§ 2 Quantorenelimination in bew. Kp.

Im ganzen Kapitel:

$$\begin{array}{ccc} K & \xrightarrow{v} & \Gamma_K \cup \{\infty\} \\ \cup & & \\ \mathcal{O}_K & \xrightarrow{res} & \overline{K} \\ \cup & & \\ \mathcal{M}_K & & \end{array}$$

$k((t)) \ni \sum_{i=N}^{\infty} a_i t^i \quad a_N \neq 0$

Leitterm $a_N t^N$

a, b haben gleichen Leitterm $\Leftrightarrow v(a) = v(b) < v(a-b)$

§ 2.1 Leitterme

Bem 2.1.1: $1 + \mathcal{M}_K$ ist eine Untergruppe von $\mathcal{O}_K^\times$

Bew: $(1+a)\cdot(1+b) \qquad a, b \in \mathcal{M}_K$

$= 1 + \underbrace{a + b + ab}_{\in \mathcal{M}_K}$

$\frac{1}{1+a} \overset{?}{\in} 1 + \mathcal{M}_K \quad \Leftrightarrow \quad \underbrace{\frac{1}{1+a} - 1}_{\shortparallel} \in \mathcal{M}_K$

$\frac{1-1-a}{1+a} = -\frac{a}{1+a}$ ($v>0$ für a, $v=0$ für $1+a$) $\Big\}\ v>0$ ✓ □

Def 2.1.2: Wir setzen $RV_K^\times := K^\times / (1 + \mathcal{M}_K)$ und $RV_K := RV_K^\times \cup \{0\}$ und schreiben $rv : K \to RV_K$ für die kanonische Abb $K^\times \to RV_K^\times$ fortgesetzt durch $0 \mapsto 0$. Für $a \in K$ nennt man $rv(a)$ den <u>Leitterm</u> von a, und RV_K ist die <u>Leittermstruktur</u> von K. Wir schreiben die Gruppenstruktur auf $RV^\times$ multiplikativ und setzen $0 \cdot \xi = 0$ für $\xi \in RV$.

Bem 2.1.3: Für $a, b \in K$ gilt $rv(a) = rv(b) \Leftrightarrow a = b = 0$ oder $v(a-b) > v(a)$

$\Downarrow$

$v(b) = v((b-a) + a) = v(a)$

Bew: Seien $a, b \in K^\times$.

$v(a-b) > v(a) \Leftrightarrow v\left(\frac{a-b}{a}\right) > 0$

$\Leftrightarrow v\left(1 - \frac{b}{a}\right) > 0 \Leftrightarrow v\left(\frac{b}{a} - 1\right) > 0 \Leftrightarrow \frac{b}{a} - 1 \in \mathcal{M}_K \Leftrightarrow \frac{b}{a} \in 1 + \mathcal{M}_K$ □

Bem: Der Name „RV" kommt von R = Residue field = Restkl-Kp
V = Value group = Wertegruppe

Bsp 2.1.4: Im Fall $K = k((t))$ bilden die Elemente der Form $a \cdot t^N \in K$ (für $a \in k^\times$, $N \in \mathbb{Z}$) ein Repräsentantensystem von $RV^\times$.
Als Gruppen habe $RV^\times \cong k^\times \times \mathbb{Z}$

$$(a_1 \cdot t^{N_1}) \cdot (a_2 \cdot t^{N_2}) = (a_1 \cdot a_2) \cdot t^{N_1+N_2}$$

Bem 2.1.5:
- Die Bewertung $v: K \longrightarrow \Gamma \cup \{\infty\}$ faktorisiert über RV; erhalte so einen Gruppenhomo $v_{RV}: RV \longrightarrow \Gamma \cup \{\infty\}$
- rv induziert einen injektiven Grphomo $\bar{K}^\times \longrightarrow RV^\times$, dessen Bild genau der Kern von $v_{RV}: RV^\times \longrightarrow \Gamma$ ist.

$$\begin{tikzcd}
M_K \arrow[d, phantom, "\cap"] & \\
O_K \arrow[d, two heads] & O_K^\times \arrow[l, phantom, "\supset"] \arrow[d, two heads] \\
\bar{K} & \bar{K}^\times \arrow[l, phantom, "\supset"]
\end{tikzcd}
\qquad
\begin{tikzcd}
1+M_K \arrow[d, phantom, "\cap"] \arrow[drr, bend left] & & \\
O_K^\times \arrow[r, hook] & K^\times \arrow[r, two heads] \arrow[dr, two heads] & \Gamma_K \cong K^\times/O_K^\times \\
& & RV_K^\times \cong K^\times/(1+M_K) \arrow[u, "v_{RV}"'] \\
& & \ker v_{RV} \cong O_K^\times/(1+M_K) = \bar{K}^\times \arrow[u, hook]
\end{tikzcd}$$

Für $a, b \in O_K^\times$: $rc(a) = rc(b)$
$\Leftrightarrow v(a-b) > 0 = v(a)$
$\Leftrightarrow rv(a) = rv(b)$

Notn 2.1.6: Die Abb. $RV \longrightarrow \Gamma \cup \{\infty\}$ wird mit v_{RV} oder v bezeichnet.

Notn 2.1.7:
- Seien $\xi_1, \dots, \xi_n, \zeta \in RV$. Wenn $a_1, \dots, a_n \in K$ existieren mit $rv(a_i) = \xi_i$ $(i = 1, \dots, n)$ und $rv(\sum a_i) = \zeta$, dann schreiben wir $\underline{\xi_1 + \dots + \xi_n \approx \zeta}$. Existiert nur ein ζ mit $\sum \xi_i \approx \zeta$, so sagen wir $\sum \xi_i$ ist <u>wohldefiniert</u> und schreiben $\sum \xi_i = \zeta$
- Für $\xi \in RV$ setzen wir $-\xi := rv(-1) \cdot \xi$

In Bsp. 2.1.4:

$$rv(a_1 t^{N_1}) + rv(a_2 t^{N_2}) \begin{cases} = rv(a_2 t^{N_2}) & N_1 > N_2 \\ = rv(a_1 t^{N_1}) & N_1 < N_2 \\ = rv((a_1 + a_2) \cdot t^{N_1}) & N_1 = N_2,\ a_1 + a_2 \neq 0 \\ \approx rv(a \cdot t^N) \quad a \in k^\times,\ N > N_1 & N_1 = N_2,\ a_1 + a_2 = 0 \end{cases}$$

Lemma 2.1.8: Seien $a_1, \dots, a_n \in K$. Dann ist $rv(a_1)+\dots+rv(a_n)$ wohldefiniert genau dann, wenn (*) $v(\sum a_i) = \min_i v(a_i)$. Ist dies nicht der Fall, so ist $rv(a_1)+\dots+rv(a_n) \approx \xi \iff v_{RV}(\xi) > \min_i v(a_i)$

Bew: Prüfe die Fälle $a_1 = 0$ oder $a_2 = 0$ von Hand. Jetzt $a_1, a_2 \neq 0$.

Seien $a_1', a_2' \in K^\times$ mit $rv(a_i') = rv(a_i)$, d.h. $v(a_i' - a_i) > v(a_i)$

Für wohldef zu zeigen: $rv(a_1 + a_2) = rv(a_1' + a_2')$

d.h. $v(\underbrace{a_1' + a_2' - a_1 - a_2}_{(a_1' - a_1) + (a_2' - a_2)}) \overset{!}{>} v(a_1 + a_2) \overset{(*)}{=} \min\{v(a_1), v(a_2)\}$

$v(a_1' + a_2' - a_1 - a_2) \geq \min\{v(a_1' - a_1), v(a_2' - a_2)\} > \min\{v(a_1), v(a_2)\}$

> $\{\sum a_i' \mid rv(a_i') = rv(a_i)\} = \{\sum a_i + b \mid v(b) > \min_i v(a_i)\}$
>
> Also: (*) $\Rightarrow rv(\sum a_i)$ wohldef.
>
> Und $\neg$(*) $\Rightarrow \dots = \{c \mid v(c) > \min_i v(a_i)\}$
>
> $\Rightarrow$ 2. Behauptung.

Also: (*) $\Rightarrow$ wohldef.

- Jetzt: Ann $v(a_1 + a_2) > \min\{v(a_1), v(a_2)\} = v(a_1)$

  Sei $\xi \in RV$ gegeben mit $v_{RV}(\xi) > v(a_1)$

  Wähle $b \in K$ mit $rv(b) = \xi$ und setze $a_1' := b - a_2$

  Dann ist $rv(a_1') = rv(a_1)$, da $v(a_1' - a_1) = v(b - a_2 - a_1) = v(\underbrace{b}_{v > v(a_1)} - \underbrace{(a_1 + a_2)}_{v > v(a_1)})$ $\quad \underbrace{}_{v > v(a_1)}$

  und $rv(a_1' + a_2) = \xi \Rightarrow rv(a_1) + rv(a_2) \approx \xi$.

$\square$

2.2 Quantorenelimination: die Aussagen

Def. 2.2.1: L_{RV} sei die zweisortige Sprache mit Sorten

- VF für einen bew. Kp. K („VF" = „valued field")
- RV für die Leitformstruktur von K

Die Symbole sind:

- die Ring-Sprache auf VF
- auf RV: • die Sprache der mult. Gruppen
  - eine 3-stellige Relation „$\xi_1 + \xi_2 \approx \xi_3$"
- $rv: VF \longrightarrow RV$

Ist K ein bew. Kp, so schreibe für die L_{RV}-Struktur (K, RV_K) oft einfach nur K.

Bem 2.2.2: Die L_{RV}-def'baren TM von K^n sind die selben wie die $L_{Ring}\cup\{V\}$-definierbaren, wobei V ein ein Rel-Symbol für den Bew-Ring ist. Insbesondere habe in L_{RV}^{eq} und $(L_{Ring}\cup\{V\})^{eq}$ Sorten für Γ, RV, $\bar{K}$, und folgendes ist def'bar: $v, rv, res, \mathcal{O}_K, \mathcal{M}_K$; $+,-,<$ auf Γ; $\cdot, \xi_1+\xi_2\approx\xi_3$ auf RV; $+,-,\cdot$ auf $\bar{K}$

$\left[\begin{array}{l} \varphi(x,\xi) \ L_{RV}\text{-Fml mit} \\ x \ VF\text{-Var}, \xi \ RV\text{-Var} \\ \varphi(K)\subset K\times RV_K \end{array}\right]$

Bew: In $L_{Ring}\cup\{V\}$: $\mathcal{O}_K$ def'bar $\Rightarrow$ auch def'bar $\mathcal{O}_K^\times$, $\mathcal{M}_K$, Γ, $\bar{K}$, RV,

In L_{RV}: Für $a,b\in K^\times$ habe $v(a)>v(b) \Leftrightarrow \underbrace{rv(a)+rv(b)=rv(b)}_{\text{in } L_{RV} \text{ ausdrückbar}}$

$\Rightarrow$ in L_{RV} def'bar: $\mathcal{M}_K, \mathcal{O}_K, \ldots\ldots$ $\square$

Bem 2.2.3: Es existiert eine L_{RV}-Theorie, deren Modelle genau die (K, RV_K) sind, für bew. Kp K.

Bew: Sei $\varphi(x)$ eine L_{RV}-Fml, die $\mathcal{O}_K$ definiert falls K ein bew. Kp ist.

Drücke aus:
- K ist Kp.
- $\varphi(K)$ ist ein Bew-Ring
- RV_K ist die die Leittermstruktur, die man aus K und der Bewertung zu $\varphi(K)$ erhält. $\square$

Def 2.2.4: Sei (p,q) eine mögliche Char. eines bew. Körpers.

HEN = Theorie der henselschen bew. Kp.

HEN_p = Theorie der henselschen bew. Kp. mit char $K=p$

$HEN_{p,q}$ = Theorie der henselschen bew. Kp. mit char $K=p$ und char $\bar{K}=q$

Bem: Diese Theorien existieren:

Henselsch lässt sich in L_{RV}^{eq} ausdrücken: Für jedes n:

$$\forall a_0,\ldots,a_n\in\mathcal{O}_K: \forall b\in\mathcal{O}_K: \Big(v\big(\textstyle\sum a_i b^i\big)>0 \wedge v\big(\sum i a_i b^{i-1}\big)=0 \rightarrow \exists b'\in\mathcal{O}_K: \big(\sum a_i (b')^i=0 \wedge v(b'-b)>0\big)\Big)$$

Bem: $HEN_0 = HEN \cup \{\overbrace{\underbrace{1+\ldots+1}_{p}}^{\text{in } K} \neq 0 \mid p \text{ prim}\}$

$HEN_{0,0} = HEN \cup \{\overbrace{\underbrace{1+\ldots+1}_{p}}^{\text{in } \bar{K}} \neq 0 \mid p \text{ prim}\}$

Überblick über QE-Resultate in bew. Körpern

K henselsch

Bsp: Ist $\mathrm{char}\,\bar{K} \neq 2$, so ist $a \in K$ ein Quadrat gdw $\mathrm{rv}(a)$ ein Quadrat in RV ist.

$\varphi(x) = \exists y \in VF: y^2 = x$ ist äquivalent zu $\exists \xi \in RV: \xi^2 = \mathrm{rv}(x)$

falls $\mathrm{char}\,\bar{K} \neq 2$.

Bsp: In $K = \mathbb{Q}((t))$: ist henselsch, $\bar{K} = \mathbb{Q}$. Insbes: $X \subset \mathbb{Q}^n$ L_{Ring}-def'bar

$\Rightarrow \{(a_1, \dots, a_n) \in \mathcal{O}_K^n \mid (\mathrm{res}(a_1), \dots, \mathrm{res}(a_n)) \in X\}$ L_{RV}-def'bar.

- $HEN_{0,0}$ (Henselsch, $\mathrm{char} = (0,0)$)

  Folgerung: Für $K \models HEN_{0,0}$ wird $Th(K)$ durch $Th(RV_K)$ festgelegt.

- VF-QE, relativ zu RV (in L_{RV})
- VF-QE, relativ zu $\bar{K}$ und Γ (in Sprache mit ac,) (Denef-Pas-QE, in L_{DP})

- HEN_0

- VF-QE, relativ zu „höheren RV", die mehr als nur den ersten Leitterm sehen.
- Denef-Pas-Variante mit ac-Abbildungen

- HEN

Nein! ($\mathbb{F}_2((t))$ ist böse.)(*)

- ACVF (alg. abg. bew. Kp)

  Folgerung: $ACVF_{p,q}$ ist vollst für jede mögliche Char (p,q)

- QE in $L_{Ring} \cup \{\underbrace{„v(a) \geq v(b)"}_{„b \mid a"}\} =: L_{Rob}$

  (Robinson-QE)

$$\boxed{\begin{array}{c} v(a) \geq v(b) \\ \Updownarrow \\ \frac{a}{b} \in \mathcal{O}_K \\ \Updownarrow \\ \exists c \in \mathcal{O}_K: b \cdot c = a \end{array}}$$

- $\mathbb{Q}_p$

- QE in $L_{Ring} \cup \{P_n \mid n \geq 2\} =: L_{mac}$

  mit $P_n(x) :\Leftrightarrow \exists y: y^n = x$

  (Macintyre-QE; analog zu $\mathbb{R}$)

(*) Habe def'bare Bij $\mathbb{F}_2((t))^2 \longrightarrow \mathbb{F}_2((t))$

$(a,b) \longmapsto a^2 + tb^2$ (vgl. Übung auf Blatt 5)

- Def. 2.2.5: • Eine RV-Expansion von L_{RV} ist eine Sprache $L \supset L_{RV}$, so dass $L \setminus L_{RV}$ „nur auf RV lebt", d.h. nur besteht aus:
  - Konst-Symb in RV
  - Fkt-Symb $RV^n \to RV$
  - Rel-Symb in RV^n

(Ist $L' \supset L$, so nennt man L' Expansion von L)

VFqf: • Sei L eine RV-Expansion von L_{RV}. Wir nennen eine L-Fml VF-quantoren-frei, wenn sie keine Quantoren hat über VF-Variablen.

• **Satz 2.2.6:** Sei $L \supset L_{RV}$ eine RV-Expansion und $T \supset HEN_{0,0}$ eine L-Theorie.
Dann ist jede L-Fml modulo T zu einer VFqf L-Fml äquivalent.

• **Bem:** T ist eigentlich unnötig.

• **Bsp** (später ausführlicher): $K = k((t))$, char $k = 0$

$a \in K$ $\quad ac(a) = res(a \cdot t^{-v(a)})$ $\quad (ac: K \to \bar{K} \subset RV)$

Sei $L := L_{RV} \cup \{ac\}$

Möchte 2.2.6. auf L anwenden.

Habe Abb. $ac_{RV}: RV \to \bar{K}$ mit: $ac(a) = ac_{RV}(rv(a))$

Arbeite also mit $L' := L_{RV} \cup \{ac_{RV}\}$.

(In L und in L' sind die selben Mengen def'bar.)

• **Bsp:** $\varphi(\overset{VF}{x}) = \exists \overset{VF}{y} : y^2 = x$

ist äquiv. zu $\psi(x) = \exists \overset{RV}{\xi} : \xi^2 = rv(x)$

• **Korollar 2.2.7:** Sei $L \supset L_{RV}$ eine RV-Expansion und $T \supset HEN$ eine L-Theorie.
Dann existiert zu jeder L-Fml φ eine VFqf L-Fml ψ und ein $N \in \mathbb{N}$ s.d. für alle $K \models T$ mit char $\bar{K} > N$ gilt:

$$\varphi(K) = \psi(K)$$

Bew: • Wähle ψ s.d. $HEN_{0,0} \vdash \forall \underline{x}: (\varphi(\underline{x}) \leftrightarrow \psi(\underline{x}))$ (mit 2.2.6)

• Ex $T_0 \subset HEN_{0,0}$ endl. s.d. $T_0 \vdash$ ——— " ———

• In T_0 kommen nur endl viele der Formeln „char $\bar{K} \neq p$" vor

$\Rightarrow$ Kann N als Maximum dieser p wählen. □

2.3 Polynome und rv

Sei K henselsch, mit Charakteristik $(0,0)$.

Motivation: Eine der Hauptarbeiten im QE-Beweis: $\exists x: rv(f(x)) = \xi$
$f \in K[x]$

Bsp: $\exists y: rv(y^2 - x) = \underbrace{rv(0)}_{\xi}$

Def 2.3.1: Sei $f = \sum a_i x^i \in K[X]$ und $b \in K$.
Wir sagen f hat eine Kollision bei b, wenn
$$v(f(b)) > \min_i v(a_i b^i)$$

Bem 2.3.2: f hat keine Kollision bei b gdw. $\sum_i rv(a_i b^i)$ wohldef ist.
Ist dies der Fall, so ist $$\sum_i rv(a_i b^i) = rv(f(b))$$
$$\overset{\shortparallel}{\sum_i rv(a_i) rv(b)^i}$$

Def 2.3.3: Sei $f \in K[X]$ ein Polynom vom Grad n. Wir nennen ein $c \in K$ eine „Nullstelle einer Abl. von f", wenn ein $l \le n$ existiert mit: $f^{(l)}(c) = 0$ (wobei $f^{(l)}$ die l-te Abl. von f ist). ($l=0$ ist auch erlaubt.) Ist $l \geq 1$, so nenne c „Nst einer echten Abl von f".

Lemma 2.3.4: Sei $f \in K[X]$. Die Menge der $b \in K$, an denen f eine Kollision hat, hat die Form
$$\{ b \in K \mid \exists c \in C : rv(b) = rv(c) \},$$
wobei C eine Teilmenge der Nst der Abl. von f ist.

Bem: $c \neq 0$ Nst von f $\Rightarrow$ f hat Kollision bei c (da $v(f(c)) = \infty$)
$\Rightarrow$ f hat — " — b $\forall$ b mit $rv(b) = rv(c)$

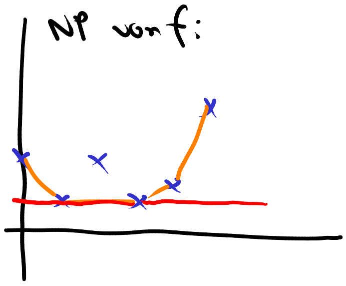
Bem: Bei 0 hat f nie eine Kollision, da $f(0) = a_0$
$\Rightarrow v(f(0)) = v(a_0) = \min_i v(a_i 0^i)$

Bew von 2.3.4: Z.z.: Hat f eine Kollision bei $b \neq 0$, so ex. eine Abl-NSt c mit $rv(c) = rv(b)$.

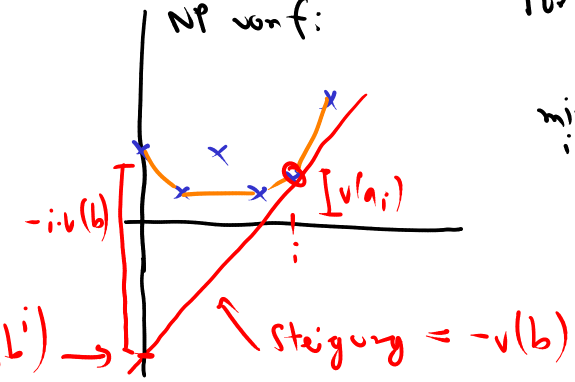
- $f = \sum_i a_i X^i$
- O.E. $b = 1$. Sonst:
  - $g(X) := f(b \cdot X)$ $\quad$ $\left(\Rightarrow g(1) = f(b)\right)$, $\quad g(X) = \sum a_i' X^i$
  - $\Rightarrow$ g hat Kollision bei 1. ($a_i' = a_i \cdot b^i$ ...)
  - Zeige Beh für g, d.h. Finde Abl-Nst c' von g mit $rv(c') = rv(1)$.
  - $\Rightarrow c := c' \cdot b$ ist Abl-NSt von f
    $rv(c) = rv(c') \cdot rv(b) = 1 \cdot rv(b)$
- O.E. $v_{gauss}(f) = 0$
  $\overset{\shortparallel}{\min_i v(a_i)}$,
  d.h. $f \in \mathcal{O}_K[X]$, $res(f) \neq 0$
- Dass f eine Kollision bei 1 hat, bedeutet: $v(f(1)) > 0$
  Also: $res(f)$ hat NSt bei 1
- Sei l die Vielfachheit dieser NSt von $res(f)$.
  Dann hat $res(f^{(l-1)})$ eine einfache NSt bei 1.
- Hensel-Bedingung liefert: Ex. $c \in \mathcal{O}_K$ mit $rv(c) = 1$ und $f^{(l-1)}(c) = 0$. $\square$

Intuition mit NP:

Falls $b=0$:
$v(f(b)) \geq \min v(a_i) \rightarrow$



Sei $b \in K$ mit $v(b)=0$
$\Rightarrow v(f(b)) \geq \min_i v(a_i \cancel{b^i})$



$v(f(b)) \geq \min v(a_i b^i) \rightarrow$

für allgemeine b:

$\min_i \underbrace{v(a_i b^i)}_{= v(a_i) + i\, v(b)}$

Def 2.3.5: Sei $f \in K[X]$ und $b, c \in K$. Wir sagen f hat eine <u>um-c-Kollision</u> bei b, wenn $g(X) := f(X+c)$ eine Kollision bei $b-c$ hat.

Bem 2.3.6: Schreibe $g(X) = \sum_i a_i X^i$.

f hat keine um-c-Koll bei b $\Leftrightarrow$ $\underbrace{v(g(b-c))}_{= v(f(b))} = \min_i v(a_i (b-c)^i)$

$\Leftrightarrow rv(f(b)) = \sum_i rv(a_i) \cdot rv(b-c)^i$

Satz 2.3.7: Sei $f \in K[X]$ und $b \in K$.

Sei c eine Abl-NSt von f so dass $v(c-b)$ maximal ist (unter allen Abl-NSt von f).

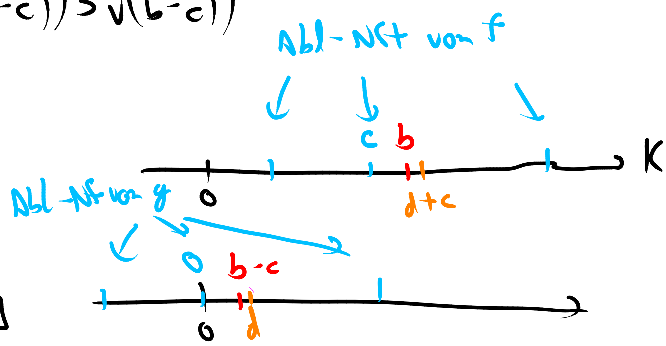
Dann hat f keine um-c-Kollision bei b.

Bew: Sei $g(X) := f(X+c)$. Z.z.: g hat keine Koll. bei $b-c$. Annahme doch.
Wende Lemma 2.3.4 auf g an. Dann finde Abl-NSt d von g mit
$rv(d) = rv(b-c)$. (d.h. $v(d-(b-c)) > v(b-c)$)

$\Rightarrow d+c$ ist Abl-NSt von f

$v(d+c-b) > v(b-c)$

d.h. $d+c$ ist Widerspruch zur Wahl von c.



$\square$

Lemma 2.3.8: Sei $n \in \mathbb{N}$. Es existiert eine VF-qf-Fml η, so dass für alle $K \models HEN_{0,0}$ und alle $a_0, \dots, a_n, b, c \in K$, $\xi \in RV_K$ gilt:

Sei $f := \sum_{i=0}^{n} a_i X^i$

$K \models \eta(a_0, \dots a_n, rv(b-c), c, \xi) \Leftrightarrow$ f hat keine um-c-Koll. bei b und $rv(f(b)) = \xi$

Bew: • Setze $g(X) := f(X+c) = \sum a_i' X^i$

a_i' ist Polynom in den a_i und in c.

• Drücke aus, dass $\sum rv(a_i') \cdot rv(b-c)^i$ wohldefiniert ist und gleich ξ ist.

□

Satz 2.3.9: Sei $f \in K[X]$ ein Polynom. Wir nehmen an, dass f mit keiner seiner echten Ableitungen eine gemeinsame Nst hat.

Sei außerdem $\xi \in RV^{\times}$ gegeben. Dann sind äquivalent:

(a) Ex. $b \in K$ mit $f(b) = 0$ und $rv(b) = \xi$

(b) Ex $b \in K$ mit $rv(b) = \xi$ so dass f eine um-c-Kollision bei b hat für $c = 0$ und für jede Nst c jeder echten Abl von f.

Bew: (a) $\Rightarrow$ (b): Klar (da $b \neq c$, für alle (c), die in (b) auftauchen, und da Nullstellen $\neq 0$ immer Kollisionsstellen sind).

(b) $\Rightarrow$ (a) • Da f Kollision bei b hat, existiert eine $\underbrace{\text{Abl-Nst}}_{\text{Kann auch Nst von f sein}}$ c, so dass $rv(c) = rv(b)$ ist (nach 2.3.4)

• Wähle eine solche Abl-Nst möglichst nah an b (d.h. mit $v(c-b)$ maximal)

• Nach 2.3.7 hat f keine um-c-Kollision bei b.

• Nach Ann (b) hat f eine um-c-Koll. bei b falls c Nst. einer echten Abl. von f ist; also muss c Nst von f selbst sein

Dieses c ist also wie in (a) gesucht. □

2.4 Beweis von Quantoren-Elimination

Lemma 2.4.1: Seien $f_i(x,\underline{z}) \in \mathbb{Z}[x,\underline{z}]$ für $i=1,2$, wobei $\underline{z}$ ein N-Tupel ist. Dann existieren endl viele qf L_{Ring}-Fmln $\varphi_\ell(\underline{z})$ und Polynome $g_\ell(x,\underline{z}), h_{i,\ell}(x,\underline{z}) \in \mathbb{Z}[x,\underline{z}]$ so dass für jeden Körper K gilt:

(a) Die $\varphi_\ell(K)$ bilden eine Partition von K^N.

(b) Ist $\underline{c} \in \varphi_\ell(K)$, so ist $g_\ell(x,\underline{c})$ der ggT von $f_1(x,\underline{c})$ und $f_2(x,\underline{c})$ (im Ring $K[x]$) (bis auf Faktor in $K^\times$)
und für $i=1,2$ gilt: $\exists d \in K^\times: f_i(x,\underline{c}) = g_\ell(x,\underline{c}) \cdot h_{i,\ell}(x,\underline{c}) \cdot d$

Bew: $f_i(x,\underline{z}) =: \sum_{j=0}^{n_i} a_{ij}(\underline{z}) \cdot x^j$

- O.E. $n_1 \geq n_2$
- Ind. über $n_1 + n_2$
- O.E. $\deg f_i(x,\underline{c}) = n_i$ für $i=1,2$. Genauer: Mache mit Hilfe der Fmln $\varphi_\ell(\underline{c})$ eine Fallunterscheidung danach, ob $a_{i,n_i}(\underline{c}) = 0$ ist.
- Falls $f_2 = 0$ (Ind. Anfang): $g = f_1$, $h_1 = 1$, $h_2 = 0$
- Falls $f_2 \neq 0$

  Ersetze f_1 durch $\hat{f}_1 := a_{2,n_2} f_1 - a_{1,n_1} \cdot f_2 \cdot x^{n_1 - n_2}$

  Erhalte $\hat{g}, \hat{h}_1, \hat{h}_2 \rightsquigarrow g := \hat{g}, h_1 = \dots, h_2 = \hat{h}_2$ □

Wir arbeiten in einer RV-Expansion $L \supset L_{RV}$ (wie in Satz 2.2.6) und in $HEN_{0,0}$ (als L-Theorie aufgefasst).

Im Folgenden: $x, \underline{z}$ VF-Variablen (auch: y)
$\underline{\zeta}$ RV-Variablen (auch: $\underline{\xi}$)

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

Bew: $L^* := L \cup \{$alle VF-qf-defbaren Relationen$\}$ und $T^* \supset T$ entsprechend.
(Genauer: L^* enthält ein neues Rel-Symb R_φ für jede VF-qf-Fml φ und T^* sagt, dass R_φ zu φ äquivalent ist.)

- Nach Annahme des Lemmas lässt sich der $\exists$-Quantor von $\exists x\,\varphi(x,\underline{z},\underline{\zeta})$ in L^* eliminieren, für φ qf L^*-Fml.

  Daraus folgt: Habe QE in L^*, T^*.
- Sei $\psi(\underline{z},\underline{\zeta})$ L-Fml. Die ist (modulo T^*) äquivalent zu einer qf L^*-Fml, und damit auch zu einer VF-qf L-Fml $\psi'(\underline{z},\underline{\zeta})$.

  Da sowohl ψ als auch ψ' L-Fmln sind, und jedes Modell von T sich zu einem Modell von T^* erweitern lässt, folgt die Äquivalenz schon aus T. □

Im Folgenden sind $m, n, r \in \mathbb{N}$, $a_{i,j}, b_j, c_i \in \mathbb{Z}[\underline{z}]$,

$$f_i = \sum_{j\le m} a_{i,j} x^j, \quad g = \sum_{j\le n} b_j x^j \in \mathbb{Z}[x,\underline{z}], \qquad \varphi \text{ VF-qf-Fml}$$

Für jede der folgenden Formen von Fmln $\psi(\underline{z},\underline{\zeta})$ führe eine Bezeichnung ein für:
Jede Formel der gegebenen Form ist zu einer VF-qf-Fml äquivalent:

B = beliebig (B) $\psi(\underline{z},\underline{\zeta}) = \exists x:\ \varphi(x,\underline{z},\underline{\zeta})$

P = Polynomial (P) $\psi(\underline{z},\underline{\zeta}) = \exists x:\ \bigwedge_{i\le r} \mathrm{rv}(f_i(x,\underline{z})) = \zeta_i$ $\quad [\exists x:\ x^2+y = \mathrm{rv}(7) \wedge z+x+1 = \mathrm{rv}(g)]$

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

E = endlich $(\mathrm{EB})_n$ $\psi(\underline{z},\underline{\zeta}) = b_n(\underline{z}) \neq 0 \wedge \exists x:\ g(x,\underline{z}) = 0 \wedge \varphi(x,\underline{z},\underline{\zeta})$

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

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

Lemma 2.4.3:
- ✓(a) (P) $\Rightarrow$ (B), $\quad (\mathrm{EP})_n \Rightarrow (\mathrm{EB})_n$
- ✓(b) (L) $\wedge\ \forall n: (\mathrm{EB})_n \Rightarrow$ (P)
- ✓(c) (L) ist wahr
- ✓(d) $(\mathrm{EL})_0$ und $(\mathrm{EP})_0$ sind wahr
- ✓(e) Für $n \ge 1$: $(\mathrm{EL})_n \wedge \forall n'<n: (\mathrm{EB})_{n'} \Rightarrow (\mathrm{EP})_n$
- (f) Für $n \ge 1$: (L) $\wedge\ \forall n'<n: (\mathrm{EB})_{n'} \Rightarrow (\mathrm{EL})_n$

Bew von Satz 2.2.6: Aus 2.4.3 folgt (B). Nach 2.6.2 folgt daraus 2.2.6. □

$\circledast = [b_n(\underline{z}) \neq 0 \wedge]$

Bew von 2.4.3:

(a) • Gegeben: $\psi(\underline{z}, \underline{\xi}) = \circledast \exists x : [g(x, \underline{z}) = 0 \wedge] \; \underset{\text{VF-qf}}{\varphi(x, \underline{z}, \underline{\xi})}$

• Aus syntaktischen Gründen kommen x und $\underline{z}$ in φ nur in den folgenden Formen vor: (1) $rv(h(x,\underline{z}))$ $\quad h \in \mathbb{Z}[x, \underline{z}]$

(2) $h_1(x, \underline{z}) = h_2(x, \underline{z})$ $\quad h_1, h_2 \in \mathbb{Z}[x, \underline{z}]$

• (2) $\Leftrightarrow rv(h_1 - h_2) = 0$, d.h. o.E nur Form (1), d.h. $\varphi(x, \underline{z}, \underline{\xi})$ ist äquiv. zu $\chi(rv(f_1(x, \underline{z})), \dots, rv(f_r(x, \underline{z})), \underline{\xi})$, für χ VF-qf.

• Das ist äquiv. zu: $\exists \xi_1, \dots \xi_r : \left(\bigwedge_i rv(f_i(x, \underline{z})) = \xi_i \wedge \chi(\xi_1, \dots, \xi_r, \underline{\xi}) \right)$

• $\psi(\underline{z}, \underline{\xi})$ ist äquiv. zu:

$\circledast \exists x : [g(x, \underline{z}) = 0 \wedge] \; \exists \xi_1, \dots \xi_r : \left(\bigwedge_i rv(f_i(x, \underline{z})) = \xi_i \wedge \chi(\xi_1, \dots, \xi_r, \underline{\xi}) \right)$

$\exists \xi_1, \dots \xi_r \circledast \exists x : \left([g(x, \underline{z}) = 0 \wedge] \bigwedge_i rv(f_i(x, \underline{z})) = \xi_i \wedge \chi(\xi_1, \dots, \xi_r, \underline{\xi}) \right)$

$\exists \xi_1, \dots \xi_r : \left(\chi(\xi_1, \dots, \xi_r, \underline{\xi}) \wedge \underbrace{\circledast \exists x : \left([g(x, \underline{z}) = 0 \wedge] \bigwedge_i rv(f_i(x, \underline{z})) = \xi_i \right)}_{\text{hat die Form (P) oder } (EP)_n \text{, also nach Annahme äquiv. zu VF-qf-Fml}} \right)$

$\Rightarrow \psi$ äquiv zu VF-qf-Fml.

(d) Habe $g(x, \underline{z}) = b_0(\underline{z})$; die Fmln sind immer falsch.

• Sei $(L)'$ die Behauptung (L) im Spezialfall $r = 1$.

Sei $(EL)'_n$ die Behauptung $(EL)_n$ im Spezialfall $r = 1$.

• Beh: $(L)' \Rightarrow (L)$, $(EL)'_n \Rightarrow (EL)_n$

Bew: $\psi = [b_n = 0 \wedge] \; \exists x : [g = 0 \wedge] \bigwedge_{i \leq r} rv(x + c_i) = \xi_i$

• Falls $r = 0$: $\psi \Leftrightarrow \exists \xi : \underbrace{[b_n = 0 \wedge] \; \exists x : [g = 0 \wedge] \; rv(x) = \xi}_{(L)' \text{ bzw } (EL)'_n}$

• Fall $r \geq 2$:

• Beh: Falls $v(\xi_1) \geq v(\xi_2)$ ist, ist $\overbrace{rv(x + c_1) = \xi_1}^{(1)} \wedge \overbrace{rv(x + c_2) = \xi_2}^{(2)}$ äquivalent zu $rv(x + c_1) = \xi_1 \wedge rv(c_2 - c_1) + \xi_1 \approx \xi_2$

(Anschauung: (1), (2) definieren Bälle B_1, B_2; B_2 mind so groß wie B_1 $\Rightarrow B_1 \subset B_2$ oder $B_1 \cap B_2 = \emptyset$)

Bew: • $(c_2 - c_1) + (x + c_1) = x + c_2$

$$\Rightarrow rv(c_2 - c_1) + \underbrace{rv(x+c_1)}_{=\varsigma_1} \approx \underbrace{rv(x+c_2)}_{=\varsigma_2}$$

• Aus $v(\varsigma_1) \geq v(\varsigma_2)$ folgt (mit 2.7.8) Wohldefiniertheit der rv-Summe.

d.h. für alle x mit $rv(x+c_1)=\varsigma_1$ habe auch $rv(x+c_2)=\varsigma_2$ □

Also: $rv(x+c_1)=\varsigma_1 \wedge rv(x+c_2)=\varsigma_2$ ist äquiv. zu

$$\underbrace{v(\varsigma_1) \geq v(\varsigma_2) \wedge rv(c_2-c_1)+\varsigma_1 \approx \varsigma_2}_{\chi_1} \wedge rv(x+c_1)=\varsigma_1$$

$$\vee \quad \underbrace{v(\varsigma_2) > v(\varsigma_1) \wedge rv(c_1-c_2)+\varsigma_2 \approx \varsigma_1}_{\chi_2} \wedge rv(x+c_2)=\varsigma_2$$

Also ist φ äquivalent zu:

$$\chi_1 \wedge [b_n \neq 0 \wedge]\ \exists x : [g = 0 \wedge] \bigwedge_{\substack{i \leq r \\ i \neq 2}} rv(x+c_i) = \varsigma_i$$

$$\vee \quad \chi_2 \wedge [b_n \neq 0 \wedge]\ \exists x : [g = 0 \wedge] \bigwedge_{\substack{i \leq r \\ i \neq 1}} rv(x+c_i) = \varsigma_i$$

Induktion über r. □

- (c) z.z.: $(L)_1$, d.h. $\varphi = \exists x \; rv(x+c) = \varsigma$

  Diese Fml ist immer wahr.

- Sei $(EP)_n^*$ die Bh. $(EP)_n$ im Spezialfall $m < n$

Bh: $(EP)_n^* \Rightarrow (EP)_n$

Bew: $\varphi = b_n \neq 0 \wedge \exists x . \left(g = 0 \wedge \bigwedge_{i \leq r} rv(f_i) = \varsigma_i \right)$

- Ann: $m \geq n$.
- Bem: Für $h(x,z)$ beliebig ändert sich φ nicht, wenn man f_i durch $f_i + g \cdot h$ ersetzt.
- Ersetze $rv(f_i) = \varsigma_i$ durch $rv(b_n \cdot f_i) = rv(b_n) \cdot \varsigma_i$ (ändert nichts am φ)
- Ersetze danach $b_n \cdot f_i$ durch $b_n \cdot f_i - a_{i,m} \cdot g \cdot X^{m-n}$ (ändert nichts am φ)
- Dies reduziert den x-Grad von f_i um 1. Wiederhole □

• Beweis von (b) und (e): z.z.: (P), $(EP)_n^*$

$$\varphi = [b_n \neq 0 \wedge] \exists x \, [g(x)=0 \wedge] \bigwedge_{i \leq r} rv(f_i(x)) = \xi_i \qquad (*)$$

• Sei η wie in 2.3.8.

• Nach 2.3.7. ex. zu jedem $K \models HEN_{0,0}$ und jeder Belegung der Variablen $\underline{z}$ und jedem $b \in K$ eine Abl.-Nst c von f, so dass f_i keine rv-c-Koll. bei b hat, d.h. $rv(f_i(b)) = \xi_i$ ist äquiv. zu

$$\exists y_i \text{ Abl-Nst von } f: \ \eta(a_{i0}, \dots, a_{im}, rv(b - y_i), y_i, \xi_i)$$

$$\underbrace{\exists y_i \left(\bigvee_{0 \leq l_i \leq m} \Big(\underbrace{\deg_x f_i \geq l_i}_{a_{il}(\underline{z}) \neq 0 \ \vee \ a_{i,l+1}(\underline{z}) \neq 0 \ \vee \dots \vee \ a_{im}(\underline{z}) \neq 0} \wedge f_i^{(l_i)}(y_i) = 0\Big) \wedge \eta(a_{i0}, \dots, a_{im}, rv(b - y_i), y_i, \xi_i) \right)}_{(\Delta)_i(b)}$$

setze dies in (*) ein und ziehe die $\exists y_i$ nach außen. Erhalte

$$\exists y_1 \cdots \exists y_r [b_n \neq 0 \wedge] \exists x \, [g(x)=0 \wedge] \bigwedge_{i \leq r} (\Delta)_i(x)$$

$\Updownarrow$

$$\underbrace{\bigvee_{l_1} \cdots \bigvee_{l_r}} \exists y_1 \cdots \exists y_r [b_n \neq 0 \wedge] \exists x \, [g(x)=0 \wedge] \bigwedge_{i \leq r} (\deg_x f_i \geq \dots) \wedge \eta(\dots)$$

• Betrachte jedes dieser Disjunkte einzeln

• Ziehe auch die $\deg_x f_i \geq l_i$ raus. Bleibt

$\deg_x f_1 \geq l_1 \wedge$ $\quad$ $\deg f_r \geq l_r$

$$\exists y_1 \cdots \exists y_r [b_n \neq 0 \wedge] \exists x \, [g(x)=0 \wedge] \bigwedge_{i \leq r} f_i^{(l_i)}(y_i) = 0 \wedge \eta(\dots)$$

• Ziehe die $f_i^{(l_i)}(y_i) = 0$ raus bis direkt innerhalb $\exists y_i$:

$$\exists y_1 \left(f_1^{(l_1)}(y_1) = 0 \wedge \left(\dots \wedge \left(\exists y_n \left(f_n^{(l_n)}(y_n) = 0 \wedge \underbrace{[b_n \neq 0 \wedge] \exists x \, [g(x)=0 \wedge] \bigwedge_{i \leq r} \eta(\dots)}\right)\right)\right)\right)$$

$\exists x$ kann eliminiert werden nach (L) bzw. $(EL)_n$

Können eliminiert werden nach $(EB)_{n'}$ für $n' = m - l_i$ $\leftarrow$ Im Fall $(EP)'_n$ habe $n' = m - l_i \leq m < n$

• Durch eine Fallunterscheidung nach $\deg_x f_i$ (also genauer: danach, welche $a_{ij}(\underline{z}) = 0$ sind) erhalte, dass die y_i-Quantoren wirklich die Form aus $(EB)_{n'}$ haben.

Habe das Problem also wie gewünscht reduziert.

- (≤) Z.z: $(EL)^1_n$, d.h. gegeben:

$$\psi = b_n \neq 0 \wedge \exists x: \left(g(x)=0 \wedge rv(x+c)=\xi\right)$$

- Wir können das „$+c$" loswerden, indem wir $g(x)$ durch $g(x-c)$ ersetzen.
- Wir können $\xi \neq 0$ annehmen:

$$\psi(x,\underline{z},\xi) = \xi=0 \wedge b_n \neq 0 \wedge g(0)=0$$
$$\vee\ \xi \neq 0 \wedge b_n \neq 0 \wedge \exists x \ldots\ldots$$

- Für $1 \leq l \leq n$:
  - Wende Lemma 2.4.1 auf $g, g^{(l)}$ an.
  - Füge die Fallunterscheidung in die Fml ein; erhalte so (für jeden Fall separat) Polynome $h, \hat{h} \in \mathbb{Z}[x,\underline{z}]$ mit: $\forall \underline{d} \in K^N: h(x,\underline{d}) = ggT(g(x,\underline{d}), g^{(l)}(x,\underline{d}))$ und $\exists r \in K^\times: g(x,\underline{d}) = h(x,\underline{d}) \cdot \hat{h}(x,\underline{d}) \cdot r$
  - Kann Vfqf ausdrücken, ob g und $g^{(l)}$ teilerfremd sind (nämlich: „$\deg_x h = 0$"). Füge eine Fallunterscheidung danach in die Fml ein.
  - Falls g und $g^{(l)}$ nicht teilerfremd sind: Habe $g(x)=0 \iff h(x)=0 \vee \hat{h}(x)=0$, d.h. ψ ist in diesem Fall äquiv. zu
    $$\exists x: (h(x,\underline{z})=0 \wedge rv(x)=\xi) \vee \exists x: \hat{h}(x,\underline{z})=0 \wedge rv(x)=\xi)$$
  - Unter all den obigen Bed. an $\underline{z}$:
    - $h, \hat{h}$ nicht-trivial, $\deg_x h \leq n-l < n$, $\deg_x \hat{h} < n$
  - Dies $\exists x$ können eliminiert werden nach $(EL)_{n'}$, $n' < n$.
- Bleibt nur noch der Fall, wo g und $g^{(l)}$ teilerfremd sind für $1 \leq l \leq n$.
- Unter diesen Bed an $\underline{z}$ (und ξ) ist (nach 2.3.9)

$$\exists x\ g(x)=0 \wedge rv(x)=\xi$$

äquiv. zu $\exists x: \forall c \in \underbrace{\{0\} \cup \text{echte Abl-Nst von } g}_{C}: (\underbrace{g \text{ hat um } -c\text{-Koll. bei } x}_{\vartheta(\underline{b}, rv(x-c), c) = \forall \xi: \neg\eta(b_0, \ldots, b_n, rv(x-c), c, \xi)} \wedge rv(x)=\xi)$

$$\Leftrightarrow \exists x\, \exists \underline{y} : \left(\{y_1, \dots, y_m\} = C \wedge \left(\bigwedge_{i \le m} \vartheta(\underline{b}, rv(x-y_i), y_i) \wedge rv(x) = \zeta \right)\right)$$

$$\Leftrightarrow \exists \underline{y} : \left(\underbrace{\{y_1, \dots, y_m\} = C}_{\bigwedge_{i \le m} \left(y_i = 0 \vee \bigvee_{1 \le l \le n} g^{(l)}(y_i) = 0\right)} \wedge \underbrace{\exists x \left(\bigwedge_{i \le m} \vartheta(\underline{b}, rv(x-y_i), y_i) \wedge rv(x) = \zeta \right)}_{\text{hat die Form (L), d.h. ist äquiv zu VF-qf } \tilde{\chi}(\underline{y}, \underline{z})}\right)$$

$$\bigwedge_{i \le n} \left(y_i = 0 \vee \bigvee_{1 \le l \le n} g^{(l)}(y_i) = 0\right) \wedge (y_1 = 0 \vee \dots \vee y_m = 0)$$

$$\wedge \bigwedge_{1 \le l \le n} \neg \underbrace{\exists y' : \left(g^{(l)}(y') = 0 \wedge y' \ne y_1 \wedge \dots \wedge y' \ne y_m\right)}_{\text{hat die Form } (\exists B)_{n'},\ n' < n \ \Rightarrow \exists y' \text{ kann eliminiert werden}}$$

$\chi(\underline{y}, \underline{z})$

Ziehe Disjunktionen nach außen. Erhalte Disj. von Fmln der Form

- $\exists y_1\, \varphi_1(y_1, \underline{z}) \wedge \dots \exists y_m\, \varphi_m(y_m, \underline{z}) : \left(\chi(\underline{y}, \underline{z}) \wedge \tilde{\chi}(\underline{y}, \underline{z})\right)$

$\varphi_i(y_i, \underline{z})$ ist entweder $y_i = 0$ oder $g^{(l_i)}(y_i) = 0$

Entferne den $\exists y_i$-Quantor und ersetze y_i durch 0

Kann Annehmen: x^{n-l_i}-Term von $g^{(l_i)}$ ist nicht 0 $\Rightarrow$ „$\exists y_i : g^{(l_i)}(y_i) = 0 \wedge$ VFqf" hat die Form $(\exists B)_{n'}$ für $n' < n$

Kann also die Quantoren $\exists y_m, \dots, \exists y_1$ der Reihe nach eliminieren. $\square$

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

- V1: Für $K \models HEN_{0,0}$ wird $Th(K)$ durch $Th(\bar{K})$ und $Th(\Gamma)$ festgelegt.
- V2: $\mathbb{Q}_p$ und $\mathbb{F}_p((t))$ sind sich ähnlich für $p \gg 0$

(60er-Jahre)

Dazu: „Zerlegen RV in $\bar{K}$ und Γ"

Def 2.5.1: Eine <u>anguläre Komponente</u> auf einem bew. Kp K ist ein Gruppenhomom. $\underline{ac}: K^\times \longrightarrow \bar{K}^\times$, der auf $\mathcal{O}_K^\times$ mit res übereinstimmt. Außerdem setzen wir $ac(0) := 0$

Bsp: Ist $\Gamma = \mathbb{Z}$ und $\varpi \in K$ mit $v(\varpi) = 1$, so ist
$x \longmapsto res(x \cdot \varpi^{-v(x)})$ eine ang. Komp.

Bem: Es existieren bew. Kp (sogar henselsche), die keine ang. Komp. besitzen.

Bem 2.5.2: Sei $ac: K \to \bar{K}$ eine ang. Komp. Dann erhalten wir eine induzierte Abb. $\underline{ac_{RV}}: RV \to \bar{K}$ (d.h. $ac(x) = ac_{RV}(rv(x))$ $\forall x \in K$).
Die Abb. $RV^\times \longrightarrow \bar{K}^\times \times \Gamma$, $\xi \longmapsto (ac_{RV}(\xi), v_{RV}(\xi))$ ist ein Gruppen-Iso.

Bew: Teil 1:

Für $x \in 1 + \mathcal{M}_K$ habe $ac(x) = res(x) = 1$, d.h. $1 + \mathcal{M}_K \subset \ker ac$
$$\underset{\mathcal{O}_K}{\cap}$$
Da $\ker rv = 1 + \mathcal{M}_K$ ist, faktorisiert ac über rv (d.h. ac_{RV} existiert).

Teil 2: • Surjektivität klar (da $v: K^\times \to \Gamma$ und $res: \mathcal{O}_K^\times \to \bar{K}^\times$ surj.)

• <u>Injektiv</u>: sei $x \in K^\times$ so, dass $rv(x)$ im Kern der obigen Abb ist, d.h. $ac(x) = 1$ und $\underbrace{v(x) = 0}$

$\Rightarrow x \in \mathcal{O}_K^\times$, d.h. $ac(x) = res(x) = 1$

$\Rightarrow x \in 1 + \mathcal{M}_K = \ker rv \quad \Rightarrow rv(x) = 1$

$\square$

Bem: Die Umkehrung gilt auch: Geeignete Isos $RV \to \bar{K} \times \Gamma$ liefern anguläre Komponenten.

Satz 2.5.3: Sei K ein bew. Kp., aufgefasst als Struktur in einer beliebigen Sprache L. Dann besitzt K eine el. Erw $K' \succ_L K$, auf der eine ang. Komp. existiert.

Bem: K endl $\Rightarrow$ Bewertung trivial, d.h. $\Gamma = \{0\}$, $\mathcal{O}_K = K$, $\mathcal{M}_K = \{0\}$, $\bar{K} = K$, $ac = id$.

Bew: • Vergrößere die Sprache L so, dass die mult. auf $\bar{K}^\times$ in L^{eq} def'bar ist.
Wähle dann K' $\aleph_1$-saturiert. Beh.: Auf K' ex. eine ang. Komp.

- Im Folgenden seien alle Gruppen abelsch (aber multiplikativ geschrieben).
- <u>Def</u>: Eine Einbettung $H \subset G$ von Gruppen heißt <u>rein</u> wenn

  für alle $g \in G$ und $n \geq 1$ gilt: $\quad g^n \in H \Rightarrow g \in H$

  ($\Leftrightarrow$ H ist gleich seiner divisiblen Hülle in G)
- <u>Def</u>: Eine Gruppe N heißt <u>(rein) injektiv</u>, wenn für jede (reine) Einbettung $H \subset G$ sich jeder Homom. $f: H \to N$ zu einem Homom. $\tilde{f}: G \to N$ fortsetzen lässt.

$$\begin{tikzcd} H \arrow[r, phantom, "\subset"] \arrow[dr, "f"'] & G \arrow[d, dashed, "\tilde{f}"] \\ & N \end{tikzcd}$$

- Satz 2.8 aus dem Seminar über Mod-Th von Moduln

  impliziert: $\quad N\ \aleph_1$-saturiert $\Rightarrow N$ rein injektiv
- $(\mathbb{K}')^\times$ ist $\aleph_1$-saturiert, also rein injektiv.

  Also: Reicht z.z.: $\mathcal{O}_{K'}^\times \subset (\mathbb{K}')^\times$ ist reine Einbettung.

  (Dann: $\mathrm{res}: \mathcal{O}_{K'}^\times \to (\mathbb{K}')^\times$ lässt sich auf $(K')^\times$ fortsetzen; die Fortsetzung ist eine ang. Komp.)
- Sei also $x \in (K')$ mit $x^n \in \mathcal{O}_{K'}^\times$. z.z.: $x \in \mathcal{O}_{K'}^\times$

$$x^n \in \mathcal{O}_{K'}^\times \Leftrightarrow v(x^n) = 0, \quad v(x^n) = n \cdot v(x) \quad \Rightarrow v(x) = 0 \Leftrightarrow x \in \mathcal{O}_{K'}^\times$$

<u>Def 2.5.4</u>: Die <u>Sprache von Denef-Pas</u> L_{DP} besteht aus 3 Sorten:

<u>Sorte</u>:	<u>Struktur darauf</u>:
VF (bew. Kp)	L_{Ring}
$\overline{VF}$ (Restkl-Kp)	L_{Ring}
Γ_∞ (Wertegruppe $\cup \{\infty\}$)	$L_{oag} = \{0, +, -, <\}$

$$\mathrm{VF} \xrightarrow{ac} \overline{\mathrm{VF}}, \qquad \mathrm{VF} \xrightarrow{v} \Gamma_\infty$$

Wir verwenden HEN, HEN_p, $HEN_{p,q}$ auch für die entsprechenden L_{DP}-Theorien.

<u>Satz 2.5.5</u>: Sei $L \supset L_{DP}$ eine $\overline{VF}$-Γ_∞-Expansion (d.h. durch Symbole, die nur auf $\overline{VF}$ und Γ_∞ leben) und sei $T \supset HEN_{0,0}$ eine L-Theorie. Dann ist jede L-Fml modulo T äquivalent zu einer VF qf-Fml.

<u>Bew</u>: Nach Bem 2.5.2 ist L_{DP} bis auf Interdefinierbarkeit die RV-Expansion $L_{RV} \cup \{ac_{RV}\}$ von L_{RV}. In $L_{RV} \cup \{ac_{RV}\}$ sind $\overline{VF}$ und Γ_∞ $\emptyset$-def'bare TM von RV.

$$\{0\} \cup \{\xi \in RV^\times \mid v_{RV}(\xi) = 0\} \qquad \{\xi \in RV^\times \mid ac(\xi) = 1\} \cup \{0\}$$

Also ist auch L interdefinierbar zu einer RV-Expansion L' von L_{RV}.

Sei φ eine L-Fml. Die ist äquivalent zu einer L'-Fml φ'

Nach 2.2.6 ex. eine VF-qf L'-Fml ψ', die zu φ' äquiv.

ist. Übersetze ψ' zurück in eine L-Fml ψ wie folgt:

- Ersetze jede RV-Variable ξ durch $(\bar{x}, \lambda)$, für $\bar{x}$ $\overline{VF}$-Var., λ Γ_∞-Var
- Ersetze $\xi_1 \cdot \xi_2$ durch $(\bar{x}_1 \cdot \bar{x}_2, \lambda_1 + \lambda_2)$
- Ersetze $\xi_1 + \xi_2 \approx \xi_3$ durch ...... [geeignete L_{DP}-Fml ohne VF-Quantoren]

$\square$

<u>Korollar 2.5.6:</u> Seien $\underline{x}$ VF-Variablen, $\bar{\underline{y}}$ $\overline{VF}$-Var und $\underline{\lambda}$ Γ_∞-Var.

Jede L_{DP}-Fml $\varphi(\underline{x}, \bar{\underline{y}}, \underline{\lambda})$ ist modulo $HEN_{0,0}$ äquivalent zu einer bool. Komb. von Fmln der Form

$$\psi((ac(f_i(\underline{x})))_i, \bar{\underline{y}}) \qquad f_i \in \mathbb{Z}[\underline{x}], \ \psi \ L_{Ring}\text{-Fml}$$

und $$\psi'((v(f_i(\underline{x})))_i, \underline{\lambda}) \qquad f_i \in \mathbb{Z}[\underline{x}], \ \psi' \ L_{oag}\text{-Fml}$$

<u>Bew:</u> Nach 2.5.5. ist φ äquiv. zu einer VFqf-Fml, d.h. φ ist äquiv. zu einer Fml der Form $\chi((ac(f_i(\underline{x})))_i, (v(f_i(\underline{x})))_i, \bar{\underline{y}}, \underline{\lambda})$ für $f_i \in \mathbb{Z}[\underline{x}]$

und χ $L_{Ring} \dot\cup L_{oag}$-Fml
$\uparrow$ auf $\overline{VF}$ $\uparrow$ auf Γ_∞

- Nenne L_{Ring}-Fmln auf $\overline{VF}$ und L_{oag}-Fmln auf Γ_∞ „rein".
- Zeige per Ind über den Aufbau von χ: χ ist äquivalent zu einer bool. Komb. von reinen Fmln:
  - Atomare Fmln sind rein
  - Bleibt z.z: $\exists z : \chi(\dots, z)$ ist äquiv zu bool. Komb. von Reinen, für χ boolkomb von reinen und z entweder $\overline{VF}$- oder Γ_∞-Variable
  - Sei z $\overline{VF}$-Variable (Γ_∞-Variable analog)
  - Ziehe Disjunktionen nach außen. Also ist χ o.E. Konjunktion von reinen Fmln ... sogar: $\chi = \psi \wedge \psi'$, ψ $\overline{VF}$-Fml, ψ' L_{oag}-Fml
  - z kommt nicht in ψ' vor. Also ist $\exists z \chi(z) \Leftrightarrow \exists z : (\psi(z) \wedge \psi')$

$$\Leftrightarrow \underbrace{\psi'}_{\text{reine } \Gamma_{oag}\text{-Fml}} \wedge \underbrace{\exists z \psi(z)}_{\text{reine } \overline{VF}\text{-Fml}}$$

$\square$

Def 2.5.7: Sei L eine Sprache und S eine Sorte von L. Sei M eine L-Struktur.

Die auf S^M <u>induzierte Struktur</u> besteht aus der Menge S^M und für jede L-definierbare Menge $X \subset (S^M)^n$ eine entsprechende n-stellige Relation.

Analog definiere die induzierte Struktur auf $\emptyset$-def'baren Mengen in M.

Korollar 2.5.8: Sei $K \models HEN_{0,0}$ in der Sprache L_{DP}.

(a) Die auf $\bar{K}$ induzierte Struktur ist (bis auf Interdef'barkeit) die L_{Ring}-Struktur.

(b) Die auf Γ_K induzierte Struktur ist (bis auf Interdef'barkeit) die L_{oag}-Struktur.

Bew: (a) • Sei $X \subset \bar{K}^n$ L_{DP}-def'bar. Nach 2.5.6 ist X schon definiert durch

bool. Komb von (i) $\psi((ac(f_i))_i, \bar{y})$ $\quad f_i \in \mathbb{Z} \quad \psi$ L_{Ring}-Fml

und (ii) $\psi'((v(f_i))_i)$ $\quad f_i \in \mathbb{Z} \quad \psi'$ L_{oag}-Fml

(i) $ac(f_i) = f_i$ (als Element von $\bar{K}$), da: $ac(0)=0$; und für $f_i \neq 0$ ist $v(f_i)=0 \Rightarrow ac(f_i) = res(f_i)$ und $res|_{\mathbb{Z}} = id_{\mathbb{Z}}$ (da Ring-Homo)

Bleibt L_{Ring}-Fml

(ii) $\psi'((v(f_i))_i)$ ist Aussage, also in K äquiv zu $\top$ oder zu $\bot$

Also ist die gesamte Fml eine Ring-Fml.

(b) Ganz analog, wobei in (ii): $v(0) \rightsquigarrow \infty$

$v(f_i) \rightsquigarrow 0$ falls $f_i \neq 0$

(Kann das $\infty \in \Gamma_\infty$ dann noch von Hand loswerden.)

Bem: <u>Nicht</u> wahr: Jede L_{DP}-Fml, die nur $\overline{VF}$-Var hat, ist modulo $HEN_{0,0}$ zu einer L_{Ring}-Fml äquivalent.

Korollar 2.5.9 (Satz von Ax-Kochen/Ershov, Version 1): Sei L entweder L_{DP} oder L_{RV}. Sind $K_1, K_2 \models HEN_{0,0}$ mit $\bar{K}_1 \equiv_{L_{Ring}} \bar{K}_2$ und $\Gamma_{K_1} \equiv_{L_{oag}} \Gamma_{K_2}$, so ist $K_1 \equiv_L K_2$

Bew: <u>Fall $L = L_{DP}$:</u> • Sei φ eine L_{DP}-Aussage.

• Nach Korollar 2.5.6 ist φ äquiv. zu b. Komb von reinen ($\overline{VF}$- oder Γ_∞-) Aussagen ψ_i. Nach Annahme habe

$$K_1 \models \psi_i \iff K_2 \models \psi_i$$

• Also $K_1 \models \varphi \iff K_2 \models \varphi$

Fall $L=L_{RV}$: • OE existieren auf K_1, K_2 ang. Komp. (nach 2.5.3).

• Füge solche ang. Komp. zur Sprache hinzu.

• Aus dem L_{DP}-Fall folgt: $K_1 \equiv_{L_{DP}} K_2$

• $\Rightarrow K_1 \equiv_{L_{RV}} K_2$ □

Korollar 2.5.10 (Transferprinzip von Ax-Kochen/Ershov): Sei L entweder L_{RV} oder L_{DP} und sei φ eine L-Aussage. Dann existiert ein $N \in \mathbb{N}$, so dass für alle $K_1, K_2 \models HEN$ (als L-Strukturen) gilt:

Ist $\bar{K}_1 \equiv_{L_{Ring}} \bar{K}_2$ und $\Gamma_{K_1} \equiv_{L_{Oag}} \Gamma_{K_2}$ und char $\bar{K}_1 \geq N$ oder $=0$, so habe

$$K_1 \models \varphi \iff K_2 \models \varphi$$

Bem: Dies gilt insbes. für $K_1 = \mathbb{Q}_p$ und $K_2 = \mathbb{F}_p((t))$ (da $\bar{K}_1 = \bar{K}_2 = \mathbb{F}_p$ und $\Gamma_{K_1} = \Gamma_{K_2} = \mathbb{Z}$)

Bsp: $\varphi =$ „3 ist ein Quadrat"

Für $p \geq 5$: 3 ist Qu. in $\mathbb{Q}_p \iff$ 3 ist Qu in $\mathbb{F}_p \iff$ 3 ist Qu in $\mathbb{F}_p((t))$

Bew (2.5.10): O.E sind K_1, K_2 Modelle von HEN in L_{DP} (mit 2.5.3; ersetze falls nötig K_1, K_2 durch el. Erw). Also ob jetzt $L = L_{DP}$.

Sei ψ eine Aussage wie in 2.5.6, die modulo $HEN_{0,0}$ zu φ äquivalent ist.

Genauer: ψ ist bool. Komb von $\overline{VF}$-Aussagen und Γ_∞-Aussagen.

Nach Kompaktheit folgt $\varphi \Leftrightarrow \psi$ schon aus einer endl. TM von $HEN_{0,0}$; insbes. gilt die Äquivalenz in allen Modellen K von HEN mit char $\bar{K} \geq N$ (für N geeignet).

Für K_1, K_2 wie oben habe:

$$\begin{array}{ccc} K_1 \models \psi & \overset{\bar{K}_1 \equiv \bar{K}_2,\ \Gamma_{K_1} \equiv \Gamma_{K_2}}{\iff} & K_2 \models \psi \\ \Updownarrow & \xleftrightarrow{\text{char}\,\bar{K} \geq N} & \Updownarrow \\ K_1 \models \varphi & & K_2 \models \varphi \end{array}$$

□

Bem: 2.5.10 folgt auch direkt aus 2.5.9 (ohne nochmal QE zu verwenden.)

Bem 2.5.11: 2.5.9 und 2.5.10 gelten auch für $\overline{VF}$-Expansionen von Γ_∞-Expans. von L_{DP}, wobei $\bar{K}_1 \equiv \bar{K}_2$ und $\Gamma_{K_1} \equiv \Gamma_{K_2}$ dann mit den entsprechenden induzierten Strukturen gefordert werden muss.

2.6 Bessere QE in Spezialfällen

Def 2.6.1: DOAG sei die Theorie der divisiblen angeordneten abelschen Gruppen $\neq \{0\}$ in der Sprache $L_{oag} = \{0, +, -, <\}$

Bem: Vgl DLO (dichte angeordnete Mengen ohne Endpt) und DTAG (torsionsfreie divisible ab. Grp)

Satz 2.6.2: DOAG hat QE und ist vollständig.

Bem: Also DOAG $= Th(\mathbb{Q})$

Bew:
- Vollständigkeit folgt aus QE und Existenz eines Primmodells (nämlich $\mathbb{Q}$) (Satz 4.2.10 vom letzen Jahr)
- Bew. von QE:
  - Betrachte $\psi(\underline{z}) = \exists x : \varphi(x, \underline{z})$, φ qf.
  - OE φ konjunktion von $t_1 = t_2$, $t_2 \neq t_2$, $t_1 < t_2$, $t_1 \geq t_2$, für t_1, t_2 L_{oag}-Terme in $x, \underline{z}$
  - Bringe t_2 nach links $\rightsquigarrow$ $t = 0$, $t \neq 0$, $t < 0$, $t \geq 0$
  - t hat die Form $\sum a_i z_i + bx$ für $a_i, b \in \mathbb{Z}$
  - Vereinfache weiter zu: φ ist Konj von $b_j x = \sum a_{ij} z_i$, $b_j x < \sum a_{ij} z_i$, $b_j x > \sum a_{ij} z_i$
  - Kann annehmen: Alle b_j sind ≥ 1.
  - Kann annehmen: Alle b_j sind gleich einem b. (Ersetze durch das kgV)
  - Kann jetzt überall bx durch x ersetzen: (Die neue Aussage sei $\exists x : \varphi'(x)$. Dann ist die alte Aussage $\exists x : \varphi'(bx)$. Diese Aussagen sind äquiv, da divisibel)
  - Falls in φ ein $x = \underbrace{\sum a_{ij} z_i}_{(*)}$ vorkommt: Setze $(*)$ in den Rest von φ für x ein und entferne $\exists x$.
  - $\exists x\, \varphi(x, \underline{z})$ ist wahr genau dann wenn jede untere Schranke an x kleiner als jede obere Schranke an x ist. (Wähle z.B. $x = \frac{\text{kleinste ob. Schr} + \text{gr. unt. Schr}}{2}$) $\square$

Satz 2.6.3: Die Theorie $ACVF_{0,0}$ (alg. abg. nicht-triv. bew. Körper der Char. $(0,0)$) hat in L_{op} (vollständige) QE.

Bew: $K \models ACVF_{0,0} \Rightarrow \bar{K} \models ACF_0 \Rightarrow \bar{K}$ hat QE in L_{Ring}

—"— $\Rightarrow \Gamma_K \models DOAG \Rightarrow \Gamma_K$ hat QE in L_{oag}

Mit 2.5.6 folgt: K hat QE. $\square$

Def 2.6.4: Die Presburger-Sprache ist $L_{Pres} = \{0, +, -, <, 1\} \cup \{\equiv_\ell \mid \ell \geq 1\}$, wobei $\equiv_\ell$ eine binäre Relation ist, die in $\mathbb{Z}$ interpretiert wird als:

$a \equiv_\ell b :\Leftrightarrow a \equiv b \mod \ell$ (d.h. $\ell \mid a-b$).

Satz 2.6.5: $\mathbb{Z}$ hat QE in der Sprache L_{Pres}.

Bew: Beweis ähnlich wie bei 2.5.2:

- $\psi(\underline{z}) = \exists x\, \varphi(x, \underline{z})$
- φ ist o.E. Konjunktion von $b_j x \begin{Bmatrix} = \\ < \\ > \\ \equiv_{\ell_j} \end{Bmatrix} \sum a_{ij} z_i + c_j$ $\qquad b_j, a_{ij}, c_j \in \mathbb{Z}$
- O.E. alle b_j gleich b
- Ersetze $\exists x\, \varphi'(bx, \underline{z})$ durch $\exists x \left(\varphi'(x, \underline{z}) \wedge x \equiv_b 0\right)$

  Auf diese Art: o.E. $b = 1$
- Falls „$x = \ldots$" in φ vorkommt: Setze das für x ein und entferne $\exists x$.
- (□) Für jede Kongruenz-Bed. $x \equiv_{\ell_j} \sum a_{ij} z_i + c_j$:

  Mache Fallunterscheidung nach Kongruenzklasse $\sum a_{ij} z_i + c_j \mod \ell_j$

  Auf diese Art reduziere zu: $x \equiv_{\ell_j} c_j'$
- Die Konjunktion aller in φ auftretenden Kongruenz-Bed. ist entweder immer falsch oder äquiv. zu einer einzigen Kongruenz-Bed. $x \equiv_\ell c$ (nach Chin. Restsatz). $\quad c \in \{0, \ldots, \ell-1\}$
- O.E. max eine obere und max eine untere Schranke an x (durch Fallunterscheidung danach, welche Schranke die schärfste ist).
- O.E. $\varphi = x > \sum a_{i1} z_i + c_1 \wedge x < \sum a_{i2} z_i + c_2 \wedge x \equiv_\ell c$

  (Falls eine Schranke nicht existiert, ist $\exists x \varphi$ immer wahr)
- O.E. ist die untere Schranke „$x > -1$" (sonst ersetze x durch $x - \sum a_{i1} z_i + c_1 + 1$; wiederhole (□)) $\quad -1?$

- $\exists x\, \varphi(x)$ ist wahr gdw. $\sum a_{i2} z_i + c_2 > c$. $\square$