einer Näherungslösung x_0 einer (nicht notwendigerweise algebraischen) Gleichung $f(X) = 0$ aus und berechnet dann mit Hilfe der Rekursion

$$x_n = x_{n-1} - \frac{f(x_{n-1})}{f'(x_{n-1})}$$

eine Folge von Näherungslösungen $(z_n)_{n\geq 0}$, die in vielen Fällen gegen eine tatsächliche Lösung konvergiert.
Bei uns ist es ähnlich: Wir gehen von einer Nährungslösung z_0 der Gleichung aus, und wenn wir $x_n = \sum\limits_{i=0}^{n} z_i p^i$ setzen, so gilt

$$x_n \equiv x_{n-1} - \frac{a(x_{n-1})}{a'(x_{n-1})} \mod p^{n+1}$$

wie sich leicht nachrechnen läßt.

ad 2) Die Tatsache, daß $a(X) \mod p$ nur einfache Nullstellen hat, ist gleichbedeutend damit, daß kein $z_0 \in \mathbb{Z}_p$ existiert mit $a(z_0) \equiv 0 \mod p$ und $a'(z_0) \equiv 0 \mod p$. □

Beispiel: Wir wollen mit Hilfe unseres Algorithmus die Gleichung

$$a(z) = z^3 + 3z^2 + 4z + 8 = 0$$

in $\mathbb{Z}_2$ lösen.
Dazu berechnen wir zunächst die Ableitung von $a(X)$: $a'(X) = 3X^2 + 6X + 4$.
Mod 2 hat die Gleichung die beiden Lösungen 0 und 1.

Fortsetzungen von 1: Da $a'(1) = 13 \not\equiv 0 \mod 2$ hat die Gleichung nach Satz 2.6 genau eine Lösung $z = z_0 + z_1 2 + z_2 4 + ...$ in $\mathbb{Z}_p$ mit $z \equiv 1 \mod 2$ ($\Leftrightarrow z_0 = 1$). Der Algorithmus sagt uns, daß z_1 die Lösung der Kongruenz

$$\frac{a(z_0)}{2} + z_1 \cdot a'(z_0) = \frac{16}{2} + z_1 13 \equiv 0 \mod 2$$

ist. Es folgt: $z_1 = 0$. Analog berechnen wir z_2, z_3, z_4, z_5, z_6:

$$\begin{array}{lcr}
z_2: & \frac{a(z_0+z_1 2)}{4} + z_2 \cdot a'(z_0) = 4 + z_2 13 \equiv 0 \mod 2 & \Rightarrow z_2 = 0 \\
z_3: & \frac{a(z_0+z_1 2+z_2 4)}{8} + z_3 \cdot a'(z_0) = 2 + z_3 13 \equiv 0 \mod 2 & \Rightarrow z_3 = 0 \\
z_4: & \frac{a(z_0+z_1 2+z_2 4+z_3 8)}{16} + z_4 \cdot a'(z_0) = 1 + z_4 13 \equiv 0 \mod 2 & \Rightarrow z_4 = 1 \\
z_5: & \frac{a(z_0+z_1 2+z_2 4+z_3 8+z_4 16)}{32} + z_5 \cdot a'(z_0) = 183 + z_5 13 \equiv 0 \mod 2 & \Rightarrow z_5 = 1 \\
z_6: & \frac{a(z_0+z_1 2+z_2 4+z_3 8+z_4 16+z_5 32)}{64} + z_6 \cdot a'(z_0) = 1954 + z_6 13 \equiv 0 \mod 2 & \Rightarrow z_6 = 0
\end{array}$$

u.s.w.

Fortsetzungen von 0: Wegen $a'(0) = 4 \equiv 0 \mod 2$ kommt der zweite Fall unseres Algorithmus zur Anwendung.

Fortsetzungen $\mod 4$:
Die lineare Kongruenz $\frac{a(0)}{2} + a'(0)z_1 = 4 + 4 \cdot z_1 \equiv 0 \mod 2$ hat die Lösungen $z_1 = 0, 1$. Die Lösungen der Kongruenz $a(z) \equiv 0 \mod 4$, mit $z \equiv 0 \mod 2$, sind daher $0 = 0 + 0 \cdot 2$ und $2 = 0 + 1 \cdot 2$.

Fortsetzungen $\mod 8$:
0: $\frac{a(0)}{4} + a'(0)z_2 = \frac{8}{4} + 4 \cdot z_2 \equiv 0 \mod 2 \Rightarrow z_2 = 0, 1$.
2: $\frac{a(2)}{4} + a'(0)z_2 = \frac{36}{4} + 4 \cdot z_2 \equiv 0 \mod 2$ ist unlösbar.
Die Kongruenz $a(z) \equiv 0 \mod 8$ hat somit die Lösungen $0 = 0 + 0 \cdot 4$ und $4 = 0 + 1 \cdot 4$.

Fortsetzungen $\mod 16$:
0: Die lineare Kongruenz $\frac{a(0)}{8} + a'(0)z_3 = 1 + 4 \cdot z_3 \equiv 0 \mod 2$ ist unlösbar, genauso wie
4: $\frac{a(4)}{8} + a'(0)z_3 = 17 + 4 \cdot z_3 \equiv 0 \mod 2$.
$\Rightarrow$ Es gibt daher keine Fortsetzung $\mod 16$ und daher keine Nullstelle z von $a(X)$ in $\mathbb{Z}_p$ mit $z \equiv 0 \mod 2$. □

Es sei auch noch einmal explizit hervorgehoben, daß die Homomorphismen α_n, β_n, $n = 1, 2, 3, ...$, eine einfache notwendige Bedingung für die Lösbarkeit algebraischer Gleichungen über $\mathbb{Z}_p$ liefern:
Ist eine Gleichung $a(X) = 0$ über $\mathbb{Z}_p$ in $\mathbb{Z}_p$ lösbar, so ist für jedes $n \in \mathbb{N}$ die Gleichung $a(X) \equiv 0 \mod p^n$ in $\mathbb{Z}$ lösbar.

Diese Überlegung und Satz 2.6 hilft uns bei den folgenden zwei Sätzen:

Eine besonders schöne Eigenschaft, die ein Körper in Bezug auf algebraische Gleichungen haben kann, ist die algebraische Abgeschlossenheit, d.h. daß jedes nicht-konstante Polynom eine Nullstelle in diesem Körper besitzt.
Der Körper der p-adischen Zahlen besitzt diese Eigenschaft nicht:

Satz 2.7 *Das Polynom $f(X) = X^p - X + 1$ hat in $\mathbb{Q}_p$ keine Nullstelle.*

Beweis: Das Polynom $f(X)$ hat in $\mathbb{Z}_p$ keine Nullstelle, da $f(X) \equiv 0 \mod p$ in $\mathbb{Z}$ nicht lösbar ist. (Das folgt aus dem kleinen Satz von Fermat: $z^p - z \equiv 0 \mod p \quad \forall z \in \mathbb{Z} \Rightarrow f(z) \equiv$

$1 \ mod\, p \quad \forall z \in \mathbb{Z}$.)
Angenommen $f(X)$ hätte eine Nullstelle r mit $\|r\|_p > 1$. Dann gilt:

$$\|r^p\|_p = \|r^p - r + r\|_p \leq \max\{\|r^p - r\|_p, \|r\|_p\} \overset{\|r\|_p \leq \|r^p\|_p}{=} \|r^p - r\|_p = 1$$

Das ist ein Widerspruch, da $\|r^p\|_p = \|r\|_p^p > 1$. □

Eine andere, bisher noch ungeklärte Frage bezüglich der algebraischen Struktur der Körper $\mathbb{Q}_p$ ist die (algebraische) Beziehung der $\mathbb{Q}_p$ untereinander.
Etwas konkreter erhebt sich z.B. die Frage, ob es zwei verschiedene Primzahlen p_1, p_2 gibt, sodaß $\mathbb{Q}_{p_1}$ und $\mathbb{Q}_{p_2}$ algebraisch isomorph sind. Man wird wahrscheinlich vermuten, daß das nicht so ist, denn die zwei Normen $|.|_{p_1}$ und $|.|_{p_2}$, die $\mathbb{Q}_{p_1}$ und $\mathbb{Q}_{p_2}$ sozusagen erzeugen, sind zu verschieden, ja in einem gewissen Sinn könnte man sogar sagen, daß sie voneinander 'unabhängig' sind. Der folgende Satz bestätigt diese Vermutung:

Satz 2.8 *Es seien p_1, p_2 zwei verschiedene Primzahlen. Dann ist $\mathbb{Q}_{p_1} \not\cong \mathbb{Q}_{p_2}$.*

Beweis: Es genügt die Existenz eines Polynoms $f(X) \in \mathbb{Q}[X] \subseteq (\mathbb{Q}_{p_1} \cap \mathbb{Q}_{p_2})[X]$ zu zeigen, welches in $\mathbb{Q}_{p_1}$ keine Nullstelle hat – in $\mathbb{Q}_{p_2}$ aber schon.
Dazu modifizieren wir das Polynom $X^{p_1} - X + 1$, von dem wir aus Satz 2.7 bereits wissen, daß es in $\mathbb{Q}_{p_1}$ keine Nullstelle hat: Wir definieren

$$f_z(X) = X^{p_1} - X(1 + p_1 z) + 1$$

für $z \in \mathbb{Z}$. Diese Polynome haben in $\mathbb{Z}_{p_1}$ keine Nullstelle, da $f_z(X) \equiv X^{p_1} - X + 1 \equiv 0 \ mod\, p_1$ keine Lösung in $\mathbb{Z}$ hat.
Genauso wie im Beweis von Satz 2.7 zeigt man, daß sie auch keine Nullstelle in $\mathbb{Q}_{p_1} \setminus \mathbb{Z}_{p_1}$ haben: Angenommen es gäbe ein $r \in \mathbb{Q}_{p_1}$ mit $\|r\|_p > 1$ und $f_z(r) = 0$ für ein $z \in \mathbb{Z}$. Dann folgt:

$$\|r^{p_1}\|_{p_1} = \|r^{p_1} - r(1+p_1 z) + r(1+p_1 z)\|_{p_1} \leq \max\{\|r^{p_1} - r(1+p_1 z)\|_{p_1}, \|r(1+p_1 z)\|_{p_1}\} =$$

$$\overset{\|r(1+p_1 z)\|_{p_1} = \|r\|_{p_1} \cdot 1 < \|r^{p_1}\|_{p_1}}{=} \|r^{p_1} - r(1+p_1 z)\|_{p_1} = 1$$

Das ist ein Widerspruch zu $\|r^{p_1}\|_{p_1} > 1$.
Nun zeigen wir, daß wir $z_0 \in \mathbb{Z}$ so wählen können, daß $f_{z_0}(X) = 0$ in $\mathbb{Q}_{p_2}$ eine Lösung hat:
Nach einer möglichen Vertauschung der Rollen der beiden Primzahlen p_1, p_2 können wir o.B.d.A. annehmen, daß $p_1 - 2 \not\equiv 0 \ mod\, p_2$ (wenn $2 \notin \{p_1, p_2\}$ wählen wir $p_2 > p_1$, sonst $p_2 < p_1$). Es sei $z_0 \in \mathbb{Z}$, sodaß $p_1 z_0 \equiv 1 \ mod\, p_2$. Dann gilt

$$f_{z_0}(1) = 1^{p_1} - (1 + p_1 z_0)1 + 1 \equiv 0 \ mod\, p_2$$

und

$$f'_{z_0}(1) \equiv p_1 1^{p_1 - 1} - (1 + p_1 z_0) = p_1 - 2 \not\equiv 0 \ mod\, p_2.$$

Aus Satz 2.6 folgt die Existenz einer Nullstelle von $f_{z_0}(X)$ in $\mathbb{Z}_{p_2}$, die $\equiv 1 \ mod\, p_2$ ist. □

Wie zu Beginn schon erwähnt, ist das Henselsche Lemma das wichtigste Ergebnis dieses Abschnittes über algebraische Gleichungen in Bezug auf unsere weiteren Überlegungen zum Satz von Skolem-Mahler-Lech.
Auch wenn wir die anderen Überlegungen nicht mehr direkt benötigen werden (d.h. ich werde sie nicht zitieren), so finde ich gerade das Verfahren zur Lösung algebraischer Gleichungen in $\mathbb{Q}_p$ besonders interessant, um einen weiteren Aspekt der p-adischen Zahlen zu erkennen:
In der Zahlentheorie ermöglichen die Homomorphismen $\alpha_n|_{\mathbb{Z}}$ und $\beta_n|_{\mathbb{Z}}$ eine einfache notwendige Bedingung für die Lösbarkeit algebraischer diophantischer Gleichungen in einer Variablen, d.h. für die Existenz von ganzen Nullstellen eines Polynoms $a(X)$ über $\mathbb{Z}$: Ist nämlich $a(X) = 0$ in $\mathbb{Z}$ lösbar, so ist die für jedes $n \in \mathbb{N}$ die Kongruenz $a(X) \equiv 0 \;\; mod\, p^n$ lösbar. Um solche diophantische Gleichungen zu lösen, kann man daher dasselbe Verfahren wie in $\mathbb{Z}_p$ anwenden (das macht man tatsächlich auch; ich kann mir gut vorstellen, daß das eine der ersten Anwendungen der 'Modulorechnung' war). Das Problem ist, daß die Lösbarkeit dieser Kongruenzen nicht hinreichend für die Existenz von Nullstellen ist. Das heißt, es kann passieren, daß eine Lösungsfolge $(s_n)_{n\geq 0}$ existiert, mit $a(s_n) \equiv 0 \;\; mod\, p^n$ für $n \in \mathbb{N}$, wobei $a(X) = 0$ jedoch unlösbar in $\mathbb{Z}$ ist.

Beispiel Wir wissen bereits, daß die Gleichung

$$a(X) = z^3 + 3z^2 + 4z + 8 = 0$$

in $\mathbb{Z}_p$ lösbar ist und daher $a(X) \equiv 0 \;\; mod\, p^n$ für jedes $n \in \mathbb{N}$ lösbar ist. Diese Gleichung ist aber nicht in $\mathbb{Z}$ lösbar, da unter den Teilern von 8 (= konstanter Koeffizient des Polynoms $a(X)$) keine Lösung ist.

Wie bereits erwähnt, liefern die Homomorphismen α_n und β_n in analoger Weise in $\mathbb{Z}_p$ eine notwendige Bedingung für die Existenz von Nullstellen. Nun wäre es natürlich interessant zu wissen, ob die Bedingung dort, in einer viel größeren Menge als $\mathbb{Z}$, sogar hinreichend ist.
Zunächst ist einmal klar, daß (im Gegensatz zu $\mathbb{Z}$, siehe Beispiel) aus der Existenz einer Lösungsfolge $(s_n)_{n\geq 0}$, mit $a(s_n) \equiv 0 \;\; mod\, p^n$ für $n \in \mathbb{N}$, und der zusätzlichen Bedingung $s_n \equiv s_{n+1} \;\; mod\, p^n$ für $n \in \mathbb{N}$ die Existenz einer Nullstelle von $a(X)$ in $\mathbb{Z}_p$ folgt: Die Folge $(s_n)_{n\geq 0}$ ist dann nämlich eine Cauchyfolge und wegen der Vollständigkeit von $\mathbb{Q}_p$ und der Abgeschlossenheit von $\mathbb{Z}_p$ konvergent gegen ein Element in $\mathbb{Z}_p$, welches dann auch Nullstelle von $a(X)$ ist. Diese Überlegung bildet die Basis für das beschriebene Verfahren zur Bestimmung der Nullstellen.
In $\mathbb{Z}_p$ ist die Bedingung mit den Homomorphismen α_n und β_n aber auch ohne zusätzliche Voraussetzung hinreichend:
Es sei $(r_n)_{n\geq 0}$ eine Folge ganzer p-adischer Zahlen, mit

$$a(r_n) \equiv 0 \;\; mod\, p^n \quad n = 1, 2, 3, ...$$

Anders geschrieben bedeutet das

$$\|a(r_n)\|_p \leq \frac{1}{p^n} \quad n = 1, 2, 3, ... \quad .$$

Da $\mathbb{Z}_p$ eine beschränkte Teilmenge von $\mathbb{Q}_p$ ist, folgt aus dem Satz von Bolzano-Weierstraß (ich werde ihn für $\mathbb{Q}_p$ in Kapitel 4 zeigen), daß $(r_n)_{n\geq 0}$ einen Häufungspunkt in $\mathbb{Z}_p$ hat. Es ist

leicht zu zeigen (mit Hilfe der Stetigkeit des Polynoms), daß dieser Häufungspunkt Nullstelle von $a(X)$ ist.
Man kann daher $\mathbb{Z}_p$ sozusagen als 'natürliche Erweiterung' von $\mathbb{Z}$ bezüglich des beschriebenen Verfahrens zur Lösung algebraischer, diophantischer Gleichungen sehen. Damit meine ich, daß auf die Frage 'Wie kann ich $\mathbb{Z}$ erweitern, sodaß das Kriterium mit den Homomorphismen α_n und β_n notwendig und hinreichend ist und damit das beschriebene Verfahren brauchbarer wird ?' die Menge der ganzen p-adischen Zahlen eine naheliegende Antwort ist.

2.6 Zusatz: Eine Erweiterung des Verfahrens zur Lösung algebraischer Gleichungen über $\mathbb{Z}_p$

Das im letzten Abschnitt beschriebene Verfahren zur Lösung algebraischer Gleichungen

$$a(X) = 0$$

über $\mathbb{Z}_p$ eignet sich besonders gut für Lösungen $z \in \mathbb{Z}_p$, die $a'(z) \not\equiv 0 \;\; mod\, p$ erfüllen. In diesem Abschnitt wollen wir zeigen, daß man das Verfahren modifizieren kann, sodaß es für die anderen Lösungen genauso gut geeignet ist. Dadurch werden wir auch eine Verallgemeinerung von Satz 2.6 beweisen können.
Wer sich nur für den Beweis des Satzes von Skolem-Mahler-Lech interessiert, kann diesen Abschnitt bis auf eine kleine Ausnahme ruhig auslassen. (In Kapitel 3 werden wir die Diskriminante eines Polynoms, die wir hier definieren, noch einmal verwenden.)

Voraussetzung, um das erweiterte Verfahren anwenden zu können, ist, daß wenn schon nicht $a(X) = 0 \;\; mod\, p$ nur einfache Nullstellen hat (Satz 2.6 (2)), es zumindest eine natürliche Zahl $m \in \mathbb{N}$ gibt, sodaß $a(X) = 0 \;\; mod\, p^m$ nur einfache Nullstellen hat. Leider ist diese Bedingung aber nicht für jedes Polynom $a(X)$ über $\mathbb{Z}_p$ erfüllt: Hat nämlich $a(X)$ eine mehrfache Nullstelle in $\mathbb{Z}_p$, dann gilt dasselbe für $a(X) = 0 \;\; mod\, p^n$.
Wenn wir also nicht bei jedem Polynom von der Existenz einer solchen natürlichen Zahl m ausgehen können, müssen wir wenigstens einen Weg finden, der alles auf solche Polynome zurückführt, für die es doch so ein m gibt. Da gelingt mit Hilfe der Diskriminante des Polynoms:

Definition 2.3 *Es sei R ein Integritätsbereich, $f(X) \in R[X]$ und $n = deg(f)$. Betrachte folgende Gleichung in den Polynomen $u(X) = u_0 + u_1X + ... + u_{n-2}X^{n-2}$ und $v(X) = v_0 + v_1X + ... + v_{n-1}X^{n-1}$:*

$$u(X)f(X) + v(X)f'(X) = 1.$$

Diese Gleichung ist äquivalent zu einem linearen Gleichungssystem mit $2n-1$ Gleichungen und den $2n-1$ Unbekannten $u_0, u_1, ...u_{n-2}, v_0, v_1, ...v_{n-1}$. Mit der Diskriminante $D(f)$ von $f(X)$ bezeichnet man die Determinante dieses linearen Gleichungssystems.

Beispiel: Wir wollen allgemein die Diskriminante eines Polynoms $f(X) = f_0 + f_1X + f_2X^2 + f_3X^3$ dritten Grades berechnen: Die Gleichung

$$u(X)f(X) + v(X)f'(X) = 1,$$

wobei $u(X) = u_0 + u_1X$ und $v(X) = v_0 + v_1X + v_2X^2$, ist nach Koeffizientenvergleich äquivalent zu

$$\begin{array}{cccccccc}
u_0f_0+ & & v_0f_1 & & & = & 1 \\
u_0f_1+ & u_1f_0+ & v_02f_2+ & v_1f_1 & & = & 0 \\
u_0f_2+ & u_1f_1+ & v_03f_3+ & v_12f_2+ & v_2f_1 & = & 0 \\
u_0f_3+ & u_1f_2+ & & v_13f_3+ & v_22f_2 & = & 0 \\
 & u_1f_3+ & & & v_23f_3 & = & 0
\end{array}$$

Die Diskriminante ist daher die Determinante folgender (5×5)-Matrix:

$$\begin{pmatrix}
f_0 & 0 & f_1 & 0 & 0 \\
f_1 & f_0 & 2f_2 & f_1 & 0 \\
f_2 & f_1 & 3f_3 & 2f_2 & f_1 \\
f_3 & f_2 & 0 & 3f_3 & 2f_2 \\
0 & f_3 & 0 & 0 & 3f_3
\end{pmatrix}$$

Diese Determinante berechnete ich mit Hilfe eines Computers und erhielt

$$D(f) = -f_1^2f_2^2f_3 + 4f_0f_2^3f_3 + 4f_1^3f_3^2 + 27f_0f_3^3 - 18f_0f_1f_2f_3^2. \quad \square$$

Ist $D \in \mathbb{Z}_p$ die Diskriminante von $a(X)$, dann gibt es zwei Polynome $u(X)$ und $v(X)$ über $\mathbb{Z}_p$ mit $deg(u) \leq n-2$ und $deg(v) \leq n-1$, sodaß

$$u(X)a(X) + v(X)a'(X) = D. \qquad (*)$$

(Zunächst ist einmal klar, daß es zwei solche Polynome über $\mathbb{Q}_p$, dem Quotientenkörper von $\mathbb{Z}_p$ gibt: Ist nämlich $D \neq 0$, so ist das Gleichungssystem (*) eindeutig über dem Körper $\mathbb{Q}_p$ lösbar. Diese Lösung $(u_0, u_1, ...u_{n-2}, v_0, v_1, ...v_{n-1})$ erhält man, wenn man die inverse Matrix A^{-1} des Gleichungssytems mit dem Vektor $(D, 0, ...0) \in \mathbb{Z}_p^{2n-1}$ multipliziert. Da die Matrix A des Gleichungssystems eine über $\mathbb{Z}_p$ ist, folgt aus der allgemeinen Formel für die Inverse einer Matrix, daß A^{-1} der Quotient einer Matrix über $\mathbb{Z}_p$ und der Diskriminante D ist. Es folgt, daß die (eindeutig bestimmten) Polynome $u(X)$ und $v(X)$ welche über $\mathbb{Z}_p$ sind. Wenn aber $D = 0$, kann man $u(X) = v(X) = 0$ wählen.)

Die Diskriminante ist eine Größe, die Auskunft über die Existenz mehrfacher Nullstellen gibt: Ist $D \neq 0$, so kann $a(X)$ keine mehrfache Nullstelle haben. Wäre nämlich $z \in \mathbb{Q}_p$ eine mehrfache Nullstelle von $a(X)$, so ist z auch Nullstelle der Ableitung $a'(X)$ und es würde

$$0 = u(z)a(z) + v(z)a'(z) = D$$

folgen.
Ist dagegen $D = 0$, so muß $a(X)$ zwar nicht unbedingt eine mehrfache Nullstelle in $\mathbb{Q}_p$ und

daher einen gemeinsamen Linearfaktor mit ihrer Ableitung $a'(X)$ haben. Es folgt aber, daß $a(X)$ und $a'(X)$ einen gemeinsamen Faktor (beliebiger Ordnung) haben: Angenommen $a(X)$ und $a'(X)$ wären teilerfremd. Dann gibt es Polynome $u_0(X), v_0(X) \in \mathbb{Q}_p[X]$ mit

$$u_0(X)a(X) + v_0(X)a'(X) = 1.$$

Es sei $b(X)$ ein Polynom über $\mathbb{Q}_p$, dessen Grad kleiner als $2n-1$ ist. Wenn wir $\overline{u}(X) = u_0(X) \cdot b(X)$ und $\overline{v}(X) = v_0(X) \cdot b(X)$ setzen, folgt

$$\overline{u}(X) \cdot a(X) + \overline{v}(X)a'(X) = b(X).$$

Nach dem Satz von der Division mit Rest existieren zwei Polynome $q(X), u(X) \in \mathbb{Q}_p$, wobei $deg(u) \leq n-2$, mit

$$\overline{u}(X) = q(X) \cdot a'(X) + u(X).$$

Wenn wir $v(X) = \overline{v}(X) + q(X)a(X)$ setzen, folgt

$$u(X) \cdot a(X) + v(X) \cdot a'(X) = b(X).$$

Wegen $deg(v \cdot a') = deg(b - u \cdot a) < 2n-1$ und $deg(a') = n-1$ folgt $deg(v) \leq n-1$.
Das Gleichungssystem

$$u(X) \cdot a(X) + v(X) \cdot a'(X) = b(X)$$

in den Polynomen $u(X)$ und $v(X)$, $deg(u) \leq n-2$, $deg(v) \leq n-1$ ist daher für jedes $b(X) \in \mathbb{Q}_p[X]$ mit $deg(b) < 2n-1$ lösbar. Folglich kann die Determinante von (*) nicht Null sein.

Nun zurück zur Bestimmung der Nullstellen von $a(X)$ in $\mathbb{Z}_p$:
Wir können annehmen, daß die Diskriminante D von $a(X)$ ungleich Null ist, denn andernfalls haben $a(X)$ und $a'(X)$ einen gemeinsamen Faktor $d(X)$, den man mit Hilfe des Euklidschen Algorithmus berechnen kann (Die Ableitung $a'(X)$ ist nicht das Nullpolynom, da wir o.B.d.A. $a(X)$ nicht-konstant annehmen und $char(\mathbb{Q}_p) = 0$). Damit reduziert sich das Problem auf die Bestimmung der Nullstellen der beiden Polynome $d(X)$ und $\frac{a(X)}{d(X)}$ deren Grad sicher kleiner als der von $a(X)$ ist. Wenn die Diskriminante $D(d)$ von $d(X)$ ebenfalls Null ist, so kann man $d(X)$ weiter zerlegen und reduziert das Problem wieder auf die Bestimmung der Nullstellen von Polynomen, deren Grad kleiner als $deg(d)$ ist u.s.w. Ist $D(d) \neq 0$, dann kann man das im folgenden beschriebene Verfahren auf das Polynom $d(X)$ anwenden (dasselbe gilt natürlich für das Polynom $\frac{a(X)}{d(X)}$; für die Anwendung des Verfahrens benötigen wir die Tatsache, daß die Polynome $d(X)$ und $\frac{a(X)}{d(X)}$ Elemente von $\mathbb{Z}_p[X]$ sind. Das muß von vornherein nicht der Fall sein. Jedoch kann das durch Multiplikation einer passenden Potenz von p erreicht werden.)

Beschreibung des erweiterten Verfahrens:

Es sei $a(X)$ ein Polynom mit Koeffizienten in $\mathbb{Z}_p$ und $D \neq 0$ die Diskriminante. Wir wählen $u(X), v(X) \in \mathbb{Z}_p[X]$, sodaß (*) erfüllt ist. Weiters sei $m \in \mathbb{N}$ so gewählt, daß $\|D\|_p = p^{-m}$. Dann hat $a(X) = 0 \ \ mod\, p^{m+1}$ nur einfache Nullstellen: Angenommen es gäbe ein ganze Zahl z mit $a(z) = 0 \ \ mod\, p^{m+1}$ und $a'(z) = 0 \ \ mod\, p^{m+1}$. Dann folgt

$$D = u(z)a(z) + v(z)a'(z) \equiv 0 \ \ mod\, p^{m+1},$$

ein Widerspruch zur Wahl von m.

Als erstes bestimmt man alle Lösungen der algebraischen Kongruenz

$$a(X) \equiv 0 \ \ mod\, p^{2m+1}$$

und wählt für diese Repräsentanten in $\{0, 1, ...p^{2m+1} - 1\}$. Führe folgende Äquivalenzrelation $\sim$ auf dieser Lösungsmenge L' ein:

$$x \sim y \Leftrightarrow y \equiv x \ \ mod\, p^{2m+1} \|a'(x)\|_p$$

Diese Äquivalenzrelation ist wohldefiniert, weil $a'(x) \not\equiv 0 \ \ mod\, p^{m+1} \quad \forall x \in L'$ und daher $p^{2m+1}\|a'(x)\|_p$ eine Potenz von p ist, deren Exponent größer als m ist, also inbesondere positiv. Die Symmetrie und die Transitivität der Äquivalenzrelation ergibt sich folgendermaßen: Wenn

$$y \equiv x \ \ mod\, p^{2m+1} \|a'(x)\|_p$$

dann folgt für die Ableitungen

$$a'(y) \equiv a'(x) \ \ mod\, p^{2m+1} \|a'(x)\|_p$$

und wegen $\|a'(x)\|_p, \|a'(y)\|_p \geq p^{-m}$ und $\|p^{2m+1}\|a'(x)\|_p\|_p < p^{-m}$ ergibt das $\|a'(x)\|_p = \|a'(y)\|_p$. Wir erhalten die Äquivalenz

$$y \equiv x \ \ mod\, p^{2m+1} \|a'(x)\|_p \Leftrightarrow x \equiv y \ \ mod\, p^{2m+1} \|a'(y)\|_p$$

aus der sich unmittelbar Symmetrie und Transitivität ergeben.

Wir wählen aus jeder Äquivalenzklasse bezüglich $\sim$ genau einen Repräsentanten und fassen diese Repräsentanten zu einer Menge $L \subseteq L'$ zusammen. Wir zeigen, daß es zu jedem Element $x_0 \in L$ ein einzige Nullstelle $x \in \mathbb{Z}_p$ von $a(X)$ gibt mit $x \equiv x_0 \ \ mod\, p^{2m+1}\|a'(x_0)\|_p$. Das funktioniert wieder durch sukzessives Fortsetzen der 'Näherungslösungen' in L:

Es sei $x_0 \in L$ beliebig. Laut Definintion ist x_0 eine Lösung der Gleichung $mod\ \ p^{2m+1}$. Wir setzen sie zu einer $mod\ \ p^{2m+2}$ fort, wobei wir diesmal den Ansatz $x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p$ wählen und $k_1 \in \{0, 1, ...p - 1\}$ noch passend bestimmen müssen.

$$\begin{gathered}
a(x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p) = \\
= a(x_0) + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p a'(x_0) + (k_1 \cdot p^{2m+1}\|a'(x_0)\|_p)^2 a_2(x_0) + ... \equiv \\
\equiv a(x_0) + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p a'(x_0) \ \ mod\, p^{2m+2}
\end{gathered}$$

Es folgt, daß k_1 Lösung folgender linearen Kongruenz in $\mathbb{Z}/p\mathbb{Z}$ sein muß:

$$\frac{a(x_0)}{p^{2m+1}} + k_1\|a'(x_0)\|_p a'(x_0) \equiv 0 \ \ mod\, p$$

Diese besitzt eine eindeutige Lösung, da $\|a'(x_0)\|_p a'(x_0) \not\equiv 0 \ \ mod\, p$.

Als nächstes setzt man die erhaltene Lösung $mod\, p^{2m+3}$ fort:

$$
\begin{gathered}
a(x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p + k_2 \cdot p^{2m+2}\|a'(x_0)\|_p) = \\
= a(x_0 + k_1 p^{2m+1}\|a'(x_0)\|_p) + k_2 \cdot p^{2m+2}\|a'(x_0)\|_p a'(x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p) + \\
(k_2 \cdot p^{2m+1}\|a'(x_0)\|_p)^2 a_2(x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p) + \ldots \equiv \\
\equiv a(x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p) + \\
k_2 \cdot p^{2m+2}\|a'(x_0)\|_p a'(x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p) \;\; mod\, p^{2m+3}
\end{gathered}
$$

Wiederum ist k_2 Lösung einer linearen Kongruenz über $\mathbb{Z}/p\mathbb{Z}$:

$$
\begin{gathered}
\frac{a(x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p)}{p^{2m+2}} + k_2\|a'(x_0)\|_p a'(x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p) \equiv \\
\equiv \frac{a(x_0 + k_1 \cdot p^{2m+1}\|a'(x_0)\|_p)}{p^{2m+2}} + k_2\|a'(x_0)\|_p a'(x_0) \equiv 0 \;\; mod\, p
\end{gathered}
$$

(Sie ist wieder eindeutig lösbar, weil $\|a'(x_0)\|_p a'(x_0) \not\equiv 0 \;\; mod\, p$.)

Im nächsten Schritt setzt man die erhaltene Kongruenz $mod\, p^{2m+4}$ fort...u.s.w.

Damit haben wir gezeigt, daß jede Näherungslösung $x_0 \in L$ eine eindeutig bestimmte Fortsetzung $x \in \mathbb{Z}_p$ hat, mit $a(x) = 0$ und $x \equiv x_0 \;\; mod\, p^{2m+1}\|a'(x_0)\|_p$.
Umgekehrt erhält man so alle Lösungen der Gleichung $a(X) = 0$ in $\mathbb{Z}_p$. Ist nämlich $z \in Z_p$ eine Nullstelle des Polynoms $a(X)$, dann gibt es ein $z_0 \in L'$ mit $z \equiv z_0 \;\; mod\, p^{2m+1}$ und daher gibt es ein $x_0 \in L$ mit $z \equiv x_0 \;\; mod\, p^{2m+1}\|a'(x)\|_p$. Die Nullstelle z ist dann die eindeutig bestimmte Forsetzung von x_0. (Dieses Verfahren bricht ja für kein $x_0 \in L$ ab.) Es folgt daher insbesondere, daß $|L|$ die Anzahl der Nullstellen von $a(X)$ in $\mathbb{Z}_p$ ist.
Dieses Verfahren ist wirklich eine Verallgemeinerung des Abschnitt 2.5 beschriebenen Verfahren: Hat nämlich $a(X) \equiv 0 \;\; mod\, p$ nur einfache Nullstellen, so kann man $m = 0$ wählen und das erweiterte Verfahren reduziert sich auf das bereits bekannte. □

Aus diesem Verfahren resultiert folgende stärkere Version von Satz 2.6:

Satz 2.9 (Henselsches Lemma) *Es sei $a(X)$ ein Polynom über $\mathbb{Z}_p$ und $z_0 \in \mathbb{Z}_p$, sodaß*

$$\|a(z_0)\|_p < \|a'(z_0)\|_p^2.$$

Dann gibt es genau ein $z \in \mathbb{Z}_p$ mit $a(z) = 0$ und $z \equiv z_0 \;\; mod\, p^{2m+1}\|a'(z_0)\|_p$, wobei $m \in \mathbb{N}$ so gewählt ist, daß $\|a'(z_0)\|_p = p^{-m}$.

Beweis: Es sei $m \in \mathbb{N}$ wie in der Formulierung des Satzes. Dann kann $a(X) \equiv 0 \;\; mod\, p^{m+1}$ keine mehrfache Nullstelle haben, die $\equiv z_0 \;\; mod\, p^{m+1}$, da $a'(z_0) \not\equiv 0 \;\; mod\, p^{m+1}$ ist. Die Voraussetzung $\|a(z_0)\|_p < \|a'(z_0)\|_p^2$ ist äquivalent dazu, daß z_0 eine Lösung $mod\;\; p^{2m+1}$ ist.
Nun kann man wie im Verfahren mit dem Ansatz $z_0 + k_1 \cdot p^{2m+1}\|a'(z_0)\|_p$ diese Nährungslösung z_0 eindeutig zu einer $mod\, p^{2m+2}$ fortsetzen...u.s.w.

Auf diese Weise erhält man eine Folge $(k_i)_{i\geq 0}$, sodaß $z = z_0 + \sum_{i=1}^{\infty} k_i p^{2m+i} \|a'(z_0)\|_p$ die geforderte Lösung ist. Sie ist $mod\, p^{m+1}$ eindeutig bestimmt, da die Folge $(k_i)_{i\geq 0}$ eindeutig bestimmt ist.

Bemerkung Das ist wirklich eine Verallgemeinerung von Satz 2.6.: Ist nämlich $z_0 \in \mathbb{Z}_p$ so, daß $a(z_0) \equiv 0 \;\; mod\, p$ und $a'(z_0) \not\equiv 0 \;\; mod\, p$, dann ist

$$\|a(z_0)\|_p < 1 = \|a_{z_0}\|_p^2$$

und $m = 0$.

Es gibt übrigens noch viele weitere Verallgemeinerungen des Henselschen Lemmas. Meistens handelt es sich dabei um Aussagen, die von der Existenz einer Näherungslösung mit bestimmten Eigenschaften auf die Existenz einer exakten Lösung schließen. Für Polynome haben wir mit Satz 2.9. schon die stärkste mir bekannte Version des Henselschen Lemmas bewiesen. Man kann die vorgestellte Methode aber auch noch auf p-adische Potenzreihen (siehe Kapitel 4) und sogar Laurentreihen anwenden.
In der Literatur habe ich noch eine andere Möglichkeit gefunden, das Henselsche Lemma zu verallgemeinern: Es sei $a(X)$ ein Polynom über $\mathbb{Z}_p$. Wenn nun zwei weitere Polynome $b_0(X)$ und $c_0(X)$ mit Koeffizienten in $\mathbb{Z}_p$ existieren, sodaß $a(X) \equiv b_0(X)c_0(X) \;\; mod\, p$, dann kann man unter geeigneten Umständen daraus schließen, daß zwei Polynome $b(X) \equiv b_0(X) \;\; mod\, p$ und $c(X) \equiv c_0(X) \;\; mod\, p$ über $\mathbb{Z}_p$ existieren, sodaß $a(X) = b(X)c(X)$ (Für $deg(b) = 1$ ergibt das unsere Henselschen Lemmata.). Auch das kann man wieder auf Laurentreihen verallgemeinern. Die allgemeinste Version des Henselschen Lemmas fand ich in [1].

Beispiele

(1) Wir betrachten noch einmal das Polynom

$$a(X) = X^3 + 3X^2 + 4X + 8$$

über $\mathbb{Z}_2$ (vgl. Beispiel, Abschnitt 2.5). Die Diskriminante dieses Polynoms beträgt $976 = 2^4 61$ und wir müssen daher $m = 4$ wählen (siehe Beispiel nach Definition 2.3). Laut Verfahren bestimmen wir alle Lösungen von $a(X) \equiv 0 \;\; mod\, 2^9$ in $\{0, 1, ...2^9 - 1\}$. Dazu probiert man am besten alle 2^9 Möglichkeiten mit einem Computer aus und erhält, daß es genau ein solches $z_0 = 433$ gibt. Es folgt, daß $a(X)$ genau eine Nullstelle in $\mathbb{Z}_2$ hat, die $\equiv z_0 \;\; mod\, 2^9 \|a'(z_0)\|_p$ ist.
Wir erfahren also im Grunde nichts Neues. Der Unterschied diese erweiterten Verfahrens im Vergleich zum einfacheren ist aber, daß man nicht ins 'Ungewisse' rechnet: Es kann dabei nämlich nicht passieren, daß man endlos lange Näherungslösungen vermeintlicher Nullstellen fortsetzt, um dann bei einer hohen Potenz von p zu bemerken, daß es keine Fortsetzung mehr gibt (wie das in Abschnitt 2.5 bei der Fortsetzung der von 0 passiert ist). Durch diese natürliche Zahl m und daher durch die Diskriminante von $a(X)$ ist dem eine (berechenbare) Grenze gesetzt. Der Preis, den man dafür bezahlen muß, ist, daß man zu Beginn nicht nur die Lösungen $mod\, 2$ berechnen muß sondern $mod\, 2^9$.

(2) Nun wollen wir das Verfahren auf das Polynom

$$b(X) = X^3 + 25X^2 + X - 9$$

in $\mathbb{Z}_3[X]$ anwenden. Die Diskriminante beträgt $-556884 = -2^2 \cdot 3 \cdot 47237$ und daher $m = 1$. Die algebraische Kongruenz

$$b(X) = 0 \ \ mod\, 3^3$$

hat die Lösungen $\{4, 7, 9, 13, 16, 22, 25\}$. Als nächstes müssen wir die den 3-adischen Absolutbetrag der Ableitungen jeder Lösung berechnen, um die Äquivalenzklassen der Äquivalenzrelation $\sim$ bestimmen zu können:

$$\|b'(4)\|_3 = 3^{-1}, \|b'(7)\|_3 = 3^{-1}, \|b'(9)\|_3 = 1, \|b'(13)\| = 3^{-1},$$
$$\|b'(16)\|_3 = 3^{-1}, \|b'(22)\|_3 = 3^{-1}, \|b'(25)\|_3 = 3^{-1}$$

Die Äquivalenzklassen sind daher:

$$\{9\}, \quad \{4, 13, 22\}, \quad \{7, 16, 25\}$$

Wir setzen $L = \{9, 4, 7\}$ und wissen bereits, daß das Polynom $b(X)$ drei verschiedene Nullstellen in $\mathbb{Z}_3$ hat (also komplett zerfällt), wobei eine $\equiv 9 \ \ mod\, 3^3$, die andere $\equiv 4 \ \ mod\, 3^2$ und die dritte $\equiv 7 \ \ mod\, 3^2$ ist. Diese könnte man nun wieder näherungsweise, durch das Lösen von linearen Kongruenzen über $\mathbb{Z}/p\mathbb{Z}$ berechnen (siehe Satz 2.9).
Übrigens: über $\mathbb{Z}_2$ hat die Gleichung $b(X) = 0$ keine einzige Nullstelle, denn $b(z) \not\equiv 0 \ \ mod\, 2^2$ für $z = 0, 1, 2, 3$.

Zum Schluß sei noch erwähnt, daß dieses Verfahren natürlich eher selten benötigt wird, um die Nullstellen p-adischer Polynome tatsächlich zu berechnen, da man an so konkreten Fragestellungen meist nur so weit interessiert ist, bis man zumindest theoretisch weiß, wie man sie (bestmöglich) lösen kann. Und ist für eine bestimmte Fragestellung doch die Berechnung der Nullstellen eines Polynoms nötig, so wird man wahrscheinlich nicht dem in gewissem Sinn bestmöglichen Verfahren den Vortritt geben, sondern dem einfacher zu merkenden und in den meisten Fällen auch schnelleren Verfahren aus Abschnitt 2.5.
Für mich war das kompliziertere Verfahren aber dennoch wichtig, um das relativ häufig verwendete Henselsche Lemma besser zu verstehen. (Der erste Beweis von Satz 2.9, den ich kennenlernte, verriet mir nicht sofort, daß er nur eine Verallgemeinerung des einfachen Verfahrens aus Abschnitt 2.5 ist und war daher zunächst undurchschaubar. Und das, obwohl dieser Beweis im Wesentlichen derselbe ist, wie der in dieser Arbeit, reduziert auf jene Schritte, die man wirklich für Satz 2.9 benötigt und nicht alleine für das Verfahren wichtig sind.)

2.7 Die ultrametrische Ungleichung

Ähnlich wie bei den reellen oder komplexen Zahlen und dem herkömmlichen Absolutbetrag haben wir nun einen vollständig normierten Körper $\mathbb{Q}_p$ in dem wir Analysis betreiben

können. Wir werden daher auch analoge Begriffe zu $\mathbb{R}$ und $\mathbb{C}$ betrachten (vor allem Potenzreihen). Zwar holt man sich einige Ideen aus der gewöhnlichen Analysis – die Beweise sind aber oft grundsätzlich anders (meistens einfacher) und ermöglichen häufig sogar stärkere Aussagen. Hauptgrund dafür ist, daß im p-adischen Fall nicht nur die herkömmliche Dreiecksungleichung $\|a+b\|_p \leq \|a\|_p + \|b\|_p$, sondern die stärkere ultrametrische Ungleichung $\|a+b\|_p \leq \max\{\|a\|_p, \|b\|_p\}$ gilt.
Aus diesem Grund verdient diese Ungleichung am Ende des Kapitels über $\mathbb{Q}_p$ einen eigenen kleinen Abschnitt. Ich zeige in ihm einfache Folgerungen aus dieser Ungleichung, die später neben den Analogien zur bekannten Analysis sozusagen das Grundwerkzeug für das Arbeiten in $\mathbb{Q}_p$ sein werden. Diese Ergebnisse sind aber auch unabhängig von ihrem späteren Nutzen interessant, weil sie ein erstes Gefühl für den großen Unterschied zur gewöhnlichen Analysis geben. Man wird sehen, daß alle analogen Behauptungen für $\mathbb{R}$ und $\mathbb{C}$ völlig absurd sind.

So sind zum Beispiel aufgrund dieser Ungleichung 'Kugeln um den Nullpunkt' $B_r(0) = \{a \in \mathbb{Q}_p | \|a\|_p \leq r\}$ additive Gruppen in $\mathbb{Q}_p$: Denn ist $a, b \in B_r(0)$, so ist

$$\|a-b\|_p \leq \max\{\|a\|_p, \|-b\|_p\} \leq r$$

und daher $a - b \in B_r(0)$ (Dasselbe gilt natürlich auch für offene Kugeln; die Begriffe 'offen' und 'abgeschlossen' beziehen sich hier nicht auf die toplogischen Eigenschaften der Kugel, sondern einfach auf die Tatsache, ob man jene a mit $\|a\|_p = r$ zur Kugel dazugibt oder nicht; siehe auch Bemerkung 4 nach Satz 4.1).
Das ist hier vielleicht schon nicht mehr so überraschend, weil wir in Abschnitt 2.5 gezeigt haben, daß die abgeschlossene Einheitskugel sogar einen Ring bildet. Die offene Einheitskugel ist auch ein Teilring von $\mathbb{Z}_p$, ja sie bildet sogar ein Ideal im Integritätsbereich der ganzen p-adischen Zahlen.
In $\mathbb{R}$ und $\mathbb{C}$ sind die Einheitskugeln natürlich keine Ringe, und allgemeiner, beliebige Kugeln um den Nullpunkt keine additiven Gruppen.

Man wird vielleicht staunen, welch unerwarteten Folgerungen der folgende, einfache Hilfssatz nach sich ziehen wird:

Hilfssatz 2.2 *Es seien $a, b \in \mathbb{Q}_p$ mit $\|b\|_p < \|a\|_p$. Dann gilt $\|a+b\|_p = \|a\|_p$.*

Beweis: Aus der ultrametrischen Ungleichung und $\|b\|_p < \|a\|_p$ folgt:

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

Dieselbe Ungleichung, anders angewandt, ergibt

$$\|a\|_p = \|a+b+(-b)\|_p \leq \max\{\|a+b\|_p, \|b\|_p\} \overset{\|b\|_p \leq \|a\|_p}{=} \|a+b\|_p. \quad \Box$$

(Dieser Hilfssatz ist nur die Verallgemeinerung der Tatsache, daß, wenn $a, b \in \mathbb{Z}$, a ist genau durch p^m (also nicht durch p^{m+1}) und b ist genau durch p^{m+k} teilbar ($k, m \in \mathbb{N}$; $k > 1$), $a+b$ genau durch p^m teilbar ist.)

Man kann diesen Hilfssatz auch anders formulieren: Sind $a, b \in \mathbb{C}$, so definieren $a, b, a+b$ ein Dreieck in der Gaußschen Ebene:

Definiert man in $\mathbb{Q}_p$ Dreiecke analog als Zahlentripel der Form $(a, b, a+b)$, so besagt Hilfssatz 2.2, daß jedes Dreieck gleichschenkelig ist: Denn angenommen die beiden 'Schenkel' a und b sind nicht gleich lang, d.h $\|b\|_p \neq \|a\|_p$, so kann man o.B.d.A. annehmen, daß $\|b\|_p < \|a\|_p$. Aus Hilfssatz 2.2 folgt $\|a+b\|_p = \|a\|_p$.

Ein weitere 'geometrische Anomalie' von $\mathbb{Q}_p$ ist die folgende: Es sei $B_r(a) = \{x \in \mathbb{Q}_p | \|x - a\|_p \leq r\}$ ($a \in \mathbb{Q}_p$, $r \in \mathbb{R}^+$) die abgeschlossene Kugel mit Radius r um den 'Mittelpunkt' a. Dann ist jeder andere 'Punkt' $b \in B_r(a)$ ebenfalls Mittelpunkt von $B_r(a)$, d.h. $B_r(a) = B_r(b)$. Das ergibt sich wiederum unmittelbar aus der ultrametrischen Ungleichung:

$$x \in B_r(a) \Rightarrow \|x-a\|_p \leq r \Rightarrow \|x-b\|_p = \|(x-a)+(a-b)\|_p \leq$$
$$\leq \max\{\|x-a\|_p, \|a-b\|_p\} \leq r \Rightarrow x \in B_r(b)$$

Es folgt $B_r(a) \subseteq B_r(b)$ und daher, aus Symmetriegründen, die Behauptung.
(Das Analoge gilt natürlich auch wieder für offene Kugeln.)

Zum Schluß noch ein zweites Ergebnis, daß wir zu einem Hilfssatz zusammenfassen werden: Zu Beginn meines Mathematikstudiums war eine der ersten Tatsachen, die ich über unendliche Reihen $\sum\limits_{i=0}^{\infty} a_i$ in $\mathbb{R}$ gelernt habe, daß für ihre Konvergenz $\lim\limits_{i\to\infty} a_i = 0$ zwar notwendig ist, aber keineswegs hinreichend. Als Paradebeispiel dient die harmonische Reihe $\sum\limits_{n=1}^{\infty} \frac{1}{n}$, die, obwohl $\frac{1}{n} \to 0$ bei $n \to \infty$, nicht konvergiert.
Im p-adischen ist das nicht so. Dort ist die Bedingung notwendig und hinreichend. Auch ein Grund, wieso in $\mathbb{Q}_p$ manches einfacher ist. (Konvergenzkriterien von Reihen, wie z.B. Wurzelkriterium, Quotientenkriterium, Leibnizkriteriun werden unnötig; Außerdem folgt daraus, daß jede konvergente Reihe sogar absolut konvergiert: Es sei $\sum\limits_{i=0}^{\infty} b_i$ konvergent. Es folgt $\lim\limits_{i\to 0} \|b_i\|_p = 0$ und daher $\sum\limits_{i=0}^{\infty} \|b_i\|_p < \infty$. Aus diesem Grund gibt es einige Sätze, die in $\mathbb{R}$ nur für absolut konvergente Reihen gelten, in $\mathbb{Q}_p$ aber für beliebige konvergente Reihen erfüllt sind; siehe z.B. Kapitel 4.)

Hilfssatz 2.3 *Es sei $(a_n)_{n\geq 0}$ eine Folge in $\mathbb{Q}_p$ mit $\|a_{n+1} - a_n\|_p \to 0$ bei $n \to \infty$. Dann ist*

$(a_n)_{n\geq 0}$ *eine Cauchyfolge und wegen der Vollständigkeit von* $\mathbb{Q}_p$ *konvergent.*

Beweis: Es sei $\varepsilon > 0$ beliebig und $N \in \mathbb{N}$, sodaß $\forall n \geq N$

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

Für $m > n > N$ folgt dann:

$$\|a_n - a_m\|_p = \|a_n - a_{n+1} + a_{n+1} - a_{n+2} + ... + a_{m-1} - a_m\|_p \leq$$

$$\leq \max\{\|a_n - a_{n+1}\|_p, ...\|a_{m-1} - a_m\|_p\} \leq \max\{\varepsilon, ...\varepsilon\} \leq \varepsilon$$

Folgerung: *Es sei* $(b_i)_{i\geq 0}$ *eine Nullfolge in* $\mathbb{Q}_p$. *Dann konvergiert die Folge der Partialsummen* $\left(\sum\limits_{i=0}^{n} b_i\right)_{n\geq 0}$.

An dieser Stelle, wo die Unterschiede der 'gewöhnlichen Analysis' und der p-adischen Analysis so offensichtlich werden, fragt man sich, ob es denn überhaupt einen Sinn hat, die rationalen Zahlen (und $\mathbb{Q}_p$) in dieser Analogie zu betrachten.
Dazu folgendes: Da die ultrametrische Ungleichung die Dreiecksungleichung impliziert wird man das meiste, daß in $\mathbb{R}$ und $\mathbb{C}$ bezüglich $|.|$ gilt, auf $\mathbb{Q}_p$ übertragen können, d.h. man bekommt viele Sätze sozusagen ohne viel Mühe geschenkt und das ist zweifellos ein Vorteil.
Andererseits entsteht bei mir auch das Gefühl, daß man auf die Weise nicht die 'ganze Wahrheit' über $\mathbb{Q}_p$ erfährt, das heißt, daß aufgrund der ultrametrischen Ungleichungen viel stärkere Aussagen gelten würden, die man aber mit Mitteln der gewöhnliche Analysis natürlich nicht zeigen kann. (Um das an einem konkreten Beispiel zu erfahren, verweise ich auf die Beweise des Identitätssatz für Potenzreihen in $\mathbb{Q}_p$, zu finden in Kapitel 4.) An dieser Stelle trennen sich die Wege der Analysis auf Basis der Dreiecksungleichung und der p-adischen Analysis. Letztere muß eigene Methoden entwickeln, um die 'ganze Wahrheit' zu erforschen.
In dieser Arbeit wird man aber kaum etwas über diese eigenen Wege erfahren. Vielleicht ist das auch ein Grund dafür, daß ich bei diesem Beweis des Satzes von Skolem-Mahler-Lech recht lange das Gefühl hatte nicht wirklich zu verstehen, wieso er überhaupt gilt. Man/Ich müßte vielleicht noch etwas tiefer graben, um die Situation besser zu verstehen.

Siehe auch Abschnitt 5.2. In Gesprächen mit anderen Mathematikern ist mir aufgefallen, daß sie mit meinem Begriff des 'wirklichen Verstehens' meist nicht viel anfangen können. Deshalb möchte ich das an dieser Stelle etwas präzisieren und das mache ich am besten mit Hilfe eines Beispieles: Es ist ein bekanntes Resultat, daß sich die drei Schwerlinien eines Dreiecks in einem Punkt schneiden. Einerseits könnte man diesen Satz mit Hilfe analytischer Geometrie beweisen, indem man sich eine beliebiges Dreieck mit den Punkten $A = (a_1, a_2)$, $B = (b_1, b_2)$ und $C = (c_1, c_2)$ im kartesischen Koordinaten vorgibt, die Gleichungen der drei Schwerlinien in Abhängigkeit von $a_1, a_2, b_1, b_2, c_1, c_2$ aufstellt und dann auf algebraischen Wege die Behauptung zeigt.
Man kann den Satz aber auch so beweisen: Wir stellen uns ein beliebiges Dreieck vor, welches aus einem homogenen Material gefertigt ist. Mit homogen meine ich, daß zwei Stückchen aus diesem Material die gleiche Masse haben, wenn auch ihr Volumen gleich ist. Da eine Schwerlinie das Dreieck

in zwei flächengleiche Teile zerlegt und wir wiederum idealerweise annehmen, daß das Dreieck an jeder Stelle gleich dick ist, folgt aus der Homogenität des Materials, daß diese zwei Teildreiecke gleich schwer sind. Legt man nun das Dreieck entlang dieser Schwerlinie auf eine Kante, so wird das Dreieck im Gleichgewicht stehen. Selbstverständlich gilt das für jede Schwerlinie des Dreiecks. Es folgt, daß der Schnittpunkt zweier solcher Schwerlinien der/ein Massenmittelpunkt des Dreieckes ist, d.h. legt man das Dreieck auf eine zur Erdoberfläche im Lot stehende Spitze, so wir das Dreieck auch noch im Gleichgewicht stehen. Es folgt, daß jedes Dreieck mindestens einen Massenmittelpunkt hat. Umgekehrt ist aber auch klar, daß ein Dreieck höchstens einen Massenmittelpunkt hat: So ein Massenmittelpunkt muß nämlich immer auf allen drei Schwerlinien liegen, wie man indirekt relativ leicht zeigt. Da in einem (nicht-ausgearteten) Dreieck der Schnitt der Schwerlinien höchstens ein Punkt ist, folgt die Behauptung (Dieser Beweis hat natürlich einige kleine Lücken. Z.B. bin ich nicht näher darauf eingegangen, wieso ein Dreieck, welches nur auf einer seiner Schwerlinien 'getragen' wird, im 'Gleichgewicht' stehen muß.).
Wenn ich mich entscheiden sollte, welcher der beiden Beweis mir besser gefällt, würde meine Wahl auf den zweiten fallen. Der erste Beweis ist für mich eigentlich nicht mehr als eine *Verifikation* des Satzes, die mir ermöglicht an das Resultat zu glauben, ohne auf das Wort eines anderen zu vertrauen. Der zweite Beweis gibt mir eher die Chance das Resultat mehr oder weniger gut zu *begreifen* , d.h. durch ihn erfahre ich auch etwas über den/einen 'tieferen Grund' des Satzes.
Eigentlich bin ich davon überzeugt, daß man für jeden Satz einen Beweis finden kann, der das Resultat ähnlich gut erklärt wie der zweite Beweis unseres Satzes. Ein Beispiel, das mich schon seit der Hälfte meines Mathematikstudiums von dieser Einstellung abzubringen versucht, ist der Potenzreihenentwicklungssatz holomorpher Funktionen in $\mathbb{C}$. Bis jetzt ist es mir noch kaum geglückt, dem 'Geheimnis' näher zu kommen, wieso der Satz in $\mathbb{R}$ nicht gilt, in $\mathbb{C}$ aber schon.

Nachdem wir in diesem Kapitel $\mathbb{Q}_p$, den Körper der p-adischen Zahlen kennengelernt haben, kehren wir zu unserer ursprünglichen Problematik rund um Rekurrenzen zurück.
Im nächsten Kapitel wenden wir uns einer algebraischen Eigenschaft von $\mathbb{Q}_p$ zu: Wir werden zeigen, daß es für einen gegebenen Körper K, der endlich erzeugt über $\mathbb{Q}$ ist, unendlich viele Primzahlen gibt, sodaß man sich K als Teilkörper von $\mathbb{Q}_p$ vorstellen kann (d.h. daß es einen Körper $K' \subseteq \mathbb{Q}_p$ gibt, sodaß $K \cong K'$.).
Ist dann eine Rekurrenz $(a_i)_{i\geq 0}$ in einen Körper F der Charakteristik 0 gegeben, so wird man sehen, daß man o.B.d.A. annehmen kann, daß F endlich erzeugt über $\mathbb{Q}$ ist und daher $F \subseteq \mathbb{Q}_p$ für unendlich viele p. Damit hat man das Problem sozusagen nach $\mathbb{Q}_p$ transferiert, d.h. es genügt den Satz in $\mathbb{Q}_p$ zu beweisen. Das gelingt dann in Kapitel 4 relativ schnell und elegant.

Kapitel 3

Verlagerung des Problems in den Körper der p-adischen Zahlen

Das Ziel dieses Kapitels ist der folgende

Satz 3.1 *Es sei K eine endlich erzeugte Körpererweiterung von $\mathbb{Q}$ und C eine endliche Teilmenge von $K \setminus \{0\}$.*
Dann gibt es für unendlich viele Primzahlen p eine Einbettung

$$\alpha_p : K \to \mathbb{Q}_p,$$

sodaß $\|\alpha_p(c)\|_p = 1 \ \forall c \in C$.

3.1 Einige Hilfssätze

Ich erinnere an die Definition der Diskriminante eines Polynoms $f(X)$ über einem Integritätsbereich R (Definition 2.3):
Die Diskriminante $D(f)$ eines Polynoms ist die Determinante des 'Gleichungssystems'

$$u(X)f(X) + v(X)f'(X) = 1,$$

wobei $deg(u) \leq deg(f) - 2$ und $deg(v) \leq deg(f) - 1$.
Es folgt die Existenz zweier Polynome $u(X), v(X) \in R[X]$ mit

$$u(X)f(X) + v(X)f'(X) = D(f).$$

In Abschnitt 2.6 haben wir bereits gesehen, daß im Falle $D(f) \neq 0$ das Polynom $f(X)$ keine mehrfachen Nullstellen haben kann: Angenommen es gäbe ein $x \in M \supseteq R$ mit $f(x) = 0$ und $f'(x) = 0$ ($\Leftrightarrow x$ ist mehrfache Nullstelle von $f(X)$), dann folgt

$$0 = u(x)f(x) + v(x)f'(x) = D(f),$$

und das ist ein Widerspruch.
Umgekehrt haben wir gezeigt, daß im Fall $D(f) = 0$, das Polynom $f(X)$ und seine Ableitung $f'(X)$ nicht unbedingt eine gemeinsame Nullstelle haben müssen, jedoch zumindest einen gemeinsamen Faktor.
Daraus ergibt sich

Hilfssatz 3.1 *Gegeben sei ein Integritätsbereich $R \supseteq \mathbb{Z}$ und K sein Quotientenkörper. Es sei $f(X) \in R[X]$ ein über K irreduzibles, nicht-konstantes Polynom. Dann ist $D(f) \neq 0$.*

Beweis: Das Polynom $f(X)$ und seine Ableitung $f'(X)$ sind teilerfremd in $K[X]$, denn wäre $ggT(f(X), f'(X)) = d(X)$ und $deg(d) \geq 1$, so würde aus der Irreduzibilität von $f(X)$ und $d(X)|f(X)$ die Gleichheit von $f(X)$ und $d(X)$ folgen. Es wäre dann $f(X)|f'(X)$, also $deg(f) \leq deg(f')$ (weil $f(X)$ nicht konstant und daher $f'(X) \not\equiv 0$). Das ist ein Widerspruch zu $deg(f') = deg(f) - 1$ (hier verwenden wir, daß K ein Körper der Charakteristik 0 ist.).

Bemerkung Diesen Hilfssatz benötigen wir später, um Satz 2.6 anzuwenden.
Ist nämlich $f(X) \in \mathbb{Z}[X]$ ein über $\mathbb{Q}$ irreduzibles Polynom, dann ist laut Hilfssatz $D(f) \in \mathbb{Z} \backslash 0$. Es sei p eine Primzahl, die $D(f)$ nicht teilt. Dann ist $D(f) \not\equiv 0 \; mod\, p$ und daher hat $f(X) \; mod\, p$ nur einfache Nullstellen.
(Es gilt nämlich allgemein: Ist $g(X)$ ein beliebiges Polynom über einem Integritätsbereich R, M ein zweiter Integritätsbereich und $\varphi : R \to M$ ein Ringhomomorphismus, dann ist $\varphi(D(g)) = D(\varphi(g))$. Daraus folgt insbesondere, daß $D(f) \; mod\, p$ die Diskriminante von $f(X) \; mod\, p$ ist.)
Nach Satz 2.6 hat $f(X)$ in $\mathbb{Z}_p$ genauso viele Nullstellen, wie $f(X) \; mod\, p$ in $\mathbb{Z}/p\mathbb{Z}$.

Hilfssatz 3.2 *Gegeben seien m Polynome $f_i(X_1, ...X_n) \in \mathbb{Z}[X_1, ...X_n] \setminus \{0\}$, $i = 1, 2, ...m$. Dann gibt es ein n-tupel ganzer Zahlen $(a_1, a_2, ...a_n)$ mit*

$$f_i(a_1, ...a_n) \neq 0 \quad \text{\textit{für} } i = 1, 2, ...m.$$

Beweis: Wir zeigen den Satz mit Induktion nach n.
Induktionsanfang $n = 1$: Nach dem Fundamentalsatz der Algebra hat $f_i(X_1)$ für fixes $i = 1, 2, ...m$ nur endlich viele Nullstellen. Es kann daher nur endlich viele ganze Zahlen geben, die der Bedingung im Hilfssatz nicht genügen. Wegen $|\mathbb{Z}| = \infty$ folgt die Behauptung.
Induktionsschritt $n - 1 \to n$: Es sei $i \in \{1, 2, ...m\}$. Wir fassen $f_i(X_1, ...X_n)$ als Polynom über dem Körper $\mathbb{Q}(X_1, ...X_{n-1})$ in der Variablen X_n auf. Aus dem Fundamentalsatz der Algebra (diesmal auf den Körper $\mathbb{Q}(X_1, ...X_{n-1})$ angewandt) resultiert, daß es nur endlich viele ganze Zahlen a, mit $f_i(X_1, ...X_{n-1}, a) \equiv 0$ gibt. Es existiert daher ein $a_n \in \mathbb{Z}$ mit

$$f_i(X_1, ...X_{n-1}, a_n) \not\equiv 0 \quad i = 1, 2, ..m.$$

Nach Induktionsvoraussetzung gibt es ein $(n-1)$-tupel $(a_1, ...a_{n-1}) \in \mathbb{Z}^{n-1}$ mit

$$f_i(a_1, ...a_{n-1}, a_n) \neq 0 \quad i = 1, 2, ...m. \square$$

Hilfssatz 3.3 *Es sei $g(X) \in \mathbb{Z}[X]$ ein nicht-konstantes Polynom. Dann gibt es unendlich viele Primzahlen p, für die die Kongruenz*

$$g(x) \equiv 0 \ \ mod\, p$$

in $\mathbb{Z}$ lösbar ist.

Beweis: Es sei $g(X) = g_0 + g_1 X + ... + g_n X^n$. Ist $g_0 = 0$, so ist die Kongruenz für jede Primzahl lösbar ($x = 0$).
Wir können daher $g_0 \neq 0$ annehmen. Der Beweis verläuft indirekt: Angenommen $g(x) \equiv 0 \ mod\, p$ ist in $\mathbb{Z}$ nur für endlich viele Primzahlen lösbar. Mit P bezeichne ich die Menge dieser Primzahlen und mit $c = \prod\limits_{p \in P} p$ ihr Produkt.
Weil $g(X)$ ein nicht-konstantes Polynom ist und $g_0 \cdot c \neq 0$, gibt es ein $k \in \mathbb{Z}$ mit $g(g_0 \cdot c \cdot k) \neq \pm g_0$. Wir definieren $r = \frac{g(g_0 \cdot c \cdot k)}{g_0}$. Da $r \neq \pm 1$ existiert ein Primteiler p^* von r.
Laut Definition von r und c gilt

$$r = g_n g_0^{n-1} c^n k^n + g_{n-1} g_0^{n-2} c^{n-1} k^{n-1} + ... + g_1 g_0^0 c \cdot k + 1 \equiv 1 \ \ mod\, p,$$

wenn $p \in P$ und daher $p^* \notin P$.
Setze $b^* = g_0 \cdot c \cdot k$.
Es folgt: $g(b^*) = g(g_0 \cdot c \cdot k) = g_0 r \equiv 0 \ \ mod\, p^*$, ein Widerspruch zu $p^* \notin P$.

Bemerkung Auch dieser Hilfssatz wird uns helfen, Satz 2.6 anzuwenden: Es sei $f(X) \in \mathbb{Z}[X]$ ein über $\mathbb{Q}$ irreduzibles Polynom. In der Bemerkung nach Hilfssatz 3.1 haben wir bereits gesehen, daß dann die Anzahl der Nullstellen von $f(X)$ in $\mathbb{Z}_p$ für fast alle Primzahlen p mit der Anzahl der Nullstellen von $f(X) \ \ mod\, p$ in $\mathbb{Z}/p\mathbb{Z}$ übereinstimmt.
Aus Hilfssatz 3 folgt, daß $f(X) \ \ mod\, p$ für unendlich viele Primzahlen zumindest eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$ besitzt. Insgesamt sehen wir, daß $f(X)$ für unendlich viele Primzahlen p zumindest eine Nullstelle in $\mathbb{Z}_p$ hat.

Hilfssatz 3.4 *Der Körper der p-adischen Zahlen $\mathbb{Q}_p$ hat unendlichen Transzendenzgrad über $\mathbb{Q}$, d.h. es existiert eine unendliche Teilmenge $T \subseteq \mathbb{Q}_p$, sodaß aus $x_1, ...x_k \in T$ und $P(X_1, ...X_k) \in \mathbb{Q}[X_1, ...X_k] \setminus \{0\}$ folgt $P(x_1, ...x_k) \neq 0$ ($\Leftrightarrow x_1, ...x_k$ sind algebraisch unabhängig über $\mathbb{Q}$).*

Beweis: Angenommen es gäbe keine unendliche Teilmenge T mit dieser Eigenschaft. Dann existiert eine endliche Teilmenge $T' \subseteq \mathbb{Q}_p$, die algebraisch unabhängig über $\mathbb{Q}$ ist, sodaß jedes $x \in \mathbb{Q}_p$ algebraisch über $\mathbb{Q}(T')$ (= der kleinste Körper über $\mathbb{Q}$, der T' enthält) ist. Dieser Körper ist abzählbar, weil T' endlich und $\mathbb{Q}$ abzählbar ist. Es gibt daher auch nur abzählbar viele algebraische Zahlen über $\mathbb{Q}(T')$ (da es nur abzählbar viele algebraische Gleichungen über $\mathbb{Q}(T')$ gibt). Der Körper $\mathbb{Q}_p$ wäre daher abzählbar.
Das ist aber nicht der Fall: Wir haben nämlich gesehen, daß zwischen den Elementen von $\mathbb{Q}_p$ und den Folgen $(a_i)_{i \in \mathbb{Z}}$ mit $a_i \in \{0, 1, ...p-1\}$ und $a_i = 0$ für kleine i eine eineindeutige Beziehung besteht. Da es überabzählbar viele solche Folgen gibt, ist auch $\mathbb{Q}_p$ überabzählbar.

3.2 Beweis des Satzes

Da $K/\mathbb{Q}$ eine endlich erzeugte Erweiterung ist, folgt aus einer einfachen Verallgemeinerung des Satzes vom primitiven Element, daß es Elemente $x_1, x_2, ...x_m \in K$ gibt, die algebraisch unabhängig über $\mathbb{Q}$ sind, und ein 'primitives' Element $y \in K$ existiert, welches algebraisch über $\mathbb{Q}(x_1, x_2, ...x_m)$ ist, sodaß

$$K = \mathbb{Q}(x_1, x_2, ...x_m)[y].$$

Die Idee des Beweises von Satz 3.1 ist relativ einfach: Da eine Einbettung $\alpha_p : K \to \mathbb{Q}_p$ durch die Bilder der Elemente $x_1, ...x_m, y$ eindeutig bestimmt ist, genügt es, grob gesagt, zu zeigen, daß in $\mathbb{Q}_p$ m über $\mathbb{Q}$ algebraisch unabhängige Zahlen liegen (die dann die Bilder von $x_1, ...x_m$ sein werden; das haben wir schon in Hilfssatz 3.4 gezeigt), und daß das Bild des Minimalpolynoms von y über $\mathbb{Q}(x_1, ...x_m)$ in $\mathbb{Q}_p$ lösbar ist (diese Lösung wird dann das Bild von y unter α_p sein; wir haben das im wesentlichen schon mit Satz 2.6, Hilfssatz 3.1 und Hilfssatz 3.3 gezeigt).
Was diesen Beweis zunächst etwas undurchschaubar macht, ist unter anderem der Aufwand, den man betreiben muß, um die zusätzliche Bedingung für die Bilder der Menge $C \subseteq K \setminus \{0\}$ herzuleiten.

Beweis Wir dürfen o.B.d.A. annehmen, daß mit jedem $c \in C$ auch sein Inverses c^{-1} in C liegt (hier verwenden wir $0 \notin C$). Es genügt daher zu zeigen, daß $\|\alpha_p(c)\|_p \leq 1 \quad \forall c \in C$ $(\|\alpha_p(c)\|_p \leq 1 \wedge \|\alpha_p(c^{-1})\|_p \leq 1 \Rightarrow \|\alpha_p(c)\|_p = 1)$.
Jedes $c \in C$ besitzt eine Darstellung der Form

$$c = \frac{U_c(y, x_1, ...x_m)}{V_c(x_1, ...x_m)},$$

wobei $U_c(Y, X_1, ...X_m) \in \mathbb{Z}[Y, X_1, ...X_m] \setminus \{0\}$ und $V_c(X_1, ...X_m) \in \mathbb{Z}[X_1, ...X_m] \setminus \{0\}$.

Es sei $G(Y)$ irreduzibel über $\mathbb{Q}(x_1, ...x_m)$,sodaß

$$G(y) = 0.$$

Da $\mathbb{Q}(X_1, ...X_m)$ der Quotientenkörper von $\mathbb{Z}[X_1, ...X_m]$ ist, können wir o.B.d.A. annehmen, daß

$$G(Y) = H(Y, x_1, ...x_m), \text{ wobei } H(Y, X_1, ...X_m) \in \mathbb{Z}[Y, X_1, ...X_m].$$

Es sei s der Grad des Polynoms H in der Unbestimmten Y (d.h. $s = deg(G)$). Wir bezeichnen den Koeffizienten von Y^s in $H(Y, X_1, ...X_m)$ mit $H_0(X_1, ...X_m)$.

$D(G)$ sei die Diskriminante des Polynoms $G(Y)$ über dem Integritätsbereich $\mathbb{Z}[x_1, ...x_m]$. Wähle $D(X_1, ...X_m) \in \mathbb{Z}[X_1, ...X_m]$, sodaß $D(x_1, ...x_m) = D(G)$. Da $G(Y)$ irreduzibel über $\mathbb{Q}(x_1, ...x_m)$, dem Quotientenkörper von $\mathbb{Z}[x_1, ...x_m]$, ist, folgt $D(x_1, ...x_m) \neq 0$ (Hilfssatz 3.1) und daher $D(X_1, ...X_m) \not\equiv 0$.

Nach Hilfssatz 3.2 gibt es ein m-tupel $(a_1, ...a_m) \in \mathbb{Z}^m$ mit

$$\begin{aligned} &D(a_1, ...a_m) \neq 0 \\ &H_0(a_1, ...a_m) \neq 0 \\ &V_c(a_1, ...a_m) \neq 0 \qquad \forall c \in C \end{aligned}$$

Wegen $H_0(a_1, ...a_m) \neq 0$, ist $H(Y, a_1, ...a_m) \in \mathbb{Z}[Y]$ nicht konstant. Es gibt daher unendlich viele Primzahlen p, sodaß

$$H(Y, a_1, ...a_m) \equiv 0 \ \ mod\, p \tag{3.1}$$

in $\mathbb{Z}$ lösbar ist (Hilfssatz 3.3).
Da $D(a_1, ...a_m) \equiv 0 \ \ mod\, p$ oder $V_c(a_1, ...a_m) \equiv 0 \ \ mod\, p$ für ein $c \in C$ höchstens endlich viele Primzahlen erfüllen (nämlich gerade die Primteiler von $D(a_1, ...a_m)$ und $V_c(a_1, ...a_m)$), gibt es eine unendliche Menge P von Primzahlen p, für die (3.1) lösbar ist und

$$\begin{aligned} &D(a_1, ...a_m) \not\equiv 0 \ \ mod\, p \\ &V_c(a_1, ...a_m) \not\equiv 0 \ \ mod\, p \qquad \forall c \in C. \end{aligned}$$

Im Folgenden sei $p \in P$.

Aus Hilfssatz 3.4 folgt, daß wir m über $\mathbb{Q}$ algebraisch unabhängige Zahlen $\theta_1, ...\theta_m \in \mathbb{Q}_p$ wählen können. Dabei dürfen wir o.B.d.A. annehmen, daß $\|\theta_i\|_p < 1$ für $i = 1, 2, ...m$, denn erfüllten die $\theta_i' s$ diese Bedingung nicht, dann erhielten wir durch Multiplikation mit einer passenden Potenz von p algebraisch unabhängige Elemente mit dieser Eigenschaft.
Wir setzen $\zeta_i := a_i + \theta_i$ für $i = 1, ...m$.
Wegen $a_i, \theta_i \in \mathbb{Z}_p$ folgt $\zeta_i \in \mathbb{Z}_p$. Außerdem ist die Menge $\{\zeta_1, ...\zeta_m\}$ auch algebraisch unabhängig über $\mathbb{Q}$.

Wähle $b \in \mathbb{Z}$ sodaß

$$H(b, a_1, ...a_m) \equiv 0 \ \ mod\, p.$$

Mit anderen Worten: $\|H(b, a_1, ...a_m)\|_p \leq \frac{1}{p} < 1$

Die Differenz $H(b, X_1, ...X_m) - H(b, Y_1, ...Y_m)$ kann auch als Polynom über $\mathbb{Z}$ in den Variablen $(X_1 - Y_1), (X_2 - Y_2), ...(X_m - Y_m), Y_1, Y_2, ...Y_m$ aufgefaßt werden, wobei in jedem Monom ein Faktor in den Variablen $(X_1 - Y_1), (X_2 - Y_2), ...(X_m - Y_m)$ vorkommt. Daraus und aus der Tatsache, daß die offene Einheitskugel ein Ideal in $\mathbb{Z}_p$ ist, folgt

$$\|H(b, \zeta_1, ...\zeta_m) - H(b, a_1, ...a_m)\|_p < 1.$$

(Wir setzen $X_i := \zeta_i$, $Y_i := a_i$ und verwenden $\|\zeta_i - a_i\|_p = \|\theta_i\|_p < 1$.)
Es folgt

$$\|H(b, \zeta_1, ...\zeta_m)\|_p \leq \max\{\|H(b, \zeta_1, ...\zeta_m) - H(b, a_1, ...a_m)\|_p, \|H(b, a_1, ...a_m)\|_p\} < 1$$

d.h. $H(b, \zeta_1, ...\zeta_m) \equiv 0 \ \ mod\, p$. (Es gilt nämlich: Ist $z \in \mathbb{Z}_p$ und $\|z\|_p < 1$, dann folgt $\|z\| \leq \frac{1}{p}$, da $\{\|x\|_p | x \in \mathbb{Q}_p\} = \{p^n | n \in \mathbb{Z}\} \cup \{0\}$. Daher ist $z \equiv 0 \ \ mod\, p$.)

Man zeigt $\|D(\zeta_1, ...\zeta_m) - D(a_1, ...a_m)\|_p < 1$ genauso, wie wir das bei der analogen Beziehung für das Polynom H gemacht haben.
Aus Hilfssatz 2.1 folgt dann $\|D(\zeta_1, ...\zeta_m)\|_p = 1$, wenn wir $a = D(a_1, ...a_m)$ und $b = D(\zeta_1, ...\zeta_m) - D(a_1, ...a_m)$ setzen (weil $a \not\equiv 0 \mod p$ und daher $\|a\|_p = 1 > \|b\|_p$).

Das Polynom $H(X, \zeta_1, ...\zeta_m)$ ist eines über $\mathbb{Z}_p$ und hat $mod\, p$ keine mehrfachen Nullstellen: Die Diskriminante von $H(X, \zeta_1, ...\zeta_m)$ beträgt $D(\zeta_1, ...\zeta_m)$, und daher ist $D(\zeta_1, ...\zeta_m) \mod p$ die Diskriminante von $H(X, \zeta_1, ...\zeta_m) \mod p$ (siehe Bemerkung nach Hilfssatz 3.3). Wegen $\|D(\zeta_1, ...\zeta_m)\|_p = 1$ ist $D(\zeta_1, ...\zeta_m) \not\equiv 0 \mod p$ und $H(X, \zeta_1, ...\zeta_m) \mod p$ kann daher keine mehrfachen Nullstellen haben.

Nach Satz 2.6 gibt es ein ganze p-adische Zahl $\eta \equiv b \mod p$, mit

$$H(\eta, \zeta_1, ...\zeta_m) = 0.$$

Jetzt sind wir in der Lage die Einbettung $\alpha_p : K \to \mathbb{Q}_p$ zu definieren:

$$\begin{aligned} \alpha_p|_{\mathbb{Q}} &= id_{\mathbb{Q}} \\ \alpha_p(x_i) &= \zeta_i \\ \alpha_p(y) &= \eta \end{aligned}$$

(Diese Einbettung ist wohldefiniert, weil die $\zeta_i's$, wie die $x_i's$, algebraisch unabhängig über $\mathbb{Q}$ sind, und η 'demselben Polynom' (d.h. dessen Bild unter α_p) wie y genügt.)

Es bleibt zu zeigen:

$$\|\alpha_p(c)\|_p \leq 1 \quad \forall c \in C$$

Laut Definition der Einbettung ist

$$\alpha_p(c) = \frac{U_c(\eta, \zeta_1, ...\zeta_m)}{V_c(\zeta_1, ...\zeta_m)} \quad \forall c \in C$$

Wegen $\eta, \zeta_1, ...\zeta_m \in \mathbb{Z}_p$ liegen Zähler und Nenner dieser Darstellung von $\alpha_p(c)$ in $\mathbb{Z}_p$. Für den Zähler gilt sogar $\|V_c(\zeta_1, ...\zeta_m)\|_p = 1$ (das zeigt man genauso wie $\|D(\zeta_1, ...\zeta_m)\|_p = 1$.).
Es folgt das Gewünschte:

$$\|\alpha_p(c)\|_p = \frac{\|U_c(\eta, \zeta_1, ...\zeta_m)\|_p}{\|V_c(\zeta_1, ...\zeta_m)\|_p} = \|U_c(\eta, \zeta_1, ...\zeta_m)\|_p \leq 1$$

3.3 Anwendung des Satzes auf unser Problem

In Kapitel 1 sind wir von einer Rekurrenz $(a_n)_{n\geq 0}$ in einem Körper K ($char(K) = 0$) ausgegangen. Wir haben gezeigt, daß eine algebraische Erweiterung $L \supseteq K$ existiert, sodaß es $\alpha_1, ...\alpha_k \in L$ und Polynome $A_1(X), ...A_k(X) \in L[X]$ gibt, mit $a_n = \sum\limits_{i=1}^{k} A_i(n)\alpha_i^n$ für

$n = 1, 2, 3, \ldots$.
Es sei $F \supseteq \mathbb{Q}$ der kleinste Teilkörper von L, der die Elemente $\alpha_1, \ldots \alpha_k$ und die Koeffizienten von $A_1(X), \ldots A_k(X)$ enthält. Dieser Körper ist endlich erzeugt über $\mathbb{Q}$. Außerdem ist in ihm das Exponentialpolynom $\sum_{i=1}^{k} A_i(n)\alpha_i^n$ definiert und damit auch die Rekurrenz $(a_n)_{n\geq 0}$.
Der in diesem Kapitel gezeigte Satz ergibt, daß F als Teilkörper von $\mathbb{Q}_p$ (für unendlich viele Primzahlen p) interpretierbar ist. (Wir werden später sehen, daß es an dieser Stelle notwendig ist, p und α_p so zu wählen, daß $\|\alpha_i\|_p = 1$ für $i = 1, \ldots k$. Dazu haben wir die zusätzliche Bedingung über die endliche Teilmenge C im Satz 3.1 bewiesen.)
Somit ist $(a_n)_{n\geq 0}$ eine Rekurrenz in $\mathbb{Q}_p$ und der Übergang geschafft.

Kapitel 4

Lösung des Problems im Körper der p-adischen Zahlen

Wir haben eben gesehen, daß alles auf die Untersuchung (spezieller) Exponentialpolynome über $\mathbb{Q}_p$ hinausläuft.
Ist $B_1(X)\beta_1^X + ... + B_m(X)\beta_m^X$ ein beliebiges Exponentialpolynom über $\mathbb{C}$ [1], so gibt es eine auf $\mathbb{C}$ konvergente Potenzreihe $b(X)$ mit

$$b(n) = B_1(n)\beta_1^n + ... + B_m(n)\beta_m^n \quad \forall n \in \mathbb{N}.$$

(Das folgt aus der Potenzreihenentwicklung der Exponentialfunktion $x \mapsto e^x$, die die Potenzreihenentwicklung von $x \mapsto \beta_i^x = e^{log(\beta_i)x}$ ergibt.)
Für p-adische Exponentialpolynome $A_1(X)\alpha_1^X + ... + A_m(X)\alpha_m^X$ wollen wir in diesem Kapitel etwas Ähnliches zeigen. Wir werden dafür dieselben Methoden wie in $\mathbb{C}$ verwenden. Der Unterschied wird aber sein, daß in $\mathbb{Q}_p$ nicht jedes Exponentialpolynom durch eine p-adische Potenzreihe charakterisierbar ist. Unsere Exponentialpolynome, bei denen $\|\alpha_i\|_p = 1$ für $i = 1, 2, ...m$, werden wir aber zumindest durch endlich viele Potenzreihen auf $\mathbb{Z}_p$ fortsetzen können.
Eine weitere Einschränkung bezüglich der Potenzreihenentwicklung p-adischer Exponentialpolynome im Vergleich zu den komplexen ist, daß sie im allgemeinen nicht auf ganz $\mathbb{Q}_p$ konvergieren, sonderen nur auf $\mathbb{Z}_p$. Das erscheint einem aber ganz natürlich, wenn man beachtet, daß bei den komplexen Zahlen der kleinste Kreis um den Nullpunkt, der die natürlichen Zahlen enthält, $\mathbb{C}$ selbst ist, während in $\mathbb{Q}_p$ der Einheitskreis $\mathbb{Z}_p$ diese Eigenschaft bereits erfüllt. (Kreise um den Nullpunkt sind ja die Konvergenzgebiete von Potenzreihen; für p-adische

[1] Jedes Exponentialpolynom über einem Körper der Charakteristik Null kann man in $\mathbb{C}$ einbetten, da man jeden endlich erzeugten Körper K über $\mathbb{Q}$ als Teilkörper der komplexen Zahlen interpretieren kann. Das zeigt man ähnlich wie Satz 3.1: Analog zu Hilfssatz 3.4 folgt aus der Überabzählbarkeit von $\mathbb{C}$ der unendliche Transzendenzgrad über $\mathbb{Q}$ und statt des Henselschen Lemmas, Hilfssatz 3.1 und Hilfssatz 3.3 verwenden wir die algebraische Abgeschlossenheit von $\mathbb{C}$, die alles viel einfacher macht.
Die Bedingung an die endliche Teilmenge $C \subseteq K \setminus \{0\}$ kann man aber bei $\mathbb{C}$ nicht immer erreichen: Ist z.B. $C = \{2\}$, so muß $|\alpha(2)| = 2$ sein, wenn $\alpha : K \to \mathbb{C}$ die Einbettung bezeichnet.

Potenzreihen werden wir das in Abschnitt 4.1 zeigen.) Insbesondere sind die natürlichen Zahlen daher eine beschränkte Teilmenge von $\mathbb{Q}_p$. Das Interessante ist, daß diese Tatsache, die für das beschriebene Manko der Potenzreihenentwicklung der p-adischen Exponentialfunktion verantwortlich ist, letztendlich der Grund dafür sein wird, daß man den Satz von Skolem-Mahler-Lech für p-adische Exponentialpolynome im Wesentlichen durch ihre Potenzreihenentwicklung beweisen kann, hingegen man in $\mathbb{C}$ mit der Potenzreihenentwicklung alleine nicht zum Ziel kommt.

Im ersten Abschnitt dieses Kapitels beschäftigen wir uns zunächst mit einigen grundlegenden Eigenschaften p-adischer Potenzreihen:

4.1 Potenzreihen über $\mathbb{Q}_p$

Unter einer Potenzreihe über $\mathbb{Q}_p$ um den 'Mittelpunkt' 0 versteht man bekanntlich einen Ausdruck der Form

$$f(X) = f_0 + f_1 X + f_2 X^2 + ... = \sum_{i=0}^{\infty} f_i X^i \quad ,$$

wobei $f_i \in \mathbb{Q}_p$, $i = 0, 1, 2...$.
Ist $\mathcal{D}$ die Menge aller p-adischen Zahlen x, für die $\left(\sum\limits_{i=0}^{N} f_i x^i\right)_{N \geq 0}$ konvergiert, so ist durch die Potenzreihe eine Funktion $f : \mathcal{D} \mapsto \mathbb{Q}_p$ gegeben.

Über dieses Konvergenzgebiet $\mathcal{D}$ kann man, ähnlich wie in $\mathbb{C}$, eine recht allgemeine Aussage treffen:
Ist $\sum\limits_{i=0}^{\infty} g_i x^i$ eine Potenzreihe über $\mathbb{C}$, dann ist $R = \frac{1}{\limsup\limits_{n\to\infty} |g_n|^{\frac{1}{n}}}$ der Konvergenzradius dieser Potenzreihe, d.h. die Reihe konvergiert für $|x| < R$ und divergiert wenn $|x| > R$. Über das Verhalten für $|x| = R$ kann man so allgemein nichts aussagen.

In $\mathbb{Q}_p$: $R = \frac{1}{\limsup\limits_{n\to\infty} \|f_n\|_p^{\frac{1}{n}}}$ ist der Konvergenzradius der Potenzreihe $\sum\limits_{i=0}^{\infty} f_i x^i$ über $\mathbb{Q}_p$ im selben Sinn.
Zum Unterschied von $\mathbb{C}$ gilt hier: Die Potenzreihe $\sum\limits_{i=0}^{\infty} f_i x^i$ konvergiert für alle x mit $\|x\|_p = R \Leftrightarrow \|f_i\|_p R^i \overset{i\to\infty}{\to} 0$ und konvergiert für kein x mit $\|x\|_p = R \Leftrightarrow \|f_i\|_p R^i \overset{i\to\infty}{\not\to} 0$. Daraus folgt insbesondere: Gibt es ein $x_0 \in \mathbb{Q}_p$, mit $\|x_0\|_p = R$ und $\sum\limits_{i=0}^{\infty} f_i x_0^i$ ist konvergent, dann konvergiert die Potenzreihe für alle x mit $\|x\|_p = R$. (In $\mathbb{C}$ widerspricht zum Beispiel die Potenzreihe $\sum\limits_{i=1}^{\infty} \frac{z^i}{i}$ dieser Äquivalenz: Ihr Konvergenzradius $R = 1$, jedoch konvergiert die Reihe für $z = -1$ und divergiert wenn $z = 1$.)
Es gilt daher der folgende

Satz 4.1 *Es sei* $f(X) = \sum_{i=0}^{\infty} f_i X^i$ *eine Potenzreihe über* $\mathbb{Q}_p$, $\mathcal{D}$ *ihr Konvergenzgebiet und* $R = \frac{1}{\limsup\limits_{n\to\infty} \|f_n\|_p^{\frac{1}{n}}}$. *Dann kann man über das Konvergenzverhalten der Potenzreihe folgende Aussagen treffen:*

(1) $\mathcal{D} = \{0\} \Leftrightarrow R = 0$

(2) $\mathcal{D} = \mathbb{Q}_p \Leftrightarrow R = \infty$

(3) Wenn $0 < R < \infty$, *dann ist*

$$\mathcal{D} = \{a \in \mathbb{Q}_p \,|\, \|a\|_p \leq R\} \Leftrightarrow \|f_n\|_p R^n \to 0$$

und

$$\mathcal{D} = \{a \in \mathbb{Q}_p \,|\, \|a\|_p < R\} \Leftrightarrow \|f_n\|_p R^n \not\to 0.$$

Beweis: Laut Hilfssatz 2.3 konvergiert $\sum_{i=0}^{\infty} f_i a^i \Leftrightarrow \|f_i a^i\|_p \overset{i\to\infty}{\to} 0 \Leftrightarrow \|f_i\|_p \|a\|_p^i \to 0 \Leftarrow \exists q < 1 : \|f_i\|_p \|a\|_p^i \leq q^i$ für fast alle i $\Leftrightarrow q < 1 : \|f_i\|_p^{\frac{1}{i}} \|a\|_p \leq q$ für fast alle i $\Leftrightarrow \exists q < 1 : \|a\|_p < \frac{q}{\|f_i\|_p^{\frac{1}{i}}}$ für fast alle i $\Leftarrow \|a\|_p < R$, d.h wenn $\|a\|_p < R$, dann konvergiert $\sum_{i=0}^{\infty} f_i a^i$.

Ganz ähnlich zeigt man: Ist $\|a\|_p > R \Rightarrow \sum_{i=0}^{\infty} f_i a^i$ divergiert.

Die Aussage über den 'Rand des Konvergenzgebietes', d.h über jene a mit $\|a\|_p = R$, folgt unmittelbar aus Hilfssatz 2.3:

$$\sum_{i=0}^{\infty} f_i a^i \text{ konvergiert} \quad \Leftrightarrow \quad \|f_i a^i\|_p = \|f_i\|_p R^i \overset{i\to\infty}{\to} 0. \quad \square$$

Bemerkungen

(1) Der Beweis in $\mathbb{C}$ funktioniert im wesentlichen genauso. Der einzige Unterschied besteht darin, daß man dort nicht Hilfssatz 2.3 zur Verfügung hat und aus diesem Grund etwas vorsichtiger argumentieren muß (man verwendet das Wurzelkriterium).

(2) Die Aussage über den Rand des Konvergenzgebietes läßt sich in $\mathbb{C}$ natürlich nicht analog zeigen, da sie dort, wie gesagt, i.a. nicht erfüllt ist. Das ist einer der wenigen Unterschiede zur gewöhnlichen Analysis, einmal abgesehen von den direkten Folgerungen aus der ultrametrischen Ungleichung, die wir in dieser Arbeit kennenlernen werden. Es ist allerdings ein Unterschied, den wir nicht benötigen werden, d.h. das schwächere Analogon aus der gewöhnliche Analysis, das keine Aussage über den Rand des Konvergenzgebietes macht, wäre in unserem Fall auch ausreichend.

(3) Das Konvergenzgebiet $\mathcal{D}$ einer p-adischen Potenzreihe ist also immer eine (abgeschlossene oder offene) Kugel. Aus Abschnitt 2.7 folgt, daß $\mathcal{D}$ eine Gruppe bezüglich der Addition ist.

(4) Noch etwas zum unspektakulären Verhalten p-adischer Potenzreihen am Rand ihres Konvergenzgebietes: In Abschnitt 2.7 haben wir außerdem gezeigt, daß bei p-adischen Kugeln $B_r(a) = \{c \in \mathbb{Q}_p | \|c-a\|_p \leq r\}$ die eigenartige Situation vorherrscht, daß jeder 'Punkt' $b \in B_r(a)$ 'Mittelpunkt' dieser Kugel ist, d.h. $B_r(b) = B_r(a)$. Insbesondere bedeutet das, daß jeder 'Randpunkt' c der Kugel (i.e. $\|c-a\| = r$) bezüglich des Mittelpunktes a zugleich auch im 'Innersten' der Kugel liegt, weil c Mittelpunkt und a sogar Randpunkt bezüglich dieses Mittelpunktes c ist. Die Begriffe 'Mittelpunkt' und 'Randpunkt' sind in p-adischen Kugeln daher relativ. Man kann aus diesem Grund auch nicht vom 'Rand' eines Konvergenzgebietes $\mathcal{D}$ im selben Sinn wie in $\mathbb{C}$ sprechen und wird sich daher auch kein Ausnahmeverhalten auf ihm erwarten.

In diesem Zusammenhang ist auch noch interessant, daß der topologische Rand einer 'abgeschlossenen' Kugel $B_r(a) = \{c \in \mathbb{Q}_p | \|c-a\|_p \leq r\}$ leer ist. Wie eben erwähnt, ist ja jeder Punkt von $B_r(a)$ innerer Punkt und damit ist $B_r(a)$ eine offene Menge. Andererseits ist $B_r(a)$ auch abgeschlossen: Es sei $(a_n)_{n\geq 0}$ eine Folge mit $\|a_n - a\|_p \leq r$ und $\lim\limits_{n\to\infty} a_n = \alpha$. Es folgt

$$r \geq \lim_{n\to\infty} \|a_n - a\|_p = \|\alpha - a\|_p$$

und daher $\alpha \in B_r(a)$. Der Rand $\partial B_r(a) = \overline{B_r(a)} \setminus B_r(a)^\circ = B_r(a) \setminus B_r(a) = \emptyset$ ist also leer.

Dasselbe gilt für 'offene' p-adische Kugeln $K_r(a) = \{c \in \mathbb{Q}_p | \|c-a\|_p < r\}$, denn wegen $\{\|z\|_p | z \in \mathbb{Q}\} = \{p^n | n \in \mathbb{Z}\} \cup \{0\}$ ist $K_r(a)$ auch eine 'abgeschlossene' Kugel: Es sei $n \in \mathbb{Z}$ maximal, sodaß $p^n < r$. Dann folgt $K_r(a) = B_{p^n}(a)$, weil es keine p-adische Zahl gibt, deren p-adischer Absolutbetrag echt zwischen p^n und r liegt.

Das zweite und zugleich letzte Ergebnis, das wir in diesem Abschnitt über Potenzreihen herleiten wollen, ist die Stetigkeit auf ihrem Konvergenzgebiet. Dazu benötigen wir zwei Hilfssätze.
Der erste Hilfssatz ist das Analogon zum Cauchyschen Doppelreihensatz in $\mathbb{C}$. Allerdings gilt er in $\mathbb{Q}_p$ in einer viel stärkeren Form, sodaß er auch gut in Abschnitt 2.7 über unerwartete Folgerungen der ultrametrischen Ungleichung gepaßt hätte.

Hilfssatz 4.1 *Es sei $(b_{ij})_{i\geq 0, j\geq 0}$ eine Doppelfolge in $\mathbb{Q}_p$. Angenommen für alle $\varepsilon > 0$ existiere eine natürliche Zahl $J(\varepsilon)$, sodaß $\|b_{ij}\|_p < \varepsilon$, wenn $\max\{i,j\} \geq J(\varepsilon)$.*
Dann konvergieren die Doppelreihen $\sum\limits_{i=0}^{\infty}\sum\limits_{j=0}^{\infty} b_{ij}$ und $\sum\limits_{j=0}^{\infty}\sum\limits_{i=0}^{\infty} b_{ij}$ gegen dieselbe p-adische Zahl.

Beweis: Aus Hilfssatz 2.3 und der Bedingung an die Doppelfolge ergibt sich, daß $\left(\sum\limits_{j=0}^{N} b_{ij}\right)_{N\geq 0}$ für jedes $i \in \mathbb{N}$ konvergiert.
Es gilt

$$\|\sum_{j=0}^{\infty} b_{ij}\|_p = \lim_{N\to\infty} \|\sum_{j=0}^{N} b_{ij}\|_p \leq \sup_{N\in\mathbb{N}} \max_{j\in\{0,1,..N\}} \|b_{ij}\|_p = \sup_{j\in\mathbb{N}} \|b_{ij}\|_p < \varepsilon,$$

wenn $i \geq J(\varepsilon)$.
Gemeinsam mit Hilfssatz 2.3 folgt daraus die Konvergenz von

$$\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right).$$

Aus Symmetriegründen ist auch

$$\sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)$$

konvergent.
Es folgt

$$\begin{aligned}
\|\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} b_{ij} - \sum_{i=0}^{N}\sum_{j=0}^{N} b_{ij}\|_p &= \|\sum_{i=N+1}^{\infty}\sum_{j=0}^{\infty} b_{ij} + \sum_{i=0}^{N}\sum_{j=N+1}^{\infty} b_{ij}\|_p \leq \\
&\leq \max_{\substack{i,j \\ \max\{i,j\}\geq N}} \|b_{ij}\|_p \leq \max_{\substack{i,j \\ \max\{i,j\}\geq J(\varepsilon)}} \|b_{ij}\|_p < \varepsilon
\end{aligned}$$

wenn $N \geq J(\varepsilon)$ und analog

$$\|\sum_{j=0}^{\infty}\sum_{i=0}^{\infty} b_{ij} - \sum_{j=0}^{N}\sum_{i=0}^{N} b_{ij}\| < \varepsilon \quad \forall N \geq J(\varepsilon).$$

Mit anderen Worten:

$$\sum_{i=0}^{N}\sum_{j=0}^{N} b_{ij} \stackrel{N\to\infty}{\rightarrow} \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} b_{ij}$$

und

$$\sum_{j=0}^{N}\sum_{i=0}^{N} b_{ij} \stackrel{N\to\infty}{\rightarrow} \sum_{j=0}^{\infty}\sum_{i=0}^{\infty} b_{ij}.$$

Das gemeinsam mit

$$\sum_{j=0}^{N}\sum_{i=0}^{N} b_{ij} = \sum_{i=0}^{N}\sum_{j=0}^{N} b_{ij}$$

ergibt die Behauptung. □

Hilfssatz 4.2 (Translationssatz) *Es sei $f(X) = f_0 + f_1X + f_2X^2 + \ldots$ eine Potenzreihe über $\mathbb{Q}_p$ und $\mathcal{D}$ ihr Konvergenzgebiet. Wähle $c \in \mathcal{D}$ und setze*

$$g_m := \sum_{n=m}^{\infty}\binom{n}{m} f_n c^{n-m}$$

für $m = 0, 1, 2, \ldots$. Dann ist $\mathcal{D}$ auch das Konvergenzgebiet der Potenzreihe $g(X) = g_0 + g_1X + g_2X^2 + \ldots$ und es gilt $f(b+c) = g(b) \quad \forall b \in \mathcal{D}$.

Beweis: Zunächst müssen wir zeigen, daß g_m wohldefiniert ist:

$$\left\| \binom{n}{m} f_n c^{n-m} \right\|_p = \left\| \binom{n}{m} \right\|_p \|f_n c^{n-m}\|_p \le 1 \cdot \|f_n c^{n-m}\|_p \overset{n\to\infty}{\to} 0.$$

($\|f_n c^n\|_p \to 0$, wenn $n \to \infty$, da $c \in \mathcal{D}$) Wiederum aus Hilfssatz 2.3 folgt daraus die Konvergenz der Reihe, die g_m definiert.
Es sei $b \in \mathcal{D}$ beliebig. Aus Bemerkung (3) nach Satz 4.1 folgt $b + c \in \mathcal{D}$. Die Rechnung

$$\begin{aligned} f(b+c) = \sum_{n=0}^{\infty} f_n (b+c)^n = \sum_{n=0}^{\infty} \sum_{m=0}^{n} \binom{n}{m} f_n c^{n-m} b^m &= \\ \overset{\text{Hilfssatz 4.1}}{=} \sum_{m=0}^{\infty} \left(\sum_{m=n}^{\infty} \binom{n}{m} f_n c^{n-m} \right) b^m &= g(b) \end{aligned}$$

ergibt die Konvergenz von $g(b)$.
(Die Summen darf man vertauschen: Setze $z_{nm} = \binom{n}{m} f_n c^{n-m} b^m$. Dann erfüllt die Doppelfolge $(z_{nm})_{n\ge0,m\ge0}$ die Voraussetzung von Hilfssatz 4.1, weil $\lim\limits_{n\to\infty} z_{nm} = 0$, wegen $c \in \mathcal{D}$, und $z_{nm} = 0$, wenn $m > n$.)
Es sei umgekehrt $b \in \mathbb{Q}_p$, sodaß $g(b)$ konvergiert. Lese obige Gleichung von rechts nach links. Es folgt: $b + c \in \mathcal{D}$. Also $b = (b + c) + (-c) \in \mathcal{D}$. □

Bemerkung Auch dieser Satz hat wieder ein schwächeres Analogon in der gewöhnlichen Analysis: Es seien $f(X)$ und $g(X)$ zwei Potenzreihen wie in Hilfssatz 4.2, nur über $\mathbb{C}$, und R der Konvergenradius von $f(X)$. Dann gilt für den Konvergenzradius R' von $g(X)$: $R' \ge R - |c|$. Diesen Satz beweist man analog mit Hilfe des Cauchyschen Doppelreihensatzes.
Liegt c insbesondere am Rand des Konvergenzgebietes, d.h. $\|c\|_p = R$, so sagt dieses Analogon in $\mathbb{C}$ (zum Unterschied von $\mathbb{Q}_p$) nichts aus.
Für den Beweis des Stetigkeitssatzes für p-adische Potenzreihen würde auch diese schwächere Version des Translationssatzes genügen (siehe Bemerkung nach Satz 4.2). Wir werden Hilfssatz 4.2 aber später noch einmal im Beweis des Satzes von Strassmann benötigen, und an dieser Stelle wäre das schwächere Analogon aus der gewöhnlichen Analysis, übertragen auf $\mathbb{Q}_p$, zuwenig. Das wird übrigens das einzige Mal sein, wo wir den Unterschied zur Analysis auf Basis der Dreiecksungleichung wirklich unbedingt benötigen.

Satz 4.2 *Eine Potenzreihe $f(X) = f_0 + f_1 X + f_2 X^2 + ...$ stellt auf ihrem Konvergenzgebiet $\mathcal{D}$ eine stetige Funktion dar.*

Beweis: Es sei $c \in \mathcal{D}$. Nach Hilfssatz 2 existiert eine auf $\mathcal{D}$ konvergente Potenzreihe $g(X) = g_0 + g_1 X + g_2 X^2 + ...$ mit $f(b + c) = g(b) \quad \forall b \in \mathcal{D}$. Wir müssen daher nur zeigen, daß $g(X)$ in 0 stetig ist, d.h. $\lim\limits_{\substack{x\to0\\x\in\mathcal{D}}} \|g(x) - g(0)\|_p = 0$.
Wegen $\|g(x) - g(0)\|_p = \|x\|_p \|g_1 + g_2 x + g_3 x^2 ...\|_p$ genügt es zu zeigen, daß $x \mapsto g_1 + g_2 x + g_3 x^2 ...$ in einer Umgebung von 0 beschränkt ist.

Es sei $r > 0$, sodaß $B_r(0) \subseteq \mathcal{D}$ und $x \in B_r(0)$. (Wenn $\mathcal{D} = \{0\}$ geht das nicht. Dann ist der Satz aber trivial.) Es folgt

$$\|g_1 + g_2 x + g_3 x^3 ...\|_p \leq \sup_{n\geq 1} \|g_n x^{n-1}\|_p = \sup_{n\geq 1} \|g_n\|_p \|x\|_p^{n-1} \leq \sup_{n\geq 1} \|g_n\|_p \|r^{n-1}\|_p < \infty,$$

weil $\sum\limits_{n=1}^{\infty} g_n r^{n-1}$ konvergiert und daher insbesondere $\|g_n r^{n-1}\|_p \overset{n\to\infty}{\to} 0$. □

Bemerkung Satz 4.2 gilt ganz analog in $\mathbb{C}$. Man beweist ihn für das Innere des Konvergenzgebietes genauso wie wir es eben in $\mathbb{Q}_p$ getan haben (die schwächeren Analoga der Hilfssätze 4.1 und 4.2 genügen dabei). Um die Stetigkeit auch am Rand des Konvergenzgebietes zu zeigen, d.h. für jene $x \in \mathcal{D}$ mit $|x| = R$, genügen diese Überlegungen nicht. In $\mathbb{C}$ hat man dafür den Abelschen Grenzwertsatz.
Trotzdem könnten wir Satz 4.2 für $\mathbb{Q}_p$ auch beweisen, indem wir den (komplizierteren) Beweis aus der gewöhnliche Analysis Wort für Wort abschreiben (d.h. der Abelsche Grenzwertsatz ist auf $\mathbb{Q}_p$ übertragbar).
Für des Innere des Konvergenzgebietes könnte man den Stetigkeitssatz auch grundsätzlich anders zeigen: Die Funktion $f : \mathcal{D}^\circ \to \mathbb{C}$ ist der gleichmäßige Limes der Polynome $f_0 + f_1 x + f_2 x^2 + ... + f_N x^N$ (für $N = 0, 1, 2, ...$). Da der gleichmäßige Limes stetiger Funktionen (Polynome sind ja stetige Funktionen) ebenfalls stetig ist, folgt die Behauptung. Auch dieser Beweis ist auf p-adische Potenzreihen übertragbar. Im p-adischen könnte man so sogar die Stetigkeit auf ganz $\mathcal{D}$ zeigen (weil $\mathcal{D}^\circ = \mathcal{D}$; siehe Bemerkung (4) nach Satz 4.1).

4.2 Zerlegung der Exponentialpolynome in p-adische Potenzreihen

Gegeben sei ein Exponentialpolynom $\sum\limits_{i=1}^{k} A_i(n)\alpha_i^n$ über $\mathbb{Q}_p$, wobei wir $\|\alpha_i\|_p = 1$ annehmen (siehe Abschnitt 3.3). In diesem Abschnitt werden wir $p-1$ Potenzreihen $f_r(X) = f_0^r + f_1^r X + f_2^r X^2 + ...$, $r = 0, 1, ...p-2$, konstruieren können, sodaß

$$f_r(s) = \sum_{i=1}^{k} A_i(r + s(p-1))\alpha_i^{r+s(p-1)} \quad \forall s \in \mathbb{Z},$$

für $r = 0, 1, ...p-2$.
Voraussetzung dafür, daß diese Gleichungen überhaupt erfüllt sein können, ist, daß die Potenzreihen $f_r(s)$, $r = 0, 1, ...p-2$, zumindest auf $\mathbb{Z}$ konvergieren. Wegen $\|1\|_p = 1$ folgt, daß die Konvergenzradien der Potenzreihen nicht kleiner als 1 sein dürfen und daher die Potenzreihen zumindest auf $\mathbb{Z}_p$ konvergieren müssen (sie müssen für alle z mit $\|z\|_p = 1$ konvergieren, weil sie das für zumindest ein z tun, nämlich für 1; siehe Satz 4.1).
Da $A_i(r + s(p-1))$ für festes r und i ein Polynom in s ist (also insbesondere eine auf $\mathbb{Z}_p$ konvergente Potenzreihe), und die Menge der auf $\mathbb{Z}_p$ konvergenten Potenzreihen einen Ring bilden, genügt es zu zeigen, daß $s \mapsto \alpha_i^{r+s(p-1)}$ durch eine Potenzreihe auf $\mathbb{Z}_p$ fortsetzbar ist,

oder einfacher $s \mapsto (\alpha_i^{p-1})^s$. Das wird in Satz 4.3 geschehen. Wesentlich wird dabei sein, daß $\|\alpha_i\|_p = 1$.

Wir betrachten zunächst folgende Möglichkeit, die Potenzreihenentwicklung der komplexen Exponentialfunktion herzuleiten:
Es sei α eine beliebige komplexe Zahl. Wir wollen die Funktion $n \mapsto \alpha^n$ $(n \in \mathbb{N})$ mit Hilfe einer Potenzreihe auf $\mathbb{C}$ fortsetzen. Wir setzen $\beta = \alpha - 1$. Aus dem binomischen Lehrsatz folgt

$$\begin{aligned} \alpha^n &= (1+\beta)^n = \sum_{i=0}^{\infty} \binom{n}{i} \beta^i = \\ &= \sum_{i=0}^{\infty} n(n-1)...(n-i+1) \frac{\beta^i}{i!} \end{aligned}$$

Das Polynom $X(X-1)...(X-i+1)$ hat ganze Koeffizienten:

$$X(X-1)...(X-i+1) = \sum_{j=0}^{\infty} k_{ij} X^j,$$

wobei $k_{ij} = 0$, wenn $j > i$.
Es folgt

$$(1+\beta)^n = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} k_{ij} n^j \frac{\beta^i}{i!}.$$

Wenn man im letzten Ausdruck die Summen vertauscht, erhält man die gewünschte Potenzreihenentwicklung.
Mit Hilfe des Cauchy'schen Doppelreihensatzes kann man zeigen, daß diese Vertauschung tatsächlich erlaubt ist. Ausschlaggebend dabei ist, daß die Folge $\left(\frac{\beta^i}{i!}\right)_{i \geq 0}$ besonders rasch gegen Null konvergiert ('$i!$ wächst schneller als jede Potenz').

Im p-adischen verwendete man denselben 'Trick', um auf die Potenzreihenentwicklung der Exponentialfunktion zu schließen. Das Vertauschen der beiden Summen wird wieder durch Hilfssatz 4.1 ermöglicht. Das Problem ist aber, daß die Folge $\left(\frac{\beta^i}{i!}\right)_{i \geq 0}$ im p-adischen nicht unbedingt eine Nullfolge ist: Für $i \in \mathbb{N}$ ist $i!$ eine ganze Zahl und daher ist ihr p-adischer Absolutbetrag kleiner oder gleich 1. Daraus folgt, daß die Folge der Kehrwerte $\left(\frac{1}{i!}\right)_{i \geq 0}$ außerhalb des Einheitskreises liegt und daher insbesondere keine Nullfolge sein kann.
Damit die Folge $\left(\frac{\beta^i}{i!}\right)_{i \geq 0}$ eine Nullfolge ist, muß daher $\|\beta\|_p$ genügend klein sein (mindestens so klein, daß $(\|\beta^i\|_p)_{i \geq 0}$ eine Nullfolge ist, i.e $\|\beta\|_p \leq \frac{1}{p}$). Um zu wissen, wie groß wir β maximal wählen dürfen, schätzen wir im nächsten Satz die Beträge der Folge $\left(\frac{1}{i!}\right)_{i \geq 0}$ nach oben ab:

Hilfssatz 4.3 *Es sei m eine natürliche Zahl. Dann ist $\|m!\|_p > p^{-\frac{m}{p-1}}$*

Beweis: Zunächst zeigen wir, daß $\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \left[\frac{m}{p^3}\right] + ...$ der Exponent M der Primzahl p in der Primfaktorzerlegung von $m!$ ist.

Für $i \geq 1$ sei $s(i)$ die Anzahl der ganzen Zahlen in $\{1, 2...m\}$, die durch p^i teilbar sind, aber nicht durch p^{i+1}. Es folgt

$$M = \sum_{i=1}^{\infty} i \cdot s(i) = \sum_{i=1}^{\infty} t(i),$$

wobei $t(i) = s(i) + s(i+1) + s(i+2) + ...$ die Anzahl der ganzen Zahlen zwischen 1 und m ist, die mindestens durch p^i teilbar sind. Wegen $t(i) = \left[\frac{m}{p^i}\right]$ ist die Behauptung damit gezeigt.
Es folgt

$$\|m!\|_p = p^{-\left(\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \left[\frac{m}{p^3}\right] + ...\right)} > p^{-\left(\frac{m}{p} + \frac{m}{p^2} + \frac{m}{p^3} + ...\right)} = p^{-\frac{m}{p-1}} \quad \square$$

Bemerkung: Eine p-adische Potenzreihe $\sum\limits_{n=0}^{\infty} a_n X^n$ konvergiert auf $\mathbb{Z}_p$ genau dann, wenn $\|a_n x^n\|_p \overset{n \to \infty}{\to} 0 \quad \forall x \in \mathbb{Z}_p \Leftrightarrow \|a_n\|_p r^n \to 0 \quad \forall r \in [0, 1] \Leftrightarrow \|a_n\|_p \to 0$.

Im folgenden Satz zeigen wir, daß im Fall $p \neq 2$ es genügt $\|\beta\|_p \leq \frac{1}{p}$ vorauszusetzen, um $n \mapsto (1 + \beta)^n$ in eine Potenzreihe zu entwickeln (für den Fall $p = 2$ würde das erst für $\|\beta\| \leq \frac{1}{p^2}$ funktionieren).

Satz 4.3 *Es sei $p \neq 2$ eine Primzahl und $b \in \mathbb{Q}_p$, sodaß $\|b\|_p \leq \frac{1}{p}$. Dann gibt es eine Potenzreihe $f_b(X) = \sum\limits_{n=0}^{\infty} f_n X^n$ über $\mathbb{Q}_p$, die auf $\mathbb{Z}_p$ konvergiert und*

$$f_b(s) = (1 + b)^s \quad \forall s \in \mathbb{Z}$$

erfüllt.

Beweis: Aus dem binomischen Lehrsatz erhalten wir für natürliches $s \geq 0$

$$(1 + b)^s = \sum_{i=0}^{\infty} \binom{s}{i} b^i = \sum_{i=0}^{\infty} s(s-1)...(s-i+1) \frac{b^i}{i!}.$$

Wie oben seien k_{ij} wieder die Koeffizienten der Polynome $X(X-1)...(X-i+1)$, $i = 0, 1, 2, ...$. Es folgt

$$(1 + b)^s = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} k_{ij} s^j \frac{b^i}{i!}.$$

Wir wollen nun die beiden Summen in diesem Ausdruck vertauschen. Nach Hilfssatz 4.1 dürfen wir das, wenn

$$\forall \varepsilon > 0 : \exists N \text{ s.d. } \left\| k_{ij} s^j \frac{b^i}{i!} \right\|_p < \varepsilon \quad \text{für } \max\{i, j\} > N \tag{4.1}$$

Aus $\|b\|_p \leq p^{-1}$ und Hilfssatz 4.3 erhalten wir

$$\left\| \frac{b^i}{i!} \right\|_p \leq p^{-i} \cdot p^{\frac{i}{p-1}} = p^{\frac{(2-p)i}{p-1}} \to 0 \text{ wenn } i \to \infty.$$

(An dieser Stelle verwenden wir $p \neq 2$.)
Wegen $\|k_{ij}s^j\frac{b^i}{i!}\|_p \leq 1 \cdot \|\frac{b^i}{i!}\|_p$ gibt es eine natürliche Zahl N, sodaß $\|k_{ij}s^j\frac{b^i}{i!}\|_p < \varepsilon \quad \forall i > N$.
Ist $j > i$, so ist $\|k_{ij}s^j\frac{b^i}{i!}\|_p = 0$, weil dann $k_{ij} = 0$ ist. Es folgt (4.1) und daher

$$(1+b)^s = \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty}\frac{b^i}{i!}k_{ij}\right)s^j =: \sum_{j=0}^{\infty} f_j s^j$$

wenn $s \in \mathbb{Z}^+$. Wir setzen

$$f_b(X) = \sum_{j=0}^{\infty} f_j X^j.$$

Die p-adische Potenzreihe $f_b(X)$ konvergiert insbesondere für $X = 1$, woraus $\|f_j\|_p \overset{j\to\infty}{\to} 0$ folgt. Gemeinsam mit der Bemerkung vor dem Satz ergibt das die Konvergenz der Potenzreihe auf $\mathbb{Z}_p$.
Zuletzt müssen wir noch zeigen, daß

$$(1+b)^s = \sum_{j=0}^{\infty} b_j s^j$$

wenn $s < 0$. Es ist $\lim\limits_{m\to\infty}(1+b)^{p^m} = 1$, weil

$$\lim_{m\to\infty}(1+b)^{p^m} = \lim_{m\to\infty}\sum_{j=0}^{\infty} b_j(p^m)^j \overset{\text{Stetigkeit, Satz 4.2}}{=} \sum_{j=0}^{\infty} b_j(0)^j = b_0 = 1.$$

Es sei also s eine negative ganze Zahl. Dann gibt es ein $M \in \mathbb{N}$, sodaß $p^m + s \geq 0$, wenn $m \geq M$.

$$(1+b)^s = (\lim_{m\to\infty}(1+b)^{p^m})(1+b)^s = \lim_{m\to\infty}(1+b)^{p^m+s} =$$
$$\overset{p^m+s\geq 0}{=} \lim_{m\to\infty}\sum_{j=0}^{\infty} b_j(p^m+s)^j \overset{\text{Stetigkeit}}{=} \sum_{j=0}^{\infty} b_j s^j \quad \square$$

Es sei γ ein ganze p-adische Zahl. Beginnt ihre p-adische Reihenentwicklung mit der Ziffer 1 ($\Leftrightarrow \gamma \equiv 1 \mod p$), dann haben wir soeben gezeigt, daß sich die Funktion $s \mapsto \gamma^s$ $(s \in \mathbb{Z})$ mit Hilfe eine p-adischen Potenzreihe auf $\mathbb{Z}_p$ fortsetzen läßt. (Setze $b = \gamma - 1$. Wegen $\gamma \equiv 1 \mod p$, folgt $\|b\|_p \leq \frac{1}{p}$).

Einen Satz dieser Art hätten wir gerne für die Funktionen $s \mapsto \alpha_i^s$, wobei α_i die k 'Wurzeln' in unserem Exponentialpolynom bezeichnen. Das Problem ist, daß $\alpha_i \equiv 1 \mod p$ im allgemeinen nicht gelten muß.
Aus $\|\alpha_i\|_p = 1$ folgt aber, daß diese 'Wurzeln' zumindest ganze p-adische Zahlen sind und daß $\alpha_i \not\equiv 0 \mod p$ für $i = 1, ...k$. In Abschnitt 2.5 haben wir gesehen, daß die Abbildung $\gamma \mapsto \gamma \mod p$ ein Homomorphismus mit Urbildbereich $\mathbb{Z}_p$ und Wertebereich $\mathbb{Z}/p\mathbb{Z}$ ist. Der kleine Satz von Fermat ergibt $\alpha_i^{p-1} \equiv 1 \mod p$. Aus Satz 4.3 folgt, daß es für $i = 1, 2, ...k$

eine auf $\mathbb{Z}_p$ konvergente Potenzreihe $\sum\limits_{j=0}^{\infty} a_{ij}X^j$ gibt, mit

$$(\alpha_i^{p-1})^s = \sum_{j=0}^{\infty} a_{ij}s^j.$$

Wenn man sich an den Beginn dieses Abschnittes erinnert war das die fehlende Zutat, um die Potenzreihenentwicklung von

$$s \mapsto \sum_{i=1}^{k} A_i(r + s(p-1))(\alpha_i^{p-1})^s \alpha_i^r \qquad r = 0, 1, ...p-2$$

zu bekommen.

Was haben wir bis jetzt erreicht?

Unsere Aufgabe ist es die Nullstellenmenge von

$$n \mapsto \sum_{i=1}^{k} A_i(n)\alpha_i^n$$

zu untersuchen.

Dazu haben wir das Exponentialpolynom in $p-1$ Teile 'zerlegt', die alle durch p-adische Potenzreihen darstellbar sind

$$\sum_{i=1}^{k} A_i(s(p-1))(\alpha_i^{p-1})^s$$

$$\sum_{i=1}^{k} A_i(1 + s(p-1))(\alpha_i^{p-1})^s \alpha_i$$

$$...$$

$$...$$

$$\sum_{i=1}^{k} A_i((p-2) + s(p-1))(\alpha_i^{p-1})^s \alpha_i^{p-2}$$

und haben dadurch das Problem auf die Untersuchung der Nullstellen jedes einzelnen Teiles zurückgeführt.

Der letzte Abschitt, bevor wir dann endlich unseren Satz beweisen können, beschäftigt sich daher mit den Nullstellen p-adischer Potenzreihen, die auf $\mathbb{Z}_p$ konvergieren.

4.3 Der Satz von Strassmann

In der Analysis wird folgender Satz bewiesen: *Es sei* $\sum\limits_{n=0}^{\infty} f_n X^n$ *eine Potenzreihe über* $\mathbb{C}$, *die auf der beschränkten und offenen Menge* $K \subseteq \mathbb{C}$ *konvergiert. Dann hat die Funktion*

$x \to \sum\limits_{n=0}^{\infty} f_n x^n$ *höchstens endlich viele Nullstellen in* K *oder* $\sum\limits_{n=0}^{\infty} f_n x^n = 0\ \forall x \in K$ ($\Leftrightarrow f_n = 0 \quad \forall n = 0, 1, 2 ...$).
Man nennt ihn 'Identitätssatz für Potenzreihen'.

Folgendes (etwas stärkere) Analogon gilt in $\mathbb{Q}_p$:

Satz 4.4 (von Strassmann) *Es sei* $f(X) = f_0 + f_1X + f_2X^2 + ...$ *eine Potenzreihe über* $\mathbb{Q}_p$*, die auf der beschränkten Menge* $K \subseteq \mathbb{Q}_p$ *konvergiert. Dann hat die Funktion* $z \mapsto f(z)$ *höchstens endlich viele Nullstellen in* K *oder* $f \equiv 0$.

Bemerkung

(1) Wir werden Satz 4.4 nur für $K = \mathbb{Z}_p$ zeigen, obwohl es kaum aufwendiger wäre, den allgemeineren Satz zu zeigen. Eigentlich nennt man nur diesen Spezialfall *Satz von Strassmann.* Im Beweis des Satzes wird man sehen, daß für diesen Fall sogar eine noch stärkere Formulierung möglich wäre..

(2) Der Satz von Strassmann ist stärker als der Identitätssatz, weil er eine Aussage über die Nullstellen einer gegeben p-adischen Potenzreihe in einer nicht notwendig offenen Teilmenge K des Konvergenzgebietes trifft. In $\mathbb{C}$ gilt dieser Satz nicht: Mit Hilfe des Weierstraß'schen Produktsatzes kann man nämlich eine auf $\{z \in \mathbb{C} \mid |z| \leq 1\}$ konvergente Potenzreihe $a(X) \not\equiv 0$ konstruieren, für die $a(z) = 0$, wenn $|z| = 1$.
Folgende Sichtweise wäre auch möglich: In Bemerkung (4) zu Satz 4.1 haben wir gesehen, daß das Konvergenzgebiet einer p-adischen Potenzreihe stets offen ist. So betrachtet sind Satz 4.4 und der Identitätssatz für Potenzreihen in $\mathbb{C}$ übertragen auf $\mathbb{Q}_p$ eigentlich äquivalent.

(3) Diese stärkere Version des Identitätssatzes wird durch den stärkeren Translationssatz (Hilfssatz 4.2) in $\mathbb{Q}_p$ ermöglicht, d.h. mit Hilfe des schwächeren, in $\mathbb{C}$ gültigen Translationsatzes könnte man auch nur den schwächeren, in $\mathbb{C}$ gültigen, Identitätssatz beweisen. Für uns wird dieses Ergebnis wesentlich sein, d.h. das schwächere Analogon aus der gewöhnlichen Analysis genügt uns in diesem Fall nicht (wie das zum Beispiel beim Beweis der Stetigkeit der Potenzreihe der Fall war; ich habe das schon in der Bemerkung nach dem Beweis des Translationssatzes erwähnt).

Der Satz von Strassmann ist ein besonders wichtiges Element unseres Satzes über lineare Rekursionsfolgen. Er ist für mich die Stelle des Beweises, die ich am wenigsten *begreife* (siehe Ende von Kapitel 2). Ich bin daher sehr froh, hier zwei völlig verschiedene Beweise des Satzes von Strassmann angeben zu können.

Erster Beweis Dieser Beweis verläuft ganz so wie in der komplexen Analysis.

1.Schritt Zunächst zeigen wir den Satz von Bolzano-Weierstraß für $\mathbb{Q}_p$: Es sei $(z_n)_{n\geq 0}$ eine Folge ganzer p-adischer Zahlen. Dann existiert eine in $\mathbb{Z}_p$ konvergente Teilfolge von $(z_n)_{n\geq 0}$.

Beweis Nach dem Dirichletschen Schubfachprinzip gibt es ein $\zeta_0 \in \{0, 1, ...p-1\}$, sodaß $z_n \equiv \zeta_0 \mod p$ für alle natürlichen Zahlen n in einer unendlichen Teilmenge M_0 der natürlichen Zahlen.
Genauso existiert ein $\zeta_1 \in \{0, 1, ...p-1\}$ mit $z_n \equiv \zeta_0 + \zeta_1 p \mod p^2$ für unendlich viele $n \in M_0$. Ich bezeichne die Menge dieser n mit M_1.
Weiters existiert ein $\zeta_2 \in \{0, 1, ...p-1\}$ und eine unendliche Menge natürlicher Zahlen $M_2 \subseteq M_1$ mit $z_n \equiv \zeta_0 + \zeta_1 p + \zeta_2 p^2 \mod p^3 \; \forall n \in M_2$ ... u.s.w.
Wenn man das unendlich lange fortsetzt, erhält man eine Folge $(\zeta_n)_{n \geq 0}$ ganzer Zahlen ($0 \leq \zeta_n < p$) und eine absteigende Folge $(M_n)_{n \geq 0}$ von unendlichen Teilmengen von $\mathbb{N}$ mit

$$m, n \in M_i \Rightarrow z_m \equiv \sum_{j=0}^{i} \zeta_j p^j \equiv z_n \mod p^{i+1} \Rightarrow \|z_m - z_n\|_p \leq p^{-(i+1)}. \tag{4.2}$$

Wähle $z_{n_0} \in M_0$, $z_{n_1} \in M_1$, $z_{n_2} \in M_2$,... .
Wegen (4.2) ist die Folge $(z_{n_i})_{i \geq 0}$ eine Cauchyfolge und deshalb, wegen der Vollständigkeit von $\mathbb{Q}_p$ und der Abgeschlossenheit von $\mathbb{Z}_p$, in $\mathbb{Z}_p$ konvergent.

2. Schritt Es sei $N = \{x \in \mathbb{Z}_p | f(x) = 0\}$. Angenommen $|N| = \infty$. Es sei $(z_n)_{n \geq 0}$ eine Folge in N, mit $z_n \neq z_m$, wenn $n \neq m$. Im 1.Schritt haben wir gezeigt, daß wir o.B.d.A. annehmen können, daß diese Folge gegen eine ganze p-adische Zahl z konvergiert. Weiters können wir annehmen, daß $z_n \neq z \; \forall n \in \mathbb{N}$.

3.Schritt In Hilfssatz 4.2 haben wir eine auf $\mathbb{Z}_p$ konvergente Potenzreihe $g(X) = g_0 + g_1 X + g_2 X^2 + ...$ konstruiert mit $f(x) = g(x - z) \; \forall x \in \mathbb{Z}_p$. Es folgt $g(z_n - z) = 0 \; \forall n \in \mathbb{N}$ und daher

$$-g_0 = g_1(z_n - z) + g_2(z_n - z)^2 + ... \quad .$$

Wegen der Stetigkeit einer p-adischen Potenzreihe auf ihrem Konvergenzgebiet strebt die rechte Seite bei $n \to \infty$ gegen 0. Wir erhalten $g_0 = 0$. Wenn man das berücksichtigt und die letzte Gleichung durch $(z_n - z)$ dividiert (das geht, da $z_n \neq z$) erhält man

$$-g_1 = g_2(z_n - z) + g_3(z_n - z)^2 + ... \quad .$$

Läßt man n wieder gegen ∞ streben, erhält man $g_1 = 0$. Nun dividiert man diese Gleichung wieder durch $(z_n - z)$ ... u.s.w.
Auf diese Weise zeigt man induktiv $g_n = 0$ für $n \in \mathbb{N}$. Es folgt $g \equiv 0$ und wegen $f(x) = g(x - z)$ ist $f \equiv 0$.

Der **zweite Beweis** ist ein 'p-adischer Beweis' des Satzes von Strassmann, d.h. ein Beweis, der in $\mathbb{C}$ kein Analogon findet.
Da die Potenzreihe $f(X) = \sum\limits_{n=0}^{\infty} f_n X^n$ auf $\mathbb{Z}_p$ konvergiert, folgt $\|f_n\|_p \overset{n \to \infty}{\to} 0$. Es gibt daher eine natürliche Zahl N, sodaß

$$\|f_N\|_p = \max_{n \in \mathbb{N}} \|f_n\|_p \text{ und } \|f_n\|_p < \|f_N\|_p \quad \forall n > N.$$

Ich zeige mit Induktion nach N, daß f dann höchstens N Nullstellen in $\mathbb{Z}_p$ hat. (Der 'p-adische Beweis' ermöglicht also zusätzlich auch noch eine Aussage über die Anzahl der Nullstellen.)

Induktionsanfang N=0: Angenommen es gäbe ein $b \in \mathbb{Z}_p$ mit $f(b) = 0$. Dann folgt

$$-f_0 = \sum_{n=1}^{\infty} f_n b^n.$$

Das ist ein Widerspruch, weil

$$\| \sum_{n=1}^{\infty} f_n b^n \|_p \leq \max_{n \in \{1,2,3,\ldots\}} \|f_n b^n\|_p \leq \max_{n \in \{1,2,3,\ldots\}} \|f_n\|_p \cdot 1 \overset{N=0}{<} \|f_0\|_p.$$

Induktionsschritt $N-1 \to N$: Es sei also $N > 0$ und $b \in \mathbb{Z}_p$ mit $f(b) = 0$. Für $c \in \mathbb{Z}_p$ beliebig folgt dann

$$\begin{aligned}
f(c) \quad &= \quad f(c) - f(b) = \sum_{n=1}^{\infty} f_n (c^n - b^n) = \\
= (c-b) \sum_{n=1}^{\infty} \sum_{j=0}^{n-1} f_n c^j b^{n-1-j} \quad &\overset{\text{Hilfssatz 4.1}}{=} \quad (c-b) \sum_{j=0}^{\infty} \left(\sum_{n=j+1}^{\infty} f_n b^{n-1-j} \right) c^j = \\
&=: \quad (c-b) \sum_{j=0}^{\infty} g_j c^j = (c-b) g(c)
\end{aligned}$$

Für die Koeffizienten der so erhaltenen Potenzreihe $g(X) = \sum_{j=0}^{\infty} g_j X^j$ folgt

$$\begin{aligned}
\|g_j\|_p = \| \sum_{n=j+1}^{\infty} f_n b^{n-1-j} \|_p \quad &\leq \quad \max_{n \in \mathbb{N}} \|f_n\|_p \leq \|f_N\|_p \\
&\text{und} \\
\|g_{N-1}\|_p = \| \sum_{n=N}^{\infty} f_n b^{n-N} \|_p \quad &= \quad \|f_N + \sum_{n=N+1}^{\infty} f_n b^{n-N} \|_p = \|f_N\|_p.
\end{aligned}$$

(In der zweiten Zeile verwenden wir Hilfssatz 2.2 und $\| \sum_{n=N+1}^{\infty} f_n b^{n-N} \|_p < \|f_N\|_p$.)
Es sei $j \geq N$:

$$\|g_j\|_p = \| \sum_{N=j+1}^{\infty} f_n b^{n-1-j} \|_p \leq \max_{n \in \{N+1, N+2, N+3, \ldots\}} \|f_n\|_p < \|f_N\|_p.$$

Die letzten 3 (Un)gleichungen zeigen, daß $N-1$ der 'Induktionsparameter' der Potenzreihe $g(X)$ ist. Aus der Induktionsvoraussetzung folgt, daß die Funktion $x \mapsto g(x)$ höchstens $N-1$ Nullstellen in $\mathbb{Z}_p$ hat.
Wegen $f(c) = 0 \Leftrightarrow (c = b \text{ oder } g(c) = 0)$ ergibt das die Behauptung. □

Eine etwas längere Bemerkung zum zweiten Beweis des Satzes von Strassmann

(Wer so kurz vor Ende des Beweises des Satzes von Skolem-Mahler-Lech schon ungeduldig ist, kann diese Bemerkung ruhig auslassen und gleich zu Abschnitt 4.4 blättern.
Außerdem enthält die Bemerkung für viele Leser wahrscheinlich nur Uninteressantes oder

Triviales.
Für mich hat ihr Inhalt aber schon einige Bedeutung, da sie sozusagen einige 'aha-Erlebnisse' meiner Arbeit zu diesem Thema enthält.)

Ich habe bereits erwähnt, daß der zweite Beweis kein Analogon in $\mathbb{C}$ hat, d.h. daß man den Identitätssatz für Potenzreihen in $\mathbb{C}$ nicht mit einer ähnlichen Methode beweisen kann. Das sieht man schon daran, daß dieser Beweis eine stärkere Aussage über die Nullstellen von Potenzreihen über $\mathbb{Q}_p$ ermöglicht, die für $\mathbb{C}$ nicht zutrifft:
Betrachte zum Beispiel das Polynom

$$p(X) = X^2 + 2X - 3$$

über $\mathbb{C}$.
Würde der Satz von Strassmann in der stärkeren Variante (damit meine ich vor allem die Aussage über die Anzahl der Nullstellen und nicht jene über die topologische Eigenschaft der Menge K; siehe Bemerkung (3) zu Satz 4.4) auch in $\mathbb{C}$ gelten, dann hätte das Polynom $p(X)$ keine Nullstelle im Einheitskreis, da sein betragsmäßig größter Koeffizient der des konstanten Monoms ist. Jedoch hat dieses Polynom eine Nullstelle im Einheitskreis, nämlich 1. (Es war natürlich von vornherein nicht zu erwarten, daß die Aussage über die Anzahl der Nullstellen im Einheitskreis auch in $\mathbb{C}$ erfüllt ist. Bei ihrem Beweis in $\mathbb{Q}_p$ haben wir nämlich x-mal die ultrametische Ungleichung verwendet.)

Dennoch erinnert mich dieser zweite Beweis an einen anderen sehr bekannten Satz und dessen Beweis:

Satz 4.5 *Es sei $p(X) \neq 0$ ein Polynom über einem Integritätsbereich R und $deg(p) = n$. Dann hat $p(X)$ höchstens n Nullstellen in R.*

Meistens zeigt man diesen Satz induktiv durch das 'Abspalten' von Nullstellen: Für den Fall $n = 0$ ist die Aussage klar. Es sei $n \geq 0$ und $x_1 \in R$ eine Nullstelle von $p(X)$. Dann zeigt eine einfache Rechnung, daß ein Polynom $q(X) \in R[X]$ existiert, mit $p(X) = (X - x_1) \cdot q(X)$ und $deg(q) = n - 1$. Die Induktionsvoraussetzung, angewandt auf das Polynom $q(X)$, ergibt die Behauptung.
Wenn man noch einmal den zweiten Beweis des Satzes von Strassmann betrachtet, so sieht man, daß wir dabei im wesentlichen derselben Idee gefolgt sind, nämlich dem Abspalten von Nullstellen. Der einzige Unterschied ist, daß wir dort, notwendigerweise, die Induktion nicht bezüglich des Grades des Polynoms geführt haben, sondern bezüglich des Index des 'rechtesten Maximum' der Koeffizienten f_i der Potenzreihe (also in gewisser Weise auch bezüglich des Index des/eines führenden Koeffizienten).

Ich möchte nun zeigen, wie man eine noch engere Analogie dieser beiden Sätze sehen kann: Es sei $f(X) = \sum_{i=0}^{\infty} f_i X^i$ eine p-adische Potenzreihe, die auf $\mathbb{Z}_p$ konvergiert ($\Leftrightarrow \|f_i\|_p \stackrel{i\to\infty}{\to} 0$). Da es uns nur auf die Nullstellenmenge der Potenzreihe $f(X)$ ankommt, können wir o.B.d.A. annehmen, daß die Koeffizienten f_i der Potenzreihe ganze p-adische Zahlen sind (wegen $\|f_i\|_p \stackrel{i\to\infty}{\to} 0$

gibt es nämlich ein $m \in \mathbb{N}$, sodaß $p^m \cdot f(X)$ eine Potenzreihe über $\mathbb{Z}_p$ ist). Man kann die p-adische Potenzreihe $f(X)$ daher $mod\, p^n$ betrachten.
Es sei $n \in \mathbb{N}$. Wiederum wegen $\|f_i\|_p \overset{i\to\infty}{\to} 0$ gibt es ein (eindeutig bestimmtes) Polynom $p_n(X)$ mit Koeffizienten in $\{0, 1, ...p^n - 1\}$, sodaß $f(X) \equiv p_n(X) \ \ mod\, p^n$. Auf dieses Weise erhält man eine Folge von Polynomen mit ganzen Koeffizienten $(p_n(X))_{n\geq 1}$ die 'äquivalent' zu $f(X)$ ist (mit äquivalent meine ich, daß man bei alleiniger Kenntnis der Folge $(p_n(X))_{n\geq 1}$, die Potenzreihe $f(X)$ berechnen kann und umgekehrt). Man beachte, daß $p_n(X) \equiv p_{n+1}(X) \ \ mod\, p^n$ für $n = 1, 2, 3, ...$.
Ist umgekehrt $(p_n(X))_{n\geq 0}$ eine beliebige Folge von Polynomen mit ganzen Koeffizienten und $p_n(X) \equiv p_{n+1}(X) \ \ mod\, p^n$ für $n = 1, 2, 3, ...$, dann gibt es es eine auf $\mathbb{Z}_p$ konvergente Potenzreihe $f(X)$, mit $f(X) \equiv p_n(X) \ \ mod\, p^n$ für $n = 1, 2, 3, ...$
Der Satz von Strassman ist daher auch ein Satz über solche Polynomfolgen $(p_n(X))_{n\geq 0}$. Für sie besagt er, daß es nur endlich ganze p-adische Zahlen z gibt, sodaß

$$p_n(z) \equiv 0 \ \ mod\, p^n \text{ für } n = 1, 2, 3, ... \quad .$$

Wir wollen schließlich noch untersuchen, wie es hier mit der konkreteren Aussage über die Anzahl der Nullstellen aussieht, d.h wie sich

$$M = \max\{N | \|f_N\|_p = \max_{n\in\mathbb{N}} \|f_n\|_p\}$$

bei der zu $f(X)$ äquivalenten Polynomfolge $(p_n(X))_{n\geq 0}$ ausdrückt. Es sei $A = \max_{n\in\mathbb{N}} \|f_n\|_p$. Wähle $m \in \mathbb{N}$, sodaß $A = p^{-m}$. Dann ist m die kleinste natürliche Zahl, sodaß $p_m(X) \not\equiv 0 \ \ mod\, p^m$. Man überlegt sich leicht, daß M der Grad des Polynoms $p_m(X) \ \ mod\, p^m$ ist. Wir erhalten also folgenden

Satz 4.6 (von Strassmann für Polynomfolgen) *Es sei $(p_n)_{n\geq 0}$ eine Folge von Polynomen mit ganzen Koeffizienten und $p_n(X) \equiv p_{n+1}(X) \ \ mod\, p^n$ für $n = 1, 2, 3, ...$.*

(1) Es sei m die kleinste natürliche Zahl, sodaß $p_m(X) \not\equiv 0 \ \ mod\, p^m$ und M der Grad des Polynoms $p_m(X) \ \ mod\, p^m$ über $\mathbb{Z}/p^m\mathbb{Z}$. Dann gibt es höchstens M ganze p-adische Zahlen z (und daher erst recht höchstens M ganze Zahlen z) mit

$$p_n(z) \equiv 0 \ \ mod\, p^n \text{ für } n = 1, 2, 3, ... \quad .$$

(2) Wenn die in (1) geforderte natürliche Zahl m nicht existiert, folgt $p_n(X) \equiv 0 \ \ mod\, p^n$ $\forall n \in \mathbb{N}$ und daher

$$p_n(z) \equiv 0 \ \ mod\, p^n \text{ für } n = 1, 2, 3, ...$$

für jede ganze p-adische Zahl z.

Dieser Satz ist eine Verallgemeinerung des folgenden Satzes:

Satz 4.7 *Es sei $p(X) \neq 0$ ein Polynom mit ganzen Koeffizienten. Dann hat $p(X)$ höchstens $deg(p)$ Nullstellen in $\mathbb{Z}$.*

(Man erhält ihn, wenn man in Satz 4.6 $p(X) = p_n(X)$ für $n = 1, 2, 3, ...$ setzt. Dieser Satz ist aber auch ein Spezialfall von Satz 4.5 für $R = \mathbb{Z}$.)

Beweisen kann man Satz 4.6 ganz einfach durch Abspalten von 'Nullstellen' mit Induktion nach M. Das Schöne ist, daß hier der Beweis offensichtlicher eine direkte Verallgemeinerung des Beweises des eben zitierten Spezialfalles ist.

Beweis: Induktionsanfang $M = 0$: Es sei $m \in \mathbb{N}$ minimal, sodaß $p_m(X) \not\equiv 0 \;\; mod\, p^m$. Der Grad von $p_m(X) \;\; mod\, p^m$ beträgt 0, d.h. $p_m(X) \;\; mod\, p^m$ ist konstant und $\not\equiv 0$. Wegen $p_n(X) \equiv p_m(X) \;\; mod\, p^m$ für $n \geq m$ kann es keine ganze p-adische Zahl z mit $p_n(z) \equiv 0 \;\; mod\, p^n$ für jede natürliche Zahl n geben.

Induktionsschritt $M - 1 \rightarrow M$: Es sei $M > 0$ und $z \in \mathbb{Z}_p$, sodaß

$$p_n(z) \equiv 0 \;\; mod\, p^n \quad \forall n \in \mathbb{N}.$$

Es folgt

$$p_n(X) \equiv p_n(X) - p_n(z) = (X - z)q_n(X) \;\; mod\, p^n,$$

wobei $q_n(X)$ ein Polynom über $\mathbb{Z}$ ist und

$$q_{n+1}(X) \equiv q_n(X) \;\; mod\, p^n.$$

Es ist klar, daß wenn $m \in \mathbb{N}$ wie beim Induktionsanfang gewählt wurde, m minimal ist, sodaß $q_m(X) \not\equiv 0 \;\; mod\, p^m$. Außerdem ist $deg(q_m) = deg(p_m) - 1$. Wenn wir zeigen, daß aus

$$p_n(z_1) \equiv 0 \;\; mod\, p^n \quad \forall n \in \mathbb{N} \qquad (*)$$

folgt

$$z_1 = z \text{ oder } q_n(z_1) \equiv 0 \;\; mod\, p^n \quad \forall n \in \mathbb{N}$$

sind wir laut Induktionsvoraussetzung fertig.

Angenommen $z_1 \neq z$. Es sei $k \in \mathbb{N}$, sodaß $\|z - z_1\|_p = p^{-k}$. Dann folgt aus (*) und der Definition von $(q_n(X))_{n \geq 0}$

$$q_{n+k}(z_1) \equiv 0 \;\; mod\, p^n \quad \forall n \in \mathbb{N}.$$

Wegen $q_n(z_1) \equiv q_{n+k}(z_1) \;\; mod\, p^n$ folgt die Behauptung. □

Erwähnenswert ist auch noch, daß wir mit Satz 4.6 eine Formulierung des Satzes von Strassmann gefunden haben, die Begriffe der p-adischen Analysis gänzlich vermeidet.

Der eine Grund, wieso ich überhaupt darüber geschrieben habe, ist, daß durch diese Formulierung der zweite Beweis (zumindest für mich) viel klarer wird, da die Analogie zum Abspalten von Nullstellen bei Polynomen über Integritätsbereichen noch offensichtlicher wird (vor allem sieht man, daß der Induktionparameter hier auch als Grad eines Polynoms auftritt).

Besonders interessant ist aber auch, daß Skolem diese zweite, von p-adischer Analysis freie Formulierung des Satzes von Strassmann verwendete (offenbar kannte er zu diesem Zeitpunkt

die p-adische Analysis nicht einmal). Er erkannte damals allerdings noch nicht diesen einfachen Beweis durch Abspalten von Nullstellen, wie ich ihn eben skizziert habe. Er bewies den Satz mit einer etwas komplizierteren Methode, die man am ehesten als Mischung des ersten und des zweiten Beweises des Satzes von Strassmann beschreiben kann (siehe [19]).
(Das war für mich übrigens eine der spannendsten Entdeckungen während des Schreibens dieser Diplomarbeit.
Einerseits fand ich es interessant, daß Skolem zu dem Beweis des Satzes über Rekurrenzen nicht über die p-adische Analysis kam. Ich fühlte mich bestätigt, da ich nicht verstand, wie man auf diese Idee mit der p-adischen Analysis in diesen Zusammenhang überhaupt kommen konnte.
Andererseits war es auch interessant etwas an einem konkreten Beispiel, wie Skolems Beweis des Satzes von Strassmann, zu erfahren, was ich (und natürlich viele andere auch) schon immer vermutet habe: Nämlich, daß alte Sätze, für die es heutzutage so einfache Beweise gibt, daß man sich kaum mehr vorstellen kann, daß sie jemals ein Problem darstellten, in ihren 'Kinderschuhen' den MathematikerInnen nicht so trivial erschienen.)

4.4 Vollendung des Beweises

Wir fassen zusammen: Gegeben sei eine Rekurrenz $(a_n)_{n\geq 0}$ in einem Körper K der Charakteristik 0 und $a_n = \sum_{i=1}^{k} A_i(n)\alpha_i^n$ ihre Darstellung als Exponentialpolynom, die wir in Kapitel 1 hergeleitet haben.
In Kapitel 3 haben wir gesehen, daß wir o.B.d.A. $K \subseteq \mathbb{Q}_p$ und $\|\alpha_i\|_p = 1$ annehmen können.
In Kapitel 4 wurde in Abschnitt 4.2 gezeigt, daß die Funktionen

$$s \mapsto \sum_{i=1}^{k} A_i(r + s(p-1))(\alpha_i^{p-1})^s \alpha_i^r = a_{r+s(p-1)} \quad \text{für} \quad r = 0, 1, ...p-2$$

durch p-adische Potenzreihen auf $\mathbb{Z}_p$ fortsetzbar ist.
Nach dem Satz von Strassmann hat $s \mapsto a_{r+s(p-1)}$ daher nur endlich viele Nullstellen in $\mathbb{Z}_p$ (und damit erst recht in $\mathbb{Z}$) oder $a_{r+s(p-1)} = 0$ für $s = 0, 1, 2, \dots$. Da die natürlichen Zahlen durch die $p-1$ arithmetischen Progressionen

$$(p-1)\mathbb{N}, \quad 1 + (p-1)\mathbb{N}, \quad \dots \quad (p-2) + (p-1)\mathbb{N}$$

disjunkt zerlegt werden, und die Rekurrenz $(a_n)_{n\geq 0}$ in jeder dieser arithmetischen Progressionen höchstens endlich viele Nullstellen besitzt oder völlig verschwindet, ist der Satz bewiesen.

Kapitel 5

Eine Variante des Beweises

Im ersten Kapitel, Abschnitt 1.2, habe ich gezeigt, daß der Satz von Skolem-Mahler-Lech nicht nur ein Satz über Rekurrenzen ist, sondern auch einer über Exponentialpolynome und die Taylorentwicklung rationaler Funktionen. Der vorgestellte Beweis verwendet nur die Sichtweise der Exponentialpolynome, d.h. daß ab der Stelle, wo wir die Äquivalenz Rekurrenz $\leftrightarrow$ Exponentialpolynom gezeigt haben, nie mehr mit Rekurrenzen oder der Taylorentwicklung rationaler Funktionen gearbeitet wird.
Für mich, die ich den Satz von Skolem-Mahler-Lech am ehesten als einen über Rekurrenzen sehe, da ich ihn in dieser Formulierung kennengelernte habe und ihn als solchen faszinierend fand, war diese Situation unbefriedigend. Hauptsächlich bezog sich diese Unzufriedenheit auf die Tatsache, daß ich durch diesen Beweis den Satz über Rekurrenzen nicht 'richtig' verstand. Zwar verstand ich jeden einzelnen Schritt, jedoch hatte ich nicht das Gefühl zu wissen, wieso der Satz überhaupt gilt. Kurz gesagt: Der Beweis war für mich nicht viel mehr als eine Verifikation des Satzes von Skolem-Mahler-Lech.
Meiner Meinung lag ein Hauptgrund dieses 'Nicht-Verstehens' in der (zu) schmalen Brücke, die der Beweis zu den Rekurrenzen schlug. Aus diesem Grund war ich sehr darum bemüht, den Beweis so zu verändern, daß die Äquivalenz Rekurrenz $\leftrightarrow$ Exponentialpolynom so weit wie möglich eliminiert wird und nur 'fundamentale' Eigenschaften der Rekurrenzen verwendet werden. Als es mir dann schließlich gelang, die Exponentialpolynome gänzlich aus dem Spiel zu lassen (siehe Abschnitt 5.1), half mir das zwar über viele meiner Probleme hinweg – ganz zufrieden war ich zunächst aber noch immer nicht. Inzwischen bin ich so weit, daß mir diese Variante des Beweises doch wesentlich dabei hilft, den Satz genügend gut zu verstehen. In Abschnitt 5.2 möchte ich daher versuchen zu erklären, was meiner Meinung nach hinter dem Satz von Skolem-Mahler-Lech steckt bzw. hinter dem vorgestellten Beweis.

(In meiner Phantasie kann ich mir schon die möglichen Einwände (fiktiver) Leser dieser Diplomarbeit vorstellen, die meine Unzufriedenheit nicht verstehen: Es ist ja gerade das Wesen der Mathematik (einfache) Beziehungen, im besten Fall Äquivalenzen zwischen verschiedenen Objekten herzustellen, um mit ihrer Hilfe neue Ergebnisse (=kompliziertere Beziehungen) herzuleiten. Da darf einem die Beziehung/Äquivalenz Rekurrenz $\leftrightarrow$ Exponentialpolynom

nicht stören, denn in der Regel wird es so sein: Je schmäler die Brücke, umso überraschender wird das anvisierte Ergebnis sein.
Da es sich hier aber um eine Diplomarbeit handelt, die sich nur mit dem Satz von Skolem-Mahler-Lech beschäftigt, war ich zu Beginn schon der Meinung, daß es meine Aufgabe sein sollte, die Brücke zum Satz von Skolem-Mahler-Lech für den Leser insgesamt etwas zu verbreitern und das möglicherweise zunächst überraschende Ergebnis durchschaubar zu machen. Oder besser, da das 'Verstehen', das ich hier meine, etwas Subjektives ist, zumindest die Autorin der Meinung sein sollte, das 'Geheimnis' des Satzes 'wirklich verstanden' zu haben. Im nachhinein betrachtet habe ich gelernt, daß dieser Anspruch, den ich eigentlich bis jetzt nicht nur bei meiner Diplomarbeit sondern auch meistens während meines Studiums verfolgt habe, doch ein recht hoher ist (darum, weil ich mir nicht ganz sicher bin, ob es mir bei dieser Diplomarbeit gelungen ist, ihm zu genügen.) Gelernt habe ich aber auch, daß dieser Anspruch an einen Beweis, nicht nur Verifikation sondern auch Erklärung des Satzes zu sein, wahrscheinlich nicht von der Masse der Mathematiker geteilt wird. Vor allem habe ich das in der verwendeten Literatur gesehen, wo ich eigentlich kaum reflektierende Bemerkungen zum Beweis des Satzes von Skolem-Mahler-Lech gefunden habe. Natürlich fallen mir hunderte von plausiblen Gründe für dieses Manko ein, angefangen damit, daß ich nur nicht an der richtigen Stelle gesucht habe, bis dahin, daß das 'richtige' Verstehen eines Satzes etwas äußerst Subjektives ist und daher aufgrund des eher sachlich gehaltenen Stils mathematischer Literatur kaum Platz für eine Reflexion dieser Art bleibt.)

5.1 Der Beweis

Es sei also $(a_n)_{n\geq 0}$ eine Rekurrenz über einem Körper K, $\text{char}(K) = 0$ und K o.B.d.A. endlich erzeugt über $\mathbb{Q}$, die der Rekurrenzrelation

$$a_n = s_1 a_{n-1} + s_2 a_{n-2} + ... + s_m a_{n-m}$$

für $n \geq m$ genügt ($s_1, s_2, ...s_m \in K$, $s_m \neq 0$).
(In diesem Abschnitt sei $(a_n)_{n\geq 0}$ immer diese beliebige, aber fixe, Rekurrenz. Die Koeffizienten der definierenden Rekurrenzrelation $s_1, s_2, ...s_m$ seien ebenfalls fix, auch wenn ich sie in Zusammenhang mit anderen Rekurrenzen als $(a_n)_{n\geq 0}$ verwende.)

In Kapitel 3 wurde gezeigt, daß wir für unsere Fragestellung $K \subseteq \mathbb{Q}_p$ (p eine Primzahl) annehmen können. Wenn wir $C = \{a_0, ...a_{m-1}, s_1, ...s_m\} \setminus \{0\}$ setzen, erlaubt uns Satz 3.1 sogar $\|a_i\|_p, \|s_j\|_p \in \{0, 1\}$, $i = 0, ...m-1, j = 1, ...m$, vorauszusetzen.
Daraus folgt insbesondere, daß $a_0, a_1, ...a_{m-1}, s_1, s_2, ...s_m$ ganze p-adische Zahlen sind. Die Rekurrenz $(a_n)_{n\geq 0}$ ist daher eine über $\mathbb{Z}_p$ und kann aus diesem Grund '$mod\, p$' betrachtet werden.
Wir wollen zunächst die Periodizität der Folge $(a_n \mod p)_{n\geq 0}$ zeigen, und mehr noch, daß wir die Periode $\Pi \in \mathbb{N}$ so wählen können, daß für jede andere Rekurrenz $(b_n)_{n\geq 0}$ über $\mathbb{Z}_p$, die derselben Rekurrenzrelation wie $(a_n)_{n\geq 0}$ genügt (i.e. $b_n = s_1 b_{n-1} + ... + s_m b_{n-m}$), Π auch Periode der Folge $(b_n \mod p)_{n\geq 0}$ ist. Dazu benötigen wir folgenden

Hilfssatz 5.1 *Es sei* $(b_n)_{n\geq 0}$ *eine Folge über* $\mathbb{Z}_p$ *mit*

$$b_n = s_1 b_{n-1} + s_2 b_{n-2} + ... + s_m b_{n-m} \quad \forall n \geq m.$$

Dann gibt es eine natürliche Zahl $R \in \{1, 2, ...p^m\}$*, sodaß*

$$b_n \equiv b_{n+R} \ mod\, p \quad \forall n \in \mathbb{N}.$$

Beweis: Betrachte folgende $p^m + 1$ m-tupel:

$$\begin{array}{c}
(b_0, b_1, \ \ ... \ \ b_{m-1}) \ mod\, p \\
(b_1, b_2, \ \ ... \ \ b_m) \ mod\, p \\
... \\
(b_{p^m}, b_{p^m+1} \ \ ... \ \ b_{p^m+m-1}) \ mod\, p
\end{array}$$

Da es genau p^m verschiedene m-tupel $mod\, p$ gibt, folgt aus dem Dirichletschen Schubfachprinzip, daß zumindest zwei dieser $p^m + 1$ m-tupel gleich sein müssen, d.h. es gibt zwei natürliche Zahlen n_1, n_2 mit $0 \leq n_1 < n_2 \leq p^m$ und

$$(b_{n_1}, ...b_{n_1+m-1}) \equiv (b_{n_2}, ...b_{n_2+m-1}) \ mod\, p. \tag{5.1}$$

Setze $R := n_2 - n_1$ ($\Rightarrow 0 < R \leq p^m$).
Wir zeigen zunächst

$$b_{n+R} \equiv b_n \ mod\, p \quad n \geq n_1.$$

Für $n = n_1, n_1 + 1, ...n_1 + m - 1$ folgt das unmittelbar aus (5.1).
Es sei also $n > n_1 + m - 1$ und

$$\begin{array}{rcl}
b_{n-1+R} & \equiv & b_{n-1} \ mod\, p \\
b_{n-2+R} & \equiv & b_{n-2} \ mod\, p \\
 & ... & \\
b_{n-m+R} & \equiv & b_{n-m} \ mod\, p
\end{array}$$

bereits gezeigt. Es folgt

$$b_{n+R} = s_1 b_{n-1+R} + ... + s_m b_{n-m+R} \equiv s_1 b_{n-1} + ... + s_m b_{n-m} = b_n \ mod\, p.$$

Es bleibt zu zeigen:

$$b_{n+R} \equiv b_n \ mod\, p$$

für $n = 0, 1, ...n_1 - 1$. Das machen wir indirekt. Angenommen es gäbe ein solches n mit

$$b_{n+R} \not\equiv b_n \ mod\, p.$$

O.B.d.A können wir annehmen, daß n maximal mit dieser Eigenschaft gewählt wurde und daher

$$b_{n+1+R} \equiv b_{n+1} \ mod\, p$$

$$b_{n+2+R} \equiv b_{n+2} \ \ mod\, p$$

$$...$$

$$b_{n+m+R} \equiv b_{n+m} \ \ mod\, p.$$

Es folgt

$$s_m b_{n+R} = -s_{m-1} b_{n+1+R} - ... - s_1 b_{n+m-1+R} + b_{n+m+R} \equiv$$

$$\equiv -s_{m-1} b_{n+1} - ... - s_1 b_{n+m-1} + b_{n+m} = s_m b_n \ \ mod\, p.$$

Aus $\|s_m\|_p = 1$ (weil $s_m \neq 0$) folgt die Invertierbarkeit von $s_m \ mod\, p$ und wir erhalten $b_{n+R} \equiv b_n \ \ mod\, p$, ein Widerspruch. □

Nun können wir Π, die gemeinsame Periode aller Rekurrenzen $mod\, p$ über $\mathbb{Z}_p$, die derselben Rekurrenzrelation wie $(a_n)_{n\geq 0}$ genügen, definieren:

$$\Pi := (p^m)!$$

Ist dann $(b_n)_{n\geq 0}$ und R wie im Hilfssatz, so folgt aus $R \in \{1, 2, ...p^m\}$, daß $R|\Pi$. Da R eine Periode der Folge $(b_n \ \ mod\, p)_{n\geq 0}$ ist, ist Π erst recht eine.

Unser Ziel ist es zu zeigen, daß sich die Π Teilfolgen

$$(a_{s_0+k\Pi})_{k\geq 0} \qquad s_0 \in \{0, 1, ...\Pi - 1\}$$

der Rekurrenz $(a_n)_{n\geq 0}$ durch p-adische Potenzreihen charakterisieren lassen (im selben Sinn wie in Kapitel 4). Dazu ist folgende Begriffsbildung recht nützlich:

Definition 5.1 *Es sei $(z_n)_{n\geq 0}$ eine beliebige Folge über $\mathbb{Q}_p$. Die Folge $(z_n^{(1)})_{n\geq 0}$, definiert durch $z_n^{(1)} := \frac{z_{n+1}-z_n}{p}$, nenne ich die '1. Differenzenfolge' von $(z_n)_{n\geq 0}$. Die '2. Differenzenfolge' $(z_n^{(2)})_{n\geq 0}$ von $(z_n)_{n\geq 0}$ sei die 1.Differenzenfolge von $(z_n^{(1)})_{n\geq 0}$ u.s.w.*
Allgemein: Die n-te Differenzenfolge von $(z_n)_{n\geq 0}$ sei die $(n-1)$-te Differenzenfolge von $(z_n^{(1)})_{n\geq 0}$.
Die 0. Differenzenfolge sei $(z_n)_{n\geq 0}$ selbst.

Satz 5.1 *Die Folge $(b_n)_{n\geq 0}$ sei wieder eine beliebige Rekurrenz über $\mathbb{Z}_p$, die derselben Rekurrenzrelation wie $(a_n)_{n\geq 0}$ genügt. Es sei $s_0 \in \{0, 1, ...\Pi - 1\}$ fest und $d_k := b_{s_0+k\Pi}$ für $k \in \mathbb{N}$. Dann ist für jedes $n \in \mathbb{N}$ die Folge $(d_k^{(n)})_{k\geq 0}$ eine über $\mathbb{Z}_p$.*

Beweis: Wir zeigen den Satz mit Induktion nach n. Für $n = 0$ ist nichts zu zeigen.
Induktionschritt $n-1 \to n$: Definiere mit Hilfe von $(b_n)_{n\geq 0}$ und Π

$$c_n = \frac{b_{n+\Pi} - b_n}{p}.$$

Die Folge $(c_n)_{n\geq 0}$ ist eine Folge über $\mathbb{Z}_p$, weil $b_{n+\Pi} \equiv b_n \mod p \; \forall n \in \mathbb{N}$. Wegen

$$\begin{aligned} c_n &= \frac{b_{n+\Pi} - b_n}{p} = \\ &= \frac{s_1(b_{n-1+\Pi} - b_{n-1}) + \ldots + s_m(b_{n-m+\Pi} - b_{n-m})}{p} = \\ &= s_1 c_{n-1} + \ldots + s_m c_{n-m} \end{aligned}$$

genügt sie derselben Rekurrenzrelation wie $(b_n)_{n\geq 0}$.
Die Rechnung

$$d_k^{(1)} = \frac{d_{k+1} - d_k}{p} = \frac{b_{s_0+(k+1)\Pi} - b_{s_0+k\Pi}}{p} = c_{s_0+k\Pi}$$

zeigt uns, daß die n-te Differenzenfolge von $(d_k)_{k\geq 0}$ die $(n-1)$-te Differenzenfolge von $(c_{s_0+k\Pi})_{k\geq 0}$ ist. Aus der Induktionsvoraussetzung (angewandt auf die Folge $(c_n)_{n\geq 0}$ anstatt auf $(b_n)_{n\geq 0}$) folgt, daß diese $(n-1)$-te Differenzenfolge eine Folge über $\mathbb{Z}_p$ ist und daher auch die n-te Differenzenfolge von $(d_k)_{k\geq 0}$. □

Im nächsten Satz werden wir zeigen, daß diese einfache Eigenschaft, die wir gerade für die Teilfolgen $(a_{s_0+k\Pi})_{k\geq 0}$ mit $s_0 \in \{0, 1, \ldots \Pi\}$ von $(a_n)_{n\geq 0}$ beobachten konnten, bereits die Entwicklung dieser Teilfolgen in p-adische Potenzreihen ermöglicht. Genauso wie in unserem ersten Beweis des Satzes von Skolem-Mahler-Lech folgt daraus, gemeinsam mit dem Identitätsatz für p-adische Potenzreihen, die Behauptung.

Satz 5.2 *Es sei $d = (d(k))_{k\geq 0}$ eine Folge über $\mathbb{Z}_p$ (wobei wir wieder $p \neq 2$ annehmen), sodaß jede ihrer Differenzenfolgen in $\mathbb{Z}_p^{\mathbb{N}}$ liegt. Dann ist $d(k) = 0$ für höchstens endlich viele k oder $d(k) = 0 \; \forall k \in \mathbb{N}$.*

Beweis: Ich erinnere an den Differenzenoperator $(\Delta d)(k) := d(k+1) - d(k)$ und an den Verschiebungsoperator $(Ed)(k) = d(k+1)$. Diese beiden Operatoren hängen in folgender Weise voneinander ab: $E = 1 + \Delta$.
Aus dem binomischen Lehrsatz folgt

$$d(k) = (E^k d)(0) = (1+\Delta)^k d(0) = \sum_{i=0}^{\infty} \binom{k}{i} \Delta^i d(0) = \sum_{i=0}^{\infty} \binom{k}{i} p^i \left(\frac{\Delta}{p}\right)^i d(0).$$

Mit Hilfe des Differenzenoperator Δ läßt sich die i-te Differenzenfolge von d auch folgendermaßen schreiben: $d^{(i)} = \left(\frac{\Delta}{p}\right)^i d$. Wenn wir für $i \in \mathbb{N}$ folgendes Polynom $(X)_i := X(X-1)\ldots(X-i+1)$ über $\mathbb{Z}$ definieren, so erhalten wir

$$d(k) = \sum_{i=0}^{\infty} (k)_i \frac{p^i}{i!} d^{(i)}(0).$$

Wegen $d^{(i)}(0) \in \mathbb{Z}_p$ und $\|\frac{p^i}{i!}\|_p \stackrel{i\to\infty}{\to} 0$ (Hilfssatz 4.3) ist die rechte Seite (nach längerem Hinsehen, vgl. Analogie zu Satz 4.3) eine p-adische Potenzreihe in k, die zumindest auf $\mathbb{Z}_p$ konvergiert. □

Ganz zufrieden wäre ich gewesen, wenn ich es geschafft hätte, Satz 5.2 direkt, ohne den Umweg über die p-adischen Potenzreihen und den Satz von Strassmann zu zeigen. Obwohl man natürlich niemals nie sagen sollte, glaube ich aber, daß ich intensiv genug probiert habe, um nun der Meinung sein zu können, daß ein anderer Beweis von Satz 5.2 wahrscheinlich nicht einfacher sein kann.
Um zu erklären, was mit 'direkt, ohne Umweg über p-adische Potenzreihen' gemeint sein könnte, möchte ich zum Schluß noch ein anderes Ergebnis über Folgen $(d_k)_{k\geq 0}$ mit Differenzenfolgen über $\mathbb{Z}_p$ zeigen, welches einerseits aus der (speziellen Form der) Potenzreihenentwicklung, die wir im Beweis von Satz 5.2 hergeleitet haben, folgen würde, sich andererseits aber auch 'direkt' zeigen läßt:

Satz 5.3 *Es sei $(d_k)_{k\geq 0}$ wie in Satz 5.2 und $n \geq 1$ eine natürliche Zahl. Dann ist p^{n-1} eine Periodelänge der Folge $(d_k \mod p^n)_{k\geq 0}$.*

Beweis: Wir zeigen die Behauptung im Satz und

$$d_k + d_{k+1} + ... + d_{k+p^n-1} \equiv 0 \mod p^n \quad \forall k \in \mathbb{N}$$

mit Induktion nach n.
Induktionsanfang n=1: Da die erste Differenzenfolge $\left(\frac{d_{k+1}-d_k}{p}\right)_{k\geq 0}$ eine Folge über $\mathbb{Z}_p$ ist, muß $d_{k+1} \equiv d_k \mod p$ für jedes $k \geq 0$ erfüllt sein. Das bedeutet, daß die Folge $(d_k \mod p)_{k\geq 0}$ konstant ist und damit ist die Behauptung im Satz für $n = 1$ gezeigt. Die zweite Behauptung ergibt sich so: Es sei $k \in \mathbb{N}$ beliebig. Dann folgt

$$d_k + d_{k+1} + ... + d_{k+p-1} \equiv d_0 + d_0 + ... + d_0 \equiv p \cdot d_0 \equiv 0 \mod p$$

Induktionsschritt $n-1 \to n$: Wieder zeigen wir zuerst die Behauptung im Satz: Die Induktionsvoraussetzung angewandt auf die erste Differenzenfolge $(d_k^{(1)})_{k\geq 0}$ ergibt

$$d_k^{(1)} + d_{k+1}^{(1)} + ... + d_{k+p^{n-1}-1}^{(1)} \equiv 0 \mod p^{n-1}$$

für alle natürlichen Zahlen k. Gemeinsam mit der Identität

$$d_{k+p^{n-1}} = d_k + p \sum_{i=k}^{k+p^{n-1}-1} d_i^{(1)}$$

folgt daraus die Behauptung im Satz.
Nun zur zweiten Behauptung: Es sei $k \in \mathbb{N}$. Aus dem eben gezeigten folgt

$$\begin{aligned} d_k + d_{k+1} + ... + d_{k+p^{n-1}-1} &\equiv d_{k+p^{n-1}} + d_{k+p^{n-1}+1} + ... + d_{k+2p^{n-1}-1} \equiv ... \\ ... &\equiv d_{k+(p-1)p^{n-1}} + d_{k+(p-1)p^{n-1}+1} + ... + d_{k+p^n-1} \mod p^n. \end{aligned}$$

und daher

$$d_k + d_{k+1} + ... + d_{k+p^n-1} \equiv p(d_k + d_{k+1} + ... + d_{k+p^{n-1}-1}) \equiv 0 \mod p^n$$

(da $d_k + d_{k+1} + ... + d_{k+p^{n-1}-1} \equiv 0 \mod p^{n-1}$ nach Induktionsvoraussetzung). □

Folgerung *Es sei $(b_n)_{n\geq 0}$ eine Rekurrenz über $\mathbb{Z}_p$, die derselben Rekurrenzrelation wie $(a_n)_{n\geq 0}$ genügt. Dann ist $p^{n-1}\Pi$ eine Periode der Folge $(b_n \mod p^n)_{n\geq 0}$.*

5.2 Vergleich der beiden Beweise

Die Grundidee beider Beweise ist dieselbe: Wir fassen die gegebene Rekurrenz $(a_n)_{n\geq 0}$ als eine Funktion $a : \mathbb{N} \to \mathbb{Q}_p$ auf, die wir mit Hilfe von endlich vielen p-adischen Potenzreihen zu einer Funktion $A : \mathbb{Z}_p \to \mathbb{Q}_p$ fortsetzen. Schließlich benützen wir analytische Mittel, um das gewünschte Ergebnis für die Nullstellenmenge der Funktion A und damit auch für a herzuleiten.

Der Unterschied liegt in der Art und Weise, wie man zu der Potenzreihenentwicklung gelangt.

Beim ersten Beweis verwendet man die explizite Darstellung der Rekurrenz durch ein Exponentialpolynom und zeigt dann, daß dieses durch endlich viele Potenzreihen charakterisierbar ist. Dabei genügt es zu zeigen, daß die 'Exponentialfunktion' $n \mapsto \alpha^n$ (wenn $\alpha \in \mathbb{Z}_p$ und $\alpha \equiv 1 \ \ mod\, p$) mit Hilfe einer p-adischen Potenzreihe auf $\mathbb{Z}_p$ fortsetzbar ist.
Im Nachhinein betrachtet, erscheint mir diese Idee recht naheliegend, wenn man erst einmal darauf gekommen ist, die Rekurrenzen über $\mathbb{Q}_p$ zu betrachten und die Darstellung durch Exponentialpolynome kennt. Denn da die Exponentialfunktion über $\mathbb{C}$ durch eine Potenzreihe darstellbar ist, wird man in $\mathbb{Q}_p$ ähnliches erwarten, auch wenn dort nicht alles so glatt verläuft wie in $\mathbb{C}$ (das Konvergenzgebiet der p-adischen Potenzreihe ist i.a. nicht ganz $\mathbb{Q}_p$ und außerdem existiert sie nicht für jede Basis $\alpha \in \mathbb{Q}_p$.).

Die in diesem Kapitel vorgestellte Variante des Beweises schließt relativ direkt, wenn auch ein wenig trickreich, mit Hilfe der Linearität der Rekursion und der Möglichkeit Folgen über $\mathbb{Z}_p \ mod\ p^n$ zu betrachten, auf die Entwicklung in p-adische Potenzreihen.

Mein Problem bei dieser Betrachtungsweise der beiden Beweise ist, daß sie mir nicht erklärt, wie man beim Beweis des Satzes auf die Idee kommen konnte, daß die p-adische Analysis eine so hilfreiche Rolle spielen kann [1]. Und daß Skolem wahrscheinlich einen guten Grund gehabt haben muß, p-adische Methoden zu verwenden, sieht man schon daran, daß er den Beweis seines Satzes fand, ohne die p-adische Analysis vorher gekannt zu haben. Er entwickelte die Elemente der p-adischen Analysis, die er in diesem Zusammenhang benötigte, selber (siehe Abschnitt 4.3).
Über Skolems Motivation p-adische Analysis zu verwenden, kann ich natürlich nichts schreiben. Ich möchte daher versuchen zu schildern, wie ich mir den Übergang zu $\mathbb{Q}_p$ erklären kann:

[1] D.h. ein plausibler Grund aus der Sichtweise der Exponentialpolynome zu $\mathbb{Q}_p$ überzugehen, ist mir schon eingefallen.
In den Abschnitten 2.5 und 2.6 haben wir gesehen, wie nützlich die p-adische Methode bei algebraischen diophantischen Gleichungen ist. Man könnte daher vermuten, daß man damit bei diophantischen Gleichungen in Exponentialpolynomen ebenso erfolgreich ist. Daß das tatsächlich so ist, beruht auf der Tatsache, daß sich p-adische Potenzreihen in einem gewissen Sinn ähnlich wie Polynome verhalten (siehe Satz von Strassmann für Polynomfolgen). Aus diesem Grund sind auch die erwähnten Verallgemeinerungen (siehe Abschnitt 2.6) des Henselschen Lemmas auf Potenzreihen möglich.
Diese Motivation, beim Beweis des Satzes von Skolem-Mahler-Lech zu $\mathbb{Q}_p$ überzugehen, ist aber meiner Meinung nach nur dann möglich, wenn man schon vorher einiges über p-adische Analysis weiß.

Es sei $(a_n)_{n\geq 0}$ wieder eine beliebige Rekurrenz, die der Rekurrenzrelation

$$a_n = s_1 a_{n-1} + s_2 a_{n-2} + ... + s_m a_{n-m}$$

für $n \geq m$ genügt. Wenn diese Rekurrenz nur endlich viele Werte annimmt (i.e. $|\{a_n|n \in \mathbb{N}\}| < \infty$), so haben wir in Hilfssatz 5.1, aber auch schon am Ende von Abschnitt 1.3, gesehen, daß $(a_n)_{n\geq 0}$ periodisch sein muß. Für solche Rekurrenzen ist der Beweis des Satzes von Skolem-Mahler-Lech daher sehr einfach (in Hilfssatz 5.1 haben wir eigentlich nicht direkt dieses Ergebnis gezeigt – aber genauso wie dort könnte man es zeigen.). Relativ bald, nachdem ich den Beweis des Satzes von Skolem-Mahler-Lech kennengelernt habe, dachte ich, daß diese leicht zu sehende Tatsache ein Grund für den Übergang zu $\mathbb{Q}_p$ sein könnte. Denn in $\mathbb{Z}_p$ sind wir ja in der Lage die Rekurrenzen $mod\, p^k$ zu betrachten: Die Rekurrenz $(a_n \;\; mod\, p^k)_{n\geq 0}$ nimmt nur endlich viele Werte an, und ist daher periodisch (siehe Hilfssatz 5.1, man kann ihn für die Folgen $(a_n \;\; mod\, p^k)_{n\geq 0}$ mit $k \neq 1$ genauso beweisen, wenn man R passend in der größeren Menge $\{1, 2, ...p^{km}\}$ wählt und beachtet, daß $s_m \;\; mod\, p^k$ invertierbar ist, weil $\|s_m\|_p = 1$; für eine quantitiative Aussage über die Periodenlänge dieser Rekurrenzen siehe Satz 5.3). Mit der Periodizität dieser Folgen alleine ist uns aber noch nicht geholfen: Es wäre ja zum Beispiel möglich, daß $(a_n \;\; mod\, p)_{n\geq 0}$ eine Nullstellenmenge der Form $\Pi\mathbb{N}$ hat, die Rekurrenz $(a_n \;\; mod\, p^2)_{n\geq 0}$ eine der Form $(\Pi + p\Pi\mathbb{N}) \cup (p\Pi\mathbb{N})$ und allgemein

$$\{n \in \mathbb{N}|a_n \equiv 0 \;\; mod\, p^k\} = (\Pi + p^{k-1}\Pi\mathbb{N}) \cup (p\Pi + p^{k-1}\Pi\mathbb{N}) \cup ... \cup (p^{k-2}\Pi + p^{k-1}\Pi\mathbb{N}).$$

Es würde $\{n \in \mathbb{N}|a_n = 0\} = \{\Pi, p\Pi, p^2\Pi, ...\}$ folgen, und das ist ja unmöglich. Da mir zusätzlich der in Kapitel 2, 3 und 4 vorgestellte Beweis des Satzes von Skolem-Mahler-Lech kaum Anlaß zur Vermutung gab, daß man mit Hilfe solcher Überlegungen doch noch einen Beweis basteln könnte, gab ich es zunächst einmal auf.

Man kann aber die Idee mit den Rekurrenzen, deren Wertebereich endlich ist, noch etwas verallgemeinern. Ich will diese Idee anhand eines Beispieles erklären: Angenommen $(a_n)_{n\geq 0}$ wäre eine Rekurrenz über $\mathbb{R}$, sodaß $a_n \geq 0 \; \forall n \in \mathbb{N}$ und $s_i \geq 0$ für $i = 1, 2, ...m$. Wir 'partitionieren' den Wertebereich $\mathbb{R}^+$ in die zwei Mengen $P = \mathbb{R}^+ \setminus \{0\}$ und $N = \{0\}$. Dann bilden diese beiden Mengen bezüglich der elementweisen Addition: $P + P = P, P + N = P, N + N = N$ ein kommutatives Monoid (mit Nullelement N) und bezüglich der elementweisen Multiplikation: $P \cdot P = P, P \cdot N = N, N \cdot N = N$ eine abelsche Gruppe (mit Einselement P). Außerdem erfüllt diese algebraische Strukur $\{P, N\}$ das Distributivgesetz und ist bezüglich der Multiplikation mit den Koeffizienten s_i abgeschlossen. Mit Hilfe der Rekurrenz $(a_n)_{n\geq 0}$ definieren wir eine Rekurrenz $(b_n)_{n\geq 0}$ über $\{P, N\}$, die derselben Rekurrenzrelation wie $(a_n)_{n\geq 0}$ genügt: Für $i = 0, 1, ...m - 1$ sei $b_i = N \Leftrightarrow a_i = 0$. Es folgt, daß die Nullstellenmenge $\{n \in \mathbb{N}|b_n = N\}$ der Rekurrenz $(b_n)_{n\geq 0}$ mit der von $(a_n)_{n\geq 0}$ übereinstimmt. Da $(b_n)_{n\geq 0}$ eine Rekurrenz über einer endlichen algebraischen Struktur mit den beschriebenen Eigenschaften ist ($\{P, N\}$ ist fast ein Körper; nur bezüglich der Addition hat P kein Inverses), erfüllt sie den Satz von Skolem-Mahler-Lech und dasselbe gilt daher für die Rekurrenz $(a_n)_{n\geq 0}$ (Genauso wie in Hilfssatz 5.1 kann man zeigen, daß eine Rekurrenz über diesem 'fast-Körper' $\{P, N\}$ ab einer gewissen Stelle periodisch ist).

Ist nun $(a_n)_{n\geq 0}$ wieder eine beliebige Rekurrenz, so könnte man sich fragen, ob man die Wertenmenge $\{a_n|n \in \mathbb{N}\}$ (oder eine Obermenge davon) vielleicht ähnlich geschickt in endlich

viele Teilmenge zerlegen kann, um dann so auf analoge Weise den Satz von Skolem-Mahler-Lech zu erhalten. Ich habe das für andere Klassen von Rekurrenzen ausprobiert – allerdings sind die präsentierten Beispiele (wenn $(a_n)_{n\geq 0}$ nur endlich viele Werte annimmt oder $(a_n)_{n\geq 0}$ eine Rekurrenz über $\mathbb{R}^+$ ist) die besten davon (Sonst müßte man bei meinen Beispielen immer relativ gekünstelte Bedingungen über den Bildbereich der Rekurrenz $(a_n)_{n\geq 0}$ voraussetzen, wie z.B. $\{a_n | n \in \mathbb{N}\} \supseteq (1+3\mathbb{Z}) \cup (2+3\mathbb{Z}) \cup \{0\}$ etc.). Hinzu kommt, daß diese Partitionen oft Körper bilden und daher von vornherein klar ist, daß sie nicht bei jeder Rekurrenz zielführend sein können: So eine Parition des Wertebereichs könnte nämlich nur bei Rekurrenzen erfolgbringend sein, deren Nullstellenmenge die Vereinigung endlich vieler arithmetischer Progressionen sind. Diese endlich vielen 'Ausnahmenullstellen', wie sie schon bei unseren einfachen Beispielen (2),(3) und (4) auftauchen, wären mit dieser Methode nicht zu bewältigen.
Wir verallgemeinern daher noch einmal: Es sei $(a_n)_{n\geq 0}$ und Π wie in Abschnitt 5.1. Wir konstruieren eine Folge von Partitionen einer Obermenge des Wertebereichs von $(a_n)_{n\geq 0}$. In der Kapitel 3 haben wir gesehen, daß wir o.B.d.A. annehmen dürfen, daß $\mathbb{Z}_p$ eine Obermenge von $\{a_n | n \in \mathbb{N}\}$ ist. Die erste Partition in der Folge sei

$$\{p\mathbb{Z}_p, 1+p\mathbb{Z}_p, ...(p-1)+p\mathbb{Z}_p\}.$$

Die nächste Partition ist eine Verfeinerung der ersten:

$$\{p^2\mathbb{Z}_p, 1+p^2\mathbb{Z}_p, ...(p^2-1)+p^2\mathbb{Z}_p\}$$

u.s.w. Allgemein:

$$\{p^k\mathbb{Z}_p, 1+p^k\mathbb{Z}_p, ...(p^k-1)+p^k\mathbb{Z}_p\} \qquad k=1,2,3,...$$

Diese Partitionen sind ähnlich geschickt gewählt wie P und N bei den Rekurrenzen mit positiven Koeffizienten und Folgengliedern, weil sie einen kommutativen Ring mit Einselement bezüglich elementweiser Operationen bilden. Sie haben allerdings den Nachteil, daß die Null nicht in einer eigenen Menge isoliert wird. Dafür ist aber zumindest $\bigcap_{k=0}^{\infty} p^k\mathbb{Z}_p = \{0\}$.
Jetzt sind wir wieder an der Stelle, wo wir auf die Periodizität der Folgen $(a_n \mod p^k)_{n\geq 0}$ schließen können, über die ich weiter oben schon geschrieben habe, daß sie ohne weitere Idee nicht zielführend sein kann (Denn ist $k \in \mathbb{N}$ fest und betrachtet man die k-te Partition in der definierten Folge, so ist $a_n \in i + p^k\mathbb{Z}_p \Leftrightarrow a_n \equiv i \mod p^k$.).
Diese notwendige Idee ist die folgende: Wir haben gesehen, daß wir zeigen müßten, daß die Nullstellenmengen der Rekurrenzen $(a_n \mod p^k)_{n\geq 0}$, $k=1,2,3,...$, nicht unabhängig voneinander jede Form annehmen können, denn sonst könnte es passieren, daß zum Beispiel $\{n \in \mathbb{N} | a_n = 0\} = \{\Pi, p\Pi, p^2\Pi, ...\}$. Es ist daher nun wichtig zu beobachten, daß die Folge $(a_n^{(1)})_{n\geq 0} := \left(\frac{a_{n+\Pi}-a_n}{p}\right)_{n\geq 0}$ auch eine Rekurrenz über $\mathbb{Z}_p$ ist, die derselben Rekurrenzrelation wie $(a_n)_{n\geq 0}$ genügt (Satz 5.1). Es folgt

$$a_{s_0+k\Pi} \equiv a_{s_0} + p\sum_{i=0}^{k-1} a_{s_0+i\Pi}^{(1)} \equiv a_0 + p(k-1)a_{s_0}^{(1)} \mod p^2$$

und daher ist die Rekurrenz $(a_n \ \ mod\, p^2)_{n\geq 0}$ schon etwas eingeschränkter, als bloß durch ihre Periodizität. Wenn man diese Rechnung induktiv fortsetzt, erhält man für den Fall $p \neq 2$ die Potenzreihenentwicklung der Folge $(a_{s_0+k\Pi})_{k\geq 0}$ und daraus die Aussage über die Nullstellenmenge der Rekurrenz $(a_n)_{n\geq 0}$ (Satz 5.2).

Man kann natürlich noch versuchen, durch ähnliche Partitionen oder Folgen von Partitionen des Wertebereichs anders zum selben Resultat oder vielleicht auch zu anderen, neuen Resultaten zu kommen. Ein Beispiel, das leider (noch) nicht zielführend ist: Bei Rekurrenzen über dem Integritätsbereich $\mathbb{F}_p[X]$ könnte man mit Hilfe des Primideals (X) auf dieselbe Weise eine Folge von Partitionen konstruieren, wie wir es in $\mathbb{Z}_p$ mit Hilfe des Primideals (p) gemacht haben: Ebenso wie $\mathbb{Z}_p/(p)\mathbb{Z}_p$ ist $\mathbb{F}_p[X]/(X)$ endlich und $\bigcap\limits_{i=1}^{\infty}(X^i) = \{0\}$. Wir wissen aber aus Abschnitt 1.3, daß der Satz von Skolem-Mahler-Lech für den Quotientenkörper $\mathbb{F}_p[X]$ nicht allgemein gilt. Daraus ergibt sich, daß irgendetwas auf dem weiteren Weg des Beweises des Satzes von Skolem-Mahler-Lech nicht auf $\mathbb{F}_p[X]$ und die definierte Folge von Partitionen übertragbar ist: In Satz 5.2 haben wir, um auf die Potenzreihenentwicklung schließen zu können, verwendet, daß der (gekürzte) Zähler des Bruchs $\frac{p^i}{i!}$ für große i durch eine große Potenz von p teilbar ist. In $\mathbb{F}_p[X]$ findet das für den Bruch $\frac{X^i}{i!}$ kein Analogon, zumal das Inverse von $i!$ für $i \geq p$ in $\mathbb{F}_p$ nicht einmal definiert ist. Aus diesem Blickwinkel wird auf einmal Hilfssatz 4.1 zu einer weiteren Schlüsselstelle, mit Hilfe dessen wir die Behauptung über die Brüche $\frac{p^i}{i!}$ hergeleitet haben.

(Um die Partitionierung von $\mathbb{F}_p[X]$ wirklich auf die in Abschnitt 1.3 definierte Folge $(u_n)_{n\geq 0}$ anwenden zu können, hätten wir statt (X) ein anderes Primideal wählen müssen, z.B. (1-X), weil $s_3 = X^2 + X \in (X)$.)

Ich möchte zum Abschluß dieses Kapitels noch zeigen, daß man den in diesem Kapitel vorgestellten Beweis des Satzes von Skolem-Mahler-Lech für den Spezialfall $K = \mathbb{Q}$ noch wesentlich vereinfachen kann. In diesem Fall kommt man nämlich ohne den Körper der p-adischen Zahlen und ohne den Einbettungsatz 3.1. aus (d.h. Kapitel 2 und 3 sind dafür unnötig):

Ist nämlich $(a_n)_{n\geq 0}$ eine Rekurrenz über $\mathbb{Q}$ mit

$$a_n = s_1 a_{n-1} + s_2 a_{n-2} + ... + s_m a_{n-m}$$

für $n \geq m$ $(s_1, s_2, ... s_m \in \mathbb{Q}$ und $s_m \neq 0)$, dann gilt für fast alle Primzahlen p, daß man die Elemente $a_0, a_1, ... a_{m-1}, s_1, s_2, ... s_m \ mod\, p$ betrachten kann und $s_m \not\equiv 0 \ mod\, p$ (nämlich genau für jene Primzahlen p, die die gekürzten Nenner der Elemente der Menge $\{a_0, a_1, ... a_{m-1}, s_1, s_2, ... s_m\} \setminus \{0\}$ nicht teilen und zusätzlich den Zähler von s_m auch nicht teilen).

Es sei p so eine Primzahl und $\mathbb{Z}^p := \{\frac{a}{b} | a, b \in \mathbb{Z}, p \nmid b\} = \mathbb{Z}_p \cap \mathbb{Q}$. $\mathbb{Z}^p$ ist ein Teilring von $\mathbb{Q}$, in dem man jedes Element $mod\, p$ betrachten kann. Wenn man im obigen Beweis nur immer $\mathbb{Z}_p$ durch diesen Ring $\mathbb{Z}^p$ ersetzt, sieht man, daß man den Satz für die Rekurrenz $(a_n)_{n\geq 0}$ über $\mathbb{Q}$ auch ohne p-adische Zahlen zeigen kann. (Im ersten Beweis, der in Kapitel 4 vorgestellt wurde, kann man das nur machen, wenn das Exponentialpolynom zur Rekurrenz $(a_n)_{n\geq 0}$ über $\mathbb{Q}$ definiert ist, d.h. wenn das Polynom $1 - s_1X - s_2X^2 - ... - s_mX^m$ nur rationale Nullstellen hat.)

Kapitel 6

Folgerungen aus dem Satz von Skolem-Mahler-Lech

Beschäfigt man sich ein wenig mit der Literatur zur Theorie der linearen Rekursionsfolgen, so bemerkt man, daß der Satz von Skolem-Mahler-Lech eine wichtige Rolle spielt. Einerseits gibt er natürlich Anlaß für unzählige Fragen über die genauere Struktur der Nullstellenmenge von Rekurrenzen. Er taucht aber auch an Stellen auf, wo man ihn zunächst vielleicht nicht erwartet hätte.
Mit diesem letzten Kapitel meiner Diplomarbeit möchte ich dem Leser daher einen kleinen Einblick in mögliche Konsequenzen geben.

Im Folgenden sei $(a_n)_{n\geq 0}$ eine Rekurrenz über dem Körper K, $\mathrm{char}(K) = 0$, die der Rekurrenzrelation

$$a_n = s_1 a_{n-1} + s_2 a_{n-2} + ... + s_m a_{n-m} \tag{6.1}$$

für $n \geq m$ genügt, wobei wir wie immer o.B.d.A. $s_m \neq 0$ annehmen. Weiters sei

$$a_n = \sum_{i=1}^{k} A_i(n)\alpha_i^n \tag{6.2}$$

das zur Rekurrenz $(a_n)_{n\geq 0}$ gehörige Exponentialpolynom, sodaß $\alpha_i \neq \alpha_j \neq 0$ für $i \neq j$. Mit $A_{ij} \in K$ bezeichnen wir den Koeffizienten von X^j im Polynom $A_i(X)$.
Schließlich seien $d \in \mathbb{N}$, $r_1, r_2, ...r_l \in \{0, 1, ...d-1\}$ und $A \subset \mathbb{N}$, $|A| < \infty$, so gewählt, daß

$$\{n \in \mathbb{N} | a_n = 0\} = \left(\bigcup_{f=1}^{l} r_f + d\mathbb{N}\right) \cup A. \tag{6.3}$$

6.1 Zwei einfache Verallgemeinerungen

An erster Stelle in diesem Abschnitt muß wohl folgende stärkere Version des Satzes von Skolem-Mahler-Lech stehen:

Satz 6.1 *Für $i = 1, 2, ...k$ seien $(a_n^{(i)})_{n\geq 0}$ Rekurrenzen über K und $P(X_1, X_2, ...X_k)$ ein Polynom in $K[X_1, X_2, ...X_k]$. Dann ist*

$$\{n \in \mathbb{N} | P(a_n^{(1)}, a_n^{(2)}, ...a_n^{(k)}) = 0\}$$

die Vereinigung einer endlichen Menge und endlich vieler arithmetischer Progressionen.

Beweis: Es genügt zu zeigen, daß die Folge $(P(a_n^{(1)}, a_n^{(2)}, ...a_n^{(k)}))_{n\geq 0}$ eine Rekurrenz ist. Am schnellsten sieht man das mit Hilfe der Exponentialpolynome: Die Menge aller Exponentialpolynome über K bildet eine Algebra (über K). Da jede Rekurrenz $(a_n^{(i)})_{n\geq 0}$ durch ein Exponentialpolynom darstellbar ist, gilt das auch für $(P(a_n^{(1)}, a_n^{(2)}, ...a_n^{(k)}))_{n\geq 0}$. Wegen der in Kapitel 1 gezeigten Äquivalenz von Rekurrenzen und Exponentialpolynomen folgt die Behauptung. □

Bemerkung Aus Satz 6.1 folgt zum Beispiel: Es sei $c \in K$ beliebig. Dann ist die 'c-Stellenmenge' $\{n \in \mathbb{N} | a_n = c\}$ die Vereinigung einer endlichen Menge und endlich vieler arithmetischer Progressionen.
Oder: Ist $(b_n)_{n\geq 0}$ eine zweite Rekurrenz über K, dann sind die Mengen $\{n \in \mathbb{N} | a_n = b_n\}$ und $\{n \in \mathbb{N} | a_n b_n = c\}$ ebenfalls Vereinigungen einer endlichen Menge und endlich vieler arithmetischer Progressionen.

Den Satz kann man aber auch in eine etwas andere Richtung verallgemeinern: Betrachte folgende lineare Abbildung $S : K^m \to K^m$:

$$S(x_1, x_2, ...x_m) = (x_2, x_3, ...x_m, s_1 x_m + s_2 x_{m-1} + ... + s_m x_1).$$

Setze $\vec{a} = (a_0, a_1, ...a_m)$. Dann ist a_n gerade die erste Koordinate von $S^n(\vec{a})$ oder, für $n \geq m$, die m-te Koordinate von $S^{n-m}(\vec{a})$. Laut Definition der Abbildung S ist die m-te Koordinate von $S^{n-m}(\vec{a})$ genau dann Null, wenn $S^{n-m-1}(\vec{a})$ orthogonal auf $\vec{s} = (s_m, s_{m-1}, ...s_1)$ steht, also genau dann, wenn $S^{n-m-1}(\vec{a})$ im $m-1$-dimensionalen Teilraum $\vec{s}^\perp$ liegt.
Die Aussage des Satzes von Skolem-Mahler-Lech in dieser Sichtweise ist daher:
Die Menge aller natürlichen Zahlen n, für die $S^n(\vec{a})$ im Teilraum $\vec{s}^\perp$ liegt, ist die Vereinigung einer endlichen Menge und endlich vieler arithmetischer Progressionen.
(Der Begriff 'orthogonal' muß im Vektorraum K^m zunächst nicht definiert sein. Gemeint ist: $(v_1, v_2, ...v_m) \perp (w_1, w_2, ...w_m) \Leftrightarrow v_1 w_1 + v_2 w_2 + ... + v_m w_m = 0$)
Folgende Verallgemeinerung ist möglich:

Satz 6.2 *Es sei $A : \mathbb{C}^m \mapsto \mathbb{C}^m$ eine beliebige invertierbare lineare Abbildung, $\vec{x} \in \mathbb{C}^m$ und W ein Teilraum des Vektorraumes $\mathbb{C}^m$. Dann ist die Menge*

$$\{n \in \mathbb{N} | A^n(\vec{x}) \in W\}$$

die Vereinigung einer endlichen Menge und endlich vieler arithmetischer Progressionen.

Beweis Ist $W = \mathbb{C}^m$, so ist nichts zu zeigen.
Wir können also annehmen, daß $dim(W) \leq m-1$. Da jeder Teilraum von $\mathbb{C}^m$, dessen Dimension kleiner als $m-1$ ist, als Schnitt endlich vieler Hyperebenen darstellbar ist, genügt es den Satz für $dim(W) = m-1$ zu zeigen.
Es gibt daher einen Vektor $\vec{w} \in \mathbb{C}^m$, sodaß $W = \vec{w}^{\perp}$ bezüglich des Standardskalarproduktes des unitären Vektorraumes $\mathbb{C}^m$ ist. Wenn wir zeigen, daß die Folge $(A^n(\vec{x}) \cdot \vec{w})_{n \geq 0}$ eine Rekurrenz ist, sind wir nach dem Satz von Skolem-Mahler-Lech fertig, denn wegen der Wahl von $\vec{w}$ ist

$$\{n \in \mathbb{N} | A^n(\vec{x}) \cdot \vec{w} = 0\} = \{n \in \mathbb{N} | A^n(\vec{x}) \in W\}$$

Da $m+1$ Vektoren in einem m-dimensionalen Vektorraum stets linear abhängig sind, gibt es eine natürliche Zahl $0 < k \leq m$ und Koeffizienten $y_1, ...y_k \in \mathbb{C}$, mit

$$A^k(\vec{x}) = y_1 A^{k-1}(\vec{x}) + y_2 A^{k-2}(\vec{x}) + ... + y_k A^0(\vec{x}). \tag{6.4}$$

Sind alle Koeffizienten $y_i = 0$, dann ist $A^k(\vec{x}) = 0$ und wegen der Invertierbarkeit von A folgt induktiv $A^0(\vec{x}) = 0$. In diesem Fall ist die Folge $(A^n(\vec{x}) \cdot \vec{w})_{n \geq 0}$ die Nullfolge und der Satz in trivialer Weise erfüllt.
Wir können also annehmen, daß nicht alle Koeffizienten $y_i = 0$ sind. Unter $n-k$-maliger Anwendung von A folgt aus (6.4)

$$A^n(\vec{x}) = y_1 A^{n-1}(\vec{x}) + y_2 A^{n-2}(\vec{x}) + ... + y_k A^{n-k}(\vec{x})$$

und daher

$$(A^n(\vec{x}) \cdot \vec{w}) = y_1(A^{n-1}(\vec{x}) \cdot \vec{w}) + y_2(A^{n-2}(\vec{x}) \cdot \vec{w}) + ... + y_k(A^{n-k}(\vec{x}) \cdot \vec{w})$$

für $n \geq m$. $\square$

Bemerkung

(1) Daß wir den Satz nur für $K = \mathbb{C}$ gezeigt haben, ist keine wesentliche Einschränkung, da man jeden endlich erzeugten Körper über $\mathbb{Q}$ in den Körper des komplexen Zahlen einbetten kann (siehe Fußnote am Beginn von Kapitel 4).

(2) Für nicht-invertierbare lineare Abbildungen gilt der Satz analog, bis auf die Möglichkeit, daß die Menge $\{n \in \mathbb{N} | A^n(\vec{x}) \in W\}$ auch noch von der Form $\{k+1, k+2, k+3, ...\}$ sein kann, wobei k eine natürliche Zahl mit $k \leq m$ ist.
Die Abbildung S ist invertierbar, weil $s_m \neq 0$.

(3) Anhand dieser Verallgemeinerung versteht man vielleicht auch etwas besser, wieso der Satz von Skolem-Mahler-Lech für Rekurrenzen der Ordnung 1 und 2 trivial ist und daher in diesen Fällen auch für Körper mit beliebiger Charakteristik gilt (siehe Abschnitt 1.2): Satz 6.2 ist für jedes $m \in \mathbb{N}$ trivial, wenn $dim(W) = m$ oder $dim(W) = 1$. Für $m = 1, 2$ sind das aber die einzig möglichen Fälle.

6.2 Ein Zerlegungssatz für Rekurrenzen

Wir erinneren uns an die Rekurrenzen $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0}$ und $(c_n)_{n\geq 0}$ aus Kapitel 1 (Abschnitt 1.1, Beispiele (2),(3) und (4)). Gemeinsam ist diesen drei Rekurrenzen, daß sie unendlich viele Nullstellen haben. Wir konnten die Nullstellenmengen relativ einfach mit Hilfe ihrer Exponentialpolynome bestimmen (einfach zum Beispiel im Vergleich zur Rekurrenz $(u_n)_{n\geq 0}$ über $\mathbb{F}_p[X]$, Abschnitt 1.3): Ist nämlich $(d_n)_{n\geq 0}$ eine von diesen Rekurrenzen, so haben wir die Existenz zweier Rekurrenzen $(e_n)_{n\geq 0}$ und $(f_n)_{n\geq 0}$ gezeigt, mit

$$d_n = e_n \cdot f_n,$$

wobei $(e_n)_{n\geq 0}$ periodisch und $\{n \in \mathbb{N} | f_n = 0\}$ endlich ist. Außerdem haben wir gezeigt, daß die Nullstellenmenge von $(e_n)_{n\geq 0}$ unendlich groß ist und wegen der Periodizität dieser Rekurrenz folgt

$$\{n \in \mathbb{N} | e_n = 0\} = \bigcup_{r\in\{0,1,...d'-1\}:e_r=0} (r + d'\mathbb{N}),$$

wenn $d' \in \mathbb{N}$ die Periodenlänge bezeichnet.
(Für $(a_n)_{n\geq 0}$ setzen wir $e_n^{(a)} = (1 + (-1)^n)$ und $f_n^{(a)} = (\sqrt{2})^n(4 - n + \frac{n^2}{16})$, bei $(b_n)_{n\geq 0}$ setzen wir $e_n^{(b)} = \left(-\left(\frac{1+\sqrt{3}i}{2}\right)^n + \left(\frac{1-\sqrt{3}i}{2}\right)^n\right)$ und $f_n^{(b)} = 3^n\left(\frac{\sqrt{3}}{3}i\right)$, und schließlich $e_n^{(c)} = (1 + (-1)^n)$ und $f_n^{(c)} = \left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)\frac{1}{2\sqrt{5}}$ bei $(c_n)_{n\geq 0}$.)
Auf diese Weise erhielten wir auch sofort den Satz von Skolem-Mahler-Lech für diese drei Rekurrenzen. In diesem Abschnitt wollen wir untersuchen, ob es ein Zufall bei der Wahl dieser Beispiele war, daß an ihrem Exponentialpolynom ziemlich schnell das Nullstellenverhalten erkennbar ist. Kann man vielleicht jede Rekurrenz $(a_n)_{n\geq 0}$, die unendlich viele Nullstellen hat, in zwei Rekurrenzen $(e_n)_{n\geq 0}$ und $(f_n)_{n\geq 0}$ mit obigen Eigenschaften zerlegen?

Dazu benötigen wir folgenden 'Identitätssatz' für Exponentialpolynome:

Hilfssatz 6.1 *Es sei $F(X) = \sum_{i=1}^{k} B_i(X)\beta_i^X$ ein Exponentialpolynom über K, wobei wir $\beta_i \neq \beta_j$, wenn $i \neq j$, und $\beta_i \neq 0$ für $i = 1, 2, ...k$ annehmen. Ist $F(n) = 0 \quad \forall n \in \mathbb{N}$, dann folgt $B_i(X) \equiv 0$ für $i = 1, 2, ...k$ und daher $F(X) \equiv 0$.*

Beweis Ich erinnere an die Definintion des Grades des Exponentialpoynoms $F(X)$:

$$deg(F) = k + \sum_{i=1}^{k} deg(B_i).$$

Wir beweisen den Hilfssatz mit Induktion nach dem Grad von $F(X)$: Für $k = 1$ ist $F(X) = B_1(X)\beta_1^X$ und wegen $\beta_1 \neq 0$ folgt $F(n) = 0 \quad \forall n \in \mathbb{N}$ genau dann, wenn $B_1(n) = 0 \quad \forall n \in \mathbb{N}$ und daher genau dann, wenn $B_1(X) \equiv 0$. Das ergibt insbesondere den Hilfssatz für $deg(F) = 1$.
Nun sei $n := deg(F) > 1$. Wir nehmen an, daß der Satz für alle Exponentialpolynome, deren

Grad kleiner als n ist, bereits gezeigt wurde. Außerdem können wir $k > 1$ annehmen. Wir dividieren das Exponentialpolynom $F(X)$ durch β_k^X und nehmen davon die erste Differenz:

$$\Delta\left(\frac{F(X)}{\beta_k^X}\right) = \left[\sum_{i=1}^{k-1}\left(\frac{\beta_i}{\beta_k}\right)^X\left(\left(\frac{\beta_i}{\beta_k}-1\right)B_i(X+1)+\Delta B_i(X)\right)\right] + \Delta B_k(X)$$

Wegen $F(n) = 0 \quad \forall n \in \mathbb{N}$ ist $\Delta\left(\frac{F(X)}{\beta_k^X}\right) = 0 \quad \forall n \in \mathbb{N}$. Da

$$\begin{aligned}
\frac{\beta_i}{\beta_k} &\neq \frac{\beta_j}{\beta_k} \quad 1 \leq i \neq j \leq k-1, \\
\frac{\beta_i}{\beta_k} &\neq 1 \quad 1 \leq i \leq k-1, \\
deg(B_i(X)) &= deg\left(\left(\frac{\beta_i}{\beta_k}-1\right)B_i(X+1)+\Delta B_i(X)\right)
\end{aligned}$$

und

$$\Delta B_k(X) \equiv 0 \text{ oder } deg(\Delta B_k(X)) < deg(B_k(X))$$

ist $\Delta\left(\frac{F(X)}{\beta_k^X}\right)$ ein Exponentialpolynom dessen Grad kleiner als der von $F(X)$ ist. Die Induktionsvoraussetzung ergibt $\Delta\left(\frac{F(X)}{\beta_k^X}\right) \equiv 0$ und daher $F(X) \equiv 0$. $\Box$

Gemeinsam mit dem Satz von Skolem-Mahler-Lech ist dieser Hilfssatz grundlegend für folgendes schöne Ergebnis:

Satz 6.3 *Es sei $(a_n)_{n\geq 0} \neq 0$ eine Rekurrenz, deren Nullstellenmenge unendlich groß ist. Dann ist zumindest einer der Brüche $\frac{\alpha_i}{\alpha_j}$, $i \neq j$, eine Einheitswurzel.*

Beweis Da $|\{n \in \mathbb{N} | a_n = 0\}| = \infty$, gibt es nach dem Satz von Skolem-Mahler-Lech eine natürliche Zahl $d > 0$ und ein $r \in \{0, 1, ...d-1\}$, sodaß

$$r + d\mathbb{N} \subseteq \{n \in \mathbb{N} | a_n = 0\}.$$

Mit anderen Worten

$$\sum_{i=1}^{k}(A_i(n \cdot d + r)\alpha_i^r)(\alpha_i^d)^n = 0 \quad \forall n \in \mathbb{N}.$$

Wenn die Aussage im Satz falsch wäre, dann hätten wir $\alpha_i^d \neq \alpha_j^d$, wenn $i \neq j$, und nach Hilfsatz 6.1. wäre für $i = 1, 2, ...k$ dann $A_i(X \cdot d + r) \equiv 0$ und daher $A_i(X) \equiv 0$. Das ist aber ein Widerspruch zu $(a_n)_{n\geq 0} \neq 0$.

Dieser Satz ermöglicht folgende interessante äquivalente Formulierung des Satzes von Skolem-Mahler-Lech:

Satz 6.4 *Der Satz von Skolem-Mahler-Lech ist äquivalent zu folgender Behauptung: Für* $i = 1, 2, ...k$ *seien* α_i *Elemente des Körpers* K*, sodaß keiner der Brüche* $\frac{\alpha_i}{\alpha_j}$ *eine Einheitswurzel ist. Weiters seien* $A_1(X), ...A_k(X)$ *Polynome über* K*, die nicht alle Null sind. Dann ist*

$$\sum_{i=1}^{k} A_i(n)\alpha_i^n = 0$$

für höchstens endlich viele natürliche Zahlen n*.*

Beweis Daß der Satz von Skolem-Mahler-Lech die Behauptung impliziert, wurde durch Satz 6.3. gezeigt.

Wir gehen also umgekehrt davon aus, daß die Behauptung stimmt und zeigen mit ihrer Hilfe den Satz von Skolem-Mahler-Lech.
Es sei $(a_n)_{n\geq 0}$ eine Rekurrenz. Ist die Nullstellenmenge von $(a_n)_{n\geq 0}$ endlich, so haben wir nichts zu zeigen.
Es sei also

$$\sum_{i=1}^{k} A_i(n)\alpha_i^n = 0$$

für unendlich viele natürliche Zahlen n. Wir formen das Exponentialpolynom um

$$\sum_{i=1}^{k} A_i(X)\alpha_i^X = \sum_{i=1}^{u} \beta_i^X \sum_{j=1}^{v} \nu_{ij}^X B_{ij}(X),$$

sodaß ν_{ij} Einheitswurzeln sind, das jedoch für keinen der Brüche $\frac{\beta_i}{\beta_j}$, $i \neq j$, zutrifft.
Es sei $d > 0$ eine natürliche Zahl mit $\nu_{ij}^d = 1$ für alle i's und j's, und $r \in \{0, 1, ...d-1\}$ beliebig. Dann ist für festes i der Ausdruck $\sum\limits_{j=1}^{v} \nu_{ij}^{r+d\cdot X} B_{ij}(r + d \cdot X)$ ein Polynom in X. Verschwindet nun die Rekurrenz $(a_n)_{n\geq 0}$ in der arithmetischen Progression $r + d\mathbb{N}$ unendlich oft, so folgt aus der Behauptung im Satz, daß $\sum\limits_{j=1}^{v} \nu_{ij}^{r+d\cdot X} B_{ij}(r + d \cdot X) \equiv 0$ für jedes i und daher

$$a_{r+dn} = 0$$

für jede natürliche Zahl n.
Das ergibt den Satz von Skolem-Mahler-Lech, da die Rekurrenz $(a_n)_{n\geq 0}$ demnach in den $d - 1$ arithmetischen Progressionen $d\mathbb{N}, 1 + d\mathbb{N}, ...(d - 1) + d\mathbb{N}$ jeweils höchstens endlich viele Nullstellen hat oder komplett verschwindet. $\square$

In Vorbereitung auf den übernächsten Satz ist folgende Charakterisierung der periodischen Rekurrenzen möglicherweise interessant:

Satz 6.5 *Die periodischen Folgen über* K *sind genau jene Rekurrenzen, deren Exponentialpolynom von der Form* $\sum\limits_{i=1}^{k} z_i\zeta_i^n$ *ist, wobei die* ζ_i*'s Einheitswurzeln und die* z_i*'s beliebige Elemente* $\neq 0$ *des Körper* K *sind.*

Beweis In Abschnitt 1.1, Beispiel (5), haben wir gesehen, daß wir zu jeder periodischen Folge eine Rekurrenzrelation definieren können, sodaß das charakteristische Polynom von der Form $X^d - 1$ ist, wobei d die Periodenlänge ist. Daraus folgt, daß jede periodische Folge eine Darstellung durch ein Exponentialpolynom wie im Satz hat (Die Koeffizienten sind Konstanten, da das Polynom $X^d - 1$ nur einfache Nullstellen hat).
Umgekehrt ist auch klar, daß jede Rekurrenz, die durch so ein Expontialpolynom definiert ist, periodisch ist.
Schließlich kann es wegen Hilfssatz 6.1. auch nicht passieren, daß eine periodische Folge eine andere Darstellung durch ein Expoentialpolynom hat, als im Satz beschrieben. □

Wir sind nun tatsächlich in der Lage den 'Zerlegungssatz' für beliebige Rekurrenzen über Körpern der Charakteristik 0 zu zeigen:

Satz 6.6 *Es sei $(a_n)_{n\geq 0}$ eine Rekurrenz, die unendlich viele Nullstellen hat. Dann gibt es zwei Rekurrenzen $(e_n)_{n\geq 0}$ und $(f_n)_{n\geq 0}$ mit*

$$a_n = e_n \cdot f_n \quad \forall n \in \mathbb{N},$$

wobei $(e_n)_{n\geq 0}$ periodisch und $\{n \in \mathbb{N} | f_n = 0\}$ endlich ist.

Bemerkung Daß $(a_n)_{n\geq 0}$ unendlich viele Nullstellen hat, impliziert natürlich, daß die periodische Rekurrenz $(e_n)_{n\geq 0}$ auch unendlich viele Nullstellen hat. Wegen ihrer Periodizität, gibt es eine natürliche Zahl $d > 0$ (die Periodenlänge), sodaß

$$\{n \in \mathbb{N} | e_n = 0\} = \bigcup_{\substack{r\in\{0,1,\ldots d-1\}: \\ e_r = 0}} (r + d\mathbb{N})$$

und daher

$$\{n \in \mathbb{N} | a_n = 0\} = \left(\bigcup_{\substack{r\in\{0,1,\ldots d-1\}: \\ e_r = 0}} (r + d\mathbb{N}) \right) \cup \{n \in \mathbb{N} | f_n = 0\}.$$

Wir sehen also, daß Satz 6.6 eine Verallgemeinerung des Satzes von Skolem-Mahler-Lech ist.

Beweis Wie im Beweis von Satz 6.4 schreiben wir das Exponentialpolynom von $(a_n)_{n\geq 0}$ in folgender Weise an:

$$\sum_{i=1}^{k} A_i(X)\alpha_i^X = \sum_{i=1}^{u} \beta_i^X \sum_{j=1}^{v} \nu_{ij}^X B_{ij}(X),$$

wobei ν_{ij} Einheitswurzeln sein sollen, die Brüche $\frac{\beta_i}{\beta_j}$ für $i \neq j$ jedoch nicht. Es seien r_f und d wie in (6.3), wobei wir o.B.d.A. annehmen dürfen, daß $\nu_{ij}^d = 1$ für $i = 1, 2, \ldots u, j = 1, 2, \ldots v$. Außerdem ist $d > 0$, weil $(a_n)_{n\geq 0}$ unendlich viele Nullstellen hat. Für festes $f \in \{1, 2, \ldots l\}$ ist $n \mapsto \nu_{ij}^{r_f + d\cdot n}$ $(n \in \mathbb{N})$ eine konstante Funktion und daher ist

$$\sum_{j=1}^{v} \nu_{ij}^{r_f+dn} B_{ij}(r_f + dn) = \sum_{j=1}^{v} \nu_{ij}^{r_f} B_{ij}(r_f + dn)$$

für festes $i \in \{1, 2, ...u\}$ ein Polynom in n. Da keiner der Brüche $\frac{\beta_i}{\beta_j}$ $(i \neq j)$ eine Einheitswurzel ist und $(a_n)_{n \geq 0}$ auf der arithmetischen Progression $r_f + d\mathbb{N}$ verschwindet, folgt aus dem Identitätssatz für Exponentialpolynome (Hilfssatz 6.1)

$$\sum_{j=1}^{v} \nu_{ij}^{r_f} B_{ij}(r_f + dX) \equiv 0 \overset{d \geq 0}{\Rightarrow} \sum_{j=1}^{v} \nu_{ij}^{r_f} B_{ij}(X) \equiv 0 \quad i = 1, 2, ..u, f = 1, 2, ...l.$$

Mit B_{ijh} bezeichnen wir den Koeffizienten von X^h im Polynom $B_{ij}(X)$. Es folgt

$$\sum_{j=1}^{v} \nu_{ij}^{r_f} B_{ijh} = 0$$

für $i = 1, 2, ...u,\ f = 1, 2, .., l$ und $h \in \mathbb{N}$. Mit η bezeichnen wir eine primitive d-te Einheitswurzel und n_{ij} seien natürliche Zahlen, sodaß $\nu_{ij} = \eta^{n_{ij}}$. Es folgt, daß η^{r_f} Nullstelle der Polynome

$$\sum_{j=1}^{v} Y^{n_{ij}} B_{ijh}$$

ist. Es gibt daher natürliche Zahlen $o_{fih} \geq 1$ und Polynome $G_{ih}(Y)$ mit

$$\sum_{j=1}^{v} Y^{n_{ij}} B_{ijh} = \prod_{f=1}^{l} (Y - \eta^{r_f})^{o_{fih}} G_{ih}(Y)$$

und

$$G_{ih}(\eta^{r_f}) \neq 0$$

für $f = 1, 2, ...l$. Wenn wir mit O_f das Minimum über alle Ordnungen o_{fih} der Nullstelle η^{r_f} bezeichnen, folgt

$$a_n = \prod_{f=1}^{l} (\eta^n - \eta^{r_f})^{O_f} \left(\sum_{i=1}^{u} \beta_i^n \sum_{h=1}^{\infty} \prod_{f=1}^{l} (\eta^n - \eta^{r_f})^{o_{fih} - O_f} G_{ih}(\eta^n) n^h \right).$$

Wir sind fertig, wenn wir zeigen, daß das Exponentialpolynom

$$f_X = \sum_{i=1}^{u} \beta_i^X \sum_{h=1}^{\infty} \prod_{f=1}^{l} (\eta^n - \eta^{r_f})^{o_{fih} - O_f} G_{ih}(\eta^X) X^h$$

nur endlich viele Nullstellen in $\mathbb{N}$ besitzt. (Das ist ein Exponentialpolynom, weil die Summe über h in Wahrheit endlich ist.)
Indirekt: Angenommen $\{n \in \mathbb{N} | f_n = 0\}$ ist unendlich. Nach dem Satz von Skolem-Mahler-Lech gibt es eine arithmetische Progression $a + b\mathbb{N}$ $(a, b \in \mathbb{N}, b > 0)$ auf der $(f_n)_{n \geq 0}$ verschwindet. Weil jede Nullstelle von f_n auch eine von a_n ist, gibt es ein $f_0 \in \{1, 2, ...l\}$ mit

$$a + b\mathbb{N} \subseteq r_{f_0} + d\mathbb{N}.$$

Genauso wie oben folgt dann

$$\prod_{f=1}^{l} (\eta^a - \eta^{r_f})^{o_{fih} - O_f} G_{ih}(\eta^a) = 0$$

für alle i und h. Wegen der Wahl von O_f gibt es zwei natürliche Zahle i und h, sodaß $O_{f_0} = o_{f_0 ih}$. Es folgt

$$G_{ih}(\eta^{r_{f_0}}) = 0,$$

ein Widerspruch zur Wahl der Polynome $G_{ih}(Y)$.
Das ergibt die Zerlegung

$$a_n = \left(\prod_{f=1}^{l} (\eta^n - \eta^f)^{O_f} \right) f_n,$$

wobei $(e_n)_{n\geq 0} := (\prod_{f=1}^{l} (\eta^n - \eta^f)^{O_f})_{n\geq 0}$ periodisch (Satz 6.5) ist und $(f_n)_{n\geq 0}$ nur endlich viele Nullstellen hat. □

Wir sehen also, daß das was wir bei den Beispielen (2),(3) und (4) in Kapitel 1 beobachtet haben, tatsächlich allgemein gilt.

Im Prinzip gibt der Satz (oder besser dessen Beweis) sogar an, wie man diese Zerlegung (die übrigens längst nicht eindeutig ist) finden kann. Notwendig dafür scheint jedoch, daß man die arithmetischen Progressionen kennt, auf der die gegeben Rekurrenz $(a_n)_{n\geq 0}$ verschwindet. Das heißt, daß sich dieses Verfahren nicht dazu eignet, die Nullstellenmenge zu berechnen bzw. zu entscheiden, ob die Nullstellenmenge der Rekurrenz unendlich oder endlich ist.

Wenn es aber möglich ist zu entscheiden, ob die Brüche $\frac{\alpha_i}{\alpha_j}$, $i \neq j$, Einheitswurzeln sind und man außerdem den Grad dieser Einheitswurzeln bestimmen kann, so kann man mit Hilfe der in diesem Abschnitt angedeuteten Ideen und etwas genauerer Argumentation (wir sind ja im Beweis von Satz 6.6 relativ grob vorgegangen), die Frage, ob die Rekurrenz unendlich viele Nullstellenmenge hat, schon beantworten. Ja, man weiß dann eigentlich schon mehr:
(im Folgenden werde ich einige Ergebnisse ohne Beweis anführen. Es handelt sich dabei hauptsächlich um Überlegungen, die auf dem Beweis von Satz 6.6 beruhen. Man findet sie, wenn nicht anders angegeben, in [18].)

Es sei S eine gegebene Menge von Einheitswurzeln. Mit $r(S)$ bezeichnen wir die kleinste natürliche Zahl ungleich Null, sodaß aus $\zeta, \eta \in S$ folgt $\zeta^{r(S)} = \eta^{r(S)}$.
Sind $S_1, S_2, ...S_h$ mehrere Mengen von Einheitswurzeln, so definieren wir

$$r(S_1, S_2, ...S_h) = \mathrm{kgV}(r(S_1), r(S_2), ...r(S_h)).$$

Wir partitionieren die Menge $\{\alpha_1, \alpha_2, ...\alpha_k\}$ der Wurzeln des charakteristischen Polynoms von $(a_n)_{n\geq 0}$ in Teilmengen $T_1, ...T_h$, wobei der Bruch von je zwei Wurzeln in ein und derselben Menge T_i eine Einheitswurzel sein soll, der Bruch zweier Wurzeln aus verschiedenen Mengen T_i und T_j jedoch nicht. Weiters soll S_i für $i = 1, 2, ...h$ die Menge aller Brüche der Form $\frac{\beta}{\gamma}$ mit $\beta, \gamma \in T_i$ sein. Die S_i's sind daher Mengen von Einheitswurzeln.
Wir setzen $r = r((a_n)_{n\geq 0}) := r(S_1, S_2, ...S_h)$.
Man kann relativ leicht zeigen, daß 'die kleinste Periode' der Nullstellenmenge von $(a_n)_{n\geq 0}$ r teilt. Im Wesentlichen ergibt sich das aus folgender Beobachtung: *Es sei $(a_n)_{n\geq 0}$ eine Rekurrenz und d minimal, sodaß es r_f's und eine Menge A wie in (6.3) gibt. Dann muß*

zumindest ein Bruch $\frac{\alpha_i}{\alpha_j}$, $i \neq j$, eine d-te Einheitswurzel sein.
(Das ist eine Verallgemeinerung von Satz (6.3)).
Insbesondere ist also auch r eine Periode. Es folgt

Satz 6.7 *Es sei $(a_n)_{n\geq 0}$ eine Rekurrenz. Dann gibt es eine natürlichen Zahl d, sodaß $\{n \in \mathbb{N} | a_n = 0\}$ die in (6.3) beschriebene Struktur hat, und d nur von den Wurzeln $\alpha_1, \alpha_2, ...\alpha_k$ des charakteristischen Polynoms $1 - s_1 X - ... - s_m X^m$ abhängt, also nur von der Rekurrenzrelation (6.1) und nicht von den Anfangswerten $a_0, a_1, ...a_{m-1}$.*

Wenn man mit r^* das kleinste gemeinsame Vielfachen von r und den Ordnungen der Einheitswurzeln in $\{\alpha_1, ...\alpha_k\}$ bezeichnet, erhält man folgenden

Satz 6.8 *Die Rekurrenz $(a_n)_{n\geq 0}$ nimmt höchstens r^* viele Werte $\neq 0$ unendlich oft an. Wenn r^* nicht existiert ($\Leftrightarrow$ kein α_i ist Einheitswurzel) und $(a_n)_{n\geq 0}$ unendlich oft den Wert c annimmt, dann folgt $c = 0$.*

Nun aber zur Frage nach der Entscheidbarkeit, ob eine Rekurrenz unendlich viele Nullstellen hat: Jean Berstel und Maurice Mignotte haben gezeigt, daß die Frage, ob die Brüche der Wurzeln eines vorgegebenen Polynoms Einheitswurzeln sind und wie groß ihre Ordnung ist, entscheidbar ist ([2]). Somit lassen sich die Mengen $S_1, S_2, ...S_h$ für die Rekurrenz $(a_n)_{n\geq 0}$ effektiv berechnen und daher insbesondere r. Ich habe bereits erwähnt, daß r durch d teilbar ist. Man kennt daher mit r ein gemeinsames Modul der arithmetischen Progressionen der Nullstellenmenge von $(a_n)_{n\geq 0}$ und kann, wie im Beweis von Satz 6.6, die Zerlegung in eine periodische Rekurrenz und eine Rekurrenz, die nur endlich oft verschwindet, berechnen. Insbesondere ist man in der Lage die Nullstellenmenge von $(a_n)_{n\geq 0}$ effektiv zu berechnen. Die Frage, ob eine Rekurrenz unendlich viele Nullstellen hat, ist also entscheidbar.

Durch die Einführung der Mengen $S_1, S_2, ...S_h$ und $r(S_1, S_2, ...S_h)$ ist sogar folgender stärkere Zerlegungssatz möglich:

Satz 6.9 *Gegeben sei eine Rekurrenz $(a_n)_{n\geq 0}$ und $r = r((a_n)_{n\geq 0})$ sei definiert wie oben. Es sei ζ eine primitive r-Einheitswurzel und R die Menge aller $t \in \{0, 1, ...r-1\}$, sodaß $(a_n)_{n\geq 0}$ auf $t + r\mathbb{N}$ verschwindet.*
Dann gibt es eine Rekurrenz $(y_n)_{n\geq 0}$, die nur endlich viele Nullstelln hat, sodaß

$$a_n = \left(\prod_{t \in R} (\zeta^n - \zeta^t)^{m_t} \right) y_n,$$

wobei m_t bestimmte positive natürliche Zahlen, mit

$$\sum_{t \in R} m_t < r$$

sind.

(Ich finde die Zerlegungssätze Satz 6.6 und Satz 6.9 aus folgendem Grund so interessant: Als ich zum ersten Mal vom Satz von Skolem-Mahler-Lech hörte, überprüfte ich ihn zunächst anhand einiger Rekurrenzen, die unendlich viele Nullstellen hatten. Ohne die Exponentialpolynome dieser Rekurrenzen zu kennen, hatte ich immer das Gefühl, daß sie das Produkt periodischer Rekurrenzen mit unendlich vielen Nullstellen und anderen Rekurrenzen mit nur endlich vielen Nullstellen sind, wie wir es in Satz 6.6 hergeleitet haben. Ich dachte daher, daß man vielleicht zuerst versuchen könnte, Satz 6.6 herzuleiten, um daraus den Satz von Skolem-Mahler-Lech als Folgerung zu erhalten.
Nun ist es umgekehrt: Wir bewiesen den Zerlegungssatz relativ einfach mit Hilfe des Satzes von Skolem-Mahler-Lech, der sich damit selbst verstärkt.)

Die folgenden 2 **Beispiele** sollen exemplarisch zeigen, was man mit Hilfe der in diesem Kapitel gezeigten oder zitierten Resultate bewerkstelligen kann:

(1) **Beispiel zu Satz 6.9**
Es sei $k \neq 0$ eine natürliche Zahl und $(a_n)_{n\geq 0}$ die Folge

$$(0,0,...0,1,1,...1,-1,-1,...-1,2,2,...2,-2,-2,...-2,. \quad . \quad .)$$

in der jede ganze Zahl genau k-mal auftritt. Wir wollen wissen, ob $(a_n)_{n\geq 0}$ eine Rekurrenz ist. Dazu betrachten wir ihre erzeugende Funktion $A(X) = \sum\limits_{n=0}^{\infty} a_n X^n$:

$$\begin{gathered} A(X) = \\ = X^k + ... + X^{2k-1} - X^{2k} - ... - X^{3k-1} + 2X^{3k} + ... + 2X^{4k-1} - 2X^{4k} - ... = \\ = X^k(1 + X + ... + X^{k-1} - X^k - ... - X^{2k-1})(1 + 2X^{2k} + 3X^{4k} + 4^{6k} + ...) \end{gathered}$$

Das ist eine rationale Funktion, da $1 + 2X^{2k} + 3X^{4k} + ... = \left(\frac{1}{1-X^{2k}}\right)^2$. Eine kleine Rechnung ergibt

$$A(X) = \frac{X^k}{(1-X)(1+X^k)^2} = \frac{X^k}{1 - X + 2X^k - 2X^{k+1} + X^{2k} - X^{2k+1}}$$

und daher die Rekurrenzrelation

$$a_n = a_{n-1} - 2a_{n-k} + 2a_{n-k-1} - a_{n-2k} + a_{n-2k-1}$$

der Folge und damit Rekurrenz $(a_n)_{n\geq 0}$.

Wir sehen, daß für jedes vorgegebene k eine Rekurrenz $(a_n)_{n\geq 0}$ existiert, sodaß jede ganze Zahl genau k-mal in ihr auftritt.
Als nächstes wollen wir wissen, ob es eine Rekurrenz $(a_n)_{n\geq 0}$ gibt, in der jede ganze Zahl unendlich oft auftritt. Satz 6.8 verneint die Frage, denn er besagt, daß höchstens endlich viele Zahlen unendlich oft in einer Rekurrenz $(a_n)_{n\geq 0}$ auftreten können.

In $\mathbb{C}$ ist die Menge der ganzen Gaußschen Zahlen $\{a+bi|a, b \in \mathbb{Z}\}$ eine Verallgemeinerung von $\mathbb{Z}$ in $\mathbb{R}$. Da wir bereits wissen, daß eine Rekurrenz existiert, in der jede ganze Zahl zumindest einmal vorkommt, könnte man meinen, daß analog auch eine Rekurrenz $(a_n)_{n\geq 0}$ existiert, in der jede ganze Gaußsche Zahl genau einmal vorkommt. Man irrt: Dann ist nämlich $(\mathrm{Re}(a_n))_{n\geq 0}$ eine Folge, in der jede ganze Zahl unendlich oft auftritt. Wenn $A(X)$ die erzeugende Funktion von $(a_n)_{n\geq 0}$ bezeichnet, so ist $\mathrm{Re}(A(X))$ die erzeugende Funktion von $(\mathrm{Re}(a_n))_{n\geq 0}$. Da $(a_n)_{n\geq 0}$ eine Rekurrenz ist, gibt es zwei Polynome $r(X)$ und $s(X)$ über $\mathbb{C}$ mit $deg(r) < deg(s)$, sodaß

$$\begin{aligned}
A(X) &= \frac{r(X)}{s(X)} = \frac{\mathrm{Re}(r(X)) + i\mathrm{Im}(r(X))}{\mathrm{Re}(s(X)) + i\mathrm{Im}(s(X))} = \\
&= \frac{\mathrm{Re}(r(X))\mathrm{Re}(s(X)) + \mathrm{Im}(r(X))\mathrm{Im}(s(X))}{\mathrm{Re}(S(X))^2 - \mathrm{Im}(S(X))^2} \\
&+ i\frac{\mathrm{Im}(r(X))\mathrm{Re}(s(X)) - \mathrm{Re}(r(X))\mathrm{Im}(s(X))}{\mathrm{Re}(S(X))^2 - \mathrm{Im}(S(X))^2}
\end{aligned}$$

und daher ist

$$\mathrm{Re}(A(X)) = \frac{\mathrm{Re}(r(X))\mathrm{Re}(s(X)) + \mathrm{Im}(r(X))\mathrm{Im}(s(X))}{\mathrm{Re}(s(X))^2 - \mathrm{Im}(s(X))^2}$$

eine rationale Funktion, die in ∞ verschwindet. Aus Abschnitt 1.2 folgt, daß $(\mathrm{Re}(a_n))_{n\geq 0}$ eine Rekurrenz ist. Das ist aber eine Widerspruch dazu, daß $(\mathrm{Re}(a_n))_{n\geq 0}$ jede ganze Zahl unendlich oft annimmt. □

(2) **Beispiel zu Satz 6.3**
Gegeben sei in Viereck mit Seiten a, b, c und d. Mit α bezeichnen wir den Winkel, den die Seiten a und d einschließen, mit β, den die Seiten b und c einschließen.

Zusätzlich seien noch zwei weitere Winkel η und θ gegeben.
Nun stelle man sich vor, daß sich die Seite a in diskreter Zeit um den Winkel η pro Zeiteinheit ein Bezug auf die Seite d fortbewegt, und genauso b in Bezug auf c um den Winkel θ pro Zeiteinheit. Zu jedem (diskreten) Zeitpunkt n probiert man nun, ob die so erhaltenen 'Winkel' mit den ursprünglichen Seiten ein Viereck bilden, d.h. ob man einen Winkel γ so finden kann, daß die Seiten a, b, c, d mit dem Winkeln $\alpha + n\eta, \beta + n\theta$ und γ wiederum ein Viereck bilden.

Wir fragen uns nun, welche Bedingungen $a, b, c, d, \alpha, \beta, \eta, \theta$ erfüllen müssen, sodaß man auf diese Weise unendlich oft zu einem Viereck kommt.
Zunächst ist einmal klar, daß man im Falle $\eta = \frac{2\Pi}{u}$ und $\theta = \frac{2\Pi}{v}$ ($u, v \neq 0$ zwei ganze Zahlen) jedenfalls zu den Zeitpunkten n, die Vielfache von $\mathrm{kgV}(u, v)$ sind, ein Viereck erhält, und zwar genau jenes, von dem man ausgegangen ist. Ein zweiter augenscheinlicher Fall ist der, wenn $a = b = c = d \Rightarrow \alpha = \beta$ und $m\eta = m\theta \ \ mod\, 2\pi$ für ein natürliches m. Wir werden zeigen, daß das die beiden einzige Fälle sind und daher die Bedingung insbesondere (fast) nicht vom ursprünglichen Viereck abhängt (außer es handelte sich um eine Raute).

Aus dem Cosinussatz leiten wir ab, daß man zum Zeitpunkt n genau dann ein Viereck erhält, wenn

$$a^2 + d^2 - 2ad\cos(\alpha + n\eta) = b^2 + c^2 - 2bc\cos(\beta + n\theta)$$

Aus dem Additiontheorem für den Cosinus folgt

$$\begin{aligned} &a^2 + d^2 - 2ad\cos(\alpha)\cos(n\eta) + 2ad\sin(\alpha)\sin(n\eta) = \\ &\quad = b^2 + c^2 - 2bc\cos(\beta)\cos(n\theta) + 2ad\sin(\alpha)\sin(n\theta) \end{aligned}$$

Es gibt daher Konstanten K_1, K_2, K_3, K_4, K_5, sodaß

$$K_1\cos(n\eta) + K_2\sin(n\eta) + K_3\cos(n\theta) + K_4\cos(n\theta) + K_5 = 0 \qquad (6.5)$$

genau dann, wenn man zum Zeitpunkt n ein Viereck erhält.
Wegen

$$cos(n\eta) = \frac{e^{in\eta} + e^{-in\eta}}{2} \qquad sin(n\eta) = \frac{e^{in\eta} - e^{-in\eta}}{2i}$$

sind $\cos(n\eta)_{n\geq 0}$ und $\sin(n\eta)_{n\geq 0}$ Rekurrenzen der Ordnung 2, wobei $e^{i\eta}$ und $e^{-i\eta}$ die Wurzeln der charakteristischen Polynome sind.
Es folgt, daß

$$K_1\cos(n\eta) + K_2\sin(n\eta) + K_3\cos(n\theta) + K_4\cos(n\theta) + K_5$$

ein Exponentialpolynom in den Wurzeln $e^{i\eta}, e^{-i\eta}, e^{i\theta}$ und $e^{-i\theta}$ ist. Der Satz von Skolem-Mahler-Lech alleine, sagt uns, daß die beschriebene Situation bis auf höchstens endlich viele Male periodisch auftritt.
Satz 6.3 erlaubt folgenden stärkeren Schluß: Hätte die Gleichung (6.5) unendlich viele natürliche Nullstellen, dann gäbe es zumindest einen Bruch zweier verschiedener Wurzeln des Exponentialpolynoms, der eine Einheitswurzel ist oder

$$K_1\cos(X\eta) + K_2\sin(X\eta) + K_3\cos(X\theta) + K_4\cos(X\theta) + K_5 \equiv 0.$$

Im zweiten Fall folgt insbesondere

$$a^2 + d^2 - 2ad\cos(\alpha + x\eta) = b^2 + c^2 - 2bc\cos(\beta + x\theta) \quad \forall x \in \mathbb{R}$$

und daher $a = b = c = d$, $\alpha = \beta$ und $\eta = \theta$. Wir erhalten eine der eingangs beschriebenen Fälle (nämlich die Raute). Beim ersten Fall reduziert sich alles auf die folgenden beiden Möglichkeiten:

(a) Ist $\frac{e^{i\eta}}{e^{-i\eta}} = e^{2i\eta}$ eine Einheitswurzel, dann auch $e^{i\eta}$. Es gibt daher ein natürliche Zahl $m \neq 0$, sodaß $m \cdot \eta = 2\Pi$. Die Seiten a, d nehmen daher im Laufe der Zeit höchstens m verschiedene Stellungen zueinander ein. Da es unendlich viele natürliche n gibt, die die Gleichung (6.5) lösen, gibt es zwei verschiedene Lösungen n_1, n_2, sodaß a und d in derselben Stellung zueinander sind. Da ein Viereck durch 4 Seiten und einen Winkel eindeutig bestimmt ist, folgt daraus, daß zu diesen beiden Zeitpunkten n_1 und n_2 die Seiten b und c auch denselben Winkel einschließen müssen. Mit anderen Worten $n_1\theta \equiv n_2\theta \mod 2\Pi$ und daher $(n_2 - n_1)\theta \equiv 0 \mod 2\Pi$. Das entspricht der ersten eingangs beschriebenen Möglichkeit.

(b) Ist $\frac{e^{i\eta}}{e^{i\theta}} = e^{2i(\eta-\theta)}$ eine Einheitswurzel, so gibt es eine natürliche Zahl $m \neq 0$, sodaß $m(\eta - \theta) \equiv 0 \mod 2\Pi$. Hätte die Gleichung (6.5) unendlich viele Lösungen, dann gibt es eine arithmetische Progression $r + m\mathbb{N}$ in der sie unendlich viele Lösungen hat, wobei wir o.B.d.A. annehmen, daß r bereits eine solche Lösung ist (hier muß nicht $r \in \{0, 1, ...m - 1\}$ gelten).
Wir betrachten nun ein anderes Ausgangsviereck: Nach wie vor soll es die Seitenlängen a, b, c, d haben, jedoch ersetzen wir α durch $\alpha + r\eta$ und β durch $\beta + r\theta$. Statt die Seite a um η zu bewegen, bewegen wir sie um $m\eta$ und b um $m\theta$. Da $m(\eta - \theta) \equiv 0 \mod 2\Pi$ sind die 'Drehwinkel' also gleich. Zum Zeitpunkt $1, 2, 3, ...$ erhalten wir nun gerade jene 'Figur', die wir beim anderen Viereck zum Zeitpunkt $r, r + m, r + 2m, ...$ erhalten hätten. Insbesondere wird das Resultat unendlich oft ein Viereck sein. Das zugehörige Exponentialpolynom ist eines in den Wurzeln $e^{im\eta}$ und $e^{-im\eta}$. Es folgt daher wieder entweder $a = b = c = d$ und $\alpha = \beta$ oder $\frac{e^{im\eta}}{e^{-im\eta}}$ ist eine Einheitswurzel. Im zweiten Fall ist daher $e^{i\eta}$ eine Einheitswurzel und genauso wie in (a) folgt daraus die Behauptung. □

Die zwei Zerlegungssätze und das letzte Beispiel sollten zum Schluß auch noch folgendes verdeutlichen: Wir haben gesehen, daß es bei der Frage nach der Nullstellenmenge von Rekurrenzen letztendlich um die ganzzahligen Lösungen Gleichungen der Form

$$A_1(X)\alpha_1^X + A_2(X)\alpha_2^X + ... + A_k(X)\alpha_k^X = 0$$

geht, in der Sprache der Zahlentheorie also um die Lösungen spezieller Diophantischer Gleichungen.
Nun scheint es in der Zahlentheorie für diophantische Gleichungen, die unendlich viele Lösungen haben, ein Prinzip zu geben, das A.J. van der Poorten folgendermaßen beschreibt:

... there are infintely many solutions if and only if it is obvious on grounds of shape and structure (in retrospect, at any rate) that there are infinitely many solutions.

Der Zerlegungssatz 6.6 und besser noch 6.9 geben den '*obvious ground*' für die Existenz unendlich vieler Lösungen von diophantischen Gleichungen dieser Form an.

Diesen '*obvious ground*' kann man auch noch in die Sprache der Rekurrenzen übersetzen: Beispiel (2) und (4) aus Kapitel 1 zeigen vielleicht schon, was damit gemeint sein könnte. Bei diesen zwei Rekurrenzen sieht man bereits an der Anfangsbedingung und an der Rekurrenzrelation, daß jedes zweite Folgenglied den Wert Null haben muß. (Was nicht heißen soll, daß man auch sofort sieht, daß das schon fast alle Nullstellen sind.) Nicht so bei Beispiel (3). Wir werden aber (exemplarisch) zeigen, daß man tatsächlich auch in diesem Fall eine andere Rekurrenzrelation finden kann, sodaß man der Rekurrenz $(b_n)_{n\geq 0}$ fast alle Nullstellen sofort ansieht: Gemäß Satz 6.6 kann man $(b_n)_{n\geq 0}$ zerlegen:

$$(e_n)_{n\geq 0} = (0, 1, 1, 0, -1, -1, 0, 1, 1, 0, -1, -1, 0, 1, 1, 0, ...)$$

wobei $e_n = e_{n-6}$ und

$$(f_n)_{n\geq 0} = (1, 3, 9, 27, 81, 243, ...)$$

mit $f_n = 3f_{n-1}$. Das/Ein charakterisches Polynom der Rekurrenz $(e_n)_{n\geq 0}$ ist dann $p_e(X) = 1 - X^6$, das der Rekurrenz $(f_n)_{n\geq 0}$ könnte $p_f(X) = 1 - 3X$ sein. Man überlegt sich leicht, daß $p_b(X) = \prod_{\alpha} p_e(\alpha X)$, wobei das Produkt über der Kehrwerte der Nullstellen von $p_f(X)$ geht (mehrfache Nullstellen müssen dabei entsprechend ihrer Vielfachheit berücksichtigt werden). Das Polynom $p_b(X)$ ist dann wie $p_e(X)$ eines in der Variablen X^6. In unserem Fall, da $deg(p_f) = 1$, läßt sich $p_b(X) = 1 - 3^6 X^6$ natürlich ganz einfach berechnen. Es folgt, daß $(b_n)_{n\geq 0}$ der Rekurrenzrelation

$$b_n = 3^6 b_{n-6}$$

für $n \geq 6$ genügt. Dieser Rekurrenzrelation sieht man nun fast alle (in diesem Fall sogar alle) Nullstellen der Rekurrenz an. (Bei diesem Beispiel hat man die Rekurrenzrelation wahrscheinlich auch ohne Berechnung des charakteristischen Polynoms erraten. Die geschilderte Vorgangsweise funktioniert aber universell.)

Literaturverzeichnis

[1] Yvette Amice, Les nombres p-adiques, Presses Universitaires de France, 1975

[2] J.Berstel and M. Mignotte, Deux proprietes decidables des suites recurrentes lineaires, Bull. Soc. Math. France 104, 1976, 175-184

[3] Burg, Haf,Wille, Höhere Mathematik für Ingenieure – Band 1, Analysis, B.G. Teubner Stuttgart, 1985

[4] J.W.S. Cassels, An embedding theorem for fields, Bull. Austral. Soc. 14, 1976, 193-198; Addendum, 14, 479-480

[5] J.W.S. Cassels, Local Fields, Cambridge University Press, 1986

[6] J.Cigler, Grundideen der Mathematik, BI-Wissenschafts-Verlag, 1992

[7] E. Hlawka und J. Schoissengeier, Zahlentheorie - Eine Einführung, Manz-Verlag, 1979

[8] N.Koblitz, p-adic Numbers, p-adic Analysis and Zeta-Functions

[9] Christer Lech, A note on recurring series, Arkiv för Matematik 2, 1953, 417-421

[10] Kurt Mahler, Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen, Proc. Akad. Wet. Amsterdam 38, 1935, 51-60

[11] Kurt Mahler, On the Taylor coefficients of rational functions, Proc. Camb. Phil. Soc. 52, 1956, 39-48; Addendum, 53, 544

[12] Kurt Mahler, Introduction to p-adic numbers and their functions, 1973

[13] G. Myerson, A.J. van der Poorten, Some Problems Concerning Recurrence Sequences, American Mathematical Monthly, Oktober 1995, 698-705

[14] A.J. van der Poorten, p-adic methods in the study of Taylor coefficients of rational functions, Bull. Austral. Math. Soc. 28, 1984, 109-117

[15] A.J. van der Poorten and R.S. Rumely, Zeros of p-adic exponential polynomials II, J. London Math. Soc. 36, 1987, 1-15

[16] A.J. van der Poorten, Some facts that should be better known; especially about rational functions, in Number Theory and Applications ed. Richard A. Mollin, Kluwer Academic Publishers, Dordrecht, 1989, 497-528

[17] W.H. Schikhof, Ultametric calculus, Cambridge University Press, 1984

[18] H.S. Shapiro, On a theorem concerning exponential polynomials, Comm. Pure. Appl. Math. 12, 1959, 487-500

[19] Th. Skolem, Einige Sätze über gewisse Reihenentwicklungen und expontentiale Beziehungen mit Anwendung auf diophantische Gleichungen, Skrifter norske Videnskaps-Akademi i Oslo, 1933, Band 2, 1-61

[20] Th. Skolem, Diophantische Gleichungen, Verlag von Julius Springer, 1938

[21] T.N. Shorey, R.Tijdeman, Exponential diophantine equations, Cambridge University Press, 1986

[22] R. Strassmann, Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen, Journal für reine und angewandte Mathematik, 1928, 159, 13-28 und 65-66

Lebens- und Studienverlauf

Ich wurde am 29. Juni 1975 als Tochter der Hausfrau Karla und des Universitätsprofessors Roland Fischer in Klagenfurt geboren.

Die Volksschule absolvierte ich in der Dr. Karl Rennerschule (1981-1983) und der VS Wölfnitz (1983-1985), die Unterstufe der Mittelschule (1985-1989) im Musikgymnasium Klagenfurt-Viktring.

Wegen meines wachsenden Interesses an der Mathematik entschied ich mich in der Oberstufe in das Ingeborg Bachmann Gymnasium, naturwissenschaftlicher Zweig, zu wechseln, wo ich am 18. Juni 1993 die Matura mit gutem Erfolg bestand. Teil meiner Matura war eine Fachbereichsarbeit aus Mathematik mit dem Titel 'Näherungsverfahren zum Lösen von Gleichungen'.

Im Herbst 1993 übersiedelte ich nach Wien, um im Wintersemester 1993/94 mit meinem Studium der Mathematik an der Universität Wien zu beginnen. Am 21. März 1995 legte ich die erste Diplomprüfung mit Auszeichnung ab und am 15. Jänner 1998 schließlich die zweite, ebenfalls mit Auszeichnung.

Die meiste Zeit während meines Studiums machte mir die Beschäftigung mit der Mathematik großen Spass. Besonderes interessant fand ich die Algebravorlesungen, die ich bei Prof. Cigler besuchte, zwei Zahlentheorievorlesungen bei Prof. Schoissengeier und die Kombinatorik bei Prof. Krattenthaler.

Von Oktober 1996 bis September 1997 arbeitete ich an meiner Diplomarbeit 'Der Satz von Skolem-Mahler-Lech: Ein Ergebnis über die Nullstellen linearer Rekursionsfolgen'. Das Thema wurde mir von Prof. Cigler vorgeschlagen.

Seit dem Wintersemester 1995/96 bin ich bei Prof. Reichel als Tutorin beschäftigt. Meine Aufgabe war und ist es, Studenten seiner Vorlesungen Lineare Algebra und Geometrie, Höhere Analysis für Lehramtskanditaten, Wahrscheinlichkeitstheorie und Analysis zu betreuen und vertretungsweise die Übungen zu diesen Lehrveranstaltungen zu leiten.