Universität Duisburg-Essen
Fakultät für Mathematik

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

Iwasawa-Algebren

Abschlussarbeit zur Erlangung des akademischen Grades

Bachelor of Science (B. Sc.)

vorgelegt von

Annika Stechemesser

Betreuer:	Prof. Dr. Jan Kohlhaase
Zweitgutachter:	Prof. Dr. Massimo Bertolini
Abgabedatum:	26. Juli 2016

Inhaltsverzeichnis

1 Einleitung

Ziel der vorliegenden Arbeit ist es, die Iwasawa-Algebra über der proendlichen Gruppe $\mathbb{Z}_p$ durch drei verschiedene Herangehensweisen zu definieren und zu zeigen, dass diese Darstellungen alle zueinander isomorph sind. Die Iwasawa-Algebra wurde benannt nach Kenkichi Iwasawa (* 11.09.1917 †26.10.1998), der durch seine Arbeit fundamentale Beiträge zur algebraischen Zahlentheorie lieferte.

Zu Beginn der Arbeit erarbeiten wir einige Grundlagen über den Körper der p-adischen Zahlen und den Ring der ganzen p-adischen Zahlen. Den Körper der p-adischen Zahlen $\mathbb{Q}_p$ führen wir als Vervollständigung des Körpers der rationalen Zahlen bezüglich des p-adischen Absolutbetrags ein. Im Anschluss daran definieren wir den Ring der ganzen p-adischen Zahlen $\mathbb{Z}_p$ als Unterring von $\mathbb{Q}_p$. Der Fokus liegt hierbei besonders auf der Untersuchung einiger topologischer Eigenschaften von $\mathbb{Z}_p$, wie beispielsweise der Hausdorff-Eigenschaft. Außerdem betrachten wir die topologische Gruppe $(\mathbb{Z}_p,+)$ und ihre offenen Untergruppen. Abschließend definieren wir im zweiten Kapitel den Ring $\mathfrak{o}$ als Bewertungsring einer Körpererweiterung vollständig bewerteter Körper über $\mathbb{Q}_p$. Über diesen Ring wollen wir im Folgenden die drei $\mathfrak{o}$-Algebren definieren.

In Abschnitt 3.1 wiederholen wir zunächst die Definition des Rings der formalen Potenzreihen über $\mathfrak{o}$. In Abschnitt 3.2 führen wir die Gruppenalgebra $\mathfrak{o}[G]$ ein und erarbeiten anschließend daran Grundlagen zu projektiven Limiten von Mengen, Gruppen und Ringen. Besonders die Eigenschaft der Verträglichkeit werden wir im vierten Kapitel benötigen. Nachdem wir proendliche topologische Räume und Gruppen kurz definiert haben,

gehen wir über zur Betrachtung von komplettierten Gruppenringen und konzentrieren uns hier besonders auf die proendliche Vervollständigung proendlicher Gruppen. Aufbauend darauf zeigen wir, dass $\mathbb{Z}_p$ ebenfalls eine proendliche Gruppe ist und definieren dann den komplettierten Gruppenring $\mathfrak{o}[\![\mathbb{Z}_p]\!]$, welcher die zweite $\mathfrak{o}$-Algebra bildet. Ziel des letzten Abschnitts des dritten Kapitels ist die Definition der Maßalgebra $\mu(\mathbb{Z}_p, \mathfrak{o})$. Dafür erarbeiten wir erst grundlegende Eigenschaften über den Raum der stetigen Funktionen von einem topologischen Raum X in den Körper K und definieren dann geeignete Verknüpfungen, sodass wir eine K-Algebra $\mu(\mathbb{Z}_p, K)$ erhalten. Schlussendlich zeigen wir, dass $\mu(\mathbb{Z}_p, \mathfrak{o})$ eine $\mathfrak{o}$-Unteralgebra dieser Algebra ist.

Das vierte Kapitel bildet das Herzstück der Arbeit. Hier zeigen wir, dass die drei zuvor definierten $\mathfrak{o}$-Algebren paarweise zueinander isomorph sind. Im ersten Abschnitt des vierten Kapitels beweisen wir, dass der Ring der formalen Potenzreihen über $\mathfrak{o}$ isomorph ist zu dem komplettierten Gruppenring der proendlichen Gruppe $\mathbb{Z}_p$. Dafür zeigen wir zunächst, dass es einen Isomorphismus zwischen $\mathfrak{o}[\![\mathbb{Z}_p]\!]$ und dem projektiven Limes der Restklassen $\mathfrak{o}[X]/(h_n)$ von Polynomen gibt. Wir benutzen den verallgemeinerten Euklidischen Algorithmus um darzulegen, dass $\mathfrak{o}[X]/(h_n)$ isomorph ist zu $\mathfrak{o}[\![X]\!]$. Den Isomorphismus zwischen $\mathfrak{o}[\![\mathbb{Z}_p]\!]$ und $\mu(\mathbb{Z}_p, \mathfrak{o})$ definieren wir über Hilfsfunktionen L_λ, die zunächst vom Raum der lokal konstanten Funktionen $C^\infty(\mathbb{Z}_p, K)$ in den Körper K abbilden. Diese setzen wir dann zu Funktionen vom Raum der stetigen Funktionen $C(\mathbb{Z}_p, K)$ nach K fort und bilden Elemente λ aus $\mu(\mathbb{Z}_p, \mathfrak{o})$ darauf ab. In der Tat ist die Abbildung ein Isomorphismus. Durch die Betrachtung der ersten beiden Isomorphismen wissen wir bereits, dass es einen Isomorphismus zwischen $\mathfrak{o}[\![X]\!]$ und der Maßalgebra $\mu(\mathbb{Z}_p, K)$ gibt. Wir konzentrieren uns in Abschnitt 4.3 auf den Zusammenhang zwischen dem Maß μ und der assoziierten formalen Potenzreihe F_μ.

Die in dieser Arbeit betrachteten Iwasawa-Algebren sind Teil der sogenannten Iwasawa-Theorie, die sich mit dem Zusammenhang zwischen der Galoisgruppe algebraischer Körpertürme und der additiven Gruppe der p-adischen Zahlen beschäftigt. Die daraus resul-

tierende Theorie über Moduln von Iwasawa liefert einen Ansatz zur Definition p-adischer L-Reihen, welche in Analogie zur Riemannschen Zeta Funktion stehen. Diese Analogie kann man deutlicher anhand des Ansatzes über Interpolation mittels Bernoulli-Zahlen erkennen, den Dirichlet zur Definition der L-Reihen gewählt hat. Die Hauptvermutung der Iwasawa-Theorie besagt letztendlich, dass der Ansatz zur Definition der p-adischen L-Reihen über Modultheorie und der Ansatz über Interpolation mithilfe von Bernoulli-Zahlen übereinstimmen (nach *Serge Lang, Cyclotomic fields 1 and 2*, Kapitel 4 und 5).

2 Der Körper der p-adischen Zahlen und der Ring der ganzen p-adischen Zahlen

2.1 Der p-adische Absolutbetrag

Im ersten Abschnitt des Kapitels wollen wir den p-adischen Absolutbetrag definieren und einige wichtige Eigenschaften erarbeiten. Dabei orientiert sich der Aufbau im Wesentlichen an Kapitel 9.1 des Buches *Einführung in die algebraische Zahlentheorie von Alexander Schmidt*, welches im Jahr 2007 beim Springer Verlag erschienen ist.

Sei p eine beliebige aber feste Primzahl. Jede rationale Zahl $q \in \mathbb{Q} \setminus \{0\}$ hat eine eindeutige Darstellung der Form $q = \frac{a}{b}p^n$ mit $a, b, n \in \mathbb{Z}, b > 0$ und $ggT(a,b) = ggT(a,p) = ggT(b,p) = 1$. Setze $\nu_p(q) := n$.

Definition 2.1.1 *Für $q \in \mathbb{Q} \setminus \{0\}$ bezeichnen wir mit $\nu_p(q)$ die p-adische Bewertung von q.*

Lemma 2.1.2 *Für $x,y \in \mathbb{Q}$ gilt:*
i) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$
ii)$\nu_p(x+y) \geq min(\nu_p(x), \nu_p(y))$
Falls $\nu_p(x) \neq \nu_p(y)$ *gilt:* $\nu_p(x+y) = min(\nu_p(x), \nu_p(y))$

Beweis Sei $x = \frac{a}{b}p^n$, $y = \frac{c}{d}p^m$ mit $a, b, c, d, n, m \in \mathbb{Z}, b, d > 0$ und a,b und p sowie c,d und p paarweise teilerfremd.

zu i): Dann gilt: $x \cdot y = \frac{a}{b}p^n \cdot \frac{c}{d}p^m = \frac{ac}{bd}p^{n+m} \Rightarrow \nu_p(xy) = n + m = \nu_p(x) + \nu_p(y)$

zu ii): Angenommen $n = m$, also $\nu_p(x) = \nu_p(y)$.

Dann gilt: $x + y = \frac{a}{b}p^n + \frac{c}{d}p^n = (\frac{ad+bc}{bd})p^n$

$$\Rightarrow \nu_p(x+y) \begin{cases} = min(\nu_p(x), \nu_p(y)) & \text{falls } ad + bc \text{ nicht durch p teilbar} \\ \geq min(\nu_p(x), \nu_p(y)) & \text{sonst} \end{cases}$$

Falls $n \neq m$: $x + y = \frac{a}{b}p^n + \frac{c}{d}p^m \Rightarrow \nu_p(x + y) = min(\nu_p(x), \nu_p(y))$ □

Nun können wir den p-adischen Absolutbetrag formal definieren:

Definition 2.1.3 *Definiere den p-adischen Absolutbetrag durch:*

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+ \qquad q \mapsto \begin{cases} p^{-\nu_p(q)} & falls\ q \neq 0 \\ 0 & falls\ q = 0 \end{cases}$$

Lemma 2.1.4 $|\cdot|_p$ *ist eine nicht-archimedische Körpernorm.*

Beweis Seien $x, y \in \mathbb{Q}$. Zu zeigen:

1. $|x|_p = 0 \Leftrightarrow x = 0$

Dies ist klar nach der Definition des p-adischen Absolutbetrags.

2. $|xy|_p = |x|_p \cdot |y|_p$. Für x oder y gleich Null ist der Fall klar.

Angenommen $x, y \neq 0$. Somit gilt:

$|xy|_p = p^{-\nu_p(xy)} = p^{-(\nu_p(x)+\nu_p(y))} = p^{-\nu_p(x)} \cdot p^{-\nu_p(y)} = |x|_p \cdot |y|_p$

3. $|x + y|_p \leq |x|_p + |y|_p$ Für x oder y gleich Null ist der Fall klar.

Angenommen $x, y \neq 0$. Es gilt:

$|x + y|_p = p^{-\nu_p(x+y)} p^{-min\{\nu_p(x),\nu_p(y)\}} \leq p^{-\nu_p(x)} + p^{-\nu_p(y)} = |x|_p + |y|_p$ da $p^{-\nu_p(q)>0}$ für $q \neq 0$

4. $|x + y|_p \leq max\{|x|_p, |y|_p\}$. Für alle $x, y \in \mathbb{Q}$ ist

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

□

Definition 2.1.5 *Für $x,y \in \mathbb{Q}$ definieren wir durch $d_p(x,y) := |x-y|_p$ den p-adischen Abstand von x und y. Eine Folge $(x_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q}$ nennen wir eine p-adische Cauchyfolge genau dann, wenn es $\forall\, \epsilon > 0$ und ein $N \in \mathbb{N}$ gibt, sodass $|x_n - x_m|_p \leq \epsilon \;\forall\, n,m \geq N$.*

Lemma 2.1.6 *Der p-adische Abstand ist eine Metrik auf $\mathbb{Q}$.*

Beweis Zu zeigen: Der p-adische Abstand $d_p(x,y)$ ist positiv definit, symmetrisch und erfüllt die Dreiecksungleichung $\forall x,y \in \mathbb{Q}$.
Seien $x,y \in \mathbb{Q}$.
1. positiv definit: $d_p(x,y) = |x-y|_p$. Da nach Definition $|q|_p = \begin{cases} p^{-\nu_p(q)} & \text{falls } q \neq 0 \\ 0 & \text{falls } q = 0 \end{cases}$
ist $|x-y|_p > 0$ für $x \neq y$ und $|x-y|_p = 0 \Leftrightarrow x = y$
2. symmetrisch: Angenommen $x \neq y$. Dann ist $d_p(x,y) = |x-y|_p = |(-1)(y-x)|_p = |(-1)|_p \cdot |y-x|_p = |y-x|_p$
3. Dreiecksungleichung: $x,y,z \in \mathbb{Q}$: $d(x,y) = |x-y|_p = |x-z+z-y|_p = |(x-z)+(z-y)|_p$
$\leq max\{|x-z|_p, |z-y|_p\} = max\{d(x,z)_p, d(z,y)_p\} \leq d(x,z)_p + d(z,y)_p$. □

Definition 2.1.7 *Ein metrischer Raum mit einer Metrik d heißt vollständig bezüglich d genau dann, wenn jede Cauchyfolge bezüglich d konvergiert.*

Bemerkung 2.1.8 *$\mathbb{Q}$ ist bezüglich des p-adischen Absolutbetrags nicht vollständig.*

Beweis Siehe *Alexander Schmidt, Einführung in die Algebraische Zahlentheorie, Beginn von Kapitel 9.1 (Der p-adische Abstand)*

2.2 Der Körper der p-adischen Zahlen $\mathbb{Q}_p$

In diesem Abschnitt wollen wir den Körper der p-adischen Zahlen als Vervollständigung der rationalen Zahlen einführen. Dabei folgen wir grob dem Vorgehen in Kapitel 9.2 des Buches *Einführung in die algebraische Zahlentheorie* von *Alexander Schmidt.*
Bezeichne weiterhin mit p eine feste, aber beliebige Primzahl.

Definition 2.2.1 *Definiere $\mathbb{Q}_p$ als die Vervollständigung von $\mathbb{Q}$ bezüglich des p-adischen Absolutbetrags. Wir nennen $\mathbb{Q}_p$ den Körper der p-adischen Zahlen. Die Elemente von $\mathbb{Q}_p$ sind demnach Äquivalenzklassen p-adischer Cauchyfolgen $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$ bezüglich der Äquivalenzrelation:*
$(x_i)_{i\in\mathbb{N}} \sim (y_i)_{i\in\mathbb{N}} \Leftrightarrow (x_i - y_i)_{i\in\mathbb{N}}$ *ist eine p-adische Nullfolge.*

Satz 2.2.2 *$\mathbb{Q}_p$ ist mit den Verknüpfungen*

$$+ : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p \quad ((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) \mapsto (x_n + y_n)_{n\in\mathbb{N}}$$
$$\cdot : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p \quad ((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) \mapsto (x_n y_n)_{n\in\mathbb{N}}$$

ein Körper.

Beweis Zeige: " + " und " $\cdot$ " sind wohldefiniert.
Seien $(x_n)_{n\in\mathbb{N}}$ und $(y_n)_{n\in\mathbb{N}}$ p-adische Cauchyfolgen. Dann gilt: $\forall\ \epsilon > 0$ gibt es ein $N_x \in \mathbb{N}$, sodass $|(x_n - x_m)|_p < \epsilon\ \forall\ n, m \geq N_x$. Analog für $(y_n)_{n\in\mathbb{N}}$.
Dann gilt für $(x_n + y_n)_{n\in\mathbb{N}}$: $\forall\ \epsilon > 0$ gibt es $N := max\{N_x, N_y\}$, sodass
$|((x_n + y_m) - (x_m + y_m))|_p = |((x_n - x_m) + (y_n - y_m))|_p$
$\leq max\{|(x_n - x_m)|_p, |(y_n - y_m)|_p\} < \epsilon$ für alle $n, m \geq N$
$\Rightarrow (x_n + y_n)_{n\in\mathbb{N}}$ ist eine p-adische Cauchyfolge.

Falls gilt $(x_n)_{n\in\mathbb{N}} \sim (x'_n)_{n\in\mathbb{N}}$ und$(y_n)_{n\in\mathbb{N}} \sim (y'_n)_{n\in\mathbb{N}}$, so gilt auch
$(x_n + y_n)_{n\in\mathbb{N}} \sim (x'_n + y'_n)_{n\in\mathbb{N}}$, da:
$(x_n)_{n\in\mathbb{N}} \sim (x'_n)_{n\in\mathbb{N}} \Leftrightarrow (x_i - x'_i)_{i\in\mathbb{N}}$ ist eine p-adische Nullfolge.
$(y_n)_{n\in\mathbb{N}} \sim (y'_n)_{n\in\mathbb{N}} \Leftrightarrow (y_i - y'_i)_{i\in\mathbb{N}}$ ist eine p-adische Nullfolge.

Betrachte $((x_i + y_i) - (x_i' + y_i'))_{i\in\mathbb{N}}$. Dann gilt

$|((x_i + y_i) - (x_i' + y_i'))|_p = |((x_i - x_i') + (y_i - y_i'))|_p \leq max\{|(x_i - x_i')|_p, |(y_i - y_i')|_p\}$

für alle $i \in \mathbb{N}$. Sei o.B.d.A. $|x_i - x_i'|_p = max\{|x_i - x_i'|_p, |y_i - y_i'|_p\}$. Dann ist

$|((x_i + y_i) - (x_i' + y_i'))|_p \leq |x_i - x_i'|_p$ für alle $i \in \mathbb{N}$

$\Rightarrow \lim_{i\to\infty} |((x_i + y_i) - (x_i' + y_i'))|_p \leq \lim_{i\to\infty} |x_i - x_i'|_p = 0.$

Da $|\cdot|_p$ eine Norm ist, gilt auch $0 \leq \lim_{i\to\infty} |((x_i + y_i) - (x_i' + y_i'))|_p$. Somit ist nach dem Einschließungslemma $\lim_{i\to\infty} |((x_i + y_i) - (x_i' + y_i'))|_p = 0 \Rightarrow ((x_i + y_i) - (x_i' + y_i'))_{i\in\mathbb{N}}$ ist eine p-adische Nullfolge $\Rightarrow (x_n + y_n)_{n\in\mathbb{N}} \sim (x_n' + y_n')_{n\in\mathbb{N}}$.

Somit ist die Verknüpfung " + " wohldefiniert.

Betrachte nun die Verknüpfung "$\cdot$": $\forall\ \epsilon > 0$ gibt es $N := max\{N_x, N_y\}$, sodass

$|x_n y_n - x_m y_m|_p = |x_n y_n - x_n y_m + x_n y_m - x_m y_m|_p = |x_n(y_n - y_m) + y_m(x_n - x_m)|_p$

$\leq max\{|x_n(y_n - y_m)|_p, |y_m(x_n - x_m)|_p\}$.

Sei o.B.d.A. $|x_n(y_n - y_m)|_p = max\{|x_n(y_n - y_m)|_p, |y_m(x_n - x_m)|_p\}$. Dann ergibt sich weiter: $|x_n y_n - x_m y_m|_p \leq |x_n(y_n - y_m)|_p = |x_n|_p |y_n - y_m|_p < c\epsilon$ für alle $n, m \geq N$, da $(x_n)_{n\in\mathbb{N}}$ als Cauchyfolge in $\mathbb{Q}$ beschränkt ist.

Es folgt $(x_n y_n)_{n\in\mathbb{N}}$ ist eine p-adische Cauchyfolge in $\mathbb{Q}$.

Falls gilt $(x_n)_{n\in\mathbb{N}} \sim (x_n')_{n\in\mathbb{N}}$ und$(y_n)_{n\in\mathbb{N}} \sim (y_n')_{n\in\mathbb{N}}$, so gilt auch

$(x_n y_n)_{n\in\mathbb{N}} \sim (x_n' y_n')_{n\in\mathbb{N}}$, da:

$|x_i y_i - x_i' y_i'|_p = |x_i y_i - x_i y_i' + x_i y_i' - x_i' y_i'|_p = |x_i(y_i - y_i') + y_n'(x_i - x_i')|_p$

$\leq max\{|x_i(y_i - y_i')|_p, |y_i'(x_i - x_i')|_p\}$

Sei o.B.d.A. $|x_i(y_i - y_i')|_p = max\{|x_i(y_i - y_i')|_p, |y_i'(x_i - x_i')|_p\}$. Dann ist

$|x_i y_i - x_i' y_i'|_p \leq |x_i(y_i - y_i')|_p$ für alle $i \in \mathbb{N}$. Also gilt

$\lim_{i\to\infty} |x_i y_i - x_i' y_i'|_p \leq \lim_{i\to\infty} x_i(y_i - y_i') = \lim_{i\to\infty} |x_i|_p \cdot \lim_{i\to\infty} |y_i - y_i'|_p = c \cdot 0 = 0.$

Da $|\cdot|_p$ eine Norm ist, gilt auch $0 \leq |x_i y_i - x_i' y_i'|_p \Rightarrow \lim_{i\to\infty} |x_i y_i - x_i' y_i'|_p$ ist eine p-adische Nullfolge $\Rightarrow (x_n y_n)_{n\in\mathbb{N}} \sim (x_n' y_n')_{n\in\mathbb{N}}$.

Daher ist die Verknüpfung " $\cdot$ " wohldefiniert.

Somit sind nun beide Verknüpfungen wohldefiniert. Die Körperaxiome lassen sich für $\mathbb{Q}_p$ mit diesen Verknüpfungen leicht zeigen, indem man auf die Eigenschaften von $\mathbb{Q}$

zurückgreift. Dies wird hier nicht explizit gezeigt. □

Bemerkung 2.2.3 *Der p-adische Betrag setzt sich in natürlicher Weise auf $\mathbb{Q}_p$ fort, indem man setzt: $|(x_n)_{n\in\mathbb{N}}|_p = \lim_{n\to\infty} |x_n|_p$. Der p-adische Abstand erfüllt auch auf $\mathbb{Q}_p$ die Eigenschaften einer Metrik.*

Da $\mathbb{Q}_p$ ein metrischer Raum ist, können wir insbesondere folgern, dass $\mathbb{Q}_p$ ein topologischer Raum und auch ein Hausdorff-Raum ist. Dies erreichen wir mithilfe des folgenden Satzes, der inhaltlich auf Kapitel 1, (S. 10/11 und S. 22) des Buches *Topologie* von *Klaus Jänich* beruht.

Satz 2.2.4 *i) Sei (X,d) ein metrischer Raum. Eine Teilmenge $V \subseteq X$ heiße offen, wenn es zu jedem $x \in V$ ein $\epsilon > 0$ gibt, sodass die Kugel $K_\epsilon(x) := \{y \in X \mid d(x,y) \leq \epsilon\}$ um x noch ganz in V liegt. Sei $\mathcal{O}(d)$ die Menge aller offenen Teilmengen von X. $\mathcal{O}(d)$ bildet eine Topologie des metrischen Raumes (X,d).*
ii)(X,d) ist Hausdorff'sch

Beweis Sei (X,d) ein metrischer Raum.
i) Zu zeigen:
1. Beliebige Vereinigungen von offenen Mengen sind offen
2. Der Durchschnitt von je zwei offenen Mengen ist offen
3. $\varnothing$ und X sind offen.
zu 1): Sei $(V_i)_{i\in\mathbb{N}}$ eine Familie von offenen Mengen. Betrachte $V := \bigcup_{i\in\mathbb{N}} V_i$. Dann gilt für jedes $x \in V$: $\exists\, i \in \mathbb{N}$, sodass $x \in V_i$. Dann gibt es ein ϵ, sodass die Kugel $K_\epsilon(x)$ noch ganz in V_i liegt. Da $V_i \subseteq V$ liegt sie also auch ganz in $V \Rightarrow V$ ist offen.
zu 2): Seien V_1, V_2 offene Mengen. Sei $V = V_1 \cap V_2$. Dann gilt für jedes $x \in V$:
$x \in V \Rightarrow x \in V_1 \cap V_2 \Rightarrow x \in V_1$ und $x \in V_2$. Also gibt es $\epsilon_1 > 0$, sodass $K_{\epsilon_1}(x) \subseteq V_1$ und $K_{\epsilon_2}(x) \subseteq V_2$. Wähle nun $\epsilon := min\{\epsilon_1, \epsilon_2\}$. Dann gilt: $K_\epsilon(x) \subseteq V$ und somit ist V offen.
zu 3): $\varnothing$ und X sind offensichtlich offen.
ii) Zu zeigen: Zu zwei beliebigen Punkten $x, y \in X$ kann man disjunkte Umgebungen finden.

Sei $x \neq y$. Dann ist $d(x,y) = \epsilon > 0$. Dann sind die Umgebungen
$U_x := \{z \mid d(x,z) < \frac{\epsilon}{2}\}$ und $U_y := \{z \mid d(y,z) < \frac{\epsilon}{2}\}$ disjunkte Umgebungen.

□

Bemerkung 2.2.5 $(\mathbb{Q}_p, +)$ *ist eine topologische Gruppe.*

Beweis Zu zeigen ist noch, dass die Inversenabbildung $(x \mapsto -x) : \mathbb{Q}_p \to \mathbb{Q}_p$ stetig ist. Zu jedem $\epsilon \geq 0$ gibt es $\delta = \epsilon \geq 0$, sodass für alle $x, y \in \mathbb{Q}_p$ gilt: Falls $|x - y|_p \leq \delta$ dann ist $|(-x) - (-y)|_p = |-x + y|_p = |(-1)(x - y)|_p = |x - y|_p \leq \epsilon$. Somit ist die Addition auf $\mathbb{Q}_p$ stetig und $(\mathbb{Q}_p, +)$ bildet eine topologische Gruppe.

Bemerkung 2.2.6 *Wir können* $\mathbb{Q}$ *als Teilmenge von* $\mathbb{Q}_p$ *betrachten, indem wir jeder rationalen Zahl* $q \in \mathbb{Q}$ *die konstante Cauchyfolge* $(q)_n \in \mathbb{N}$ *zuordnen.*

Lemma 2.2.7 $\mathbb{Q}$ *liegt dicht in* $\mathbb{Q}_p$.

Beweis $\mathbb{Q}_p$ ist die Vervollständigung des metrischen Raumes $\mathbb{Q}$ bezüglich $|\cdot|_p$, somit liegt $\mathbb{Q}$ nach Konstruktion dicht in $\mathbb{Q}_p$.

2.3 Der Ring der ganzen p-adischen Zahlen

In diesem Abschnitt wollen wir den Ring der ganzen p-adischen Zahlen definieren und einige Eigenschaften erarbeiten, die wir in den weiteren Kapiteln benutzen wollen. Betrachte von nun an die p-adischen Zahlen als Elemente $x \in \mathbb{Q}_p$.

Definition 2.3.1 *Definiere* $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |q|_p \leq 1\}$. *Wir nennen* $\mathbb{Z}_p$ *den Ring der ganzen p-adischen Zahlen.*

Satz 2.3.2 $\mathbb{Z}_p$ *ist ein Teilring von* $\mathbb{Q}_p$.

Beweis Zu zeigen ist hier vor allem die Abgeschlossenheit von $\mathbb{Z}_p$ unter Addition und Multiplikation. Seien $x, y \in \mathbb{Z}_p$. Dann gilt nach *Lemma 2.1.4*:
$|x + y|_p \leq max\{|x|_p, |y|_p\} \leq 1$

$\Rightarrow x + y \in \mathbb{Z}_p$

$|xy|_p = |x|_p \cdot |y|_p \leq 1 \Rightarrow xy \in \mathbb{Z}_p$.

Die Verknüpfungen erfüllen somit die Abgeschlossenheit. Da gilt $+_{\mathbb{Z}_p} = +_{\mathbb{Q}_p|\mathbb{Z}_p}$ und $\cdot_{\mathbb{Z}_p} = \cdot_{\mathbb{Q}_p|\mathbb{Z}_p}$ erfüllen die Verknüpfungen offensichtlich die Ringaxiome. □

Korollar 2.3.3 *$\mathbb{Z}_p$ ist als Teilmenge von $\mathbb{Q}_p$ abgeschlossen.*

Beweis $\mathbb{Z}_p$ entspricht nach Definition der abgeschlossenen Kreisscheibe $B_1(0, |\cdot|_p)$. Somit ist $\mathbb{Z}_p$ abgeschlossen. □

Korollar 2.3.4 *$\mathbb{Z}_p$ ist als Teilmenge von $\mathbb{Q}_p$ vollständig.*

Beweis $\mathbb{Z}_p$ ist eine abgeschlossene Teilmenge der vollständigen Menge $\mathbb{Q}_p$ und somit auch vollständig. □

Bemerkung 2.3.5 *$\mathbb{Z}_p$ ist ein metrischer Raum.*

Beweis $d_p(x, y) := |x - y|_p$ erfüllt alle Eigenschaften einer Metrik auch auf $\mathbb{Z}_p$, somit ist $\mathbb{Z}_p$ ein metrischer Raum.

Korollar 2.3.6 *Nach 2.2.4 ist $\mathbb{Z}_p$ auch ein topologischer Raum und ein Hausdorffraum.*

Korollar 2.3.7 *$\mathbb{Z}_p$ ist eine topologische Gruppe.*

Beweis Dies folgt aus Bemerkung 2.2.5.

Im Folgenden wollen wir die Einheiten und die Ideale in $\mathbb{Z}_p$ untersuchen. Das Lemma über die Ideale von $\mathbb{Z}_p$ stammt auf dem Buch *Algebraische Zahlentheorie* von *Jürgen Neukirch, (S.117).*

Lemma 2.3.8 *Die Einheitengruppe von $\mathbb{Z}_p$ ist $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$.*

Beweis " $\Rightarrow$ " Sei $x \in \mathbb{Z}_p^*$. Dann gibt es $x^{-1} \in \mathbb{Z}_p^*$ sodass

$1 = |1|_p = |xx^{-1}|_p = |x|_p|x^{-1}|_p \leq |x|_p \leq 1$.

Somit ist $|x|_p = 1$.

" $\Leftarrow$ " Sei $|x|_p = 1$. Dann ist $x \in \mathbb{Q}_p^*$. Daher gibt es $x^{-1} \in \mathbb{Q}_p^*$, sodass

$1 = |xx^{-1}|_p = |x|_p|x^{-1}|_p = |x^{-1}|_p$. Somit ist $|x^{-1}|_p \leq 1 \Rightarrow x^{-1} \in \mathbb{Z}_p$. □

Nachdem wir nun die Einheiten in $\mathbb{Z}_p^*$ kennen, wenden wir uns den Idealen zu. Betrachte dazu zunächst das folgende Korollar:

Korollar 2.3.9 *Jedes $x \in \mathbb{Z}_p \setminus \{0\}$ lässt sich schreiben als $x = p^m u$ mit $m \in \mathbb{N}$ und $u \in \mathbb{Z}_p^*$.*

Beweis Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $|x|_p \leq 1$ ist, ist $|x|_p = p^{-m}$ mit $m \in \mathbb{N}$. Setze $u := p^{-m}x \in \mathbb{Q}_p^*$. Dann ist $|u|_p = p^m p^{-m} = 1$ und daher gilt nach 2.3.8 $u \in \mathbb{Z}_p^*$. □

Satz 2.3.10 *Die von Null verschiedenen Ideale von $\mathbb{Z}_p$ sind die Hauptideale $p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \nu_p(x) \geq n\}$ mit $n \in \mathbb{N}$.*

Beweis Sei $\mathfrak{a} \subset \mathbb{Z}_p$ ein Ideal, $\mathfrak{a} \neq 0$ und sei $x = p^m u, u \in \mathbb{Z}_p^*$ ein Element in $\mathfrak{a}$ mit minimalem m. Da $|x|_p \leq 1$ ist, ist $m \geq 0$. Dann gilt: $\mathfrak{a} = p^m\mathbb{Z}_p$, denn für alle $y \in \mathfrak{a}$ gilt : $y = p^n u', u' \in \mathbb{Z}_p^* \Rightarrow n \geq m$, da wir m minimal gewählt haben. Somit ergibt sich: $y = (p^{n-m}u')p^m \in p^m\mathbb{Z}_p$. Also gilt $\mathfrak{a} \subseteq p^m\mathbb{Z}_p$.
Da $x = p^m u$ und $u \in \mathbb{Z}_p^*$, gibt es $u^{-1} \in \mathbb{Z}_p^*$, sodass auch $xu^{-1} = p^m \in \mathfrak{a}$ ist. Also folgt $p^m\mathbb{Z}_p \subseteq \mathfrak{a}$. □

Unmittelbar folgt das Korollar:

Korollar 2.3.11 *$\mathbb{Z}_p$ ist ein Hauptidealring. Die Ideale bilden die absteigende Kette:* $\mathbb{Z}_p \supsetneq p\mathbb{Z}_p \supsetneq p^2\mathbb{Z}_p \ldots \supsetneq (0)$

Bemerkung 2.3.12 *$p^n\mathbb{Z}_p$ ist offen und abgeschlossen $\forall n \in \mathbb{N}$.*

Beweis $p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq \frac{1}{p^n}\}$ ist eine abgeschlossene Kugel um 0 bezüglich der Metrik d_p, also per Definition eine abgeschlossene Menge. Außerdem gilt $\forall\ x \in p^n\mathbb{Z}_p$: Für $\epsilon = \frac{1}{p^n}$ liegt die Kugel $K_{\frac{1}{p^n}}(x) := \{y \in \mathbb{Q}_p \mid |x - y|_p \leq \frac{1}{p^n}\}$ ganz in $p^n\mathbb{Z}_p$. $\Rightarrow p^n\mathbb{Z}_p$ ist offen. □

Bislang haben wir $\mathbb{Z}_p$ als Ring betrachtet. Allerdings können wir $\mathbb{Z}_p$ auch als Gruppe mit der Verknüpfung Addition betrachten. Da wir bereits die Ideale von $\mathbb{Z}_p$ kennen, kennen wir auch die Untergruppen der Gruppe $(\mathbb{Z}_p, +)$, denn es gilt:

Lemma 2.3.13 *Sei R ein Ring. Dann ist jedes Ideal* $\mathfrak{a}$ *auch eine additive Untergruppe von R.*

Beweis Die Aussage folgt direkt aus der Definition des Ideals.

Korollar 2.3.14 *Die Ideale von R sind bezüglich der Addition sogar Normalteiler von R.*

Beweis Nach Definition es Rings ist R bezüglich der Addition abelsch. Somit sind die Ideale als Untergruppen der abelschen Gruppe R Normalteiler.

Dank dieser Aussagen ist nun klar: Die offenen und normalen Untergruppen von $\mathbb{Z}_p$ sind $p^n\mathbb{Z}_p, n \in \mathbb{N}$. Wie oben gesehen handelt es sich automatisch auch um abgeschlossene Teilmengen von $\mathbb{Z}_p$.

2.4 Der Bewertungsring $\mathfrak{o}$

Sei $K/\mathbb{Q}_p$ eine Körpererweiterung vollständig bewerteter Körper, also K vollständig bezüglich eines Betrags $|\cdot|$, der sich auf $\mathbb{Q}_p$ zum p-adischen Absolutbetrag einschränkt. Dann definieren wir durch $\mathfrak{o} := \{x \in K \mid |x| \leq 1\}$ den Bewertungsring von K. Analog zum Beweis von Satz 2.3.2 erkennt man, dass $\mathfrak{o}$ bezüglich der Verknüpfungen " + " und " $\cdot$ " abgeschlossen ist und daher einen Ring bildet.

Beispiel 2.4.1 *1)* $K = \mathbb{Q}_p$*, dann ist* $\mathfrak{o} = \mathbb{Z}_p$*.*
2) Sei $\overline{\mathbb{Q}}_p$ *ein algebraischer Abschluss von* $\mathbb{Q}_p$*. Man kann zeigen, dass sich* $|\cdot|_p$ *eindeutig zu einem Absolutbetrag* $|\cdot|$ *auf* $\overline{\mathbb{Q}}_p$ *fortsetzt. Die Komplettierung von* $\overline{\mathbb{Q}}_p$ *bezüglich* $|\cdot|$ *wird mit* $\mathbb{C}_p$ *bezeichnet und heißt der Körper der komplexen p-adischen Zahlen.* $|\cdot|$ *setzt sich eindeutig auf* $\mathbb{C}_p$ *fort, sodass* $K = \mathbb{C}_p$ *ein weiteres Beispiel bildet.*

Der Bewertungsring $\mathfrak{o}$ ist der Ring, über dem wir im Folgenden gewisse Algebren definieren werden.

3 Die drei $\mathfrak{o}$-Algebren

In diesem Kapitel wollen wir die drei $\mathfrak{o}$-Algebren aus der Einleitung zunächst definieren.

3.1 Der Ring der formalen Potenzreihen $\mathfrak{o}[\![X]\!]$

Definition 3.1.1 *Betrachte den kommutativen Ring $\mathfrak{o}$. Definiere $\mathfrak{o}[\![X]\!]$ als die Menge aller Symbole der Form $\sum_{i=0}^{\infty} a_i X^i, a_i \in \mathfrak{o}$ für alle $i \in \mathbb{N}$ mit der Gleichheitsdefinition $\sum_{i=0}^{\infty} a_i X^i = \sum_{i=0}^{\infty} b_i X^i :\Leftrightarrow a_i = b_i$ für alle $i \in \mathbb{N}$. Es handelt sich hierbei um die Menge aller $\mathfrak{o}$-wertigen Folgen $\sum_{i=0}^{\infty} a_i X^i = (a_i)_{i\in\mathbb{N}}$.*
Die Menge $\mathfrak{o}[\![X]\!]$ kann mit den folgenden Operationen versehen werden:
$+ : \mathfrak{o}[\![X]\!] \times \mathfrak{o}[\![X]\!] \to \mathfrak{o}[\![X]\!] \quad (\sum_{i=0}^{\infty} a_i X^i, \sum_{i=0}^{\infty} b_i X^i) \mapsto \sum_{i=0}^{\infty} (a_i + b_i) X^i$
$\cdot : \mathfrak{o}[\![X]\!] \times \mathfrak{o}[\![X]\!] \to \mathfrak{o}[\![X]\!] \quad (\sum_{i=0}^{\infty} a_i X^i, \sum_{i=0}^{\infty} b_i X^i) \mapsto \sum_{k=0}^{\infty} \sum_{i=0}^{k} (a_i b_{k-i}) X^k$
Gemeinsam mit diesen Verknüpfungen bildet $\mathfrak{o}[\![X]\!]$ einen Ring, nämlich den Potenzreihenring über $\mathfrak{o}$. Das Einselement ist $\sum_{i=0}^{\infty} a_i X^i$ mit $a_0 = 1, a_i = 0 \ \forall \ i \geq 1$. Somit ist $\mathfrak{o}[\![X]\!]$ insbesondere auch eine $\mathfrak{o}$-Algebra.

Die Beweisidee für die Rückrichtung des folgenden Satzes stammt aus dem Buch *Einführung in die Algebra und Zahlentheorie, (S. 15)* von *Rainer Schulze-Pillot.*

Satz 3.1.2 *Sei $f \in \mathfrak{o}[\![X]\!]$. Dann ist $f = \sum_{i=0}^{\infty} a_i X^i$ eine Einheit in $\mathfrak{o}[\![X]\!]$ genau dann, wenn $a_0 \in \mathfrak{o}^*$.*

Beweis " $\Rightarrow$ " Sei $f = \sum_{i=0}^{\infty} a_i X^i$ eine Einheit. Dann gibt es $g = \sum_{i=0}^{\infty} b_i X^i \in \mathfrak{o}[\![X]\!]$, sodass $f \cdot g = (\sum_{i=0}^{\infty} a_i X^i) \cdot (\sum_{i=0}^{\infty} b_i X^i) = 1 \Leftrightarrow a_0 b_0 + \sum_{k=1}^{\infty} (\sum_{i=0}^{k} a_i b_{k-i}) X^k = 1 \Leftrightarrow a_0 b_0 = 1$ und

$\sum_{i=0}^{k} a_i b_{k-i} = 0 \ \forall\ k \in \mathbb{N}_{\geq 1} \Rightarrow \exists\ b_0 \in \mathfrak{o}$, sodass $a_0 \cdot b_0 = 1 \Rightarrow a_0$ liegt in $\mathfrak{o}^*$

" $\Leftarrow$ " Sei $a_0 \in \mathfrak{o}^*$. Dann gibt es $b_0 \in \mathfrak{o}^*$, sodass $a_0 b_0 = 1$. Setze $b_0 := a_0^{-1}$. Für $n \geq 1$ definiere $b_n \in \mathfrak{o}$ durch $b_n := -a_0^{-1}(b_0 a_n + b_1 a_{n-1} + ... + b_{n-1} a_1)$ und setze $g := \sum_{i=0}^{\infty} b_i X^i$. Die Definition der Multiplikation für formale Potenzreihen ergibt dann $f \cdot g = 1$. □

3.2 Der komplettierte Gruppenring der proendlichen Gruppe $\mathbb{Z}_p$

Im folgenden Abschnitt wollen wir die $\mathfrak{o}$-Algebra $\mathfrak{o}[\![\mathbb{Z}_p]\!]$ genau definieren. Dafür beschäftigen wir uns zunächst allgemein mit dem Gruppenring $\mathfrak{o}[G]$ über eine Gruppe G und erarbeiten Grundlagen zu projektiven Limiten von Mengen, Gruppen und Ringen. Darauf aufbauend betrachten wir proendliche Räume und Gruppen, sowie komplettierte Gruppenringe, um schlussendlich $\mathfrak{o}[\![\mathbb{Z}_p]\!]$ definieren zu können.

3.2.1 Der Gruppenring $\mathfrak{o}[G]$

Wir definieren den Gruppenring $\mathfrak{o}[G]$ nach dem Buch *Einführung in die Algebra 2 ,(§33)* von *Falko Lorenz.*

Definition 3.2.1 *Sei G eine Gruppe. Bezeichne mit $\mathfrak{o}[G]$ den freien o-Linksmodul mit Basis $\{g \mid g \in G\}$. Auf $\mathfrak{o}[G]$ können wir zunächst die Standard-Addition als Verknüpfung definieren:*

$+$: $\mathfrak{o}[G] \times \mathfrak{o}[G] \to \mathfrak{o}[G] \quad (\sum_{g\in G} a_g g, \sum_{g\in G} b_g g) \mapsto \sum_{g\in G} (a_g + b_g) g$ Die Multiplikation lässt sich definieren durch die distributive Fortsetzung der Gruppenmultiplikation auf G:

$\cdot : \mathfrak{o}[G] \times \mathfrak{o}[G] \to \mathfrak{o}[G] \quad (\sum_{g\in G} a_g g, \sum_{g\in G} b_g g) \mapsto \sum_{g,h\in G} a_g b_h gh = \sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} b_t) g$

Bezeichnet $e \in G$ das neutrale Element von G, so setzen wir $1 = \sum_{g\in G} b_g g$ mit

$$b_g := \begin{cases} 1 & \text{falls } g = e \\ 0 & \text{sonst} \end{cases}$$

Außerdem setzen wir für $\lambda \in \mathfrak{o}$: $\lambda \cdot \sum_{g\in G} a_g g = \sum_{g\in G} \lambda a_g g$.

Satz 3.2.2 $\mathfrak{o}[G]$ *ist mit den angegebenen Verknüpfungen eine* $\mathfrak{o}$*-Algebra mit Einselement 1.*

Beweis 1) Zeige: 1_e ist das Einselement. Sei $\sum_{g\in G} a_g g \in \mathfrak{o}[G]$. Es gilt:
$\sum_{g\in G} a_g g \cdot 1_e = \sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g$ mit $b_g = 1$ für $g = e, b_g = 0$, sonst. Dann ergibt sich weiterhin:
$\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g = \sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} b_t) g = \sum_{g\in G} a_{ge} g = \sum_{g\in G} a_g g.$

Andererseits gilt aber auch: $1_e \cdot \sum_{g\in G} a_g g = \sum_{g\in G} b_g g \cdot \sum_{g\in G} a_g g b_g = 1$ für $g = e, b_g = 0$, sonst. Dann ergibt sich weiterhin: $\sum_{g\in G} b_g g \cdot \sum_{g\in G} a_g g = \sum_{g\in G} (\sum_{t\in G} b_{gt^{-1}} a_t) g$ mit $b_{gt^{-1}} = 1$ für $t^{-1} = g^{-1}, 0$ sonst. Somit gilt: $\sum_{g\in G} (\sum_{t\in G} b_{gt^{-1}} a_t) g = \sum_{g\in G} a_g g$.

2) Zu zeigen ist Distributivität, also $(x+y)z = xz+yz$ und $x(y+z) = xy+xz \;\forall\; x, y, z \in \mathfrak{o}[G]$.

Seien $x = \sum_{g\in G} a_g g, y = \sum_{g\in G} b_g g$ und $z = \sum_{g\in G} c_g g \in \mathfrak{o}[G]$. Dann gilt:
$$
\begin{aligned}
&(x+y)z = (\sum_{g\in G} a_g g + \sum_{g\in G} b_g g) \cdot \sum_{g\in G} c_g g \\
&= (\sum_{g\in G} (a_g + b_g) g) \cdot (\sum_{g\in G} c_g g) \\
&= \sum_{g\in G} (\sum_{t\in G} (a_{gt^{-1}} + b_{gt^{-1}}) c_t) g \\
&= \sum_{g\in G} (\sum_{t\in G} (a_{gt^{-1}} c_t + b_{gt^{-1}} c_t)) g \\
&= \sum_{g\in G} (\sum_{t\in G} (a_{gt^{-1}} c_t) + (\sum_{t\in G} (b_{gt^{-1}} c_t)) g \\
&= \sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} c_t) g + \sum_{g\in G} (\sum_{t\in G} b_{gt^{-1}} c_t) g \\
&= (\sum_{g\in G} a_g g)(\sum_{g\in G} c_g g) + (\sum_{g\in G} b_g g)(\sum_{g\in G} c_g g) = xz + yz
\end{aligned}
$$

$$
\begin{aligned}
&x(y+z) = (\sum_{g\in G} a_g g) \cdot (\sum_{g\in G} b_g g + \sum_{g\in G} c_g g) \\
&= (\sum_{g\in G} a_g g) \cdot (\sum_{g\in G} (b_g + c_g) g) \\
&= \sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} (b_t + c_t)) g \\
&= \sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} b_t + a_{gt^{-1}} c_t)) g \\
&= \sum_{g\in G} ((\sum_{t\in G} a_{gt^{-1}} b_t) + (\sum_{t\in G} a_{gt^{-1}} c_t)) g \\
&= \sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} b_t) g + \sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} c_t) g \\
&= (\sum_{g\in G} a_g g)(\sum_{g\in G} b_g g) + (\sum_{g\in G} a_g g)(\sum_{g\in G} c_g g) = xy + xz
\end{aligned}
$$

3) Multiplikation mit Ringelementen: Sei $\lambda \in \mathfrak{o}$ und x, y wie in 2). Dann ergibt sich:

$\lambda(xy) = \lambda \cdot (\sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} b_t)g)$
$= \sum_{g\in G} \lambda(\sum_{t\in G} a_{gt^{-1}} b_t)g$
$= \sum_{g\in G} (\sum_{t\in G} \lambda a_{gt^{-1}} b_t)g$
$= (\sum_{g\in G} \lambda a_g g)(\sum_{g\in G} b_g g)$
$= (\lambda(\sum_{g\in G} a_g g))(\sum_{g\in G} b_g g) = (\lambda x)y$
Andererseits ergibt sich aber auch:
$\lambda(xy) = \lambda \cdot (\sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} b_t)g)$
$= \sum_{g\in G} \lambda(\sum_{t\in G} a_{gt^{-1}} b_t)g$
$= \sum_{g\in G} (\sum_{t\in G} a_{gt^{-1}} \lambda b_t)g$
$= (\sum_{g\in G} a_g g)(\sum_{g\in G} \lambda b_g g) = (\sum_{g\in G} a_g g)(\lambda(\sum_{g\in G} b_g g)) = x(\lambda y)$ □

3.2.2 Projektive Limiten von Mengen, Gruppen und Ringen

Dieser Abschnitt orientiert sich an §2 des Kapitels *Allgemeine Klassenkörpertheorie* des Buches *Algebraische Zahlentheorie* von *Jürgen Neukirch.*

Allgemein kann man sagen, dass der projektive Limes eine Verallgemeinerung der Bildung des Durchschnitts darstellt.
Betrachte einen topologischen Raum X und eine Familie von Teilmengen $\{X_i\}_{i\in I}$, mit der Indexmenge I, die falls sie die Mengen X_i und X_j enthält, auch $X_i \cap X_j$ enthält. Dann gilt: $\varprojlim_{i\in I} = \bigcap_{i\in I} X_i$. Die Indexmenge I wird zu einer gerichtete geordneten Menge, indem man $i \leq j$ setzt, falls $X_j \subseteq X_i$. In der Menge I gibt es somit zu jedem Paar i, j ein k, sodass $i \leq k$ und $j \leq k$.
Bezeichne mit f_{ij} die Inklusion $X_j \hookrightarrow X_i$ für $i \leq j$ und erhalte dadurch ein System $\{X_i, f_{ij}\}$ von Mengen und Abbildungen. Dieses Prinzip kann verallgemeinert werden, indem man die Inklusionen f_{ij} durch beliebige Abbildungen ersetzt. Basierend darauf ergeben sich die folgenden Definitionen:

Definition 3.2.3 *Sei I eine gerichtet geordnete Menge. Ein projektives oder auch verträgliches System über I ist eine Familie* $\{X_i, f_{ij} \mid i, j \in I, i \leq j\}$ *von topologischen Räumen*

X_i und stetigen Abbildungen $f_{ij} : X_j \to X_i$ derart, dass $f_{ii} = idX_i$ und $f_{ik} = f_{ij} \circ f_{jk}$ gilt für $i \leq j \leq k$.

Definition 3.2.4 *Der projektive Limes $\varprojlim_{i \in I} X_i$ des projektiven Systems $\{X_i, f_{ij}\}$ ist als die Teilmenge $X = \{(x_i)_{i \in I} \in \prod_{i \in I} X_i \mid f_{ij}(x_j) = x_i \text{ für } i \leq j\}$ des direkten Produkts $\prod_{i \in I} X_i$ definiert.*

Haben die Megen des projektiven System $X_i, i \in I$ bestimmte Eigenschaften, so kann man unter Umständen Rückschlüsse auf die Eigenschaften des projektiven Limes $\varprojlim_{i \in I} X_i$ ziehen. Nützlich ist dabei beispielsweise der folgende Satz:

Satz 3.2.5 (Satz von Tychonoff) *Ist $(X_i)_{i \in I}$ eine Familie kompakter, topologischer Räume, dann ist auch das kartesische Produkt $\prod_{i \in I} X_i$ mit der Produkttopologie kompakt.*

Beweis Siehe beispielsweise Kapitel 10.3 in dem Buch *Topologie* von *Klaus Jänich.*

Der Satz von Tychonoff bildet die Grundlage für den folgenden Satz:

Satz 3.2.6 *Der projektive Limes $\varprojlim_{i \in I} X_i$ kompakter Hausdorff-Räume ist kompakt.*

Beweis Nach Voraussetzung sind die Mengen $X_i, i \in I$ kompakt, somit ist nach dem Satz von Tychonoff auch das direkte Produkt kompakt. Da alle X_i hausdorff'sch sind, ist auch das direkte Produkt hausdorff'sch und enthält $X = \varprojlim_{i \in I} X_i$ als abgeschlossenen Unterraum. Dies ergibt sich auf folgende Art und Weise:
Schreibe $X = \bigcap_{i \leq j} X_{ij}$ mit $X_{ij} := \{(x_k)_{k \in I} \in \prod_{k \in I} X_k \mid f_{ij}(x_j) = x_i\}$. Da der Durchschnitt beliebig vieler abgeschlossener Mengen wieder abgeschlossen ist, muss also nur die Abgeschlossenheit der X_{ij} gezeigt werden. Bezeichne dafür mit $pr_i : \prod_{k \in I} X_k \to X_i$ die i-te Projektion. Dann sind die Abbildungen $g := pr_i$ und $f := f_{ij} \circ p_j : \prod_{k \in I} X_k \to X_i$ stetig, da die Projektion nach Definition der Produkttopologie stetig ist und f als Verkettung stetiger Funktionen ebenfalls stetig ist. Mithilfe dieser Funktionen kann man nun X_{ij} schreiben als: $X_{ij} = \{x \in \prod_{k \in I} X_k \mid g(x) = f(x)\}$. An dieser Stelle erinnern wir uns an das folgende Lemma aus der Topologie:

Lemma: Sei X ein Hausdorff-Raum. Sind $f, g : Y \to X$ zwei stetige Abbildungen von einem weiteren topologischen Raum Y nach X, so ist die Menge $\{y \in Y \mid f(y) = g(y)\}$ abgeschlossen.

Somit können wir X_{ij} als abgeschlossene Menge identifizieren. Also ist X auch abgeschlossen. Da jede abgeschlossene Teilmenge eines kompakten Raumes kompakt ist, ist X somit kompakt. □

Bemerkung 3.2.7 *Hier wurde der projektive Limes für topologische Räume definiert. Für algebraische Strukturen wie Ringe und Gruppen hat man analoge Begriffe mit derselben mengentheoretischen Definition. Die Übergangsabbildungen $f_{ij} : X_j \to X_i, i \leq j$, sind dabei Homomorphismen von Ringen beziehungsweise Gruppen.*

3.2.3 Proendliche topologische Räume und Gruppen

Dieser Abschnitt über proendliche topologische Räume und Gruppen ist sehr kurz gehalten und dient im Wesentlichen dazu, sich mit den folgenden Definitionen vertraut zu machen, die aus dem Buch *The Cohomology of Number Fields, (§1.1)* von *Neukirch, Schmidt* und *Wingberg* entnommen sind:

Definition 3.2.8 *Sei T ein topologischer Hausdorff-Raum. T heißt ein proendlicher Raum, wenn T der projektive Limes von endlichen diskreten Räumen ist.*

Definition 3.2.9 *Sei G eine topologische Hausdorff-Gruppe. G heißt eine proendliche Gruppe, wenn G der projektive Limes von endlichen, diskreten Gruppen ist.*

3.2.4 Komplettierte Gruppenringe

Die Ausführungen über komplettierte Gruppenringe stammen in Grundzügen aus §19 des Buches *p-adic Lie Groups* von *Peter Schneider*, allerdings behandeln wir das Thema hier etwas ausführlicher und ergänzen insbesondere den Beweis des Satzes 3.2.12.

Sei G eine topologische Gruppe. Bezeichne von nun an mit $N(G)$ die Menge aller normalen, offenen Untergruppen von endlichem Index in G.

Definition 3.2.10 *Wir definieren eine partielle Ordnung auf $N(G)$ durch: Für $M, N \in N(G)$, setze $M \preccurlyeq N$, wenn $N \subseteq M$. Dann ist $(N(G), \preccurlyeq)$ eine gerichtet geordnete Menge. Für $N_1, N_2 \in N(G)$ gilt nämlich $N_1 \preccurlyeq N_1 \cap N_2$ und $N_2 \preccurlyeq N_1 \cap N_2$. Hierbei ist $N_1 \cap N_2 \in N(G)$. In der Tat ist nämlich zusammen mit N_1 und N_2 auch $N_1 \cap N_2$ ein offener Normalteiler von G. Außerdem ist $(g(N_1 \cap N_2) \mapsto (gN_1, gN_2)) : G/(N_1 \cap N_2) \to G/N_1 \times G/N_2$ ein wohldefinierter und injektiver Gruppenhomomorphismus, sodass $N_1 \cap N_2$ endlichen Index in G hat. Definiere darüber hinaus Homomorphismen $\varphi_{N'N} : G/N \to G/N' \quad gN' \mapsto gN$ für $N' \preccurlyeq N \Leftrightarrow N \subseteq N'$.*

Satz 3.2.11 *Die Menge $\{G/N \mid N \in N(G)\}$ bildet zusammen mit den Abbildungen $\varphi_{N'N}, N, N' \in N(G)$ ein projektives System von Gruppen.*

Beweis Zu zeigen: $\varphi_{NM} = \varphi_{NN'} \circ \varphi_{N'M} \forall M \preccurlyeq N' \preccurlyeq N \Leftrightarrow N \subseteq N' \subseteq M$.
Es gilt $\varphi_{NM}(gM) = gN$ und $\varphi_{NN'}(\varphi_{N'M}(gM)) = \varphi_{NN'}(gN') = gN$. □

Definition 3.2.12 *Für eine Gruppe G betrachte das projektive System $\{\{G/N \mid N \in N(G)\}, \varphi_{N'N}\}$. Definiere die proendliche Vervollständigung von G als $\hat{G} := \varprojlim_{N \in N(G)} G/N$.*

Hierbei ist $\hat{G}$ dann eine proendliche Gruppe. Bei der proendlichen Vervollständigung proendlicher Gruppen ändert sich die gegebene Gruppe nicht. Das liegt an dem folgenden Satz.

Satz 3.2.13 *Ist G eine proendliche Gruppe, so gilt algebraisch und topologisch $G \cong \hat{G}$.*

Beweis Sei G eine proendliche Gruppe. Dann ist G nach Definition der projektive Limes von endlichen, diskreten Gruppen. Jede endliche diskrete Gruppe ist kompakt und hausdorff'sch und somit ist, wie in 3.2.6 gezeigt, auch G kompakt und hausdorff'sch.
Wir haben bereits gezeigt, dass $((G/N)_{N \in N(G)}, \varphi_{N'N})$ ein projektives System bildet. Betrachte den kanonischen Gruppenhomomorphismus
$\pi : G \to \varprojlim_{N \in N(G)} (G/N) \quad g \mapsto (gN)_{N \in N(G)}$.

Zeige: π ist ein Homöomorphismus und insbesondere ein Gruppenisomorphismus.

Betrachte dafür zunächst den kanonischen Homomorphismus

$\pi_N : G \to G/N \quad g \mapsto gN \; N \in N(G)$.

Versieht man G/N mit der diskreten Topologie, so ist π_N stetig. Mithilfe dieser Familie von Homomorphismen können wir nun π schreiben als: $\pi(g) = (\pi_N(g))_{N \in N(G)}$. Dann ist π stetig, da alle Komponentenfunktionen stetig sind. Noch zu zeigen ist nun also Bijektivität und die Stetigkeit der Umkehrabbildung.

Als Nächstes wollen wir die Injektivität zeigen. Dafür betrachten wir den Kern von π. Ein Element g wird genau dann auf das neutrale Element des projektiven Limes abgebildet, wenn es in jeder offenen, normalen Untergruppe $N \in N(G)$ liegt. Also gilt $ker(\pi) = \bigcap_{N \in N(G)} N$. Die N bilden eine Umgebungsbasis der 1, da in jeder Umgebung der 1 eine offene, normale Untergruppe von G enthalten ist. Da G aber hausdorff'sch ist, gibt es zu jedem $g \in G, g \neq 1$ disjunkte, offene Umgebungen U_g und U_1 von g und 1. Da in dieser Umgebung von 1 aber ein N enthalten ist, kann g nicht in N liegen. Somit gilt $\bigcap_{N \in N(G)} N = \{1\} \Rightarrow ker(\pi) = \{1\} \Rightarrow \pi$ ist injektiv.

Nun zeigen wir die Surjektivität. Zeige: Das Bild von π liegt dicht in $\varprojlim_{N \in N(G)} G/N$.

Sei $(g_N N)_{N \in N(G)} \in \varprojlim_{N \in N(G)} G/N$. Betrachte die natürliche Projektion

$pr_{N'} : \varprojlim_{N \in N(G)} G/N \to G/N' \, , N' \in N(G)$. Dann ist $pr_{N'}^{-1}(\{g_{N'} N'\}) \subseteq \varprojlim_{N \in N(G)} G/N$ eine offene Umgebung von $(g_N N)_{N \in N(G)}$ weil:

1) $pr_{N'}^{-1}(\{g_{N'} N'\})$ ist offen, da G/N' eine diskrete Menge ist und somit $\{g_{N'} N'\}$ offen. Da $pr_{N'}$ stetig ist und das Urbild einer offenen Menge unter einen stetigen Funktion offen ist, muss $pr_{N'}^{-1}(\{g_{N'} N'\})$ offen sein.

2)Es gilt: $\pi(g_{N'}) = (g_{N'} N)_{N \in N(G)} \in pr_{N'}^{-1}(\{g_{N'} N'\}), da : pr_{N'}((g_N N)_{N \in N(G)}) = g_{N'} N'$

Somit gibt es für jede offene Menge U aus $\varprojlim_{N \in N(G)} G/N$ ein $\pi(g) \in Im(\pi)$, sodass $(U \cap Im(G)) \supseteq \pi(g) \Rightarrow U \cap Im(\pi) \neq \varnothing$ für jedes U $\Rightarrow Im(\pi)$ liegt dicht in $\varprojlim_{N \in N(G)} G/N$.

Somit ist der Abschluss des Bildes $\overline{Im(\pi)} = \varprojlim_{N \in N(G)} G/N$. Da aber sowohl G, als auch $\varprojlim_{N \in N(G)} G/N$ kompakt sind und π stetig ist, ist $Im(\pi)$ bereits abgeschlossen. Somit gilt

$Im(\pi) = \overline{Im(\pi)} = \varprojlim_{N \in N(G)} G/N$. Also ist π surjektiv.
Schlussendlich gilt nach einem allgemeinen Satz der Topologie: Jede stetige Bijektion zwischen kompakten Räumen ist ein Homöomorphismus. Somit folgt: π ist ein Homöomorphismus. Damit haben wir gezeigt, dass für die proendliche Gruppe G gilt:
$G \cong \hat{G}$. □

Nun wollen wir uns kurz klarmachen, dass auch die algebraischen Gruppenringe $\mathfrak{o}[G/N]$ für variierendes $N \in N(G)$ ein projektives System von Ringen bilden. Dies halten wir in der folgenden Definition und dem anschließenden Satz fest:

Definition 3.2.14 *Sei G eine topologische Gruppe und N(G) weiterhin die Menge aller offenen, normalen Untergruppen von endlichem Index in G. Es seien die Gruppenhomomorphismen $\varphi_{N'N}$ wie in 3.2.10 definiert. Dann ist nach 3.2.11 $\{\{G/N \mid N \in N(G)\}, \varphi_{N'N}\}$ ein projektives System. Dann induziert jeder Gruppenhomomorphismus $\varphi_{N'N}$ einen Homomorphismus von $\mathfrak{o}$-Algebren, der gegeben ist durch:*
$\mathfrak{o}[\varphi_{N'N}] : \mathfrak{o}[G/N] \to \mathfrak{o}[G/N'] \quad \sum_{h \in G/N} a_h h \mapsto \sum_{h \in G/N'} a_h \varphi_{N'N}(h)$.

Satz 3.2.15 *Die Menge $\{\mathfrak{o}[G/N], N \in N(G)\}$ bildet gemeinsam mit den induzierten $\mathfrak{o}$-Algebrenhomomorphismen $\mathfrak{o}[\varphi_{N'N}]$ ein projektives System von $\mathfrak{o}$-Algebren.*

Beweis Nach Konstruktion gilt: $\mathfrak{o}[\varphi_{NN'} \circ \varphi_{N'M}] = \mathfrak{o}[\varphi_{NN'}] \circ \mathfrak{o}[\varphi_{N'M}]$ für Homomorphismen $\varphi_{NN'}$ und $\varphi_{N'M}$. Außerdem gilt: $\mathfrak{o}[id_{G/N}] = id_{\mathfrak{o}[G/N]}$. Somit bildet dann die Menge $\{\mathfrak{o}[G/N] \mid N \in N(G)\}$ gemeinsam mit den induzierten Homorphismen $\mathfrak{o}[\varphi_{NN'}]$ ein projektives System von $\mathfrak{o}$-Algebren. □

Nun können wir den komplettierten Gruppenring definieren.

Definition 3.2.16 *Es sei G eine proendliche Gruppe. Dann definieren wir*
$\mathfrak{o}[\![G]\!] := \varprojlim_{N \in N(G)} \mathfrak{o}[G/N]$
und bezeichnen dies als den komplettierten Gruppenring von G über $\mathfrak{o}$.

Bemerkung 3.2.17 *Nach Konstruktion ist $\varprojlim_{N \in N(G)} \mathfrak{o}[G/N]$ eine $\mathfrak{o}$-Algebra.*

3.2.5 Definition von $\mathfrak{o}[\![\mathbb{Z}_p]\!]$

Um den komplettierten Gruppenring $\mathfrak{o}[\![\mathbb{Z}_p]\!]$ zu definieren, müssen wir zunächst zeigen, dass $\mathbb{Z}_p$ eine proendliche Gruppe ist, also der projektive Limes von endlichen, diskreten Gruppen. Betrachte dafür den folgenden Satz, der aus dem Skriptum zur Veranstaltung *p-adische Analysis* von *Prof. Dr. Jan Kohlhaase* stammt:

Satz 3.2.18 *i) Versieht man für $n \in \mathbb{N}$ den Ring $\mathbb{Z}_p/p^n\mathbb{Z}_p$ mit der diskreten Topologie und $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p$ mit der Teilraumtopologie der Produkttopologie auf $\prod_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p$, so ist die natürliche Abbildung $\alpha : \mathbb{Z}_p \to \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p \quad x \mapsto (x+p^n\mathbb{Z}_p)_{n\in\mathbb{N}}$ ein Homöomorphismus und Isomorphismus von Ringen.*

ii) Für jedes $n \in \mathbb{N}$ ist die natürliche Abbildung $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ bijektiv.

Beweis Zeige zunächst *i*). Addition und Multiplikation auf $\varprojlim_{n\in\mathbb{N})} \mathbb{Z}_p/p^n\mathbb{Z}_p$ sind komponentenweise zu verstehen. Dann gilt für α:

$\alpha(x+y) = ((x+y)+p^n\mathbb{Z}_p)_{n\in\mathbb{N}}$

$= ((x+p^n\mathbb{Z}_p)+(y+p^n\mathbb{Z}_p))_{n\in\mathbb{N}}$

$= (x+p^n\mathbb{Z}_p)_{n\in\mathbb{N}} + (y+p^n\mathbb{Z}_p)_{n\in\mathbb{N}} = \alpha(x)+\alpha(y)$

$\alpha(xy) = ((xy)+p^n\mathbb{Z}_p)_{n\in\mathbb{N}}$

$= ((x+p^n\mathbb{Z}_p)(y+p^n\mathbb{Z}_p))_{n\in\mathbb{N}}$

$= (x+p^n\mathbb{Z}_p)_{n\in\mathbb{N}}(y+p^n\mathbb{Z}_p)_{n\in\mathbb{N}} = \alpha(x)\cdot\alpha(y)$

$\forall x, y \in \mathbb{Z}_p$ und

$\alpha(1) = (1+p1n\mathbb{Z}_p)_{n\in\mathbb{N}} = 1_{\varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p}$

$\Rightarrow \alpha$ ist ein Homomorphismus von Ringen.

Zeige nun die Stetigkeit von α. α ist stetig bezüglich der Produkttopologie genau dann, wenn für alle n aus $\mathbb{N}$ $(pr_n \circ \alpha)$ stetig ist, wobei

$pr_n : \varprojlim_{m\in\mathbb{N}} \mathbb{Z}_p/p^m\mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p \; (x+p^m\mathbb{Z}_p)_{m\in\mathbb{N}} \mapsto x+p^n\mathbb{Z}_p$ die natürliche Projektion ist.

Betrachte die Verkettung $(pr_n \circ \alpha) : \mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p$. Diese ist ein Gruppenhomomorphismus zwischen topologischen Gruppen und somit stetig genau dann, wenn $(pr_n \circ \alpha)^{-1}(U)$ offen ist für jede Nullumgebung U. Für jedes $n \in \mathbb{N}$ ist $ker(pr_n \circ \alpha) = p^n\mathbb{Z}_p$. Da $p^n\mathbb{Z}_p$ nach

2.3.12 offen in $\mathbb{Z}_p$ ist, ist $pr_n \circ \alpha$ stetig und somit auch α stetig bezüglich der Produkttopologie.

Ein Element $x \in \mathbb{Z}_p$ liegt im Kern von α, falls $x \in p^n\mathbb{Z}_p \ \forall\ n \in \mathbb{N} \Rightarrow ker(\alpha) = \bigcap_{n\in\mathbb{N}} p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq p^{-n} \ \forall\ n \in \mathbb{N}\} = \{0\} \Rightarrow \alpha$ ist injektiv.
Zu zeigen ist nun also noch Surjektivität. Betrachte dafür $(x_n)_{n\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p$. Wähle zu jedem x_n ein Element $\tilde{x}_n \in \mathbb{Z}_p$ mit $x_n = \tilde{x}_n + p^n\mathbb{Z}_p$. Aufgrund der Verträglichkeit von $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p$ gilt: $\tilde{x}_{n+1} - \tilde{x}_n \in p^n\mathbb{Z}_p \ \forall\ n \in \mathbb{N} \Rightarrow (\tilde{x}_n)_{n\in\mathbb{N}}$ ist eine Cauchyfolge in $\mathbb{Z}_p$. Da $\mathbb{Z}_p$ nach 2.3.3 und 2.3.4 als Teilmenge von $\mathbb{Q}_p$ abgeschlossen und vollständig ist, existiert $x = \lim_{n\to\infty} \tilde{x}_n \in \mathbb{Z}_p$. Wegen der Verträglichkeit gilt auch:
$\tilde{x}_{n+m} - \tilde{x}_n = \underbrace{\tilde{x}_{n+m} - \tilde{x}_{n+m-1}}_{\in p^{n+m-1}\mathbb{Z}_p} + \ldots + \underbrace{\tilde{x}_{n+1} - \tilde{x}_n}_{\in p^n\mathbb{Z}_p} \in p^n\mathbb{Z}_p \forall m \in \mathbb{N}$
Da $p^n\mathbb{Z}_p$ als offene Untergruppe der topologischen Gruppe $\mathbb{Z}_p$ zugleich auch abgeschlossen ist, wie in 2.3.12 gezeigt, folgt:
$x - \tilde{x}_n = \lim_{m\to\infty}(\tilde{x}_{n+m}) - \tilde{x}_n = \lim_{m\to\infty}(\tilde{x}_{n+m}) - \lim_{m\to\infty}(\tilde{x}_n) = \lim_{m\to\infty}(\underbrace{\tilde{x}_{n+m} - \tilde{x}_n}_{\in p^n\mathbb{Z}_p}) \in p^n\mathbb{Z}_p$
Somit gilt $x - \tilde{x}_n \in p^n\mathbb{Z}_p \Rightarrow x = \tilde{x}_n + a$ mit $a \in p^n\mathbb{Z}_p \Rightarrow \alpha(x) = (x_n)_{n\in\mathbb{N}} \Rightarrow \alpha$ ist surjektiv und somit auch bijektiv.
Um zu zeigen, dass α ein Homöomorphismus ist, fehlt nun nur noch die Stetigkeit der Umkehrabbildung. Zu zeigen ist, dass unter α^{-1} jedes Urbild einer offenen Menge offen ist. Die offenen Mengen in $\mathbb{Z}_p$ sind nach 2.3.12 gerade $p^m\mathbb{Z}_p$ für $m \in \mathbb{N}$. Betrachte also das Urbild $(\alpha^{-1})^{-1}(p^m\mathbb{Z}_p) = \alpha(p^m\mathbb{Z}_p)$. Zu zeigen ist also, dass $\alpha(p^m\mathbb{Z}_p)$ offen ist für alle $m \in \mathbb{N}$.
Ist $(x_n)_{n\in\mathbb{N}} \in (\varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p) \cap (\prod_{n=0}^{m} \{0\} \times \prod_{n>m} \mathbb{Z}_p/p^n\mathbb{Z}_p)$, so ist nach Konstruktion $\alpha^{-1}((x_n)_{n\in\mathbb{N}}) \in p^m\mathbb{Z}_p$. Ist $x \in p^m\mathbb{Z}_p$, so liegt $\alpha(x)$ in obigem Schnitt.
$(\varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p) \cap (\prod_{n=0}^{m} \{0\} \times \prod_{n>m} \mathbb{Z}_p/p^n\mathbb{Z}_p)$ ist offen bezüglich der Produkttopologie, somit ist $\alpha(p^m\mathbb{Z}_p) \subseteq \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p$ offen und daher α^{-1} stetig. Also folgt insgesamt: α ist ein Homöomorphismus.

Zeige nun ii). Betrachte die natürliche Abbildung

$\phi : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p \; a + p^n\mathbb{Z} \mapsto a + p^n\mathbb{Z}_p$.

Zu zeigen ist: ϕ ist bijektiv. Wir beweisen zuerst die Injektivität. Sei $x \in \mathbb{Z}, x \in p^n\mathbb{Z}_p$. Zu zeigen: $x \in p^n\mathbb{Z}_p$. Es ist $|x|_p \leq p^{-n}$, das heißt x ist nach Definition des p-adischen Absolutbetrags auf $\mathbb{Q}$ (definiert in 2.1.3) durch p^n teilbar $\Rightarrow x \in p^n\mathbb{Z}$.

Nun zeigen wir die Surjektivität. Betrachte $x \in \mathbb{Z}_p$. Dann muss für die Surjektivität gelten $(x + p^n\mathbb{Z}_p) \cap \mathbb{Z} \neq \varnothing$, denn ist $y \in (x + p^n\mathbb{Z}_p) \cap \mathbb{Z}$, dann gilt:

$y \in (x + p^n\mathbb{Z}_p)$ und $y \in \mathbb{Z}$

$\Leftrightarrow y = x + ap^n$ mit $a \in \mathbb{Z}_p$ und $y \in \mathbb{Z}$

$\Rightarrow x + ap^n \in \mathbb{Z} \Rightarrow x \in \mathbb{Z}/p^n\mathbb{Z}$

Da $\mathbb{Q}$ nach 2.2.7 dicht in $\mathbb{Q}_p$ liegt, gibt es zunächst $\frac{a}{b} \in (x+p^n\mathbb{Z}_p)\cap\mathbb{Q}$, unter der Annahme, dass $ggT(a,b) = 1$. Ist $z \in \mathbb{Z}_p$ mit $x + p^n z = \frac{a}{b}$, dann gilt $|\frac{a}{b}|_p = |x + p^n z|_p \leq 1$ und somit muss gelten $p \nmid b$, denn sonst wäre $\nu_p(b) \geq 1 \Rightarrow \nu_p(a)$ müsste größer gleich 1 sein, damit $p^{-\nu_p(a)+\nu_p(b)}$ noch kleiner gleich 1 ist. Also würde p auch a teilen und somit wären a und b nicht mehr teilerfremd. Also gilt $ggT(p,b) = 1$ und daher auch $ggT(p^n,b) = 1$, das heißt es existieren $r, s \in \mathbb{Z}$ mit $rb + sp^n = 1$. Setze $m := ar \in \mathbb{Z}$. Dann gilt: $\frac{a}{b} - m = \frac{a-abr}{b} = \frac{a-a(1-sp^n)}{b} = \frac{asp^n}{b}$. Da $ggT(p,b) = 1$, gilt $|b|_p = 1$ und somit $b \in \mathbb{Z}_p^*$, also folgt insgesamt: $\frac{asp^n}{b} \in p^n\mathbb{Z}_p \Rightarrow \frac{a}{b} - m \in p^n\mathbb{Z}_p \Rightarrow \frac{a}{b} + p^n\mathbb{Z}_p = m + p^n\mathbb{Z}_p \Rightarrow x + p^n\mathbb{Z}_p = \frac{a}{b} + p^n\mathbb{Z}_p = m + p^n\mathbb{Z}_p$ und $(m + p^n\mathbb{Z}_p) \cap \mathbb{Z} \neq \varnothing \Rightarrow \phi$ ist surjektiv und somit auch bijektiv. □

Bemerkung 3.2.19 *Es gilt nach 3.2.18* $\mathbb{Z}_p \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$*, somit ist* $\mathbb{Z}_p$ *der projektive Limes von endlichen, diskreten Gruppen, also eine proendliche Gruppe.*

Bemerkung 3.2.20 *Wir haben soeben im Beweis von ii) gezeigt, dass es für beliebiges* $n \in \mathbb{N}$ *für jedes* $x \in \mathbb{Z}_p$ *ein* $m \in \mathbb{Z}$ *gibt, sodass* $x - m \in p^n\mathbb{Z}_p$*. Da wir* n *beliebig klein machen können, gibt es in jeder Umgebung von* x *ein* $m \in \mathbb{Z}$*. Somit liegt* $\mathbb{Z}$ *dicht in* $\mathbb{Z}_p$*.*

Korollar 3.2.21 $\mathbb{Z}_p$*ist kompakt.*

Beweis $\mathbb{Z}_p$ und $\varprojlim_{n\in\mathbb{N})} \mathbb{Z}/p^n\mathbb{Z}$ sind homöomorph. Die endlichen, diskreten Mengen $\mathbb{Z}/p^n\mathbb{Z}$ sind kompakt und somit ist nach Satz 3.2.6 auch $\mathbb{Z}/p^n\mathbb{Z}$ kompakt. □

Nun haben wir gezeigt, dass $\mathbb{Z}_p$ die nötigen Voraussetzungen erfüllt und können nun den komplettierten Gruppenring definieren:

Definition 3.2.22 $\mathfrak{o}[\![\mathbb{Z}_p]\!] := \varprojlim_{n\in\mathbb{N}} \mathfrak{o}[\mathbb{Z}_p/p^n\mathbb{Z}_p]$

3.3 Die Maßalgebra $\mu(\mathbb{Z}_p, \mathfrak{o})$

Ziel dieses Abschnitts ist die Definition der Maßalgebra $\mu(\mathbb{Z}_p, \mathfrak{o})$, wobei wir Maße hier als stetige Linearformen auf dem Raum der K-wertigen, stetigen Funktionen auf $\mathbb{Z}_p$ verstehen, deren Norm kleiner als 1 ist. Daher werden wir zunächst einige Eigenschaften für den Raum der stetigen Funktionen von einem topologischen Raum X nach K erarbeiten und danach die K-Algebra $\mu(\mathbb{Z}_p, \mathfrak{o})$ definieren, wobei unser besonderes Augenmerk auf der Definition des Faltungsproduktes liegt. Schlussendlich zeigen wir, dass die Maßalgebra $\mu(\mathbb{Z}_p, \mathfrak{o})$ eine $\mathfrak{o}$-Unteralgebra von $\mu(\mathbb{Z}_p, K)$ ist. Grundlage dieses Teils der Arbeit ist das Skript zur Vorlesung *p-adische Analysis* von *Prof. Dr. Jan Kohlhaase.*

3.3.1 Der Raum der stetigen Funktionen $C(X, K)$

Definition 3.3.1 *Sei $(K, |\cdot|)$ ein vollständiger, nichtarchimedisch bewerteter Körper und X ein topologischer Raum. Dann bezeichnen wir mit C(X,K) den K-Vektorraum aller stetigen Abbildungen f: $X \to K$.*

Lemma 3.3.2 *Ist X kompakt und f: $X \to K$ stetig, dann gilt*
$sup\{|f(x)| \mid x \in X\} < \infty$. Der Raum C(X,K) ist bezüglich der durch
$\|f\|_\infty := sup\{|f(x)| \mid x \in X\}$ definierten Norm vollständig.

Beweis $|\cdot| : K \to \mathbb{R}$ ist stetig. Da die Verkettung stetiger Funktionen stetig ist, ist auch $|\cdot| \circ f$ stetig. Da X nach Voraussetzung kompakt ist, ist nach dem Satz von Weierstrass auch $|f(X)| \subseteq \mathbb{R}$ kompakt und dadurch insbesondere auch beschränkt.
Sei $l^\infty(X)$ der K-Vektorraum der beschränkten, K-wertigen Abbildungen $f : X \to K$ bezüglich der Norm $\|f\|_\infty$. $l^\infty(X)$ ist ein Banachraum (siehe Skriptum zur p-adischen Analysis, Lemma 8.1) und es gilt: $C(X, K) \subseteq l^\infty(X)$. Ist nun $(f_n)_{n\in\mathbb{N}}$ eine Cauchyfolge

in $C(X,K)$ bezüglich $\|\cdot\|_\infty$, so konvergiert diese Folge in $l^\infty(X)$, daher gibt es ein f, sodass $\lim_{n\to\infty} f_n =: f$. Zu zeigen: $f \in C(X,K)$ oder äquivalent formuliert: f ist stetig.
Zu $\epsilon > 0$ wähle $n \in \mathbb{N}$ mit $\|f - f_n\|_\infty < \epsilon$. Da $(f_n)_{n\in\mathbb{N}} \in C(X,K)$ ist, ist f_n stetig, also existiert zu jedem $x \in X$ eine offene Umgebung $x \in U \subseteq X$, sodass $|f_n(x) - f_n(y)| < \epsilon$ für alle $y \in U$. Dann gilt aber auch:
$|f(x) - f(y)| = |f(x) - f_n(x) + f_n(x) - f_n(y) + f_n(y) - f(y)|$
$\leq max\{\|f - f_n\|_\infty, |f_n(x) - f_n(y)|\} \leq \epsilon$
$\Rightarrow$ f ist stetig $\Rightarrow$ jede Cauchyfolge konvergiert in $C(X,K)$ bezüglich $\|\cdot\|_\infty \Rightarrow C(X,K)$ ist vollständig. □

Bemerkung 3.3.3 *C(X,K) ist ein Banachraum und damit auch ein topologischer Raum bezüglich der durch $d(f,g) := \|f - g\|_\infty$ definierten Metrik.*

3.3.2 Die K-Algebra $\mu(\mathbb{Z}_p, K)$

Sei von nun an $X = \mathbb{Z}_p$.

Definition 3.3.4 *Bezeichne mit $C(\mathbb{Z}_p,K)' := \{\ell : C(\mathbb{Z}_p,K) \to K \mid \ell$ K-linear und stetig$\}$ die Menge aller K-linearen und stetigen Abbildungen von $C(\mathbb{Z}_p,K)$ nach K.*

Ziel ist es nun eine zweite Verknüpfung neben der Addition zu definieren.

Definition 3.3.5 *Für $x \in \mathbb{Z}_p$ und $f \in C(\mathbb{Z}_p,K)$ definieren wir $\tau_x(f) \subset C(\mathbb{Z}_p,K)$ durch $\tau_x(f)(y) := f(x+y)$, wobei wir verwenden, dass $(\mathbb{Z}_p,+)$ nach 2.3.7 eine topologische Gruppe ist.*

Lemma 3.3.6 *Sei $f \in C(\mathbb{Z}_p,K)$ und $\ell \in C(\mathbb{Z}_p,K)'$. Dann ist die Abbildung $(x \mapsto \ell(\tau_x(f))) : \mathbb{Z}_p \to K$ stetig.*

Beweis Sei $\epsilon \in \mathbb{R}_{\geq 0}$. Aufgrund der Stetigkeit von ℓ existiert ein $\delta \in \mathbb{R} > 0$, sodass $|\ell(g)| \leq \epsilon$ für alle $g \in C(\mathbb{Z}_p,K)$ mit $\|g\|_\infty \leq \delta$. Da f eine stetige Funktion ist, gibt es zu jedem $x \in \mathbb{Z}_p$ ein $\delta_x \in \mathbb{R}_{\geq 0}$ mit $|f(x) - f(y)| \leq \delta$ für alle $y \in B_{\delta_x}(x)$, wobei $B_{\delta_x}(x)$ die offene Kugel um x mit Radius δ_x bezeichnet. Da $\mathbb{Z}_p$ nach 3.2.21 kompakt ist, besitzt die

offene Überdeckung $(B_{\delta_x}(x))_{x\in\mathbb{Z}_p}$ von $\mathbb{Z}_p$ eine endliche Teilüberdeckung $(B_{\delta_{x_i}}(x_i))_{1\le i\le n}$. Sei $\delta_1 := min\{\delta_{x_1}, ..., \delta_{x_n}\}$. Sind $x, y \in \mathbb{Z}_p$ mit $|x-y| \le \delta_1$, so folgt:

$|(\tau_x(f) - \tau_y(f))(z)|$

$= |f(z+x) - f(z+y)|$

$= |f(z+x+y-y) - f(z+y)|$

$= |f((z+y)+(x-y)) - f(z+y)| \le \delta$

für alle $z \in \mathbb{Z}_p$, da $z+y, z+x$ immer in einem $B_{\delta_{xi}}(x_i)$ enthalten sind. Daher gilt für $|x-y| \le \delta_i$ stets $\|\tau_x(f) - \tau_y(f)\|_\infty \le \delta$ und somit aufgrund der K-Linearität von ℓ

$|\ell(\tau_x(f)) - \ell(\tau_y(f))| = |\ell(\tau_x(f) - \tau_y(f))| \le \epsilon$ □

Lemma 3.3.7 *Seien $\ell_1, \ell_2 \in C(\mathbb{Z}_p, K)'$. Dann ist $(\ell_1 * \ell_2)(f) := \ell_2(x \mapsto \ell_1(\tau_x(f)))$ K-linear und stetig.*

Beweis Wie im vorherigen Beweis existiert aufgrund der Stetigkeit von ℓ_2 zu jedem $\epsilon \in \mathbb{R}_{>0}$ ein $\delta \in \mathbb{R}_{>0}$ mit $|\ell_2(g)| < \epsilon$ für alle $g \in C(\mathbb{Z}_p, K)$ mit $\|g\|_\infty \le \delta$. Zu δ existiert $\delta_1 \in \mathbb{R}_{>0}$ mit $|\ell_1(g)| \le \delta$ für alle $g \in C(\mathbb{Z}_p, K)$ mit $\|g\|_\infty \le \delta_1$. Ist $\|f\|_\infty \le \delta_1$, so ist auch $\|\tau_x(f)\|_\infty = \sup\{|\tau_x(f)(y)| \mid y \in X\} = \sup_{y\in\mathbb{Z}_p} f(\underbrace{x+y}_{\in\mathbb{Z}_p}) \le \delta_1 \ \forall x \in \mathbb{Z}_p$. Daher gilt

$|\ell_1(\tau_x(f))| \le \delta \ \forall \ x \in \mathbb{Z}_p$, das heißt $\|x \mapsto \ell_1(\tau_x(f))\|_\infty \le \delta$. Somit ist $|(\ell_1 * \ell_2)(f)| \le \epsilon \Rightarrow (\ell_1 * \ell_2)(f)$ ist stetig im Nullpunkt von $C(\mathbb{Z}_p, K)$.

Nun zeigen wir die K-Linearität. Seien $f, g \in C(\mathbb{Z}_p, K)$. Dann gilt:

$(\ell_1 * \ell_2)(f+g)$

$= \ell_2(x \mapsto \ell_1(\tau_x(f+g)))$

$= \ell_2(x \mapsto \ell_1((f+g)(x+y))$

$= \ell_2(x \mapsto (\ell_1(f(x+y))) + (\ell_1(g(x+y)))$

$= \ell_2(x \mapsto \ell_1(\tau_x(f))) + \ell_2(x \mapsto \ell_1(\tau_x(g)))$

$= (\ell_1 * \ell_2)(f) = (\ell_1 * \ell_2)(g)$

Sei $a \in K$. Dann ergibt sich:

$(\ell_1 * \ell_2)(af)$

$= \ell_2(x \mapsto \ell_1(\tau_x(af)))$

$= \ell_2(x \mapsto \ell_1(af(x+y)))$

$= \ell_2(x \mapsto a \cdot \ell_1(f(x+y)))$

$= a \cdot \ell_2(x \mapsto \ell_1(\tau_x(f+g)))$

$= a \cdot (\ell_1 * \ell_2)$

Aus der K-Linearität und der Stetigkeit im Nullpunkt folgt nach einem allgemeinen Prinzip nun die Stetigkeit überall.

Also haben wir gezeigt: Es gilt $(\ell_1 * \ell_2)(f) \in C(\mathbb{Z}_p, K)'$. □

Definition 3.3.8 *Die Verknüpfung*

$* : C(\mathbb{Z}_p, K)' \times C(\mathbb{Z}_p, K)' \to C(\mathbb{Z}_p, K)' \quad (\ell_1, \ell_2) \mapsto (\ell_1 * \ell_2)(f)$

heißt das Faltungsprodukt von ℓ_1 und ℓ_2.

An dieser Stelle wollen wir noch einen weiteren Funktionenraum einführen:

Definition 3.3.9 *Ist X ein topologischer Raum, so heißt eine Abbildung $f : X \to K$ lokal konstant, falls zu jedem $x \in X$ eine offene Umgebung $U \subseteq X$ von X existiert mit $f(x) = f(y)$ für alle $y \in U$. Bezeichne mit $C^\infty(X, K)$ den K-Vektorraum aller lokal konstanten Abbildungen $f : X \to K$. Eine Abbildung f heißt konstant modulo $p^m\mathbb{Z}_p$, wenn f auf jeder Restklasse $x + p^m\mathbb{Z}_p$ einen konstanten Wert annimmt, das heißt für alle $x, \alpha \in \mathbb{Z}_p : f(x) = f(x + p^m\alpha)$.*

Proposition 3.3.10 *$C^\infty(\mathbb{Z}_p, K)$ ist bezüglich $\|\cdot\|_\infty$ ein dichter Untervektorraum von $C(\mathbb{Z}_p, K)$.*

Bevor wir die Proposition beweisen, beweisen wir folgendes Lemma:

Lemma 3.3.11 *Ist $U = (U_i)_{i \in I}$ eine offene Überdeckung von $\mathbb{Z}_p$, so existiert $j \in \mathbb{N}$, sodass die endliche, offene Überdeckung $V := (b + p^j\mathbb{Z}_p)_{b \in \mathbb{Z}/p^j\mathbb{Z}}$ von $\mathbb{Z}_p$ eine Verfeinerung von U ist, das heißt zu jedem $b \in \mathbb{Z}/p^j\mathbb{Z}$ existiert ein $i \in I$ mit $b + p^j \subseteq U_i$.*

Beweis Da U_i offen ist, existieren zu $i \in I$ und $x \in U_i$ und ein Element $j(x) \in \mathbb{N}$ mit $x + p^{j(x)}\mathbb{Z}_p \subseteq U_i$ und da $\mathbb{Z}$ nach 3.2.20 dicht in $\mathbb{Z}_p$ liegt, gibt es $b(x) \in \mathbb{Z}$ mit $x + p^{j(x)}\mathbb{Z}_p = b(x) + p^{j(x)}\mathbb{Z}_p$.

Dann ist $V' := (b(x) + p^{j(x)}\mathbb{Z}_p)_{x \in \mathbb{Z}_p}$ eine offene Überdeckung von $\mathbb{Z}_p$, die U verfeinert.

Da $\mathbb{Z}_p$ nach 3.2.21 kompakt ist, enthält jede offene Überdeckung von $\mathbb{Z}_p$ eine endliche Teilüberdeckung. Also existieren $x_1, ..., x_n \in \mathbb{Z}_p$ mit $\mathbb{Z}_p = \bigcup_{i=1}^{n} (b(x_i) + p^{j(x_i)}\mathbb{Z}_p)$. Dann gilt für $j := max\{j(x_1), ..., j(x_n)\}$: Zu jedem $j \in \mathbb{Z}/p^j\mathbb{Z}$ existiert ein $i \in I$ mit $b + p^j\mathbb{Z}_p \subseteq U_i$. □

Nun beweisen wir die Proposition:

Beweis (Proposition) Zu zeigen: In jeder Umgebung von $f \in C(\mathbb{Z}_p, K)$ gibt es ein $g \in C^\infty(\mathbb{Z}_p, K)$. Sei $f \in C(\mathbb{Z}_p, K)$ und $\epsilon > 0$ gegeben. Gesucht ist $g \in C^\infty(\mathbb{Z}_p, K)$ mit $\|g - f\|_\infty < \infty$, das heißt es soll für alle $x \in \mathbb{Z}_p$ gelten: $|f(x) - g(x)| < \epsilon$. f ist stetig, somit gibt es zu jedem $x \in \mathbb{Z}_p$ eine offene Umgebung $U(x) \subseteq \mathbb{Z}_p$ mit $|f(x) - f(y)| < \epsilon$ für alle $y \in U(x)$. Dann bilden die offenen Umgebungen $(U(x))_{x\in\mathbb{Z}_p}$ eine offene Überdeckung von $\mathbb{Z}_p$ und es gibt nach Lemma 2.3.11 ein $j \in \mathbb{N}$, sodass die endliche offene Überdeckung $V = (b+p^j\mathbb{Z}_p)_{b\in\mathbb{Z}/p^j\mathbb{Z}}$ von $\mathbb{Z}_p$ eine Verfeinerung von $(U(x))_{x\in\mathbb{Z}_p}$ ist, das heißt zu jedem $b \in \mathbb{Z}/p^j\mathbb{Z}$ existiert ein $x \in \mathbb{Z}_p$ mit $b+p^j\mathbb{Z}_p \subseteq U(x)\ \forall\ x \in \mathbb{Z}_p$. Betrachte dann die Funktion $g : \mathbb{Z}_p \to K$ mit $g\,|_{b+p^j\mathbb{Z}_p} = c$, mit $c \in f(U(x))$, zum Beispiel $c := f(x)$. Dann ist $g \in C^\infty(\mathbb{Z}_p, K)$ und $\forall x \in b+p^j\mathbb{Z}_p \subseteq U(x)$ gilt: $|f(x) - g(x)| = |f(x) - c| = |f(x) - f(y)| < \epsilon$ für ein $y \in U(x)$. Da $(b + p^j\mathbb{Z}_p)_{b\ \in\mathbb{Z}/p^j\mathbb{Z}_p}$ eine offene Überdeckung von $\mathbb{Z}_p$ bilden, gilt $\forall x \in \mathbb{Z}_p : |f(x) - g(x)| < \epsilon$. Also gibt es in jeder Umgebung von f eine lokal konstante Funktion g $\Rightarrow C^\infty(\mathbb{Z}_p, K)$ liegt dicht in $C(\mathbb{Z}_p, K)$. □

Mithilfe der lokal konstanten Funktionen können wir nun den folgenden Satz zeigen:

Satz 3.3.12 *Zusammen mit dem Faltungsprodukt ist $C(\mathbb{Z}_p, K)'$ eine kommutative K-Algebra mit 1. Für $\ell_1, \ell_2 \in C(\mathbb{Z}_p, K)'$ gilt für die Operatornorm bezüglich $\|\cdot\|_\infty$:*
$\|\ell_1 * \ell_2\| \leq \|\ell_1\| \cdot \|\ell_2\|$.

Beweis 1) Zeige: Das Einselement ist $\delta_0 := (f \mapsto f(0)) \in C(\mathbb{Z}_p, K)'$
$(\ell_1 * \delta_0)(f) = \delta_0(x \mapsto \ell_1(\tau_x(f))) = \ell_1(\tau_0(f)) = \ell_1(f(0 + y)) = \ell_1(f)$
$(\delta_0 * \ell_1) = \ell_1(x \mapsto \delta_0(\tau_x(f))) = \ell_1(x \mapsto f(x + 0)) = \ell_1(f)$
2) Assoziativität: Seien $\ell_1, \ell_2, \ell_3 \in C(\mathbb{Z}_p, K)', f \in C(\mathbb{Z}_p, K)$.
$((\ell_1 * \ell_2) * \ell_3)(f) = \ell_3(x \mapsto (\ell_1 * \ell_2)(\tau_x(f)))$
$= \ell_3(x \mapsto (\ell_2(y \mapsto \ell_1(\tau_y(\tau_x(f))))))$

$= \ell_3(x \mapsto (\ell_2(y \mapsto \ell_1(\tau_{x+y}(f)))))$

$= \ell_3(x \mapsto (\ell_2(\tau_x(y \mapsto \ell_1(\tau_y(f))))))$

$= (\ell_2 * \ell_3)(y \mapsto \ell_1(\tau_y(f)))$

$= (\ell_1 * (\ell_2 * \ell_3))(f)$

3) Distributivität: Seien $\ell_1, \ell_2, \ell_3 \in C'(\mathbb{Z}_p, K)$

$((\ell_1 + \ell_2) * \ell_3)(f)$

$= \ell_3(x \mapsto (\ell_1 + \ell_2)(\tau_x(f)))$

$= \ell_3(x \mapsto (\ell_1(\tau_x(f)) + \ell_2(\tau_x(f)))$

$= \ell_3((x \mapsto (\ell_1(\tau_x(f)))) + (x \mapsto (\ell_2(\tau_x(f)))))$

$= \ell_3((x \mapsto (\ell_1(\tau_x(f))))) + \ell_3((x \mapsto (\ell_2(\tau_x(f)))))$

$= (\ell_1 * \ell_3) + (\ell_1 * \ell_2)$

4) Kommutativität: Seien $\ell_1, \ell_2 \in C(\mathbb{Z}_p, K)'$. Da ℓ_1 und ℓ_2 K-linear und stetig sind, können sie als Operatoren vom normierten Raum $C(\mathbb{Z}_p, K)$ in den normierten Raum K betrachtet werden. Da $C^\infty(\mathbb{Z}_p, K)$ nach 3.3.10 dicht in $C(\mathbb{Z}_p, K)$ liegt und $C(\mathbb{Z}_p, K)$, wie in 3.3.2 gezeigt, ein Banachraum ist, gibt es für jeden Operator $T : C^\infty(\mathbb{Z}_p, K) \to K$ eine eindeutige Fortsetzung zu einem Operator $\overline{T} : C(\mathbb{Z}_p, K) \to K$. Somit genügt es zu zeigen, dass $\ell_1 * \ell_2$ und $\ell_2 * \ell_1$ auf charakteristischen Funktionen $\mathbf{1}_{b+p^j\mathbb{Z}_p}$ der Mengen $b + p^j\mathbb{Z}_p \subseteq \mathbb{Z}_p$ übereinstimmen mit $b \in \mathbb{Z}_p, j \in \mathbb{N}$.$\mathbf{1}_{b+p^j\mathbb{Z}_p}$ ist eine lokal konstante Funktion. Für $x' \in \mathbb{Z}_p$ und $\alpha \in p^j\mathbb{Z}_p$ gilt: $\tau'_x(\mathbf{1}_{b+p^j\mathbb{Z}_p}) = \mathbf{1}_{b-x'+p^j\mathbb{Z}_p} = \mathbf{1}_{b-x'-\alpha+p^j\mathbb{Z}_p} = \tau_{x'+\alpha}(\mathbf{1}_{b+p^j\mathbb{Z}_p})$ im Sinne einer Abbildungsgleichheit, denn für $y \in \mathbb{Z}_p$ gilt:
Falls $\tau_{x'}(\mathbf{1}_{b+p^j\mathbb{Z}_p})(y) = 1$, so gilt $x' + y \in (b + p^j\mathbb{Z}_p) \Leftrightarrow y \in (b - x' + p^j\mathbb{Z}_p)$ und daher $\mathbf{1}_{b-x'+p^j\mathbb{Z}_p}(y) = 1$. Da $\alpha \in p^j\mathbb{Z}_p$ gilt auch $y \in (b - x' - \alpha + p^j\mathbb{Z}_p)$, also $\mathbf{1}_{b-x'-\alpha+p^j\mathbb{Z}_p}(y) = 1$. Dann gilt auch: $x' + \alpha + y \in (b + p^j\mathbb{Z}_p)$ und somit $\tau_{x'+\alpha}(\mathbf{1}_{b+p^j\mathbb{Z}_p})(y) = 1$. Somit gilt Abbildungsgleichheit. Da ℓ_1 K-linear ist, impliziert dies, dass die Funktion $x' \mapsto \ell_1(\tau_{x'}(\mathbf{1}_{b+p^j\mathbb{Z}_p}))$ gleich $\sum_{x' \in \mathbb{Z}_p/p^j\mathbb{Z}_p} \ell_1(\mathbf{1}_{b-x'+p^j\mathbb{Z}_p}) \cdot \mathbf{1}_{x'+p^j\mathbb{Z}_p}$ ist. Es folgt:

$(\ell_1 * \ell_2)(\mathbf{1}_{b+p^j\mathbb{Z}_p})$

$= \ell_2(x' \mapsto \ell_1(\tau_{x'}(\mathbf{1}_{b+p^j\mathbb{Z}_p})))$

$= \ell_2(\sum_{x' \in \mathbb{Z}_p/p^j\mathbb{Z}_p} \ell_1(\mathbf{1}_{b-x'+p^j\mathbb{Z}_p}) \cdot \mathbf{1}_{x'+p^j\mathbb{Z}_p})$

$$= \sum_{x' \in \mathbb{Z}_p/p^j\mathbb{Z}_p} \ell_2(\ell_1(\mathbf{1}_{b-x'+p^j\mathbb{Z}_p}) \cdot \mathbf{1}_{x'+p^j\mathbb{Z}_p})$$
$$= \sum_{x' \in \mathbb{Z}_p/p^j\mathbb{Z}_p} \ell_1(\mathbf{1}_{b-x'+p^j\mathbb{Z}_p}) \cdot \ell_2(\mathbf{1}_{x'+p^j\mathbb{Z}_p}).$$

Die Abbildung $(x' + p^j\mathbb{Z}_p \mapsto b - x' + p^j\mathbb{Z}_p) : \mathbb{Z}_p/p^j\mathbb{Z}_p \to \mathbb{Z}_p/p^j\mathbb{Z}_p$ ist bijektiv. Setze $x := b - x' \Leftrightarrow x' = b - x$. Dann ergibt sich:

$(\ell_2 * \ell_1)(\mathbf{1}_{b+p^j\mathbb{Z}_p}) = \sum_{x' \in \mathbb{Z}_p/p^j\mathbb{Z}_p} \ell_1(\mathbf{1}_{b-x'+p^j\mathbb{Z}_p}) \cdot \ell_2(\mathbf{1}_{x'+p^j\mathbb{Z}_p}) = \sum_{x \in \mathbb{Z}_p/p^j\mathbb{Z}_p} \ell_1(\mathbf{1}_{x+p^j\mathbb{Z}_p}) \cdot \ell_2(\mathbf{1}_{b-x+p^j\mathbb{Z}_p})$
$= (\ell_2 * \ell_1)(\mathbf{1}_{b+p^j\mathbb{Z}_p})$

Somit stimmen ℓ_1 und ℓ_2 auf charakteristischen Funktionen der Form $\mathbf{1}_{b+p^j\mathbb{Z}_p}$ überein, daher ist das Faltungsprodukt kommutativ.

Für $f \in C(\mathbb{Z}_p, K)$ gilt schließlich für jedes $x' \in \mathbb{Z}_p$:

$|\ell_1(\tau_{x'}(f))| \leq \|\ell_1\| \cdot \|\tau_{x'}(f)\|_\infty = \|\ell_1\| \cdot \|f\|_\infty$ und daher $\|x' \mapsto \ell_1(\tau_{x'}(f))\|_\infty \leq \|\ell_1\|\|f\|_\infty$.

Dies liefert $|(\ell_1 * \ell_2)(f)| \leq \|\ell_2\|\|\ell_1\|\|f\|_\infty$ und damit $\|\ell_1 * \ell_2\| \leq \|\ell_1\|\|\ell_2\|$

Wir haben nun gezeigt: $\mu(\mathbb{Z}_p, K)$ ist eine K-Banach-Algebra bezüglich $\|\cdot\|$ □

3.3.3 Die $\mathfrak{o}$-Unteralgebra $\mu(\mathbb{Z}_p, \mathfrak{o})$

Bezeichne mit $\mu(\mathbb{Z}_p, \mathfrak{o})$ die Menge $\mu(\mathbb{Z}_p, \mathfrak{o}) := \{\mu \in \mu(\mathbb{Z}_p, K) \mid \|\mu\| \leq 1\}$.

Satz 3.3.13 *$\mu(\mathbb{Z}_p, \mathfrak{o})$ ist eine $\mathfrak{o}$-Unteralgebra von $\mu(\mathbb{Z}_p, K)$.*

Beweis Zu zeigen: $\mu(\mathbb{Z}_p, \mathfrak{o})$ ist ein $\mathfrak{o}$-Untermodul von $\mu(\mathbb{Z}_p, \mathfrak{o})$ und $\mu(\mathbb{Z}_p, \mathfrak{o})$ ist unter dem Faltungsprodukt abgeschlossen. Zeige zuerst: $\mu(\mathbb{Z}_p, \mathfrak{o})$ ist ein $\mathfrak{o}$-Untermodul von $\mu(\mathbb{Z}_p, K)$.

1) Für das Einselement δ_0 gilt:

$\|\delta_0\| = \sup_{f \in C(\mathbb{Z}_p, K)\setminus\{0\}} \frac{|\delta_0(f)|}{\|f\|_\infty} = \sup_{f \in C(\mathbb{Z}_p, K)\setminus\{0\}} \frac{|f(0)\|}{\|f\|_\infty} \leq 1 \Rightarrow \delta_0 \in \mu(\mathbb{Z}_p, \mathfrak{o})$

2) Seien $\ell_1, \ell_2 \in \mu(\mathbb{Z}_p, \mathfrak{o})$.

$\|\ell_1 + \ell_2\| \leq max\{\|\ell_1\|, \|\ell_2\|\} \leq 1$, da $|\cdot|$ nichtarchimedisch ist. Somit ist $\mu(\mathbb{Z}_p, \mathfrak{o})$ unter der Addition abgeschlossen.

3) Sei $a \in \mathfrak{o}$, $\ell_1 \in \mu(\mathbb{Z}_p, \mathfrak{o})$

$\|a \cdot \ell_1\| = \underbrace{|a|}_{\leq 1} \cdot \|\ell_1\| \leq \|\ell_1\| \leq 1$

$\Rightarrow \mu(\mathbb{Z}_p, \mathfrak{o})$ ist ein $\mathfrak{o}$-Unterraum von $\mu(\mathbb{Z}_p, K)$.

Zeige nun die Abgeschlossenheit unter dem Faltungsprodukt. Seien $\ell_1, \ell_2 \in \mu(\mathbb{Z}_p, \mathfrak{o})$. Dann gilt nach 3.3.12:

$\|\ell_1 * \ell_2\| \leq \|\ell_1\| \cdot \|\ell_2\| \leq 1 \cdot 1 = 1$

Somit haben wir gesehen: $\mu(\mathbb{Z}_p, \mathfrak{o})$ ist eine $\mathfrak{o}$-Unteralgebra von $\mu(\mathbb{Z}_p, \mathfrak{o})$ □

4 Die Iwasawa-Isomorphismen

Nachdem wir in Kapitel 2 drei scheinbar sehr unterschiedliche Algebren definiert haben, wollen wir in diesem Kapitel zeigen, dass sie tatsächlich paarweise zueinander isomorph sind.

4.1 Der Isomorphismus zwischen $\mathfrak{o}[\![X]\!]$ und $\mathfrak{o}[\![\mathbb{Z}_p]\!]$

Um zu zeigen, dass der Potenzreihenring über $\mathfrak{o}$ isomorph ist zu dem komplettierten Gruppenring über die proendliche Gruppe $\mathbb{Z}_p$, zeigen wir zunächst, dass $\mathfrak{o}[\![\mathbb{Z}_p]\!] \cong \varprojlim_{n\in\mathbb{N}} \mathfrak{o}[X]/(h_n)$, wobei $h_n = (1+X)^{p^n} - 1$ ist und anschließend daran, dass $\mathfrak{o}[\![x]\!] \cong \varprojlim_{n\in\mathbb{N}} \mathfrak{o}[X]/(h_n)$ ist.

Die Grundidee des Beweises stammt aus Abschnitt §3.2 des Buches *Cyclotomic fields 1 and 2* von *Serge Lang*, allerdings arbeiten wir den Beweis hier sehr viel genauer aus.

4.1.1 Der Isomorphismus zwischen $\mathfrak{o}[\![\mathbb{Z}_p]\!]$und dem projektiven Limes von $\mathfrak{o}[X]/(h_n)$

Sei Γ eine topologische Gruppe, die isomorph ist zu $\mathbb{Z}_p$ und multiplikativ geschrieben wird. Sei γ ein beliebiger aber fester Erzeuger der Gruppe, sodass der Isomorphismus zwischen $\mathbb{Z}_p$ und Γ geschrieben werden kann als: $\varphi : \mathbb{Z}_p \to \Gamma \;\; x \mapsto \gamma^x$ für $x \in \mathbb{Z}_p$.
Sei $\Gamma_n = \Gamma/\Gamma^{p^n} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$. Dann ist Γ_n zyklisch und von Ordnung p^n und wird erzeugt vom Bild γ_n von γ in Γ/Γ^{p^n}. Man erhält das kommutative Diagramm

$$\begin{array}{ccc} \mathfrak{o}[\Gamma_{n+1}] & \xrightarrow{\varphi_{n+1}} & \mathfrak{o}[T]/(T^{p^{n+1}}-1) \\ \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} \\ \mathfrak{o}[\Gamma_n] & \xrightarrow[\varphi_n]{} & \mathfrak{o}[T]/(T^{p^n}-1) \end{array}$$

wobei $\mathfrak{o}[\Gamma_{n+1}]$ und $\mathfrak{o}[\Gamma_n]$ die Gruppenalgebren über Γ_{n+1} beziehungsweise Γ_n sind. Dabei ist für alle $n \in \mathbb{N}$ definiert durch:
$\varphi_n : \mathfrak{o}[\Gamma_n] \to \mathfrak{o}[T]/(T^{p^n}-1) \quad (\sum_{i=0}^{p^n-1} a_i \gamma_{p^n}^i) \mapsto a_0 + ... + a_{p^n-1} T^{p^n-1} + (T^{p^n}-1)$ mit $\gamma_{p^n}^{p^n} = 1$.
Die Abbildungen ϕ_2 ist die kanonische Restklassenabbildung
$\phi_2 : \mathfrak{o}[T]/(T^{p^{n+1}}-1) \to \mathfrak{o}[T]/(T^{p^n}-1) \quad g + (T^{p^{n+1}}-1) \mapsto g + (T^{p^n}-1)$
Also wird die Restklasse von g in $\mathfrak{o}[T]/(T^{p^{n+1}}-1)$ auf die Restklasse von g in $\mathfrak{o}[T]/(T^{p^n}-1)$ abgebildet. Diese Abbildung ist wohldefiniert, da $(T^{p^{n+1}}-1) \subseteq (T^{p^n}-1)$ ist. Beachte hierfür, dass
$(T^{p^{n+1}}-1) = ((T^{p^n})^p - 1) = (T^{p^n}-1)((T^{p^n})^{p-1} + (T^{p^n})^{p-2} + ... + T^{p^n} + 1)$.
Die Abbildung ϕ_1 ist der bereits im Satz 3.2.10 betrachtete Homomorphismus von $\mathfrak{o}$-Algebren, der durch die Restklassenabbildung $\Gamma_{n+1} \to \Gamma_n$ $\Gamma^{p^{n+1}} \mapsto \alpha\Gamma^{p^n}$ induziert wird. Mit der Definition dieser Abbildungen ist klar: $\phi_1 \circ \varphi_n = \varphi_{n+1} \circ \phi_2$.

Setze nun $X = T - 1$, dann ist $T = X + 1$. Somit gilt $\mathfrak{o}[T] = \mathfrak{o}[X]$ und
$\mathfrak{o}[T]/(T^{p^n}-1) \hat{=} \mathfrak{o}[X]/((X+1)^{p^n}-1)$.

Definition 4.1.1 *Definiere* $h_n := h_n(X) := (X+1)^{p^n} - 1 \; \forall n \in \mathbb{N}$.

Definition 4.1.2 *Ein Polynom* $f \in \mathfrak{o}[X]$ *heißt ausgezeichnetes Polynom, wenn alle Koeffizienten von f mit Ausnahme des Leitkoeffizienten durch p teilbar sind.*

Bemerkung 4.1.3 h_n *ist für alle n aus* $\mathbb{N}$ *ein ausgezeichnetes Polynom.*

Beweis Zu zeigen: Alle Koeffizienten von h_n, mit Ausnahme des Leitkoeffizienten, sind durch p teilbar.

$(X+1)^{p^n} - 1 = \sum_{k=0}^{p^n} \binom{p^n}{k} X^{p^n-k} \cdot 1^k - 1 = X^{p^n} + \sum_{k=1}^{p^n-1} \frac{p^n}{k!\cdot(p^n-k)!} X^{p^n-k} + 1 - 1$

$= X^{p^n} + \sum_{k=1}^{p^n-1} \underbrace{\frac{p^n}{k!\cdot(p^n-k)!}}_{teilbar\ durch\ p} X^{p^n-k}$

$\Rightarrow$ Alle Koeffizienten außer dem Leitkoeffizienten sind durch p teilbar. □

Satz 4.1.4 (Verallgemeinerter Euklidischer Algorithmus) *Sei $\mathfrak{m}$ das maximale Ideal von $\mathfrak{o}$. Sei $f(x) = \sum_{i=0}^{\infty} a_i X^i$ eine Potenzreihe in $\mathfrak{o}[\![x]\!]$, sodass nicht alle a_i in $\mathfrak{m}$ liegen. Seien $a_0, ..., a_{n-1} \in \mathfrak{m}$ und $a_n \in \mathfrak{o}^*$. Dann gibt es für jedes $g \in \mathfrak{o}[\![X]\!]$ eine eindeutige Lösung der Gleichung $g = qf + r$ mit $q \in \mathfrak{o}[\![X]\!], r \in \mathfrak{o}[X]$ und $deg(r) \leq n-1$.*

Beweis Siehe beispielsweise *Serge Lang, Cyclotomic Fields 1 and 2*, Kapitel 5, §2, Theorem 2.1.

Bemerkung 4.1.5 *Jedes ausgezeichnete Polynom h kann als Potenzreihe aufgefasst werden. $a_n \in \mathfrak{o}^*$ ist dann der Leitkoeffizient.*

Mithilfe des Verallgemeinerten Euklidischen Algortihmus können wir nun den folgenden Satz zeigen:

Satz 4.1.6 *φ_n ist für alle $n \in \mathbb{N}$ ein Ringisomorphismus.*

Beweis Zeige zunächst, dass φ_n ein Ringhomomorphismus ist.

Addition:

$\varphi_n(\sum_{i=0}^{p^n-1} a_i \gamma_{p^n}^i + \sum_{i=0}^{p^n-1} b_i \gamma_{p^n}^i)$

$= \varphi_n(\sum_{i=0}^{p^n-1} (a_i + b_i) \gamma_{p^n}^i)$

$= (a_{p^n-1} + b_{p^n-1}) T^{p^n-1} + ... + (a_0 + b_0) + (T^{p^n} - 1)$

$= (a_{p^n-1} T^{p^n-1} + ... + a_0) + (b_{p^n-1} T^{p^n-1} + ... + b_0) + (T^{p^n} - 1)$

$= \varphi_n(\sum_{i=0}^{p^n-1} a_i \gamma_{p^n}^i) + \varphi_n(\sum_{i=0}^{p^n-1} b_i \gamma_{p^n}^i)$

Multiplikation:

$\varphi_n(\sum_{i=0}^{p^n-1} a_i \gamma_{p^n}^i \cdot \sum_{i=0}^{p^n-1} b_i \gamma_{p^n}^i)$

$$= \varphi_n\Big(\sum_{s=0}^{2(p^n-1)} \Big(\sum_{r=0}^{s} a_{s-r}b_r\Big)\gamma_{p^n}^{s-r+r}\Big)$$
$$= \sum_{s=0}^{2(p^n-1)} \Big(\sum_{r=0}^{s} a_{s-r}b_r\Big)T^s$$
$$= \varphi_n\Big(\sum_{i=0}^{p^n-1} a_i\gamma_{p^n}^i\Big) \cdot \varphi_n\Big(\sum_{i=0}^{p^n-1} b_i\gamma_{p^n}^i\Big)$$

Einselement: Das Einselement in $\mathfrak{o}[\Gamma_n]$ ist gerade $\sum_{i=0}^{p^n-1} a_i\gamma_{p^n}^i$ mit $a_0 = 1$ und $a_i = 0$ für $1 \leq i \leq p^n - 1$. Dann ist $\varphi_n(1) = 1 + (T^{p^n} - 1) = 1_{\mathfrak{o}[T]/(T^{p^n}-1)}$

Zeige nun Bijektivität:

Um Injektivität zu zeigen, betrachten wir den Kern. Sei $g \in \mathfrak{o}[\Gamma_n]$ im Kern von φ_n. Schreibt man $g = \sum_{i=0}^{p^n-1} a_n\gamma_{p^n}^i$, so folgt $\sum_{i=0}^{p^n-1} a_iT^i \in (T^{p^n} - 1)$, was aus Gradgründen nur dann möglich ist, wenn $a_0 = ... = a_{p^n-1} = 0$. Es folgt $ker(\varphi_n) = \{0\}$, das heißt φ_n ist injektiv.

Nun zeigen wir noch Surjektivität. Sei $f \in \mathfrak{o}[T]$. Schreibe $\tilde{f} := f(T + 1) \in \mathfrak{o}[T] = \mathfrak{o}[X]$ als $\tilde{f} = qh_n + r$ in $\mathfrak{o}[X]$ für geeignetes $q \in \mathfrak{o}[X]$ wie in 4.1.4. Schreibt man $r(X - 1) = \sum_{i=0}^{p^n-1} a_iX^i$, so gilt $\varphi_n(\sum_{i=0}^{p^n-1} a_i\gamma_{p^n}^i) = \sum_{i=0}^{p^n-1} a_iT^i = r(T - 1) = r(X) \equiv \tilde{f}(X) \bmod (T^{p^n} - 1)$, da $h_n(X) = T^{p^n} - 1$. Nun ist aber $\tilde{f}(X) = \tilde{f}(T - 1) = f(T) \Rightarrow \varphi_n$ ist surjektiv.

Insgesamt folgt nun: φ_n ist ein Ringisomorphismus. □

Bemerkung 4.1.7 *Der Isomorphismus φ_n ist abhängig vom Erzeuger γ.*

Da $\mathfrak{o}[\Gamma_n] \cong \mathfrak{o}[X]/(h_n)$ gilt: $\varprojlim_{n\in\mathbb{N}} \mathfrak{o}[\Gamma_n] \cong \varprojlim_{n\in\mathbb{N}} \mathfrak{o}[X]/(h_n)$ und somit auch
$\mathfrak{o}[\![\mathbb{Z}_p]\!] \cong \varprojlim_{n\in\mathbb{N}} \mathfrak{o}[X]/(h_n)$
Wir wollen an dieser Stelle noch sehen, dass $\varprojlim_{n\in\mathbb{N}} \mathfrak{o}[X]/(h_n)$ mit geeigneten Abbildungen tatsächlich ein projektives System bildet. Definiere dafür die zunächst die Abbildungen.

Definition 4.1.8 *Definiere für alle $i \in \mathbb{N}$ die Abbildungen*
$f_{i,i+1} : \mathfrak{o}[X]/h_{i+1}\mathfrak{o}[X] \to \mathfrak{o}[X]/h_i\mathfrak{o}[X] \quad r_{i+1} + (h_{i+1}) \mapsto r_{i+1} + (h_i)$.

Korollar 4.1.9 $\{\mathfrak{o}[X]/(h_i), f_{i,i+1} \mid i \in \mathbb{N}\}$ *bildet ein projektives System.*

Beweis Zu zeigen ist, dass h_{n+1} ein Vielfaches von h_n in $\mathfrak{o}[X]$ ist. Da aber nach 4.1.1 h_n definiert ist durch $h_n = (X+1)^{p^n} - 1 = T^{p^n} - 1$ ist dies äquivalent zu der Aussage: $T^{p^{n+1}} - 1$ ist ein Vielfaches von $T^{p^n} - 1$ in $\mathfrak{o}[T]$.
Da wir $T^{p^{n+1}} - 1$ auch schreiben können als $T^{p^{n+1}} = (T^{p^n} - 1)(\sum_{j=0}^{p-1} T^{p^n} j)$, ist die Aussage wahr und daher $\varprojlim_{n\in\mathbb{N}} \mathfrak{o}[X]/(h_n)$ wohldefiniert. □

4.1.2 Der Isomorphismus zwischen dem projektiven Limes von $\mathfrak{o}[X]/(h_n)$ und $\mathfrak{o}[\![X]\!]$

Wir definieren die Abbildung
$\epsilon : \mathfrak{o}[\![X]\!] \to \varprojlim_{n\in\mathbb{N}} \mathfrak{o}[X]/(h_n) \quad g \mapsto (r_n + h_n\mathfrak{o}[X])_{n\geq 0}$

Satz 4.1.10 *ϵ ist wohldefiniert.*

Beweis Zu zeigen: $r_{i+1} + (h_i) = r_i + (h_i)$ für alle $i \in \mathbb{N}$.
Nach dem verallgemeinerten Euklidischen Algorithmus (4.1.4) gibt es ein $g \in \mathfrak{o}[\![X]\!]$ mit $g = q_{i+1} \cdot h_{i+1} + r_{i+1},\ r_{i+1} \in \mathfrak{o}[x]$ und $deg(r_{i+1}) < p^{i+1}$ aber zugleich gilt auch $g = q_i \cdot h_i + r_i$ mit $r_i \in \mathfrak{o}[X]$ mit $deg(r_i) < p^i < p^{i+1}$.
Dann können wir aber r_{i+1} wiederum als Element von $\mathfrak{o}[\![X]\!]$ auffassen und somit mithilfe des verallgemeinerten Euklidischen Algorithmus (4.1.4) ausdrücken durch:
$r_{i+1} = f_i \cdot h_i + k_i$ mit $k_i \in \mathfrak{o}[X]$ und $deg(k_i) < p^i$.
Dann ergibt sich:
$g = q_{i+1} \cdot h_{i+1} + f_i \cdot h_i + k_i = q_{i+1} \cdot q' \cdot h_i + f_i \cdot h_i + k_i = (q_{i+1} \cdot q' + f_i)h_i + k_i$.
Aufgrund der Eindeutigkeit des Restes folgt $k_i = r_i$. Somit gilt:
$g = r_i + (h_i) = k_i + (h_i) = k_i + f_i + h_i + (h_i) = r_{i+1} + (h_i) \Rightarrow r_{i+1} + (h_i) = r_i + (h_i)$
$\Rightarrow \epsilon$ ist wohldefiniert. □

Satz 4.1.11 *ϵ ist ein Isomorphismus.*

Beweis Zeige zunächst, dass ϵ ein Ringhomomorphismus ist. Seien $g, g' \in \mathfrak{o}[\![X]\!]$. Dann gilt nach dem erweiterten Euklidischen Algorithmus (4.1.4):
$g = f_n h_n + r_n \forall\ n \in \mathbb{N}\ g' = f'_n h_n + r'_n\ \forall\ n \in \mathbb{N}$.

$\Rightarrow g + g' = (f_n h_n + r_n) + (f'_n h_n + r'_n) = f_n h_n + f'_n h_n + r_n + r'_n = (f_n + f'_n)h_n + r_n + r'_n \forall n \in \mathbb{N}.$

$\Rightarrow$ Der Rest von $g + g'$ entspricht dem Rest von g addiert zu dem Rest von $g' \forall n \in \mathbb{N}$.

$\Rightarrow \epsilon(g + g') = \epsilon(g) + \epsilon(g')$.

$g \cdot g' = (f_n h_n + r_n) \cdot (f'_n h_n + r'_n) = f_n h_n f'_n h_n + f_n h_n r'_n + r_n f_n h_n + r_n r'_n$

$= (f_n f'_n h_n + f_n r'_n + r_n f'_n)h_n + r_n r'_n$

$\Rightarrow$ Der Rest von $g \cdot g'$ entspricht dem Rest von g multipliziert mit dem Rest von $g' \ \forall \ n \in \mathbb{N} \Rightarrow \epsilon(g \cdot g') = \epsilon(g) \cdot \epsilon(g')$

$\Rightarrow \epsilon$ ist ein Homomorphismus. Zeige nun die Bijektivität. Um zu beweisen, dass ϵ injektiv ist, zeigen wir zunächst per Induktion: $h_n = (X + 1)^{p^n} - 1 \in (p, X)^{n+1}$.

Induktionsanfang:

$$n = 1 \quad h_1 = (X + 1)^p - 1 = \underbrace{X^p}_{= X \cdot X^{p-1} \in (X,p)^2} + \underbrace{\sum_{j=1}^{p-1} \underbrace{\binom{p}{j}}_{\in p\mathfrak{o}[X]} \underbrace{X^j}_{\in X\mathfrak{o}[X]}}_{\in (p,X)^2}$$

$\Rightarrow (X + 1)^p - 1 \in (p, X)^2$

Induktionsvoraussetzung: Es gelte $(X + 1)^{p^n} - 1 \in (p, X)^{n+1}$ für $n \in \mathbb{N}$ fest aber beliebig.

Induktionsschritt:

$h_{n+1} = (1 + X)^{p^{n+1}} - 1$

$= ((1 + X)^{p^n})^p - 1$

$= ((1 + X)^{p^n} - 1 + 1)^p - 1$

$= (h_n + 1)^p - 1$

$= \sum_{j=0}^{p} \binom{p}{j} h_n^j - 1$

$$= \underbrace{h_n^p}_{\in (p,X)^{n+2}} + \underbrace{\sum_{j=1}^{p-1} \underbrace{\binom{p}{j}}_{\in (p,X)} \underbrace{h_n^j}_{\in (p,X)^{n+1}}}_{\in (p,X)^{n+2}}$$

Somit ist $h_n = (X + 1)^{p^n} - 1 \in (p, X)^{n+1}$ für alle $n \in \mathbb{N}$. Wir wollen zeigen, dass im Kern von ϵ nur die Null liegt. Ein Element liegt im Kern genau dann, wenn es für alle n aus $\mathbb{N}$ im von h_n erzeugten Hauptideal liegt. Wir gezeigt, dass $h_n \in (p, X)^{n+1}$ ist, es genügt als zu zeigen, dass $\bigcap_{n \in \mathbb{N}} (p, X)^{n+1} = \{0\}$ ist. Dafür betrachten wir die Menge

$\mathfrak{J} := \{ \sum_{m=0}^{\infty} a_m X^m \mid \forall m \leq n : a_m \in p^{n-m}\mathfrak{o}\} \subseteq \mathfrak{o}[\![X]\!]$ mit beliebigem, aber festem $n \in \mathbb{N}$.
Zunächst zeigen wir, dass $\mathfrak{J}$ ein Ideal ist.

1. Zeige: $\mathfrak{J} \neq \varnothing$. Es gilt $0 = \sum_{m=0}^{\infty} 0 \cdot X^m$ und $0 \in p^{n-m}\mathfrak{o} \ \forall \ m \leq n \Rightarrow 0 \in \mathfrak{J} \Rightarrow \mathfrak{J} \neq \varnothing$

2. Zeige: Für $f, g \in \mathfrak{J}$ gilt $f + g \in \mathfrak{J}$. Sei $f = \sum_{m=0}^{\infty} a_m X^m, g = \sum_{m=0}^{\infty} b_m X^m$.
Dann ist $f + g = \sum_{m=0}^{\infty} a_m X^m + \sum_{m=0}^{\infty} b_m X^m = \sum_{m=0}^{\infty} (a_m + b_m) X^m$, wobei $(a_m + b_m) \in p^{n-m}\mathfrak{o}$ für $m \leq n$, da a_m und $b_m \in p^{n-m}\mathfrak{o}$ für $m \leq n$.

3. Zeige: Für $\lambda \in \mathfrak{o}[\![X]\!]$ und $f \in \mathfrak{J}$ ist $\lambda \cdot f \in \mathfrak{J}$. Wenn $\lambda \in \mathfrak{o}[\![X]\!]$, dann ist $\lambda = \sum_{m=0}^{\infty} c_m X^m$ für geeignete $c_n \in \mathfrak{o}$. Sei $f = \sum_{m=0}^{\infty} a_m X^m$. Dann ist $\lambda \cdot f = \sum_{m=0}^{\infty} \sum_{m=0}^{k} (a_m b_{k-m}) X^k$, wobei $a_i \in p^{n-m}\mathfrak{o}$ für $m \leq n$. Daher ist auch $(a_i b_{k-i}) \in p^{n-m}\mathfrak{o}$ für $m \leq n$ und daher auch die Summe in $p^{n-m}\mathfrak{o}$. Also ist $\lambda \cdot f \in \mathfrak{J}$.

Somit haben wir nun gesehen, dass $\mathfrak{J}$ ein Ideal ist. Als Nächstes zeigen wir, dass eine Gleichheit zwischen den Idealen $\mathfrak{J}$ und $\sum_{m=0}^{n} p^{n-m} X^m \mathfrak{o}[\![X]\!]$ in $\mathfrak{o}[\![X]\!]$ gilt. Zeige dafür $\mathfrak{J} \subseteq \sum_{m=0}^{n} p^{n-m} X^m \mathfrak{o}[\![X]\!]$ und $\mathfrak{J} \supseteq \sum_{m=0}^{n} p^{n-m} X^m \mathfrak{o}[\![X]\!]$.

" $\subseteq$ " Sei $\sum_{m=0}^{\infty} a_m X^m \in \mathfrak{J}$. Da $a_m \in p^{n-m}\mathfrak{o}$ können wir a_m schreiben als $a_m = p^{n-m} a'_m$ mit $a'_m \in \mathfrak{o}$. Für $0 \leq m \leq n-1$ gilt dann:

$$\sum_{m=0}^{\infty} a_m X^m = \underbrace{\sum_{m=0}^{n} p^{n-m} X^m \cdot a'_m}_{\in \sum_{m=0}^{n} p^{n-m} X^m \mathfrak{o}[\![X]\!]} + \underbrace{X^n \cdot \sum_{m=n}^{\infty} a_m X^{m-n}}_{\in \sum_{m=0}^{n} p^{n-m} X^m \mathfrak{o}[\![X]\!]}$$

" $\supseteq$ " Es gilt $p^{n-m} \in \mathfrak{J}$. Da $\mathfrak{J}$ ein Ideal ist, ist $p^{n-m} X^m \in \mathfrak{J} \Rightarrow \sum_{m=0}^{n} p^{n-m} X^m \mathfrak{o}[\![X]\!] \subseteq \mathfrak{J}$.

Nun zeigen wir die Gleichheit zwischen den Idealen $\sum_{m=0}^{n} p^{n-m} X^m \mathfrak{o}[\![X]\!]$ und $(p, X)^n$ in $\mathfrak{o}[\![X]\!]$, indem wir wieder Mengeninklusionen in beide Richtungen zeigen.

" $\subseteq$ " $\sum_{m=0}^{n} p^{n-m} X^m \in (p, X)^n \Rightarrow \sum_{m=0}^{n} p^{n-m} X^m \mathfrak{o}[\![X]\!] \subseteq (p, X)^n$
" $\supseteq$ " Diese Richtung zeigen wir mit Induktion über n. Der Induktionsanfang ist für n = 0 klar. Es sei für $n \in \mathbb{N}$ fest aber beliebig $(p, X)^n \subseteq \sum_{m=0}^{n} p^{n-m} X^m \mathfrak{o}[\![X]\!]$. Nun machen wir den Induktionsschritt von n nach $n+1$. Es gilt:

$$
\begin{aligned}
&(p,X)^{n+1} = p(p,X)^n + X(p,X)^n \\
&= p(\sum_{m=0}^{n} p^{n-m}X^m\mathfrak{o}[\![X]\!]) + X(\sum_{m=0}^{n} p^{n-m}X^m\mathfrak{o}[\![X]\!]) \\
&= \sum_{m=0}^{n} p^{n+1-m}X^m\mathfrak{o}[\![X]\!] + \sum_{m=0}^{n} p^{n-m}X^{m+1}\mathfrak{o}[\![X]\!] \\
&= \sum_{m=0}^{n} p^{n+1-m}X^m\mathfrak{o}[\![X]\!] + \sum_{m=0}^{n} p^{n+1-1-m}X^{m+1}\mathfrak{o}[\![X]\!] \\
&= \sum_{m=0}^{n} p^{n+1-m}X^m\mathfrak{o}[\![X]\!] + \sum_{m=0}^{n} p^{n+1-(m+1)}X^{m+1}\mathfrak{o}[\![X]\!] = \sum_{m=0}^{n+1} p^{n+1-m}X^m\mathfrak{o}[\![X]\!] \\
&\Rightarrow (p,X)^{n+1} \subseteq \sum_{m=0}^{n} p^{n-m}X^m\mathfrak{o}[\![X]\!]
\end{aligned}
$$

Also haben wir nun gezeigt: $(p,X)^n = \sum_{m=0}^{n} p^{n-m}X^m\mathfrak{o}[\![X]\!] = \mathfrak{J}$

$\Rightarrow \bigcap_{n\geq 1} (p,X)^n = \bigcap_{n\geq 1} \mathfrak{J} = \{ \sum_{m=0}^{\infty} a_m X^m \mid \forall n \in \mathbb{N} : a_m \in p^{n-m}\mathfrak{o}\} = \{0\}$.
Somit folgt $\bigcap_{n\geq 1} h_n = \{0\} \Rightarrow ker(\epsilon) = 0 \Rightarrow \epsilon$ ist injektiv.

Nun fehlt nur noch die Surjektivität, deren Beweis wir im Folgenden skizzieren wollen.

Zu zeigen: Für jede Folge von Resten $(r_n + h_n\mathfrak{o}[X])_{n\geq 0}$ gibt es eine Potenzreihe $g \in \mathfrak{o}[\![X]\!]$, sodass $\epsilon(g) = (r_n + h_n\mathfrak{o}[X])_{n\geq 0}$.

Sei $(r_n + h_n\mathfrak{o}[X])_{n\geq 0}$ eine explizite Folge von Resten. Aufgrund der Verträglichkeit gilt: $r_{n+1} - r_n \in h_n\mathfrak{o}[X] \subseteq h_n\mathfrak{o}[\![X]\!]$. Schreiben wir $r_n = \sum_{m=0}^{\infty} a_m^{(n)} X^m \in \mathfrak{o}[\![X]\!]$, so ist für jedes $m \in \mathbb{N}$ die Koeffizientenfolge$(a_m^{(n)})_{n\in\mathbb{N}}$ eine p-adische Cauchyfolge in $\mathfrak{o}$, weil $h_n\mathfrak{o}[\![X]\!] \subseteq (p,X)^{n+1}$. Daher konvergiert jede Koeffizientenfolge $(a_m^{(n)})_{n\in\mathbb{N}}$ gegen ein $a_m \in \mathfrak{o}$. Damit liegt die zugehörige Potenzreihe $g := \sum_{m=0}^{\infty} a_m X^m$ in $\mathfrak{o}[\![X]\!]$. Sie erfüllt $\epsilon(g) = (r_n + h_n\mathfrak{o}[\![X]\!])_{n\geq 0}$. Somit ist ϵ bijektiv. Wir haben gezeigt: ϵ ist ein Isomorphismus. □

Nun wissen wir, dass es insgesamt einen Isomorphismus $\psi : \mathfrak{o}[\![X]\!] \to \mathfrak{o}[\![\mathbb{Z}_p]\!]$ gibt mit $\psi := \varphi^{-1} \circ \epsilon$, wobei φ^{-1} aus den Komponentenfunktionen φ_n^{-1} besteht.

4.2 Der Isomorphismus zwischen $\mathfrak{o}[\![\mathbb{Z}_p]\!]$ und $\mu(\mathbb{Z}_p, \mathfrak{o})$

Um zu zeigen, dass der komplettierte Gruppenring der proendlichen Gruppe $\mathbb{Z}_p$ isomorph ist zu der Maßalgebra $\mu(\mathbb{Z}_p, \mathfrak{o})$, konstruieren wir Linearformen L_λ auf der Menge der

lokal konstanten K-wertigen Funktionen auf $\mathbb{Z}_p$. Hierbei wird $\mu(\mathbb{Z}_p, \mathfrak{o})$ weiterhin als $\mathfrak{o}$-Unteralgebra von $\mu(\mathbb{Z}_p, K)$ verstanden.

Definition 4.2.1 *Sei $\lambda \in (\lambda_n)_{n\in\mathbb{N}} \in \mathfrak{o}[\![\mathbb{Z}_p]\!]$. Definiere eine Abbildung $L_\lambda : C^\infty(\mathbb{Z}_p, K) \to K$ wie folgt. Für $f \in C^\infty(\mathbb{Z}_p, K)$ finde $m \in \mathbb{N}$, sodass f konstant modulo $p^m\mathbb{Z}_p$ ist und setze: $L_\lambda(f) := \sum_{x\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_m(x)f(x)$, wobei $\lambda_m = \sum_{x\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_m(x)x$.*

Bevor wir zeigen, dass L_λ wohldefiniert ist, zeigen wir, dass es für jede lokal konstante Funktion $f \in C^\infty(\mathbb{Z}_p, K)$ ein $m \in \mathbb{N}$ gibt, sodass f konstant modulo $p^m\mathbb{Z}_p$ ist.

Lemma 4.2.2 *Für $f \in C^\infty(\mathbb{Z}_p, K)$ existiert $m \in \mathbb{N}$, sodass f konstant modulo $p^m\mathbb{Z}_p$ ist.*

Beweis Sei $f \in C^\infty(\mathbb{Z}_p, K)$. f ist lokal konstant, daher gibt es für alle $x \in \mathbb{Z}_p$ ein $m(x) \in \mathbb{N}$, sodass $f|_{x+p^{m(x)}\mathbb{Z}_p}$ konstant ist, wobei $x+p^{m(x)}\mathbb{Z}_p$ eine kleine, offene Umgebung von x in $\mathbb{Z}_p$ ist. Da $\mathbb{Z}_p$ nach 3.2.21 kompakt ist, besitzt jede offene Überdeckung von $\mathbb{Z}_p$ eine endliche Teilüberdeckung. Die offenen Umgebungen $x + p^{m(x)}\mathbb{Z}_p$ bilden eine offene Überdeckung von $\mathbb{Z}_p$, daher gilt $\bigcup_{x\in\mathbb{Z}_p} (x + p^{m(x)}\mathbb{Z}_p) = \bigcup_{i=1}^{s} (x_i + p^{m_i(x)}\mathbb{Z}_p)$. Setze nun $m := min\{m(x_i)\}$. Dann ist f auf jeder Teilmenge der Form $x + p^m\mathbb{Z}_p$ konstant $\Rightarrow$ Es gibt ein m, sodass f konstant modulo $p^m\mathbb{Z}_p$ ist. □

Zeige nun:

Satz 4.2.3 *L_λ ist wohldefiniert.*

Beweis Angenommen f ist modulo $p^m\mathbb{Z}_p$ und $p^n\mathbb{Z}_p$ konstant mit $m, n \in \mathbb{N}, m \neq n$. Sei o.B.d.A. $n > m$. Dann gilt:

für m: $\lambda_m = \sum_{x\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_m(x)x \in \mathfrak{o}[\mathbb{Z}_p/p^m\mathbb{Z}_p] \quad L_\lambda(f) = \sum_{x\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_m(x)f(x)$

für n: $\lambda_n = \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)y \in \mathfrak{o}[\mathbb{Z}_p/p^n\mathbb{Z}_p] \quad L_\lambda(f) = \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)f(y)$

Damit L_λ wohldefiniert ist, muss gelten: $\sum_{x\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_m(x)f(x) = \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)f(y)$

λ_n und λ_m sind beide Folgenglieder der Folge $\lambda = (\lambda_i)_{i\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}} \mathfrak{o}[\mathbb{Z}_p/p^n\mathbb{Z}_p]$. Daher sind λ_n und λ_m verträglich. Unter der Übergangsabbildung $\varphi : \mathfrak{o}[\mathbb{Z}_p/p^n\mathbb{Z}_p] \to \mathfrak{o}[\mathbb{Z}_p/p^m\mathbb{Z}_p]$ des

projektiven Limes $\mathfrak{o}[\![\mathbb{Z}_p]\!]$ wird daher λ_n auf λ_m abgebildet.

Betrachte dafür $\lambda_n = \sum_{\substack{y \in \mathbb{Z}_p / p^n\mathbb{Z}_p = \\ \rho(y)+p^n\mathbb{Z}_p}} c_n(y)y$, wobei $\rho(y)$ der Repräsentant in Abhängigkeit von y ist. Bilde nun λ_n auf λ_m ab, wobei der Repräsentant fest bleibt, jetzt aber als Element von $p^m\mathbb{Z}_p$ betrachtet wird:

$$\sum_{\rho(y)+p^n\mathbb{Z}_p} c_n(y)y \mapsto \sum_{y \in \mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y) \cdot (\rho(y) + p^m\mathbb{Z}_p) = \lambda_m = \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_m(x)x$$

Da $n > m$ können in $\mathbb{Z}_p/p^m\mathbb{Z}_p$ Elemente aus $\mathbb{Z}_p/p^n\mathbb{Z}_p$ zusammenfallen. Berücksichtigt man dies, so ergibt sich eine weitere Darstellung von λ_m in Standardschreibweise:

$$\sum_{y \in \mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y) \cdot (\rho(y) + p^m\mathbb{Z}_p) = \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} \Big(\sum_{\substack{y \in \mathbb{Z}_p/p^n\mathbb{Z}_p \\ \rho(y)+p^m\mathbb{Z}_p = x}} c_n(y) \Big) x$$

Dann gilt nach Koeffizientenvergleich für alle x aus $\mathbb{Z}_p/p^m\mathbb{Z}_p$:

$$c_m(x) = \sum_{\substack{y \in \mathbb{Z}_p/p^n\mathbb{Z}_p \\ \rho(y)+p^m\mathbb{Z}_p = x}} c_n(y)$$

Da f konstant modulo $p^n\mathbb{Z}_p$ und $p^m\mathbb{Z}_p$ ist, gilt:

Für $y_1 = \rho(y_1) + p^n\mathbb{Z}_p, y_2 = \rho(y_2) + p^n\mathbb{Z}_p$ mit $\rho(y_1) + p^m\mathbb{Z}_p = x = \rho(y_2) + p^m\mathbb{Z}_p$ gilt: $f(y_1) = f(x) = f(y_2)$.

Dann folgt insgesamt:

$$\sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_m(x)f(x) = \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} \Big(\sum_{\substack{y \in \mathbb{Z}_p/p^n\mathbb{Z}_p \\ \rho(y)+p^m\mathbb{Z}_p = x}} c_n(y) \Big) f(x) = \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} \Big(\sum_{\substack{y \in \mathbb{Z}_p/p^n\mathbb{Z}_p \\ \rho(y)+p^m\mathbb{Z}_p = x}} c_n(y) \Big) f(y)$$

$$= \sum_{x \in \mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)f(y)$$

$$\Rightarrow \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_m(x)f(x) = \sum_{x \in \mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)f(y), \text{ also ist } L_\lambda \text{ wohldefiniert.} \qquad \square$$

Da wir schlussendlich L_λ als Element von $\mu(\mathbb{Z}_p, \mathfrak{o})$ betrachten wollen, müssen wir zeigen, dass sich L_λ zu einem eindeutigen Element in $\mu(\mathbb{Z}_p, \mathfrak{o})$ fortsetzt. Bevor wir diese Fortsetzung zeigen können, zeigen wir zunächst, dass L_λ folgende Eigenschaften besitzt:

Lemma 4.2.4 *Sei L_λ wie in 4.2.1 definiert, $\lambda \in \mathfrak{o}[\![\mathbb{Z}_p]\!]$. Dann gilt:*

i) L_λ ist K-linear

ii) L_λ ist stetig

iii) $\|L_\lambda\| \leq 1$

Beweis i) Seien f und $g \in C^\infty(\mathbb{Z}_p, K)$: Sei f konstant modulo $\mathbb{Z}_p/p^m\mathbb{Z}_p$ und g konstant

modulo $p^n\mathbb{Z}_p$. Sei o.B.d.A. $n > m$. Aufgrund der Verträglichkeit erhält man analog wie im vorherigen Beweis

$$c_m(x) = \sum_{\substack{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p \\ \rho(y)+p^m\mathbb{Z}_p=x}} c_n(y)$$

Da f konstant modulo $\mathbb{Z}_p/p^m\mathbb{Z}_p$ ist und $n > m$ ist, ist f auch konstant modulo $\mathbb{Z}_p/p^n\mathbb{Z}_p$ und dann folgt analog zum obigen Beweis:

$$L_\lambda(f) = \sum_{x\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_m(x)f(x) = \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)f(y).$$

Betrachte nun :

$$\begin{aligned}
&L_\lambda(f+g) = \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)(f+g)(y) \\
&= \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)(f(y)+g(y)) \\
&= \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)f(y) + c_n(y)g(y) \\
&= \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)f(y) + \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)g(y) \\
&= L_\lambda(f) + L_\lambda(g)
\end{aligned}$$

Für alle $a \in K$ gilt:

$$L_\lambda(af) = \sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)af(y) = a(\sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)(f(y)) = a\cdot L_\lambda(f)$$

Somit ist L_λ K-linear.

ii) und iii) können wir gemeinsam zeigen. Betrachte die folgende Abschätzung:

$$|L_\lambda(f)| = |\sum_{y\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(y)f(y)| \leq max(\underbrace{|c_n(y)|}_{\in\mathfrak{o}\Rightarrow|c_n(y)|\leq 1} |f(y)|) \leq \|f\|_\infty.$$

Da $C^\infty(\mathbb{Z}_p, K)$ und K normierte Räume sind und L_λ K-Linear ist, gilt:

L_λ ist stetig $\Leftrightarrow sup\frac{|L_\lambda(f)|}{\|f\|_\infty} \leq c$, wobei c eine endliche Konstante ist.

Es ergibt sich aufgrund der obigen Abschätzung:

$sup\frac{|L_\lambda(f)|}{\|f\|_\infty} \leq sup\frac{\|f\|_\infty}{\|f\|_\infty} = 1 \Rightarrow L_\lambda$ ist stetig und $\|L_\lambda\| \leq 1$. □

Nun wollen wir $L_\lambda : C^\infty(\mathbb{Z}_p, K) \to K$ zu $\hat{L}_\lambda : C(\mathbb{Z}_p, K) \to K$ fortsetzen. Da $C^\infty(\mathbb{Z}_p, K)$ nach 3.3.10 dicht in $C(\mathbb{Z}_p, K)$ liegt, gibt es für beliebiges $f \in C(\mathbb{Z}_p, K)$ eine Funktionenfolge $(f_n)_{n\in\mathbb{N}} \in C^\infty(\mathbb{Z}_p, K)$, die gegen f konvergiert. Setze $\hat{L}_\lambda(f) := \lim_{n\to\infty} L_\lambda(f_n)$.

Lemma 4.2.5 *Die Fortsetzung von L_λ zu $\hat{L}_\lambda$ ist eindeutig.*

Beweis Angenommen es gilt $f = \lim_{n\to\infty} f_n$ und $f = \lim_{n\to\infty} g_n$. Da $(f_n)_{n\in\mathbb{N}}$ und $(g_n)_{n\in\mathbb{N}}$ in $C^\infty(\mathbb{Z}_p, K)$ liegen, ist auch $(f_n - g_n)_{n\in\mathbb{N}}$ in $C^\infty(\mathbb{Z}_p, K)$. Da die Folgen denselben Grenzwert haben, gilt $\lim_{n\to\infty}(f_n - g_n) = 0$ in $C^\infty(\mathbb{Z}_p, K)$. Dann gilt aber auch $\lim_{n\to\infty} L_\lambda(f_n - g_n) = 0 \in K$. Da L_λ nach 4.2.4 K-linear ist ergibt sich:

$\lim_{n\to\infty}(L_\lambda(f_n - g_n)) = 0 \in K$
$\Leftrightarrow \lim_{n\to\infty}(L_\lambda(f_n) - L_\lambda(g_n)) = 0$
$\Leftrightarrow \lim_{n\to\infty} L_\lambda(f_n) - \lim_{n\to\infty} L_\lambda(g_n) = 0$
$\Leftrightarrow \lim_{n\to\infty} L_\lambda(f_n) = \lim_{n\to\infty} L_\lambda(g_n)$
$\Rightarrow \hat{L}_\lambda$ ist eindeutig. □

Nun wollen wir zeigen, dass $\hat{L}_\lambda$ ein Element der Maßalgebra ist.

Satz 4.2.6 *Sei $\hat{L}_\lambda$ so wie oben definiert. Dann gilt: $\hat{L}_\lambda \in \mu(\mathbb{Z}_p, \mathfrak{o})$.*

Beweis Sei $f \in C(\mathbb{Z}_p, K), (f_n)_{n\in\mathbb{N}} \in C^\infty(\mathbb{Z}_p, K)$ eine Funktionenfolge mit $\lim_{n\to\infty}(f_n) = f$. Zu zeigen: $\hat{L}_\lambda$ ist K-linear, stetig und $\|\hat{L}_\lambda\| \leq 1$.

K-Linearität: Sei auch $g \in C(\mathbb{Z}_p, K), (g_n)_{n\in\mathbb{N}} \in C^\infty(\mathbb{Z}_p, K)$, sodass $\lim_{n\to\infty}(g_n) = g$. Dann gilt:

$\hat{L}_\lambda(f+g) = \lim_{n\to\infty} L_\lambda(f_n + g_n) = \lim_{n\to\infty}(L_\lambda(f_n) + L_\lambda(g_n)) = \lim_{n\to\infty} L_\lambda(f_n) + \lim_{n\to\infty} L_\lambda(g_n)$
$= \hat{L}_\lambda(f) + \hat{L}_\lambda(g)$

Sei $a \in K$

$\hat{L}_\lambda(af) = \lim_{n\to\infty} L_\lambda(af_n) = \lim_{n\to\infty} aL_\lambda(f_n) = a\lim_{n\to\infty} L_\lambda(f_n) = a\hat{L}_\lambda(f)$

Somit ist $\hat{L}_\lambda$ K-linear. Stetigkeit und $\|\hat{L}_\lambda\| \leq 1$ können abermals gemeinsam gezeigt werden. Betrachte:

$sup\frac{|\hat{L}_\lambda(f)|}{\|f\|_\infty} = sup\frac{|\lim_{n\to\infty} L_\lambda(f_n)|}{\|\lim_{n\in\infty}(f_n)\|_\infty} = sup\lim_{n\to\infty}\frac{|L_\lambda(f_n)|}{\|f_n\|_\infty} \leq 1$

Dies gilt, da die Normen stetig sind. Somit haben wir gezeigt: $\hat{L}_\lambda \in \mu(\mathbb{Z}_p, \mathfrak{o})$. □

Nun können wir eine Abbildung ϕ von $\mathfrak{o}[\![\mathbb{Z}_p]\!]$ nach $\mu(\mathbb{Z}_p, \mathfrak{o})$ definieren durch:

$\phi : \mathfrak{o}[\![\mathbb{Z}_p]\!] \to \mu(\mathbb{Z}_p, \mathfrak{o}) \quad \lambda \mapsto \hat{L}_\lambda$

Satz 4.2.7 *ϕ ist ein Isomorphismus von $\mathfrak{o}$-Algebren.*

Beweis Zeige zunächst: ϕ ist ein Ringhomomorphismus.

Seien $\lambda_1, \lambda_2 \in \mathfrak{o}[\![\mathbb{Z}_p]\!]$. Wir müssen zeigen: $\hat{L}_{\lambda_1+\lambda_2} = \hat{L}_{\lambda_1} + \hat{L}_{\lambda_2}$.

Sei $f \in C(\mathbb{Z}_p, K)$ beliebig. Da $\lambda_1 + \lambda_2 \in \mathfrak{o}[\![\mathbb{Z}_p]\!]$ ist, gilt für die m-te Komponente

$\lambda_{m_1} = \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_1}(x)x$ von λ_1 beziehungsweise $\lambda_{m_2} = \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_2}(x)x$ von λ_2:

$\lambda_{m_1} + \lambda_{m_2} = \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_1}(x)x + \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_2}(x)x \ \forall\ m \in \mathbb{N}$.

Schreiben wir $f \in C(\mathbb{Z}_p, K)$ als $f = \lim_{i\to\infty} f_i$, und ist f_i konstant modulo $p^m\mathbb{Z}_p$, so gilt:

$L_{\lambda_1+\lambda_2}(f_i) = \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} (c_{m_1}(x) + c_{m_2}(x))f_i(x)$

$= \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_1}(x)f_i(x) + \sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_2}(x)f_i(x)$

$= L_{\lambda_1}(f_i) + L_{\lambda_2}(f_i)$.

Dann gilt für die Fortsetzung:

$\hat{L}_{\lambda_1+\lambda_2}(f) = \lim_{i\to\infty}(L_{\lambda_1+\lambda_2}(f_i)) = \lim_{i\to\infty}(L_{\lambda_1}(f_i) + L_{\lambda_2}(f_i)) = \lim_{i\to\infty}(L_{\lambda_1}(f_i)) + \lim_{i\to\infty}(L_{\lambda_2}(f_i))$

$= \hat{L}_{\lambda_1}(f) + \hat{L}_{\lambda_2}(f)$

Somit folgt für die Abbildung ϕ: $\phi(\lambda_1 + \lambda_2) = \hat{L}_{\lambda_1} + \hat{L}_{\lambda_2} = \phi(\lambda_1) + \phi(\lambda_2)$.

Zu zeigen: $(\hat{L}_{\lambda_1} * \hat{L}_{\lambda_2})(f) = \hat{L}_{\lambda_1\lambda_2}(f)$ mit $f \in C(\mathbb{Z}_p, K)$ beliebig. Dies ist äquivalent zu $\lim_{n\to\infty}(L_{\lambda_1} * L_{\lambda_2})(f_n) = \lim_{n\to\infty}(L_{\lambda_1\lambda_2})(f_n)$ Wir beweisen, dass für jedes Folgenglied $f_n \in (f_n)_{n\in\mathbb{N}}$ gilt: $L_{\lambda_1\lambda_2}(f_n) = (L_{\lambda_1} * L_{\lambda_2})(f_n)$.

Sei f_n konstant modulo $p^m\mathbb{Z}_p$. Dann gilt für die jeweils m-te Komponente von λ_1 beziehungsweise λ_2:

$\lambda_{m_1} \cdot \lambda_{m_2} = (\sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_1}(x)f(x))(\sum_{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_2}(y)f(y)) = \sum_{\substack{x \in \mathbb{Z}_p/p^m\mathbb{Z}_p \\ y \in \mathbb{Z}_p/p^m\mathbb{Z}_p}} c_{m_1}(x)c_{m_2}(y)(x+y)$

Sei $f_n \in C(\mathbb{Z}_p, K)$ konstant modulo $p^m\mathbb{Z}_p$. Dann ist auch $(x \mapsto \tau_x(f_n))$ konstant modulo $p^m\mathbb{Z}_p$ und daher auch $(x \mapsto L_{\lambda_1}(\tau_x(f_n)))$ konstant modulo $p^m\mathbb{Z}_p$. Somit gilt für $L_{\lambda_1\lambda_2}(f_n)$:

$L_{\lambda_1\lambda_2}(f_n) = L_{\lambda_2}(x \mapsto L_{\lambda_1}(\tau_x(f_n)))$

$= \sum_{z \in \mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_2}(z) \cdot L_{\lambda_1}(\tau_z(f_n))$

$$= \sum_{z\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_2}(z)\cdot\Big(\sum_{y\in\mathbb{Z}/p^m\mathbb{Z}} c_{m_1}(y)\tau_z(f_n)(y)\Big)$$
$$= \sum_{z\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_2}(z)\cdot\Big(\sum_{y\in\mathbb{Z}/p^m\mathbb{Z}} c_{m_1}(y) f_n(z+y)\Big)$$
$$= \sum_{z\in\mathbb{Z}_p/p^m\mathbb{Z}_p}\ \sum_{y\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_2}(z)c_{m_1}(y) f_n(z+y)$$
$$= \sum_{z,y\in\mathbb{Z}_p/p^m\mathbb{Z}_p} c_{m_2}(z)c_{m_1}(y) f_n(z+y)$$
$$= L_{\lambda_1\lambda_2}(f_n) = (L_{\lambda_1} * L_{\lambda_2})(f_n).$$

Also ist $\lim_{n\to\infty} L_{\lambda_1\lambda_2}(f_n) = \lim_{n\to\infty} (L_{\lambda_1} * L_{\lambda_2})(f_n) \Rightarrow \hat{L}_{\lambda_1\lambda_2}(f) = (\hat{L}_{\lambda_1} * \hat{L}_{\lambda_2})(f)$.

Zu zeigen ist nun noch, dass $\phi(1_{\mathfrak{o}[\![\mathbb{Z}_p]\!]}) = 1_{\mu(\mathbb{Z}_p,\mathfrak{o})}$. Es gilt $\phi(1_{\mathfrak{o}[\![\mathbb{Z}_p]\!]}) = (\lambda_n)_{n\in\mathbb{N}} \in \mathfrak{o}[\![\mathbb{Z}_p]\!]$ mit $\lambda_n = \sum_{x\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(x)x$ und $c_n(x) = \begin{cases} 1 & \text{falls } x = 0 + p^n\mathbb{Z}_p \\ 0 & \text{sonst} \end{cases}$

Nach 3.3.12 ist $1_{\mu(\mathbb{Z}_p,\mathfrak{o})} = \delta_0$, wobei $\delta_0 := (f \mapsto f(0)) \in C(\mathbb{Z}_p, K)'$. Wir zeigen Abbildungsgleichheit zwischen $\phi(1_{\mathfrak{o}[\![\mathbb{Z}_p]\!]})$ und δ_0. Sei $f \in C^\infty(\mathbb{Z}_p, K)$ konstant modulo $p^n\mathbb{Z}_p$, dann gilt nach Konstruktion $\phi(1_{\mathfrak{o}[\![\mathbb{Z}_p]\!]})(f) = \sum_{x\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_n(x)f(x) = f(0) = \delta_0(f)$.

Da n beliebig war, stimmen damit $\phi(1_{\mathfrak{o}[\![\mathbb{Z}_p]\!]})$ und δ_0 auf $C^\infty(\mathbb{Z}_p, K)$ überein, aus Stetigkeitsgründen dann aber sogar auf $C(\mathbb{Z}_p, K)$. Daher gilt $\phi(1_{\mathfrak{o}[\![\mathbb{Z}_p]\!]}) = \delta_0$.

$\Rightarrow \phi$ ist ein Ringhomomorphismus.

Nun beweisen wir Injektivität. Zu zeigen: $\hat{L}_{\lambda_1} = \hat{L}_{\lambda_2} \Rightarrow \lambda_1 = \lambda_2$.

Wenn zwischen $\hat{L}_{\lambda_1}$ und $\hat{L}_{\lambda_2}$ Abbildungsgleichheit gilt, gilt $\hat{L}_{\lambda_1}(f) = \hat{L}_{\lambda_2}(f)$ für alle $f \in C(\mathbb{Z}_p, K)$, also insbesondere auch für $f \in C^\infty(\mathbb{Z}_p, K) \subseteq C(\mathbb{Z}_p, K)$. Da $\hat{L}_\lambda\,|_{C^\infty(\mathbb{Z}_p,K)} = L_\lambda$ muss somit auch gelten: $L_{\lambda_1}(f) = L_{\lambda_2}(f)$ für alle $f \in C^\infty(\mathbb{Z}_p, K)$. Betrachte nun die Funktion $f := \mathbb{1}_{b+p^n\mathbb{Z}_p}$. f ist konstant modulo $p^n\mathbb{Z}_p$. Daher gilt für die n-te Komponente $\lambda_{n_1} = \sum_{\substack{b+p^n\mathbb{Z}_p \\ \in\mathbb{Z}_p/p^n\mathbb{Z}_p}} c_n(b+p^n\mathbb{Z}_p)(b+p^n\mathbb{Z}_p)$ von λ_1:

$$L_{\lambda_1}(f) = \sum_{x\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_{n_1}(x)f(x) = \sum_{x\in\mathbb{Z}_p/p^n\mathbb{Z}_p} c_{n_1}(x)\mathbb{1}_{b+p^n\mathbb{Z}_p}(x) = c_{n_1}(b+p^n\mathbb{Z}_p)$$

Analog folgt $L_{\lambda_2}(\mathbb{1}_{b+p^n\mathbb{Z}_p}) = c_{n_2}(b+p^n\mathbb{Z}_p)$. Da aber nach Voraussetzung gilt: $L_{\lambda_1}(\mathbb{1}_{b+p^n\mathbb{Z}_p}) = L_{\lambda_2}(\mathbb{1}_{b+p^n\mathbb{Z}_p})$ gilt auch $c_{n_1}(b+p^n\mathbb{Z}_p) = c_{n_2}(b+p^n\mathbb{Z}_p)$ für alle $b+p^n\mathbb{Z}_p \in \mathbb{Z}_p/p^n\mathbb{Z}_p$. Also gilt $\lambda_{n_1} = \lambda_{n_2}$ für alle $n \in \mathbb{N} \Rightarrow \lambda_1 = \lambda_2$. Somit gilt Injektivität.

Abschließend müssen wir noch die Surjektivität zeigen. Sei $\mu \in \mu(\mathbb{Z}_p, K)$. Zu zeigen: Es gibt $\lambda = (\lambda_n)_{n\in\mathbb{N}} \in \mathfrak{o}[\![\mathbb{Z}_p]\!]$ mit $\hat{L}_\lambda = \mu$. Setze

$\lambda_n := \sum_{\overline{b}\in\mathbb{Z}_p/p^n\mathbb{Z}_p} \underbrace{\mu(\mathbb{1}_{\overline{b}})}_{\in\mathfrak{o}} \overline{b} \quad \in \mathfrak{o}[\mathbb{Z}_p/p^n\mathbb{Z}_p]$ für $n \geq 1$.

Um zu beweisen, dass dieses $\lambda = (\lambda_n)_{n\in\mathbb{N}}$ das Gesuchte ist, müssen wir beweisen, dass $(\lambda_n)_{n\in\mathbb{N}} \in \mathfrak{o}[\![\mathbb{Z}_p]\!]$ ist, also die λ_n unter den entsprechenden Abbildungen eine verträgliche Familie bilden. Danach bleibt noch zu zeigen, dass für dieses λ tatsächlich gilt: $L_\lambda = \mu$.

Sei $f_{n,n+1} : \mathfrak{o}[\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p] \to \mathfrak{o}[\mathbb{Z}_p/p^n\mathbb{Z}_p]$ die Übergangsabbildung gegeben durch

$$\sum_{\overline{b}\in\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p} c_{n+1}(\overline{b})\overline{b} \mapsto \sum_{\overline{b}\in\mathbb{Z}_p/p^n\mathbb{Z}_p} \Big(\sum_{\substack{\overline{b}'\in\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \\ \overline{b}'\mapsto\overline{b}}} c_{n+1}(\overline{b}')\Big)\overline{b}$$

Es gilt:

$$f_{n,n+1}(\lambda_{n+1}) = f_{n,n+1}\Big(\sum_{\overline{b}\in\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p} \mu(\mathbb{1}_{\overline{b}})\overline{b}\Big) = \sum_{\overline{b}\in\mathbb{Z}_p/p^n\mathbb{Z}_p} \Big(\sum_{\substack{\overline{b}'\in\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \\ \overline{b}'\mapsto\overline{b}}} \mu(\mathbb{1}_{\overline{b}'})\Big)\overline{b}$$

$$= \sum_{\overline{b}\in\mathbb{Z}_p/p^n\mathbb{Z}_p} \mu(\mathbb{1}_{\overline{b}})\overline{b} = \lambda_n$$

Somit haben wir die Verträglichkeit gezeigt. Wir haben schon gesehen: $L_\lambda(\mathbb{1}_b)$ ist der Koeffizient vor $\overline{b} = b + p^n\mathbb{Z}_p$ von λ_n. Somit nehmen L_λ und μ auf allen Funktionen der Form $\mathbb{1}_{b+p^n\mathbb{Z}_p}$, $n \in \mathbb{N}, b \in \mathbb{Z}_p$ denselben Wert an. L_λ und μ sind beide K-linear, daher stimmen sie auch auf allen Linearkombinationen von Funktionen der Form $\mathbb{1}_{b+p^n\mathbb{Z}_p}$ $n \in \mathbb{N}, b \in \mathbb{Z}_p$ überein, also auf ganz $C^\infty(\mathbb{Z}_p, K)$. Aufgrund der Eindeutigkeit der in 4.2.5 gezeigten Fortsetzung gilt dann auch: $\hat{L}_\lambda = \mu$. Wir haben nun insgesamt gezeigt: ϕ ist ein Isomorphismus. □

4.3 Der induzierte Isomorphismus zwischen $\mathfrak{o}[\![X]\!]$ und $\mu(\mathbb{Z}_p, \mathfrak{o})$

Da wir bereits Isomorphismen $\psi : \mathfrak{o}[\![X]\!] \to \mathfrak{o}[\![\mathbb{Z}_p]\!]$ (siehe S. 43) und $\phi : \mathfrak{o}[\![\mathbb{Z}_p]\!] \to \mu(\mathbb{Z}_p, \mathfrak{o})$ (siehe 4.2.7) gefunden haben, wissen wir, dass Abbildungen $\gamma : \mathfrak{o}[\![X]\!] \to \mu(\mathbb{Z}_p, \mathfrak{o})$ mit $\gamma = \phi \circ \psi$ und $\gamma^{-1} : \mu(\mathbb{Z}_p, \mathfrak{o}) \to \mathfrak{o}[\![X]\!]$ mit $\gamma^{-1} = \psi^{-1} \circ \phi^{-1}$ existieren, die Isomorphismen

sind. Somit gibt es zu jedem Maß μ eine assoziierte Potenzreihe $F_\mu = \sum_{i=0}^{\infty} a_i X^i$. Wir wollen den Zusammenhang zwischen dem Maß und der assoziierten formalen Potenzreihe konkretisieren, indem wir die Koeffizienten $a_i, i \in \mathbb{N}$, von F_μ bestimmen.

Sei $\psi : \mathfrak{o}[\![X]\!] \to \mathfrak{o}[\![\mathbb{Z}_p]\!]$ der erste Isomorphismus. Nach Konstruktion ist seine Komposition mit der n-ten Projektion $pr_n : \mathfrak{o}[\![\mathbb{Z}_p]\!] \to \mathfrak{o}[\mathbb{Z}_p/p^n\mathbb{Z}_p]$ gegeben durch $pr_n(\psi(X)) = pr_n(\varphi^{-1}(\epsilon(X))) = \gamma_n - 1$ mit $\gamma_n = 1 + p^n\mathbb{Z}_p \in \mathbb{Z}_p/p^n\mathbb{Z}_p = \Gamma_n$. Der Kern dieser Abbildung ist dann das Hauptideal, das von $(X+1)^{p^n} - 1$ erzeugt wird.

Sei $\phi : \mathfrak{o}[\![\mathbb{Z}_p]\!] \to \mu(\mathbb{Z}_p, \mathfrak{o})$ der zweite Isomorphismus. Betrachte die Umkehrabbildung $\phi^{-1} : \mathfrak{o}[\![\mathbb{Z}_p]\!] \to \mu(\mathbb{Z}_p, \mathfrak{o})$. Dann ist die Verkettung von ϕ^{-1} mit der n-ten Projektion pr_n gegeben durch: $(pr_n \circ \phi^{-1}) : \mu(\mathbb{Z}_p, \mathfrak{o}) \to \mathfrak{o}[\mathbb{Z}_p/p^n\mathbb{Z}_p],\ \mu \mapsto \sum_{r=0}^{p^n-1} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})\gamma_n^r$.

Dies folgt aus der Konstruktion von ϕ. Der Surjektivitätsbeweis von ϕ (4.2.7) zeigt nämlich $\mu = \hat{L}_\lambda = \phi(\lambda)$ mit $\lambda = (\lambda_n)_(n \in \mathbb{N})$ und $\lambda_n = \sum_{x \in \mathbb{Z}_p/p^n\mathbb{Z}_p} \mu(\mathbb{1}_{x+p^n\mathbb{Z}_p})x = (pr_n \circ \phi^{-1})(\mu)$. Zu jedem $x \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ existiert aber nach 3.2.18 ii) genau ein $0 \le r < p^n$ mit $x + p^n\mathbb{Z}_p = r + p^n\mathbb{Z}_p = r(1 + p^n\mathbb{Z}_p) = \gamma_n^r$ (in multiplikativer Schreibweise).

Definition 4.3.1 *Definiere die Abbildung* $\binom{x}{k} : \mathbb{Z}_p \to \mathbb{Q}_p$ *durch* $x \mapsto \frac{x(x-1)\cdot\ldots\cdot(x-k+1)}{k!}$.

Mithilfe dieser Vorüberlegungen können wir nun den folgenden Satz formulieren:

Satz 4.3.2 *Für alle* $\mu \in \mu(\mathbb{Z}_p, \mathfrak{o})$ *gilt:* $(\psi^{-1} \circ \phi^{-1})(\mu) = \sum_{k=0}^{\infty} \mu(\binom{x}{k})x^k$.

Beweis Sei $N \in \mathbb{N}$ und $F := \sum_{k=0}^{\infty} \mu(\binom{x}{k})x^k$. Dies ist eine formale Potenzreihe in $\mathfrak{o}[\![X]\!]$, da $\mu(\binom{x}{k}) \in \mathfrak{o}$. Wir wollen zeigen, dass $(\psi^{-1} \circ \phi^{-1})(\mu) = F$.
Für $n \in \mathbb{N}$ setze $F_n := \sum_{k=0}^{p^n-1} \underbrace{\left(\sum_{r=0}^{p^n-1} \binom{r}{k}\mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})\right)}_{\in \mathfrak{o}} X^k \in \mathfrak{o}[X] \subseteq \mathfrak{o}[\![X]\!]$.
Wir betrachten im Zuge des Beweises das folgende Lemma:

Lemma 4.3.3 *Für* $k \in \mathbb{N}$ *ist die Abbildung* $\binom{x}{k}$ *stetig.*

Beweis Da $k \in \mathbb{N}$ ist, ist der Nenner für alle k ungleich Null und die Abbildung $\binom{x}{k}$ als Produkt stetiger Funktionen stetig.

Die Abbildung $\binom{x}{k}$ ist sogar eine Abbildung von $\mathbb{Z}_p$ nach $\mathbb{Z}_p$. Denn für $m \in \mathbb{Z}$ ist auch der Binomialkoeffizient $\binom{m}{k}$ ganzzahlig. Nach Bemerkung 3.2.20 liegt $\mathbb{Z}$ dicht in $\mathbb{Z}_p$, daher gibt es für jedes $x \in \mathbb{Z}_p$ eine Folge $(m_n)_{n\in\mathbb{N}}$ von ganzen Zahlen mit $\lim\limits_{n\to\infty} m_n = x$. Da $\binom{x}{k}$ stetig ist und $\mathbb{Z}_p$ als Teilmenge von $\mathbb{Q}_p$ abgeschlossen ist, ergibt sich:
$\binom{x}{k} = \binom{\lim\limits_{n\to\infty} m_n}{k} = \lim\limits_{n\to\infty} \underbrace{\binom{m_n}{k}}_{\in\mathbb{Z}} \in \mathbb{Z}_p$
Aufgrund der Stetigkeit von $\binom{x}{k}$ gibt es zu festem $N \in \mathbb{N}$ und jedem $x \in \mathbb{Z}_p$ ein $n(k)_x \in \mathbb{N}$, sodass $\binom{x}{k} - \binom{y}{k} \in p^N\mathbb{Z}_p$ gilt für alle $y \in \mathbb{Z}_p$ mit $x - y \in p^{n(k)_x}\mathbb{Z}_p$. Ist $x_1, ..., x_{p^n} \in \mathbb{Z}_p$ ein Repräsentantensystem von $\mathbb{Z}_p/p^n\mathbb{Z}_p$, so setze $n(k) := max\{N, n(k)_{x_1}, ..., n(k)_{x_{p^n}}\}$. Dann gilt $\binom{x}{k} - \binom{y}{k} \in p^N\mathbb{Z}_p$ für alle $x, y \in \mathbb{Z}_p$ mit $x - y \in p^{n(k)}\mathbb{Z}_p$. Betrachte nun $\binom{x}{k} - \sum\limits_{r=0}^{p^n-1} \binom{r}{k}\mathbb{1}_{r+p^n\mathbb{Z}_p}$ mit $n \geq n(k)$. Wir werten die Funktion auf einem beliebigen $y \in \mathbb{Z}_p$ aus und erhalten $\binom{y}{k} - \binom{r_y}{k}$, wobei $y \in r_y + p^n\mathbb{Z}_p$. Da Äquivalenzklassen entweder gleich oder disjunkt sind, ist r_y eindeutig. Es ist $y - r_y \in p^n\mathbb{Z}_p \subseteq p^{n(k)}\mathbb{Z}_p$, da $n \geq n(k)$. Aufgrund unserer obigen Ergebnisse wissen wir, dass dann auch gilt $|\binom{y}{k} - \binom{r_y}{k}|_p \leq p^{-N}$. Da $y \in \mathbb{Z}_p$ beliebig war, gilt bezüglich der Supremumsnorm:
$\|\binom{x}{k} - \sum\limits_{r=0}^{p^n-1} \binom{r}{k}\mathbb{1}_{r+p^n\mathbb{Z}_p}\|_\infty = \sup\limits_{x\in\mathbb{Z}_p} |\binom{x}{k} - \sum\limits_{r=0}^{p^n-1} \binom{r}{k}\mathbb{1}_{r+p^n\mathbb{Z}_p}(x)|_p \leq p^{-N}$ falls $n \geq n(k)$.

Da μ K-linear ist, ergibt sich:
$\mu(\binom{x}{k} - \sum\limits_{r=0}^{p^n-1} \binom{r}{k}\mathbb{1}_{r+p^n\mathbb{Z}_p})$
$= \mu(\binom{x}{k}) - \mu(\sum\limits_{r=0}^{p^n-1} \binom{r}{k}\mathbb{1}_{r+p^n\mathbb{Z}_p})$
$= \mu(\binom{x}{k}) - \sum\limits_{r=0}^{p^n-1} \binom{r}{k}\mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})$

Wir haben bereits gezeigt, dass für alle $\mu = L_\lambda \in \mu(\mathbb{Z}_p, \mathfrak{o})$ gilt: $|\mu(f)| = |L_\lambda(f)| \leq \|f\|_\infty$ für alle $f \in C(\mathbb{Z}_p, K)$. Somit ist $\mu(\binom{x}{k}) - \sum\limits_{r=0}^{p^n-1} \binom{r}{k}\mu(\mathbb{1}_{r+p^n\mathbb{Z}_p}) \in p^N\mathfrak{o}$ für $n \geq n(k)$.

Setze nun $n := max\{n(k) \mid 0 \leq k \leq p^N\} \geq N$. Dann ist
$F - F_n$

$$= \sum_{k=0}^{\infty} \mu(\binom{x}{k}) X^k - \sum_{k=0}^{p^n-1} (\sum_{r=0}^{p^n-1} \binom{r}{k} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})) X^k$$

$$= (\sum_{k=0}^{p^N-1} \mu(\binom{x}{k}) X^k + \sum_{k=p^N}^{\infty} \mu(\binom{x}{k}) X^k) - (\sum_{k=0}^{p^N-1} (\sum_{r=0}^{p^n-1} \binom{r}{k} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})) X^k + \sum_{k=p^N}^{p^n-1} (\sum_{r=0}^{p^n-1} \binom{r}{k} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})) X^k)$$

$$= (\sum_{k=0}^{p^N-1} \mu(\binom{x}{k}) X^k - \sum_{k=0}^{p^N-1} (\sum_{r=0}^{p^n-1} \binom{r}{k} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})) X^k) + (\sum_{k=p^N}^{\infty} \mu(\binom{x}{k}) X^k - \sum_{k=p^N}^{p^n-1} (\sum_{r=0}^{p^n-1} \binom{r}{k} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})) X^k)$$

$$= (\sum_{k=0}^{p^N-1} \underbrace{(\mu(\binom{x}{k}) - \sum_{r=0}^{p^n-1} \binom{r}{k} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p}))}_{\in p^N \mathfrak{o}} X^k) +$$

$$\underbrace{((\sum_{k=p^N}^{\infty} \mu(\binom{x}{k}) X^{k-p^N}) X^{p^N} - (\sum_{k=p^N}^{p^n-1} (\sum_{r=0}^{p^n-1} \binom{r}{k} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})) X^{k-p^N}) X^{p^N})}_{\in X^{p^N} \mathfrak{o}[\![X]\!]}$$

$$\Rightarrow F - F_n \in (p, X)^N \subseteq \mathfrak{o}[\![X]\!].$$

Nun wollen wir zeigen, dass auch $(\psi^{-1} \circ \phi^{-1})(\mu) - F_n$ in $(p, X)^N$ liegt. Dafür zeigen wir zunächst, dass $(\psi^{-1} \circ \phi^{-1})(\mu) - F_n$ im Kern von $pr_n \circ \psi$ liegt. Es gilt:

$(pr_n \circ \psi)((\psi^{-1} \circ \phi^{-1})(\mu)) = pr_n(\phi^{-1}(\mu)) = \sum_{r=0}^{p^n-1} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p}) \gamma_n^r$

Andererseits gilt aber auch:

$$(pr_n \circ \psi)(F_n)$$

$$= (pr_n \circ \psi)(\sum_{k=0}^{p^n-1} (\sum_{r=0}^{p^n-1} \binom{r}{k} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})) X^k)$$

$$= \sum_{k=0}^{p^n-1} (\sum_{r=0}^{p^n-1} \binom{r}{k} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p}))(\gamma_n - 1)^k$$

$$= \sum_{r=0}^{p^n-1} \underbrace{(\sum_{k=0}^{p^n-1} \binom{r}{k} (\gamma_n - 1)^k)}_{\gamma_n^r} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p})$$

$$= \sum_{r=0}^{p^n-1} \mu(\mathbb{1}_{r+p^n\mathbb{Z}_p}) \gamma_n^r$$

Da ψ ein Isomorphismus, also insbesondere auch ein Homomorphismus ist, folgt $(pr_n \circ \psi)((\psi^{-1} \circ \phi^{-1})(\mu) - F_n) = 0$ wie behauptet. Es ergibt sich sogar $(\psi^{-1} \circ \phi^{-1})(\mu) - F_n \in ker(pr_n \circ \psi) = ((X+1)^{p^n} - 1)\mathfrak{o}[\![X]\!] \subseteq (p, X)^{n+1} \subseteq (p, X)^n \subseteq (p, X)^N$ da $N \geq n$, wobei die Inklusion $((X+1)^{p^n} - 1) \subseteq (p, X)^{n+1}$ im Beweis von 4.1.11 gezeigt wurde.

Damit folgt insgesamt:

$F - ((\psi^{-1} \circ \phi^{-1})(\mu)) = F - F_n + F_n - ((\psi^{-1} \circ \phi^{-1})(\mu))$

$= \underbrace{F - F_n}_{\in (p,X)^N} - \underbrace{((\psi^{-1} \circ \phi^{-1})(\mu) - F_n)}_{\in (p,X)^N} \in (p, X)^N.$

Da $N \in \mathbb{N}$ beliebig war, folgt

$F - ((\psi^{-1} \circ \phi^{-1})(\mu)) \in \bigcap_{N \in \mathbb{N}} (p, X)^N = \{0\}$, wobei die Gleichung $\bigcap_{N \in \mathbb{N}} (p, N)^N = \{0\}$ im Beweis von 4.1.11 gezeigt wurde.

$\Rightarrow F = ((\psi^{-1} \circ \phi^{-1})(\mu))$. Also ist $(\psi^{-1} \circ \phi^{-1})(\mu) = \sum_{k=0}^{\infty} \mu(\binom{x}{k}) X^k$ □

Somit haben wir herausgefunden, dass die Koeffizienten der zu μ assoziierten Potenzreihe F_μ gerade $\mu(\binom{x}{k})$ sind.

Bemerkung 4.3.4 *Der Isomorphismus $(\psi^{-1} \circ \phi^{-1}) : \mu(\mathbb{Z}_p, \mathfrak{o}) \to \mathfrak{o}[\![X]\!]$ von $\mathfrak{o}$-Algebren wird auch als p-adische Fouriertransformation bezeichnet. Er ist nach dem obigen Satz gegeben durch $\mu \mapsto \sum_{k=0}^{\infty} \mu(\binom{x}{k}) X^k$.*

Durch diese Abbildungsvorschrift steht der Isomorphismus in engem Bezug zum sogenannten Satz von der Mahlerentwicklung.

Satz 4.3.5 (von der Mahlerentwicklung) *Eine Funktion φ von $\mathbb{Z}_p$ nach $\mathfrak{o}$ ist stetig genau dann, wenn Elemente a_n aus $\mathfrak{o}$ existieren, sodass $|a_n| \to 0$ und $\varphi(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$. Die Folge $(a_n)_{n \in \mathbb{N}}$ ist eindeutig bestimmt durch φ.*

Beweis Siehe *Cyclotomic fields 1 and 2, Serge Lang*, Kapitel 4, §1 theorem 1.3

Eigenständigkeitserklärung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbständig angefertigt habe. Ich habe außer den im Literaturverzeichnis und im Text genannten Hilfsmitteln keine weiteren verwendet und alle Stellen der Arbeit, die anderen Werken dem Wortlaut oder dem Sinn nach entnommen sind, unter Angabe der Quellen als Entlehnung kenntlich gemacht.

Annika Stechemesser Mülheim an der Ruhr, den 26.07.2016

Literaturverzeichnis

1. JÄNICH, KLAUS (2005) Topologie, Springer-Verlag Berlin Heidelberg, achte Auflage

2. KOHLHAASE, JAN Skriptum zur Veranstaltung p-adische Analysis

3. LANG, SERGE(1990) Cyclotomic Fields 1 and 2, Springer-Verlag New York Berlin Heidelberg London Paris Tokyo

4. LORENZ, FALKO (1997) Einführung in die Algebra 2, Mannheim, zweite Auflage

5. NEUKIRCH, JÜRGEN (1992) Algebraische Zahlentheorie, Springer-Verlag Berlin Heidelberg

6. NEUKIRCH, JÜRGEN; SCHMIDT, ALEXANDER; WINGBERG,KAI(1999) The Cohomology of Number Fields, Springer-Verlag Berlin Heidelberg, zweite Auflage

7. SCHMIDT, ALEXANDER (2007) Einführung in die algebraische Zahlentheorie, Springer-Verlag Berlin Heidelberg

8. SCHNEIDER, PETER (2011) p-Adic Lie Groups, Springer-Verlag Heidelberg Dordrecht London New York

9. SCHULZE-PILLOT, RAINER (2015) Einführung in Algebra und Zahlentheorie, Springer-Verlag Berlin Heidelberg, dritte Auflage