p-adische Zahlen und das Henselsche Lemma

Emma Bach - Proseminar Elementare Zahlentheorie, WS25/26

28. Oktober 2025

Definition 1.1. Sei p eine Primzahl. Wir nennen folgende Abbildung $\mathbb{Z} \to \mathbb{N}_0$ die ***p*-adische Bewertung** auf $\mathbb{Z}$:

$$v_p(n) = \begin{cases} \max\{k \in \mathbb{N}_0 : p^k \mid n\} & n \neq 0 \\ \infty & n = 0 \end{cases}$$

Die p-adische Bewertung ist auch bekannt als die **Vielfachheit von p in n**. Die p-adische Bewertung kann durch die Vorschrift $v_p\left(\frac{r}{s}\right) = v_p(r) - v_p(s)$ auf die rationalen Zahlen erweitert werden.

Definition 1.2. Der p-adischen Betrag $|-|_p$ auf $\mathbb{Q}$ ist die Abbildung:

$$|n|_p = \frac{1}{p^{v_p(n)}}$$

Satz 1.3. __Satz von Ostrowski:__ *Jeder Betrag auf $\mathbb{Q}$ ist entweder der triviale Betrag, oder äquivalent zu $|-|_p$ für eine Primzahl p, oder äquivalent zum Standardabsolutbetrag $|-|$.*

Definition 2.4. Wir bezeichnen die Vervollständigung des Rings $\mathbb{Z}$ gemäß der durch den p-adischen Absolutbetrag erzeugten Metrik als die ***p*-adischen ganzen Zahlen** $\mathbb{Z}_p$. Analog bezeichnen wir die Vervollständigung des Rings $\mathbb{Q}$ gemäß der p-adischen Metrik als die ***p*-adischen Zahlen** $\mathbb{Q}_p$. Die Konstruktion verläuft analog zur Konstruktion von $\mathbb{R}$ aus Cauchyfolgen in $\mathbb{Q}$.

Proposition 2.5. *Jede Reihe der Form*

$$x = \sum_{n=m}^{\infty} d_n p^n,$$

*wobei $m \in \mathbb{Z}_{\leq 0}$, $d_n \in \{0, 1, \ldots, p-1\}$, konvergiert in $\mathbb{Q}_p$. Wir nennen die Folge d_n die **p-adische Darstellung von** x. Jede p-adische Zahl kann als eine solche Reihe dargestellt werden.*

Wir können jede p-adische Zahl z somit analog zur Standarddarstellung Basis p schreiben:

$$z = \ldots d_4 d_3 d_2 d_1 d_0, d_{-1} \ldots d_m$$

In manchen Quellen werden p-adische Zahlen umgekehrt geschrieben, mit der kleinsten Ziffer links.

Proposition 2.6. *Sei p beliebig. So ist in der p-adischen Darstellung von -1 jede Ziffer $p-1$. Die 5-adische Darstellung von -1 ist also $\ldots 4444$ und die 7-adische Darstellung ist $\ldots 66666$. Somit ist bei der Darstellung p-adischer Zahlen kein Vorzeichen nötig.*

Satz 3.7. __Henselsches Lemma:__ *Sei $f(x)$ ein Polynom mit Koeffizienten $c_i \in \mathbb{Z}_p$. Sei $f'(x)$ die Ableitung von $f(x)$. Sei außerdem $a \in \mathbb{Z}_p$, sodass:*

$$f(a) \equiv 0 \mod p$$
$$f'(a) \not\equiv 0 \mod p$$

Dann existiert ein eindeutiges $\alpha \in \mathbb{Z}_p$, sodass:

$$f(\alpha) = 0$$
$$\alpha \equiv a \mod p$$

Anwendung 3.8. *Das Polynom $f(x) = x^2 + 1$ erfüllt für $p = 5$ und $a = 2$ die gefragten Bedingungen. Somit existiert eine Nullstelle in $\mathbb{Z}_5$, also $i = \sqrt{-1} \in \mathbb{Z}_5$.*

Anwendung 3.9. *Sei $u \in \mathbb{Z}_p$. Sei $k \not\equiv 0 \mod p$. Sei n eine Zahl mit $n \equiv u \mod p$, welche eine k-te Wurzel in $\mathbb{Z}/p\mathbb{Z}$ hat. Dann hat u eine k-te Wurzel in $\mathbb{Z}_p$.*