Inhaltsverzeichnis

Warning: This document is full of typos and probably also contains some more serious mistakes! Use at your own risk!

KAPITEL 1

Ziele

1. Diophantische Gleichungen lösen durch Reduktion modulo k

• Diophantische Gleichungen lösen: Gegeben: $f \in \mathbb{Z}[x_1, \ldots, x_n]$. Gesucht: $a_1, \ldots, a_n \in \mathbb{Z}$ so dass $f(a_1, \ldots, a_n) = 0$. (Oder allgemeiner $f_1, \ldots, f_\ell \ldots$; oder noch allgemeiner: Gleichungen und Ungleichungen).

• Ist schwierig. Bsp: $x^k + y^k = z^k$ für $k \geq 3$.

• Ist nicht entscheidbar.

• Um zu zeigen, dass es eine Lösung gibt: Lösung angeben. Aber wie zeigt man, dass es keine gibt?

• Eine Möglichkeit: Reduktion modulo k:
$f(x_1, \ldots, x_n) = 0 \Rightarrow f(x_1, \ldots, x_n) \equiv 0 \pmod{k}$.
Falls $x_i \equiv x_i' \pmod{k}$, dann ist auch $f(x_1, \ldots, x_n) \equiv f(x_1', \ldots, x_n') \pmod{k}$.
Also: Prüfe, ob $f(x_1, \ldots, x_n) \equiv 0 \pmod{k}$ für alle $x_1, \ldots, x_n \in \{0, \ldots, k-1\}$; wenn das nie der Fall ist, dann hat auch $f(x_1, \ldots, x_n) = 0$ keine Lsg.

Beispiel 1.1. *Es gibt sicher keine Quadratzahlen x^2, y^2 mit $x^2 = 3y^2$. Aber wäre $x^2 = 3y^2 - 1$ möglich?*
Nein, durch Reduktion modulo 3 (oder modulo 4): $x^2 \bmod 3$ ist $0, 1$ $\Rightarrow x^2 + 1$ ist nicht durch 3 teilbar.

• Lösungen modulo k sind Lösungen im Ring $\mathbb{Z}/k\mathbb{Z}$. Formal:

Konvention 1.2. *Ringe sind immer kommutativ, mit 1.*

Notation 1.3. *R Ring; Tupel: $\underline{x} := (x_1, \ldots, x_n) \in R^n$*
$\phi\colon R \to S$ Ring-Homo $\rightsquigarrow$ $\phi(\underline{x}) := (\phi(x_1), \ldots, \phi(x_n))$

Notation 1.4. *R Ring, $f \in \mathbb{Z}[\underline{x}]$, $\underline{a} \in R^n$; dann habe $f(\underline{a}) \in R$:*
Die kanonische Abb. $\iota\colon \mathbb{Z} \to R, n \mapsto 1 + \cdots + 1$ (n Mal) induziert Abb. $\mathbb{Z}[\underline{x}] \to R[\underline{x}]$. Setze $f(\underline{a}) := \iota(f)(\underline{a})$.

Notation 1.5. *Wenn $f \in \mathbb{Z}[\underline{x}]$ und R ein Ring, dann schreibe $Z_f(R)$ für die Lösungen von f in R, also*

$$Z_f(R) = \{\underline{a} \in R^n \mid f(\underline{a}) = 0\}.$$

• $\phi\colon R \to S$ Ring-Homo, $f \in \mathbb{Z}[\underline{x}] \rightsquigarrow \phi(f(\underline{a})) = f(\phi(\underline{a}))$; insbes. $\phi\colon Z_f(R) \mapsto Z_f(S)$.

• Wir haben Ring-Homos $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/k\mathbb{Z}, a \mapsto a + k\mathbb{Z} =: a \bmod k$;
Also: Falls $Z_f(\mathbb{Z}/k\mathbb{Z}) = \emptyset$ für ein k, dann $Z_f(\mathbb{Z}) = \emptyset$.

• Wenn man zeigen will, dass f keine Lösung hat, muss man evtl. viele k durchprobieren. Gut wäre also, wenn wir beantworten könnten:

Ziel 1.6. *Gegeben: $f \in \mathbb{Z}[\underline{x}]$. Gibt es ein $k \in \mathbb{N}$ mit $Z_f(\mathbb{Z}/k\mathbb{Z}) = \emptyset$?*

2. Reduktion modulo Primpotenzen reicht

• Statt alle k reicht: k Primpotenz.

Lemma 1.7. *(Chinesischer Restsatz) Sind $k_1, \ldots, k_s$ teilerfremd, $k := k_1 \cdots k_s$, $a_i \in \mathbb{Z}$, so ist*

$$x \equiv a_1 \pmod{k_1}, \ldots, x \equiv a_s \pmod{k_s}$$

lösbar, und die Lösungsmenge hat die Form $b + k\mathbb{Z}$ für ein $b \in \mathbb{Z}$.

Lemma 1.8. *(Chinesischer Restsatz, mit Ringen formuliert) Sind $k_1, \ldots, k_s$ teilerfremd, $k := k_1 \cdots k_s$, so hat man einen Isomorphismus von Ringen*

$$\phi\colon \mathbb{Z}/k\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_s\mathbb{Z}, a \mapsto (a \bmod k_1, \ldots, a \bmod k_s)$$

Beweis. Ring-Homo ist klar; betrachte jetzt $(a_1 + k_1\mathbb{Z}, \ldots, a_s + k_s\mathbb{Z}) \in \mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_s\mathbb{Z}$ $(a_i \in \mathbb{Z})$. Nach 1.7 gibt es $b \in \mathbb{Z}$ mit $b \equiv a_i \pmod{n_i}$, also ist $b + k\mathbb{Z}$ ein Urbild; also surjektiv. Injektiv, da andere Lösungen sich um $k\mathbb{Z}$ unterscheiden. □

• Da ϕ Ring-Iso, habe Bijektion $Z_f(\mathbb{Z}/n\mathbb{Z}) \to Z_f(\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}) = Z_f(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times Z_f(\mathbb{Z}/n_s\mathbb{Z})$.

• Insbesondere: Falls $k = p_1^{r_1} \cdots p_s^{r_s}$: f hat Lösungen modulo k genau dann wenn f Lösungen hat modulo $p_i^{r_i}$ für alle i.

• Äquivalent zu 1.6 ist jetzt also:

Ziel 1.9. *Gegeben: $f \in \mathbb{Z}[\underline{x}]$. Gibt es eine Primzahl p und ein $r \in \mathbb{N}$ mit $Z_f(\mathbb{Z}/p^r\mathbb{Z}) = \emptyset$?*

3. Verbesserung: zusammenpassende Lösungen

• Fixiere p prim

• Betrachte $\ldots \twoheadrightarrow (\mathbb{Z}/p^3\mathbb{Z})^n \twoheadrightarrow (\mathbb{Z}/p^2\mathbb{Z})^n \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^n$.

• Sei $\underline{a} \in \mathbb{Z}^n$ eine Lösung von f. Dann passen die Lösungen $\underline{a}_r := \underline{a} \bmod p^r \in Z_f(\mathbb{Z}/p^r\mathbb{Z})$ alle zusammen: $\underline{a}_{r+1} \bmod p^r = \underline{a}_r$.
Anders ausgedrückt: Eine Lösung $\underline{a}_r \in \mathbb{Z}/p^r\mathbb{Z}$ kann nur dann einer Lösung $\underline{a} \in \mathbb{Z}$ entsprechen, wenn es Urbilder von $\underline{a}_r$ in jedem $Z_f(\mathbb{Z}/p^s\mathbb{Z})$ gibt, für $s > r$.

Beispiel 1.10. *Gibt es eine nicht-triviale Lösung von $3x = 0$ in $\mathbb{Z}$? Natürlich nicht, aber...*

Für jedes r gibt es nicht-triviale Lösungen in $\mathbb{Z}/3^r\mathbb{Z}$: $x = 3^{r-1}$, $x = 2 \cdot 3^{r-1}$.

Aber: Die nicht-triv. Lösungen in $\mathbb{Z}/3^r\mathbb{Z}$ haben kein Urbild in $\mathbb{Z}/3^{r+1}\mathbb{Z}$.

• Also: Definiere die Menge der „zusammenpassenden Folgen“:

Definition 1.11. *Die **ganzen p-adischen Zahlen** sind definiert durch:*

$$\mathbb{Z}_p := \{(a_r)_{r\geq 0} \mid a_r \in \mathbb{Z}/p^r\mathbb{Z}, a_{r+1} \bmod p^r = a_r\}.$$

Das ist ein Ring mit elementweiser Addition und Multiplikation.

• Also: $f((\underline{a}_r)_{r\geq 0}) = 0$ heißt: $f(\underline{a}_r) = 0$ für alle r. Anders ausgedrückt: Jede Lösung in $Z_f(\mathbb{Z}_p)$ ist eine Folge von Lösungen $\underline{a}_r \in \mathbb{Z}/p^r\mathbb{Z}$ die zusammenpasst. Ein etwas besseres Kriterium zum prüfen, ob f unlösbar in $\mathbb{Z}$ ist, ist jetzt also: Gibt es ein p, so dass $Z_f(\mathbb{Z}_p) = \emptyset$?

• 1.10 hat keine nicht-triviale Lösung in $\mathbb{Z}_3$.

• Also verbessertes Ziel:

Ziel 1.12. *Gegeben: $f \in \mathbb{Z}[\underline{x}]$. Gibt es eine Primzahl p mit $Z_f(\mathbb{Z}_p) = \emptyset$?*

• Wir werden $\mathbb{Z}_p$ genauer unter die Lupe nehmen und sehen, wie man dort solche Fragen lösen kann.

4. Anzahl der Lösungen

• Nächste Frage: Wie viele Lösungen modulo p^r gibt es? Fixiere p (prim) und setze $\tilde{N}_r := \#Z_f(\mathbb{Z}/p^r\mathbb{Z})$.

• Und: wie viele dieser Lösungen kommen von Lösungen in $\mathbb{Z}_p$? Also:

$$N_r := \#\{\underline{a} \in (\mathbb{Z}/p^r\mathbb{Z})^n \mid \text{Ex. } (\underline{b}_s)_s \in \mathbb{Z}_p^n \text{ mit } \underline{a} = \underline{b}_r\}$$

• Es gibt starke Zusammenhänge zwischen den $\tilde{N}_r$ für verschiedene r (aber festes p); genauso für $N_r \ldots$

Definition 1.13. *Sei K ein Körper. Definiere die **formalen Potenzreihen** über K durch:*

$$K[[t]] := \{\sum_{r\in\mathbb{N}} a_r t^r \mid a_r \in K\}.$$

Dies ist ist ein Ring, indem man $+$ und $\cdot$ so definiert, wie es die Notation suggeriert:

$$\sum_{r\in\mathbb{N}} a_r t^r + \sum_{r\in\mathbb{N}} b_r t^r = \sum_{r\in\mathbb{N}} (a_r + b_r) t^r$$

$$(\sum_{r\in\mathbb{N}} a_r t^r) \cdot (\sum_{r\in\mathbb{N}} b_r t^r) = \sum_{r\in\mathbb{N}} (\sum_{\substack{s,s'\geq 0 \\ s+s'=r}} a_s b_{s'}) t^r$$

• Nullteilerfrei: $a_r, b_{r'}$ jeweils erste Koeff $\neq 0$, dann ist der Koeff. $r + r'$ vom Produkt gleich $a_r b_{r'}$, also auch $\neq 0$. Also:

Definition 1.14. *Sei $K((t))$ der Quotientenkörper von $K[[t]]$.*

• ($K((t))$ werden wir später noch genauer beschreiben.)

• Da $K[t] \subset K[[t]]$ haben wir auch $K(t) \subset K((t))$.

• Achtung: $K(t) \cap K[[t]]$ is mehr als nur $K[t]$. Beispiel: $(\sum_{r\in\mathbb{N}} t^r) \cdot (1 - t) = 1$. Also ist $\sum_{r\in\mathbb{N}} t^r = \frac{1}{1-t} \in K(t) \cap K[[t]]$.

• Zurück zu unseren diophantischen Gleichungen:

Definition 1.15. *Sei $f \in \mathbb{Z}[\underline{x}]$. Zwei Varianten der **Poincaré-Reihe** von f:*

$$\tilde{P}_f(t) := \sum_{r\in\mathbb{N}} \tilde{N}_r t^r \in \mathbb{Q}[[t]]$$

und

$$P_f(t) := \sum_{r\in\mathbb{N}} N_r t^r \in \mathbb{Q}[[t]].$$

Theorem 1.16 (Denef)**.** $\tilde{P}_f(t), P_f(t) \in \mathbb{Q}(t)$.

• Das sagt viel über $\tilde{N}_r$, N_r aus. (Z.B.: $\mathbb{Q}[[t]]$ ist überabzählbar, $\mathbb{Q}(t)$ ist abzählbar.)

5. Überblick

• $\mathbb{Z}_p$ und $K[[t]]$ sind „Henselsche Bewertungsringe“. Wir werden uns solche Ringe (und deren Quotientenkörper, „Henselsche bewertete Körper“) genauer anschauen.

• Die Frage die uns interessiert, ist ja:

$$\exists(\underline{x} \in (\mathbb{Z}_p)^n)\, f(\underline{x}) = 0?$$

Dabei handelt es sich um eine „Formel erster Stufe'". Solche Formeln werden wir definieren und untersuchen. Insbesondere: Wie wird man Quantoren in Formeln los? (‘"Quantoren-Elimination'") Das wird einer der zentralen Sätze der Vorlesung.

• Dann: Beweis vom Satz von Denef.

• Das ganze für alle hinreichend großen Primzahlen p gleichzeitig.

• Am Ende auch nochmal für kleine p.

6. Literatur

Modelltheorie:

• D. Marker: Model theory: an introduction

• W. Hodges: Model theory
und
W. Hodges: A shorter model theory

Bewertete Körper:

• A. Engler, A. Prestel: Valued fields

Modelltheorie von bewerteten Körpern:

• Z. Chatzidakis: Théorie des modèles des corps valués. (Vorlesungsskript auf französisch.) `http://www.logique.jussieu.fr/~zoe/M208/cours08.pdf`

• J. Flenner: Relative decidability and definability in Henselian valued fields. (Artikel) `http://arxiv.org/abs/0910.2682`

KAPITEL 2

Bewertete Körper

1. Absolutbeträge

Definition 2.1. *K Körper. Ein **Absolutbetrag** auf K is eine Abb. $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ mit:*

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

Definition 2.2. *$|\cdot|$ heißt **nicht-archimedisch**, wenn die „ultrametrische Dreiecksungleichung" gilt:*

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

*Sonst **archimedisch**.*

Bemerkung 2.3. *Absolutbetrag induziert Metrik.*

- $|1| = 1$, $|-1| = 1$; insbes $|x| = |-x|$.
- $|\frac{1}{x}| = \frac{1}{|x|}$

Beispiel 2.4. *Trivialer Betrag: $|0| = 0$, $|x| = 1$ für $x \neq 0$.*
(Nicht-archimedisch.)

Beispiel 2.5. *Falls $K = \mathbb{R}$ (oder $K = \mathbb{Q}$): der „normale" Absolutbetrag: $|x|_0 = x$ falls $x > 0$ und $|x|_0 = -x$ falls $x < 0$.*
(Archimedisch.)

Beispiel 2.6. *Auf $\mathbb{Q}$: Sei p prim. Setze $|x|_p := p^{-r}$ falls $x = p^r \cdot \frac{m}{n}$, mit $m, n \in \mathbb{Z}$ nicht durch p teilbar. Und $|0|_p = 0$.*

Δ: $p^r \cdot \frac{m}{n} + p^{r'} \cdot \frac{m'}{n'} = \frac{p^r mn' + p^{r'} m'n}{nn'}$ ist durch $p^{\min\{r,r'\}}$ teilbar (mindestens), d. h. wir haben: $|x + y|_p \leq \max\{|x|_p, |y|_p\}$; also nicht-archimedisch.

- Statt p^r könnte man genauso gut auch a^r nehmen für irgend ein $a > 1$.
- Wir werden sehen: „Im Wesentlichen" sind das alle Absolutbeträge auf $\mathbb{Q}$.

Beispiel 2.7. *Auf $K(t)$:*

- *Sei $a \in K$. $|x|_a := e^{-r}$ falls $x = (t-a)^r \cdot \frac{f}{g}$, wobei $f, g \in K[t]$ keine Nullstelle bei a haben. ($r =$ Vielfachheit der Nst bei a.)*
- *Allgemeiner: Zu irred. Polynom $p \in K[t]$ habe $|x|_p := e^{-r}$ falls $x = p^r \cdot \frac{f}{g}$, mit $f, g \in K[t]$ nicht durch p teilbar.*
- *Und: $|\frac{f}{g}|_\infty := e^{\deg f - \deg g}$. ($\deg g - \deg f =$ „Vielfachheit der Nst bei ∞“.)*

Übung 2.8. *Zeige ultrametrische Δ-UGl für $|\cdot|_\infty$ auf $K(t)$*

• All diese Beispiele auf $K(t)$ sind trivial auf K. Das sind im wesentlichen alle.

Lemma 2.9. *$A := \{n \cdot 1 \mid n \in \mathbb{Z}\}$. ($1 \in K$)*

- *Wenn $|\cdot|$ nicht-archimedisch, dann $|A|$ durch 1 beschränkt.*
- *Wenn $|\cdot|$ archimedisch, dann $|A|$ unbeschränkt. (Insbes hat K Charakteristik 0.)*

BEWEIS. (1) Klar. (Induktion über n)

(2) Annahme: Durch C beschränkt: Dann zeige u-m-Δ.

$$|x+y|^n = |(x+y)^n| \leq \sum_\nu |\binom{n}{\nu} x^\nu y^{n-\nu}| \leq \sum_\nu C \max\{|x|,|y|\}^n = (n+1)C \max\{|x|,|y|\}^n$$

Jetzt n-te Wurzel ziehen, $n \to \infty$; liefert u-m-Δ. □

Schreibe n für $n \cdot 1 \in K$.

Proposition 2.10. *Auf $A := \mathbb{Z} \cdot 1$ habe einen der folgenden Fälle:*

(1) *$|\cdot|$ ist trivial auf A.*
(2) *$|n| = |n|_p^\lambda$ für eine Primzahl p und $\lambda \in (0, \infty)$.*
(3) *Ex. $\lambda \in (0, 1]$ mit $|n \cdot 1| = |n|_0^\lambda$.*

In den Fällen (1), (2) ist $|\cdot|$ nicht-archimedisch (auf ganz K), sonst archimedisch.

BEWEIS. • $|n| \leq n \cdot |1| = n$.

• $a, b \in \mathbb{N}_{\geq 2}$, $n \in \mathbb{N}$.
Schreibe b^n in Basis a: $b^n = \sum_{i \leq m} c_i a^i$, wobei $m \leq n \log_a b$. Es folgt:

$$|b^n| \leq \sum_{i \leq m} |c_i a^i| \leq \sum_{i \leq m} a \max\{|a|^m, 1\} = (m+1)a \max\{|a|^m, 1\} \leq (n \log_a b + 1)a \max\{|a|^{n \log_a b}, 1\}$$

Also:

$$|b| \leq \sqrt[n]{(n \log_a b + 1)a}\, \sqrt[n]{\max\{|a|^{n \log_a b}, 1\}}$$

$n \to \infty$ liefert:

$$(\star) \qquad |b| \leq \max\{|a|^{\log_a b}, 1\}$$

Erster Fall: Für alle $a \geq 2$ habe $|a| > 1$ (insbes: archimedisch). Aus $(\star)$ folgt $|b| \leq |a|^{\log_a b}$ und $|a| \leq |b|^{\log_b a}$, also Gleichheit, also $|a| = a^\lambda$ für ein $\lambda \in \mathbb{R}_{>0}$. Wegen $|a| \leq a$: $\lambda \leq 1$.

Zweiter Fall: Es gibt $a \in \mathbb{N}$, $a \geq 2$ mit $|a| \leq 1$.
Aus $(\star)$ folgt $|b| \leq 1$ für alle $b \in \mathbb{N}$.

Wenn $|\cdot|$ nicht trivial auf $\mathbb{Z} \cdot 1$ ist, gibt es $a \geq 2$ mit $|a| < 1$. Schreibe $a = \prod_i p_i^{r_i}$. Es folgt: Ex. p prim mit $|p| < 1$.

Annahme, $|p| < 1, |q| < 1$. Wähle $e \in \mathbb{N}$ mit $|p^e|, |q^e| < \frac{1}{2}$.
Schreibe $mp^e + nq^e = 1$. Aber: $|mp^e + nq^e| \leq |m| \cdot |p^e| + |n| \cdot |q^e| < 1$.
Widerspruch.

Mit Primfaktorzerlegung folgt jetzt: $|\cdot|$ ist was es sein soll auf $\mathbb{Z}$. □

Korollar 2.11. *(Satz von Ostrowski) Die einzigen Absolutbeträge auf $\mathbb{Q}$ sind der triviale, $|\cdot|_0^\lambda$ für $\lambda \in (0,1)$, und $|\cdot|_p^\lambda$ für $\lambda \in (0,\infty)$, p prim.*

Übung 2.12. *Zeige: Falls K alg. abg. ist, sind $|\cdot|_a^\lambda$ ($a \in K$, $\lambda \in \mathbb{R}_{>0}$) und $|\cdot|_\infty^\lambda$ ($\lambda \in \mathbb{R}_{>0}$) die einzigen Abs-Beträge auf $K(t)$, die trivial auf K sind. (Ähnlich wie Beweis von 2.10.)*

2. Vervollständigung

Absolutbetrag definiert Metrik und damit Topologie.

Lemma 2.13. *Plus, mal, $a \mapsto -a$, $a \mapsto \frac{1}{a}$ sind stetig.*

BEWEIS. Seien $|a - a'| < \delta, |b - b'| < \delta$.

$|a + b - (a' + b')| \leq |a - a'| + |b - b'| < 2\delta$.

$|ab - a'b'| = |(a - a')b + a(b - b') - (a - a')(b - b')| < \delta|b| + |a|\delta + \delta^2$.

$a \mapsto -a$: klar

$a \mapsto \frac{1}{a}$: Übung. □

• Bezüglich der Metrik kann man vervollständigen:

Ganz allgemein: (M, d) metrischer Raum $\rightsquigarrow$ Habe Pseudo-Metrik auf der Menge $\mathcal{C}(M)$ der Cauchy-Folgen in M, mit $d((a_i)_i, (a_i')_i) := \lim_{i\to\infty}(a_i - a_i')$. („Pseudo"-Metrik heißt: d kann 0 sein.)

• Identifiziere Punkte mit Abstand 0 $\rightsquigarrow$ Erhalte Vervollständigung $\hat{M}$ von M. ($\hat{M}$ ist definiert durch: Habe $M \hookrightarrow \hat{M}$, $\hat{M}$ ist vollständig, und M ist dicht in $\hat{M}$)

• Stetige Abbildungen $f\colon M \to M'$ setzen sich eindeutig stetig fort zu $\hat{M} \to \hat{M}'$. ($f((a_i)_i) = (f(a_i))_i$)

• Insbesondere: $K, |\cdot|$ Körper mit Absolutbetrag $\rightsquigarrow$ $\hat{K}$ ist auch Körper mit Absolutbetrag.

Beispiel 2.14. *Vervollständigung von $\mathbb{Q}$ bzgl. $|\cdot|_0$ ist $\mathbb{R}$.*

Beispiel 2.15. *Vervollständigung von K bzgl. trivialer Bewertung ist K selbst.*

Beispiel 2.16. *Vervollständigung von $\mathbb{Q}$ bzgl. $|\cdot|_p$ heißt $\mathbb{Q}_p$: die **p-adischen Zahlen**.*

• Was eine Cauchy-Folge ist, hängt nur von der Topologie ab; also auch $\hat{K}$.

• $|\cdot|$ und $|\cdot|^\lambda$ ($\lambda \in \mathbb{R}_{>0}$) induzieren die gleiche Topologie.

• Also:

Proposition 2.17. *Die Vervollständigungen von $\mathbb{Q}$ sind $\mathbb{Q}$ (bei trivialem Absolutbetrag), $\mathbb{R}$ und $\mathbb{Q}_p$ für alle p prim.*

3. Absolutbeträge aus maximalen Idealen

Definition 2.18. *Sei R Ring, $I \subset R$ Ideal. Die **Vervollst von R bzgl. I** ist $\hat{R}_I := \varprojlim_r R/I^r$.*

• Habe kanonische Abb. $R \to \hat{R}_I$; falls $\bigcup_r I^r = \emptyset$, dann ist die Abb. injektiv.

Proposition 2.19. *R Hauptidealring, $\mathfrak{m} = (p)$ maximales Ideal.*

1. *Habe auf $K := \operatorname{quot} R$ Absolutbetrag $|x| := |x|_\mathfrak{m} := e^{-r}$ falls $x = p^r \frac{a}{b}$, $a, b \in R \setminus \mathfrak{m}$.*
2. *Die Vervollst. von R bzgl. $|\cdot|$ ist gleich $\hat{R}_\mathfrak{m}$.*
3. *Schreibe $\hat{K}_\mathfrak{m}$ für Vervollst von K bzgl. $|\cdot|$.*
   Wir haben $\hat{R}_\mathfrak{m} = \{x \in \hat{K}_\mathfrak{m} \mid |x| \leq 1\}$.

Insbes. $\hat{R}_{\mathfrak{m}}^{\times} = \{x \in \hat{K}_{\mathfrak{m}} \mid |x| = 1\}$, $\hat{K}_{\mathfrak{m}} = \operatorname{quot} \hat{R}_{\mathfrak{m}}$, *und jedes Elem von* $\hat{K}_{\mathfrak{m}}$ *hat die Form* $p^r a$ *mit* $r \in \mathbb{Z}$ *und* $a \in \hat{R}_{\mathfrak{m}}^{\times}$.

Bemerkung 2.20. *Das ginge auch allgemeiner für R Dedekind-Ring.*

BEWEIS. (1) Wie 2.6 und 2.7.

(2) Schreibe $\hat{R}'$ für Vervollst von R bzgl. $|\cdot|_{\mathfrak{m}}$.

• Sei $a = (a_i + \mathfrak{m}^i)_i \in \hat{R}_{\mathfrak{m}}$, $a_i \in R$. Wir definieren Abb. nach $\hat{R}'$ durch $a \mapsto \lim_{i\to\infty} a_i$.

• $(a_i)_i$ ist Cauchy-Folge, da für $i \le j$: $a_i - a_j \in \mathfrak{m}^i$, also $|a_i - a_j| \le e^{-i}$.

• Bild hängt nicht von Repräsentanten a_i ab: Differenz von Repräsentanten ist 0-Folge.

• Injektiv: Annahme $(a_i)_i$ Nullfolge. Fixiere r. Ex. $i \ge r$ mit $|a_i| \le e^{-r}$; also $a_i \in \mathfrak{m}^r$; also $a_r \in \mathfrak{m}^r$. Es folgt $a = 0$.

• Surjektiv: Sei Cauchy-Folge $(b_i)_i$ gegeben. Durch ausdünnen oBdA $|b_i - b_{i+1}| \le e^{-i}$, also erhalte $b = (b_i + \mathfrak{m}^i)_i \in \hat{R}_{\mathfrak{m}}$.

(3) Leichte Richtung: Für $x \in R$ habe $|x| \le 1$. Daraus folgt: $x \in \hat{R}_{\mathfrak{m}} \Rightarrow |x| \le 1$.

Betrachte jetzt $a = \lim_i a_i \in \hat{K}_{\mathfrak{m}}$ (mit $a_i \in K$). Annahme: $|a| \le 1$. Z.Z: $a \in \hat{R}_{\mathfrak{m}}$.

• (Achtung: Falls $a_i = \frac{b_i}{c_i}$ sind (b_i), (c_i) i.A. keine Cauchy-Folgen.)

• Für alle $i \gg 0$ habe $|a_i| \le 1$ (sonst $|a_i| \ge e$, also $|a| \ge e$). Also oBdA $|a_i| \le 1$ für alle i.

• Wir zeigen: $a_i \in \hat{R}_{\mathfrak{m}}$. Da $\hat{R}_{\mathfrak{m}}$ abgeschlossen, folgt dann $a \in \hat{R}_{\mathfrak{m}}$.

• Schreibe $a_i = p^{r_i} \frac{b_i}{c_i}$, $b_i, c_i \in R \setminus \mathfrak{m}$, $r_i \ge 0$. Wir müssen also nur zeigen: $c \in R \setminus \mathfrak{m} \Rightarrow c$ ist invertierbar in $\hat{R}_{\mathfrak{m}}$.

• Dazu suchen wir eine Folge $d_i \in R$ mit $\lim c \cdot d_i = 1$.

• Sei $\bar{c}$ Bild von c in $R/\mathfrak{m}$ und d_1 ein Urbild vom Inversen von $\bar{c}$. Es folgt: $d_1 \cdot c - 1 \in \mathfrak{m}$, also $|d_1 \cdot c - 1| \le e^{-1}$.

• Jetzt induktiv: Sei d_i gegeben. Definiere $d_{i+1} := d_i \cdot (2 - d_i \cdot c)$.

• $|1 - cd_{i+1}| = |1 - 2cd_i + (cd_i)^2| = |1 - cd_i|^2 \ldots \to 0$.

Jetzt habe: $x \in \hat{K}_\mathfrak{m} \Rightarrow x \in \hat{R}_\mathfrak{m}$ oder $\frac{1}{x} \in \hat{R}_\mathfrak{m}$, also insbes. $\hat{K}_\mathfrak{m} = \text{quot}\, \hat{R}_\mathfrak{m}$. □

Beispiel 2.21. *Die Vervollständigung von $\mathbb{Z}$ bzgl. der p-adischen Norm ist gleich dem $\mathbb{Z}_p$ aus der ersten Vorlesung. ($\mathfrak{m} = p\mathbb{Z}$).*

Ein Element von $\mathbb{Z}/p^r\mathbb{Z}$ ist eine r-stellige Zahl in Basis p. Damit erhalte: Elemente von $\mathbb{Z}_p$ sind "Zahlen in Basis p mit unendlich vielen Stellen vor dem Komma". Elemente von $\mathbb{Q}_p \setminus \mathbb{Z}_p$ haben die Form $p^{-r}a$, $r < 0$, also "endlich viele Nachkommastellen". Mit den üblichen Rechnenregeln, aber Division muss man von rechts anfangen.

Bsp ($p = 5$): $-1_5 = \ldots 444444_5$ $\quad \frac{1}{10_5} = 0,1_5$ $\quad \frac{1}{2} = \ldots 22223_5$
$\frac{12_5}{3} = \ldots 13134_5$

$|x|_p = p^{-r}$ falls x mit r Nullen endet. Bsp: $|\ldots 340100|_5 = 5^{-2}$.

Beispiel 2.22. *Mit $R = K[t]$, $\mathfrak{m} = tK[t]$ erhält man $\hat{R}_\mathfrak{m} = K[[t]]$. Also: $K[[t]]$ = Vervollst. von $K[t]$ bzgl. $|\cdot|_0$.*
$K((t)) := \text{quot}\, K[[t]] = \{\sum_{i=-N}^{\infty} a_i t^i\}$.

4. Bewertete Körper

Notation 2.23. *Für $n = p^r \frac{m}{n} \in \mathbb{Q}$, $p \nmid m, n$, setze $v_p(n) := r$ (und $v_p(0) := \infty$.)*

Erinnerung: Auf $\mathbb{Q}$: $|x|_p = p^{-v_p(x)}$.

Notation 2.24. *Falls $f \in K(t)$ eine r-fache NSt bei $a \in K$ hat, setze $v_a(f) := r$ (Pole zählen als negative Nullstellen; $v_a(0) := \infty$).*

Erinnerung: Auf $K(t)$: $|f|_a = e^{-v_a(f)}$.

Manchmal ist es praktischer, mit v_p zu arbeiten statt mit $|\cdot|_p \ldots$

Definition 2.25. *Eine **angeordnete abelsche Gruppe** ist eine abelsche Gruppe Γ mit Ordnungsrelation, so dass gilt: $a < a' \Rightarrow a + b < a' + b$.*

Bemerkung 2.26. *$a < b$ ist festgelegt durch $\Gamma_{\geq 0} = \{a \in \Gamma \mid a \geq 0\}$.*
Eine Menge A tut's als $\Gamma_{\geq 0}$ tut's wenn:
$a \notin A \Rightarrow -a \in A$; $a, -a \in A \Rightarrow a = 0$. $a, b \in A \Rightarrow a + b \in A$

Beispiel 2.27. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}_{>0}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}_{>0}, \cdot)$.
Lexikographische Produkte: $\Gamma \times \Gamma'$ mit $(a, b) \geq 0 \iff a \geq 0$ oder ($a = 0$ und $b \geq 0$).
Nicht-Beispiel: $(\mathbb{Q}^\times, \cdot)$*: $1 < 2$ aber $1 \cdot (-1) \not< 2 \cdot (-1)$.*

Lemma 2.28. *Angeordnete abelsche Gruppen sind torsionsfrei.*

BEWEIS. Annahme: $a+\cdots+a=0$. Falls $a>0$ folgt $a+\cdots+a>0$; Widerspruch. Entprechend mit $a<0$. □

Definition 2.29. *K Körper. Eine **Bewertung** auf K ist eine Abbildung $v\colon K \twoheadrightarrow \Gamma \cup \{\infty\}$, mit Γ angeordnete abelsche Gruppe, so dass gilt:*

- $v(x)=\infty \iff x=0$
- $v(xy)=v(x)+v(y)$ *($v\colon K^\times \to \Gamma$ ist Gruppenhomo)*
- $v(x+y)\geq \min\{v(x),v(y)\}$.

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

*Zwei Bewertungen $v\colon K\to\Gamma$, $v'\colon K\to\Gamma'$ heißen **äquivalent** $:\iff$ ex. ordungserhaltenden Gruppeniso $\phi\colon\Gamma\to\Gamma'$ mit $v'=\phi\circ v$.*

Beispiel 2.30. *Die $v_p\colon \mathbb{Q}\to\mathbb{Z}\cup\{\infty\}$, $v_a\colon K(t)\to\mathbb{Z}\cup\{\infty\}$ von oben.*

Lemma 2.31. *Jeder Körper K mit nicht-arch. Absolutbetrag $|\cdot|$ ist bewerteter Körper mit $\Gamma := \operatorname{im}|\cdot|$, wobei man die umgekehrte Ordnung nimmt. (Und umgekehrt: Wenn sich Γ in $(\mathbb{R}_{>0},\cdot)$ einbetten lässt, induziert die Bewertung einen nicht-arch. Absolutbetrag.)*

BEWEIS. Klar. □

Beispiel 2.32. *Trivialer Absolutbetrag liefert triviale Bewertung $K\to\{0,\infty\}$, $0\mapsto\infty$, rest $\mapsto 0$.*

Lemma 2.33. (1) $v(1)=0$, $v(-x)=v(x)$.
(2) $x,y\in K$, $v(x)\neq v(y)\Rightarrow v(x+y)=\min\{v(x),v(y)\}$.

BEWEIS. (1) klar.
(2) Annahme: $v(x+y)>v(y)<v(x)$. Dann $v(y)=v((x+y)+(-x))<\min\{v(x+y),v(x)\}$. Widerspruch. □

[Anschauung: Dreieck.]

5. Bewertungsringe

Definition 2.34. *Ein **Bewertungsring** ist ein Integritätsbereich $\mathcal{O}$, so dass für alle $a\in\operatorname{quot}\mathcal{O}$ gilt: $a\in\mathcal{O}$ oder $a^{-1}\in\mathcal{O}$.*

Lemma 2.35. *Sei K bewerteter Körper.*

- $\mathcal{O}:=\{a\in K\mid v(a)\geq 0\}$ *ist Bewertungsring mit Quot-Körper K.*

- $\mathcal{O}^\times = \{a \in K \mid v(a) = 0\}$. *(Also:* $\mathcal{O}^\times = \ker v$*.)*
- $\mathcal{M} = \{a \in K \mid v(a) > 0\}$ *ist (einziges) maximales Ideal in* $\mathcal{O}$*.* *(*$\bar{K} := \mathcal{O}/\mathcal{M}$ *heißt* ***Restklassenkörper****.)*

Bemerkung 2.36. *In Abs-Betrag-Sprache wäre* $\mathcal{O} = \{a \in K \mid |a| \leq 1\}$*, also „Einheitsball".*

BEWEIS. • $\mathcal{O}$ abg. unter + nach Δ-Ugl.; abg. unter $\cdot$ auch ok.

• Für alle $a \in K$ gilt $a \in \mathcal{O}$ oder $\frac{1}{a} \in \mathcal{O}$, also $K = \operatorname{quot} \mathcal{O}$ und $\mathcal{O}$ Bewertungsring.

• $a \in \mathcal{O}^\times \iff a \in \mathcal{O} \wedge \frac{1}{a} \in \mathcal{O} \iff v(a) \geq 0 \wedge v(\frac{1}{a}) = -v(a) \geq 0$.

• $\mathcal{M}$ ist Ideal; Maximalität und Eindeutigkeit ist dann klar. □

Beispiel 2.37.
- *Bew-Ring von trivialer Bewertung ist* K *selbst. Das maximale Ideal ist* (0)*, der Restkl-Kp ist* K*.*
- *Bewring von* $\mathbb{Q}, v_p$ *ist* $\mathbb{Z}_{(p)} := \{\frac{m}{n} \mid m, n \in \mathbb{Z}, p \nmid n\}$. $\mathcal{M} = p\mathbb{Z}_{(p)}$*; Restkl-Kp ist* $\mathbb{F}_p$*.*
- *Bewring von* $\mathbb{Q}_p$ *ist* $\mathbb{Z}_p$*.* $\mathcal{M} := p\mathbb{Z}_p$*; Restkl-Kp ist* $\mathbb{F}_p$*.*
- *Bewring von* $K((t))$ *ist* $K[[t]]$*,* $\mathcal{M} = tK[[t]]$*, Restkl-Kp ist* K*.*

Übung 2.38. *Bew-Ring von* $K(t)$ *mit Bewertung* $|\cdot|_\infty$*.*

Wir haben sogar:

Proposition 2.39. *Sei* K *bewerteter Körper. 2.35 induziert Bijektion*

$$\{\textit{Bewertungen auf } K\}/\textit{Äquivalenz} \quad \leftrightarrow \quad \{\textit{Bewertetungsringe mit Quot-Kp. } K\}$$

BEWEIS. Aus $\mathcal{O}$ definiere $v' \colon K^\times \to \Gamma' := K^\times/\mathcal{O}^\times$ wobei Ordnung auf Γ' definiert durch: $v(a) \geq 0 \iff a \in \mathcal{O}$.

• $v'(xy) = v'(x) + v'(y)$: klar.

• ≥ 0-Menge wohldef: $v'(a) = v'(a'), a \in \mathcal{O} \Rightarrow a' \in \mathcal{O}$: ok.

• ≥ 0-Menge definiert Ordnung: Für alle a gilt: $v'(a) \geq 0$ oder $-v'(a) = v'(\frac{1}{a}) \geq 0$; Wenn $a \in \mathcal{O}$ und $\frac{1}{a} \in \mathcal{O}$, dann $a \in \mathcal{O}^\times$, also $v'(a) = 0$; $v'(a) \geq 0, v'(b) \geq 0 \Rightarrow v'(a) + v'(b) \geq 0$ da $a + b \in \mathcal{O}$.

• Δ-Ugl: OBdA $v'(x) \leq v'(y)$, also $\frac{y}{x} \in \mathcal{O}$, und z.z: $v'(x + y) \geq v'(x)$. $v'(x + y) = v'(x) + v'(1 + \frac{y}{x})$. $1 + \frac{y}{x} \in \mathcal{O}$, also v' davon ≥ 0.

$\mathcal{O} \rightsquigarrow v' \rightsquigarrow \mathcal{O}'$: $\mathcal{O} = \mathcal{O}'$ ist klar.

$v \rightsquigarrow \mathcal{O} \rightsquigarrow v'$:

• v, v' haben den gleichen Kern, also habe Iso $\Gamma \to \Gamma'$, der mit v, v' kompatibel ist.

• $v(a) \geq 0 \iff v'(a) \geq 0 \Rightarrow$ Ordnungen passen. □

[Diagramm mit: Was entspricht was]

[Diagramm mit Körpern, Ringen, Idealen, Vervollständigungen]

6. Topologie auf bewerteten Körpern

Definition 2.40.
- ***Offener Ball***: $\{x \in K \mid v(x-a) > \gamma\} =: B(a, > \gamma)$;
- ***abgeschlossener Ball***: $\{x \in K \mid v(x-a) \geq \gamma\} =: B(a, \geq \gamma)$.
- *Die **Bewertungs-Topologie** auf K sei die Topologie mit den offenen Bällen als Präbasis.*

• Wenn Γ diskret (d.h. ex. minimales positives Element $1 \in \Gamma$), dann sind offene und abgeschlossene Bälle das gleiche: $B(a, > \gamma) = B(a, \geq \gamma + 1)$.

Lemma 2.41.
(1) *Sei B ein Ball (offen oder abg.). Dann ist jedes $a \in B$ ein Mittelpunkt von B, d.h. $B = B(a, {}_{(}\geq_{)}\, \gamma)$*
(2) *Für je zwei Bälle B_1, B_2 gilt: $B_1 \subset B_2$ oder $B_2 \subset B_1$ oder $B_1 \cap B_2 = \emptyset$.*
Insbes.: Schnitt von offenen Bällen ist wieder offener Ball; also bilden die offenen Bälle nicht nur eine Präbasis sondern sogar eine Basis der Topologie.
(3) *Alle Bälle sind topologisch abgeschlossen (auch die offenen). Insbesondere: K ist völlig unzusammenhängend.*

BEWEIS. (1) Sei $B = B(b, {}_{(}\geq_{)}\, \gamma)$ und $a \in B$, also $v(a-b) \; {}_{(}\geq_{)}\, \gamma$. Dann: $v(x-a) \; {}_{(}\geq_{)}\, \gamma \Rightarrow v(x-b) = v(x-a) + v(a-b) \; {}_{(}\geq_{)}\, \gamma$
... und umgekehrt.

(2) Falls $a \in B_1 \cap B_2$ schreibe $B_i = B(a, {}_{(}\geq_{)}\, \gamma_i) \ldots$

(3) Das Komplement von $B := B(a, {}_{(}\geq_{)}\, \gamma)$ ist die Vereinigung der $B(b, > \gamma)$, über alle $b \notin B$. □

[Bild von $\mathbb{Z}_3$]

Lemma 2.42. *$\mathbb{Z}_p$ ist kompakt.*

BEWEIS. (Skizze)

• Annahme: $(X_i)_{i\in I}$ Überdeckung ohne endliche Teilüberdeckung. OBdA $X_i = B(x_i, > \gamma_i)$.

• Wenn jeder Ball $B(a, \geq 1)$ ($a \in \{0, \ldots, p-1\}$ eine endl. Teilüberdeckung hätte, dann auch ganz $\mathbb{Z}_p$. Wähle Ball B_1 ohne endl. Teilüberdeckung.

• Wiederhole für Subbälle davon; finde B_2. Etc. Nenne den Limes-Punkt a_0.

• Sei i gegeben. Für n groß genug ist B_n kleiner als X_i, also entweder ganz drin oder ganz draußen. Nur ganz draußen ist möglich. Insbes $a_0 \notin X_i$.

• Widerspruch. □

7. Henselsche Körper

Proposition 2.43. *(**Hensels Lemma**) Sei K ein vollständiger bewerteter Körper mit $\Gamma = \mathbb{Z}$. (vollst. bzgl. der zugehörigen Metrik.)*

(∗) *Sei $f \in \mathcal{O}[x]$, $a \in \mathcal{O}$, $v(f(a)) > 0$, $v(f'(a)) = 0$. Dann ex. $a_0 \in \mathcal{O}$ mit $f(a_0) = 0$ und $v(a_0 - a) > 0$.*

Beweis. "Newton-Approximation"

[Bild]

• Setze $a' := a - \frac{f(a)}{f'(a)}$. Offenbar ist $v(a' - a) = v(f(a))$.

• Zeige noch zwei Dinge: (i) $v(f(a')) > v(f(a))$; (ii) $v(f'(a')) = 0$. Danach können wir das gleiche mit a' machen und erhalten a'', etc.; Limes a_0 existiert (nach Vollständigkeit) und erfüllt $v(a_0 - a) > 0$, und Stetigkeit von f impliziert: $f(a_0) = 0$.

• OBdA $a = 0$.

• Schreibe $f(x) = \sum_i b_i x^i$; also $b_0 = f(0), b_1 = f'(0)$.

• $f(a') = \sum_i b_i (a')^i = \sum_i b_i \cdot (-\frac{b_0}{b_1})^i = b_0 - b_0 + (\frac{b_0}{b_1})^2 \cdot \text{rest}$.

• Also $v(f(a')) \geq 2v(f(0)) \Rightarrow$ (i)

• $f'(a') = \sum_i c_i (a')^i$ mit $c_0 = f'(0)$. Aus $v(a') > 0$ folgt $v(f'(a') - f'(0)) > 0$, also insbes. $v(f'(a')) > 0$. □

Bemerkung 2.44. *Man könnte (*) auch schreiben als:* $\mathrm{res}(f(a)) = 0$, $\mathrm{res}(f'(a)) \neq 0$.

Beispiel 2.45. $\sqrt{2} \in \mathbb{Z}_7$*?*

Hat $f(x) = x^2 - 2$ *eine Nst in* $\mathbb{F}_7$*? Ja, z.B.* 3.
$f'(3) = 2 \cdot 3 \not\equiv 0 \mod 7$. *Also ex. nach Hensels Lemma eine Nst. mit* 3 *als letzter Ziffer.*

Übung 2.46.
(1) *Rechne ein paar weitere Ziffern von* $\sqrt{2} \in \mathbb{Z}_7$ *aus.*
(2) *Bestimme* $\{x \in \mathbb{Q}_7 \mid x \text{ hat Wurzel in } \mathbb{Q}_7\}$.
Hinweis: Ist $y^2 = x$*, so gilt* $\mathrm{res}(y^2) = \mathrm{res}(x)$ *und* $v(x) = 2v(y)$.

Definition 2.47. *K heißt* ***henselsch****, falls* $(*)$ *(aus 2.43) gilt.*

Lemma 2.48. *Algebraisch abgeschlossene Körper sind henselsch.*

Um das zu zeigen, zeigen wir erst mal:

Lemma 2.49. *K bewertet* $\Rightarrow$ *habe Bewertung auf* $K(x)$*, die gegeben ist durch:* $v(\sum a_i x^i) = \min_i v(a_i)$ *(und* $v(f(x)/g(x)) = v(f(x)) - v(g(x))$*). Diese Bewertung heißt* ***Gauß-Bewertung****.*

BEWEIS. • Es reicht, (1) $v(fg) = v(f) + v(g)$ und (2) die Δ-Ugl nachzurechnen für $f, g \in K[x]$. (Sonst: multipliziere die Nenner erst weg.) Aus (1) folgt dann auch, dass es bei der Definition von $v(f(x)/g(x))$ nicht auf die Wahl von f, g ankommt.

• Δ-Ugl ist klar.

(1): Z.z: $v(fg) = v(f) + v(g)$, für $f = \sum a_i x^i$, $g = \sum b_j x^j$.

• Monome vom Produkt sind Summen von irgendwelchen $a_i b_j$, also (mit Δ-Ugl) $v(fg) \geq \min_{i,j}(v(a_i) + v(b_j)) = v(f) + v(g)$. Bleibt Gleichheit zu zeigen.

• Seien m, n minimal mit $v(f) = v(a_m)$, $v(g) = v(b_n)$. Dann habe im Produkt das Monom $sx^{m+n} = \sum_{i=0}^{m+n} a_i b_{m+n-i} x^{m+n}$. In dieser Summe hat der Summand $a_m b_n$ kleinere Bewertung als alle anderen (nämlich $v(f) + v(g)$), also ist $v(s) = v(f) + v(g)$, also $v(fg) = v(f) + v(g)$. □

BEW. VON 2.48. • Behauptung: Es reicht, $(*)$ für irreduzible f zu zeigen. (Lineare Poly. sind einfach.)

• Sei also $f \in \mathcal{O}[x]$, $v(f(a)) > 0$, $v(f'(a)) = 0$, und sei $f = g \cdot h$.

• A priori sind $g, h \in K[x]$. Aber: Betrachte Gauß-Bewertung auf $K[x]$. Ein Polynom f liegt in $\mathcal{O}[x]$ gdw. $v(f) \geq 0$.
OBdA $v(g) = 0$; sonst teile g durch Koeffizient mit minimaler Bewertung. Danach: $v(f) \geq 0, v(g) = 0, v(f) = v(g) + v(h) \Rightarrow v(h) \geq 0$. Also: $g, h \in \mathcal{O}[x]$.

Jetzt zurück zu Hensel:

• $v(f(a)) > 0 \Rightarrow$ oBdA $v(g(a)) > 0$.

• Dann etwas rechnen $\Rightarrow v(g'(a)) = 0$.

• $(*)$ auf g anwenden liefert gesuchte NSt von f. □

Proposition 2.50. *Zu jedem bewerteten Körper K gibt es einen kleinsten henselschen bewerteten Körper K^h, der K enthält. K^h heißt* ***henselsche Hülle****.*
K^h liegt im alg. Abschluss von K und ist eindeutig (bis auf Isomorphismus über K).

Bew-Idee. (Details siehe [EP] := Engler, Prestel: Valued fields.)

Existenz:

• Zeige, dass man Bewertungen auf beliebige (algebraische) Körpererweiterungen fortsetzen kann [EP, 3.1.2], insbes. auf alg. Abschluss.

• Wähle Fortsetzung auf alg. Abschluss und nimm Schnitt über alle henselschen Zwischenkörper.

Eindeutigkeit:

• Auf normalen Körpererweiterungen ist die Fortsetzung der Bewertung eindeutig bis auf Automorphismus [EP, 3.2.15]. (Achtung: Automorphismen wichtig.)

• Insbes ist die Bewertung auf dem alg. Abschluss eindeutig. □

Beispiel 2.51. *Ist K Körper mit Absolutbetrag und $\hat{K}$ die Vervollständigung, so ist $\hat{K}$ i.A. größer als K^h; aber $K^h = \hat{K} \cap$ alg. Abschluss von K.*

KAPITEL 3

Basics of model theory

The basic objects of study of model theory are (first order) definable sets. Definable sets should be thought of as a generalization of solution systems of equations. The corresponding generalizations of systems of equations are called "formulas".

Systems of equations make sense in different contexts, e.g. fields, rings, vector spaces, groups; all these will be called "structures". The type of equations which make sense depend on the structure; for example, linear equations with integer coefficients make sense in all of the above examples, whereas polynomial equations only make sense in fields and rings. Moreover, on $\mathbb{R}$, it makes sense to also consider inequations $f(x) < g(x)$, whereas in $\mathbb{C}$, it does not. Thus we need a formalism which allows us to describe the kinds of operations which make sense in a given structure; this will be called a "language".

1. Languages, structures, formulas

Definition 3.1. *A **language** is a set L function symbols and relation symbols. Each function and relation symbol has an arity $\in \mathbb{N}$.*

0-ary functions are usually called constants.

Here are some standard languages:

Beispiel 3.2.

- $L_{\text{ag}} = \{0, +, -\}$*, the language of abelian groups, where* 0 *is a constant symbol,* $+$ *is a binary function symbol and* $-$ *is a unary function symbol.*
- $L_{\text{ring}} = L_{\text{ag}} \cup \{\cdot\}$*, the language of rings, where* $\cdot$ *is a binary function symbol.*
- $L_{\text{oag}} = L_{\text{ag}} \cup \{<\}$*, the language of ordered abelian groups, where* $<$ *is a binary relation symbol.*

Definition 3.3. *Let L be a language. An **L-structure** is a set M together with the following:*

- *For each ℓ-ary function symbol f in L, a function $f^M \colon M^\ell \to M$.*
- *For each ℓ-ary relation symbol R in L, a subset $R^M \subset M^\ell$.*

*f^M and R^M are called the **interpretation** of f and M in M. When there is no risk of confusion, we will also write f and R instead of f^M and R^M.*

Any abelian group is naturally an L_{ag}-structure, any ring is naturally an L_{ring}-structure, and any ordered abelian group is naturally an L_{oag}-structure (where $<^G = \{(g,h) \in G^2 \mid g < h\}$). However, up to now, nothing prevents us from interpreting the above languages in a completely different way. Later, we will introduce the notion of a "theory" which will allow us to specify what kind of L-structures we want to consider. But first, let us define formulas. A formula can be seen as a statement about certain variables; these variables will be called the "free variables" of the formula. If ϕ is an L-formula and M is an L-structure, then elements of M can be plugged into the free variables of the formula and we can test whether the formula holds for these elements.

Definition 3.4. *Let L be a language, and let $\underline{x} = (x_1, \dots, x_n)$ be variables. We recursively define L-**terms** and L-**formulas** with free variables $\underline{x}$ as follows:*

(1) *x_i is an L-term (for any $i = 1, \dots, n$)*
(2) *if $t_1, \dots, t_\ell$ are L-terms and f is an ℓ-ary function symbol in L, then $f(t_1, \dots, t_\ell)$ is an L-term*
(3) *if $t_1, \dots, t_\ell$ are L-terms and R is an ℓ-ary relation symbol in L, then $R(t_1, \dots, t_\ell)$ is an L-formula*
(4) *if t_1 and t_2 are L-terms, then $t_1 = t_2$ is an L-formula.*
(5) *if ϕ_1 and ϕ_2 are L-formulas, then $\neg\phi_1$ and $\phi_1 \wedge \phi_2$ are L-formulas*
(6) *if ϕ is an L-formula with free variables $\underline{x}, y$, then $\exists y\, \phi$ is an L-formulas with free variables $\underline{x}$.*

If ϕ is a formula or a term, we sometimes write $\phi(\underline{x})$ to say that ϕ has free variables $\underline{x}$.

*A formula without free variables is called a **sentence**.*

*Formulas without sub-formulas (i.e., of the form (3) or (4)) are called **atomic***

Beispiel 3.5. *$\phi_1 = \exists x\, x \cdot y = 1$ is an L_{ring}-formula in the free variable y.*

$\phi_2 = \exists x\, \neg x + 0 = x$ is an L_{ag}-sentence.

Definition 3.6. *Let L be a language, let M be an L-structure and let $\underline{x} = (x_1, \ldots, x_n)$ be a tuple of variables. For an L-term $t(\underline{x})$, we define the **interpretation** of t in M to be the following function $t^M(\underline{a})\colon M^n \to M$.*

- *If $t = x_i$, then $t^M(\underline{a}) = a_i$.*
- *If $t = f(t_1, \ldots, t_\ell)$, then $t^M(\underline{a}) = f^M(t_1^M(\underline{a}), \ldots, t_\ell^M(\underline{a}))$.*

*For an L-formula $\phi(\underline{x})$, and $\underline{a} \in M^n$ a tuple of elements of the same length, we define what it means for $\underline{a}$ to **satisfy** ϕ (in M); this is denoted by $M \models \phi(\underline{a})$.*

- *If $\phi = R(t_1, \ldots, t_\ell)$, then $M \models \phi(\underline{a})$ iff $\underline{a} \in R^M$.*
- *If $\phi = (t_1 = t_2)$, then $M \models \phi(\underline{a})$ iff $t_1^M(\underline{a}) = t_2^M(\underline{a})$.*
- *If $\phi = \neg\psi$, then $M \models \phi(\underline{a})$ iff $M \not\models \psi(\underline{a})$.*
- *If $\phi = \psi_1 \wedge \psi_2$, then $M \models \phi(\underline{a})$ iff $M \models \psi_1(\underline{a})$ and $M \models \psi_2(\underline{a})$.*
- *If $\phi(\underline{x}) = \exists y\, \psi(\underline{x}, y)$, then $M \models \phi(\underline{a})$ iff there exists an element $b \in M$ such that $M \models \psi(\underline{a}, b)$.*

*We write $\phi(M) := \{\underline{a} \in M^n \mid M \models \phi(\underline{a})\}$ and also call this the set **defined** by ϕ in M.*

*If ϕ is a sentence, then we say that ϕ **holds** in M (or: M satisfies ϕ) iff $M \models \phi$.*

Beispiel 3.7. *Consider again the previous example.*

If R is a ring and $\phi_1 = \exists x\, x \cdot y = 1$, then $\phi_1(R) = R^\times$.

If G is a group and $\phi_2 = \exists x\, \neg x + 0 = x$, then G does not satisfy ϕ_2. ($G \not\models \phi_2$.)

Notation 3.8. *We will use a lot of suggestive notation for formulas, partially specific to some languages. Here are the most important ones:*

- *We use the following "logic" notation:*
  $\phi_1 \vee \phi_2$ means $\neg(\neg\phi_1 \wedge \neg\phi_2)$
  $\forall y\, \phi$ means $\neg\exists y\, \neg\phi$
  $\phi_1 \to \phi_2$ means $\neg\phi_1 \vee \phi_2$
  $\phi_1 \leftrightarrow \phi_2$ means $(\phi_1 \to \phi_2) \wedge (\phi_2 \to \phi_1)$
  $\top$ is a formula which is always true, e.g., $\forall x\, x = x$
  $\bot = \neg\top$ is always false. $t_1 \neq t_2$ means $\neg t_1 = t_2$.
  (In formulas, it is customary to use the single-line arrows for implication to distinguish them from the "real" implication $\Rightarrow$.)

- *If a function symbol of L is denoted by $+$, we will write corresponding formulas as $t_1 + t_2$. Also, $t_1 \cdot t_2 + t_3$ will mean $(t_1 \cdot t_2) + t_3$, for example.*
- *Formally, the L_{ag}-terms $s_1 = (t_1 + t_2) + t_3$ and $s_2 = t_1 + (t_2 + t_3)$ are different. However, we will only interpret L_{ag}-terms and formulas in structures M which are (abelian) groups, and in that case, $s_1^M = s_2^M$. Thus we will often omit the parenthesis.*
- *In L_{ring}, we write n for $1 + \cdots + 1$ (n times) and t^n for $t \cdots t$ (n times). (Again, this is only well-defined when interpreted in a ring.)*

Beispiel 3.9. *"$\forall x \, \forall y \, (x + y = y + x)$" is an L_{ring}-sentence satisfied by every ring.*

Übung 3.10. *Suppose that $\phi(\underline{x}, y)$ is an L-formula.*

(1) *Show that there exists a formula $\psi(\underline{x})$ such that for any L-structure M, $\psi(M) = \{\underline{x} \in M^n \mid$ there exists exactly one $y \in M$ such that $(\underline{x}, y) \in \phi(M)\}$.*

The formula $\psi(\underline{x})$ will be denoted by $\exists^{=1} y \, \phi(\underline{x}, y)$.

(2) *In a similar way, show that there are formulas for: there exist at least n / at most n / exactly n different b such that $\phi(\underline{x}, b)$ holds.*

An important aspect of formulas is that only quantifiers over elements of the structure are possible (and not, for example, over subsets of the structure); this limits the expressive power of formulas in such a way that we will be able to get general results about arbitrary formulas.

Beispiel 3.11. *Consider the L_{ring}-formula $\phi(x) = \exists y \, y^2 = x$. Then $\mathbb{C} \models \phi(-1)$ but $\mathbb{R} \not\models \phi(-1)$.*

Übung 3.12. *Let ϕ_1 and ϕ_2 be L-formulas in the same free variables.*

(1) *Show that $(\phi_1 \vee \phi_2)(M) = \phi_1(M) \cup \phi_2(M)$.*
(2) *Show that for any L-formula ϕ and any L-structure M, $(\neg\neg\phi)(M) = \phi(M)$.*

*We will call formulas **equivalent** if they define the same set in any structure; we will not distinguish between equivalent formulas.*

(3) *Give an example structure M which shows that the L_{ring}-formulas $x = y$ and $x + 0 = y$ are* not *equivalent. (Can M be a ring?)*

[Übersicht über Definitionen]

2. Mehrsortige Sprachen und Strukturen

Ziel: Durch Formeln definierbare Mengen in henselschen bewerteten Körpern verstehen.

Aber: Wie passen bewertete Körper in diesen Formalismus? Die haben nicht nur eine Menge und Funktionen/Prädikate darauf, sondern mehere: K, Γ. Deswegen verallgemeinerte Def:

Definition 3.13. *(Skizze)*

- *Eine **mehrsortige Sprache** L ist eine Sprache, bei der man außerdem noch eine Menge von Sorten hat, und für jedes Funktionssymbol und Relationssymbol sagt man dazu, auf welchen Sorten es lebt. (Bsp: Für eine n-stellige Funktion gibt man n Sorten für den Definitionsbereich an und eine Bildsorte.)*
- *Eine L-Struktur besteht aus je einer Menge für jede Sorte und Interpretationen der Funktions-Symb und Rel-Symb. als Funktionen und Relationen auf den entsprechenden Sorten.*
- *In Formeln hat jede Variable eine feste Sorte. Insbes. muss man bei einer „L-Formel mit freien Variablen $\underline{x}$“ noch für jedes x_i die Sorte angeben, die gemeint ist, und auch in „$\exists y \phi(\underline{x}, y)$“ ist y einer festen Sorte zugeornet.*
- *Die Interpretation einer Formel funktioniert auf naheliegende Art; dabei läuft jeder Quantor über eine Sorte.*

Beispiel 3.14. *Bewertete Körper sind zwei-sortige Strukturen in der* Sprache der bewerteten Körper L_{vf}*, die aus folgendem besteht:*

- *Zwei Sorten:* VF, Γ'.
- *Auf* VF *die Sprache* $L_{\mathrm{ring}} = \{0, 1, +, -, \cdot\}$. *(Also z. B.:* $+$ *ist Funktion* $\mathrm{VF} \times \mathrm{VF} \to \mathrm{VF}$*)*
- *Auf* Γ' *die Sprache* $L_{\mathrm{oag}} = \{0, +, -, <\}$
- *Eine Funktion* $v\colon \mathrm{VF} \to \Gamma'$.
- *Eine Konstante* $\infty \in \Gamma'$

(Die Konstante ∞ ist nötig, damit v eine Funktion ist. Damit $+$, $-$ Fkt auf Γ' sind, setze sie irgendwie auf ∞ fort, z. B. $\infty + a = \infty$, etc.)

Falls K ein bew. Körper (als L_{vf}-Struktur) ist, sollte man am besten VF^K *und* Γ^K *schreiben für die entsprechenden Mengen der Struktur K. Wir werden aber oft K und Γ statt dessen schreiben.*

Die Formel $\phi(x) = (v(x) \geq 0)$ (wobei x eine VF*-Variable ist) definiert den Bewertungsring, und $\phi(x) = (v(x) > 0)$ definiert maximales Ideal.*

3. Definierbare Elemente, Mengen und Funktionen

Definition 3.15. *L Sprache, M L-Struktur, $A \subset M$ $\rightsquigarrow$ $L(A) := L \cup A$, wobei $a \in A$ Konstanten-Symbol ist, dass in M durch sich selbst interpretiert wird.*

Definition 3.16.

- *Mengen der Form $\phi(M)$ für ϕ L-Formel heißen **$\emptyset$-definierbar** (oder auch **L-definierbar**). Falls ϕ eine $L(A)$-Formel ist, heißt $\phi(M)$ **A-definierbar**. (Und A heißt **Parameter-Menge**.) **Definierbar** heißt A-definierbar für beliebiges A.*
- *Ein Element $b \in M$ heißt A-definierbar, falls $\{b\}$ A-definierbar ist.*
- *Eine Fkt $M^n \to M$ heißt A-defbar, falls ihr Graph ($\subset M^{n+1}$) A-defbar ist.*

Bemerkung 3.17. *X ist A-defbar genau dann wenn es eine L-Formel $\phi(\underline{x}, \underline{y})$ gibt und ein Tupel $\underline{a} \in A$ mit $\underline{b} \in X \iff \phi(\underline{b}, \underline{a})$.*

Beispiel 3.18. *K Körper (als L_{ring}-Struktur), $f \in K[\underline{x}]$. Dann ist die Nst-Menge von f definierbar. (Als Parameter-Menge reichen die Koeffizienten von f.)*

Beispiel 3.19. *K bewerteter Körper (als L_{vf}-Struktur). Dann ist jeder offene (oder abg.) Ball defbar: $\phi(x) = v(x - a) > \lambda$, wobei a, λ Parameter sind.*

Beispiel 3.20. *Endliche und co-endliche Mengen (in M^n) sind immer defbar.*

Um zu zeigen, dass es auch nicht-defbare Mengen gibt, ist folgendes Lemma praktisch:

Lemma 3.21. *Ist σ Automorphismus von M mit $\phi\restriction_A = \mathrm{id}_A$, und ist $\phi \in L(A)$, dann ist $\phi(M) = \sigma(\phi(M))$.*

Beweis. Übung (inkl. exakter Def. von Automorphismus.) □

Beispiel 3.22. *Sei M eine Menge, als Struktur über der leeren Sprache. Dann ist $X \subset M$ defbar genau dann, wenn X endlich oder co-endlich ist.*

(Zum Beweis verwende, dass in einer Formel nur endlich viele Parameter vorkommen können.)

Beispiel 3.23. *Consider $\mathbb{C}$ in the ring language. Claim: a is $\emptyset$-definable iff $a \in \mathbb{Q}$.*

Proof: if $a = \frac{r}{s}$*, it is defined by the formula* $x \cdot \underbrace{(1 + \cdots + 1)}_{s} = \underbrace{1 + \cdots + 1}_{r}$*.*

For the other direction, note that if $\sigma \colon \mathbb{C} \to \mathbb{C}$ *is an automorphism, then for any term* t*,* $t(\sigma(\underline{a})) = \sigma(t(\underline{a}))$ *and then, for any formula* ϕ*,* $\mathbb{C} \models \phi(\underline{a})$ *iff* $\mathbb{C} \models \phi(\sigma(\underline{a}))$*. Now since any* $a \in \mathbb{C} \setminus \mathbb{Q}$ *can be moved by an automorphism, if* $a \in \phi(\mathbb{C})$ *for some formula* ϕ*, then we automatically also find another element* $\sigma(a) \in \phi(\mathbb{C})$*.*

$\emptyset$-defbare Dinge kann man zur Sprache hinzufügen ohne dass sich ändert, was definierbar ist:

Lemma 3.24. *Let* M *be an* L*-structure and* $A \subset M$ *any parameter-set.*

(1) *If* $X \subset M^n$ *is an* L*-definable set, then adding a predicate to* L *which is interpreted by* X *does not change the* A*-definable sets.*
(2) *If* $f \colon M^n \to M$ *is a function whose graph is* L*-definable as a subset of* M^{n+1}*, then adding a function to* L *which is interpreted by* f *does not change the* A*-definable sets. (In particular, this works for* 0*-ary functions, i.e., definable elements can be added as constants.)*

Beweis. (1) Exercise.

(2) Let $\phi(x_1, \ldots, x_n, y)$ be a formula defining the graph of f, and suppose that ψ is a formula in the bigger language which contains a term $t' = f(t_1, \ldots, t_n)$. Denote by χ the smallest sub-formula of ψ around this occurence of t'. Then replace t' by a new variable y, and replace χ by $\exists y \, (\phi(t_1, \ldots, t_n, y) \wedge \chi)$. Do this for every occurence of f. □

Beispiel 3.25. 0 *is not really necessary in the language of abelian group, since it is definable by* $\phi(x) = \forall y \, x + y = y$*. Similarly, the function* $x \mapsto -x$ *is not necessary since it can be defined by* $\phi(x, y) = x + y = 0$*.*

In a similar way, in fields, division can be defined (using any convention for $\frac{a}{0}$*).*

Beispiel 3.26. *In bew. Kp. können wir ein Prädikat für den Bewertungsring hinzufügen.*

Beispiel 3.27. *In* $\mathbb{C}$ *sind Nst-Mengen von Polynomen über* $\mathbb{Q}$ $\emptyset$*-defbar.*

Das zeigt auch: Wenn uns die Struktur der Formeln gar nicht interessiert, dann brauchen wir keine Fkt-Symbole; nimm statt dessen Rel-Symbole für deren Graphen. (Dann haben Formeln aber mehr Quantoren. Statt $x = 1+1+1$ muss man dann schreiben: $\exists y\,\mathrm{summe}(1,1,y) \wedge \mathrm{summe}(1,y,x)$.)

Beispiel 3.28. *Consider $\mathbb{Q}_p$ in the ring language. Claim: $\mathbb{Z}_p$ is $\emptyset$-definable.*

Suppose $p > 2$ ($p = 2$: exercise). Claim: $\phi(x) = \exists y\, y^2 = px^2 + 1$ defines $\mathbb{Z}_p$.

$a \notin \mathbb{Z}_p \Rightarrow v(a) < 0 \Rightarrow v(pa^2) < 0$ and odd $\Rightarrow v(pa^2+1)$ odd. But $v(y^2)$ is even for any y.

If $a \in \mathbb{Z}_p$, apply Hensel's Lemma to $f(y) = y^2 - (pa^2+1)$: $v(f(1)) = v(1 - pa^2 - 1) > 0$, $f'(y) = 2y$, $v(f'(1)) = v(2) = 0$. Hence a solution y exists.

4. Imaginäre Sorten

Beispiel 3.29. *Sei K bew. Kp (in der Sprache L_{vf}). Zur Erinnerung: $\bar{K} = \mathcal{O}/\mathcal{M}$, und* $\mathrm{res}\colon \mathcal{O} \twoheadrightarrow \bar{K}$.

Formal ist $\phi(x) = \exists y \in \bar{K} \mid \mathrm{res}(x) = y^2$ keine Formel. Wir könnten $\bar{K}$ als Sorte zu L_{vf} hinzufügen (zusammen mit L_{ring} darauf und res*). Andererseits lässt sich ϕ auch in eine richtige L_{vf}-Formel übersetzen:*
$\exists y \in \mathcal{O}\ \mathrm{res}(x) = \mathrm{res}(y)^2$
$\exists y \in \mathcal{O}\ \mathrm{res}(x) = \mathrm{res}(y^2)$
$\exists y \in \mathcal{O}\ x - y^2 \in \mathcal{M}$

Allgemein gilt:

Lemma 3.30. *Sei M L-Struktur, $X \subset M^n$ $\emptyset$-defbar, und sei $\sim$ eine $\emptyset$-defbare Äqu-Rel auf X. Sei $L' \subset L$ mit einer neuen Sorte Q und einem neuen Fkt-Symb. $\pi\colon M^n \to Q$. Sei M' die L'-Strutkur, die man aus M erhält mit $Q^{M'} := M^n/\!\sim$ und π die kanonische Projektion.*

Dann sind die defbaren Mengen in M und die defbaren Mengen in den alten Sorten von M' die gleichen.

*(Q heißt **imaginäre Sorte** von M, und die Elemente von Q heißen **imaginäre Elemente**.)*

(Im obigen Beispiel ist $X = \mathcal{O}$ und $x \sim y \iff x - y \in \mathcal{M}$.)

Beispiel 3.31. *Sei $L = L_{\mathrm{ring}} \cup \mathcal{O}$, wobei $\mathcal{O}$ 1-st. Relation ist. Sei K ein bew. Körper als L-Struktur, wobei $\mathcal{O}$ der Bew-Ring ist. Dann ist Γ'*

imaginäre Sorte von K:
Nimm $X = K$ und $x \sim y \iff x = y = 0$ oder $\frac{x}{y} \in \mathcal{O}$ und $\frac{y}{x} \in \mathcal{O}$.

5. Theories

Given a language L, we now introduce a general formalism to specify that we are only interested in particular L-structures (e.g. if $L = L_{\text{ring}}$, we might only be interested in rings or even only in fields).

Definition 3.32. *Let L be a language.*

- *An L-**theory** is a set of L-sentences.*
- *An L-structure M **satisfies** a theory T if it satisfies all its sentences; in that case, we also say that M is a **model** of T, and we write this as $M \models T$.*
- *A theory is **consistent** if it does have a model. Most of the time, we will only consister consistent theories.*
- *Two theories are equivalent if they have the same models. (We will only be interested in theories up to equivalence.)*
- *A sentence ϕ **follows** from a theory T if for any model $M \models T$, we have $M \models \phi$. We denote this by $T \vdash \phi$.*

Here are some standard theories:

Definition 3.33.

- *T_{ag} is the L_{ag}-theory consisting of the axioms of abelian groups, formulated as sentences (e.g., $\forall x\, x+0 = x$).*
- *T_{ring} is the L_{ring}-theory consisting of the axioms of commutative rings with unit.*
- *T_{ACF} is the L_{ring}-theory consisting of axioms for algebraically closed fields; more precisely, it consists of the field axioms, together with, for each $n \geq 1$, a sentence saying that polynomials of degree n have zeros:*

$$\forall y_0 \ldots \forall y_{n-1}\, \exists x\, (x^n + y_{n-1}x^{n-1} \cdots + y_1 x + y_0 = 0).$$

- *T_{vf}: L_{vf}-Theorie der bewerteten Körper:*
  - *K ist Körper*
  - *$\Gamma' = \Gamma \cup \{\infty\}$ mit Γ angeordnete abelsche Gruppe.*
  - *v ist Bewertung.*
- *T_{Hen}: L_{vf}-Theorie der henselschen bewerteten Körper: T_{vf} und außerdem, für jedes n:*

Für all f Poly. vom Grad n und $a \in \mathcal{O}$ mit $v(f(a)) > 0$, etc.

Note that for T_{ag} and T_{ring}, a single sentence would suffice (the conjunction of all axioms); however, T_{ACF} inherently needs infinitely many axioms.

Übung 3.34. *Show the following basic properties:*

(1) $T \vdash \phi$ *iff* $T \cup \{\neg\phi\}$ *is inconsistent.*
(2) *(*T *is inconsistent) iff (*$T \vdash \bot$*), iff (*$T \vdash \phi$ *for all* ϕ*), iff (there exists* ϕ *with* $T \vdash \phi$ *and* $T \vdash \neg\phi$*).*
(3) *If* $T \vdash \phi$ *and* $T \vdash \phi \to \psi$ *then* $T \vdash \psi$*.*
(4) T_1 *and* T_2 *are equivalent iff the sets* $\{\phi \mid T_i \vdash \phi\}$ *are equal for* $i = 1, 2$*.*

6. Complete theories

Now one questions is: how much can we say about a structure by fixing a theory? We already saw that there is a theory whose models are exactly the groups, but is there, for example, a theory whose only model is $\mathbb{C}$? An obvious candidate for such a theory would be to take *all* sentences which hold in $\mathbb{C}$.

Definition 3.35.
- *Let* M *be an* L*-structure. Then* $\text{Th}(M)$ *is the set of all sentences* ϕ *such that* $M \models \phi$*; we call this the* ***theory of*** M*.*
- *Two* L*-structures* M*,* M' *are* ***elementarily equivalent****, written as* $M \equiv M'$ *or* $M \equiv_L M'$*, iff* $\text{Th}(M) = \text{Th}(M')$*.*

One can prove that all algebraically closed fields of the same characteristic are elementarily equivalent. In particular, $\text{Th}(\mathbb{C})$ does not characterize $\mathbb{C}$. In fact, 3.39 is even a stronger statement.

Theories of structures have an important property: for any sentence ϕ, exactly one of ϕ and $\neg\phi$ is contained in $\text{Th}(A)$.

Definition 3.36. *Let* T *be an* L*-theory.* T *is called* ***complete*** *if for any* L*-sentence* ϕ*, exactly one of* $T \vdash \phi$ *and* $T \vdash \neg\phi$ *holds.*

Obviousely, T is consistent iff there exists a $T' \supset T$ which is complete. And: T is complete iff there exists M with $T = \text{Th}(M)$.

Definition 3.37. *If* $M \subset M'$ *are* L*-structures, we say that* M' *is an* ***elementary extension*** *of* M*, written as* $M \prec M'$*, iff* $M \equiv_{L(M)} M'$*.*

Beispiel 3.38. $M := \mathbb{N}$*,* $M' := \mathbb{Z}_{\geq -1}$ *in the language with only the sucessor function* S*. Then* $M \cong M'$ *(and hence* $M \equiv M'$*) but not* $M \prec M'$*, since* $\neg\exists x\, S(x) = 0$ *holds in* M *but not in* M'*.*

We will prove:

Proposition 3.39. *$K \subset K'$ alg. closed fields. Then $K \prec K'$.*

Lemma 3.40. *(Tarski's Test) For $M \subset M'$ we have $M \prec M'$ iff for each $L(M)$-formula $\phi(x)$ such that $M' \models \exists x\, \phi(x)$, there is an $a \in M$ such that $M' \models \phi(a)$.*

Beweis. "$\Rightarrow$": $M' \models \phi(a') \Rightarrow M' \models \exists x\, \phi(x) \Rightarrow M \models \exists x\, \phi(x) \Rightarrow$ there exists $a \in M$ s.th. $M \models \phi(a) \Rightarrow M' \models \phi(a)$.

"$\Leftarrow$": we prove $M' \models \phi \iff M \models \phi$ by induction on the structure of ϕ (only for sentences ϕ). Only the case $\phi = \exists x\, \psi(x)$ is non-trivial.

$M' \models \phi \iff \exists (a' \in M')\, M' \models \psi(a') \iff \exists (a \in M)\, M' \models \psi(a) \iff \exists (a \in M)\, M \models \psi(a) \iff M \models \phi$. □

Proof of 3.39 if K has infinite transcendence degree. Suppose that there exists $a' \in K'$ such that $K' \models \phi(a')$. ϕ uses only finitely many parameters $\underline{b} \in K$; let L be the field generated by $\underline{b}$ over the prime field.

First case: a' is algebraic over L. Then $a' \in K$ since $L \subset K$ and K algebraically closed.

Second case: a' is transcendental over L. Choose $a \in K$ transcendental over L (this exists since K has infinite tr-deg but L has finite tr-deg). There exists $\sigma \in \mathrm{Aut}(K'/L)$ with $\sigma(a') = a$. Since $\sigma(\underline{b}) = \underline{b}$, we have $\sigma(\phi(K')) = \phi(K')$ and hence $K' \models \phi(\sigma(a'))$. □

The case where K has finite transcendence degree requires the compactness theorem...

7. The compactness theorem

This is *the* most imporant theorem of model theory.

Theorem 3.41. *(Compactness) For any L-theory T and any L-sentence ϕ with $T \vdash \phi$, there exists a finite subset $T_0 \subset T$ such that $T_0 \vdash \phi$.*

Let me give a second formulation.

Theorem 3.42. *(Also compactness) A theory T' is consistent if and only if T' is **finitely satisfyable**, i.e., each finite subset is consistent.*

And a third one: Let S be the set of all complete theories (in a given language L). The family of sets $X_\phi := \{T \in S \mid T \vdash \phi\}$ (where ϕ is

an L-formula) is closed under intersection, hence it forms a basis of a topology on S, the **Stone topology**.

Note: X_ϕ is clopen, since its complement is $X_{\neg\phi}$. An aribtrary closed set is one of the form $X_\Phi := \{T \in S \mid \Phi \subset T\}$ for Φ a set of formulas.

Übung 3.43. *S is Hausdorff and satisfies T4 (i.e., any two disjoint closed sets can be separated by open sets).*

Theorem 3.44. *(Also compactness) S is compact (with the Stone topology).*

3.42 implies 3.41 by taking $T' = T \cup \{\neg\phi\}$; 3.41 implies 3.42 by taking $T = T'$ and $\phi = \bot$.

A family of open sets $(X_\phi)_{\phi\in\Phi}$ is a cover of S iff there is no complete theory containing $\Psi := \{\neg\phi \mid \phi \in \Phi\}$, i.e., Ψ is inconsistent. Thus 3.44 says: any inconsistent set Ψ has a finite subset, which is inconsistent. This is 3.42.

The first version can be interpreted as follows: if we prove ϕ using T, then the proof should have finite length, and hence only finitely many sentences from T can be used in the proof. Indeed, there is a formal proof system which allows to argue like this; the fact that such formal proofs always exist (in this system) is Gödel's completeness theorem. (Hence Gödel's completeness theorem implies the compactness theorem.) However, we will use a different proof.

First, we need some definitions.

Definition 3.45. *Let I be a set. An **ultra-filter** on I is a finitely additive probability measure μ on I which takes values only in $\{0, 1\}$.*

Beispiel 3.46. *If $a \in I$, then the measure concentrated at a is an ultra-filter.*

The set of ultra-filters on I is the Stone-Čech compactification of I as a discrete set.

Lemma 3.47. *A map $\mu\colon I \to \{0, 1\}$ is a ultra-filter iff the following two conditions hold (for $A, B \subset I$).*

(1) $\mu(A) + \mu(I \setminus A) = 1$
(2) $\mu(A \cap B) = \min\{\mu(A), \mu(B)\}$.

Beweis. Using (1), (2) is equivalent to (2') $\mu(A\cup B) = \max\{\mu(A), \mu(B)\}$, which looks almost like additivity.

$\Rightarrow$: Clear.

$\Leftarrow$: (2') $\Rightarrow \mu(I) \geq \mu(\emptyset)$; with (1): $\mu(I) = 1$.
Additivity follows from (2') if for disjoint A, B, we can not have $\mu(A) = \mu(B) = 1$. But this would imply $\mu(I \setminus B) = 0$ which together with $A \subset I \setminus B$ contradicts (2'). □

Lemma 3.48. *If $A \subset \mathcal{P}(I)$ satisfies: $X_1 \cap \cdots \cap X_n \neq \emptyset$ for all $X_i \in A$, then there exists an ultra-filter μ on I such that $\mu(X) = 1$ for all $X \in A$.*

Beweis. Without loss, A is closed under intersection and supersets.

Define $\mu_0(X) = 1$ if $X \in A$ and 0 otherwise. Then μ_0 satisfies 3.47 (2). Moreover we have $(\frac{1}{2})$ $\mu_0(X) + \mu_0(I \setminus X) \leq 1$.

Suppose there exist "bad" Y with $\mu_0(Y) + \mu_0(I \setminus Y) = 0$. Choose such an Y and set $\mu_1(X) := \mu_0(X \cup Y)$.

Then μ_1 still satisfies (2) (since $(A \cap B) \cup Y = (A \cup Y) \cap (B \cup Y)$) and $(\frac{1}{2})$ (since otherwise, $\mu_0(X \cup Y) = \mu_0((I \setminus X) \cup Y) = 1$ and hence $\mu_0((X \cup Y) \cap ((I \setminus X) \cup Y)) = \mu_0(Y) = 1$).

Now $\mu_1 \geq \mu_0$ and $\mu_1(I \setminus Y) = \mu_0(I) = 1$, hence μ_1 is better than μ_0 (less bad sets). Thus one can apply Zorn's Lemma. □

Beispiel 3.49. *Now we can construct ultra-filters which are not concentrated in one point. Let I be infinite and let A be the set of all co-finite sets. By Lemma 3.48, we find an ultra-filter with $\mu(X) = 0$ for all X finite.*

Definition 3.50. *Let $(M_i)_{i \in I}$ be a family of L-structures and let μ be an ultra-filter on I. The **ultra-product** $\prod_\mu M_i$ is the quotient of $\prod_{i \in I} M_i$ by the following equivalence relation:*

$$(a_i)_i \sim (b_i)_i \iff \mu(a_i = b_i) = 1$$

The ultra-product becomes an L-structure as follows:

- *If $R \in L$ is a relation symbol, then $(\underline{a}_i)_i \in R \iff \mu(\underline{a}_i \in R) = 1$*
- *If $f \in L$ is a function symbol, then $f((\underline{a}_i)_i) = (b_i)_i \iff \mu(f(\underline{a}_i) = b_i) = 1$*

We will see below that we get well-defined functions on the ultra-product.

Proposition 3.51. *(Łoś's theorem) $\prod_\mu M_i \models \phi((\underline{a}_i)_{i \in I})$ iff $\mu(M_i \models \phi(\underline{a}_i)) = 1$.*

BEWEIS. If there are function symbols f in the language, we replace them by relation symbols R for their graphs. Once we have finished the proof for the modified structures, we know that $\forall \underline{x} \exists^{=1} y\, R(\underline{x}, y)$ holds in the ultra-product, so it is indeed also a structure in the original language.

Now do induction over the structure of ϕ.

Notation: Fix $(\underline{a}_i)_I$, and let I_ϕ the set where $M_i \models \phi(\underline{a}_i)$.

For atomic formulas, it's true by definition.

$\phi = \neg\psi$: I_ϕ is the complement of I_ψ, hence $\mu(I_\phi) = 1 \iff \mu(I_\psi) = 0$.

$\phi = \psi_1 \wedge \psi_2$: $I_\phi = I_{\psi_1} \cap I_{\psi_2}$, so $\mu(I_\phi) = 1$ iff $\mu(I_{\psi_1}) = 1$ and $\mu(I_{\psi_2}) = 1$.

$\phi(\underline{x}) = \exists y \psi(\underline{x}, y)$. We have to show: $\mu(I_\phi) = 1$ iff there is a $(b_i)_{i \in I}$ such that $\mu(M_i \models \psi(\underline{a}_i, b_i)) = 1$
"$\Leftarrow$": $M_i \models \psi(\underline{a}_i, b_i)$ implies $i \in I_\phi$, hence $\mu(I_\phi) = 1$.
"$\Rightarrow$": $i \in I_\phi$ implies that there exists an $b_i \in M_i$ with $M_i \models \psi(\underline{a}_i, b_i)$. Choose the remaining b_i arbitrarily. Then $\mu(I_\phi) = 1$ implies $\mu(M_i \models \psi(\underline{a}_i, b_i)) = 1$. □

Beispiel 3.52. *Wenn die M_i Körper sind, ist das Ultraprodukt M auch ein Körper. Wenn μ-fast alle M_i die gleiche Charakteristik haben, dann hat M auch diese Charakteristik; ansonsten hat M Charakteristik 0.*

Übung 3.53. *Wieso folgt daraus, dass man „Charakteristik 0 haben" nicht mit endlich vielen Axiomen ausdrücken kann?*

Beispiel 3.54. *Wenn die M_i endliche Körper sind, ist das Ultraprodukt M i.A. unendlich, verhält sich aber aus modelltheoretischer Sicht wie ein großer endlicher Körper; man nennt M dann* ***pseudo-endlich****. (Z.B.: Defbare Abbildungen sind injektiv genau dann, wenn sie surjektiv sind.)*

Now we can prove compactness:

PROOF OF 3.42. For each finite set $S \subset T$, choose a model of S; denote all those models by $(M_i)_{i \in I}$.

For each $\phi \in T$, consider the set $X_\phi = \{i \in I \mid M_i \models \phi\}$; let A be the set of all X_ϕ.

For finitely many X_ϕ we find an M_i which lies in the intersection (by construction), hence we can apply Lemma 3.48 to get an ultra-filter μ with $\mu(X_\phi) = 1$. Now the corresponding ultra-product $\prod_\mu M_i$ is a model of T. □

8. Löwenheim-Skolem

Theorem 3.55. *(Löwenheim-Skolem aufwärts) Sei M unendliche L-Struktur, $\kappa > |M| + |L|$ Kardinalzahl. Dann ex. $M' \succ M$ mit $|M'| = \kappa$.*

Theorem 3.56. *(Löwenheim-Skolem abwärts) Sei M unendliche L-Struktur und $X \subset M$. Dann ex. $M' \prec M$ mit $X \subset M'$ und $|M'| = |X| + |L| + \aleph_0$.*

Bew. von aufwärts und abwärts. Bei aufwärts reicht es, $|M'| \geq \kappa$ zu finden. Danach wende abwärts an mit der Sprache $L(M)$ (so dass das Resultat Elem. Erw. von M ist) und $X \subset M'$ mit $|X| = \kappa$ an.

Um so ein großes M' zu finden, füge κ viele Konstantensymbole zur Sprache $L(M)$ hinzu und wende Kompaktheit an auf die (endlich erfüllbare) Theorie $\mathrm{Th}(M) \cup \{\text{alle Konstanten verschieden}\}$.

Abwärts:

• OBdA $X = \emptyset$ (ersetze die Sprache durch $L(X)$)

• OBdA ist L relational (d. h. keine Fkt-Symb.)

• Idee: Fange an mit $M_0 \subset M$ beliebig an mit $|M_0| = |L| + \aleph_0$ und vergrößere es so lange, bis es als M' tut. Wir müssen nur dafür sorgen, dass das Tarskis Test erfüllt ist.

• Sei also M_i gegeben. Sei Φ die Menge der $L(M_i)$-Formeln $\phi(x)$ in einer freien Var, so dass es ein $a_\phi \in M$ gibt mit $M \models \phi(a_\phi)$. Setze

$$M_{i+1} := M_i \cup \{a_\phi \mid \phi \in \Phi\}$$

• Offenbar ist Tarskis Test in M_{i+1} erfüllt für alle $L(M_i)$-Formeln. Setze $M' := \bigcup_i M_i$. Das erfüllt Tarsis Test ganz.

• Und: $|M_{i+1}|$ is max. so groß wie es $L(M_i)$-Formeln gibt, also $|M_i| + |L| + |\aleph_0| = |L| + |\aleph_0|$. Also $|M'| = |L| + |\aleph_0|$. □

Recall 3.39: If $K \subset K'$ are algebraically closed, then $K \prec K'$; we still have to do the case when K has finite transcendence degree.

Reducing finite tr-deg to infinite tr-deg. Consider $K \subset K'$ as an $L := L_{\mathrm{ring}} \cup \{P\}$ structure, where P is a predicate for K. Let $K'' \subset K'''$ be an elementary extension of $K \subset K'$ with $|K''|$ uncountable. Then $K'' \prec K'''$, i.e. for every formula $\phi(x)$, (K'', K''') satisfies:

$(\exists x\, \phi(x)) \to (\exists x\, P(x) \wedge \phi(x))$. Thus (K, K') also satisfies this, i.e., $K \prec K'$. □

As an application, we get a short proof of (the weak) Hilbert's Nullstellensatz.

Theorem 3.57. *If K is algebraically closed and $f_i \in K[\underline{x}]$ are polynomials with $(f_1, \ldots, f_k) \neq K[\underline{x}]$, then there exists $\underline{a} \in K^n$ with $f_i(\underline{a}) = 0$ for all i.*

BEWEIS. Let M be a maximal ideal containing I. Then in $K[\underline{x}]/M$, we have $f_i(\underline{x}) = 0$ for all i. Let L be the algebraic closure of $K[\underline{x}]/M$. Then $K \prec L$ by 3.39. Thus we can already find $\underline{a} \in K$ with $K \models \bigwedge_i f_i(\underline{a}) = 0$. □

9. Quantoren-Elimination

Definition 3.58. *Eine L-Theorie T hat **Quantoren-Elimination (QE)** wenn es zu jeder L-Formel $\phi(\underline{x})$ eine quantoren-freie L-Formel $\psi(\underline{x})$ gibt mit $T \vdash \forall \underline{x} \phi(\underline{x}) \leftrightarrow \psi(\underline{x})$.*

Lemma 3.59. *Um QE zu zeigen reicht es, den Quantor in Formeln der Form $\phi(\underline{x}) = \exists y\, \psi(\underline{x}, y)$ zu eliminieren, wobei ψ Konjunktion von atomaren Formeln und negierten atomaren Formeln ist. Außerdem kann man annehmen, dass y in jedem Atom von ψ vorkommt.*

BEWEIS. Reduktion auf Formeln der Form $\phi(\underline{x}) = \exists y\, \psi(\underline{x}, y)$ für ψ quantorenfrei durch Induktion über den Aufbau der Formel. Schreibe dann ψ in disjunktiver Normalform und ziehe die Disjunktion aus dem Quantor raus. Die Atome ohne y können auch noch rausgezogen werden. □

Theorem 3.60. *Die Theorie der alg. abg. Körper T_{ACF} hat Quantoren-Elimination.*

Bemerkung 3.61. *Das bedeutet: Definierbare Mengen sind das gleiche wie konstruktible Mengen.*

BEWEIS. (Wir geben sogar einen Algorithmus an, um die quantorenfreie Formel zu bekommen.)

Nach dem Lemma OBdA $\phi(\underline{x}) = \exists y \bigwedge_i f_i(\underline{x}, y) =/\neq 0$.

Fasse die Polynome auf als Polynome in y mit Koeff. in $\mathbb{Z}[\underline{x}]$.

OBdA Leitkoeffizienten $\neq 0$. (Erklärung: Falls $f = \sum_{j \leq n} a_j y^j$ in ϕ vorkommt, mit $a_j \in \mathbb{Z}[\underline{x}]$, dann ist „$a_n = 0$“ eine quantorenfreie Formel mit

freien Variablen $\underline{x}$. Wenn $\chi(\underline{x})$ äquivalent zu ϕ ist unter der Bedingung $a_n = 0$, dann ist ϕ immer äquivalent zu $(a_n \neq 0 \wedge \chi) \vee (a_n = 0 \wedge \phi')$, wobei ϕ' aus ϕ entsteht, indem man den Summanden mit a_n ganz weg lässt. Das ganze kann man mit ϕ' wiederholen...)

OBdA alle $\deg f_i \geq 1$. (Sonst kommt y nicht vor, und es kann aus dem Existenzquantor rausgezogen werden.)

Wenn's nur Ungleichungen sind, ist die Formel äquivalent zu $\top$ (d. h. für alle $\underline{x}$ wahr), da jede Ungleichung nur endlich viele y ausschließt.

OBdA gibt's nur eine Ungleichung. (Die kann man alle zusammenmultiplizieren.)

Wir machen Induktion über die Summe der Grade der f_i.

Annahme, es gibt eine Gleichung f_i gibt, deren Grad kleiner gleich einem anderen f_j ist: Wenn ich f_j ersetze durch $af_j + bf_i$, ändert sich am Wahrheitsgehalt der Formel nix. Auf diese Art kann man den Grad von f_j verkleinern (Division mit Rest...).

Am Ende ist nur noch eine Gleichung f_1 übrig, und wenn's eine Ungleichung gibt, dann hat die kleineren Grad. Die Gleichung hat mehr Lösungen, als die Ungleichung ausschließt, also ist die Formel wahr für alle $\underline{x}$. □

KAPITEL 4

QE in Henselian valued fields

Die Aussage soll sein: Die Theorie der henselschen Körper der Charakteristik 0 hat QE; aber in welcher Sprache?

Erinnerung: $\operatorname{char} k \neq 2 \Rightarrow a$ ist Quadrat $\iff v(a)$ in Γ durch 2 teilbar und, wenn $b \in K$ ist mit $2v(b) = a$, dann: $\operatorname{res}(\frac{a}{b^2})$ ist Quadrat in k.

Das zeigt: In L_{vf} habe keine QE. Zwei Probleme:
1. Wie sagt man, dass $v(a)$ durch 2 teilbar ist?
2. Wie sagt man, dass $\operatorname{res}(a)$ ein Quadrat ist?

Es kann noch schlimmer sein:

Beispiel 4.1. *$K = \mathbb{Q}((t))$: $\mathbb{Q}$ ist nicht entscheidbar, also auch nicht K.*

Teillösung: Wir zeigen nur "QE relativ zum Restklassenkörper und zur Wertegruppe": Jede Formel ist äquivalent zu einer, die nur Quantoren über den Restklassenkörper und über die Wertegruppe hat.

Nächstes Problem: „$\operatorname{res}(a)$ ist ein Quadrat" macht keinen Sinn wenn $a \notin R$. Lösung: Leittermstruktur.

1. Leading term structure

Let K be a Henselian valued field.

$1 + \mathcal{M}$ is a subgroup of $K^\times$.

Definition 4.2. $\mathrm{RV}^\times := (K^\times/(1+\mathcal{M}))$, $\mathrm{RV} := \mathrm{RV}^\times \cup \{0\}$; $\mathrm{rv}\colon K \to \mathrm{RV}$ *canonical map "**leading term structure**".*

Bemerkung 4.3. $\mathrm{rv}(a) = \mathrm{rv}(b) \iff v(a-b) > v(a) \iff v(a-b) > v(b)$ *(oder $a = b = 0$).*

Beispiel 4.4. *Falls $K = k((t))$: Sei $a = \sum_{i \geq m} a_i t^i$, $b = \sum_{i \geq n} b_i t^i$ mit $a_m \neq 0, b_n \neq 0$. Dann ist $\mathrm{rv}(a) = \mathrm{rv}(b) \iff m = n \wedge a_m = b_n$.*

In diesem Beispiel habe also Repräsentantensystem von $\mathrm{RV}^\times$ der Form $a \cdot t^n$, $a \in k^\times$.
Also: $\mathrm{RV}^\times = k^\times \times \Gamma$

I.A. habe nur k.e.S. $k^\times \hookrightarrow \mathrm{RV}^\times \overset{v_{\mathrm{RV}}}{\twoheadrightarrow} \Gamma$:
Ex. von v_{RV} ist klar; Kern davon ist $\mathrm{rv}(\mathcal{O}^\times)$; für $a, b \in \mathcal{O}^\times$ ist $\mathrm{rv}(a) = \mathrm{rv}(b) \iff a - b \in \mathcal{M}$; also $\ker v_{\mathrm{RV}} \cong k^\times$.

Definition 4.5. *Language:* $L_{\mathrm{RV}} := L_{\mathrm{ring}} \cup \{\mathrm{RV}, \mathrm{rv}, \cdot, \xi_1 + \xi_2 \approx \xi_3\}$, *where:*
$\mathrm{rv}\colon K \to \mathrm{RV}$ *is the canonical map.*
$\cdot\colon \mathrm{RV} \times \mathrm{RV} \to \mathrm{RV}$ *with* $\mathrm{rv}(a) \cdot \mathrm{rv}(b) = \mathrm{rv}(a \cdot b)$
$\xi_1 + \xi_2 \approx \xi_3$ *is a ternary relation which holds iff there exist* a_i *with* $\mathrm{rv}(a_i) = \xi_i$ *and* $a_1 + a_2 = a_3$.

Falls es ein eindeutiges ξ_3 gibt mit $\xi_1 + \xi_2 \approx \xi_3$ („$\xi_1 + \xi_2$ **wohldefiniert**“), dann schreibe $\xi_1 + \xi_2 = \xi_3$.
Schreibe $-\mathrm{rv}(a)$ für $\mathrm{rv}(-a)$. (Habe $v_{\mathrm{RV}}(\xi) = v_{\mathrm{RV}}(-\xi)$)

Bemerkung 4.6. *Wenn* $v_{\mathrm{RV}}(\xi_1) < v_{\mathrm{RV}}(\xi_2)$, *dann* $\xi_1 + \xi_2 = \xi_1$.
Wenn $v_{\mathrm{RV}}(\xi_1) = v_{\mathrm{RV}}(\xi_2)$ *aber* $\xi_1 \neq -\xi_2$*: Für Repräsentanten* a_i *habe* $v(a_1 + a_2) = v(a_1)$, *also ist* $\xi_1 + \xi_2$ *wohldefiniert.*
Wenn $\xi_1 = -\xi_2$*:* $v(a_1 + a_2) > v(a_1)$*; für alle* $a \in K$ *mit* $v(a) > v(a_1)$ *gibt es Repräsentanten* a_i *mit* $a_1 + a_2 = a$. *Also ist* $\xi_1 + \xi_2 \approx \xi_3 \iff v_{\mathrm{RV}}(\xi_3) > v_{\mathrm{RV}}(\xi_1)$.

Anders ausgedrückt: $\mathrm{rv}(a_1) + \mathrm{rv}(a_2)$ *ist wohldef* $\iff v(a_1 + a_2) = \min\{v(a_1), v(a_2)\}$. *(Und das gleiche geht auch für längere Summen.)*

Lemma 4.7. *Die* L_{vf}*-defbaren und die* L_{RV}*-defbaren Teilmengen von* K^n *sind die gleichen.*

Beweis. „L_{vf}-defbar $\Rightarrow$ L_{RV}-defbar“: $\mathrm{rv}(x) = \mathrm{rv}(1) \iff x \in 1 + \mathcal{M}$, also $\mathcal{M}$ defbar, also $\mathcal{O}$ defbar.

„L_{RV}-defbar $\Rightarrow$ L_{vf}-defbar“: klar, da $1 + \mathcal{M}$ L_{vf}-defbar. □

In dieser Sprache kann man die Menge der Quadrate in K (falls $\mathrm{char}\, k \neq 2$) ohne K-Quantoren definieren: $\{x \mid \exists(\xi \in \mathrm{RV})\ \mathrm{rv}(x) = \xi^2\}$

• Falls $x = y^2$, dann ist auch $\mathrm{rv}(x) = \mathrm{rv}(y)^2$.

• Ist umgekehrt $\mathrm{rv}(x) = \mathrm{rv}(y)^2$, so ist $x' := y^2$ ein Quadrat mit $\mathrm{rv}(x') = \mathrm{rv}(x)$. Ob x ein Quadrat ist, hängt nur von $\mathrm{rv}(x)$ ab, also ist auch x ein Quadrat.

2. Das QE-Theorem

Definition 4.8. *In der Sprache L_{RV}: Sei $T_{\mathrm{Hen(p)}}$ die Theorie der henselschen Körper mit* $\operatorname{char} K = p$*; sei $T_{\mathrm{Hen(p,q)}}$ die Theorie der henselschen Körper mit* $\operatorname{char} K = p$ *und* $\operatorname{char} k = q$*.*

Bemerkung 4.9. *Nur $p = q$ oder $p = 0$ sind möglich.*

Jetzt können wir das Theorem formulieren.

Theorem 4.10. *Sei $\phi(\underline{u})$ eine L_{RV}-Formel. Dann gibt es eine L_{RV}-Formel $\psi(\underline{u})$, die nur Quantoren über* RV *hat („*VF***-quantorenfrei***"), so dass $T_{\mathrm{Hen(0,0)}} \vdash \forall \underline{u}\,(\phi(\underline{u}) \leftrightarrow \psi(\underline{u}))$.*

Es gibt eine Variante des Theorems für $T_{\mathrm{Hen(0)}}$, aber die ist technisch komplizierter. Beispiel-Problem: Die Quadrate falls $\operatorname{char} k = 2$: Da muss man mehrere Leitterme betrachten. Brauche entsprechende Verallgemeinerungen von RV in der Sprache.

Trotzdem haben wir auch so schon „QE für fast alle Charakteristiken":

Korollar 4.11. *Sei $\phi(\underline{u})$ eine L_{RV}-Formel. Dann gibt es ein p_0 und eine* VF*-quantorenfreie L_{RV}-Formel $\psi(\underline{u})$, so dass für alle Henselschen Körper K mit* $\operatorname{char} k \geq p_0$ *gilt: $\phi(K) = \psi(K)$.*

Beweis. $T_{\mathrm{Hen(0,0)}} = \{K$ henselsch, $\operatorname{char} k \neq p$ für alle $p\}$. Zu einem gegebenen ϕ finde ψ mit 4.10. Nach Kompaktheit folgt $T_{\mathrm{Hen(0,0)}} \vdash \forall \underline{u}\,(\phi(\underline{u}) \leftrightarrow \psi(\underline{u}))$ schon aus einer endlichen Teilmenge von $T_{\mathrm{Hen(0,0)}}$; muss also nur endlich viele Charakteristiken ausschließen. □

Im Beispiel der Quadrate muss man nur $\operatorname{char} k = 2$ ausschließen.

3. Beweis: Erste Reduktion

Nach 3.59, reicht es, $\phi(\underline{u}) = \exists (y \in K)\, \psi(y, \underline{u})$ mit ψ K-quantorenfrei (und Konjunktion von Atomen und negierten Atomen) zu betrachten. (Damit 3.59 angewandt werden kann, gehen wir kurz über zur Sprache $L^* := L_{\mathrm{RV}} \cup \{$alle VF-qf. defbaren Relationen$\}$.)

Schreibe $\underline{u} = (\underline{z}, \underline{\zeta})$ für $\underline{z}$ K-Variablen und $\underline{\zeta}$ RV-Variablen. Betrachte die K-Terme in ψ genauer. Die kommen nur vor in der Form $f(y, \underline{z}) = 0$ oder $\mathrm{rv}(f(y, \underline{z}))$. Der erste Fall lässt sich auch schreiben als $\mathrm{rv}(f(y, \underline{z})) = 0$; also habe oBdA nur den zweiten Fall.

Seien $\mathrm{rv}(f_i(y,\underline{z}))$ die vorkommenden K-Terme (für $i \leq \ell$). Schreibe ψ um zu:

$$\exists((\eta_i)_{i\leq\ell} \in \mathrm{RV}^\ell)\,\big(\psi' \wedge \bigwedge_i \mathrm{rv}(f_i(y,\underline{z})) = \eta_i\big),$$

wobei ψ' aus ψ entsteht, indem man $\mathrm{rv}(f_i(y,\underline{z}))$ durch η_i ersetzt.

In ψ' kommt kein y mehr vor, also kann man ϕ umschreiben zu

$$\exists((\eta_i)_{i\leq\ell} \in \mathrm{RV}^\ell)\,\big(\psi' \wedge \exists y \bigwedge_i \mathrm{rv}(f_i(y,\underline{z})) = \eta_i\big),$$

Anders ausgedrückt: OBdA hat ϕ die Form

$$(\star) \qquad \exists(y \in K) \bigwedge_i \mathrm{rv}(f_i(y,\underline{z})) = \eta_i$$

wobei $\underline{z}$ K-Variablen sind und η_i RV-Variablen.

(Insbes: $f_i \neq 0 \;\rightsquigarrow\; \mathrm{rv}(f_i) \neq 0 \;\rightsquigarrow\; \exists\eta\, \eta \neq 0 \wedge \mathrm{rv}(f_i) = \eta$.)

4. Nachtrag: Fortsetzung von Bewertungen

Proposition 4.12. *Ist K bew. Kp. und $L \supset K$ eine Körpererweiterung, so lässt sich die Bewertung von K auf L fortsetzen.*

Beweis. Wir konstruieren Bew-Ring $\mathcal{O}_L \subset L$ mit Quot-Körper L und $\mathcal{O}_K \subset \mathcal{O}_L$ und $\mathcal{M}_K \subset \mathcal{M}_L$. Dann fertig:
Es reicht zu zeigen: $K \cap \mathcal{O}_L = \mathcal{O}_K$.
Habe $x \in K \cap \mathcal{O}_L \Rightarrow \frac{1}{x} \notin \mathcal{M}_L \supset \mathcal{M}_K \Rightarrow x \notin \mathcal{O}_K$.

Wende Zornsches Lemma an auf Paare (I,R) mit $I \subsetneq R \subset L$ (R Ring, I Ideal) und Halbordnung $(I,R) \leq (I',R') \iff I \subset I', R \subset R'$.

Sei $(\mathcal{M}_L, \mathcal{O}_L)$ maximal. Dann:

- $\mathcal{M}_L$ ist maximales Ideal.
- $\mathcal{O}_L$ ist lokaler Ring. (Sonst lokalisiere.)

Annahme: $\alpha \in L$ aber $\alpha \notin \mathcal{O}_L$, $\alpha^{-1} \notin \mathcal{O}_L$.

Wenn $\mathcal{M}_L$ in $\mathcal{O}_L[\alpha]$ ein echtes Ideal erzeugt, können wir $\mathcal{O}_L$ zu $\mathcal{O}_L[\alpha]$ vergrößern. Also $\sum_{i\leq m} a_i\alpha^i = 1$ für $a_i \in \mathcal{M}_L$. Entsprechend $\sum_{i\leq n} b_i\alpha^{-i} = 1$.

Wir nehmen an, m, n sind minimal. Und OBdA $m \geq n$.

OBdA $b_0 = 0$. Sonst: Ziehe b_0 ab von $\sum_{i\leq n} b_i\alpha^{-i}$ und teile durch $1-b_0$.

$\Rightarrow \alpha^n =$ Polynom in kleineren α-Potenzen.

Widerspruch zu Minimalität von m. □

5. Intermezzo: Newton-Polygone

Sei K beliebiger bewerteter Körper.

Definition 4.13. *Sei $f = \sum a_i x^i \in K[x]$. Betrachte die Punkte $(i, v(a_i)) \in \mathbb{N} \times \Gamma$. Das **Newton-Polygon** ist die konvexe Hülle dieser Punkte. [Bild]*

Lemma 4.14. *Ist $v(x)$ gegeben, so kann man $v(f(x))$ meistens vom Newton-Polygon ablesen: Zeichne eine Gerade L mit Steigung $-v(x)$ ein, so dass sie das NP von unten berührt. Sei λ die y-Koordinate vom Schnitt von L mit der y-Achse. Falls L das NP nur in einem Punkt trifft, ist $v(f(x)) = \lambda$; sonst ist $v(f(x)) \geq \lambda$. [Bild]*

Beweis. Sei $(i, v(a_i))$ Ecke vom NP und L Gerade durch diese Ecke mit Steigung $-v(x)$; dann ist $\lambda = v(a_i x^i)$. Daraus folgt das Lemma. □

Definition 4.15. *Wir sagen, f hat eine **Kollision** bei x falls $v(f(x)) > \min_i v(a_i x^i)$.*

Bemerkung 4.16. *Multiplikation von f mit Faktor a verschiebt das das NP um $v(a)$ nach oben; Substitution $x \mapsto ax$ „kippt“ das NP um $v(a)$. [Bild]*

Lemma 4.17. *Seien $\alpha_1, \ldots, \alpha_n$ die NSt von f, so sortiert dass $v(\alpha_1) \geq v(\alpha_2) \geq \cdots \geq v(\alpha_n)$. Dann ist $-v(\alpha_i)$ die Steigung des Newton-Polygons zwischen $i-1$ und i. [Bild]*

Beweis. OBdA $a_n = 1$; also $v(a_n) = 0$ und $f = \prod_i (x - \alpha_i)$.

Zu zeigen: $v(a_i) \geq \sum_{j=i+1}^{n} v(\alpha_i)$, und Gleichheit falls $v(\alpha_i) > v(\alpha_{i+1})$.

a_i ist (bis auf Vorzeichen) die Summe von allen Produkten von $n - i$ Nullstellen, also ist $v(a_i) \geq$ Minimum von Summe von $n-i$ Nullstellenbewertungen. Das Minimum erhält man mit $v(\alpha_{i+1})+\cdots+v(\alpha_n)$. Wenn $v(\alpha_i) > v(\alpha_{i+1})$ hat jeder andere Summand echt größere Bewertung, also hat dann a_i genau die minimale Bewertung. □

Bemerkung 4.18. *Daraus ergibt sich eine nette geometrische Konstruktion für das NP von Produkten von Polynomen. [Bild]*

Bemerkung 4.19. *Daraus folgt das Eisensteinsche Irreduzibilitäts-Kriterium: $f = x^n + \sum_i a_i x^i$ mit $p \mid a_i$, $p^2 \nmid a_0 \Rightarrow$ NP hat nur ein Segment mit nicht-ganzzahliger Steigung $\Rightarrow$ das NP eines Faktors hätte eine Ecke mit nicht-ganzzahliger y-Koordinate $\Rightarrow$ der Faktor hat Koeffizienten $\notin \mathbb{Q}_p$, also auch $\notin \mathbb{Q}$.*

Eine Eigenschaft von NP, die wir nicht so richtig beweisen aber auch nicht verwenden:

Proposition 4.20. *Ist K henselsch, so lässt sich f schreiben als Produkt von f_i, wobei jedes f_i einem geraden Segment des NP entspricht. (Das NP von f_i ist – bis auf Verschiebung – dieses gerade Segment.)*

BEWEIS. Wir verwenden folgende alternativ-Charakterisierung von Henselschen Körpern: K ist henselsch genau dann, wenn die Fortsetzung der Bewertung auf den algebraischen Abschluss $\tilde{K}$ eindeutig ist.

Zu zeigen ist nur: Ist f irreduzibel, so ist $v(\alpha)$ gleich für alle NSt α von f.

Das folgt daraus, dass $\mathrm{Gal}(\tilde{K}/K)$ transitiv auf den NSt von f operiert aber andererseits die Bewertung erhält (wegen Eindeutigkeit der Bewertung). □

Spezialfall: Segment der Länge 1 entspricht einer NSt von f; diese NSt liegt bereits in K. Das sieht man auch direkt mit Hensels Lemma:

• Kippe und verschiebe NP so, dass das Segment horizontal ist und bei y-Koordinate 0. Anders ausgedrückt: OBdA $v_{\mathrm{gauss}}(f) = 0$ und $\mathrm{res}(f) = x^m \cdot (\mathrm{res}(a_m) + x\,\mathrm{res}(a_{m+1}))$ mit $\mathrm{res}(a_m), \mathrm{res}(a_{m+1}) \neq 0$; und wir suchen NSt α mit $v(\alpha) = 0$.

• $\mathrm{res}(f)$ hat einfache NSt bei $\mathrm{res}(-\frac{a_m}{a_{m+1}})$; also liftet das zur gesuchten NSt von f.

Hensels Lemma sagt noch ein kleines bisschen mehr: Annahme, das NP hat ein horizontales Segment der Länge 1 bei y-Koordinate 0. Ist $b \in K$ mit $v(b) = 0$ und $v(f(b)) > 0$ (d.h.: f hat Kollision bei b „am“ horizontalen Segment), dann hat f eine NSt. α mit $v(b - \alpha) > 0$.

Durch Verschieben und kippen des NP kriegt man eine entsprechende Aussage für Kollisionen an beliebigen Segmenten der Länge 1. Bei Segmenten der Länge > 1 hat, können wir i.A. keine NSt erwarten (evtl. hätte die Nst eine Bewertung, die gar nicht in Γ liegt). Aber wir haben:

Proposition 4.21. *Sei f gegeben. Die Menge der b, so dass f eine Kollision bei b hat, ist eine Vereinigung von Bällen der Form $B(\alpha, > v(\alpha)) = \mathrm{rv}^{-1}(\mathrm{rv}(\alpha))$, wobei:*

- *Das NP hat ein Segment $(\mu, v(a_\mu))$—$(\nu, v(a_\nu))$ mit Steigung $-v(\alpha)$.*
- *$\alpha \neq 0$ ist eine Nullstelle der ℓ-ten Ableitung von f für ein ℓ mit $0 \leq \ell < \nu - \mu$.*

(Aber nicht alle solche Nullstellen α müssen einen Kollisionsball geben.)

BEWEIS. Vorbemerkung: f hat keine Kollision bei 0, da nur ein Summand.

Annahme: f hat Kollision bei b. Wenn $\mathrm{rv}(c) = \mathrm{rv}(b)$, dann ist auch $\mathrm{rv}(a_i c^i) = \mathrm{rv}(a_i b^i)$; daraus folgt: Kollision bei $c \iff$ Kollision bei b. Bleibt, eine Ableitungsnullstelle im Ball $B(b, > v(b))$ zu finden.

OBdA ist das NP-Segment wieder waagerecht (also $v(b) = 0$) und $v_{\mathrm{gauss}}(f) = 0$.

Betrachte $\mathrm{res}(f) = x^\mu g(x)$, wobei $g(x)$ Grad $\nu - \mu$ hat. Das hat eine NSt bei $\mathrm{res}(b) \neq 0$ mit Vielfachheit höchstens $\nu - \mu$.

Wähle ℓ so groß, dass $(x^\mu g)^{(\ell)}$ einfache NSt bei $\mathrm{res}(b)$ hat. Wende darauf Hensel an. Erhalte so NSt α von $f^{(\ell)}$ mit $\mathrm{res}\,\alpha = \mathrm{res}(b)$. □

6. Proof to QE

6.1. Computing $\mathrm{rv}(f(x))$ by shifting. Let $f = \sum_i a_i x^i$ be a polynomial. We would like to compute $\mathrm{rv}(f(x))$ from $\mathrm{rv}(x)$. (Then in $(\star)$, the quantifier over K could be replaced by a quantifier over RV). This is possible if and only if $v(f(x)) = \min_i v(a_i x^i)$, i.e., the collisions are the problem. The following Prop. tells us that by considering finitely many translates of f, we can get rid of collisions.

We say that α is a **zero of a derivative** of f if there exists an $i < \deg f$ such that $f^{(i)}(\alpha) = 0$; $i = 0$ is allowed.

Proposition 4.22. *For every f and x, there exists a zero α of a derivative of f such that the following holds. Write $f(x) = \sum a_i(x-\alpha)^i$. Then $v(f(x)) = \min_i\{v(a_i(x-\alpha)^i\}$. In particular, $\mathrm{rv}(f(x)) = \sum \mathrm{rv}(a_i)\,\mathrm{rv}(x-\alpha)^i$.*

BEWEIS. Choose α to be a zero of a derivative of f which is as close as possible to x (i.e., $v(\alpha - x)$ maximal). Without loss, $\alpha = 0$. By 4.21, if f has a collision at x, then we find a zero β of a derivative of f with $\mathrm{rv}(\beta) = \mathrm{rv}(x)$, i.e., $v(\beta - x) > v(\alpha - x)$. Contradiction. □

We already saw that in certain cases, a collision yields a zero of f. If not only f itself has a collision but also a bunch of translates, then we can always find a zero (under some assumptions).

By a **strict derivative** of f, we mean a derivative $\neq f$.

Proposition 4.23. *Suppose that f has no common zero with any of its strict derivatives, and let $\eta \in \mathrm{RV}^\times$ be given. Then f has a zero in $\mathrm{rv}^{-1}(\eta)$ iff there exists an $x \in \mathrm{rv}^{-1}(\eta)$ such f has a collision at x and moreover, for all zeros α of strict derivatives of f, we have the following. Write $f(x) = \sum a_i(x-\alpha)^i$. Then $v(f(x)) > \min_i\{v(a_i(x-\alpha)^i\}$.*

Beweis. $\Rightarrow$: If f has a zero at $x \in \mathrm{rv}^{-1}(\eta)$, then $v(f(x)) > \min_i\{v(a_i(x-\alpha)^i\}$ for any $\alpha \neq x$. Since f has no common zero with any of its strict derivatives, taking for α the zeros of the strict derivatives is ok.

$\Leftarrow$: Since f has a collision at x, there exists a zero of f or of a derivative inside $\mathrm{rv}^{-1}(\eta)$. If there is a zero of f, we are done. Otherwise, let b be a zero of a derivative closest to x. Since we have a collision at x after shifting by b, there is a zero b' of g or of a derivative with $v(b'-x) > v(b-x)$, either contradicting the assumption, or b' is a zero of f itself, which is also fine. □

6.2. The degree 1 case. Recall: We want to eliminate the quantifier of

$$(\star) \qquad \exists(x \in K) \bigwedge_i \mathrm{rv}(f_i(x, \underline{z})) = \eta_i$$

where $\underline{z}$ are K-variables and the η_i are RV-variables. (More precisely, we want to show that it is equivalent to a formula without K-quantifiers.)

We think of f_i as a polynomial in x, with coefficients in $\mathbb{Z}[\underline{z}]$. As for QE in alg. closed fields, we can assume that the leading coefficient of each f_i (which depends on $\underline{z}$) is non-zero.

Lemma 4.24. *If $\deg f_i \leq 1$ for all i, then the quantifier can be eliminated.*

Beweis. • Without loss, no $\deg f_i = 0$.

• Write $f_i(x) = a_i(x+b_i)$. We have $\mathrm{rv}(f_i(x)) = \eta_i$ iff $\mathrm{rv}(x+b_i) = \frac{\eta_i}{\mathrm{rv}(a_i)}$. In other words, without loss $a_i = 1$.

• Each "$\mathrm{rv}(x+b_i) = \eta_i$" defines a ball (namely $\mathrm{rv}^{-1}(\eta_i) - b_i$). The question is whether the intersection of all those balls is non-empty. Since the intersection of two balls is either empty or the smaller one of the two balls, it suffices to check that for each pair of balls, we have

$$\mathrm{rv}^{-1}(\eta_i) - b_i \cap \mathrm{rv}^{-1}(\eta_j) - b_j \neq \emptyset.$$

Claim: This is equivalent to

$$\eta_i + \mathrm{rv}(b_j - b_i) \approx \eta_j$$

Proof of the claim:

• $\Rightarrow$ is clear: if x is in the intersection, then we get the $\approx$-formula by applying rv to $(x + b_i) + (b_j - b_i) = (x + b_j)$.

• $\Leftarrow$: The $\approx$-formula implies the existence of y, y' with $\mathrm{rv}(y) = \eta_i$, $\mathrm{rv}(y') = \eta_j$ and $\mathrm{rv}(y' - y) = \mathrm{rv}(b_j - b_i)$. Do finish, we need to modify these such that $y' - y = b_j - b_i$. This modification is possible iff $v(b_j - b_i) \geq \min\{v(y), v(y')\}$; but this inequality is also implied by the $\approx$-formula. □

6.3. Applying 4.22. • Let $f(x) = \sum a_j x^j$ be given. (Recall: $a_j \in \mathbb{Z}[\underline{z}]$.)

• Define a'_j by $f(x + b) = \sum a'_j x^k$. We have $a'_j \in \mathbb{Z}[\underline{z}, b]$.

• Thus $f(x) = \sum a'_j (x - b)^j$.

• Now let ϕ_f be the formula saying that we have no collision at x when we use this translated version to compute $\mathrm{rv}(f(x))\ldots$ and that η is the result. More precisely:

$$\phi_f(x, b, \eta, \underline{z}) = \quad \sum_j \mathrm{rv}(a'_j)\,\mathrm{rv}(x - b)^j = \eta$$

• Now we can rewrite "$\mathrm{rv}(f(x, \underline{z})) = \eta$" as follows: $\exists b\, \phi_f(x, b, \eta, \underline{z})$.

This might look stupid, since it only introduced an additional quantifier, but:

• We can add "$\wedge(f(b) = 0 \vee f'(b) = 0 \vee \cdots \vee f^{(\deg f - 1)}(b) = 0)$" to the formula, which turns the quantifier into a finite one.

• Note that x now only appears linearly.

We now plug this into $(\star)$, but we write it down slightly differently: different b's for the different derivatives of f.

$$\exists (b_{ij})_{ij} \left(\bigwedge_{ij} f_i^{(j)}(b_{ij}) = 0 \wedge \exists x \bigwedge_i \bigvee_j \phi_{f_i}(x, b_{ij}, \eta_i, \underline{z}) \right)$$

Now the $\exists x$ can be eliminated by 4.24. (Recall that we can move the other RV-stuff out of the $\exists x$ quantifier.)

We are left to eliminate the quantifiers over the b_{ij}. We will do this one at a time. It seems that we didn't gain much, but we did. The formula we have to eliminate the quantifier from now has the form

$$(\star') \qquad \exists (x \in K)\, g(x) = 0 \wedge \bigwedge_i \mathrm{rv}(f_i(x, \underline{z})) = \eta_i$$

We don't know anything about the new f_i (since they can be the result of the elimination of the inner $\exists b_{ij}$; in particular, e.g. we know nothing about the degrees of the f_i). But we have this new $g(x) = 0$, and here, we indeed know that $\deg g$ is at most the maximum of the degrees of the old f_i. (This will be useful for induction.)

Now we prove that this quantifier can be eliminated by induction on the degree of g. (Note that the case $\deg g = 1$ is trivial.)

6.4. Remainder of proof. In the formula, replacing f_i by $f_i + ag$ does not change anything. Also, we can replace $\mathrm{rv}(f_i(x, \underline{z})) = \eta_i$ by $\mathrm{rv}(bf_i(x, \underline{z})) = \mathrm{rv}(b)\eta_i$. So using the Euclidean algorithm, we can reduce to the case where $\deg f_i < \deg g$ for all i.

Now apply 4.22 again, exactly as before (but only to the polynomials f_i). We get:

$$\exists (b_{ij})_{ij} \left(\bigwedge_{ij} f_i^{(j)}(b_{ij}) = 0 \wedge \exists x\, g(x) = 0 \wedge \bigwedge_i \bigvee_j \phi_{f_i}(x, b_{ij}, \eta_i) \right)$$

Since there is this $g(x) = 0$ left, this time it is not so clear how to eliminate the $\exists x$ quantifer. But suppose we can eliminate it. Then we are again in the situation $(\star')$ (for each $\exists b_{ij}$), but with strictly smaller $\deg g$ (since $\deg f_i < \deg g$). Thus once we know how to eliminate the above $\exists x$ quantifier, we are done by induction.

So it remains to eliminate the $\exists x$ quantifier. Again, we pull out all the RV stuff, and we are left with a formula of the form

$$\exists (x \in K)\, g(x) = 0 \wedge \bigwedge_i \mathrm{rv}(x - z_i) = \eta_i$$

Using again that the intersection of the balls is the smallest of the balls (and that whether the intersection is non-empty is definable), we can consider each ball $\mathrm{rv}(x - z_i) = \eta_i$ separately, i.e. without loss the formula is

$$\exists(x \in K)\, g(x) = 0 \wedge \mathrm{rv}(x - z) = \eta$$

By translating with z, we may reduce to

$$(\star'') \qquad \exists(x \in K)\, g(x) = 0 \wedge \mathrm{rv}(x) = \eta$$

Our goal is now to apply 4.23. (The case $\eta = 0$ is trivial.) For this we need that g and $g^{(\ell)}$ have no common zero. Assume that they do have a common factor. Then we can write $g = f \cdot h$, where h is the gcd of g and $g^{(\ell)}$. Note that we can obtain f and h without quantifiers. Now $(\star'')$ is equivalent to $(\exists(x \in K)\, f(x) = 0 \wedge \mathrm{rv}(x) = \eta) \vee (\exists(x \in K)\, h(x) = 0 \wedge \mathrm{rv}(x) = \eta)$. Since $\deg f, \deg h < \deg g$, we can apply induction.

Now let us turn the right hand side of 4.23 into a formula.

Set

$$\psi(x, b, \underline{z}) := \neg\exists(\eta \in \mathrm{RV})\, \phi_g(x, b, \eta, \underline{z})$$

This says: if we use the version of g translated by b to compute $\mathrm{rv}(g(x))$, then we have a collision.

Let $\chi((y_i)_i, \underline{z})$ be a formula saying that each y_i is a zero of a strict derivative of g ("strict" meaning: not g itself), and each zero of a strict derivative appears as one of the y_i:

$$\chi((y_i)_i, \underline{z}) = \left(\bigwedge_i \bigvee_{\ell \geq 1} g^{(\ell)}(y_i) = 0 \right) \wedge \bigwedge_{\ell \geq 1} \neg\exists y \left(g^{(\ell)}(y) = 0 \wedge \bigwedge_i y \neq y_i \right)$$

(. . . It suffices to take $(\deg g)^2$ variables y_i.)

Then by the 4.23, $(\star'')$ is equivalent to

$$\exists(y_i)_i\, \chi((y_i)_i, \underline{z}) \wedge \exists x \left(\psi(x, 0, \underline{z}) \wedge \left(\bigwedge_i \psi(x, y_i, \underline{z}) \right) \wedge \mathrm{rv}(x) = \eta \right)$$

It looks like we only introduced a whole bunch of additional quantifiers, but:

• Inside the $\exists y$ in χ, we have $g^{(\ell)}(y) = 0$, which has degree less than $\deg g$, so we can apply induction.

• In the formula inside the $\exists x$ quantifier, x only appears in the form $\mathrm{rv}(x - y_i)$, so this quantifier can be eliminated by the degree 1 case.

• Inside $\exists y_i$, we have $\bigvee_{\ell \geq 1} g^{(\ell)}(y_i) = 0$; the disjunction can be pulled to the outside, and then we again have a polynomial $g^{(\ell)}(y_i) = 0$ of degree less than $\deg g$, thus induction works.

7. QE in the Denef-Pas langugage

In our proof, concerning the part of the language on the RV sort, we used that we have $+ \approx$ and $\cdot$, but we didn't use that there is nothing else, so if we want, we can add any additional language. It is rather unclear how formulas with quantifiers over RV look like, so the following is useful:

• Without loss, we have the sorts Γ and k.

• We add an **angular component** map $\mathrm{ac}\colon K^\times \to k^\times$ do the language: $\mathrm{ac}(x)$ is the "first non-zero digit of x". (And we set $\mathrm{ac}(0) := 0$.) Since the first non-zero digit is determined by $\mathrm{rv}(x)$, we can write $\mathrm{ac} = \mathrm{ac}_{\mathrm{RV}} \circ \mathrm{rv}$; thus in reality, it suffices to add the map $\mathrm{ac}_{\mathrm{RV}}$ to the language, which is allowed.

• Formally (for arbitrary valued field) an angular component map is any group homomorphism $\mathrm{ac}_{\mathrm{RV}} \circ \mathrm{rv}$ such that $\mathrm{ac}_{\mathrm{RV}}$ is the identity on $k^\times$. (Recall that we can identity $k^\times$ with $\{\xi \in \mathrm{RV} \mid v_{\mathrm{RV}}(\xi) = 0\}$). In other words, it's a splitting of the sequence $k^\times \hookrightarrow \mathrm{RV}^\times \twoheadrightarrow \Gamma$.

• Once we have ac in our language, we can replace RV and rv by $k, \Gamma, \mathrm{ac}, v$ (with the usual language on k, Γ). One easily checks that the $+$, $\cdot$ on RV are definable in that language. If one is not used to the RV-sort, this new language is more intuitive.

Definition 4.25. *Let L_{DP} be this new language. (This is also called the **Denef-Pas language**....)*

Note what (the original) VF-qe means: any formula $\phi(\underline{x}, \underline{\xi})$ with $\underline{x}$ VF-variables and $\underline{\xi}$ RV-variables, is equivalent to a formula of the form $\chi(\mathrm{rv}(f_i(\underline{x})), \ldots, \underline{\xi})$, where χ is a formula living purely on the RV-sort. (If we have $f_i = f_j$ in our formula, replace this by $\mathrm{rv}(f_i - f_j) = 0$.)

In L_{DP}, we get: any formula is of the form $\chi(\mathrm{ac}(f_i(\underline{x})), \ldots, v(g_i(\underline{x})), \ldots, \underline{u}, \underline{\lambda})$ ($\underline{u}$ from k, $\underline{\lambda}$ from Γ), where χ lives only in the sorts k and Γ.

... but there is no connection between k and Γ in L_{DP}. From this we can deduce:

Korollar 4.26. *Every formula $\phi(\underline{x}, \underline{u}, \underline{\lambda})$ is equivalent to a finite disjoint union (more precisely: a disjunction...) of formulas of the form $\chi(\mathrm{ac}(f_i(\underline{x})), \ldots, \underline{u}) \wedge \chi'(v(f_i(\underline{x})), \ldots, \underline{\lambda})$, where χ lives only on k and χ' only on Γ.*

Now we can try to also eliminate the quantifiers of χ and χ'.

Concerning χ: if $k = \mathbb{Q}$ for example, then there is no chance. If k is alg. closed, then we proved qe.

Concerning χ': There are two important cases:

• Γ is divisible (i.e., elementarily equivalent to $\mathbb{Q}$); this is the case when K is alg. closed. In that case, we have complete quantifier elimination.

• $\Gamma = \mathbb{Z}$. In that case, we don't have qe. E.g. $\exists x\, nx = y$ is not qf-definable for any fixed $n \geq 2$; but we get qe after adding these sets to the language:

Proposition 4.27. *$\mathbb{Z}$ has qe in the Presburger language $L_{\mathrm{Pres}} = \{0, 1, +, -, <, (\equiv_n)_n\}$, where $x \equiv_n y$ iff $x - y \in n\mathbb{Z}$.*

One deduces: any definable set is a finite disjoint union of sets which are polyhedra intersected with congruence conditions; in other words, positive boolean combintations of $f_i(\underline{x}) \geq 0$ and $g_j(\underline{x}) \equiv_n 0$ for affine linear f_i, g_i.

This implies:

Proposition 4.28. *For any L_{Pres}-definable function $f\colon X \to \mathbb{Z}$ with $X \subset \mathbb{Z}^n$ there exists a partition of X into finitely many definable sets A such that each $f\restriction_A$ is affine linear ... but with coefficients from $\mathbb{Q}$.*

Example: $f\colon 2\mathbb{Z} \to \mathbb{Z}$, defined by $f(x) = y \iff y + y = x$.

8. QE in $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$

Let's use L_{DP} with L_{Pres} on Γ; call this L_{DPP}.

We proved: For every formula ϕ, there exists a VF-qf formula ψ such that the theory of Henselian fields of char $(0, 0)$ implies equivalence. By compactness, a finite subset of the theory suffices, thus we have:

Korollar 4.29. *For every L-formula ϕ there exists a formula ψ with quantifiers only over the residue field such that in every Henselian field of sufficiently large characteristic (depending on ϕ) and with value group $\Gamma \equiv \mathbb{Z}$, ϕ and ψ define the same set.*

In particular, this works in $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$. In particular, by taking for ϕ a sentence we get:

Korollar 4.30. *(Ax-Kochen, Eršov) For any first-order sentence ϕ, there exists an N such that ϕ holds in $\mathbb{Q}_p$ iff ϕ holds in $\mathbb{F}_p((t))$.*

BEWEIS. For p sufficiently big, ϕ is equivalent to a formula ψ of the form given in 4.26. Since there are no variables (and in particular no valued field variables), all polynomials f_i are constant, i.e. we have $v(n)$ and/or $\mathrm{ac}(n)$ for some integers n. For $p > n$, we have $v(n) = 0$ and $\mathrm{ac}(n) = n \in k$, so without loss, these f_i don't appear at all. Now ψ only lives on the residue field and the value group. Since $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ have the same residue field and the same value group, ψ holds in one of them iff it holds in the other one. □

In $\mathbb{Q}_p$, since the residue field is finite, we can replace any formula by a formula without quantifiers which explicitely lists all elements. Thus we proved:

Korollar 4.31. *For every L-formula ϕ there exists an N such that for every $p > N$, ϕ is equivalent to a qf-formula on $\mathbb{Q}_p$.*

But note that this is *not* uniform: ϕ depends on p.

In a slightly different language, we can get the last corollary for all p, and in a more complicated language also uniform in p.

KAPITEL 5

Back to Poincaré series

1. The original goal

Recall the original motivation of the lecture:

- We have a polynomial $f \in \mathbb{Z}[\underline{x}]$ (where $\underline{x}$ is an n-tuple).
- We set

$$\begin{aligned} \tilde{Y}_r &:= Z_f(\mathbb{Z}/p^r\mathbb{Z}) \\ Y_r &:= \{\underline{a} \in (\mathbb{Z}/p^r\mathbb{Z})^n \mid \exists \underline{b} \in \mathbb{Z}_p^n \, f(\underline{b}) = 0, \underline{b} \mod p^r = \underline{a}\} \\ \tilde{N}_r &:= \#\tilde{Y}_r \qquad N_r := \#Y_r \end{aligned}$$

- We want to prove that the Poincaré series

$$\tilde{P}_f(t) := \sum_{r \in \mathbb{N}} \tilde{N}_r t^r \in \mathbb{Q}[[t]]$$

and

$$P_f(t) := \sum_{r \in \mathbb{N}} N_r t^r \in \mathbb{Q}[[t]]$$

are rational, i.e., in $\mathbb{Q}(t)$. And we'd like to understand how they depend on p.

We'll do everything only for p big enough. Here is the final result.

Theorem 5.1. *For every $f \in \mathbb{Z}[\underline{x}]$, there exists an $N \in \mathbb{N}$ such that for $p > N$, $P_f(t)$ and $\tilde{P}_f(t)$ are rational functions in t, depending on p as follows. There exist finitely many L_{ring}-formulas ψ_i and rational functions $g_i \in \mathbb{Q}(p,t)$ such that for all $p \geq N$, $P_f(t) = \sum_i \#\psi_i(\mathbb{F}_p) \cdot g_i$.*

First, we rewrite and generalize the problem:

- Let X_r, $\tilde{X}_r$ be the preimages of Y_r, $\tilde{Y}_r$ in $\mathbb{Z}_p^n$.
- On $\mathbb{Q}_p$, we have a natural measure μ (coming from the Haar measure on $\mathbb{Z}_p$ w.r.t. addition): $\mu(B(a, \geq r)) = p^{-r}$; this induces a measure on the product $\mathbb{Q}_p^n$: with $\mu(B(\underline{a}, \geq r)) = p^{-nr}$.

• Thus $N_r = \mu(X_r) \cdot p^{nr}$ and (and similarly for $\tilde{N}_r$)

• Thus $P_f(t) := \sum_{r\in\mathbb{N}} \mu(X_r)(p^n t)^r = Q(p^n t)$, where $Q(t) = \sum_{r\in\mathbb{N}} \mu(X_r)t^r$.

• Note that the family of definable sets X_r is defined by a single formula with parameter $r \in \mathbb{N} \subset \Gamma$. We will show more generally:

Theorem 5.2. *For a family of definable set X_r ($r \in \mathbb{N}$), the series $Q(t) = \sum_{r\in\mathbb{N}} \mu(X_r)t^r$ is of the same form as in 5.1.*

2. Uniform p-adic integration

We will compute the measure of a definable set coordinate by coordinate. For this, we also need to be able to integrate. Note that the functions and integrals are defined on $\mathbb{Q}_p$ (or on some other sorts of $\mathbb{Q}_p$) but take values in $\mathbb{Q}$ (which is nothing in our structure).

The plan is as follows.

• For each definable set S (in arbitrary sorts), we will define a class D_S of functions from S to $\mathbb{Q}$.

• If $f \in D_{S\times\mathbb{Z}_p}$ and f is bounded, then for every $s \in S$, the integral $\int_{\mathbb{Z}_p} f(s,x)dx$ exists and is also bounded (as a function in s). We will show that $\int_{\mathbb{Z}_p} f(s,x)dx \in D_S$.

Using this, we deduce our goal as follows: Let X_r be given as above. Define $f\colon \mathbb{N}\times\mathbb{Z}_p^n \to \mathbb{Z}$ by: $f(r,\underline{a}) = 1$ iff $\underline{a} \in X_r$ and $= 0$ otherwise. Then $\mu(X_r) = \int_{\mathbb{Z}_p^n} f(r,\underline{x})d\underline{x}$. We will have $f \in D_{\mathbb{N}\times\mathbb{Z}_p^n}$, so after integrating coordinate by coordinate, we will get that $r \mapsto \mu(X_r)$ is in $D_{\mathbb{N}}$.

Since we want to do everything uniformly in p, we work with formulas in L_{DPP}, and we formally consider the functions in D_S as depending on p. So if S is given by a formula ϕ, then we will have functions on $\bigcup_{p\in\mathbb{P}} \phi(\mathbb{Q}_p)$. However, to simplify the notation, I will write "functions on S", making the p only implicit.

Some functions we will need:

(1) The function $f\colon \mathbb{N}\times\mathbb{Z}_p^n \to \Gamma$ from above. More generally, we will put arbitrary definable functions from S to Γ into D_S.
(2) The integral of the characteristic function of $\{x \mid v(x) \geq r\}$ is p^r. In a fixed $\mathbb{Q}_p$, this is just a value, but since we do it uniformly in p, we need to have the function p^r in D_S. Similarly, the measure of the set $\{x \in \mathbb{Z}_p \mid \mathrm{ac}(x) = 1\}$ is

$p^{-1} + p^{-2} + p^{-3} + \cdots = \frac{1}{p(1-p)}$, so let us simply put all rational functions in p into D_S.

(3) A variant of the above: for a definable function $\beta\colon S \to \Gamma$, we can also measure the set (depending on s) $\{x \mid v(x) \geq \beta(s)\}$, thus in D_S, we need the function $s \mapsto p^{\beta(s)}$.

(4) Suppose that X is a definable subset of $S \times \mathbb{F}_p^\ell$ and define $f\colon S \times \mathbb{Z}_p^\ell \to \mathbb{Z}$ by $f(s, \underline{a}) = 1$ iff $(s, \mathrm{res}(\underline{a})) \in X$ and 0 otherwise. We also need to have $s \mapsto \int_{\mathbb{Z}_p^\ell} f(s, \underline{x}) d\underline{x}$ in D_S. At a given s, this integral is just $p^{-1}\#\{\underline{b} \in \mathbb{F}_p^\ell \mid (s, \underline{b}) \in X\}$. In other words, we have to count points over the residue field. In each fixed $\mathbb{Q}_p$, this is easy, but uniformly, we don't know. (The formula for X might still have quantifiers.) Thus we simply put all functions of the form $s \mapsto \#\{\underline{b} \in k^\ell \mid (s, \underline{b}) \in X\}$ into D_S.

Definition 5.3. *Let D_ϕ be the $\mathbb{Q}$-algebra of functions from $\bigcup_{p \in \mathbb{P}} \phi(\mathbb{Q}_p)$ to $\mathbb{Q}$ generated by (1)–(4) above.*

3. Deducing rationality

We need the following lemma on generalized geometric series:

Lemma 5.4. *For any polynomial $f(x)$ (with coefficients from any ring R), the power series $\sum_{\lambda \in \mathbb{N}} f(\lambda) t^\lambda$ is a rational function in t (i.e. lies in $R(t)$).*

Beweis. It suffices to consider $\sum_{\lambda \in \mathbb{N}} \lambda^i t^\lambda$ for each fixed i.

For $i = 0$, this is just a usual geometric series. Otherwise: exercise. (For example, note that $(\sum_\lambda t^\lambda)^2 = \sum_\lambda (\lambda + 1) t^\lambda$ or so.) □

Proof of 5.2. By the previous arguments, we have to show that $\sum_{r \in \mathbb{N}} f(r) t^r$ is rational for $f \in D_{\mathbb{N}}$.

• Any factor in $f(r)$ which does not depend on r (but maybe on p) may be pulled out of the sum. So the question is: how can $f(r)$ depend on r?

• We have functions counting the points in the residue field. By 4.26, after a finite partition of $\mathbb{N}$ into definable sets A, each counting-points-function is constant on A. We split the series into a corresponding finite sum of series and treat each summand separately. (Now our series are of the form $\sum_{r \in A} f(r) t^r$ for $A \subset \mathbb{N}$ definable.) Now the counting point functions are factors in front of the series, which is ok.

• Other functions depending on r are of the form $\beta(r)$ or $p^{\beta(r)}$ for $\beta\colon A \to \mathbb{Z}$ definable. Since these β are functions from the value group to itself, by QE we may assume that they are defined using only L_{Pres} on the value group. (In particular, they do not depend on p.) By 4.28, after another cutting of A into finitely many pieces, we may assume that each β is linear.

• Our function f is a sum of products of functions $\beta(r)$ and $p^{\beta(r)}$. Treat each summand separately. Group $p^{\beta(r)} \cdot p^{\beta'(r)}$ to $p^{\beta(r)+\beta'(r)}$. Pull p^{const} out. We get $f(r) = g(r)p^{ar}$, where g is a polynomial, and our series is $\sum_A g(r)(p^a t)^r$.

• By qe again, A is L_{Pres}-definable (and independent of p), and by qe, it is a finite disjoint union of sets of the form $\{r \in \mathbb{Z} \mid M \leq r < N, r \equiv_r a\}$ (with possibly $N = \infty$). If N is finite, then the series is a polynomial in t and p; otherwise, it can be rewritten in the form

$$\sum_{i=0}^{\infty} g(ci+d)(p^a t)^{ci+d} = (p^a t)^d \sum_{i=0}^{\infty} g(ci+d)(p^{ac}t^d)^i.$$

Now we can apply 5.4, which gives a rational function in $p^{ac}t^d$. □

4. Integrating one variable

Let $f \in D_{S\times\mathbb{Z}_p}$ be given. We want to determine $s \mapsto \int_{\mathbb{Z}_p} f(s,x)dx$.

We consider f as a function from $\mathbb{Z}_p \to \mathbb{Z}$ depending on s (and on p); f can be decomposed into a finite sum, and all factors of f which do not depend on x can be pulled out of the integral. After that, f is a product of functions of the form $\beta(x)$, $p^{\beta(x)}$, and $s \mapsto \#\{\underline{b} \in k^\ell \mid (s,\underline{b}) \in X\}$ for some definable $\beta\colon S \times \mathbb{Z}_p \to \mathbb{Z}$ and $X \subset S \times \mathbb{F}_p^\ell$.

The graph $\{(x,\lambda) \in K \times \Gamma \mid \beta(x) = \lambda\}$ of a function β is a disjoint union of sets defined by formulas of the form

$$\chi(\dots v(f_i(x)), \dots, \lambda) \wedge \chi'(\dots \mathrm{ac}(f_i(x)), \dots),$$

where the parameters from S may also appear in f_i, χ, χ'.

By 4.22, $\mathrm{rv}(f_i(x))$ only depends on $\mathrm{rv}(x-\alpha)$ where α runs through the zeros of derivatives of f_i. Hence we can replace all f_i by linear polynomials of the form $x-\alpha$… well almost: we would need some definable way to get α from s. Let's deal with this problem later. (Note: in the quantifier elimination, we had to be very careful about the coefficients of our polynomials so that we don't introduce new quantifiers. Here, we're happy if the coefficients are any definable functions in s.) So let's

assume now that the graph of each β appearing in f is a finite union of

$$\chi(\dots v(x-\alpha_i),\dots,\lambda)\wedge\chi'(\dots \mathrm{ac}(x-\alpha_i),\dots).$$

In a similar way, we can treat the functions $s\mapsto \#\{\underline{b}\in k^\ell \mid (s,\underline{b})\in X\}$ appearing in f; the result is that there are finitely many α_i such that the dependence of f from x is only via $v(x-\alpha_i)$ and $\mathrm{ac}(x-\alpha_i)$. (But the α_i may depend on s.)

Define a partition of K into definable sets A_i as follows: put x into A_i if $v(x-\alpha_i)$ is maximal. (If there are several equal $v(x-\alpha_i)$, choose e.g. the minimal i.) It suffices to show $\int A_i f dx\in D_S$ separately for each A_i. So fix one.

On A_i, f only depends on $\mathrm{rv}(x-\alpha_i)$ (this value determines all other $\mathrm{rv}(x-\alpha_j)$). Without loss, $\alpha_i=0$. Hence we can assume now that the graph of each β is a finite union of things of the form

$$\chi_\ell(v(x),\lambda)\wedge\chi'_\ell(\mathrm{ac}(x))$$

The set A_i is a ball, with some balls of the form $\mathrm{rv}^{-1}(\xi)$ removed (with $\xi=\mathrm{rv}(\alpha_j)$. Thus if we extend the $f\restriction_{A_i}$ by 0 to the whole of $\mathcal{O}$, it still has the above form, i.e., now we don't have to bother about A_i anymore.

For each ℓ and each $u\in k^\times$, we can compute the integral b_ℓ of the function defined by $\chi_\ell(v(x),\lambda)$ on the set $\{x\in\mathcal{O}\mid \mathrm{ac}(x)=u\}$. This integral doesn't depend on u. The total integral of f is obtained by multiplying b_ℓ by $\#(\chi'\ell(k))$ (where k is the residue field) and then summing over all ℓ. Thus we now only need to consider functions β defined by $\chi(v(x),\lambda)$. (And without loss $u=1$.)

Now the integral becomes a sum over $v(x)$. Write g for the function $\mathbb{N}\to\mathbb{Z}$ such that $f(x)=g(v(x))$. Then

$$\int_{\{x\mid \mathrm{ac}(x)=1\}} f dx = p\cdot\sum_{r\in\mathbb{N}} g(r)\cdot p^r$$

This sum looks exactly as the one in the proof of 5.2, except that t is replaced by p. So the same proof works to get rationality of that series (but we have to check how the result depends on s). Again, we partition the index set $\mathbb{N}$ into subsets A where each β is linear. We get

$$\sum_{\{r\mid M\le r<N, r\equiv_n a\}} h(r)p^{mr+b}$$

where h is a polynomial whose coefficients depend on s, M, N, a, b are constants depending on s and n,m are constants *not* depending on s.

In the same way as before, we reduce to the case

$$\sum_{r\in\mathbb{N}} h(r)p^{mr}$$

The important thing to note here is that m still does not depend on s. (In the substition to get rid of $r \equiv_n a$, we take the n-th power of p^{mr+b}, which is ok.)

Now we apply 5.4 again and obtain a rational function in $p^m \ldots$ and now it's good that m does not depend on s.

5. Epilogue

What we just did was a baby version of motivic integration. To get the "full" version, instead of working with functions on $\bigcup_p \phi(\mathbb{Q}_p)$, one works in an abstract algebra with the generators (1) – (4) with suitable relations. (One difficulty is to find out what "suitable" means.) As a result, one can even "integrate" in Henselian fields of characteristic $(0, 0)$. The result of the integral is an abstract object (an element of our algebra) which does contain some "geometric" information, since there are formulas involved.

A good quick introduction to motivic integraition is given in:
Hales: What is motivic measure?