Proposition 3.3.6.5. *Sei R ein kommutativer Ring mit 1, außerdem $p, q \in R[[x]]$ mit $p(x) = \sum_{n=0}^{\infty} a_n x^n$ und $q(x) = \sum_{n=0}^{\infty} b_n x^n$. Mit R^*, $R[[x]]^*$ und $R[x]^*$ seien die Einheitengruppen der Ringe R, $R[[x]]$ bzw. $R[x]$ bezeichnet. Dann gilt:*

1. $\mathrm{ord}(p+q) \geq \min\{\mathrm{ord}(p), \mathrm{ord}(q)\}$
2. $\mathrm{grad}(p+q) \leq \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$
3. $\mathrm{ord}(pq) \geq \mathrm{ord}(p) + \mathrm{ord}(q)$. *Ist R ein Integritätsbereich, so gilt sogar Gleichheit.*
4. $\mathrm{grad}(pq) \leq \mathrm{grad}(p) + \mathrm{grad}(q)$. *Ist R ein Integritätsbereich, so gilt sogar Gleichheit.*
5. *Ist R ein Integritätsbereich, so auch $R[[x]]$ und $R[x]$.*
6. *Genau dann ist $p \in R[[x]]^*$, wenn $a_0 \in R^*$. Ist $q = p^{-1}$ das multiplikative Inverse von p, dann erfüllen die Koeffizienten $b_0 = a_0^{-1}$ und für alle $n = 1, 2, \ldots$ die Rekursion $b_n = -b_0(a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_n b_0)$. Ist speziell R ein Körper, so ist $p \in R[[x]]^*$ genau dann, wenn $\mathrm{ord}(p) = 0$.*
7. *Wenn R Integritätsbereich ist, dann gilt für alle $p \in R[x]$: Genau dann ist $p \in R[x]^*$, wenn $\mathrm{grad}(p) = 0$ und $p = a_0$ mit $a_0 \in R^*$.*

UE 187 ▶ Übungsaufgabe 3.3.6.6. (F) Beweisen Sie Proposition 3.3.6.5, und zeigen Sie durch (möglichst einfache) Beispiele, dass man „$\leq$" bzw. „$\geq$" im Allgemeinen nicht durch „$=$" ersetzen kann. **◀ UE 187**

1) •) $l := \min\{\mathrm{ord}(p), \mathrm{ord}(q)\}$, also $\forall k \in \mathbb{N}: k < l \Rightarrow a_k = 0 \wedge b_k = 0 \Rightarrow \forall k \in \mathbb{N}: k < l \Rightarrow a_k + b_k = 0$

$\Rightarrow \mathrm{ord}(p+q) \geq l$

•) $p = 1 \wedge q = -1$, dann ist $\mathrm{ord}(p) = \mathrm{ord}(q) = \min\{\mathrm{ord}(p), \mathrm{ord}(q)\} = 0 < \infty = \mathrm{ord}(0) = \mathrm{ord}(p+q)$

2) •) $l := \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$, also $\forall k \in \mathbb{N}: k > l \Rightarrow a_k = b_k = 0 \Rightarrow \forall k \in \mathbb{N}: k > l \Rightarrow a_k + b_k = 0$

$\Rightarrow \mathrm{grad}(p+q) \leq l = \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$

•) $p = 1 \wedge q = -1$, dann ist $\mathrm{grad}(p+q) = \mathrm{grad}(0) = -\infty < 0 = \max\{\mathrm{grad}(p), \mathrm{grad}(q)\}$

3) •) $l := \mathrm{ord}(p)$ und $k := \mathrm{ord}(q)$ sowie $pq = \sum_{n=0}^{\infty} c_n x^n$ mit $c_n = \sum_{i=0}^{n} a_i b_{n-i}$

Sei $j \in \mathbb{N}$ mit $j < l+k$ bel. $c_j = \sum_{i=0}^{j} a_i b_{j-i}$, $\forall i < l: a_i = 0$, also $c_j = \sum_{i=l}^{j} a_i b_{j-i}$

$\forall i \in \{l, \ldots, k+l\}: j - i < k + l - i \leq k$ also $b_{j-i} = 0$ und damit $c_j = 0$, daraus folgt

$\mathrm{ord}(pq) \geq k + l = \mathrm{ord}(p) + \mathrm{ord}(q)$

•) Sei R nun Integritätsbereich, dann ist $c_{l+k} = \sum_{i=0}^{l+k} a_i b_{l+k-i} = a_l b_k \neq 0$ wegen $a_l \neq 0 \wedge b_k \neq 0 \wedge$ Nullteilerfreiheit

also $\mathrm{ord}(pq) = l + k = \mathrm{ord}(p) + \mathrm{ord}(q)$

•) Betrachte $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$, nach Satz 3.3.3.3. ein endlicher Ring

$1 + 4\mathbb{Z}$ ist außerdem Einselement und der Ring ist kommutativ

$p = 2 + 4\mathbb{Z}$ und $q = 2 + 4\mathbb{Z}$, dann ist $\mathrm{ord}(p) + \mathrm{ord}(q) = 0 < \infty = \mathrm{ord}(0) = \mathrm{ord}(pq)$

4) •) $\forall j > l + k$: $c_j = \sum_{i=0}^{j} a_i b_{j-i}$ wegen $b_{j-i} = 0$ für $j - i > k \Leftrightarrow j - k > i$ ist $c_j = \sum_{i=j-k}^{j} a_i b_{j-i}$ und wegen

$j - k > l$ ist $\forall i \in \{j-k, \ldots, j\}: a_i = 0$ also $c_j = 0$ und damit $\mathrm{grad}(pq) \leq l + k = \mathrm{grad}(p) + \mathrm{grad}(q)$

•) R Integritätsbereich: $c_{l+k} = \sum_{i=0}^{l+k} a_i b_{l+k-i} = a_l b_k \neq 0$, wegen $a_l \neq 0 \wedge b_k \neq 0$, also $\mathrm{grad}(pq) = \mathrm{grad}(p) + \mathrm{grad}(q)$

•) $\mathbb{Z}_4$: $p = 2+4\mathbb{Z} \wedge q = 2+4\mathbb{Z}$, $\operatorname{grad}(p) + \operatorname{grad}(q) = 0 > -\infty = \operatorname{grad}(0) = \operatorname{grad}(pq)$

5) Als Integritätsbereich ist R insbesondere ein kommutativer Ring mit 1, nach Prop. 3.3.6.3 sind also $R[[x]]$ und $R[x]$ kommutative Ringe mit 1.

wegen $1 \neq 0$ in R ist auch $(0)_{n\in\mathbb{N}} \neq (1,0,\dots)$ in $R[[x]]$ bzw. $R[x]$ und wenn $\operatorname{ord}(q) = l \in \mathbb{N}$ und $pq = 0$, dann

ist nach (3): $\infty = \operatorname{ord}(0) = \operatorname{ord}(pq) = \operatorname{ord}(p) + \operatorname{ord}(q) = \operatorname{ord}(p) + l \Rightarrow \operatorname{ord}(p) = \infty \Rightarrow p = (0)_{n\in\mathbb{N}}$

Also sind $R[[x]]$ und $R[x]$ nullteilerfrei und damit Integritätsbereiche.

6) „$\Rightarrow$" $p \in R[[x]]^*$ mit $q = p^{-1}$, also $pq = 1 = c_0 = \sum_{i=0}^{0} a_i b_{0-i} = a_0 b_0 \Rightarrow b_0 = a_0^{-1} \Rightarrow a_0 \in R^*$

„$\Leftarrow$" $a_0 \in R^*$ mit $b_0 = a_0^{-1}$; $b_n = -b_0(a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_n b_0)$; $pq = \sum_{n=0}^{\infty} c_n x^n$ mit $c_n = \sum_{i=0}^{n} a_i b_{n-i}$

$c_0 = a_0 b_0 = 1$; $c_1 = \sum_{i=0}^{1} a_i b_{1-i} = a_0(-b_0(a_1 b_0)) + a_1 b_0 = -a_1 b_0 + a_1 b_0 = 0$

Sei nun $\forall\, 0 < k < n+1: c_k = 0$

$$c_{n+1} = \sum_{i=0}^{n+1} a_i b_{n+1-i} = a_{n+1} b_0 - \sum_{i=0}^{n} a_i b_0 \sum_{j=0}^{n-i} a_{j+1} b_{n-i-j} = a_{n+1} b_0 - a_0 b_0 \sum_{j=0}^{n} a_{j+1} b_{n-j} - \sum_{i=1}^{n} a_i b_0 \sum_{j=0}^{n-i} a_{j+1} b_{n-i-j}$$

$$= -a_0 b_0 \sum_{j=0}^{n-1} a_{j+1} b_{n-j} - \sum_{i=1}^{n} a_i b_{n-i} b_0 a_1 - \sum_{i=1}^{n-1} a_i b_0 a_2 b_{n-1-i} - \dots - \sum_{i=1}^{1} a_i b_0 a_n b_{1-i}$$

$$= -\sum_{i=0}^{n-1} b_0 a_{i+1} \sum_{j=0}^{n-i} a_j b_{n-i-j} = -\sum_{i=0}^{n} b_0 a_{i+1} c_{n-i} = 0$$

•) R Körper: $p \in R[[x]]^* \Leftrightarrow a_0 \in R^* \Leftrightarrow a_0 \neq 0 \Leftrightarrow \operatorname{ord}(p) = 0$

7) $p \in R[x]$, R Integritätsbereich

„$\Rightarrow$" sei $p \in R[x]^*$ mit $pq = (1,0,\dots)$

$\operatorname{grad}(pq) = 0 = \operatorname{grad}(p) + \operatorname{grad}(q) \Rightarrow \operatorname{grad}(p) = \operatorname{grad}(q) = 0$, also $p = a_0 \wedge q = b_0 \wedge$

$a_0 b_0 = 1 \Rightarrow a_0 \in R^*$

„$\Leftarrow$" $p = a_0$ mit $a_0 \in R^*$ mit $a_0 b_0 = 1$

$q := b_0 \Rightarrow pq = (1,0,\dots) \Rightarrow p \in R[x]^*$

Satz 3.3.6.10. *Ist R ein Körper, so bilden die formalen Laurentreihen (zusammen mit der Inklusionsabbildung $\iota\colon R[[x]] \to R[[[x]]]$, $(a_n)_{n\in\mathbb{N}} \mapsto (a_n)_{n\in\mathbb{Z}}$ mit $a_n = 0$ für alle $n < 0$, als isomorpher Einbettung) einen Quotientenkörper von $R[[x]]$.*

UE 189 ▶ Übungsaufgabe 3.3.6.11. (W) Beweisen Sie Satz 3.3.6.10, indem Sie jene Beweisschritte, die oben nur skizzenhaft angedeutet worden sind, ausführlich durchführen. Genauer sind folgende Schritte zu tun: ◀ **UE 189**

1. Definieren Sie sorgfältig die fundamentalen Operationen von $R[[[x]]]$ (Addition, Nullelement, additive Inverse, Multiplikation, Einselement).
2. Zeigen Sie, dass es sich dabei um einen kommutativen Ring mit 1 handelt.
3. Zeigen Sie, dass sich jedes $q \in R[[[x]]] \setminus \{0\}$ *eindeutig* in der Form $x^n\bar{q}(x)$ schreiben lässt, mit $n \in \mathbb{Z}$, und $\bar{q}(x) \in R[[x]]^*$. (Mit $R[[x]]^*$ bezeichnen wir die Einheiten von $R[[x]]$, siehe 3.3.6.5.)
4. Zeigen Sie, dass jedes $q \in R[[[x]]] \setminus \{0\}$ ein multiplikatives Inverses in $R[[[x]]]$ hat. (Somit ist $R[[[x]]]$ ein Körper.)
5. Zeigen Sie, dass $R[[[x]]]$ mit ι tatsächlich ein Quotientenkörper von $R[[x]]$ ist.

1) „+" $(a_n)_{n\in\mathbb{Z}} + (b_n)_{n\in\mathbb{Z}} := (a_n + b_n)_{n\in\mathbb{Z}}$

„0" $(0)_{n\in\mathbb{Z}}$

„−" $(-a_n)_{n\in\mathbb{Z}} = -(a_n)_{n\in\mathbb{Z}}$

„·" $(a_n)_{n\in\mathbb{Z}} \cdot (b_n)_{n\in\mathbb{Z}} := (c_n)_{n\in\mathbb{Z}}$ mit $c_n := \sum_{i\in\mathbb{Z}} a_i b_{n-i}$; $x^m x^k = x^{m+k}$ (weil $a_i b_{n-i} = 1 \Leftrightarrow n = m+k$)

„1" $(e_n)_{n\in\mathbb{Z}}$ mit $\forall k \in \mathbb{Z}\setminus\{0\} = 0 \wedge e_0 = 1$ mit

$(e_n)_{n\in\mathbb{Z}} (a_n)_{n\in\mathbb{Z}} = \left(\sum_{i\in\mathbb{Z}} e_i a_{n-i}\right)_{n\in\mathbb{Z}} = (a_n)_{n\in\mathbb{Z}}$

2) a) $(R[[[x]]], +, 0, -)$ ist eine abelsche Gruppe, weil es direkte Summe abelscher Gruppen ist

b) $(R[[[x]]], +, 0, \cdot)$ ist Halbring, denn

b.i) $(R[[[x]]], +, 0)$ ist kommutatives Monoid

b.ii) $(R[[[x]]], \cdot)$ ist Halbgruppe, denn

$\left((a_n)_{n\in\mathbb{Z}} \cdot (b_n)_{n\in\mathbb{Z}}\right) \cdot (c_n)_{n\in\mathbb{Z}} = \left(\sum_{i\in\mathbb{Z}} a_i b_{n-i}\right)_{n\in\mathbb{Z}} \cdot (c_n)_{n\in\mathbb{Z}} = \left(\sum_{i\in\mathbb{Z}} \left(\sum_{j\in\mathbb{Z}} a_j b_{i-j}\right) c_{n-i}\right)_{n\in\mathbb{Z}}$

$= \left(\sum_{i\in\mathbb{Z}} \sum_{j\in\mathbb{Z}} a_j b_{i-j} c_{n-i}\right)_{n\in\mathbb{Z}} = \left(\sum_{j\in\mathbb{Z}} a_j \left(\sum_{i\in\mathbb{Z}} b_{i-j} c_{n-i}\right)\right)_{n\in\mathbb{Z}} \overset{„i = i+j"}{=} \left(\sum_{j\in\mathbb{Z}} a_j \left(\sum_{i\in\mathbb{Z}} b_i c_{n-j-i}\right)\right) =$

$= (a_n)_{n\in\mathbb{Z}} \left(\sum_{i\in\mathbb{Z}} b_i c_{n-i}\right)_{n\in\mathbb{Z}} = (a_n)_{n\in\mathbb{Z}} \left((b_n)_{n\in\mathbb{Z}} (c_n)_{n\in\mathbb{Z}}\right)$

b.iii) kommutativ, denn $(a_n)_{n\in\mathbb{Z}} (b_n)_{n\in\mathbb{Z}} = \left(\sum_{i\in\mathbb{Z}} a_i b_{n-i}\right)_{n\in\mathbb{Z}} \overset{„i = n-i"}{=} \left(\sum_{i\in\mathbb{Z}} b_i a_{n-i}\right)_{i\in\mathbb{Z}} = (b_n)_{n\in\mathbb{Z}} (a_n)_{n\in\mathbb{Z}}$

b.iv) Das Distributivgesetz gilt, denn · ist kommutativ und linksdistributiv:

$(a_n)_{n\in\mathbb{Z}} \left((b_n)_{n\in\mathbb{Z}} + (c_n)_{n\in\mathbb{Z}}\right) = (a_n)_{n\in\mathbb{Z}} (b_n + c_n)_{n\in\mathbb{Z}} = \left(\sum_{i\in\mathbb{Z}} a_i (b_{n-i} + c_{n-i})\right)_{n\in\mathbb{N}} =$

$= \left(\sum_{i\in\mathbb{Z}} a_i b_{n-i} + \sum_{i\in\mathbb{Z}} a_i c_{n-i}\right)_{n\in\mathbb{Z}} = \left(\sum_{i\in\mathbb{Z}} a_i b_{n-i}\right)_{n\in\mathbb{Z}} + \left(\sum_{i\in\mathbb{Z}} a_i c_{n-i}\right)_{n\in\mathbb{Z}} = (a_n)_{n\in\mathbb{Z}} (b_n)_{n\in\mathbb{Z}} + (a_n)_{n\in\mathbb{Z}} (c_n)_{n\in\mathbb{Z}}$

c) Einselement siehe Punkt 1

3) $q \in R[[[x]]] \setminus \{0\}$ bel. mit $q = (q_n)_{n\in\mathbb{Z}} \wedge \ell \in \mathbb{Z}$ mit $q_\ell \neq 0$

$k := \min\{n \in \mathbb{Z} \mid q_n \neq 0\}$ $\qquad q(x) = \sum_{n=k}^{\infty} q_n x^n = x^k \sum_{n=0}^{\infty} q_{k+n} x^n = x^k \sum_{n=0}^{\infty} \bar{q}_n x^n =: \bar{q}(x)$

Nach Prop. 3.3.6.5 Punkt 6.:

$\bar{q}(x) \in R[[x]]^* \Leftrightarrow \bar{q}_0 \in R^* \Leftrightarrow \bar{q}_0 \neq 0 \Leftrightarrow q_k \neq 0$

also haben wir Existenz

Eindeutigkeit: $q(x) = x^k \bar{q}(x) = x^m \bar{p}(x)$ mit $\bar{q}(x), \bar{p}(x) \in R[[x]]^* \Leftrightarrow \bar{q}(x), \bar{p}(x) \in R[[x]] \wedge \bar{q}_0, \bar{p}_0 \neq 0$

also insbes. $x^k \bar{q}_0 = x^k q_k = x^m \bar{p}_0 = x^m q_m \Leftrightarrow x^k = x^m \Leftrightarrow k = m$

also $x^k \bar{q}(x) = x^k \bar{p}(x) \Leftrightarrow x^k (\bar{q}(x) - \bar{p}(x)) = 0 \Leftrightarrow \bar{q}(x) = \bar{p}(x)$ (formal: multiplizieren)

4) $q \in R[[[x]]] \setminus \{0\}$ wie in 3) $\quad q(x)\, x^{-k} \bar{q}^{-1}(x) = x^{k-k} \bar{q}(x) \bar{q}^{-1}(x) = 1$, also $q^{-1}(x) = x^{-k} \bar{q}^{-1}(x)$

also ist $R[[[x]]]$ ein Körper

5) •) $R[[x]]$ ist nach Prop. 3.3.6.5 Punkt 5 ein Integritätsbereich

•) $\iota: R[[x]] \to R[[[x]]]: \sum_{n\in\mathbb{N}} a_n x^n \mapsto \sum_{n\in\mathbb{Z}} a_n x^n$ mit $\forall n < 0: a_n = 0$ ist isomorphe Einbettung von $R[[x]]$ als Ring mit 1 in $R[[[x]]]$

•) Nach Punkt 4) hat jedes $\iota(q)$ mit $q \in R[[x]] \setminus \{0\}$ ein multiplikatives Inverses in $R[[[x]]]$

•) Sei nun Q ein weiterer kommutativer Ring mit Einselement und $\iota': R[[x]] \to Q$ isomorphe Einbettung, wobei $\forall q \in R[[x]] \setminus \{0\}: \iota'(q)$ besitzt Inverses.

$$\begin{tikzcd} R[[x]] \arrow[r, "\iota"] \arrow[dr, "\iota'"'] & R[[[x]]] \arrow[d, "\varphi"] \\ & Q \end{tikzcd}$$

$$\varphi: R[[[x]]] \to Q: q \longmapsto \begin{cases} 0, \text{ falls } q = 0 \\ \iota'(\bar{q}(x))\, \iota'(x^{-k})^{-1}, \text{ falls } q = x^k \bar{q}(x) \wedge k < 0 \text{ (siehe 3)} \\ \iota'(q(x)), \text{ falls } q = x^k \bar{q}(x) \wedge k \geq 0 \text{ (dann ist } q \in R[[x]]) \end{cases}$$

i) injektiv: $\varphi(p) = \varphi(q) \Leftrightarrow \iota'(\bar{q}(x))\, \iota'(x^{-k})^{-1} = \iota'(\bar{p}(x))\, \iota'(x^{-m})^{-1} \Leftrightarrow$

$\Leftrightarrow \iota'(\bar{q}(x))\, \iota'(x^{-m}) = \iota'(\bar{p}(x))\, \iota'(x^{-k}) \Leftrightarrow \iota'(\bar{q}(x) x^{-m}) = \iota'(\bar{p}(x) x^{-k}) \Leftrightarrow$

$\Leftrightarrow x^{-m} \bar{q}(x) = x^{-k} \bar{p}(x)$ und mit (3) gilt $q = p$

ii) strukturerhaltend: geht auf Strukturerhaltung von ι' zurück

iii) $\iota' = \varphi \circ \iota$

Eindeutigkeit: $\iota' = \varphi' \circ \iota = \varphi \circ \iota$, $\forall q \in \iota(R[[x]]): \varphi'(q) = \varphi(q)$

$q \in R[[[x]]] \setminus \iota(R[[x]])$; $\varphi'(q) = \varphi'(x^k \bar{q}(x)) = \varphi'(x^k)\, \varphi(\bar{q}(x)) = \varphi'((x^{-k})^{-1})\, \varphi(\bar{q}(x)) =$

$= \varphi'(x^{-k})^{-1} \varphi(\bar{q}(x)) = \varphi(x^{-k})^{-1} \varphi(\bar{q}(x)) = \varphi(x^k)\, \varphi(\bar{q}(x)) = \varphi(x^k \bar{q}(x)) = \varphi(q)$

Also ist $R[[[x]]]$ ein Quotientenkörper.

1. Zeigen Sie: Ist V ein endlichdimensionaler Vektorraum über einem Körper, so ist $\mathrm{End}(V)$ als Ring einfach (besitzt also nur die trivialen Ideale).
2. Zeigen Sie, dass dies für unendlichdimensionale Vektorräume nicht gilt. Hinweis: Betrachten Sie alle Endomorphismen mit endlichdimensionalem Bild.

1) Sei V ein endlichdim. Vektorraum über einem Körper K und $R := \mathrm{End}(V) = \{f : V \to V \mid f \text{ linear}\}$ ist nach Prop. 3.3.8.1. ein Ring mit 1

- $(f+g)(a) := f(a) + g(a)$
- $0(a) := 0$
- $(-f)(a) := -f(a)$
- $fg(a) := f(g(a))$
- $1(a) := a.$

Sei $\{0\} \neq I \trianglelefteq \mathrm{End}(V)$ ein Ideal. und $g \in \mathrm{End}(V)$, $b_1 \in V$: $g(b_1) = c_1 \neq 0$

Seien nun $B = \{b_1, \dots, b_n\}$ und $C = \{c_1, \dots c_n\}$ Basen von V

$\alpha_k : V \to V$: $b_k \mapsto b_1 \wedge b_j \mapsto 0$ für $j \neq k$ (linear fortgesetzt)

$\beta_l : V \to V$: $c_1 \mapsto b_l \wedge c_j \mapsto 0$ für $j \neq l$

$f_{kl} := \beta_l \circ g \circ \alpha_k$: $b_k \mapsto b_1 \mapsto c_1 \mapsto b_l$ und $b_j \mapsto 0 \mapsto 0 \mapsto 0$ für $j \neq k$

wegen $\mathrm{End}(V) I \subseteq I \wedge I\,\mathrm{End}(V) \subseteq I$ ist $f_{kl} \in I$

$f_{klc} := c\, f_{kl} \in I$ mit $c \in K$

$f \in \mathrm{End}(V)$ bel. mit $f(b_k) = \sum\limits_{l=1} c_{kl} b_l$

$f = \sum\limits_{k=1}^{n} \sum\limits_{l=1}^{n} f_{klc_{kl}}$, denn $j \in \{1, \dots, n\}$ bel.: $\sum\limits_{k=1}^{n} \sum\limits_{l=1}^{n} f_{klc_{kl}}(b_j) = \sum\limits_{l=1}^{n} c_{jl}\, f_{jl}(b_j) = \sum\limits_{l=1}^{n} c_{jl}\, b_l = f(b_j)$

2) $I := \{f : V \to V \mid \dim f(V) < \infty\}$

$I \leq \mathrm{End}(V)$, weil für $f_1, f_2 \in I$ gilt nach dem Dimensionssatz

$$\dim(f_1(V) + f_2(V)) = \dim(f_1(V)) + \dim(f_2(V)) - \dim(f_1(V) \cap f_2(V)) < \infty$$

Sei nun $g \in \mathrm{End}(V)$ bel. und $f \in I$ bel.

•) Nach der Rangformel gilt $\dim g(f(V)) = \dim f(V) - \mathrm{def}(g) \leq \dim f(V) < \infty$

also $gf \in I$

•) $\dim f(g(V)) \leq \dim f(V) < \infty$ also $fg \in I$

Es ist also $\mathrm{End}(V) I \subseteq I$ und $I\, \mathrm{End}(V) \subseteq I$

UE 208 ► Übungsaufgabe 3.4.5.5. (E) Beweisen Sie folgende Variante des Hauptsatzes 3.4.5.2: ◄ **UE 208**
Jede endliche abelsche Gruppe A ist direkte Summe zyklischer Gruppen C_{m_i}, $i = 1, \ldots, n$, deren Ordnungen $m_i > 1$ eine Teilerkette $m_1 | m_2 | \ldots | m_n$ bilden. Die m_i sind durch A eindeutig bestimmt. Hinweis: Aus Lemma 3.4.4.1 folgt leicht, dass direkte Summen zyklischer Gruppen mit teilerfremden Ordnungen wieder zyklisch sind. Damit lässt sich die hier zu beweisende Variante ohne große Mühe aus dem Hauptsatz in der Version von ableiten.

Sei A eine endliche abelsche Gruppe

inneres dir. Prod. $\cong$ äußeren dir. Prod.

Fall 1: „$\exists m \in \mathbb{N} : \exists r \in \mathbb{N} : A \cong C_m^r$", dann sind wir offensichtlich fertig.

Fall 2: „$\nexists m \in \mathbb{N}\ \nexists r \in \mathbb{N} : A \cong C_m^r$" Aus dem Hauptsatz über endliche abelsche Gruppen 3.4.5.2 erhalten wir eine Darstellung $A \cong C_{p_1^{k_1}}^{q_1} \oplus \cdots \oplus C_{p_l^{k_l}}^{q_l}$ mit

$\forall i, j \in \{1, \ldots, l\} : q_i, k_i \in \mathbb{N} \setminus \{0\} \wedge (i \neq j \Rightarrow p_i \neq p_j) \wedge p_i \in \mathbb{P}$ und o.B.d.A. $q_1 \geq q_2 \geq \cdots \geq q_l$

$n := q_1$; $\forall j \in \{1, \ldots, l-1\} : \forall i \in \{1, \ldots, q_j - q_{j+1}\} :$ $m_i := \prod_{s=1}^{j} p_j^{k_j}$

Nun gilt sicher $m_1 | m_2 | \cdots | m_n$

und wir wissen bereits aus Übungsaufgabe 3.7.4.15:

$\forall i \in \{1, \ldots, n\} :$ $C_{m_i} \cong \bigoplus_{p \in \mathbb{P}} C_{p^{e_p}}$, wobei $m_i = \prod_{p \in \mathbb{P}} p^{e_p}$, also, dass C_{m_i} eine zyklische Gruppe ist

Beispiel: $A \cong C_{p_1^{k_1}}^{q_1} \oplus C_{p_2^{k_2}}^{q_2} \oplus C_{p_3^{k_3}}^{q_3} \cong C_{p_1^{k_1}}^{q_1-q_2} \oplus C_{p_1^{k_1}}^{q_2} \oplus C_{p_2^{k_2}}^{q_2} \oplus C_{p_3^{k_3}}^{q_3} \cong$

$\cong C_{p_1^{k_1}}^{q_1-q_2} \oplus C_{p_1^{k_1}}^{q_2-q_3} \oplus C_{p_2^{k_2}}^{q_2-q_3} \oplus C_{p_1^{k_1}}^{q_3} \oplus C_{p_2^{k_2}}^{q_3} \oplus C_{p_3^{k_3}}^{q_3} \cong$

$\underbrace{C_{p_1^{k_1}} \oplus \cdots \oplus C_{p_1^{k_1}}}_{q_1-q_2} \oplus \underbrace{C_{\prod_{i=1}^{2} p_i^{k_i}} \oplus \cdots \oplus C_{\prod_{i=1}^{2} p_i^{k_i}}}_{q_1-q_3} \oplus \underbrace{C_{\prod_{i=1}^{3} p_i^{k_i}} \oplus \cdots \oplus C_{\prod_{i=1}^{3} p_i^{k_i}}}_{q_3}$

Hinweis nicht verwendet! falsch?

Übungsaufgabe 3.4.5.7. (F) Sei p eine Primzahl.

1. Wie viele Untergruppen hat $C_p \times C_p$?
2. Wie viele Untergruppen hat C_{p^2}?

(Hinweis: Überlegen Sie sich zuerst, dass alle nichttrivialen Untergruppen zyklisch sein müssen.)

1) $C_p \times C_p = \{(a+p\mathbb{Z}, b+p\mathbb{Z}) \mid a,b \in \mathbb{Z}\}$

Sei $U \leq C_p \times C_p$

Fall 1: „$\exists (\bar{a},\bar{b}) \in U: \bar{a} \neq \bar{b}$", also $\bar{a} \neq 0 \vee \bar{b} \neq 0$

Fall 1.1 „$\bar{a} \neq 0$"

Fall 1.1.1: „$\bar{b}=0$" Nach Prop. 3.2.4.9. ist $\bar{a}$ ein erzeugendes Element von C_p

es ist also $\langle(\bar{a},\bar{0})\rangle = C_p \times \{0\}$ eine Untergruppe von $U \leq C_p \times C_p$

Fall 1.1.2: „$\bar{b} \neq 0$" dann sind $\bar{a}$ und b erzeugende Elemente und es gibt $\alpha, \beta \in \mathbb{N}$:

$\alpha \bar{a} = 0 \wedge \beta \bar{b} = 0$, wobei $\alpha \bar{b} \neq 0 \wedge \beta \bar{a} \neq 0$ warum?

$\alpha(\bar{a},\bar{b}) = (0, \alpha\bar{b}) \in U \rightsquigarrow$ nach Fall 1.2.1 also auch $(\bar{0},\bar{1}) \in U$

$\beta(\bar{a},\bar{b}) = (\beta\bar{a}, 0) \in U \longrightarrow$ nach Fall 1.1.1 also auch $(\bar{1},\bar{0}) \in U$

mit $(\bar{0},\bar{1})$ und $(\bar{1},\bar{0}) \rightsquigarrow U = C_p \times C_p$

Fall 1.2 „$\bar{a}=0$" dann ist $\bar{b} \neq 0$

Fall 1.2.1: „$\bar{a}=0$": wie Fall 1.1.1: $\{0\} \times C_p \leq U \leq C_p \times C_p$

Fall 1.2.2.: „$\bar{a} \neq 0$": wie Fall 1.1.2.: $U = C_p \times C_p$

Fall 2: „$\nexists (\bar{a},\bar{b}) \in U: \bar{a} \neq \bar{b}$"

Fall 2.1: „$U = \{0\}$"

Fall 2.2.: „$U \neq \{0\}$" also gilt es $(\bar{a},\bar{a}) \in U$ mit $\bar{a} \neq 0$ und $\{(\bar{a},\bar{a}) \mid \bar{a} \in C_p\} \leq U \leq C_p \times C_p$

Es gibt 5 Untergruppen: $\{0\}$, $\{0\} \times C_p$, $C_p \times \{0\}$, $\{(\bar{a},\bar{a}) \in C_p \times C_p \mid \bar{a} \in C_p\}$, $C_p \times C_p$

2) Sei $U \leq C_{p^2}$

Fall 1: „$U = \{0\}$"

Fall 2: „$U \neq \{0\}$" also $\exists\ \bar{a} \in U$ mit $\bar{a} \neq 0$

Fall 2.1 „$\bar{a} = \bar{p}$" $\{n\bar{p} \mid n \in \mathbb{Z}\} \leq U \leq C_{p^2}$

Fall 2.2 „$\bar{a} \neq \bar{p}$" $\forall \bar{b} < \overline{p^2}$: $\bar{b}\,\bar{a} \neq 0$, denn sonst hätte p^2 eine weitere Primzahlzerlegung

warum?

also ist $|U| = p^2 = |C_{p^2}|$ deshalb $U = C_{p^2}$

Es gibt 3 Untergruppen: $\{0\}$, $\{n\bar{p} \mid n \in \mathbb{Z}\}$, C_{p^2}

UE 212 ▶ Übungsaufgabe 3.4.5.9. (A) Sei p eine Primzahl. Wie viele Automorphismen hat $C_p \times C_p$? (Hinweis: Verwenden Sie Ihr Wissen aus der Linearen Algebra.) ◀ **UE 212**

Sei $\varphi: C_p \times C_p \to C_p \times C_p$ ein Automorphismus

$\varphi(\bar{0},\bar{0}) = (\bar{0},\bar{0})$ und $\varphi(\bar{1},\bar{0}) = (\bar{a},\bar{b}) \neq 0$, weil φ injektiv ist

Fall 1: „$\bar{a} \neq 0$"

Fall 1.1: „$\bar{b} \neq \bar{0} \wedge \bar{b} \neq \bar{a}$" es ist $\varphi(C_p \times \{0\})$ eine Untergruppe von $C_p \times C_p$ mit gleich vielen Elementen wie $C_p \times \{0\}$, eine entsprechende gibt es aber nicht ↯

Fall 1.2: „$b = \bar{0}$" dann ist $\varphi(C_p \times \{0\}) = C_p \times \{0\}$, es gibt p Möglichkeiten

Fall 1.3: „$\bar{b} = \bar{a}$" dann ist $\varphi(C_p \times \{0\}) = \{(\bar{a},\bar{a}) \mid \bar{a} \in C_p\}$, es gibt p Möglichkeiten

Fall 2: „$\bar{a} = \bar{0}$" dann ist $\bar{b} \neq \bar{0}$ und $\varphi(C_p \times \{0\}) = \{0\} \times C_p$

Für $\varphi(\bar{0},\bar{1})$ funktioniert alles analog, bloß $\forall (\bar{x},\bar{y}) \in \varphi(C_p \times \{0\}): (\bar{x},\bar{y}) \notin \varphi(\{0\} \times C_p)$

Also: Für $\varphi(\bar{1},\bar{0})$ gibt es $3p$ Mglkt. und für $\varphi(\bar{0},\bar{1})$ gibt es $2p$ Mglkt.

insgesamt: $3p \cdot 2p = 6p$ Automorphismen

funktioniert das dann alles?

Satz 3.5.2.5. *Jede archimedisch angeordnete abelsche Gruppe G lässt sich als solche isomorph in die geordnete additive Gruppe $\mathbb{R}$ der reellen Zahlen einbetten. (Umgekehrt ist jede additive Untergruppe von $\mathbb{R}$ archimedisch angeordnet.) Ist $\iota : G \to \mathbb{R}$ eine solche isomorphe Einbettung, so sind alle anderen gegeben durch sämtliche Abbildungen $\lambda\iota$ mit reellem $\lambda > 0$.*

UE 215 ▶ Übungsaufgabe 3.5.2.6. (W) Beweisen Sie Satz 3.5.2.5. Anleitung für die Existenz von ι: Gehen Sie für nichttriviales G von einem positiven Element $g \in G$ aus, das Sie auf die reelle Zahl $1 = \iota(g)$ abbilden. Wegen der archimedischen Eigenschaft definiert das einen eindeutigen ordnungsverträglichen Homomorphismus ι, der (wieder wegen der archimedischen Eigenschaft) sogar injektiv sein muss. **◀ UE 215**

Fall 1: „$G = \{0\}$"

Fall 2: „$G \neq 0$", also $0 \neq g \in G$, o.B.d.A. $g \in G^+$ (sonst $:= -g$) sei also $\iota(g) = 1$, damit ist $\forall k \in \mathbb{Z} : \iota(kg) = k\,\iota(g) = k$

$h \in G \setminus \mathbb{Z}g$ wieder o.B.d.A: $h \in G^+$

$\forall n \in \mathbb{N}\setminus\{0\} : m_n := \min \{k \in \mathbb{N} \mid nh \leq kg\}$

also $n\,\iota(h) = \iota(nh) \leq \iota(m_n g) = m_n \Leftrightarrow \iota(h) \leq \frac{m_n}{n}$

und $m_n - 1 = \iota((m_n - 1)g) \leq \iota(nh) = n\,\iota(h) \Leftrightarrow \frac{m_n - 1}{n} \leq \iota(h)$

also $\forall n \in \mathbb{N} : \frac{m_n - 1}{n} \leq \iota(h) \leq \frac{m_n}{n}$

Und wegen $\frac{m_n}{n} - \frac{m_n - 1}{n} = \frac{1}{n} \xrightarrow{n \to \infty} 0$ erhalten wir so eine Cauchyfolge in $\mathbb{R}$, die wegen der Vollst. von $\mathbb{R}$ konvergiert gegen $x \in \mathbb{R}$ und es muss deshalb $\iota(h) = x$ sein

Zur Injektivität: Sei $h \in G \setminus \{0\}$, o.B.d.A. $h \in G^+$

$\exists n \in \mathbb{N} : 1 \leq n\,\iota(h)$, weil $\mathbb{R}$ archimedisch angeordnet ist

also $\frac{1}{n} \leq \iota(h)$ und damit $\iota(0) = 0 < \iota(h)$

daraus erhalten wir die Injektivität, denn für $a \neq b \in G$ gilt

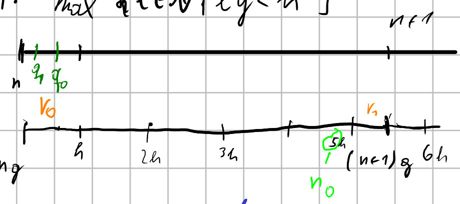
$\iota(a) - \iota(b) = \iota(a - b) \neq 0 \Rightarrow \iota(a) \neq \iota(b)$

Zur „Eindeutigkeit": Sei nun α weitere isomorphe Einbettung mit $\alpha(g) = \lambda = \lambda\iota(g) = \iota(\lambda g)$

Wie vorhin $\lambda\frac{m_n - 1}{n} = \frac{m_n - 1}{n}\alpha(g) \leq \alpha(h) \leq \frac{m_n}{n}\alpha(g) = \lambda\frac{m_n}{n}$

$\Rightarrow \alpha(h) = \lambda\,\iota(g)$

Da G archimedisch angeordnet ist $\exists\, l \in \mathbb{N}: h < lg$ und sei $n := \max\{l \in \mathbb{N} \mid lg < h\}$



$r_0 := \min\{h - ng,\ (n+1)g - h\}$

$n_0 := \max\{m \in \mathbb{N} \mid m r_0 \leq g\}$

$q_0 := \frac{1}{n_0 + 1} \qquad (\iota(h) \geq q_0)$

$r_1 := g - n_0 r_0$

$n_1 := \max\{m \in \mathbb{N} \mid m r_1 \leq g\}$

$q_1 := q_0 \frac{1}{(n_1+1)}$, wobei $q_1 = 0$ falls $r_1 = 0$

$r_k := g - n_{k-1} r_{k-1}$

$n_k := \max\{m \in \mathbb{N} \mid m r_k \leq g\}$, wobei $n_k = \infty$

$q_k := \prod_{i=0}^{k-1} q_i \frac{1}{n_k + 1}$, wobei $q_k = 0$, falls $r_k = 0$

„$\iota(h) = q_0 + q_0 \overbrace{\iota(r_1)}^{\text{kenne ich nicht}}$"

„$\iota(r_1) = \frac{1}{n_1+1} + \frac{1}{n_1+1}\iota(r_2)$"

„also „$\iota(h) = q_0 + q_0\left(\frac{1}{n_1+1} + \frac{1}{n_1+1}\iota(r_2)\right) =$

$= q_0 + \underbrace{q_0 \frac{1}{n_1+1}}_{q_1} + q_0 \frac{1}{n_1+1}\iota(r_2)$"

$$\iota(h) = \begin{cases} n + \sum_{i=0}^{\infty} q_i, & \text{falls } r_0 = h - ng \\ n+1 - \sum_{i=0}^{\infty} q_i, & \text{falls } r_0 = (n+1)g - h \end{cases}$$

$\forall n \in \mathbb{N}: \sum_{i=0}^{n} q_i \leq \frac{1}{n_0}$ (nach Konstruktion) und die Folge $\left(\sum_{i=0}^{n} q_i\right)_{n \in \mathbb{N}}$ ist mon. wachsend also konvergent

- $h_1, h_2 \in G$ bel. $\iota(h_1) + \iota(h_2) = m_1 + \sum_{i=0}^{\infty} q_i + m_2 + \sum_{i=0}^{\infty} p_i = (m_1 + m_2) \sum_{i=0}^{\infty}(q_i + p_i) \overset{?}{=} \iota(h_1 + h_2)$
- $h_1, h_2 \in G$ mit $h_1 < h_2$

  $\iota(h_2 - h_1) > 0$ und $\iota(h_2) = \iota(h_1) + \iota(h_2 - h_1) > \iota(h_1)$
- $\iota(h_1) = \iota(h_2) \Rightarrow h_1 = h_2$, also ι injektiv

Sei nun α eine weitere isomorphe Einbettung von (nichttrivialem) G in $\mathbb{R}$

betrachte $\alpha(g) = \lambda \in \mathbb{R}$ damit ist α eindeutig festgelegt

Ang. $\exists\, h \in G$: mit o.B.d.A.: $\alpha(h) < \lambda\iota(h)$ fehlt noch!