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

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

wobei die Koeffizienten a_i in $\{0, 1, \ldots, p-1\}$ 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

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

wobei die Koeffizienten a_i in $\{0, 1, \ldots, p-1\}$ liegen, z.B.: für $p = 5$ und $n = 216$:

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

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

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

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

mit $0 \leq a_i < p$ für $i \in \mathbb{N}_0$.

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

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

mit $0 \leq a_i < p$ für $i \in \mathbb{N}_0$.

Dabei ist $\sum_{i=0}^{\infty} a_i p^i$ rein formal gemeint,

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

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

mit $0 \leq a_i < p$ für $i \in \mathbb{N}_0$.

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

$$s_n = \sum_{i=0}^{n-1} a_i p^i = a_0 + a_1 p + a_2 p^2 + \dots + a_{n-1} p^{n-1}.$$

Wir betrachten nun die Folge der Restklassen der Partialsummen $(\overline{s}_n)_{n\in\mathbb{N}} \in \prod_{m=1}^{\infty} \mathbb{Z}/p^m\mathbb{Z}$:

$$\overline{s}_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}.$$

Wir betrachten nun die Folge der Restklassen der Partialsummen $(\overline{s}_n)_{n\in\mathbb{N}} \in \prod_{m=1}^{\infty} \mathbb{Z}/p^m\mathbb{Z}$:

$$\overline{s}_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}.$$

Die Folgenelemente $\overline{s}_n$ erfüllen eine „Kompatibilitätsbedingung“:

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

Wir betrachten nun die Folge der Restklassen der Partialsummen $(\overline{s}_n)_{n\in\mathbb{N}} \in \prod_{m=1}^{\infty} \mathbb{Z}/p^m\mathbb{Z}$:

$$\overline{s}_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}.$$

Die Folgenelemente $\overline{s}_n$ erfüllen eine „Kompatibilitätsbedingung“:

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

Mit der kanonischen Projektion

$$\begin{aligned} \phi_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} &\to \mathbb{Z}/p^n\mathbb{Z} \\ \overline{a} &\mapsto a \bmod p^n, \end{aligned}$$

Wir betrachten nun die Folge der Restklassen der Partialsummen $(\overline{s}_n)_{n\in\mathbb{N}} \in \prod_{m=1}^{\infty} \mathbb{Z}/p^m\mathbb{Z}$:

$$\overline{s}_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}.$$

Die Folgenelemente $\overline{s}_n$ erfüllen eine „Kompatibilitätsbedingung“:

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

Mit der kanonischen Projektion

$$\begin{aligned} \phi_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} &\to \mathbb{Z}/p^n\mathbb{Z} \\ \overline{a} &\mapsto a \bmod p^n, \end{aligned}$$

gilt also $\phi_n(\overline{s}_{n+1}) = \overline{s}_n$.

Mit den ϕ_n entsteht eine Folge

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\phi_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\phi_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\phi_3} \dots.$$

Mit den ϕ_n entsteht eine Folge

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\phi_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\phi_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\phi_3} \dots.$$

Ein solches System wird projektives System genannt, genauer:

Mit den ϕ_n entsteht eine Folge

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\phi_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\phi_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\phi_3} \dots.$$

Ein solches System wird projektives System genannt, genauer:

Definition 2.1

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

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

Mit den ϕ_n entsteht eine Folge

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\phi_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\phi_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\phi_3} \ldots.$$

Ein solches System wird projektives System genannt, genauer:

Definition 2.1

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

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

Die Teilmenge

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

Mit den ϕ_n entsteht eine Folge

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\phi_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\phi_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\phi_3} \ldots.$$

Ein solches System wird projektives System genannt, genauer:

Definition 2.1

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

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

Die Teilmenge

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

heißt projektiver Limes des Systems.

Bemerkung 2.2

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 2.2

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).

Definition 2.3 (Ganze p-adische Zahlen)

Der projektive Limes des Systems $(\mathbb{Z}/p^n\mathbb{Z}, \phi_n)$

$$\mathbb{Z}_p := \varprojlim (\mathbb{Z}/p^n\mathbb{Z}, \phi_n)$$

heißt der Ring der ganzen p-adischen Zahlen.

Bemerkung 2.2

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).

Definition 2.3 (Ganze p-adische Zahlen)

Der projektive Limes des Systems $(\mathbb{Z}/p^n\mathbb{Z}, \phi_n)$

$$\mathbb{Z}_p := \varprojlim (\mathbb{Z}/p^n\mathbb{Z}, \phi_n)$$

heißt der Ring der ganzen p-adischen Zahlen.

Notation: Setze im Folgenden $A_n := \mathbb{Z}/p^n\mathbb{Z}$.

Bemerkung 2.2

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).

Definition 2.3 (Ganze p-adische Zahlen)

Der projektive Limes des Systems $(\mathbb{Z}/p^n\mathbb{Z}, \phi_n)$

$$\mathbb{Z}_p := \varprojlim (\mathbb{Z}/p^n\mathbb{Z}, \phi_n)$$

heißt der Ring der ganzen p-adischen Zahlen.

Notation: Setze im Folgenden $A_n := \mathbb{Z}/p^n\mathbb{Z}$. Außerdem bezeichne $\pi_n \colon \mathbb{Z}_p \to A_n$ die kanonische Projektion.

Bemerkung 2.4

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

Bemerkung 2.4

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 2.4

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. Die Inklusion

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p, a \mapsto (a \bmod p, a \bmod p^2, \ldots)$$

Bemerkung 2.4

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. Die Inklusion

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p, a \mapsto (a \bmod p, a \bmod p^2, \ldots)$$

ist ein injektiver Ringhomomorphismus.

Bemerkung 2.4

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. Die Inklusion

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p, a \mapsto (a \bmod p, a \bmod p^2, \ldots)$$

ist ein injektiver Ringhomomorphismus. Damit wird $\mathbb{Z}$ zum Teilring von $\mathbb{Z}_p$.

Bemerkung 2.4

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. Die Inklusion

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p, a \mapsto (a \bmod p, a \bmod p^2, \ldots)$$

   ist ein injektiver Ringhomomorphismus. Damit wird $\mathbb{Z}$ zum Teilring von $\mathbb{Z}_p$.

3. $\mathbb{Z}_p$ erbt als Teilring nun also die komponentenweise Addition und Multiplikation des Produktrings $\prod_{n=1}^{\infty} A_n$,

Bemerkung 2.4

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. Die Inklusion

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p, a \mapsto (a \bmod p, a \bmod p^2, \ldots)$$

ist ein injektiver Ringhomomorphismus. Damit wird $\mathbb{Z}$ zum Teilring von $\mathbb{Z}_p$.

3. $\mathbb{Z}_p$ 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 2.5

Versieht man A_n mit der diskreten Topologie (d.h. alle Teilmengen sind offen)

Bemerkung 2.5

Versieht man A_n mit der diskreten Topologie (d.h. alle Teilmengen sind offen) und $\prod_{n=1}^{\infty} A_n$ mit der Produkttopologie (kleinste Topologie, s.d. die kanonischen Projektionen $\prod_{m=1}^{\infty} A_m \twoheadrightarrow A_n$ stetig sind),

Bemerkung 2.5

Versieht man A_n mit der diskreten Topologie (d.h. alle Teilmengen sind offen) und $\prod_{n=1}^{\infty} A_n$ mit der Produkttopologie (kleinste Topologie, s.d. die kanonischen Projektionen $\prod_{m=1}^{\infty} A_m \twoheadrightarrow A_n$ stetig sind), wird $\mathbb{Z}_p$ zu einem topologischen Ring.

Satz 2.6 (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 2.6 (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 2.6 (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 2.6 (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 2.7

$\mathbb{Z}_p$ ist kompakt.

Korollar 2.7

$\mathbb{Z}_p$ ist kompakt.

Beweisskizze.

- Nach 2.6 ist $\prod_{n=1}^{\infty} A_n$ kompakt.

Korollar 2.7

$\mathbb{Z}_p$ ist kompakt.

Beweisskizze.

- Nach 2.6 ist $\prod_{n=1}^{\infty} A_n$ kompakt.
- $\mathbb{Z}_p$ ist abgeschlossen in $\prod_{n=1}^{\infty} A_n$.

Korollar 2.7

$\mathbb{Z}_p$ ist kompakt.

Beweisskizze.

- Nach 2.6 ist $\prod_{n=1}^{\infty} A_n$ kompakt.
- $\mathbb{Z}_p$ ist abgeschlossen in $\prod_{n=1}^{\infty} A_n$.
- Als abgeschlossene Teilmenge eines kompakten Raums ist $\mathbb{Z}_p$ kompakt. □

Lemma 2.8

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

Lemma 2.8

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 2.8

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 2.8

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

Lemma 2.8

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. $p^n\mathbb{Z}_p \subseteq \ker \pi_n$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \mathbb{Z}_p$.

Lemma 2.8

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. $p^n\mathbb{Z}_p \subseteq \ker \pi_n$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \mathbb{Z}_p$. Dann ist $p^n x_n \equiv 0 \pmod{p^n}$.

Lemma 2.8

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. $p^n\mathbb{Z}_p \subseteq \ker \pi_n$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \mathbb{Z}_p$. Dann ist $p^n x_n \equiv 0 \pmod{p^n}$. Damit folgt $\pi_n(p^n x) = 0$,

Lemma 2.8

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. $p^n\mathbb{Z}_p \subseteq \ker \pi_n$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \mathbb{Z}_p$. Dann ist $p^n x_n \equiv 0 \pmod{p^n}$. Damit folgt $\pi_n(p^n x) = 0$, also $p^n x \in \ker \pi_n$.

Lemma 2.8

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. $p^n\mathbb{Z}_p \subseteq \ker \pi_n$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \mathbb{Z}_p$. Dann ist $p^n x_n \equiv 0 \pmod{p^n}$. Damit folgt $\pi_n(p^n x) = 0$, also $p^n x \in \ker \pi_n$.

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

Lemma 2.8

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. $p^n\mathbb{Z}_p \subseteq \ker \pi_n$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \mathbb{Z}_p$. Dann ist $p^n x_n \equiv 0 \pmod{p^n}$. Damit folgt $\pi_n(p^n x) = 0$, also $p^n x \in \ker \pi_n$.

Z.z.: $\ker \pi_n \subseteq p^n\mathbb{Z}_p$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \ker \pi_n$. Sei weiter ein $m \geq n$.

Lemma 2.8

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. $p^n\mathbb{Z}_p \subseteq \ker \pi_n$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \mathbb{Z}_p$. Dann ist $p^n x_n \equiv 0 \pmod{p^n}$. Damit folgt $\pi_n(p^n x) = 0$, also $p^n x \in \ker \pi_n$.

Z.z.: $\ker \pi_n \subseteq p^n\mathbb{Z}_p$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \ker \pi_n$. Sei weiter ein $m \geq n$. Wegen Kompatibilität folgt

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

Lemma 2.8

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. $p^n\mathbb{Z}_p \subseteq \ker \pi_n$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \mathbb{Z}_p$. Dann ist $p^n x_n \equiv 0 \pmod{p^n}$. Damit folgt $\pi_n(p^n x) = 0$, also $p^n x \in \ker \pi_n$.

Z.z.: $\ker \pi_n \subseteq p^n\mathbb{Z}_p$. Sei dazu $x = (\overline{x}_m)_{m\in\mathbb{N}} \in \ker \pi_n$. Sei weiter ein $m \geq n$. Wegen Kompatibilität folgt

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

Also folgt $\overline{x}_m \in p^n A_m$.

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen).

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex.

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex. ein (eindeutiges) $\overline{y}_{m-n} \in A_{m-n}$,

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex. ein (eindeutiges) $\overline{y}_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$.

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex. ein (eindeutiges) $\overline{y}_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Setze nun $y := (\overline{y}_{m-n})_{m>n}$.

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex. ein (eindeutiges) $\overline{y}_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Setze nun $y := (\overline{y}_{m-n})_{m>n}$. Nun bleibt noch zu verifizieren, dass $y \in \mathbb{Z}_p$

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex. ein (eindeutiges) $\overline{y}_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Setze nun $y := (\overline{y}_{m-n})_{m>n}$. Nun bleibt noch zu verifizieren, dass $y \in \mathbb{Z}_p$ und $x = p^n y$

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex. ein (eindeutiges) $\overline{y}_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Setze nun $y := (\overline{y}_{m-n})_{m>n}$. Nun bleibt noch zu verifizieren, dass $y \in \mathbb{Z}_p$ und $x = p^n y$ (Übungsaufgabe).

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex. ein (eindeutiges) $\overline{y}_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Setze nun $y := (\overline{y}_{m-n})_{m>n}$. Nun bleibt noch zu verifizieren, dass $y \in \mathbb{Z}_p$ und $x = p^n y$ (Übungsaufgabe). Damit folgt $x \in p^n\mathbb{Z}_p$.

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex. ein (eindeutiges) $\overline{y}_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Setze nun $y := (\overline{y}_{m-n})_{m>n}$. Nun bleibt noch zu verifizieren, dass $y \in \mathbb{Z}_p$ und $x = p^n y$ (Übungsaufgabe). Damit folgt $x \in p^n\mathbb{Z}_p$.

Die behauptete Isomorphie folgt jetzt direkt aus dem Homomorphiesatz.

Es ist

$$A_{m-n} = \mathbb{Z}/p^{m-n}\mathbb{Z} \xrightarrow{\sim} p^n\mathbb{Z}/p^m\mathbb{Z} = p^n A_m$$
$$\overline{a} \longmapsto \overline{p^n a}$$

ein Gruppenisomorphismus (nachrechnen). Das heißt es ex. ein (eindeutiges) $\overline{y}_{m-n} \in A_{m-n}$, s.d. $p^n y_{m-n} \equiv x_m \pmod{p^m}$. Setze nun $y := (\overline{y}_{m-n})_{m>n}$. Nun bleibt noch zu verifizieren, dass $y \in \mathbb{Z}_p$ und $x = p^n y$ (Übungsaufgabe). Damit folgt $x \in p^n\mathbb{Z}_p$.

Die behauptete Isomorphie folgt jetzt direkt aus dem Homomorphiesatz. □

Lemma 2.9

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

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

Lemma 2.9

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

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

(ii) $p \nmid u$

Lemma 2.9

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

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

(ii) $p \nmid u$

(iii) $0 \neq \overline{u}_1 \in \mathbb{Z}/p\mathbb{Z}$

Beweis.

(ii) $\Longleftrightarrow$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

Beweis.

(ii) $\Longleftrightarrow$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\Longrightarrow$ (iii):

Beweis.

(ii) $\Longleftrightarrow$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\Longrightarrow$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$.

Beweis.

(ii) $\Longleftrightarrow$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\Longrightarrow$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb.

Beweis.

(ii) $\Longleftrightarrow$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\Longrightarrow$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$,

Beweis.

(ii) $\Longleftrightarrow$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\Longrightarrow$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

Beweis.

(ii) $\Longleftrightarrow$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\Longrightarrow$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

(iii) $\Longrightarrow$ (i):

Beweis.

(ii) $\Longleftrightarrow$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\Longrightarrow$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

(iii) $\Longrightarrow$ (i): Sei umgekehrt $\overline{u_1} \neq 0$.

Beweis.

(ii) $\iff$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\implies$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

(iii) $\implies$ (i): 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 $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\implies$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

(iii) $\implies$ (i): 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 $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\implies$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

(iii) $\implies$ (i): Sei umgekehrt $\overline{u_1} \neq 0$. Wegen Kompatibilität folgt damit $p \nmid u_n \ \forall n \in \mathbb{N}$, denn ang. $p \mid u_n$ für ein $n \in \mathbb{N}$. Dann folgt

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

Beweis.

(ii) $\iff$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\implies$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

(iii) $\implies$ (i): Sei umgekehrt $\overline{u_1} \neq 0$. Wegen Kompatibilität folgt damit $p \nmid u_n \ \forall n \in \mathbb{N}$, denn ang. $p \mid u_n$ für ein $n \in \mathbb{N}$. Dann folgt

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

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

Beweis.

(ii) $\iff$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\implies$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

(iii) $\implies$ (i): Sei umgekehrt $\overline{u_1} \neq 0$. Wegen Kompatibilität folgt damit $p \nmid u_n \ \forall n \in \mathbb{N}$, denn ang. $p \mid u_n$ für ein $n \in \mathbb{N}$. Dann folgt

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

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

Beweis.

(ii) $\iff$ (iii) ist klar wegen $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\implies$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

(iii) $\implies$ (i): Sei umgekehrt $\overline{u_1} \neq 0$. Wegen Kompatibilität folgt damit $p \nmid u_n \ \forall n \in \mathbb{N}$, denn ang. $p \mid u_n$ für ein $n \in \mathbb{N}$. Dann folgt

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

Da p prim folgt insbesondere $(p^n, u_n) = 1$. Also ex. $a, b \in \mathbb{Z}$, 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 $\ker \pi_1 = p\mathbb{Z}_p$.

(i) $\implies$ (iii): Sei dazu $u = (\overline{u_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p^\times$. Dann ex. ein $v = (\overline{v_n})_{n\in\mathbb{N}} \in \mathbb{Z}_p$ mit $uv = 1$ insb. $\overline{u}_1\overline{v}_1 = \overline{1}$, also $\overline{u}_1 \neq 0$.

(iii) $\implies$ (i): Sei umgekehrt $\overline{u_1} \neq 0$. Wegen Kompatibilität folgt damit $p \nmid u_n \ \forall n \in \mathbb{N}$, denn ang. $p \mid u_n$ für ein $n \in \mathbb{N}$. Dann folgt

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

Da p prim folgt insbesondere $(p^n, u_n) = 1$. Also ex. $a, b \in \mathbb{Z}$, 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 $v := (\overline{u}_1^{-1}, \overline{u}_2^{-1}, \ldots) = u^{-1} \in \mathbb{Z}_p$. $\square$

Beispiel 2.10

Für $p = 2$ ist

Beispiel 2.10

Für $p = 2$ ist

$$7 = (\overline{7}, \overline{7}, \ldots) = (\overline{1}, \overline{3}, \overline{7}, \overline{7}, \ldots) \in \mathbb{Z}_2,$$

Beispiel 2.10

Für $p = 2$ ist

$$7 = (\overline{7}, \overline{7}, \ldots) = (\overline{1}, \overline{3}, \overline{7}, \overline{7}, \ldots) \in \mathbb{Z}_2,$$

d.h. nach 2.9 ist $\frac{1}{7} \in \mathbb{Z}_2$.

Beispiel 2.10

Für $p = 2$ ist

$$7 = (\overline{7}, \overline{7}, \ldots) = (\overline{1}, \overline{3}, \overline{7}, \overline{7}, \ldots) \in \mathbb{Z}_2,$$

d.h. nach 2.9 ist $\frac{1}{7} \in \mathbb{Z}_2$. Die ersten 6 Folgenelemente sind

$$\frac{1}{7} = (\overline{1}, \overline{3}, \overline{7}, \overline{7}, \overline{23}, \overline{55}, \ldots).$$

Lemma 2.11

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

Lemma 2.11

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

Lemma 2.11

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 2.11

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

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex.

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$,

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$,

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$,

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$, dann ist $\forall m \geq n+1$:

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$, dann ist $\forall m \geq n+1$:

$$x_m \equiv x_{n+1} \pmod{p^{n+1}} \not\equiv 0 \pmod{p^{n+1}}.$$

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$, dann ist $\forall m \geq n+1$:

$$x_m \equiv x_{n+1} \pmod{p^{n+1}} \not\equiv 0 \pmod{p^{n+1}}.$$

Falls $n = 0$, dann setze $u = x \in \mathbb{Z}_p^\times$.

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$, dann ist $\forall m \geq n+1$:

$$x_m \equiv x_{n+1} \pmod{p^{n+1}} \not\equiv 0 \pmod{p^{n+1}}.$$

Falls $n = 0$, dann setze $u = x \in \mathbb{Z}_p^\times$. Sonst ist $x \in \ker \pi_n$, insbesondere ex.

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$, dann ist $\forall m \geq n+1$:

$$x_m \equiv x_{n+1} \pmod{p^{n+1}} \not\equiv 0 \pmod{p^{n+1}}.$$

Falls $n = 0$, dann setze $u = x \in \mathbb{Z}_p^\times$. Sonst ist $x \in \ker \pi_n$, insbesondere ex. nach 2.8 ein $u \in \mathbb{Z}_p$ mit $x = p^n u$.

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$, dann ist $\forall m \geq n+1$:

$$x_m \equiv x_{n+1} \pmod{p^{n+1}} \not\equiv 0 \pmod{p^{n+1}}.$$

Falls $n = 0$, dann setze $u = x \in \mathbb{Z}_p^\times$. Sonst ist $x \in \ker \pi_n$, insbesondere ex. nach 2.8 ein $u \in \mathbb{Z}_p$ mit $x = p^n u$. Jetzt bleibt zu verifizieren, dass $u \in \mathbb{Z}_p^\times$ (Übungsaufgabe).

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$, dann ist $\forall m \geq n+1$:

$$x_m \equiv x_{n+1} \pmod{p^{n+1}} \not\equiv 0 \pmod{p^{n+1}}.$$

Falls $n = 0$, dann setze $u = x \in \mathbb{Z}_p^\times$. Sonst ist $x \in \ker \pi_n$, insbesondere ex. nach 2.8 ein $u \in \mathbb{Z}_p$ mit $x = p^n u$. Jetzt bleibt zu verifizieren, dass $u \in \mathbb{Z}_p^\times$ (Übungsaufgabe).

(ii) Eindeutigkeit:

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$, dann ist $\forall m \geq n+1$:

$$x_m \equiv x_{n+1} \pmod{p^{n+1}} \not\equiv 0 \pmod{p^{n+1}}.$$

Falls $n = 0$, dann setze $u = x \in \mathbb{Z}_p^\times$. Sonst ist $x \in \ker \pi_n$, insbesondere ex. nach 2.8 ein $u \in \mathbb{Z}_p$ mit $x = p^n u$. Jetzt bleibt zu verifizieren, dass $u \in \mathbb{Z}_p^\times$ (Übungsaufgabe).

(ii) Eindeutigkeit: Man verwende, dass Einheiten in Ringen keine Nullteiler sind.

Beweis.

(i) Existenz: Sei $x \in \mathbb{Z}_p \setminus \{0\}$. Da $x \neq 0$ ex. wegen Kompatibilität ein maximales $n \in \mathbb{N}_0$, s.d. $\overline{x}_n = \pi_n(x) = 0$, denn sei $\overline{x}_n = 0$ und $\overline{x}_{n+1} \neq 0$, dann ist $\forall m \geq n+1$:

$$x_m \equiv x_{n+1} \pmod{p^{n+1}} \not\equiv 0 \pmod{p^{n+1}}.$$

Falls $n = 0$, dann setze $u = x \in \mathbb{Z}_p^\times$. Sonst ist $x \in \ker \pi_n$, insbesondere ex. nach 2.8 ein $u \in \mathbb{Z}_p$ mit $x = p^n u$. Jetzt bleibt zu verifizieren, dass $u \in \mathbb{Z}_p^\times$ (Übungsaufgabe).

(ii) Eindeutigkeit: Man verwende, dass Einheiten in Ringen keine Nullteiler sind. Die Details sind Übungsaufgabe.

□

Definition 2.12 (p-Bewertung)

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

Definition 2.12 (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 2.12 (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 2.12 (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 2.13

Wegen 2.11 ist die p-Bewertung wohldefiniert.

Definition 2.12 (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 2.13

Wegen 2.11 ist die p-Bewertung wohldefiniert.
Per Konvention setze $n + \infty = \infty$ und $\infty > n$ für $n \in \mathbb{N}_0$.

Definition 2.12 (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 2.13

Wegen 2.11 ist die p-Bewertung wohldefiniert.
Per Konvention setze $n + \infty = \infty$ und $\infty > n$ für $n \in \mathbb{N}_0$. Es lässt sich leicht verifizieren, dass für $x, y \in \mathbb{Z}_p$ gilt:

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

Definition 2.12 (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 2.13

Wegen 2.11 ist die p-Bewertung wohldefiniert.
Per Konvention setze $n + \infty = \infty$ und $\infty > n$ für $n \in \mathbb{N}_0$. Es lässt sich leicht verifizieren, dass für $x, y \in \mathbb{Z}_p$ gilt:

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

Daraus lässt sich ebenfalls direkt folgern, dass $\mathbb{Z}_p$ nullteilerfrei ist (Übungsaufgabe).

Wir können v_p verwenden, um eine Metrik auf $\mathbb{Z}_p$ zu definieren:

Wir können v_p verwenden, um eine Metrik auf $\mathbb{Z}_p$ zu definieren:

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

mit der Konvention $\exp(-\infty) = 0$.

Wir können v_p verwenden, um eine Metrik auf $\mathbb{Z}_p$ zu definieren:

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

mit der Konvention $\exp(-\infty) = 0$.

Bemerkung 2.14 (Bälle)

Es sei im Folgenden stets

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

Wir können v_p verwenden, um eine Metrik auf $\mathbb{Z}_p$ zu definieren:

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

mit der Konvention $\exp(-\infty) = 0$.

Bemerkung 2.14 (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 $v_p(x) \in \mathbb{N}_0$ gilt

Wir können v_p verwenden, um eine Metrik auf $\mathbb{Z}_p$ zu definieren:

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

mit der Konvention $\exp(-\infty) = 0$.

Bemerkung 2.14 (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 $v_p(x) \in \mathbb{N}_0$ gilt

$$\overline{B(x, e^{-n})} = \{y \in \mathbb{Z}_p \mid v_p(x - y) \geq n\}$$

Wir können v_p verwenden, um eine Metrik auf $\mathbb{Z}_p$ zu definieren:

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

mit der Konvention $\exp(-\infty) = 0$.

Bemerkung 2.14 (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 $v_p(x) \in \mathbb{N}_0$ gilt

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

Wir können v_p verwenden, um eine Metrik auf $\mathbb{Z}_p$ zu definieren:

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

mit der Konvention $\exp(-\infty) = 0$.

Bemerkung 2.14 (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 $v_p(x) \in \mathbb{N}_0$ gilt

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

Lemma 2.15 (Topologie auf $\mathbb{Z}_p$)

Die Topologie auf $\mathbb{Z}_p$ wird induziert durch die Metrik $d(\cdot, \cdot)$.

Lemma 2.15 (Topologie auf $\mathbb{Z}_p$)

Die Topologie auf $\mathbb{Z}_p$ wird induziert durch die Metrik $d(\cdot,\cdot)$. $\mathbb{Z}_p$ ist vollständig.

Lemma 2.15 (Topologie auf $\mathbb{Z}_p$)

Die Topologie auf $\mathbb{Z}_p$ wird induziert durch die Metrik $d(\cdot,\cdot)$. $\mathbb{Z}_p$ ist vollständig.

Beweisskizze.

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

Lemma 2.15 (Topologie auf $\mathbb{Z}_p$)

Die Topologie auf $\mathbb{Z}_p$ wird induziert durch die Metrik $d(\cdot,\cdot)$. $\mathbb{Z}_p$ ist vollständig.

Beweisskizze.

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

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

Lemma 2.15 (Topologie auf $\mathbb{Z}_p$)

Die Topologie auf $\mathbb{Z}_p$ wird induziert durch die Metrik $d(\cdot,\cdot)$. $\mathbb{Z}_p$ ist vollständig.

Beweisskizze.

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

Lemma 2.15 (Topologie auf $\mathbb{Z}_p$)

Die Topologie auf $\mathbb{Z}_p$ wird induziert durch die Metrik $d(\cdot,\cdot)$. $\mathbb{Z}_p$ ist vollständig.

Beweisskizze.

- $d(\cdot,\cdot)$ 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 $v + p^n\mathbb{Z}_p = B(v, e^{-(n-1)})$.
- $B(v, e^{-(n-1)}) = v + p^n\mathbb{Z}_p$ offen bezüglich der Produkttopologie.

Z.z.: $\mathbb{Z}_p$ vollständig.

Z.z.: $\mathbb{Z}_p$ vollständig. Da $\mathbb{Z}_p$ nach 2.7 kompakt ist, hat jede Folge in $\mathbb{Z}_p$ eine konvergente Teilfolge.

Z.z.: $\mathbb{Z}_p$ vollständig. Da $\mathbb{Z}_p$ nach 2.7 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 $\mathbb{Z}_p$.

$\square$

Bemerkung 2.16

Es ist leicht nachzurechnen, dass $d(\cdot, \cdot)$ die ultrametrische Ungleichung (auch starke Dreiecksungleichung) erfüllt,

Bemerkung 2.16

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 $x, y, z \in \mathbb{Z}_p$.

Bemerkung 2.16

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 $x, y, z \in \mathbb{Z}_p$. Damit folgt das eine Folge $(u_n)_{n \in \mathbb{N}} \subseteq \mathbb{Z}_p$ genau dann konvergiert,

Bemerkung 2.16

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 $x, y, z \in \mathbb{Z}_p$. Damit folgt das eine Folge $(u_n)_{n\in\mathbb{N}} \subseteq \mathbb{Z}_p$ genau dann konvergiert, wenn $\lim_{n\to\infty}(u_{n+1} - u_n) = 0$.

Bemerkung 2.16

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 $x, y, z \in \mathbb{Z}_p$. Damit folgt das eine Folge $(u_n)_{n\in\mathbb{N}} \subseteq \mathbb{Z}_p$ genau dann konvergiert, wenn $\lim_{n\to\infty}(u_{n+1} - u_n) = 0$.

Definition 2.17

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

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

Bemerkung 2.18

1. Ein Element $x \in \mathbb{Q}_p \setminus \{0\}$,

Bemerkung 2.18

1. Ein Element $x \in \mathbb{Q}_p \setminus \{0\}$, kann eindeutig als

Bemerkung 2.18

1. Ein Element $x \in \mathbb{Q}_p \setminus \{0\}$, kann eindeutig als

$$x = p^r w$$

dargestellt werden, für ein $r \in \mathbb{Z}$ und $w \in \mathbb{Z}_p^\times$.

Bemerkung 2.18

1. Ein Element $x \in \mathbb{Q}_p \setminus \{0\}$, kann eindeutig als

$$x = p^r w$$

dargestellt werden, für ein $r \in \mathbb{Z}$ und $w \in \mathbb{Z}_p^\times$.
Damit setzt sich die Definition von v_p und $d(\cdot, \cdot)$ auf $\mathbb{Q}_p$ fort.

Bemerkung 2.18

1. Ein Element $x \in \mathbb{Q}_p \setminus \{0\}$, kann eindeutig als

$$x = p^r w$$

dargestellt werden, für ein $r \in \mathbb{Z}$ und $w \in \mathbb{Z}_p^\times$.
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 2.18

1. Ein Element $x \in \mathbb{Q}_p \setminus \{0\}$, kann eindeutig als

$$x = p^r w$$

dargestellt werden, für ein $r \in \mathbb{Z}$ und $w \in \mathbb{Z}_p^\times$.
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 $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.

3. $\mathbb{Q}_p$ kann auch als Vervollständigung von $\mathbb{Q}$ bezüglich der p-adischen Metrik $d(\cdot, \cdot)$ definiert werden.

3. $\mathbb{Q}_p$ kann auch als Vervollständigung von $\mathbb{Q}$ bezüglich der p-adischen Metrik $d(\cdot, \cdot)$ definiert werden. Somit ist auch $\mathbb{Q}$ dicht in $\mathbb{Q}_p$.

3. $\mathbb{Q}_p$ kann auch als Vervollständigung von $\mathbb{Q}$ bezüglich der p-adischen Metrik $d(\cdot, \cdot)$ definiert werden. Somit ist auch $\mathbb{Q}$ dicht in $\mathbb{Q}_p$. Man kann ebenfalls zeigen, dass $\mathbb{Q}_p$ lokal kompakt ist.

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

$$f^{(1)}(X_1, \ldots, X_m) = 0$$
$$\vdots$$
$$f^{(r)}(X_1, \ldots, X_m) = 0$$

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

Lemma 2.19

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

Lemma 2.19

Sei $D_1 \leftarrow D_2 \leftarrow \ldots$ *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 2.19

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

Beweisskizze.

- Zeige Aussage für p_n surjektiv.

Lemma 2.19

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

Beweisskizze.

- Zeige Aussage für p_n surjektiv.
- Betrachte

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

Lemma 2.19

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

Beweisskizze.

- Zeige Aussage für p_n surjektiv.
- Betrachte

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

- Zeige, dass $D_{n,m}$ monoton fallende, nicht leere Folge mit Grenzwert E_n ist.

Lemma 2.19

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 $D \neq \emptyset$.

Beweisskizze.

- Zeige Aussage für p_n surjektiv.
- Betrachte

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

- Zeige, dass $D_{n,m}$ monoton fallende, nicht leere Folge mit Grenzwert E_n ist.
- Folgere, dass $\varprojlim (D_n, p_n) \supseteq \varprojlim (E_n, p_n|_{E_n}) \neq \emptyset$. □

Definition 2.20

Ein Element $x = (x_1, \ldots, x_m) \in (\mathbb{Z}_p)^m$ (bzw.

Definition 2.20

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

Definition 2.20

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

Satz 2.21

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

Definition 2.20

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

Satz 2.21

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

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

Definition 2.20

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

Satz 2.21

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

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

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

Definition 2.20

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

Satz 2.21

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

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

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

Falls die $f^{(i)}$ homogen sind

Definition 2.20

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

Satz 2.21

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

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

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

Falls die $f^{(i)}$ homogen sind und die Lösungen in (i) und (ii) primitiv, dann ist dies äquivalent zu

Definition 2.20

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

Satz 2.21

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

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

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

Falls die $f^{(i)}$ homogen sind und die Lösungen in (i) und (ii) primitiv, dann ist dies äquivalent zu

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

Beweis.

(i) $\Longrightarrow$ (ii) ist trivial.

Beweis.

(i) $\Longrightarrow$ (ii) ist trivial.

(ii) $\Longrightarrow$ (i): Betrachte

$$D := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\}$$

Beweis.

(i) $\Longrightarrow$ (ii) ist trivial.

(ii) $\Longrightarrow$ (i): Betrachte

$$D := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\}$$

und

$$D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}.$$

Beweis.

(i) $\Longrightarrow$ (ii) ist trivial.

(ii) $\Longrightarrow$ (i): Betrachte

$$D := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\}$$

und

$$D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}.$$

Es bezeichne $(\phi_n)^m \colon (A_{n+1})^m \to (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet.

Beweis.

(i) $\Longrightarrow$ (ii) ist trivial.

(ii) $\Longrightarrow$ (i): Betrachte

$$D := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\}$$

und

$$D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}.$$

Es bezeichne $(\phi_n)^m \colon (A_{n+1})^m \to (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet. Dann ist $(D_n, (\phi_n)^m)$ ein projektives System mit $D = \varprojlim (D_n, (\phi_n)^m)$.

Beweis.

(i) $\Longrightarrow$ (ii) ist trivial.

(ii) $\Longrightarrow$ (i): Betrachte

$$D := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\}$$

und

$$D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}.$$

Es bezeichne $(\phi_n)^m \colon (A_{n+1})^m \to (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet. Dann ist $(D_n, (\phi_n)^m)$ ein projektives System mit $D = \varprojlim (D_n, (\phi_n)^m)$.
Sei nun $D_n \neq \emptyset \ \forall n \in \mathbb{N}$.

Beweis.

(i) $\Longrightarrow$ (ii) ist trivial.

(ii) $\Longrightarrow$ (i): Betrachte

$$D := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\}$$

und

$$D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}.$$

Es bezeichne $(\phi_n)^m \colon (A_{n+1})^m \to (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet. Dann ist $(D_n, (\phi_n)^m)$ ein projektives System mit $D = \varprojlim (D_n, (\phi_n)^m)$.
Sei nun $D_n \neq \emptyset \ \forall n \in \mathbb{N}$. Da $D_n \subseteq (A_n)^m$ endlich folgt mit 2.19 $D \neq \emptyset$.

Beweis.

(i) $\Longrightarrow$ (ii) ist trivial.

(ii) $\Longrightarrow$ (i): Betrachte

$$D := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\}$$

und

$$D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}.$$

Es bezeichne $(\phi_n)^m \colon (A_{n+1})^m \to (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet. Dann ist $(D_n, (\phi_n)^m)$ ein projektives System mit $D = \varprojlim (D_n, (\phi_n)^m)$.
Sei nun $D_n \neq \emptyset \ \forall n \in \mathbb{N}$. Da $D_n \subseteq (A_n)^m$ endlich folgt mit 2.19 $D \neq \emptyset$.

(i) $\Longrightarrow$ (iii) klar

Beweis.

(i) $\Longrightarrow$ (ii) ist trivial.

(ii) $\Longrightarrow$ (i): Betrachte

$$D := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (\mathbb{Z}_p)^m\}$$

und

$$D_n := \{\text{gemeinsame NS von } f^{(i)} \text{ in } (A_n)^m \pmod{p^n}\}.$$

Es bezeichne $(\phi_n)^m \colon (A_{n+1})^m \to (A_n)^m$ die Abbildung, die ϕ_n komponentenweise anwendet. Dann ist $(D_n, (\phi_n)^m)$ ein projektives System mit $D = \varprojlim (D_n, (\phi_n)^m)$.
Sei nun $D_n \neq \emptyset \ \forall n \in \mathbb{N}$. Da $D_n \subseteq (A_n)^m$ endlich folgt mit 2.19 $D \neq \emptyset$.

(i) $\Longrightarrow$ (iii) klar und (iii) $\Longrightarrow$ (i): „Runterskalieren“ der Nullstelle. Details sind Übungsaufgabe. $\square$

Wir möchten nun betrachten, unter welchen Umständen eine Lösung $\pmod{p^n}$ zu einer echten Lösung in $\mathbb{Z}_p$ entwickelt werden kann.

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

Lemma 2.22 (Henselsches Lemma)

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

Lemma 2.22 (Henselsches Lemma)

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

Lemma 2.22 (Henselsches Lemma)

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

Lemma 2.22 (Henselsches Lemma)

Sei $f = a_m X^m + \ldots + a_0 \in \mathbb{Z}_p[X]$ *und*
$f' = a_m m X^{m-1} + \ldots + a_1 \in \mathbb{Z}_p[X]$ *seine Ableitung. Weiter sei*
$x \in \mathbb{Z}_p$, *s.d.* $f(x) \equiv 0 \pmod{p^n}$ *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 2.22 (Henselsches Lemma)

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

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

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 sei $z \in \mathbb{Z}_p$ 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 sei $z \in \mathbb{Z}_p$ 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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

$$a_i y^i =$$

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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

für $R_i \in \mathbb{Z}_p$. Aufsummieren und addieren von a_0 liefert mit $R \in \mathbb{Z}_p$

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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

für $R_i \in \mathbb{Z}_p$. Aufsummieren und addieren von a_0 liefert mit $R \in \mathbb{Z}_p$

$$f(y) =$$

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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

für $R_i \in \mathbb{Z}_p$. Aufsummieren und addieren von a_0 liefert mit $R \in \mathbb{Z}_p$

$$f(y) = f(x) +$$

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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

für $R_i \in \mathbb{Z}_p$. Aufsummieren und addieren von a_0 liefert mit $R \in \mathbb{Z}_p$

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

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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

für $R_i \in \mathbb{Z}_p$. Aufsummieren und addieren von a_0 liefert mit $R \in \mathbb{Z}_p$

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

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 sei $z \in \mathbb{Z}_p$ und $y := x + p^{n-k} z$. Damit erfüllt $y \equiv x \pmod{p^{n-k}}$. Der binomische Lehrsatz liefert

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

für $R_i \in \mathbb{Z}_p$. Aufsummieren und addieren von a_0 liefert mit $R \in \mathbb{Z}_p$

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

eine „Taylorentwicklung“.

„Taylorentwicklung“:

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

„Taylorentwicklung“:

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

Einsetzen von $f(x) = p^n b$ und $f'(x) = p^k c$ liefert:

„Taylorentwicklung“:

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

Einsetzen von $f(x) = p^n b$ und $f'(x) = p^k c$ liefert:

$$f(y) = p^n b - p^{n-k} z p^k c + p^{2n-2k} z^2 R$$

„Taylorentwicklung“:

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

Einsetzen von $f(x) = p^n b$ und $f'(x) = p^k c$ liefert:

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

„Taylorentwicklung“:

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

Einsetzen von $f(x) = p^n b$ und $f'(x) = p^k c$ liefert:

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

Also mit $z := -bc^{-1}$ folgt

„Taylorentwicklung“:

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

Einsetzen von $f(x) = p^n b$ und $f'(x) = p^k c$ liefert:

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

Also mit $z := -bc^{-1}$ folgt

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

„Taylorentwicklung“:

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

Einsetzen von $f(x) = p^n b$ und $f'(x) = p^k c$ liefert:

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

Also mit $z := -bc^{-1}$ folgt

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

„Taylorentwicklung“:

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

Einsetzen von $f(x) = p^n b$ und $f'(x) = p^k c$ liefert:

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

Also mit $z := -bc^{-1}$ folgt

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

denn da $2k < n$ folgt $2n - 2k \geq n + 1$.

Anwenden der „Taylorentwicklung“ auf f' liefert

Anwenden der „Taylorentwicklung“ auf f' liefert

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

Anwenden der „Taylorentwicklung“ auf f' liefert

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

Anwenden der „Taylorentwicklung“ auf f' liefert

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

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

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 $p \nmid s$

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 2.23

Sei $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ *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 2.23

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

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

Satz 2.23

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

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

Satz 2.23

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

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

Satz 2.23

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

Beweis.

Sei zunächst $m = 1$.

Beweis.

Sei zunächst $m = 1$. Mit 2.22 angewendet auf $x^{(0)} := x$, erhält man $x^{(1)} \in \mathbb{Z}_p$ mit

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

Beweis.

Sei zunächst $m = 1$. Mit 2.22 angewendet auf $x^{(0)} := x$, erhält man $x^{(1)} \in \mathbb{Z}_p$ mit

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

Wende 2.22 nun auf $x^{(1)}$ und $n+1$ an.

Beweis.

Sei zunächst $m = 1$. Mit 2.22 angewendet auf $x^{(0)} := x$, erhält man $x^{(1)} \in \mathbb{Z}_p$ mit

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

Wende 2.22 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 2.22 angewendet auf $x^{(0)} := x$, erhält man $x^{(1)} \in \mathbb{Z}_p$ mit

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

Wende 2.22 nun auf $x^{(1)}$ und $n+1$ an. Induktiv erhält man eine Folge $(x^{(q)})_{q\in\mathbb{N}}$ mit den Eigenschaften

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

Nun verifziert man leicht, dass $x^{(q)}$ eine Cauchy-Folge ist

Beweis.

Sei zunächst $m = 1$. Mit 2.22 angewendet auf $x^{(0)} := x$, erhält man $x^{(1)} \in \mathbb{Z}_p$ mit

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

Wende 2.22 nun auf $x^{(1)}$ und $n+1$ an. Induktiv erhält man eine Folge $(x^{(q)})_{q\in\mathbb{N}}$ mit den Eigenschaften

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

Nun verifziert man leicht, dass $x^{(q)}$ eine Cauchy-Folge ist und gegen ein $y \in \mathbb{Z}_p$ konvergiert

Beweis.

Sei zunächst $m = 1$. Mit 2.22 angewendet auf $x^{(0)} := x$, erhält man $x^{(1)} \in \mathbb{Z}_p$ mit

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

Wende 2.22 nun auf $x^{(1)}$ und $n+1$ an. Induktiv erhält man eine Folge $(x^{(q)})_{q\in\mathbb{N}}$ mit den Eigenschaften

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

Nun verifziert man leicht, dass $x^{(q)}$ eine Cauchy-Folge ist und gegen ein $y \in \mathbb{Z}_p$ konvergiert mit $f(y) = 0$

Beweis.

Sei zunächst $m = 1$. Mit 2.22 angewendet auf $x^{(0)} := x$, erhält man $x^{(1)} \in \mathbb{Z}_p$ mit

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

Wende 2.22 nun auf $x^{(1)}$ und $n+1$ an. Induktiv erhält man eine Folge $(x^{(q)})_{q\in\mathbb{N}}$ mit den Eigenschaften

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

Nun verifziert man leicht, dass $x^{(q)}$ eine Cauchy-Folge ist und gegen ein $y \in \mathbb{Z}_p$ konvergiert mit $f(y) = 0$ 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

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

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

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

□

Aus dem letzten Satz können wir einfache Schlussfolgerungen ziehen.

Aus dem letzten Satz können wir einfache Schlussfolgerungen ziehen.

Korollar 2.24

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

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

und es sei mind.

Aus dem letzten Satz können wir einfache Schlussfolgerungen ziehen.

Korollar 2.24

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

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

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

Aus dem letzten Satz können wir einfache Schlussfolgerungen ziehen.

Korollar 2.24
Sei $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ *und* $x \in \mathbb{Z}_p$ *mit*

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

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

Beweis.
Das ist der Fall $n = 1$ und $k = 0$ in 2.23.

Aus dem letzten Satz können wir einfache Schlussfolgerungen ziehen.

Korollar 2.24

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

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

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

Beweis.

Das ist der Fall $n = 1$ und $k = 0$ in 2.23. □

Beispiel 2.25

Es ist $\sqrt{2} \in \mathbb{Z}_7$,

Beispiel 2.25

Es ist $\sqrt{2} \in \mathbb{Z}_7$, denn für $f = X^2 - 2 \in \mathbb{Z}_7[X]$ gilt

Beispiel 2.25

Es ist $\sqrt{2} \in \mathbb{Z}_7$, denn für $f = X^2 - 2 \in \mathbb{Z}_7[X]$ gilt

$$f(3) = 3^2 - 2 = 7 \equiv 0 \pmod{7}$$

Beispiel 2.25

Es ist $\sqrt{2} \in \mathbb{Z}_7$, denn für $f = X^2 - 2 \in \mathbb{Z}_7[X]$ gilt

$$f(3) = 3^2 - 2 = 7 \equiv 0 \pmod 7$$

und $f'(x) = 2X$ also $f'(3) = 6 \not\equiv 0 \pmod 7$.

Korollar 2.26

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

Korollar 2.26

Sei $f = \sum_{i=1}^{m} \sum_{j=1}^{m} a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \ldots, X_m]$ *eine quadratische Form mit* $a_{ij} = a_{ji}$

Korollar 2.26

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

Korollar 2.26

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

Korollar 2.26

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

Für $p \neq 2$ *gilt:*

Korollar 2.26

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

Für $p \neq 2$ *gilt: Falls* $f(x) \equiv a \pmod{p}$,

Korollar 2.26

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

Für $p \neq 2$ *gilt: Falls* $f(x) \equiv a \pmod{p}$, *hebt sich* x *zu einer echten Lösung.*

Korollar 2.26

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

Für $p \neq 2$ *gilt: Falls* $f(x) \equiv a \pmod{p}$, *hebt sich* x *zu einer echten Lösung.*

Im Fall $p = 2$ *gilt:*

Korollar 2.26

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

Für $p \neq 2$ *gilt: Falls* $f(x) \equiv a \pmod{p}$, *hebt sich* x *zu einer echten Lösung.*

Im Fall $p = 2$ *gilt: Falls* $f(x) \equiv a \pmod{8}$,

Korollar 2.26

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

Für $p \neq 2$ *gilt: Falls* $f(x) \equiv a \pmod{p}$, *hebt sich* x *zu einer echten Lösung.*

Im Fall $p = 2$ *gilt: Falls* $f(x) \equiv a \pmod{8}$, *hebt sich* x *zu einer echten Lösung.*

Korollar 2.26

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

Für $p \neq 2$ *gilt: Falls* $f(x) \equiv a \pmod{p}$, *hebt sich* x *zu einer echten Lösung.*

Im Fall $p = 2$ *gilt: Falls* $f(x) \equiv a \pmod{8}$, *hebt sich* x *zu einer echten Lösung.*

Beweis.

Folgerungen aus 2.24. Beweise sind Übungsaufgaben. □

Literatur

- Serre J-P. *A Course in Arithmetic*. New York; Heidelberg; Berlin: Springer; 1973.
- Neukirch J. *Algebraische Zahlentheorie*. 1st ed. Berlin; Heidelberg [u.a.]: Springer; 2007.
- Schmidt A. *Einführung in die algebraische Zahlentheorie*. Berlin; Heidelberg [u.a.]: Springer; 2007.
- Jänich K. *Topologie*. 8th ed. Berlin; Heidelberg [u.a.]: Springer; 2005.