1. Eine funktionentheoretische Sichtweise der ganzen und der rationalen Zahlen

Vereinbarung. In dieser Vorlesung sei ein Ring stets ein kommutativer Ring mit Einselement. Für einen Ringhomomorphismus $\phi : A \to B$ gelte $\phi(1) = 1$. Ist B ein Ring und $A \subset B$ ein Unterring, so enthalte A das Einselement von B.

1.1. Definition. Sei A ein Ring. Dann versteht man unter dem *Spektrum* von A die Menge aller Primideale von A. Das *Maximalspektrum* von A ist die Menge aller maximalen Ideale von A.

Bezeichnung. Wir bezeichnen mit $\mathrm{Spec}(A)$ das Spektrum und mit $\mathrm{Specm}(A)$ das Maximalspektrum des Ringes A. Da jedes maximale Ideal prim ist, gilt $\mathrm{Specm}(A) \subset \mathrm{Spec}(A)$.

Beispiele. a) In einem Hauptidealring A sind bekanntlich die Primideale außer dem Nullideal (0) genau die von Primelementen $p \in A$ erzeugten Hauptideale (p). Diese Ideale sind sogar maximal. Deshalb gilt für jeden Hauptidealring A

$$\mathrm{Spec}(A) = \mathrm{Specm}(A) \cup \{(0)\}.$$

b) Sei speziell $A := \mathbb{Z}$ der Ring der ganzen Zahlen und

$$\mathbb{P} := \{2, 3, 5, 7, 11, 13, 17, \ldots\}$$

die Menge aller Primzahlen. Damit hat man eine bijektive Abbildung

$$\mathbb{P} \xrightarrow{\sim} \mathrm{Specm}(\mathbb{Z}), \quad p \mapsto (p).$$

c) Sei $A = k[X]$ der Ring aller Polynome in einer Unbestimmten X mit Koeffizienten aus einem algebraisch abgeschlossenen Körper k (z.B. $k = \mathbb{C}$). Dann sind die Primelemente von $k[X]$ die linearen Polynome und man bekommt eine bijektive Abbildung

$$k \xrightarrow{\sim} \mathrm{Specm}(k[X]), \quad a \mapsto (X - a).$$

Ist der Körper k nicht algebraisch abgeschlossen, so hat man immer noch eine injektive Abbildung $k \to \mathrm{Specm}(k[X])$, die aber nicht mehr surjektiv ist. Für den Ring $\mathbb{R}[X]$ kann man z.B. zeigen, dass man eine natürliche surjektive Abbildung

$$\mathbb{C} \longrightarrow \mathrm{Specm}(\mathbb{R}[X]), \quad a \mapsto \mathfrak{m}_a := \{f(X) \in \mathbb{R}[X] : f(a) = 0\},$$

hat, bei der jeweis zwei konjugiert komplexe Zahlen dasselbe Bild haben.

d) Es gibt auch Ringe, für die das Spektrum viel größer als das Maximalspektrum ist. Sei etwa $A := k[X_1, \ldots, X_n]$ der Polynomring in $n \geqslant 2$ Unbestimmten über einem algebraisch abeschlossenen Körper k. Für einen Punkt $a = (a_1, \ldots, a_n) \in k^n$ ist

$$\mathfrak{m}_a := \{f \in k[X_1, \ldots, X_n] : f(a) = 0\}$$

ein maximales Ideal. Aus dem sog. Hilbertschen Nullstellensatz folgt, dass die Abbildung

$$k^n \longrightarrow \mathrm{Specm}(k[X_1, \ldots, X_n]), \quad a \mapsto \mathfrak{m}_a\,,$$

bijektiv ist. Es gibt aber noch viele andere Primideale. Z.B. ist das von einem beliebigen irreduziblen Polynom $f(X_1, \ldots, X_n)$ erzeugte Hauptideal ein Primideal, das aber nicht maximal ist.

1.2. Definition. Sei A ein Ring und $\mathfrak{p} \in \mathrm{Specm}(A)$ ein maximales Ideal. Dann heißt der Körper

$$\kappa(\mathfrak{p}) := A/\mathfrak{p}$$

der *Restklassenkörper* von A an der *Stelle* $\mathfrak{p}$.

Man hat die natürliche Quotientenabbildung

$$\mathrm{eval}_\mathfrak{p} : A \to \kappa(\mathfrak{p}), \quad f \mapsto f \bmod \mathfrak{p}$$

Nach Definition gilt $\mathrm{Ker}(\mathrm{eval}_\mathfrak{p}) = \mathfrak{p}$, also ist $\mathrm{eval}_\mathfrak{p}(f) = 0$ genau dann, wenn $f \in \mathfrak{p}$.

Man interpretiert $\mathrm{eval}_\mathfrak{p}(f)$ als den Funktionswert des Elementes $f \in A$ an der Stelle $\mathfrak{p}$ und schreibt manchmal auch suggestiv $f(\mathfrak{p})$ für $\mathrm{eval}_\mathfrak{p}(f)$.

Diese Interpretation wird nahegelegt durch das erste der folgenden

Beispiele:

a) Sei $A := k[X]$ der Polynomring in einer Unbestimmten X über einem algebraisch abgeschlossenen Körper k. Für $a \in k$ sei $\mathfrak{m}_a$ das von $X - a$ erzeugte Hauptideal. Wie bereits in 1.1, Beispiel c) gesagt, entstehen so alle maximalen Ideale von A und man hat somit eine bijektive Beziehung $k \to \mathrm{Specm}(A)$, $a \mapsto \mathfrak{m}_a$. Daher kann man $\mathrm{Spec}(A)$ mit k identifizieren. Man hat eine kanonische Isomorphie

$$\kappa(\mathfrak{m}_a) = k[X]/(X - a) \cong k,$$

denn das Hauptideal $(X - a) \subset k[X]$ besteht aus allen Polynomen, die die Nullstelle $a \in k$ haben, also ist jedes Polynom $f(X)$ modulo $(X - a)$ zum konstanten Polynom mit dem Wert $f(a) \in k$ äquivalent. Die Abbildung

$$\mathrm{eval}_a := \mathrm{eval}_{\mathfrak{m}_a} : k[X] \longrightarrow \kappa(\mathfrak{m}_a) = k$$

wird hier gegeben durch $\mathrm{eval}_a(f) = f(a)$, ist also die gewöhnliche Auswertung des Polynoms f an der Stelle a.

b) Für den Ring $\mathbb{Z}$ der ganzen Zahlen besteht $\mathrm{Specm}(\mathbb{Z})$ genau aus allen von den Primzahlen $p \in \mathbb{P}$ erzeugten Hauptidealen $(p) \subset \mathbb{Z}$ und man hat die Isomorphie

$$\kappa(p) = \mathbb{Z}/(p) \cong \mathbb{F}_p,$$

wobei $\mathbb{F}_p$ den endlichen Körper mit p Elementen bezeichnet. In diesem Fall ist also

$$\mathrm{eval}_p : \mathbb{Z} \to \mathbb{F}_p, \qquad x \mapsto \mathrm{eval}_p(x) := (x \bmod p) \in \mathbb{F}_p$$

die Abbildung, die einer ganzen Zahl $x \in \mathbb{Z}$ ihre Restklasse modulo p zuordnet.

Eine ganze Zahl $x \in \mathbb{Z}$ liefert somit eine Funktion auf dem Maximalspektrum $\mathrm{Specm}(\mathbb{Z})$, wobei der Wert $x(p)$ an der Stelle $(p) \in \mathrm{Specm}(\mathbb{Z})$ im Körper $\mathbb{F}_p$ liegt.

1.3. Jacobson-Radikal. Wir untersuchen jetzt die Frage, ob jedes Element $x \in A$ eines Ringes durch seine Funktionswerte $\mathrm{eval}_{\mathfrak{m}}(x) \in \kappa(\mathfrak{m})$, $\mathfrak{m} \in \mathrm{Specm}(A)$, eindeutig bestimmt ist. Dies ist offenbar äquivalent damit, dass der Ring-Homomorphismus

$$\phi : A \to \prod_{\mathfrak{m} \in \mathrm{Specm}(A)} A/\mathfrak{m}, \qquad x \mapsto (\mathrm{eval}_{\mathfrak{m}}(x))_{\mathfrak{m} \in \mathrm{Specm}(A)}$$

injektiv ist. Dazu ist folgender Begriff nützlich.

Definition. Unter dem *Jacobson-Radikal* eines Ringes A versteht man den Durchschnitt aller seiner maximalen Ideale, in Zeichen

$$\mathfrak{j}(A) := \bigcap_{\mathfrak{m} \in \mathrm{Specm}(A)} \mathfrak{m}\,.$$

Damit gilt $\mathrm{Ker}(\phi) = \mathfrak{j}(A)$. Also sind genau dann alle Elemente eines Rings A durch ihre Funktionswerte auf dem Maximalspektrum von A eindeutig bestimmt, wenn das Jacobson-Radikal von A verschwindet. Für den Ring $\mathbb{Z}$ der ganzen Zahlen ist dies der Fall:

Behauptung. $\mathfrak{j}(\mathbb{Z}) = (0)$.

Beweis. Angenommen, dies sei nicht der Fall. Dann gibt es eine ganze Zahl x mit $0 \neq x \in \mathfrak{j}(\mathbb{Z})$. Wir können annehmen, dass $x > 0$ (andernfalls ersetze man x durch $-x$). Dann ist

$$z := 1 + x \geqslant 2,$$

also keine Einheit von $\mathbb{Z}$ und daher in mindestens einem maximalen Ideal $\mathfrak{m}$ enthalten. (Da die maximalen Ideale von $\mathbb{Z}$ genau die durch Primzahlen erzeugten Hauptideale

(p) sind, heißt dies einfach, dass z durch wenigstens eine Primzahl teilbar ist.) Da nach Voraussetzung ebenfalls $x \in \mathfrak{m}$, würde daraus wegen $1 = z - x$ folgen $1 \in \mathfrak{m}$, Widerspruch! Damit ist die Behauptung bewiesen.

Aus $\mathfrak{j}(\mathbb{Z}) = (0)$ folgt nun, dass die Abbildung

$$\phi : \mathbb{Z} \to \prod_{p \in \mathbb{P}} \mathbb{F}_p \qquad (\mathbb{P} \text{ Menge aller Primzahlen})$$

injektiv ist. Da alle $\mathbb{F}_p$ endlich, aber $\mathbb{Z}$ unendlich ist, ergibt sich hieraus ein weiterer Beweis dafür, dass es unendlich viele Primzahlen gibt.

1.4. Definition. Unter einem *lokalen Ring* versteht man einen Ring A, der ein einziges maximales Ideal $\mathfrak{m} \subset A$ besitzt. Der Körper $\kappa := A/\mathfrak{m}$ heißt der Restklassenkörper des lokalen Rings.

In einem lokalen Ring A ist jedes Element im Komplement des maximalen Ideals invertierbar. Denn wäre $t \in A \setminus \mathfrak{m}$ nicht invertierbar, so wäre das Hauptideal $At \subsetneqq A$ in einem maximalen Ideal $\mathfrak{m}_1$ enthalten und $\mathfrak{m}_1 \neq \mathfrak{m}$, Widerspruch!
Umgekehrt gilt: Ist A ein Ring und $\mathfrak{m} \subsetneqq A$ ein echtes Ideal, so dass alle Elemente von $A \setminus \mathfrak{m}$ invertierbar sind, so ist $\mathfrak{m}$ das einzige maximale Ideal, also A ein lokaler Ring.

Ein typisches *Beispiel* eines lokalen Rings ist der Ring $\mathbb{C}\{z\}$ aller komplexen Potenzreihen

$$f(z) = \sum_{n=0}^{\infty} c_n z^n, \quad c_n \in \mathbb{C},$$

mit positivem Konvergenzradius, der aber von f abhängen kann. Jede solche Potenzeihe stellt eine in einer gewissen Umgebung des Nullpunkts $0 \in \mathbb{C}$ holomorphe Funktion dar. Das maximale Ideal $\mathfrak{m} \subset \mathbb{C}\{z\}$ besteht aus allen Funktionen mit $f(0) = 0$. Jede Funktion $f \in \mathbb{C}\{z\} \setminus \mathfrak{m}$, d.h. $f(0) \neq 0$, ist in einer gewissen Umgebung des Nullpunkts ungleich 0, also ist $1/f(z)$ dort holomorph und kann in eine Potenzreihe entwickelt werden, die zu $\mathbb{C}\{z\}$ gehört.

Weitere Beispiele lokaler Ringe erhält man durch den Prozess der Lokalisierung, den wir als nächstes besprechen.

1.5. Lokalisierung. Sei A ein Integritätsbereich, d.h. ein nullteilerfreier kommutativer Ring mit Einselement $1 \neq 0$. Dann ist der Quotientenkörper $K := \mathrm{Quot}(A)$ definiert. Für ein Primideal $\mathfrak{p} \in \mathrm{Spec}(A)$ ist die *Lokalisierung* von A an der Stelle $\mathfrak{p}$ definiert als

$$A_{\mathfrak{p}} := \Big\{ \frac{x}{s} \in K : x \in A,\ s \in A \setminus \mathfrak{p} \Big\}.$$

Es ist leicht nachzurechnen, dass $A_{\mathfrak{p}}$ ein Unterring von K mit $A \subset A_{\mathfrak{p}}$ ist.

Wir bezeichnen mit $\mathfrak{p}A_\mathfrak{p}$ das von $\mathfrak{p}$ erzeugte Ideal im Ring $A_\mathfrak{p}$. Es gilt

$$\mathfrak{p}A_\mathfrak{p} := \left\{\frac{p}{s} : p \in \mathfrak{p},\ s \in A \setminus \mathfrak{p}\right\}.$$

Das Komplement $A_\mathfrak{p} \setminus \mathfrak{p}A_\mathfrak{p} = \{t/s : t, s \in A \setminus \mathfrak{p}\}$ besteht aus allen invertierbaren Elementen von $A_\mathfrak{p}$. Daraus folgt, dass $\mathfrak{p}A_\mathfrak{p}$ ein maximales Ideal ist, und zwar das einzige maximale Ideal von $A_\mathfrak{p}$. Also ist $A_\mathfrak{p}$ ein lokaler Ring.

Beispiele:

a) Ein typisches Beispiel wird geliefert durch den Polynomring $A := k[X]$ über einem Körper k. Der Quotientenkörper von A ist dann der Körper $k(X)$ aller rationalen Funktionen in der Unbestimmten X. Für einen Punkt $a \in k$ sei $\mathfrak{m}_a := (X - a) \subset k[X]$ das maximale Ideal aller durch den Linearfaktor $X - a$ teilbaren Polynome, d.h. aller Polynome $f(X) \in k[X]$ mit $f(a) = 0$. Die Lokalisierung $A_{\mathfrak{m}_a}$ besteht dann aus allen rationalen Funktionen

$$F(X) = \frac{g(X)}{f(X)}, \qquad f(X), g(X) \in k[X], \quad f(a) \neq 0,$$

d.h. allen rationalen Funktionen, die in a keinen Pol haben. Der Wert $F(a) \in k$ ist also wohldefiniert.

b) Für den Ring $\mathbb{Z}$ der ganzen Zahlen und das durch eine Primzahl p erzeugte maximale Ideal $(p) \subset \mathbb{Z}$ besteht die Lokalisierung

$$\mathbb{Z}_{(p)} = \left\{\frac{n}{s} \in \mathbb{Q} : n, s \in \mathbb{Z},\ p \nmid s\right\}$$

aus allen rationalen Zahlen, deren Nenner nicht durch p teilbar ist.

1.6. Satz. *Sei A ein Integritätsbereich und $\mathfrak{m} \in \mathrm{Specm}(A)$ ein maximales Ideal. Dann ist die durch die Inklusion $A \subset A_\mathfrak{m}$ induzierte Abbildung*

$$\phi : A/\mathfrak{m} \longrightarrow A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$$

ein Isomorphismus.

Beweis. Die Injektivität folgt daraus, dass ϕ ein Homomorphismus zwischen Körpern ist.

Zur Surjektivität. Sei $z \in A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$ repräsentiert durch $x/s \in A_\mathfrak{m}$, ($x \in A$, $s \in A \setminus \mathfrak{m}$). Das Element s ist invertierbar modulo $\mathfrak{m}$, es gibt also ein $t \in A$ mit $st = 1 + \xi$, $\xi \in \mathfrak{m}$. Daher ist $(st)(x/s) = (tx)/1$ modulo $\mathfrak{m}A_\mathfrak{m}$ zu x/s äquivalent, repräsentiert also ebenfalls z. Es folgt, dass z das Bild unter ϕ des Elements $(tx \bmod \mathfrak{m}) \in A/\mathfrak{m}$ ist, q.e.d.

Bemerkung. Der Satz bedeutet, dass sich die in 1.2 definierte Abbildung

$$\mathrm{eval}_\mathfrak{m} : A \ \to\ \kappa(\mathfrak{m}) = A/\mathfrak{m}$$

auf die Lokalisierung $A_{\mathfrak{m}} \supset A$ fortsetzen lässt. Die Fortsetzung werde wieder mit

$$\mathrm{eval}_{\mathfrak{m}} : A_{\mathfrak{m}} \to \kappa(\mathfrak{m})$$

bezeichnet.

1.7. Satz (p-adische Entwicklung). *Sei p eine Primzahl. Dann gibt es zu jedem Element $x \in \mathbb{Z}_{(p)}$ eine eindeutig bestimmte Folge von Zahlen $a_n \in \{0, 1, \ldots, p-1\}$, $n \geqslant 0$, so dass*

$$x - \sum_{n=0}^{N} a_n p^n \ \in \ (p)^{N+1} \quad \textit{für alle } N \geqslant 0. \tag{1}$$

Hier ist (p) das von p erzeugte (maximale) Ideal in $\mathbb{Z}_{(p)}$. Es ist $(p)^{N+1} = (p^{N+1})$.
Statt (1) schreibt man auch

$$x = \sum_{n=0}^{\infty} a_n p^n \tag{2}$$

Dies ist zunächst nur als Abkürzung für (1) zu verstehen. Führt man jedoch auf $\mathbb{Z}_{(p)}$ eine Topologie ein, bei der die Mengen $x + (p)^N$, $N \geqslant 0$, eine Umgebungsbasis des Punktes $x \in \mathbb{Z}_{(p)}$ bilden, so konvergiert die unendliche Reihe (d.h. die Folge der Partialsummen) tatsächlich gegen x. Wir werden auf diese Topologie später noch zurückkommen.

Beweis. a) Wir zeigen zunächst die Existenz der Reihen-Entwicklung durch Induktion nach N.
Für den *Induktionsanfang* $N = 0$ betrachten wir das Bild $\overline{x} \in \mathbb{F}_p$ von x unter der Abbildung $\mathbb{Z}_{(p)} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$. Das Körperelement $\overline{x} \in \mathbb{F}_p$ wird durch eine ganze Zahl $a_0 \in \{0, 1, \ldots, p-1\}$ repräsentiert, d.h. es gilt $x - a_0 \in (p)$.

Induktionsschritt $N-1 \to N$. Nach Induktions-Voraussetzung ist $x - \sum_{n=0}^{N-1} a_n p^n \in (p)^N$, d.h.

$$x - \sum_{n=0}^{N-1} a_n p^n = \xi_N p^N \quad \text{mit } \xi_N \in \mathbb{Z}_{(p)}.$$

Nach dem Induktionsanfang gibt es ein $a_N \in \{0, 1, \ldots, p-1\}$ mit $\xi_N - a_N \in (p)$, also $\xi_N p^N - a_N p^N \in (p)^{N+1}$. Daraus folgt

$$x - \sum_{n=0}^{N} a_n p^n \in (p)^{N+1}, \qquad \text{q.e.d.}$$

b) *Zur Eindeutigkeit.* Sei $x = \sum_{n=0}^{\infty} b_n p^n$ eine zweite Entwicklung von x und m der kleinste Index mit $a_m \neq b_m$. Dann gilt

$$(a_m - b_m)\, p^m \ \in \ (p)^{m+1}.$$

Daraus folgt $a_m \equiv b_m \bmod p$. Da $a_m, b_m \in \{0, 1, \ldots, p-1\}$, ist dies nur möglich, wenn $a_m = b_m$, Widerspruch!

Beispiele

a) Für eine positive ganze Zahl $x \in \mathbb{Z} \subset \mathbb{Z}_{(p)}$ hat man die schon aus der Elementar-Mathematik bekannte abbrechende p-adische Entwicklung

$$x = a_0 + a_1 p + \ldots + a_n p^n, \qquad a_\nu \in \{0, 1, \ldots, p-1\}.$$

Dabei ist n die kleinste natürliche Zahl mit $x < p^{n+1}$.

b) Schon für die Zahl -1 bricht die p-adische Entwicklung nicht ab. Es gilt nämlich

$$-1 = \sum_{n=0}^{\infty} (p-1) p^n.$$

Dies beweist man so: Da $\sum_{\nu=0}^{n} p^\nu = (1 - p^{n+1})/(1-p)$, gilt für die n-te Partialsumme

$$x_n := \sum_{\nu=0}^{n} (p-1) p^\nu = -(1 - p^{n+1}), \quad \text{also} \quad -1 - x_n \in (p)^{n+1}, \quad \text{q.e.d.}$$

c) Als weiteres Beispiel berechnen wir die 5-adische Entwicklung der rationalen Zahl $x := 1/3 \in \mathbb{Z}_{(5)}$. Nach dem Beweis von Satz 1.7 hat man zuerst das Bild $\overline{x}$ von x unter der Abbildung $\mathbb{Z}_{(5)} \to \mathbb{Z}_{(5)}/5\mathbb{Z}_{(5)} \cong \mathbb{F}_5$ zu bestimmen. Da das Inverse von $3 \in \mathbb{F}_5$ gleich 2 ist, ist $\overline{x} = 2$, also ist der 0-te Koeffizient der 5-adischen Entwicklung $a_0 = 2$. In der Tat ist

$$x - a_0 = \frac{1}{3} - 2 = \frac{1-6}{3} = -\frac{1}{3} \cdot 5 \ \in \ 5\mathbb{Z}_{(5)}.$$

Als nächstes hat man das Bild von $\xi_1 := -1/3$ in $\mathbb{F}_5$ zu betrachten. Dies ist das Negative des Bildes von $1/3$ also $\overline{\xi}_1 = 3$. Deswegen ist $a_1 = 3$. Da $-1/3 - 3 = -10/3 = -(2/3) \cdot 5$, folgt

$$x - a_0 - a_1 \cdot 5 = -\frac{2}{3} \cdot 5^2 \ \in \ 5^2\mathbb{Z}_{(5)}.$$

Das Bild von $\xi_2 := -2/3$ in $\mathbb{F}_5$ ist $\overline{\xi}_2 = 2\overline{\xi}_1 \equiv 6 \equiv 1 \bmod 5$, also $a_2 = 1$. Wegen $-2/3 - 1 = -5/3 = -1/3 \cdot 5$, folgt

$$x - a_0 - a_1 \cdot 5 - a_2 \cdot 5^2 = -\frac{1}{3} \cdot 5^3 \ \in \ 5^3\mathbb{Z}_{(5)}.$$

Da $\xi_3 := -1/3 = \xi_1$, sieht man, dass sich von jetzt ab die Entwicklung wiederholt, d.h. $a_{m+2} = a_m$ für alle $m \geqslant 1$, also

$$\frac{1}{3} = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + 1 \cdot 5^6 + \dots$$

Man kann beweisen (Übung!), dass die p-adische Entwicklung jeder rationalen Zahl $x \in \mathbb{Z}_{(p)}$ periodisch wird.

1.8. Definition. Ein *diskreter Bewertungsring* ist ein Hauptidealring A mit genau einem maximalen Ideal $\mathfrak{m} \neq (0)$.

Da A Hauptidealring ist, wird das maximale Ideal von einem Primelement erzeugt, $\mathfrak{m} = (\pi)$. Dieses Primelement π ist dann bis auf Multiplikation mit einer Einheit das einzige Primelement von A. Jedes Element $x \in A$, $x \neq 0$, lässt sich schreiben als

$$x = u\pi^n, \quad \text{mit einer Einheit } u \in A^* \text{ und } n \in \mathbb{Z},\ n \geqslant 0.$$

Man setzt $\mathrm{ord}_\pi(x) := n$. Die Funktion

$$v := \mathrm{ord}_\pi : A \setminus \{0\} \to \mathbb{Z}$$

ist eine sog. *Bewertung*, d.h. es gilt

(i) $v(xy) = v(x) + v(y)$ für alle $x, y \in A \setminus \{0\}$,

(ii) $v(x+y) \geqslant \min(v(x), v(y))$ für alle $x, y \in A \setminus \{0\}$, $x + y \neq 0$.

Dies erklärt den Namen Bewertungsring.

Beispiele

a) Für jede Primzahl p ist $\mathbb{Z}_{(p)}$ ein diskreter Bewertungsring.

b) Sei allgemeiner R ein Hauptidealring und $\pi \in R$ ein Primelement. Dann ist die Lokalisierung $R_{(\pi)}$ ein diskreter Bewertungsring. Sei etwa $R := k[X]$ der Polynomring in einer Unbestimmten über einem Körper k und $a \in k$. Dann ist $X - a$ ein Primelement, also die Lokalisierung

$$A := k[X]_{(X-a)}$$

ein diskreter Bewertungsring. A besteht aus allen rationalen Funktionen $F(X) \in k(X)$, die in a keinen Pol haben. Die Bewertung $v(F)$ ist in diesem Fall die Nullstellenordnung der Funktion F im Punkt a.

c) Der Ring $\mathbb{C}\{z\}$ aller konvergenten Potenzreihen in z mit komplexen Koeffizienten ist ebenfalls ein diskreter Bewertungsring.

Der Satz 1.7 kann auf beliebige diskrete Bewertungsringe verallgemeinert werden.

1.9. Satz. *Sei A ein diskreter Bewertungsring mit maximalem Ideal (π). Sei $\mathfrak{R} \subset A$ ein Repräsentantensystem für den Restklassenkörper $\kappa := A/(\pi)$, d.h. durch die kanonische Quotientenabbildung $A \to \kappa$ wird $\mathfrak{R}$ bijektiv auf κ abgebildet. Dann gibt es zu jedem $x \in A$ eine eindeutig bestimmte Folge von Elementen $a_n \in \mathfrak{R}$, $n \geqslant 0$, so dass*

$$x - \sum_{n=0}^{N} a_n \pi^n \ \in \ (\pi)^{N+1} \quad \textit{für alle } N \geqslant 0.$$

Man schreibt hierfür wieder $x = \sum_{n=0}^{\infty} a_n \pi^n$.

Der *Beweis* kann fast wörtlich von Satz 1.7 übernommen werden.

1.10. Vervollständigung. Sei A ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = (\pi)$. Wir führen auf A die Topologie ein, für welche die Mengen

$$U_N(a) := a + \mathfrak{m}^N, \quad N \geqslant 0,$$

eine Umgebungsbasis des Punktes $a \in A$ bilden. Dies ist die sog. $\mathfrak{m}$-*adische Topologie* auf A. Da

$$\bigcap_{N=0}^{\infty} \mathfrak{m}^N = \bigcap_{N=0}^{\infty} (\pi^N) = (0),$$

ist diese Topologie Hausdorffsch. Eine Folge $(x_n)_{n\in\mathbb{N}}$ von Elementen $x_n \in A$ konvergiert genau dann gegen $a \in A$, wenn zu jedem $N \in \mathbb{N}$ ein $n_0 \in \mathbb{N}$ existiert, so dass

$$x_n - a \ \in \ \mathfrak{m}^N \qquad \text{für alle } n \geqslant n_0.$$

Eine Folge $(x_n)_{n\in\mathbb{N}}$ heißt *Cauchyfolge*, falls zu jedem $N \in \mathbb{N}$ ein $n_0 \in \mathbb{N}$ existiert, so dass

$$x_n - x_m \ \in \ \mathfrak{m}^N \qquad \text{für alle } n, m \geqslant n_0.$$

Z.B. ist jede Potenzreihe

$$\sum_{n=0}^{\infty} a_n \pi^n, \qquad a_n \in A,$$

d.h. die Folge der Partialsummen $x_n := \sum_{\nu=0}^{n} a_\nu \pi^\nu$, $n \geqslant 0$, eine Cauchyfolge, da für alle $n \geqslant m \geqslant N$ gilt

$$x_n - x_m = \sum_{\nu=m+1}^{n} a_\nu \pi^\nu \in (\pi)^N.$$

Jede konvergente Folge ist eine Cauchyfolge, die Umkehrung gilt aber im Allgemeinen nicht. Falls jede Cauchyfolge in A konvergiert, heißt A vollständig.

Ist A nicht vollständig, so kann man eine *Vervollständigung* $\widehat{A} \supset A$ auf folgende Weise konstruieren:
Sei $\mathrm{Cauchy}(A)$ die Menge aller Cauchyfolgen $(x_n)_{n\in\mathbb{N}}$ in A. Bzgl. komponentenweiser Addition und Multiplikation ist $\mathrm{Cauchy}(A)$ ein Ring. Sei $\mathrm{Null}(A)$ die Menge aller Nullfolgen in A. Natürlich gilt $\mathrm{Null}(A) \subset \mathrm{Cauchy}(A)$ und man prüft leicht nach, dass $\mathrm{Null}(A)$ ein Ideal von $\mathrm{Cauchy}(A)$, ja sogar ein Primideal ist. Dann definiert man

$$\widehat{A} := \mathrm{Cauchy}(A)/\mathrm{Null}(A).$$

Ordnet man jedem Ringelement $x \in A$ die Restklasse der konstanten Folge

$$(x, x, x, \ldots) \in \mathrm{Cauchy}(A)$$

zu, so erhält man eine injektive Abbildung $A \to \widehat{A}$ und man identifiziert A mit seinem Bild in $\widehat{A}$. Für eine konkrete Darstellung der Elemente von $\widehat{A}$ ist folgendes Lemma nützlich.

1.11. Lemma. *Sei A ein diskreter Bewertungsring mit maximalem Ideal (π) und $\mathfrak{R} \subset A$ ein Repräsentantensystem des Restklassenkörpers $\kappa = A/(\pi)$. Dann gibt es zu jeder Cauchyfolge $(x_n)_{n\in\mathbb{N}} \in \mathrm{Cauchy}(A)$ eine eindeutig bestimmte unendliche Reihe*

$$\sum_{n=0}^{\infty} a_n \pi^n, \quad a_n \in \mathfrak{R},$$

die zur Cauchyfolge (x_n) äquivalent ist, d.h. die Folge der Partialsummen $\left(\sum_{\nu=0}^{n} a_\nu \pi^\nu\right)_{n\in\mathbb{N}}$ unterscheidet sich von der gegebenen Cauchyfolge nur um eine Nullfolge.

Beweis. a) *Existenz.* Da (x_n) eine Cauchyfolge ist, gibt es zu jedem $n \geqslant 0$ ein ν_n, so dass $x_\ell - x_m \in (\pi)^{n+1}$ für alle $\ell, m \geqslant \nu_n$. Da die Cauchyfolgen $(x_n)_{n\in\mathbb{N}}$ und $(x_{\nu_n})_{n\in\mathbb{N}}$ äquivalent sind, d.h. sich nur um eine Nullfolge unterscheiden, bedeutet es keine Einschränkung der Allgemeinheit, anzunehmen, dass $x_\ell - x_m \in (\pi)^{n+1}$ für alle $\ell, m \geqslant n$. Wir konstruieren jetzt induktiv $a_\nu \in \mathfrak{R}$, $\nu = 0, 1, 2, \ldots$, so dass

$$x_n - \sum_{\nu=0}^{n} a_\nu \pi^\nu \in (\pi)^{n+1} \quad \text{für alle } n \geqslant 0.$$

Induktionsanfang $n = 0$. Nach Definition des Repräsentantensystems gibt es ein $a_0 \in \mathfrak{R}$ mit $x_0 - a_0 \in (\pi)$.

Induktionsschritt $n \to n+1$. Da $x_n - x_{n+1} \in (\pi)^{n+1}$, folgt

$$x_{n+1} - \sum_{\nu=0}^{n} a_\nu \pi^\nu =: \xi_{n+1} \in (\pi)^{n+1}.$$

Das Element ξ_{n+1} lässt sich schreiben als $\xi_{n+1} = \alpha\pi^{n+1}$ mit $\alpha \in A$. Wählt man $a_{n+1} \in \mathfrak{R}$ mit $\alpha - a_{n+1} \in (\pi)$, so folgt $\xi_{n+1} \equiv a_{n+1}\pi^{n+1} \bmod (\pi)^{n+2}$, also

$$x_{n+1} - \sum_{\nu=0}^{n+1} a_\nu \pi^\nu \in (\pi)^{n+2}, \qquad \text{q.e.d.}$$

b) *Eindeutigkeit.* Es genügt zu zeigen: Sind $\sum_{n=0}^{\infty} a_n\pi^n$ und $\sum_{n=0}^{\infty} b_n\pi^n$, $(a_n, b_n \in \mathfrak{R})$, zwei Potenzreihen, deren Differenz gegen 0 konvergiert (d.h. die Partialsummen der Reihe $\sum_{n=0}^{\infty}(a_n - b_n)\pi^n$ bilden eine Nullfolge), so gilt $a_n = b_n$ für alle n. Angenommen, dies sei nicht der Fall und sei m der kleinste Index mit $a_m \neq b_m$. Dann gilt $(a_m - b_m) \notin (\pi)$, also $(a_m - b_m)\pi^m \notin (\pi)^{m+1}$. Da $(a_\nu - b_\nu)\pi^\nu \in (\pi)^{m+1}$ für alle $\nu > m$, folgt

$$\sum_{\nu=0}^{n}(a_\nu - b_\nu)\pi^\nu \notin (\pi)^{m+1} \quad \text{für alle } n > m.$$

Also kann die Reihe $\sum_{\nu=0}^{\infty}(a_\nu - b_\nu)\pi^\nu$ nicht gegen 0 konvergieren, Widerspruch!
Damit ist Lemma 1.11 bewiesen.

1.12. p-adische Zahlen. Speziell für den diskreten Bewertungsring $\mathbb{Z}_{(p)}$ bedeutet das Lemma 1.11 folgendes: Jedes Element ξ der Vervollständigung $\widehat{\mathbb{Z}}_{(p)}$ besitzt eine eindeutige Darstellung der Form

$$\xi = \sum_{n=0}^{\infty} a_n p^n, \qquad a_n \in \{0, 1, \ldots, p-1\}, \tag{3}$$

und umgekehrt konvergiert jede solche Reihe $\sum_{n=0}^{\infty} a_n p^n$ gegen ein Element von $\widehat{\mathbb{Z}}_{(p)}$.
Die Vervollständigung $\widehat{\mathbb{Z}}_{(p)}$ wird mit $\mathbb{Z}_p$ bezeichnet[1], $\mathbb{Z}_p$ heißt der Ring der ganzen p-adischen Zahlen. Der Ring $\mathbb{Z}_p$ ist wieder ein diskreter Bewertungsring mit maximalem Ideal $p\mathbb{Z}_p$ und Restklassenkörper

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

Dass $\mathbb{Z}_p$ vollständig ist, folgt ebenfalls aus Lemma 1.11, denn jede Cauchyfolge $(x_n)_{n\in\mathbb{N}} \in \mathrm{Cauchy}(\mathbb{Z}_p)$ ist äquivalent zu den Partialsummen einer Potenzreihe der Gestalt (3), welche in $\mathbb{Z}_p$ konvergiert.

Der Quotientenkörper $\mathbb{Q}_p := \mathrm{Quot}(\mathbb{Z}_p)$ ist der Körper der p-adischen Zahlen. Man kann zeigen, dass sich jedes Element $\xi \in \mathbb{Q}_p$ in eine Laurentreihe

$$\xi = \sum_{n=n_0}^{\infty} a_n p^n, \quad n_0 \in \mathbb{Z}, \quad a_n \in \{0, 1, \ldots, p-1\}$$

entwickeln lässt.

[1] Man beachte: Wir bezeichnen mit $\mathbb{Z}_p$ *nicht* den Restklassenring $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$.