Kurzskript Modelltheorie II

Immi Halupczok

2. Mai 2024

Inhaltsverzeichnis

Modelltheorie II

1 Bewertete Körper

1.1 Beträge

Definition 1.1.1 *Sei K ein Körper. Ein **Betrag** auf K ist eine Abbildung $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ mit:*

(a) $|a| = 0 \iff a = 0$
(b) $|ab| = |a| \cdot |b|$
(c) $|a + b| \leq |a| + |b|$ *(**Dreiecksungleichung**).*

*(Manchmal nennt man das auch eine **Norm** auf K; es gibt aber auch etwas anderes, was man einen Norm auf einem Körper nennt.)*

Beispiel 1.1.2 *Auf $K \subseteq \mathbb{R}$: der normale Absolutbetrag: $|a|_{\mathbb{R}} = a$ falls $a \geq 0$ und $|a|_{\mathbb{R}} = -a$ falls $a \geq 0$.*

Beispiel 1.1.3 *Auf $K \subseteq \mathbb{C}$: der komplexe Betrag: $|a+ib|_{\mathbb{C}} = \sqrt{a^2 + b^2}$ für $a, b \in \mathbb{R}$.*

Beispiel 1.1.4 *Der **triviale Betrag** auf einem beliebigen Körper K: $|0|_0 = 0$, $|a|_0 = 1$ für $a \in K^\times$.*

Bemerkung 1.1.5 *Es gilt: $|1| = 1$; $|a| = |-a|$; $|\frac{1}{a}| = \frac{1}{|a|}$ für $a \in K^\times$.*

Definition 1.1.6 *Ein Betrag $|\cdot|$ heißt **nicht-archimedisch**, wenn die **ultrametrische Dreiecksungleichung** gilt:*

$$|a + b| \leq \max\{|a|, |b|\}$$

*Sonst heißt $|\cdot|$ **archimedisch**.*

Beispiel 1.1.7 *Sei R ein faktorieller Ring, $K = \operatorname{Frac} R$, und sei $p \in R$ ein irreduzibles Element. Dann lässt sich jedes Element $a \in K^\times$ schreiben in der Form $a = p^r \cdot \frac{m}{n}$, mit $m, n \in R$ nicht durch p teilbar und $r \in \mathbb{Z}$ beliebig. Sei außerdem s eine beliebige relle Zahl größer als 1. Dann wird durch $|a|_p := s^{-r}$ (und $|0|_p := 0$) ein (nicht-archimedischer) Betrag auf K definiert. Man nennt dies den p**-adischen Betrag** (oder die p**-adische Norm**).*

Bemerkung 1.1.8 *Ist $R = \mathbb{Z}$ und p eine Primzahl, so ist es üblich, $s = p$ zu wählen, d. h. der p-adische Betrag auf $\mathbb{Q}$ ist $|a|_p := p^{-r}$.*

Satz 1.1.9 (Satz von Ostrowski) *Die einzigen Beträge auf $\mathbb{Q}$ sind der triviale, $x \mapsto |x|_{\mathbb{R}}^{\lambda}$ für $\lambda \in (0,1]$, und $x \mapsto |x|_p^{\lambda}$ für $\lambda \in (0,\infty)$ und p prim.*

Lemma 1.1.10 *Sei K ein Körper mit einem Betrag $|\cdot|$, und sei $A := \{|n \cdot 1| \mid n \in \mathbb{Z}\}$. Ist $|\cdot|$ archimedisch, so ist A unbeschränkt. (Insbesondere hat K Charakteristik 0.) Ist $|\cdot|$ nicht-archimedisch, so ist $A \subseteq [0,1]$.*

Beispiel 1.1.11 *Ist k ein beliebiger Körper, $R = k[t]$, $a \in k$ und $f = t - a$, so gilt für $q \in k(t) = \operatorname{Frac} R$: Ist $|q|_f = 2^r$, so hat q eine r-fache Nullstelle bei a, wobei Polstellen als negative Nullstellen angesehen werden.*

1.2 Vervollständigung

Lemma 1.2.1 *Sei K ein Körper und $|\cdot|$ ein Betrag auf K. Dann ist $d(a,b) := |a-b|$ eine Metrik auf K. Addition, Multiplikation, $x \mapsto -x$ und $x \mapsto \frac{1}{x}$ (für $x \neq 0$) sind stetig bezüglich der von dieser Metrik induzierten Topologie.*

Satz 1.2.2 *Sei K ein Körper mit einem Betrag $|\cdot|$, und sei $\hat{K}$ die Vervollständigung von K bezüglich der von $|\cdot|$ induzierten Metrik. Dann lassen sich die Addition, die Multiplikation und der Betrag von K auf eindeutige Weise stetig auf $\hat{K}$ fortsetzen, und $\hat{K}$ wird auf diese Art auch ein Körper mit Betrag.*

Beispiel 1.2.3 *Die Vervollständigung von $\mathbb{Q}$ bezüglich $|\cdot|_{\mathbb{R}}$ ist $\mathbb{R}$.*

Definition 1.2.4 *Sei p eine Primzahl. Der Körper $\mathbb{Q}_p$ der **p-adischen Zahlen** ist die Vervollständigung von $\mathbb{Q}$ bezüglich des p-adischen Betrags.*

Korollar 1.2.5 (zum Satz von Ostrowski) *Die Vervollständigungen von $\mathbb{Q}$ bezüglich beliebigen Beträgen auf $\mathbb{Q}$ sind: $\mathbb{Q}$ selbst (wenn der Betrag trivial ist); $\mathbb{R}$; und $\mathbb{Q}_p$ für alle Primzahlen p.*

Satz 1.2.6 *Sei p eine Primzahl.*

(a) *Seien $r_i \in \{0, 1, \ldots, p-1\}$ für alle $i \geq \mathbb{Z}$. Wir nehmen an, dass ein $N \in \mathbb{Z}$ existiert, so dass $r_i = 0$ für alle $i < N$ ist. Dann konvergiert die Folge*

$$a_m := \sum_{i=N}^{m} r_i p^i$$

bezüglich der p-adischen Norm gegen ein Element

$$a := \sum_{i \in \mathbb{Z}} r_i p^i := \lim_{m \to \infty} a_m$$

aus $\mathbb{Q}_p$. Ist N minimal mit $r_N \neq 0$, so ist $|a|_p = p^{-N}$.

(b) *Jedes Element $a \in \mathbb{Q}_p$ lässt sich auf eindeutige Weise als ein solcher Limes schreiben.*

Definition 1.2.7 *Die **ganzen p-adischen Zahlen** sind definiert als $\mathbb{Z}_p := \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$.*

Bemerkung 1.2.8 *Es gilt $\mathbb{Z}_p = \{\sum_{i\geq 0} r_i p^i \mid r_i \in \{0, \dots, p-1\}$ für alle $i\}$, wobei der Grenzwert in $\mathbb{Q}_p$ berechnet wird.*

Bemerkung 1.2.9 *$\mathbb{Z}_p$ ist ein Unterring von $\mathbb{Q}_p$.*

Satz 1.2.10 *$\mathbb{Z}_p$ ist der topologische Abschluss von $\mathbb{Z}$ in $\mathbb{Q}_p$.*

Definition 1.2.11 *Sei k ein Körper. Die Menge der **formalen Laurent-Reihen** über k ist definiert als die Menge der formalen Summen der Form*

$$k(\!(t)\!) := \{\sum_{i\geq N} r_i t^i \mid N \in \mathbb{Z}, \forall i\colon r_i \in k\}.$$

*Die Summe und das Produkt von zwei solchen Reihen sind so definiert, wie man es bei Reihen erwartet. Der (t-adische) Betrag einer formalen Reihe $a = \sum_{i\geq N} r_i t^i \in k(\!(t)\!)$ mit $r_N \neq 0$ ist $|a|_t := 2^{-N}$. (Und: $|0|_t := 0$.) Die **formalen Potenzreihen** sind*

$$k[\![t]\!] := \{a \in k(\!(t)\!) \mid |a|_t \leq 1\} = \{\sum_{i\geq 0} r_i t^i \mid \forall i\colon r_i \in k\}.$$

Satz 1.2.12 *$k(\!(t)\!)$ ist die Vervollständigung von $k(t)$ bezüglich des t-adischen Betrags aus Beispiel 1.1.11; insbesondere ist $k(\!(t)\!)$ ein Körper. Die Teilmenge $k[\![t]\!]$ bildet einen Unterring, und sie ist der topologische Abschluss von $k[t]$ in $k(\!(t)\!)$.*

1.3 Bewertete Körper

Definition 1.3.1 *Eine **angeordnete abelsche Gruppe** ist eine abelsche Gruppe Γ mit Ordnungsrelation $<$, so dass für alle $\alpha, \alpha', \beta \in \Gamma$ gilt: $\alpha < \alpha' \Rightarrow \alpha+\beta < \alpha'+\beta$.*

Beispiel 1.3.2 $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ $(\mathbb{R}_{>0}, \cdot)$.

Bemerkung 1.3.3 *Angeordnete abelsche Gruppen sind torsionsfrei.*

Definition 1.3.4 *Sei K ein Körper. Eine **Bewertung** auf K ist eine Abbildung $v\colon K \twoheadrightarrow \Gamma \cup \{\infty\}$, wobei Γ eine angeordnete abelsche Gruppe ist, so dass für alle $a, b \in K$ gilt:*

- $v(a) = \infty \iff a = 0$
- $v(ab) = v(a) + v(b)$
- $v(a+b) \geq \min\{v(a), v(b)\}$.

Ein Körper mit Bewertung heißt ***bewerteter Körper****.* Γ *heißt* ***Wertegruppe****.*

Zwei Bewertungen $v\colon K \to \Gamma$, $v'\colon K \to \Gamma'$ *heißen* ***äquivalent****, wenn ein ordungserhaltender Gruppenisomorphismus* $\alpha\colon \Gamma \to \Gamma'$ *existiert mit* $v' = \alpha \circ v$.

Bemerkung 1.3.5 *Ist* (K, v) *ein bewerteter Körper mit Wertegruppe* $\Gamma \subseteq (\mathbb{R}, +)$*, so wird durch* $|x| := 2^{-v(x)}$ *ein nicht-archimedischer Betrag auf* K *definiert. Ist umgekehrt* $|\cdot|$ *ein nicht-archimedischer Betrag auf einem Körper* K*, so erhält man eine Bewertung* $v(x) := -\log(|x|)$ *auf* K*, deren Wertegruppe eine Untergruppe von* $(\mathbb{R}, +)$ *ist.*

Beispiel 1.3.6 *Den p-adischen Beträgen aus Beispiel 1.1.7 entsprechen jeweils p-adische Bewertungen (mit Wertegruppe* $\mathbb{Z}$*): Ist* R *ein faktorieller Ring,* $K = \operatorname{Frac} R$ *und* $p \in R$ *irreduzibel, so ist die p-adische Bewertung auf* K *definiert durch* $v_p(p^r \cdot \frac{m}{n}) = r$*, für* $r \in \mathbb{Z}$ *und* $m, n \in R$ *nicht durch p-teilbar.*

Bemerkung 1.3.7 *Sei* (K, v) *ein bewerteter Körper. Dann gilt für* $a, b \in K$*:*

(a) $v(1) = 0$*;* $v(-a) = v(b)$*;* $v(\frac{1}{a}) = -v(a)$
(b) *Ist* $v(a) \neq v(b)$*, so ist* $v(a+b) = \min\{v(a), v(b)\}$.
(c) *Sind* $a_1, \ldots, a_n \in K$ *mit* $\sum_{i=1}^{n} a_i = 0$*, so tauch die minimale Bewertung mehrfach auf, d. h. es existieren* $j \neq j'$ *mit* $v(a_j) = v(a_{j'}) = \min\{v(a_1), \ldots, v(a_n)\}$.

Definition 1.3.8 *Sei* (K, v) *ein bewerteter Körper mit Wertegruppe* Γ.

(a) *Ein* ***offener Ball*** *in* K *ist eine Teilmenge der Form* $B_{>\gamma}(a) := \{x \in K \mid v(x-a) > \gamma\}$ *für* $a \in K$, $\gamma \in \Gamma$.
(b) *Ein* ***abgeschlossener Ball*** *in* K *ist eine Teilmenge der Form* $B_{\geq\gamma}(a) := \{x \in K \mid v(x-a) \geq \gamma\}$ *für* $a \in K$, $\gamma \in \Gamma$.
(c) *Die* ***Bewertungs-Topologie*** *auf* K *ist die Topologie mit den offenen Bällen als Basis.*

Bemerkung 1.3.9 (a) *„Jeder Punkt eines Balls ist Mittelpunkt des Balls“: Für* $b \in B_{>\gamma}(a)$ *beliebig gilt* $B_{>\gamma}(a) = B_{>\gamma}(b)$*; und analog für abgeschlossene Bälle.*
(b) *Sind* $B_1, B_2 \subseteq K$ *zwei Bälle, so ist entweder einer der Bälle im anderen enthalten oder* $B_1 \cap B_2 = \emptyset$.

Bemerkung 1.3.10 *Ist* $B \subseteq K$ *ein offener* <u>*oder*</u> *abgeschlossener Ball, so ist* B *topologisch offen* <u>*und*</u> *abgeschlossen.*

1.4 Bewertungsringe

Lemma 1.4.1 *Sei (K, v) ein bewerteter Körper. Dann gilt:*

(a) $\mathcal{O}_K := \{a \in K \mid v(a) \geq 0\}$ *ist ein Unterring von* K.
(b) *Die Einheiten dieses Rings sind* $\mathcal{O}_K^\times = \{a \in K \mid v(a) = 0\}$.
(c) $\mathcal{M}_K := \{a \in K \mid v(a) > 0\}$ *ist das einzige maximale Ideal von* $\mathcal{O}_K$.

Definition 1.4.2 *Den Ring $\mathcal{O}_K$ aus Lemma 1.4.1 nennt man den* ***Bewertungsring*** *von v. Den Quotient $\bar{K} := \mathcal{O}_K/\mathcal{M}_K$ nennt man den* ***Restklassenkörper****. Die Abbildung $\mathcal{O}_K \to \bar{K}$ heißt* ***Restklassenabbildung*** *und wird mit* res *bezeichnet (und manchmal auch als $a \mapsto \bar{a}$ geschrieben).*

Beispiel 1.4.3 (a) *Ist $K = k(\!(t)\!)$, so ist $\mathcal{O}_K = k[\![t]\!]$, $\mathcal{M}_K = tk[\![t]\!]$, $\bar{K} = k$ und* $\operatorname{res}(\sum_{i\in\mathbb{N}} r_i t^i) = r_0$.
(b) *Ist $L = \mathbb{Q}_p$, so ist $\mathcal{O}_K = \mathbb{Z}_p$, $\mathcal{M}_K = p\mathbb{Z}_p$, $\bar{K} = \mathbb{F}_p$ und* $\operatorname{res}(\sum_{i\in\mathbb{N}} r_i p^i) = r_0$.

Bemerkung 1.4.4 *Eine Bewertung auf einem Körper K ist (bis auf Äquivalenz) eindeutig durch den Bewertungsring $\mathcal{O}_K$ festgelegt: Die Bewertung ist ein surjektiver Gruppenhomorphismus von $K^\times$ nach Γ mit Kern $\mathcal{O}_K^\times$; es gilt also $\Gamma \cong K^\times/\mathcal{O}_K^\times$. Außerdem ist die Ordnung auf Γ dadurch festgelegt, dass $v(a) \geq 0$ genau dann, wenn $a \in \mathcal{O}_K$ ist.*

Definition 1.4.5 *Ein (abstrakter)* ***Bewertungsring*** *von einem Körper K ist ein Unterring $R \subseteq K$, so dass gilt: Für alle $a \in K$ ist $a \in R$ oder $\frac{1}{a} \in R$.*

Bemerkung 1.4.6 *Ist K ein bewerteter Körper, so ist der Bewertungsring $\mathcal{O}_K$ insbesondere ein abstrakter Bewertungsring.*

Satz 1.4.7 *Jeder abstrakte Bewertungsring eines Körpers K ist der Bewertungsring einer Bewertung auf K.*

Beispiel 1.4.8 *Ist $\mathbb{R}^* \succ \mathbb{R}$ eine elementare Erweiterung, so können wir auf $\mathbb{R}^*$ eine Bewertung definieren, die die Größenordnung von Elementen misst. Es ist die Bewertung, die als Bewertungsring die Menge der „endlichen“ Zahlen hat: $\mathcal{O}_{\mathbb{R}^*} := \{a \in \mathbb{R}^* \mid \exists b \in \mathbb{R}\colon |a|_{\mathbb{R}} < b\}$. Der Restklassenkörper zu dieser Bewertung ist $\mathbb{R}$.*

Definition 1.4.9 *Sei K ein bewerteter Körper und $\bar{K}$ sein Restklassenkörper. Man sagt, K hat* ***Charakteristik*** *(p, q), wenn* $\operatorname{char} K = p$ *und* $\operatorname{char} \bar{K} = q$ *ist. Ist $q = p$, so sagt man auch, K hat* ***Äquicharakteristik*** *p. Ist $q \neq p$, so sagt man, K hat* ***gemischte Charakteristik****.*

Bemerkung 1.4.10 *Als Charakteristiken von bewerteten Körpern können auftreten:* $(0, 0)$, $(0, p)$ *und* (p, p), *für Primzahlen p.*

1.5 Fortsetzung von Bewertungen

Definition 1.5.1 *Seien (K_1, v_1) und (K_2, v_2) bewertete Körper mit $K_1 \subseteq K_2$ und seien Γ_1 und Γ_2 die entsprechenden Wertegruppen. Wir nennen v_2 eine **Fortsetzung** von v_1 (auf K_2), wenn v_1 äquivalent ist zur Einschränkung $v_2|_{K_1}$.*

Bemerkung 1.5.2 *Nach Bemerkung 1.4.4 ist das äquivalent zu: $\mathcal{O}_{K_1} = \mathcal{O}_{K_2} \cap K_1$. Außerdem gilt dann auch $\mathcal{O}_{K_1}^\times = \mathcal{O}_{K_2}^\times \cap K_1$ und $\mathcal{M}_{K_1} = \mathcal{M}_{K_2} \cap K_1$, und man erhält eine natürliche Einbettung $\bar{K}_1 \subseteq \bar{K}_2$.*

Satz 1.5.3 *Ist $K \subseteq L$ eine Körpererweiterung, so lässt sich jede Bewertung auf K zu einer Bewertung auf L fortsetzen.*

1.6 Newton-Polygone

Im folgenden sei K ein bewerteter Körper mit Wertegruppe Γ und $\Gamma_\mathbb{Q} = \{\frac{\gamma}{n} \mid \gamma \in \Gamma, n \in \mathbb{N}_{\geq 1}\}$ die divisible Hülle von Γ.

Definition 1.6.1 *Sei $f = \sum_{i=0}^n a_i X^i \in K[X]$ ein Polynom mit $a_n \neq 0$. Das **Newton-Polygon** von f ist der Streckenzug durch die Punkte $(\ell, \mathrm{NP}_f(\ell)) \in \mathbb{N} \times \Gamma_\mathbb{Q}$, für $0 \leq \ell \leq n$, wobei*

$$\mathrm{NP}_f(\ell) = \min\left\{ v(a_\ell), \min_{i<\ell, j>\ell} \frac{(\ell - i)v(a_j) + (j - \ell)v(a_i)}{j - i} \right\}.$$

*Aufeinanderfolgende Teilstrecken, die auf einer Geraden liegen, nennt man ein **Segment** des Newtonpolygons.*

Satz 1.6.2 *Sei $f = \sum_{i=0}^n a_i X^i \in K[X]$ ein Polynom vom Grad n. Wir setzen die Bewertung von K auf beliebige Weise auf K^{alg} fort und schreiben $f = a_n \cdot \prod_{i=1}^n (X - \alpha_i)$, mit $\alpha_i \in K^{\mathrm{alg}}$ und $v(\alpha_1) \geq v(\alpha_2) \geq \cdots \geq v(\alpha_n)$. Dann ist $\mathrm{NP}_f(\ell) = v(a_n) + \sum_{i>\ell} v(\alpha_i)$ für $\ell = 0, \ldots, n$; oder anders ausgedrückt: $v(\alpha_\ell) = \mathrm{NP}_f(\ell) - \mathrm{NP}_f(\ell + 1)$ für $\ell = 1, \ldots, n$.*

Korollar 1.6.3 *Ist $f \in \mathcal{O}_K[X]$ ein normiertes Polynom, so liegen alle Nullstellen von f in $\mathcal{O}_K$.*

Korollar 1.6.4 *Wenn wir die Bewertung von K auf beliebige Weise auf K^{alg} fortsetzen, so hat diese Fortsetzung als Wertegruppe $\Gamma_\mathbb{Q}$.*

Korollar 1.6.5 *Sind $f, g \in K[X]$ Polynome vom Grad n und m und ist $h = f \cdot g$, so lässt sich NP_h wie folgt aus NP_f und NP_g bestimmen:*

- $\mathrm{NP}_h(m + n) = \mathrm{NP}_f(n) + \mathrm{NP}_g(m)$

- *Die Segmente von* NP_h *sind genau die Segmente von* NP_f *und die Segmente von* NP_g*, so sortiert, dass* NP_h *konvex ist; also formal: Ist* $\lambda_i = \mathrm{NP}_f(i) - \mathrm{NP}_f(i-1)$ *für* $i = 1, \ldots, n$*, und analog* $\mu_i = \mathrm{NP}_g(i) - \mathrm{NP}_g(i-1)$ *und* $\nu_i = \mathrm{NP}_h(i) - \mathrm{NP}_h(i-1)$*, so erhält man die Folge* $\nu_1, \ldots, \nu_{m+n}$*, indem man die Folge* $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_m$ *aufsteigend sortiert.*

Korollar 1.6.6 (Verallgemeinertes Eisensteinsches Irreduzibilitäts-Kriterium) *Sei* $f \in K[X]$ *ein Polynom vom Grad* n *über einem Körper* K*. Wenn eine Bewertung auf* K *existiert, so dass* $\mathrm{NP}_f(\ell) \notin \Gamma$ *für* $1 \leq \ell \leq n-1$ *gilt, so ist* f *irreduzibel.*

1.7 Henselsche Körper

Definition 1.7.1 *Ein bewerteter Körper* K *heißt* ***henselsch****, wenn gilt: Sind* $f \in \mathcal{O}_K[X]$ *und* $a \in \mathcal{O}_K$ *mit* $v(f(a)) > 0$ *und* $v(f'(a)) = 0$*, so existiert (mindestens) ein* $a_0 \in \mathcal{O}_K$ *mit* $f(a_0) = 0$ *und* $v(a_0 - a) > 0$*.*

Satz 1.7.2 (Hensels Lemma) *Sei* K *ein bewerteter Körper mit Wertegruppe* $\Gamma = \mathbb{Z}$*, der vollständig ist bezüglich der Metrik* $d(a,b) := 2^{-v(a-b)}$*. Dann ist* K *henselsch.*

Bemerkung 1.7.3 *Eine zu Definition 1.7.1 äquivalente Formulierung ist:* K *ist henselsch, wenn für jedes* $f \in \mathcal{O}_K[X]$ *gilt: Jede einfache Nullstelle* $\bar{a} \in \bar{K}$ *von* $\mathrm{res}(f)$ *lässt sich zu einer Nullstelle* $b \in \mathrm{res}^{-1}(\bar{a})$ *von* f *liften.*

Satz 1.7.4 (Newtons Lemma) *Sei* K *wie in Satz* **??** *bewerteter Körper mit Wertegruppe* $\Gamma = \mathbb{Z}$*, sei* $f \in \mathcal{O}_K[X]$ *ein Polynom, und sei* $a \in \mathcal{O}_K$ *so, dass* $v(f(a)) > 2v(f'(a))$ *gilt. Dann existiert genau ein* $b \in \mathcal{O}_K$ *mit* $f(b) = 0$ *und* $v(b-a) \geq v(f(a)) - v(f'(a))$*.*

Bemerkung 1.7.5 *In henselschen Körpern gilt sogar Newtons Lemma (Übung).*

Beispiel 1.7.6 *Algebraisch abgeschlossene bewertete Körper sind henselsch.*

Beispiel 1.7.7 *Der Körper* $\mathbb{R}^* \succ \mathbb{R}$ *mit der Bewertung aus Beispiel 1.4.8 ist henselsch.*

Bemerkung 1.7.8 *Man kann zeigen: Ein bewerteter Körper* K *ist henselsch genau dann, wenn die Bewertung von* K *genau eine Fortsetzung auf den algebraischen Abschluss* K^{alg} *besitzt.*

Bemerkung 1.7.9 *Man kann zeigen: Zu jedem bewerteten Körper* K *gibt es einen kleinsten henselschen bewerteten Körper* $K^h \subseteq K^{\mathrm{alg}}$*, der* K *enthält.* K^h *ist (als bewerteter Körper) eindeutig bis auf Automorphismus über* K *und heißt* ***henselsche Hülle*** *von* K*.*

Bemerkung 1.7.10 *Man kann zeigen: Ist K Körper mit Betrag und $\hat{K}$ die Vervollständigung, so ist $K^h = \hat{K} \cap K^{\mathrm{alg}}$.*

1.8 Anwendung auf diophantische Gleichungen

Konvention: Alle Ringe sind kommutativ und mit 1.

Notation 1.8.1 *Sei $\underline{f} := (f_1, \ldots, f_\ell) \in \mathbb{Z}[X_1, \ldots, X_n]^\ell$ ein Tupel von Polynomen und sei R ein Ring. Dann schreiben wir*

$$V_{\underline{f}}(R) := \{\underline{a} \in R^n \mid f_1(\underline{a}) = \cdots = f_\ell(\underline{a}) = 0\}$$

für die Lösungen des Gleichungssystems „$\underline{f} = 0$“ in R^n.

Bemerkung 1.8.2 *Die Lösbarkeit von diophantischen Gleichungen ist unentscheidbar: Es gibt keinen Algorithmus, der ein Polynom $f \in \mathbb{Z}[X_1, \ldots, X_n]$ nimmt und entscheidet, ob $V_f(\mathbb{Z})$ nicht-leer ist.*

Bemerkung 1.8.3 *Ist $V_f(\mathbb{Z})$ nicht-leer, so ist auch $V_f(\mathbb{Z}/m\mathbb{Z})$ nicht-leer für alle $m \geq 1$.*

Lemma 1.8.4 *Sei $\underline{f} \in \mathbb{Z}[X_1, \ldots, X_n]^\ell$ und $m \geq 1$. Ist $m = \prod_i p_i^{r_i}$ die Primfaktorzerlegung von m, so induzieren die kanonischen Projektionen $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/p_i^{r_i}\mathbb{Z}$ eine Bijektion*

$$V_{\underline{f}}(\mathbb{Z}/m\mathbb{Z}) \to \prod_i V_{\underline{f}}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$$

Bemerkung 1.8.5 *Für jede Primzahl p und jedes $r \geq 0$ gilt: $\mathbb{Z}/p^r\mathbb{Z} \cong \mathbb{Z}_p/p^r\mathbb{Z}_p$.*

Definition 1.8.6 *Sei $\underline{f} \in \mathbb{Z}[X_1, \ldots, X_n]^\ell$ und p prim. Die **Poincaré-Reihe** zu $\underline{f}$ ist die formale Potenzreihe*

$$P_{\underline{f},p}(Z) := \sum_{r \in \mathbb{N}} N_r Z^r \in \mathbb{Q}[[Z]],$$

für $N_r := \#V_{\underline{f}}(\mathbb{Z}/p^r\mathbb{Z})$.

Satz 1.8.7 *Sei $\underline{f} \in \mathbb{Z}[X_1, \ldots, X_n]^\ell$ und p prim. Die Poincaré-Reihe $P_{\underline{f},p}(Z)$ ist eine rationale Funktion in Z, d. h. $P_{\underline{f},p}(Z) \in \mathbb{Q}(Z)$.*

Beispiel 1.8.8 *Ist f das Null-Polynom in n Variablen, so ist $P_{f,p}(Z) = \frac{1}{1-p^n Z}$.*

Satz 1.8.9 *Sei $\underline{f} \in \mathbb{Z}[X_1, \ldots, X_n]^\ell$. Dann existieren ein Polynom $h \in \mathbb{Z}[Z, P]$ und Ringformeln $\phi_0, \ldots, \phi_m$, $\phi'_0, \ldots, \phi'_m$, so dass für jede Primzahl p gilt:*

$$P_{\underline{f},p}(Z) = \frac{\sum_{i=0}^m (\#\phi_i(\mathbb{F}_p) - \#\phi'_i(\mathbb{F}_p))Z^i}{h(Z,p)}.$$