Modelltheorie II

:= Modelltheorie bewerteter Körper

§1 Bewertete Körper

Tauchen auf in der Zahlentheorie:

- Vervollständigungen von $\mathbb{Q}$
- $\mathbb{Q}$ „kennt" die Primzahlen
- $K[X]$, $a \in K$, $f \in K[X]$
  Vielfachheit der Nst a von f
- In Algebra-Vorlesung:
  - R faktoriell $\Rightarrow R[X]$ faktoriell
  - Eisensteinsches Irred-Krit.
- $\mathbb{R} \prec \mathbb{R}^*$ „Größenordnung" von Elementen

Ziele: • Modelltheorie von „netten" bew. Körpern „verstehen"
(QE, Dimensionstheorie, IE?)

Literatur: Engler, Prestel: Valued fields

§ 1.1 Beträge

Def. 1.1.1: Sei K ein Körper. Ein <u>Betrag</u> (Betragsfunktion) auf K ist eine Abb. $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ mit: $\forall x, y \in K$:

(a) $|x| = 0 \iff x = 0$

(b) $|x \cdot y| = |x| \cdot |y|$

(c) $|x + y| \leq |x| + |y|$ (Dreiecksungleichung)

Bsp 1.1.2: $K = \mathbb{R}$: $|x|_{\mathbb{R}} := \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$

Bsp 1.1.3: $K = \mathbb{C}$ $\quad |x + iy|_{\mathbb{C}} := \sqrt{x^2 + y^2}$ $\quad (x, y \in \mathbb{R})$

Bsp: Auf $K = \mathbb{C}$. $\underbrace{|x + iy|}_{z} := \sqrt[4]{x^2 + y^2} = \sqrt{|x + iy|_{\mathbb{C}}}$ $\quad (x, y \in \mathbb{R})$

$$|z + z'| = \sqrt{|z + z'|_{\mathbb{C}}} \overset{?}{\leq} |z| + |z'| = \sqrt{|z|_{\mathbb{C}}} + \sqrt{|z'|_{\mathbb{C}}}$$

$$\Updownarrow$$

$$|z + z'|_{\mathbb{C}} \leq |z|_{\mathbb{C}} + \underbrace{2 \cdot \sqrt{|z|_{\mathbb{C}} \cdot |z'|_{\mathbb{C}}}}_{\geq 0} + |z'|_{\mathbb{C}}$$

$$\text{—''—} \leq \text{—''—} \qquad + \qquad \text{—''—}$$

Bsp 1.1.4: K beliebig. $|x|_0 := \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$

Bem 1.1.5: Es gilt:

(a) $|1| = 1$

(b) $|x| = |-x| \quad \forall x \in K$

(c) $\left|\frac{1}{x}\right| = \frac{1}{|x|} \quad \forall x \in K^\times$

Bew: (a) $|1| \cdot |1| = |1| \Rightarrow |1| = 1$

(b) $|-1| \cdot |-1| = |(-1) \cdot (-1)| = 1 \Rightarrow |-1|^2 = 1 \Rightarrow |-1| = 1$

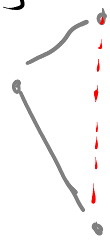
$\Rightarrow |-x| = |(-1) \cdot x| = |-1| \cdot |x| = |x|$

(c) $\left|\frac{1}{x}\right| \cdot |x| = \left|\frac{1}{x} \cdot x\right| = |1| = 1$ $\quad \square$

Def 1.1.6: Ein Betrag $|\cdot|$ heißt <u>nicht-archimedisch</u> wenn die <u>ultrametrische Dreiecks-Ungl.</u> gilt, d.h.:

$$\forall x,y \in K: \quad |x+y| \leq \max\{|x|,|y|\}$$

Sonst heißt $|\cdot|$ <u>archimedisch</u>.



Bsp:
- $|\cdot|_0$ ist nicht-arch.
- $|\cdot|_{\mathbb{R}}, |\cdot|_{\mathbb{C}}$ sind arch.

Bsp. 1.1.7: Sei p eine Primzahl. Definiere den p-adischen Betrag $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$ durch:

- $|0|_p := 0$
- Für $x = p^r \cdot \frac{m}{n} \in \mathbb{Q}^\times \qquad r \in \mathbb{Z}, \; m,n \in \mathbb{Z}, \; p \nmid m,n$:

$$|x|_p := p^{-r}$$

Dies ist ein nicht-arch. Betrag.

Bew: (a) ✓

(b) $x = p^r \cdot \frac{m}{n}, \quad x' = p^{r'} \cdot \frac{m'}{n'} \quad \Rightarrow \quad x \cdot x' = p^{r+r'} \cdot \frac{m \cdot m'}{n \cdot n'}$

$$|x \cdot x'|_p = p^{-(r+r')} = p^{-r} \cdot p^{-r'} = |x|_p \cdot |x'|_p$$

(c) O.E. $r \leq r' \qquad (\Leftrightarrow |x|_p \geq |x'|_p.)$

$$x+y = p^r \cdot \frac{m}{n} + p^{r'} \cdot \frac{m'}{n'}$$

$$= p^r \cdot \underbrace{\left(\frac{m}{n} + p^{r'-r} \cdot \frac{m'}{n'}\right)}_{= \frac{mn' + p^{r'-r} \cdot m' \cdot n}{n \cdot n'}}$$

$mn' + p^{r'-r} \cdot m' \cdot n = p^s \cdot m''$

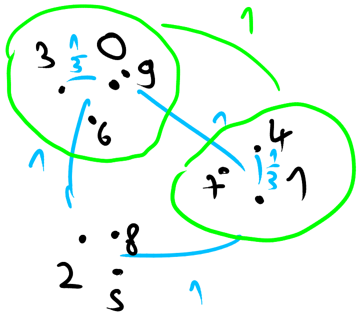
$n \cdot n' \longleftarrow p \nmid n \cdot n'$

$$= p^{r+s} \cdot \frac{m''}{n \cdot n'}$$

$$\Rightarrow |x+y|_p = p^{-(r+s)} = p^{-r} \cdot p^{-s} = |x|_p \cdot p^{-s} \leq |x|_p \qquad \square$$

Anschauung: $|a-b|$ gibt den „Abstand" zw. a und b an.

$\mathbb{Q}$ mit $|\cdot|_3$:



$|1|_3 = 1$

$|2|_3 = 1$

$|3|_3 = 3^{-1}$

$|4|_3 = 1$

$\vdots$

$|6|_3 = 3^{-1}$

$\vdots$

$|9|_3 = 3^{-2}$

$\vdots$

$\left|\frac{1}{3}\right|_3 = 3$

$\cdot \frac{1}{3}$

Änderung

Bsp 1.1.8: Sei K ein Körper und $a \in K$. Setze $p := x - a$.

Definiere $|\cdot|_p : K(X) \longrightarrow \mathbb{R}_{\geq 0}$ durch:

$$|0|_p := 0$$

$$\left|\frac{f}{g}\right|_p := e^{-v\left(\frac{f}{g}\right)} \quad \text{wobei} \quad f, g \in K[X] \setminus \{0\}$$

$v_p\left(\frac{f}{g}\right) :=$ Vielfachheit von a als NST von f − Vielfachheit von a als NST von g.

Allgemeiner, für $p \in K[X]$ irred.:

Für $h = p^r \cdot \frac{\hat{f}}{\hat{g}}$, $\hat{f}, \hat{g} \in K[X] \setminus \{0\}$, $h \in K(X)^\times$, $p \nmid \hat{f}, \hat{g}$

setze $v_p(h) = r$ und $|h|_p := e^{-v_p(h)}$

Dies ist ein nicht-arch. Betrag.

Bsp. 1.1.9: Sei K ein Körper.

Definiere $|\cdot|_\infty : K(X) \longrightarrow \mathbb{R}_{\geq 0}$ durch:

$$|0|_\infty := 0$$

$$\left|\frac{f}{g}\right|_\infty := e^{-v\left(\frac{f}{g}\right)} \quad f, g \in K[X] \setminus \{0\}$$

$v\left(\frac{f}{g}\right) = \deg g - \deg f =$ „Vielfachheit der NST bei ∞"

Dies ist ein nicht-arch. Betrag.

Satz 1.1.10 (Satz von Ostrowski): Die einzigen Beträge auf $\mathbb{Q}$ sind:

- $|\cdot|_0$
- $x \longmapsto |x|_{\mathbb{R}}^\lambda$ $\quad \lambda \in (0, 1]$
- $x \longmapsto |x|_p^\lambda$ $\quad \lambda > 0$

Lemma 1.1.11: Sei $(K, |\cdot|)$ ein Kp. mit Betrag und sei

$$A := \{ |n\cdot 1| \mid n \in \mathbb{Z} \}.$$

(1) Ist $|\cdot|$ archimedisch, so ist A unbeschränkt.

(2) Ist $|\cdot|$ nicht-arch, so ist $A \subset [0,1]$

Bew: (2) Reicht, $|n|$ für $n \geq 0$ zu betrachten. Ind. über n:

$$|n+1| \leq \max\{\underbrace{|n|}_{\substack{\leq 1 \\ (\text{Ind.})}}, \underbrace{|1|}_{\substack{= \\ 1}}\} \leq 1.$$

(1) Ann A ist beschränkt, d.h. $|n| \leq C \quad \forall n \quad (C \in \mathbb{R})$.

Zid: Folgere: $|\cdot|$ ist nicht-arch. $\qquad (x,y \in K,\ n \in \mathbb{N},\ n \geq 1)$

$$|x+y|^n = |(x+y)^n| = \left| \sum_{i=0}^n \binom{n}{i} x^i y^{n-i} \right|$$

$$\leq \sum_{i=0}^n \left| \binom{n}{i} x^i y^{n-i} \right| = \sum_{i=0}^n \underbrace{\left|\binom{n}{i}\right|}_{\leq C} \underbrace{|x|^i \cdot |y|^{n-i}}_{\leq \max\{|x|,|y|\}^n} \leq (n+1)\, C \cdot \max\{|x|, |y|\}^n$$

$\sqrt[n]{\ }$ ziehen: $|x+y| \leq \underbrace{\sqrt[n]{(n+1)\cdot C}}_{\to 1} \cdot \max\{|x|, |y|\}$

Für $n \to \infty$:

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

$\square$

Bew 1.1.10: Sei $|\cdot|$ ein Betrag auf $\mathbb{Q}$.

- Es reicht $|n|$, für $n \in \mathbb{N}$ zu bestimmen, da:
  - $|-n| = |n|$
  - $\left|\frac{m}{n}\right| = \frac{|m|}{|n|}$

- **Bem:** (*) $|n| = |\underbrace{1 + \ldots + 1}_{n \text{ mal}}| \leq |\underbrace{1 + \ldots + 1}_{n-1 \text{ mal}}| + |1| \leq \ldots \leq \underbrace{|1| + \ldots + |1|}_{\substack{n \text{ mal} \\ = n}}$

- Seien $a, b \in \mathbb{N}$, $a, b \geq 2$. Zid: Vergleiche $|a|, |b|$.
  - Schreibe b^n in Basis a, d.h. $b^n = c_0 + c_1 \cdot a + c_2 a^2 + \ldots + c_m a^m$

    mit $c_i \in \{0, 1, \ldots, a-1\}$, $m \leq \log_a(b^n) = n \cdot \log_a b$

    $\Updownarrow$

    $a^m \leq b^n$

- $|b|^n = |b^n| = \left|\sum_{i=0}^{m} c_i a^i\right| \le \sum_{i=0}^{m} \underbrace{|c_i|}_{\le c_i < a} \cdot \underbrace{|a|^i}_{\le \max\{|a|^m, 1\}}$

$$\le (m+1)\cdot a \cdot \max\{|a|^m, 1\}$$

$$\le (n \log_a b + 1)\cdot a \cdot \max\{|a|^{n \log_a b}, 1\}$$

$$\Rightarrow |b| \le \underbrace{\sqrt[n]{n(\log_a b + 1)\cdot a}}_{\to 1} \cdot \max\{|a|^{\log_a b}, 1\}$$

- Für $n \to \infty$:

(*) $\quad |b| \le \max\{|a|^{\log_a b}, 1\}$

- Fall 1: Für alle $a \ge 2$ ist $|a| > 1$ (Insbes. $|\cdot|$ archimedisch)

Dann: $|b| \le |a|^{\log_a b}$ Kehrwerte voneinander

$|a| \le |b|^{\log_b a}$

$$|a| \le |b|^{\log_b a} \le \left(|a|^{\log_a b}\right)^{\log_b a} = |a|$$

$\Rightarrow \quad = \quad =$

Wähle λ s.d. $|2| = 2^{\lambda}$.

$$\Rightarrow |b| = |2|^{\log_2 b} = 2^{\lambda \log_2 b} = b^{\lambda} \qquad \forall\, b \ge 2$$

Bleibt z.z.: $0 < \lambda \le 1$

- $|2| > 1$ nach Annahme $\Rightarrow \lambda > 0$

  $|2| \le 2$ nach (*) $\Rightarrow \lambda \le 1$

- Fall 2: Ex. $a \ge 2$ mit $|a| \le 1$.

Aus (*) folgt: $|b| \le 1 \quad \forall\, b \ge 2$ (Insbes. $|\cdot|$ nicht-arch)

- Falls $|b| = 1 \quad \forall\, b \ge 2$: $|\cdot|$ trivial $\Rightarrow$ fertig

Also o.E. $|a| < 1$.

- Sei $a = \prod_i p_i^{r_i}$ die Primfaktorzerlegung

$\Rightarrow |a| = \prod_i |p_i|^{r_i}$

$\Rightarrow$ Ex. Primzahl p mit $|p| < 1$

- Ann. q ist eine weitere Primzahl mit $|q| < 1$.
  - Wähle $e \in \mathbb{N}$ s.d. $|p|^e, |q|^e < \frac{1}{2}$
  - Finde $m, n \in \mathbb{Z}$ s.d. $m \cdot p^e + n \cdot q^e = 1$

$$\Rightarrow |1| = |m\cdot p^e + n\cdot q^e| \leq \underbrace{|m|}_{\leq 1}\cdot \underbrace{|p|^e}_{<\frac{1}{2}} + \underbrace{|n|}_{\leq 1}\cdot \underbrace{|q|^e}_{<\frac{1}{2}} < 1 \quad \lightning$$

Also: $|q| = 1$ für alle Primzahlen $q \neq p$.

- $b \in \mathbb{N}$ beliebig $\Rightarrow |b| = |\underbrace{\prod_i p_i^{s_i}}_{\text{Primfaktorzerl. von } b,\ \text{o.E. } p_1 = p}| = \prod_i |p_i|^{s_i} = |p_1|^{s_1}$

Also: Für $b = p^r \cdot m$, $p \nmid m$ habe $|b| = |p|^r = (p^{-r})^\lambda$

für λ so, dass $p^{-\lambda} = |p|$

$(|p| < 1 \Rightarrow \lambda > 0)$ $\square$

§ 1.2 Vervollständigungen

__Lemma 1.2.1:__ Sei $(K, |\cdot|)$ ein Körper mit Betrag. Dann ist $d(a,b) := |a-b|$ eine Metrik auf K.

Addition, Multiplikation, $a \mapsto -a$, $\underbrace{a \mapsto \frac{1}{a}}_{\text{für } a \neq 0}$ sind stetig bezügl. dieser Metrik.

__Bew:__ Metrik: Klar

__Stetigkeit von +:__ Seien a,b gegeben. Seien a',b' mit $|a-a'| < \delta$, $|b-b'| < \delta$

z.z. $|(a'+b') - (a+b)| < \varepsilon$ (Genauer: $\forall \varepsilon \exists \delta \ldots$)

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

__Stetigkeit von −:__ Genauso trivial

__Stetigkeit von $\cdot$:__ Seien a,b gegeben. Seien a',b' mit $|a-a'| < \delta$, $|b-b'| < \delta$

(*)
$$|a'\cdot b' - a\cdot b| = |(a'-a)b + a\cdot(b'-b) + (a'-a)(b'-b)|$$
$$\cancel{a'b} - ab + \cancel{ab'} - \cancel{ab} + a'b' - \cancel{ab'} - \cancel{a'b} + \cancel{ab}$$
$$\leq \delta |b| + |a|\cdot\delta + \delta^2$$

__Stetigkeit von $a \mapsto \frac{1}{a}$:__ a geg. Sei a' mit $|a-a'| < \delta$

Wähle δ so klein, dass $\delta < \frac{1}{2}\cdot|a|$

$$\left|\frac{1}{a}-\frac{1}{a'}\right| = \left|\frac{a'-a}{aa'}\right| \leq \frac{\delta}{|a|\cdot\frac{1}{2}|a|}$$

NR: $a' + (a-a') = a$

$\Rightarrow |a| \leq |a'| + \underbrace{|a-a'|}_{\leq \delta < \frac{1}{2}|a|}$

$\Rightarrow |a'| \geq |a| - \frac{1}{2}\cdot|a| = \frac{1}{2}|a|$

$\square$

Satz 1.2.2: Sei $(K, |\cdot|)$ ein Körper mit Betrag und $\hat{K}$ die Vervollständigung. Dann lassen sich $+, \cdot, -, x \mapsto \frac{1}{x}$ und $|\cdot|$ (eindeutig) stetig auf $\hat{K}$ fortsetzen, und $\hat{K}$ wird so auch ein Körper mit Betrag.

Bsp. 1.2.3: $(\mathbb{Q}, |\cdot|_{\mathbb{R}}) \rightsquigarrow \hat{\mathbb{Q}} = \mathbb{R}$

Bsp: $|\cdot|$ trivialer Betrag auf $K \Rightarrow \hat{K} = K$

Bew: • Sei $(a_i)_{i\in\mathbb{N}} \in \hat{K}$. Dann existiert „$\lim |a_i| = \lim d(a_i, 0)$" und $(a_i \in K)$

$\|(a_i)_i\| = d((a_i)_i, 0) \leftarrow$ in $\hat{K}$

ist eine wohldefinierte stetige Fkt $\hat{K} \to \mathbb{R}_{\geq 0}$

Insbes ist $|a_i|$ beschränkt (für a_i Cauchy-Folge)

• **Beh:** Die Menge der Cauchy-Folgen in K bildet einen Ring.

- Abg unter $+, -$: leicht.
- Abg unter $\cdot$: Seien $(a_i)_i$, $(b_i)_i$ Cauchy-Folgen

Seien $|a_i|$ durch A und $|b_i|$ durch B beschränkt.

Sei N so groß dass $|a_i - a_j| < \delta$, $|b_i - b_j| < \delta$ $\forall i, j \geq N$

$$|a_ib_i - a_jb_j| \overset{(*)}{\leq} \delta\cdot|a_i| + \delta\cdot|b_i| + \delta^2 \leq \delta\cdot A + \delta\cdot B + \delta^2$$
$$\leq \delta\cdot(A + B + \delta)$$

• **Beh:** Die Menge der Nullfolgen bildet ein Ideal.

- Abg. unter $+, -$: leicht.
- $(a_i)_i$ Chauchy, $(b_i)_i$ 0-Folge $\Rightarrow (a_ib_i)_i$ Nullfolge.

$(\ |a_i \cdot b_i| \leq A\cdot|b_i|\ )$

Schranke für $|a_i|$

- $\hat{K} = \text{Cauchyfolgen} / \text{Nullfolgen}$

- Beh: Die Menge der Nullfolgen bildet ein maximales Ideal.
  (Dann: $\hat{K}$ Körper)

  Zeige sogar: $(a_i)_i$ Cauchy, nicht Nullfolge $\Rightarrow (a_i)_i$ invertierbar,
  d.h. $\left(\frac{1}{a_i}\right)_i$ bilden Cauchy-Folge.

  - $(a_i)_i$ nicht 0-Folge $\Rightarrow$ O.E. kein $a_i = 0$.
    $$\Rightarrow \lim_i |a_i| \neq 0$$
    $$\Rightarrow \exists\, C > 0 \ \forall i: |a_i| > C$$
  - Sei N so, dass $|a_i - a_j| < \delta \quad \forall i,j > N$.
  - $$\left|\frac{1}{a_i} - \frac{1}{a_j}\right| = \left|\frac{a_j - a_i}{a_i a_j}\right| \leq \frac{\delta}{C^2}$$

- Prüfe noch: $|\cdot|$ ist ein Betrag auf $\hat{K}$
  - $|(a_i)_i| = 0 \overset{?}{\Leftrightarrow} (a_i)_i = 0$ in $\hat{K}$
    $$\Updownarrow$$
    $(a_i)_i$ ist Nullfolge
  - $$|(a_i)_i \cdot (b_i)_i| \overset{?}{=} |(a_i)_i| \cdot |(b_i)_i|$$
    $$\lim_i (|a_i||b_i|) = (\lim_i |a_i|)(\lim_i |b_i|)$$
  - $$|(a_i)_i + (b_i)_i| \overset{?}{\leq} |(a_i)_i| + |(b_i)_i|$$
    $$\lim_i (|a_i| + |b_i|) \leq (\lim_i |a_i|) + (\lim_i |b_i|)$$

$\square$

Def 1.2.4: Sei p eine Primzahl. Die Menge der <u>p-adischen Zahlen</u> ist die Menge der formalen Summen der Form
$$\mathbb{Q}_p := \left\{ \sum_{i \geq N} r_i p^i \;\middle|\; N \in \mathbb{Z},\ \forall i: 0 \leq r_i < p \right\}$$
Die Summe und das Produkt von p-adischen Zahlen sind so definiert wie bei der Darstellung von Zahlen in Basis p.

Der (p-adische) Betrag $|a|_p$ von $a = \sum_{i \geq N} r_i p^i$ mit $r_N \neq 0$ ist p^{-N}; $|0|_p := 0$. Die <u>ganzen p-adischen Zahlen</u> sind

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

Bsp: $p = 5$

- $$\begin{array}{l} 1 \cdot 5^0 + 3 \cdot 5^1 + 4 \cdot 5^3 \\ + 4 \cdot 5^{-1} + 2 \cdot 5^1 + 2 \cdot 5^3 \\ \hline 4 \cdot 5^{-1} + 1 \cdot 5^0 + 0 \cdot 5^1 + 1 \cdot 5^2 + 1 \cdot 5^3 + 1 \cdot 5^4 \end{array} \qquad \begin{array}{r} 4031_5 \\ + \; 2020{,}4 \\ \hline 11101{,}4 \end{array}$$

- $\sum_{i \geq 0} 4 \cdot p^i$ $\qquad \ldots 44444_5$

  $1 \cdot p^0$ $\qquad + \quad 1$

  $\ldots 00000$

(nicht auch)

Satz 1.2.5: $(\mathbb{Q}_p, |\cdot|_p)$ ist ein Körper mit Betrag; es ist isomorph zur Vervollst von $\mathbb{Q}$ bzgl $|\cdot|_p$. $\mathbb{Z}_p$ ist der topologische Abschluss von $\mathbb{Z}$ in $\mathbb{Q}_p$.

Bsp: $\underset{\substack{\| \\ 4}}{\overset{a_1}{\underset{\|}{4_5}}}, \underset{\substack{\| \\ 5 \cdot 4 + 4 = 24}}{\overset{a_2}{\underset{\|}{44_5}}}, \underset{\substack{\| \\ 124}}{\overset{a_3}{\underset{\|}{444_5}}}, \ldots \in \mathbb{Q}$

$(a_i)_i$ ist Cauchy-Folge bzgl $|\cdot|_5$:

$|a_1 - a_2|_5 = 5 \cdot 4 = 5^{-1}$

$|a_2 - a_3|_5 = 4 \cdot 5^2 = 5^{-2}$

Bew: • $\mathbb{Q}_p$ mit $(+, \cdot)$ ist ein Ring (und $\mathbb{Z}_p$ ein Unterring)

- Assoz, Komm, Distrib: Nachrechnen wie bei Darstellung von Zahlen in Basis p.
- $\sum_i 0 \cdot p^i = 0$ ist additiv neutrales Elem
- $1 \cdot p^0 =: 1$ ist multiplikativ neutrales Elem
- $-\left(\sum_{i \geq N} r_i p^i \right) = \sum_{i \geq N} (p - 1 - r_i) p^i + 1 \cdot p^N$

  $\sum_{i \geq N} (p - 1 - r_i) p^i + 1 \cdot p^N + \sum_{i \geq N} r_i p^i$

$$=\underbrace{\big((p-1-r_N)+1+r_N\big)}_{=p}p^N+(p-1-r_{N+1}+r_{N+1})\cdot p^{N+1}$$
$$+(p-1-r_{N+2}+r_{N+2})\cdot p^{N+2}+\dots$$

$$=0\cdot p^N+0\cdot p^{N+1}+0\cdot p^{N+2}+\dots$$

- $|\cdot|_p$ auf $\mathbb{Q}_p$ erfüllt die Betrags-Axiome (und induziert deshalb eine Metrik)
  - $|a|_p=0 \iff a=0$ ✓
  - $$\Big|\underbrace{\sum_{i\geq N} r_i p^i}_{\substack{r_N\neq 0\\ |\cdot|_p=p^{-N}}}\cdot \underbrace{\sum_{i\geq M} s_i p^i}_{\substack{s_M\neq 0\\ |\cdot|_p=p^{-M}}}\Big|_p=\Big|\underbrace{\sum_{i\geq N}\sum_{j\geq M} r_i s_j p^{i+j}}_{=\sum_\ell\left(\sum_{i+j=\ell} r_i s_j\right)p^\ell=\sum_\ell t_\ell p^\ell,\ 0\leq t_\ell<p}\Big|_p=(*)$$

$\ell=N+M \Rightarrow \sum_{i+j=\ell} r_i s_j = r_N s_M \neq 0$

$\ell<N+M \Rightarrow \sum_{i+j=\ell} r_i s_j = 0$ (da $i<N$ oder $j<M$)

$\Rightarrow t_\ell=0\ \forall \ell<M+N$

sogar: nicht durch p teilbar, da s_M, s_N nicht durch p teilbar

$\Rightarrow t_{M+N}\neq 0$

$\Rightarrow (*)=p^{-(M+N)}$

- $$\Big|\underbrace{\sum_{i\geq N} r_i p^i+\sum_{i\geq M} s_i p^i}_{\sum_{i\geq K}(r_i+s_i)\cdot p^i}\Big|_p\leq \max\Big\{\Big|\underbrace{\sum_{i\geq N} r_i p^i}_{\substack{r_N\neq 0\\ |\cdot|=p^{-N}}}\Big|_p,\Big|\underbrace{\sum_{i\geq M} s_i p^i}_{\substack{s_M\neq 0\\ |\cdot|=p^{-M}}}\Big|_p\Big\}$$

$K\geq \min\{M,N\}$

$|\cdot|=p^{-K}\leq p^{-\min\{M,N\}}=\max\{p^{-M},p^{-N}\}$

• $\mathbb{Q}_p$ ist vollst. bezüglich der von $|\cdot|_p$ induzierten Metrik:

• Sei $(a_i)_{i\in\mathbb{N}}$ eine Cauchy-Folge,

$$a_i = \sum_{j\geq N_i} r_{ij}\, p^j$$

• Nach Ausdünnung kann annehmen: $|a_i - a_{i+1}|_p \leq p^{-(i+1)}$

d.h. $a_i - a_{i+1} = \sum_{j\geq i+1} s_j\, p^j$

$$\begin{array}{c} \| \\ \sum_j (r_{ij} - r_{i+1,j})\, p^j \end{array}$$

$$\Rightarrow r_{ij} = r_{i+1,j} \quad \forall j \leq i$$

$$\begin{array}{llllll} a_0 & r_{0N_0}, & \cdots, & r_{00}, & r_{01}, & r_{02}, \cdots \\ & \| & \cdots & \| & & \\ a_1 & r_{1N_0}, & \cdots, & r_{10}, & r_{11}, & r_{12}, \cdots \\ & \| & \cdots & \| & \| & \\ a_2 & r_{2N_0}, & \cdots, & r_{20}, & r_{21}, & r_{22} \\ & \| & & \| & \| & \| \\ a_3 & & & & & \end{array}$$

• Setze $a := \sum_{j=N_0}^{-1} r_{0j}\, p^j + \sum_{j=0}^{\infty} r_{jj}$

Beh: $a = \lim_i a_i$

$$|a - a_i|_p < p^{-i}$$

• $\mathbb{Z}_p$ ist die Vervollst. von $\mathbb{Z}$ bezgl. $|\cdot|_p$ (mit der natürlichen Einbettung $\mathbb{Z} \longrightarrow \mathbb{Z}_p$ (für pos. Zahlen: Darstellungen in Basis p)):

z.z.: • $\mathbb{Z}_p$ vollst. (da für $a_i \in \mathbb{Z}_p$ Cauchy gilt: $\lim_i a_i \in \mathbb{Z}_p$)

• $|\cdot|_p$ auf $\mathbb{Z}$ und auf $\mathbb{Z}_p$ stimmen überein.

$a \in \sum_{i=N}^{M} r_i\, p^i \in \mathbb{Z}$, $r_N \neq 0$ $\Rightarrow$ $|a|_p = p^{-N}$ ← $\mathbb{Z}_p$-Sinn

$= p^N \cdot \sum_{i=0}^{M-N} r_{i+N}\, p^i \Longrightarrow |a|_p = p^{-N}$ ← $\mathbb{Z}$-Sinn

$$\begin{array}{ccccc} \mathbb{Q} & \subset & \hat{\mathbb{Q}} & \overset{(2)}{\supseteq} & \mathbb{Q}_p \\ \cup & & \cup & & \\ & & \mathrm{Quot}\,\hat{\mathbb{Z}} & \overset{(1)}{\supseteq} & \\ & & \cup & & \cup \\ \mathbb{Z} & \subset & \hat{\mathbb{Z}} = \mathbb{Z}_p & & \end{array}$$

• $\mathbb{Z}$ ist dicht in $\mathbb{Z}_p$: $a = \sum_{i\geq 0} r_i\, p^i \in \mathbb{Z}_p$ ist Limes von

$$a_j := \sum_{i=0}^{j} r_i\, p^i \in \mathbb{Z}$$

(1) • $\mathbb{Q}_p$ ist in der $\underbrace{\text{Vervollst. von } \mathbb{Q}}_{=:\,\hat{\mathbb{Q}}}$ enthalten, da:

• $\mathbb{Z}_p = \hat{\mathbb{Z}} \subset \hat{\mathbb{Q}}$

• $\hat{\mathbb{Q}}$ Körper $\Rightarrow \mathrm{Quot}\,\mathbb{Z}_p \subset \hat{\mathbb{Q}}$

- $\mathbb{Q}_p \subset \operatorname{Quot} \mathbb{Z}_p$, da für $a = \sum_{i \geq N} r_i p^i \in \mathbb{Q}_p$ gilt: Falls $N \geq 0$: $a \in \mathbb{Z}_p$.
  Falls $N < 0$

$$a = \frac{\overbrace{\sum_{i \geq 0} r_{i-N} \cdot p^i}^{\in \mathbb{Z}_p}}{\underbrace{p^{-N}}_{\in \mathbb{Z}_p}}$$

- Um zu zeigen, dass $\mathbb{Q}_p = \hat{\mathbb{Q}}$ ist, bleibt z.z.: $\mathbb{Q}_p \supset \hat{\mathbb{Q}}$:

(2) Dazu bleibt z.z.: $\mathbb{Q} \subset \mathbb{Q}_p$

Dazu zu zeigen: $\frac{1}{q} \in \mathbb{Q}_p \;\; \forall q$ prim

- Falls $q = p$: $\frac{1}{q} = 1 \cdot p^{-1}$ ✓
- Falls $q \neq p$:

Finde Folge $(a_i)_{i \in \mathbb{N}}$, $a_i \in \mathbb{Z}$ s.d. $\lim_{i \to \infty} a_i = \frac{1}{q}$

im Sinne von $|\cdot|_p$, d.h. $\lim |a_i - \frac{1}{q}|_p = 0$

Möchte dafür $|\underbrace{a_i - \frac{1}{q}}_{\frac{1}{q} \cdot (q a_i - 1)}|_p \leq p^{-i}$

$|\frac{1}{q}|_p = 1$

$$|q a_i - 1|_p \leq p^{-i}$$
$$\Updownarrow$$
$$p^i \mid q a_i - 1$$
$$\Longleftrightarrow \exists z: z \cdot p^i = q a_i - 1$$

Da q und p^i teilerfremd, existieren solche z und a_i nach dem chin. Restsatz.

$\square$

Bsp: $\frac{1}{2} \in \mathbb{Q}_3$? Gesucht ist $\sum_{i=0}^{\infty} r_i p^i =: a$ mit $2 \cdot a = 1$

$a_0 := r_0, \quad \underbrace{r_0 + r_1 \cdot p}_{a_1}, \quad \underbrace{r_0 + r_1 p + r_2 p^2}_{a_2}, \; \ldots \; \longrightarrow \frac{1}{2}$

Wähle r_0 so, dass $|2a_0 - 1|_3 \leq 3^{-1}$, d.h. $3 \mid 2a_0 - 1$

$r_0 = 2$ tut's

Wähle r_1 so, dass $|2a_1 - 1|_3 \leq 3^{-2}$, d.h. $9 \mid \underbrace{2a_1 - 1}$

$2\cdot(2+3\cdot r_1) - 1$

$r_1 = 2$ tut's. $\qquad 3 + 3r_1$

...

<u>Anmerkung:</u> Noch eine Möglichkeit, $\mathbb{Z}_p$ und $\mathbb{Q}_p$ zu definieren:

$$\mathbb{Z}_p = \varprojlim_i \mathbb{Z}/p^i\mathbb{Z} := \{(z_i)_{i\in\mathbb{N}} \mid \forall i: z_i \in \mathbb{Z}/p^i\mathbb{Z},\ \pi_i(z_i) = z_{i-1}\}$$

wobei $\longrightarrow \mathbb{Z}/p^3\mathbb{Z} \xrightarrow[\pi_3]{} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow[\pi_2]{} \mathbb{Z}/p^1\mathbb{Z} \xrightarrow[\pi_1]{} \mathbb{Z}/p^0\mathbb{Z}$

<u>Bsp:</u> $a = \sum_{i=0}^{\infty} r_i p^i$

$$z_j = \sum_{i=0}^{j-1} r_i p^i + p^j\mathbb{Z} \qquad \in \mathbb{Z}/p^j\mathbb{Z}$$

$$\pi_j(z_j) = z_{j-1} \quad \forall j$$

$\mathbb{Q}_p := \mathrm{Quot}\,\mathbb{Z}_p$

<u>Korollar 1.2.6:</u> Die Vervollst von $\mathbb{Q}$ bzgl. Beträgen sind $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}_p$ (p prim)

<u>Def 1.2.7:</u> Sei K ein Körper. Der Körper der <u>formalen Laurent-Reihen</u> ist

$$K((t)) := \{\sum_{i=N}^{\infty} r_i t^i \mid r_i \in K,\ N \in \mathbb{Z}\}$$

Die Addition und Mult ist wie für Reihen definiert.

$$\left(\sum_i r_i t^i\right)\cdot\left(\sum_j s_j t^j\right) = \sum_k \underbrace{\left(\sum_{i+j=k} r_i s_j\right)}_{\in K} t^k$$

Der t-adische Betrag von $a = \sum_{i=N}^{\infty} r_i t^i$ mit $r_N \neq 0$ ist $|a|_t = e^{-N}$

Die formalen <u>Potenzreihen</u> sind $K[[t]] := \{\sum_{i=0}^{\infty} r_i t^i \mid r_i \in K\}$

<u>Satz 1.2.8:</u> $(K((t)), |\cdot|_t)$ ist die Vervollst von $(K(t), |\cdot|_t)$. $K[[t]]$ ist der top. Abschluss von $K[t]$ in $K((t))$.

Bem: Beweis analog zu $\mathbb{Q}_p$.

$\mathbb{F}_p((t))$ und $\mathbb{Q}_p$ unterscheiden sich nur dadurch, ob es einen Übertrag (bei + und ·) gibt oder nicht. Bsp in $\mathbb{F}_5((t))$

$$\begin{array}{r} 4031 \\ +\ 2020{,}4 \\ \hline \dots 001001{,}4 \end{array}$$

„Für große p ist $\mathbb{F}_p((t)) \approx \mathbb{Q}_p$"

Ziel: Mache dies präzise.

Genauer: Wir werden zeigen:

Für jede $L_{Ring}\cup\{\dots\}$-Aussage ψ existiert ein $N_0 \in \mathbb{N}$ s.d.

$\forall p > N_0$: $\quad \mathbb{F}_p((t)) \models \psi \iff \mathbb{Q} \models \psi$

(„Transfer-Prinzip von Ax-Kochen/Ershov")

$\left(N_0 \approx \underbrace{2^{2^{2^{\# \text{Quantoren in } \psi}}}}\ \text{oder mehr} \right)$

1.3 Bewertete Körper

Def 1.3.1: Eine angeordnete abelsche Gruppe (aaG) ist eine abelsche Gruppe Γ mit einer Ordnungsrelation $<$, so dass für alle $a, a', b \in \Gamma$ gilt: $\quad a < a' \Rightarrow a + b < a' + b$.

Bsp 1.3.2:
- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{R}_{>0}, \cdot)$

(Nicht-Bsp: $(\mathbb{R}^\times, \cdot)$)

Bem: $a > 0 \iff -a < 0$, da: $a > 0 \iff a + (-a) > \underset{=0}{0} + \underset{=-a}{(-a)}$

Bsp. 1.3.3: Sind Γ, Γ' aaG, so ist auch $\Gamma \times \Gamma'$ eine aaG mit der Lexikographischen Ordnung („Lexikographisches Produkt")
(d.h. $(a, a') < (b, b') \iff a < b \vee (a = b \wedge a' < b')$)

Lemma 1.3.4: aaG sind torsionsfrei

Bew: Annahme nicht, also z.B. $a \in \Gamma \setminus \{0\}$ mit $\underbrace{a + \dots + a}_{n\text{ Mal}} = 0$
O.E. $a > 0$

$\Rightarrow a + a > a > 0$

$\Rightarrow \dots \underbrace{a + \dots + a}_{n\text{ Mal}} > \dots > a + a > a > 0$

$\underbrace{a + \dots + a}_{n\text{ Mal}} = 0$ ↯ $\square$

Def 1.3.5: Sei K ein Körper. Eine <u>Bewertung</u> auf K ist eine Abb. $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ für eine aaG Γ mit:

Motivation: „$x \mapsto e^{-v(x)}$ soll nicht-arch. Betrag sein"

(a) $v(x) = \infty \iff x = 0$

(b) $v(x \cdot y) = v(x) + v(y)$ ← d.h. $v : K^\times \to \Gamma$ ist Gruppenhomo

(c) $v(x + y) \geq \min\{v(x), v(y)\}$ (ultrametrische Dreiecksungleichung)

Ein Körper mit einer Bewertung heißt <u>bewerteter Körper</u>. Γ ist die <u>Wertegruppe</u>. Zwei Bewertungen $v : K \to \Gamma$, $v' : K \to \Gamma'$ heißen äquivalent, wenn ein Isomorphismus $\varphi : \Gamma \to \Gamma'$ existiert mit $v' = \varphi \circ v$.

von aaG, d.h. Gruppeniso, der die Ordnung respektiert.

Bsp: 1.3.6: R faktorieller Ring, $K := \mathrm{Quot}\, R$, $p \in R$ prim.

Für $a = p^r \cdot \frac{b}{c} \in K^\times$ mit $r \in \mathbb{Z}$, $b, c \in R \setminus (p)$

setze $v_p(a) := r$. $\quad v_p(0) := \infty$

Dies ist eine Bewertung (vgl. Bsp. 1.1.7)

<u>Bsp. von Bsp:</u>
- p-adische Bewertung auf $\mathbb{Q}$ (für p prim)
- p-adische Bewertung auf $K(X)$ (für p irred. Polynom)

Lemma 1.3.7: Ist (K, v) ein bew. Kp mit Wertegruppe $\Gamma \subset (\mathbb{R}, +)$, so wird durch $|x| := e^{-v(x)}$ ein Betrag auf K definiert.

Bew: Klar.

Lemma 1.3.8: Ist $(K, |\cdot|)$ ein Kp. mit nicht-archimed. Betrag, so wird durch $v(x) := -\log(|x|)$ eine Bewertung auf K definiert mit Wertegruppe $\Gamma \subset (\mathbb{R}, +)$

Bew: Klar.

Bsp: Jeder Körper hat eine triviale Bew. mit Wertegruppe $\Gamma = \{0\}$:

$$v(x) = \begin{cases} \infty & x = 0 \\ 0 & x \neq 0 \end{cases}$$

Bem 1.3.9: Ist (K,v) ein bew. Kp, so gilt für $x,y\in K$:

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

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

(c) Sind $x_1,\dots,x_n\in K$ so, dass nur ein j existiert mit $\min_i v(x_i)=v(x_j)$, so ist $v(x_1+\dots+x_n)=\min_i v(x_i)$

Bew: (a) Klar.

(b) Siehe Übung.

Def 1.3.10: Sei (K,v) ein bew. Kp. mit Wertegruppe Γ.

(a) Ein <u>offener Ball</u> in K ist eine Menge der Form
$$B_{>\gamma}(a):=\{x\in K \mid v(x-a)>\gamma\} \quad \text{für } a\in K,\ \gamma\in\Gamma$$

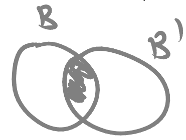
(b) Ein <u>abgeschlossener Ball</u> in K ist eine Menge der Form
$$B_{\geq\gamma}(a):=\{x\in K \mid v(x-a)\geq\gamma\} \quad \text{für } a\in K,\ \gamma\in\Gamma$$

(c) Die <u>Bewertungstopologie</u> auf K ist die Topologie mit den offenen Bällen als Basis.

($B_{\geq 0}(0)$ ist der „Einheitsball": $= \{x\in K \mid v(x)\geq 0\} = \{x\in K \mid |x|\leq 1\}$)

Bem 1.3.11: Sind $B,B'\subset K$ Bälle, so gilt entweder $B\subsetneq B'$ oder $B\supsetneq B'$ oder $B=B'$ oder $B\cap B'=\emptyset$

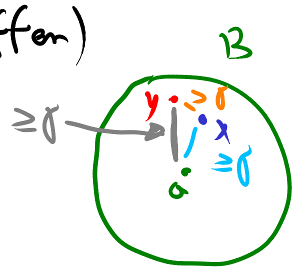
Nicht:



Bem 1.3.12: Abgeschlossene Bälle sind in der Bew-Topologie sowohl offen als auch abgeschlossen.

Bew: Sei $B=B_{\geq\gamma}(a)$

- **Beh:** $\forall\, x\in B:\ B_{>\gamma}(x)\subset B$ $\quad(\Rightarrow B$ offen$)$

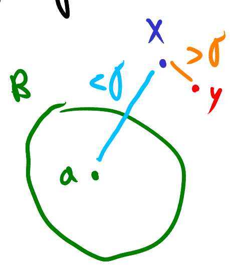


Bew: • Sei $y\in B_{>\gamma}(x)$, d.h. $v(y-x)>\gamma$.

- $x\in B \Rightarrow v(x-a)\geq\gamma$.
- $y \overset{?}{\in} B \Leftrightarrow v(y-a)\overset{?}{\geq}\gamma$

$$v(y-a) = v(y-x+x-a)\geq\min\{\underbrace{v(y-x)}_{>\gamma},\underbrace{v(x-a)}_{\geq\gamma}\}\geq\gamma$$

- **Beh:** $\forall\, x\in K\setminus B:\ B_{>\gamma}(x)\subset K\setminus B$ $\quad(\Rightarrow B$ abg.$)$



  - Sei $x\notin B \Rightarrow v(x-a)<\gamma$
  - Sei $y\in B_{>\gamma}(x)$, d.h. $v(y-x)>\gamma$.
  - Ann $y\in B$, d.h. $v(y-a)\geq\gamma$

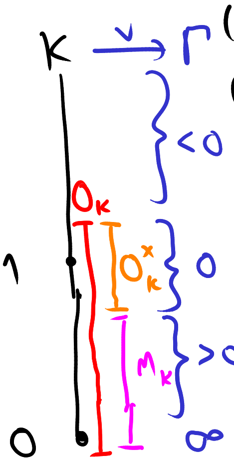
$$\Rightarrow v(x-a)=v(x-y+y-a)\geq\min\{\overbrace{v(x-y)}^{>\gamma},\overbrace{v(y-a)}^{\geq\gamma}\}\geq\gamma \ ↯$$

1.4 Bewertungsringe

Def 1.4.1: Sei K ein Körper. Ein Bewertungsring (von K) ist ein Unterring $\mathcal{O}_K \subset K$ so dass für alle $a \in K$ gilt: $a \in \mathcal{O}_K$ oder $\frac{1}{a} \in \mathcal{O}_K$.
(Allgemeiner: Ein kommutativer Integritätsbereich R heißt Bewertungsring, wenn er ein Bew.-Ring von $\operatorname{Quot} R$ ist.)

Bem: $\mathcal{O}_K$ ist Bew.-Ring von $K \Rightarrow K = \operatorname{Quot} \mathcal{O}_K$.

Lemma 1.4.2: Sei (K, v) ein bew. Kp.



(a) $\mathcal{O}_K := B_{\geq 0}(0) = \{x \in K \mid v(x) \geq 0\}$ ist ein bew. Ring.

(b) $\mathcal{O}_K^\times = \{x \in K \mid v(x) = 0\}$

(c) Das einzige max. Ideal von $\mathcal{O}_K$ ist $\mathcal{M}_K := \{x \in K \mid v(x) > 0\}$

Bem: $K \setminus \mathcal{O}_K = \{\frac{1}{a} \mid a \in \mathcal{M}_K \setminus \{0\}\}$

Def. 1.4.3: Den Bew.-Ring $\mathcal{O}_K$ aus L. 1.4.2 nennt man den Bew.-Ring von v.
Den Quotient $\bar{K} := \mathcal{O}_K / \mathcal{M}_K$ nennt man den Restklassenkörper (von $\mathcal{O}_K$ oder von v). Die natürliche Abb. $\mathcal{O}_K \to \bar{K}$ wird mit res bezeichnet (oder mit $a \mapsto \bar{a}$).

Bsp: $(\mathbb{Q}_p, v_p)$: $\mathcal{O}_{\mathbb{Q}_p} = \{a \mid v(a) \geq 0\} = \mathbb{Z}_p$

Max. Ideal: $\{\sum_{i \geq 1} r_i p^i \mid r_i \in \{0, \dots, p-1\}\} = p \cdot \mathbb{Z}_p$

Restkl.-Kp: $\mathbb{Z}_p / p\mathbb{Z}_p = \mathbb{F}_p$, res: $\sum_{i \geq 0} r_i p^i \mapsto r_0$

$(K((t)), v_t)$: $\mathcal{O}_{K((t))} = \{a \mid v(a) \geq 0\} = K[[t]]$ Max. Ideal: $t \cdot K[[t]]$
Restkl.-Kp: $K[[t]] / tK[[t]] = K$

Bew 1.4.2: (a) • $\mathcal{O}_K$ ist ein Ring:

$a, b \in \mathcal{O}_K$ (d.h. $v(a), v(b) \geq 0$)

• $\Rightarrow v(a+b) \geq \min\{v(a), v(b)\} \geq 0 \Rightarrow a+b \in \mathcal{O}_K$

• $\Rightarrow v(a \cdot b) = v(a) + v(b) \geq 0 \Rightarrow a \cdot b \in \mathcal{O}_K$

• $\Rightarrow v(-a) = v(a) \geq 0 \Rightarrow -a \in \mathcal{O}_K$

• $\mathcal{O}_K$ ist Bew.-Ring von K:

• Sei $a \in K$. Falls $v(a) \geq 0$: $a \in \mathcal{O}_K$

Falls $v(a) < 0$: $v(\frac{1}{a}) > 0 \Rightarrow \frac{1}{a} \in \mathcal{O}_K$

(b) $\underbrace{a \in \mathcal{O}_K}_{v(a)\geq 0}$ ist eine Einheit $\Leftrightarrow \underbrace{\frac{1}{a} \in \mathcal{O}_K}_{\Leftrightarrow v(\frac{1}{a})\geq 0 \Leftrightarrow v(a)\leq 0}$

$\Leftrightarrow v(a) = 0$

(c) Reicht z.z.: $M_K := \{a \in \mathcal{O}_K \mid v(a) > 0\}$ ist ein Ideal.

(Dann: automatisch einziges max. Ideal)

$a, b \in M_K$ (d.h. $v(a), v(b) > 0$), $c \in \mathcal{O}_K$ (d.h. $v(c) \geq 0$)

- $\Rightarrow v(a+b) \geq \min\{v(a), v(b)\} > 0 \Rightarrow a+b \in M_K$
- $\Rightarrow v(a\cdot c) = v(a) + v(c) > 0 \Rightarrow a\cdot c \in M_K$

$\square$

<u>Satz 1.4.4:</u> Sei K ein Kp. Lemma 1.4.2. induziert eine Bijektion

$$\{\text{Bewertungen auf } K\}/\text{Äquivalenz} \xrightarrow{1:1} \{\text{Bewertungsringe von } K\}$$

<u>Bem:</u> Es folgt: Bew-Ringe haben genau ein max. Ideal.

<u>Bew 1.4.4:</u> • Äquivalente Bewertungen haben den selben Bew-Ring: klar.

$$\begin{tikzcd} K \arrow[r, "v"] \arrow[dr, "v'"'] & \Gamma \arrow[d, phantom, "\cong" rotate=90] \\ & \Gamma' \end{tikzcd}$$

- Sei $\mathcal{O}_K$ ein Bew-Ring von K.

  Definiere $v' : K^\times \longrightarrow K^\times/\mathcal{O}_K^\times =: \Gamma'$ als die kanonische Abb.

  $v'(0) := \infty$

  (Schreibe Γ' additiv)

  Definiere Ordnung auf Γ' durch: $v'(a) \geq v'(b) :\Leftrightarrow \frac{a}{b} \in \mathcal{O}_K$

- „$\geq$" ist wohldef: Sei $v'(a_1) = v'(a_2) \Rightarrow a_2 = a_1 \cdot e, \ e \in \mathcal{O}_K^\times$

  Sei $v'(b_1) = v'(b_2) \Rightarrow b_2 = b_1 \cdot e', \ e' \in \mathcal{O}_K^\times$

  Ann: $\frac{a_1}{b_1} \in \mathcal{O}_K \Rightarrow \frac{a_2}{b_2} = \frac{a_1}{b_1} \cdot \frac{e}{e'} \in \mathcal{O}_K$

- „$\geq$" ist Ord-Rel:
  - $\frac{a}{a} \in \mathcal{O}_K \Rightarrow v'(a) \geq v'(a)$ ✓
  - Transitivität: $\frac{a}{b} \in \mathcal{O}_K$, $\frac{b}{c} \in \mathcal{O}_K \Rightarrow \frac{a}{b}\cdot\frac{b}{c} = \frac{a}{c} \in \mathcal{O}_K$
  - Antisymmetrie: z.z.: $v(a) \geq v(b) \wedge v(b) \geq v(a) \Rightarrow v(a) = v(b)$

    $\Downarrow \qquad \Downarrow$

    $\underbrace{\frac{a}{b} \in \mathcal{O}_K \qquad \frac{b}{a} \in \mathcal{O}_K}_{\frac{a}{b} \in \mathcal{O}_K^\times}$ $\Longrightarrow v(a) = v(b)$

• „≥" ist kompat mit Gruppen-Op:

$$v(a)\geq v(b) \Rightarrow \underbrace{v(a)+v(c)}_{\overset{\shortparallel}{v(a\cdot c)}} \geq \underbrace{v(b)+v(c)}_{v(b\cdot c)}$$

$$\Updownarrow \qquad\qquad\qquad\qquad \Updownarrow$$

$$\frac{a}{b}\in O_K \qquad\qquad\qquad \frac{a\cdot c}{b\cdot c}\in O_K$$

• <u>Bewertungsaxiome:</u>

  • $v(a)=\infty \iff a=0$: per Def.

  • $v(a)+v(b)=v(a\cdot b)$: ✓

  • Δ-UGL: $v(a+b)\overset{?}{\geq}\min\{v(a),v(b)\}$

    • O.E.: $v(a)\geq v(b)$, d.h. $\frac{a}{b}\in O_K$

    • <u>z.z.:</u> $v(a+b)\geq v(b)$, d.h. $\frac{a+b}{b}\in O_K$

$$\frac{a+b}{b} = \underset{\underset{O_K}{\cap}}{\frac{a}{b}} + \underset{\underset{\underset{v'(1)}{O_K}}{\cap}}{1} \qquad ✓$$

• Die Abb. $O_K \longmapsto v' \longmapsto \underbrace{\{x\in K \mid \underbrace{v'(x)\geq \overset{\shortparallel}{0}}_{\overset{\Updownarrow}{\frac{x}{1}\in O_K}}\}}_{=O_K}$ ist die Identität:

• Bei $v \longmapsto \underset{\overset{\shortparallel}{\{x\in K \mid v(x)\geq 0\}}}{O_K} \longmapsto v'$ sind v und v' äquivalent:

$$\ker v = \{x\in K \mid v(x)=0\} = O_K^\times = \ker v'$$

$$\begin{tikzcd} K^\times \arrow[r, two heads, "v"] \arrow[dr, two heads, "v'"'] & \Gamma \arrow[d, dashed, "\wr"] \\ & \Gamma' = K^\times/O_K^\times \end{tikzcd}$$

Habe also Iso $\Gamma \to \Gamma'$

Bleibt z.z.: Ordnungserhaltend, d.h. $\forall a\in K^\times$: $v(a)\geq 0 \overset{?}{\iff} v'(a)\geq 0$

$$\Updownarrow \qquad \Updownarrow$$

$$a\in O_K$$

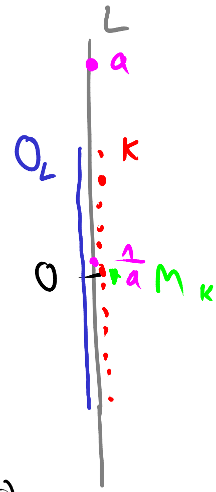
nach Def von O_K

nach Def von v'. □

Auf K:

	Bewertungen $\overset{1:1}{\longleftrightarrow}$ Bew.-Ringe	
Beträge	$\cup$	bis auf Äquiv.
$\cup$		
nicht-Arch. Beträge $\overset{1:1}{\longleftrightarrow}$	Bewertungen mit $\Gamma\subset\mathbb{R}$	

Bsp. 1.4.5: Seien $K \subset L$ angeordnete Körper. Dann ist
$$\mathcal{O}_L := \{ a \in L \mid \exists b, b' \in K : b < a < b' \}$$
ein Bew-Ring (und liefert also eine Bew. auf L)



Bew: • Prüfe: • $\mathcal{O}_L$ ist Ring.

• Sei $a \in L$. Ann $a \notin \mathcal{O}_L$. Beh: $\frac{1}{a} \in \mathcal{O}_L$

Bew: O.E. $a > 0$.

$a \notin \mathcal{O}_L \Rightarrow a > 1. \Rightarrow 0 < \frac{1}{a} < 1 \Rightarrow \frac{1}{a} \in \mathcal{O}_L$ $\square$

Bsp vom Bsp: $K = \mathbb{R} \precneqq L$ (oder $\mathbb{R} \subsetneq L$). Dann für $a, b \in L$:

$v(a) < 0 \iff a \notin \mathcal{O}_L \iff |a|$ ist „unendl groß" (d.h. $> r \ \forall r \in \mathbb{R}$)

$v(a) < v(b) \iff v\left(\frac{a}{b}\right) < 0 \iff \left|\frac{a}{b}\right|$ unendl. groß

$\iff a$ hat größere Größenordnung als b.

$v(a) > 0 \iff v\left(\frac{1}{a}\right) < 0 \iff |a|$ unendl. klein, d.h. $0 < |a| < r \ \forall r \in \mathbb{R}_{>0}$

$\Updownarrow$

$a \in M_K$

Anschauung: In $\mathbb{Q}$ mit der 5-ad. Bew.: $v(1) = v(2) = \ldots = v(4) = 0$

$v(5) = 1$ d.h. 5 hat kleinere Größenordnung. („5 ist fast gleich 0")

(„$\mathbb{Q}$ mit der 5-ad. Bew. hat fast Charakteristik 5")

Formal: Der Restklassenkp hat Char $= 5$.

Def. 1.4.6: Sei K ein bew. Kp mit Restkl-kp $\bar{K}$. Man sagt K hat <u>Charakteristik (p, q)</u>, für p, q prim oder 0, wenn $p = \operatorname{char} K$ und $q = \operatorname{char} \bar{K}$.

Falls $p = q$: K hat <u>Äqui-Charakteristik</u> p

Falls $p \neq q$: K hat <u>gemischte Charakteristik</u>.

Bsp: • $\mathbb{Q}_p$ hat Char. $(0, p)$

• $K((t))$ hat Char (p, p), für $p = \operatorname{char} K$. ($p$ prim oder 0)

($\operatorname{char} K((t)) = p$, da $K \subset K((t))$
$a \mapsto a \cdot t^0$)

Bem 1.4.7: Als Charakteristiken von bew. Körpern kommen vor:

$(0,0)$, $(0,p)$, (p,p), für p prim.

Bew: Wenn char $K = p$ ist (p prim), dann ist $p = 0$ in $\mathcal{O}_K$ und damit auch in $\bar{K} = \mathcal{O}_K / \mathcal{M}_K$ $\Rightarrow$ char $\bar{K} = p$.

1.5 Fortsetzungen von Bewertungen

($K \subset L$ Körpererw., v Bew. auf K. Wie lässt sich v auf L fortsetzen?)

- <u>Def 1.5.1:</u> Seien (K_1, v_1) und (K_2, v_2) bew. Kp. mit $K_1 \subset K_2$.
  Man nennt v_2 eine Fortsetzung von v_1, wenn v_1 äquivalent zu $v_2|_{K_1}$ ist.
  $\mathcal{O}_{K_i} :=$ Bew von v_i in K_i
- <u>Bem 1.5.2:</u> Dies ist äquivalent zu: $\mathcal{O}_{K_1} = \underbrace{\mathcal{O}_{K_2} \cap K_1}$

  Bew. Ring von $v_2|_{K_1}$ ist $\{x \in K_1 \mid v_2(x) \geq 0\}$

  Außerdem gilt dann: $\underset{\{0\} \cup \{\frac{1}{a} \mid a \in K_1 \setminus \mathcal{O}_{K_1}\}}{\mathcal{M}_{K_1}} = \underset{\{0\} \cup \{\frac{1}{a} \mid a \in K_2 \setminus \mathcal{O}_{K_2}\}}{\mathcal{M}_{K_2}} \cap K_1$

  Man erhält Einbettungen der Wertegruppen $\Gamma_1 \hookrightarrow \Gamma_2$ und der Restklassenkörper $\bar{K}_1 \hookrightarrow \bar{K}_2$

  $\mathcal{O}_{K_1}/\mathcal{M}_{K_1} \rightarrow \mathcal{O}_{K_2}/\mathcal{M}_{K_2}$

  da $\mathcal{O}_{K_1} \subset \mathcal{O}_{K_2}$, $\mathcal{M}_{K_1} \subset \mathcal{M}_{K_2}$

- <u>Satz 1.5.3:</u> Ist (K, v) ein bew. Kp. und $L \supset K$ eine Körpererw., so lässt sich v auf L fortsetzen.

  <u>Bew:</u> <u>Beh:</u> Es reicht, ein Bew-Ring $\mathcal{O}_L$ von L zu konstruieren mit $\mathcal{O}_L \supset \mathcal{O}_K$ und $\mathcal{M}_L \supset \mathcal{M}_K$

  Bew-Ring zu v

  <u>Dann:</u> • $\mathcal{O}_K \subset \mathcal{O}_L \cap K$

  • $\mathcal{O}_K \supset \mathcal{O}_L \cap K$: Sei $a \in \mathcal{O}_L \cap K \setminus \{0\}$

  $\Rightarrow \frac{1}{a} \notin \mathcal{M}_L \Rightarrow \frac{1}{a} \notin \mathcal{M}_K \Rightarrow a \in \mathcal{O}_K$

  • $\Rightarrow \mathcal{O}_K = \mathcal{O}_L \cap K$. Also fertig.

  Bleibt also, $\mathcal{O}_L$ wie oben zu konstruieren.

- Betrachte $\{ (R, I) \mid R \subset L$ Ring mit $O_K \subset R$
  $I \subsetneq R$ Ideal mit $M_K \subset I \}$
- Partiell geordnet durch $(R,I) \le (R', I') \Leftrightarrow R \subset R' \wedge I \subset I'$
- $\neq \emptyset$, da (O_K, M_K) drin.
- Jede Kette $(R_s, I_s)_{s \in S}$ hat Supremum $(\bigcup_s R_s, \bigcup_s I_s)$.
- Nach dem Zornschen Lemma ex. ein Maximum $=(O_L, M_L)$.
- Beh: O_L ist Bew-Ring von L mit max Ideal M_L.
  (Dann: Fertig)

  Bew: • M_L ist max. Ideal in O_L
  (Sonst, d.h. falls $I \underset{O_L}{\supsetneq} M_L$, dann ist $(O_L, I) > (O_L, M_L)$ ↯)

  • O_L ist ein Lokaler Ring ($:\Leftrightarrow O_L^\times = O_L \setminus M_L$):
  Sonst: $R := \{ \frac{a}{b} \in L \mid a \in O_L, b \in O_L \setminus M_L \}$
  (Lokalisierung an M_L)
  R ist ein Ring und M_L erzeugt ein echtes Ideal I in R
  $\Rightarrow (R, I) > (O_L, M_L)$
  (Elemente von $O_L \setminus M_L$ sind Einheiten in R.)

  • Bleibt z.z: Für $a \in L$ gilt: $a \in O_L$ oder $\frac{1}{a} \in O_L$.

  Ann: $a \notin O_L$, $\frac{1}{a} \notin O_L$
  - Betrachte in $O_L[a] = \{ \sum_{i \le m} b_i a^i \mid b_i \in O_L \}$
    das von M_L erzeugte Ideal:
    $I := \{ \sum_{i \le m} b_i a^i \mid b_i \in M_L \}$ $\quad \neq$, da $a \notin O_L$
    Falls $I \neq O_L[a]$, ist $(O_L[a], I) > (O_L, M_L)$,
    also Widerspruch zur Maximalität.
    Also $1 \in I$, d.h. $1 = \sum_{i \le m} b_i a^i$ für gewisse $b_i \in M_L$
  - Analog erhalte: $1 = \sum_{i \le m'} b_i' a^{-i}$ für gewisse $b_i' \in M_L$
  - Wir nehmen an, dass m, m' minimal gewählt sind.
  - Außerdem o.E. $m \ge m'$

• Beh: O.E. $b_0' = 0$

Sonst: $1 - b_0' = \sum_{1 \le i \le m'} b_i' a^{-i}$

Habe: $b_0' \in M_L \Rightarrow 1 - b_0' \notin M_L \Rightarrow 1 - b_0' \in O_L^\times$

$$\Rightarrow 1 = \sum_{1 \le i \le m'} \frac{b_i'}{1-b_0'} \cdot a^{-i}$$

$$\bullet \Rightarrow a^m = \sum_{1 \le i \le m'} \underbrace{b_i' \cdot a^{m-i}}$$

Da $m \ge m'$: Nicht-negative a-Potenz

$$\Rightarrow 1 = \underbrace{\sum_{i=0}^{m-1} b_i a^i + b_m \underbrace{a^m}_{b_m \cdot \sum_{1 \le i \le m'} b_i' \cdot a^{m-i}}}_{= \sum_{i=0}^{m-1} c_i a^i}$$

↯ zur Minimalität von m.

□

Bsp 1.5.4: Sei K ein bew. Kp. Dann erhalte auf $K(X)$ wie folgt eine Bewertungsfortsetzung durch:

Für $f = \sum_{i=0}^n a_i X^i \in K[X]$ setze $v(f) := \min_i v(a_i)$

(Für $\frac{f}{g} \in K(X)$, $f, g \in K[X]$, setze $v(\frac{f}{g}) = v(f) - v(g)$))

Diese Bewertung auf $K(X)$ nennt man die Gauß-Bewertung.

Bew: • $v(f) = \infty \Leftrightarrow f = 0$

• $v(f \cdot g) = v(f) + v(g)$ für $f, g \in K[X]$:

$f = \sum_{i=0}^n a_i X^i$, $g = \sum_{j=0}^m b_j X^j$

Sei i_0 minimal so, dass $v(f) = v(a_{i_0})$ $\qquad f \cdot g =: \sum_k c_k X^k$

Sei j_0 minimal so, dass $v(g) = v(b_{j_0})$

Betrachte den $X^{i_0+j_0}$-Koeff von $f \cdot g$: $\sum_{\substack{i,j \\ i+j = i_0+j_0}} a_i b_j =: c_{i_0+j_0}$

$$v(c_{i_0+j_0}) \overset{(*)}{\ge} \min_{\substack{i,j \\ i+j=i_0+j_0}} \underbrace{v(a_i b_j)}_{= v(a_i) + v(b_j)} = v(a_{i_0}) + v(b_{j_0})$$

- Unter den $a_i b_j$ aus der Summe ist $a_{i_0} b_{j_0}$ das einzige mit der minimalen Bewertung:

$$\left.\begin{array}{l}\text{Falls } i < i_0: \quad v(a_i) > v(a_{i_0}) \\ \qquad\qquad\qquad v(b_j) \geq v(b_{j_0})\end{array}\right\} v(a_i b_j) > v(a_{i_0} b_{j_0})$$

Falls $i > i_0$: $j < j_0$ ... analog.

- Nach Bem. 1.3.9 (iteriert) folgt „=" bei (*)
- $$\left.\begin{array}{l}\text{Also: } v(c_{i_0+j_0}) = v(f) + v(g) \\ \text{Außerdem: } v(c_k) \geq \min\limits_{i,j} v(a_i b_j) \geq v(f) + v(g)\end{array}\right\} v(f \cdot g) = v(f) + v(g)$$

- Δ-Ugl: $v\left(\frac{f_1}{g_1} + \frac{f_2}{g_2}\right) \overset{?}{\geq} \min\left\{v\left(\frac{f_1}{g_1}\right), v\left(\frac{f_2}{g_2}\right)\right\}$ $\qquad f_i, g_i \in K[X]$

Multiplizieren alles mit $g_1 \cdot g_2$, also reicht es zu prüfen:

$$v(f_1 + f_2) \geq \min\{v(f_1), v(f_2)\}$$

$$f_i = \sum_j a_{ij} X^j$$

$$v(f_1 + f_2) = \min_j \underbrace{v(a_{1j} + a_{2j})}_{\min\{\underbrace{v(a_{1j})}_{\geq v(f_1)}, \underbrace{v(a_{2j})}_{\geq v(f_2)}\}} \geq \min\{v(f_1), v(f_2)\}$$

$\square$

<u>Bem</u>: Dies wird verwendet um zu zeigen:

Sei R ein faktorieller Ring und $f \in R[X]$ irreduzibel als Element von $R[X]$ aber nicht konst.

Dann ist f auch als Element von $(\mathrm{Quot}\, R)[X]$ irreduzibel.

1.6 Newton-Polygone

Sei K ein bew. Kp. mit Wertegruppe Γ, und sei

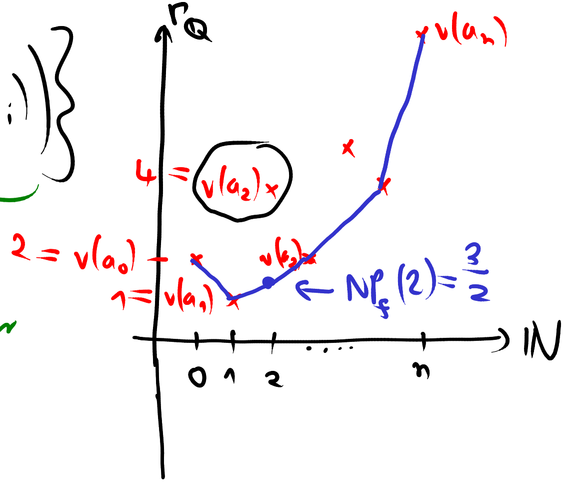
$$\Gamma_{\mathbb{Q}} = \left\{\frac{\gamma}{n} \;\middle|\; \gamma \in \Gamma,\ n \in \mathbb{N}\right\}$$

die divisible Hülle von Γ.

<u>Def 1.6.1</u>: Sei $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom vom Grad n. Das <u>Newton-Polygon</u> von f ist die Abb. $NP_f : \{0, \dots, n\} \to \Gamma_{\mathbb{Q}}$, die gegeben ist durch

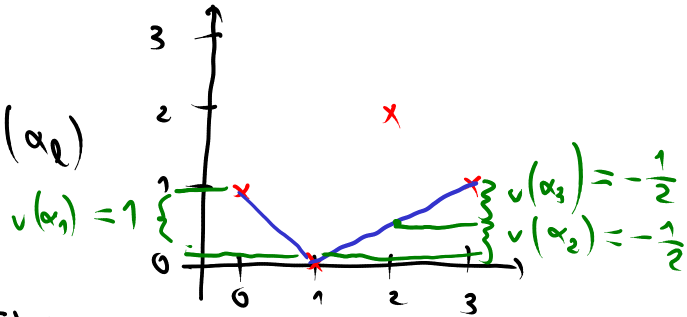
$$NP_f(l) = \min\left\{ v(a_l),\ \min_{\substack{i<l \\ j>l}} \underbrace{\left(\frac{l-i}{j-i}\cdot v(a_j) + \frac{j-l}{j-i}\cdot v(a_i) \right)} \right\}$$

y-Koord. des Schnittpunktes der Gerade durch $(i, v(a_i)), (j, v(a_j))$ mit der Gerade bei $x = l$



Satz 1.6.2: Sei $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom vom Grad n.
Wir setzen die Bewertung von K beliebig auf K^{alg} fort (geht nach 1.5.3).
und schreiben $f = a_n \cdot \prod_{i=1}^{n} (X - \alpha_i)$, für $\alpha_i \in K^{alg}$ mit
$v(\alpha_1) \geq v(\alpha_2) \geq \dots \geq v(\alpha_n)$.
Dann ist $NP_f(l) = v(a_n) + \sum_{i=l+1}^{n} v(\alpha_i)$ für $0 \leq l \leq n$

Anders ausgedrückt:
$$NP_f(l-1) - NP_f(l) = v(\alpha_l)$$



(Die Bew. der α_i sind die Steigungen der Segmente mit umgekehrtem Vorzeichen.)

Bew:
- OE $a_n = 1$. Sonst: Setze $g(X) := \frac{1}{a_n} \cdot f(X)$.
$$NP_g(l) = NP_f(l) - v(a_n)$$
- Betrachte $p(l) := \sum_{i=l+1}^{n} v(\alpha_i)$
- Es reicht zu zeigen: (1) $v(a_l) \geq p(l)$ $\quad \forall l$
(2) Falls $v(a_l) > p(l)$ gilt, ist $v(\alpha_l) = v(\alpha_{l+1})$ und $0 < l < n$
- $a_l = \sum_{\substack{I \subset \{1,\dots,n\} \\ |I| = n-l}} \prod_{i \in I} (-\alpha_i)$ $\qquad I = \{l+1, l+2, \dots, n\}$

$$v(a_l) \underset{(\square)}{\geq} \underbrace{\min_{I} \sum_{i \in I} v(\alpha_i)}_{(\Delta)} \underset{\text{da } v(\alpha_0) \geq \dots \geq v(\alpha_n)}{=} \sum_{i=l+1}^{n} v(\alpha_i) = p(l) \qquad \Rightarrow (1)$$

• (2) Ann: $v(\alpha_\ell) > v(\alpha_{\ell+1})$:

Dann ist für $I \neq \{\ell+1, \dots, n\}$: $\sum_{i\in I} v(\alpha_i) > \sum_{i=\ell+1}^{n} v(\alpha_i)$

D.h. in (Δ) taucht das Minimum genau einmal auf.

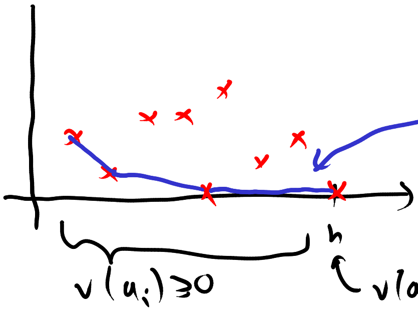
Durch iteriertes Anwenden von 1.3.9 erhalte „=" bei ($\Box$).

$\Box$

Korollar 1.6.3: Ist $f \in \mathcal{O}_K[X]$ normiert und $\alpha \in K$ eine NSt von f, so ist $\alpha \in \mathcal{O}_K$.

$$f = \sum_{i=0}^{n} a_i X^i, \quad a_n = 1$$

Bew:



Alle Steigungen ≤ 0, d.h. alle Bew. von NSt ≥ 0

$\Box$

Wertegruppe einer Fortsetzung von v auf K^{alg}

Korollar 1.6.4: Ist $f \in K[X]$, $\gamma \in \Gamma^{alg}$ und sind $\alpha_1, \dots, \alpha_k$ alle NSt von f in K^{alg} mit $v(\alpha_i) = \gamma$, so ist $k \cdot \gamma \in \Gamma$. (Insbes: $\alpha_i \in \Gamma_\mathbb{Q}$; also $\Gamma^{alg} \subset \Gamma_\mathbb{Q}$)

sogar = nach Übung

Satz 1.6.5 (Verallgemeinertes Eisensteinsches Irred-Krit): Sei L ein Körper und $f \in L[X]$ ein Polynom vom Grad n. Wenn eine Bewertung $v: L \to \Gamma \cup \{\infty\}$ existiert, so dass

$$NP_f(\ell) \notin \Gamma \quad \text{für } 1 \leq \ell \leq n-1$$

so ist f irreduzibel.

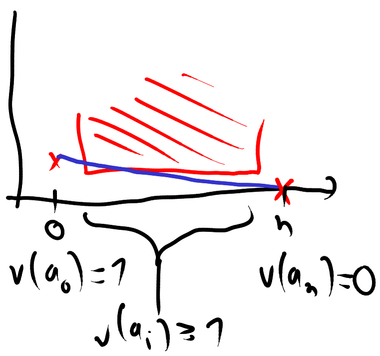
Bsp: Ist $f \in \mathbb{Z}[X]$ und p prim und

$p \nmid a_n$,

$p \mid a_i \quad \forall i < n$

$p^2 \nmid a_0$

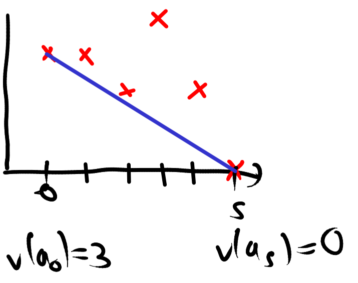
so ist $NP_f =$



$(0 < NP_f(\ell) < 1$ für $1 \leq \ell \leq n-1)$

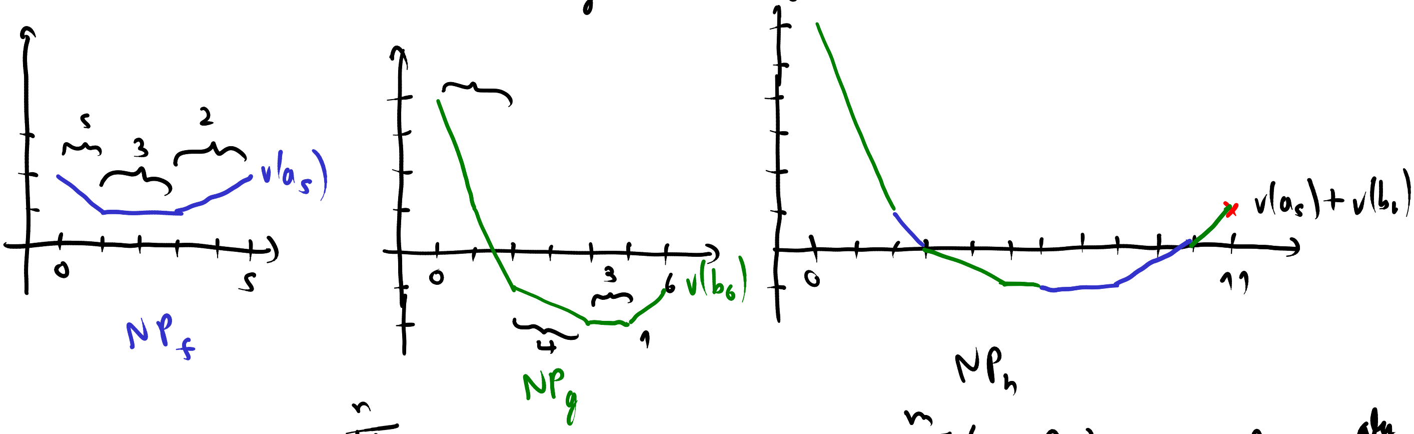
$\Rightarrow f$ irred.

Bsp:



$$\left.\begin{array}{l} v(a_1) \geq 3 \\ v(a_2) \geq 2 \\ v(a_3) \geq 2 \\ v(a_4) \geq 1 \end{array}\right\} \Rightarrow f \text{ irred.}$$

Satz 1.6.6: Sind $f, g \in K[X]$ und $h := f\cdot g$, so erhält man NP_h aus NP_f und NP_g wie folgt:



Bew: Sei $f = a_n \prod_{i=1}^{n} (x-\alpha_i)$ und $g = b_m \cdot \prod_{j=1}^{m} (x-\beta_j)$, $\alpha_i, \beta_j \in K^{alg}$

$v(\alpha_1) \geq \dots \geq v(\alpha_n)$

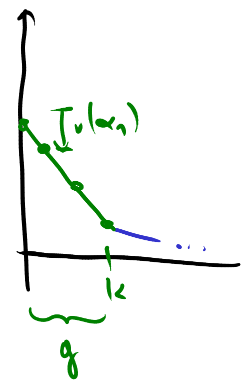
$v(\beta_1) \geq \dots \geq v(\beta_m)$

Sei $h = c_\ell \cdot \prod_{k=1}^{\ell} (x-\gamma_k)$ $\quad v(\gamma_1) \geq \dots \geq v(\gamma_\ell)$

Dann ist
- $\ell = n+m$
- $v(c_\ell) = v(a_n) + v(b_m)$
- Die γ_k sind genau die α_i und die β_j, nach Bewertung sortiert.

□

Bew 1.6.5: Wenn $f = g\cdot h$ wäre:



- Arbeite in K^{alg}
- O.E α NSt α_1 von g mit $v(\alpha_1) \geq v(\beta)$ $\forall \beta$ NSt von h
- Seien $\alpha_1, \dots, \alpha_k$ alle NSt von g mit $v(\alpha_i) = v(\alpha_1)$
- $\Rightarrow NP_f(0) - NP_f(k) = v(\alpha_1) + \dots + v(\alpha_k) \in \Gamma$ nach Kor. 1.6.4
- ↯ zu $NP_f(0) \in \Gamma$, $NP_f(k) \notin \Gamma$ nach Annahme.

□

1.7 Henselsche Körper

bezgl. der zugehörigen Metrik

Satz 1.7.1 (Hensels Lemma): Sei K ein vollst. bewerteter Körper mit $\Gamma = \mathbb{Z}$.

Sei $f \in O_K[X]$ und sei $a \in O_K$ so dass gilt:

(*) $$v(f(a)) > 0 \;\wedge\; v(f'(a)) = 0$$

Dann ex. genau ein $b \in O_K$ mit $f(b) = 0$ und $v(b-a) > 0$.

Bem 1.7.2: Sei $\bar f$ das Bild von $f \in K[X]$, d.h. für $f = \sum a_i X^i$ sei $\bar f := \sum \mathrm{res}(a_i) X^i$; sei $\bar a = \mathrm{res}(a)$

$$O_K \xrightarrow{\mathrm{res}} O_K/\mathfrak{m}_K = \bar K$$

$(*) \iff \bar f(\bar a) = 0 \ \wedge\ \bar f'(\bar a) \neq 0$

$v(f(a)) > 0 \iff \mathrm{res}(f(a)) = 0$, $\mathrm{res}(f(a)) = \bar f(\bar a)$

Also sagt 1.7.1: Hat $\bar f$ eine einfache NSt bei $\bar a \in \bar K$, so lässt sich $\bar a$ auf eindeutige Weise zu einer NSt b von f in O_K liften.
(„Lift" heißt: $\mathrm{res}(b) = \bar a$)

$v(b-a) > 0$ $\Downarrow$ $\mathrm{res}(b) = \mathrm{res}(a) = \bar a$

Satz 1.7.3 (starke Version von 1.7.1; Newtons Lemma):

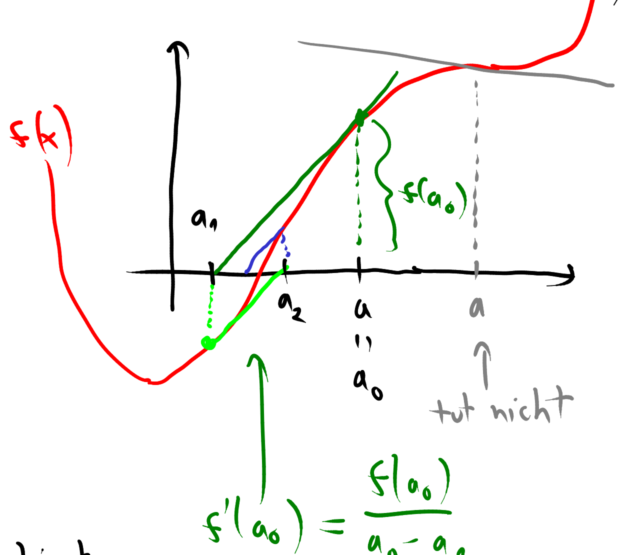
Sei K ein vollst. bewerteter Körper mit $\Gamma = \mathbb{Z}$.

Sei $f \in O_K[X]$ und sei $a \in O_K$ so dass gilt:

$(*)$ $$v(f(a)) > 2\, v(f'(a))$$

Dann ex. genau ein $b \in O_K$ mit $f(b) = 0$ und $v(b-a) \geq v(f(a)) - v(f'(a))$ $\big(> v(f'(a))\big)$

Bew: $\lambda := v(f'(a_0))$



Setze $a_0 := a$ und

$$a_{i+1} := a_i - \frac{f(a_i)}{f'(a_i)}$$

Beh: (1) $v(f'(a_{i+1})) = \lambda$

(2) $v(a_{i+1} - a_i) \geq v(f(a_i)) - \lambda$

(3) $v(f(a_{i+1})) > v(f(a_i))$

Danach: • (2) & (3) $\Rightarrow$ $\lim_i a_i =: b$ existiert

• (3) $\Rightarrow$ $\lim f(a_i) = f(b) = 0$

• (3) $\Rightarrow$ $v(f(a_i)) \geq v(f(a_0)) \overset{(2)}{\Rightarrow} v(a_{i+1} - a_i) \geq v(f(a_0)) - \lambda$

$$b - a = \sum_{i=0}^{\infty} \underbrace{(a_{i+1} - a_i)}_{v \,\geq\, v(f(a)) - \lambda} \quad \Rightarrow \quad v(b-a) \geq v(f(a)) - \lambda$$

Bew der Beh:

(2) $$v(a_{i+1} - a_i) = v\left(\frac{f(a_i)}{f'(a_i)}\right) = v(f(a_i)) - \underbrace{v(f'(a_i))}_{=\,\lambda}$$

• Sei $f(x) = \sum_{j=0}^{n} b_j (x - a_i)^j$

d.h. $g(x) := f(a_i + x) = \sum_j b_j x^j$

$b_j \in \mathcal{O}_K$, da $f \in \mathcal{O}_K[X]$ und $a_i \in \mathcal{O}_K$

da $v(a_i - a) \geq v(f(a)) - \lambda > \lambda \geq 0$

$b_0 = g(0) = f(a_i)$

$b_1 = g'(0) = f'(a_i)$. Nach Ind: $\underset{v(b_1)}{v(f'(a_i))} = \lambda$

(1) $v(f'(a_{i+1})) = v(g'(a_{i+1} - a_i))$

$$g'(a_{i+1} - a_i) = \underbrace{b_1}_{v = \lambda} \underbrace{+ 2 b_2 \cdot (a_{i+1} - a_i) + 3 \cdot b_2 (a_{i+1} - a_i)^2 + \ldots}_{(a_{i+1} - a_i) \cdot h(a_{i+1} - a_i)}$$

$\underbrace{(a_{i+1} - a_i)}_{v(\cdot) \geq v(f(a_i)) - \lambda} \cdot h(a_{i+1} - a_i)$, Koeff in $\underbrace{\mathcal{O}_K}_{v(\ ) \geq 0}$

$v(\cdot) \geq v(f(a_i)) - \lambda \overset{(3)}{\geq} v(f(a)) - \lambda$

$\overset{(*)}{>} 2 \cdot \lambda - \lambda = \lambda$

$\Rightarrow v(g'(a_{i+1} - a_i)) = \lambda$

(3) $f(a_{i+1}) = g(a_{i+1} - a_i) = g\left(-\frac{g(0)}{g'(0)}\right) = g\left(-\frac{b_0}{b_1}\right)$

nach Def von a_{i+1}

$$= \underbrace{b_0 + \underbrace{b_1 \left(-\frac{b_0}{b_1}\right)}_{= -b_0}}_{= 0} + \underbrace{b_2 \cdot \left(-\frac{b_0}{b_1}\right)^2 + \ldots}_{= \underbrace{(a_{i+1} - a_i)^2}_{v \geq 2(v(f(a_i)) - \lambda)} \cdot \underbrace{\tilde{h}(a_{i+1} - a_i)}_{v \geq 0}}$$

Also: $v(f(a_{i+1})) \geq v(f(a_i)) + \underbrace{v(f(a_i))}_{\overset{(3)}{\geq} v(f(a)) \overset{(*)}{>} 2 \cdot \lambda} - 2\lambda > v(f(a_i))$

Also: Existenz von b gezeigt.

Eindeutigkeit:

- Sei b NSt. von f, O.E $b=0$
- z.z.: Für $b' \neq b$ mit $v(b'-b) \geq v(f(a)) - \lambda$ gilt $f(b') \neq 0$

Schreibe $f(x) = \sum_{i=1}^{n} b_i x^i$

$v(b_1) = v(f'(0)) = \lambda$

$$f(b') = b' \cdot \underbrace{(\underbrace{b_1}_{v=\lambda} + \underbrace{\underbrace{b'}_{v \geq v(f(a)) - \lambda \overset{(*)}{>} \lambda} \cdot \underbrace{\ldots\ldots}_{v \geq 0}}_{v > \lambda})}_{v=\lambda}$$

$\Rightarrow f(b') \neq 0$ $\square$

<u>Bsp</u>: Bestimme alle Quadrate in $\mathbb{Q}_p$ für $p \neq 2$

<u>Beh</u>: Für $a \in \mathbb{Q}_p^\times$: a ist Quadrat $\Leftrightarrow$ $2 \mid v(a)$ und r_N ist ein Quadrat in $\mathbb{F}_p$.

$a = \sum_{i=N}^{\infty} r_i p^i$, $r_N \neq 0$

„$\Rightarrow$":

$a = b^2 \Rightarrow v(a) = 2 \cdot v(b) \Rightarrow 2 \mid v(a)$

$$a = \left(\sum_{i=M}^{\infty} s_i p^i\right)^2 = \sum_{i=N}^{\infty} r_i p^i$$

$s_M \neq 0$

Erhalte $N = 2M$ und $r_N \equiv s_M^2 \mod p$

d.h. r_N ist Quadrat in $\mathbb{F}_p$

„$\Leftarrow$": • $2 \mid v(a)$. Wähle $c \in K$ mit $2v(c) = v(a)$

$a' := \frac{a}{c^2}$ $\Rightarrow v(a') = v(a) - 2 \cdot v(c) = 0$

a ist Quadrat $\Leftrightarrow$ a' ist Quadrat

Also: O.E $v(a) = 0$

wohldef, da $v(a)=0$

- a ist Quadrat $\Leftrightarrow$ $\overbrace{X^2 - a}^{f}$ hat NSt
- Nach Bem 1.7.2, zu prüfen, für $\bar{f} := \mathrm{res}(f) = X^2 - \mathrm{res}(a)$:
  - Suche $\bar{b} \in \mathbb{F}_q$ mit $\bar{f}(\bar{b}) = 0$, $\bar{f}'(\bar{b}) \neq 0$.

• Dann ex. ein Lift b von $\bar{b}$ mit $f(b)=0$, d.h. $a=b^2$.

• $\mathrm{res}(a) = r_0$ (als Element von $\mathbb{F}_p$)

Nach Ann. ex. $\bar{b} \in \mathbb{F}_p^\times$ mit $\bar{b}^2 = \mathrm{res}(a)$ in $\mathbb{F}_p$

Also $\bar{f}(\bar{b}) = 0$

$\bar{f}'(x) = 2\cdot x$

$\bar{f}'(\bar{b}) = 2\cdot \bar{b} \neq 0$ □

Def 1.7.4: Ein bew. Kp K heißt henselsch, wenn gilt:
Sind $f \in \mathcal{O}_K[X]$ und $a \in \mathcal{O}_K$ mit $v(f(a)) > 0$ und $v(f'(a)) = 0$, so existiert (mindestens) ein $b \in \mathcal{O}_K$ mit $f(b) = 0$ und $v(b-a) > 0$.

Bsp 1.7.5: Nach 1.7.1 ist jeder vollst. bew. Kp mit Wertegruppe $\mathbb{Z}$ henselsch; insbes. $\mathbb{Q}_p$, $k((t))$ (k beliebiger Körper)

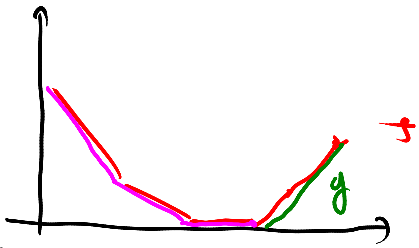
Bsp 1.7.6: Jeder alg. abg. bew. Kp ist henselsch.

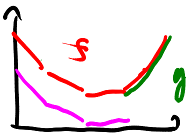
Bew: Sei $K = K^{alg}$, $f \in \mathcal{O}_K[X]$

• $\Rightarrow$ $f = \prod_i (x - \alpha_i) \cdot g(x)$ $\alpha_i \in \mathcal{O}_K$, g hat keine NSt in $\mathcal{O}_K$.

• Beh: $g \in \mathcal{O}_K[X]$

Bew mit Newton-Polygonen:





• Außerdem: $NP_g(\ell) > 0 \ \forall \ell > 0$;
d.h. $\mathrm{res}(g)$ ist konstantes Polynom.

• $\mathrm{res}(f) = \prod (x - \mathrm{res}(\alpha_i)) \cdot \mathrm{res}(g(x))$

Sei $\bar{a}$ NSt von $\mathrm{res}(f)$. Da $\mathrm{res}(g(x))$ konst., ist $\bar{a}$ NSt von $\prod(x - \mathrm{res}(\alpha_i))$, also $\bar{a} = \mathrm{res}(\alpha_i)$ für ein i. α_i ist der gesuchte Lift.

• (Wenn $\mathrm{res}(g)$ das Nullpolynom wäre, wäre $(\mathrm{res}(f))'(\bar{a}) = 0$ ↯) □

Bem 1.7.7: Ein Körper K ist henselsch, wenn die Fortsetzung seiner Bewertung auf K^{alg} eindeutig ist.

Bew von „⇐": • Sei $f \in \mathcal{O}_K[X]$ und sei $a \in \mathcal{O}_K$ mit $v(f(a)) > 0$, $v(f'(a)) = 0$

• O.E. $a = 0$

• $f = \prod_i (x - \alpha_i) \cdot g$, für $\alpha_i \in K^{alg}$, $g \in \mathcal{O}_{K^{alg}}[X]$
g hat keine NSt in $\mathcal{O}_{K^{alg}}$

• $\mathrm{res}(f)$ hat eine einfache NSt bei 0

- Die NSt von $res(f)$ sind genau die $res(\alpha_i)$
- D.h. ex genau ein i s.d. $res(\alpha_i)=0$,
  d.h. f hat genau eine NSt α_{i_0} mit $v(\alpha_{i_0})>0$
- Sei $\sigma \in Aut(K^{alg}/K)$ beliebig.
- Da $v\circ\sigma$ eine Bew. auf K^{alg} ist, die die Bewertung auf K fortsetzt, und da die Fortsetzung der Bew. von K eindeutig ist, ist $v\circ\sigma = v$.
- $\Rightarrow v(\sigma(\alpha_{i_0}))>0$
  Da α_{i_0} die einzige NSt von f ist mit $v>0$: $\sigma(\alpha_{i_0})=\alpha_{i_0}$
- $\alpha_{i_0}\in K$. Da $v(\alpha_{i_0})>0$: $res(\alpha_{i_0})=0=res(a)$
  $(v(\alpha_{i_0}-a)>0)$ $\square$

ohne Beweis

Bem 1.7.8: Zu jedem bew. Kp K existiert ein (bis auf Isomorphie über K eindeutiger) kleinster henselscher Körper K^h, der K enthält. K^h nennt man die henselsche Hülle von K.

Bem 1.7.9: Ist $\Gamma=\mathbb{Z}$, so ist $K^h = \underset{\substack{\uparrow\\ \text{Vervollst von } K}}{\hat{K}} \cap K^{alg}$

1.8 Anwendung auf diophantische Gleichungen

Konvention: Alle Ringe sind kommutativ und mit 1.

Notation 1.8.1: Sei $\underline{f}=(f_1,\dots,f_\ell)\in(\mathbb{Z}[X_1,\dots,X_n])^\ell$ und sei R ein Ring. Dann schreibe

Im Folgenden $\underline{X}=(X_1,\dots,X_n)$

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

„Diophantisches Gleichungssystem" = Sei $\underline{f}$ wie oben. Ziel: Bestimme $V_{\underline{f}}(\mathbb{Z})$.

Bem 1.8.2: Es gibt keinen Algorithmus, der als Eingabe ein Tupel $\underline{f}\in\mathbb{Z}[\underline{X}]^\ell$ nimmt und ausgibt, ob $V_{\underline{f}}(\mathbb{Z})$ leer ist oder nicht.

Bsp: $X_1^k+X_2^k-X_3^k=0$ hat Lösung in $\mathbb{Z}$ g.d.w. $k=2$.

Bem 1.8.3: Ist $V_{\underline{f}}(\mathbb{Z})$ nicht-leer, so ist auch $V_{\underline{f}}(\mathbb{Z}/m\mathbb{Z})$ nicht-leer.
($\varphi: R\to S$ Ring-Homo induziert $V_{\underline{f}}(R)\to V_{\underline{f}}(S)$)

Deshalb erstes Ziel: Verstehe $V_{\underline{f}}(\mathbb{Z}/m\mathbb{Z})$ für alle m.

Lemma 1.8.4: Sei $\underline{f} \in \mathbb{Z}[\underline{X}]^l$ und $m \geq 1$. Ist $m = \prod p_i^{r_i}$ die Primfaktorzerlegung, so induzieren die natürlichen Abb. $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/p_i^{r_i}\mathbb{Z}$ eine Bijektion

$$V_{\underline{f}}(\mathbb{Z}/m\mathbb{Z}) \xrightarrow{1:1} \prod_i V_{\underline{f}}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$$

Bew: Chinesischer Restsatz $\left(\mathbb{Z}/m\mathbb{Z} \cong \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}\right)$

Also neues Ziel: Verstehe $V_{\underline{f}}(\mathbb{Z}/p^r\mathbb{Z})$ für alle p prim und $r \geq 1$.

Bem 1.8.5: Für p prim und $r \geq 0$ gilt: $\mathbb{Z}/p^r\mathbb{Z} \cong \mathbb{Z}_p/p^r\mathbb{Z}_p$ (als Ringe)

Bew:
$$\left.\begin{aligned} \mathbb{Z}_p &= \left\{ \sum_{i\geq 0} a_i p^i \;\middle|\; \dots \right\} \\ p^r\mathbb{Z}_p &= \left\{ \sum_{i\geq r} a_i p^i \;\middle|\; \dots \right\} \end{aligned}\right\} \Rightarrow \mathbb{Z}_p/p^r\mathbb{Z}_p \xrightarrow{1:1} \left\{ \sum_{i=0}^{r-1} a_i p^i \;\middle|\; \dots \right\} \xrightarrow{1:1} \mathbb{Z}/p^r\mathbb{Z}$$

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook] \arrow[rr, bend right] & \mathbb{Z}_p \arrow[r, two heads] & \mathbb{Z}_p/p^r\mathbb{Z}_p \end{tikzcd}$$

Kern davon ist $\mathbb{Z} \cap p^r\mathbb{Z}_p = p^r\mathbb{Z}$

Def 1.8.6: Sei $\underline{f} \in \mathbb{Z}[\underline{X}]^l$ und p prim. Die <u>Poincaré-Reihe</u> von $\underline{f}$ ist

$$P_{\underline{f},p}(Z) := \sum_{r\geq 0} N_r \cdot Z^r \qquad \in \mathbb{Q}[[Z]]$$

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

Satz 1.8.7: $P_{\underline{f},p}(Z) \in \mathbb{Q}(Z)$

(d.h.: ex $g, h \in \mathbb{Q}[Z]$ s.d. $P_{\underline{f},p} = \frac{g}{h}$ in $\mathbb{Q}((Z))$)

Bsp 1.8.8: Sei $\underline{f}$ das 0-Polynom in n Variablen.

- Dann ist $V_{\underline{f}}(\mathbb{Z}/p^r\mathbb{Z}) = (\mathbb{Z}/p^r\mathbb{Z})^n \Rightarrow N_r = p^{r \cdot n}$
- $P_{\underline{f},p} = \sum_{r\geq 0} p^{r\cdot n} \cdot Z^r = \sum_{r\geq 0} (p^n \cdot Z)^r = \frac{1}{1-p^n Z}$

$$(1-p^nZ)\cdot \sum_{r\geq 0}(p^nZ)^r = \sum_{r\geq 0}(p^nZ)^r - \sum_{r\geq 1}(p^nZ)^r = 1$$

Satz 1.8.9: Sei $\underline{f} \in (\mathbb{Z}[\underline{X}])^n$. Dann existieren $g_p \in \mathbb{Z}[Z]$ für jede Primzahl p und $h \in \mathbb{Z}[Z, P]$ s.d.:

$$P_{\underline{f},p}(Z) = \frac{g_p(Z)}{h(Z,p)}$$

Außerdem existieren L_{ring}-Formeln $\varphi_0, \dots, \varphi_m, \varphi_0', \dots, \varphi_m'$ s.d. gilt:

$$g_p(Z) = \sum_{i=0}^{m} \left(\#\varphi_i(\mathbb{F}_p) - \#\varphi_i'(\mathbb{F}_p)\right) \cdot Z^i \quad \forall p$$