Vortrag 2: Die p-adischen Zahlen

Christian Merten

Seminar „Quadratische Formen”, 22. April 2021

Sei $p \in \mathbb{N}$ eine im Folgenden fest gewählte Primzahl.

Genauso wie eine natürliche Zahl $m \in \mathbb{N}$ bezüglich der Basis 10 dargestellt werden kann, ist das auch bezüglich der Basis p möglich. Jede natürliche Zahl besitzt also eine p-adische Entwicklung der Form

$$m = a_0 + a_1 p + \ldots + a_n p^n$$

wobei die Koeffizienten a_i in $\{0, 1, \ldots, p-1\}$ liegen. Die Darstellung ist damit eindeutig.

Beispiel 2.1

Diese Darstellung finden wir durch sukzessives Dividieren mit Rest. Für $n = 216$ erhalten wir für $p = 5$

$$\begin{aligned} 216 &= 1 + 5 \cdot 43 \\ 43 &= 3 + 5 \cdot 8 \\ 8 &= 3 + 5 \cdot 1 \\ 1 &= 1 \end{aligned}$$

Also insgesamt

$$216 = 1 + 3 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3.$$

Um nun auch negative und sogar gebrochene Zahlen darstellen zu können, gehen wir zu unendlichen Reihen über:

Definition 2.2 (Ganze p-adische Zahlen)

Eine ganze p-adische Zahl ist eine formale unendliche Reihe

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \dots$$

mit $0 \leq a_i < p$ für $i \in \mathbb{N}_0$. Die Menge dieser formalen Reihen wird mit $\mathbb{Z}_p$ bezeichnet.

Bemerkung 2.3

$\sum_{i=0}^{\infty} a_i p^i$ ist rein formal gemeint, d.h. bezeichnet einfach die Folge der Partialsummen

$$s_n = \sum_{i=0}^{n-1} a_i p^i \in \mathbb{Z}, \quad n \in \mathbb{N}.$$

Womit können wir jetzt die ganzen Zahlen $\mathbb{Z}$ in den p-adischen Zahlen $\mathbb{Z}_p$ identifizieren? Wie kann also beispielsweise -1 in $\mathbb{Z}_p$ dargestellt werden? Dazu stellen wir folgendes fest

Lemma 2.4

Sei $a \in \mathbb{Z}$. Die Restklasse $a \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}$ wird in eindeutiger Darstellung durch

$$a \equiv a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1} \ (mod\ p^n)$$

gegeben, wobei $0 \leq a_i < p$ für $i \in \{0, \ldots, n-1\}$.

Beweis.

Per Induktion. Für $n = 1$ ist offenbar $a \equiv a_0 \pmod{p}$ mit $0 \leq a_0 < p$. Sei nun die Behauptung für $n-1$ gezeigt. Dann ex. eine eindeutige Darstellung

$$a \equiv a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-2} p^{n-2} \pmod{p^{n-1}}$$

Also

$$a = a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-2} p^{n-2} + g p^{n-1}$$

für ein $g \in \mathbb{Z}$. Sei $0 \leq a_{n-1} < p$, s.d. $g \equiv a_{n-1} \pmod{p}$, also $g = a_{n-1} + hp$ für $h \in \mathbb{Z}$. a_{n-1} ist also eindeutig durch a bestimmt und es folgt

$$a = a_0 + \ldots + a_{n-2} p^{n-2} + a_{n-1} p^{n-1} + h p^n$$

Jede ganze Zahl a definiert nun eine Folge von Restklassen $\overline{s_n} = \overline{a} \in \mathbb{Z}/p^n\mathbb{Z}$ für $n \in \mathbb{N}$, die nach 2.4 von der Gestalt

$$\begin{aligned} s_1 &\equiv a_0 \pmod{p} \\ s_2 &\equiv a_0 + a_1 p \pmod{p^2} \\ &\vdots \end{aligned}$$

sind mit eindeutig bestimmten Koeffizienten $a_0, a_1, \ldots \in \{0, \ldots, p-1\}$. Die Zahlenfolge

$$s_n = a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1}$$

definiert nun eine ganze p-adische Zahl $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$, die wir die p-adische Entwicklung von a nennen.

Beispiel 2.5

Was ist jetzt die p-adische Entwicklung von -1? Es ist

$$-1 = (p-1) + (p-1)p + \ldots + (p-1)p^{n-1} - p^n$$
$$\text{also } -1 \equiv (p-1) + (p-1)p + \ldots + (p-1)p^{n-1} \pmod{p^n}.$$

Es ist also $-1 = (p-1) + (p-1)p + (p-1)p^2 + \ldots \in \mathbb{Z}_p$ die p-adische Entwicklung von -1.

Um $\mathbb{Z}_p$ eine algebraische Struktur zu geben, könnten wir mit diesen Reihen mit Überträgen rechnen, so wie wir es von der Basis 10 gewohnt sind. Einfacher wird es jedoch, wenn wir eine ganze p-adische Zahl $x = \sum_{i=0}^{\infty} a_i p^i$ mit der Folge der Restklassen $\overline{s_n} \in \mathbb{Z}/p^n\mathbb{Z}$ der Partialsummen identifizieren.

Dazu benötigen wir noch eine Vorüberlegung und einige Begriffe.

Definition 2.6

Ein projektives System ist eine Folge von Mengen $(D_n)_{n\in\mathbb{N}}$ und eine Folge von Abbildungen $(p_n)_{n\in\mathbb{N}}$ mit $p_n\colon D_{n+1} \to D_n$

$$D_1 \xleftarrow{p_1} D_2 \leftarrow \ldots \leftarrow D_n \xleftarrow{p_n} D_{n+1} \leftarrow \ldots.$$

Die Teilmenge

$$D = \varprojlim (D_n, p_n) = \left\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} D_n \mid p_n(a_{n+1}) = a_n \forall n \in \mathbb{N} \right\}$$

heißt projektiver Limes des Systems.

Bemerkung 2.7

Falls die D_n Ringe und die p_n Ringhomomorphismen sind, wird $\varprojlim (D_n, p_n)$ zum Teilring des Produktrings $\prod_{n=1}^{\infty} D_n$ (leicht nachzurechnen).

Setze im Folgenden $A_n := \mathbb{Z}/p^n\mathbb{Z}$. Dann erhalten wir für $n \in \mathbb{N}$ einen kanonischen Homomorphismus

$$\begin{aligned} \phi_n \colon A_{n+1} &\to A_n \\ \overline{a} &\mapsto \overline{a}. \end{aligned}$$

Satz 2.8

Ordnet man jeder ganzen p-adischen Zahl

$$x = \sum_{i=0}^{\infty} a_i p^i$$

die Folge $(\overline{s}_n)_{n\in\mathbb{N}}$ *der Restklassen*

$$\overline{s}_n = \sum_{i=0}^{n-1} a_i p^i \ (mod\ p^n) \in A_n$$

zu, so erhält man eine Bijektion

$$\mathbb{Z}_p \xrightarrow{\sim} \varprojlim (A_n, \phi_n).$$

Beweis.

Die Zuordnung ist wohldefiniert, da

$$s_{n+1} = a_0 + a_1 p + \ldots + a_n p^n \equiv a_0 + a_1 p + \ldots + a_{n-1} p^{n-1} \pmod{p^n} = s_n.$$

Die Bijektivität folgt direkt aus 2.4 $\square$

Bemerkung 2.9

Die Koeffizienten der p-adischen Entwicklung von $a \in \mathbb{Z}$ ergeben sich durch die Kongruenzen

$$a \equiv a_0 + a_1 p + \ldots + a_{n-1} p^{n-1} \pmod{p^n}$$

mit $0 \leq a_i < p$. Bei der Identifizierung $\mathbb{Z}_p = \varprojlim (A_n, \phi_n)$ geht $a \in \mathbb{Z}$ daher über in

$$(a \bmod p, a \bmod p^2, a \bmod p^3, \ldots) \in \prod_{n=1}^{\infty} A_n.$$

$\mathbb{Z}$ wird so zum Teilring von $\varprojlim (A_n, \phi_n)$.

Beispiel 2.10 (2.5 fortgesetzt)

Mit 2.9 folgt also

$$-1 = (p-1, p^2-1, p^3-1, \ldots) \in \varprojlim (A_n, \phi_n).$$

Wir identifizieren nun im Folgenden stets $\mathbb{Z}_p = \varprojlim (A_n, \phi_n)$. π_n bezeichne den kanonischen Projektionshomomorphismus $\pi_n \colon \mathbb{Z}_p \to A_n$.

Bemerkung 2.11

1. Per Definition ist $x \in \mathbb{Z}_p$ also ein Element $x \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ mit der „Kompatibilitätsbedingung":

$$x_{n+1} \equiv x_n \pmod{p^n}.$$

2. $\mathbb{Z}_p$ erbt als Teilring nun also die komponentenweise Addition und Multiplikation des Produktrings $\prod_{n=1}^{\infty} A_n$, d.h. für $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$ gilt

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}} \quad (a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (a_n \cdot b_n)_{n\in\mathbb{N}}.$$

3. Versieht man A_n mit der diskreten Topologie (d.h. alle Teilmengen sind offen) und $\prod_{n=1}^{\infty} A_n$ mit der Produkttopologie (die von den Urbildern der kanonischen Projektionen π_n erzeugt wird), wird $\mathbb{Z}_p$ zu einem topologischen Ring.

Satz 2.12 (von Tychonoff)

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

Beweis.

Der Satz ist äquivalent zum Auswahlaxiom. Ein Beweis findet sich beispielsweise in Klaus Jänich: *Topologie*. □

Korollar 2.13

$\mathbb{Z}_p$ ist kompakt.

Beweis.

Nach 2.12 ist $\prod_{n=1}^{\infty} A_n$ kompakt. Außerdem ist

$$\mathbb{Z}_p = \bigcap_{n\in\mathbb{N}} \left\{ x \in \prod_{n=1}^{\infty} A_n \mid \phi_n(\pi_{n+1}(x)) = \pi_n(x) \right\} = \bigcap_{n\in\mathbb{N}} f_n^{-1}(\{0\})$$

mit $f_n \colon \prod_{n=1}^{\infty} A_n \to A_n, x \mapsto \phi_n(\pi_{n+1}(x)) - \pi_n(x)$. Es ist f_n stetig, da π_n per Definition der Produkttopologie und ϕ_n als Abbildung zwischen diskreten Räumen stetig sind. Da $\{0\} \subseteq A_n$ abgeschlossen, folgt die Behauptung. □

Lemma 2.14

Es ist π_n surjektiv und $\ker \pi_n = p^n\mathbb{Z}_p$ $\forall n \in \mathbb{N}$. Insbesondere gilt

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z} = A_n.$$

Beweis.

Die Surjektivität ist klar. Z.z.: $\ker \pi_n = p^n\mathbb{Z}_p$. Sei dazu $x \in \mathbb{Z}_p$. Dann ist $p^n x_n \equiv 0 \pmod{p^n}$. Also $\pi_n(p^n x) = 0$. Damit $p^n\mathbb{Z}_p \subseteq \ker \pi_n$.

Sei nun $x = (x_m)_{m\in\mathbb{N}} \in \ker \pi_n$ und $m \geq n$. Wegen Kompatibilität folgt

$$x_m \equiv x_n \pmod{p^n} \equiv 0 \pmod{p^n}.$$

Also folgt $x_m \in p^n A_m$.

Es ist (nachrechnen)

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \cong p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m.$$

Das heißt es ex. ein eindeutiges $y_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Setze nun $y := (y_{m-n})_{m>n}$. Es lässt sich nachrechnen, dass $y \in \mathbb{Z}_p$. Es bleibt zu zeigen, dass $p^n y = x$. Z.z.: $x = p^n y$. Für $m \leq n$ ist $x_m = 0 = p^n y_m$. Für $m > n$ ist wegen Kompatibilität

$$p^n y_m = p^n y_{m+n-n} \equiv x_{m+n} \pmod{p^{m+1}} \equiv x_m \pmod{p^m}.$$

Insgesamt folgt also $x = p^n y$. Insgesamt folgt also $\ker \pi_n = p^n\mathbb{Z}_p$. Die behauptete Isomorphie folgt jetzt direkt aus dem Homomorphiesatz. □

Lemma 2.15

Für $u \in \mathbb{Z}_p$ sind äquivalent

(i) $u \in \mathbb{Z}_p^\times$

(ii) $p \nmid u$

(iii) $0 \neq u_1 \in \mathbb{Z}/p\mathbb{Z}$

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (ii). Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann $\exists v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u_1 v_1} \equiv 1 \pmod{p}$ also insbesondere $p \nmid u_1 \implies \overline{u_1} \neq 0$.
Sei umgekehrt $\overline{u_1} \neq 0$. Wegen Kompatibilität folgt damit $p \nmid u_n$ $\forall n \in \mathbb{N}$, denn ang. $p \mid u_n$ für ein $n \in \mathbb{N}$. Dann folgt

$$0 \equiv u_n \pmod{p} \equiv u_1 \pmod{p} \quad \lightning.$$

Da p prim folgt insbesondere $(p^n, u_n) = 1$. Also ex. nach euklid. Alg. $a, b \in \mathbb{Z}$, s.d. $1 = ap^n + bu_n$, also $1 = \overline{bu_n}$ mit $\overline{b} \in A_n$. Also $\overline{u_n} \in A_n^\times$ und damit
$v := (\ldots \overline{u_n}^{-1}, \overline{u_{n-1}}^{-1}, \ldots, \overline{u_1}^{-1}) = u^{-1} \in \mathbb{Z}_p$. $\square$

Lemma 2.16

Für $x \in \mathbb{Z}_p \setminus \{0\}$ ex. $n \in \mathbb{N}_0$ und $u \in \mathbb{Z}_p^\times$, s.d.

$$x = p^n u.$$

Diese Darstellung ist eindeutig.

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein $n \in \mathbb{N}_0$ maximal, s.d. $x_n = \pi_n(x) = 0$. Also ist $x \in \ker \pi_n$, insbesondere ex. nach 2.14 ein $u \in \mathbb{Z}_p$ mit $x = p^n u$. Ang.: $p \mid u$, dann ist $\pi_1(u) = 0$ also ex. wieder nach 2.14 ein $v \in \mathbb{Z}_p$ mit $u = pv$. Dann ist aber

$$\pi_{n+1}(x) = \pi_{n+1}(p^n u) = \pi_{n+1}(p^{n+1} v) = 0.$$

Widerspruch zur Maximalität von n.

(ii) Eindeutigkeit: Sei $x = p^n u = p^m v$ mit $u, v \in \mathbb{Z}_p^\times$ und $n, m \in \mathbb{N}_0$. Sei o.E. $n \geq m$. Es ist $\pi_n(x) = \pi_n(p^n)\pi_n(u) = 0$ also auch $0 = \pi_n(x) = \pi_n(p^m)\pi_n(v)$. Da $v \in \mathbb{Z}_p^\times$ ist $\pi_n(v) \in A_n^\times$, also kein Nullteiler. Also folgt $\pi_n(p^m) = 0$ und damit $p^m \equiv 0 \pmod{p^n}$, also $m \geq n$. Insgesamt also $m = n$. Nun gilt weiter $x = p^n u = p^n v$, also $p^n(u - v) = 0$. Ang. $u - v \neq 0$. Dann ist nach (i) $u - v = p^k w$ mit $k \in \mathbb{N}_0$ und $w \in \mathbb{Z}_p^\times$. Also $0 = p^n(u - v) = p^{n+k} w$. Da $w \in \mathbb{Z}_p^\times$ also kein Nullteiler, folgt $0 = p^{n+k} \in \mathbb{Z}$ ↯.

□

Definition 2.17 (p-Bewertung)

Für $x \in \mathbb{Z}_p \setminus \{0\}$ sei $x = p^n u$ mit $u \in \mathbb{Z}_p^\times$. Dann setze

$$v_p(x) := n$$

und setze $v_p(0) := \infty$. $v_p(x)$ heißt die p-Bewertung von x.

Bemerkung 2.18

Wegen 2.16 ist die p-Bewertung wohldefiniert.
Per Konvention setze $n + \infty = \infty$ und $\infty > n$ für $n \in \mathbb{N}_0$.

Lemma 2.19 (Eigenschaften der p-Bewertung)

Für $x, y \in \mathbb{Z}_p$ gilt

$$v_p(xy) = v_p(x) + v_p(y), \quad v_p(x+y) \geq \min(v_p(x), v_p(y)).$$

Beweis.

Folgt direkt durch Nachrechnen. □

Korollar 2.20

$\mathbb{Z}_p$ ist nullteilerfrei.

Beweis.

Seien $x, y \in \mathbb{Z}_p$ mit $xy = 0$. Dann folgt

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

Also $v_p(x) = \infty$ oder $v_p(y) = \infty$, also $x = 0$ oder $y = 0$. □

Lemma 2.21 (Topologie auf $\mathbb{Z}_p$)

Die Topologie auf $\mathbb{Z}_p$ wird induziert durch die Metrik

$$d(x, y) = \exp(-v_p(x - y)).$$

$\mathbb{Z}_p$ ist vollständig und $\mathbb{Z}$ ist dicht in $\mathbb{Z}_p$.

Bemerkung 2.22 (Bälle)

Es sei im Folgenden stets

$$B(x, r) = \{y \in \mathbb{Z}_p \mid d(x, y) < r\} \text{ und}$$
$$\overline{B(x, r)} = \{y \in \mathbb{Z}_p \mid d(x, y) \leq r\}.$$

Da $d(x, y) \in \{\exp(n) \mid n \in \mathbb{Z}\}$ gilt

$$\begin{aligned}\overline{B(x, e^{-n})} &= \{y \in \mathbb{Z}_p \mid v_p(x - y) \geq n\} \\ &= \{y \in \mathbb{Z}_p \mid v_p(x - y) > n - 1\} \\ &= B(x, e^{-(n-1)}).\end{aligned}$$

Beweis.

$d(\cdot,\cdot)$ ist eine Metrik (nachrechnen). Sei nun

$$S := \{\pi_n^{-1}(B) \mid B \subseteq A_n, n \in \mathbb{N}\}.$$

Die offenen Mengen von $\mathbb{Z}_p$ bezüglich der Produkttopologie sind dann per Definition gegeben als $\langle S \rangle$, wobei mit $\langle \ldots \rangle$ die durch endliche Schnitte und beliebige Vereinigungen erzeugten Mengen gemeint sind.
Für $D \in S$ ist $D = \pi_n^{-1}(B) = (A_1, \ldots, A_{n-1}, B, A_{n+1}, \ldots) \subseteq \mathbb{Z}_p$ wobei $B \subseteq A_n$ für ein $n \in \mathbb{N}$. Für $U \in \langle S \rangle$ ist dann $U = (B_1, \ldots, B_n, A_{n+1}, \ldots)$ mit $B_n \subsetneq A_n$ für $n \in \mathbb{N}_0$. Sei nun $0 \in U$. Dann ist $p^n\mathbb{Z}_p \subseteq U$.

Für beliebiges $V \subseteq \mathbb{Z}_p$ offen ex. nun für $v \in V$ ein $n_v \in \mathbb{N}_0$, s.d. $v + p^{n_v}\mathbb{Z}_p \subseteq V$. Also folgt

$$V = \bigcup_{v \in V} (v + p^{n_v}\mathbb{Z}_p).$$

Nun ist aber

$$a \in v + p^n\mathbb{Z}_p \iff v_p(a-v) \geq n \iff a \in \overline{B(v, e^{-n})} = B(v, e^{-(n-1)}).$$

Also folgt

$$V = \bigcup_{v \in V} B(v; e^{-(n-1)})$$

also V auch offen bezüglich $d(\cdot,\cdot)$. Umgekehrt sei U offen bezüglich $d(\cdot,\cdot)$. Dann ist U Vereinigung von offenen (bezüglich $d(\cdot,\cdot)$) Bällen. Da $p^n\mathbb{Z}_p = \pi_n^{-1}(\{0\})$, sind diese auch offen bezüglich der Produkttopologie.

Z.z.: $\mathbb{Z}_p$ vollständig. Da $\mathbb{Z}_p$ nach 2.13 kompakt ist, hat jede Folge in $\mathbb{Z}_p$ eine konvergente Teilfolge. Insbesondere hat also jede Cauchy-Folge eine konvergente Teilfolge und damit konvergiert jede Cauchy-Folge in $\mathbb{Z}_p$.
Z.z.: $\mathbb{Z}$ dicht in $\mathbb{Z}_p$. Sei $x = (x_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$. Setze $y_n \in \mathbb{Z}$, s.d. $y_n \equiv x_n \pmod{p^n}$. Dann ist für $n \in \mathbb{N}$ fest, $y_n \equiv x_m \pmod{p^m}$ $\forall m \leq n$, also $v_p(y_n - x) \geq n$. Also

$$d(y_n, x) = \exp(-v_p(y_n - x)) \leq \exp(-n) \xrightarrow{n\to\infty} 0.$$

□

Definition 2.23

Der Quotientenkörper der ganzen p-adischen Zahlen $\mathbb{Z}_p$ heißt Körper der p-adischen Zahlen

$$\mathbb{Q}_p := Q(\mathbb{Z}_p).$$

Bemerkung 2.24

1. Ein Element $x = \frac{a}{b} \in \mathbb{Q}_p^\times$ mit $a, b \in \mathbb{Z}_p$, $b \neq 0$ kann eindeutig als $x = p^r w$ mit $r \in \mathbb{Z}$ und $w \in \mathbb{Z}_p^\times$ dargestellt werden, denn nach 2.16 ist

$$x = \frac{a}{b} = \frac{p^n u}{p^m v} = p^{n-m} \underbrace{uv^{-1}}_{\in \mathbb{Z}_p^\times}.$$

   Damit setzt sich die Definition von v_p auf $\mathbb{Q}_p$ fort. Es gilt $v_p(x) \geq 0 \iff x \in \mathbb{Z}_p$.
2. Nach (1) ist also $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.

Lemma 2.25 (Topologie auf $\mathbb{Q}_p$)

$\mathbb{Q}_p$ mit der von $\mathbb{Z}_p$ geerbten Metrik $d(x,y) = \exp(-v_p(x-y))$ ist lokal kompakt und enthält $\mathbb{Z}_p$ als offenen Teilring. $\mathbb{Q}$ ist dicht in $\mathbb{Q}_p$.

Beweis.

Da $x \in \mathbb{Z}_p \iff v_p(x) \geq 0 \iff v_p(x) > -1$ folgt $\mathbb{Z}_p = \overline{B(0,1)} = B(0,e)$, also $\mathbb{Z}_p$ offen. Da $\mathbb{Z}_p$ kompakt, folgt, dass $B(x,e)$ kompakt $\forall x \in \mathbb{Q}_p$, also $\mathbb{Q}_p$ lokal kompakt. Außerdem ist $\mathbb{Z}$ dicht in $\mathbb{Z}_p$, d.h. für $x \in \mathbb{Q}_p$ mit $x = p^k u$ und $k \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$ ex. eine Folge $(y_n)_{n\in\mathbb{N}} \subseteq \mathbb{Z}$ mit $y_n \xrightarrow{n\to\infty} u$. Dann setze $z_n := p^k y_n \in \mathbb{Q}$. Dann folgt direkt $z_n = p^k y_n \xrightarrow{n\to\infty} p^k u = x$. □

Bemerkung 2.26

1. $\mathbb{Q}_p$ kann auch als Vervollständigung von $\mathbb{Q}$ bezüglich der p-adischen Metrik $d(\cdot,\cdot)$ definiert werden (analog zu $\mathbb{R}$ als Vervollständigung von $\mathbb{Q}$ bezüglich $|\cdot|$).
2. Es ist leicht nachzurechnen, dass $d(\cdot,\cdot)$ die ultrametrische Ungleichung (auch starke Dreiecksungleichung) erfüllt, d.h.

$$d(x,z) \leq \max(d(x,y), d(y,z))$$

für $x, y, z \in \mathbb{Q}_p$. Damit folgt das eine Folge $(a_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q}_p$ genau dann konvergiert, wenn $\lim_{n\to\infty}(u_{n+1} - u_n) = 0$ (was in $\mathbb{R}$ bezüglich $|\cdot|$ falsch ist).

Lemma 2.27

Sei $D_1 \leftarrow D_2 \leftarrow \ldots$ ein projektives System und $D = \varprojlim (D_n, p_n)$ sein inverser Limes. Falls $D_n \neq \emptyset$ und endlich folgt $D \neq \emptyset$.

Beweis.

Sei zunächst $p_n \colon D_{n+1} \to D_n$ surjektiv. Dann ex. für alle $x_n \in D_n$ ein $x_{n+1} \in D_{n+1}$, s.d. $p_n(x_{n+1}) = x_n$. Da $D_1 \neq \emptyset$ folgt $D \neq \emptyset$ induktiv.
Im Allgemeinen bezeichne für $m, n \in \mathbb{N}$:

$$D_{n,m} := (p_n \circ \ldots \circ p_{n+m-1})(D_{n+m}).$$

Da $D_{n+m} \neq \emptyset$ folgt $D_{n,m} \neq \emptyset$ und da D_k endlich folgt $\#p_k(D_{k+1}) \leq \#D_{k+1}\ \forall k \in \mathbb{N}$. D.h. $\#D_{n,m}$ ist monoton fallend in m bei festem n. Da $D_{n,m} \neq \emptyset$ wird die Folge stationär, d.h. es ex. ein $m_0 \in \mathbb{N}$, s.d. $D_{n,m_0} = D_{n,m}\ \forall m \geq m_0$. Sei E_n dieser Grenzwert.

Beh.: $p_n(E_{n+1}) = E_n \ \forall n \in \mathbb{N}$. Sei dazu $n \in \mathbb{N}$. Nun ex. ein $m_0 \in \mathbb{N}$, s.d. $E_{n+1} = D_{n+1,m_0}$ und $E_n = D_{n,m_0} = D_{n,m_0+1}$. Damit folgt

$$\begin{aligned} p_n(E_{n+1}) &= p_n(D_{n+1,m_0}) \\ &= p_n((p_{n+1} \circ \ldots \circ p_{n+m_0})(D_{n+1+m_0})) \\ &= (p_n \circ p_{n+1} \circ \ldots \circ p_{n+m_0})(D_{n+m_0+1}) \\ &= D_{n,m_0+1} \\ &= E_n. \end{aligned}$$

Also sind die Einschränkungen $p_n|_{E_{n+1}} : E_{n+1} \to E_n$ surjektiv, $E_n \neq \emptyset$ und endlich, also folgt nach der Vorüberlegung $\varprojlim (E_n, p_n|_{E_n}) \neq \emptyset$, also insbesondere $D \neq \emptyset$. □

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ Polynome in den ganzen p-adischen Zahlen. Dann sind äquivalent:

(i) *Die $f^{(i)}$ haben eine gemeinsame Nullstelle in $(\mathbb{Z}_p)^m$.*

(ii) *Für $n \in \mathbb{N}$ haben die Polynome $f^{(i)}$ $(mod\ p^n)$ eine gemeinsame Nullstelle in $(A_n)^m$.*

Beweis.

Sei $D = \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\} \subseteq (\mathbb{Z}_p)^m$ und $D_n := \{$ gemeinsame NS von $f^{(i)}$ in $(A_n)^m \pmod{p^n}\}$. Es bezeichne $(\phi_n)^m \colon (A_{n+1})^m \to (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet. Dann ist $(D_n, (\phi_n)^m)$ ein projektives System mit $D = \varprojlim (D_n, (\phi_n)^m)$.

Sei nun $D \neq \emptyset$ und $x \in D$. Dann ist $\pi_n(x) \in D_n\ \forall n \in \mathbb{N}$. Seien umgekehrt $D_n \neq \emptyset\ \forall n \in \mathbb{N}$. Da $D_n \subseteq A_n$ endlich folgt mit 2.27 $D \neq \emptyset$. □

Definition 2.29

Ein Element $x = (x_1, \ldots, x_m) \in (\mathbb{Z}_p)^m$ (bzw. $(A_n)^m$) heißt primitiv, falls ein $x_i \in \mathbb{Z}_p^\times$ (bzw. $\in A_n^\times$) ist.

Definition 2.30

Sei R ein Ring. Ein Polynom $f \in R[X_1, \ldots, X_m]$ heißt homogen vom Grad 2, falls in $R[X_1, \ldots, X_m][T]$ gilt

$$f(TX_1, \ldots, TX_m) = T^k f(X_1, \ldots, X_m).$$

Ein homogenes Polynom vom Grad 2 heißt quadratische Form.

Beispiel 2.31

Das Polynom $f = X^5 + X^3Y^2 + XY^4 \in \mathbb{Z}[X, Y]$ ist homogen, aber $g = X^2 + X + Y^2 \in \mathbb{Z}[X, Y]$ ist nicht homogen.

Korollar 2.32

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ *homogene Polynome. Dann sind äquivalent*

(i) *Die* $f^{(i)}$ *haben eine nichttriviale gemeinsame Nullstelle in* $(\mathbb{Q}_p)^m$.

(ii) *Die* $f^{(i)}$ *haben eine gemeinsame primitive Nullstelle in* $(\mathbb{Z}_p)^m$.

(iii) *Für* $n \in \mathbb{N}$ *haben die Polynome* $f^{(i)}$ $(mod\ p^n)$ *eine gemeinsame primitive Nullstelle.*

Beweis.

(i) $\Longrightarrow$ (ii): Sei $x = (x_1, \ldots, x_m)$ eine nichttriviale gemeinsame Nullstelle der $f^{(i)}$. Dann setze

$$k := \min(v_p(x_1), \ldots, v_p(x_m)) \text{ und } y = p^{-k}x.$$

Sei $i \in \{1, \ldots, m\}$, s.d. $k = v_p(x_i)$. Dann ist $v_p(y_i) = v_p(p^{-k}) + v_p(x_i) = -k + k = 0$. Also $y_i \in \mathbb{Z}_p^\times$ und damit y primitiv. Außerdem gilt für ein $n \in \mathbb{N}$

$$f^{(i)}(y) = f^{(i)}(p^{-k}x) \overset{\text{Homog.}}{=} p^{-nk} f^{(i)}(x) = 0.$$

(ii) $\Longrightarrow$ (i) ist trivial und (ii) $\Longleftrightarrow$ (iii) folgt aus 2.28. $\square$

Bemerkung 2.33

Die Voraussetzung homogenes Polynom ist notwendig, wie am Beispiel:

$$f = pX - 1 \in \mathbb{Z}_p[X]$$

deutlich wird, denn $f(p^{-1}) = 0$, aber im Körper $\mathbb{Q}_p$ hat das lineare Polynom f maximal eine Nullstelle und $p^{-1} \notin \mathbb{Z}_p$.

Wir möchten nun betrachten, unter welchen Umständen eine Lösung $\pmod{p^n}$ zu einer echten Lösung in $\mathbb{Z}_p$ entwickelt werden kann. Dazu verwenden wir die p-adische Version des Newton Verfahrens.

Lemma 2.34 (Henselsches Lemma)

Sei $f = a_m X^m + \ldots + a_0 \in \mathbb{Z}_p[X]$ *und*
$f' = a_m m X^{m-1} + \ldots + a_1 \in \mathbb{Z}_p[X]$ *seine Ableitung. Weiter sei*
$x \in \mathbb{Z}_p$, *s.d.* $f(x) \equiv 0 \ (mod\ p^n)$ *für ein* $n \in \mathbb{N}$ *und* $v_p(f'(x)) = k$
mit $0 \leq 2k < n$. *Dann existiert ein* $y \in \mathbb{Z}_p$, *s.d.*

$$f(y) \equiv 0 \ (mod\ p^{n+1}), v_p(f'(y)) = k \text{ und } y \equiv x \ (mod\ p^{n-k}).$$

hi

Beweis.

Nach Voraussetzung ist $f(x) = p^n b$ und $f'(x) = p^k c$ mit $b \in \mathbb{Z}_p$ und $c \in \mathbb{Z}_p^\times$. Dann setze $z := -bc^{-1}$ und $y := x + p^{n-k}z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

$$a_i y^i = a_i \sum_{j=0}^{i} \binom{i}{j} x^{i-j} (p^{n-k}z)^j = a_i x^i + a_i i x^{i-1} p^{n-k} z + p^{2n-2k} z^2 R_i$$

für $R_i \in \mathbb{Z}_p$. Aufsummieren und addieren von a_0 liefert mit $R \in \mathbb{Z}_p$ eine „Taylorentwicklung”:

$$f(y) = f(x) + p^{n-k} z f'(x) + p^{2n-2k} z^2 R.$$

Da $2k < n$ folgt $2n - 2k \geq n + 1$. Einsetzen liefert nun

$$\begin{aligned} f(y) &= p^n b - p^{n-k} b c^{-1} p^k c + p^{2n-2k} z^2 R \\ &= p^{2n-2k} z^2 R \\ &\equiv 0 \pmod{p^{n+1}}. \end{aligned}$$

Anwenden der „Taylorentwicklung" auf f' liefert

$$\begin{aligned} f'(y) &= f'(x) + p^{n-k} z f''(x) + p^{2n-2k} z^2 R \\ &= p^k c + p^{n-k} z f''(x) + p^{2n-2k} z^2 R \\ &= p^k (\underbrace{c + p^{n-2k} z f''(x) + p^{2n-3k} z^2 R}_{=:s}). \end{aligned}$$

Es ist $n - 2k > 0$ und $2n - 3k > 0$, aber $c \in \mathbb{Z}_p^\times$, also $p \nmid s$ und damit $s \in \mathbb{Z}_p^\times$ und $v_p(f'(y)) = k$. □

Zum Studium der quadratischen Formen benötigen wir noch die auf m Variablen verallgemeinerte Version des Henselschen Lemmas.

Satz 2.35

Sei $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ und $x = (x_i) \in (\mathbb{Z}_p)^m$, s.d. $f(x) \equiv 0 \ (mod\ p^n)$. Weiter existiere ein $1 \leq j \leq m$, s.d. $v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k$ mit $0 \leq 2k < n$. Dann existiert eine Nullstelle $y \in (\mathbb{Z}_p)^m$ von f mit $y \equiv x \ (mod\ p^{n-k})$.

Beweis.

Sei zunächst $m = 1$. Mit 2.34 angewendet auf $x^{(0)} := x$, erhält man $x^{(1)} \in \mathbb{Z}_p$ mit

$$f(x^{(1)}) \equiv 0 \pmod{p^{n+1}},\ v_p(f'(x^{(1)})) = k \text{ und } x^{(1)} \equiv x^{(0)} \pmod{p^{n-k}}.$$

Wende 2.34 nun auf $x^{(1)}$ und $n+1$ an. Induktiv erhält man eine Folge $(x^{(q)})_{q\in\mathbb{N}}$ mit den Eigenschaften

$$x^{(q+1)} \equiv x^{(q)} \pmod{p^{n+q-k}} \text{ und } f(x^{(q)}) \equiv 0 \pmod{p^{n+q}}.$$

Es gilt nun $v_p(x^{(q+1)} - x^{(q)}) \geq n + q - k$, also $d(x^{(q+1)}, x^{(q)}) \xrightarrow{q\to\infty} 0$. Also ist $x^{(q)}$ eine Cauchy Folge und konvergiert gegen ein $y \in \mathbb{Z}_p$. Dann gilt

$$0 = \lim_{q\to\infty} f(x^{(q)}) = f(\lim_{q\to\infty} x^{(q)}) = f(y)$$

und $y \equiv x \pmod{p^{n-k}}$.

Sei nun $m > 1$. Ersetze in f die Variablen X_i durch x_i für $i \neq j$. Dann sei $g \in \mathbb{Z}_p[X_j]$ das entstandene Polynom in einer Variablen. Wende nun den Fall für $m = 1$ auf g an. Dann erhalten wir ein $y_j \in \mathbb{Z}_p$ mit $y_j \equiv x_j \pmod{p^{n-k}}$ und $g(y_j) = 0$. Setze nun $y_i := x_i$ für $i \neq j$. Dann ist $y \equiv x \pmod{p^{n-k}}$ und

$$f(y) = f(y_1, \ldots, y_m) = f(x_1, \ldots, x_{j-1}, y_j, x_{j+1}, \ldots, x_m) = g(y_j) = 0.$$

□

Aus dem letzten Satz können wir einfache Schlussfolgerungen für quadratische Formen ziehen.

Korollar 2.36

Sei $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ *und* $x \in \mathbb{Z}_p$ *mit*

$$f(x) \equiv 0 \ (mod\ p)$$

und es sei mind. eine partielle Ableitung $\frac{\partial f}{\partial X_j}(x) \not\equiv 0 \ (mod\ p)$*, dann hebt sich* x *zu einer echten Nullstelle.*

Beweis.

Das ist der Fall $n = 1$ und $k = 0$ in 2.35. □

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^{m} \sum_{j=1}^{m} a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \ldots, X_m]$ eine quadratische Form mit $a_{ij} = a_{ji}$ und sei $p \nmid \det(a_{ij})$. Sei weiter $a \in \mathbb{Z}_p$. Dann hebt sich jede primitive Lösung der Gleichung $f(x) \equiv a \pmod{p}$ zu einer echten Lösung.

Beweis.

Mit 2.36 g.z.z., dass mind. eine partielle Ableitung $\pmod{p}$ nicht verschwindet. Sei $A = (a_{ij}) \in \mathbb{Z}_p^{m \times m}$. Da $\det(a_{ij}) \not\equiv 0 \pmod{p}$ folgt $\det(a_{ij}) \in \mathbb{F}_p^{\times}$ und damit $\ker A = \{0\}$. Es gilt weiter

$$\frac{\partial f}{\partial X_i} = 2 \sum_{j=1}^{m} a_{ij} X_j \text{ also } \begin{pmatrix} \partial_{X_i} f(x) \\ \vdots \\ \partial_{X_m} f(x) \end{pmatrix} = 2Ax.$$

Da x primitiv ist $x \neq 0 \in \mathbb{F}_p^m$ und damit mind. eine partielle Ableitung $\not\equiv 0 \pmod{p}$. □