Lineare Algebra 2, SS06
M. Hortmann

Blatt 12

Die Bearbeitung ist freiwillig und geht nicht mehr in die Bewertung ein.

Eine geordnete Menge $(I, \leqslant)$ heißt (nach oben) gerichtet, wenn zu je zwei Elementen $i, j \in I$ ein $k \in I$ existiert mit $i \leqslant k$ und $j \leqslant k$.

Ist eine Familie von Ringen $(R_i)_{i \in I}$ gegeben, sowie für jedes Paar $i, j \in I$ mit $i \leqslant j$ ein Ringhomomorphismus $\varphi_j^i : R_j \to R_i$ mit der Verträglichkeitsbedingung $i \leqslant j \leqslant k \Rightarrow \varphi_k^i = \varphi_j^i \circ \varphi_k^j$, so spricht man von einem projektiven System von Ringen. Der projektive Limes $R = \varprojlim_{i \in I} R_i$ ist durch folgende Eigenschaften (bis auf Isomorphie) eindeutig charakterisiert:

Es gibt eindeutig bestimmte Abbildungen $\varphi^i : R \to R_i$, so daß für $i \leqslant j$ $\varphi^i = \varphi_j^i \circ \varphi^j$.

Man kann den projektiven Limes konstruieren als Menge derjenigen Tupel $a = (a_i)_{i \in I}$ in $\bigtimes_{i \in I} R_i$, für die gilt $\varphi_j^i(a_j) = a_i$ und definiert dann z.B. $a + b := (a_n + b_n)$

Nehmen wir z.B. $\mathbb{N}$ mit der natürlichen Ordnung $\leqslant$, wählen eine Primzahl *p* und setzen $R_n := \mathbb{Z}_{p^n}$. Ist $n \leqslant m$, so ist $\varphi_m^n : R_m \to R_n$, $\varphi(x) = x \,\%\, p^n$ ein Ringhomomorphismus. Da jedes Element von R_m sich eindeutig in der Form $\sum_{i=0}^{m-1} a_i p^i$ mit $0 \leqslant a_i < p$ schreiben läßt, haben wir $\varphi_m^n\left(\sum_{i=0}^{m-1} a_i p^i\right) = \sum_{i=0}^{n-1} a_i p^i$. Alternativ fassen wir Elemente von R_n als Strings der Länge *n* von Elementen von $\mathbb{Z}_p$ auf und lassen bei Anwendung von φ_m^n einfach die ersten (*m*-*n*) Elemente (links) weg.

Damit läßt sich der projektive Limes *R* auffassen als Menge der Folgen (a_n) mit $a_n \in \mathbb{Z}_p$ und sich ein solches Element vorstellen als (unendlich langen) String $\ldots a_n \ldots a_2 a_1 a_0$. Elemente, für die gilt $\exists n_0 \; \forall n \geqslant n_0 : \quad a_n = 0$ werden als natürliche Zahlen interpretiert, die durch ihre Darstellung $\sum_{i=0}^{m-1} a_i p^i$ mit $0 \leqslant a_i < p$ im Stellensystem zur Basis *p* gegeben sind.

Ein Element $a = (a_n)_{n \in \mathbb{N}} \in R$ läßt sich nun sogar identifizieren mit der unendlichen Reihe $\sum_{i=0}^{\infty} a_i p^i$, die ja bezüglich der *p*-Norm eine Cauchyfolge bilden. Die *p*-Norm läßt sich in

natürlicher Weise auf den projektiven Limes R fortsetzen, indem wir setzen:
$\|a\| := 2^{-\text{Anzahl der Nullen am rechten Ende des Strings } a}$.

Z.B. ist $\left\| a - \sum_{i=0}^{n-1} a_i p^i \right\|_p \leqslant 2^{-n}$. Damit gilt dann auch bzgl der durch die p-Norm gegebenen Metrik $a = \lim_{n\to\infty} \sum_{i=0}^{n} a_i p^i$.

Man nennt die Elemente des eben beschriebenen projektiven Limes R auch p-adische ganze Zahlen.

Aufgabe 1

Gehen Sie aus von p=7 und betrachten Sie die p-adischen ganzen Zahlen mit p=7 .
Beschreiben Sie einen Algorithmus zur Berechnung von $\sqrt{2}$ in diesem Ring, also eine Methode zur Konstuktion einer Zahlenfolge $b_n \in \mathbb{Z}$, so daß $\left\| b_n^2 - 2 \right\|_p \to 0$, m.a.W.: $b_n^2 - 2$ wird mit wachsendem n durch immer höhere Potenzen von 7 teilbar.

Hier die ersten Schritte:

Da $3^2 - 2 = 7$, beginne man mit $b_0 = a_0 = 3$.

Im nächsten Schritt besttimme man a_1 und $b_1 = a_1 7 + a_0$, so daß $b_1^2 - 2 = (a_1 7 + a_1)^2 - 2$ durch $49 = 7 \cdot 7$ teilbar ist.
Dieser Ansatz ergibt $a_1^2 \cdot 49 + 2 a_0 a_1 7 + a_0^2 - 2 = a_1^2 \cdot 49 + 2 \cdot 3 a_1 7 + 9 - 2 = a_1^2 \cdot 49 + 2 \cdot 3 a_1 7 + 7$, und diese Zahl ist durch 49 teilbar, wenn $2 \cdot 3 a_1 + 1 \equiv 0 \bmod 7$, also $a_1 = -1/6$ in $\mathbb{Z}_7$, also $a_1 = 1$
Damit wird $b_1 = a_1 7 + a_0 = 10$ und $b_1^2 - 7 = 2 \cdot 49$

Im dritten Schritt suchen wir a_2 und $b_2 = a_2 7^2 + b_1 = a_2 7^2 + a_1 7 + a_0$, so daß $b_2^2 - 2$ durch 7^3 teilbar ist. Damit wird $b_2^2 - 2 = (a_2 7^2 + b_1)^2 - 2 = a_2 7^4 + 2 a_2 b_1 7^2 + b_1^2 - 2 = a_2 7^4 + 2 a_2 10 \cdot 7^2 + 2 \cdot 7^2$, und dies ist offenbar durch 7^3 teilbar, wenn $2 a_2 3 + 2 \equiv 0 \bmod 7$, woraus $a_2 = -2/6 = 2 \in \mathbb{Z}_7$ folgt. Damit wird $b_2 = 108 = 2 \cdot 7^2 + 1 \cdot 7 + 3$ und $b^2 - 2 = 4 \cdot 7^4 + 6 \cdot 7^3$.

a) Man berechne nach diesem Verfahren b_6 und $b_6^2 - 2$.

b) Man programmiere den Algorithmus in Pari und berechne die Folge (a_n) bis $n = 100$.