Modelltheorie II – Kurzskript

Inhaltsverzeichnis

1 Bewertete Körper **2**
- 1.1 Beträge 2
- 1.2 Vervollständigung 3
- 1.3 Bewertete Körper 4
- 1.4 Bewertungsringe 5
- 1.5 Fortsetzung von Bewertungen 5
- 1.6 Newton-Polygone 6
- 1.7 Henselsche Körper 6
- 1.8 Anwendung auf diophantische Gleichungen 7

2 Quantorenelimination in bewerteten Körpern **8**
- 2.1 Leitterme 8
- 2.2 Quantorenelimination: Die Aussagen 9
- 2.3 Polynome und rv 10
- 2.4 Beweis von Quantorenelimination 10
- 2.5 Der Satz von Ax-Kochen/Ershov und andere Folgerungen 11
- 2.6 Bessere Quantorenelimination in Spezialfällen 12

3 Rationalität von Poincaré-Reihen **13**
- 3.1 Zerlegung in krumme Quader 13
- 3.2 Messen in $\mathbb{Q}_p$ 13
- 3.3 Rationalität von Presburger-Poincaré-Reihen 14
- 3.4 Rationalität von L_{DP}-Poincaré-Reihen 14

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) $|x| = 0 \iff x = 0$
(b) $|xy| = |x| \cdot |y|$
(c) $|x+y| \leq |x| + |y|$ *(**Dreiecksungleichung**).*

Beispiel 1.1.2 *Auf $K \subset \mathbb{R}$: der normale Betrag: $|x|_{\mathbb{R}} = x$ falls $x \geq 0$ und $|x|_{\mathbb{R}} = -x$ falls $x \geq 0$.*

Beispiel 1.1.3 *Auf $K \subset \mathbb{C}$: der komplexe Betrag: $|x+iy|_{\mathbb{C}} = \sqrt{x^2+y^2}$ für $x, y \in \mathbb{R}$.*

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

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

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

$$|x+y| \leq \max\{|x|, |y|\}$$

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

Beispiel 1.1.7 *Sei p eine Primzahl. Ist $x = p^r \cdot \frac{m}{n} \in \mathbb{Q}^\times$, für $m, n \in \mathbb{Z}$ nicht durch p teilbar und $r \in \mathbb{Z}$ beliebig, so setzen wir $|x|_p = p^{-r}$. Außerdem setzen wir $|0|_p = 0$. Dies ist ein (nicht-archimedischer) Betrag auf $\mathbb{Q}$, der* ***p-adische Betrag****.*

Beispiel 1.1.8 *Sei K ein beliebiger Körper und $p \in K[X]$ ein beliebiges irreduzibles Polynom. Dann lässt sich jedes Element $f \in K(X)^\times$ schreiben als $f = p^r \cdot \frac{g}{h}$, für $g, h \in K[X]$, die nicht durch p teilbar sind und $r \in \mathbb{Z}$. Wir setzen dann $|f|_p := e^{-r}$; außerdem setzen wir $|0|_p = 0$. Dies definiert einen nicht-archimedischen Betrag auf $K(X)$. Ist $p = X - a$, für $a \in K$, so gibt $|f|_p$ die Vielfachheit der Nullstelle a von f an (wobei Polstellen negativ zählen).*

Beispiel 1.1.9 *Sei K ein beliebiger Körper. Für $f = \frac{g}{h} \in K(X)^\times$ (mit $g, h \in K[X]$) setzen wir $|f|_\infty := e^{\deg f - \deg f}$. Außerdem setzen wir $|0|_\infty := 0$. Dies ist ein (nicht-archimedischer) Betrag auf $K(X)$.*

Satz 1.1.10 (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 1.1.11 *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. (Inbesondere hat K Charakteristik 0.) Ist $|\cdot|$ nicht-archimedisch, so ist $A \subset [0,1]$.*

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. Die Menge der **p-adischen Zahlen** ist definiert als die Menge der formalen Summen der Form*

$$\mathbb{Q}_p := \{\sum_{i \geq N} r_i p^i \mid N \in \mathbb{Z}, \forall i\colon 0 \leq r_i < p\},$$

*Die Summe und das Produkt von zwei p-adischen Zahlen sind so definiert, wie bei der Darstellung von Zahlen in Basis p. Der (p-adische) Betrag einer p-adischen Zahl $a = \sum_{i \geq N} r_i p^i \in \mathbb{Q}_p$ mit $r_N \neq 0$ ist definiert durch $|a|_p := p^{-N}$. (Und: $|0|_p := 0$.) Die **ganzen p-adischen Zahlen** sind*

$$\mathbb{Z}_p := \{\sum_{i \geq 0} r_i p^i \in \mathbb{Q}_p \mid \forall i\colon 0 \leq r_i < p\}.$$

Satz 1.2.5 *$(\mathbb{Q}_p, |\cdot|_p)$ ist (bis auf Isomorphie) die Vervollständigung von $\mathbb{Q}$ bezüglich des p-adischen Betrags auf $\mathbb{Q}$; $\mathbb{Z}_p$ ist der topologische Abschluss von $\mathbb{Z}$ in $\mathbb{Q}_p$.*

Bemerkung: $\mathbb{Z}_p$ lässt sich auch als inverser Limes definieren:

$$\mathbb{Z}_p := \varprojlim_r \mathbb{Z}/p^r\mathbb{Z} := \{(z_r)_{r \in \mathbb{N}} \mid \forall r\colon z_r \in \mathbb{Z}/p^r\mathbb{Z}, \pi_r(z_r) = z_{r-1}\},$$

wobei $\pi_r\colon \mathbb{Z}/p^r\mathbb{Z} \to \mathbb{Z}/p^{r-1}\mathbb{Z}$ die kanonische Abbildung ist.

Korollar 1.2.6 *Die Vervollständigungen von $\mathbb{Q}$ bezüglich beliebigen Beträgen auf $\mathbb{Q}$ sind: $\mathbb{Q}$ selbst (bei trivialem Betrag); $\mathbb{R}$; $\mathbb{Q}_p$ für alle Primzahlen p.*

Definition 1.2.7 *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 definiert durch $|a|_t := e^{-N}$. (Und: $|0|_t := 0$.) Die **formalen Potenzreihen** sind*

$$K[[t]] := \{\sum_{i \geq 0} r_i t^i \in \mathbb{Q}_p \mid \forall i\colon r_i \in K\}.$$

Satz 1.2.8 *$(K((t)), |\cdot|_t)$ ist (bis auf Isomorphie) die Vervollständigung von $K(t)$ bezüglich des t-adischen Betrags auf $K(t)$; $K[[t]]$ 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 $a, a', b \in \Gamma$ gilt: $a < a' \Rightarrow a + b < a' + b$.*

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

Beispiel 1.3.3 *Sind Γ und Γ' angeordnete abelsche Gruppen, so ist auch $\Gamma \times \Gamma'$ mit der* ***lexikographischen Ordnung*** *eine angeordnete abelsche Gruppe: $(a, b) \geq 0 \iff a \geq 0$ oder ($a = 0$ und $b \geq 0$).*

Lemma 1.3.4 *Angeordnete abelsche Gruppen sind torsionsfrei.*

Definition 1.3.5 *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 gilt:*
- $v(x) = \infty \iff x = 0$
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \min\{v(x), v(y)\}$.

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 $\phi \colon \Gamma \to \Gamma'$ existiert mit $v' = \phi \circ v$.*

Beispiel 1.3.6 *Sei R ein faktorieller Ring, $K = \mathrm{Quot}(R)$, und sei $p \in R$ prim. Wir definieren die* ***p-adische Bewertung*** *$v_p \colon K \to \mathbb{Z} \cup \{\infty\}$ wie folgt. $v_p(0) := \infty$. Und: Ist $x = p^r \cdot \frac{m}{n} \in K^\times$, für $m, n \in R$ nicht durch p teilbar und $r \in \mathbb{Z}$ beliebig, so setzen wir $v_p(x) := r$.*

Lemma 1.3.7 *Ist (K, v) ein bewerteter Körper mit $\Gamma \subset (\mathbb{R}, +)$, so wird durch $|x| := a^{-v(x)}$ ein Betrag auf K definiert, für beliebige reelle $a > 1$.*

Lemma 1.3.8 *Ein nicht-archimedischer Betrag $|\cdot|$ auf einem Körper K induziert eine Bewertung auf K: $v(x) := -\log(|x|)$; die Wertegruppe ist eine Untergruppe von $(\mathbb{R}, +)$.*

Bemerkung 1.3.9 *Sei (K, v) ein bewerteter Körper. Dann gilt für $x, y \in K$:*

(a) $v(1) = 0$; $v(-x) = v(x)$; $v(\frac{1}{x}) = -v(x)$

(b) *Ist $v(x) \neq v(y)$, so ist $v(x + y) = \min\{v(x), v(y)\}$.*

Definition 1.3.10 *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 1.3.11 *Der Schnitt von zwei (offen/abgeschlossenen/beliebigen) Bällen ist wieder ein (offener/abgeschlossener/beliebiger) Ball.*

Bemerkung 1.3.12 *Abgeschlossene Bälle sind topologisch auch offen.*

1.4 Bewertungsringe

Definition 1.4.1 *Sei K ein Körper. Ein* ***Bewertungsring*** *(von K) ist ein Unterring $\mathcal{O}_K \subset K$, so dass für alle $a \in K$ gilt: $a \in \mathcal{O}_K$ oder $\frac{1}{a} \in \mathcal{O}_K$. Allgemeiner nennt man einen kommutativen Integritätsbereich* ***Bewertungsring****, wenn er ein Bewertungsring seines Quotientenkörpers ist.*

Bemwerkung: Ist $\mathcal{O}_K$ ein Bewertungsring von K, so ist $K = \operatorname{Quot} \mathcal{O}_K$.

Lemma 1.4.2 *Sei (K, v) ein bewerteter Körper.*

- *$\mathcal{O}_K := \{a \in K \mid v(a) \geq 0\}$ ist ein Bewertungsring mit Quotienten-Körper K.*
- *$\mathcal{O}_K^\times = \{a \in K \mid v(a) = 0\}$.*
- *$\mathcal{M}_K := \{a \in K \mid v(a) > 0\}$ ist das einzige maximale Ideal von $\mathcal{O}_K$.*

Definition 1.4.3 *Den Ring $\mathcal{O}_K$ aus Lemma 1.4.2 nennt man auch den* ***Bewertungsring von*** *v. Den Quotient $\bar{K} := \mathcal{O}_K / \mathcal{M}_K$ nennt man den* ***Restklassenkörper****. Die Abbildung $\mathcal{O}_K \to \bar{K}$ wird oft mit res bezeichnet (und manchmal auch als $a \mapsto \bar{a}$ geschrieben).*

Satz 1.4.4 *Sei K ein Körper. Lemma 1.4.2 induziert Bijektion*

$$\{\textit{Bewertungen auf } K\}/\textit{Äquivalenz} \quad \stackrel{1:1}{\longleftrightarrow} \quad \{\textit{Bewertetungsringe in } K\}$$

Beispiel 1.4.5 *Seien $K \subset L$ angeordnete Körper, und sei $\mathcal{O}_L := \{a \in L \mid \exists b \in K\colon -b \leq a \leq b\}$ der konvexe Abschluss von K in L. Dann ist $\mathcal{O}_L$ ein Bewertungsring.*

Definition 1.4.6 *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 1.4.7 *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 $K_1 \subset K_2$ 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 Satz 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 $\bar{K}_1 \subset \bar{K}_2$.*

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

Beispiel 1.5.4 *Ist K ein bewerteter Körper, so erhält man auf $K(X)$ eine Bewertung durch $v(\sum_{i=0}^n a_i x^i) := \min_i v(a_i)$ (und $v(f(x)/g(x)) := v(f(x)) - v(g(x))$). Diese Bewertung heißt* ***Gauß-Bewertung****.*

1.6 Newton-Polygone

Im folgenden sei K ein bewerteter Körper mit Wertegruppe Γ und $\Gamma_{\mathbb{Q}}$ 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 die Abbildung $p\colon \{0, \dots, n\} \to \Gamma_{\mathbb{Q}} \cup \{\infty\}$, die gegeben ist durch:*

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

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 $\ell = 0, \dots, n$.*

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 *Sei $f \in \mathcal{O}_K[X]$ ein normiertes Polynom; wir setzen die Bewertung von K auf beliebige Weise auf K^{alg} fort und schreiben Γ^{alg} für die zugehörige Wertegruppe. Besitzt f genau k viele Nullstellen in K^{alg} mit Bewertung $\gamma \in \Gamma^{\mathrm{alg}}$, so ist $k\gamma \in \Gamma$. Insbesondere ist $\Gamma^{\mathrm{alg}} = \Gamma_{\mathbb{Q}}$.*

Satz 1.6.5 (Verallgemeinertes Eisensteinsches Irreduzibilitäts-Kriterium) *Sei $f \in L[X]$ ein Polynom vom Grad n über einem Körper L. Wenn eine Bewertung auf L existiert, so dass $\mathrm{NP}_f(\ell) \notin \Gamma$ für $1 \leq \ell \leq n - 1$ gilt, so ist f irreduzibel.*

Satz 1.6.6 *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 $i = 1, \dots, n$, 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 $\nu_1, \dots, \nu_{m+n}$, indem man die Folge $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_m$ aufsteigend sortiert.*

1.7 Henselsche Körper

Satz 1.7.1 (Hensels Lemma) *Sei K ein vollständiger bewerteter Körper mit $\Gamma = \mathbb{Z}$ (vollständig bezüglich der zugehörigen Metrik). Seien $f \in \mathcal{O}_K[X]$, $a \in \mathcal{O}_K$ mit $v(f(a)) > 0$ und $v(f'(a)) = 0$. Dann existiert genau ein $b \in \mathcal{O}_K$ mit $f(b) = 0$ und $v(b - a) > 0$.*

Bemerkung 1.7.2 *Eine äquivalente Formulierung ist: Ist $f \in \mathcal{O}_K[X]$ und ist $\bar{a} \in \bar{K}$ eine einfache Nullstelle von $\mathrm{res}(f)$, so besitzt f genau eine Nullstelle in $\mathrm{res}^{-1}(\bar{a})$.*

Satz 1.7.3 (Newtons Lemma) *Sei K ein vollständiger bewerteter Körper mit $\Gamma = \mathbb{Z}$ (vollständig bezüglich der zugehörigen Metrik). Seien $f \in \mathcal{O}_K[X]$, $a \in \mathcal{O}_K$ mit $v(f(a)) > 2v(f'(a))$. Dann existiert genau ein $b \in \mathcal{O}_K$ mit $f(b) = 0$ und $v(b - a) \geq v(f(a)) - v(f'(a))$ $(> v(f'(a)))$.*

Definition 1.7.4 *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 $v(a_0 - a) > 0$.*

Beispiel 1.7.5 *Nach Satz 1.7.1 sind vollständige bewertete Körper mit Wertegruppe $\mathbb{Z}$ henselsch.*

Beispiel 1.7.6 *Algebraisch abgeschlossene bewertete Körper immer henselsch.*

Bemerkung 1.7.7 *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 1.7.8 *Man kann zeigen: Zu jedem bewerteten Körper K gibt es einen kleinsten henselschen bewerteten Körper $K^h \subset K^{\mathrm{alg}}$, der K enthält. K^h ist (als bewerteter Körper) eindeutig bis auf Automorphismus über K und heißt* ***henselsche Hülle*** *von K.*

Bemerkung 1.7.9 *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 $\underline{f} := (f_1, \dots, f_\ell) \in \mathbb{Z}[X_1, \dots, X_n]^\ell$ ein Tupel von Polynomen und sei R ein Ring. Dann schreiben wir*

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

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 $f \in \mathbb{Z}[X_1, \dots, X_n]$ 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 $\underline{f} \in \mathbb{Z}[X_1, \dots, X_n]^\ell$ 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 $\underline{f} \in \mathbb{Z}[X_1, \dots, X_n]^\ell$ 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:*

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

2 Quantorenelimination in bewerteten Körpern

Im gesamten Kapitel ist K ein bewerteter Körper: Außerdem ist v die Bewertung, Γ (oder Γ_K) die Wertegruppe, $\mathcal{O}_K$ der Bewertungsring, $\mathcal{M}_K \subset \mathcal{O}_K$ das maximale Ideal und $\bar{K}$ der Restklassenkörper.

2.1 Leitterme

Sei K ein bewerteter Körper.

Bemerkung 2.1.1 *$1 + \mathcal{M}_K$ ist eine Untergruppe der multiplikativen Gruppe $K^\times$.*

Definition 2.1.2 *Wir setzen $\mathrm{RV}_K^\times := K^\times/(1 + \mathcal{M}_K)$ und $\mathrm{RV}_K := \mathrm{RV}_K^\times \cup \{0\}$ und schreiben $\mathrm{rv}\colon K \to \mathrm{RV}$ für die kanonische Abbildung $K^\times \to \mathrm{RV}_K^\times$, fortgesetzt durch $0 \mapsto 0$. Für $a \in K$ nennt man $\mathrm{rv}(a)$ den **Leitterm** von a, und RV_K ist die **Leittermstruktur**. Für die Gruppe $\mathrm{RV}_K^\times$ verwenden wir multiplikative Notation. Außerdem setzen wir $0 \cdot \xi = 0$ für $\xi \in \mathrm{RV}_K$.*

Bemerkung 2.1.3 *Für $a, b \in K$ gilt $\mathrm{rv}(a) = \mathrm{rv}(b)$ genau dann, wenn $v(a-b) > v(a)$ ist oder $a = b = 0$.*

Beispiel 2.1.4 *Im Fall $K = k((t))$ bilden die Elemente der Form $at^m \in K$ (für $a \in k$, $m \in \mathbb{Z}$) ein Repräsentantensystem von $\mathrm{RV}^\times$; es gilt $\mathrm{RV}^\times \cong k^\times \times \Gamma$ (als Gruppen).*

Bemerkung 2.1.5 *Die Bewertung $v\colon K \to \Gamma_K \cup \{\infty\}$ faktorisiert über RV_K, d. h., es existiert ein Gruppenhomomorphismus $f\colon \mathrm{RV}_K \to \Gamma_K \cup \{\infty\}$, so dass $v = f \circ \mathrm{rv}$ gilt. Außerdem induziert rv einen injektiven Gruppenhomomorphismus $\bar{K}^\times \to \mathrm{RV}_K^\times$, dessen Bild genau der Kern von $f|_{\mathrm{RV}_K^\times}$ ist.*

Notation 2.1.6 *Die Abbildung $f\colon \mathrm{RV}_K \to \Gamma_K \cup \{\infty\}$ aus Bemerkung 2.1.5 bezeichnen wir in Zukunft mit v_{RV} (oder vielleicht auch einfach mit v).*

Notation 2.1.7 *Seien $\xi_1, \ldots, \xi_n, \zeta \in \mathrm{RV}$. Wenn $a_i \in K$ existieren mit $\mathrm{rv}(a_i) = \xi_i$ und $\mathrm{rv}(a_1 + \cdots + a_n) = \zeta$, so schreiben wir $\zeta \approx \xi_1 + \cdots + \xi_n$. Wenn genau ein ζ existiert mit $\zeta \approx \xi_1 + \cdots + \xi_n$, so sagen wir, $\xi_1 + \cdots + \xi_n$ ist **wohldefiniert**, und wir schreiben $\zeta = \xi_1 + \cdots + \xi_n$. Außerdem setzen wir $-\xi_1 := \mathrm{rv}(-1) \cdot \xi_1$.*

Lemma 2.1.8 *Seien $a_1, \ldots, a_n \in K$. Dann ist $\mathrm{rv}(a_1) + \cdots + \mathrm{rv}(a_n)$ wohldefiniert genau dann, wenn $v(a_1 + \cdots + a_n) = \min\{v(a_1), \ldots, v(a_n)\}$ ist. Ist dies nicht der Fall, so gilt $\mathrm{rv}(a_1) + \cdots + \mathrm{rv}(a_n) \approx \zeta$ für alle $\zeta \in \mathrm{RV}$ mit $v(\zeta) > \min\{v(a_1), \ldots, v(a_n)\}$.*

2.2 Quantorenelimination: Die Aussagen

Definition 2.2.1 *Wir definieren* L_{RV} *als die zweisortige Sprache mit Sorten* VF *(für einen bewerteten Körper) und* RV *(für die zugehörige Leittermstruktur) und den folgenden Symbolen:*

- *die Ringsprache auf* VF
- *auf* RV *die Sprache der multiplikativen Gruppen und ein dreistelliges Relationssymbol für „*$\xi_1 + \xi_2 \approx \xi_3$*".*
- *ein Funktionssymbol* $\mathrm{rv}\colon \mathrm{VF} \to \mathrm{RV}$ *für die Abbildung* $\mathrm{rv}\colon K \to \mathrm{RV}_K$*.*

Ist K *ein bewerteter Körper, so werden wir die* L_{RV}*-Struktur* (K, RV_K) *oft auch einfach mit* K *bezeichnen.*

Bemerkung 2.2.2 *In* $L := L_{\mathrm{ring}} \cup \{V\}$*, wobei* V *ein Relationssymbol für den Bewertungsgring eines bewerteten Körpers ist. Dann sind, für bewertete Körper* K*, die* L*-definierbaren Teilmengen von* K^n *die selben wie die* L_{RV}*-definierbaren Teilmengen. Sowohl in* L^{eq} *als auch in* $L_{\mathrm{RV}}^{\mathrm{eq}}$ *existieren Sorten für* RV_K*,* $\bar{K}$ *und* $\Gamma \cup \{\infty\}$*. Außerdem sind in beiden Sprachen definierbar:* $\mathcal{O}_K \subset K$*;* $\mathcal{M}_K \subset K$*; die Ring-Sprache auf* $\bar{K}$*; die angeordnete-abelsche-Gruppen-Sprache auf* Γ_K*;* $v\colon K \to \Gamma \cup \{\infty\}$*;* $\mathrm{rv}\colon K \to \mathrm{RV}_K$*;* $v_{\mathrm{RV}}\colon \mathrm{RV}_K \to \Gamma_K \cup \{\infty\}$*;* $\mathrm{res}\colon \mathcal{O}_K \to \bar{K}$*.*

Bemerkung 2.2.3 *Es existiert eine* L_{RV}*-Theorie, deren Modelle genau die* (K, RV_K) *sind, für bewertete Körper* K*.*

Definition 2.2.4 *Seien* (p, q) *eine mögliche Charakteristik von bewerteten Körpern (vgl. Bemerkung 1.4.7). Wir schreiben* HEN *für die Theorie der henselschen bewerteten Körper,* $\mathrm{HEN}_p \supset \mathrm{HEN}$ *für die Theorie der henselschen bewerteten Körper der Charakteristik* p *(bei beliebiger Restklassenkörper-Charakteristik) und* $\mathrm{HEN}_{p,q} \supset \mathrm{HEN}_p$ *für die Theorie der henselschen bewerteten Körper der Charakteristik* (p, q)*.*

Bemerkung: Diese Theorien existieren. Es gilt: $\mathrm{HEN}_0 = \mathrm{HEN} \cup \{\mathrm{char}\, K \neq p \mid p \text{ prim}\}$ und $\mathrm{HEN}_{0,0} = \mathrm{HEN} \cup \{\mathrm{char}\, \bar{K} \neq p \mid p \text{ prim}\}$.

Definition 2.2.5 *Eine* RV***-Expansion*** *von* L_{RV} *ist eine Sprache* $L \supset L_{\mathrm{RV}}$*, so dass* $L \setminus L_{\mathrm{RV}}$ *„nur auf* RV *lebt", d. h. nur aus Konstanten in* RV*, Funktionssymbolen* $\mathrm{RV}^\ell \to \mathrm{RV}$ *und Relationssymbolen auf* RV^ℓ *besteht.*

Sei L *eine* RV*-Expansion von* L_{RV}*. Wir nennen eine* L*-Formel* VF***-quantorenfrei*** *(kurz: „*VF*-qf"), wenn sie keine Quantoren über Variablen der Sorte* VF *enthält.*

Satz 2.2.6 *Sei* $L \supset L_{\mathrm{RV}}$ *eine* RV*-Expansion und sei* $T \supset \mathrm{HEN}_{0,0}$ *eine* L*-Theorie. Dann ist jede* L*-Formel ist modulo* T *äquivalent zu einer* VF*-quantorenfreien* L*-Formel.*

Korollar 2.2.7 *Sei* $L \supset L_{\mathrm{RV}}$ *eine* RV*-Expansion und sei* $T \supset \mathrm{HEN}_0$ *eine* L*-Theorie. Dann existiert für jede* L*-Formel* $\phi(\underline{x})$ *ein* $N_0 > 0$ *und eine* VF*-quantorenfreie* L*-Formel* $\psi(\underline{x})$*, so dass gilt: Ist* $K \models T$ *ein Modell mit* $\mathrm{char}\, \bar{K} = 0$ *oder* $\mathrm{char}\, \bar{K} > N_0$*, so ist* $\phi(K) = \psi(K)$*.*

2.3 Polynome und rv

Definition 2.3.1 *Sei $f = \sum_i a_i X^i \in K[X]$ und $b \in K$. Wir sagen, f hat eine* ***Kollision*** *bei b, wenn $v(f(b)) > \min_i v(a_i b^i)$ ist.*

Bemerkung 2.3.2 *f hat keine Kollision bei b genau dann, wenn $\sum_i \mathrm{rv}(a_i)\,\mathrm{rv}(b)^i$ wohldefiniert ist. In diesem Fall ist die Summe gleich $\mathrm{rv}(f(b))$.*

Definition 2.3.3 *Sei $f \in K[X]$ ein Polynom vom Grad n. Wir nennen ein $c \in K$ eine „**Nullstelle einer Ableitung** von f“, wenn ein $0 \leq \ell \leq n$ existiert, so dass $f^{(\ell)}(c) = 0$ ist. (Hierbei bezeichnet $f^{(\ell)}$ die ℓ-te Ableitung von f.) Ist $\ell \geq 1$, so nennen wir c eine „**Nullstelle einer echten Ableitung** von f“.*

Lemma 2.3.4 *Sei $f \in K[X]$ ein Polynom vom Grad n. Dann hat die Menge der $b \in K$, an denen f eine Kollision hat, die Form*

$$\{b \in K \mid \exists c \in C\colon \ \mathrm{rv}(b) = \mathrm{rv}(c)\},$$

wobei $C \subset K$ eine Teilmenge der Nullstellen der Ableitungen von f ist.

Definition 2.3.5 *Sei $f \in K[X]$ und seien $b, c \in K$. Wir sagen, f hat eine* ***um-c-Kollision*** *bei b, wenn das um c verschobene Polynom $g(X) := f(X + c)$ eine Kollision bei $b - c$ hat.*

Bemerkung 2.3.6 *Schreiben wir $f(X + c) =: g(X) = \sum_i a_i X^i$, so hat f hat keine um-c-Kollision bei b genau dann, wenn $\mathrm{rv}(f(c)) = \sum_i \mathrm{rv}(a_i) \cdot \mathrm{rv}(b - c)^i$ gilt.*

Satz 2.3.7 *Seien $f \in K[X]$ und $b \in K$ gegeben, und sei c eine Nullstelle einer Ableitung von f, so dass $v(b - c)$ maximal ist. Dann hat f keine um-c-Kollision bei b.*

Lemma 2.3.8 *Es existiert eine VF-qf-Formel η so dass $\eta(a_0, \ldots, a_n, \mathrm{rv}(b - c), c, \zeta)$ genau dann gilt (für $a_i, b, c \in K, \zeta \in \mathrm{RV}_K$), wenn das Polynom $f = \sum a_i X^i$ keine um-c-Kollision bei b hat und außerdem $\mathrm{rv}(f(b)) = \zeta$ gilt.*

Satz 2.3.9 *Sei $f \in K[X]$ ein Polynom. Wir nehmen an, dass f mit keiner seiner strikten Ableitungen eine gemeinsame Nullstelle hat. Sei außerdem $\zeta \in \mathrm{RV}^\times$ gegeben. Dann sind äquivalent:*

(a) *Es existiert eine Nullstelle $b \in K$ von f mit $\mathrm{rv}(b) = \zeta$.*

(b) *Es existiert ein $b \in K$ mit $\mathrm{rv}(b) = \zeta$, so dass f eine um-c-Kollision bei b hat sowohl für $c = 0$ als auch für jede Nullstelle c jeder echten Ableitung von f.*

2.4 Beweis von Quantorenelimination

Lemma 2.4.1 *Seien $f_i(x, \underline{z}) \in \mathbb{Z}[x, \underline{z}]$ für $i = 1, 2$, mit $a_{i,j} \in \mathbb{Z}[\underline{z}]$, wobei $\underline{z}$ ein N-Tupel ist. Dann existieren endlich viele quantorenfreie L_{ring}-Formeln $\phi_\ell(\underline{z})$ und Polynome $g_\ell(x, \underline{z}), h_{i,\ell}(x, \underline{z}) \in \mathbb{Z}[x, \underline{u}]$ so dass für jeden Körper K gilt:*

(a) *Die Mengen $\phi_\ell(K)$ bilden eine Partition von K^N.*

(b) *Ist $\underline{c} \in \phi_\ell(K)$, so ist $g_\ell(x, \underline{c})$ der ggT von $f_1(x, \underline{c})$ und $f_2(x, \underline{c})$ (bis auf einen Faktor in $K^\times$), und es existieren $d_1, d_2 \in K^\times$ so dass $f_i(x, \underline{c}) = d_i \cdot h_{i,\ell}(x, \underline{c}) \cdot g_\ell(x, \underline{c})$ für $i = 1, 2$.*

Wir arbeiten in einer RV-Expansion $L \supset L_{\mathrm{RV}}$ wie in Satz 2.2.6 und in $\mathrm{HEN}_{0,0}$ (als L-Theorie aufgefasst). Im Folgenden ist x immer eine VF-Variable, $\underline{z}$ ein Tupel von VF-Variablen und $\underline{\zeta}$ ein Tupel von RV-Variablen.

Lemma 2.4.2 *Satz 2.2.6 folgt aus: Für jede* VF*-qf-Formel* $\phi(x, \underline{z}, \underline{\zeta})$ *ist* $\exists x \phi(x, \underline{z}, \underline{\zeta})$ *zu einer* VF*-qf-Formel äquivalent.*

Im Folgenden sind $m, n, r \in \mathbb{N}$, $a_{i,j}, b_j, c_i \in \mathbb{Z}[\underline{z}]$, $f_i = \sum_{j \le m} a_{i,j} x^j, g = \sum_{j \le n} b_j x^j \in \mathbb{Z}[x, \underline{z}]$. Außerdem ist $\phi(x, \underline{z}, \underline{\zeta})$ eine VF-qf-Formel. Für jede der folgenden Formen von Formeln $\psi(\underline{z}, \underline{\zeta})$ führen wir eine Bezeichnungen ein für die Behauptung, dass jede Formel dieser Form äquivalent zu einer VF-qf-Formel ist:

(B) $\psi(\underline{z}, \underline{\zeta}) = \exists x \colon \phi(x, \underline{z}, \underline{\zeta})$

(P) $\psi(\underline{z}, \underline{\zeta}) = \exists x \colon \bigwedge_{i \le r} \mathrm{rv}(f_i(x, \underline{z})) = \zeta_i$

(L) $\psi(\underline{z}, \underline{\zeta}) = \exists x \colon \bigwedge_{i \le r} \mathrm{rv}(x + c_i(\underline{z})) = \zeta_i$

$(\mathrm{EB})_n$ $\psi(\underline{z}, \underline{\zeta}) = b_n(\underline{z}) \neq 0 \wedge \exists x \colon \big(g(x, \underline{z}) = 0 \wedge \phi(x, \underline{z}, \underline{\zeta})\big)$

$(\mathrm{EP})_n$ $\psi(\underline{z}, \underline{\zeta}) = b_n(\underline{z}) \neq 0 \wedge \exists x \colon \Big(g(x, \underline{z}) = 0 \wedge \bigwedge_{i \le r} \mathrm{rv}(f_i(x, \underline{z})) = \zeta_i\Big)$

$(\mathrm{EL})_n$ $\psi(\underline{z}, \underline{\zeta}) = b_n(\underline{z}) \neq 0 \wedge \exists x \colon \Big(g(x, \underline{z}) = 0 \wedge \bigwedge_{i \le r} \mathrm{rv}(x + c_i(\underline{z})) = \zeta_i\Big)$

(B = beliebig, P = polynomial, L = linear, E = endlich).

Lemma 2.4.3 (a) *(B) folgt aus (P), und* $(EB)_n$ *folgt aus* $(EP)_n$.

(b) *Gilt (L) und* $(EP)_n$ *für alle* n*, so gilt (P).*

(c) *(L) ist wahr.*

(d) $(EL)_0$ *und* $(EP)_0$ *sind wahr.*

(e) *Für* $n \ge 1$*: Aus* $(EL)_n$ *und* $(EB)_{n'}$ *für alle* $n' < n$ *folgt* $(EP)_n$

(f) *Für* $n \ge 1$*: Aus (L) und* $(EB)_{n'}$ *für alle* $n' < n$ *folgt* $(EL)_n$

2.5 Der Satz von Ax-Kochen/Ershov und andere Folgerungen

Definition 2.5.1 *Eine* ***anguläre Komponente*** *auf einem bewerteten Körper* K *ist ein Gruppenhomomorphismus* $\mathrm{ac} \colon K^\times \to \bar{K}^\times$*, der auf* $\mathcal{O}_K^\times$ *mit* res *übereinstimmt. Wir setzen außerdem* $\mathrm{ac}(0) := 0$.

Bemerkung 2.5.2 *Sei* $\mathrm{ac} \colon K \to \bar{K}$ *eine anguläre Komponente. Dann erhalten wir eine induzierte Abbildung* $\mathrm{ac}_{\mathrm{RV}} \colon \mathrm{RV} \to \bar{K}$ *(d. h.* $\mathrm{ac}(a) = \mathrm{ac}_{\mathrm{RV}}(\mathrm{rv}(a))$ *für* $a \in K$*) und einen Gruppen-Isomorphismus* $\mathrm{RV}^\times \to \bar{K}^\times \times \Gamma, \xi \mapsto (\mathrm{ac}_{\mathrm{RV}}(\xi), v(\xi))$.

Satz 2.5.3 *Sei* K *ein bewerteter Körper, aufgefasst als Struktur in einer beliebigen Sprache. Dann besitzt* K *eine elementare Erweiterung* $K' \succ K$*, auf der eine anguläre Komponente existiert.*

Definition 2.5.4 *Die* ***Sprache von Denef-Pas*** L_{DP} *ist die folgende drei-sortige Sprache: eine Sorte* VF *für einen bewerteten Körper; eine Sorte* Γ_∞ *für die Wertegruppe mit* ∞*; eine Sorte* $\bar{\mathrm{VF}}$ *für den Restklassenkörper; die Ringsprache auf* VF*; die Ringsprache auf* $\bar{\mathrm{VF}}$*; die Sprache* $L_{\mathrm{oag}} = \{0, +, -, <\}$ *der angeordneten abeschen Gruppen auf* Γ*;* $v \colon \mathrm{VF} \to \Gamma_\infty$*; eine angulären Komponente* $\mathrm{ac} \colon \mathrm{VF} \to \bar{\mathrm{VF}}$*. Wir verwenden die Bezeichnungen* HEN*,* HEN_p*,* $\mathrm{HEN}_{p,q}$ *auch für die entsprechenden Theorien in* L_{DP}*, wobei dann die Aussage hinzukommt, dass* ac *eine anguläre Komponente ist.*

Satz 2.5.5 *Sei $L \supset L_{\mathrm{DP}}$ eine $\bar{\mathrm{V}}\mathrm{F}$-$\Gamma_\infty$-Expansion (d. h. durch Symbole, die nur auf $\bar{\mathrm{V}}\mathrm{F}$ und Γ_∞ leben) und sei $T \supset \mathrm{HEN}_{0,0}$ eine L-Theorie. Dann ist jede L-Formel ist modulo T äquivalent zu einer VF-quantorenfreien L-Formel.*

Korollar 2.5.6 *Sei $\underline{x}$ ein Tupel von VF-Variablen, $\underline{y}$ ein Tupel von $\bar{\mathrm{V}}\mathrm{F}$-Variablen und $\underline{\lambda}$ ein Tupel von Γ_∞-Variablen. Jede L_{DP}-Formel $\phi(\underline{x}, \underline{y}, \underline{\lambda})$ ist äquivalent zu einer endlichen boolschen Kombination von Formeln der Formen $\psi((\mathrm{ac}(f_i(\underline{x}))_i, \underline{y})$ für L_{ring}-Formen ψ und $\psi'((v(f_i(\underline{x}))_i, \underline{\lambda})$ für L_{oag}-Formeln ψ'.*

Definition 2.5.7 *Sei L eine Sprache und S eine Sorte von L. Die auf S **induzierte Sprache** ist die Sprache L' bestehend aus einem Relationssymbol für jede Formel, die eine Teilmenge von S^n definiert. Jede L-Struktur $\mathcal{M}$ liefert eine L'-Struktur mit Grundmenge $S^{\mathcal{M}}$; diese nennen wir die von L auf S **induzierte Struktur**.*

Korollar 2.5.8 *Sei $K \models \mathrm{HEN}_{0,0}$, in der Sprache L_{DP}.*
- (a) *Die auf $\bar{K}$ induzierte Struktur ist die L_{ring}-Struktur (bis auf Interdefinierbarkeit).*
- (b) *Die auf Γ_K induzierte Struktur ist die L_{oag}-Struktur (bis auf Interdefinierbarkeit).*

Korollar 2.5.9 (Satz von Ax-Kochen/Ershov, Version 1) *Sei L entweder L_{RV} oder L_{DP}. Sind K_1 und K_2 Modelle der L-Theorie $\mathrm{HEN}_{0,0}$ mit $\bar{K}_1 \equiv_{L_{\mathrm{ring}}} \bar{K}_2$ und $\Gamma_{K_1} \equiv_{L_{\mathrm{oag}}} \Gamma_{K_2}$, so ist bereits $K_1 \equiv_L K_2$.*

Korollar 2.5.10 (Satz von Ax-Kochen/Ershov, Version 2; Transferprinzip) *Sei L entweder L_{RV} oder L_{DP}, und sei ϕ eine L-Aussage. Dann existiert ein $N \in \mathbb{N}$, so dass für alle L-Strukturen $K_1, K_2 \models \mathrm{HEN}$ gilt: Ist $\bar{K}_1 \equiv_{L_{\mathrm{ring}}} \bar{K}_2$, $\Gamma_{K_1} \equiv_{L_{\mathrm{oag}}} \Gamma_{K_2}$, und ist $\mathrm{char}\,\bar{K}_1$ entweder 0 oder größer as N, so habe*

$$K_1 \models \phi \iff K_2 \models \phi.$$

Bemerkung 2.5.11 *Korollare 2.5.9 und 2.5.10 gelten auch in $\bar{\mathrm{V}}\mathrm{F}$-Expansionen von Γ_∞-Expansionen von L_{DP}, wenn man $\bar{K}_1 \equiv \bar{K}_2$ und $\Gamma_{K_1} \equiv \Gamma_{K_2}$ für die entsprechenden induzierten Strukturen fordert.*

2.6 Bessere Quantorenelimination in Spezialfällen

Definition 2.6.1 *Wir schreiben DOAG für die Theorie der nicht-trivialen divisiblen angeordneten abelschen Gruppen in der Sprache L_{oag}.*

Satz 2.6.2 *Die Theorie DOAG hat Quantorenelimination und ist vollständig.*

Satz 2.6.3 *Die Theorie $\mathrm{ACVF}_{0,0}$ der algebraisch abgeschlossenen nicht-trivial bewerteten Körper der Charakteristik $(0,0)$ hat in der Sprache L_{DP} (vollständige) Quantoren-Elimination.*

Definition 2.6.4 *Die **Sprache von Presburger** ist $L_{\mathrm{Pres}} = L_{\mathrm{oag}} \cup \{1\} \cup \{\equiv_\ell \mid \ell \geq 1\}$, wobei $\equiv_\ell$ eine binäre Relation ist, die in $\mathbb{Z}$ interpretiert wird als: $a \equiv_\ell b \iff a \equiv b \mod \ell$.*

Satz 2.6.5 *In der Sprache L_{Pres} hat $\mathbb{Z}$ Quantorenelimination.*

3 Rationalität von Poincaré-Reihen

3.1 Zerlegung in krumme Quader

Im folgenden ist K ein Modell von $\mathrm{HEN}_{0,0}$ in einer RV-Expansion L von L_{RV}. Außerdem ist $A \subset K \cup \mathrm{RV}$ immer eine Parametermenge.

Definition 3.1.1 *Seien $\lambda_1, \ldots, \lambda_n \in \Gamma_K \cup \{\infty\}$. Ein **krummer Quader** mit Radien $\lambda_1, \ldots, \lambda_n$ ist eine definierbare Teilmenge $Q \subset K^n$ der folgenden Form:*

(a) *Im Fall $n = 1$: Q ist ein offener Ball mit Radius λ_1 (falls $\lambda_1 < \infty$), oder ein Punkt (falls $\lambda_1 = \infty$).*

(b) *Im Fall $n > 1$: Die Projektion $Q' := \pi(Q) \subset K^{n-1}$ auf die ersten $n-1$ Koordinaten ist ein krummer Quader mit Radien $\lambda_1, \ldots, \lambda_{n-1}$, und für jedes $\underline{x} \in Q'$ ist die Faser $\{y \in K \mid (\underline{x}, y) \in Q\}$ ein krummer Quader mit Radius λ_n.*

Satz 3.1.2 *Sei $X \subset K^n \times \mathrm{RV}^m$ A-definierbar. Dann existiert eine A-definierbare Abbildung $f \colon K^n \to \mathrm{RV}^k$, deren nicht-leere Fasern krumme Quader sind, und so dass für $\underline{b}, \underline{b}' \in K^n$ gilt: Ist $f(\underline{b}) = f(\underline{b}')$ so sind auch die Fasern $X_{\underline{b}}$ und $X_{\underline{b}'}$ gleich. (Hierbei $X_{\underline{b}} = \{\underline{\xi} \in \mathrm{RV}^m \mid (\underline{b}, \underline{\xi}) \in X\}$.)*

Bemerkung 3.1.3 *Der Satz gilt auch uniform in den Parametern und uniform in allen Modellen von $\mathrm{HEN}_{0,0}$, d. h. die Formel, die f definiert hängt nur von der Formel, die X definiert, ab.*

Lemma 3.1.4 *Ist $C \subset K$ endlich und A-definierbar, so existiert eine A-definierbare Abbildung $f \colon K \to \mathrm{RV}^N$, so dass für $a, a' \in K$ gilt: $f(a) = f(a')$ genau dann, wenn für alle $c \in C$ gilt: $\mathrm{rv}(a - c) = \mathrm{rv}(a' - c)$.*

Bemerkung 3.1.5 *Das Lemma gilt auch uniform in den Parametern und uniform in allen Modellen von $\mathrm{HEN}_{0,0}$.*

3.2 Messen in $\mathbb{Q}_p$

Satz 3.2.1 *Auf jeder lokal kompakten topologischen Gruppe existiert ein bis auf Skalierung eindeutiges links-invariantes Borel-Maß.*

Definition 3.2.2 *Das Maß aus Satz 3.2.1 heißt **Haar-Maß**.*

Satz 3.2.3 *$\mathbb{Z}_p$ ist kompakt. Insbesondere ist $(\mathbb{Q}_p, +)$ eine lokal-kompakte topologische Gruppe.*

Definition 3.2.4 *Von nun an sei μ das Haar-Maß auf $(\mathbb{Q}_p, +)$, das so normiert ist, dass $\mu(\mathbb{Z}_p) = 1$ ist. Das Produktmaß auf $\mathbb{Q}_p^n$ bezeichnen wir auch mit μ.*

Lemma 3.2.5 *Das Haarmaß eines Balls $B_{>\lambda}(a) = B_{\geq \lambda+1}(a) \subset \mathbb{Q}_p$ ist $p^{-\lambda-1}$.*

Satz 3.2.6 *L_{DP}-definierbare Teilmengen $X \subset \mathbb{Q}_p^n$ sind Borel-messbar. Genauer: Ist $f \colon \mathbb{Q}_p^n \to \mathrm{RV}^N$ wie in Satz 3.1.2, so gilt: $\mu(X) = \sum_{\underline{\xi} \in f(X)} p^{-g(\underline{\xi})-n}$, wobei $g(\underline{\xi}) \in \mathbb{Z} \cup \{\infty\}$ die Summe der Radien $\lambda_1, \ldots, \lambda_n$ des krummen Quaders $f^{-1}(\underline{\xi})$ ist.*

3.3 Rationalität von Presburger-Poincaré-Reihen

In diesem Abschnitt arbeiten wir in der Sprache L_{Pres} (vgl. Definition 2.6.4).

Konvention 3.3.1 *Mit einer* ***linearen Abbildung*** *von* $\mathbb{Z}^n$ *nach* $\mathbb{Z}^m$ *meinen wir eine Abbildung der Form* $f(\underline{x}) = A\underline{x} + \underline{b}$*, für eine Matrix* $A \in \mathbb{Z}^{n\times m}$ *und* $\underline{b} \in \mathbb{Z}^m$*.*

Lemma 3.3.2 (Presbuger-Zellzerlegung) *Jede definierbare Teilmenge von* $\mathbb{Z}^n$ *lässt sich als disjunkte Vereinigung von endlich vielen Mengen der folgenden Formen schreiben:*

$$\{(\underline{x}, y) \in X \times \mathbb{Z} \mid f(\underline{x}) \leq ry < g(\underline{x}), y \equiv_\ell c\},$$

für $X \subset \mathbb{Z}^{n-1}$ *definierbar,* f *und* g *linear oder gleich* $\pm\infty$*,* $\ell, r \geq 1$ *und* $0 \leq c < \ell$*.*

Satz 3.3.3 (Rektilinearisierung) *Jede definierbare Teilmenge von* $\mathbb{Z}^n$ *lässt sich als disjunkte Vereinigung von endlich vielen Mengen der Form* $f_i(\mathbb{N}^k)$ *schreiben, wobei* $f_i\colon \mathbb{Z}^k \to \mathbb{Z}^n$ *eine injektive lineare Abbildung ist.*

Definition 3.3.4 *Sei* $X \subset \mathbb{N}^n$ *eine beliebige Teilmenge. Die* ***Poincaré-Reihe*** *zu* X *ist die formale Potenzreihe* $P_X(Z_1, \dots, Z_n) := \sum_{\underline{r}\in X} \underline{Z}^{\underline{r}} \in \mathbb{Z}[[Z_1, \dots, Z_n]]$*. Hierbei verwenden wir Multiindex-Notation:* $\underline{Z}^{\underline{r}} = Z_1^{r_1} \cdots Z_n^{r_n}$

Satz 3.3.5 *Ist* $X \subset \mathbb{N}^n$ *definierbar, so ist die Poincaré-Reihe* P_X *eine rationale Funktion; genauer:* $P_X = g(\underline{Z})/h(\underline{Z})$ *für Polynome* $g, h \in \mathbb{Z}[\underline{Z}]$*, wobei* h *ein Produkt von Polynomen der Form* $1 - \underline{Z}^{\underline{a}}$ *ist, für Tupel* $\underline{a} \in \mathbb{N}^n \setminus \{0\}$*.*

3.4 Rationalität von L_{DP}-Poincaré-Reihen

Definition 3.4.1 *Sei* $X \subset \mathbb{Q}_p^n \times \mathbb{N}^m$ *so, dass für jedes* $\underline{r} \in \mathbb{N}^m$ *die Faser* $X_{\underline{r}}$ *messbar ist und endliches Maß hat. Dann definieren wir die zugehörige* ***Poincaré-Reihe*** *als*

$$P_X(\underline{Z}) := \sum_{\underline{r}\in\mathbb{N}^m} \mu(X_{\underline{r}})\underline{Z}^{\underline{r}}.$$

Satz 3.4.2 *Sei* $\phi(\underline{x}, \underline{\lambda})$ *eine* L_{DP}*-Formel, wobei* $\underline{x}$ *ein* n*-Tupel von* VF*-Variablen ist und* $\underline{\lambda}$ *ein* m*-Tupel von* Γ_∞*-Variablen. Wir nehmen an, dass für jede Primzahl* p *gilt:* $\phi(\mathbb{Q}_p) \subset \mathbb{Q}_p^n \times \mathbb{N}^m$*, und für jedes Tupel* $\underline{r} \in \mathbb{N}^m$ *hat die Menge* $\phi(\mathbb{Q}_p, \underline{r})$ *endliches Maß. Dann existiert ein* $M > 0$*, ein Polynom* $h \in \mathbb{Z}[\underline{Z}, P]$ *und endlich viele Ringformeln* $\psi_{\underline{\ell}}$*,* $\psi'_{\underline{\ell}}$ *(*$\underline{\ell} \in I \subset \mathbb{N}^m$*), so dass für jede Primzahl* $p \geq M$ *gilt:*

$$P_{\phi(\mathbb{Q}_p)}(\underline{Z}) = \frac{\sum_{\underline{\ell}\in I}(\#\psi_{\underline{\ell}}(\mathbb{F}_p) - \#\psi'_{\underline{\ell}}(\mathbb{F}_p))\underline{Z}^{\underline{\ell}}}{h(\underline{Z}, p)}.$$

Lemma 3.4.3 *Ist* $P \in \mathbb{Q}[[\underline{Y}, \underline{Z}]]$ *eine rationale Funktion und ist* $\underline{a} \in \mathbb{C}^n$ *so, dass* P *absolut konvergiert, wenn man* $\underline{a}$ *für* $\underline{Y}$ *einsetzt (so dass man* $P(\underline{a}, \underline{Z}) \in \mathbb{Q}[[\underline{Z}]]$ *erhält), so ist auch* $P(\underline{a}, \underline{Z})$ *eine rationale Funktion.*

Index

RV-Expansion, 9
VF=quantorenfrei, 9
p-adische Bewertung, 4
p-adische Zahlen, 3
p-adischer Betrag, 2
VF-qf, 9

abelsche Gruppe
    angeordnete, 4
abgeschlossener Ball, 4
ACVF, 12
angeordnete abelsche Gruppe, 4
anguläre Komponente, 11
archimedisch, 2
Ax-Kochen/Ershov
    Satz von, 12

Betrag, 2
    p-adischer, 2
    archimedischer, 2
    trivialer, 2
bewerteter Körper, 4
Bewertung, 4
Bewertungs-Topologie, 4
Bewertungsring, 5
Bewertungsring von v, 5

Charakteristik, 5

DOAG, 12
Dreiecksungleichung, 2
    ultrametrische, 2

Eisensteinsches Irreduzibilitäts=Kriterium
    verallgemeinertes, 6

formale Laurent-Reihen, 3
formale Potenzreihen, 3
Fortsetzung, 5

ganze p-adische Zahlen, 3
Gauß-Bewertung, 5
gemischte Charakteristik, 5
Gruppe
    angeordnete abelsche, 4

Haar-Maß, 13
Hensels Lemma, 6
henselsche Hülle, 7

induzierte Sprache, 12
induzierte Struktur, 12
Irreduzibilitäts=Kriterium
    verallgemeinertes Eisensteinsches, 6

Kollision, 10
Kollision um, 10
krummer Quader, 13
Körper
    bewerteter, 4

Leitterm, 8
Leittermstruktur, 8
Lemma
    von Hensel, 6
    von Newton, 6
lexikographische Ordnung, 4

Newton-Polygon, 6
Newtons Lemma, 6
nicht-archimedisch, 2
Nullstelle einer Ableitung, 10
Nullstelle einer echten Ableitung, 10

offener Ball, 4

Poincaré-Reihe, 7, 14
Presburger
    Sprache, 12

Restklassenkörper, 5
Ring
    Bewertungsring, 5

satz
    Hensels Lemma, 6
    Newtons Lemma, 6
Satz von Ax-Kochen/Ershov, 12
Satz von Ostrowski, 2
Sprache von Denef-Pas, 11
Sprache von Presburger, 12

Transferprinzip, 12
trivialer Betrag, 2

ultrametrische Dreiecksungleichung, 2

um-c-Kollision, 10

Verallgemeinertes Eisensteinsches Irreduzibilitäts=Kriterium, 6

Wertegruppe, 4
wohldefiniert
Summe in RV, 8

Äquicharakteristik, 5
äquivalente Bewertungen, 4