

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.

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,

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.

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

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

$$m = a_0 + a_1p + \dots + a_np^n$$

wobei die Koeffizienten a_i in $\{0, 1, \dots, p-1\}$ liegen.

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

$$m = a_0 + a_1p + \dots + a_np^n$$

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

Beispiel 2.1

Für $n = 216$ erhalten wir für $p = 5$

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

Beispiel 2.1

Für $n = 216$ erhalten wir für $p = 5$

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

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 $i \in \mathbb{N}_0$.

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.

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,

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

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

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?

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?

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 $a \in \mathbb{Z}$.

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

$$a \equiv a_0 + a_1p + a_2p^2 + \dots + a_{n-1}p^{n-1} \pmod{p^n}$$

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

Beweis.

Per Induktion.

Beweis.

Per Induktion. Für $n = 1$ ist offenbar $a \equiv a_0 \pmod{p}$ mit $0 \leq a_0 < p$.

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.

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.

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

$$a \equiv a_0 + a_1p + a_2p^2 + \dots + a_{n-2}p^{n-2} \pmod{p^{n-1}}.$$

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

$$a \equiv a_0 + a_1p + a_2p^2 + \dots + a_{n-2}p^{n-2} \pmod{p^{n-1}}.$$

Also

$$a = a_0 + a_1p + a_2p^2 + \dots + a_{n-2}p^{n-2} + gp^{n-1}$$

für ein $g \in \mathbb{Z}$.

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

$$a \equiv a_0 + a_1p + a_2p^2 + \dots + a_{n-2}p^{n-2} \pmod{p^{n-1}}.$$

Also

$$a = a_0 + a_1p + a_2p^2 + \dots + a_{n-2}p^{n-2} + gp^{n-1}$$

für ein $g \in \mathbb{Z}$. Sei $0 \leq a_{n-1} < p$,

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

$$a \equiv a_0 + a_1p + a_2p^2 + \dots + a_{n-2}p^{n-2} \pmod{p^{n-1}}.$$

Also

$$a = a_0 + a_1p + a_2p^2 + \dots + a_{n-2}p^{n-2} + gp^{n-1}$$

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 $h \in \mathbb{Z}$.

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

$$a \equiv a_0 + a_1p + a_2p^2 + \dots + a_{n-2}p^{n-2} \pmod{p^{n-1}}.$$

Also

$$a = a_0 + a_1p + a_2p^2 + \dots + a_{n-2}p^{n-2} + gp^{n-1}$$

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

$$a = a_0 + \dots + a_{n-2}p^{n-2} + a_{n-1}p^{n-1} + hp^n$$



Jede ganze Zahl a definiert eine Folge von Restklassen

$$\overline{s_n} = \overline{a} \in \mathbb{Z}/p^n\mathbb{Z} \text{ für } n \in \mathbb{N},$$

Jede ganze Zahl a definiert 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

$$s_1 \equiv a_0 \pmod{p}$$

$$s_2 \equiv a_0 + a_1 p \pmod{p^2}$$

$$\vdots$$

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

Jede ganze Zahl a definiert 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

$$s_1 \equiv a_0 \pmod{p}$$

$$s_2 \equiv a_0 + a_1 p \pmod{p^2}$$

$$\vdots$$

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

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

Jede ganze Zahl a definiert 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

$$s_1 \equiv a_0 \pmod{p}$$

$$s_2 \equiv a_0 + a_1 p \pmod{p^2}$$

$$\vdots$$

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

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

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 ?

Beispiel 2.5

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

Beispiel 2.5

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

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

Beispiel 2.5

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

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

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

Beispiel 2.5

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

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

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

Es ist also $-1 = (p-1) + (p-1)p + (p-1)p^2 + \dots \in \mathbb{Z}_p$ 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.

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.

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 einige Begriffe.

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 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 $p_n: D_{n+1} \rightarrow D_n$

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

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 $p_n: D_{n+1} \rightarrow D_n$

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

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.

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 $p_n: D_{n+1} \rightarrow D_n$

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

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).

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

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

$$\begin{aligned}\phi_n: A_{n+1} &\rightarrow A_n \\ \bar{a} &\mapsto a \bmod p^n.\end{aligned}$$

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

$$\begin{aligned}\phi_n: A_{n+1} &\rightarrow A_n \\ \bar{a} &\mapsto a \bmod p^n.\end{aligned}$$

Es ist also für $a \in A_{n+1}$, $b \in A_n$: $\phi_n(a) = b \iff a \equiv b \pmod{p^n}$.

Satz 2.8

Ordnet man jeder ganzen p -adischen Zahl

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

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

$$\bar{s}_n = \sum_{i=0}^{n-1} a_i p^i \pmod{p^n} \in A_n$$

zu,

Satz 2.8

Ordnet man jeder ganzen p -adischen Zahl

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

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

$$\bar{s}_n = \sum_{i=0}^{n-1} a_i p^i \pmod{p^n} \in A_n$$

zu, so erhält man eine Bijektion

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

Beweis.

Die Zuordnung ist wohldefiniert, da

$$s_{n+1} = a_0 + a_1p + \dots + a_np^n \equiv a_0 + a_1p + \dots + a_{n-1}p^{n-1} \pmod{p^n} = s_n.$$

Beweis.

Die Zuordnung ist wohldefiniert, da

$$s_{n+1} = a_0 + a_1p + \dots + a_np^n \equiv a_0 + a_1p + \dots + a_{n-1}p^{n-1} \pmod{p^n} = s_n.$$

Bijektivität: Sei $(x_n)_{n \in \mathbb{N}} \in \varprojlim (A_n, \phi_n)$.

Beweis.

Die Zuordnung ist wohldefiniert, da

$$s_{n+1} = a_0 + a_1p + \dots + a_np^n \equiv a_0 + a_1p + \dots + a_{n-1}p^{n-1} \pmod{p^n} = s_n.$$

Bijektivität: Sei $(x_n)_{n \in \mathbb{N}} \in \varprojlim (A_n, \phi_n)$. Dann ist $\phi_n(x_{n+1}) = x_n$,

Beweis.

Die Zuordnung ist wohldefiniert, da

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

Bijektivität: Sei $(x_n)_{n \in \mathbb{N}} \in \varprojlim (A_n, \phi_n)$. Dann ist $\phi_n(x_{n+1}) = x_n$, also $x_{n+1} \equiv x_n \pmod{p^n}$ für $n \in \mathbb{N}$.

Beweis.

Die Zuordnung ist wohldefiniert, da

$$s_{n+1} = a_0 + a_1p + \dots + a_np^n \equiv a_0 + a_1p + \dots + a_{n-1}p^{n-1} \pmod{p^n} = s_n.$$

Bijektivität: Sei $(x_n)_{n \in \mathbb{N}} \in \varprojlim (A_n, \phi_n)$. Dann ist $\phi_n(x_{n+1}) = x_n$, also $x_{n+1} \equiv x_n \pmod{p^n}$ für $n \in \mathbb{N}$. Insbesondere ex. nach 2.4 eindeutige Koeffizienten $0 \leq a_i < p$,

Beweis.

Die Zuordnung ist wohldefiniert, da

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

Bijektivität: Sei $(x_n)_{n \in \mathbb{N}} \in \varprojlim (A_n, \phi_n)$. Dann ist $\phi_n(x_{n+1}) = x_n$, also $x_{n+1} \equiv x_n \pmod{p^n}$ für $n \in \mathbb{N}$. Insbesondere ex. nach 2.4 eindeutige Koeffizienten $0 \leq a_i < p$, s.d.

$$x_n \equiv a_0 + a_1 p + \dots + a_{n-1} p^{n-1} \pmod{p^n}$$

für alle $n \in \mathbb{N}$.

Beweis.

Die Zuordnung ist wohldefiniert, da

$$s_{n+1} = a_0 + a_1p + \dots + a_np^n \equiv a_0 + a_1p + \dots + a_{n-1}p^{n-1} \pmod{p^n} = s_n.$$

Bijektivität: Sei $(x_n)_{n \in \mathbb{N}} \in \varprojlim (A_n, \phi_n)$. Dann ist $\phi_n(x_{n+1}) = x_n$, also $x_{n+1} \equiv x_n \pmod{p^n}$ für $n \in \mathbb{N}$. Insbesondere ex. nach 2.4 eindeutige Koeffizienten $0 \leq a_i < p$, s.d.

$$x_n \equiv a_0 + a_1p + \dots + a_{n-1}p^{n-1} \pmod{p^n}$$

für alle $n \in \mathbb{N}$. Also ist $x = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ das eindeutige Urbild von $(x_n)_{n \in \mathbb{N}}$. □

Bemerkung 2.9

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

$$a \equiv a_0 + a_1p + \dots + a_{n-1}p^{n-1} \pmod{p^n}$$

mit $0 \leq a_i < p$.

Bemerkung 2.9

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

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

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

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

Bemerkung 2.9

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

$$a \equiv a_0 + a_1p + \dots + a_{n-1}p^{n-1} \pmod{p^n}$$

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

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

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

Bemerkung 2.9

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

$$a \equiv a_0 + a_1p + \dots + a_{n-1}p^{n-1} \pmod{p^n}$$

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

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

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

Beispiel 2.10 (2.5 fortgesetzt)

Mit 2.9 folgt also

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

Beispiel 2.10 (2.5 fortgesetzt)

Mit 2.9 folgt also

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

Wir identifizieren nun im Folgenden stets $\mathbb{Z}_p = \varprojlim (A_n, \phi_n)$.

Beispiel 2.10 (2.5 fortgesetzt)

Mit 2.9 folgt also

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

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

Beispiel 2.10 (2.5 fortgesetzt)

Mit 2.9 folgt also

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

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

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“:

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

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 $\prod_{n=1}^{\infty} A_n$,

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

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

Bemerkung 2.12

1. Erinnerung:

Bemerkung 2.12

1. Erinnerung: $(X, \mathcal{T})$ mit $\mathcal{T} \subseteq \mathcal{P}(X)$ heißt topologischer Raum und $\mathcal{T}$ das System der offenen Teilmengen,

Bemerkung 2.12

1. Erinnerung: $(X, \mathcal{T})$ mit $\mathcal{T} \subseteq \mathcal{P}(X)$ heißt topologischer Raum und $\mathcal{T}$ das System der offenen Teilmengen, falls endl. Schnitte und beliebige Vereinigungen offener Mengen wieder offen sind.

Bemerkung 2.12

1. Erinnerung: $(X, \mathcal{T})$ mit $\mathcal{T} \subseteq \mathcal{P}(X)$ heißt topologischer Raum und $\mathcal{T}$ das System der offenen Teilmengen, falls endl. Schnitte und beliebige Vereinigungen offener Mengen wieder offen sind.
2. Versieht man A_n mit der diskreten Topologie (d.h. alle Teilmengen sind offen)

Bemerkung 2.12

1. Erinnerung: $(X, \mathcal{T})$ mit $\mathcal{T} \subseteq \mathcal{P}(X)$ heißt topologischer Raum und $\mathcal{T}$ das System der offenen Teilmengen, falls endl. Schnitte und beliebige Vereinigungen offener Mengen wieder offen sind.
2. 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),

Bemerkung 2.12

1. Erinnerung: $(X, \mathcal{T})$ mit $\mathcal{T} \subseteq \mathcal{P}(X)$ heißt topologischer Raum und $\mathcal{T}$ das System der offenen Teilmengen, falls endl. Schnitte und beliebige Vereinigungen offener Mengen wieder offen sind.
2. 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.

Bemerkung 2.12

1. Erinnerung: $(X, \mathcal{T})$ mit $\mathcal{T} \subseteq \mathcal{P}(X)$ heißt topologischer Raum und $\mathcal{T}$ das System der offenen Teilmengen, falls endl. Schnitte und beliebige Vereinigungen offener Mengen wieder offen sind.
2. 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 2.13 (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.

Satz 2.13 (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.

Satz 2.13 (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*.

Satz 2.13 (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 2.14

$\mathbb{Z}_p$ ist kompakt.

Korollar 2.14

$\mathbb{Z}_p$ ist kompakt.

Beweis.

Nach 2.13 ist $\prod_{n=1}^{\infty} A_n$ kompakt.

Korollar 2.14

$\mathbb{Z}_p$ ist kompakt.

Beweis.

Nach 2.13 ist $\prod_{n=1}^{\infty} A_n$ kompakt. Außerdem ist

Korollar 2.14

$\mathbb{Z}_p$ ist kompakt.

Beweis.

Nach 2.13 ist $\prod_{n=1}^{\infty} A_n$ kompakt. Außerdem ist

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

Korollar 2.14

$\mathbb{Z}_p$ ist kompakt.

Beweis.

Nach 2.13 ist $\prod_{n=1}^{\infty} A_n$ kompakt. Außerdem ist

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

Korollar 2.14

$\mathbb{Z}_p$ ist kompakt.

Beweis.

Nach 2.13 ist $\prod_{n=1}^{\infty} A_n$ kompakt. Außerdem ist

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

mit $f_n: \prod_{n=1}^{\infty} A_n \rightarrow A_n, x \mapsto \phi_n(\pi_{n+1}(x)) - \pi_n(x)$.

Korollar 2.14

$\mathbb{Z}_p$ ist kompakt.

Beweis.

Nach 2.13 ist $\prod_{n=1}^{\infty} A_n$ kompakt. Außerdem ist

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

mit $f_n: \prod_{n=1}^{\infty} A_n \rightarrow A_n, x \mapsto \phi_n(\pi_{n+1}(x)) - \pi_n(x)$. Es ist f_n stetig, da π_n per Definition der Produkttopologie und ϕ_n als Abbildung zwischen diskreten Räumen stetig sind.

Korollar 2.14

$\mathbb{Z}_p$ ist kompakt.

Beweis.

Nach 2.13 ist $\prod_{n=1}^{\infty} A_n$ kompakt. Außerdem ist

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

mit $f_n: \prod_{n=1}^{\infty} A_n \rightarrow A_n, x \mapsto \phi_n(\pi_{n+1}(x)) - \pi_n(x)$. 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 2.15

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

Lemma 2.15

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

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

Lemma 2.15

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.

Lemma 2.15

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. $\ker \pi_n = p^n \mathbb{Z}_p$.

Lemma 2.15

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 $x \in \mathbb{Z}_p$.

Lemma 2.15

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

Lemma 2.15

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 $\pi_n(p^n x) = 0$.

Lemma 2.15

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 $p^n \mathbb{Z}_p \subseteq \ker \pi_n$.

Lemma 2.15

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 $m \geq n$.

Lemma 2.15

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

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

Lemma 2.15

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)

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

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.

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 $y_{m-n} \in A_{m-n}$,

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.
 $p^n y_{m-n} \equiv x_m \pmod{p^m}$.

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.
 $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Es bleibt zu zeigen, dass $p^n y = x$.

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.
 $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Es bleibt zu zeigen, dass $p^n y = x$.
Z.z.: $x = p^n y$.

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.
 $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Es bleibt zu zeigen, dass $p^n y = x$.
Z.z.: $x = p^n y$. Für $m \leq n$ ist $x_m = 0 = p^n y_m$.

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.
 $p^n y_{m-n} \equiv x_m \pmod{p^m}$. 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

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

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.
 $p^n y_{m-n} \equiv x_m \pmod{p^m}$. 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 $x = p^n y$.

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.
 $p^n y_{m-n} \equiv x_m \pmod{p^m}$. 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 $\ker \pi_n = p^n \mathbb{Z}_p$.

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.
 $p^n y_{m-n} \equiv x_m \pmod{p^m}$. 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.

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.
 $p^n y_{m-n} \equiv x_m \pmod{p^m}$. 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 2.16

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.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii).

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). Sei dazu $u = (\overline{u_n})_{n \in \mathbb{N}} \in \mathbb{Z}_p^\times$.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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 $p \nmid u_1 \implies \overline{u_1} \neq 0$.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ also insbesondere $p \nmid u_1 \implies \overline{u_1} \neq 0$. Sei umgekehrt $\overline{u_1} \neq 0$.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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 $n \in \mathbb{N}$.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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

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

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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

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

Da p prim folgt insbesondere $(p^n, u_n) = 1$.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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

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

Da p prim folgt insbesondere $(p^n, u_n) = 1$. Also ex.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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

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

Da p prim folgt insbesondere $(p^n, u_n) = 1$. Also ex. nach euklid.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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

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

Da p prim folgt insbesondere $(p^n, u_n) = 1$. Also ex. nach euklid. Alg.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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

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

Da p prim folgt insbesondere $(p^n, u_n) = 1$. Also ex. nach euklid. Alg. $a, b \in \mathbb{Z}$,

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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

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

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 $\overline{b} \in A_n$.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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

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

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 $v := (\dots \overline{u_n}^{-1}, \overline{u_{n-1}}^{-1}, \dots, \overline{u_1}^{-1}) = u^{-1} \in \mathbb{Z}_p$.

Beweis.

(ii) $\iff$ (iii) ist klar wegen Kompatibilität. b.z.z. (i) $\iff$ (iii). 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. $\overline{u_1} \overline{v_1} \equiv 1 \pmod{p}$ 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

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

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
 $v := (\dots \overline{u_n}^{-1}, \overline{u_{n-1}}^{-1}, \dots, \overline{u_1}^{-1}) = u^{-1} \in \mathbb{Z}_p.$



Lemma 2.17

Für $x \in \mathbb{Z}_p \setminus \{0\}$ ex.

Lemma 2.17

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

Lemma 2.17

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

$$x = p^n u.$$

Lemma 2.17

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.

Lemma 2.17

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 $x \in \mathbb{Z}_p \setminus \{0\}$.

Lemma 2.17

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.

Lemma 2.17

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,

Lemma 2.17

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. $x_n = \pi_n(x) = 0$.

Lemma 2.17

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.

Lemma 2.17

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. $x_n = \pi_n(x) \neq 0$. Also ist $x \in \ker \pi_{n+1}$, insbesondere ex. nach 2.15 ein $u \in \mathbb{Z}_p$ mit $x = p^{n+1}u$.

Lemma 2.17

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 2.15 ein $u \in \mathbb{Z}_p$ mit $x = p^n u$. Ang.

Lemma 2.17

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 2.15 ein $u \in \mathbb{Z}_p$ mit $x = p^n u$. Ang.: $p \mid u$, dann ist $\pi_1(u) = 0$ also ex.

Lemma 2.17

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. $x_n = \pi_n(x) \neq 0$. Also ist $x \in \ker \pi_{n+1}$, insbesondere ex. nach 2.15 ein $u \in \mathbb{Z}_p$ mit $x = p^{n+1}u$. Ang.: $p \mid u$, dann ist $\pi_1(u) = 0$ also ex. wieder nach 2.15 ein $v \in \mathbb{Z}_p$ mit $u = pv$.

Lemma 2.17

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 2.15 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 2.15 ein $v \in \mathbb{Z}_p$ mit $u = pv$. Dann ist aber

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

Lemma 2.17

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 2.15 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 2.15 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 .

Lemma 2.17

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 2.15 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 2.15 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 $n, m \in \mathbb{N}_0$.

(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. $n \geq m$.

(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 $0 = \pi_n(x) = \pi_n(p^m) \pi_n(v)$.

(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.

(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 $m \geq n$.

(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 $m = n$.

(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 $p^n(u - v) = 0$.

(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.

(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. $u - v \neq 0$.

(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 $w \in \mathbb{Z}_p^\times$.

(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 $0 = p^n(u - v) = p^{n+k} w$.

(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 $0 = p^{n+k} \in \mathbb{Z} \nmid$.

(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 $0 = p^{n+k} \in \mathbb{Z} \nrightarrow$.



Definition 2.18 (p -Bewertung)

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

Definition 2.18 (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 $v_p(0) := \infty$.

Definition 2.18 (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 .

Definition 2.18 (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 2.19

Wegen 2.17 ist die p -Bewertung wohldefiniert.

Definition 2.18 (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 2.19

Wegen 2.17 ist die p -Bewertung wohldefiniert.

Per Konvention setze $n + \infty = \infty$ und $\infty > n$ für $n \in \mathbb{N}_0$.

Definition 2.18 (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 2.19

Wegen 2.17 ist die p -Bewertung wohldefiniert.

Per Konvention setze $n + \infty = \infty$ und $\infty > n$ für $n \in \mathbb{N}_0$.

Lemma 2.20 (Eigenschaften der p -Bewertung)

Für $x, y \in \mathbb{Z}_p$ gilt

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

Lemma 2.20 (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.

Lemma 2.20 (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 2.21

$\mathbb{Z}_p$ ist nullteilerfrei.

Korollar 2.21

$\mathbb{Z}_p$ ist nullteilerfrei.

Beweis.

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

Korollar 2.21

$\mathbb{Z}_p$ ist nullteilerfrei.

Beweis.

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

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

Korollar 2.21

$\mathbb{Z}_p$ 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 $y = 0$.

Korollar 2.21

$\mathbb{Z}_p$ 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 2.22 (Topologie auf $\mathbb{Z}_p$)

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

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

Lemma 2.22 (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.

Lemma 2.22 (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.

Bemerkung 2.23 (Bälle)

Es sei im Folgenden stets

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

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

Lemma 2.22 (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.

Bemerkung 2.23 (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

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

Beweisskizze.

Grobe Beweisschritte

- ▶ $d(\cdot, \cdot)$ ist eine Metrik.



Beweisskizze.

Grobe Beweisschritte

- ▶ $d(\cdot, \cdot)$ ist eine Metrik.
- ▶ Die offenen Mengen $V \subseteq \mathbb{Z}_p$ bezüglich der Produkttopologie sind von der Form

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



Beweisskizze.

Grobe Beweisschritte

- ▶ $d(\cdot, \cdot)$ ist eine Metrik.
- ▶ Die offenen Mengen $V \subseteq \mathbb{Z}_p$ bezüglich der Produkttopologie sind von der Form

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

- ▶ Es ist $v + p^n \mathbb{Z}_p = B(v, e^{-(n-1)})$.



Beweisskizze.

Grobe Beweisschritte

- ▶ $d(\cdot, \cdot)$ ist eine Metrik.
- ▶ Die offenen Mengen $V \subseteq \mathbb{Z}_p$ bezüglich der Produkttopologie sind von der Form

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

- ▶ Es ist $v + p^n \mathbb{Z}_p = B(v, e^{-(n-1)})$.
- ▶ $v + p^n \mathbb{Z}_p$ offen bezüglich der Produkttopologie, da $p^n \mathbb{Z}_p = \ker \pi_n = \pi_n^{-1}(\{0\})$.



Z.z.: $\mathbb{Z}_p$ vollständig.

Z.z.: $\mathbb{Z}_p$ vollständig. Da $\mathbb{Z}_p$ nach 2.14 kompakt ist, hat jede Folge in $\mathbb{Z}_p$ eine konvergente Teilfolge.

Z.z.: $\mathbb{Z}_p$ vollständig. Da $\mathbb{Z}_p$ nach 2.14 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 $\mathbb{Z}_p$.



Definition 2.24

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

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

Definition 2.24

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

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

Bemerkung 2.25

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,

Bemerkung 2.25

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 2.17 ist

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

Bemerkung 2.25

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 2.17 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 und $d(\cdot, \cdot)$ auf $\mathbb{Q}_p$ fort.

Bemerkung 2.25

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 2.17 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 und $d(\cdot, \cdot)$ auf $\mathbb{Q}_p$ fort.
Es gilt

$$x \in \mathbb{Z}_p \iff v_p(x) \geq 0 \iff v_p(x) > -1 \iff x \in B(0, e).$$

Bemerkung 2.25

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 2.17 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 und $d(\cdot, \cdot)$ auf $\mathbb{Q}_p$ fort.
Es gilt

$$x \in \mathbb{Z}_p \iff v_p(x) \geq 0 \iff v_p(x) > -1 \iff x \in B(0, e).$$

2. Nach (1) ist also $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.

Bemerkung 2.25

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 2.17 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 und $d(\cdot, \cdot)$ auf $\mathbb{Q}_p$ fort.
Es gilt

$$x \in \mathbb{Z}_p \iff v_p(x) \geq 0 \iff v_p(x) > -1 \iff x \in B(0, e).$$

2. Nach (1) ist also $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.

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 $|\cdot|$).

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 $|\cdot|$). Somit ist auch $\mathbb{Q}$ dicht in $\mathbb{Q}_p$.

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 $|\cdot|$). Somit ist auch $\mathbb{Q}$ dicht in $\mathbb{Q}_p$.
2. Es ist leicht nachzurechnen, dass $d(\cdot, \cdot)$ die ultrametrische Ungleichung (auch starke Dreiecksungleichung) erfüllt,

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 $|\cdot|$). Somit ist auch $\mathbb{Q}$ dicht in $\mathbb{Q}_p$.
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 $x, y, z \in \mathbb{Q}_p$.

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 $|\cdot|$). Somit ist auch $\mathbb{Q}$ dicht in $\mathbb{Q}_p$.
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,

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 $|\cdot|$). Somit ist auch $\mathbb{Q}$ dicht in $\mathbb{Q}_p$.
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 $\lim_{n \rightarrow \infty} (u_{n+1} - u_n) = 0$

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 $|\cdot|$). Somit ist auch $\mathbb{Q}$ dicht in $\mathbb{Q}_p$.
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 $\lim_{n \rightarrow \infty} (u_{n+1} - u_n) = 0$.

p -adische Gleichungen

Wir wollen nun Gleichungen in den ganzen p -adischen Zahlen untersuchen.

p -adische Gleichungen

Wir wollen nun Gleichungen in den ganzen p -adischen Zahlen untersuchen. Also Gleichungssysteme der folgenden Art

p -adische Gleichungen

Wir wollen nun Gleichungen in den ganzen p -adischen Zahlen untersuchen. Also Gleichungssysteme der folgenden Art

$$f^{(1)}(X_1, \dots, X_m) = 0$$

$$\vdots$$

$$f^{(r)}(X_1, \dots, X_m) = 0$$

mit Polynomen $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$.

Lemma 2.27

Sei $D_1 \leftarrow D_2 \leftarrow \dots$ ein projektives System und $D = \varprojlim (D_n, p_n)$ sein projektiver Limes.

Lemma 2.27

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

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ surjektiv.

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ surjektiv. Dann ex.

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ surjektiv. Dann ex. für alle $x_n \in D_n$ ein $x_{n+1} \in D_{n+1}$,

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ surjektiv. Dann ex. für alle $x_n \in D_n$ ein $x_{n+1} \in D_{n+1}$, s.d. $p_n(x_{n+1}) = x_n$.

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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.

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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 $m, n \in \mathbb{N}$:

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

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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 $m, n \in \mathbb{N}$:

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

Da $D_{n+m} \neq \emptyset$ folgt $D_{n,m} \neq \emptyset$ und da D_k endlich folgt $\#p_k(D_{k+1}) \leq \#D_{k+1} \forall k \in \mathbb{N}$.

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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 $m, n \in \mathbb{N}$:

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

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 .

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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 $m, n \in \mathbb{N}$:

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

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,

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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 $m, n \in \mathbb{N}$:

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

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.

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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 $m, n \in \mathbb{N}$:

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

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 $m_0 \in \mathbb{N}$,

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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 $m, n \in \mathbb{N}$:

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

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. $D_{n,m_0} = D_{n,m} \forall m \geq m_0$.

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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 $m, n \in \mathbb{N}$:

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

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.

Lemma 2.27

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

Beweis.

Sei zunächst $p_n: D_{n+1} \rightarrow D_n$ 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 $m, n \in \mathbb{N}$:

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

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.

Nun ist $p_n(E_{n+1}) = E_n$ (nachrechnen).

Nun ist $p_n(E_{n+1}) = E_n$ (nachrechnen).

Also sind die Einschränkungen $p_n|_{E_{n+1}}: E_{n+1} \rightarrow E_n$ surjektiv,

Nun ist $p_n(E_{n+1}) = E_n$ (nachrechnen).

Also sind die Einschränkungen $p_n|_{E_{n+1}}: E_{n+1} \rightarrow E_n$ surjektiv,
 $E_n \neq \emptyset$ und endlich,

Nun ist $p_n(E_{n+1}) = E_n$ (nachrechnen).

Also sind die Einschränkungen $p_n|_{E_{n+1}}: E_{n+1} \rightarrow E_n$ surjektiv, $E_n \neq \emptyset$ und endlich, also folgt nach der Vorüberlegung

$$\varprojlim (E_n, p_n|_{E_n}) \neq \emptyset,$$

Nun ist $p_n(E_{n+1}) = E_n$ (nachrechnen).

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

Nun ist $p_n(E_{n+1}) = E_n$ (nachrechnen).

Also sind die Einschränkungen $p_n|_{E_{n+1}}: E_{n+1} \rightarrow E_n$ 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 $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ Polynome in den ganzen p -adischen Zahlen.

Satz 2.28

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

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

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ eine gemeinsame Nullstelle in $(A_n)^m$.

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ 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 $D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}$.

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ 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 $D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}$. Es bezeichne $(\phi_n)^m: (A_{n+1})^m \rightarrow (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet.

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ 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 $D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}$. Es bezeichne $(\phi_n)^m: (A_{n+1})^m \rightarrow (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet. Dann ist $(D_n, (\phi_n)^m)$ ein projektives System mit $D = \varprojlim (D_n, (\phi_n)^m)$.

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ 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 $D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}$. Es bezeichne $(\phi_n)^m: (A_{n+1})^m \rightarrow (A_n)^m$ 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 $x \in D$.

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ 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 $D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}$. Es bezeichne $(\phi_n)^m: (A_{n+1})^m \rightarrow (A_n)^m$ 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 $\pi_n(x) \in D_n \forall n \in \mathbb{N}$.

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ 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 $D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}$. Es bezeichne $(\phi_n)^m: (A_{n+1})^m \rightarrow (A_n)^m$ 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 $D_n \neq \emptyset \forall n \in \mathbb{N}$.

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ 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 $D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}$. Es bezeichne $(\phi_n)^m: (A_{n+1})^m \rightarrow (A_n)^m$ 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 $D \neq \emptyset$.

Satz 2.28

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ 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 $D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}$. Es bezeichne $(\phi_n)^m: (A_{n+1})^m \rightarrow (A_n)^m$ 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 $x = (x_1, \dots, x_m) \in (\mathbb{Z}_p)^m$ (bzw.

Definition 2.29

Ein Element $x = (x_1, \dots, x_m) \in (\mathbb{Z}_p)^m$ (bzw. $\in (A_n)^m$) heit primitiv, falls ein $x_i \in \mathbb{Z}_p^\times$ (bzw.

Definition 2.29

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

Definition 2.29

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

Definition 2.30

Sei R ein Ring.

Definition 2.29

Ein Element $x = (x_1, \dots, x_m) \in (\mathbb{Z}_p)^m$ (bzw. $\in (A_n)^m$) 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 $f \in R[X_1, \dots, X_m]$ heißt homogen vom Grad k , falls in $R[X_1, \dots, X_m][T]$ gilt

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

Definition 2.29

Ein Element $x = (x_1, \dots, x_m) \in (\mathbb{Z}_p)^m$ (bzw. $\in (A_n)^m$) 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 $f \in R[X_1, \dots, X_m]$ heißt homogen vom Grad k , falls in $R[X_1, \dots, X_m][T]$ gilt

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

Ein homogenes Polynom vom Grad 2 heißt quadratische Form.

Definition 2.29

Ein Element $x = (x_1, \dots, x_m) \in (\mathbb{Z}_p)^m$ (bzw. $\in (A_n)^m$) 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 $f \in R[X_1, \dots, X_m]$ heißt homogen vom Grad k , falls in $R[X_1, \dots, X_m][T]$ gilt

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

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.

Definition 2.29

Ein Element $x = (x_1, \dots, x_m) \in (\mathbb{Z}_p)^m$ (bzw. $\in (A_n)^m$) 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 $f \in R[X_1, \dots, X_m]$ heißt homogen vom Grad k , falls in $R[X_1, \dots, X_m][T]$ gilt

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

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 $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ *homogene Polynome*.

Korollar 2.32

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

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

Korollar 2.32

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ *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 $(\mathbb{Z}_p)^m$.

Korollar 2.32

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ eine gemeinsame primitive Nullstelle.

Korollar 2.32

Seien $f^{(i)} \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $f^{(i)} \pmod{p^n}$ eine gemeinsame primitive Nullstelle.

Beweis.

(i) $\implies$ (ii): Sei $x = (x_1, \dots, x_m)$ eine nichttriviale gemeinsame Nullstelle der $f^{(i)}$.

Beweis.

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

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

Beweis.

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

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

Sei $i \in \{1, \dots, m\}$,

Beweis.

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

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

Sei $i \in \{1, \dots, m\}$, s.d. $k = v_p(x_i)$.

Beweis.

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

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

Sei $i \in \{1, \dots, m\}$, s.d. $k = v_p(x_i)$. Dann ist
 $v_p(y_i) = v_p(p^{-k}) + v_p(x_i) = -k + k = 0$.

Beweis.

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

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

Sei $i \in \{1, \dots, m\}$, 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.

Beweis.

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

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

Sei $i \in \{1, \dots, m\}$, 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 $n \in \mathbb{N}$

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

Beweis.

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

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

Sei $i \in \{1, \dots, m\}$, 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 $n \in \mathbb{N}$

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

(ii) $\implies$ (i) ist trivial und (ii) $\iff$ (iii) folgt aus 2.28. □

Bemerkung 2.33

Die Voraussetzung homogenes Polynom ist notwendig,

Bemerkung 2.33

Die Voraussetzung homogenes Polynom ist notwendig, wie am Beispiel:

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

deutlich wird,

Bemerkung 2.33

Die Voraussetzung homogenes Polynom ist notwendig, wie am Beispiel:

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

deutlich wird, denn $f(p^{-1}) = 0$,

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 $p^{-1} \notin \mathbb{Z}_p$.

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 (mod p^n) zu einer echten Lösung in $\mathbb{Z}_p$ entwickelt werden kann.

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 (mod p^n) zu einer echten Lösung in $\mathbb{Z}_p$ entwickelt werden kann. Dazu verwenden wir die p -adische Version des Newton Verfahrens.

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 (mod 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 $f = a_m X^m + \dots + a_0 \in \mathbb{Z}_p[X]$ und
 $f' = a_m m X^{m-1} + \dots + a_1 \in \mathbb{Z}_p[X]$ seine Ableitung.

Lemma 2.34 (Henselsches Lemma)

Sei $f = a_m X^m + \dots + a_0 \in \mathbb{Z}_p[X]$ und
 $f' = a_m m X^{m-1} + \dots + a_1 \in \mathbb{Z}_p[X]$ seine Ableitung. Weiter sei
 $x \in \mathbb{Z}_p$,

Lemma 2.34 (Henselsches Lemma)

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

Lemma 2.34 (Henselsches Lemma)

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

Lemma 2.34 (Henselsches Lemma)

Sei $f = a_m X^m + \dots + a_0 \in \mathbb{Z}_p[X]$ und $f' = a_m m X^{m-1} + \dots + a_1 \in \mathbb{Z}_p[X]$ seine Ableitung. Weiter sei $x \in \mathbb{Z}_p$, s.d. $f(x) \equiv 0 \pmod{p^n}$ 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.

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

Beweis.

Nach Voraussetzung ist $f(x) = p^n b$ und $f'(x) = p^k c$ mit $b \in \mathbb{Z}_p$ und $c \in \mathbb{Z}_p^\times$.

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 $y := x + p^{n-k}z$.

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

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 $R_i \in \mathbb{Z}_p$.

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 $2n - 2k \geq n + 1$.

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

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

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

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

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

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 $c \in \mathbb{Z}_p^\times$,

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.

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

Satz 2.35

Sei $f \in \mathbb{Z}_p[X_1, \dots, X_m]$ und $x = (x_i) \in (\mathbb{Z}_p)^m$,

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

Satz 2.35

Sei $f \in \mathbb{Z}_p[X_1, \dots, X_m]$ und $x = (x_i) \in (\mathbb{Z}_p)^m$, s.d.
 $f(x) \equiv 0 \pmod{p^n}$.

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

Satz 2.35

Sei $f \in \mathbb{Z}_p[X_1, \dots, X_m]$ und $x = (x_i) \in (\mathbb{Z}_p)^m$, s.d.
 $f(x) \equiv 0 \pmod{p^n}$. Weiter existiere ein $1 \leq j \leq m$,

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

Satz 2.35

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

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

Satz 2.35

Sei $f \in \mathbb{Z}_p[X_1, \dots, X_m]$ und $x = (x_i) \in (\mathbb{Z}_p)^m$, s.d.

$f(x) \equiv 0 \pmod{p^n}$. 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 $y \equiv x \pmod{p^{n-k}}$.

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

Satz 2.35

Sei $f \in \mathbb{Z}_p[X_1, \dots, X_m]$ und $x = (x_i) \in (\mathbb{Z}_p)^m$, s.d.

$f(x) \equiv 0 \pmod{p^n}$. 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 $y \equiv x \pmod{p^{n-k}}$.

Beweis.

Sei zunächst $m = 1$.

Beweis.

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

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

Beweis.

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

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

Wende 2.34 nun auf $x^{(1)}$ und $n + 1$ an.

Beweis.

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

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

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

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

Beweis.

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

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

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
$$d(x^{(q+1)}, x^{(q)}) \xrightarrow{q \rightarrow \infty} 0.$$

Beweis.

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

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

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 $d(x^{(q+1)}, x^{(q)}) \xrightarrow{q \rightarrow \infty} 0$. Also ist $x^{(q)}$ eine Cauchy Folge und konvergiert gegen ein $y \in \mathbb{Z}_p$.

Beweis.

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

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

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 $d(x^{(q+1)}, x^{(q)}) \xrightarrow{q \rightarrow \infty} 0$. Also ist $x^{(q)}$ eine Cauchy Folge und konvergiert gegen ein $y \in \mathbb{Z}_p$. Dann gilt

$$0 = \lim_{q \rightarrow \infty} f(x^{(q)}) = f\left(\lim_{q \rightarrow \infty} x^{(q)}\right) = f(y)$$

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

Beweis.

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

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

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 $d(x^{(q+1)}, x^{(q)}) \xrightarrow{q \rightarrow \infty} 0$. Also ist $x^{(q)}$ eine Cauchy Folge und konvergiert gegen ein $y \in \mathbb{Z}_p$. Dann gilt

$$0 = \lim_{q \rightarrow \infty} f(x^{(q)}) = f\left(\lim_{q \rightarrow \infty} x^{(q)}\right) = f(y)$$

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

Sei nun $m > 1$.

Sei nun $m > 1$. Ersetze in f die Variablen X_i durch x_i für $i \neq j$.

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.

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.

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 $g(y_j) = 0$.

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 $i \neq j$.

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

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

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

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



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

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

Korollar 2.36

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

$$f(x) \equiv 0 \pmod{p}$$

und es sei mind.

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

Korollar 2.36

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

$$f(x) \equiv 0 \pmod{p}$$

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

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

Korollar 2.36

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

$$f(x) \equiv 0 \pmod{p}$$

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

Beweis.

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

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

Korollar 2.36

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

$$f(x) \equiv 0 \pmod{p}$$

und es sei mind. eine partielle Ableitung $\frac{\partial f}{\partial X_j}(x) \not\equiv 0 \pmod{p}$, 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 $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ eine quadratische Form mit $a_{ij} = a_{ji}$ und sei $p \nmid \det(a_{ij})$.

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ eine quadratische Form mit $a_{ij} = a_{ji}$ und sei $p \nmid \det(a_{ij})$. Sei weiter $a \in \mathbb{Z}_p$.

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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.

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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.

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $(\bmod p)$ nicht verschwindet.

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $A = (a_{ij}) \in \mathbb{Z}_p^{m \times m}$.

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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 $\ker A = \{0\}$.

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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

$$\frac{\partial f}{\partial X_i} = 2 \sum_{j=1}^m a_{ij} X_j \text{ also } \begin{pmatrix} \partial_{X_1} f(x) \\ \vdots \\ \partial_{X_m} f(x) \end{pmatrix} = 2Ax.$$

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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

$$\frac{\partial f}{\partial X_i} = 2 \sum_{j=1}^m a_{ij} X_j \text{ also } \begin{pmatrix} \partial_{X_1} f(x) \\ \vdots \\ \partial_{X_m} f(x) \end{pmatrix} = 2Ax.$$

Da x primitiv ist $x \neq 0 \in \mathbb{F}_p^m$ und damit mind.

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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

$$\frac{\partial f}{\partial X_i} = 2 \sum_{j=1}^m a_{ij} X_j \text{ also } \begin{pmatrix} \partial_{X_1} f(x) \\ \vdots \\ \partial_{X_m} f(x) \end{pmatrix} = 2Ax.$$

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

Korollar 2.37

Sei $p \neq 2$ und $f = \sum_{i=1}^m \sum_{j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \dots, X_m]$ 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

$$\frac{\partial f}{\partial X_i} = 2 \sum_{j=1}^m a_{ij} X_j \text{ also } \begin{pmatrix} \partial_{X_1} f(x) \\ \vdots \\ \partial_{X_m} f(x) \end{pmatrix} = 2Ax.$$

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