Mehrdimensionales Lemma von Hensel und Anwendungen

Bachelorarbeit

zur Erlangung des akademischen Grades
Bachelor of Science
im Studiengang Mathematik
der Naturwissenschaftlich-Technischen Fakultät VI
-Mathematik und Informatik-
der Universität des Saarlandes

von

Ruwen Hollenbach

Saarbrücken, 2013

Ich versichere hiermit, dass ich die vorliegende Arbeit
selbstständig verfasst und keine anderen als die
angegebenen Quellen und Hilfsmittel benutzt habe.

Saarbrücken, den 01.10.2013

(*Ruwen Hollenbach*)

Danksagung

An dieser Stelle möchte ich mich bei allen bedanken, die mich über mein ganzes Studium hinweg, und während der Bearbeitung dieser Bachelorarbeit unterstützt haben. Vor allem danke ich natürlich meiner Familie, die mich immer unterstützt hat und mir auch einfach mal zuhörte, wenn ich über Probleme in meiner Arbeit philosophierte. Zudem danke ich speziell meinen Eltern für die finanzielle Rückendeckung und die häusliche Unterstützung während meines Mathematikstudiums.
Ein besonderer Dank gilt Prof. Dr. Ernst-Ulrich Gekeler, der sich immer sehr viel Zeit für die Betreuung meiner Arbeit genommen hat.
Ein ganz großes Dankeschön auch an Timo Holz, der mir bei stilistischen Fragen bezüglich des Umgangs mit LaTeX stets und unverzüglich geholfen hat.

Einführung

Im Jahre 1897 entdeckte [1] Kurt Hensel, ein deutscher Mathematiker, die p-adischen Zahlen, welche man zur damaligen Zeit tatsächlich eher als Erfindung wahrgenommen hatte. In Hensels Buch über algebraische Zahlen [Hen08] definiert er diese neuartigen und erst einmal rein formalen Objekte wie folgt

> *"Unter einer Zahlgröße für den Bereich p oder von einer p-adischen Zahl will ich jede Reihe:*
>
> $$c_0 + c_1 p + c_2 p^2 + c_3 p^3 + \dots$$
>
> *mit modulo p reduzierten Koeffizienten, mag sie nun abbrechen oder nicht, verstehen, wenn eine Vorschrift existiert, nach welcher ihre Ziffern oder Koeffizienten soweit berechnet werden können als man nur will."*

Die Menge der p-adischen Zahlen bezeichnen wir mit $\mathbb{Z}_p$. Etwas moderner würde man diese Menge heutzutage definieren als:

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, \dots, p-1\} \ \forall i \in \mathbb{N} \right\}$$

In den darauffolgenden Jahren entwickelte Hensel im Alleingang die Theorie dieser neuen Objekte (wobei damit auch Ergebnisse über den Quotientenkörper $\mathbb{Q}_p$ gemeint sind). Neben vielen anderen wichtigen Ergebnissen, bewies er den Satz, der heute noch unter dem Namen *Lemma von Hensel* [2] bekannt ist. Die originale Version des Satzes befasste sich mit

> *"der Zerlegung der ganzen Funktionen mit p-adischen Koeffizienten in ihre irreduktiblen Faktoren"*

; dabei steht der Begriff *ganze Funktion* für Polynome und *irreduktibel* bedeutet einfach irreduzibel. Wir befassen uns in dieser Arbeit jedoch mit einer etwas anderen Variante, die Hensel für seine p-adischen Zahlen wie folgt formulieren würde:

[1] Die Antwort auf die Frage, ob Mathematiker Erfinder oder Entdecker sind, muss jeder für sich selbst finden. Jedoch liefern gerade die p-adischen Zahlen ein gutes Argument in beide Richtungen; hier wirken die p-adischen Zahlen wie eine Erfindung, aber schon in Kapitel 1 werden wir sehen, warum sie in natürlicher Weise als 'Entdeckung' auftreten (Stichwort: Komplettierung).

[2] Nach dem man die Theorie der p-adischen Zahlen in den Jahren nach Hensel erweitert hatte, wurde die Bezeichnung *Lemma von Hensel* für so ziemlich alle Ergebnisse verwendet, die entweder (im geeigneten Rahmen) äquivalent zur usprünglichen Version sind oder deren Beweisidee auf solchen Liftungen beruht, wie sie auch in Hensels Original durchgeführt wurden.

Satz 0.0.1 *Sei $f \in \mathbb{Z}_p[X]$. Nehmen wir an, dass ein $x \in \mathbb{Z}_p$ exisitert mit*

$$f(x) \equiv 0 \ mod\ p^n \qquad und \qquad f'(x) \not\equiv 0 \ mod\ p^k,$$

wobei $\mathbb{N} \ni k < n/2$. Dann existiert ein eindeutiges $\zeta \in \mathbb{Z}_p$ mit $f(\zeta) = 0$ und $\zeta \equiv x \ mod\ p^{n-k}$.

Inspiriert von Hensels Buch über algebraische Zahlen[Hen08], stellte Josef Kürschak 1912 das erste Axiomensystem zur Definition einer *Bewertung* vor.
Er formuliert seine Axiome wie folgt:

(i) $||a|| > 0$, falls $a \neq 0$, und $||0|| = 0$;
(ii) $||1 + a|| \leq 1 + ||a||$;
(iii) $||ab|| = ||a||\ ||b||$;
(iv) $\exists a\ :\ ||a|| \neq 0, 1$.

Sein Bestreben war es, unter anderem die p-adischen Zahlen, losgelöst von der formalen Definition Hensels, auf ein solides Fundament zu stellen; ähnlich wie es Cantor schon mit den reellen Zahlen getan hatte. Nachdem die Bewertungstheorie nach Kürschak entwickelt war, wurden noch weitere Erweiterungen vorgenommen.

Die nächste relevante Erweiterung gelang durch Krull und sein Paper über die *Allgemeine Bewertungstheorie*. Er arbeitete mit einer verallgemeinerten Definition einer Bewertung; ein sehr fruchtbarer Gedanke, wie sich im Laufe der Zeit herausstellen sollte. Durch die allgemeine Definition kamen neue Phänomene hinzu; z.B der *Rang* einer Bewertung etc. aber das wird in dieser Arbeit nicht behandelt.

Die vorliegende Arbeit beschäftigt sich primär mit dem Beweis des mehrdimensionalen Lemmas von Hensel, mit Hilfe des mehrdimensionalen Newton-Verfahrens. Grob gesprochen ist das Lemma von Hensel ein Ergebnis über die Approximation von Nullstellen von Systemen aus multivariaten konvergenten formalen Potenzreihen. Man hat eine Bedingung an das System und zeigt, dass uns diese Bedingung eine gute Approximation an eine Nullstelle liefert und wendet dann das Newton-Verfahren an um die Nullstelle zu finden.

Während der Bearbeitung des Themas entwickelte sich das Bestreben, die notwendige Theorie so zu entwickeln, dass zumindest die Kapitel 2 und 3, von Lesern mit geringen Vorkenntnissen in Algebra und Zahlentheorie und Basiswissen im Bereich der Analysis, verstanden werden können. Diese Vorgehensweise hat leider den Nachteil, dass die Beweise nicht mehr so elegant sind, wie es in anderen Arbeiten zu diesem Thema eventuell der Fall ist. Dennoch habe ich mich für Quantität (Anzahl der erreichbaren Leser) statt Qualität (Eleganz der geführten Beweise) entschieden; schon alleine deshalb, weil es schon sehr viele elegante Abhandlungen zum Lemma von Hensel gibt. Wer aber lieber den eleganten Weg sehen möchte und auch das entsprechende Vorwissen hat, findet in dieser Arbeit an den gegebenen Stelle auch Querverweise auf Literatur, die mehr Wert auf die elegante Darstellung legt.

In Kapitel 1 dieser Arbeit führen wir zuerst die Absolutbeträge ein und danach die, für die Arbeit, wichtigsten Bewertungsbegriffe; die diskrete Bewertung und die (exponentielle) Bewertung. Dabei werden wir sehen, dass kaum ein nennenswerter Unterschied zwischen den Absolutbeträgen und den Bewertungen besteht. Dennoch werden beide Begriffe auch in der

heutigen Literatur noch häufig getrennt. Ein Beispiel dafür, warum diese Trennung sinnvoll ist, ist die Einführung von Krull-Bewertungen als eine natürliche Verallgemeinerung der Bewertungen. Außerdem scheint es, als ob Absolutbeträge oft in Arbeiten verwendet werden, in denen es um eher analytische Aussagen geht und Bewertungen vielfach in Arbeiten auftreten, in denen man mehr Wert auf die algebraischen Ergebnisse legt. Inmitten wichtiger Ergebnisse aus der Bewertungstheorie, führen wir auch den Begriff des vollständig bewerteten Körpers ein, ein Objekt das uns durch die ganze restliche Arbeit hinweg begleitet. Die vollständig bewerteten Körper und ihre Bewertungsringe stellen das Fundament auf dem die vorliegende Arbeit überhaupt erst Sinn macht.

Danach geht es in Kapitel 2 weiter mit den vollständigen bewerteten Körper und einem der bekanntesten Ergebnisse die man in diesem Rahmen beweisen kann: dem Lemma von Hensel. Üblicherweise wird das Lemma von Hensel für Polynome bewiesen, aber der Beweis ändert sich nicht, wenn man stattdessen konvergente formale Potenzreihen betrachtet und die dadurch gewonnene Verallgemeinerung wiegt die zusätzliche Arbeit problemlos auf. Wir werden sehen, dass das Lemma von Hensel im Prinzip nichts weiter, als ein Korollar zur 'Taylor-Entwicklung' für konvergente formale Potenzreihen ist.

In Kapitel 3 kommen wir dann endlich zum Hauptteil der Arbeit: dem Beweis des mehrdimensionalen Lemma von Hensel. Dabei ist zu beachten, dass wir versuchen mit dem Beweis auch gleich einen Algorithmus zu liefern, der uns die Nullstelle liefert. Die notwendige Vorarbeit ist, wie schon erwähnt, nicht sehr elegant darzulegen, was mir der Leser verzeihen möge. Wir führen zuerst einmal die multivariaten formalen Potenzreihen ein und versuchen die Menge dieser Potenzreihen so einzuschränken, dass es Sinn macht sie als bestimmte Funktionen zu betrachten. Dieser Gedanke führt uns unweigerlich zu den konvergenten formalen Potenzreihen. Um im weiteren Verlauf ähnlich wie in Kapitel 2 argumentieren zu können, müssen wir im mehrdimensionalen Setting die richtige Metrik und die richtige Matrixnorm einführen. Nachdem das alles erledigt ist, ist auch der Beweis des mehrdimensionalen Lemmas von Hensel nicht mehr als ein Korollar zur mehrdimensionalen Variante der 'Taylor-Entwicklung'. Zur Abrundung des Kapitels werden noch zwei interessante Korollar zitiert. Das interessantere von beiden beschäftigt sich mit der Frage, ob man noch sinnvolle Bedingungen angeben kann, wenn man ein unterbesetztes System von Potenzreihen hat; damit ist gemeint, dass die Anzahl der Variablen die Anzahl der betrachteten Potenzreihen übersteigt.

Kapitel 4 beschäftigt sich mit der praktischen und theoretischen Verwendung von Hensels Lemma. Man sollte anmerken, dass die angegeben Anwendungen nur ein kleiner Teil aller bisher bekannten Anwendungsmöglichkeiten des Lemmas von Hensel sind, was dem Leser klarmachen sollte, wie wichtig dieses Ergebnis für die Mathematik ist.

Im Anhang wird dann noch kurz auf Krull-Bewertungen und Henselsche Körper eingegangen. Nachdem wir die ganze Zeit nur mit den einfachsten Bewertungen gearbeitet haben, soll der Anhang dem interessierten Leser vermitteln, dass diese Arbeit nicht einmal die Spitze des Eisbergs ist. Nach Krulls Verallgemeinerung des Bewertungsbegriffs haben sich sehr viele neue und interessante Teilbereiche gebildet. Einer davon ist zum Beispiel die Behandlung Henselscher Körper und der Henselisierung nichthenselscher Körper. Eine Bearbeitung dieser neueren Konzepte, wäre aber mindestens eine weitere Bachelorarbeit wert, sodass ich mich in dieser Arbeit mit gutem Gewissen nur für eine kommentierte Auflistung der fundamentalsten Ergebnisse entschieden habe.

Inhaltsverzeichnis

Symbolverzeichnis

$\mathbb{F}_p$	endlicher Körper mit p Elementen
$\mathbb{N}$	natürliche Zahlen inklusive 0
$\mathbb{Q}_p$	p-adische Zahlen
$\mathbb{Z}_p$	p-adische ganze Zahlen
$A^\times$	Einheitengruppe von A
B^{ad}	Adjunkte der Matrix B
$discr(f)$	Diskriminante vom Polynom f
K_{sep}	separabler Abschluss von K
char(K)	Charakteristik des Körper K
ker	Kern einer Abbildung

1. Grundlagen

In diesem Kapitel geben wir einen kurzen Einblick in die Theorie der *Absolutbeträge* und *Bewertungen*. Die Theorie wird aber nur soweit entwickelt wie es für die folgenden Kapitel notwendig ist. Da die Theorie aber sehr interessant und weitreichend ist, seien für den interessierten Leser die Bücher von O. Endler [End72] und von A.J Engler und A. Prestel [EP05] empfohlen.

Im folgenden bezeichnet K immer einen Körper.

1.1. Absolutbeträge (multiplikativ)

Definition Eine Abbildung $|.| : K \to \mathbb{R}_{\geq 0}$ heißt *Absolutbetrag*, wenn sie folgende Eigenschaften erfüllt:

(1) $|x| > 0$ für alle $x \neq 0$ und $|0| = 0$;
(2) $|xy| = |x||y|$, für alle $x, y \in K$;
(3) $|x + y| \leq |x| + |y|$, für alle $x, y \in K$ (Dreiecksungleichung).

Der Absolutbetrag mit $|x| = 1$ für alle $0 \neq x \in K$ nennt man den *trivialen* Absolutbetrag; dieser ist aber uninteressant und wird deshalb nicht betrachtet. Wenn wir also in dieser Arbeit von einem *Absolutbetrag* reden, so meinen wir immer einen nichttrivialen.

Gilt anstatt (3) die stärkere Bedingung:

(3') $|x + y| \leq \max\{|x|, |y|\}$, für alle $x, y \in K$ (starke Dreiecksungleichung),

so nennt man $|.|$ *nichtarchimedisch* und anderenfalls *archimedisch*.

Beispiele. (i) Die üblichen Absolutbeträge auf $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind archimedische Absolutbeträge. (ii) Für eine Primzahl $p \in \mathbb{P}$ definieren wir den *p-adischen* Absolutbetrag $|.|_p$ durch $|0|_p = 0$ und: Sei $x \in \mathbb{Q}$ mit Darstellung $x = p^{\nu}(\frac{m}{n})$, wobei $m \in \mathbb{N}$, $n, \nu \in \mathbb{Z}$ und p teilt nicht m oder n. Dann ist

$$|x|_p = |p^{\nu}\frac{m}{n}|_p = e^{-\nu}.$$

Diese Abbildung definiert einen nichtarchimedischen Absolutbetrag, wie man leicht nachprüft. Dabei muss die Basis nicht unbedingt e sein (oft verwendet man auch p als Basis); wichtig ist nur, dass die Basis größer als 1 ist.

(iii) Analog dazu definiert man für jedes irreduzible Polynom $p \in K[X]$ einen nichtarchimedischen Absolutbetrag $|.|_p$ auf $K(X)$ wie folgt:
$|0|_p = 0$ und für $f \in K(X)$, mit Darstellung $f = p^\nu(\frac{g}{h})$, wobei $\nu \in \mathbb{Z}$, $g, h \in K[X]$ und p teilt nicht g oder h, ist

$$|f|_p = |p^\nu \frac{g}{h}|_p = e^{-\nu}.$$

Auch hier prüft man leicht nach, dass die soeben definierte Abbildung tatsächlich einen nichtarchimedsichen Absolutbetrag definiert.

Bemerkungen. (i) $|1|^2 = |1^2| = |1|$, also $|1| = 1$;
(ii) $|-1|^2 = |(-1)^2| = |1| = 1$, also $|-1| = |1|$. Damit hat man $|-x| = |x|$;
(iii) $|.|$ ist ein Gruppenhomomorphismus von $(K^\times, \cdot)$ nach $(\mathbb{R}_{>0}, \cdot)$, also gilt $|x|^{-1} = |x^{-1}|$;
(iv) $|n| \leq 1$, für alle $n \in \mathbb{N}$, denn $|n| = \underbrace{|1 + \cdots + 1|}_{n-mal} \leq \max\{1\} = 1$.

Eine der wichtigsten Eigenschaften nichtarchimedischer Absolutbeträge auf K ist die folgende:

$$|x| < |y| \Rightarrow |x + y| = |y|.$$

Beweis. Wäre $|x + y| < |y| = \max\{|x|, |y|\}$, so hätte man

$$|y| = |(x + y) - x| \leq \max\{|x + y|, |x|\} < |y|;$$

einen Widerspruch. Also gilt die gewünschte Gleichheit.

Durch Induktion erhält man, dass auch für $x_1, \ldots, x_n \in K$ gilt

$$|x_i| < |x_j| \text{ für alle } i \in \{1, \ldots, n\} \setminus \{j\} \Rightarrow |x_1 + \cdots + x_n| = |x_j|.$$

Man sagt in diesem Fall, dass der "*Stärkere gewinnt*" und an Stellen, wo wir diese Eigenschaft verwenden, werden wir das auch genau so kennzeichnen.

Jeder Absolutbetrag $|.|$ definiert durch

$$d(x, y) := |x - y|$$

eine Metrik auf K. Somit können wir $(K, |.|)$ als metrischen Raum auffassen und definieren die Begriffe *Konvergenz*, *Cauchy-Folge*, *Vollständigkeit*, etc. wie üblich.

In Körpern versehen mit einem nichtarchimedischen Absolutbetrag vereinfachen sich Konvergenzbetrachtungen etc. aber erheblich, wie folgende Proposition zeigt:

Proposition 1.1.1 *Sei $(K, |.|)$ ein Körper K versehen mit einem nichtarchimedischen Absolutbetrag. Dann gelten:*

1. *$(a_n)_{n\in\mathbb{N}}$ ist eine Cauchy-Folge $\Leftrightarrow |a_n - a_{n+1}| \overset{n\to\infty}{\longrightarrow} 0$;*

2. *Sei* $(K, |.|)$ *zusätzlich vollständig.*
   $\sum_{n=0}^{\infty} a_n$ *konvergiert* $\Leftrightarrow a_n \overset{n\to\infty}{\longrightarrow} 0$*;*

3. $(a_n)_{n\in\mathbb{N}} \overset{n\to\infty}{\longrightarrow} a \neq 0 \Rightarrow \exists N \in \mathbb{N}$ *sodass* $|a_n| = |a|$ *für alle* $n \geq N$.

Beweis. 1. "⇒": klar. "⇐": Sei $\epsilon > 0$ und $N \in \mathbb{N}$ sodass $|a_n - a_{n+1}| < \epsilon$. Dann gilt wegen der starken Dreiecksungleichung:

$$|a_n - a_{n+m}| \leq \max_{0\leq i<m} |a_{n+i} - a_{n+i+1}| < \epsilon \quad \forall n \geq N,\ m \geq 0$$

Somit ist $(a_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge.
2. Nach 1. wissen wir, dass $\sum_{n=0}^{\infty} a_n$ genau dann Cauchy-Folge ist, wenn $|S_n - S_{n+1}| \overset{n\to\infty}{\longrightarrow} 0$, wobei $S_n = \sum_{i=0}^{n} a_i$. Aber $|S_n - S_{n+1}| = |\sum_{i=0}^{n} a_i - \sum_{i=0}^{n+1} a_n| = |a_{n+1}|$. Da $(K, |.|)$ als vollständig vorausgesetzt wurde, ist die Behauptung damit bewiesen.
3. Sobald $|a_n - a| < |a|$ für alle n ab einem gewissen $N \in \mathbb{N}$, gilt wegen der obigen Eigenschaft, dass $|a_n| = |(a_n - a) + a| = |a|$. □

Diese Eigenschaften sind der Grund, warum Körper versehen mit nichtarchimedischen Absolutbeträgen so interessant sind. Zudem treten solche Körper in natürlicher Weise in sehr vielen Bereichen der Mathematik auf, sodass es wichtig ist, diese nichtarchimedischen (oft auch *ultrametrisch* genannt) Räume gesondert von der gewöhnlichen Theorie metrischer Räume zu behandeln.

Zwei Absolutbeträge $|.|_1$ und $|.|_2$ heißen genau dann *äquivalent* ($|.|_1 \sim |.|_2$), wenn ein $c \in \mathbb{R}_{>0}$ existiert, sodass

$$|x|_1 = |x|_2^c, \text{ für alle } x \in K.$$

Ein fundamentales Ergebnis über die Äquivalenzklassen von Absolutbeträgen auf $\mathbb{Q}$ ist:

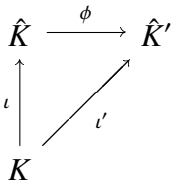
Satz 1.1.2 (Ostrowski) *Jeder nichttriviale Absolutbetrag auf* $\mathbb{Q}$ *ist entweder zum üblichen archimedischen Absolutbetrag oder zu einem p-adischen Absolutbetrag (*$p \in \mathbb{P}$*) äquivalent.*

Beweis. [vgl. Rob00]

Man sieht direkt, dass $\mathbb{Q}$, versehen mit einem p-adischen Absolutbetrag nicht vollständig ist. Nun ist jedem bekannt, dass $\mathbb{R}$ die Vervollständigung von $\mathbb{Q}$ bezüglich des üblichen archimedischen Absolutbetrags auf $\mathbb{Q}$ ist, doch wie sieht es mit der Vervollständigung bezüglich eines p-adischen Absolutbetrages aus? Ist die Vervollständigung noch ein Körper und kann man die nichtarchimedischen Absolutbeträge sinnvoll erweitern? Auf diese Frage liefert der nachfolgende Satz die Antwort.

Satz 1.1.3 *Für jeden Körper K versehen mit einem Absolutbetrag* $|.|$ *existiert ein Körper* $\hat{K}$*, vollständig bezüglich eines Absolutbetrages* $|\hat{.}|$*, und eine dichte Einbettung* $\iota : K \to \hat{K}$*, sodass*

$|x| = \widehat{|\iota(x)|}$, *für alle* $x \in K$. *Ist* $(\hat{K}', \iota')$ *ein weiteres solches Paar, so existiert ein eindeutiger isometrischer Isomorphismus* $\phi : \hat{K} \to \hat{K}'$, *sodass das Diagramm*



kommutiert.

Beweis. [vgl. EP05]

Bemerkung. Der Satz zeigt insbesondere, dass $|\hat{.}|$ nichtarchimedisch ist, falls $|.|$ nichtarchimedisch war.

Die Vervollständigung von $\mathbb{Q}$ bezüglich eines p-adischen Absolutbetrages bezeichen wir mit $\mathbb{Q}_p$ [1]. Diese Körper und ihre Eigenschaften spielen in vielen Zweigen der Zahlentheorie und auch in anderen Bereiche eine große Rolle. Ein Beispiel für das Vorkommen dieser Körper ist:

Beispiel: Satz 1.1.4 (Hasse-Minkowski) *Sei* $q \in \mathbb{Q}[X_1, \ldots, X_n]$ *eine quadratische Form mit ganzzahligen Koeffizienten. Dann gilt:*

$$q(X_1, \ldots, X_n) = 0 \textit{ hat eine Lösung über } \mathbb{Q}$$
$$\Leftrightarrow q(X_1, \ldots, X_n) = 0 \textit{ hat Lösungen über } \mathbb{R} \textit{ und allen } \mathbb{Q}_p$$

Bemerkung. (i) Diesen Satz kann man auf algebraische Zahlkörper K (d.h. endliche algebraische Erweiterungen von $\mathbb{Q}$) erweitern. (ii) Auf den ersten Blick sieht man der Aussage ihre Relevanz nicht an, weil die Suche nach einer Lösung in $\mathbb{Q}$ auf die Suche nach Lösungen in unendlich vielen anderen Körpern zurückgeführt wird. Aber Lösungen in $\mathbb{R}$ zu finden ist verhältnismäßig einfach und mit Hilfe des *Lemmas von Hensel*, dass wir hier beweisen werden (siehe Kapitel 3), ist auch die Suche nach Lösungen über $\mathbb{Q}_p$ in vielen Fällen um einiges einfacher als das Ausgangsproblem (Finden einer Lösung in $\mathbb{Q}$).

Im nächsten Abschnitt wollen wir eine additive Variante für nichtarchimedische Absolutbeträge definieren, die bei Untersuchung der algebraischen Eigenschaften nichtarchimedischer Körper eher Verwendung findet; z.B bei der Entwicklung der Theorie Henselscher Körper, welche aber in der Regel in einem allgemeineren Rahmen (Stichwort: Krull-Bewertungen [2]) formuliert wird.

[1] Nun haben wir $\mathbb{Q}_p$, wie in der Einführung angekündigt, endlich als 'Entdeckung' etabliert.

[2] Zu Krull-Bewertungen und Henselschen Körpern findet man eine kurze Zusammenfassung im Anhang.

1.2. Bewertung

In der Literatur taucht der Begriff *Bewertung* mit teilweise sehr verschiedenen Bedeutungen auf; z.B wird eine Bewertung häufig so definiert, dass sie den Bedingungen des oben definierten Absolutbetrages genügt, üblicher ist es jedoch, Bewertungen von Absolutbeträgen zu trennen. Einer der Gründe für diese Trennung ist die zuvor angesprochene Erweiterung auf Krull-Bewertungen. In der eigentlichen Arbeit werden wir aber nur mit zwei Bewertungsbegriffen arbeiten müssen und diese stehen in engem Zusammenhang mit den Absolutbeträgen.

(a) Diskrete Bewertungen

Definition Eine Abbildung $v : K \to \mathbb{Z} \cup \{\infty\}$ heißt *diskrete Bewertung*, wenn die folgenden Eigenschaften gelten:

(1) $v(x) \in \mathbb{Z}$ für $x \neq 0$ und $v(0) = \infty$;
(2) $v(xy) = v(x) + v(y)$, für alle $x, y \in K$;
(3) $v(x + y) \geq \min\{v(x), v(y)\}$, für alle $x, y \in K$.

Ist diese Abbildung zusätzlich surjektiv, so nennt man sie *normiert*. Einen Körper K, versehen mit einer normierten diskreten Bewertung v, oft kurz als (K, v) notiert, nennen wir einen *diskret bewerteten Körper*.

Beispiel. Auf $\mathbb{Q}$ hat man für jede Primzahl $p \in \mathbb{P}$ eine diskrete Bewertung v_p. Setze dazu $v_p(0) := \infty$ und sei $x \in \mathbb{Q}$ mit $x = p^{\mu}(\frac{m}{n})$, wobei $m \in \mathbb{N}$, $n, \mu \in \mathbb{Z}$ und p teilt nicht m oder n, so setzen wir $v_p(x) := \mu$. Diese Bewertungen nennt man die p-adischen Bewertungen von $\mathbb{Q}$ und es besteht folgender Zusammenhang zu den vorher definierten p-adischen Absolutbeträgen:

$$v_p(x) = -\log |x|_p \quad \forall x \in \mathbb{Q} |x|_p = e^{-v(x)} \quad \forall x \in \mathbb{Q}$$

Die Sätze 1.2.2 und 1.2.3 machen genauere Aussagen über die Beziehung zwischen Bewertungen und Absolutbeträgen.

Wie im Fall von Absolutbeträgen, wollen wir auch hier die triviale diskrete Bewertung ($v(0) = \infty$ und $v(x) = 0$ für $0 \neq x \in K$) von unserer Betrachtung ausschließen. Wenn wir ab sofort von einer diskreten Bewertung sprechen, meinen wir immer eine nichttriviale.

Bemerkungen. (i) Wie man an Eigenschaft (2) sieht, ist jede Bewertung v insbesondere ein Gruppenhomomorphismus von $(K, *)$ nach $(\mathbb{Z}, +)$.
(ii) Ist die Bewertung nicht normiert, so ist $v(K)$ eine echte Untergruppe von $\mathbb{Z}$, also $v(K) = a\mathbb{Z}$ für ein $a \in \mathbb{N}$ und $\frac{1}{a}v$ ist eine normierte diskrete Bewertung.

Diskrete Bewertungen spielen eine große Rolle in vielen Bereichen der Mathematik, wie z.B der Zahlentheorie und der algebraischen Geometrie. Einige interessante Beispiele hierfür sind in Kapitel 4 aufgeführt. Aber zuerst wollen wir uns ein wenig mit der Struktur beschäftigen, die eine solche diskrete Bewertung auf dem zugrundeliegenden Körper K erzeugt.

Dazu betrachten wir die Mengen $A_v := \{x \in K \mid v(x) \geq 0\}$ und $\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}$. Dabei ist $A_v \subset K$ (ausgestattet mit Addition und Multiplikation des zugrundeliegenden Körpers K) ein kommutativer Ring mit 1 und Einheitengruppe $A_v^\times = \{x \in K \mid v(x) = 0\}$ und $\mathfrak{m}_v$ ist ein maximales Ideal von A_v.

Beweis. Für die Aussage, dass A_v ein Ring ist, müssen wir nur zeigen, dass A_v unter Addition und Multiplikation abgeschlossen ist. Die Eigenschaften von v liefern uns

$$v(x+y) \geq \min\{v(x), v(y)\} \geq 0 \quad \text{und} \quad v(xy) = v(x) + v(y) \geq 0,$$

für alle $x, y \in A_v$. Somit ist A_v ein Ring.
Außerdem gilt offensichtlich für $x \in A_v$

$$v(x) = 0 \Leftrightarrow x^{-1} \in A_v,$$

woraus die Aussage über die Einheiten folgt. Die Tatsache, dass $\mathfrak{m}_v$ ein maximales Ideal von A_v ist, folgt daraus, dass jedes Element aus $A_v \setminus \mathfrak{m}_v$ eine Einheit ist.

Somit haben wir sogar gezeigt, dass $(A_v, \mathfrak{m}_v)$ ein lokaler Ring ist. Wir nennen den Ring A_v den *Bewertungsring von K bezüglich v* oder oft auch einfach nur den Bewertungsring von K_v, falls klar ist, welche Bewertung verwendet wurde.

Bemerkung. Ist v nicht nomiert mit $v(K) = a\mathbb{Z}$ so gilt für $x \in K$

$$v(x) \geq 0 \Leftrightarrow \frac{1}{a}v(x) \geq 0;$$
$$v(x) > 0 \Leftrightarrow \frac{1}{a}v(x) > 0.$$

Man sagt, dass zwei diskrete Bewertungen v_1, v_2 *äquivalent* sind, falls $v_1 = av_2$ mit $a \in \mathbb{Q}$. Man sieht leicht, dass in jeder Äquivalenzklasse genau eine normierte diskrete Bewertung ist.

Die Bewertungsringe von K, bezüglich einer diskreten Bewertung, hängen nur von der Äquivalenzklasse ab und sind unabhängig von der Auswahl eines Repräsentanten. Somit können wir uns problemlos auf den Fall normierter diskreter Bewertungen beschränken.

Ab sofort verstehen wir unter einem diskret bewerteten Körper immer einen Köper K, ausgestattet mit einer normierten diskreten Bewertung v.

Definition Sei R ein noetherscher Integritätsring mit $K := Quot(A)$. Dann nennen wir R einen *diskreten Bewertungsring*, falls gilt:

$$\forall 0 \neq x \in K \text{ ist } x \in A \text{ oder } x^{-1} \in A.$$

Wir zeigen nun, dass der Bewertungsring eines diskret bewerteten Körpers (K, v) nach obiger Definiton ein diskreter Bewertungsring ist.

Proposition 1.2.1 *Sei (K, v) ein diskret bewerteter Körper mit Bewertungsring A_v. Dann gilt*
(i) A_v ist ein Integritätsring und Quot(A_v)=K.
(ii) A_v ist noethersch.

Beweis. (i) Nehmen wir an, es existieren $0 \neq x, y \in A_v$ mit $xy = 0$. Dann haben wir

$$v(xy) = v(x) + v(y) < \infty = v(0).$$

Das ist offensichtlich ein Widerspruch und es folgt, dass A_v ein Integritätsring ist. Damit ist auch der Quotientenkörper Quot(A_v) sinnvoll definiert. Zudem gilt für alle $x \in K$ mit $v(x) < 0$, dass $v(x^{-1}) > 0$, also $x^{-1} \in A_v$ und dies zeigt die Gleichheit der beiden Körper.
(ii) Sei $I \subset A_v$ ein Ideal. Wir zeigen, dass I endlich erzeugt ist.
Mit der Definition von A_v folgt

$$v(I) \subset v(A_v) = \mathbb{N},$$

und wir wissen, dass jede Teilmenge von $\mathbb{N}$ ein kleinstes Element besitzt. Das kleinste Element von $v(I)$ bezeichnen wir mit d. Es existiert also ein $t \in I$ mit $v(t) = d$, welches sogar Erzeuger von I ist, denn:
Beachte, dass $v(t^{-1}) = -d$. Sei $x \in I$, also insbesondere $v(x) \geq d$. Dann ist wegen $v(t^{-1}x) = v(t^{-1}) + v(v) \geq 0$, $t^{-1}x \in A_v$ und wir haben

$$x = t \underbrace{(t^{-1}x)}_{\in A_v},$$

sodass t tatsächlich der Erzeuger von I ist. Wir haben somit nicht nur gezeigt, dass A_v noethersch ist, sondern, dass A_v ein Hauptidealring ist. Mithin ist also auch das maximale Ideal von A_v ein Hauptideal. □

Bemerkung. (i) Einen Erzeuger π des maximalen Ideals von A_v nennt man *lokalen Parameter* oder auch *Uniformisierende*.
(ii) Alle Ideale I von A_v sind von der Form

$$I = \mathfrak{m}_v^d = (\pi^d) \text{ für ein } d \in \mathbb{N}.$$

(iii) Sei $x \in K$, dann hat x eine eindeutige Darstellung

$$x = u\pi^k, \text{ wobei } u \in A_v^\times \text{ und } k \in \mathbb{Z}.$$

Dies zeigt, dass

$$K = \pi^{\mathbb{Z}} \times A_v^\times.$$

Somit ist ein Bewertungsring von K bezüglich einer diskreten Bewertung v ein diskreter Bewertungsring, eine Aussage die in gewissem Sinne auch umgekehrt richtig ist. Der folgende Satz zeigt uns, wie normierte diskrete Bewertungen mit diskreten Bewertungsringen und mit bestimmten nichtarchimedischen Absolutbeträgen zusammenhängen. Insbesondere liefert er die angesprochene Umkehrung.

Satz 1.2.2 *Sei K ein Körper. Dann gibt es kanonische Bijektionen zwischen den Mengen der*

a) normierten diskreten Bewertungen auf K;

b) Äquivalenzklassen von nicht-archimedischen Absolutbeträgen |.| auf K, für die gilt:

$$\log |K^*| \text{ ist diskret in } \mathbb{R};$$

c) diskreten Bewertungsringe $A \subset K$ mit Quot(A)=K.

Beweis. [Gek13]

Der Begriff der diskreten Bewertung lässt sich ganz einfach erweitern, indem wir den Wertebereich erweitern.

(b) Exponentielle Bewertungen

Definition Eine Abbildung $v : K \to \mathbb{R} \cup \{\infty\}$ heißt *exponentielle Bewertung*, wenn die folgenden Eigenschaften gelten:

(1) $v(x) \in \mathbb{R}$ für $x \neq 0$ und $v(0) = \infty$;
(2) $v(xy) = v(x) + v(y)$, für alle $x, y \in K$;
(3) $v(x + y) \geq \min\{v(x), v(y)\}$, für alle $x, y \in K$.

Satz 1.2.3 *Sei K ein Körper. Dann gibt es eine kanonische Bijektion zwischen den Mengen der*

a) nichtarchimedischen Absolutbeträgen |.| von K,

b) exponentiellen Bewertungen auf K.

Beweis. Wir haben die offensichtlich wohldefinierten und inversen Abbildungen

$$\begin{aligned} |.| &\mapsto v_{|.|}, \quad & v_{|.|}(x) &= -\log|x|; \\ v &\mapsto |.|_v, \quad & |x|_v &= e^{-v(x)}; \end{aligned}$$

mit den Konventionen $-\log 0 = \infty$ und $e^{-\infty} = 0$. □

Indem wir einer Bewertung den zugehörigen nichtarchimedischen Absolutbetrag zuordnen, können wir nun auch von vollständigen bewerteten Körpern sprechen.

Im weiteren Verlauf der Arbeit nennen wir exponentielle Bewertungen einfach nur noch Bewertungen.

Wie für die diskreten Bewertungen gilt auch hier, dass $A_v := \{x \in K \mid v(x) \geq 0\}$ ein lokaler Integritätsring mit maximalem Ideal $\mathfrak{m}_v = \{x \in K \mid v(x) > 0\}$ ist. Den lokalen Ring $(A_v, \mathfrak{m}_v)$ nennen wir den *Bewertungsring von K bezüglich v*. Wenn es die Situation erfordert, unterscheiden wir zwischen *diskreten Bewertungsringen*, die von diskreten Bewertungen induziert

werden und *Bewertungsringen*, die von nicht-diskreten (d.h heißt dichten oder surjektiven exponentiellen Bewertungen) induziert werden.

Wir nennen zwei Bewertungen v_1 und v_2 äquivalent, falls ein $c \in \mathbb{R}$ existiert, sodass $v_1 = cv_2$. Wie im Fall diskreter Bewertungen, gilt, dass äquivalente Bewertungen dieselben Bewertungsringe erzeugen.

Definition Ein Unterring $A \subset K$ von K heißt *Bewertungsring* von K, falls $x \in A$ oder $x^{-1} \in A$ für alle $0 \neq x \in K$.

Man sieht direkt, dass für einen bewerteten Körper (K, v) der Bewertungsring von K bezüglich v ein Bewertungsring von K nach obiger Definition ist. Dabei ist zu beachten, dass vom Ring A nicht gefordert ist, dass er noethersch ist. Es folgen nun Beispiele für eben solche nicht-diskreten Bewertungsringe. [3]

Beispiele. (i) Sei K ein Körper und X eine Unbestimmte. Dann definieren wir K_{Pui}, den Körper der Puiseux-Reihen, als die Menge der formalen Ausdrücke

$$f = \sum_{i=k}^{\infty} a_i X^{i/n}, \qquad \text{wobei } k \in \mathbb{Z} \text{ und } n \in \mathbb{N};$$

versehen mit denselben Verknüpfungen, die wir in Kapitel 2 einführen. Durch $v(0) = \infty$ und $v(f) =$"kleinster Bruch i/n, sodass $a_i \neq 0$", wird eine Bewertung mit $v(K_{Pui}^{\times}) = \mathbb{Q}$ definiert. Man sieht sofort, dass der zugehörige Bewertungsring aus den formalen Ausdrücken der Form

$$f = \sum_{i=0}^{\infty} a_i X^{i/n}$$

besteht. Nach Satz 1.2.2 ist dieser Ring nicht noethersch, denn wäre er noethersch, so wäre die soeben definierte Bewertung äquivalent zu einer normierten diskreten Bewertung von K, was offensichtlich nicht geht (da $v(K_{Pui}^{\times}) = \mathbb{Q}$ keine diskrete Untergruppe von $(\mathbb{R}, +)$ ist).

(ii) Ein weiteres Beispiel für einen bewerteten Körper (K, v) mit $v(K^{\times}) = \mathbb{Q}$ ist der algebraische Abschluss $\mathbb{Q}_p^a$ von $\mathbb{Q}_p$ mit der eindeutigen Fortsetzung von v_p (siehe Korollar 1.2.5 unten). Diese Aussage ist nichttrivial, aber leicht nachzuvollziehen, wenn man das richtige Werkzeug zur Hand hat, welches wir hier aber nicht entwickeln wollen. Einen schönen Beweis dieser Tatsache findet man in [Rob00, Ch 3, 1.2].

(iii) Nun möchten wir noch einen Körper konstruieren, der eine surjektive Bewertung besitzt. Sei also K ein Körper und X eine Unbestimmte. Für ein $\alpha \in \mathbb{R}$ bilden wir die formale Potenz X^{α}, mit der Konvention, dass $X^0 = 1$. Mit den formalen Polynomen $f(X) = a_1 X^{\alpha_1} + a_2 X^{\alpha_2} + \cdots + a_n X^{\alpha_n}$, mit $a_i \in K$ und $\alpha_{i+1} > \alpha_i$, rechnen wir genauso, wie mit gewöhnlichen Polynomen.

[3] Wir geben hier nur Beispiele an, die von nicht-diskreten exponentiellen Bewertungen induziert werden, aber es gibt durchaus auch Bewertungsringe, die nicht von solchen erzeugt werden. Es besteht jedoch eine 1:1 Beziehung zwischen Bewertungsringen und äquivalenten Krull-Bewertungen.

Mit den gewöhnlichen Verknüpfungen bildet die Menge aller Polynome der obigen Gestalt, einen Integritätsring, den wir mit R bezeichnen. Somit existiert der Quotientenkörper Quot(R) von R und man kann, wie folgt, eine Bewertung v definieren:
Wir setzen $v(0) = \infty$. Jedes Element $h(X) = \frac{f(X)}{g(X)}$ von Quot(R) lässt sich schreiben, als

$$h(X) = X^{\alpha}\frac{a_0 + a_1X^{\alpha_1} + \cdots + a_nX^{\alpha_n}}{b_0 + b_1X^{\beta_1} + \ldots b_mX^{\beta_m}};$$

und wir setzen $v(h) = \alpha$. Somit liefert uns v eine surjektive Bewertung. Diese Vorgehensweise kann man im Rahmen der Krull-Bewertungen noch erweitern, dafür muss man $\mathbb{R}$ nur durch eine linear geordnete abelsche Gruppe ersetzen (siehe [Kru32]).

Zu den wichtigsten Ergebnissen der Bewertungstheorie gehören die Erweiterungssätze, die sich damit beschäftigen, wieviele Fortsetzungen w von v in einem Erweiterungskörper L von K existieren (unter den verschiedensten Voraussetzungen, wie z.B $L|K$ endlich/ seperabel/ inseperabel/ transzendent etc.). Für uns ist dabei der folgende Satz ausschlaggebend:

Satz 1.2.4 *Sei (K, v) ein vollständiger bewerteter Körper und $L|K$ eine endliche Körpererweiterung. Dann existiert genau eine Bewertung w von L, die v erweitert (d.h. $w|_K = v$). Mit dieser Bewertung ist L auch vollständig.*

Beweis. [vgl. End72, 2.7+13.2] Der Beweis aus dem Buch von Endler ist über das ganze Buch verteilt, aber die Aussage ist dafür viel allgemeiner als wir sie brauchen.

Da jede algebraische Erweiterung die Vereinigung ihrer endlichen Teilerweiterungen ist, erhalten wir direkt:

Korollar 1.2.5 *Sei (K, v) vollständig und $L|K$ eine algebraische Erweiterung. Dann existiert genau eine Erweiterung w von v auf L.*

Man beachte, dass L jetzt nicht mehr vollständig bezüglich w sein muss. Aus diesem Korollar erhalten wir nun eine hilfreiche Aussage über die Analogie zwischen der Topologie bewerteter Körper und ihren algebraischen Erweiterungen.

Korollar 1.2.6 (Krasner's Lemma) *Sei (K, v) ein vollständiger bewerteter Körper und K_{sep} ein seperabler Abschluss von K . Nach Korollar 1.2.5 existiert eine eindeutige Fortsetzung von v auf K_{sep}, die wir auch mit v bezeichnen. Sei $a \in K_{sep}$ und $a = a_1, a_2, \ldots, a_n$ die zugehörigen konjugierten Elemente. Existiert ein Element $b \in K_{sep}$ mit*

$$v(a - b) > v(a - a_i) \quad \text{für} \quad i = 2, \ldots, n;$$

so ist $K(a) \subset K(b)$.

Beweis. Seien $b = b_1, \ldots, b_m$ die konjugierten Elemente von b, dann betrachten wir $K(a_1, \ldots, a_n, b_1, \ldots b_m)$. Dieser Körper ist eine Galoiserweiterung von K, da $K \subset K(a_1, \ldots, a_n, b_1, \ldots b_m)$ eine separable und normale Körpererweiterung ist. Somit ist auch $K(b) \subset K(a_1, \ldots, a_n, b_1, \ldots b_m)$ eine Galoiserweiterung, deren Galoisgruppe wir G nennen. Insbesondere gilt also, dass

$$K(b) = K(a_1, \ldots, a_n, b_1, \ldots b_m)^G \ (:= \{x \in K(a_1, \ldots, a_n, b_1, \ldots b_m) \mid \sigma(x) = x \quad \forall \sigma \in G\})$$

Wir müssen nun zeigen, dass $\sigma(a) = a$ für alle $\sigma \in G$. Für alle weiteren Fortsetzungen von v auf endliche Körpererweiterungen verwenden wir ebenfalls die Bezeichnung v . Man sieht sofort, dass jedes σ aus G eine Fortsetzung von v (auf $K(b)$) auf $K(a_1, \ldots, a_n, b_1, \ldots b_m)$ liefert. Aufgrund der Eindeutigkeit der Fortsetzungen nach *Satz 1.2.4* gilt aber die Gleichheit all dieser Fortsetzungen. Sei nun $\tau \in G$ ein $K(b)$-Automorphismus, dann erhalten wir

$$v(a - b) = v\tau(a - b) = v(\tau(a - b)) = v(\tau(a) - b) > v(a - a_i)$$

Daraus folgt

$$\begin{aligned} v(a - \tau(a)) &= v((a - b) + (b - \tau(a))) \\ &\geq v(a - b) \\ &> v(a - a_i) \quad \text{für } i = 2, \ldots, n. \end{aligned}$$

Also muss $\tau(a) = a$ sein und die Behauptung wurde gezeigt. □

2. Hensels Lemma (eindimensional)

Üblicherweise wird das Lemma von Hensel für *Polynome* über vollständigen nichtarchimedischen Körpern bewiesen, aber der Beweis ändert sich nur geringfügig, wenn wir *formale beschränkte Potenzreihen* betrachten. Diese werden im folgenden Abschnitt eingeführt.

2.1. Formale konvergente Potenzreihen

Sei K ein beliebiger Körper. Einen Ausdruck der Form $\sum_{n\in\mathbb{N}} a_n X^n$ bezeichnet man als *formale Potenzreihe über K*. Dabei sind die $a_n \in K$ und X steht für eine Unbekannte. Die Menge der formalen Potenzreihen kann wie folgt mit einer Addition und einer Multiplikation versehen werden:

$$\sum_{n\in\mathbb{N}} a_n X^n + \sum_{n\in\mathbb{N}} b_n X^n := \sum_{n\in\mathbb{N}} (a_n + b_n) X^n;$$
$$\sum_{n\in\mathbb{N}} a_n X^n * \sum_{n\in\mathbb{N}} b_n X^n := \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) X^n.$$

Man sieht, dass sowohl die Summe als auch das Produkt zweier formaler Potenzreihen wieder eine formale Potenzreihe ist. Es ist offensichtlich, dass die Menge der formalen Potenzreihe zusammen mit der soeben definierten Addition und Multiplikation einen kommutativen Ring $K[[X]]$ mit Einselement ($1 \in K$) definiert.

Bemerkung. Sei $A \subset K$ ein Unterring von K. Dann ist die analog definierte Menge $A[[X]]$ der *formalen Potenzreihen über A*, versehen mit der Addition und Multiplikation wie oben, ebenso ein Ring und es ist $A[[X]] \subset K[[X]]$.

Definition Sei $f(X) = \sum_{n\in\mathbb{N}} a_n X^n \in K\{X\}$. Dann ist die *formale Ableitung* f' (oder $\frac{df}{dx}$) von f definiert durch:

$$f'(X) := \sum_{n=1}^{\infty} a_n n X^{n-1}.$$

(Man beachte, dass die Summe hier bei 1 startet.)

Da das Lemma von Hensel Aussagen über die Existenz von Nullstellen macht, müssen wir uns auf solche formale Potenzreihen beschränken, die irgendwie als Funktionen aufgefasst werden können. Das bringt uns zu den *konvergenten formalen Potenzreihen*.

Für den weiteren Verlauf des Abschnitts ist K ein vollständiger Körper bezüglich eines nichtarchimedischen Absolutbetrages $|.|$ und A sein Bewertungsring, wenn nichts anderes gesagt wird.

Da $A = \{x \in K \mid |x| \leq 1\}$ die Einheitskugel bezüglich der, von $|.|$ induzierten Metrik ist, ist A als Teilmenge des metrischen Raumes K abgeschlossen. Zusätzlich gilt folgendes:

Ist $\sum_{i=0}^{\infty} a_i$ eine konvergente Reihe mit $a_i \in A$ so ist ihr Grenzwert wieder in A, denn:

Da A ein Ring ist, ist jede Partialsumme der Reihe ein Element in A. Nach Voraussetzung konvergiert die Folge der Partialsummen und aufgrund der Vollständigkeit von K und der Abgeschlossenheit von A, ist A selbst vollständig; d.h die Partialsummenfolge hat ihren Grenzwert in A.

Definition Eine formale Potenzreihe $f(X) = \sum_{n=0}^{\infty} a_n X^n \in K[[X]]$ heißt *konvergente formale Potenzreihe*, falls $|a_n| \overset{n\to\infty}{\longrightarrow} 0$. Die Menge der konvergenten formalen Potenzreihen bezeichnen wir mit $K\{X\}$.

Gilt $|a_n| \overset{n\to\infty}{\longrightarrow} 0$, so haben wir für alle $x \in A$:

$$|a_n x^n| = |a_n| \underbrace{|x^n|}_{\leq 1} \leq |a_n| \overset{n\to\infty}{\longrightarrow} 0;$$

also insbesondere $a_n x^n \overset{n\to\infty}{\longrightarrow} 0$, sodass $\sum_{n=0}^{\infty} a_n x^n$ nach Proposition 1.1.1 konvergiert. Somit definiert jedes $f(X) = \sum_{n=0}^{\infty} a_n X^n \in K\{X\}$ eine Funktion von A nach K, indem wir $x \in A$ auf $f(x) := \sum_{n=0}^{\infty} a_n x^n$ abbilden.

Proposition 2.1.1 *Seien $f = \sum_{n\in\mathbb{N}} a_n X^n, g = \sum_{n\in\mathbb{N}} b_n X^n \in K\{X\}$ zwei konvergente formale Potenzreihen. Dann gilt:*
(i) $f + g \in K\{X\}$ und $(f + g)(x) = f(x) + g(x)$ für alle $x \in A$
(ii) $f * g \in K\{X\}$ und $(f * g)(x) = f(x)g(x)$ für alle $x \in A$
(iii) $f' \in K\{X\}$

Beweis. (i)Aus $|a_n + b_n| \leq |a_n| + |b_n|$ folgt $f + g \in K\{X\}$. Die Gleichheit ist ist klar.
(ii) Da $|a_n| \overset{n\to\infty}{\longrightarrow} 0$ ist $|a_n x^n| \overset{n\to\infty}{\longrightarrow} 0$ für alle $x \in A$, also können wir $a_n x^n$ durch a_n ersetzen. Seien $A := \sum_{n\in\mathbb{N}} a_n$ und $B := \sum_{n\in\mathbb{N}} b_n$. Es bleibt zu zeigen:

$$|c_n| \overset{n\to\infty}{\longrightarrow} 0 \text{ und } \sum_{n=0}^{\infty} c_n = AB,$$

wobei $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Da $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$ Nullfolgen sind, gilt $\sup_{n\in\mathbb{N}} |a_n|, \sup_{n\in\mathbb{N}} |b_n| < \infty$ und wir setzen
$m := \max\{\sup |a_n|, \sup |b_n|\}$. Sei $\varepsilon > 0$ und $N \in \mathbb{N}$ so gewählt, dass

$$|a_n| < \frac{\varepsilon}{m}, |b_n| < \frac{\varepsilon}{m}, \text{ für alle } n \geq \lfloor N/2 \rfloor.$$

Weil für $n \geq N$ in der Summe $\sum_{k=0}^{n} a_k b_{n-k}$ entweder k oder $n-k$ größer als $N/2$ ist gilt:

$$|\sum_{k=0}^{n} a_k b_{n-k}| \leq \max_{k=0,\ldots,N} \{|a_k b_{n-k}|\} = |a_l b_{n-l}| \text{ für ein } l \in \{0,\ldots,n\},$$
$$\leq \left\{ \begin{array}{ll} \frac{|a_l|}{m}\varepsilon, & \text{falls } l \leq N/2 \\ \\ \frac{|b_l|}{m}\varepsilon, & \text{falls } l > N/2 \end{array} \right\} < \varepsilon, \text{ da } m > |a_l|, |b_l|.$$

Somit ist die erste Behauptung gezeigt.
Für die zweite Behauptung zeigen wir, dass $(\sum_{n=0}^{N} a_n \sum_{n=0}^{N} b_n - \sum_{n=0}^{N} c_n)_N$ eine Nullfolge ist. Man sieht direkt, dass

$$\sum_{n=0}^{N} a_n \sum_{n=0}^{N} b_n - \sum_{n=0}^{N} c_n = \sum_{\substack{k,l \leq N \\ k+l>N}} a_k b_l.$$

Seien $\varepsilon > 0$ und $N \in \mathbb{N}$ wie oben. Dann gilt:

$$|\sum_{\substack{k,l \leq N \\ k+l>N}} a_k b_l| < \varepsilon;$$

mit derselben Begründung wie oben. Sei $C := \sum_{n\in\mathbb{N}} c_n$. Dann haben wir insgesamt

$$AB - C = \lim_{N\to\infty} \sum_{\substack{k,l \leq N \\ k+l>N}} a_k b_l = 0.$$

Somit ist also auch die zweite Behauptung gezeigt.
(iii) Da $|n| \leq 1$ für alle $n \in \mathbb{N}$ ist mit $|a_n| \overset{n\to\infty}{\longrightarrow} 0$ auch $|a_n n| = |a_n||n| \leq |a_n| \overset{n\to\infty}{\longrightarrow} 0$. □

Zu $A[[X]]$ definieren wir $A\{X\}$ als die Menge der $f = \sum_{n=0}^{\infty} a_n X^n \in K\{X\}$ mit $a_n \in A$ für alle n. Offensichtlich ist $A\{X\}$, versehen mit den zuvor definierten Verknüpfungen ein Unterring von $K\{X\}$. Offensichtlich ist $A\{X\} \subset A[[X]]$. Man hat also insgesamt die folgenden Ketten von Inklusionen:

$$K[X] \subset K\{X\} \subset K[[X]];$$
$$A[X] \subset A\{X\} \subset A[[X]].$$

Bemerkung. Ist $f \in A\{X\}$, so ist auch $f' \in A\{X\}$.

Proposition 2.1.2 ("Taylor-Entwicklung") *Seien $f(X) = \sum_{n=0}^{\infty} a_n X^n \in A\{X\}$ und $x, h \in A$. Dann existieren $r, s \in A$, sodass*

$$(i) f(x+h) = f(x) + f'(x)h + h^2 r;$$
$$(ii) f(x+h) = f(x) + hs.$$

Beweis. (i) Betrachten wir $F_N(X,Y) := f_N(X+Y) := \sum_{n=0}^{N} a_n(X+Y)^n$, so ergibt sich:

$$\begin{aligned} F_N(X,Y) = \sum_{n=0}^{N} a_n(X+Y)^n &= \sum_{n=0}^{N} a_n\left[X^n + nYX^{n-1} + Y^2 g_n(X,Y)\right] \\ &= \sum_{n=0}^{N} a_n X^n + Y\sum_{n=0}^{N} a_n n X^{n-1} + Y^2 \sum_{n=0}^{N} a_n g_n(X,Y). \end{aligned}$$

wobei $g_n(X,Y) \in A[X,Y]$.
Setzen wir nun $x, h \in A$ ein, so konvergiert die linke Seite der Gleichung für $N \to \infty$ gegen $f(x+h)$. Wir müssen noch zeigen, dass der dritte Summand der rechten Seite für $N \to \infty$ konvergiert (die ersten beiden sind klar). Aber auch das ist trivial, denn $g_n(x,h) \in A$ (also insbesondere $|g_n(x,h)| \leq 1$) und somit gilt:

$$|a_n g_n(x,h)| = |a_n||g_n(x,h)| \leq |a_n| \overset{n\to\infty}{\longrightarrow} 0.$$

Also konvergiert $\sum_{n=0}^{\infty} a_n g_n(x,h)$ und da alle $a'_n := a_n g_n(x,h) \in A$, ist auch der Grenzwert in A; diesen Grenzwert bezeichen wir mit r.
Somit haben wir die gewünschte Darstellung für $f(x+h)$, denn:

$$\begin{aligned} &\lim_{N\to\infty} \underbrace{\left[f_N(x+h) - \sum_{n=0}^{N} a_n x^n + h\sum_{n=0}^{N} a_n n x^{n-1} + h^2 \sum_{n=0}^{N} a_n g_n(x,h)\right]}_{=0} = 0 \\ &= \lim_{N\to\infty} f_N(x+h) - \left[\lim_{N\to\infty}\sum_{n=0}^{N} a_n x^n + h\lim_{N\to\infty}\sum_{n=0}^{N} a_n n x^{n-1} + h^2 \lim_{N\to\infty}\sum_{n=0}^{N} a_n g_n(x,h)\right] \\ &= f(x+h) - f(x) - hf'(x) - h^2 r \end{aligned}$$

Dies zeigt die Behauptung.
(ii) zeigt man komplett analog. □

2.2. Lemma von Hensel

Satz 2.2.1 (Lemma von Hensel) *Sei $f \in A\{X\}$. Nehmen wir an, dass ein $x \in A$ existiert mit*

$$|f(x)| < |f'(x)|^2,$$

so existiert ein eindeutiges $\zeta \in A$ mit $f(\zeta) = 0$ und $|\zeta - x| < |f'(x)|$.

Beweis. Dieser Beweis folgt [Rob00].
Beachte, dass $|f(x)| < 1$ und $0 < |f'(x)| \leq 1$.
(i) *Abschätzungen bezüglich des Abstandes von $\hat{x} := x - \frac{f(x)}{f'(x)}$ zu x.*
Laut Voraussetzung ist $c := |\frac{f(x)}{f'(x)^2}| < 1$ und man hat

$$\begin{aligned} \hat{x} - x &= -\frac{f(x)}{f'(x)} = -\frac{f(x)}{f'(x)^2} f'(x); \\ |\hat{x} - x| &= c|f'(x)| < |f'(x)|; \end{aligned}$$

und analog dazu

$$(\hat{x}-x)^2 = \left(\frac{f(x)}{f'(x)}\right)^2 = \frac{f(x)}{f(x)^2}f(x);$$
$$|\hat{x}-x|^2 = c|f(x)| < |f(x)|.$$

Proposition 2.1.2 (i) mit $h = -\frac{f(x)}{f'(x)}$ liefert uns

$$f(\hat{x}) = \underbrace{f(x) + (\hat{x}-x)f'(x)}_{=0} + (\hat{x}-x)^2 r, \text{ mit } r \in A;$$
$$|f(\hat{x})| \leq |\hat{x}-x|^2 = c|f(x)| < |f(x)|.$$

Also ist $\hat{x}$ eine verbesserte Annäherung an eine Nullstelle. Wenden wir nun Proposition 2.1.2 (ii) mit $h = -\frac{f(x)}{f'(x)}$ auf f' an, so haben wir

$$f'(\hat{x}) = f'(x) + (\hat{x}-x)s, \text{ mit } s \in A.$$
$$|f'(\hat{x}) - f'(x)| \leq |\hat{x}-x| = c|f'(x)| < |f'(x)|.$$

Daraus folgt

$$|f'(\hat{x})| = |\underbrace{f'(x)}_{\text{Stärkster gewinnt}} + (f'(\hat{x}) - f'(x))| = |f'(x)|$$

(ii) *Weitere Iterationen*.
Sei nun $\hat{\hat{x}} := \hat{x} - \frac{f(\hat{x})}{f'(\hat{x})}$. Wir setzen

$$\hat{c} := |\frac{f(\hat{x})}{f'(\hat{x})}| \leq \frac{c|f(x)|}{|f'(x)|^2} = c^2.$$

Dieselben Überlegungen wie oben liefern hier

$$|f(\hat{\hat{x}})| \leq \hat{c}|f(\hat{x})| \leq \hat{c}c|f(x)| \leq c^3|f(x)|;$$

und mit $|f(x)| = c|f'(x)|^2$ erhalten wir

$$|f(\hat{\hat{x}})| \leq c^4|f'(x)|^2.$$

Induktiv definieren wir die Folge $(x_i)_{i\in\mathbb{N}}$ mit $x_{i+1} := \hat{x}_i$ ($x_0 = x$) und $c_{i+1} := \hat{c}_i$ ($c_0 = c$). Genau wie zuvor hat man

$$|f(x_i)| \leq c_{i-1}|f(x_{i-1})| \leq c_{i-1}\cdots c_1 c|f(x_0)| \leq c^{2^i-1}|f(x_0)| = c^{2^i}|f'(x_0)|^2 \overset{i\to\infty}{\longrightarrow} 0;$$
$$|x_2 - x_1| = |\hat{\hat{x}} - \hat{x}| \leq c^2|f'(x_0)|.$$

Mit Induktion nach i erhält man leicht

$$|x_{i+1} - x_i| \leq c^{2^i}|f'(x_0)| < c|f'(x_0)| = |x_1 - x_0|\,.$$

Insbesondere gilt

$$|x_i - x_0| = |x_1 - x_0| = c|f'(x_0)| \text{ für } i \geq 1 (*).$$

(iii) *Bestimmung der Nullstelle.*
Da $c^{2^i}|f'(x_0)| \xrightarrow{i\to\infty} 0$, ist $(x_i)_{i\in\mathbb{N}}$ eine Cauchy-Folge, und da K vollständig und A abgeschlossen ist, konvergiert $(x_i)_{i\in\mathbb{N}}$ mit $A \ni \zeta := \lim_{i\to\infty} x_i$. Mit $(*)$ und der Tatsache, dass $|.|$ eine stetige Abbildung ist, gilt

$$|\zeta - x_0| = |x_1 - x_0| = c|f'(x_0)| < |f'(x_0)|,$$

und nach obiger Überlegung und der Tatsache, dass f eine stetige Abbildung ist, haben wir

$$f(\zeta) = f(\lim_{i\to\infty} x_i) = \lim_{i\to\infty} f(x_i) = 0.$$

Somit ist ζ eine Nullstelle mit den geforderten Eigenschaften.
(iv) *Eindeutigkeit von ζ.*
Sei η eine weitere Nullstelle mit diesen Eigenschaften. Wir schreiben $\eta = \zeta + h$ und haben $|h| = |\eta - \zeta| < |f'(x)| = |f'(\zeta)|$. Mit Proposition 2.1.2 (i) sieht man

$$\begin{aligned} 0 = f(\eta) &= \underbrace{f(\zeta)}_{=0} + hf'(\zeta) + h^2 r, \text{ mit } r \in A; \\ 0 &= h(f'(\zeta) + hr) = h(f'(\zeta) + hr); \end{aligned}$$

und $f'(\zeta) + hr \neq 0$, da $|f'(\zeta) + hr| = |f'(\zeta)| > 0$; also ist $h = 0$ und $\eta = \zeta$. □

Korollar 2.2.2 *Sei $0 \neq f = \sum_{i\in\mathbb{N}} a_i X^i \in K\{X\}$ und a_j so, dass $|a_j| = \max_{i\in\mathbb{N}} |a_i|$. Nehmen wir an, dass ein $x \in A$ existiert mit*

$$|f(x)| < \frac{|f'(x)|^2}{\max\limits_{i\in\mathbb{N}} |a_i|}.$$

Dann existiert ein eindeutiges $\zeta \in A$ mit $f(\zeta) = 0$ und $|\zeta - x| < \frac{|f'(x)|}{|a_j|}$.

Beweis. Wir betrachen $\tilde{f}(X) := \frac{f(X)}{a_j} \in A\{X\}$ (f und $\tilde{f}$ haben dieselben Nullstellen) und erhalten mit der Voraussetzung

$$\begin{aligned} |f(x)| &< \frac{|f'(x)|^2}{|a_j|^2}|a_j| \\ \Leftrightarrow |\tilde{f}(x)| = \frac{|f(x)|}{|a_j|} &< \frac{|f'(x)|^2}{|a_j|^2} = |\tilde{f}'(x)|^2 \end{aligned}$$

Mit dem *Lemma von Hensel* folgt somit die Existenz einer Nullstelle $\zeta \in A$ von $\tilde{f}$ und offensichtlich ist diese auch eine Nullstelle von f. Die Eindeutigkeit der Nullstelle folgt ebenfalls aus dem Lemma von Hensel. □

Wir schließen dieses Kapitel mit einer Aussage ab, die man des Öfteren unter dem Namen *Lemma von Hensel-Rychlik* findet. Aber die Beweisidee unterscheidet sich stark von der bisherigen Methode, was unter Anderem daran liegt, dass der folgende Satz eine reine Existenzaussage liefert. Dafür definieren wir zuerst die Diskriminante eines Polynoms $f = c_n X^n + \cdots + c_1 X + c_0$ als

$$discr(f) := (-1)^{\frac{n(n-1)}{2}} c_n^{2n-2} \prod_{1 \le i < j \le n} (a_i - a_j)^2 = c_n^{2n-2} \prod_{i \neq j} (a_i - a_j).$$

Satz 2.2.3 (Lemma von Hensel-Rychlik) *Sei (K, v) ein vollständig bewerteter Körper mit Bewertungsring A und sei $f \in A[X]$. Existiert nun ein b mit*

$$v(f(b)) > v(discr(f)),$$

so hat f in K eine Nullstelle.

Bemerkungen. (i) Die untere Schranke ist hier, im Gegensatz zum Lemma von Hensel, nicht mehr von b abhängig, deshalb hat man aber auch keine genaue Aussage über die Lage der Nullstelle.
(ii) Der Beweis stammt aus [Kuh13]. Die Beweisidee ist dabei, zu zeigen, dass es eine Nullstelle a gibt, von der man sagen kann, dass sie 'am nächsten' an b liegt und dann Krasner's Lemma anzuwenden. Gerade Krasner's Lemma ist eines der wichtigsten Hilfsmittel in der Theorie Henselscher (und insbesondere vollständig bewerteter) Körper (siehe Anhang A).

3. Hensels Lemma (mehrdimensional)

Im ganzen Kapitel bezeichnen K einen vollständigen bewerteten Körper, A den zugehörigen Bewertungsring und $\mathfrak{m}$ das eindeutige maximale Ideal von A, wenn nichts anderes gesagt wird.

Da wir versuchen die mehrdimensionale Version von Hensel's Lemma ganz analog zur einfachen Version zu formulieren und zu beweisen, ist etwas mehr Vorarbeit von Nöten, als in anderen Arbeiten zu diesem Thema. Hier zahlt es sich besonders aus, dass wir den analytischen Formalismus (Absolutbeträge statt Bewertungen) zur Betrachtung bewerteter Körper gewählt haben, weil die folgenden Betrachtungen alle analytischer Natur sind und deshalb der Umgang mit Beträgen und Normen intuitiver erscheint.

3.1. Multivariate formale Potenzreihen

Der Leser mit Vorkenntnissen in Topologie kann die Behandlung multivariater Potenzreihen auch in [Bou89, Ch.3 §4] nachschlagen; dort werden die Begriffe mit Hilfe der $\mathfrak{m}$-adischen Topologie definiert, wodurch sich einige Beweise vereinfachen. Um aber auch Leser mit geringen Vorkenntnissen an das erstaunliche Ergebnis des mehrdimensionalen Lemmas von Hensel heranführen zu können, wird hier eine Alternative entwickelt.

Notation. Für ein n-Tupel $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ ("Multiindex") und ein $\zeta = (\zeta_1, \ldots, \zeta_n) \in K^n$ setzen wir

$$\zeta^\alpha := \zeta_1^{\alpha_1} \cdots \zeta_n^{\alpha_n};$$

und für ein Tupel von Unbestimmten $X = (X_1, \ldots, X_n)$ setzen wir

$$X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}.$$

Mit dieser Notation lassen sich nun *multivariate formale Potenzreihen* sehr kompakt definieren, als formale Ausdrücke der Form $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$ mit $a_\alpha \in K$. Ganz analog zu Kapitel 2 schreiben wir für die Menge der *(multivariaten) formalen Potenzreihen* $K[[X]]$ oder $K[[X_1, \ldots, X_n]]$ und definieren darauf zwei Verknüpfungen (Addition und Multiplikation):

$$\sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha + \sum_{\alpha \in \mathbb{N}^n} b_\alpha X^\alpha := \sum_{\alpha \in \mathbb{N}^n} (a_\alpha + b_\alpha) X^\alpha$$

$$\sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha * \sum_{\alpha \in \mathbb{N}^n} b_\alpha X^\alpha := \sum_{\alpha \in \mathbb{N}^n} \left(\sum_{\substack{\beta, \gamma \in \mathbb{N}^n \\ \beta + \gamma = \alpha}} a_\beta b_\gamma \right) X^\alpha$$

Es ist direkt klar, dass es sich bei $K[[X]]$, versehen mit diesen beiden Verknüpfungen, um einen kommutativen Ring mit 1 handelt. Dieser Ring ist für unsere Zwecke aber noch viel zu groß. Den richtigen Unterring werden wir im nächsten Abschnitt einführen, zuvor brauchen wir aber noch zwei fundamentale Objekte, die für die Formulierung sowie für den Beweis des Lemmas von Hensel unverzichtbar sind.

Bemerkung. Wir definieren $A[[X_1, \dots, X_n]]$ als die Menge der formalen Potenzreihen mit Koeffizienten in A. Mit den obigen Verknüpfungen ist klar, dass auch $A[[X_1, \dots X_n]]$ ein kommutativer Ring mit 1 ist und wir haben $A[[X_1, \dots, X_n]] \subset K[[X_1 \dots, X_n]]$.

Definition. (i) Zu einer formalen Potenzreihe $f = \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha X^\alpha \in K[[X_1, \dots, X_n]]$ und $1 \leq i \leq n$ heißt die formale Potenzreihe

$$\frac{\partial f}{\partial X_i} := \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha \alpha_i X_1^{\alpha_1} \cdots X_{i-1}^{\alpha_{i-1}} X_i^{\alpha_i - 1} X_{i+1}^{\alpha_{i+1}} \cdots X_n^{\alpha_n}$$

die *formale partielle Ableitung* von f nach X_i.

(ii) Zu formalen Potenzreihen $f_1, \dots f_n \in K[[X_1, \dots, X_n]]$ nennt man

$$J_f(X) := \begin{pmatrix} \frac{\partial f_1}{\partial X_1}(X) & \frac{\partial f_1}{\partial X_2}(X) & \dots & \frac{\partial f_1}{\partial X_n}(X) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial X_1}(X) & \frac{\partial f_m}{\partial X_2}(X) & \dots & \frac{\partial f_m}{\partial X_n}(X) \end{pmatrix}$$

die *Jacobimatrix* von $f = (f_1, \dots f_n)$.

3.2. Multivariate konvergente formale Potenzreihen

In diesem Abschnitt beschäftigen wir uns mit der Interpretation von formalen Potenzreihen als Funktionen von A^n nach K. Es ist klar, dass das nicht für alle formalen Potenzreihen möglich ist, weil wir dort keine Konvergenzbedingungen haben, die eine wohldefinierte Abbildung gewährleisten. Zunächst müssen wir also einen Unterring von $K[[X]]$ finden, für dessen Elemente, das Einsetzen von Werten aus A^n wohldefiniert ist.

Definition. Wir nennen ein $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha \in K[[X]]$ eine *(multivariate) konvergente formale Potenzreihe*, falls eine Bijektion $\sigma : \mathbb{N} \to \mathbb{N}^n$ existiert, für die $|a_{\sigma(n)}| \overset{n \to \infty}{\longrightarrow} 0$ gilt.

Die Menge der multivariaten konvergenten Potenzreihen bezeichnen wir mit $K\{X\} = K\{X_1, \dots X_n\}$. Nun gilt es zu zeigen, dass diese Menge, versehen mit den Verknüpfungen aus Abschnitt 3.1, ein Ring ist und wir die konvergenten formalen Potenzreihen auch tatäschlich als Funktionen von A^n nach K auffassen können.

Sei $f(X) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha \in K\{X\}$, d.h. $|a_\sigma(n)| \overset{n\to\infty}{\longrightarrow} 0$ für eine Bijektion $\sigma : \mathbb{N} \to \mathbb{N}^n$. Insbesondere ist $a_{\sigma(n)} \overset{n\to\infty}{\longrightarrow} 0$, sodass $\sum_{n\geq 0} a_{\sigma(n)}$ nach Proposition 1.1.1 konvergiert. Für jedes $x = (x_1, \dots x_n) \in A^n$ haben wir somit

$$|a_{\sigma(n)}x^{\sigma(n)}| = |a_{\sigma(n)}| \underbrace{|x_1^{\sigma(n)_1} \cdots x_n^{\sigma(n)_n}|}_{\leq 1} \leq |a_{\sigma(n)}| \overset{n\to\infty}{\longrightarrow} 0.$$

Also konvergiert auch $(a_{\sigma(n)}x^{\sigma(n)})_{n\in\mathbb{N}}$ gegen Null, sodass $\sum_{n\in\mathbb{N}} a_{\sigma(n)}x^{\sigma(n)}$ konvergiert. Sei $x \in A^n$, so können wir nun das Einsetzen von x in $f(X) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha$ definieren durch

$$f(x) := \sum_{n\in\mathbb{N}} a_{\sigma(n)}x^{\sigma(n)}.$$

So lässt sich f zwar als Funktion von A^n nach K auffassen, aber die implizite Abhängigkeit von der gewählten Bijektion stört. Die folgende Proposition wird uns zeigen, dass der Wert $f(x)$ gar nicht wirklich von der Wahl der Bijektion, sondern tatsächlich nur von f abhängt.

Proposition 3.2.1 *Sei $(a_i)_{i\in\mathbb{N}}$ eine Folge in K. Wir nehmen an, dass $|a_n| \overset{n\to\infty}{\longrightarrow} 0$, sodass $\sum_{n=0}^\infty a_n$ konvergiert. Sei s der Grenzwert der Reihe, so gilt:*

$$\textit{Für jede Bijketion } \sigma : \mathbb{N} \to \mathbb{N} \textit{ haben wir } s = \sum_{n\geq 0} a_{\sigma(n)}.$$

Beweis. Für ein $\varepsilon > 0$ definieren wir

$$I(\varepsilon) := \{n \mid |a_n| > \varepsilon\}.$$

Da die Reihe konvergent ist, ist $I(\varepsilon)$ offensichtlich endlich. Wir zeigen nun, dass

$$\sum_{n=0}^N a_n - \sum_{n=0}^N a_{\sigma(n)} = \sum_{n=0}^N (a_n - a_{\sigma(n)}) \overset{N\to\infty}{\longrightarrow} 0;$$

für alle Bijektion $\sigma : \mathbb{N} \to \mathbb{N}$.
Sei σ eine beliebige aber feste Bijektion. In der Reihe $\sum_{n=0}^\infty a_n$ können wir endliche viele Summanden miteindander vertauschen ohne den Grenzwert zu ändern. O.B.d.A. können wir also voraussetzen, dass $a_n = a_{\sigma(n)}$ für alle $n \in I(\varepsilon)$.
Nun wählen wir N so groß, dass

$$I(\varepsilon) \subset \{0, \dots, N\} \text{ und } I(\varepsilon) \subset \{\sigma(0), \dots \sigma(N)\}.$$

Somit erhalten wir

$$\Big|\sum_{n=0}^N (a_n - a_{\sigma(n)})\Big| = \Big|\sum_{n\in\{0,\dots,N\}\setminus I(\varepsilon)} (a_n - a_{\sigma(n)})\Big| \leq \max_{n\in\{0,\dots,N\}\setminus I(\varepsilon)} |a_n - a_{\sigma(n)}|$$
$$\leq \varepsilon.$$

Somit ist die Behauptung bewiesen. □

Sei $f(X) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha \in K\{X\}$. Sei $\sigma : \mathbb{N} \to \mathbb{N}^n$ eine Bijektion für die $|a_{\sigma(n)}| \overset{n\to\infty}{\longrightarrow} 0$ gilt. Jede weitere Bijektion $\tau : \mathbb{N} \to \mathbb{N}^n$ lässt sich darstellen als eine Verknürpfung $\sigma \circ \eta$, wobei $\eta : \mathbb{N} \to \mathbb{N}$ eine Bijektion von $\mathbb{N}$ nach $\mathbb{N}$ ist. Damit liefert uns die letzte Proposition die Unabhängigkeit der Abbildung

$$f : A^n \to K; \quad x \mapsto f(x) := \sum_{n\in\mathbb{N}} a_{\sigma(n)} x^{\sigma(n)}$$

von der gewählten Bijektion $\sigma : \mathbb{N} \to \mathbb{N}^n$. Insbesondere kann für alle $x \in A^n$ zusammen eine Bijektionσ gewählt werden.

Somit können wir die konvergenten formalen Potenzreihen nun als Funktionen von A^n nach K interpretieren.

Bleibt zu zeigen, dass $K\{X_1, \dots, X_n\}$ auch wirklich ein Ring ist und die Auwertungsabbildung $f \mapsto f(x)$ für alle $x \in A^n$ zumindest $(f + g)(x) = f(x) + g(x)$ erfüllt.

Proposition 3.2.2 *Seien $f = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha, g = \sum_{\alpha\in\mathbb{N}} b_\alpha X^\alpha \in K\{X_1, \dots, X_n\}$ zwei konvergente formale Potenzreihen. Dann gilt:*
(i) $f + g \in K\{X_1, \dots, X_n\}$ und $(f + g)(x) = f(x) + g(x)$ für alle $x \in A$,
(ii) $f * g \in K\{X_1, \dots, X_n\}$ und $(f * g)(x) = f(x)g(x)$ für alle $x \in A$.

Beweis. Da $f, g \in K\{X_1, \dots, X_n\}$, haben wir $|a_{\sigma(n)}|, |b_{\sigma(n)}| \overset{n\to\infty}{\longrightarrow} 0$ für eine Bijektion $\sigma : \mathbb{N} \to \mathbb{N}^n$. Also gilt:

$$|a_{\sigma(n)} + b_{\sigma(n)}| < \underbrace{|a_{\sigma(n)}|}_{\to 0} + \underbrace{|b_{\sigma(n)}|}_{\to 0} \overset{n\to\infty}{\longrightarrow} 0,$$

sodass $f + g \in K\{X_1, \dots, X_n\}$. Die geforderte Gleichheit ist damit auch klar.
(ii) Es gilt

$$(f * g)(X) = \sum_{\alpha\in\mathbb{N}^n} \left(\sum_{\substack{\beta,\gamma\in\mathbb{N}^n \\ \beta+\gamma=\alpha}} a_\beta b_\gamma \right) X^\alpha = \sum_{\alpha\in\mathbb{N}^n} \underbrace{\left(\sum_{\substack{\beta\in\mathbb{N}^n \\ \beta_i\le\alpha_i}} a_\beta b_{\alpha-\beta} \right)}_{=:c_\alpha} X^\alpha.$$

Seien $A := \sum_{\alpha\in\mathbb{N}^n} a_\alpha$ und $B := \sum_{\alpha\in\mathbb{N}^n} b_\alpha$. Es genügt (siehe Proposition 1.1.1)

$$|c_{\sigma(n)}| \overset{n\to\infty}{\longrightarrow} 0 \quad \text{und} \quad \sum_{n\ge 0} c_{\sigma(n)} = AB \quad \text{für eine Bijektion } \sigma : \mathbb{N} \to \mathbb{N}^n$$

zu zeigen. Für jede Bijektion $\sigma : \mathbb{N} \to \mathbb{N}^n$ gilt für $c_{\sigma(m)}$:

$$c_{\sigma(m)} = \sum_{\substack{\beta\in\mathbb{N}^n \\ \beta_i\le\sigma(m)_i}} a_\beta b_{\sigma(m)-\beta} = \sum_{\beta_1=0}^{\sigma(m)_1} \sum_{\beta_2=0}^{\sigma(m)_2} \cdots \sum_{\beta_n=0}^{\sigma(m)_n} a_{(\beta_1,\dots,\beta_n)} b_{(\sigma(m)_1-\beta_1,\dots\sigma(m)_n-\beta_n)} \quad (\star)$$

Für die weitere Argumentation wählen wir $\sigma = K_n^{-1}$, wobei $K_n(x_1, \ldots, x_n) = \sum_{k=1}^{n} \binom{k-1+x_1+\cdots+x_k}{k}$ die Cantorsche n-Tupelfunktion bezeichnet. Diese Abbildung erlaubt es uns die Bedingung $|a_{\sigma(n)}| \to 0$, $|b_{\sigma(n)}| \to 0$ sinnvoll auf die Multiindex-Schreibweise zu übertragen.
Wir setzen $r :=\max\{\sup|a_\alpha|, \sup|b_\alpha|\}$ $(< \infty)$. Sei $\varepsilon > 0$. Dann existiert ein $N \in \mathbb{N}$, sodass

$$|a_{\sigma(n)}| < \frac{\varepsilon}{r} \quad \text{und} \quad |b_{\sigma(n)}| < \frac{\varepsilon}{r} \quad \text{für alle } n \geq N.$$

Für dieses N und wegen der besonderen Wahl von σ gilt nun

$$|a_{(\beta_1,\ldots,\beta_n)}| < \frac{\varepsilon}{r} \text{ und } |b_{(\beta_1,\ldots,\beta_n)}| < \frac{\varepsilon}{r} \quad \forall \beta \text{ mit } \beta_1 + \cdots + \beta_n > \sigma(N)_1 + \cdots + \sigma(N)_n. \quad (\star\star)$$

In einem zweiten Schritt wählen wir N groß genug, sodass

$$|a_{(\beta_1,\ldots,\beta_n)}| < \frac{\varepsilon}{r} \text{ und } |b_{(\beta_1,\ldots,\beta_n)}| < \frac{\varepsilon}{r} \quad \forall \beta \text{ mit } \beta_1 + \cdots + \beta_n > \lfloor \frac{1}{2}(\sigma(N)_1 + \cdots + \sigma(N)_n) \rfloor.$$

Beachte, dass

$$\sigma(m)_1 + \cdots + \sigma(m)_n \geq \sigma(N)_1 + \cdots + \sigma(N)_n$$

für alle $m \geq N$. Mit $(\star)$ folgt also für $m \geq N$

$$\begin{aligned}
|c_{\sigma(m)}| &\leq \max_{\substack{\beta_i=0,\ldots,\sigma(m)_i \\ i=1,\ldots,n}} |a_{(\beta_1,\ldots,\beta_n)} b_{(\sigma(m)_1-\beta_1,\ldots,\sigma(m)_n-\beta_n)}| \\
&= |a_{(\gamma_1,\ldots,\gamma_n)} b_{(\sigma(m)_1-\gamma_1,\ldots,\sigma(m)_n-\gamma_n)}| \text{ für ein } \gamma \in \mathbb{N}^n \text{ mit } \gamma_i \leq \sigma(m)_i \\
&\leq \left\{ \begin{array}{ll} \frac{|a_{(\gamma_1,\ldots,\gamma_n)}|}{r}\varepsilon, & \text{falls } \gamma_1 + \cdots + \gamma_n \leq \lfloor \frac{1}{2}(\sigma(m)_1 + \ldots \sigma(m)_n) \rfloor \\ \frac{|b_{(\sigma(m)_1-\gamma_1,\ldots,\sigma(m)_n-\gamma_n)}|}{r}\varepsilon, & \text{falls } \gamma_1 + \cdots + \gamma_n > \lfloor \frac{1}{2}(\sigma(m)_1 + \ldots \sigma(m)_n) \rfloor \end{array} \right\} \\
&< \varepsilon\,, \quad \text{da } |a_{(\gamma_1,\ldots,\gamma_n)}|, |b_{(\sigma(m)_1-\gamma_1,\ldots,\sigma(m)_n-\gamma_n)}| < r.
\end{aligned}$$

Somit wurde der erste Teil, modulo einer ausführlichen Betrachtung der Cantorschen Tupelfunktion, gezeigt. Für eine Einführung in die n-Tupelfunktion empfehle ich [CR99]; dort wird besonders der Zusammenhang zu unseren Summenabschätzungen in $(\star\star)$ klar. Den zweiten Teil der Aussage beweist man ähnlich wie die Gleichheit in Proposition 1.1.1, aber diese Rechnung ist genauso unübersichtlich wie die bisherige und wird deshalb weggelassen; zumal wir diese Aussage im restlichen Abschnitt nicht benötigen. □

Somit handelt es sich bei $K\{X\} = K\{X_1, \ldots, X_n\}$ tatsächlich um einen Ring; der offensichtlich kommutativ ist und $1 \in K \subset K\{X\}$ als Einselement hat.

In Kapitel 2 haben wir schon gesehen, wie hilfreich analytische Konzepte beim Beweis von Aussagen über bewertete Körper sind und genau so wollen wir hier auch verfahren. Der nächste Schritt ist also die Definition einer geeigneten Metrik auf K^n; wichtig ist vor allem, dass A^n bezüglich dieser Metrik die abgeschlossene Einheitskugel ist.

Definitionen. (i) Sei $(K, |.|)$ ein vollständiger bewerteter Körper. Eine Abbildung $||.|| : K^n \to \mathbb{R}_{\geq 0}$ heißt $|.|$-Norm (oder kurz *Norm*), falls die folgenden Eigenschaften gelten:
(1) $||x|| = 0 \Leftrightarrow x = 0$;
(2) $||\lambda x|| = |\lambda| ||x||$ für alle $\lambda \in K$, $x \in K^n$;
(3) $||x + y|| \leq ||x|| + ||y||$, für alle $x, y \in K^n$. (Dreiecksungleichung)

(ii) Eine Abbildung $||.|| : K^{n\times m} \to \mathbb{R}_{\geq 0}$ heißt $|.|$-Matrixnorm, falls folgendes gilt:
(1) $||A|| = 0 \Leftrightarrow A = 0$;
(2) $||\lambda A|| = |\lambda| ||A||$, für alle $\lambda \in K$, $A \in K^{n\times m}$;
(3) $||A + B|| \leq ||A|| + ||B||$, für alle $A, B \in K^{n\times m}$.

Gilt statt (3) die stärkere Bedingung
(3') $||x + y|| \leq \max\{||x||, ||y||\}$ (starke Dreiecksungleichung);
so nennen wir die $|.|$-Norm *nichtarchimedisch*; ansonsten *archimedisch*. Dieselben Bezeichnungen nutzen wir auch für $|.|$-Matrixnormen.

Jede $|.|$-Norm $||.||$ liefert eine Metrik d auf K^n, durch

$$d(x, y) := ||x - y|| \text{ für alle } x, y \in K^n.$$

Wenn wir ab sofort von *Vollständigkeit*, *Cauchy-Folge*, *Abgeschlossenheit*, etc. sprechen, so meinen wir immer die üblichen Begriffe bezüglich der, zu $||.||$ gehörenden, Metrik.

Wir definieren auf K^n eine $|.|$-Norm $||.|| : K^n \to \mathbb{R}_{\geq 0}$ durch

$$||x|| := \max\{|x_1|, \ldots, |x_n|\} \text{ für alle } x = (x_1, \ldots, x_n) \in K^n.$$

Es ist offensichtlich, dass diese Abbildung eine Norm definiert und da $|.|$ nichtarchimedisch war, ist auch $||.||$ nichtarchimedisch.
Zusätzlich dazu definieren wir noch eine Matrixnorm $||.|| : K^{n\times n} \to \mathbb{R}_{\geq 0}$ durch

$$||A|| := \max_{0\leq i,j\leq n} |a_{ij}| \text{ für alle } A = (a_{ij})_{0\leq i,j\leq n} \in K^{n\times n}.$$

Auch diese Abbildung ist nichtarchimedisch, weil $|.|$ nichtarchimedisch ist.

Bemerkungen. (i) Unsere Matrixnorm erfüllt $||AB|| \leq ||A||\, ||B||$ für alle $A, B \in K^{n\times n}$.
(ii) Für alle $x \in K^n$ und $A \in K^{n\times n}$ gilt $||Ax|| \leq ||A||\, ||x||$.

Beweis. (i) Die Einträge der Matrix AB sind von der Form $a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots a_{in}b_{jn}$ für $0 \leq i, j \leq n$ und es gilt $|a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots a_{in}b_{jn}| \leq \max_{k\in\{1,\ldots,n\}} |a_{ik}bkj|$. Somit ist die Behauptung klar.
(ii) Geht komplett analog.

Betrachten wir nun ein $f(X) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha \in K\{X\}$, so ist f als Funktion von $(K^n, ||.||)$ nach $(K, |.|)$ stetig; dabei steht das Tupel $(K^n, ||.||)$ für den K-Vektorraum K^n, versehen mit der Metrik, die durch $||.||$ induziert wird.

Beweis. f kann als Funktion von K^n nach K als Grenzwert der gleichmäßig konvergenten Folge $(\sum_{n=0}^{N} a_{\sigma(n)} X_{N\in\mathbb{N}}^{\sigma(n)})$ aufgefasst werden. Dabei ist $\sigma : \mathbb{N} \to \mathbb{N}^n$ eine beliebige Bijektion. Die einzelnen Folgeglieder sind, als einfache Polynome, offensichtlich stetig. Somit liefert uns ein Standardergebnis aus der Analysis, dass auch f stetig ist.

Im späteren Beweis des Lemmas von Hensel benötigen wir, dass $(K^n, \|.\|)$ ein vollständiger metrischer Raum ist. Deshalb zuerst einmal folgender einfacher Satz:

Satz 3.2.3 *Sei* $(K, |.|)$ *vollständiger Körper. Dann ist auch* $(K^n, \|.\|)$ *vollständig.*

Beweis. (i) $(x^k)_{k\in\mathbb{N}}$ eine Folge in K^n mit $x^k = (x_1^k, \ldots, x_n^k)$. Dann gilt:

$$x^k \overset{k\to\infty}{\longrightarrow} x = (x_1, \ldots, x_n) \Leftrightarrow x_i^k \overset{k\to\infty}{\longrightarrow} x_i \text{ für alle } i \in \{1, \ldots, n\}.$$

" $\Rightarrow$ ": Folgt aus $|x_i^k - x_i| \leq \|x^k - x\|$.
" $\Leftarrow$ ": Für $i \in \{1, \ldots, n\}$ haben wir: $\forall\, \varepsilon\, \exists N_i \in \mathbb{N} :\ |x_i^k - x_i| < \varepsilon\ \forall k \geq N_i$.
Wähle nun $N := \max_{1\leq i\leq n} \{N_1, \ldots, N_n\}$. Dann gilt:

$$\|x^k - x\| = \max_{i=1,\ldots,n} |x_i^k - x_i| < \varepsilon\ \forall k \geq N.$$

Damit hat man $x^k \overset{k\to\infty}{\longrightarrow} x$.

(ii) Sei $(x^k)_{k\in\mathbb{N}}$ eine Cauchy-Folge in K^n, d.h

$$\forall \varepsilon > 0\ \exists N \in \mathbb{N} :\ \|x^k - x^l\| < \varepsilon\ \forall k, l \geq N.$$

Insbesondere gilt dann:

$$|x_i^k - x_i^l| < \varepsilon\ \forall k, l \geq N,\ \forall i \in \{1, \ldots, n\}$$

Also sind die $(x_i^k)_{k\in\mathbb{N}}$ Cauchy-Folgen in K und da $(K, |.|)$ vollständig ist, konvergieren diese Folgen gegen ein $x_i \in K$. Nach (i) ist x^k also konvergent mit Grenzwert $x = (x_1, \ldots, x_n) \in K^n$. □

Bemerkung. Ähnlich wie im Fall von nichtarchimedischen Absolutbeträgen, kann man auch für nicht-archimedische Normen zeigen, dass

$$(x^k)_{k\in\mathbb{N}} \text{ ist Cauchy-Folge in } K^n \Leftrightarrow \|x^{k+1} - x^k\| \overset{k\to\infty}{\longrightarrow} 0.$$

Proposition 3.2.4 *Sei* $f = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha \in A\{X_1, \ldots, X_n\}$. *Dann ist auch* $\frac{\partial f}{\partial X_i} \in A\{X_1, \ldots, X_n\}$, *für alle* $1 \leq i \leq n$.

Beweis. Da $f \in A\{X_1, \ldots, X_n\}$, gilt

$$|a_{\tau(n)}| \overset{n\to\infty}{\longrightarrow} 0 \text{ für jede Bijektion } \tau : \mathbb{N} \to \mathbb{N}^n.$$

Da $|\alpha_i| \leq 1$ für alle $i \in \{1, \ldots, n\}$, ist klar, dass die partiellen Ableitungen konvergente formale Potenzreihen sind. □

Proposition 3.2.5 (Multivariate Taylor-Entwicklung) *Sei $f \in A\{X_1, \dots, X_n\}$. Dann existieren $g_{ij} \in A = \{X, Y\} = A\{X_1, \dots, X_n, Y_1, \dots, Y_n\}$ sodass:*

$$f(X+Y) = f(X) + \left(\frac{\partial f}{\partial X_1}(X), \dots, \frac{\partial f}{\partial X_n}(X)\right) Y + \sum_{1 \le i \le j \le n} g_{ij}(X,Y) Y_i Y_j. \ (*)$$

Dabei ist der zweite Term die Kurzschreibweise für $\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(X) Y_i$.

Beweis. Wir betrachten $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$ als formale Potenzreihe in $A[[X_1, \dots, X_n]]$

$$\begin{aligned}
f(X+Y) &= \sum a_\alpha (X+Y)^\alpha = \sum a_\alpha (X_1+Y_1)^{\alpha_1}(X_2+Y_2)^{\alpha_2} \cdots (X_n+Y_n)^{\alpha_n} \\
&= \sum a_\alpha (X_1^{\alpha_1} + \alpha_1 Y_1 X_1^{\alpha_1 - 1} + Y_1^2 \dots) \cdots (X_n^{\alpha_n} + \alpha_n Y_n X_n^{\alpha_n - 1} + Y_n^2 \dots) \\
&= \sum a_\alpha (X_1^{\alpha_1} \cdots X_n^{\alpha_n} + \alpha_1 Y_1 X_1^{\alpha_1 - 1} X_2^{\alpha_2} \cdots X_n^{\alpha_n} + X_1^{\alpha_1} \cdots X_{n-1}^{\alpha_{n-1}} \alpha_n Y_n X_n^{\alpha_n - 1} \\
&\quad + \text{Terme der Form } Y_i Y_j g_{ij}^{(\alpha)}(X,Y), \text{ mit } g_{ij}^{(\alpha)} \in A[X_1, \dots, X_n, Y_1, \dots, Y_n]) \\
&= \sum a_\alpha X^\alpha + \sum a_\alpha \alpha_1 Y_1 X_1^{\alpha_1 - 1} X_2^{\alpha_2} \cdots X_n^{\alpha_n} + \sum a_\alpha \alpha_n Y_n X_1^{\alpha_1} \cdots X_{n-1}^{\alpha_{n-1}} X_n^{\alpha_n - 1} \\
&\quad + \sum_{\alpha \in \mathbb{N}^n} a_\alpha \sum_{1 \le i \le j \le n} Y_i Y_j g_{ij}^{(\alpha)}(X,Y) \\
&= f(X) + \frac{\partial f}{\partial X_1}(X) Y_1 + \cdots + \frac{\partial f}{\partial X_n}(X) Y_n + \sum_{\alpha \in \mathbb{N}^n} a_\alpha \sum_{1 \le i \le j \le n} Y_i Y_j g_{ij}^{(\alpha)}(X,Y) \\
&= f(X) + \frac{\partial f}{\partial X_1}(X) Y_1 + \cdots + \frac{\partial f}{\partial X_n}(X) Y_n + \sum_{1 \le i \le j \le n} Y_i Y_j \sum_{\alpha \in \mathbb{N}^n} a_\alpha g_{ij}^{(\alpha)}(X,Y)
\end{aligned}$$

Wir definieren nun $g_{ij}(X,Y) := \sum_{\alpha \in \mathbb{N}^n} a_\alpha g_{ij}^{(\alpha)}(X,Y)$.
Da $f \in A\{X_1, \dots, X_n\}$, gilt

$$|a_{\tau(n)}| \overset{n \to \infty}{\longrightarrow} 0 \text{ für jede Bijektion } \tau : \mathbb{N} \to \mathbb{N}^n. \quad (**)$$

Die $g_{ij} = \sum_{\alpha \in \mathbb{N}^n} a_\alpha g_{ij}^{(\alpha)}(X,Y)$ lassen sich in $A[[X_1, \dots, X_n, Y_1, \dots, Y_n]]$ darstellen als $\sum_{(\beta,\gamma) \in \mathbb{N}^n \times \mathbb{N}^n} c_{(\beta,\gamma)} X^\beta Y^\gamma$. Dabei ist jedes $c_{(\beta,\gamma)}$ das Produkt aus natürlichen Zahlen (den α_i) und Koeffizienten a_α und damit betraglich kleiner als jedes a_α, dass darin vorkommt. Somit folgt $|c_{\sigma(n)}| \overset{n \to \infty}{\longrightarrow} 0$, für jede Bijektion $\sigma : \mathbb{N} \to \mathbb{N}^n \times \mathbb{N}^n$ offensichtlich aus $(**)$. Damit sind die $g_{ij} \in A\{X_1, \dots, X_n, Y_1, \dots, Y_n\}$. □

Korollar 3.2.6 *Seien $f \in A\{X_1, \dots, X_n\}$ und $x, h \in A^n$. Dann gilt:*

$$f(x+h) = f(x) + \left(\frac{\partial f}{\partial X_1}(x), \dots, \frac{\partial f}{\partial X_n}(x)\right) h + \sum_{1 \le i \le j \le n} g_{ij}(x,h) h_i h_j.$$

Beweis. Fasse f, durch $f(X,Y) = f(X)$, auf natürliche Weise als Element von $A\{X_1, \dots X_n, Y_1, \dots Y_n\}$ auf. Wende Proposition 3.2.5 an um auf die gewünschte Darstellung zu kommen. Dann liefert

uns Proposition 3.2.2

$$f(x+h) = \left[f(X) + \left(\frac{\partial f}{\partial X_1}(X), \dots, \frac{\partial f}{\partial X_n}(X) \right) Y + \sum_{1 \le i \le j \le n} g_{ij}(X,Y) Y_i Y_j \right](x,h)$$
$$\overset{3.2.2}{=} f(x) + \left(\frac{\partial f}{\partial X_1}(x), \dots, \frac{\partial f}{\partial X_n}(x) \right) h + \sum_{1 \le i \le j \le n} g_{ij}(x,h) h_i h_j.$$

Somit ist die Behauptung gezeigt. □

Korollar 3.2.7 *Sei $f \in A\{X_1, \dots, X_n\}$. Dann gilt für alle $x, h \in A^n$:*

(i) $f(x+h) = f(x) + \left(\frac{\partial f}{\partial X_1}(x) + \cdots + \frac{\partial f}{\partial X_n} \right) h + h_k^2 r$, wobei $r \in A$ und $k \in \{1, \dots, n\}$, sodass $|h_k| = max_{1 \le i \le n} |h_i|$;
(ii) $|f(x+h)| \le |f(x) + (\frac{\partial f}{\partial X_1}(x), \dots, \frac{\partial f}{\partial X_n}(x))h| + \|h\|^2$;
(iii) $f(x+h) = f(x) + h_k s$, wobei $s \in A$ und $k \in \{1, \dots, n\}$ mit $|h_k| = max_{1 \le i \le n} |h_i|$.

Beweis. (i) Sei $k \in \{1, \dots, n\}$ so gewählt, dass $|h_k| = \|h\|$. Korollar 3.2.6 liefert uns

$$f(x+h) = f(x) + \left(\frac{\partial f}{\partial X_1}(x) + \cdots + \frac{\partial f}{\partial X_n} \right) h + h_k^2 \underbrace{\sum_{1 \le i,j \le n} g_{ij}(x,h) \frac{h_i h_j}{h_k^2}}_{=:r}$$

Da die $g_{ij} \in A\{X_1, \dots, X_n, Y_1, \dots, Y_n\}$ ist $g_{ij}(x,h) \in A$, also
$|g_{ij}(x.h)| \le 1$. Zudem ist nach Wahl von k: $\left| \frac{h_i h_j}{h_k^2} \right| \le 1$, sodass $r \in A$.
(ii) folgt aus (i)
(iii) Sei $k \in \{1, \dots, n\}$ so gewählt, wie oben. Korollar 3.2.6 liefert uns

$$f(x+h) = f(x) + h_k \underbrace{\left(\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(x) \frac{h_i}{h_k} + \sum_{1 \le i \le j \le n} g_{ij}(x,h) \frac{h_i h_j}{h_k} \right)}_{=:s}$$

Wir wissen, dass $\frac{\partial f}{\partial X_i}(x), g_{ij}(x,h) \in A$. Nach unserer Wahl von k gilt $\left| \frac{h_i}{h_k} \right| \le 1$; also ist $\frac{h_i}{h_k} \in A$. Dasselbe gilt natürlich auch für $\frac{h_i h_j}{h_k}$. Insgesamt haben wir somit, dass $s \in A$. □

Bemerkung. Die starke Dreiecksungleichung liefert uns natürlich eine bessere Abschätzung, aber diese wird hier nicht benötigt.

Korollar 3.2.8 *Sei $f = (f_1, \dots, f_n) \in A\{X_1, \dots, X_n\}^n$. Dann gilt für $x, h \in A$:*

$$\|f(x+h)\| \le \|f(x) + J_f(x)h\| + \|h\|^2$$

Beweis. (i) Sei $k \in \{1, \dots, n\}$ so, dass $\|f(x+h)\| = |f_k(x+h)|$. Dann haben wir

$$\|f(x+h)\| = |f_k(x+h)| \overset{3.2.7}{\le} \left| f_k(x) + \left(\frac{\partial f_k}{\partial X_1}(x), \dots, \frac{\partial f_k}{\partial X_n}(x) \right) h \right| + \|h\|^2$$
$$\le \|f(x) + J_f(x)h\| + \|h\|^2.$$

□

3.3. Hensels Lemma und Korollare

Bevor wir das Lemma von Hensel endlich beweisen können, brauchen wir noch eine kleine Hilfsaussage.

Lemma 3.3.1 *Sei $B \in K^{n\times n}$ invertierbar. Gilt $\|C - B\| < \frac{1}{\|B^{-1}\|}$, so ist C invertierbar.*

Beweis. Man beachte, dass $C = B + (C - B) = B[I + B^{-1}(C - B)]$. Ist $x \neq 0$, so haben wir

$$\|B^{-1}(C - B)x\| \leq \|B^{-1}\| \, \|C - B\| \, \|x\| \overset{(*)}{<} \|B^{-1}\| \, \|B\| \, \|x\| \leq \|x\|$$

Die Ungleichung $(*)$ gilt, weil $1 = \|I\| = \|BB^{-1}\| \leq \|B\|\|B^{-1}\|$; daraus folgt $\frac{1}{\|B^{-1}\|} \leq \|B\|$ und zusammen mit der Voraussetzung erhalten wir $\|C - B\| < \|B\|$. Somit gilt $B^{-1}(C - B)x \neq -x$; also $[I + B^{-1}(C - B)]x \neq 0$, also $Cx \neq 0$, da B invertierbar ist. Das zeigt, dass C invertierbar ist. □

Jetzt haben wir alles, was wir zum Beweis des mehrdimensionalen Lemmas von Hensel benötigen. Die technisch erscheinende Vorarbeit bisher, diente nur dazu das Werkzeug zur Verfügung zu stellen um die mehrdimensionale Variante so analog wie möglich zu formulieren und zu beweisen. Somit kommen wir nun zum Hauptergebnis dieses Abschnitts.

Satz 3.3.2 (Mehrdimensionale Version von Hensels Lemma) *Sei K ein vollständiger Körper mit Bewertungsring A und $f = (f_1, f_2, \ldots, f_n) \in A\{X_1, \ldots, X_n\}^n$. Gibt es ein $x \in A^n$ sodass $detJ_f(x) \in A^\times$ und*

$$\|f(x)\| < 1,$$

so existiert ein eindeutiges $\zeta \in A^n$, sodass $f(\zeta) = 0$ und $\|\zeta - x\| < 1$.

Beweis. Die Idee des Beweises ist es, dass eindimensionale Newton-Verfahren aus dem Beweis zu Satz 2.2.1 durch das mehrdimensionale Newton-Verfahren zu ersetzen und analog zu argumentieren.

(i) *Vorbereitung*. Da $\frac{\partial f_i}{\partial X_j}(x) \in A$ für alle $1 \leq i, j \leq n$, ist $J_f(x) \in A^{n\times n}$. Da $detJ_f(x) \in A^\times$, ist auch $J_f^{-1}(x) \in A^{n\times n}$. Genau wie in 3.3.1 erhalten wir

$$1 = \|E\| = \|J_f(x)^{-1}J_f(x)\| \leq \|J_f(x)^{-1}\|\|J_f(x)\|.$$

Somit ist $\|J_f(x)^{-1}\| \geq \frac{1}{\|J_f(x)\|}$. Da beide Matizen in $A^{n\times n}$ sind, gilt $\|J_f(x)^{-1}\|, \|J_f(x)\| \leq 1$. Insgesamt haben wir also nun $\|J_f(x)^{-1}\| = \|J_f(x)\| = 1$.

(ii) *Abschätzungen des Abstandes von $\hat{x} = x - J_f(x)^{-1}f(x)$ zu x.*
Die Voraussetzung ist $c := \|f(x)\| < 1$. Somit haben wir

$$\|\hat{x} - x\| = \|J_f(x)^{-1}f(x)\| \leq \|J_f(x)^{-1}\|\|f(x)\| = c\|J_f(x)\| < \|J_f(x)\|$$

und analog dazu

$$\|\hat{x} - x\|^2 = \|J_f(x)^{-1} f(x)\|^2 \leq \underbrace{\|J_f(x)^{-1}\|^2}_{=1} \|f(x)\|^2 = \|f(x)\|\|f(x)\| = c\|f(x)\| < \|f(x)\|.$$

Korollar 3.2.8 mit $h = \hat{x} - x$ liefert uns nun:

$$\|f(\hat{x})\| \leq \underbrace{\|f(x) + J_f(x)^{-1}(\hat{x} - x)\|}_{=0} + \|\hat{x} - x\|^2 \leq c\|f(x)\| < \|f(x)\|.$$

Mit Hilfe von Korollar 3.2.7 ergibt sich für $i, j \in \{1, \ldots, n\}$

$$\frac{\partial f_i}{\partial X_j}(\hat{x}) = \frac{\partial f_i}{\partial X_j}(x) + (\hat{x} - x)_k r^{(ij)}, \text{ wobei } r^{(ij)} \in A \text{ und } k \in \{1, \ldots, n\}$$
$$\text{mit } |(\hat{x} - x)_k| = \|\hat{x} - x\|.$$

Somit erhält man

$$J_f(\hat{x}) = J_f(x) + (\hat{x} - x)_j B, \text{ wobei } B = \begin{pmatrix} r^{(11)} & r^{(12)} & \ldots & r^{(1n)} \\ \vdots & \vdots & \ddots & \vdots \\ r^{(n1)} & r^{(n2)} & \ldots & r^{(nn)} \end{pmatrix}$$
$$, \|J_f(\hat{x}) - J_f(x)\| = |(\hat{x} - x)_j| \|B\| \leq \|\hat{x} - x\| \leq c\|J_f(x)\| < \|J_f(x)\|.$$

Dies zeigt

$$\|J_f(\hat{x})\| = \| \underbrace{J_f(x)}_{\text{stärkster gewinnt}} + (J_f(\hat{x}) - J_f(x))\| = \|J_f(x)\|.$$

(iii) *Weitere Iterationen*. Da $\|J_f(\hat{x}) - J_f(x)\| < \|J_f(x)\| = \frac{1}{\|J_f(x)^{-1}\|}$ liefert uns Lemma 3.3.1, dass $J_f(\hat{x})$ invertierbar ist und da $\|J_f(x)\| = \|J_f(\hat{x})\| = 1$ ist auch $\|J_f(\hat{x})^{-1}\| = 1$ und es folgt, dass $detJ_f(\hat{x}) \in A^\times$. Also ist es möglich $\hat{\hat{x}} := \hat{x} - J_f(\hat{x})^{-1} f(\hat{x})$ zu definieren. Zudem hat man $\hat{c} := \|f(\hat{x})\| \leq c\|f(x)\| = c^2$ und man erhält

$$\|f(\hat{\hat{x}})\| \leq \hat{c}\|f(\hat{x})\| \leq \hat{c}c\|f(x)\| \leq c^{2+1}\|f(x)\| \leq c^4$$

Der Rest des von (iii) verläuft nun komplett analog zum Beweis des einfachen Lemmas von Hensel. Man muss nur den Absolutbetrag durch die Norm und K (bzw. A) durch K^n (bzw. A^n) ersetzen. Die Invertierbarkeit der Jacobimatrix über A in jedem Iterationsschritt zeigt man mit Induktion mit Hilfe der Rechnungen aus (ii) und Lemma 3.3.1. Somit existiert also eine Nullstelle $\zeta \in A^n$.

(iv) *Eindeutigkeit*. Sei $\eta \in A^n$ eine weitere Nullstelle mit $\eta \in A^n$ und $\|\eta - x\| < 1$; und somit auch $\|\eta - \zeta\| < 1$. Wir schreiben $\eta = \zeta + h$ und es gilt offensichtlich $\|h\| = \|\eta - \zeta\| < 1$.

Nach Korollar 3.2.7 haben wir

$$0 = f(\eta) = \underbrace{f(\zeta)}_{=0} + J_f(\zeta)h + h_k^2 r, \text{ wobei } k \in \{1, \dots, n\}, \text{ sodass } |h_k| = \|h\| \text{ und } r \in A^n.$$

$$= h_k[J_f(\zeta) \underbrace{\begin{pmatrix} \frac{h_1}{h_k} \\ \vdots \\ \frac{h_{k-1}}{h_k} \\ 1 \\ \frac{h_{k+1}}{h_k} \\ \vdots \\ \frac{h_n}{h_k} \end{pmatrix}}_{=:h'} + h_k r].$$

Nun machen wir ein paar allgemeinere Aussagen über Matrizen über dem Bewertungsring A. Sei $B \in A^{n\times n}$ mit $detB \in A^\times$; d.h. B ist invertierbar und $B^{-1} \in A^{n\times n}$. Sei $x \in \mathfrak{m}^{(n)}$. Da $\mathfrak{m}$ ein Ideal ist und $b_{ij}x_j \in \mathfrak{m}$ für alle $1 \le i, j \le n$, sind alle Komponenten von Bx Elemente aus $\mathfrak{m}$; also $Bx \in \mathfrak{m}^{(n)}$. Weil B^{-1} ebenfalls eine Matrix aus $A^{n\times n}$ ist und deshalb die selbe Begründung für B^{-1} gilt, haben wir durch B einen Isomorphismus

$$B : \mathfrak{m}^{(n)} \to \mathfrak{m}^{(n)}, x \mapsto Bx$$

gegeben. Bezeichne B^{ad} die Adjunkte Matrix von B und I die $n \times n$ Einheitsmatrix so wissen wir, dass

$$B^{ad}B = (detB)I.$$

Sei $x \in \mathfrak{m}^{(n)}$. Dann gilt $B^{ad}Bx = (detB)x \in \mathfrak{m}^{(n)}$, weil $detB \in A^\times$. Da B eingeschränkt auf $\mathfrak{m}^{(n)}$ ein Isomorphismus ist, muss $B^{ad}(x) \in \mathfrak{m}^{(n)}$ für alle $x \in \mathfrak{m}^{(n)}$.
In unserer Situation ist nun $B = J_f(\zeta)$ und $x = h_k r$. Insgesamt ergibt sich nach Anwenden von $J_f(\zeta)^{ad}$ auf beiden Seiten der obigen Gleichung

$$0 = h_k[detJ_f(\zeta)h' + J_f(\zeta)^{ad}h_k r]$$

Nach unseren vorherigen Überlegungen wissen wir, dass $\|J_f(\zeta)^{ad}h_k r\| < 1$ und aufgrund der besonderen Form von h' haben wir $\|(detJ_f(\zeta))h'\| = |detJ_f(\zeta)|$ (= 1, weil $J_f(\zeta)$ invertierbar über A; diese Aussage steckt in Schritt 3). Somit erhalten wir letztendlich

$$0 = |h_k| \, \| \underbrace{(detJ_f(\zeta))h'}_{\text{Stärkster gewinnt}} + J_f(\zeta)^{ad}h_k r\| = |h_k| \, \|(detJ_f(\zeta)h'\| = \|h\| \, |detJ_f(\zeta)|$$

Da $detJ_f(\zeta) \neq 0$, muss also $\|h\| = 0$ und die Eindeutigkeit wurde gezeigt. □

Korollar 3.3.3 *Sei $f = (f_1, \dots, f_n) \in A\{X_1, \dots, X_n\}^n$. Seien $a \in A^n$ und $e \in A$ sodass $J_f(a)M' = eI_n$ für eine Matrix $M' \in A^{n\times n}$. Nehmen wir an, dass $f(a) \in eJ_f(a)\mathfrak{m}^{(n)}$; d.h. es existiert ein $b \in \mathfrak{m}^{(n)}$ sodass $f(a) = eJ_f(a)b$. Dann existiert ein eindeutiges $a' \in A^n$ mit $f(a') = 0$ und $a' \equiv a \bmod e\mathfrak{m}^{(n)}$.*

Beweis. [vgl. Fis97]
Wenden wir Proposition 3.2.7 auf die f_i an, so erhält man

$$f_i(a + eX) = f_i(a) + (\frac{\partial f}{\partial X_1}(a), \dots, \frac{\partial f}{\partial X_n}(a))eX + e^2 r_i(X)$$

Insgesamt hat man somit

$$f(a + eX) = f(a) + J_f(a)eX + e^2 \underbrace{(r_1(X), \dots r_n(X))}_{=:R(X)} = eJ_f(a)\left[b + X + M'R(X)\right] \tag{3.1}$$

Wir setzen $A\{X_1, \dots X_n\} \ni h(X) := b + X + M'R(X)$ und sehen sofort, dass $J_h(0) = I_n$ und $|h(0)| = |b| < 1$. Nach Satz 3.3.2 existiert ein eindeutiges $x \in \mathfrak{m}^{(n)}$ mit $h(x) = 0$. Somit ist $a' = a + ex$ die gesuchte Nullstelle für die $a' \equiv a \ mod \ e\mathfrak{m}^{(n)}$ gilt.
Sei nun $a'' = a + ex'$ eine weitere Nullstelle mit $x' \in \mathfrak{m}^{(n)}$. Dann ergibt Multiplikation mit $J_f(a)^{ad}$ auf beiden Seiten von (3.1) $0 = e \det(J_f(a))\, h(x')$ und da $J_f(a)M'$ ein Isomorphismus ist, ist $det(J_f(a)M') \neq 0$ und deshalb auch $detJ_f(a) \neq 0$. Somit muss $h(x') = 0$ sein. Das zeigt die Eindeutigkeit. □

Bemerkung. Das letzte Korollar umfasst insbesondere den Fall, dass $M' = J_f(a)^{ad}$ und $e = \det J_f(a)$.

Korollar 3.3.4 *Sei $\tilde{f} = (f_1, \dots, f_r) \in A\{X_1, \dots, X_n\}^r$, $1 \leq r \leq n$. Seien $a \in A^n$ und $e \in A$ und $S' \in A^{r\times r}$ sodass $SS' = eI_r$ für $S = (\frac{\partial f_i}{\partial X_j}(a))_{i,j=1,\dots r}$ ist. Nehmen wir an, dass $f(a) \in eS\mathfrak{m}^{(r)}$; d.h. es existiert ein $\tilde{b} \in \mathfrak{m}^{(r)}$, sodass $f(a) = eS\tilde{b}$. Dann existiert ein $a' \in A^n$ mit $\tilde{f}(a') = 0$ und $a' \equiv a \ mod \ e\mathfrak{m}^{(n)}$.*

Beweis. [vgl. RPC00]
Wir ergänzen $\tilde{f} = (f_1, \dots, f_r)$ zu einem System von n Potenzreihen durch Hinzufügen von $f_i(X) = X_i - a_i$ für $i = r+1, \dots, n$. Wir setzen nun $f := (f_1, \dots, f_n)$ und $b := (b_1, \dots b_n)$, wobei $(b_1, \dots, b_r) = \tilde{b}$ und $b_{r+1} = \cdots = b_n = 0$. Dann haben wir $f(a) = eJ_f(a)b$ und $J_f(a)M' = eI_n$, wobei $M' \in A^{n\times n}$ aus S' durch Ergänzen von e auf der Diagonalen und sonst überall Nullen, entsteht. Somit können wir Korollar 3.3.3 verwenden und erhalten eine Nullstelle a' von f. Diese ist natürlich auch eine Nullstelle von $\tilde{f}$ und es gilt wie gewünscht $a' \equiv a \ mod \ e\mathfrak{m}^{(n)}$.

Zum Schluss des Kapitels wollen wir noch eine verallgemeinerte Version des mehrdimensionalen Lemmas von Hensel angeben.

Satz 3.3.5 *Sei $(K, |.|)$ ein vollständig bewerteter Körper mit Bewertungsring A und $f = (f_1, \dots, f_n) \in A\{X_1, \dots, X_n\}^n$. Gibt es ein $x \in A^n$, sodass*

$$\|f(x)\| < |detJ_f(x)|^2.$$

Dann existiert ein eindeutiges $\zeta \in A^n$, sodass $f(\zeta) = 0$ und $\|\zeta - x\| < |detJ_f(x)|$.

Beweis. [siehe Kuh11]

Bemerkung. Wir haben leider keine Möglichkeit unsere Beweismethode sinnvoll auf diesen Fall anzuwenden. In unserer Form wird zwar deutlich, warum wir die Bedingung benötigen, dass die Determinante der Jacobimatrix eine Einheit ist, aber es wird nicht klar warum das für die Konvergenz des Newton-Verfahren auch wirklich notwendig ist. In [RPC00] findet sich ein Beweis zu unserer Form des Lemmas von Hensel, der auf einer Version des Banachschen Fixpunktsatzes beruht. Dort wird deutlich wo und wie die Bedingung über die Determinante genau eingeht.

4. Anwendungen

Das Lemma von Hensel hat viele Anwendungen in Theorie und Praxis und in diesem Kapitel sollen die einfachsten Beispiele erarbeitet werden. Als Anwendungen werden in diesem Sinne auch Ergebnisse bezeichnet, deren Beweise auf dem Lemma von Hensel aufbauen, die aber entweder zu interessant sind, oder sich nicht wirklich in Kapitel 2 einbinden ließen, sodass eine Aufführung als Korollar zu Satz 2.3 nicht gerechtfertigt wäre.
Für Anwendungsbeispiele aus anderen mathematischen Teilgebieten werden die notwendigen Begriffe eingeführt und die wichtigen Ergebnisse im jeweiligen Abschnitt aufgeführt (oft ohne Beweis).

4.1. Quadratische Körpererweiterungen von $\mathbb{Q}_p$

Für diesen Abschnitt ist es besser $\mathbb{Q}_p$ so aufzufassen wie es auch Hensel zu seiner Zeit tat. In Kapitel 1 hatten wir $\mathbb{Q}_p$ abstrakt eingeführt, als die Komplettierung von $\mathbb{Q}$ bezüglich eines p-adischen Absolutbetrags. Wir wollen $\mathbb{Q}_p$ nun konstruktiver beschreiben und das gelingt durch die folgende Proposition.

Proposition 4.1.1 *Sei* $Q := \left\{\sum_{i=m}^{\infty} a_i p^i \mid a_i \in \{0, \dots, p-1\}, m \in \mathbb{Z}\right\}$. *Dann gilt:*

$$(\mathbb{Q}_p, v_p) = (Q, v).$$

Dabei ist v definiert durch $v(0) = \infty$ *und* $v(\sum_{i=m}^{\infty} a_i p^i) =$ *"kleinstes k mit* $a_k \neq 0$*".*

Beweis. Die einzelnen Beweisschritte sind einfach und langweilig, deshalb wird der Beweis nur skizziert. Zu zeigen sind:

1. Q ist ein Körper; Multiplikation und Addition sind dabei Erweiterungen der Rechenregeln für natürliche Zahlen in p-adischer Darstellung (Stichwort 'Übertrag').
2. v ist eine Bewertung auf Q.
3. Q ist vollständig bezüglich des zu v gehörigen Absolutbtetrag.
4. Es existiert eine Einbettung $\iota : \mathbb{Q} \to Q$ mit $v_p(x) = v(\iota(x))$ für alle $x \in \mathbb{Q}$.

Hat man diese Aussagen überprüft, so liefert uns *Satz 1.1.3* die gewünschte Gleichheit. □

Bemerkung. Obige Darstellung für $\mathbb{Q}_p$ liefert zusätzlich

$$\mathbb{Z}_p = \left\{\sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{1, \dots, p-1\}\right\}$$

Für die vorliegende Situation ($K = \mathbb{Q}_p, A = \mathbb{Z}_p$) hat man folgenden hilfreichen Spezialfall von Hensels Lemma:

Satz 4.1.2 *(Spezialfall von Hensels Lemma) Sei $f \in \mathbb{Z}_p[X]$. Nehmen wir an, dass ein $x \in \mathbb{Z}_p$ exisitert mit*

$$f(x) \equiv 0 \; mod \; p^n \qquad und \qquad f'(x) \not\equiv 0 \; mod \; p^k,$$

wobei $\mathbb{N} \ni k < n/2$. Dann existiert ein eindeutiges $\zeta \in \mathbb{Z}_p$, sodass $f(\zeta) = 0$, $\zeta \equiv x \; mod \; p^{n-k}$ und $v(f'(\zeta)) = v(f'(x))$.

Wir wissen, dass jede quadratische Erweiterung eines Körper K mit char$K \neq 2$ von Quadratwurzeln erzeugt wird, denn:
Sei $f = aX^2 + bX + c \in K[X]$ ein quadratisches Polynom. Dann gilt für die Nullstellen (die Mitternachtsformel):

$$x_{1,2} = \underbrace{\frac{-b}{2a}}_{\in K} \pm \frac{\sqrt{b^2 - 4ac}}{2a}.$$

Also müssen wir, um die quadratischen Erweiterungen von $\mathbb{Q}_p$ zu klassifizieren, nur die Gruppe der Quadrate von $\mathbb{Q}_p$ untersuchen. Dieses Problem reduziert sich wegen

$$\mathbb{Q}_p \cong p^{\mathbb{Z}} \times \mathbb{Z}_p^\times \quad \text{(siehe Bemerkung aus Kapitel 1)}$$

sogar auf die Untersuchung der Gruppe $(\mathbb{Z}_p^\times)^2$.
Wir haben die (mod p)-Reduktionsabbildung

$$\bar{\cdot}: \mathbb{Z}_p \to \mathbb{F}_p, x = \sum_{i=0}^{\infty} a_i p^i \mapsto \bar{x} = a_0 + p\mathbb{Z}.$$

Lemma 4.1.3 *Sei $p \in \mathbb{P}$ eine ungerade Primzahl. Dann liefert uns die obige Reduktionsabbdilung einen Isomorphismus*

$$\bar{\cdot}: (\mathbb{Z}_p^\times)^2 \to (\mathbb{F}_p^\times)^2$$

Sei $p = 2$, so gilt

$$a \text{ ist ein Quadrat in } \mathbb{Z}_2^\times \Leftrightarrow a \in 1 + 8\mathbb{Z}_2$$

Beweis. Sei p eine ungerade Primzahl.
"$\Rightarrow$" Hat $X^2 - a = 0$ eine Lösung $x \in \mathbb{Z}_p$, so ist klar, dass $x^2 - a \equiv 0 \bmod p$, also ist $\bar{x}$ die gesuchte Lösung in $\mathbb{F}_p$.
"$\Leftarrow$" Wir wenden das Lemma von Hensel einfach auf $f(X) = X^2 - a' \in \mathbb{Z}_p$ an; dabei sei a' der Repräsentant von $\bar{a}$ mit $0 < a' < p$. Nach Voraussetzung ist $\bar{a}$ ein Quadrat, also gilt

$$f(a') \equiv 0 \bmod p \qquad und \qquad f'(a') = 2x \not\equiv 0 \bmod p.$$

Somit liefert uns Satz 4.1.2 die Existenz einer wohlbestimmten Nullstelle a von f mit $a \equiv a' \bmod p$.
Sei nun $p = 2$.
"$\Rightarrow$" Das ist eine leichte Rechnung, die man ad-hoc durchführen kann. Unter der Annahme, dass $a = x^2$ ist, geht man einfach die verschiedenen Möglichkeiten für die zweite und dritte Stelle von x in der Darstellung aus Prop. 4.1.1 durch und erhält die gewünschte Aussage. (Beachte: $\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$)
"$\Leftarrow$" Ist $a \in 1 + 8\mathbb{Z}_2$ so wenden wir Satz 4.1.2 mit Startwert $x_0 = 1$ auf $f(X) = X^2 - a$ an, denn offensichtlich gilt

$$f(1) = 1 - a \equiv 0 \bmod 2^3 \qquad \text{und} \qquad f'(1) \equiv 0 \bmod p.$$

Somit existiert also eine Nullstelle $x \in \mathbb{Z}_2^\times$ von f und a.

Nun sind wir in der Lage die quadratischen Körpererweiterung von $\mathbb{Q}_p$ (für alle $p \in \mathbb{P}$)), bis auf Isomorphie zu bestimmen.

Korollar 4.1.4 *Sei $p \in \mathbb{P}$. Dann hat $\mathbb{Q}_p$ bis auf Isomorphie drei quadratische Körpererweiterungen. Sei $1 < a < p$ kein Quadrat modulo p. Dann sind die drei Isomorphieklassen gegeben durch*

$$\mathbb{Q}_p(\sqrt{a}), \mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{ap})$$

Sei $p = 2$. Dann hat $\mathbb{Q}_p$,bis auf Isomorphie, 7 quadratische Körpererweiterungen. Mögliche Repräsentanten sind

$$\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{\pm 5}), \mathbb{Q}_2(\sqrt{\pm 2}), \mathbb{Q}_2(\sqrt{\pm 10}).$$

Beweis. $\mathbb{P} \ni p \neq 2$: Mit Lemma 4.1.3 ergibt sich

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 = (p^{\mathbb{Z}}/p^{2\mathbb{Z}}) \times (\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Somit ist

$$|\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2| = 4$$

und die Behauptung gezeigt.
$p = 2$: In $\mathbb{Z}_p$ gilt $-1 = 1 + \sum_{n=1}^{\infty} 1 \cdot 2^n$. Daraus folgt

$$\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2 = \{\pm 1\} \cdot (1 + 4\mathbb{Z}_2)$$

und mit Lemma 4.1.3 erhalten wir

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = (2^{\mathbb{Z}}/2^{2\mathbb{Z}}) \times (\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2) = \mathbb{Z}/2\mathbb{Z} \times \{\pm 1\} \times (1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Also haben wir

$$|\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2| = 8$$

und die Behauptung wurde bewiesen. □

4.2. Einheitswurzeln in $\mathbb{Q}_p$

Dieser Abschnitt folgt [Cla13].

Sei ζ eine n-te Einheitswurzel in $\mathbb{Q}_p$, d.h $\zeta^n = 1$. Dann ist $nv(\zeta) = v(1) = 0$, also $v(\zeta) = 0$ und somit ist jede Einheitswurzeln in $\mathbb{Z}_p^\times \subset \mathbb{Q}_p^\times$. Hier liefert uns das Lemma von Hensel eine starke Aussage über die Gruppe der Einheitswurzeln $\mu(\mathbb{Q}_p)$. Aber zuvor brauchen wir zwei wichtige und grundlegende Ergebnisse aus der Algebra, die wir hier ohne Beweis einfach nur nennen wollen. Diese Ergebnisse stehen so oder so ähnlich in jedem Buch über Algebra; hier sei nur [Lan02] genannt.

Lemma 4.2.1 (Gauß'sches Lemma) *Sei R ein Hauptidealring und K der zugehörige Quotientenkörper. Für ein Polynom $f \in R[X]$ gilt*

$$f \text{ ist irreduzibel in } R[X] \Leftrightarrow f \text{ ist irreduzibel in } K[X] \text{ und primitiv}.$$

Dabei heißt ein Polynom $f \in R[X]$:

1. *irreduzibel*, falls für jede Darstellung $f = gh$ mit $g, h \in R[X]$ gilt, dass f oder $g \in R^\times$;

2. *primitiv*, falls keine Nicht-Einheit von R alle Koeffizienten von f teilt.

Satz 4.2.2 (Eisensteinkriterium) *Sei R ein Integritätsring mit zugehörigem Quotientenkörper K und sei $f(X) = a_d X^d + \cdots + a_1 X + a_0 \in R[X]$. Existiert ein Primideal $\mathfrak{p}$ von R sodass $a_d \notin \mathfrak{p}$, $a_i \in \mathfrak{p}$ für alle $0 \leq i < d$ und $a_0 \notin \mathfrak{p}^2$. Dann gilt:*

$$f \text{ primitiv } \Rightarrow f \text{ irreduzibel in } R[X].$$

Satz 4.2.3 *Ist $p \in \mathbb{P}$ eine Primzahl. Dann ist die (mod p)-Reduktionsabbildung $r : \mu(\mathbb{Q}_p) \to \mathbb{F}_p^\times$ ein Gruppenisomorphismus. Insbesondere ist $\mu(\mathbb{Q}_p)$ also eine zyklische Gruppe der Ordnung $p - 1$.*

Beweis. *Surjektivität:* Sei $\bar{a} \in \mathbb{F}_p^\times$. Wir betrachten $f(X) = X^{p-1} - 1$. Dann gilt

$$\bar{a}^{p-1} - 1 = 0 \in \mathbb{F}_p \quad \text{und} \quad (p-1)\bar{a}^{p-2} \neq 0 \in \mathbb{F}_p$$

Somit existiert für jedes $a \in \mathbb{Z} \subset \mathbb{Z}_p$ mit $0 < a < p$ eine Nullstelle a' von f in $\mathbb{Z}_p$ mit $a' \equiv a \bmod p$. *Injektivität:* Die Injektivität beweisen wir in 2 Schritten.
(i) Wir zeigen zuerst, dass es in $\mathbb{Q}_p$ keine nichttrivialen p-ten Einheitswurzeln gibt. Dazu müssen wir zeigen, dass $\phi_p(X) = \frac{X^p - 1}{X - 1}$ über $\mathbb{Q}_p$ irreduzibel ist.
Für $f(X) = \phi_p(X + 1)$ gilt

$$f(X) = \frac{(X+1)^p - 1}{X + 1 - 1} = X^{p-1} + \binom{p}{1} X^{p-2} + \cdots + \binom{p}{p-2} X + p.$$

Wendet man nun das Eisensteinkriterium auf f mit $R = \mathbb{Z}_p$ und $\mathfrak{p} = (p)$ an, so erhält man, dass $f(X)$ und damit auch $\phi_p(X) = f(X-1)$ irreduzibel über $\mathbb{Z}_p$ sind. Mit dem Gauß'schen Lemma folgt somit die Irreduzibilität von f in $\mathbb{Q}_p$. Das zeigt die Behauptung.
(ii) Wir nehmen an, dass der Kern von r nichttrivial ist. Als nichttriviale Torsionsgruppe die nach (i) kein Element der Ordnung p enthält, existiert ein Element der Primordnung $l \neq p$, d.h es existiert eine primitive l-te Einheitswurzel $\tilde{x}$ sodass $r(\tilde{x}) = 1$ und somit auch $r(\tilde{x}^k) = 1$ für alle k. Als l-te Einheitswurzel erfüllt $\tilde{x}$: $\tilde{x}^{l-1} + \cdots + \tilde{x} + 1 = 0$. Reduktion modulo p liefert uns $l = 0$; ein Widerspruch. Somit muss der Kern trivial sein und r ist ein Isomorphismus. □

4.3. Satz von der impliziten Funktion über vollständigen bewerteten Körpern

In diesem Abschnitt formulieren wir ein Korollar zur mehrdimensionalen Version von Hensels Lemma aus 3.3.5

Satz 4.3.1 (Satz von der impliziten Funktion) *Seien $(K, |.|)$ ein vollständig bewerteter Körper und A der zugehörige Bewertungsring. Seien $f_1, \ldots, f_n \in A\{X_1, \ldots, X_m, Y_1, \ldots, Y_n\}$, mit $m < n$. Wir setzen $Z = (X_1, \ldots, X_m, Y_1, \ldots, Y_n)$ und*

$$J(Z) := \begin{pmatrix} \frac{\partial f_1}{\partial Y_1}(Z) & \frac{\partial f_1}{\partial Y_2}(Z) & \ldots & \frac{\partial f_1}{\partial Y_n}(X) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial Y_1}(Z) & \frac{\partial f_n}{\partial Y_2}(Z) & \ldots & \frac{\partial f_n}{\partial Y_n}(Z) \end{pmatrix}.$$

Nehmen wir an, dass $f = (f_1, \ldots, f_n)$ eine Nullstelle $z = (x_1, \ldots, x_m, y_1, \ldots, y_n) \in A^{m+n}$ besitzt und $\det(J(z)) \neq 0$. Wir setzen $x := (x_1, \ldots, x_m)$ und $y := (y_1, \ldots y_m)$. Dann existiert für alle $x' = (x'_1, \ldots, x'_m) \in A^m$ mit $\|x - x'\| < |detJ(z)|^2$ ein eindeutig bestimmtes $y' = (y'_1, \ldots, y'_n) \in A^n$, sodass $f(x'_1, \ldots, x'_m, y'_1, \ldots, y'_n) = 0$ und

$$\|y - y'\| \leq |detJ(z)|$$

Beweis. Wir ergänzen unser System von Potenzreihen, durch die m einfachen linearen Polynome $X_i - x'_i$ zum System $\tilde{f} := (X_i - x'_i, \ldots, X_m - x'_m, f_1, \ldots, f_n)$. Die Jacobimatrix von $\tilde{f}$ sieht wie folgt aus

$$\begin{pmatrix} E_m & 0 \\ 0 & J(Z) \end{pmatrix}.$$

Dabei steht E_m für die $m \times m$ Einheitsmatrix und die Nullen repräsentieren jeweils eine $m \times n$ und eine $n \times m$ Nullmatrix. Wir sehen also, dass $|detJ_{\tilde{f}}(z)| = |detJ(z)|$. Nach Voraussetzung

haben wir zudem $\|x - x'\| < |detJ(z)|^2 = |detJ_{\tilde{f}}(z)|^2$ und $f_i(z) = 0$ für $1 \leq i \leq n$, sodass wir

$$\|\tilde{f}(z)\| = \left\| \begin{pmatrix} x_1 - x'_1 \\ \vdots \\ x_m - x'_m \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\| < |detJ_{\tilde{f}}(z)|^2.$$

Wir wenden nun das multidimensionale Lemma von Hensel auf $\tilde{f}$ an und erhalten eine eindeutige Nullstelle $z' = (x'_1, \ldots, x'_m, y'_1, \ldots y'_n)$, sodass $\|z - z'\| < |det(J_{\tilde{f}}(z)| = |detJ(z)|$. Insbesondere folgt daraus $\|y - y'\| < |detJ(z)|$. □

5. Zusammenfassung und Schlusswort

In der vorliegenden Arbeit ist es uns gelungen, das mehrdimensionale Lemma von Hensel komplett analog zum einfachen Lemma von Hensel zu beweisen. Alles war wir dazu tun mussten, war eine genaue Betrachtung der gemachten Argumente und Schlüsse und danach der Transfer der eindimensionalen auf die mehrdimensionale Situation. Dazu mussten wir einige Umwege gehen, aber sobald der richtige Rahmen stand, konnte es auch schon losgehen.

Ich habe im Laufe der Arbeit, sehr oft darauf verwiesen, dass wir uns mit einem sehr angenehmen Spezialfall befassen in dem wir mit bekannten analytischen Methoden argumentieren konnten und dennoch haben wir in Kapitel 4 einige schöne und sehr nützliche Ergebnisse aus unseren Lemmata herleiten können. Jetzt stellt man sich vielleicht die Frage, was man dann wohl erst mit Ergebnissen in einem allgemeineren Rahmen herleiten könnte und das wäre auch schon ein weiteres Thema für eine Arbeit. Überhaupt ist es so, dass die Thematik rund um das Lemma von Hensel und der Bewertungstheorie, sehr viel Stoff zur Bearbeitung bereitstellt. Man könnte versuchen diese Arbeit auf ein rein algebraisches Fundament zu stellen und alle gemachten Aussagen neu zu formulieren und zu beweisen. Man könnte aber auch andere Ausgangssituationen untersuchen und anstatt vollständiger bewerteter Körper, sphärisch vollständige oder sogar henselsche Körper zu untersuchen. Wenn man schon mit henselschen Körpern arbeitet, könnte man versuchen die Äquivalenz zwischen einfachem und mehrdimensionalen Lemma von Hensel zu zeigen. Man sieht, dass die Möglichkeiten unbegrenzt sind.

Das eigentliche Schlusswort steckt schon in Kapitel 4, denn dort haben wir ja schon gerechtfertigt, warum sich zumindest jeder Leser mit einem Interesse für die Zahlentheorie, mit dem Thema dieser Arbeit auseinandersetzen sollte, oder, wenn man so will, sogar muss. Wem das als Motivation aber noch nicht reicht, sollte sich im Anhang davon überzeugen, dass es ein sehr großes Interesse an Ergebnissen aus diesen theoretischen Teilbereichen besteht.

A. Anhang

A.1. Krull-Bewertungen

Das Ziel dieses Abschnitts ist es, die Bewertungen aus Kapitel 1 zu verallgemeinern, Henselsche Körper einzuführen und die Bedingung 'henselsch' zu sein, zu diskutieren.

In Kapitel 1 haben wir Bewertungen eingeführt mit Wertebereichen $\mathbb{Z}$ und $\mathbb{R}$, aber eigentlich brauchten wir nur eine additive Struktur und mussten die angenommenen Werte auf irgendeine Weise sinnvoll vergleichen können. Aber wir brauchten keine weitere Struktur auf den Wertemengen, wie z.B dass $\mathbb{Z}$ und $\mathbb{R}$ Ringe sind etc., und deshalb beschränken wir uns bei der Definition von Krull-Bewertungen auch nur auf diese nötigen Eigenschaften.

Sei Γ eine additiv notierte abelsche Gruppe. Wir nennen Γ *linear geordnet*, falls eine Ordnungsrelation $\leq$ (oder $\geq$ mit $\alpha \geq \beta :\Leftrightarrow \beta \leq \alpha$) auf Γ definiert ist, die folgende Eigenschaften erfüllt: Es seien $\alpha, \beta, \gamma, \delta \in \Gamma$ beliebig.

1. Es gilt stets entweder $\alpha \geq \beta$, $\alpha \leq \beta$;
2. Aus $\alpha \geq \beta$ und $\beta \geq \alpha$ folgt $\alpha = \beta$;
3. Ist $\alpha \geq \gamma, \beta \geq \delta$, so ist stets auch $\alpha + \beta \geq \gamma + \delta$.

Beispiele. (i) Die Standardbeispiele für linear geordnete Gruppen sind $\mathbb{Z}$ und $\mathbb{R}$ mit ihrer natürlichen Ordnung.
(ii) Auf $(\mathbb{Z}^2, +)$ definiere $(x_1, x_2) \leq (y_1, y_2)$ genau dann, wenn $x_1 \leq y_1$ und $x_2 \leq y_2$. Dann ist $(\mathbb{Z}^2, +, \leq)$ eine geordnete abelsche Gruppe.
(ii) Auf $(\mathbb{Z}^2, +)$ definiere $(x_1, x_2) \leq (y_1, y_2)$ genau dann, wenn $x_1 < y_1$ oder $x_1 = y_1$ und $x_2 \leq y_2$; das ist die sogenannte lexikographische Ordnung.

Definition Sei K ein Körper und Γ eine linear geordnete abelsche Gruppe. Eine Abbildung $v : K \to \Gamma \cup \{\infty\}$ heißt *Krull-Bewertung*, falls :

1. v ist surjektiv,
2. $v(x) \in \Gamma$ für alle $x \neq 0$ und $v(0) = \infty$,
3. $v(xy) = v(x) + v(y)$ für alle $x, y \in K$ (mit den üblichen Rechenregeln für ∞)
4. $v(x + y) \geq \min\{v(x), v(y)\}$.

Die Gruppe Γ nennt man in diesem Fall die *Bewertungsgruppe* von v.

Bemerkungen (i) Für jede Krull-Bewertung v von K ist $A_v := \{x \in K \mid v(x) \geq 0\}$ ein Bewertungsring.
(ii) Für jede linear geordnete abelsche Gruppe Γ existiert ein Körper K mit einer Bewertung v, der Γ als Bewertungsgruppe hat ([siehe Kru32]

Man sagt zwei Krull-Bewertungen v_1, v_2 von K mit Bewertungsgruppen Γ_1, Γ_2 sind *äquivalent*, falls ein ordnugnserhaltender Isomorphismus $\iota : \Gamma_1 \to \Gamma_2$ (d.h $\alpha > \beta \Leftrightarrow \iota(\alpha) > \iota(\beta)$) existiert.

In Kapitel 1 haben wir bereits Bewertungsringe eingeführt und gezeigt, dass die *Bewertungsringe bezüglich diskreter und exponentieller Bewertungen* von K Bewertungsringe sind. Aber es existieren durchaus Bewertungsringe die nicht durch eine solche Bewertung induziert wurden. Durch die Verallgemeinerung auf Krull-Bewertungen erfassen wir jetzt auch solche komplizierteren Bewertungsringe.

Satz A.1.1 *Die Abbildung $v \to A_v$ induziert eine Bijektion von der Menge der Äquivalenzklassen von Krull-Bewertungen von K auf die Menge der Bewertungsringe von K.*

Beweis. [siehe End72, 7.1]

Sei $(L, w)|(K, v)$ eine Körpererweiterung von bewerteten Körpern mit Krull-Bewertungen v und w. Wir nennen w eine *Erweiterung* von v, falls der Bewertungsring von L bezüglich w eine Erweiterung des Bewertungsrings von K bezüglich v ist. Dabei ist ein Bewertungsring $B \subset L$ eine *Erweiterung* des Bewertungsringes $A \subset K$, falls

$$A = B \cap K \quad \text{und} \quad \mathfrak{m}_A = \mathfrak{m}_B \cap K,$$

wobei $\mathfrak{m}_A$ das maximale Ideal von A und $\mathfrak{m}_B$ das maximale Ideal von B bezeichnet.

A.2. Henselsche Körper

In diesem Kapitel geben wir einen Überblick über bewertete Henselsche Körper und eine Vielzahl ihrer charakteristischen Eigenschaften.

Definition Ein bewerteter Körper (K, v) mit einer Krull-Bewertung v heißt *henselsch*, falls v in jeder endlichen Körpererweiterung $L|K$ eine eindeutige Erweiterung w besitzt.

Die Henselschen Körper tragen nicht grundlos den Namen von Kurt Hensel, denn eine der charakterisierenden Eigenschaften dieser Objekte ist die Bedingung, dass das Lemma von Hensel erfüllt ist. Aber das ist nur eine von vielen äquivalenten Bedingungen und je nachdem welches Buch oder welche Veröffentlichung man zu dem Thema liest, findet man unterschiedliche - aber oft äquivalente - Definitionen. Unsere Definition verweist direkt auf die starke strukturelle Anforderung an solche Körper, wohingegen eine Definition mit Hilfe des Lemmas von Hensel fast schon unintuitiv wirkt. Dennoch zeigt die Äquivalenz dieser beiden Definitionen, wie leicht man diese starke Struktur auf K erreicht. Ein erster Schritt diese Definition greifbarer zu machen und die Vielzahl von zu untersuchenden Körpererweiterungen drastisch zu verringern, liefert uns:

Satz A.2.1 *Sei (K, v) ein bewerteter Körper. K ist genau dann henselsch, wenn v eine eindeutige Erweiterung in K_{sep} besitzt.*

Beweis. [siehe EP05]

Nun wollen wir uns mit den gängigsten Äquivalenzen von Definition A.2.1 auseinandersetzen. Dabei wird man sich auf den ersten Blick an vielen Stellen vielleicht wundern, wie es sein kann, dass man mit dieser Bedingung einem Körper K eine solche Struktur aufzwingt. Zusätzlich wird der Leser, der das erste Mal mit henselschen Körpern konfrontiert wird, eventuell erschlagen von der Vielfalt der hier aufgeführten Äquivalenzen; doch das sollte klarmachen, welches Interesse an diesen Objekten besteht und welchen Stellenwert die henselschen Körper in der Mathematik haben.

Satz A.2.2 *Sei (K, v) ein bewerteter Körper mit Bewertungsring $(A, \mathfrak{m})$, dabei bezeichnet $\mathfrak{m}$ das maximale Ideal von A. Es bezeichne $k := A/\mathfrak{m}$ den Restklassenkörper und $\bar{}: A \to k$ die kanonische Restklassenabbildung. Die folgenden Aussagen sind äquivalent:*

1. *K ist henselsch.*
2. *Ist $f = 1 + X + X^2 g(X)$, mit $g(X) \in \mathfrak{m}[X]$, so besitzt f eine Nullstelle $a \in A$ mit $\bar{a} = -1$*
3. *Sei $f = X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0 \in A[X]$ ein unitäres Polynom mit $\bar{c}_{n-1} \neq 0$ und $\bar{c}_{n-2} = \cdots = \bar{c}_0 = 0$. Dann spaltet in $A[X]$ ein linearer Faktor $X + c$ ab, mit $\bar{c} = \bar{c}_{n-1}$.*
4. *Sei $f \in A[X]$ ein unitäres Polynom. Hat $\bar{f}$ eine einfache Nullstelle $\bar{b} \in k$ so hat f eine Nullstelle $a \in A$, sodas $\bar{a} = \bar{b}$.*
5. *Sei $f \in A[X]$. Existiert ein $b \in A$ mit $vf(b) > 0$ und $vf'(b) = 0$, so hat f eine Nullstelle $a \in A$, sodass $\bar{a} = \bar{b}$.*
6. *Sei $f \in A[X]$. Existiert ein $b \in A$ mit $vf(b) > 2vf'(b)$, so besitzt f eine Nullstelle $a \in A$, sodass $v(a - b) > vf'(b)$.*
7. *Sei $f \in A[X]$. Hat $\bar{f} = \bar{g}\bar{h}$ in $k[X]$ eine Faktorisierung in zwei relativ teilerfremde Polynome aus $k[X]$, existeren in den Urbildern von $\bar{g}$ bzw. $\bar{h}$ Polynome $g, h \in A[X]$, sodass $f = gh$ und deg(g)=deg($\bar{g}$).*
8. *Es existiert mindestens eine Fortsetzung von v auf K_{sep} (die wir auch v nennen) und für jede Fortsetzung gilt für jedes Element $a \in K_{sep}$ die folgende Aussage: Es sei $b \in K_{sep} \setminus K$ so, dass*

$$v(a - b) > \max\{v(a - \sigma(a)) \mid \sigma \in K \text{ mit } \sigma(a) \neq a\},$$

   dann ist $a \in K(b)$. Insbesondere gilt $K(a) \subset K(b)$.
9. *Sei $f \in A[X]$. Existiert ein $b \in K$ mit $vf(b) > v\,\mathrm{discr} f$, so besitzt f eine Nullstelle in K.*
10. *Sei $f \in A[X]$ irreduzibel, so ist $\bar{f}$ eine Potenz eines irreduziblen Polynoms in $k[X]$; d.h es existiert ein $\bar{g} \in k[X]$, sodass $\bar{f} = \bar{g}^s$ für ein $s \in \mathbb{N}$.*

Im Hauptteil der Arbeit haben wir für vollständige bewertete Körper die Eigenschaften 1.,5. und 7. gezeigt, also handelt es sich bei diesen Körpern insbesondere um Henselsche Körper.

Aber man sieht sofort, dass nicht alle henselschen Körper vollständig sein müssen; so hat zum Beispiel Ribenboim das Lemma von Hensel für sphärisch vollständige Körper gezeigt, indem er auf eine, von ihm formulierte, Version des Banachschen Fixpunktsatzes für sphärisch vollständige Räume zurückgriff. Damit ist die Klasse der henselschen Körper immernoch nicht ausgeschöpft, aber das soll nicht Gegenstand dieser Arbeit sein.

Zum Schluss noch Folgendes: Nakayama zeigte, dass für jeden bewerteten Körper K ein kleinster Erweiterungskörper K^h existiert, der henselsch ist. Dieser ist bis auf Isomorphie eindeutig bestimmt. Den Körper K^h nennt man die Henselisierung von K.
Für diskret oder exponentiell bewertete Körper ist das keine große Überraschung, weil wir schon wissen, dass die Vervollständigung dieser Körper henselsch ist, und man ganz sicher einen kleinsten solchen Körper in der Vervollständigung findet, aber für Krull-bewertete Körper, die nicht mehr so einfach zu 'vervollständigen' sind - und deren Vervollständigung in vielen Fällen gar nicht henselsch ist - liefert uns die Henselisierung eine sinnvolle Alternative zur Vervollständigung [1].

[1] Die Vervollständigung erfolgt über Filter und hat nicht mehr viel mit dem zu tun was wir in dieser Arbeit behandelt haben.

Literaturverzeichnis

[Bou89] N. Bourbaki. *Commutative Algebra: Chapters 1-7*. Elements of Mathematics: Commutative Algebra, Chapters 1-7. Springer, 1989.

[Cla13] Pete L. Clark. Chapter 3: The Fundamental In/Equality, Hensel and Krasner. `http://www.math.uga.edu/~pete/MATH8410.html`, Sept 2013.

[CR99] Patrick Cegielski and Denis Richard. On arithmetical first-order theories allowing encoding and decoding of lists. *Theoretical Computer Science*, 222(1–2):55 – 75, 1999.

[End72] O. Endler. *Valuation theory*. Universitext (1979). Springer-Verlag, 1972.

[EP05] A.J. Engler and A. Prestel. *Valued Fields*. Springer monographs in mathematics. Springer, 2005.

[Fis97] Benji Fisher. A note on Hensel's Lemma in several variables. *Proceedings of the American Mathematical Society*, 125(11):3185–3189, 1997.

[Gek13] E.-U. Gekeler. Mtischift zur Vorlesung: Algebraische Zahlentheorie I an der Universität des Saarlandes, WS 2012/13.

[Hen08] K. Hensel. *Theorie der algebraischen Zahlen*. Number v. 1 in Cornell University Library historical math monographs. B. G. Teubner, 1908.

[Kru32] Wolfgang Krull. Allgemeine Bewertungstheorie. *Journal für die reine und angewandte Mathematik*, 167:160–196, 1932.

[Kuh11] Fraz-Viktor Kuhlmann. Maps on ultrametric spaces, hensel's lemma, and differential equations over valued fields. *Communications in Algebra*, 39:1730–1776, 2011.

[Kuh13] Franz-Viktor Kuhlmann. Chapter 9: Hensel's Lemma. `http://math.usask.ca/~fvk/Fvkbook.htm`, Sept 2013.

[Lan02] S. Lang. *Algebra*. Graduate texts in mathematics. Springer, 2002.

[Rob00] A. Robert. *A Course in P-adic Analysis*. Graduate Texts in Mathematics. Springer, 2000.

[RPC00] P. Ribenboim and S. Priess-Crampe. A general Hensel's Lemma. *Journal of Algebra*, 232:269–281, 2000.