Prof. Dr. Annette Werner
M.Sc. Adrian Zorbach

Nicht-archimedische Zahlen
Wintersemester 2016/17

# — Blatt 10 —

Abgabe bis 09. Januar 2017, 10 Uhr im Fach zum Tutorium.

Wir wollen Hensel's Lemma verstehen: Ein Polynom

$$f = a_n X^n + \cdots + a_1 X^1 + a_0 \in \mathbb{Z}_p[X]$$

hat eine *Reduktion*

$$\overline{f} = \overline{a_n} X^n + \cdots + \overline{a_1} X^1 + \overline{a_0} \in \mathbb{F}_p[X].$$

Das Lemma von Hensel besagt: Hat $\overline{f}$ eine *einfache Nullstelle* (d. h. $\overline{f}(\overline{x}) = 0$ und $\overline{f}'(\overline{x}) \neq 0$), so gibt es einen *Lift* $x \in \mathbb{Z}_p$ mit $f(x) = 0$.

Den Beweis finden Sie im Skript (cf. Beweis zu Satz 8.1). Es wird eine Folge $x_n \in \mathbb{Z}_p$ konstruiert mit

$$x_n \to x.$$

Wir starten mit einem Lift $x_1 \in \mathbb{Z} \subset \mathbb{Z}_p$, d. h. $\overline{x_1} = x$. Damit gilt

$$\overline{f(x_1)} = \overline{f}(\overline{x_1}) = \overline{f}(\overline{x}) = 0, \tag{1}$$

also

$$f(x_1) \in p^1 \mathbb{Z}_p.$$

Wir haben also zwar evtl. noch nicht $f(x_1) = 0$, aber immerhin schon $|f(x_1) - 0| \leq p^{-1}$. Klar, dass wir nun versuchen wollen induktiv $x_n$ zu konstruieren, sodass $(x_n)$ konvergiert und $f(x_n) \to 0$ gilt. Unsere Induktionsannahmen können wir also wie folgt wählen: Für bereits konstruierte $x_1, \ldots, x_N$ gelte

(i) $|f(x_n) - 0| \leq p^{-n}$ für $n \leq N$

(ii) $|x_{n+1} - x_n| \leq p^{-n}$ für $n + 1 \leq N$

Die erste Bedingung ist für unser $x_1$ und $N = 1$ erfüllt; die zweite auch (trivialerweise).

Nehmen wir an, wir haben $x_1, \ldots, x_N$ konstruiert, dann machen wir den Ansatz

$$x_{N+1} = x_N + p^N y \tag{2}$$

mit $y \in \mathbb{Z}_p$, sodass Bedingung (ii) weiterhin erfüllt wird. Wir wollen nun $y$ so wählen, dass auch (i) gilt. Dafür machen wir *Taylor-Entwicklung* um $x_N$

$$f(x_N + \varepsilon) = f(x_N) + f'(x_N)\varepsilon + \mathcal{O}(\varepsilon^2)$$

und setzen $\varepsilon = p^N y$ ein: Dann ist modulo $p^{N+1}$

$$f(x_{N+1}) = f(x_N) + f'(x_N) p^N y. \tag{3}$$

Wegen (i) gilt $f(x_N) = p^N z_N$ für $z_N \in \mathbb{Z}_p$ und die Gleichung

$$0 = z_N + f'(x_N)y \tag{4}$$

hat wegen $\overline{f'}(\overline{x}) \neq 0$ modulo $p$ eine (eindeutige) Lösung. Sei $y \in \mathbb{Z}_p$ ein (beliebiger) Lift von dieser. Dann gilt modulo $p^{N+1}$

$$\begin{aligned} f(x_{N+1}) &= f(x_N) + f'(x_N)p^N y \\ &= p^N \left(z_N + f'(x_N)y\right) \\ &\in p^{N+1}\mathbb{Z}_p. \end{aligned}$$

Das ist gerade der Nachweis für Bedingung (i).

**Aufgabe 1.** (8 Punkte)

- Gleichung (4) kann in $\mathbb{Q}_p$ umgeformt werden zu

  $$p^N y = -p^N (f'(x_N))^{-1} z_N.$$

  Eingesetzt in (2) erhalten wir

  $$x_{N+1} = x_N - \frac{f(x_N)}{f'(x_N)}. \tag{5}$$

  (Recherchieren Sie an dieser Stelle doch mal das *Newton-Verfahren.*) Beweisen Sie Hensel's Lemma *selbst*, indem Sie

  (i) Taylorentwicklung von $f$ bei $x_N$ machen ...

  (ii) und mithilfe von (5) den Betrag $|f(x_{N+1})|$ berechnen.

  (iii) Benutzen Sie $|f(x_1)| \leq p^{-1}$ und $|f'(x_1)| = 1$, um induktiv $|f(x_N)| \leq p^{-N}$, $|f'(x_N)| = 1$ und $|x_{N+1} - x_N| \leq p^{-N}$ zu zeigen.

  (iv) Zeigen Sie, dass $x = \lim x_N$ und $f(x) = 0$ gilt.

  *Bemerkung.* So sieht man sehr schön, wo $|f(x_1)| < 1$, bzw. $\overline{f}(\overline{x}) = 0$ eingeht und dass die Konstruktion von $x$ sogar *eindeutig* ist; gegeben einen Lift $x_1$ von $\overline{x}$.

Nun zu einer Anwendung des Lemmas (bzw. dessen Beweis):

- Es gilt $3^2 \equiv 2 \mod 7$, also ist $\overline{f} = (X - \overline{3})(X + \overline{3}) = X^2 - \overline{2} \in \mathbb{F}_7[X]$ die Reduktion von etwa $f_1 = X^2 - 9 \in \mathbb{Z}_7$, aber auch von $f_2 = X^2 - 2 \in \mathbb{Z}_7$. Finden Sie die Nullstellen von $f_1$ und $f_2$ über $\mathbb{Z}_7$.

Was passiert, wenn $\overline{x}$ keine *einfache* Nullstelle ist, d. h. wenn $\overline{f'}(\overline{x}) = 0$ gilt? Nehmen wir an, dass $\overline{f''}(\overline{x}) \neq 0$ noch erfüllt ist. Finden Sie Beispiele (falls möglich):

- Für $x$ gibt es keinen Lift $x$ mit $f(x) = 0$.
- Für $x$ gibt es trotzdem noch einen Lift $x$ mit $f(x) = 0$.