Lösung 8

Aufgabe 1.
Es ist $v(1) = v(1 \cdot 1) = 2v(1)$, also $v(1) = 0$ und damit $1 \in R_v$. Weiter ist $0 = v(1) = 2v(-1)$ also $-1 \in R_v$. Da R_v ein Ring ist, folgt $\mathbb{Z} \subseteq R_v$. Weil v per Definition surjektiv ist, existieren teilerfremde ganze Zahlen a, b mit $b \neq 0$ und $1 = v(\frac{a}{b}) = v(a) - v(b)$. Insbesondere ist $v(a) = 1 + v(b) \geq 1$.

Da a und b teilerfremd sind, gibt es $r, s \in \mathbb{Z}$ mit $1 = ra + sb$. Es folgt

$$0 = v(1) = v(ra + sb) \geq \min\{v(a) + v(r),\ v(b) + v(s)\} \geq 0\,.$$

Wegen $v(a) \geq 1$ und $v(b) \geq 0$ muß also $v(b) = v(s) = 0$ gelten. Damit wird $v(r) = 1$. Ferner dürfen wir ohne Einschränkung annehmen, daß r positiv ist.

Sei nun $r = \prod_{i=1}^t p_i^{e_i}$ die Faktorisierung von r in paarweise verschiedene Primfaktoren mit $e_i \neq 0$ für alle $1 \leq i \leq t$. Dann ist $1 = v(r) = \sum_{i=1}^t \underbrace{e_i}_{\geq 1} \cdot \underbrace{v(p_i)}_{\geq 0}$. Daraus folgt, daß genau eine der Primzahlen p_i mit 1 bewertet wird. Diese heiße p.

Sei nun $q \neq p$ eine weitere Primzahl. Wir behaupten $v(q) = 0$. Dazu gehen wir analog zu oben vor. Wieder gibt es $r, s \in \mathbb{Z}$ mit $1 = rp + sq$. Es folgt

$$0 = v(1) = v(rp + sq) \geq \min\{v(r) + 1, v(s) + v(q)\} \geq 0\,.$$

Wegen $v(r) \geq 0$ folgt $v(s) = v(q) = 0$ wie behauptet.

Also ist $v(z) = \max\{k \geq 0 \mid p^k \text{ teilt } z\}$ für jede ganze Zahl $z \in \mathbb{Z}$. Ist nun $x \in \mathbb{Q}$, so existieren $e, u, w \in \mathbb{Z}$ mit $x = p^e \cdot \frac{u}{w}$ und $\gcd(p, uw) = 1$. Damit wird $v(x) = v(p^e) + v(u) - v(w) = e + 0 - 0 = e$. Damit ist v die p-adische Bewertung von Beispiel 7.9. und R_v ist die Lokalisierung von $\mathbb{Z}$ an $p\mathbb{Z}$.

Aufgabe 2.

(a) Ist $|x|_v \neq |y|_v$, so ist $v(x) \neq v(y)$ also $v(x + y) = \min\{v(x), v(y)\}$. Damit ist $|x + y|_v = \max\{|x|_v,\ |y|_v\}$.

Seien nun $x, y, z \in K$ beliebig aber paarweise verschieden. Wir haben zu zeigen, daß mindestens zwei der Längen $|x - y|_v$, $|x - z|_v$ und $|y - z|_v$ gleich sind. Ist das von den drei Punkten aufgespannte Dreieck nicht gleichseitig, so ist ohne Einschränkung $|x - y|_v > |y - z|_v$. Es folgt $|x - z|_v = |(x - y) - (y - z)|_v = \max\{|x - y|_v,\ |y - z|_v\} = |x - y|_v$. Das war zu zeigen.

(b) Ist (a_n) eine Cauchy-Folge, so existiert ein $N \in \mathbb{N}$ mit $|a_n - a_m|_v \leq 1$ für alle $n, m \geq N$. Dann gilt für alle $n \geq N$

$$|a_n|_v = |a_n - a_N + a_N|_v \leq \max\{|a_n - a_N|_v, |a_N|_v\}\,.$$

Wählen wir also $r = \max(\{1\} \cup \{|a_i|_v \mid 1 \leq i \leq N\})$ so ist $|a_n|_v \leq r$ für alle $n \in \mathbb{N}$.

(c) Angenommen die Aussage ist falsch. D.h. zu jedem $\delta > 0$ und $N \in \mathbb{N}$ gibt es ein $m \geq N$ mit $|a_n|_v \leq \delta$.

Sei nun $\varepsilon > 0$ beliebig. Dann existiert ein $N \in \mathbb{N}$ mit $|a_n - a_m|_v \leq \varepsilon$ für alle $n, m \geq N$. Laut Annahme gibt es dann ein $k \geq N$ mit $|a_k|_v \leq \varepsilon$. Es folgt $|a_n|_v = |a_n - a_k + a_k|_v \leq \max\{|a_n - a_k|_v, |a_k|_v\} \leq \varepsilon$ für alle $n \geq N$. Also ist $(a_n)_n$ eine Nullfolge im Widerspruch zur Voraussetzung.

(d) Bezeichne $\mathcal{X}$ die Menge der Cauchy-Folgen. Dann enthält $\mathcal{X}$ die konstanten Folgen. Also insbesondere sind 1 und 0 in $\mathcal{X}$. Seien nun (a_n) und (b_n) zwei Cauchy-Folgen.

Zu $1 \geq \varepsilon > 0$ existieren $N \in \mathbb{N}$ mit $|a_n - a_m|_v < \varepsilon$ und $|b_n - b_m|_v < \varepsilon$ für alle $n, m \geq N$. Sei nun $(c_n) = (a_n) + (b_n)$ und $(d_n) = (a_n) \cdot (b_n)$ d.h. $c_n = a_n + b_n$ und $d_n = a_n \cdot b_n$ für alle $n \in \mathbb{N}$.

Es ist $|c_n - c_m|_v = |a_n + b_n - a_m - b_m|_v \le \max\{|a_n - a_m|_v, |b_n - b_m|_v\} < \varepsilon$ für alle $n, m \ge N$. Also ist $(c_n) \in \mathcal{X}$.

Nach Teil (b) existiert ein $r \in \mathbb{R}$ mit $|a_n|_v, |b_n|_v \le r$ für alle $n \in \mathbb{N}$. Also ist

$$\begin{aligned} |d_n - d_m|_v &= |a_n \cdot b_n - a_m \cdot b_m|_v = |a_n \cdot (b_n - b_m) + b_m \cdot (a_n - a_m)|_v \\ &\le \max\{|a_n|_v \cdot |b_n - b_m|_v + |b_m|_v \cdot |a_n - a_m|_v\} \le r \cdot \varepsilon\,. \end{aligned}$$

Dies zeigt $(d_n) \in \mathcal{X}$. Damit ist $\mathcal{X}$ ein Teilring des Rings aller Folgen in K.

Bezeichne $\mathcal{N}$ die Menge aller Nullfolgen in K. Da $\mathcal{N}$ die Folge enthält welche konstant 0 ist, ist $\mathcal{N}$ nicht leer. Weiter ist klar, daß die Summe zweier Nullfolgen eine Nullfolge ist.

Ist $(a_n) \in \mathcal{N}$ und $\varepsilon > 0$ beliebig, so gibt es $N \in \mathbb{N}$ mit $|a_n|_v \le \varepsilon$ für alle $n \ge N$. Es folgt $|a_n - a_m|_v \le \max\{|a_n|_v, |a_m|_v\} \le \varepsilon$ für alle $n, m \ge N$. Also ist $\mathcal{N} \subseteq \mathcal{X}$. Ist zusätzlich $(b_n) \in \mathcal{X}$, so gibt es nach Teil (b) ein $r \in \mathbb{R}$ mit $|a_n|_v \le r$ für alle $n \in \mathbb{N}$. Es folgt $|a_n b_n|_v \le r\varepsilon$ für alle $n \ge N$. Damit ist $(a_n) \cdot (b_n)$ eine Nullfolge. Somit haben wir gezeigt, daß $\mathcal{N}$ ein Ideal in $\mathcal{X}$ ist.

Aufgabe 3.

Bemerkung 1: Ist $d \in \mathbb{Z}$ teilerfremd zu p, so ist $p \in (\mathbb{Z}/d\mathbb{Z})^*$. Bezeichne m die Ordnung von p in dieser Gruppe. Dann ist d ein Teiler von $p^m - 1$ also $dk = p^m - 1$ für ein $k \in \mathbb{Z}$. Es folgt $\frac{1}{d} = \frac{-k}{1-p^m} = -k \sum_{i=0}^{\infty} p^{mi}$.

Bemerkung 2: Ist $x = \sum_{i=0}^{\infty} a_i p^i$ mit $0 \le a_i \le p-1$ und $a_i \ne 0$, so ist $-x = \sum_{i=0}^{\infty} b_i p^i$ wobei $b_0 = p - a_0$ und $b_i = p - 1 - a_i$ sonst. (Beachte: Es ist $0 \le b_j \le p-1$ stets.)
Beweis: Es ist $\sum_{i=0}^{\infty} b_i p^i = p - a_0 + \sum_{i=1}^{\infty}(p-1-a_i)p^i = p - a_0 + \sum_{i=1}^{\infty}(p-1)p^i - \sum_{i=1}^{\infty} a_i p^i = 1 - \sum_{i=0}^{\infty}(p-1)p^i - \sum_{i=0}^{\infty} a_i p^i = 1 - 1 - x = -x$ wie behauptet.

(a) Schreiben wir die Koeffizienten untereinander, so ergibt sich (wenn man links beginnt)

	0	1	2	3	4	4	
	2	4	1	0	3	0	
Übertrag				1		1	
$\sum$	2	0	4	3	2	0	1

Also ist $a + b = 2 \cdot 5^{-2} + 4 + 3 \cdot 5 + 2 \cdot 5^2 + 5^4$.

Genauso multiplizieren wir a und b:

$2a$	2	4	1	4	4	1				
$4a$		4	3	3	3	2	3			
a			1	2	3	4	4			
$3a$					3	1	0	4	4	2
Übertrag			1	1	2	3	2	1	1	1
$\sum$	2	3	1	0	0	3	4	0	0	3

Also ist $ab = 2 \cdot 5^{-3} + 3 \cdot 5^{-2} + 5^{-1} + 3 \cdot 5^2 + 4 \cdot 5^3 + 3 \cdot 5^6$.

(b) Nach Bemerkung 2 ist $-1 = \sum_{i=0}^{\infty}(p-1)p^i$.

(c) Wenden wir die Bemerkungen 1 und 2 auf $d = 3$ und $p = 7$ an. Es ist dann $m = 1$ und $7 - 1 = 3 \cdot 2$. Also $\frac{1}{3} = -\sum_{i=0}^{\infty} 2 \cdot 7^i = 5 + \sum_{i=1}^{\infty} 4 \cdot 7^i$.

(d) In diesem Fall ist $d = 3$ und $p = 5$. Es wird $m = 2$ und $5^2 - 1 = 3 \cdot 8$. Also

$$\frac{1}{3} = -8 \sum_{i=0}^{\infty} 5^{2i} = -\sum_{i=0}^{\infty}(3 + 1 \cdot 5) \cdot 5^{2i} = 2 + \sum_{i=0}^{\infty}(3 + 1 \cdot 5) \cdot 5^{2i+1}\,.$$

(e) In diesem Fall ist $d = 13$ und $p = 5$. Es wird $m = 4$ und $5^4 - 1 = 13 \cdot 48$. Also

$$\frac{1}{5 \cdot 13} = -48 \sum_{i=0}^{\infty} 5^{4i-1} = -\sum_{i=0}^{\infty}(3+4\cdot5+1\cdot5^2+0\cdot5^3)\cdot5^{4i-1} = 2+\sum_{i=0}^{\infty}(0+3\cdot5+4\cdot5^2+1\cdot5^3)\cdot5^{4i}\,.$$

Aufgabe 4.

(a) Klar, denn jedes $x \in \mathbb{N}_0$ hat bekanntlich eine Darstellung in der Basis p.

(b) Angenommen, es ist $x = \sum_{i=k}^{\infty} a_i p^i$ mit $a_i = a_{i+\ell}$ für alle $i \geq N$. Subtrahiert man $\sum_{i=k}^{N-1} a_i p^i \in \mathbb{N}_0$ von x und muliplizert anschließend mit einer geeigneten p-Potenz, so darf man annehmen, daß $x = \sum_{i=0}^{\infty} a_i p^i$ mit $a_i = a_{i+\ell}$ für alle $i \geq 0$. Dann folgt

$$x = \sum_{i=0}^{\infty} \underbrace{(a_0 + a_1 \cdot p + \cdots + a_{\ell-1} p^{\ell-1})}_{=:b \in \mathbb{Z}} \cdot p^{i\ell} = \frac{b}{1-p^\ell} \in \mathbb{Q}\,.$$

Sei nun umgekehrt $x \in \mathbb{Q}$. Ohne Einschränkung ist $x > 0$ wie Bemerkung 2 von oben zeigt. Wir schreiben dann $x = p^\ell \cdot (a + \frac{b}{d})$ mit $\ell \in \mathbb{Z},\ a, b \in \mathbb{N}_0,\ \gcd(p, bd) = 1$ und $b < d$. Es genügt dann zu zeigen, daß die p-adische Entwicklung von $a + \frac{b}{d}$ periodisch ist, denn die Multiplikation mit p^ℓ verschiebt die Darstellung lediglich.

Wir behandeln zunächst den Fall $a = 0$. Dann ist nach Bemerkung 1 von oben: $\frac{b}{d} = \sum_{i=0}^{\infty} b \cdot p^{mi}$ mit $m = \min\{k > 0 \mid d \text{ teilt } p^k - 1\}$. Insbesondere ist $0 \leq b < d \leq p^m - 1 < p^m$. Daher ist die Darstelung von b zur Basis p von der Form $b_0 + b_1 p^1 + b_2 p^2 + \cdots + b_{m-1} p^{m-1}$ mit $0 \leq b_i \leq p-1$ stets. Also hat $\frac{b}{d}$ eine periodische Darstellung (vgl. Aufgabe 3), sagen wir $\frac{b}{d} = \sum_{i=0}^{\infty} b'_i p^i$ mit $b'_i = b_j$ wobei $i = rm + j$ mit $0 \leq j \leq m-1$ und $r \in \mathbb{N}_0$.

Sei nun $a \in \mathbb{N}$ beliebig. Dann hat a nach Teil (1) eine endliche Darstellung sagen wir nur die ersten t Summanden seien ungleich 0. Nun addieren wir diese endliche Summe zur p-adischen Darstellung von $\frac{b}{d}$ hinzu. Wir erhalten so $a + \frac{b}{d} = \sum_{i=0}^{\infty} c_i p^i$ mit $0 \leq c_i \leq p-1$ stets.

Klar ist: beim ersten Koeffizienten addieren wir zwei Zahlen $\leq p-1$, also kann der Übertrag maximal 1 sein. Beim zweiten Koeffizienten addieren wir wiederum zwei Zahlen $\leq p-1$ und maximal einen Übertrag von 1. Diese Zahl ist echt kleiner als $2p$. Also tritt wiederum höchstens ein Übertrag von 1 auf, usw..

Es gibt also zwei Fälle:

1.) Es gibt einen Index $i > t$ bei dem kein Übertrag stattfindet. Dann ist $c_j = b'_j$ für alle $j \geq i$ und die p-adische Darstellung $\sum_{i=0}^{\infty} c_i p^i$ ist daher periodisch.

2.) Für jedes $i > t$ findet ein Übertrag um 1 statt. Aber dann ist die Darstellung natürlich auch periodisch!

Hier ist noch ein zweiter Beweis nach A. Nehnes und N. Pawlitta für die Tatsache, daß jedes $x \in \mathbb{Q}$ eine periodische p-adische Entwicklung hat:

Sei $x := \frac{a}{b} \in \mathbb{Q}$ mit teilerfremden $a, b \in \mathbb{Z}$ und $b > 0$. Ohne Einschränkung ist $x \in \mathbb{Z}_p$ also $p \nmid b$. Dann gibt es $a_i \in \{0, \ldots, p-1\}$ mit $x = \sum_{i=0}^{\infty} a_i p^i$. Damit erfüllt a_0 die Kongruenz $a - ba_0 \equiv_p 0$ und allgemein $a - b\sum_{i=0}^{n-1} a_i p^i \equiv_{p^n} 0$.

Setzen wir $c_n := (a - b\sum_{i=0}^{n-1} a_i p^i)/p^n$ für alle $n \geq 0$, so ist also

$$c_n \in \mathbb{Z} \quad \text{und} \quad c_n \equiv_p a_n \qquad \text{für alle } n \in \mathbb{N}_0\,.$$

D.h. c_n bestimmt a_n eindeutig. Weiter ist $c_{n+1} = (c_n - ba_n)/p$ stets. Damit bestimmen a_n und c_n auch c_{n+1} eindeutig. Zusammenfassend haben wir damit gezeigt daß c_n die die Zahl c_{n+1} bereits eindeutig festlegt! Insbesondere genügt es daher zu zeigen, daß die Folge (c_n) mindestens eine Wiederholung besitzt.

Bezeichne $|.|$ den gewöhnlichen Betrag in $\mathbb{Q}$, so gilt

$$\begin{aligned} |c_n| &\leq |a|/p^n + bp^{-n} \sum_{i=0}^{n-1} a_i p^i \leq |a| + bp^{-n} \sum_{i=0}^{n-1} (p-1)p^i \\ &= |a| + b(p^n - 1)/p^n \leq |a| + b\,. \end{aligned}$$

Insbesondere nimmt die Folge (c_n) also nur endlich viele Werte an. Damit kommt es unweigerlich zu einer Wiederholung. Wie bereits gezeigt, führt dies zu einer Periode in (a_n).