Lineare Algebra II

Dozent: Prof. Mohamed Barakat / Mitschrift: Alexander Köster

30. August 2018

Eine Sammlung des Vorlesungs- und Übungsstoffes der (linearen) Algebra.

Diese Sammlung ersetzt keine Klausurvorbereitung. Sie wurde unabhängig von der Universität erstellt und beinhaltet nur die wichtigsten Sätze und Algorithmen.
Bis auf ein paar Anpassungen, Ergänzungen, eigene Lösungen von „trivialen Übungen“ und Übungsaufgaben, unterliegt der Inhalt dem Urheberrecht von Prof. Barakat. Ich bin sehr dankbar für die Detailtiefe seiner Vorlesung, die die Veranstaltung deutlich lehrreicher gemacht hat als übliche Vorlesungen der Linearen Algebra.

Besonders wichtige Sätze und Anmerkungen sind in violett geschrieben.
Beispiele sind in pink geschrieben.

Inhaltsverzeichnis

6 Moduln

Moduln verallgemeinern die Vektorraumstruktur über Ringe, statt über Körper.

6.1 Moduln

Definition 6.1.1: Modul / Linksmodul

Sei R ein Ring mit Eins. Eine Abelsche Gruppe $(M,+)$ heißt **R-Modul** ['mo:dʊl] (nicht [mo'du:l]!) (genauer: R-Linksmodul), falls eine Abbildung

$$\begin{aligned} \cdot : R \times M &\longrightarrow M \\ (r,\ m) &\longmapsto r \cdot m \end{aligned}$$

gegeben ist, wobei $\forall r,s \in R,\ m,n \in M$:

(1) $r(m+n) = rm + rn$

(2) $(r+s)m = rm + sm$

(3) $(rs)m = r(sm)$

(4) $1_R \cdot m = m$

Ist M ein R-Modul, so heißt eine Teilmenge $T \subseteq M$ ein **Teilmodul**, in Zeichen $T \leq M$, falls:

- $T \neq \emptyset$
- $\forall t_1, t_2 \in T,\ a \in R : at_1 + t_2 \in T$

Ein Vektorraum ist also nichts anderes als ein Modul über einem Körper.

Übung 6.1.Ü1:

Teilmoduln von einem R-Modul M sind genau die Teilmengen $T \subseteq M$, die unter Einschränkung von Addition und Multiplikation wieder R-Moduln sind.

Beispiel 6.1.2: Moduln, die wir kennen

(1) Jede Abelsche Gruppe $(M,+)$ ist ein $\mathbb{Z}$-Modul mit

$$\underset{\in\mathbb{Z}}{a} \cdot \underset{\in M}{m} := \begin{cases} \overbrace{m + \cdots + m}^{a\text{-mal}} & \text{falls } a > 0 \\ 0_M & \text{falls } a = 0 \\ -\underbrace{(m + \cdots + m)}_{a\text{-mal}} & \text{falls } a < 0 \end{cases}$$

(2) Sei $\mathcal{V}$ ein K-Vektorraum für einen Körper K und $\varphi \in \mathrm{End}_K(\mathcal{V})$.
Dann wird $\mathcal{V}$ zu einem $K[x]$-Modul durch

$$p(x) \cdot V := p(\varphi)(V) \in \mathcal{V} \quad \forall p(x) \in K[x], V \in \mathcal{V}$$

Beweis:

Seien $p(x), q(x) \in K[x],\ V, W \in \mathcal{V}$. Es gilt:

(1) $p(x) \cdot (V+W) = p(\varphi)(V+W) = p(\varphi)(V) + p(\varphi)(V) = p(x) \cdot V + p(x) \cdot W$
da φ und damit Kombinationen von φ in p linear sind.

(2) $(p(x)+q(x)) \cdot V = (p+q)(\varphi)(V) = \big(p(\varphi) + p(\varphi)\big)(V) = p(\varphi)(V) + q(\varphi)(V)$
per Definition von werteweiser Addition von Polynomen.

(3) Analog gilt das per Def. für (ebenfalls werteweise) Multiplikation in $K[x]$.

(4) $1_{K[x]} \cdot V = f(\varphi)(V) = \varphi^0(V) = \mathrm{id}_{\mathcal{V}}(V) = V$, wobei $f(x) = 1 = x^0 \in K[x]$

□

Übung 6.1.Ü2:

Seien R und S Ringe, $\psi : R \to S$ ein Ringhomomorphismus und M ein S-Modul. Dann wird ein R-Modul M zu einem S-Modul durch $rm := \psi(r)m$ für $r \in R,\ m \in M$.

Erinnerung:

Ein **Ringhomomorphismus** ist eine Abbildung $\varphi : R \to S$ zwischen zwei Ringen $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$, wenn für alle $r_1, r_2 \in R$ gilt:

$$\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2) \quad \text{und} \quad \varphi(r_1 \cdot_R r_2) = \varphi(r_1) \cdot_S \varphi(r_2)$$

Bemerkung 6.1.3: Modulerzeugnis

Sei M ein R-Modul.

(1) Sei $\mathcal{T}$ eine Menge von Teilmoduln von M. Dann gilt:

$$\bigcap_{T \in \mathcal{T}} T \leq M$$

(2) Sei $X \subseteq M$. Dann ist

$$\langle X \rangle := \bigcap_{X \subseteq T \leq M} T$$

das **Erzeugnis** von X, d.h. der kleinste Teilmodul, der X enthält.

(3) Es gilt für $X \subseteq M$:

$$\langle X \rangle = \left\{ m \in M \,\middle|\, \exists k \in \mathbb{N}_0,\ a \in R^k,\ v \in X^k : a_1 v_1 + \cdots + a_k v_k = m \right\}$$

Konvention: Die leere Linearkombination entspricht 0.

Beweis:

Die Menge auf der rechten Seite, nenne sie $\overline{X}$, ist ein R-Teilmodul von M. Es gilt $X \subseteq \overline{X}$, da R eine 1 besitzt. Also ist per Definition das Erzeugnis $\langle X \rangle \subseteq \overline{X}$. Aber andererseits ist $\overline{X}$ in jedem Teilmodul von M enthalten, welcher X enthält, da man in Teilmoduln die Elemente von X natürlich linearkombinieren kann. $\Rightarrow \overline{X} \subseteq \langle X \rangle \Rightarrow \overline{X} = \langle X \rangle$ □

Gilt für $B \subseteq M$, dass $\langle B \rangle = M$, nennt man B auch **Erzeugendensystem** (EZS) von M.

Definition 6.1.4: Modulhomomorphismus

Seien M, N zwei R-Moduln. Eine Abbildung $\varphi : M \to N$ heißt **R-Modulhomomorphismus**, falls φ mit beiden Operationen verträglich ist. D.h.:

$$\varphi(rm_1 + m_2) = r\varphi(m_1) + \varphi(m_2) \quad \forall m_1, m_2 \in M,\ s, r \in R$$

In diesem Fall heißt die Faser über 0 der **Kern** von φ:

$$\operatorname{Kern} \varphi := \varphi^{-1}(\{0_N\}) = \left\{ m \in M \,\middle|\, \varphi(m) = 0_N \right\}$$

Bemerkung 6.1.5:

Seien M, N zwei R-Moduln und $\varphi : M \to N$ ein R-Modulhomomorphismus.

(1) Die Komposition von R-Modulhomomorphismen ist ein R-Modulhomomorphismus.

(2) $\operatorname{Kern}\varphi$ ist ein Teilmodul von M und $\operatorname{Bild}\varphi := \{\varphi(m) \mid m \in M\}$ ein Teilmodul von N.

(3) φ ist injektiv $\Leftrightarrow \operatorname{Kern}\varphi = \{0\}$
φ ist surjektiv $\Leftrightarrow \operatorname{Bild}\varphi = N$

(4) Ist φ bijektiv (**R-Modulisomorphismus**), so ist die mengentheoretische Umkehrabbildung φ^{-1} wieder ein R-Modulisomorphismus.
Insbesondere ist die Isomorphie von Moduln eine Äquivalenzrelation.

(5) R-Modulhomomorphismen von M in sich heißen **R-Modulendomorphismen**.

$$\operatorname{End}_R(M) := \{\varphi : M \to M \mid \varphi\ R\text{-Modulhomomorphismus}\}$$

heißt der **Endomorphismenring** des R-Moduls M. Es ist $\operatorname{End}_R(M)$ ein Ring und im Falle, dass R kommutativ ist, sogar eine R-Algebra.

Beweis zu 6.1.5:

Analog zu K-Vektorraumhomomorphismen:
Seien M, N, P drei R-Moduln, $\varphi : M \to N$, $\psi : N \to P$ zwei R-Modulhomomorphismen.

(1) Seien $m_1, m_2 \in M$, $r \in R$. Dann gilt durch die Linearität von φ und ψ:
$(\psi \circ \varphi)(rm_1 + m_2) = \psi\left(\varphi(rm_1 + m_2)\right) = \psi\left(r\varphi(m_1) + \varphi(m_2)\right) = r\left(\psi \circ \varphi\right)(m_1) + \left(\psi \circ \varphi\right)(m_2)$
$\Rightarrow \psi \circ \varphi$ ist ein R-Modulhomomorphismus. □

(2)
- $\varphi(0_M) = \varphi(0_R \cdot 0_M) = 0_R \cdot \varphi(0_M) = 0_N \Rightarrow 0_M \in \operatorname{Kern}\varphi \Rightarrow \operatorname{Kern}\varphi \neq \emptyset$
- Seien $k_1, k_2 \in \operatorname{Kern}\varphi$, d.h. $\varphi(k_1) = \varphi(k_2) = 0_N$. $\Rightarrow r\varphi(k_1) + \varphi(k_2) = 0_N \Rightarrow rk_1 + k_2 \in \operatorname{Kern}\varphi$.

$\Rightarrow \operatorname{Kern}\varphi$ ist ein R-Teilmodul von M. □

- $0_R \in R$. $\Rightarrow \varphi(0_R \cdot 0_M) = 0_N \in \operatorname{Bild}\varphi$.
- Seien $y_1, y_2 \in \operatorname{Bild}\varphi$, d.h. $\exists x_1, x_2 \in M : \varphi(x_1) = y_1,\ \varphi(x_2) = y_2$.
$\Rightarrow \varphi(rx_1 + x_2) = r\varphi(x_1) + \varphi(x_2) = ry_1 + y_2 \Rightarrow ry_1 + y_2 \in \operatorname{Bild}\varphi$

$\Rightarrow \operatorname{Bild}\varphi$ ist ein R-Teilmodul von N. □

(3) „⇒“ Sei φ injektiv. Natürlich ist dann $\operatorname{Kern}\varphi = \varphi^{-1}(\{0_N\})$ maximal einelementig, und da $0_M \in \operatorname{Kern}\varphi$, ist $\operatorname{Kern}\varphi = \{0_M\}$.

„⇐“ Sei φ nicht injektiv, d.h. $\exists m_1, m_2 \in M : m_1 \neq m_2 \wedge \varphi(m_1) = \varphi(m_2)$. $\Rightarrow 0_N = \varphi(m_1) - \varphi(m_2) = \varphi(m_1 - m_2)$ und da $m_1 \neq m_2 \Rightarrow m_1 - m_2 \neq 0_M$, ist $\operatorname{Kern}\varphi \neq \{0_M\}$. Also: $\operatorname{Kern}\varphi = \{0_M\} \Rightarrow \varphi$ injektiv.

Und dass $\operatorname{Bild}\varphi = N \Leftrightarrow \varphi$ surjektiv ist praktisch die Definition von Surjektiv. □

(4) Sei φ bijektiv, d.h. $\exists \varphi^{-1} : N \to M$ mit $\varphi \circ \varphi^{-1} = \mathrm{id}_N$ und $\varphi^{-1} \circ \varphi = \mathrm{id}_M$. Seien $n_1, n_2 \in N$, $r \in R$.

$$\begin{aligned} &\Rightarrow && \varphi\left(r\varphi^{-1}(n_1) + \varphi^{-1}(n_2)\right) = rn_1 + n_2 \\ \varphi^{-1}\text{ von links } &\Rightarrow && \varphi^{-1} \circ \varphi\left(r\varphi^{-1}(n_1) + \varphi^{-1}(n_2)\right) = \varphi^{-1}(rn_1 + n_2) \\ &\Rightarrow && r\varphi^{-1}(n_1) + \varphi^{-1}(n_2) = \varphi^{-1}(rn_1 + n_2) \end{aligned}$$

□

id_M ist ein Modulisomorphismus, also ist Isomorphie von Moduln reflexiv. Mit φ^{-1} ist nach obigem Beweis ein Isomorphismus gegeben, der die Isomorphie von Moduln symmetrisch macht. Und nach (1) zusammen mit der Eigenschaft, dass Komposition bijektiver Abbildungen bijektiv ist, ist Isomorphie transitiv, damit also eine Äquivalenzrelation. □

(5) Werteweise Addition und Multiplikation von Modulendomorphismen und Multiplikation mit Ringelementen ist durch die Linearität von Modulhomomorphismen abgeschlossen und durch Distributivgesetze verträglich.

□

Bemerkung 6.1.A1: Alternative Definition von R-Moduln

(1) Eine Abelsche Gruppe $(M,+)$ heißt **R-Modul**, falls ein Ringhomomorphismus

$$\rho_M : R \longrightarrow \mathrm{End}(M)$$

gegeben ist, für den $\rho_M(1_R) = \mathrm{id}_M$ gilt, wobei $\mathrm{End}(M)$ mit bildweiser Addition als Ringaddition und Komposition als Ringmultiplikation aufgefasst wird (und damit $1_{\mathrm{End}(M)} = \mathrm{id}_M$).

(2) Ein Gruppenhomomorphismus $\varphi : M \to N$ zwischen zwei R-Moduln (d.h. $\forall m_1, m_2 \in M : \varphi(m_1 +_M m_2) = \varphi(m_1) +_N \varphi(m_2)$) gegeben mit den Ringhomomorphismen ρ_M und ρ_N heißt **R-Modulhomomorphismus**, falls gilt: $\varphi \circ \rho_M(r) = \rho_N(r) \circ \varphi \ \forall r \in R$

Beweis:

Diese Definitionen sind äquivalent zu den oben zuerst erwähnten Definitionen.

(1) „⇒“: Sei M ein R-Modul nach der ursprünglichen Definition 6.1.1.
Konstruiere ρ_M durch:

$$\begin{aligned} \rho_M : R &\longrightarrow \mathrm{End}(M) \\ r &\longmapsto (m \mapsto rm) \end{aligned}$$

Es gilt für $r, s \in R$:

$$\rho_M(r+s) = (m \mapsto (r+s)m) = (m \mapsto rm + sm) = (m \mapsto rm) + (m \mapsto sm) = \rho_M(r) + \rho_M(s)$$

nach dem zweiten Modulaxiom und

$$\rho_M(rs) = (m \mapsto (rs)m) = (m \mapsto r(sm)) = (m \mapsto rm) \circ (m \mapsto sm) = \rho_M(r) \circ \rho_M(s)$$

nach dem dritten Modulaxiom. Somit ist ρ_M ein Ringhomomorphismus.
Nach dem letzten Modulaxiom gilt $\rho_M(1_R) = (m \mapsto 1_R m) = (m \mapsto m) = \mathrm{id}_M$.

„⇐“: Sei M ein R-Modul mit ρ_M nach der neuen Definition.
Definiere die Modulmultiplikation durch:

$$\begin{aligned} \cdot : R \times M &\longrightarrow M \\ (r,\ m) &\longmapsto \rho_M(r)(m) \end{aligned}$$

Dann gilt für $r, s \in R,\ m, n \in M$:

- $r(m+n) = \rho_M(r)(m+n) = \rho_M(r)(m) + \rho_M(r)(n) = rm + rn$,
  da $\rho_M(r) \in \mathrm{End}(M)$ und damit linear.
- $(r+s)m = \rho_M(r+s)(m) = \rho_M(r)(m) + \rho_M(s)(m) = rm + sm$
  und $(rs)m = \rho_M(rs)(m) = \rho_M(r)(m) \circ \rho_M(s)(m) = r(sm)$,
  da ρ_M Ringhomomorphismus.
- $1_R m = \rho_M(1_R)(m) = \mathrm{id}_M(m) = m$

□

(2) „⇒“: Sei $\varphi : M \to N$ ein R-Modulhomomorphismus nach der ursprünglichen Definition 6.1.4, und ρ_M, ρ_N die Ringhomomorphismen definiert wie im Beweis von (1) „⇒“.
Betrachte für $r \in R$:

$$\big(\varphi \circ \rho_M(r)\big) = \varphi \circ (m \mapsto rm) = \big(m \mapsto \varphi(rm)\big) = \big(m \mapsto r\varphi(m)\big) = (n \mapsto rn) \circ \varphi = \rho_N(r) \circ \varphi$$

„⇐“: Sei $\varphi : M \to N$ ein R-Modulhomomorphismus nach der neuen Definition. Sei die Modulmultiplikation definiert wie im Beweis von (1) „⇐“.
Dann gilt für $r \in R,\ m_1, m_2 \in M$:

$$\begin{aligned} \varphi(rm_1 + m_2) &= \varphi(rm_1) + \varphi(m_2) = \varphi\big(\rho_M(r)(m_1)\big) + \varphi(m_2) = \big(\varphi \circ \rho_M(r)\big)(m_1) + \varphi(m_2) \\ &= \big(\rho_N(r) \circ \varphi\big)(m_1) + \varphi(m_2) = \rho_N(r)\big(\varphi(m_1)\big) + \varphi(m_2) = r\varphi(m_1) + \varphi(m_2) \end{aligned}$$

□

Ein wichtiger Struktursatz für Vektorräume war der **Steinitz'sche Austauschsatz**, der uns vielfältige Möglichkeiten eröffnete, Basen zu konstruieren. Dieser ist für allgemeine R-Moduln **falsch**. (Denn Inverse im Körper sind im Beweis von Steinitz wichtig.)

Beispiel 6.1.6: Gegenbeispiel zu Steinitz in Moduln:

Sei $R := \mathbb{Z}$ und $M := \mathbb{Z}^{3\times 1}$. Dann wird M durch Einschränken der $\mathbb{Q}$-Vektorraumstruktur von $\mathbb{Q}^{3\times 1}$ zu einem $\mathbb{Z}$-Modul.
Jedes Element von M ist eine eindeutige $\mathbb{Z}$-Linearkombination aus der Standardbasis:

$$E = (e_1, e_2, e_3)$$

Jedoch ist $(e_1, e_2, 2e_3)$ eine $\mathbb{Z}$-linear unabhängige Teilmenge von M, aber **keine** Basis mehr, da sie kein Erzeugendensystem mehr ist:

$$\langle e_1, e_2, 2e_3\rangle = \left\{ \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} \,\middle|\, z_3 \text{ gerade} \right\} \subsetneq M, \quad \text{z.B. } M \ni \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \notin \langle e_1, e_2, 2e_3\rangle$$

Übung 1.2:

Sei R ein kommutativer Ring und M, N seien R-Linksmoduln. Dann ist

$$\mathrm{Hom}_R(M,N) := \{f : M \to N \mid f \text{ ist } R\text{-Modulhomomorphismus}\}$$

ein R-Linksmodul mit werteweiser Addition und werteweiser Ringmultiplikation.

Beweis:
$\mathrm{Hom}_R(M,N) \subseteq N^M$, somit vererben sich die Eigenschaften der additivien Abelschen Gruppe.
Ist diese Teilmenge abgeschlossen? Seien $f, g \in \mathrm{Hom}_R(M,N)$, $r \in R$, $m_1, m_2 \in M$ beliebig.

$$\begin{aligned}(f+g)(rm_1+m_2) &= f(rm_1+m_2) + g(rm_1+m_2)\\ &= rf(m_1) + f(m_2) + rg(m_1) + g(m_2)\\ &= r(f(m_1)+g(m_2)) + f(m_2) + g(m_2) = r(f+g)(m_1) + (f+g)(m_2)\end{aligned}$$

$\Rightarrow f+g \in \mathrm{Hom}_R(M,N)$

Seien nun $f, g, h \in \mathrm{Hom}_R(M,N)$, $r, s \in R$ beliebig. Per Definition gilt:

- $r(f+g) = rf + rg \Leftrightarrow \forall m \in M : r(f(m)+g(m)) = rf(m) + rg(m)$
- $(r+s)f = rf + sf \Leftrightarrow \forall m \in M : (r+s)f(m) = rf(m) + sf(m)$
- $(rs)f = r(sf) \Leftrightarrow \forall m \in M : (rs)f(m) = r(sf(m))$
- $1_R f = f \Leftrightarrow \forall m \in M : 1_R f(m) = f(m)$

Dies sind alles Tautologien, da die rechte Seite der Äquivalenz im Modul und damit insbesondere der Gruppe N trivialerweise gilt.

Zuletzt ist $\mathrm{Hom}_R(M,N)$ unter Ringmultiplikation abgeschlossen, denn:
Seien $f \in \mathrm{Hom}_R(M,N)$, $r, s \in R$, $m_1, m_2 \in M$ beliebig.

$$\begin{aligned}(rf)(sm_1+m_2) &= rf(sm_1+m_2)\\ &= r(sf(m_1)+f(m_2))\\ &= rsf(m_1) + rf(m_2) = s(rf)(m_1) + rf(m_2)\end{aligned}$$

$\Rightarrow rf \in \mathrm{Hom}_R(M,N)$ □

Übung 6.1.Ü3:

Die Spalten der Matrix $A \in \mathbb{Z}^{n\times n}$ bilden genau dann ein Erzeugendensystem des $\mathbb{Z}$-Moduls $\mathbb{Z}^{n\times 1}$, wenn $A \in \mathrm{GL}_n(\mathbb{Z})$.

Bemerkung 6.1.7:

Sei R ein Ring.

(1) R kann als R-Modul aufgefasst werden, durch $R \times R \to R,\ (r,s) \mapsto rs$.
Beweis: Axiome von R direkt übertragen.
Diesen Modul bezeichnen wir als den **regulären R-Modul** ${}_R R$ (${}_R$ links wegen *Links*modul).
Seine Teilmoduln heißen auch **Linksideale**. Dazu später noch mehr.

(2) Ist M ein R-Modul und $m \in M$, dann gibt es genau einen R-Modulhomomorphismus

$$\varphi_m : {}_R R \to M,\ 1 \mapsto m \quad \Rightarrow r \mapsto rm \text{ wegen Linearität, da 1 ein EZS von } {}_R R \text{ ist.}$$

(3) Sind M und N zwei R-Moduln, so ist auch die **direkte Summe** $M \oplus N$ durch die R-Operation

$$r \cdot (m,n) = (rm, rn) \quad \text{für } m \in M,\ n \in N$$

ein R-Modul.

(4) Ist A eine beliebige Menge, so ist $R^A := \{f : A \to R\}$ ein R-Modul mit werteweiser Addition und Multiplikation. Im Fall $A = \underline{n}$ schreiben wir R^n statt $R^{\underline{n}}$.

Beweis zu 6.1.7:

(2) φ_m ist offensichtlich wohldefiniert und linear.
Sei ψ ein weiterer Modulhomomorphismus mit dieser Eigenschaft. Dann gilt:
$\psi(r) = \psi(r \cdot 1) = r\psi(1) = rm = \varphi_m(r)$, also muss $\psi = \varphi$. □

(3) Seien $r,s \in R,\ m_1, m_2 \in M,\ n_1, n_2 \in N$.

- $r\big((m_1,n_1)+(m_2,n_2)\big) = r(m_1+m_2,\ n_1+n_2) = \big(r(m_1+m_2),\ r(n_1+n_2)\big) = (rm_1+rm_2,\ rn_1+rn_2) = (rm_1,rn_1)+(rm_2,rn_2) = r(m_1,n_1)+r(m_2,n_2)$
- Andere Distributivgesetze analog, folgt alles aus den Modulaxiomen, die für M und N gelten.
- $1_R(m_1,n_1) = (1m_1,\ 1n_1) = (m_1,n_1)$

□

(4) Seien $r,s \in R,\ f,g : A \to R$. Sei $x \in A$ beliebig.

- $(r(f+g))(x) = r(f+g)(x) = rf(x) + rg(x) = (rf)(x) + (rg)(x) \Rightarrow r(f+g) = rf + rg$
- $((r+s)f)(x) = (r+s)f(x) = rf(x) + sf(x) \Rightarrow (r+s)f = rf + sf$
- $((rs)f)(x) = rsf(x) = r(sf(x)) \Rightarrow (rs)f = r(sf)$
- $(1_R f)(x) = 1_R f(x) = f(x)$

per Definition der werteweisen Verknüpfungen und Distributivgesetze in R. □

Bemerkung 6.1.8: Der freie Modul

Sei A eine Menge und $\forall a \in A$ sei $e_a \in R^A$ die **charakteristische Funktion** von $\{a\}$ definiert durch

$$e_a(b) = \begin{cases} 0_R & b \neq a \\ 1_R & b = a \end{cases} \quad \forall b \in A$$

Dann ist der von e_a für ein $a \in A$ erzeuge R-Teilmodul von R^A gegeben durch

$$\mathrm{Fr}_R(A) := \langle e_a \mid a \in A \rangle_R = \big\{ f \in R^A \,\big|\, |\{a \in A \mid f(a) \neq 0_R\}| < \infty \big\} \leq R^A$$

$\mathrm{Fr}_R(A)$ heißt der **freie R-Modul auf A**. Ist $|A| < \infty$, so gilt $\mathrm{Fr}_R(A) = R^A$.

Satz 6.1.9: Modulbasis freier Moduln

Sei R ein Ring und A eine Menge.
Der Modul $\mathrm{Fr}_R(A) := \langle e_a \mid a \in A \rangle_R \leq R^A$ hat folgende Eigenschaft: Für jeden R-Modul M und jede Abbildung $\psi : A \to M$ gibt es *genau* einen R-Modulhomomorphismus

$$\widetilde{\psi} : \mathrm{Fr}_R(A) \to M,\ \widetilde{\psi}(e_a) = \psi(a)\ \forall a \in A \text{ (kurz: } \widetilde{\psi} \circ e = \psi)$$

Moduln, die isomorph zu $\mathrm{Fr}_R(A)$ sind, heißen **frei** auf dem Erzeugendensystem (EZS), welches $(e_a)_{a \in A}$ vermöge $\widetilde{\psi}$ entspricht. Ein freies EZS heißt auch **R-Modulbasis**.

Beweis zu 6.1.9:
Jedes Element aus $\mathrm{Fr}_R(A)$ hat eine **eindeutige** Darstellung als $\sum_{a \in A} r_a e_a$ mit $r_a \in R$, $r_a = 0$ für alle bis auf endlich viele $a \in A$. Daher ist

$$\begin{aligned} \widetilde{\psi} : \mathrm{Fr}_R(A) &\longrightarrow M \\ \sum_{a \in A} r_a e_a &\longmapsto \sum_{a \in A} r_a \psi(a) \end{aligned}$$

eine wohldefinierte Abbildung, von der man leicht zeigt, dass sie die Bedingung $\widetilde{\psi}(e_a) = \psi(a)\ \forall a \in A$ per Konstruktion erfüllt, und ist somit auch der einzige R-Modulhomomorphismus mit dieser Eigenschaft. □

Beispiel 6.1.10: Freie Moduln

- ${}_R R$ ist frei auf $\{1\}$ (${}_R R \cong R^1$)
- Der Spaltenmodul $R^{n \times 1}$ ist frei auf den Einheitsspalten $(e_1, e_2, \ldots, e_n)$

6.2 Homomorphiesatz & Chinesischer Restsatz

6.2.a Homomorphiesatz für Moduln

Auch analog zu VRen: Wir haben nämlich dafür keinen Körper gebraucht.

Bemerkung 6.2.1: Faktormoduln

Sei R ein Ring und M ein R-Modul mit $U \leq M$.

(1) Für $m \in M$ heißt $m + U := \{m + u \mid u \in U\}$ die **Restklasse** von m nach U.
Man schreibt manchmal auch kurz $\overline{m}$, wenn der Teilmodul klar ist.
Die Menge $M/U := \{m + U \mid m \in M\}$ aller Restklassen von U in M bilden den **Faktormodul** von M nach U vermöge der folgenden Verknüpfungen:

$$\begin{aligned} + : M/U \times M/U &\longrightarrow M/U \\ (m_1 + U,\ m_2 + U) &\longmapsto (m_1 + m_2) + U \end{aligned}$$

$$\begin{aligned} \cdot : R \times M/U &\longrightarrow M/U \\ (r,\ m + U) &\longmapsto rm + U \end{aligned}$$

(2) Der **natürliche Epimorphismus**

$$\begin{aligned} \nu := \nu_U : M &\longrightarrow M/U \\ m &\longmapsto m + U \end{aligned}$$

ist ein R-Modulepimorphismus, und $\mathrm{Kern}(\nu_U) = U$.

Beweis zu 6.2.1:

(1) Wir müssen zeigen, dass $+$ und $\cdot$ wohldefiniert sind.
Seien $m_1, m_2, n_1, n_2 \in M$, $r \in R$ mit $m_1 + U = n_1 + U$ und $m_2 + U = n_2 + U$,
d.h. $m_1 - n_1 =: u_1 \in U$ und $m_2 - n_2 =: u_2 \in U$.
$\Rightarrow m_1 + m_2 - (n_1 + n_2) = u_1 + u_2 \in U$ und $rm_1 - rn_1 = ru_1 \in U$.
$\Rightarrow (m_1 + m_2) + U = (n_1 + n_2) + U$ und $rm_1 + U = rn_1 + U$.
Die Modulaxiome ergeben sich aus den Körperaxiomen von R; $U = 0 + U$ ist das Nullelement von M/U.

(2) Dies folgt direkt aus der Definition des Produktes und der Addition von Restklassen. Siehe auch LA1. □

Satz 6.2.2: Homomorphiesatz für R-Moduln

Sei $\varphi : M \to N$ ein R-Modulhomomorphismus. Dann faktorisiert φ als $\varphi = \widetilde{\varphi} \circ \nu_{\operatorname{Kern}\varphi}$ über $M/\operatorname{Kern}\varphi$ mit dem R-Modulepimorphismus $\nu_{\operatorname{Kern}\varphi}$ und dem R-Modulmonomorphismus

$$\begin{aligned} \widetilde{\varphi}\colon M/\operatorname{Kern}\varphi &\longrightarrow N \\ m + \operatorname{Kern}\varphi &\longmapsto \varphi(m) \end{aligned}$$

Beweis zu 6.2.2:
Analog Homomorphiesatz für VRe:
Es ist $M/\operatorname{Kern}\varphi = M/\sim_\varphi$, wobei $\sim_\varphi$ die Bildgleichheitsäquivalenzrelation von φ ist. Außerdem, für $\nu := \nu_{\operatorname{Kern}\varphi}$, ist $\sim_\varphi = \sim_\nu$, denn für $m, n \in M$ gilt: $\varphi(m) = \varphi(n) \Leftrightarrow m - n \in \operatorname{Kern}\varphi = \operatorname{Kern}\nu \Leftrightarrow \nu(m) = \nu(n)$.
Klar ist damit also, dass $\widetilde{\varphi}$ ein wohldefinierter Monomorphismus ist.
Und es gilt für $m \in M$ per Def., dass $\widetilde{\varphi}(\nu(m)) = \widetilde{\varphi}\left(m + \operatorname{Kern}\varphi\right) = \varphi(m)$. □

Bemerkung 6.2.3:

Ist M ein endlich erzeugter R-Modul, so gibt es ein $n \in \mathbb{N}$ und einen R-Modulepimorphismus

$$\varepsilon : R^{n\times 1} \to M$$

Insbesondere ist $M = R^{n\times 1}/\operatorname{Kern}\varepsilon$.

Beweis zu 6.2.3:
Sei $\psi : \underline{n} \to M$ gegeben, sodass $\operatorname{Bild}\psi$ ein EZS von M ist. Der nach Satz 6.1.9 eindeutig bestimmte R-Modulhomomorphismus $\varepsilon := \widetilde{\psi} : R^{n\times 1} \to M$ mit $\varepsilon \circ e = \psi$ ist dann ein Epimorphismus (wobei $e := (e_1, \ldots, e_n)$ hier die Standardbasis aus Einheitsvektoren in $R^{n\times 1}$ ist), da das ganze EZS getroffen wird. □

Definition 6.2.4: Zyklische Moduln

R-Moduln, die von einem Element erzeugt werden, heißen **zyklisch**.

Beispiel 6.2.5: Zyklische Moduln

(1) Jede zyklische Abelsche Gruppe ist von der Form $\mathbb{Z}/K$, wobei K ein Linksideal von $\mathbb{Z}$ ist.

(2) Jede Abelsche Gruppe, die von n Elementen erzeugt wird, ist von der Form $\mathbb{Z}^n/K$, wobei K ein $\mathbb{Z}$-Teilmodul von $\mathbb{Z}^n = \operatorname{Fr}_{\mathbb{Z}}(\underline{n})$ ist.

(3) Sei K ein Körper und $\mathcal{V}$ ein endlich erzeugter K-VR mit $\varphi \in \operatorname{End}(\mathcal{V})$, sodass das Minimalpolynom und charakteristische Polynom von φ übereinstimmen ($\mu_\varphi = \chi_\varphi =: p(x) \in K[x]$), so ist $\mathcal{V}$ als $K[x]$-Modul zyklisch, und es gilt $\mathcal{V} \cong_{K[x]} K[x]/\langle p(x)\rangle$.

6.2.b Ideale

Definition 6.2.6: IDEAL

Sei R ein Ring.

(1) $I \subseteq R$ heißt (zweiseitiges) **Ideal** von R, in Zeichen $I \trianglelefteq R$, falls
- $I \neq \emptyset$
- Für $a, b \in I,\ r, s \in R$ gilt: $ra + bs \in I$ (Achtung Reihenfolge!)

(2) Sind $I_1, I_2 \trianglelefteq R$, so heißt das kleinste Ideal, welches I_1 und I_2 enthält, die **Summe** von I_1 und I_2; in Zeichen: $I_1 + I_2$.

Beispiel 6.2.7: IDEALE

(1) Für $R = \mathbb{Z}$ ist $3\mathbb{Z} = \langle 3 \rangle = \{3z \mid z \in \mathbb{Z}\}$ ein Ideal: $\langle 3 \rangle \lhd \mathbb{Z}$

(2) Ist K ein Körper, $a \in K$, dann ist

$$\{p(x) \in K[x] \mid p(a) = 0\} = \langle x - a \rangle = \{q(x)(x-a) \mid q(x) \in K[x]\} \lhd K[x]$$

(3) Ist R ein kommutativer Ring, so sind die Ideale genau die R-Teilmoduln von ${}_R R$, sprich die Linksideale.

(4) Der Durchschnitt einer Menge von Idealen ist wieder ein Ideal.

(5) Ist $M \subseteq R$, so heißt $\langle M \rangle := \bigcap_{M \subseteq I \trianglelefteq R} I$ das von M erzeugte Ideal in R.
Ist $M = \{a_1, \ldots, a_n\}$, so schreibt man $\langle a_1, \ldots, a_n \rangle$.

(6) Ist R ein kommutativer Ring, so heißt $\langle a \rangle = \{ra \mid r \in R\}$ das von a erzeugte **Hauptideal**.

(7) Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann ist $\operatorname{Kern} \varphi := \{r \in R \mid \varphi(r) = 0\}$ ein Ideal in R.

Übung 6.2.Ü1:

(1) Das von $M \subseteq R$ erzeugte Ideal ist

$$\langle M \rangle = \left\{ \sum_{i=1}^{n} a_i m_i b_i \;\middle|\; n \in \mathbb{N}_0,\ a_i, b_i \in R,\ m_i \in M \right\}$$

(2) Die Ideale von $\mathbb{Z}^{n \times n}$ sind genau die Teilmengen $a\mathbb{Z}^{n \times n}$ mit $a \in \mathbb{Z}$.

Beweis:

(1) Nenne die rechte Seite $\mathscr{LK}(M)$.
- $M \subseteq \mathscr{LK}(M)$ durch $n = 1,\ a_1 = 1_R,\ b_1 = 1_R$ und jedes $m \in M$ als m_1.
- $\mathscr{LK}(M) \trianglelefteq R$ durch die Definition als Summen und Ringaxiome.

Somit ist $\mathscr{LK}(M)$ ein Ideal, das M enthält.
- Ist $I \trianglelefteq R$ mit $M \subseteq I$, so ist per Definition des Ideals auch $\mathscr{LK}(M) \subseteq I$.

Damit ist $\mathscr{LK}(M)$ im Schnitt aller Ideale, die M enthalten, also, da $\mathscr{LK}(M)$ selbst ein Ideal ist, gleich dem Erzeugnis. □

(2) *Übung.*

□

Satz 6.2.8:

Sei R ein Ring und $I \trianglelefteq R$ ein Ideal.
Dann ist der **Restklassenring** $R/I = \{r+I \mid r \in R\}$ ein Ring mit den vertreterweisen Verknüpfungen

$$\begin{aligned} +: R/I \times R/I &\longrightarrow R/I \\ (r+I,\ s+I) &\longmapsto (r+s)+I \end{aligned}$$

$$\begin{aligned} \cdot: R/I \times R/I &\longrightarrow R/I \\ (r+I,\ s+I) &\longmapsto rs+I \end{aligned}$$

und der **natürliche Epimorphismus**

$$\begin{aligned} \nu = \nu_I : R &\longrightarrow R/I \\ r &\longmapsto r+I \end{aligned}$$

ist ein Ringepimorphismus mit $I = \operatorname{Kern} \nu_I$ (auch „natürlicher Ringepimorphismus“).
Ist R kommutativ, so auch R/I.

Beweis zu 6.2.8:
Da $I \leq R$ ein R-Teilmodul ist, ist R/I wieder ein R-Modul und wir brauchen uns nur noch um die Wohldefiniertheit der Multiplikation zu kümmern.
Seien also $r+I = r'+I,\ s+I = s'+I$ für $r, r', s, s' \in R$. Dann existieren $a, b \in I$ mit $r' = r+a,\ s' = s+b$, und wir erhalten $r's' - rs = (r+a)-(s+b)-rs = rs+rb+as+ab-rs \in I$, d.h. $(r+I)(s+I)$ ist wohldefiniert. Das Assoziativ- und die Distributivgesetze übertragen sich von R.
Dass ν ein Epimorphismus ist, ist gerade die Definition der Multiplikation von Restklassen.
Bei Körpern ist das trivial – die einzigen Ideale sind der Körper selbst und $\{0\}$. □

Korollar 6.2.9: Homomorphiesatz für Ringe

Seien R, S Ringe und $\varphi : R \to S$ ein Ringhomomorphismus.
Dann ist $\operatorname{Kern} \varphi$ ein Ideal in R und $\operatorname{Bild} \varphi$ ein Teilring von S, und

$$\begin{aligned} \overline{\varphi}: R/\operatorname{Kern}\varphi &\longrightarrow \operatorname{Bild}\varphi \\ r+\operatorname{Kern}\varphi &\longmapsto \varphi(r) \end{aligned}$$

ist ein wohldefinierter Ringisomorphismus.

Beweis zu 6.2.9:
Analog anderer Homomorphiesätze. □

Als „*abstract nonsense*“ gilt der Homomorphiesatz in fast allen abstrakten Strukturen.

Übung 1.3.i:

Sei R ein Ring, M_1, M_2 seien R-Moduln, $T_1 \leq M_1,\ T_2 \leq M_2$.
Sei $\varphi : M_1 \to M_2$ ein R-Modulhomomorphismus.
Dann ist $\overline{\varphi} : M_1/T_1 \to M_2/T_2,\ \overline{m} \mapsto \overline{\varphi(m)}$ genau dann ein wohldefinierter R-Modulhomomorphismus, wenn $\varphi(T_1) \subseteq T_2$.

Beweis:
„⇒“: Sei $t_1 \in T_1$ beliebig.

$$\Rightarrow \overline{\varphi(t_1)} = \overline{\varphi}\left(\overline{t_1}\right) = \overline{\varphi}\left(\overline{0}\right) = \overline{\varphi(0)} = \overline{0}$$
$$\Rightarrow \varphi(t_1) - 0 \in T_2 \Rightarrow \varphi(t_1) \in T_2$$
$$\Rightarrow \varphi(T_1) \subseteq T_2.$$

„⇐“: Sei $\varphi(T_1) \subseteq T_2$.

Zunächst: $\overline{\varphi}$ erfüllt die Eigenschaften eines R-Modulhom., da für $r \in R,\ m_1, n_1 \in M_1$ gilt:

$$\begin{aligned}\overline{\varphi}(r\overline{m_1} + \overline{n_1}) &= \overline{\varphi}\left(\overline{rm_1 + n_1}\right) = \overline{\varphi(rm_1 + n_1)} = \overline{r\varphi(m_1) + \varphi(n_1)} \\ &= r\overline{\varphi(m_1)} + \overline{\varphi(n_1)} = r\overline{\varphi}(\overline{m_1}) + \overline{\varphi}(\overline{n_1})\end{aligned}$$

Nun ist noch Wohldefiniertheit zu zeigen. Seien dazu $m_1, n_1 \in M_1$ mit $\overline{m_1} = \overline{n_1}$ in M_1/T_1. Betrachte:

$$\begin{aligned}&\overline{\varphi}(\overline{m_1}) \overset{!}{=} \overline{\varphi}(\overline{n_1}) \\ \Leftrightarrow\ &\overline{\varphi}(\overline{m_1}) - \overline{\varphi}(\overline{n_1}) = \overline{0} \\ \Leftrightarrow\ &\overline{\varphi}(\overline{m_1} - \overline{n_1}) = \overline{0} \\ \Leftrightarrow\ &\overline{\varphi}\left(\overline{0}\right) = \overline{0} \\ \Leftrightarrow\ &\overline{\varphi(0)} = \overline{0} \\ \Leftrightarrow\ &\overline{0} = \overline{0}\end{aligned}$$

was offensichtlich gilt. Also ist $\overline{\varphi}$ wohldefiniert.

□

Bemerkung 6.2.10: Annihilator

Sei M ein R-Modul. Dann ist der **Annihilator** von M

$$\mathrm{Ann}_R(M) := \{r \in R \mid rm = 0\ \forall m \in M\}$$

ein Ideal von R, der Kern des Ringhomomorphismus

$$\begin{aligned}R &\longrightarrow \mathrm{End}_{\mathbb{Z}}(M) \\ r &\longmapsto (m \mapsto rm)\end{aligned}$$

Weiter ist M ein $R/\mathrm{Ann}_R(M)$-Modul.

Bemerkung 6.2.11:

Seien R, S Ringe.
$R \times S$-Moduln sind direkte Summen von R-Moduln und S-Moduln.

Beweis zu 6.2.11:

Sei M ein R-Modul und N ein S-Modul.
Dann ist $M \oplus N$ ein $R \times S$-Modul durch

$$(r,s)\cdot(m,n) := (rm, sn)\ \forall r \in R,\ s \in S,\ m \in M,\ n \in N$$

Sei umgekehrt L ein $R \times S$-Modul. Dann sind

$$\begin{aligned}M &:= (R \times \{0\})L = (1,0)L, \\ N &:= (\{0\} \times S)L = (0,1)L\end{aligned}$$

Teilmoduln von L, sodass $M \oplus N \cong L$.
Es ist $\mathrm{Ann}_{R\times S}(M) \supseteq \underbrace{\{0\} \times S}_{\trianglelefteq R\times S}$ und $\mathrm{Ann}_{R\times S}(N) \supseteq R \times \{0\}$.

Also ist M ein $(R \times S)/\mathrm{Ann}_{R\times S}(M)$-Modul und ein $\underbrace{(R \times S)/(\{0\} \times S)}_{\cong R}$-Modul.

Also ist M ein R-Modul und N analog dazu ein S-Modul. □

Definition 6.2.12: R-Algebra

Sei R ein kommutativer Ring mit Eins.
Eine **R-Algebra** A ist ein Ring mit Eins, der gleichzeitig ein R-Modul ist, sodass die Multiplikation R-bilinear ist, d.h. $(ra)b = r(ab) = a(rb)$ für $r \in R$, $a, b \in A$.

Ein **R-Algebrenhomomorphismus** ist ein Ringhomomorphismus, der gleichzeitig R-Modulhomomorphismus ist.

Übung 6.2.Ü2:

Sei A eine R-Algebra. Dann ist $\alpha : R \to A,\ r \mapsto r1_A$ ein R-Algebrenhomomorphismus.

Beweis:
Für $r, s, t \in R$ gilt:

$$\alpha(r+s) = (r+s)1_A = r1_A + s1_A = \alpha(r) + \alpha(s)$$
$$\alpha(rs) = (rs)1_A = r1_A s1_A = \alpha(r)\alpha(s)$$
$$\alpha(rs+t) = (rs+t)1_A = rs1_A + t1_A = r\alpha(s) + \alpha(t)$$

Damit ist α Ringhomomorphismus und R-Algebrenhom. ($R = {}_R R$ ist trivialerweise auch eine R-Algebra.) □

Beispiel 6.2.13: Algebren

(1) $\mathbb{C}[x]$ ist eine $\mathbb{C}$-Algebra.
Sei $\bar{\cdot} : \mathbb{C} \to \mathbb{C},\ a + b\mathrm{i} \mapsto a - b\mathrm{i}$ $(a, b \in \mathbb{R})$ (Konjugation). Dann ist

$$\begin{aligned} \mathbb{C}[x] &\longrightarrow \mathbb{C}[x] \\ \sum_{k=0}^{n} a_k x^k &\longmapsto \sum_{k=0}^{n} \overline{a_k} x^k \end{aligned}$$

ein Ringhomomorphismus, der aber kein $\mathbb{C}$-Algebrenhomomorphismus ist. ($\overline{\mathrm{i}x} = -\mathrm{i}x$ – nicht $\mathbb{C}$-linear)
Allerdings ist $\mathbb{C}[x] \to \mathbb{C}[x]$ ein $\mathbb{R}$-Algebrenhomomorphismus.

(2) Ist A eine R-Algebra und $I \trianglelefteq A$, so ist A/I eine R-Algebra und $\nu_I : A \to A/I$ ist ein R-Algebrenhomomorphismus.

(3) Jeder Ring ist eine $\mathbb{Z}$-Algebra vermöge $z \cdot r := \begin{cases} \underbrace{r + \cdots + r}_{z\text{-mal}} & z > 0 \\ -(\underbrace{r + \cdots + r}_{z\text{-mal}}) & z < 0 \\ 0_R & z = 0 \end{cases}$

6.2.c Euklidische Ringe

Definition 6.2.14: Spezielle Ringe

Sei R ein kommutativer Ring mit Eins.

(1) R heißt **Integritätsbereich** (IB) oder **nullteilerfrei**, falls $1 \neq 0$ in R gilt und $\forall a,b \in R : ab = 0 \Rightarrow a = 0 \vee b = 0$.

(2) R heißt **Hauptidealbereich** (HIB), falls R ein Integritätsbereich ist und jedes Ideal in R ein Hauptideal ist, d.h. $\forall I \trianglelefteq R : \exists a \in R : I = \langle a \rangle$.

(3) R heißt **Euklidischer Ring** oder **Euklidischer Bereich**, falls eine Abbildung $\nu : R \to \mathbb{Z}_{\geq 0}$ mit folgenden Eigenschaften existiert:

(a) $\forall r \in R : \nu(r) = 0 \Leftrightarrow r = 0$

(b) $\forall r_1, r_2 \in R : \nu(r_1 r_2) = \nu(r_1)\nu(r_2)$

(c) $\forall a \in R,\ b \in R \setminus \{0\} : \exists q, r \in R : a = qb + r$ mit $\nu(r) < \nu(b)$

Beispiel 6.2.15:

(1) Jeder Teilring eines Körpers ist ein IB.

(2) Offenbar ist jeder Körper ein Euklidischer Ring mit $\nu(0) := 0,\ \nu(a) := 1\ \forall a \in K^* = K \setminus \{0\}$

(3) $\mathbb{Z}$ ist Euklidischer Bereich mit $\nu(a) := |a|\ \forall a \in \mathbb{Z}$ und der Division mit Rest für ganze Zahlen.

(4) Sei K ein Körper. Dann ist $K[x]$ ein Euklidischer Bereich mit $\nu(p) := 2^{\mathrm{Grad}(p)}$ für $p \neq 0$ und Polynomdivision. (2^{Grad} weil Gradformel $\mathrm{Grad}(pq) = \mathrm{Grad}\, p + \mathrm{Grad}\, q$)

(5) Der Ring $\mathbb{Z}[x] := \left\{ p(x) \in \mathbb{Q}[x] \,\middle|\, p(x) = \sum_{i=0}^{n} a_i x^i,\ a_i \in \mathbb{Z}\ \forall i \in \{0\} \cup \underline{n} \right\}$ ist ein Integritätsbereich, da er ein Teilring des Körpers $\mathbb{Q}(x) = \left\{ \frac{p(x)}{q(x)} \,\middle|\, p(x) \in \mathbb{Q}[x],\ q(x) \in \mathbb{Q}[x] \setminus \{0\} \right\}$ ist.
Jedoch ist $\mathbb{Z}[x]$ kein HIB, da $\langle 2, x \rangle$ kein Hauptideal ist.

Beweis:
Es ist $\langle 2,x \rangle = \{a_1 \cdot 2 \cdot b_1 + a_2 \cdot x \cdot b_2 \,|\, a_1, a_2, b_1, b_2 \in \mathbb{Z}[x]\} = \left\{ 2z_0 + z_1 x + z_2 x^2 + \ldots \,\middle|\, z_i \in \mathbb{Z} \right\}$.
Gäbe es $p \in \langle 2,x \rangle$ mit $\langle 2,x \rangle = \langle p \rangle$, so müsste es ein $q \in \mathbb{Z}[x]$ geben, sodass $p \cdot q = 2$, und $r \in \mathbb{Z}[x]$ mit $p \cdot r = x$. Nach der Gradformel muss dann gelten: $\mathrm{Grad}\, p + \mathrm{Grad}\, q = \mathrm{Grad}\, 2 = 0$ $\Rightarrow \mathrm{Grad}\, p = \mathrm{Grad}\, q = 0 \Rightarrow p \in \mathbb{Z}$. Damit $pr = x$, muss $p = \pm 1$ (kein anderer Teiler in $\mathbb{Z}$).
Nach obiger Ausformulierung des Inhalts von $\langle 2,x \rangle$ ist aber $\pm 1 \notin \langle 2,x \rangle$, da 2 kein Teiler von 1 oder -1 ist. Somit kann ein solches Polynom nicht in diesem Ideal existieren. □

Satz 6.2.16: Quotientenkörper

Sei R ein Integritätsbereich.
Dann gibt es einen Körper K, sodass $R \subseteq K$ Teilring von K ist und $K = \left\{ ab^{-1} \,\middle|\, a \in R,\ b \in R \setminus \{0\} \right\}$.
K ist bis auf Ring-Isomorphie *eindeutig* durch R festgelegt, man nennt diesen auch den **Quotientenkörper** oder *field of fractions*, und schreibt $K =: \mathrm{Quot}(R) =: \mathrm{Frac}(R)$.
Man schreibt dann oft: $ab^{-1} = b^{-1}a = {}^{a}/_{b} = \frac{a}{b}$ für $ab^{-1} \in \mathrm{Quot}(R)$

Beweis zu 6.2.16:

Existenz:
Definiere $\widetilde{K} := R \times (R \setminus \{0\}) = \left\{ (a,b) \,\middle|\, a \in R,\ b \in R \setminus \{0\} \right\}$. und eine Äquivalenzrelation $\approx$ auf $\widetilde{K}$ durch:

$$(a,b) \approx (c,d) :\Leftrightarrow ad = bc$$

Setze die Menge der Äquivalenzklassen auf $K := \widetilde{K}/\!\approx$. Definiere nun $\frac{a}{b} := [(a,b)]_{\approx}$ (ÄK von (a,b)).
Addition und Multiplikation werden folgendermaßen definiert:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Die Addition ist wohldefiniert, denn: Da $b,d,bd \neq 0$, sind die Ausdrücke auf beiden Seiten wohldefiniert. Zum Beweis der Vertreterunabhängigkeit seien $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'} \Leftrightarrow ab' = a'b$ und $cd' = c'd$.
z.z. $\frac{ad+bc}{bd} \overset{!}{=} \frac{a'd'+b'c'}{b'd'}$
Zeige Analog die Vertreterunabhängigkeit der Multiplikation, und prüfe die Körperaxiome.

Eindeutigkeit: Sei K' ein weiterer Körper mit $R \subseteq K'$. Dann ist die Abbildung $\varepsilon : K \to K'$, $\frac{a}{b} \mapsto ab^{-1}$ ein wohldefinierter Homomorphismus. Daraus folgt sofort: ε ist ein Monomorphismus, also $K \cong \operatorname{Bild}\varepsilon$. □

Übung 6.2.Ü3:

Der Ring $\mathbb{Z}[\mathrm{i}] := \mathbb{Z}[x]/\langle x^2+1\rangle$ mit $\mathrm{i} := \overline{x}$ ist Euklidischer Bereich mit $\nu(a+b\mathrm{i}) := a^2+b^2$ für $a,b \in \mathbb{Z}$.

Beweis:

- $\nu(a+b\mathrm{i}) = a^2+b^2 = 0 \Leftrightarrow a = b = 0 \Leftrightarrow a+b\mathrm{i} = 0$
- $\nu((a+b\mathrm{i})(c+d\mathrm{i})) = (ac-bd)^2(ad-bc)^2 = \left(a^2+b^2\right)\left(c^2+d^2\right) = \nu(a+b\mathrm{i})\nu(c+d\mathrm{i})$
- Seien $a := a_1+a_2\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$, $b := b_1+b_2\mathrm{i} \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$.

$$\underset{\in \operatorname{Quot}(\mathbb{Z}[\mathrm{i}])}{\frac{a}{b}} = \frac{a_1+a_2\mathrm{i}}{b_1+b2\mathrm{i}} = \frac{(a_1+a_2\mathrm{i})(b_1-b_2\mathrm{i})}{(b_1+b_2\mathrm{i})(b_1-b_2\mathrm{i})} = \frac{\overbrace{(a_1b_1+a_2b_2)}^{=:x} - \overbrace{(a_1b_2-a_2b_1)}^{=:x_2}\mathrm{i}}{\nu(b)} =: (*)$$

Mit erweitertem Euklidischen Algorithmus in $\mathbb{Z}$:

$$x_1 = \frac{1}{2}\nu(b)\cdot q_1 + r_1,\ r_1 < \frac{1}{2}\nu(b)$$
$$x_2 = \frac{1}{2}\nu(b)\cdot q_2 + r_2,\ r_2 < \frac{1}{2}\nu(b)$$

$$(*) = \frac{\left(\frac{1}{2}\nu(b)q_1+r_1\right) - \left(\frac{1}{2}\nu(b)q_2+r_2\right)\mathrm{i}}{\nu(b)} = \frac{\frac{1}{2}\nu(b)(q_1-q_2\mathrm{i}) + (r_1-r_2\mathrm{i})}{\nu(b)}$$

$$= \frac{1}{2}\underbrace{(q_1+q_2\mathrm{i})}_{=:q\in\mathbb{Z}[\mathrm{i}]} + \frac{\overbrace{r_1-r_2\mathrm{i}}^{=:r}}{\nu(b)} = \frac{1}{2}q + \frac{r}{\nu(b)}$$

$$\Leftrightarrow a = \frac{1}{2}qb + \frac{rb}{\nu(b)} = \frac{1}{2}qb + \frac{r}{b_1-b_2\mathrm{i}}$$

$$\begin{aligned}\nu\left(\frac{r}{b_1-b_2\mathrm{i}}\right) &= \nu(r)\nu\left((b_1-b_2\mathrm{i})^{-1}\right) = \nu(r)\nu(b_1-b_2\mathrm{i})^{-1} \\ &= \left(r_1^2+r_2^2\right)\nu(b_1-b_2\mathrm{i})^{-1} < \left(\left(\tfrac{1}{2}\nu(b)\right)^2 + \left(\tfrac{1}{2}\nu(b)\right)^2\right)\cdot\nu(b_1-b_2\mathrm{i})^{-1} \\ &= \frac{1}{2}\nu(b)^2\cdot\nu(b)^{-1} = \frac{1}{2}\nu(b) < \nu(b)\end{aligned}$$

□

Man hat für die Elemente in $\operatorname{Quot}R$ allerdings üblicherweise keine Normalform (d.h. die Elemente sind nicht eindeutig durch ab^{-1} dargestellt.

Beispiel 6.2.17:

(1) $\operatorname{Quot}\mathbb{Z} = \mathbb{Q}$. Hier lernt man eine Normalform in der Schule kennen (gekürzte Brüche).
(2) Sei K ein Körper. Dann heißt $K(x) := \operatorname{Quot}(K[x])$ der **Körper der rationalen Funktionen in einer Variablen**.
(3) Sei K ein Körper. Dann heißt $K(x_1,\ldots,x_n) = \operatorname{Quot}(K[x_1,\ldots,x_n])$ der **Körper der rationalen Funktionen** über K.

Definition 6.2.18: Teilbarkeit

Sei R ein IB und $a, b \in R$.

(1) $d \in R$ teilt a genau dann, wenn $q \in R$ existiert mit $a = qd$, also genau dann, wenn $a \in \langle d \rangle$. Bezeichnung: $d \mid a$

(2) $a \in R \setminus (R^* \cup \{0\})$ heißt **prim**, falls: $\forall b_1, b_2 \in R : a \mid (b_1 b_2) \Rightarrow a \mid b_1 \vee a \mid b_2$

(3) Eine Zahl $d \in R$ heißt **größter gemeinsamer Teiler** von a und b ($d =: \mathrm{ggT}(a,b)$) genau dann, wenn: $d \mid a, b$ und $\forall c \in R$ mit $c \mid a, b$ folgt: $c \mid d$.

(4) Eine Zahl $v \in R$ heißt **kleinstes gemeinsames Vielfaches** von a und b ($v =: \mathrm{kgV}(a,b)$), wenn: $a, b \mid v$ und $\forall w \in R$ mit $a, b \mid w$ folgt: $v \mid w$.

Bemerkung 6.2.19:

Sei R ein IB., insbesondere kommutativ, und $a, b \in R$.
Dann gilt: $a \mid b \Leftrightarrow b \in \langle a \rangle \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$

Satz 6.2.20:

Sei R ein HIB, $a, b \in R$. Dann existieren $\mathrm{ggT}(a,b) \in R$ und $\mathrm{kgV}(a,b) \in R$ und sind eindeutig bestimmt bis auf Multiplikation mit Einheiten in R.

Übung 3.4:

Sei R ein HIB, $a, b \in R \setminus \{0\}$. Dann gilt:

(1) $\langle \mathrm{ggT}(a,b) \rangle = \langle a \rangle + \langle b \rangle$

(2) $\langle \mathrm{kgV}(a,b) \rangle = \langle a \rangle \cap \langle b \rangle$

(3) $\langle a \rangle \langle b \rangle = \langle ab \rangle$

Beweis zu 6.2.20:

(1) Wir betrachten das Erzeugnis $\langle a \rangle + \langle b \rangle = \langle a, b \rangle \overset{R \text{ ist HIB}}{=} \langle d \rangle$ mit $d \in R$ geeignet.
Also $\langle a \rangle \subseteq \langle d \rangle$ und $\langle b \rangle \subseteq \langle d \rangle$.
$\Rightarrow d \mid a \wedge d \mid b$.
Ist umgekehrt $c \in R$ ein Teiler von a und b, so heißt dies, dass $a \in \langle c \rangle$ und $b \in \langle c \rangle$.
$\Rightarrow \langle d \rangle = \langle a \rangle + \langle b \rangle \subseteq \langle c \rangle$
$\Rightarrow c \mid d$
$\Rightarrow \langle a \rangle + \langle b \rangle = \langle \mathrm{ggT}(a,b) \rangle$.

(2) Da R ein HIB ist, sei $v \in R$ mit $\langle a \rangle \cap \langle b \rangle = \langle v \rangle$, d.h. $\forall w \in \langle v \rangle : w \in \langle a \rangle \wedge w \in \langle b \rangle$.
Insbesondere ist also $v \in \langle a \rangle$ und $v \in \langle b \rangle$, also $a, b \mid v$.
Da $w \in \langle a \rangle \wedge w \in \langle b \rangle \Leftrightarrow a, b \mid w$ für w wie oben, aber $w \in \langle v \rangle \Rightarrow v \mid w$, ist $v = \mathrm{kgV}(a,b)$ per Definition.

(3) $\forall n \in \mathbb{N},\ x, y \in R^n : \sum_{i=1}^{n} x_i a \cdot y_i b \in \langle ab \rangle \Rightarrow \langle a \rangle \langle b \rangle \subseteq \langle ab \rangle$
$ab \in \langle a \rangle \langle b \rangle \Rightarrow \langle ab \rangle \subseteq \langle a \rangle \langle b \rangle$
$\Rightarrow \langle a \rangle \langle b \rangle = \langle ab \rangle$

□

Bemerkung 6.2.21:

Sei R ein Euklidischer Ring mit Norm ν. Dann ist R ein HIB.

Beweis zu 6.2.21:

Wir zeigen zunächst, dass R nullteilerfrei ist.
Seien $a, b \in R$ mit $ab = 0$.
$\Rightarrow 0 = \nu(0) = \nu(ab) = \nu(a)\nu(b)$
$\Rightarrow \nu(a) = 0 \vee \nu(b) = 0 \Rightarrow a = 0 \vee b = 0$

Nun zeigen wir, dass jedes Ideal ein Hauptideal ist.
Sei $\langle 0 \rangle \neq I \trianglelefteq R$. Wähle ein $a \in I \setminus \{0\}$ mit $\nu(a) \in \mathbb{Z}_{\geq 0}$ minimal (dies ist möglich, da $\mathbb{Z}_{\geq 0}$ wohlgeordnet ist).
Behauptung: $I = \langle a \rangle$.
Ist nämlich $b \in I$, so dividiere b durch a mit Rest

$$b = aq + \underset{\in I}{r} \text{ mit } \nu(r) < \nu(a)$$

$\Rightarrow r = 0 \Rightarrow b = qa \Rightarrow b \in \langle a \rangle$ □

Übung 2.4:

Sei $n \in \mathbb{N}$, $m \in \mathbb{Z}$, $\overline{m} := m + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n \rangle$.

- $\overline{m}$ ist Einheit in $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow n, m$ teilerfremd
- $\overline{m}$ ist Nullteiler in $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow n, m$ nicht teilerfremd
- Ist $n = \prod_{i=1}^{N} p_i^{m_i}$ die Primfaktorzerlegung von n, so ist

$$\mathrm{Nil}\left(\mathbb{Z}/n\mathbb{Z}\right) := \mathrm{Nil}(n) := \left(\prod_{i=1}^{N} p_i\right)\mathbb{Z} = \left\{ \overline{r} \cdot \prod_{i=1}^{N} \overline{p_i} \;\middle|\; \overline{r} \in \mathbb{Z}/n\mathbb{Z} \right\}$$

die Menge aller nilpotenten Elemente in $\mathbb{Z}/n\mathbb{Z}$.

Übung 6.2.Ü4: Erweiterter Euklidischer Algorithmus

Sei R ein Euklidischer Ring mit Norm ν.
Dann gibt es in R einen **Euklidischen Algorithmus**, der bei Eingabe zweier Zahlen aus R den größten gemeinsamen Teiler und eine Bézout-Identität ausgibt:

Eingabe: $a, b \in R$ beliebig.

Algorithmus: (I) $n := 0$
Solange $b \neq 0$:
$n := n + 1$
Division mit Rest: $a = q_n b + r$
speichere q_n, r
$a := b$
$b := r$
Dann ist $a = \mathrm{ggT}(a, b)$.

(II) Setze nun (rekursiv) $A_1 := \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$, $A_k := \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \cdot A_{k-1}$ für $k \geq 2$.
Berechne $A_n = \prod_{i=1}^{n-1} \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} =: \begin{pmatrix} * & * \\ x & y \end{pmatrix}$.
Dann sind x, y so, dass $\mathrm{ggT}(a, b) = xa + yb$.

Beweis:

- Der Algorithmus beruht darauf, eine Division mit Rest zu haben, was in Euklidischen Ringen per Definition der Fall ist.

Sei in diesem Beweis $*_i$ die Variable $*$ im Iterationsschritt i.

- Per Definition gilt bei der Division in Euklidischen Ringen:

$$a = qb + r \text{ mit } \nu(b) > \nu(r)$$

Da in jedem Schritt b durch r ersetzt wird, ist die Folge $(\nu(b_n))_n$ streng monoton fallend in $\mathbb{Z}_{\geq 0}$ und somit wird in jedem Fall nach spätestens n Schritten die Abbruchbedingung $b = 0$ erreicht (da $\nu(b) = 0 \Rightarrow b = 0$).

- Dass (II) terminiert, ist dann klar, da n nach Ausführung von (I) eine eindeutige endliche Zahl in $\mathbb{Z}_{\geq 0}$ ist und dieser Schritt damit eine einfache Berechnung ist.
- Da $a_n = q_n a_{n-1} + a_{n-2}$, gilt: $\mathrm{ggT}(a_n, a_{n-1}) = \mathrm{ggT}(a_{n-1}, a_{n-2})$ für alle $n \geq 3$. Diese Kette endet also mit $\mathrm{ggT}(a,b) = \cdots = \mathrm{ggT}(0_R, a_n) = a_n$

  Der Algorithmus (I) berechnet also tatsächlich den ggT (eindeutig bis auf Multiplikation mit Einheiten aus $R^\times$).
- Für die A_k gilt:

  $$A_k \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} \text{ und damit } A_n \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \mathrm{ggT}(a,b) \\ 0 \end{pmatrix}$$

  was nach der Definition der Matrixmultiplikation genau die Bézout-Identität ist.

□

Es gilt (bis auf Einheiten):

$$\prod_{i=1}^{n} a_i \sim \mathrm{ggT}(a_1, \ldots, a_n)\,\mathrm{kgV}(a_1, \ldots, a_n)$$

6.2.d Der chinesische Restsatz

Seien alle Ringe in diesem Kapitel kommutativ mit Eins.

Satz 6.2.22: Chinesischer Restsatz

Sei R ein Ring und $I_1, \ldots, I_n$ paarweise teilerfremde Ideale in R, d.h. $I_i + I_j = R \ \forall i \neq j$. Dann gilt:

$$R \Big/ \bigcap_{i=1}^{n} I_i \longmapsto R/I_1 \times \cdots \times R/I_n$$
$$r + \bigcap_{i=1}^{n} I_i \longrightarrow (r + I_1, \ \ldots, \ r + I_n)$$

ist ein Isomorphismus.

Bei Anwendungen will man häufig das Inverse von diesem Isomorphismus konstruieren. Man nennt den Satz auch den **Hauptsatz über das Lösen von simultanen Kongruenzen**. Dies ist wie folgt zu verstehen: Für $I \trianglelefteq R$ schreibt man für Elemente $r, s \in R$ mit $r + I = s + I$ oft:

$$r \equiv s \mod I$$

Der obige Satz lautet dann: Für beliebige $r_1, \ldots, r_n \in R$: $\exists x \in R$ mit $x \equiv r_i \mod I_i \ \forall i \in \underline{n}$ und x ist eindeutig modulo $\bigcap_{i=1}^{n} I_i$.

Beweis zu 6.2.22:

Der Fall $n = 2$ ist einfach: Der offensichtliche Homomorphismus

$$\nu_{I_1} \times \nu_{I_2} : R \longrightarrow R/I_1 \times R/I_2$$
$$r \longmapsto (r + I_1, r + I_2)$$

hat als Kern $I_1 \cap I_2$, und ist wegen $I_1 + I_2 = R$ surjektiv ($1 = \underset{\in I_1}{a_1} + \underset{\in I_2}{a_2} \Rightarrow$

$$a_2 \mapsto (a_2 + I_1, \ a_2 + I_2) = (1 + I_1, \ 0 + I_2)$$
$$a_1 \mapsto (a_1 + I_1, \ a_1 + I_1) = (0 + I_1, \ 1 + I_2)$$

dann Linearkombinationen).

Die Behauptung folgt aus dem Homomorphiesatz für Ringe. Der allgemeine Beweis ist per Induktion. Der Induktionsschritt benutzt $n = 2$ und ist bei $n = 3$ bereits sichtbar.

Behauptung: $I_1 + (I_2 \cap I_3) = R$.

Zum Beweis: Es existieren $e_1, e_1' \in I_1,\ e_2 \in I_2,\ e_3 \in I_3$, sodass $e_1' + e_3 = 1 = e_1 + e_2$.

$$\Rightarrow 1 = 1 \cdot 1 = (e_1' + e_2)(e_1' + e_3) = \underbrace{\underbrace{e_1 e_1'}_{\in I_1} + \underbrace{e_1 e_3}_{\in I_1}}_{=: e_{11} \in I_1} + \underbrace{\underbrace{e_2 e_1'}_{\in I_1} + \underbrace{e_2 e_3}_{\in I_2 \cap I_3}}_{=: e_{23} \in I_2 \cap I_3}$$

Damit ist klar: $R = R \cdot 1 \cdot R = \underbrace{R e_{11} R}_{\in I_1} + \underbrace{R e_{23} R}_{\in I_2 \cap I_3} \subseteq I_1 + I_2 \cap I_3$

Wende $n = 2$ an:

$$R \Big/ (I_1 \cap (I_2 \cap I_3)) \cong R/I_1 \times R/(I_2 \cap I_3) \cong R/I_1 \times R/I_2 \times R/I_3$$

mit dem entsprechenden Isomorphismus. □

Übung 6.2.Ü5:

Sei q die Quersumme und a die alternierende Summe von natürlichen Zahlen. Dann gilt:

- $n \equiv q(n) \mod 9$
- $n \equiv a(n) \mod 11$

d.h.: Jede natürliche Zahl $M \in \mathbb{Z}_{\geq 0}$ kann dargestellt werden als $M = \sum_{i=0}^{n} m_i \cdot 10^i$ mit $m \in \{0, 1, \ldots, 9\}^n,\ n \in \mathbb{Z}_{\geq 0}$.
Die Quersumme eines solchen M ist dann $q(M) := \sum_{i=0}^{n} m_i$ und die alternierende Summe $a(M) = \sum_{i=0}^{n} (-1)^i m_i$.

Beweis:

Quersumme mit 9:

$$\begin{aligned} n &= a_0 \cdot 1 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + 10^n \\ &\equiv a_0 + a_1 \cdot 1 + a_2 \cdot 1 + \cdots + a_n \cdot 1 \mod 9 \\ &= q(n) \mod 9 \end{aligned}$$

Alternierende Summe mit 11:

$$\begin{aligned} n &= a_0 \cdot 1 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + 10^n \\ &\equiv a_0 + a_1 \cdot (-1) + a_2 \cdot (-1)^2 + \cdots + a_n \mod 11 \\ &\equiv a_0 - a_1 + a_2 - \ldots \mod 11 \\ &= a(n) \mod 11 \end{aligned}$$

□

Beispiel 6.2.23:

Durch Kombination der 9er-Probe mittels Quersumme $(\mod 9)$, der 10er-Probe mittels letzter Stelle und der 11er-Probe mittels alternierender Summe $(\mod 11)$ kann man Rechnen mit ganzen Zahlen, wo nur Addition und Multiplikation verwendet werden, $\mod 990$ verifizieren.

$$\mathbb{Z}/\langle 990 \rangle = \mathbb{Z}/(\langle 9 \rangle \cap \langle 10 \rangle \cap \langle 11 \rangle) \cong \mathbb{Z}/\langle 9 \rangle \times \mathbb{Z}/\langle 10 \rangle \times \mathbb{Z}/\langle 11 \rangle$$

Bsp.: $s := 124,\ t := 351$
Wir wollen $(s+t) \cdot t = 166275$ prüfen.

- Modulo 10: $(4+1) \cdot 1 \stackrel{!}{=} 5$ ✓
- Modulo 9: $(7+0) \cdot 0 \stackrel{!}{=} 0$ ✓
- Modulo 11: $((4-2+1)+(1-5+3)) = (3+(-1)) \cdot (-1) = -2 \stackrel{!}{=} 5-7+2-1 = -1$ ✗

Satz 6.2.24: Chinesischer Restsatz für Euklidische Bereiche

Sei R ein Euklidischer Bereich, $I_i = \langle a_i \rangle$ mit $\operatorname{ggT}(a_i, a_j) = 1 \ \forall i \neq j$. Dann gilt:

$$\bigcap_{i=1}^{n} \langle a_i \rangle = \langle \operatorname{kgV}(a_1, \ldots, a_n) \rangle = \left\langle \prod_{i=1}^{n} a_i \right\rangle$$

und

$$\varphi : R \Big/ \left\langle \prod_{i=1}^{n} a_i \right\rangle \xrightarrow{\sim} \bigtimes_{i=1}^{n} R/\langle a_i \rangle$$
$$r + \left\langle \prod_{i=1}^{n} a_i \right\rangle \longmapsto (r + \langle a_1 \rangle, \ldots, r + \langle a_n \rangle)$$

ist ein Isomorphismus, dessen Inverse durch den Euklidischen Algorithmus berechnet werden kann.

Beweis zu 6.2.24:

Da $\operatorname{ggT}(a_i, a_j) = 1 \ \forall i \neq j$ ist, ist $\operatorname{kgV}(a_1, \ldots, a_n) = \prod_{i=1}^{n} a_i$ und somit $\bigcap_{i=1}^{n} \langle a_i \rangle = \left\langle \prod_{i=1}^{n} a_i \right\rangle$.

Es genügt also, einen „Algorithmus“ anzugeben, der das Inverse realisiert. Ein allgemeines Element auf der rechten Seite hat die Form $X = (r_1 + \langle a_1 \rangle, \ldots, r_n + \langle a_n \rangle)$.

Gesucht: ein einzelnes $r \in R$ mit $r + \langle a_o \rangle = r_i + \langle a_i \rangle \ \forall i \in \underline{n}$, also $\varphi\left(r + \left\langle \prod_{i=1}^{n} a_i \right\rangle\right) = X$.

Dazu setze $B_i := \prod_{j \neq i} a_j$. Der $\operatorname{ggT}(a_i, a_j) = 1 \ \forall i \neq j. \Rightarrow \operatorname{ggT}(a_i, B_i) = 1 \Rightarrow \exists x_i, y_i \in R : \ 1 = x_i a_i + y_i B_i$ (Bézout-Koeffizienten).

Setze $e_i := y_i B_i$. Dann ist $e_i + \langle a_i \rangle = 1 + \langle a_i \rangle$ und $e_i + \langle a_j \rangle = 0 + \langle a_j \rangle \ \forall j \neq i$.

$\Rightarrow \varphi(e_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$ mit 1 an i-ter Stelle

$$\Rightarrow \varphi^{-1}(X) = \underbrace{\sum_{i=1}^{n} r_i e_i}_{\text{gesuchtes } r} + \left\langle \prod_{i=1}^{n} a_i \right\rangle$$

□

Beispiel 6.2.25: KONGRUENZENSYSTEM

Wir wollen das simultane Kongruenzensystem

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 4 \\ x &\equiv 3 \mod 5 \end{aligned}$$

lösen (eindeutig modulo $60 = 3 \cdot 4 \cdot 5$).
Wir haben den Isomorphismus

$$\varphi : \mathbb{Z}/\langle 60 \rangle \xrightarrow{\sim} \mathbb{Z}/\langle 3 \rangle \times \mathbb{Z}/\langle 4 \rangle \times \mathbb{Z}/\langle 5 \rangle .$$

und wir haben das Problem gelöst, wenn wir

$$\begin{aligned} e_1 + \langle 60 \rangle &= \varphi^{-1}\left(\overline{1}, \overline{0}, \overline{0}\right) \\ e_2 + \langle 60 \rangle &= \varphi^{-1}\left(\overline{0}, \overline{1}, \overline{0}\right) \\ e_3 + \langle 60 \rangle &= \varphi^{-1}\left(\overline{0}, \overline{0}, \overline{1}\right) \end{aligned}$$

kennen. Die Lösungsmenge ist dann $1 \cdot e_1 + 2 \cdot e_2 + 3 \cdot e_3 + \langle 60 \rangle$.
Mit Hilfe des Euklidischen Algorithmus' (oder scharfes Hingucken) erhalte für 3 und $4 \cdot 5$ etc. folgende Bézout-Identitäten:

$$\begin{aligned} 1 &= 7 \cdot 3 + (-1) \cdot 20 && \Rightarrow e_1 = -20 \\ 1 &= 4 \cdot 4 + (-1) \cdot 15 && \Rightarrow e_2 = -15 \\ 1 &= 5 \cdot 5 + \underbrace{(-2) \cdot 12}_{\text{Urbilder}} && \Rightarrow e_3 = -24 \end{aligned}$$

Also $x \in -122 + \langle 60 \rangle = -2 + \langle 60 \rangle$.

Beispiel 6.2.26: LAGRANGE-INTERPOLATION

Sei K ein Körper und $p(x) \in K[x]$. Wie wir schon wissen (LA1), gilt für $a \in K$:

$$p(a) = 0 \Leftrightarrow p(x) \in \langle x-a \rangle \trianglelefteq K[x]$$

vgl. TAYLOR-ENTWICKLUNG: $p(x) = p(a) + p'(a)(x-a) + \frac{p''(a)}{2!}(x-a)^2 + \dots$ wenn der Körper nicht zu große Fakultäten wieder zu 0 schickt. (Man kann sich dies also als „Taylor für beliebige Körper" vorstellen.)

Sind nun $a_1, \dots, a_n \in K$ paarweise verschiedene Elemente, so sind die Hauptideale $\langle x - a_i \rangle$ paarweise teilerfremd und der chinesische Restsatz liefert:

$$K[x] \Big/ \left\langle \prod_{i=1}^{n} (x-a_i) \right\rangle \cong \bigtimes_{i=1}^{n} \underbrace{K/\langle x-a_i \rangle}_{\cong K}$$

Die Restklassen der Elemente $\widetilde{e}_i(x) := \prod_{j \neq i} (x - a_j)$ liefern auf der rechten Seite Tupel, deren Komponenten alle Null bis auf der i-ten Stelle sind; dort steht $\widetilde{e}_i(a_i) = \prod_{j \neq i} (a_i - a_j)$.
Man hat also $(0, 0, \dots, 0, e_i(a_i), 0, \dots, 0)$, man muss für $(0, \dots, 0, 1, 0, \dots, 0)$ also noch normieren.
Hieraus ergibt sich die **Lagrange-Interpolation**: Eine Abbildung $f : K \to K$ wird interpoliert an den Stützstellen a_i durch das Polynom vom Grad $< n$:

$$\sum_{i=1}^{n} f(a_i) \frac{\widetilde{e}_i(x)}{\widetilde{e}_i(a_i)}$$

Wenn man z.B. im Falle $K = \mathbb{R}$ auch noch Ableitungen an der Stelle a_i vorgeben will, muss man mit $\langle (x-a_i)^k \rangle$ arbeiten anstelle von $\langle x - a_i \rangle$. Dies ist die **Hermit-Interpolation**.
(Erweitert die Lagrange-Multiplikation, lässt sich aber genauso durch den chinesischen Restsatz beweisen und lösen.)

(Eigentlich ist jede Interpolation ein Spezialfall des chinesischen Restsatzes.)

Definition 6.2.27: NULLTEILER UND NILPOTENZ

Sei R ein Ring, kommutativ mit Eins (kmE.), und $a \in R \setminus \{0\}$.
Man nennt a einen **Nullteiler**, wenn ein $b \in R \setminus \{0\}$ existiert mit $ab = 0$.
Weiter heißt a **nilpotent**, falls ein $n \in \mathbb{N}$ existiert mit $a^n = 0$.

Klar sind nilpotente Elemente Nullteiler, aber die Umkehrung ist falsch.
(z.B.: Sei K ein Körper. $0 = (1,0) \cdot (0,1) \in K \times K$, aber keiner von beiden ist nilpotent.)

Beispiel 6.2.28:

(1) Seien $m,k \in \mathbb{N}$. Dann gilt: $m + \langle m^k \rangle \in \mathbb{Z}/\langle m^k \rangle$ ist nilpotentes Element.

(2) **Wurzelziehen:**
Aus dem chinesischen Restsatz bekommen wir:

$$\pi_1 \times \pi_2 : \mathbb{R}[x]/\langle x^2-2 \rangle \xrightarrow{\sim} \underbrace{\mathbb{R}[x]/\langle x-\sqrt{2} \rangle}_{\cong \mathbb{R}} \times \underbrace{\mathbb{R}[x]/\langle x+\sqrt{2} \rangle}_{\cong \mathbb{R}}$$

Wir wollen auf der rechten Seite rechnen, können aber nur auf der linken Seite Nullteiler erkennen.
Unser Ziel ist, eine numerische Approximation von $\sqrt{2}$ zu bestimmen. Klar: Die einzigen Nullteiler der Form $a + \overline{x}$ (links) mit $a \in \mathbb{R}$ sind $\sqrt{2} + \overline{x}$ und $-\sqrt{2} + \overline{x}$ (rechts).
IDEE: Sei $b \in \mathbb{Q}_{\geq 1}$ so gewählt, dass $a := \overline{x} - b$ auf der rechten Seite einem (a_1, a_2) entspricht, mit $|a_1| < 1$ und $|a_2| > 1$ (Absolutbeträge).
Es ist $a^2 = 2 - 2\overline{x}b + b^2$. Dann ist $\left|a_1^2\right| < |a_1| < 1$ und $\pi_1\left(\frac{a^2}{-2b}\right) = \pi_1\left(\overline{x} - \frac{b^2+2}{2b}\right)$ hat einen noch kleineren Betrag, sodass $\frac{b^2+2}{2b}$ eine noch bessere Approximation von $\sqrt{2}$ ist als b.
Durch fortgesetztes Quadrieren verdoppelt sich die Anzahl der signifikanten Dezimalstellen, wir haben quadratische Konvergenz. Fängt man bei $b = 1$ an, so erhält man:

$$\begin{aligned} 1 & \\ \frac{3}{2} &= 1{,}5 \\ \frac{17}{12} &= 1{,}41\overline{6} \\ \frac{577}{408} &= 1{,}414215686 \\ \frac{665857}{470832} &= 1{,}\underbrace{41421356}_{\text{stimmen exakt}}\ldots \end{aligned}$$

Übung 6.2.Ü6:

Vgl. **Newton-Verfahren** aus der Numerik:
Linearisieren der Funktion (d.h. nutze LGS, um nicht-lineares GLS „$x^2 - 2 = 0$“ zu lösen).
„Anfang von Taylor“:

$$0 = f(x_n) + f'(x_n)(x_{n+1} - x_n)$$

„Dreisatz“ = Gauß-Algorithmus:

$$\begin{aligned} \Rightarrow x_{n+1} &= x_n - \frac{f(x_n)}{f'(x_n)} \\ &= x_n - \frac{x_n^2 - 2}{2x_n} = \frac{x_n^2 + 2}{2x_n} \widehat{=} \frac{b^2+2}{2b} \end{aligned}$$

6.2.e Der chinesische Restsatz und die Hauptraumzerlegung

Die Hauptraumzerlegung erinnert stark an den chinesischen Restsatz.
Wdh.:
Sei dazu K ein Körper, $\mathcal{V}$ ein endlich erzeugter (e.e.) K-VR und $\alpha \in \mathrm{End}(\mathcal{V})$ mit Minimalpolynom

$$\mu_\alpha = p_1^{n_1} \cdots p_k^{n_k}$$

wobei die p_i paarweise teilerfremde irreduzible normierte Polynome in $K[x]$ sind.

Unter der obigen Voraussetzung lässt sich $\mathcal{V}$ eindeutig schreiben als eine direkte Summe von α-invarianten Teilräumen $\mathcal{U}_i$:

$$\mathcal{V} = \bigoplus_{i=1}^{n} \mathcal{U}_i$$

sodass das Minimalpolynom von $\alpha|_{\mathcal{U}_i}$ gleich $p_i^{n_i}$ ist.
Setzt man $q_i := \underbrace{\prod_{j \neq i} p_j^{n+i}}$, so ist $\mathcal{U}_i = \mathrm{Bild}(q_i(\alpha))$.

das „Auftauchen" dieser Elemente wollen wir jetzt durch den chinesischen Restsatz verstehen.

Bemerkung 6.2.29:

(1) Das **Minimalpolynom** von α war definiert als normierter Erzeuger des Kerns des **Einsetzungshomomorphismus**

$$\begin{aligned} \varepsilon_\alpha : K[x] &\longrightarrow \mathrm{End}(\mathcal{V}) \\ p &\longmapsto p(\alpha) \end{aligned}$$

$$\begin{aligned} &\mathrm{Kern}\,\varepsilon_\alpha = \langle \mu_\alpha \rangle \\ &\mathrm{Bild}\,\varepsilon_\alpha = K[\alpha] \leq \mathrm{End}(\mathcal{V}) \\ &\overset{\text{Hom.satz}}{\Longrightarrow} K[x] \Big/ \langle \mu_\alpha \rangle \cong K[\alpha] \end{aligned}$$

(2) Setzt man $R = K[x]/\langle \mu_\alpha \rangle$, so wird $\mathcal{V}$ ein R-Modul durch

$$\left(p + \langle \mu_\alpha \rangle\right) V = \varepsilon_\alpha(p)(V) = p(\alpha)(V)$$

für $V \in \mathcal{V}$.

(3) Die Struktur von R bekommen wir aus dem chinesischen Restsatz:

$$R = K[x] \Big/ \langle p_1^{n_1} \cdots p_k^{n_k} \rangle \cong K[x] \Big/ \langle p_1^{n_1} \rangle \times \cdots \times K[x] \Big/ \langle p_k^{n_k} \rangle$$

und Urbilder der **Idempotenten** $\pi_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ mit 1 an der i-ten Stelle können mit dem Algorithmus 6.2.24 ermittelt werden, indem wir mit dem erweiterten Euklidischen Algorithmus

$$\mathrm{ggT}\left(p_i^{n_i}, q_i\right) = 1 = x_i p_i^{n_i} + \underbrace{y_i q_i}_{=B_i}$$

und $e_i = \varepsilon_\alpha(y_i q_i) = y_i(\alpha) q_i(\alpha)$ setzen.
Aus einer Übungsaufgabe aus LA1 wissen wir, dass

$$\mathrm{Bild}(e_i) = \mathrm{Bild}(q_i(\alpha)) = \mathcal{U}_i$$

(4) Also ist $\mathcal{V}$ ein Modul über dem Produktring

$$K[x] \Big/ \langle p_1^{n_1} \rangle \times \cdots \times K[x] \Big/ \langle p_k^{n_k} \rangle$$

und die direkte Zerlegung (Hauptraumzerlegung)

$$\mathcal{V} = \bigoplus_{i=1}^{k} \mathcal{U}_i$$

liefert eine Zerlegung von $\mathcal{V}$ in eine direkte Summe von $K[x]/\langle p_i^{n_i} \rangle$-Moduln für $i \in \underline{k}$, d.h. sie ist nichts anderes als die Zerlegung von $\mathcal{V}$ gemäß Bemerkung 6.2.11, wobei $\mathcal{U}_i$ in natürlicher Weise ein $K[x]/\langle p_i^{n_i} \rangle$-Modul ist.

Zusammenfassend:

- $\mathcal{V}$ ist $K[x]$-Modul
- $\mathcal{V}$ ist $K[x]/\langle \mu_\alpha \rangle$-Modul ($\mu_\alpha$ ist Annihilator)
  $= \mathcal{V}$ ist $K[x]/\langle p_1^{n_1} \cdots p_k^{n_k} \rangle$-Modul
- $\mathcal{V}$ ist $K[x]/\langle p_1^{n_1} \rangle \times \cdots \times K[x]/\langle p_k^{n_k} \rangle$-Modul

6.3 Elementare Teilbarkeitstheorie für Ringe

Definition 6.3.1:

Sei R ein Ring (kmE.) und $a, b \in R$.

(1) a **teilt** b (in R) oder b ist ein **Vielfaches** von a (in R), falls ein $r \in R$ existiert mit $b = ra$, in Zeichen: $a \mid b$.

(2) a ist **assoziiert** zu b (in R), in Zeichen $a \sim b$, falls $a \mid b$ und $b \mid a$.

Klar: Die Vielfachen von a bilden das von a erzeugte Hauptideal $\langle a \rangle$.
Teilen ist eine transitive Relation auf R und das Assoziiertsein ($\sim$) ist eine ÄR auf R.
Auch klar: für $a, b \in R$: Falls $e \in R^*$ existiert mit $a = eb$, dann gilt $a \sim b$.
Für die Umkehrung brauchen wir die Annahme, dass R ein IB ist.

Bemerkung 6.3.2:

In einem Integritätsbereich sind die Assoziiertenklassen der Elemente gegeben durch $R^* a$.
Anders formuliert: R^* operiert auf R vermöge

$$\begin{aligned} R^* \times R &\longrightarrow R \\ (e,\ a) &\longmapsto ea \end{aligned}$$

und es gilt $\sim_{R^*} = \sim$.

Beweis zu 6.3.2:
Es ist klar, dass jedes Element der Form $u \cdot a$ mit u Einheit zu $a = u^{-1}(ua)$ assoziiert ist.
Sei nun $b \mid a,\ a \mid b$. Dann existieren $r, s \in R : a = br,\ b = as$. Ist $a = 0$, folgt $b = as = 0 \cdot s = 0$.
Sei also $a \neq 0$. Wir wollen zeigen, dass sowohl r als auch s Einheiten sind, und sogar zueinander invers.

$$\begin{aligned} & a = br = asr \\ & \Rightarrow a(1 - sr) = 0 \\ & \underset{a \neq 0}{\overset{R \text{ IB}}{\Longrightarrow}} 1 - rs = 0 \ \Rightarrow rs = 1 \end{aligned}$$

□

Bemerkung 6.3.3:

Sei R ein IB.
So ist der Polynomring

$$R[x_1,\dots,x_n] = R[x_1,\dots,x_{n-1}][x] = \dots$$

auch ein IB.
Dazu definieren wir den **Grad** (auch **Totalgrad**) eines Polynoms

$$p = p(x) = \sum a_{i_1}\cdots a_{i_n} x_1^{i_1}\cdots x_n^{i_n} \in R[x_1,\dots,x_n]$$

als

$$\operatorname{Grad} p := \max\left\{ i_1+\cdots+i_n \,\middle|\, a_{i_1\cdots i_n} \neq 0 \right\}$$

für $p \neq 0$ und $\operatorname{Grad} 0 := -\infty$.

Für $p,q \in R[x_1,\dots,x_n]\setminus\{0\}$ gilt:

$$\operatorname{Grad}(pq) = \operatorname{Grad} p + \operatorname{Grad} q$$

d.h. $R[x_1,\dots,x_n]$ ist ein IB.

Nächste Frage: Was ist mit Restklassenringen von IBen?

Definition 6.3.4:

Sei R ein Ring (kmE.).

(1) Ein Ideal $I \trianglelefteq R$ heißt **Primideal** oder **als Ideal prim**, falls $I \neq R$ und $\forall r,s \in R : r,s \notin I \Rightarrow rs \notin I$.
(d.h. R/I hat keine Nullteiler)

(2) Ein Ideal $I \trianglelefteq R$ heißt **maximales Ideal**, falls $I \neq R = \langle 1\rangle$ und für jedes $J \trianglelefteq R$ mit $I \subseteq J \subseteq R$ gilt: $J = I$ oder $J = R$.

Bemerkung 6.3.5:

Sei R ein Ring (kmE.) und $I \trianglelefteq R$.

(1) R/I ist genau dann ein IB, wenn I ein Primideal ist.

(2) R/I ist genau dann ein Körper, wenn I ein maximales Ideal ist.

Beweis zu 6.3.5:

(1) Per Definition.

(2) R/I ist ein Körper, genau dann, wenn jedes

$$r+I \in {}^{R}\!/_{I} \setminus \{0+I\}$$

ein multiplikatives Inverses hat.
Sei also $r \notin I$. Dann ist

$$\langle r, I\rangle = \langle r\rangle + I \quad (= R \text{ wenn } I \text{ maximal})$$

ein Ideal in R. D.h.:

$$\exists a \in R : \ 1 = ar + i \text{ mit } i \in I$$
$$\Rightarrow 1 + I = ar + i + I = ar + I = (a+I)(r+I)$$

$\Rightarrow (a+I)$ ist das multiplikative Inverse zu $(r+I)$.
Die Umkehrung geht genauso.

□

Beispiel 6.3.6:

(1) Sei R ein IB. Das Hauptideal $\langle x \rangle \trianglelefteq R[x]$ ist ein Primideal. Denn: $R[x]/\langle x \rangle \cong R$

(2) Sei R ein Ring (kmE.) und I maximal $\Rightarrow I$ prim.

(3) Sei R ein Ring (kmE.). Genau dann ist $\langle 0 \rangle$ ein Primideal, wenn $R \cong R/\{0\}$ ein IB ist.

Nun kommen wir zur Teilbarkeitstheorie in IBen, also zurück zu Elementen.

Definition 6.3.7:

Sei R ein IB.

(1) Ein Element $a \in R \setminus (R^* \cup \{0\})$ heißt **irreduzibel** oder „unzerlegbar“, falls jede Faktorisierung von a trivial ist, d.h.: falls $a = a_1 a_2 \Rightarrow a_1 \in R^* \vee a_2 \in R^*$.
Sonst heißt a **reduzibel** oder „zerlegbar“.

(2) Ein Element $a \in R \setminus (R^* \cup \{0\})$ heißt **prim**, falls

$$a \mid (b_1 b_2) \Rightarrow a \mid b_1 \vee a \mid b_2 \quad \forall b_1, b_2 \in R$$

(Dies ist auch die Definition einer **Primzahl** in $\mathbb{Z}$.)

Dass diese Begriffe in manchen Ringen auseinanderfallen, hat zu vielen falschen Beweisen von *Fermat's Last Theorem* geführt, u.a. von Cauchy.

Beispiel 6.3.8:

(1) Im $R = \mathbb{Z}$ ist $2 \in \mathbb{Z}$ prim und irreduzibel.

(2) Sei K ein IB und $R = K[x]$. Dann ist x irreduzibel (da von Grad 1).

$$x = pq,\ 1 = \operatorname{Grad} x = \underbrace{\operatorname{Grad}(p)}_{\substack{0\\1}} \underbrace{\operatorname{Grad}(q)}_{\substack{1\\0}}$$

und prim, da:
Sei $x \mid a(x)b(x)$ und $x \nmid a$

$\Leftrightarrow a(0) \neq 0$
$\Rightarrow b(0) = 0$ da R IB ist
$\Rightarrow x \mid b(x)$

Bemerkung 6.3.9:

Sei R IB und $a \in R$.

(1) a prim $\Rightarrow a$ irreduzibel.

(2) a prim $\Leftrightarrow \langle a \rangle$ als Ideal prim und $\langle a \rangle \neq \langle 0 \rangle$ ist.

Beweis zu 6.3.9:

(1) Sei a prim und reduzibel, d.h. $a = a_1 a_2$ mit $a_i \notin R^*$ $(i \in \underline{2})$. Dann gilt $a \mid a_1 a_2 \overset{a \text{ prim}}{\Longrightarrow} a \mid a_1$ oder $a \mid a_2$, aber $a \nmid a_1$, da sonst $a \sim a_1$, und somit a_2 Einheit, und $a \nmid a_2$, da sonst $a \sim a_2$ und somit $a_1 \in R^*$. $\lightning$
d.h. prim $\Rightarrow$ irreduzibel. □

(2) Sei $a \in R$ prim. Dann ist $\langle a \rangle \neq 0$. Weiter gilt $\forall r, s \in R : rs \in \langle a \rangle \Leftrightarrow a \mid rs \Leftrightarrow a \mid r \vee a \mid s \Leftrightarrow r \in \langle a \rangle \vee s \in \langle a \rangle$
Die Umkehrung gilt genauso.

□

Übung 6.3.Ü1:

Es gibt irreduzible Elemente, die nicht prim sind.

Beweis:

Es ist $\mathbb{Z}\left[\sqrt{-5}\right] := \{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$. Sei $\nu\left(a+b\sqrt{-5}\right) := a^2+5b^2$ für $a+b\sqrt{-5} \in \mathbb{Z}\left[\sqrt{-5}\right]$.
Zunächst: Für ν gilt, mit $a+b\sqrt{-5}, c+d\sqrt{-5} \in \mathbb{Z}\left[\sqrt{-5}\right]$:

$$\begin{aligned}\nu\left((a+b\sqrt{-5})\left(c+d\sqrt{-5}\right)\right) &= \nu\left(ac-5bd+(ad+bc)\sqrt{-5}\right)\\ &= (ac-5bd)^2+5(ad+bc)^2 = a^2c^2-10abcd+5^2b^2d^2+5a^2d^2+10abcd+5b^2c^2\\ &= a^2c^2+5^2b^2d^2+5a^2d^2+5b^2c^2 = \left(a^2+5b^2\right)\left(c^2+5d^2\right) = \nu\left(a+b\sqrt{-5}\right)\nu\left(c+d\sqrt{-5}\right)\end{aligned}$$

also ist ν multiplikativ. D.h. für $z_1, z_2 \in \mathbb{Z}\left[\sqrt{-5}\right]$ gilt insbesondere:

$$\underbrace{z_1 \mid z_2}_{\text{in } \mathbb{Z}[\sqrt{-5}]} \Rightarrow \underbrace{\nu(z_1) \mid \nu(z_2)}_{\text{in } \mathbb{N}}$$

Sei $2 = \left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)$ mit $a,b,c,d \in \mathbb{Z}$, d.h.

$$\begin{aligned}&\nu(2) = \nu\left(\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)\right) = \nu\left(a+b\sqrt{-5}\right)\nu\left(c+d\sqrt{-5}\right)\\ &\Leftrightarrow 2^2 = \left(a^2+5b^2\right)\left(c^2+5d^2\right)\end{aligned}$$

Da $a^2+5b^2 \geq 0 \ \forall a,b \in \mathbb{Z}$, gilt hier, damit $\left(a^2+5b^2\right) \mid 2^2 = 4$ gilt:

$$a^2+5b^2 \in \{1,2,4\}$$

Ist $a^2+5b^2 = 1$, wäre $a+b\sqrt{-5}$ eine Einheit, und wäre $a^2+5b^2 = 4$, folgt $c^2+5d^2 = 1 \Rightarrow c+d\sqrt{-5}$ Einheit.
Die einzige weitere Möglichkeit wäre also

$$a^2+5b^2 = c^2+5d^2 = 2$$

Dies kann aber nie eintreten, da

$$\begin{aligned}1^2+5\cdot 0^2 &= 1 < 2\\ 2^2+5\cdot 0^2 &= 4 > 2\\ 0^2+5\cdot 1^2 &= 5 > 2\end{aligned}$$

$\Rightarrow 2$ kann in $\mathbb{Z}\left[\sqrt{-5}\right]$ nicht von nicht-Einheiten faktorisiert werden und ist damit irreduzibel.
Sei $3 = \left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)$ mit $a,b,c,d \in \mathbb{Z}$. Analog 2 gilt dann:

$$\begin{aligned}&\nu(3) = 3^2 = 9 = \nu\left(a^2+5b^2\right)\nu\left(c^2+5d^2\right) = \left(a^2+5b^2\right)\left(c^2+5d^2\right)\\ &\Rightarrow a^2+5b^2 \in \{1,3,9\}\end{aligned}$$

also ist die einzige Möglichkeit für eine Faktorisierung aus nicht-Einheiten

$$a^2+5b^2 = c^2+5d^2 = 3$$

was ebenfalls nie eintreten kann, womit 3 ebenfalls in $\mathbb{Z}\left[\sqrt{-5}\right]$ irreduzibel ist.
Sei $1+\sqrt{-5} = \left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)$ mit $a,b,c,d \in \mathbb{Z}$.

$$\begin{aligned}&\Rightarrow \nu\left(1+\sqrt{-5}\right) = \nu\left(a+b\sqrt{-5}\right)\nu\left(c+d\sqrt{-5}\right)\\ &\Leftrightarrow 1^2+5\cdot 1^2 = 6 = \left(a^2+5b^2\right)\left(c+5d^2\right)\\ &\Rightarrow a^2+5b^2 \in \{1,2,3,6\}\end{aligned}$$

Analog $2,3$ fallen 1 und 6 hier als Möglichkeiten trivialerweise weg. 2 und 3 wurden allerdings oben bereits als unmögliche Normergebnisse eingestuft. Somit ist auch $1+\sqrt{-5}$ in $\mathbb{Z}\left[\sqrt{-5}\right]$ irreduzibel.

Analog dazu ist auch $v\left(1-\sqrt{-5}\right)=6 \Rightarrow 1-\sqrt{-5}$ irreduzibel.

Nun betrachte:

$$3\cdot 2 \overset{!}{=} \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$$
$$\Leftrightarrow 6 \overset{!}{=} 1^2+\sqrt{-5}-\sqrt{-5}-\sqrt{-5}^2 = 1-(-5)=6 \quad \checkmark$$

Klar ist also: $2 \mid 6,\ 3 \mid 6,\ \left(1\pm\sqrt{-5}\right) \mid 6$.

$$\Rightarrow 2 \mid \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right), \text{ aber } 2 \nmid \left(1\pm\sqrt{-5}\right), \text{ da diese irreduzibel sind.}$$
$$3 \mid \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right), \text{ aber } 3 \nmid \left(1\pm\sqrt{-5}\right), \text{ da diese irreduzibel sind.}$$
$$\left(1\pm\sqrt{-5}\right) \mid (3\cdot 2), \text{ aber } \left(1\pm\sqrt{-5}\right) \nmid 3,2, \text{ da diese irreduzibel sind.}$$

Damit sind $2,\ 3,\ 1+\sqrt{-5}$ und $1-\sqrt{-5}$ nicht prim in $\mathbb{Z}\left[\sqrt{-5}\right]$. □

An dieser Stelle sei bemerkt, dass genau diese uneindeutige Faktorisierung Herrn Dedekind („Vater der modernen Algebra“) dazu bewegt hat, den Begriff „Ideal“ (Abk. „ideale Zahlen“) einzuführen, um zu einer eindeutigen Teilbarkeitstheorie zu kommen.
Im obigen Gegenbeispiel kann man nämlich alle vier Zahlen als Ideale noch weiter zerlegen:

$$\langle 2\rangle = \left\langle 2,\ 1+\sqrt{-5}\right\rangle\left\langle 2,\ 1-\sqrt{-5}\right\rangle$$
$$\langle 3\rangle = \left\langle 3,\ 1+\sqrt{-5}\right\rangle\left\langle 3,\ 1-\sqrt{-5}\right\rangle$$
$$\left\langle 1+\sqrt{-5}\right\rangle = \left\langle 2,\ 1+\sqrt{-5}\right\rangle\left\langle 3,\ 1+\sqrt{-5}\right\rangle$$
$$\left\langle 1-\sqrt{-5}\right\rangle = \left\langle 2,\ 1-\sqrt{-5}\right\rangle\left\langle 3,\ 1-\sqrt{-5}\right\rangle$$

Satz 6.3.10:

Ist R ein HIB, so ist jedes irreduzible Element prim.

Beweis zu 6.3.10:
Sei $a \in R \setminus (R^* \cup \{0\})$ irreduzibel. Wir wissen, dass a genau dann prim ist, wenn $\langle a\rangle$ ein Primideal $\neq \langle 0\rangle$ ist.
Wir werden sogar mehr zeigen, nämlich dass das Hauptideal $\langle a\rangle$ ein maximales ist (damit automatisch prim).
Dafür sei $\langle a\rangle \subseteq I \subsetneq R$. Da R ein HIB, ist $I=\langle d\rangle$ für ein $d \in R\setminus(R^*\cup\{0\})$. Somit ist $a \in \langle d\rangle$. $\Rightarrow \exists d' \in R : a = d'd$
Da a irreduzibel ist, ist d' eine Einheit. $\Rightarrow a \sim d \Rightarrow \langle a\rangle = \langle d\rangle = I$.
$\Rightarrow \mathbb{Z}\left[\sqrt{-5}\right]$ ist kein HIB. □

Korollar 6.3.11:

Ist R ein HIB, so ist jedes Primideal, das ungleich $\{0\}$ ist, ein maximales Ideal.

Beispiel 6.3.12:

(1) $\mathbb{Z}[x]$ ist kein HIB, denn das Primideal $\langle x \rangle$ ist kein maximales Ideal.

$$\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z} \text{ (kein Körper)}$$

(2) $K[x,y]$ (sogar für K Körper) ist ebenfalls kein HIB, denn

$$K[x,y]/\langle y \rangle \cong K[x] \text{ (kein Körper)}$$

(3) $\mathbb{Z}$ ist ein HIB. Die Primzahlen sind bis auf Multiplikation mit $\mathbb{Z}^* = \{-1, 1\}$ die irreduziblen Elemente in $\mathbb{Z}$ (die gängigen Primzahlen, aber auch z.B. -2).
Die $\mathbb{F}_p := \mathbb{Z}/\langle p \rangle$ für Primzahlen p sind die einzigen Restklassen**körper** in $\mathbb{Z}$.

(4) Für jeden Körper K ist $K[x]$ ein HIB (sogar ein Euklidischer Ring) und die irreduziblen Polynome in $K[x]$ sind gleich den Primelementen in $K[x]$ und gleich den irreduziblen Elementen in $K[x]$.
Die Resklassenkörper von $K[x]$ sind alle von der Form $K[x]/\langle p(x) \rangle$ mit $p(x)$ irreduzibles Polynom.

Satz 6.3.13:

Sei R ein HIB, $a \in R/(R^* \cup \{0\})$. Dann gibt es im Wesentlichen genau eine eindeutige Faktorisierung in Primpotenzfaktoren (Primfaktorzerlegung), d.h. $\exists a_1, \ldots, a_n \in R$ prim mit $a = a_1 \cdots a_n$.
Die Eindeutigkeit bedeutet: Ist $a = b_1 \cdots b_m$ eine weitere Zerlegung in Primelemente, so ist $m = n$ und nach Umnummerierung $a_i \sim b_i \forall i \in \underline{n}$.

Beweis zu 6.3.13:
(analog $\mathbb{Z}$)
Ist a irreduzibel, so ist a schon prim und wir sind fertig, sonst ist a irreduzibel, sprich $a = bc$ mit $b, c \notin R^*$. Fahre mit b und c fort und zerlege sie weiter. Falls dieser Prozess etwa für b nicht aufhört, dann haben wir eine unendliche Teilerkette

$$\ldots \mid b_{i+1} \mid b_i \mid \ldots \mid b_1 = b \mid a$$

konstruiert (wobei keiner assoziiert zum vorherigen ist) und die unendliche Idealkette

$$\langle a \rangle \subseteq \underbrace{\langle b_1 \rangle}_{=b} \subseteq \langle b_2 \rangle \subseteq \ldots$$

Definiere $I := \bigcup_i \langle b_i \rangle \trianglelefteq R$. $\Rightarrow I = \langle d \rangle$ (da R HIB)

$$\text{Da } d \in I = \bigcup_{i=1}^{\infty} \langle b_i \rangle : \exists i \text{ mit } d \in \langle b_i \rangle : \ \langle b_i \rangle = \langle b_j \rangle \ \forall j \geq i \quad \lightning \text{ (echte Teilerkette/Idealkette)}$$

Die Eindeutigkeit: Sei $a = a_1 \cdots a_n = b_1 \cdots b_m$ mit a_i, b_j irreduzibel. Da a_1 prim ist $\Rightarrow \exists j : a_1 \mid b_j$. Da b_j irreduzibel, folgt $a_1 \sim b_j$, usw. (Induktion). □

6.4 Moduln über HIB

6.4.a Der Struktursatz

Die e.e. Moduln haben eine schöne Form für Normalformen, die Bézout-Identität. Algorithmisch zugänglich sind also Euklidische Ringe, in denen man die Bézout-Identität durch den Euklidischen Algorithmus erhält.

Definition 6.4.1: Torsion

Sei R ein IB und M ein R-Modul. Ein $m \in M$ heißt **Torsionselement**, falls das **Annihilatorideal**

$$\mathrm{Ann}_R(m) := \{r \in R \mid rm = 0\}$$

von Null verschieden ist.
Der **Torsionsmodul**, also der Teilmodul aller Torsionselemente, wird mit $\mathrm{T}(M)$ bezeichnet.

(Beachte: R ist kommutativ, sonst wäre die Behauptung „$\mathrm{T}(M)$ Teilmodul“ i.A. falsch.)

Der Modul M heißt **torsionsfrei**, falls $\mathrm{T}(M) = \{0\}$ ist („nahe VR“).
M heißt **Torsionsmodul**, falls $M = \mathrm{T}(M)$ („weit weg von VR“).

Es gilt: $\mathrm{Ann}_R(M) = \bigcap_{m \in M} \mathrm{Ann}_R(m)$.

Beispiel 6.4.2:

Sei R ein HIB mit $K := \mathrm{Quot}(R)$.

(1) K ist ein nicht-endlich-erzeugter, torsionsfreier R-Modul.
Beweis: *später.*

(2) K/R ist ein nicht-endlich-erzeugter Torsionsmodul.
Beweis: *Noch zu schwierig für uns.*

(3) Jeder freier R-Modul ist torsionsfrei, insbesondere ${}_RR = R$ ist selbst torsionsfrei.

(4) Ist M beliebier R-Modul, so ist $M/\mathrm{T}(M)$ torsionsfrei.
Beweis:
Sei $m \in \mathrm{T}(M) \subseteq M$. In $M/\mathrm{T}(M)$ gilt damit: $m + \mathrm{T}(M) = 0 + \mathrm{T}(M)$.
$\Rightarrow m + \mathrm{T}(M)$ ist in $M/\mathrm{T}(M)$ nur das triviale Torsionselement.
Gibt es noch andere Torsionselemente in $M/\mathrm{T}(M)$?
Sei $n \in M$ so, dass $n + \mathrm{T}(M)$ ein Torsionselement in $M/\mathrm{T}(M)$.

$$\begin{aligned} &\Rightarrow \exists r \in R \setminus \{0\} : \; r \cdot (n + \mathrm{T}(M)) = 0 + \mathrm{T}(M) \\ &\qquad\qquad \Leftrightarrow (rn) + \mathrm{T}(M) = 0 + \mathrm{T}(M) \\ &\qquad\qquad \Leftrightarrow rn \in \mathrm{T}(M) \\ &\Rightarrow \exists a \in R \setminus \{0\} : \; \overbrace{ar}^{\in R \setminus \{0\}}\, n = 0 \\ &\Rightarrow \exists s \in R \setminus \{0\} : \; sn = 0 \Rightarrow \mathrm{Ann}_R(n) \supseteq \{0, s\} = \{0, ar\} \neq \{0\} \end{aligned}$$

Also ist $n \in \mathrm{T}(M)$.

$\Rightarrow \mathrm{T}\big(M/\mathrm{T}(M)\big) = \{0 + \mathrm{T}(M)\}$, d.h. $M/\mathrm{T}(M)$ ist torsionsfrei. □

(5) Jeder zyklische Modul (sprich, von einem Element erzeugt) ist entweder isomorph zu ${}_RR = R$ oder zu ${}_RR/Ra$ für ein $a \in R$.
Beweis:
$R \twoheadrightarrow M = \langle m \rangle$, $r \mapsto rm$, Homomorphiesatz. □

Im letzten Fall haben wir einen Torsionsmodul. $a \cdot \overline{1} = \overline{a} = 0$
Obwohl ${}_RR/Ra$ und $R/\langle a \rangle$ als Abelsche Gruppen und als R-Moduln isomorph sind, schreiben wir ${}_RR/Ra$, um von Faktormoduln zu sprechen, und $R/\langle a \rangle$, wenn wir von Restklassenringen sprechen. Da $\mathrm{Ann}_R(R/Ra) = \langle a \rangle$, ist R/Ra ein $R/\langle a \rangle$-Modul, und als solcher sogar frei.

(6) Endliche direkte Summen der Moduln aus (5) sind typische e.e. R-Moduln.

(7) Faktormoduln von $R^{n \times 1}$ sind alle e.e. R-Moduln, wie wir bereits wissen.

ZIEL: Wir wollen zeigen, dass die Moduln aus (7) nicht allgemeiner sind als die Moduln aus (6), also jeden Modul aus (7) auf einen Modul der Form aus (6) zurückführen. Sprich: Jeder e.e. R-Modul von einem HIB ist eindliche direkte Summe von zyklischen R-Moduln (d.h. Moduln der Form ${}_RR$ und ${}_RR/Ra$).

Lemma 6.4.3:

Sei R ein IB und $(e_1,\dots,e_n)$ die Standardbasis von $R^{n\times 1}$, also ein freies EZS des freien Moduls $\mathrm{Fr}_R(\underline{n}) = R^{n\times 1}$. Sei $\mathbb{Z}_{\geq 0} \ni k \leq n$ und $d_1,\dots,d_k \in R\setminus\{0\}$. Dann gilt:

$$\begin{aligned} R^{n\times 1}\Big/\langle d_1e_1,\dots,d_ke_k\rangle &= \left(\bigoplus_{i=1}^{n} Re_i\right)\Big/\left(\bigoplus_{i=1}^{k} Rd_ie_i\right)\\ &\cong \bigoplus_{i=1}^{k} Re_i/Re_id_i \oplus \bigoplus_{i=k+1}^{n} Re_i\\ &\cong \bigoplus_{i=1}^{k} {}_RR/Rd_i \oplus R^{(n-k)\times 1} \end{aligned}$$

Falls in dieser Situation noch zusätzlich $d_i \mid d_{i+1}\ \forall i \in \underline{(k-1)}$ gilt, so nennt man das Tupel $(e_1,\dots,e_n)$ und $(d_1e_1,\dots,d_ke_k)$ **kompatible Basen**, genauer: ein Paar kompatibler Basen (Basis = freies EZS).

Was bringt das? Man darf „modulo“ mit Einträgen vertauschen! Z.B.: $\overline{\begin{pmatrix} r_1\\ r_2\end{pmatrix}} \cong \begin{pmatrix}\overline{r_1}\\ \overline{r_2}\end{pmatrix}$

Beweis zu 6.4.3:

Es gilt:

$$R^{n\times 1} = \left\{\sum_{i=1}^{n} r_ie_i \;\middle|\; r\in R^n\right\} = \bigoplus_{i=1}^{n} Re_i$$

$$\langle d_1e_1,\dots,d_ke_k\rangle_R = \bigoplus_{i=1}^{k} Rd_ie_i$$

$$\Rightarrow R^{n\times 1}\Big/\langle d_1e_1,\dots,d_ke_k\rangle = \bigoplus_{i=1}^{n} Re_i\Big/\bigoplus_{i=1}^{k} Rd_ie_i$$

Sei

$$\varphi : \bigoplus_{i=1}^{n} Re_i \longrightarrow \bigoplus_{i=1}^{k} Re_i/Rd_ie_i \oplus \bigoplus_{i=k+1}^{n} Re_i$$

$$\sum_{i=1}^{n} r_ie_i \longmapsto \left(\sum_{i=1}^{k} r_ie_i + Rd_ie_i\right) + \sum_{i=k+1}^{n} r_ie_i$$

φ ist ein R-Modulhomomorphismus und surjektiv, und $\mathrm{Kern}\,\varphi = \langle d_1e_1,\dots,d_ke_k\rangle$.
Nach dem Homomorphiesatz gilt:

$$\left(\bigoplus_{i=1}^{n} Re_i\right)\Big/\langle d_1e_1,\dots,d_ke_k\rangle = \left(\bigoplus_{i=1}^{n} Re_i\right)\Big/\mathrm{Kern}\,\varphi \cong \mathrm{Bild}\,\varphi = \bigoplus_{i=1}^{k} Re_i/Rd_ie_i \oplus \bigoplus_{i=k+1}^{n} Re_i$$

Sei

$$\psi : R^{n\times 1} \longrightarrow \bigoplus_{i=1}^{k} {}_RR/Rd_i \oplus R^{(n-k)\times 1}$$

$$\begin{pmatrix} r_1\\ \vdots\\ r_n\end{pmatrix} \longmapsto (r_1+Rd_i,\dots,r_k+Rd_k,r_{k+1},\dots,r_n)$$

ψ ist R-Modulhomomorphismus und surjektiv (entspricht dem natürlichen Epimorphismus in den ersten k Komponenten, danach der Identität), und $\mathrm{Kern}\,\psi = \langle d_1e_1,\dots,d_ke_k\rangle_R$.
Aus dem Homomorphiesatz folgt die Behauptung. □

Lemma 6.4.4:

Sei R ein HIB, $M \cong R^{n\times 1}$ ein freier R-Modul vom Rang n. Dann ist jeder Teilmodul von M wieder endlich erzeugter freier R-Modul vom Rang $k \leq n$, d.h. auf k freien Erzeugern.

Beweis zu 6.4.4:
Der Fall $n = 1$ ist klar: Man hat Teilmoduln von ${}_R R$ nur $R/R \cdot 0$ (frei von Rang 0) oder R/Ra (frei von Rang 1), also (Haupt-)Ideale von R, erzeugt von einem Element.
Sei nun $T \leq M$ und $(e_1, \ldots, e_n)$ die Standardbasis von $M \cong R^{n\times 1}$. Zu der Zerlegung $M = Re_1 \oplus \langle e_2, \ldots, e_n \rangle_R$ gehört die Projektion

$$\begin{aligned} \pi : \quad M &\longrightarrow Re_1 \\ \sum_{i=1}^{m} m_i e_i &\longmapsto m_1 e_1 \end{aligned}$$

(leicht z.z.: R-Modulhom.) Dann ist $\pi(T) \leq Re_1$. Im Fall $\pi(T) = \{0\} \leq Re_1$ greift die Induktionsannahme, da dann dieser Teilraum $T = \operatorname{Kern}\pi\big|_T \leq \underbrace{\langle e_2, \ldots, e_n \rangle}_{\operatorname{Kern}\pi} = R^{(n-1)\times 1}$.
Im Fall $\pi(T) = Rde_1$ für ein $d \in R \setminus \{0\}$:
Beachte: $\pi(T)$ ist frei auf de_1. Wähle $t \in T$ mit $\pi(t) = de_1$, dann definiert

$$\begin{aligned} \iota : Rde_1 &\longrightarrow T \\ de_1 &\longmapsto t \end{aligned}$$

einen R-Modulhomomorphismus und es gilt:

$$T = \underbrace{Rt}_{\text{Bild}\,\iota} \oplus \operatorname{Kern}\pi\big|_T$$

Wegen $\operatorname{Kern}\pi\big|_T \leq \langle e_2, \ldots, e_n \rangle_R$ können wir die Induktionsannahme verwenden und sind fertig. □

Wir wollen jetzt die Existenz kompatibler Basen beweisen, indem wir sowohl beim Teilmodul $R^{k\times 1} \cong T$ als auch bei $R^{n\times 1} \cong M$ Basistransformationen vornehmen.

Bemerkung 6.4.5:

Sei R ein Ring kmE.

(1) Die Beschreibung von Homomorphismen von freien R-Moduln in freie R-Moduln (alle e.e.) geschieht wie bei VRen durch Matrizen bzgl. Basen.

(2) Automorphismen von freien R-Moduln (vom Rang n) werden durch invertierbare quadratische Matrizen in

$$\mathrm{GL}_n(R) := (R^{n\times n})^* = \{A \in R^{n\times n} \mid \det A \in R^*\}$$

beschrieben, der **generellen linearen Gruppe über R**.

Sei nun R ein HIB.

(3) Für $a, b \in R \setminus \{0\}$ mit $\mathrm{ggT}(a,b) =: d$ gibt es $s, t \in R$ mit $sa + tb = d$.
Es gilt

$$\mathrm{U}_{(a,b)} := \begin{pmatrix} s & t \\ -\frac{b}{d} & \frac{a}{d} \end{pmatrix} \in \mathrm{GL}_2(R)$$

$$\Rightarrow \mathrm{U}_{(a,b)} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$$

Hauptsatz 6.4.6: Strukturssatz für R-Moduln

Sei R ein HIB und $C \in R^{k\times n}$. Dann existieren $A \in \mathrm{GL}_k(R)$ und $B \in \mathrm{GL}_n(R)$, sodass

$$ACB = \left(\begin{array}{c|c} \operatorname{Diag}(d_1, \ldots, d_l) & 0 \\ \hline 0 & 0 \end{array}\right) = \left(\begin{array}{ccc|c} d_1 & 0 & \cdots & 0 & \\ 0 & d_2 & \ddots & \vdots & 0 \\ \vdots & \ddots & \ddots & 0 & \\ 0 & \cdots & 0 & d_l & \\ \hline & 0 & & & 0 \end{array}\right) \in R^{k\times n}$$

mit $d_i \in R \setminus \{0\}$, $l \leq \min\{k, n\}$ und $d_i \mid d_{i+1}$ für $i \in \underline{(l-1)}$.
Die Matrix ACB nennt man **Smith-Normalform** (SNF).

Beweis zu 6.4.6:
Setze $C_1 := C$. Wir führen invertierbare Zeilenoperationen durch und erhalten $C_2 := A_1C_1$, $C_3 := A_2C_2$, …, $C_r := A_{r-1}C_{r-1}$, sodass die erste Spalte von C_r gleich $(d, 0, \ldots, 0)^{\mathrm{tr}} \in R^{k\times 1}$. Dabei sind A_i Permutationsmatrizen (Ver_k) oder der Form

$$\begin{pmatrix} \mathrm{U}_{(a,b)} & 0 \\ 0 & \mathrm{I}_{k-2} \end{pmatrix} \in R^{k\times k}$$

wenn die obersten 2 Einträge der Spalte a, b der jeweils ersten Spalte von C_i von Null verschieden sind.
BEACHTE: d ist der größte gemeinsame Teiler aller Einträge der ersten Spalte von C_1.
Danach führen wir invertierbare Spaltenoperationen durch und erhalten $C_{r+1} := C_rB_1$, …, $C_{r+s} := C_{r+s-1}B_s$, sodass die erste Zeile von C_{r+s} gleich $(d', 0, \ldots, 0)$ ist. Dabei sind die B_is Permutationsmatrizen (Ver_n) oder von der Form

$$\begin{pmatrix} \mathrm{U}_{(a,b)}^{\mathrm{tr}} & 0 \\ 0 & \mathrm{I}_{n-2} \end{pmatrix} \in R^{k\times k}$$

wenn die ersten 2 Einträge a, b der jeweils ersten Zeile von C_i von Null verschieden sind. Klar: $d' \mid d$
Aber leider ist die erste Spalte von C_{r+s} eventuell wieder verschmutzt und wir müssen die Zeilenoperationen wiederholen. Da aber R keine echten Teilerketten besitzt, hat man nach endlich vielen Schritten t eine Matrix der Form

$$C_t = \left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & C' \end{array}\right)$$

Rekursives Anwenden der Methode auf C' liefert nach endlich vielen Schritten Matrizen

$$A' \in \mathrm{GL}_k(R),\ B' \in \mathrm{GL}_n(R)$$

sodass

$$C' = A'CB' = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_l & \\ \hline & 0 & & 0 \end{array}\right)$$

mit $d_i \in R \setminus \{0\}$.
Sollte für ein i noch die Bedingung $d_i \mid d_{i+1}$ verletzt sein, sind noch weitere Umformungen notwendig: Berechne im betroffenen Teil der Matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d_i & 0 \\ 0 & d_{i+1} \end{pmatrix} = \begin{pmatrix} d_i & d_{i+1} \\ 0 & d_{i+1} \end{pmatrix}$$

Also erhält man eine Matrix, die man mit anfänglicher Methode wieder auf die Form

$$\begin{pmatrix} \mathrm{ggT}(d_i, d_{i+1}) & 0 \\ 0 & \mathrm{kgV}(d_i, d_{i+1}) \end{pmatrix}$$

transformieren kann.
Nach endlich vielen Schritten haben wir unser Ziel erreicht. □

Übung 6.4.Ü1: SNF ÜBER EUKLIDISCHEN BEREICHEN

Für Matrizen über Euklidischen Bereichen kann man einen anderen Algorithmus verwenden, der immer Elemente mit dem größten v-Wert abbaut.

Beispiel 6.4.7:

Sei $R = \mathbb{Z}$ und $A = \begin{pmatrix} 6 & 2 \\ 8 & 7 \end{pmatrix} \in \mathbb{Z}^{2\times 2}$.

$\mathrm{ggT}(6,8) = 2$

$U_1 := \mathrm{U}_{(6,8)} = \begin{pmatrix} -1 & 1 \\ -4 & 3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$

$U_1 A = \begin{pmatrix} 2 & 5 \\ 0 & 13 \end{pmatrix}$

$\mathrm{ggT}(2,5) = 1$

$W_1 := \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$

$U_1 A W_1 = \begin{pmatrix} 1 & 0 \\ -13 & 26 \end{pmatrix}$

$U_2 := \begin{pmatrix} 1 & 0 \\ 13 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$

$U_2 U_1 A W_1 = \begin{pmatrix} 1 & 0 \\ 0 & 26 \end{pmatrix}$

und $1 \mid 26$. ✓

Definition 6.4.A1: Bézout-Ring

Sei R ein IB. R heißt **Bézout-Ring**, falls für $a, b \in R$ immer ein $d \in R$ existiert, sodass $\langle a, b\rangle = \langle d\rangle$.

Bemerkung 6.4.A2: Bézout-Identitäten

(1) Sei R ein IB. R ist genau dann ein Bézout-Ring, wenn es für alle $a, b \in R$ eine **Bézout-Identität** gibt, d.h. $\exists s, t \in R:\ \mathrm{ggT}(a,b) = sa + tb$. Es gilt dann $\langle a, b\rangle = \langle \mathrm{ggT}(a,b)\rangle$.

(2) Jeder HIB ist ein Bézout-Ring.

Man kann alles, was wir bisher für HIB definiert haben, auch in beliebigen Bézout-Ringen anwenden.

Beispiel 6.4.8: Simultane Kongruenzen

Die simultanen Kongruenzen

$$x_1 + x_2 \equiv 0 \mod \mathbb{Z}$$
$$x_1 - x_2 \equiv \frac{1}{4} \mod \mathbb{Z}$$

sind für $x_1, x_2 \in \mathbb{R}$ zu lösen.
Wir schreiben dies als erweiterte Matrix:

$$Ax \equiv b \mod \mathbb{Z}$$
$$\left(\begin{array}{cc|c} 1 & 1 & 0 \\ 1 & -1 & \frac{1}{4} \end{array}\right)$$

und führen Zeilenumformungen auf die erweiterte Matrix (die wir uns nicht merken müssen) und Spaltenumformungen *auf den linken Teil* („Hauptteil“) der Matrix, die wir uns aber merken müssen, aus.

$$\begin{aligned} & Ax \equiv b \mod \mathbb{Z} \\ \Leftrightarrow\ & UAx \equiv Ub \mod \mathbb{Z} \\ \Leftrightarrow\ & \underbrace{UAW}_{=:D} \underbrace{\left(W^{-1}x\right)}_{\substack{=:y \\ \Leftrightarrow x = Wy}} \equiv Ub \mod \mathbb{Z} \end{aligned}$$

$$W = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

$$\left(\begin{array}{cc|c} 1 & 1 & 0 \\ 1 & -1 & \frac{1}{4} \end{array}\right) \overset{U}{\rightsquigarrow} \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & -2 & \frac{1}{4} \end{array}\right) \overset{W}{\rightsquigarrow} \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 2 & \frac{1}{4} \end{array}\right)$$

Zu lösen:

$$Dy \equiv Ub \mod \mathbb{Z}$$
$$y_1 \equiv 0 \mod \mathbb{Z}$$
$$2y_2 \equiv \frac{1}{4} \mod \mathbb{Z}$$
$$y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad Ub = \begin{pmatrix} 0 \\ \frac{1}{4} \end{pmatrix}$$ (dass das $= b$, ist Zufall!)
$$y_1 = z_1 \text{ mit } z_1 \in \mathbb{Z},$$
$$2y_2 - \frac{1}{4} = z_2 \text{ mit } z_2 \in \mathbb{Z}$$
$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} z_1 \\ \frac{1}{8} + \frac{z_2}{2} \end{pmatrix} \text{ mit } z_1, z_2 \in \mathbb{Z}$$

Die endgültige Lösung ist

$$x = Wy = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} z_1 \\ \frac{1}{8} + \frac{z_2}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{8} + z_1 + \frac{1}{2}z_2 \\ -\frac{1}{8} - \frac{1}{2}z_2 \end{pmatrix} \text{ mit } z_1, z_2 \in \mathbb{Z}$$

Beispiel 6.4.9: Lineare Differentialgleichungssysteme mit konstanten Koeffizienten

Lineare DGL-Systeme mit konstanten Koeffizienten erweisen sich als Kongruenzensysteme über $\mathbb{R}[x]$ oder $\mathbb{C}[x]$. Solange die rechte Seite Null ist, ist keine aufwändige Analysis notwendig. Im inhomogenen Fall braucht man aus der Analysis die Methode der Variation der Konstanten.

Seien x_1, x_2, x_3 unendlich oft diffbare Funktionen auf $\mathbb{R}$, oder Elemente von $\mathbb{R}[[t]]$.
Gesucht sind Lösungen des DGL-Systems:

$$x_1' - x_2' + x_3'' = 0$$
$$x_1 + x_2'' + x_3' = 0$$

x' ist Ableitung von x. In $\mathbb{R}[[x]]$: $\left(\sum_{i=1}^{\infty} a_i x^i\right)' = \sum_{i=1}^{\infty} i a_i x^{i-1}$ (gliedweise)

In Matrizen:

$$Cx = C\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \text{ mit } C = \begin{pmatrix} \mathrm{D} & -\mathrm{D} & \mathrm{D}^2 \\ 1 & \mathrm{D}^2 & \mathrm{D} \end{pmatrix}$$

mit $\mathrm{D} \in \mathbb{R}[\mathrm{D}]$, wobei D auf x_i wie die Ableitung nach t wirkt: $\mathrm{D}x_i = x_i'$

$$Cx = 0 \Leftrightarrow UCW\underbrace{\left(W^{-1}x\right)}_{=y} = 0$$

$$\begin{pmatrix} \mathrm{D} & -\mathrm{D} & \mathrm{D}^2 \\ 1 & \mathrm{D}^2 & \mathrm{D} \end{pmatrix} \overset{U}{\rightsquigarrow} \begin{pmatrix} 1 & -\mathrm{D}^2 & \mathrm{D} \\ 0 & -\mathrm{D} - \mathrm{D}^3 & 0 \end{pmatrix} \overset{W}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \mathrm{D} + \mathrm{D}^3 & 0 \end{pmatrix}$$

mit $U = \mathrm{Ver}_2(1,2)\mathrm{Add}_2(1,2;\mathrm{D})$ und $W = \begin{pmatrix} 1 & \mathrm{D}^2 & -\mathrm{D} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$\mathrm{D}y = 0,\ \begin{pmatrix} y_1 \\ y_2''' + y_2' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Es gilt (Analysis/Physik):

$$y_2''' + y_2' = \left(y_2'' + y_2'\right)' = 0$$
$$\Leftrightarrow y_2'' + y_2 = a \in \mathbb{R}$$
$$\Leftrightarrow y_2 = a + b\sin t + c\cos t,\ b, c \in \mathbb{R} \text{ (harmonischer Oszillator)}$$

Somit folgt für unser y:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0 \\ a + b\sin t + c\cos t \\ f(t) \end{pmatrix}$$
$$\Rightarrow x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = Wy = \begin{pmatrix} b\sin t + c\cos t - f'(t) \\ a + b\sin t + c\cos t \\ f(t) \end{pmatrix}$$

wobei $f(t) \in \mathbb{R}[[t]]$ beliebig.

Hauptsatz 6.4.10: Hauptsatz über endlich erzeugte R-Moduln

Sei R ein HIB.

(1) Ist M endlich erzeugter R-Modul, so gibt es $s,t \in \mathbb{Z}_{\geq 0}$ und $d_1,\dots,d_t \in R \setminus (R^* \cup \{0\})$ mit $d_i \mid d_{i+1}$ $\forall i \in \underline{(t-1)}$, sodass

$$M \underset{R}{\cong} R^{s\times 1} \oplus \bigoplus_{i=1}^{t} R/Rd_i$$

(2) Gilt

$$R^{s\times 1} \oplus \bigoplus_{i=1}^{t} R/Rd_i \underset{R}{\cong} R^{s'\times 1} \oplus \bigoplus_{i=1}^{t'} R/Rd'_i$$

mit $s,t,s',t' \in \mathbb{Z}_{\geq 0}$ und $d_1,\dots,d_t,d'_1,\dots,d'_{t'} \in R \setminus (R^* \cup \{0\})$ mit $d_i \mid d_{i+1}$ $\forall i \in \underline{(t-1)}$ und $d'_i \mid d'_{i+1}$ $\forall i \in \underline{(t'-1)}$, so gilt $s' = s$ und $t' = t$ und $d_i \sim d'_i$ $\forall i \in \underline{(t-1)}$.

Man nennt $s =: \mathrm{Rang}(M)$ den **Rang** (genauer: **torsionsfreier Rang**) von M und die d_i sind die **Elementarteiler** von M.

Beweis zu 6.4.10:

(1) Folgt sofort aus den vorangegangenen Lemmata und Satz 6.4.6:

M bis auf Isomorphie gegeben als Faktormodul $R^{k\times 1}/N$, wobei der Teilmodul $N \leq R^{k\times 1}$ durch die Spalten einer $k \times n$-Matrix C gegeben ist ($C \in R^{k\times n}$, n beliebig).

Invertierbare Spaltenumformungen von C sind Übergänge zu anderen EZS der Teilmoduln N. Invertierbare Zeilenumformungen von C sind Übergänge zu anderen Basen von $R^{k\times 1}$.

Sei D die Smith-Normalform von C. Dann gilt:

$$\begin{aligned} M &\cong R^{k\times 1}/\langle C_{-,1},\dots,C_{-,n}\rangle \cong R^{k\times 1}/\langle D_{-,1},\dots,D_{-,n}\rangle \\ &\cong \underbrace{R/Rd_1 \oplus \cdots \oplus R/Rd_t}_{\cong \mathrm{T}(M)} \oplus \underbrace{R \oplus \cdots \oplus R}_{s} \\ &\cong \bigoplus_{i=1}^{t} {}_R R/Rd_i \oplus R^{s\times 1} \end{aligned}$$

mit $d_i \in R \setminus (R^* \cup \{0\})$.

□

Übung 5.2.ii:

Sei $B := \begin{pmatrix} 2 & \cdot & \cdot & \cdot \\ \cdot & 3 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \in \mathbb{Z}^{5\times 4}$, $M := \langle B_{-,1}, \ldots, B_{-,4} \rangle \leq \mathbb{Z}^{5\times 1}$.

Da $2 \nmid 3 \nmid 1$, berechnet sich die SNF von B folgendermaßen:

$$\rightsquigarrow \begin{pmatrix} \mathrm{ggT}(2,3) & \cdot & \cdot & \cdot \\ \cdot & \mathrm{kgV}(2,3) & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 6 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \mathrm{ggT}(6,1) & \cdot & \cdot \\ \cdot & \cdot & \mathrm{kgV}(6,1) & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 6 & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} = \mathrm{SNF}(B)$$

Nach 6.4.10 gilt also

$$\mathbb{Z}^{5\times 1} \big/ M \cong \mathbb{Z}^{5\times 1} \big/ \langle \mathrm{SNF}(B)_{-,1}, \ldots, \mathrm{SNF}(B)_{-,4} \rangle \cong \cancel{\mathbb{Z}}/\cancel{\mathbb{Z}} \oplus \cancel{\mathbb{Z}}/\cancel{\mathbb{Z}} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}^{2\times 1}$$

und der Modul hat damit Rang 2, mit einzigem (echtem) Elementarteiler 6.

Sei im Folgenden R ein HIB.

Korollar 6.4.11:

Sei M ein e.e. R-Torsionsmodul mit $\mathrm{Ann}(M) = \langle d \rangle$. Ist $d \sim \prod_i p_i^{n_i}$ die Faktorisierung von d in Potenzen von Primelementen.
Dann ist M ebenfalls ein Modul über dem Restklassenring

$$R/\mathrm{Ann}(M) = R/\langle d \rangle = R \Big/ \langle \textstyle\prod_i p_i^{n_i} \rangle,$$

der sich nach dem chinesischen Restsatz wie folgt zerlegt:

$$R/\langle d \rangle \cong \bigtimes_i R \Big/ \langle p_i^{n_i} \rangle$$

und entsprechend zerlegt sich M nach 6.2.11 als

$$M \cong \bigoplus_i \left(R \Big/ \langle p_i^{n_i} \rangle \right) M = \bigoplus_i M \Big/ p_i^{n_i} M$$

und $M/p_i^{n_i} M$ ist ein $R/\langle p_i^{n_i} \rangle$-Modul.
Ist $p \in R$ prim, so sind die e.e. $R/\langle p^n \rangle$-Moduln durch endliche monoton steigende Folgen a natürlicher Zahlen $\leq n$. Die Folge $a = (a_1, \ldots, a_t)$ liefert den Modul

$${}_R R/_R p^{a_1} \oplus \cdots \oplus {}_R R/_R p^{a_t} = \bigoplus_{i=1}^{t} {}_R R/_R p^{a_i}$$

Beispiel 6.4.12:

Sei $M = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z} = \mathrm{T}(M)$ ein $\mathbb{Z}$-Torsionsmodul.
Dann ist $\mathrm{Ann}(M) = \langle 24 \rangle$ und M ist ein Modul über dem Restklassenring

$$\mathbb{Z}/\mathrm{Ann}(M) = \mathbb{Z}/\langle 24 \rangle \underset{\text{chin. Rs.}}{\cong} \mathbb{Z}/\langle 3 \rangle \times \mathbb{Z}/\langle 8 \rangle$$

Entsprechend zerlegt sich M als

$$\begin{aligned}
&\left(\mathbb{Z}/\langle 3 \rangle\right) M \oplus \left(\mathbb{Z}/\langle 8 \rangle\right) M = M/3M \oplus M/8M \\
&= \mathbb{Z}/(3\mathbb{Z}+3\mathbb{Z}) \oplus \mathbb{Z}/(6\mathbb{Z}+3\mathbb{Z}) \oplus \mathbb{Z}/(24\mathbb{Z}+3\mathbb{Z}) \\
&\quad \oplus \mathbb{Z}/(3\mathbb{Z}+8\mathbb{Z}) \oplus \mathbb{Z}/(6\mathbb{Z}+8\mathbb{Z}) \oplus \mathbb{Z}/(24\mathbb{Z}+8\mathbb{Z}) \\
&= \overset{\mathrm{ggT}(3,3)}{\mathbb{Z}/3\mathbb{Z}} \oplus \overset{\mathrm{ggT}(3,6)}{\mathbb{Z}/3\mathbb{Z}} \oplus \overset{\mathrm{ggT}(3,24)}{\mathbb{Z}/3\mathbb{Z}} \oplus \overset{\{0\}}{\cancel{\mathbb{Z}/1\mathbb{Z}}} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}
\end{aligned}$$

Korollar 6.4.13:

Sei M ein e.e. torsionsfreier R-Modul.
Dann ist M frei (von endlichem Rang).

Vgl. Hauptsatz: $M = \underbrace{R^{n\times 1}}_{\text{frei}} \oplus \cancel{R/Rd_1 \oplus \cdots \oplus R/Rd_t}$ (torsionsfrei)

Dies ist für $R = \mathbb{Z}[x]$ falsch (kein HIB):
Betrachte $\langle 2, x \rangle_R \leq R$. Dieser Teilmodul ist torsionsfrei, aber nicht frei (s. Homomorphiesatz).

Dies ist ebenfalls falsch für nicht e.e. R-Moduln!
Ist z.B. $R = \mathbb{Z}$, so ist $\mathbb{Q}$ ein torsionsfreier $\mathbb{Z}$-Modul. Jedoch ist $\mathbb{Q}$ nicht frei.
Denn je zwei rationale Zahlen $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ erlauben eine nicht-triviale $\mathbb{Z}$-Linearkombination der Null:

$$(cb)\frac{a}{b} - (da)\frac{c}{d} = 0 \quad \text{(mit } a,b,c,d \in \mathbb{Z}\text{)}$$

Korollar 6.4.14:

Sei R ein HIB mit $K := \mathrm{Quot}(R) \neq R$.
Dann ist K ein nicht e.e. torsionsfreier R-Modul.

Beweis zu 6.4.14:
K ist R-Modul via $r \cdot \frac{a}{b} := \frac{ra}{b}$ für $a, b, r \in R$.
K ist torsionsfrei:

$$\frac{a}{b} \in \mathrm{T}(K) \Rightarrow \exists t \in R \setminus \{0\} : t\frac{a}{b} = \frac{ta}{b} = 0 = \frac{0}{b} \Rightarrow bta = 0 \Rightarrow a = 0 \Rightarrow \frac{a}{b} = 0$$

$\Rightarrow \mathrm{T}(K) = \{0\}$
K ist nicht e.e., denn, angenommen, $K = \left\langle \frac{a_1}{b_1}, \ldots, \frac{a_k}{b_k} \right\rangle_R$.

$$\Rightarrow \forall \kappa \in K : \kappa = r_1\frac{a_1}{b_1} + \cdots + r_k\frac{a_k}{b_k} = \frac{r_1a_1b_2\cdots b_k + \cdots + r_ka_kb_1\cdots b_{k-1}}{b_1\cdots b_k} = r \cdot \frac{1}{b_1\cdots b_k} \in \left\langle \frac{1}{b_1\cdots b_k} \right\rangle$$

$$\Rightarrow K = \left\langle \frac{1}{b_1\cdots b_k} \right\rangle_R$$

$$\overset{6.4.10}{\Longrightarrow} K \cong R$$

und mit $R \subseteq K \Rightarrow R = K$ ↯ zur Annahme $K \neq R$. □

Übung 5.4.iii:

Sei K ein Körper, $R := K[x]/\langle x^5 \rangle$.
GESUCHT: Alle e.e. R-Moduln, die als K-VR Dimension 5 haben.
$K[x]$ ist HIB, $x \in K[x]$ ist prim.
Nach 6.4.11 gilt: Alle e.e. $K[x]/\langle x^5 \rangle$-Moduln sind von der Form

$$\bigoplus_{i=1}^{k}{}_{K[x]} K[x]/\langle x^{a_i} \rangle \text{ , } a_i \leq 5 \text{ monoton steigend, } k \in \mathbb{N}$$

$$K[x]/\langle x^i \rangle \cong \{a_{i-1}x^{i-1} + \cdots + a_1 x^1 + a_0 \mid a_i \in K\} = \langle x^{i-1}, \ldots, x^1, x^0 \rangle_K$$

als K-VR-Isomorphismus. (z.B. $\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{R}[x]_{\text{Grad}<2}$)

$$\Rightarrow \text{Dim}_K \left({}_{K[x]} K[x]/\langle x^{a_i} \rangle \right) = a_i$$

$$\text{Dim}_K(\mathcal{V} \oplus \mathcal{W}) = \text{Dim}_K \mathcal{V} + \text{Dim}_K \mathcal{W}$$

$\Rightarrow$ Suche alle Partitionen von 5. $\Rightarrow$ Alle e.e. $K[x]/\langle x^5 \rangle$-Moduln, die als K-VRe die Dimension 5 haben, sind isomorph zu:

- $K[x]/\langle x^5 \rangle$
- $K[x]/\langle x^4 \rangle \oplus K[x]/\langle x \rangle$
- $K[x]/\langle x^3 \rangle \oplus K[x]/\langle x^2 \rangle$
- $K[x]/\langle x^3 \rangle \oplus K[x]/\langle x \rangle \oplus K[x]/\langle x \rangle$
- $K[x]/\langle x^2 \rangle \oplus K[x]/\langle x^2 \rangle \oplus K[x]/\langle x \rangle$
- $K[x]/\langle x^2 \rangle \oplus K[x]/\langle x \rangle \oplus K[x]/\langle x \rangle \oplus K[x]/\langle x \rangle$
- $K[x]/\langle x \rangle \oplus K[x]/\langle x \rangle \oplus K[x]/\langle x \rangle \oplus K[x]/\langle x \rangle \oplus K[x]/\langle x \rangle$

6.4.b Hauptsatz über endlich erzeugte Abelsche Gruppen

$\mathbb{Z}$-Moduln sind nichts anderes als Abelsche Gruppen!

$$(A,+), \quad \overset{\in \mathbb{Z}}{z} \cdot \underset{\in A}{a} := \begin{cases} \overbrace{a + \cdots + a}^{z} & z > 0 \\ 0_A & z = 0 \\ -(\underbrace{a + \cdots + a}_{z}) & z < 0 \end{cases}$$

Korollar 6.4.15: HAUPTSATZ ÜBER ENDLICH ERZEUGTE ABELSCHE GRUPPEN

Sei $G = \langle g_1, \ldots, g_n \rangle$ eine e.e. Abelsche Gruppe.
Dann gibt es $r, t \in \mathbb{Z}_{\geq 0}$, $f_1, \ldots, f_r, h_1, \ldots, h_t \in G$ und $d_1, \ldots, d_t \in \mathbb{Z}$ mit $d_i \mid d_{i+1}$ $\forall i \in \underline{(t-1)}$ mit

$$G = \langle f_1 \rangle \times \cdots \times \langle f_r \rangle \times \langle h_1 \rangle \times \cdots \times \langle h_t \rangle = \bigtimes_{i=1}^{r} \langle f_i \rangle \times \bigtimes_{i=1}^{t} \langle h_i \rangle$$

$$\cong \mathbb{Z}^{r \times 1} \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z} \quad = \mathbb{Z}^{r \times 1} \oplus \bigoplus_{i=1}^{t} \mathbb{Z}/d_i\mathbb{Z}$$

Die Abelsche Gruppe G ist genau dann endlich, wenn ihr Rang als $\mathbb{Z}$-Modul Null ist, bzw. sie als $\mathbb{Z}$-Modul ein Torsionsmodul ist. In diesem Fall ist $|G| = d_1 \cdots d_t$ und G ist ein Modul über $\mathbb{Z}/\langle d_t \rangle$ bzw. über $\mathbb{Z}/\langle d_1 \cdots d_t \rangle = \mathbb{Z}/\langle |G| \rangle$.

Korollar 6.4.16:

(1) Sei G eine endliche Abelsche Gruppe der Ordnung $|G| = p_1^{n_1} \cdots p_s^{n_s}$.
Dann ist G ein $\mathbb{Z}\Big/\langle \prod_{i=1}^{s} p_i^{n_i} \rangle$-Modul. Dieser Ring ist nach dem chinesischen Restsatz

$$\cong \bigtimes_{i=1}^{s} \mathbb{Z}\Big/\langle p_i^{n_i} \rangle$$

Dementsprechend lässt sich G eindeutig schreiben als

$$G = \bigoplus_{i=1}^{s} P_i = \bigoplus_{i=1}^{s} G\Big/p_i^{n_i} G$$

wobei $|P_i| = p_i^{n_i}$ ist.

(2) Sei P eine Abelsche Gruppe von Primzahlpotenzordnung $|P| = p^n > 1$ („endliche Abelsche p-Gruppe“). Dann gibt es ein eindeutiges $t \in \mathbb{N}$ und $a_1 \leq \cdots \leq a_t \in \mathbb{N}$ mit $\sum_{i=1}^{t} a_i = n$ und

$$P \cong \mathbb{Z}\Big/p^{a_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}\Big/p^{a_t}\mathbb{Z}$$

Beispiel 6.4.17:

Klassifiziere die Abelschen Gruppen mit 24 Elementen.
→ zerlege 24 als $2^3 \cdot 3^1$ und fange an, die Exponenten zu partitionieren: Wir erhalten 3 Abelsche Gruppen (bis auf Isomorphie).

(1) $\mathbb{Z}/24\mathbb{Z} = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$
entsprechend der Partitionen $3 = 3,\ 1 = 1$

(2) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$
entsprechend der Partitionen $3 = 1 + 2,\ 1 = 1$, und die Isomorphie wegen

$$\begin{pmatrix} 2 & \cdot & \cdot \\ \cdot & 4 & \cdot \\ \cdot & \cdot & 3 \end{pmatrix} \overset{\text{SNF}}{\rightsquigarrow} \begin{pmatrix} 1 & \cdot & \cdot \\ \cdot & 2 & \cdot \\ \cdot & \cdot & 12 \end{pmatrix} \quad (\text{und } \mathbb{Z}/1\mathbb{Z} = \{0\})$$

(3) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
entsprechend der Partitionen $3 = 1 + 1 + 1,\ 1 = 1$, und die Isomorphie wegen

$$\begin{pmatrix} 2 & \cdot & \cdot & \cdot \\ \cdot & 2 & \cdot & \cdot \\ \cdot & \cdot & 2 & \cdot \\ \cdot & \cdot & \cdot & 3 \end{pmatrix} \overset{\text{SNF}}{\rightsquigarrow} \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 2 & \cdot & \cdot \\ \cdot & \cdot & 2 & \cdot \\ \cdot & \cdot & \cdot & 6 \end{pmatrix}$$

Übung 5.4.i:

Seien $p,q,r \in \mathbb{N}$ paarweise verschiedene Primzahlen und $n := p^3q^2r$.
GESUCHT: Alle Abelsche Gruppen mit Ordnung n.
Nach 6.4.16.(1) ist jede Abelsche Gruppe G der Ordnung n ein $\mathbb{Z}/\langle n\rangle \cong \mathbb{Z}/\langle p^3\rangle \times \mathbb{Z}/\langle q^2\rangle \times \mathbb{Z}/\langle r\rangle$-Modul, und damit

$$G = {}^{G}/_{p^3G} \oplus {}^{G}/_{q^2G} \oplus {}^{G}/_{rG}$$

mit $\left|G/p^3G\right| = p^3$, $\left|G/q^2G\right| = q^2$, $\left|G/rG\right| = r$.
Für diese gilt nach 6.4.16.(2) allerdings dann, dass

$$\begin{aligned} G/_{p^3G} &\cong \mathbb{Z}/_{p^3\mathbb{Z}} \text{ oder } \cong \mathbb{Z}/_{p^2\mathbb{Z}} \oplus \mathbb{Z}/_{p\mathbb{Z}} \text{ oder } \cong \bigoplus_{i=1}^{3} \mathbb{Z}/_{p\mathbb{Z}} \\ G/_{q^2G} &\cong \mathbb{Z}/_{q^2\mathbb{Z}} \text{ oder } \cong \mathbb{Z}/_{q\mathbb{Z}} \oplus \mathbb{Z}/_{q\mathbb{Z}} \\ G/_{rG} &\cong \mathbb{Z}/_{r\mathbb{Z}} \end{aligned}$$

Bis auf Isomorphie haben alle Abelsche Gruppen der Ordnung n also eine der folgenden $3 \cdot 2 = 6$ Formen:

- $\mathbb{Z}/_{p^3\mathbb{Z}} \oplus \mathbb{Z}/_{q^2\mathbb{Z}} \oplus \mathbb{Z}/_{r\mathbb{Z}}$
- $\mathbb{Z}/_{p^2\mathbb{Z}} \oplus \mathbb{Z}/_{p\mathbb{Z}} \oplus \mathbb{Z}/_{q^2\mathbb{Z}} \oplus \mathbb{Z}/_{r\mathbb{Z}}$
- $\mathbb{Z}/_{p\mathbb{Z}} \oplus \mathbb{Z}/_{p\mathbb{Z}} \oplus \mathbb{Z}/_{p\mathbb{Z}} \oplus \mathbb{Z}/_{q^2\mathbb{Z}} \oplus \mathbb{Z}/_{r\mathbb{Z}}$
- $\mathbb{Z}/_{p^3\mathbb{Z}} \oplus \mathbb{Z}/_{q\mathbb{Z}} \oplus \mathbb{Z}/_{q\mathbb{Z}} \oplus \mathbb{Z}/_{r\mathbb{Z}}$
- $\mathbb{Z}/_{p^2\mathbb{Z}} \oplus \mathbb{Z}/_{p\mathbb{Z}} \oplus \mathbb{Z}/_{q\mathbb{Z}} \oplus \mathbb{Z}/_{q\mathbb{Z}} \oplus \mathbb{Z}/_{r\mathbb{Z}}$
- $\mathbb{Z}/_{p\mathbb{Z}} \oplus \mathbb{Z}/_{p\mathbb{Z}} \oplus \mathbb{Z}/_{p\mathbb{Z}} \oplus \mathbb{Z}/_{q\mathbb{Z}} \oplus \mathbb{Z}/_{q\mathbb{Z}} \oplus \mathbb{Z}/_{r\mathbb{Z}}$

Übung 5.4.ii:

GESUCHT: Alle Abelschen Gruppen der Ordnung 3125.
Da $3125 = 5^5$, haben die Abelschen Gruppen dieser Ordnung eine der folgenden 7 Formen:

- $\mathbb{Z}/_{3125\mathbb{Z}}$
- $\mathbb{Z}/_{625\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}}$
- $\mathbb{Z}/_{125\mathbb{Z}} \oplus \mathbb{Z}/_{25\mathbb{Z}}$
- $\mathbb{Z}/_{125\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}}$
- $\mathbb{Z}/_{25\mathbb{Z}} \oplus \mathbb{Z}/_{25\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}}$
- $\mathbb{Z}/_{25\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}}$
- $\mathbb{Z}/_{5\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}} \oplus \mathbb{Z}/_{5\mathbb{Z}}$

Korollar 6.4.18: ELEMENTORDNUNG

Sei G eine endliche Abelsche Gruppe und $a \in G$.
Das $n \in \mathbb{N}$ mit $\langle n\rangle = \mathrm{Ann}_{\mathbb{Z}}(a)$ nennt man **Ordnung von a**.

Es gilt $\mathrm{ord}(a) = |\langle a\rangle|$ und $\mathrm{ord}(a) \,\big|\, |G|$.

Existiert ein $a \in G$, sodass $G = \langle a\rangle$, so heißt G **zyklische Gruppe**.
$\mathrm{C}_m := \left(\mathbb{Z}/m\mathbb{Z}, +\right)$ ist bis auf Isomorphie die einzige zyklische Gruppe der Ordnung $m \in \mathbb{Z}_{\geq 0}$.

Wir wollen unsere Ergebnisse jetzt auf Einheitengruppen von Restklassenringen $\mathbb{Z}/\langle m\rangle$ von $\mathbb{Z}$ anwenden.

$$\left(\mathbb{Z}/\langle m\rangle\right)^* = \left\{a + m\mathbb{Z} \,\middle|\, a \in \underline{(m-1)},\ \mathrm{ggT}(a,m) = 1\right\}$$

Definition 6.4.19: Die Eulersche φ-Funktion

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N},\ n \longmapsto \left|\left(\mathbb{Z}/\langle n\rangle\right)^*\right|$$

Bemerkung 6.4.20:

(1) **Kleiner Fermat'scher Satz**
Sei $p \in \mathbb{Z}$ Primzahl.

$$\Rightarrow \varphi(p) = \left|\left(\mathbb{Z}/\langle p\rangle\right)^*\right| = p - 1$$

Insbesondere gilt für $a \in \mathbb{Z}$, dass $a^p \equiv a \mod p$ ($\Leftrightarrow a^{p-1} \equiv 1 \mod p$).

(2) Ist p eine Primzahl, so ist

$$\left(\mathbb{Z}/p^n\mathbb{Z}\right)^* = \mathbb{Z}/p^n\mathbb{Z} \setminus p\left(\mathbb{Z}/p^n\mathbb{Z}\right)$$

also $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

(3) Ist $m = \prod_{j=1}^{s} p_j^{\alpha_j}$ mit paarweise verschiedenen Primzahlen p_j und $\alpha_j \in \mathbb{N}$, dann ist

$$\mathbb{Z}/\langle m\rangle = \bigtimes_{j=1}^{s} \mathbb{Z}\Big/\left\langle p_j^{\alpha_j}\right\rangle$$

nach dem chinesischen Restsatz also auch

$$\left(\mathbb{Z}/\langle m\rangle\right)^* = \bigtimes_{i=1}^{s}\left(\mathbb{Z}\Big/\left\langle p_i^{\alpha_i}\right\rangle\right)^*$$

(4) Ist m wie oben, so ist $\varphi(m) = \varphi\left(p_1^{\alpha_1}\right)\cdots\varphi\left(\varphi_s^{\alpha_s}\right) = \prod_{j=1}^{s} p_j^{\alpha_{j-1}}\left(p_j - 1\right)$

φ effizient (ohne Primzerlegung) auszurechnen, ist ein bisher ungelöstes Problem.

d	1	2	3	4	6	12	$\sum$
$\varphi(d)$	1	1	2	2	2	4	12

Lemma 6.4.21:

Sei $m \in \mathbb{N}$. Dann gilt: $\sum_{d|m} \varphi(d) = m$

Beweis zu 6.4.21:
Sei $m = \prod_{j=1}^{s} p_j^{\alpha_j}$. Führe Induktion über $n := \sum_{j=1}^{s} \alpha_j$.
Fall $n = 1$: m ist Primzahl.

$$\Rightarrow \varphi(1) + \varphi(p) = 1 + (p-1) = p$$

Induktionsschritt:

$$\sum_{d|m} \varphi(d) = \underbrace{\sum_{d\left|\frac{m}{p_1}\right.} \varphi(d)}_{\frac{m}{p_1}\text{ (IV)}} + \underbrace{\sum_{d\left|\frac{m}{p_1^{\alpha_1}}\right.} \varphi\left(p_1^{\alpha_1} d\right)}_{\varphi\left(p_1^{\alpha_1}\right)\varphi(d)} = \frac{m}{p_1} + p_1^{\alpha_1 - 1}(p_1 - 1)\cdot\frac{m}{p_1^{\alpha_1}} = m$$

□

Satz 6.4.22:

Sei K ein endlicher Körper. Dann ist seine Einheitengruppe K^* zyklisch.

(Es gilt sogar allgemeiner:
Sei K ein Körper und G eine endliche Untergruppe von K^*. Dann ist G zyklisch.

Beweis zu 6.4.22:
Betrachte $(K^*, \cdot)$ als $\mathbb{Z}$-Modul über $z \cdot a := a^z$ für $z \in \mathbb{Z},\ a \in K^*$.
Wir zeigen: Für jeden Teiler d von $|K^*| = |K| - 1$ hat K^* genau $\varphi(d)$ Elemente der Ordnung m.
Denn: Sei $\psi(d) := |\{a \in K^* \mid \operatorname{ord}(a) = d\}|$. Dann gilt mit 6.4.18 die Implikation

$$d \nmid (|K| - 1) \Rightarrow \psi(d) = 0$$

Ist $a \in K^*$ und $\operatorname{ord}(a) = d$, so ist $\langle a \rangle$ die Menge der verschiedenen Nullstellen von $x^d - 1 \in K[x]$.
Die Elemente der Ordnung d in $\langle a \rangle \leq K^*$ sind genau die a^m mit $\operatorname{ggT}(m, d) = 1$.
Aber die Anzahl dieser Elemente ist genau $\varphi(d)$. Also ist $\varphi(d) \leq \psi(d)$.
Mit dem vorherigen Lemma

$$|K| - 1 = \sum_{d \mid (|K|-1)} \varphi(d) \leq \sum_{d \mid (|K|-1)} \psi(d) = |K^*| = |K| - 1$$

$\Rightarrow \varphi(d) = \psi(d)\ \forall d \mid (|K| - 1)$
Insbesondere ist $\psi(|K| - 1) \neq 0$ und $K^* = \langle a \rangle$ für jedes Element a mit $\operatorname{ord}(a) = |K| - 1$. □

Satz 6.4.23:

Sei p eine Primzahl, $\alpha \geq 1$.

(1) Ist $p > 2$, so ist $\left(\mathbb{Z}/\langle p^\alpha \rangle\right)^* \cong \left(\mathbb{Z}/p^{\alpha-1}\mathbb{Z}, +\right) \oplus \left(\mathbb{Z}/(p-1)\mathbb{Z}, +\right)$

(2) Ist $p = 2,\ \alpha \geq 2$, so ist $\left(\mathbb{Z}/\langle 2^\alpha \rangle\right)^* \cong \left(\mathbb{Z}/2\mathbb{Z}\right) \oplus \left(\mathbb{Z}/2^{\alpha-2}\mathbb{Z}\right) \ncong \mathbb{Z}/2^{\alpha-1}\mathbb{Z}$

Beweis zu 6.4.23:
(1) Zeige $\left(\mathbb{Z}/\langle p^\alpha \rangle\right)^*$ ist zyklisch. (Der Rest folgt aus chinesischem Restsatz.)
Mit Hilfe des binomischen Lehrsatzes zeigt man: Ist $\beta \geq 1$ und $b \in \mathbb{Z}$ mit $p \nmid b$, dann ist

$$\left(1 + p^\beta b\right)^p = 1 + p^{\beta+1} \cdot c \text{ mit } c \in \mathbb{Z},\ p \nmid c \qquad (*)$$

$$1 + \underbrace{p p^\beta b}_{p^{\beta+1} b} + p^{>\beta+1}$$

$$1 + p^{\beta+1} \underbrace{\left(b + p^{>0} \cdots\right)}_{p \nmid c}$$

Ist $a \in \mathbb{Z}$ mit $\langle a + p\mathbb{Z} \rangle = \underbrace{\left(\mathbb{Z}/\langle p \rangle\right)^*}_{\mathbb{F}_p^*}$, so ist nach Fermat (oder dem Teilersatz)

$$a^{p-1} = 1 + pb \text{ für ein } b \in \mathbb{Z}$$

Gilt $p \nmid b$, so ist $\langle a + p^\alpha \mathbb{Z} \rangle = \left(\mathbb{Z}/\langle p^\alpha \rangle\right)^*$ wegen $(*)$.
Falls $p \mid b$, dann ersetze a durch $a + b$ und erhalte $\langle a + b + p\mathbb{Z} \rangle = \left(\mathbb{Z}/\langle p^\alpha \rangle\right)^*$ durch $(*)$.

□

Damit haben wir die Struktur der Einheitengruppe von $\mathbb{Z}/\langle m \rangle$ bestimmt, denn dieser Ring ist nach dem chinesischen Restsatz isomorph zu

$$\mathbb{Z}\Big/\langle p_1^{\alpha_1} \rangle \times \cdots \times \mathbb{Z}\Big/\langle p_s^{\alpha_s} \rangle$$

falls $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ eine Primfaktorzerlegung von m ist. Also ist seine Einheitengruppe das direkte Produkt der Einheitengruppen

$$\left(\mathbb{Z}/\langle m \rangle\right)^* \cong \left(\mathbb{Z}\Big/\langle p_1^{\alpha_1} \rangle\right)^* \times \cdots \times \left(\mathbb{Z}\Big/\langle p_s^{\alpha_s} \rangle\right)^*$$

was wir bereits in der letzten Bemerkung gebraucht haben.

7 Normalformen für Matrizen

7.1 Ähnlichkeit von Matrizen

ZIEL: Normalformen von Endomorphismen bzw. von quadratischen Matrizen (als Endomorphismen aufgefasst).

Definition 7.1.1: ÄHNLICHKEIT/KONJUGATION

Sei $\mathcal{V}$ ein e.e. K-VR der Dimension n.

(1) Zwei Endomorphismen $\alpha, \beta \in \mathrm{End}(\mathcal{V})$ heißen **ähnlich** oder **konjugiert** unter $\mathrm{GL}(\mathcal{V})$, falls ein $\gamma \in \mathrm{GL}(\mathcal{V})$ existiert mit

$$\alpha = \gamma \circ \beta \circ \gamma^{-1}$$

d.h. α, β liegen in der selben Bahn unter der Gruppenoperation

$$\begin{aligned} \mathrm{GL}(\mathcal{V}) \times \mathrm{End}(\mathcal{V}) &\longrightarrow \mathrm{End}(\mathcal{V}) \\ (\gamma,\ \alpha) &\longmapsto \gamma \circ \alpha \circ \gamma^{-1} \end{aligned}$$

(2) Zwei Matrizen $A, B \in K^{n\times n}$ heißen **ähnlich** oder **konjugiert** unter $\mathrm{GL}_n(K)$, falls ein $g \in \mathrm{GL}_n(K)$ existiert mit

$$A = gBg^{-1}$$

d.h. A und B sind in der selben Bahn unter der Gruppenoperation

$$\begin{aligned} \mathrm{GL}_n(K) \times K^{n\times n} &\longrightarrow K^{n\times n} \\ (g,\ A) &\longmapsto g \circ A \circ g^{-1} \end{aligned}$$

(3) Sei R ein IB. Zwei Matrizen $A, B \in R^{n\times m}$ heißen **äquivalent** über R, wenn es ein $g \in \mathrm{GL}_n(R)$ und ein $h \in \mathrm{GL}_m(R)$ gibt mit

$$gAh = B \quad \text{bzw.} \quad gAh^{-1} = B$$

d.h. A und B liegen in der selben Bahn unter der Gruppenoperation

$$\begin{aligned} (\mathrm{GL}_n(R) \times \mathrm{GL}_m(R)) \times K^{n\times m} &\longrightarrow K^{n\times m} \\ ((g,h),\ A) &\longmapsto g \circ A \circ h^{-1} \end{aligned}$$

Klar: Äquivalenz und Ähnlichkeit sind Äquivalenzrelationen.

Der Struktursatz 6.4.6 (SNF) kann auch so formuliert werden: Über einem HIB ist jede Matrix äquivalent zu einer Diagonalmatrix, wobei die Diagonaleinträge eine Teilerkette bilden.

Ähnliche Matrizen sind äquivalent. Die Umkehrung ist jedoch falsch.
z.B. ist jede Matrix in $\mathrm{GL}_n(K)$ äquivalent über K zur Einheitsmatrix I_n, aber dies ist i.A. falsch für die Ähnlichkeit:

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \not\sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ für } \mathrm{char}(K) \neq 2$$

Die Matrizen, die einen festen Endomorphismus beschreiben, sind ähnlich (→ Basiswechselformel) und bilden sogar eine Ähnlichkeitsklasse. Umgekehrt sind zwei Endomorphismen genau dann durch dieselbe Matrix beschreibbar (über verschiedenen Basen), wenn sie konjugiert sind.

Bemerkung 7.1.2: Invarianten der Ähnlichkeitsklassen

μ_α, χ_α sind Invarianten der Ähnlichkeitsklassen, aus denen man z.B. die Spur und die Determinante ablesen kann.
Für jedes Polynom $p \in K[x]$ ist

$$\begin{aligned} \mathrm{End}(\mathcal{V}) &\longrightarrow \mathbb{Z}_{\geq 0} \\ \alpha &\longmapsto \mathrm{Dim}(\mathrm{Kern}(p(\alpha))) \end{aligned}$$

eine Invariante.

Bemerkung 7.1.3:

Ist $\mu_\alpha(x) = \prod_{i=1}^{l} p_i^{m_i}$ die Zerlegung des Minimalpolynoms in normierte, paarweise verschiedene Polynome p_i, dann gilt:

(1) Das charakteristische Polynom ist gegeben durch

$$\chi_\alpha = \prod_{i=1}^{l} p_i^{c_i},\ c_i \geq m_i$$

(2) Man hat eine kanonische Zerlegung von $\mathcal{V}$ in die $\boldsymbol{p_i}$**-Haupträume**

$$\mathcal{V}_i = \mathrm{Kern}\left(p_i^{m_i}(\alpha)\right) = \mathrm{Bild}(q_i(\alpha)) \text{ mit } q_i := \prod_{j \neq i} p_j^{m_j}$$

die alle α-invariant sind, und es gilt $\mathcal{V} = \bigoplus_{i=1}^{l} \mathcal{V}_i$.

(3) Die Projektionen der Zerlegung sind gegeben durch

$$\pi_i = (a_i q)(\alpha)$$

wobei $a_i \in K[x]$ mit $1 = a_1 q_1 + \cdots + a_n q_n$.

(4) Für die Dimension der Haupträume gilt:

$$\mathrm{Dim}\left(\mathrm{Kern}\left(p_i^{m_i}\right)\right) = c_i \cdot \mathrm{Grad}(p_i)$$

(wobei c_i die Potenz in χ_α ist)

(5) Im Fall $m_i = 1$ ist $\mathrm{Kern}\left(p_i^{m_i}(\alpha)\right)$ ein $K[x]/\langle p_i \rangle$-VR und aus einer Basis über $K[x]/\langle p_i \rangle$ konstruiert man leicht eine K-Basis, die für die Einschränkung von α auf $\mathcal{V}_i = \mathrm{Kern}\left(p_i^{m_i}(\alpha)\right)$ die Matrix $\mathrm{Diag}\left(\mathrm{M}_{p_i}, \ldots, \mathrm{M}_{p_i}\right)$ liefert, wobei M_{p_i} die Begleitmatrix von p_i ist.
Wichtiger Spezialfall:

$$p_i(x) = x - a_i \text{ für } a_i \in K$$

Dann ist $\mathrm{M}_{p_i} = (a_i)$ und wir haben vorausgesetzt ($m_i = 1$) eine Basis aus Eigenvektoren für den Hauptraum

$$\mathcal{V}_i = \mathrm{E}_{a_i}(\alpha)$$

Erinnerung:
Für $p = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ (normiert und von Grad d in $K[x]$) ist die **Begleitmatrix**

$$\mathrm{M}_p := \begin{pmatrix} 0 & 0 & & \cdots & 0 & -a_0 \\ 1 & 0 & & & & -a_1 \\ 0 & 1 & & & \vdots & \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & 0 & \\ 0 & 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix} \in K^{d\times d}$$

und es gilt $\mu_{\mathrm{M}_p} = p$.

Übung 7.1.Ü1: Vorübung

Sei K ein Körper, $\mathcal{V}$ ein K-VR mit $\mathrm{Dim}\,\mathcal{V} = n \in \mathbb{N}$, $\alpha \in \mathrm{End}(\mathcal{V})$ mit $\mu_\alpha = p^r$ für $p \in K[x]$ irreduzibel, normiert und $r \in \mathbb{N}$.
Dann produziert der Algorithmus zur Berechnung des Minimalpolynoms μ_α einen Vektor $V \in \mathcal{V}$ mit $\mu_{\alpha,V} = \mu_\alpha$.

Beweis:
Wegen $\mu_\alpha = p^r$, $\mu_{\alpha,V} \mid \mu_\alpha \ \forall V \in \mathcal{V}$ und p irreduzibel, gilt im i-ten Schritt des Algorithmus:

(1) $\mu_{\alpha,V_i} = p^{r_i}$, $r_i \le r$.

(2) $\mu_{\alpha,i} = \mathrm{kgV}\left(\mu_{\alpha,V_i}, \mu_{\alpha,V_{i-1}}\right) = \mathrm{kgV}(p^{r_i}, p^{r_{i-1}}) = p^{\max\{r_i, r_{i-1}\}} = p^{r_i} = \mu_{\alpha,V_i}$

$\Rightarrow$ d.h. in jedem Schritt des Algorithmus gilt $\mu_{\alpha,i} = \mu_{\alpha,V_i}$.
Da der Algorithmus terminiert, und im letzten Schritt $\mu_{\alpha,i} = \mu_\alpha$ gilt, existiert also ein $V \in \mathcal{V}$ mit $\mu_{\alpha,V} = \mu_\alpha$.
Dieses V entsteht immer im letzten Schritt (V_i). □

Definition 7.1.4: Zentralisator

Sei $\mathcal{V}$ ein e.e. K-VR der Dimension n und $\alpha \in \mathrm{End}(\mathcal{V})$.
Dann heißt

$$\mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha) := \{\beta \in \mathrm{End}(\mathcal{V}) \mid \beta \circ \alpha = \alpha \circ \beta\} \le \mathrm{End}(\mathcal{V}) \text{ (Unteralgebra)}$$

der **Zentralisator** bzw. die Zentralisatoralgebra von α.
Für $A \in Kn \times n$ ist die Zentralisatoralgebra von A definiert als

$$\mathrm{C}_{K^{n\times n}}(A) := \{X \in K^{n\times n} \mid X\underbrace{A = A}_{\text{„zentral“}}X\}$$

Bemerkung 7.1.5:

$\mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha)$ ist Kern der linearen Selbstabbildung

$$\begin{aligned} \mathrm{End}(\mathcal{V}) &\longrightarrow \mathrm{End}(\mathcal{V}) \\ \gamma &\longmapsto \gamma\circ\alpha - \alpha\circ\gamma \end{aligned}$$

Beispiel 7.1.6:

(1) Ist $A \in K^{2\times 2}$ mit $A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, so ist

$$\mathrm{C}_{K^{n\times n}}(A) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \, a, b \in K \right\}$$

denn (LGS):

$$\begin{pmatrix} a & c \\ d & b \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & c \\ d & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & c \\ 0 & b \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ d & b \end{pmatrix} \qquad = \begin{pmatrix} 0 & c \\ -d & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$\Leftrightarrow c = d = 0$

(2) Für $A := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{2\times 2}$ $(A = \mathrm{M}_{x^2+x+1})$ ist $\mathrm{C}_{\mathbb{F}_2^{2\times 2}}(A) = \mathbb{F}_2[A] \cong \mathbb{F}_4$.

$$\begin{aligned} \varphi_A : \mathbb{F}_2[x] &\longrightarrow \mathbb{F}_2^{2\times 2} \\ x &\longmapsto A \end{aligned}$$

Es ist $\operatorname{Bild}\varphi_A = \mathbb{F}_2[A]$ und $\operatorname{Kern}\varphi_A = \langle x^2+x+1 \rangle = \langle \mu_A \rangle$.

$$\mathbb{F}_2[A] \cong \mathbb{F}_2[x] \Big/ \langle x^2+x+1 \rangle \cong \mathbb{F}_4$$

(3) Betrachtet man die Blockdiagonalmatrix

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & A \end{array}\right) \in \mathbb{F}_2^{4\times 4}$$

so ist ihr Zentralisator isomorph zu $\mathbb{F}_4^{2\times 2}$.

Satz 7.1.7:

Sei $\alpha \in \operatorname{End}(\mathcal{V})$ etc. wie in 7.1.3.
Setze $\mathcal{V}_i := \pi_i(\mathcal{V}) = q_i(\alpha)(\mathcal{V})$, $\alpha_i = \alpha|_{\mathcal{V}_i} : \mathcal{V}_i \to \mathcal{V}_i$.

(1) Für $\beta \in \mathrm{C}_{\operatorname{End}(\mathcal{V})}(\alpha)$ und $1 \le i \ne j \le l$ gilt:

$$\pi_i \circ \beta \circ \pi_j = 0$$

d.h. β respektiert die Zerlegung von $\mathcal{V}$ in Haupträume und somit gilt insbesondere

$$\beta = \sum_{i=1}^{l} \underbrace{\pi_i \circ \beta \circ \pi_i}_{\in \mathrm{C}_{\operatorname{End}(\mathcal{V}_i)}(\alpha_i)}$$

und

$$\mathrm{C}_{\operatorname{End}(\mathcal{V})}(\alpha) = \bigtimes_{i=1}^{l} \mathrm{C}_{\operatorname{End}(\mathcal{V}_i)}(\alpha_i)$$

(2) Sei $\mu_\alpha(x) = \chi_\alpha(x)$, also das MinPoly und das char. Polynom stimmen überein. Dann ist $(\mathrm{id}_\mathcal{V}, \alpha, \ldots, \alpha^{n-1})$ mit $n = \operatorname{Dim}\mathcal{V}$ eine K-VRbasis von $\mathrm{C}_{\operatorname{End}(\mathcal{V})}(\alpha)$ und $\mathrm{C}_{\operatorname{End}(\mathcal{V})}(\alpha) = K[\alpha]$.

Beweis zu 7.1.7:

(1) Da $\beta \in \mathrm{C}_{\operatorname{End}(\mathcal{V})}(\alpha)$ mit α vertauschbar, ist es auch mit jedem Polynom in α vertauschbar, insbesondere

mit den π_is. Damit folgen die ersten Aussagen.

$$\pi_i \circ \beta \circ \pi_j = \underbrace{\pi_i \circ \pi_j}_{=0} \circ \beta$$

Weiter ist $\pi_i \in \mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha)$ für jedes i und als Polynom in α ist π_i mit jedem Element in $\mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha)$ vertauschbar.

Daher ist mit $\mathrm{id}_{\mathcal{V}} = \sum_{i=1}^{l} \pi_i$ auch

$$\mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha) = \bigoplus_{i=1}^{l} \pi_i \mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha)$$

und $\pi_i \mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha) = \mathrm{C}_{\mathrm{End}(\mathcal{V}_i)}(\alpha_i)$.

(2) Aus der Vorübung schließen wir, dass jeder Hauptraum $\mathcal{V}_i$ einen Vektor V_i enthält, dessen MinPoly $\mu_{\alpha_i,V_i} = p_i^{m_i}$ ist. Wegen $\mu_\alpha = \chi_\alpha$ liefert die Summe dieser Vektoren einen Vektor $V := \sum_i V_i$, dessen MinPoly $\mu_{\alpha,V} = \mu_\alpha$ ist.

Unter diesen gegebenen Voraussetzungen ist $\left(V, \alpha(V), \ldots, \alpha^{n-1}(V)\right)$ eine Basis von $\mathcal{V}$.

Sei nun $\beta \in \mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha)$ und $\beta(V) = V' = \sum_{i=0}^{n-1} b_i \alpha^i(V)$ für geeignete $b_i \in K$.

Dann ist $\beta(\alpha(V)) = \alpha\left(\beta(V)\right) = \alpha(V')$ und allgemeiner:

$$\beta\left(\alpha^j(V)\right) = \alpha^j\left(V'\right), \text{ also } \beta\left(\alpha^j(V)\right) = \left(\sum_{i=0}^{n-1} b_i \alpha^i\right)\left(\alpha^j(V)\right)$$

$\Rightarrow \beta = \sum_i b_i \alpha^i$, da $\left(\alpha^0(V), \ldots, \alpha^{n-1}(V)\right)$ ein EZS von $\mathcal{V}$.

□

Übung 7.1.Ü2:

Im Falle $\mu_\alpha = \chi_\alpha$ ist $\mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha)$ als K-Algebra isomorph zu $K[x]/\langle \mu_\alpha \rangle$.

Übung 7.1.Ü3: 7.1.7 für Matrizen

Sei $A \in K^{n\times n}$, $\mu_A(x) = \prod_{i=1}^{l} p_i^{m_i}$ und $\chi_A = \prod_{i=1}^{l} p_i^{c_i}$, $c_i \geq m_i$.

Setze $\mathcal{V}_i := \pi_i\left(K^{n\times 1}\right) = q_i\left(\widetilde{A}\right)\left(K^{n\times 1}\right)$.

(1) Für $B \in \mathrm{C}_{K^{n\times n}}(A)$ und Basis $\mathcal{B}_i$ von $\mathcal{V}_i$ $(i \in \underline{l})$ ist

$$B_i := {}^{\mathcal{B}_i}\widetilde{B}^{\mathcal{B}_i}\big|_{\mathcal{V}_i} \in \mathrm{C}_{K^{d_i\times d_i}}(A_i),\ d_i := \mathrm{Dim}\,\mathcal{V}_i$$

und damit gilt für eine der Zerlegung angepassten Basis $\mathcal{B}$ von $K^{n\times n}$:

$${}^{\mathcal{B}}\widetilde{B}^{\mathcal{B}} = \mathrm{Diag}(B_1, \ldots, B_l)$$
$$\mathrm{C}_{K^{n\times n}}(A) = \left\{\mathrm{Diag}(X_1, \ldots, X_l) \,\middle|\, X_i \in \mathrm{C}_{K^{d_i\times d_i}}(A_i)\right\}$$

(2) Sei $\mu_A = \chi_A$. Dann ist $\left(I_n, A, \ldots, A^{n-1}\right)$ eine K-VRbasis von $\mathrm{C}_{K^{n\times n}}(A)$ und $\mathrm{C}_{K^{n\times n}}(A) = K[A]$.

Die Situation aus 7.1.7.(2) hat einen Namen:

Definition 7.1.8: Zyklischer VR

Sei $\alpha \in \mathrm{End}(\mathcal{V})$. Jeder Vektor $V \in \mathcal{V}$ mit $\langle V \rangle_\alpha := K[\alpha](V) = \mathcal{V}$ heißt **zyklischer Vektor** von $\mathcal{V}$ bzgl. α. Falls ein solcher existiert, heißt $\mathcal{V}$ **zyklischer Vektorraum** bzgl. α.
In Modultheorie: zyklischer $K[x]$-Modul.

Bemerkung 7.1.9:

$\mathcal{V}$ ist genau dann zyklisch bzgl. α, wenn $\mu_\alpha = \chi_\alpha \Leftrightarrow \operatorname{Grad}\mu_\alpha = \operatorname{Dim}\mathcal{V}$.

Beweis zu 7.1.9:

„⇐“: Sei $\mathcal{V}$ zyklisch bzgl. $\alpha \in \operatorname{End}(\mathcal{V})$, d.h. $\exists V \in \mathcal{V} : \mathcal{V} = K[\alpha]V$.

Da $\mathcal{V} = K[\alpha]V$, wähle für den Algorithmus für das Minimalpolynom ebendieses V. Dann gilt sofort:

$$\mathcal{W} := K[\alpha]V = \mathcal{V}$$

somit ist $\mu_{\alpha,V} = \mu_\alpha$.

Es folgt auch, dass man aus $K[\alpha]V$ leicht eine Basis für $\mathcal{V}$ konstruieren kann:

$$\mathcal{V} = \langle V, \alpha(V), \alpha^2(V), \ldots, \alpha^{n-1}(V)\rangle \text{ (linear unabhängig)}, \; n := \operatorname{Dim}\mathcal{V}$$

Im Algorithmus wird $\mu_{\alpha,V}$ konstruiert aus genau diesen basiserzeugenden Polynomen $q_i(x) := x^i$:

$$\mu_{\alpha,V}(x) = \sum_{i=1}^{n} a_i q_i(x) \text{ mit } \sum_{i=1}^{n} a_i q_i(\alpha)(V) = 0$$

Somit ist $\operatorname{Grad}\mu_{\alpha,V} = \max_{i\in\underline{n}}(\operatorname{Grad} q_i) = \operatorname{Grad} q_n = n = \operatorname{Dim}\mathcal{V}$.

Es gilt immer $\operatorname{Grad}\chi_\alpha = \operatorname{Dim}\mathcal{V} = n$ und normiert. Hier ist $\mu_{\alpha,V} = \mu_\alpha$ und μ_α per Definition normiert, und $\mu_\alpha \mid \chi_\alpha$ nach Hamilton-Cayley. Damit ist, zusammen mit dem gleichen Grad, $\mu_\alpha = \chi_\alpha$.

„⇒“: Sei $\mu_\alpha = \chi_\alpha$.

Nach der Vorübung gibt es in jedem p_i-Hauptraum $\mathcal{V}_i$ von $\mathcal{V}$ einen Vektor V_i mit $\mu_{\alpha,V_i} = \mu_{\alpha|_{\mathcal{V}_i}} = p_i^{m_i}$ mit $p_i \in K[x]$ irreduzibel und normiert, $m_i \in \mathbb{N}$.

Sei $V := \sum_{i=1}^{l} V_i \in \bigoplus_{i=1}^{l} \mathcal{V}_i = \mathcal{V}$. Es gilt:

$$0 = \pi_i\left(\mu_{\alpha,V}(\alpha)(V)\right) = \pi_i\Big(\underbrace{\left(a_0V_1 + \cdots + a_k\alpha^k(V_1)\right)}_{\in\mathcal{V}_1} + \cdots + \underbrace{\left(a_0V_l + \cdots + a_k\alpha^k(V_l)\right)}_{\in\mathcal{V}_l}\Big)$$

$$= a_0V_i + \cdots + a_k\alpha^k(\mathcal{V}_i)$$

$$\Rightarrow \mu_{\alpha,V_i} \mid \mu_{\alpha,V} \mid \chi_\alpha = p_1^{m_1}\cdots p_l^{m_l} \;\forall i$$

$$\Rightarrow \mu_\alpha = p_1^{m_1}\cdots p_l^{m_l} \mid \mu_{\alpha,V} \mid \chi_\alpha$$

□

Beispiel 7.1.10:

Sei $A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in K^{2\times 2}$.

Ist $K^{2\times 1}$ ein zyklischer VR bzgl. $\widetilde{A}$?

$$\mu_A = \mu_{\widetilde{A}} = (x-0)(x-1)$$

$$\Rightarrow \operatorname{Grad}\mu_A = \operatorname{Dim}K^{2\times 1} = 2$$

$\Rightarrow$ zyklisch bzgl. $\widetilde{A}$.

Für $B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in K^{3\times 3}$ ist $\mu_B = (x-0)(x-1)$.

$\Rightarrow \operatorname{Grad}\mu_B = 2 \neq \operatorname{Dim}K^{3\times 1} = 3 \Rightarrow$ nicht zyklisch bzgl. $\widetilde{B}$.

7.2 Normalformen für Matrizen

7.2.a Die rationale kanonische Form

Satz 7.2.1:

(1) Jede Matrix $A \in K^{n\times n}$ macht $K^{n\times 1}$ zu einem $K[x]$-Modul, in dem x vermöge A operiert, also durch

$$p(x)V := p(A)V \ \forall V \in K^{n\times 1},\ p \in K[x]$$

Wir bezeichnen ihn mit M_A.

(2) Es ist $\mathrm{Ann}_{K[x]}(M_A) = \langle \mu_A \rangle \trianglelefteq K[x]$ (wenn $\mathrm{Dim}\,\mathcal{V} \neq 0$ sogar $\triangleleft K[x]$) das vom Minimalpolynom von A erzeugte Ideal.

(3) $\mathrm{End}_{K[x]}(\mathrm{M}_A) \cong \mathrm{C}_{K^{n\times n}}(A) = \{X \in K^{n\times n} \mid XA = AX\}$

(4) Für $A, B \in K^{n\times n}$ gilt $\mathrm{M}_A \cong \mathrm{M}_B \Leftrightarrow \exists g \in \mathrm{GL}_n(K):\ A = g^{-1}Bg \overset{\text{also}}{\Longleftrightarrow} A$ und B sind ähnlich.
Ähnlichkeit von Matrizen ist also einfach nur Isomorphie von Moduln!

Beweis zu 7.2.1:

(1) hatten wir schon früher bemerkt.

(2) "

(3) Der $K[x]$-Modul M_A wird durch Einschränkung auf $K \leq K[x]$ zu einem K-Modul, also einem K-VR.
Insbesondere sind alle $K[x]$-Modulhomomorphismen gleichzeitig K-VR-Homomorphismen und somit gegeben durch Multiplikation mit einer Matrix aus $K^{n\times n}$.

Für $X \in K^{n\times n}$ ist die K-lineare Abbildung $\widetilde{X} \overset{!}{\in} \mathrm{End}_{K[x]}(\mathrm{M}_A)$ genau dann, wenn $\widetilde{X}(xV) = x\widetilde{X}(V)\ \forall V \in K^{n\times 1}$, also genau dann, wenn $XAV = AXV\ \forall V \in K^{n\times 1} \Rightarrow XA = AX$. □

(4) Sei $\widetilde{X} : \mathrm{M}_A \xrightarrow{\sim} \mathrm{M}_B$ ein Isomorphismus.
Dann ist insbesondere die K-lineare Abbildung $\widetilde{X}$ bijektiv, also $X \in \mathrm{GL}_n(K)$.
Weiter erfüllt $\widetilde{X}$ die Bedingung $\widetilde{X}(AV) = x\widetilde{X}(V) = B\left(\widetilde{X}(V)\right) \Rightarrow XA = BX \Rightarrow A = X^{-1}BX$.

□

Definition 7.2.2: Charakteristische Matrix

Sei $A \in K^{n\times n}$. Die **charakteristische Matrix** $\mathfrak{X}(A)$ (Fraktur-X) ist definiert als

$$\mathfrak{X}(A) := x\mathrm{I}_n - A \in K[x]^{n\times n}$$

Damit ist $\chi_A = \det(\mathfrak{X}(A)) \in K[x]$.

Satz 7.2.3:

Sei $A \in K^{n\times n}$. Der Kern des $K[x]$-Modulepimorphismus

$$f_A : \underbrace{K[x]^{n\times n}}_{\mathrm{Fr}_{K[x]}(n)} \longrightarrow \underbrace{\mathrm{M}_A}_{\equiv K^{n\times 1}},\ f_A(e_i) = e_i$$

ist der Teilmodul $\mathrm{S}(\mathfrak{X}(A)) \leq K[x]^{n\times 1}$, der frei auf den Spalten von $\mathfrak{X}(A)$ ist (von Rang n).

Beachte: e_i hat zwei Bedeutungen. Als Argument der Funktion f_A ist es die i-te Einheitsspalte in $K[x]^{n\times 1}$ und als Bild die i-te Einheitsspalte in $K^{n\times 1}$.

Beweis zu 7.2.3:

Für $p = \begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} \in K[x]^{n\times 1}$ ist

$$f_A(p) = f_A\left(\sum_i p_i e_i\right) = \sum_i p_i(A) \cdot \underbrace{f_A(e_i)}_{e_i \in K^{n\times 1}} = \sum_i p_i(A) e_i$$

Insbesondere haben wir $\forall 1 \le j \le n:\ f_A(xe_j) = Ae_j = A_{-,j}$ und somit

$$f_A(\underbrace{xe_j - A_{-,j}}_{\mathfrak{X}(A)_{-,j}}) = f_A\left(xe_j - \sum_{i=1}^{n} A_{i,j} e_j\right) = A_{-,j} - A_{-,j} = 0$$

Somit ist die j-te Spalte von $\mathfrak{X}(A)_{-,j} = xe_j - A_{-,j}$ im Kern von $f_A\ \forall 1 \le j \le n$.
Bezeichne mit $N_A := \mathrm{S}(\mathfrak{X}(A))$ diesen Spaltenraum.
Da N_A im Kern von f_A liegt, ist die Abbildung $\overline{f_A} : K[x]^{n\times 1}/N_A \twoheadrightarrow \mathrm{M}_A$ wohldefiniert und weiterhin surjektiv (die K-Dimension von M_A ist n).

BEHAUPTUNG: $(e_1 + N_A, \ldots, e_n + N_A)$ ist ein EZS von $K[x]^{n\times 1}/N_A$.
Dazu sei $p = \begin{pmatrix} p_1(x) \\ \vdots \\ p_n(x) \end{pmatrix} \in K[x]^{n\times 1}$.
Wir zeigen durch Induktion nach $\mathrm{Grad}\, p := \{\mathrm{Grad}\, p_i \mid i \in \underline{n}\}$, dass ein $c \in K^{n\times 1}$ und $C \in N_A$ ex. mit $p = c + C$.
Dies ist klar für $\mathrm{Grad}\, p = 0$, da dann $p = c \in K^{n\times 1}$.
Sonst dividiere alle p_i mit $\mathrm{Grad}\, p_i = \mathrm{Grad}\, p$ sukzessive mit Rest durch $(x - A_{i,i})$, also $p_i = q_i(x - A_{i,i}) + r_i$, und ersetze p durch $p - \underbrace{q_i \mathfrak{X}(A)_{-,i}}_{\in N_A}$.
Da $\mathrm{Grad}\, q_i = \mathrm{Grad}(p_i) - 1$ ist, verringert sich der $\mathrm{Grad}\, p$ nach der sukzessiven Einsetzung um 1 und die Induktionsvoraussetzung greift. □Behauptung.
Also ist die K-Dimension von $K[x]^{n\times 1}/N_A$ höchstens n und somit $\overline{f_A}$ ein Isomorphismus.
Dass N_A frei auf den Spalten von $\mathfrak{X}(A)$ ist, folgt, da $\det(\mathfrak{X}(A)) = \chi_A \neq 0$. □

Korollar 7.2.4: RKF / FROBENIUS-NORMALFORM

Als $K[x]$-Modul ist $\mathrm{M}_A \cong K[x]^{n\times 1}/\mathrm{Kern}\, f_A = K[x]^{n\times 1}/\mathrm{S}(\mathfrak{X}(A))$.
Nach dem Struktursatz 6.4.6 gibt es Matrizen $\mathfrak{g}, \mathfrak{h} \in \mathrm{GL}_n(K[x])$ mit

$$\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}(f_1(x), \ldots, f_n(x))$$

sodass $f_i(x) \in K[x]$ normiert, $f_1(x) \mid f_2(x) \mid \ldots \mid f_n(x)$.
Ist $d_i := \mathrm{Grad}\, f_i$ und $s := \min\{i \in \underline{n} \mid d_i > 0\}$, so ist

$$\chi_A = \det(\mathfrak{X}(A)) = \prod_{i=1}^{n} f_i(x) = \prod_{i=s}^{n} f_i(x)$$
$$\mu_A = f_n(x)$$

und

$$\begin{aligned} \mathrm{M}_A &\underset{K[x]}{\cong} K[x]/\langle f_1(x)\rangle \oplus \cdots \oplus K[x]/\langle f_n(x)\rangle \\ &\cong K[x]/\langle f_s(x)\rangle \oplus \cdots \oplus K[x]/\langle f_n(x)\rangle \\ &\cong \mathrm{M}_{\mathrm{RKF}(A)} \end{aligned}$$

mit $\mathrm{RKF}(A) := \mathrm{Diag}(\mathrm{M}_{f_1}, \ldots, \mathrm{M}_{f_n}) = \mathrm{Diag}(\mathrm{M}_{f_s}, \ldots, \mathrm{M}_{f_n})$, wobei M_{f_i} die Begleitmatrix von f_i bezeichnet (M_{f_i} ist leer, falls $d_i = 0$ ist).
Die f_i sind nach 6.4.10 eindeutig bestimmt (als Elementarteiler von $\mathfrak{X}(A)$).
Die zu A ähnliche Blockdiagonalmatrix $\mathrm{RKF}(A)$ heißt die **rationale kanonische Form** oder auch **Frobenius-Normalform** von A.

Bemerkung 7.2.5:

Sei $\mathrm{RKF}(A) := \mathrm{Diag}(f_s, \dots, f_n)$. Dann ist M_A die direkte Summe von $n-s+1$ zyklische $K[x]$-Moduln $K[x]/\langle f_i \rangle$. Jede solche Zerlegung von M_A hat mindestens ebensoviele zyklische Summanden (sonst hätte man andere Elementarteiler).

Bemerkung 7.2.6: ACHTUNG!

Im Gegensatz zur Hauptraumzerlegung ist die Zerlegung in 7.2.5 nur bis auf Isomorphie eindeutig.

Ist $\alpha = \widetilde{A}$ und sind B, B' Basen von $\mathcal{V} = K^{n\times 1}$ mit ${}^B\alpha^B = \mathrm{Diag}(f_s, \dots, f_n) = {}^{B'}\alpha^{B'}$, so ist der Endomorphismus $\beta \in \mathrm{End}(\mathcal{V})$ mit $\beta(B_i) = B'_i \ \forall i \in \underline{n}$ eine Einheit im Zentralisator von α:

$$\beta \in \mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha)^* = \mathrm{C}_{\mathrm{End}(\mathcal{V})}(\alpha) \cap \mathrm{GL}(\mathcal{V}) =: \mathrm{Aut}_\alpha(\mathcal{V})$$

ist die Menge der **α-Automorphismen** in $\mathcal{V}$.

Korollar 7.2.7: ZUSAMMENFASSUNG:

Seien $A, B \in K^{n\times n}$. Dann sind äquivalent:

(1) A und B sind ähnlich.
(2) $\mathfrak{X}(A)$ und $\mathfrak{X}(B)$ sind ähnlich.
(3) $\mathfrak{X}(A)$ und $\mathfrak{X}(B)$ sind äquivalent über $K[x]$
(4) M_A und M_B sind isomorphe $K[x]$-Moduln ($\mathrm{M}_A \cong_{K[x]} \mathrm{M}_\mathrm{B}$)
(5) A und B haben dieselbe rationale kanonische Form $\mathrm{RKF}(A) = \mathrm{RKF}(B)$
(6) $\mathfrak{X}(A)$ und $\mathfrak{X}(B)$ haben die gleiche Smith-Normalform.

Bemerkung 7.2.8: PRF / WEIERSTRASS-FORM

Sei $A \in K^{n\times n}$ mit Minimalpolynom $\mu_A = \prod_{i=1}^{l} p_i^{m_i}$ und charakteristischem Polynom $\chi_A = \prod_{i=1}^{l} p_i^{c_i}$ und $\mathcal{V}_i = \mathrm{Kern}\left(p_i^{m_i}(A)\right)$ der p_i-Hauptraum.
Dann ist $K^{n\times 1} = \bigoplus_{i=1}^{l} \mathcal{V}_i$ eine $\widetilde{A}$-invariante Zerlegung.
Bezüglich einer an diese Zerlegung angepasste Basis hat $\widetilde{A}$ also eine Matrix $\mathrm{Diag}(A_1, \dots, A_l)$ in Blockdiagonalgestalt.
Ist $\mathrm{RKF}(A_i) = \mathrm{Diag}\left(\mathrm{M}_{p_i^{a_{i,1}}}, \dots, \mathrm{M}_{p_i^{a_{i,s_i}}}\right)$ mit $a_{i,1} \le \dots \le a_{i,s_i} \in \mathbb{N}$, $c_i = a_{i,1} + \dots + a_{i,s_i}$, $m_i = a_{i,s_i}$, so ist A ähnlich zu $\mathrm{PRF}(A) := \mathrm{Diag}\left(\mathrm{RKF}(A_1), \dots, \mathrm{RKF}(A_l)\right) = \mathrm{Diag}\left(\mathrm{M}_{p_1^{a_{1,1}}}, \dots, \mathrm{M}_{p_l^{a_{l,s_l}}}\right)$
$\mathrm{PRF}(A)$ heißt die **primäre rationale Form** oder **Weierstraß-Form** von A.

Beispiel 7.2.9:

Sei $K = \mathbb{Q}$ und $A = \begin{pmatrix} -6 & 6 & 0 & 6 \\ -4 & 6 & -1 & 3 \\ -6 & 12 & -3 & 3 \\ -6 & 12 & -3 & 3 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$.

Dann ist $\mathfrak{X}(A) := \begin{pmatrix} x+6 & -6 & 0 & -6 \\ 4 & x-6 & 1 & -3 \\ 6 & -12 & x+3 & -3 \\ 6 & -12 & 3 & x-3 \end{pmatrix} \in \mathbb{Q}[x]^{4\times 4}$ und $\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}\left(1, 1, x, x^3\right)$, wobei

$$\mathfrak{g} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{24}x + \frac{1}{4} & -\frac{3}{4} & 0 & \frac{1}{4} \\ \frac{1}{6}x^2 - x - 4 & x + 12 & -4 & x \end{pmatrix}$$

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & \frac{1}{4}x + 3 \\ -\frac{1}{2} & 1 & x - 3 & -\frac{1}{4}x^2 + \frac{3}{4}x + 3 \\ -\frac{1}{6} & 0 & 1 & \frac{3}{4}x + 3 \end{pmatrix}$$

Also erhält man $\mathrm{RKF}(A) = \mathrm{PRF}(A) = \mathrm{Diag}(\mathrm{M}_x, \mathrm{M}_{x^3}) = \left(\begin{array}{c|ccc} 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right)$.

(gleich, da wir ein irreduzibles $p = x$ haben)

Beispiel 7.2.10:

Sei $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$. Dann findet man $\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}\left(1, 1, x^3 + x^2 - x + 1\right)$, wobei

$$\mathfrak{g} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ x & x^2 & 1 \end{pmatrix},\ \mathfrak{h} = \begin{pmatrix} 0 & -1 & x+1 \\ 0 & 0 & 1 \\ -1 & -x & x^2 + x - 1 \end{pmatrix}$$

Also ist $p = x^3 + x^2 - x + 1 = \mu_A = \chi_A = (x+1)^2(x-1)$,

$$\mathrm{RKF}(A) = \mathrm{M}_p = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

$$\mathrm{PRF}(A) = \mathrm{Diag}\left(\mathrm{M}_{x-1}, \mathrm{M}_{(x+1)^2}\right) = \mathrm{Diag}(\mathrm{M}_{x-1}, \mathrm{M}_{x^2+2x+1}) = \left(\begin{array}{c|cc} 1 & \cdot & \cdot \\ \hline \cdot & 0 & -1 \\ \cdot & 1 & -2 \end{array}\right)$$

Übung 7.1:

Sei $A := \begin{pmatrix} 1 & 1 & \cdot & \cdot \\ 1 & 1 & 1 & 1 \\ 1 & \cdot & \cdot & 1 \\ \cdot & 1 \cdot & 1 & \end{pmatrix} \in {\mathbb{F}_2}^{4\times 4} \Rightarrow \mathfrak{X}(A) = xI_4 - A \overset{\mathbb{F}_2}{=} xI_4 + A = \begin{pmatrix} x+1 & 1 & \cdot & \cdot \\ 1 & x+1 & 1 & 1 \\ 1 & \cdot & x & 1 \\ \cdot & 1 & \cdot & x+1 \end{pmatrix}$.
Dann findet man $\mathfrak{g}, \mathfrak{h} \in \mathrm{GL}_4(\mathbb{F}_2[x])$, sodass

$$\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}\left(1, 1,\ x+1,\ x^3+x\right)$$

und $1 \mid 1 \mid x+1 \mid x^3+x = (x+1)\left(x^2+x\right)$.

$$\Rightarrow \mathrm{RKF}(A) = \mathrm{Diag}(\mathrm{M}_1,\ \mathrm{M}_1,\ \mathrm{M}_{x+1},\ \mathrm{M}_{x^3+x}) = \mathrm{Diag}(\mathrm{M}_{x+1},\ \mathrm{M}_{x^3+x}) = \left(\begin{array}{c|ccc} 1 & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \end{array}\right)$$

$\chi_A = 1 \cdot 1 \cdot (x+1)\left(x^3+x\right) = x^4+x^2 = (x+1)^3 x$ als Produkt der Elementarteiler und $\mu_A = x^3+x = (x+1)^2$ als letzter Elementarteiler von $\mathfrak{X}(A)$.

Die $\widetilde{A}$-invariante Zerlegung ergibt als einzige mögliche Exponentenfolge für $p_1 := x,\ p_2 := x+1$: $a_{11} := 1,\ a_{21} := 1,\ a_{22} := 2$ ($a_{11} = 1$ einzige Zerlegung von 1, $a_{21} + a_{22} = 3$ (Potenz in χ_A) und $a_{22} = 2$ (Potenz in μ_A)).

$$\Rightarrow \mathrm{PRF}(A) = \mathrm{Diag}\left(\mathrm{M}_{p_1^{a_{11}}}, \mathrm{M}_{p_2^{a_{21}}}, \mathrm{M}_{p_2^{a_{22}}}\right) = \mathrm{Diag}\left(\mathrm{M}_x,\ \mathrm{M}_{x+1},\ \mathrm{M}_{(x+1)^2}\right) = \left(\begin{array}{cc|cc} \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \end{array}\right)$$

Übung 7.3: Ähnlichkeit und Transponieren

Sei K ein Körper, $n \in \mathbb{N}$ und $A \in K^{n\times n}$. Dann ist A ähnlich zu A^{tr}.

Beweis:

Betrachte die charakteristische Matrix $\mathfrak{X}(A)$ und $\mathfrak{X}\left(A^{\mathrm{tr}}\right)$. Es gilt:

$$\mathfrak{X}(A) = x\mathrm{I}_n - A,$$
$$\mathfrak{X}\left(A^{\mathrm{tr}}\right) = x\mathrm{I}_n - A^{\mathrm{tr}} = x{\mathrm{I}_n}^{\mathrm{tr}} - A^{\mathrm{tr}} = (x - \mathrm{I}_n - A)^{\mathrm{tr}} = \mathfrak{X}(A)$$

Seien nun $\mathfrak{g}, \mathfrak{h} \in \mathrm{GL}_n(K)$, sodass $\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{SNF}(A)$.
Da die SNF eine Diagonalmatrix ist, gilt klarerweise:

$$\mathrm{SNF}(A) = \mathrm{SNF}(A)^{\mathrm{tr}}$$
$$\Leftrightarrow \mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = (\mathfrak{g}\mathfrak{X}(A)\mathfrak{h})^{\mathrm{tr}} = \mathfrak{h}^{\mathrm{tr}} \cdot (\mathfrak{g}\mathfrak{X}(A))^{\mathrm{tr}} = \mathfrak{h}^{\mathrm{tr}}\mathfrak{X}(A)^{\mathrm{tr}}\mathfrak{g}^{\mathrm{tr}} = \mathfrak{h}^{\mathrm{tr}}\mathfrak{X}\left(A^{\mathrm{tr}}\right)\mathfrak{g}^{\mathrm{tr}}$$

Ebenfalls gilt (LA1): $\mathfrak{h}^{\mathrm{tr}}, \mathfrak{g}^{\mathrm{tr}} \in \mathrm{GL}_n(K)$. Multipliziere also nun beide Seiten mit $\mathfrak{g}^{-1}$ von links und $\mathfrak{h}^{-1}$ von rechts:

$$\mathfrak{g}^{-1}\mathfrak{g}\mathfrak{X}(A)\mathfrak{h}\mathfrak{h}^{-1} = \mathfrak{X}(A) = \underbrace{\mathfrak{g}^{-1}\mathfrak{h}^{\mathrm{tr}}}_{\in \mathrm{GL}_n(K)}\mathfrak{X}\left(A^{\mathrm{tr}}\right)\underbrace{\mathfrak{g}^{\mathrm{tr}}\mathfrak{h}^{-1}}_{\in \mathrm{GL}_n(K)}$$

Also existieren $g, h \in \mathrm{GL}_n(K)$ (nämlich $g := \mathfrak{g}^{-1}\mathfrak{h}^{\mathrm{tr}}$ und $h := \mathfrak{g}^{\mathrm{tr}}\mathfrak{h}^{-1}$), sodass

$$\mathfrak{X}(A) = g\mathfrak{X}\left(A^{\mathrm{tr}}\right)h$$

d.h. $\mathfrak{X}(A)$ ist äquivalent zu $\mathfrak{X}\left(A^{\mathrm{tr}}\right)$. Nach 7.2.7 sind A und A^{tr} damit ähnlich. □

7.2.b Trennende Invarianten

Satz 7.2.11:

Sei $\alpha \in \operatorname{End}(\mathcal{V})$ mit $\mu_\alpha = p^m$ mit $p \in K[x]$ irreduzibel, $m \in \mathbb{N}$. Setze $v := p(\alpha)$.
Dann sind folgende Aussagen äquivalent:

(1) $\mathcal{V}$ ist zyklisch bzgl. α.

(2) $\operatorname{Dim}_K \operatorname{Kern} v = \operatorname{Grad} p$

(3) $\operatorname{Rang} v = \operatorname{Dim} \mathcal{V} - \operatorname{Grad} p$

(4) $\mu_\alpha = \chi_\alpha$

(5) Sämtliche α-invarianten Teilräume von $\mathcal{V}$ bilden eine Kette gegeben durch

$$\langle v^i(\mathcal{V})\rangle_\alpha = v^i(\mathcal{V}) = \operatorname{Bild} v^i \text{ für } i \in (\{0\} \cup \underline{m})$$

Beweis zu 7.2.11:

Zunächst eine allgemeine Vorbemerkung, die nur die gemeinsamen Voraussetzungen nutzt:
Sei $\mathcal{V}_i := \operatorname{Bild} v^i$. Nach Definition des Minimalpolynoms ist $\mathcal{V}_{m-1} \neq \{0\}$, aber $\mathcal{V}_m = \{0\}$.
Da $v = p(\alpha)$ mit α kommutiert, sind die $\mathcal{V}_i$s allesamt α-invariant, d.h. $\alpha(\mathcal{V}_i) \subseteq \mathcal{V}_i$.
Es ist $\mathcal{V} = \mathcal{V}_0 > \mathcal{V}_1 > \cdots > \mathcal{V}_{m-1} > \mathcal{V}_m = \{0\}$, wobei die Faktoren $\mathcal{V}_i/\mathcal{V}_{i+1} = v(\mathcal{V}_{i-1}/\mathcal{V}_i)$ epimorphe Bilder voneinander sind.

$$\begin{array}{ll} \bullet\ \mathcal{V}_0 = \mathcal{V} \cong K[x]/\langle p^m\rangle & \\ \Big| d & \\ \bullet\ \mathcal{V}_1 \cong \langle p\rangle/\langle p^m\rangle & \\ \Big| d & \\ \bullet\ \mathcal{V}_2 \cong \langle p^2\rangle/\langle p^m\rangle & \\ \vdots & \\ \bullet\ \mathcal{V}_{m-1} \cong \langle p^{m-1}\rangle/\langle p^m\rangle & \\ \Big| d & \\ \bullet\ \mathcal{V}_m = \{0\} \cong \langle p^m\rangle/\langle p^m\rangle & \end{array}$$

Insbesondere ist

$$\underbrace{\operatorname{Dim}\mathcal{V}_{m-1}}_{\operatorname{Dim}\mathcal{V}_{m-1} - \underbrace{\operatorname{Dim}\mathcal{V}_m}_{=0}} \leq \cdots \leq \operatorname{Dim}\mathcal{V}_i - \operatorname{Dim}\mathcal{V}_{i+1} \leq \operatorname{Dim}\mathcal{V}_{i-1} - \operatorname{Dim}\mathcal{V}_i \leq \cdots \leq \underbrace{\operatorname{Dim}\underbrace{\mathcal{V}_0}_{\mathcal{V}} - \operatorname{Dim}\underbrace{\mathcal{V}_1}_{\operatorname{Bild} v}}_{\operatorname{Dim}\operatorname{Kern} v}$$

Das MinPoly des von α auf $\mathcal{V}_i/\mathcal{V}_{i+1}$ induzierten Endomorphismus α_i ist $\mu_{\alpha_i} = p$. Insbesondere ist nach 5.5.7 (LA1) die Dimension der Faktorräume $\operatorname{Dim}(\mathcal{V}_i/\mathcal{V}_{i+1}) = \operatorname{Dim}\mathcal{V}_i - \operatorname{Dim}\mathcal{V}_{i+1}$ ein Vielfaches von $d = \operatorname{Grad} p$.

(2)⇔(3) ist der Homomorphiesatz.

(1)⇔(4) ist 7.1.9.

(4)⇒(2): Ist $\mu_\alpha = \chi_\alpha$, so ist $dm = \operatorname{Grad}\mu_\alpha = \operatorname{Grad}\chi_\alpha = n$ und die echt absteigende Kette von TRen oben hat die Länge $m = \frac{n}{d}$. Damit muss aber $\operatorname{Dim}\mathcal{V}_i - \operatorname{Dim}\mathcal{V}_{i+1} = d$ sein $\forall i$, also auch $\operatorname{Dim}\operatorname{Kern} v = \operatorname{Dim}\mathcal{V}_0 - \operatorname{Dim}\mathcal{V}_1 = d$.

(2)⇒(4): Ist $\operatorname{Dim}\operatorname{Kern} v$ = d, so folgt $\operatorname{Dim}\mathcal{V}_i - \operatorname{Dim}\mathcal{V}_{i+1} = d\ \forall i$ und daher $m = \frac{n}{d}$.

(1)⇒(5): Ist $\mathcal{W} \leq \mathcal{V}$ ein α-invarianter TR, so gibt es ein größtes i mit $\mathcal{W} \leq \mathcal{V}_i$. Aber jedes $W \in \mathcal{W} \setminus \mathcal{V}_{i+1}$ erfüllt bereits, dass sein α-Erzeugnis ganz $\mathcal{V}_i$ ist, da auch mit $\mathcal{V}$ jedes $\mathcal{V}_i$ zyklischer Modul für $\alpha|_{\mathcal{V}_i}$ ist.

(5)⇒(1): Klar, da dann alle Vektoren in $\mathcal{V} \setminus \mathcal{V}_1$ (und nur diese) demnach zyklisch sein müssen.

□

Übung 7.4:

Sei $A := \begin{pmatrix} 1 & 1 & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \\ 1 & 1 & \cdot & \cdot \\ \cdot & 1 & 1 & 1 \end{pmatrix} \in {\mathbb{F}_2}^{4\times 4}$.

$\mathbb{F}_2^{4\times 1}$ ist zyklisch bzgl. $\widetilde{A}$, denn $\mu_A = x^4+1 = (x+1)^4$, also $\operatorname{Grad}\mu_A = 4 \operatorname{Dim} {\mathbb{F}_2}^{4\times 4}$ (7.1.9).
Nach 7.2.11 ist für $p := x+1$ ($\mu_A = p^4$), $v := p\left(\widetilde{A}\right) = \widetilde{A} + \mathrm{id}_{{\mathbb{F}_2}^{4\times 1}}$:

- $\operatorname{Dim}\operatorname{Kern} v = \operatorname{Grad} p = 1$
- $\operatorname{Rang} v = \operatorname{Dim} {\mathbb{F}_2}^{4\times 1} - \operatorname{Grad} p = 4 - 1 = 3$
- Für die Standardbasis $\mathcal{S}$ von ${\mathbb{F}_2}^{4\times 1}$ ist

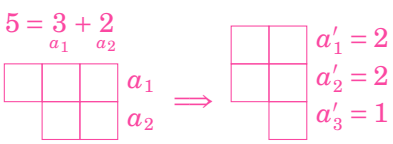
$$ {}^{\mathcal{S}}v^{\mathcal{S}} = A + \mathrm{I}_4 = \begin{pmatrix} \cdot & 1 & \cdot & 1 \\ \cdot & 1 & 1 & \cdot \\ 1 & 1 & 1 & \cdot \\ \cdot & 1 & 1 & \cdot \end{pmatrix} $$

  Damit ist:
  - $\mathcal{V}_0 := \operatorname{Bild} v^0 = \operatorname{Bild}\mathrm{id}_{\mathcal{V}} = \mathcal{V}$
  - $\mathcal{V}_1 := \operatorname{Bild} v^1 = \left\langle \begin{pmatrix} \cdot \\ \cdot \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \cdot \\ 1 \\ 1 \end{pmatrix} \right\rangle < \mathcal{V}_0$
  - $\mathcal{V}_2 := \operatorname{Bild} v^2 = \left\langle \begin{pmatrix} \cdot \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \cdot \\ \cdot \\ 1 \\ \cdot \end{pmatrix} \right\rangle < \mathcal{V}_1$
  - $\mathcal{V}_3 := \operatorname{Bild} v^3 = \left\langle \begin{pmatrix} \cdot \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle < \mathcal{V}_2$
  - $\mathcal{V}_4 = \operatorname{Bild} v^4 = \langle 0 \rangle < \mathcal{V}_3$.
- $\mathbb{F}_2^{4\times 1}$ ist zyklisch bzgl. jedem $V \in {\mathbb{F}_2}^{4\times 1} \setminus \mathcal{V}_1$.

Definition 7.2.12: Partitionen

(1) Eine **Partition** der natürlichen Zahl $c \in \mathbb{N}$ ist ein k-Tupel $a = (a_1, \ldots, a_k) \in \mathbb{N}^k$ für ein $k \in \mathbb{N}$ mit $a_1 \geq \cdots \geq a_k$ und $a_1 + \cdots + a_k = c$.

(2) Ist $a = (a_1, \ldots, a_k) \in \mathbb{N}^k$ eine Partition von $c \in \mathbb{N}$, so ist die **konjugierte Partition** a' von a definiert durch $a'_i := \left|\{j \mid a_j \geq i\}\right|$
Man visualisiert üblicherweise die Partition durch Kästchen, die man linksbündig in Zeilen untereinander anordnet, mit a_i Kästchen in der i-ten Zeile.
Dies nennt man **Young-Tableaux** oder **-Diagramme**. Die Tableux von a und a' sind transponiert.



Definition 7.2.13:

Sei $\mathcal{V}$ ein K-VR und $\alpha \in \mathrm{End}(\mathcal{V})$ mit $\chi_\alpha = p^c,\ p \in K[x]$ irreduzibel.
Dann gibt es eine K-Basis B von $\mathcal{V}$ mit

$$ {}^B\alpha^B = \mathrm{Diag}\left(\mathrm{M}_{p^{a_1}}, \ldots, \mathrm{M}_{p^{a_k}}\right) $$

entsprechend dem $K[x]$-Modulisomorphismus

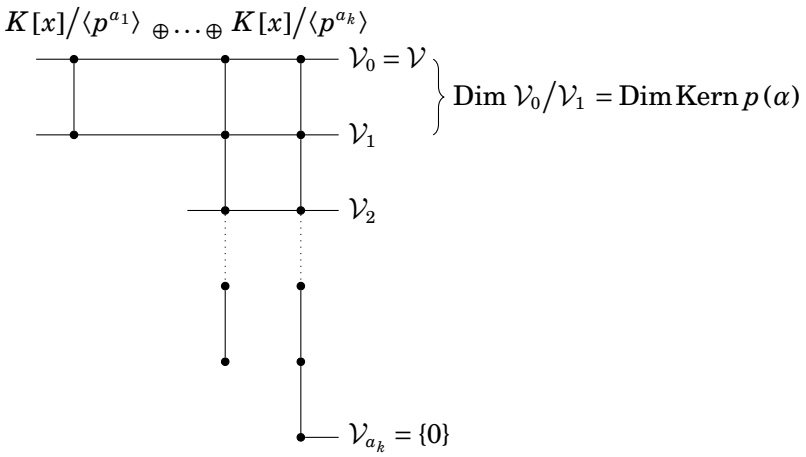
$$ \mathcal{V} \underset{K[x]}{\cong} K[x]/\langle p^{a_1}\rangle \oplus \cdots \oplus K[x]/\langle p^{a_k}\rangle $$

für eine eindeutig durch α definierte Partition $(a_k, \ldots, a_1)$ von c.
Diese Partition heißt **die durch α definierte Partition**.

Korollar 7.2.14:

Seien α und p wie oben, $d := \mathrm{Grad}\, p$ und $a = (a_k, \ldots, a_1)$ die durch α definierte Partition.
Sei $\mathcal{V}_i = p(\alpha)^i(\mathcal{V}) = \mathrm{Bild}\left(p(\alpha)^i\right)$ für $i \in \left(\{0\} \cup \underline{a_k}\right)$.
Dann gilt $\mathcal{V} = \mathcal{V}_0 > \mathcal{V}_1 > \cdots > \mathcal{V}_{a_{k-1}} > \mathcal{V}_{a_k} = \{0\}$ und $\mathrm{Dim}\left(\mathcal{V}_i/\mathcal{V}_{i+1}\right) = d a'_j$ mit a' der zu a konjugierten Partition. i.A. ist $\mathcal{V} \cong K[x]/\langle p^{a_1}\rangle \oplus \cdots \oplus K[x]/\langle p^{a_k}\rangle$ mit $a_k \geq \cdots \geq a_1 > 0$ und $\sum_i a_i = c$.

Beweis zu 7.2.14:
Wende Satz 7.2.11 auf die zyklischen Faktoren an. □



Beispiel 7.2.15:

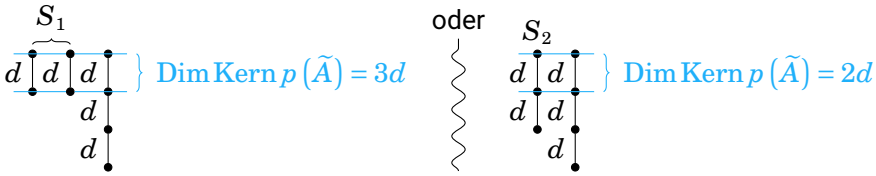
Sei $p \in K[x]$ normiert und irreduzibel vom Grad d und $A \in K^{5d\times 5d}$ mit $\mu_A = p^3$. $\Rightarrow \chi_A = p^5$.
Betrachte Partitionen, wo der größte Teil 3 ist:

$$S_1 := K[x]/\langle p\rangle \oplus K[x]/\langle p\rangle \text{ oder } S_2 := K[x]/\langle p^2\rangle$$

Dann hat man zwei Möglichkeiten für die Ähnlichkeitsklasse von A:

$$A \sim \mathrm{Diag}\left(\mathrm{M}_p, \mathrm{M}_p, \mathrm{M}_{p^3}\right) \text{ oder } \mathrm{Diag}\left(\mathrm{M}_{p^2}, \mathrm{M}_{p^3}\right)$$

entsprechend der Modulisomorphismen mit $\mathrm{M}_A \cong S_1 \oplus K[x]/\langle p^3\rangle$ bzw. $\mathrm{M}_A \cong S_2 \oplus K[x]/\langle p^3\rangle$.



d.h. durch die Berechnung des Kernes von $p(\widetilde{A})$ erhalten wir nach Voraussetzung entweder $3d$ oder $2d$ und können allein damit entscheiden, zu welcher Ähnlichkeitsklasse A gehört.

Wir erhalten mit μ_α und der durch α definierten Partition endlich trennende Invarianten für die Ähnlichkeitsklassen von Endomorphismen!

Satz 7.2.16:

Zwei Endomorphismen $\alpha, \beta \in \mathrm{End}(\mathcal{V})$ sind genau dann ähnlich, sprich unter $\mathrm{GL}(\mathcal{V})$ konjugiert, wenn gilt:

(1) die Minimalpolynome sind $\mu_\alpha = \mu_\beta$, und

(2) für jeden normierten, irreduziblen Teiler $p \in K[x]$ des MinPolys sind die Partitionen des p-Hauptraums von $(\mathcal{V}, \alpha)$ und $(\mathcal{V}, \beta)$ gleich.

Beispiel 7.2.17: Ähnlichkeitsklassen in $\mathbb{C}^{3\times 3}$

Seien $a, b, c \in \mathbb{C}$ paarweise verschieden, d.h. $a \neq b \neq c \neq a$.

χ_A	μ_A	Partitionen	Vertreter
$(x-a)^3$	$(x-a)^1$	$(1,1,1)$	$\mathrm{Diag}(a,a,a)$
	$(x-a)^2$	$(2,1)$	$\mathrm{Diag}\left(a, \mathrm{M}_{(x-a)^2}\right)$
	$(x-a)^3$	(3)	$\mathrm{M}_{(x-a)^3}$
$(x-a)^2(x-b)$	$(x-a)^1(x-b)^1$	$(1,1),(1)$	$\mathrm{Diag}(a,a,b)$
	$(x-a)^2(x-b)^1$	$(2),(1)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^2}, b\right)$
$(x-a)(x-b)(x-c)$	$(x-a)(x-b)(x-c)$	$(1),(1),(1)$	$\mathrm{Diag}(a,b,c)$

Beispiel 7.2.18: Ähnlichkeitsklassen in $\mathbb{C}^{4\times 4}$

Seien $a,b,c,d \in \mathbb{C}$ paarweise verschieden.

χ_A	μ_A	Partitionen	Vertreter
$(x-a)^4$	$(x-a)^1$	$(1,1,1,1)$	$\mathrm{Diag}(a,a,a,a)$
	$(x-a)^2$	$(2,2)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^2},\mathrm{M}_{(x-a)^2}\right)$
		$(2,1,1)$	$\mathrm{Diag}\left(a,a,\mathrm{M}_{(x-a)^2}\right)$
	$(x-a)^3$	$(3,1)$	$\mathrm{Diag}\left(a,\mathrm{M}_{(x-a)^3}\right)$
	$(x-a)^4$	(4)	$\mathrm{M}_{(x-a)^4}$
$(x-a)^3(x-b)$	$(x-a)^1(x-b)^1$	$(1,1,1),(1)$	$\mathrm{Diag}(a,a,a,b)$
	$(x-a)^2(x-b)^1$	$(2,1),(1)$	$\mathrm{Diag}\left(a,\mathrm{M}_{(x-a)^2},b\right)$
	$(x-a)^3(x-b)^1$	$(3),(1)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^3},b\right)$
$(x-a)^2(x-b)^2$	$(x-a)^1(x-b)^1$	$(1,1),(1,1)$	$\mathrm{Diag}(a,a,b,b)$
	$(x-a)^2(x-b)^1$	$(2),(1,1)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^2},b,b\right)$
	$(x-a)^2(x-b)^2$	$(2),(2)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^2},\mathrm{M}_{(x-b)^2}\right)$
$(x-a)^2(x-b)(x-c)$	$(x-a)^1(x-b)^1(x-c)^1$	$(1,1),(1),(1)$	$\mathrm{Diag}(a,a,b,c)$
	$(x-a)^2(x-b)^1(x-c)^1$	$(2),(1),(1)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^2},b,c\right)$
$(x-a)(x-b)(x-c)(x-d)$	$\prod_{j\in\{a,b,c,d\}}(x-j)$	$(1),(1),(1),(1)$	$\mathrm{Diag}(a,b,c,d)$

Übung 8.1.i: Allgemeine Ähnlichkeitsklassen zu einem Polynom

Sei K ein Körper und $a,b \in K$ mit $a \neq b$.
Gesucht: Alle Ähnlichkeitsklassen von $A \in K^{6\times 6}$ mit $\chi_A = (x-a)^4(x-b)^2$.

μ_A	Partitionen	Vertreter
$(x-a)^1(x-b)^1$	$(1,1,1,1),(1,1)$	$\mathrm{Diag}(a,a,a,a,b,b)$
$(x-a)^2(x-b)^1$	$(2,1,1),(1,1)$	$\mathrm{Diag}\left(a,a,\mathrm{M}_{(x-a)^2},b,b\right)$
	$(2,2),(1,1)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^2},\mathrm{M}_{(x-a)^2},b,b\right)$
$(x-a)^3(x-b)^1$	$(3,1),(1,1)$	$\mathrm{Diag}\left(a,\mathrm{M}_{(x-a)^3},b,b\right)$
$(x-a)^4(x-b)^1$	$(4),(1,1)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^4},b,b\right)$
$(x-a)^1(x-b)^2$	$(1,1,1,1),(2)$	$\mathrm{Diag}\left(a,a,a,a,\mathrm{M}_{(x-b)^2}\right)$
$(x-a)^2(x-b)^2$	$(2,1,1),(2)$	$\mathrm{Diag}\left(a,a,\mathrm{M}_{(x-a)^2},\mathrm{M}_{(x-b)^2}\right)$
	$(2,2),(2)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^2},\mathrm{M}_{(x-a)^2},\mathrm{M}_{(x-b)^2}\right)$
$(x-a)^3(x-b)^2$	$(3,1),(2)$	$\mathrm{Diag}\left(a,\mathrm{M}_{(x-a)^3},\mathrm{M}_{(x-b)^2}\right)$
$(x-a)^4(x-b)^2$	$(4),(2)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^4},\mathrm{M}_{(x-b)^2}\right)$

Übung 7.2: Nicht-trennende Invarianten

Seien $A_1 := \begin{pmatrix} \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \end{pmatrix}$, $A_2 := \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, $A_3 := \begin{pmatrix} 2 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix} \in \mathbb{F}_3^{3\times 3}$.

Es gilt:

- $\mathrm{Spur}(A_1) = \mathrm{Spur}(A_2) = 0 \neq 1 = \mathrm{Spur}(A_3)$
- $\mathrm{Rang}(A_1) = 2 \neq 1 = \mathrm{Rang}(A_2)$

$\Rightarrow$ die Matrizen sind alle paarweise in verschiedenen Ähnlichkeitsklassen.

Übung 8.1.ii: Ähnlichkeitsklassen in $\mathbb{F}_2^{3\times 3}$

Zunächst: Betrachte alle irreduziblen Polynome in $\mathbb{F}_2[x]$ mit Grad ≤ 3:

$$x,\ x+1,\ x^2+x+1,\ x^3+x^2+1,\ x^3+x+1$$

χ_A	μ_A	Partitionen	Vertreter
x^3	x^1	$(1,1,1)$	$0 \in \mathbb{F}_2^{3\times 3}$
	x^2	$(2,1)$	$\mathrm{Diag}(0, \mathrm{M}_{x^2})$
	x^3	(3)	$\mathrm{Diag}(\mathrm{M}_{x^3})$
$(x+1)^3$	$(x+1)^1$	$(1,1,1)$	$\mathrm{Diag}(1,1,1)$
	$(x+1)^2$	$(2,1)$	$\mathrm{Diag}\left(1, \mathrm{M}_{(x+1)^2}\right)$
	$(x+1)^3$	(3)	$\mathrm{M}_{(x+1)^3}$
$(x+1)^2 x$	$(x+1)^1 x^1$	$(1,1),(1)$	$\mathrm{Diag}(1,1,0)$
	$(x+1)^2 x^1$	$(2),(1)$	$\mathrm{Diag}\left(\mathrm{M}_{(x+1)^2}, 0\right)$
$(x+1)x^2$	$(x+1)^1 x^1$	$(1),(1,1)$	$\mathrm{Diag}(1,0,0)$
	$(x+1)^1 x^2$	$(1),(2)$	$\mathrm{Diag}(1, \mathrm{M}_{x^2})$
$\left(x^2+x+1\right)x$	$\left(x^2+x+1\right)^1 x^1$	$(1),(1)$	$\mathrm{Diag}(\mathrm{M}_{x^2+x+1}, 0)$
$(x+1)\left(x^2+x+1\right)$	$(x+1)^1\left(x^2+x+1\right)^1$	$(1),(1)$	$\mathrm{Diag}(1, \mathrm{M}_{x^2+x+1})$
$\left(x^3+x^2+1\right)$	$\left(x^3+x^2+1\right)^1$	(1)	$\mathrm{M}_{x^3+x^2+1}$
$\left(x^3+x+1\right)$	$\left(x^3+x+1\right)^1$	(1)	M_{x^3+x+1}

Übung 8.1.iii: Ähnlichkeitsklassen in $\mathbb{R}^{3\times 3}$

Seien $a,b,c \in \mathbb{R}$ paarweise verschieden und $p,q \in \mathbb{R}$ mit $\frac{p^2}{4} - q < 0$.
(Dann sind die irreduziblen Polynome in $\mathbb{R}[x]$ genau $x-a$ und x^2+px+q (vgl. pq-Formel).)

χ_A	μ_A	Partitionen	Vertreter
$(x-a)^3$	$(x-a)^1$	$(1,1,1)$	$\mathrm{Diag}(a,a,a)$
	$(x-a)^2$	$(2,1)$	$\mathrm{Diag}\left(a, \mathrm{M}_{(x-a)^2}\right)$
	$(x-a)^3$	(3)	$\mathrm{M}_{(x-a)^3}$
$(x-a)^2(x-b)$	$(x-a)^1(x-b)^1$	$(1,1),(1)$	$\mathrm{Diag}(a,a,b)$
	$(x-a)^2(x-b)^1$	$(2),(1)$	$\mathrm{Diag}\left(\mathrm{M}_{(x-a)^2}, b\right)$
$(x-a)(x-b)(x-c)$	$(x-a)^1(x-b)^1(x-c)^1$	$(1,1),(1),(1)$	$\mathrm{Diag}(a,b,c)$
$(x-a)\left(x^2+px+q\right)$	$(x-a)^1\left(x^2+px+q\right)^1$	$(1),(1)$	$\mathrm{Diag}\left(a, \mathrm{M}_{x^2+px+q}\right)$

7.2.c Die Jordan-Normalform

Aus der primäre rationalen Form erhält man durch eine andere Basiswahl die sogenannte Jordan-Normalform. Dazu genügt es, den zyklischen Fall mit einer Primkomponente zu betrachten ($\mathcal{V} = K[x]/\langle p^m \rangle$).

Satz 7.2.19: JORDAN-BLOCK

Sei $\alpha \in \mathrm{End}(\mathcal{V})$ mit $\chi_\alpha = \mu_\alpha = p^m$ mit $p \in K[x]$ normiert und irreduzibel.
Setze $v := p(\alpha)$, $d := \mathrm{Grad}\, p$.
Jeder $V \in \mathcal{V} \setminus v(\mathcal{V})$ liefert eine Basis

$$B = \Big(\underbrace{V, \alpha(V), \ldots, \alpha^{d-1}(V)}_{d},$$
$$\underbrace{v(V), \alpha(v(V)), \ldots, \alpha^{d-1}(v(V))}_{d},$$
$$\vdots$$
$$\underbrace{v^{m-1}(V), \alpha\left(v^{m-1}(V)\right), \ldots, \alpha^{d-1}\left(v^{m-1}(V)\right)}_{d} \Big)$$

(m solcher „Pakete“) von $\mathcal{V}$, sodass die Matrix von α bzgl. B gegeben ist durch

$${}^B\alpha^B = \mathrm{J}_m(p) := \begin{pmatrix} \mathrm{M}_p & 0 & \cdots & \cdots & 0 \\ \mathrm{N}_d & \mathrm{M}_p & \ddots & & \vdots \\ 0 & \mathrm{N}_d & \mathrm{M}_d & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \mathrm{N}_d & \mathrm{M}_p \end{pmatrix} \in K^{dm \times dm}, \text{ wobei } \mathrm{N}_d := \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix} \in K^{d \times d}$$

mit m Begleitmatrizen in J_m.

Beweis zu 7.2.19:
Nachrechnen. Sei $p := x^d + p_{d-1}x^{d-1} + \cdots + p_1 x^1 + p_0$.

$$\Rightarrow \mathrm{M}_p = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & -p_0 \\ 1 & & & \vdots \\ & \ddots & & \vdots \\ 0 & & 1 & -p_{d-1} \end{array}\right)$$

$$v(V) = p(\alpha)(V) = \alpha^d(V) + p_{d-1}\alpha^{d-1}(V) + \cdots + p_0 V$$
$$\Rightarrow \alpha^d(V) = -p_0 V - p_1 \alpha(V) - \cdots - p_{d-1}\alpha^{d-1}(V) + 1 \cdot v(V)$$

□

$$p = x - a \Rightarrow \mathrm{N}_1 = (1) \in K^{1\times 1}$$
$$\Rightarrow \mathrm{J}_m(p) = \begin{pmatrix} a & & & \\ 1 & a & & \\ & \ddots & \ddots & \\ & & 1 & a \end{pmatrix} \text{ Jordan-Normalform.}$$

In der Literatur wird oft vorausgesetzt, dass K algebraisch abgeschlossen ist. Dies hier ist aber für *beliebige* Körper.

Korollar 7.2.20: JORDAN-NORMALFORM

Sei $A \in K^{n\times n}$ mit $\mathrm{PRF}(A) = \mathrm{Diag}\left(\mathrm{M}_{p_1}^{a_{1,1}}, \ldots, \mathrm{M}_{p_l}^{a_{l,s_l}}\right)$.
Dann ist A ähnlich zu

$$\mathrm{JNF}(A) := \mathrm{Diag}\left(\mathrm{J}_{a_{1,1}}(p_1), \ldots, \mathrm{J}_{a_{l,s_l}}(p_l)\right)$$

der **Jordan-Normalform** von A.

Beispiel 7.2.21: JORDAN-NORMALFORMEN

Im Beispiel 7.2.9 mit $A = \begin{pmatrix} -6 & 6 & 0 & 6 \\ -4 & 6 & -1 & 3 \\ -6 & 12 & -3 & 3 \\ -6 & 12 & -3 & 3 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$ ist

$$\mathrm{RKF}(A) = \mathrm{PRF}(A) = \mathrm{Diag}(\mathrm{M}_x, \mathrm{M}_{x^3}) = \left(\begin{array}{c|ccc} 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right) = \mathrm{JNF}(A)$$

Im Beispiel 7.2.10 mit $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$ erhält man

$$\mu_A = \chi_A = (x+1)^2(x-1)$$

$$\mathrm{RKF}(A) = \mathrm{M}_{\mu_A} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

$$\mathrm{PRF}(A) = \mathrm{Diag}\left(1, \mathrm{M}_{(x-1)^2}\right) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & -1 \\ 0 & 1 & -2 \end{array}\right)$$

$$\mathrm{JNF}(A) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & -1 & 0 \\ 0 & 1 & -1 \end{array}\right) \text{ (Eigenwerte)}$$

Übung 8.3: JORDAN-NORMALFORM

Sei $A := \begin{pmatrix} \cdot & 1 & 1 & 1 \\ \cdot & 1 & \cdot & 1 \\ 1 & 1 & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \end{pmatrix} \in \mathbb{F}_2^{4\times 4}$. Es ist $\mathfrak{X}(A) = \begin{pmatrix} x & 1 & 1 & 1 \\ \cdot & x+1 & & \cdot \quad 1 \\ 1 & 1 & x+1 & \cdot \\ \cdot & 1 & \cdot & x \end{pmatrix}$.

$$\Rightarrow \mathrm{SNF}(\mathfrak{X}(A)) = \mathrm{Diag}\left(1, 1, x^2+x+1, x^2+x+1\right)$$

$$\Rightarrow \mathrm{RKF}(A) = \mathrm{Diag}(\mathrm{M}_{x^2+x+1}, \mathrm{M}_{x^2+x+1}),\ \mu_A = x^2+x+1,\ \chi_A = \left(x^2+x+1\right)^2$$

$\Rightarrow \mathrm{PRF}(A) = \mathrm{RKF}(A)$, da $a_1 = 1,\ a_2 = 1$ die einzige mögliche Partition ist.

$$\Rightarrow \mathrm{JNF}(A) = \mathrm{Diag}\left(\mathrm{J}_1\left(x^2+x+1\right), \mathrm{J}_1\left(x^2+x+1\right)\right),\ \mathrm{J}_1\left(x^2+x+1\right) = (\mathrm{M}_{x^2+x+1})$$

$$\Rightarrow \mathrm{JNF}(A) = \mathrm{PRF}(A) = \mathrm{RKF}(A)$$

7.2.d Transformationsmatrizen

Bemerkung 7.2.22:

Sei $S = \mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}(f_1, \ldots, f_n)$ die SNF von $\mathfrak{X}(A) \in K[x]^{n\times n}$, wobei die f_is normiert sind. Seien $f_1 = \cdots = f_{s-1} = 1$ und $d_i := \mathrm{Grad}(f_i) \geq 1 \ \forall i \geq s$. Dann gilt $d_s + \cdots + d_n = n$.
Für $i \geq s,\ 1 \leq j \leq n$ sei

$$\mathfrak{g}_{i,j} \equiv c_{i,j,0} + c_{i,j,1}x^1 + \cdots + c_{i,j,d-1}x^{d-1} \mod f_i$$

Setze

$$P_j^{(i)} := \begin{pmatrix} c_{i,j,0} \\ \vdots \\ c_{i,j,d-1} \end{pmatrix} \in K^{d_i \times 1} \quad \text{und} \quad P_j := \begin{pmatrix} P_j^{(s)} \\ \vdots \\ P_j^{(n)} \end{pmatrix} \in K^{n\times 1}$$

Dann ist die Matrix $P := (P_1, \ldots, P_n) \in K^{n\times n}$ invertierbar und es gilt $PAP^{-1} = \mathrm{RKF}(A)$.

Beispiel 7.2.23:

Ist $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$ aus 7.2.10, so kann

$$\mathfrak{g} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ x & x^2 & 1 \end{pmatrix}$$

gewählt werden und es ergibt sich gemäß voriger Vorschrift

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

und man erhäkt $PAP^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} = \mathrm{RKF}(A)$.

Die Berechnung der SNF von $\mathfrak{X}(A)$ ist aufwändig. Eine Transformationsmatrix P erhält man auf einfache Weise durch direktes Nachrechnen mit Matrizen über K:

Da $\mu_A = \chi_A$, ist $\mathbb{Q}^{3\times 1}$ ein zyklischer Modul. Beginnt man mit dem ersten Einheitsvektor

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},\ Ae_1 = e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},\ A^2e_1 = Ae_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$$

so erhält man direkt eine Basis $B = (e_1, e_2, Ae_2)$ mit ${}^B\widetilde{A}^B = \mathrm{M}_{\mu_A}$, d.h.

$$T := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

erfüllt $T^{-1}AT = \mathrm{M}_{\mu_A} = \mathrm{RKF}(A)$ und somit $P := T^{-1}$.

Beispiel 7.2.24:

Sei A wie in 7.2.9 mit $A = \begin{pmatrix} -6 & 6 & 0 & 6 \\ -4 & 6 & -1 & 3 \\ -6 & 12 & -3 & 3 \\ -6 & 12 & -3 & 3 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$, also $\mathfrak{g}\mathfrak{X}(A)\mathfrak{h} = \mathrm{Diag}(1,1,x,x^3)$,

$$\mathfrak{g} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{24}x + \frac{1}{4} & -\frac{3}{4} & 0 & \frac{1}{4} \\ \frac{1}{6}x^2 - x - 4 & x + 12 & -4 & x \end{pmatrix} \leftarrow \text{geht um die unteren 2 Zeilen}$$

$$\overset{\mathrm{mod}\, x}{\Longrightarrow} P = \begin{pmatrix} \frac{1}{4} & -\frac{3}{4} & 0 & \frac{1}{4} \\ -4 & 12 & -4 & 0 \\ -1 & 1 & 0 & 1 \\ \frac{1}{6} & 0 & 0 & 0 \end{pmatrix}$$

und $PAP^{-1} = \mathrm{Diag}(\mathrm{M}_x, \mathrm{M}_{x^3})$.

Beispiel 7.2.25:

Sei A wie in 7.2.9 mit $A = \begin{pmatrix} -6 & 6 & 0 & 6 \\ -4 & 6 & -1 & 3 \\ -6 & 12 & -3 & 3 \\ -6 & 12 & -3 & 3 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$. $\mu_A = x^3$.

Der erste Standardbasisvektor E_1 hat als MinPoly $\mu_{A,E_1} = x^3$.

$$(E_1, AE_1, A^2E_1) = \begin{pmatrix} 1 & -6 & -24 \\ 0 & -4 & -12 \\ 0 & -6 & -12 \\ 0 & -6 & -12 \end{pmatrix}$$

Es ist $\langle E_1 \rangle_A = \langle E_1, E_2, E_3 + E_4 \rangle = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle$ (einfacheres EZS, z.B. durch Spaltengauß).

Wir sehen: $E_3 \notin \langle E_1, AE_1, A^2E_1 \rangle = \langle E_1, E_2, E_3 + E_4 \rangle$. Man rechnet nach: $AE_3 = AE_1 - \frac{1}{4}A^2E_1$, also setze $F := 2\left(E_1 - \frac{1}{4}AE_1 - E_3\right) = \begin{pmatrix} 5 \\ 2 \\ 1 \\ 3 \end{pmatrix} \in \mathbb{Q}^{4\times 1}$. Dann gilt $AF = 0$.

Insgesamt liefert $B := (F, E_1, AE_1, A^2E_1)$ eine Basis von $\mathbb{Q}^{4\times 1}$ mit ${}^B\widetilde{A}^B = \mathrm{Diag}(\mathrm{M}_x, \mathrm{M}_{x^3}) = \mathrm{RKF}(A)$.

Wir wollen aber einen Algorithmus, der nicht nur in Spezialfällen funktioniert! Das Beispiel war nur der *zyklische* Fall mit *einer* Primärkomponente.
Unsere Aufgabe ist es, das vorherige Beispiel auf den Fall von mehreren Blöcken zu verallgemeinern.
Der Einfachheit halber nehmen wir an, dass $\mu_\alpha = (x-a)^m$ gilt, also nur eine Primärkomponente $\Rightarrow$ nur ein Hauptraum (sonst Hauptraumzerlegung durchführen), und (nur um das Verfahren klarer zu machen!) der Grad des irreduziblen Polynoms 1 ist.

Bemerkung 7.2.26: Algorithmus zur Bestimmung der Jordan-Normalform mit Kernen von ν^i

Sei $\alpha \in \mathrm{End}(\mathcal{V})$ mit $\mu_\alpha = p^m = (x-a)^m$ und setze $\nu := p(\alpha) = \alpha - a\mathrm{id}_\mathcal{V}$. Sei $\mathcal{W}_i := \mathrm{Kern}\,\nu^i$.
Dann ist $\{0\} = \mathcal{W}_0 < \mathcal{W}_1 < \cdots < \mathcal{W}_{m-1} < \mathcal{W}_m = \mathcal{V}$.

Vorbemerkung: Für die Elemente $V \in \mathcal{W}_j \setminus \mathcal{W}_{j-1}$ gilt $\nu^j(V) = 0$ und $\nu^{j-1}(V) \neq 0$.
Außerdem ist $\nu : \mathcal{W}_j/\mathcal{W}_{j-1} \hookrightarrow \mathcal{W}_{j-1}/\mathcal{W}_{j-2}$ injektiv, da $\nu^{-1}(\mathcal{W}_{j-2}) \leq \mathcal{W}_{j-1}$.

(1) Ergänze eine Basis von $\mathcal{W}_{m-1}$ durch $V_1, \ldots, V_k$ zu einer Basis von $\mathcal{W}_m = \mathcal{V}$. Dann bilden die Restklassen $(V_1 + \mathcal{W}_{m-1}, \ldots, V_k + \mathcal{W}_{m-1})$ eine Basis von $\mathcal{V}/\mathcal{W}_{m-1} = \mathcal{W}_m/\mathcal{W}_{m-1}$.
Da $\nu : \mathcal{W}_m/\mathcal{W}_{m-1} \hookrightarrow \mathcal{W}_{m-1}/\mathcal{W}_{m-2}$ injektiv ist, sind auch $(\nu(V_1) + \mathcal{W}_{m-2}, \ldots, \nu(V_k) + \mathcal{W}_{m-2})$ linear unabhängig, und man erhält induktiv:

$$\begin{aligned} B_m := \big(&V_1, \nu(V_1), \ldots, \nu^{m-1}(V_1),\\ &V_2, \nu(V_2), \ldots, \nu^{m-1}(V_2),\\ &\vdots\\ &V_k, \nu(V_k), \ldots, \nu^{m-1}(V_k)\end{aligned}$$

ist eine Basis eines α-invarianten TRes mit ${}^{B_m}\alpha^{B_m} = \mathrm{Diag}\big(\underbrace{\mathrm{J}_m(a), \ldots, \mathrm{J}_m(a)}_{k}\big)$.

$$\overset{\text{Def. } \nu}{\Longrightarrow} \quad \alpha(V_i) = aV_i + \nu(V_i) \text{ passt zu } \mathrm{J}_m(a) \text{ in } \begin{pmatrix} a & * \\ 1 & \\ 0 & * \\ \vdots & \end{pmatrix}$$

$$\vdots$$

$$\alpha\left(\nu^{m-1}(V_i)\right) = a\nu^{m-1}(V_i) \quad \text{passt zu } \mathrm{J}_m(a) \text{ in } \begin{pmatrix} & \vdots & \\ * & 0 & \\ * & a & \end{pmatrix}$$

(2) Ergänze eine Basis von $\mathcal{W}_{m-2} \oplus \langle \nu(V_1), \ldots, \nu(V_k) \rangle \leq \mathcal{W}_{m-1}$ durch Vektoren $W_1, \ldots, W_l$ zu einer Basis von $\mathcal{W}_{m-1}$ ($l \in \mathbb{Z}_{\geq 0}$).

$$\begin{aligned} B_{m-1} := \big(&W_1, \nu(W_1), \ldots, \nu^{m-2}(W_1),\\ &\vdots\\ &W_l, \nu(W_l), \ldots, \nu^{m-2}(W_l)\big)\end{aligned}$$

ist dann Basis eines α-invarianten TRes mit

$${}^{B_m, B_{m-1}}\alpha^{B_m, B_{m-1}} = \mathrm{Diag}\big(\underbrace{\mathrm{J}_m(a), \ldots, \mathrm{J}_m(a)}_{k}, \underbrace{\mathrm{J}_{m-1}(a), \ldots, \mathrm{J}_{m-1}(a)}_{l}\big)$$

(3) Wiederhole (2) mit $m-1$ anstelle von m, dann mit $m-2$, etc.

Im zyklischen Fall entsprechen sich die $\mathcal{V}_i$s und $\mathcal{W}_j$s:

$\mathcal{V}_0 = \mathcal{W}_m$
d
$\mathcal{V}_1 = W_{m-1}$
d
$\mathcal{V}_2 = \mathcal{W}_{m-2}$
$\mathcal{V}_{m-1} = \mathcal{W}_1$
d
$\mathcal{V}_m = \mathcal{W}_0 = \{0\}$

Beispiel 7.2.27: Jordan-Normalform-Algorithmus

Sei $A := \begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 2 & 0 & 2 \\ 1 & 2 & 2 & 1 \\ 2 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{F}_3^{4\times 4}$ hat das MinPoly $\mu_A = \underbrace{(x-2)}_{=:p}^{3=:m}$.
Es gilt

$$\underbrace{(A-2\mathrm{I}_4)^2}_{\nu^{m-1}} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 1 \end{pmatrix} \Rightarrow \operatorname{Rang}(A-\mathrm{I}_4)^2 = 1$$

$\mathcal{W}_2 = \mathcal{W}_{m-1} = \operatorname{Kern}\nu^{m-1} = \operatorname{Kern}\widetilde{(A-2\mathrm{I}_4)^2} = \langle E_1, E_3, \ldots\rangle$
Klar: $E_2 \notin \mathcal{W}_{m-1}$

$$B_m = B_3 = \left(E_2, (A-2\mathrm{I}_4)E_2, (A-2E_4)^2E_2\right)$$

$${}^{B_m}\widetilde{A}^{B_m} = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix} \Rightarrow A \sim \left(\begin{array}{ccc|c} 2 & 0 & 0 & \cdot \\ 1 & 2 & 0 & \cdot \\ 0 & 1 & 2 & \cdot \\ \hline \cdot & \cdot & \cdot & 2 \end{array}\right) = \operatorname{Diag}(\mathrm{J}_3(2), \mathrm{J}_1(2))$$

Also liefert $B = (B_m, B_{m-2}) = \left(E_2,\ (A-2\mathrm{I}_4)E_2,\ (A-2\mathrm{I}_4)^2E_2,\ E_3\right)$.

Übung 8.2: Jordan-Normalform

Seien $a,b,c,d \in \mathbb{F}_5$ und $A := \left(\begin{array}{c|c} \mathrm{M}_{x^4-1} & \begin{smallmatrix} a & \cdot & \cdot & \cdot \\ \cdot & b & \cdot & \cdot \\ \cdot & \cdot & c & \cdot \\ \cdot & \cdot & \cdot & d \end{smallmatrix} \\ \hline 0 & \mathrm{M}_{x^4-x^3} \end{array}\right) \in \mathbb{F}_5^{8\times 8}$.

$$\Rightarrow \chi_A = \left(x^4+4\right)\left(x^4+4x^3\right) = x^3(x+1)(x+2)(x+3)(x+4)^2$$
$$q := \operatorname{kgV}\left(x^4+4,\ x^4+4x^3\right) = \operatorname{kgV}\left((x+1)(x+2)(x+3)(x+4),\ x^3(x+4)\right)$$
$$= x^3(x+1)(x+2)(x+3)(x+4)$$

Es gilt $q \mid \mu_A \mid \chi_A$ (LA1).

$$\Rightarrow \mu_A = q \vee \mu_A = \chi_A, \text{ d.h. } \mu_A \in \left\{x^3(x+1)(x+2)(x+3)(x+4)^{m_5} \mid m_5 \in \underline{2}\right\}$$

Nur der $p_5 := (x+4)$-Hauptraum würde durch andere Wahl von m_5 in μ_A verändert.
Nach 7.1.3 gilt: $\operatorname{Dim}\operatorname{Kern} p_i^{m_i} = c_i \cdot \operatorname{Grad} p_i$ für $\mu_A = \prod_i p_i^{m_i},\ \chi_A = \prod_i p_i^{c_i}$
Bestimme also $\operatorname{Dim}_K \mathcal{V}_5 = \operatorname{Dim}_K\left(\operatorname{Kern}\left(\widetilde{A+4\mathrm{I}_8}\right)\right) = \operatorname{Dim}_K\left(\operatorname{Kern}\left(\widetilde{A-\mathrm{I}_8}\right)\right)$.
Gauß liefert: $\operatorname{Rang}(A-\mathrm{I}_8) = \begin{cases} 6 & \text{falls } d = 0 \\ 7 & \text{falls } d \neq 0 \end{cases}$

$$\Rightarrow \operatorname{Dim}\operatorname{Kern}\left(\widetilde{A-\mathrm{I}_8}\right) = \operatorname{Dim}\mathcal{V} - \operatorname{Dim}\operatorname{Bild}\left(\widetilde{A-\mathrm{I}_8}\right) = \operatorname{Dim}\mathcal{V} - \operatorname{Rang}A = \begin{cases} 2 & \text{falls } d = 0 \\ 1 & \text{falls } d \neq 0 \end{cases}$$

⋮

FALL 1: $d = 0$

$$\operatorname{Dim}_K \operatorname{Kern} \widetilde{(A - \mathrm{I}_8)^2} \overset{7.2.26}{>} \operatorname{Dim}_K \operatorname{Kern} \widetilde{(A - \mathrm{I}_8)} = 2 = 2 \cdot \operatorname{Grad}(x-1)$$

Für $m_5 = 2$ folgt $\lightning \Rightarrow m_5 = 1$. $\Rightarrow$ Elementarteiler sind $x-1,\ \mu_A$.

$$\begin{aligned}
\operatorname{RKF}(A) &= \operatorname{Diag}\left(\mathrm{M}_{x-1},\ \mathrm{M}_{\mu_A}\right) \\
\operatorname{PRF}(A) &= \operatorname{Diag}(\mathrm{M}_{x-1},\ \mathrm{M}_{x^3},\ \mathrm{M}_{x-1},\ \mathrm{M}_{x-2},\ \mathrm{M}_{x-3},\ \mathrm{M}_{x-4}) \\
\operatorname{JNF}(A) &= \operatorname{Diag}(\mathrm{J}_1(x-1),\ \mathrm{J}_3(x),\ \mathrm{J}_1(x-1),\ \mathrm{J}_1(x-2),\ \mathrm{J}_1(x-3),\ \mathrm{J}_1(x-4)) \\
&= \operatorname{Diag}\left(1,\ \begin{pmatrix} \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \end{pmatrix},\ 1,\ 2,\ 3,\ 4\right)
\end{aligned}$$

FALL 2: $d \neq 0$

Falls $m_5 = 1 \Rightarrow \operatorname{Dim}_K \operatorname{Kern}\left(\widetilde{A - \mathrm{I}_8}\right) = 1 \neq 2 = 2 \cdot \operatorname{Grad}(x-1) \lightning \Rightarrow m_5 = 2$

Elementarteiler ist nur $\mu_A = \chi_A$.

$$\begin{aligned}
\operatorname{RKF}(A) &= \mathrm{M}_{\mu_A} \\
\operatorname{PRF}(A) &= \operatorname{Diag}\left(\mathrm{M}_{(x-1)^2},\ \mathrm{M}_{x^3},\ \mathrm{M}_{x-3},\ \mathrm{M}_{x-4}\right) \\
\operatorname{JNF}(A) &= \operatorname{Diag}(\mathrm{J}_2(x-1),\ \mathrm{J}_3(x),\ \mathrm{J}_1(x-2),\ \mathrm{J}_1(x-3),\ \mathrm{J}_1(x-4))
\end{aligned}$$

Übung 8.4: JORDAN-NORMALFORM-ALGORITHMUS

Sei $A := \begin{pmatrix} 2 & -4 & -2 & 4 \\ 1 & 1 & -1 & 1 \\ \cdot & -1 & 1 & 1 \\ 1 & 2 & \cdot & \cdot \end{pmatrix} \in K^{4\times 4}$.

GESUCHT: $J_K := \operatorname{JNF}(A)$ und $X_K \in \mathrm{GL}_4(K)$ mit $X_K A X_K^{-1} = J_K$ für...

(i) $K = \mathbb{F}_2$:

$$\Rightarrow A = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & 1 & 1 \\ \cdot & 1 & 1 & 1 \\ 1 & \cdot & \cdot & \cdot \end{pmatrix} \in \mathbb{F}_2^{4\times 4}$$

Es ist $\mu_A = x^2$, da $A^2 = 0$ in $\mathbb{F}_2$.

$$\begin{aligned}
&\Rightarrow \nu = \widetilde{A} + 0 \cdot \mathrm{id}_{\mathbb{F}_2^{4\times 1}} = \widetilde{A} \\
&\Rightarrow \mathcal{W}_0 = \operatorname{Kern} \nu^0 = \{0\}, \\
&\quad \mathcal{W}_1 = \operatorname{Kern} \nu^1 = \operatorname{Kern} \widetilde{A}, \\
&\quad \mathcal{W}_2 = \operatorname{Kern} \nu^2 = \operatorname{Kern} 0 = \mathbb{F}_2^{4\times 1}
\end{aligned}$$

Es ist $\mathcal{W}_1 = \operatorname{Kern} \widetilde{A} = \left\langle \begin{pmatrix} \cdot \\ 1 \\ \cdot \\ 1 \end{pmatrix}, \begin{pmatrix} \cdot \\ \cdot \\ 1 \\ 1 \end{pmatrix} \right\rangle$ (Gauß). Klar: $e_1, e_2 \notin \mathcal{W}_1$.

$$\Rightarrow B = \left(\begin{pmatrix} \cdot \\ 1 \\ \cdot \\ 1 \end{pmatrix}, \begin{pmatrix} \cdot \\ \cdot \\ 1 \\ 1 \end{pmatrix}, e_1, e_2 \right) \text{ ist Basis von } \mathcal{W}_2 = \mathbb{F}_2^{4\times 1}$$

$$\Rightarrow B_2 = (e_1, v(e_1), e_2, v(e_2)) = \left(e_1, \begin{pmatrix} \cdot \\ 1 \\ \cdot \\ 1 \end{pmatrix}, e_2, \begin{pmatrix} \cdot \\ 1 \\ 1 \\ \cdot \end{pmatrix} \right)$$

$$\Rightarrow {}^{B_2}\widetilde{A}^{B_2} = \mathrm{Diag}(\mathrm{J}_2(0),\ \mathrm{J}_2(0)) = \left(\begin{array}{cc|cc} \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \end{array}\right) = J_{\mathbb{F}_2} \text{ und } X_{\mathbb{F}_2} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & 1 & 1 \\ \cdot & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & \cdot \end{pmatrix}$$

(ii) $K = \mathbb{Q}$

Bestimme μ_A: Algorithmus liefert $\chi_A = \mu_A = \mu_{A,e_4} = (x-2)^2 \cdot \underbrace{(x^2-2)}_{\substack{\text{zerfällt nicht} \\ \text{über } \mathbb{Q}}}$

$$\Rightarrow \mathrm{RKF}(A) = \mathrm{M}_{\mu_A},\ \mathrm{PRF}(A) = \mathrm{Diag}\left(\mathrm{M}_{(x-2)^2}, \mathrm{M}_{x^2-2}\right)$$
$$= \mathrm{Diag}\left(\mathrm{J}_2(x-2),\ \mathrm{J}_1\left(x^2-2\right)\right) = \mathrm{JNF}(A) = J_{\mathbb{Q}}$$

Bestimme die Haupträume $\mathcal{V}_i$ von $\mathbb{Q}^{4\times 1}$ bzgl. A:

$$\mathcal{V}_1 := \mathrm{Kern}\left(\widetilde{(A-2\mathrm{I}_4)^2}\right) = \left\langle \begin{pmatrix} 1 \\ \cdot \\ \cdot \\ \cdot \end{pmatrix}, \begin{pmatrix} \cdot \\ 1 \\ \cdot \\ 1 \end{pmatrix} \right\rangle$$

$$\mathcal{V}_2 := \mathrm{Kern}\left(\widetilde{A^2-2\mathrm{I}_4}\right) = \left\langle \begin{pmatrix} 1 \\ \cdot \\ \cdot \\ -1 \end{pmatrix}, \begin{pmatrix} \cdot \\ \cdot \\ 1 \\ 1 \end{pmatrix} \right\rangle$$

Es ist $\mu_{\widetilde{A}|_{\mathcal{V}_1}} = (x-2)^2$. Setze $v_1 := \widetilde{A} - 2\mathrm{id}_{\mathcal{V}_1}$.

$$\Rightarrow \mathcal{W}_0 = \mathrm{Kern}\, v_1^0 = \{0\}$$

$$\mathcal{W}_1 = \mathrm{Kern}\, v_1^1 = \left\langle \begin{pmatrix} \cdot \\ 1 \\ \cdot \\ 1 \end{pmatrix} \right\rangle \text{ (Gauß)}$$

$$\mathcal{W}_2 = \mathrm{Kern}\, v_1^2 = \mathrm{Kern}\, 0 = \mathcal{V}_1$$

Klar: $e_1 \notin \mathcal{W}_1$ und $\mathcal{W}_1 + \langle e_1 \rangle = \mathcal{V}_1$.

$$\Rightarrow B_2^{(1)} := (e_1, v(e_1)) = \left(e_1, \begin{pmatrix} \cdot \\ 1 \\ \cdot \\ 1 \end{pmatrix} \right) \text{ mit } {}^{B_2^{(1)}}\widetilde{A}\big|_{\mathcal{V}_1}{}^{B_2^{(1)}} = \mathrm{J}_2(x-2)$$

Es ist $\mu_{A|_{\mathcal{V}_2}} = x^2 - 2$. Setze $v_2 := \widetilde{A}^2 - 2\mathrm{id}_{\mathcal{V}_2}$.

$$\Rightarrow \mathcal{W}_0 = \operatorname{Kern} v_2^2 = \{0\}$$
$$\mathcal{W}_1 = \operatorname{Kern} v_2^1 = \operatorname{Kern} 0 = \mathcal{V}_2$$

Da $x^2 - 2$ vom Grad 2 ist, muss im Algorithmus zur Ergänzung von $\mathcal{W}_0$ zu einer Basis von $\mathcal{W}_1$ nicht nur der Vektor V, sondern auch das Bild des Vektors AV zur Basis hinzugefügt werden.

$$\Rightarrow B_1^{(2)} := \left(\begin{pmatrix} 1 \\ \cdot \\ \cdot \\ -1 \end{pmatrix}, A \begin{pmatrix} 1 \\ \cdot \\ \cdot \\ -1 \end{pmatrix} \right) = \left(\begin{pmatrix} 1 \\ \cdot \\ \cdot \\ -1 \end{pmatrix}, \begin{pmatrix} -2 \\ \cdot \\ -1 \\ 1 \end{pmatrix} \right)$$

$$\Rightarrow {}^{B_2^{(1)} B_1^{(2)}}\widetilde{A}^{B_2^{(1)} B_1^{(2)}} = J_{\mathbb{Q}} \Rightarrow X_{\mathbb{Q}} = \begin{pmatrix} 1 & 0 & 1 & -2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & -1 & 1 \end{pmatrix}$$

(iii) $K = \mathbb{C}$

Hier zerfällt μ_A in $\mu_A = (x-2)^2 \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$.

- Für $x - 2$ nehme $B_1 := B_2^{(1)}$ aus (ii).
- $x - \sqrt{2}$: $\mathcal{W}_0 = \{0\}$, $\mathcal{W}_1 = \left\langle \begin{pmatrix} -\sqrt{2} \\ 0 \\ 1+\sqrt{2} \\ 1 \end{pmatrix} \right\rangle \Rightarrow B_2 := \left(\begin{pmatrix} -\sqrt{2} \\ 0 \\ 1+\sqrt{2} \\ 1 \end{pmatrix} \right)$, ${}^{B_2}\widetilde{A}^{B_2} = \mathrm{J}_1\left(x - \sqrt{2}\right) = \left(\sqrt{2}\right)$
- $x + \sqrt{2}$: $\mathcal{W}_0 = \{0\}$, $\mathcal{W}_1 = \left\langle \begin{pmatrix} -\sqrt{2} \\ 0 \\ 1-\sqrt{2} \\ 1 \end{pmatrix} \right\rangle \Rightarrow B_3 := \left(\begin{pmatrix} -\sqrt{2} \\ 0 \\ 1-\sqrt{2} \\ 1 \end{pmatrix} \right)$, ${}^{B_3}\widetilde{A}^{B_3} = \mathrm{J}_1\left(x + \sqrt{2}\right) = \left(-\sqrt{2}\right)$

$$\Rightarrow J_{\mathbb{C}} = \mathrm{JNF}(A) = \mathrm{Diag}\left(\mathrm{J}_2(x-2), \mathrm{J}_1\left(x - \sqrt{2}\right), \mathrm{J}_1\left(x + \sqrt{2}\right)\right) = \begin{pmatrix} 2 & 0 & \cdot & \cdot \\ 1 & 2 & \cdot & \cdot \\ \cdot & \cdot & \sqrt{2} & 0 \\ \cdot & \cdot & 0 & \sqrt{2} \end{pmatrix}$$

$$X_{\mathbb{C}} = (B_1, B_2, B_3) = \begin{pmatrix} 1 & 0 & \sqrt{2} & -\sqrt{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1+\sqrt{2} & 1-\sqrt{2} \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

7.2.e Eine Anwendung: Lineare Differentialgleichungssysteme

In diesem Abschnitt wollen wir die Jordan-Normalform benutzen, um lineare Differentialgleichungssysteme zu lösen. Im Wesentlichen geht es um die Berechnung der Matrixexponentialfunktion.

$$y'(t) = \underset{\in \mathbb{R}}{a}\, y(t) \Longleftrightarrow y = ce^{at}$$

Definition 7.2.28: Lineares Differentialgleichungssystem

Sei $A \in \mathbb{R}^{n\times n}$. Sind $u_i(t)$ reelle differenzierbare Funktionen $\forall i \in \underline{n}$, so setze

$$u(t) := \begin{pmatrix} u_1(t) \\ \vdots \\ u_n(t) \end{pmatrix} \text{ und } u'(t) := \begin{pmatrix} u_1'(t) \\ \vdots \\ u_n'(t) \end{pmatrix}$$

Dann heißt

$$u'(t) = Au(t) \qquad (*)$$

ein **lineares Differentialgleichungssystem** (mit konstanten Koeffizienten).
Die Lösungsmenge von $(*)$ ist

$$L(*) = \{u(t) \mid u_i(t) \text{ reelle, diffbare Funktionen mit } u'(t) = Au(t)\}$$

Satz 7.2.29: Matrixexponentialfunktion

(Aus der Analysis, aber auch über den formalen Potenzreihen $K[[x]]$ rein algebraisch über jedem Körper beweisbar.)

Sei $A \in \mathbb{R}^{n\times n}$. Dann ist die **Exponentialreihe**

$$\exp(A) := \sum_{k=0}^{\infty} \frac{1}{k!} A^k$$

konvergent und die Abbildung $\mathbb{R} \to \mathbb{R}^{n\times n}$, $t \mapsto \exp(tA)$ auf jedem beschränkten Intervall gleichmäßig stetig bzgl. der Maximumsnorm $\|M\| := \max\{M_{i,j} \mid i,j \in \underline{n}\}$.

Bemerkung 7.2.30: Eigenschaften der Matrixexponentialfunktion

Seien $A, B \in \mathbb{R}^{n\times n}$. Dann gilt:

(1) Aus $AB = BA$ folgt

$$\exp(A)\exp(B) = \exp(B)\exp(A) = \exp(A+B)$$

(2) $\exp(0) = \mathrm{I}_n$

(3) $\exp(A)$ ist invertierbar mit $\exp(A)^{-1} = \exp(-A)$.

(4) $\frac{\mathrm{d}}{\mathrm{d}t}(\exp(tA)) = A\exp(tA) = \exp(tA)A$

Beweis zu 7.2.30:

(1) Gelte $AB = BA$. Dann ist

$$\begin{aligned} \exp(A+B) &= \sum_{k=0}^{\infty} \frac{1}{k!}(A+B)^k \\ &= \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} A^j B^{k-j} \\ &= \sum_{k=0}^{\infty} \sum_{j=0}^{k} \frac{1}{k!} \frac{k!}{j!(k-j)!} A^j B^{k-j} \\ &= \left(\sum_{j=0}^{\infty} \frac{1}{j!} A^j\right)\left(\sum_{m=0}^{\infty} \frac{1}{m!} B^m\right) \\ &= \exp(A)\exp(B) \end{aligned}$$

Andere Gleichung ist klar, tausche A und B.

(2) Klar.

(3) Folgt sofort aus den ersten beiden Punkten.

(4) Gliedweise Differentiation.

□

Satz 7.2.31:

(aus der Analysis)

Sei $A \in \mathbb{R}^{n\times n}$. Das lineare Differentialgleichungssystem

$$u'(t) = Au(t)$$

hat die Lösungsmenge

$$L = \{u : \mathbb{R} \to \mathbb{R}^n \mid u(t) = \exp(tA)c \text{ mit } c \in \mathbb{R}^n\}$$

Die eindeutige Lösung des Anfangswertproblems

$$u'(t) = Au(t),\ u(t_0) = u_0 \in \mathbb{R}^n$$

ist $u(t) = \exp(A(t-t_0))u_0$.

Diese Lösungsmenge ist ein VR der Dimension n. Ist $(b_1,\dots,b_n)$ eine Basis von $\mathbb{R}^n$, so ist

$$(\exp(tA)b_1,\dots,\exp(tA)b_n)$$

eine Basis des Lösungsraums.
Die Jordan-Normalform von A wird benutzt, um eine solche Basis zu finden.
Wir formilieren dies nur für zyklische VRe mit $\mu_A = \chi_A = (x-\lambda)^n$. Der allgemeine Fall folgt durch einfaches Zusammensetzen im Sinne des Hauptsatzes (Moduln „bestehen“ aus zyklischen Moduln).

Satz 7.2.32:

Sei $A \in \mathbb{R}^{n\times n}$, $\mu_A = \chi_A = (x-\lambda)^n$. Sei $b_1 \in \mathbb{R}^n$ ein zyklischer Vektor, also

$$b_2 := (A - \lambda \mathrm{I}_n)b_1,$$
$$\vdots$$
$$b_n := (A-\lambda \mathrm{I}_n)^{n-1}b_1 = (A-\lambda \mathrm{I}_n)b_{n-1}$$

und $Ab_n = \lambda b_n$.
Dann ist $(b_1,\dots,b_n)$ eine Basis von $\mathbb{R}^n$ und $(\exp(tA)b_1,\dots,\exp(tA)b_n)$ eine Basis des Lösungsraums L.
Es gilt für $l \in \underline{n}$ $\forall k \in \mathbb{N}$:

$$A^k b_l = \sum_{j=0}^{n-l} \lambda^{k-j} \binom{k}{j} b_{j+l}$$

und für alle $t \in \mathbb{R}$:

$$\exp(tA)b_l = \underbrace{\exp(t\lambda)}_{\in \mathbb{R}} \underbrace{\left(\sum_{j=0}^{n-l} \frac{t^j}{j!} b_{j+l}\right)}_{\in \mathbb{R}^n}$$

(jetzt nur noch eine endliche Summe von Vektoren, und eine normale e-Funktion).

Beweis zu 7.2.32:

Wir zeigen, dass für die längste Summe ($l = 1$) gilt:

$$A^k b_1 = \sum_{j=0}^{n-1} \lambda^{k-j} \binom{k}{j} b_{j+1}$$

(die Aussage für $l > 1$ ist analog, sogar Spezialfall). Dazu gehen wir mit Induktion nach k vor. Für $k = 0$ trivial: $b_1 = b_1$
Der Induktionsschritt:

$$\begin{aligned}
A^{k+1} b_1 = A\left(A^k b_1\right) &= A\left(\sum_{j=0}^{n-1} \lambda^{k-j} \binom{k}{j} b_{j+1}\right) \\
&= \sum_{j=0}^{n-1} \lambda^{k-j} \binom{k}{j} b_{j+2} + \sum_{j=0}^{n-1} \lambda^{k-j} \binom{k}{j} b_{j+1} \\
&= \sum_{j=0}^{n-1} \lambda^{k-j+1} \binom{k}{j-1} b_{j+1} + \sum_{j=0}^{n-1} \lambda^{k-j+1} \binom{k}{j+1} b_{j+1} \\
&= \sum_{j=0}^{n-1} \lambda^{l-j+1} \left(\binom{k}{j-1} + \binom{k}{j}\right) b_{j+1} \\
&= \sum_{j=0}^{n-1} \lambda^{k+1-j} \binom{k+1}{j} b_{j+1}
\end{aligned}$$

□Induktion.

Mit dieser Formel beweisen wir:

$$\begin{aligned}
\exp(tA) b_l &= \sum_{k=0}^{\infty} \frac{t^k}{k!} \left(A^k b_l\right) \\
&= \sum_{k=0}^{\infty} \frac{t^k}{k!} \sum_{j=0}^{n-l} \lambda^{k-j} \binom{k}{j} b_{j+l} \\
&= \sum_{k=0}^{\infty} \sum_{j=0}^{n-l} \frac{t^{k-j}}{(k-j)!} \lambda^{k-j} \cdot \frac{t^j}{j!} b_{j+l} \\
&= \underbrace{\left(\sum_{i=0}^{\infty} \frac{t^i}{i!} \lambda^i\right)}_{\exp(t\lambda)} \left(\sum_{j=0}^{n-l} \frac{t^j}{j!} b_{j+l}\right)
\end{aligned}$$

□

8 Gruppen & Operationen

8.1 Operationen von Gruppen auf Mengen

8.1.a Wiederholung und erste Beispiele

Eine **Gruppe** ist eine Menge G mit einer Verknüpfung $\cdot : G \times G \to G$ mit Assoziativgesetz, einem Neutralelement und einem Inversen zu jedem Element. Ist eine Gruppe kommutativ, so heißt sie **Abelsche Gruppe**.

Die **Ordnung** der Gruppe G ist die Anzahl der Elemente in G, also $\operatorname{ord} G = |G| = \begin{cases} n \in \mathbb{N} & \text{falls } G \text{ endlich} \\ \infty & \text{falls } G \text{ unendlich} \end{cases}$

Für $g \in G$ ist $\operatorname{ord} g := |\langle g \rangle|$ die **Ordnung vom Element g**, mit $\langle g \rangle := \{g^z \mid z \in \mathbb{Z}\}$ (zyklische Untergruppe).
G heißt **zyklische Gruppe**, falls $\exists g \in G : \langle g \rangle = G$.

Die zyklische Gruppe der Ordnung n bezeichnen wir mit $\mathrm{C}_n := \left(\mathbb{Z}/n\mathbb{Z}, +\right)$ (falls man sie additiv schreibt). Zyklische Gruppen sind Abelsch.
Nach dem Hauptsatz über e.e. Abelsche Gruppen ist jede solche eine direkte Summe (bzw. direktes Produkt) von zyklischen.

Weitere bereits bekannte Beispiele für Gruppen:

- die **symmetrische Gruppe**:

$$\mathrm{S}_n = \mathrm{S}_{\underline{n}} = \{\pi : \underline{n} \to \underline{n} \mid \pi \text{ bijektiv}\}$$

mit $|\mathrm{S}_n| = n!$

- die **Generelle lineare Gruppe** eines VRes $\mathcal{V}$ der invertierbaren Endomorphismen: $\mathrm{GL}(\mathcal{V})$
- die **Generelle lineare Gruppe** der invertierbaren $n \times n$-Matrizen über einem (kommutativen) Ring R: $\mathrm{GL}_n(R)$

Definition 8.1.1: Operation

G operiert auf M (von links), falls es eine Verknüpfung

$$\begin{aligned} G \times M &\longrightarrow M, \\ (g,\ m) &\longmapsto gm \end{aligned}$$

gibt mit $1m = m$ und $g(hm) = (gh)m \ \forall m \in M,\ g,h \in G$.
Eine Menge mit einer Operation nennt man **G-Menge**, und man schreibt $G \circlearrowright M$.

Bemerkung 8.1.2: Bahn

Die Gruppe G operiere auf M.
Die **Bahn** von $m \in M$ unter G ist definiert als die Teilmenge

$$Gm := \{gm \mid g \in G\}$$

Die Menge aller Bahnen bildet eine Partition (im Mengensinne, s.u.) von M:

$$G\backslash M := \{Gm \mid m \in M\}$$

Zwei Bahnen sind also immer disjunkt oder gleich.
Nicht zu verwechseln mit dem Mengendifferenz-Zeichen! Diese Schreibweise hier bedeutet, wir „faktorisieren" die Menge von links. Man schreibt aber auch manchmal M/G.

Erinnerung: Partition (Mengenlehre)

Eine Partition $\mathcal{P}$ von einer Menge M ist eine Teilmenge $\mathcal{P} \subseteq \mathrm{Pot}(M)$ mit den Eigenschaften:

- $\emptyset \notin \mathcal{P}$
- $\forall X, Y \in \mathcal{P} : X \cap Y = \emptyset \vee X = Y$ (d.h. alle Elemente paarweise disjunkt)
- $M = \bigcup_{X \in \mathcal{P}} X$

Beweis zu 8.1.2:

- $G\backslash M \ni Gm \neq \emptyset$, da $1m \in Gm$.
- Seien $Gm, Gn \in G\backslash M$.
  Angenommen, $Gm \cap Gn \neq \emptyset$, d.h. $\exists x \in Gm \cap Gn :\ x = gm = hn$ für geeignete $g,h \in G$. Dann gilt aber: $m = g^{-1}x = g^{-1}hn \in Gn$ und damit $Gm \subseteq Gn$; sowie gleichzeitig auch $n = h^{-1}x = h^{-1}gm \Rightarrow Gn \subseteq Gm$.
  $\Rightarrow Gm = Gn$
- $M = \bigcup_{m \in M} Gm = \bigcup_{Gm \in G\backslash M} Gm$, da $m = 1m \in Gm \ \forall m \in M$.

□

Korollar 8.1.3: Bahngleichheitsrelation

G operiere auf M. Dann ist die Relation $\sim_G \subseteq M \times M$, definiert durch $a \sim_G b :\Leftrightarrow Ga = Gb$ (a und b liegen in derselben Bahn, d.h. $\exists g \in G : a = gb$), eine ÄR auf M.

Definition 8.1.4: Untergruppe und Stabilisator

Sei G eine Gruppe.

(1) $U \subseteq G$ heißt **Untergruppe** von G und man schreibt $U \leq G$, falls

- $U \neq \emptyset \Leftrightarrow U \ni 1_G$
- $g,h \in U \Rightarrow gh^{-1} \in U$

d.h. U ist unter allen 3 Operationen von G abgeschlossen.
(Man kann eine Gruppe sehen als eine Struktur aus drei Abbildungen:

- Verknüpfung $\cdot : G \times G \to G,\ (g,h) \mapsto gh$ (binär)
- Invertieren: $\cdot^{-1} : G \to G,\ g \mapsto g^{-1}$ (unär)
- Wahl der Eins: $1 : \{*\} \to G,\ * \mapsto 1_G$ (nulär))

(2) G operiere auf M. Für $m \in M$ ist

$$\mathrm{Stab}_G(m) := G_m := \{g \in G \mid gm = m\} \subseteq G$$

der **Stabilisator** von m in G.

Bemerkung 8.1.5:

G operiere auf M.

(1) Für $m \in M$ gilt: $\mathrm{Stab}_G(m) \leq G$.

(2) Ist $m \in M,\ g \in G$, so gilt: $\mathrm{Stab}_G(gm) = g\,\mathrm{Stab}_G(m)\,g^{-1}$
In anderer Schreibweise: $G_{gm} = G_m^g := gG_mg^{-1}$

Beweis zu 8.1.5:

(1)
- $1m = m\ \forall m \in M \Rightarrow 1 \in \mathrm{Stab}_G(m) \Rightarrow \mathrm{Stab}_G(m) \neq \emptyset$
- Ist $h \in \mathrm{Stab}_G(m) \Rightarrow hm = m \Rightarrow h^{-1}hm = h^{-1}m \Leftrightarrow m = h^{-1}m \Rightarrow h^{-1} \in \mathrm{Stab}_G(m)$.
- Seien $g,h \in \mathrm{Stab}_G(m)$, d.h. $gm = m,\ hm = m. \Rightarrow ghm = gm = m \Rightarrow gh \in \mathrm{Stab}_G(m)$

(2) Sei $h \in \mathrm{Stab}_G(gm)$.

$$\Rightarrow hgm = gm$$
$$\Rightarrow g^{-1}hgm = m$$
$$\Rightarrow g^{-1}hg \in \mathrm{Stab}_G(m) \Leftrightarrow h \in g\,\mathrm{Stab}_G(m)\,g^{-1}$$

□

Übung 9.1:

G operiere auf M. Dann operiert G auch auf n-Tupeln von Elementen von M via

$$G \times M^n \longrightarrow M^n,\ (g,(m_1,\ldots,m_n)) \longmapsto (gm_1,\ldots,gm_n)$$

und es gilt $\mathrm{Stab}_G((m_1,\ldots,m_n)) = \bigcap_{i=1}^{n} \mathrm{Stab}_G(m_i)$ für $m \in M^n$.

Beweis:

(i) Man operiert komponentenweise. Sei $m \in M^n$.

- $1m = 1(m_1,\ldots,m_n) \overset{\text{Def.}}{=} (1m_1,\ldots,1m_n) \overset{\text{in } M}{=} (m_1,\ldots,m_n) = m$
- Für $g,h \in G$ gilt:

$$\begin{aligned} g(h(m_1,\ldots,m_n)) &= g(hm_1,\ldots,hm_n) = (g(hm_1),\ldots,g(hm_n)) \\ &= ((gh)m_1,\ldots,(gh)m_n) = (gh)(m_1,\ldots,m_n) \end{aligned}$$

(ii) Intuitiv ist die Form des Stabilisators klar: Damit man auf einem Tupel wie mit Eins operiert, muss auf jeder Komponente wie mit Eins operiert werden.

Es gilt für $m \in M^n$:

$$\begin{aligned}\mathrm{Stab}_G(m) = \mathrm{Stab}_G((m_1,\dots,m_n)) &= \{g \in G \mid g(m_1,\dots,m_n) = (m_1,\dots,m_n)\} \\ &= \{g \in G \mid (gm_1,\dots,gm_n) = (m_1,\dots,m_n)\} \\ &= \left\{g \in G \,\middle|\, \forall i \in \underline{n} : gm_i = m_i\right\}\end{aligned}$$

und damit $s \in \mathrm{Stab}_G((m_1,\dots,m_n)) \Leftrightarrow \forall i \in \underline{n} : sm_i = m_i$

$$\begin{aligned}&\Leftrightarrow \forall i \in \underline{n} :\ s \in \{g \in G \mid gm_i = m_i\} \\ &\Leftrightarrow \forall i \in \underline{n} :\ s \in \mathrm{Stab}_G(m_i) \\ &\Leftrightarrow s \in \bigcap_{i=1}^{n} \mathrm{Stab}_G(m_i)\end{aligned}$$

□

Übung 9.1.ii:

S_4 operiert durch Anwenden auf $M := \underline{4}$. GESUCHT: Vertretersystem der Bahnen auf M^2.

Sei $\pi \in \mathrm{S}_4$, $(a,b) \in M^2$.

FALL 1: $a \neq b$:

$$\pi(a,b) = (\pi(a),\pi(b)),\ \pi(a) \neq \pi(b)$$

da π bijektiv. Sei $(a',b') \in M^2$, $a' \neq b'$.

$$\begin{aligned}&\Rightarrow \exists \pi \in \mathrm{S}_4 : \pi(a) = a',\ \pi(b) = b' \\ &\Rightarrow \pi(a,b) = (a',b') \\ &\Rightarrow \mathrm{S}_4(a,b) = \left\{(a',b') \,\middle|\, a' \neq b'\right\}\end{aligned}$$

FALL 2: $a = b$:

$$\pi(a,b) = \pi(a,a) = (\pi(a),\pi(a))$$

Sei $(a',a') \in M^2$.

$$\begin{aligned}&\Rightarrow \exists \pi \in \mathrm{S}_4 : \pi(a) = a' \\ &\mathrm{S}_4(a,a) = \left\{(a',a') \,\middle|\, a' \in M\right\}\end{aligned}$$

$\Rightarrow \mathrm{S}_4 \backslash M^2 = \{\mathrm{S}_4(1,2),\ \mathrm{S}_4(1,1)\}$ d.h. Vertreter sind z.B. $(1,2)$ und $(1,1)$.

Außerdem gilt:

$$\begin{aligned}\mathrm{Stab}_{\mathrm{S}_4}(1) &= \{\pi \in \mathrm{S}_4 \mid \pi(1) = 1\} \\ &= \left\{\mathrm{id}_M, \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 1&3&2&4\\\hline\end{array}, \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 1&2&4&3\\\hline\end{array}, \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 1&4&3&2\\\hline\end{array}, \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 1&4&2&3\\\hline\end{array}, \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 1&3&4&2\\\hline\end{array}\right\}\end{aligned}$$

$$\mathrm{Stab}_{\mathrm{S}_4}((1,2)) = \{\pi \in \mathrm{S}_4 \mid \pi(1) = 1 \wedge \pi(2) = 2\} = \left\{\mathrm{id}_M, \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 1&2&4&3\\\hline\end{array}\right\}$$

Bemerkung 8.1.6: LINKSNEBENKLASSEN

Sei G eine Gruppe, $U \leq G$ eine Untergruppe.
Dann operiert U auf G durch inverse Rechtsmultiplikation, nämlich

$$U \times G \longrightarrow G,$$
$$(u, g) \longmapsto g u^{-1}$$

(damit Axiome gelten: Sei $u * g := g u^{-1}$. Dann gilt: $u' * (u * g) = (u' \cdot u) g$.)
Die Bahnen

$$gU := \{ g u^{-1} \mid u \in U \} = \{ g u' \mid u' \in U \}$$

heißen **Linksnebenklassen** von U in G.
Die Menge der Linksnebenklassen bezeichnen wir mit G/U.
Die Mächtigkeit von G/U, sprich die Anzahl der Linksnebenklassen,

$$\left| G/U \right| =: [G : U]$$

heißt der **Index** von U in G.

Korollar 8.1.7: SATZ VON LAGRANGE

Sei G eine endliche Gruppe und $U \leq G$. Dann teilt die Ordnung von U die Ordnung von G:

$$|U| \,\big|\, |G|$$

und es gilt: $\frac{|G|}{|U|} = [G : U]$

Bsp.: Wie viele Untergruppen hat S_3?
$|S_3| = 3! = 6$, $|\mathrm{Pot}(S_3)| = 2^6 = 64$
Sind alle Mengen aus der Potenzmenge Untergruppen? Nein!

Lagrange:

$$\mathrm{Pot}(S_3) = \underbrace{\mathrm{Pot}_0(S_3)}_{=\{\emptyset\}} \cup \underbrace{\mathrm{Pot}_1(S_3)}_{\substack{\text{6-elementig,} \\ \text{nur 1 Element} \\ \text{„gut“: } \{1\}}} \cup \underbrace{\mathrm{Pot}_2(S_3)}_{\substack{6 \cdot 5 \text{ (1 muss} \\ \text{drin sein)}}} \cup \underbrace{\mathrm{Pot}_3(S_3)}_{\binom{6}{3}_2 = 20 \not< 15} \cup \underbrace{\mathrm{Pot}_4(S_3)}_{4 \not< 6} \cup \underbrace{\mathrm{Pot}_5(S_3)}_{5 \not< 6} \cup \underbrace{\mathrm{Pot}_6(S_3)}_{=\{S_3\}}$$

↑ Man kann noch mehr einschränken!
So hat man die Anzahl der potenziellen Untergruppen schonmal reduziert auf 22 statt 64. (FYI: tatsächlich gibt es 6 Untergruppen.)

Beweis zu 8.1.7:
Die Abbildung $U \to gU$, $u \mapsto g u^{-1}$ ist eine Bijektion.
Also haben zwei Nebenklassen die gleiche Mächtigkeit, nämlich die von U. Nun ist G eine disjunkte Vereinigung von Bahnen, also $G = g_1 U \cup \cdots \cup g_s U$ mit $s := [G : U]$ und $|G| = \sum_{i=1}^{s} |g_i U| = s\,|U|$. □

Definition 8.1.8: LINEARE OPERATION

Die Operation der Gruppe G auf den K-VR $\mathcal{V}$ heißt **linear**, falls $\forall g \in G$ die Abbildung

$$\hat{g} : \mathcal{V} \longrightarrow \mathcal{V},$$
$$V \longmapsto gV$$

linear ist.

Beispiel 8.1.9:

Sei $M := \mathbb{F}_2^3$. Die symmetrische Gruppe $G = \mathrm{S}_3$ operiert auf M durch

$$(\pi, (a_1, a_2, a_3)) \mapsto \left(a_{\pi^{-1}(1)}, a_{\pi^{-1}(2)}, a_{\pi^{-1}(3)}\right)$$

Bahnen:

$$\{(0,0,0)\}, \{(1,1,1)\}, \{(1,0,0),(0,1,0),(0,0,1)\}, \{(1,1,0),(1,0,1),(0,1,1)\}$$

$$\mathrm{Stab}_{\mathrm{S}_3}((1,1,1)) = \left\{\mathrm{id}, \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 3 & 2 \end{array}\right\}$$

In der Tat ist diese Operation linear:

$${}^{\mathcal{S}}\pi^{\mathcal{S}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

wenn $\mathcal{S}$ die Standardbasis von $\mathbb{F}_2^3$ ist.

Bemerkung 8.1.10:

(1) G operiere auf der Menge M, so erhält man einen Gruppenhomomorphismus

$$\begin{aligned} G &\longrightarrow \mathrm{S}_M, \\ g &\longmapsto (\widehat{g} : m \mapsto gm) \end{aligned}$$

Umgekehrt definiert jeder Gruppenhomomorphismus $\varphi : G \to \mathrm{S}_M$ eine Operation von G auf M. Eine Operation ist also ein Spezialfall von einem Homomorphismus.

(2) Operiere G auf dem K-VR $\mathcal{V}$ linear. So liefert dies einen Gruppenhomomorphismus

$$\begin{aligned} G &\longrightarrow \mathrm{GL}(\mathcal{V}) \leq \mathrm{S}_{\mathcal{V}} \\ g &\longmapsto (\widehat{g} : V \mapsto gV) \end{aligned}$$

(Auch bei „Gruppe auf Gruppe“ wird auf die Automorphismengruppe abgebildet, wie $\mathrm{GL}(\mathcal{V})$.)

Beweis zu 8.1.10:

(1) „⇒“: $\Phi : G \times M \to M$ sei Operation. Sei $\varphi : G \to \mathrm{S}_M$, $g \mapsto \widehat{g} := \Phi(g, \cdot) : m \mapsto gm = \Phi(g,m)$.

$$\begin{aligned} \varphi(g_1 g_2)(m) &= \widehat{g_1 g_2}(m) = (g_1 g_2)m \\ &= g_1(g_2 m) = \widehat{g_1}(\widehat{g_2}(m)) \\ &= \left(\varphi(g_1) \circ \varphi(g_2)\right)(m) \end{aligned}$$

und $\varphi(1) = \mathrm{id}_M$.

„⇐“: Sei $\varphi : G \to \mathrm{S}_M$ ein Gruppenhomomorphismus. $\rightsquigarrow \Phi(g,m) := \varphi(g)(m)$.
z.z.: $\Phi : G \times M \to M$ ist Operation.

- $\Phi(1_G, m) = \varphi(1_G)(m) = \mathrm{id}_M(m) = m$
- $\Phi(gh, m) = \varphi(gh)(m) = \left(\varphi(g) \circ \varphi(h)\right)(m) = \varphi(g)\left(\varphi(h)(m)\right) = \Phi(g, \Phi(h,m))$

(2) Folgt aus (1), da $\widehat{g}$ linear ist.
Aussagen wichtiger als Beweis. □

Definition 8.1.11: Adjektive der Operationen

Die Operation von G auf M heißt

(1) **transitiv**, falls M eine Bahn bildet, d.h. $M = Gm$ für ein $m \in M$ (und somit $\forall m \in M$).

(2) ~~regulär~~ oder **scharf transitiv**, falls sie transitiv ist und der Stabilisator trivial ist, also $\mathrm{Stab}_G(m) = \{1\}$, für ein und somit für alle $m \in M$.

(3) **treu**, falls $gm = m \ \forall m \in M \Rightarrow g = 1$ (nur 1 stabilisiert *alle* Elemente).
„Die Gruppe tut alles, was sie kann" – vgl. „treu linear" = Φ Monomorphismus.

Satz 8.1.12:

Die Gruppe G operiert auf der Menge M. Folgende Aussagen sind äquivalent:

(1) G operiert scharf transitiv.

(2) Zu je zwei $m, n \in M$ gibt es genau ein $g \in G$ mit $gm = n$.
(Man ist versucht, dieses g als eine Art „Richtungsvektor" $\overrightarrow{mn}$ zu bezeichnen; siehe 9.1.3.)

(3) Für jedes feste $m_0 \in M$ ist die Abbildung

$$\begin{aligned} G &\longrightarrow M, \\ g &\longmapsto gm_0 \end{aligned}$$

bijektiv.

(4) $\exists m_0 \in M : (G \to M,\ g \mapsto gm_0)$ ist bijektiv.

Beweis zu 8.1.12:

(1)⇒(2): Wegen der Transitivität existiert ein solches g wie in (2) gefordert, und wegen der trivialen Stabilisatoren ist g auch eindeutig:

$$gm = n = hm \Rightarrow h^{-1}gm = m \Rightarrow h^{-1}g \in \mathrm{Stab}_G(m) = \{1\} \Rightarrow g = h$$

(2)⇒(3): Definiert ist die Abbildung immer. Sie ist surjektiv, da G nach (2) transitiv operiert, und sie ist injektiv wegen der vorausgesetzten Eindeutigkeit.

(3)⇒(4): trivial.

(4)⇒(1): $\mathrm{Stab}_G(m_0) = \{1\}$ wegen der vorausgesetzten Injektivität. Wegen der vorausgesetzten Surjektivität ist die Operation transitiv.

□

Beispiel 8.1.13: Scharf transitive Operationen

(1) G operiert auf sich per Linksmultiplikation scharf transitiv.

$$\begin{aligned} G \times G &\longrightarrow G, \\ (g,h) &\longmapsto gh \end{aligned}$$

Beweis:
z.B. wegen (2): $gh = l \Leftrightarrow g = lh^{-1}$ □

(2) Sei $\mathcal{V}$ ein e.e. K-VR und $\mathcal{B}(\mathcal{V}) \subseteq \mathcal{V}^n$ die Menger aller Basen von $\mathcal{V}$. Dann operiert $\mathrm{GL}(\mathcal{V})$ scharf transitiv auf $\mathcal{B}(\mathcal{V})$ vermöge

$$g(B_1, \ldots, B_n) := (g(B_1), \ldots, g(B_n))$$

(lineare Abbildung definiert durch die Bilder der Basisvektoren).

Beispiel 8.1.14:

Sei $L = \{x \in K^n \mid Ax = b\} \neq \emptyset$ die Lösungsmenge eines LGS, und sei $\mathcal{U} = \{x \in K^n \mid Ax = 0\}$ die Lösungsmenge des dazugehörigen homogenen LGS.
Dann operiert $\mathcal{U}$ auf L scharf transitiv (siehe Schule/LA1): Hat man eine partikuläre Lösung $x_0 \in L$, so ist $\{x + y \mid y \in \mathcal{U}\} = L$ die Lösungsmenge des inhomogenen Systems.

Beispiel 8.1.15:

Ist $\varphi : \mathcal{V} \to \mathcal{W}$ eine lineare Abbildung von K-VRen und $W \in \operatorname{Bild}\varphi$, so operiert $\operatorname{Kern}\varphi$ scharf transitiv auf $\varphi^{-1}(\{W\})$ (Faser).
Dies ist die koordinatenfreie Version von Beispiel 8.1.14.

8.1.b Die Konjugationsoperation

Definition 8.1.16: KONJUGATION

Sei G eine Gruppe. Dann operiert G auf sich selbst durch **Konjugation**

$$\begin{aligned} G \times G &\longrightarrow G, \\ (g,m) &\longmapsto \kappa_g(m) := gmg^{-1} \end{aligned}$$

Die Bahnen dieser Operation heißen **Konjugiertenklassen**. Der Stabilisator von $m \in G$ wird als **Zentralisator** bezeichnet:

$$\mathrm{C}_G(m) := \operatorname{Stab}_G(m) = \left\{g \in G \,\middle|\, g^{-1}mg = m\right\} = \{g \in G \mid gm = mg\}$$

Bemerkung 8.1.17:

Für $g \in G$ ist die Abbildung $\kappa_g : G \to G,\ m \mapsto gmg^{-1}$ ein Gruppenautomorphismus (d.h. bijektiver Gruppenhomomorphismus von G in sich selbst) mit $\kappa_g^{-1} = \kappa_{g^{-1}}$.

Beweis zu 8.1.17:
$\kappa_g(hh') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = \kappa_g(h)\kappa_g(h')$
$\kappa_g(1) = gg^{-1} = 1$
$\kappa_g\left(\kappa_{g^{-1}}(h)\right) = \kappa_g\left(g^{-1}h\left(g^{-1}\right)^{-1}\right) = gg^{-1}hgg^{-1} = h$ □

Übung 8.1.Ü1:

Sei G eine Gruppe.

(1) Die Menge der Automorphismen von G bildet mit der Komposition eine Gruppe $(\operatorname{Aut}(G), \circ)$, die **Automorphismengruppe** von G.

(2) $\kappa : G \to \operatorname{Aut}(G),\ g \mapsto \kappa_g$ ist ein Gruppenhomomorphismus.

(3) Es ist $\operatorname{Kern}\kappa = \mathrm{Z}(G) := \{g \in G \mid gh = hg\ \forall h \in G\}$ das **Zentrum** von G.

Beweis:

(1) Seien $\alpha, \beta, \gamma \in \operatorname{Aut}(G)$. Es gilt:

- Komposition ist generell assoziativ: $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$
- $\mathrm{id}_G \in \operatorname{Aut}(G)$ und $\mathrm{id}_G \circ \alpha = \alpha \circ \mathrm{id}_G = \alpha \Rightarrow 1_{\operatorname{Aut}(G)} = \mathrm{id}_G$
- $\alpha^{-1} \in \operatorname{Aut}(G)$ mit $\alpha \circ \alpha^{-1} = \alpha^{-1}\alpha = \mathrm{id}_G$ per Definition von $\operatorname{Aut}(G)$

Somit ist $\mathrm{Aut}(G)$ eine Gruppe.

(2) Seien $g,h \in G$ beliebig. Für $\kappa(gh) = \kappa_{gh}$ gilt für beliebige $m \in G$:

$$\kappa_{gh}(m) = ghm(gh)^{-1} = ghmh^{-1}g^{-1} = g\left(hmh^{-1}\right)g^{-1} = g(\kappa_h(m))g^{-1} = \kappa_g(\kappa_h(m))$$

$\Rightarrow \kappa_{gh} = \kappa_g \circ \kappa_h \Rightarrow \kappa$ ist Gruppenhomomorphismus.

(3) $g \in \mathrm{Kern}\,\kappa \Leftrightarrow \kappa_g = 1_{\mathrm{Aut}(G)} = \mathrm{id}_G \Leftrightarrow \forall m \in G : gmg^{-1} = m \Leftrightarrow \forall m \in G : gm = mg \Leftrightarrow g \in \mathrm{Z}(G)$

□

Bemerkung 8.1.A1:

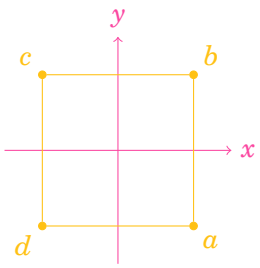
Sei G eine Gruppe.
Dann ist $\mathrm{Z}(G) = \{g \in G \mid |Gg| = 1\}$, wobei Gg die Bahn der Konjugationsoperation ist.

Beweis:

$g \in \mathrm{Z}(G) \Leftrightarrow \forall m \in G :\ gm = mg \Leftrightarrow \forall m \in G :\ mgm^{-1} = g \Leftrightarrow \underbrace{\{mgm^{-1} \mid m \in G\}}_{=Gg} = \{g\} \Leftrightarrow |Gg| = 1$ □

Übung 8.1.Ü2: DIEDERGRUPPE [di'e:dər]

Betrachte $D_8 := \left\langle \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{=:s}, \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{=:r} \right\rangle$ als Symmetriegruppe eines Quadrats.



s ist *Spiegelung*: $sa = c$
r ist *Rotation*: $ra = b$

Genauer: $a = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, $b = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $c = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$, nutze Matrixmultiplikation.

GESUCHT: Untergruppen $U \leq D_8$:

$\mathrm{ord}\,U$	U
1	$\{\mathrm{I}_2\}$
2	Selbstinverse Erzeuger: • alle Spiegelungen – an der Diagonale 1 $\langle s \rangle$ – an der y-Achse $\langle rs \rangle$ – an der Diagonale 2 $\langle r^2 s \rangle$ – an der x-Achse $\langle r^3 s \rangle$ • Drehung um 180° $\langle r^2 \rangle$
4	• reine Drehungen: $\langle r \rangle = \{r^i \mid i \in \underline{4}\}$ • $\langle r^2, s \rangle = \{r^2, s, r^2 s, \mathrm{I}_2\}$ • $\langle r^2, rs \rangle$
8	D_8

Beweis:

Es ist

$$D_8 = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

Schränke die möglichen Untergruppen durch Lagrange (8.1.7) auf 1-, 2-, 4- und 8-elementige Teilmengen mit $1_{D_8} = \mathrm{I}_2$ ein. Zeige dann durch Matrixmultiplikation, welche der Gruppen abgeschlossen sind. □

GESUCHT: Konjugiertenklassen und Zentrum von D_8.
Es sind die Operationen konjugiert, die miteinander vertauschen. Also sind die Konjugiertenklassen:
$D_8\mathrm{I}_2$, $D_8 s$, $D_8 r$, $D_8 sr$, $D_8 r^2$ (nachrechnen: disjunkt und zusammen D_8).
Das Zentrum von D_8 ist $\mathrm{Z}(D_8) = \{\mathrm{I}_2, r^2\} = \{\mathrm{I}_2, -\mathrm{I}_2\}$ (nach 8.1.A1).

8.1.c Parametrisierung aller Mengen mit transitiven Operationen

Wir wollen eine Struktur in allen transitiven G-Mengen finden.

Definition 8.1.18: ÄHNLICHKEIT VON G-MENGEN

Sei G eine Gruppe, M, N zwei G-Mengen.
Eine Abbildung $\varphi : M \to N$ heißt **G-äquivariant**, wenn gilt:

$$\varphi(gm) = g\varphi(m) \ \forall g \in G,\ m \in M$$

M und N heißen **ähnlich** (als G-Mengen), falls es eine G-äquivariante Bijektion $\varphi : M \to N$ gibt; in Zeichen: $M \underset{G}{\cong} N$. Die Abbildung φ heißt dann auch **Ähnlichkeit** der G-Mengen M und N.

Beispiel 8.1.19:

Sind $U \leq S \leq G$ Untergruppen von G, so ist die Abbildung

$$\begin{aligned} G/U &\longrightarrow G/S\,, \\ gU &\longmapsto gS \end{aligned}$$

eine G-äquivariante Abbildung.

Übung 10.1:

Sei G eine Gruppe und $U, V \leq G$ Untergruppen.
Dann ist jede G-äquivariante Abbildung $\varphi : G/U \to G/V$ von der Form

$$\varphi_h : G/U \to G/V\,,\ gU \mapsto ghV \text{ mit } h^{-1}Uh \leq V$$

Beweis:
Sei $\varphi : G/U \to G/V$ eine G-äquivariante Abbildung. Es gilt:

- $\varphi(1U) = hV \in G/V \Rightarrow \varphi(gU) = g\varphi(1U) = ghV$
- $hV = \varphi(1U) = \varphi(uU)$ für $u \in U$
  $= u\varphi(1U) = uhV \ \forall u \in U$
  $\Rightarrow V = h^{-1}uhV \ \forall u \in U$
  $\Rightarrow h^{-1}uh \cdot 1 = h^{-1}uh \in V$
  $\Rightarrow h^{-1}Uh \subseteq V$
- $1 \in h^{-1}Uh \neq \emptyset$, da $1 \in U$
- $h^{-1}uh,\ h^{-1}\tilde{u}h \in h^{-1}Uh$
  $\Rightarrow \left(h^{-1}uh\right)\left(h^{-1}\tilde{u}h\right)^{-1} = \left(h^{-1}uh\right)\left(h^{-1}u^{-1}h\right) = h^{-1}\underbrace{u\tilde{u}}_{\in U}h \in h^{-1}Uh$

□

Satz 8.1.20: BAHNENSATZ

Sei M eine transitive G-Menge und $m \in M$. Dann sind M und $G/\mathrm{Stab}_G(m)$ als G-Mengen ähnlich. Genauer ist die Abbildung

$$\begin{aligned}\overline{\varphi}_m : {}^{G}/_{\mathrm{Stab}_G(m)} &\longrightarrow M,\\ g\,\mathrm{Stab}_G(m) &\longmapsto gm\end{aligned}$$

eine G-Ähnlichkeit.

Beweis zu 8.1.20:
Offenbar ist die Abbildung $\varphi_m : G \to M,\ g \mapsto gm$ eine surjektive G-äquivariante Abbildung, wobei G durch Linksmultiplikation auf sich operiert.
Die Fasern von φ_m sind gerade die Linksnebenklassen von G nach $\mathrm{Stab}_G(m)$:

$$\varphi^{-1}(\{gm\}) = g\,\mathrm{Stab}_G(m)\ \ \forall g \in G$$

Also, nach dem Homomorphiesatz für Mengen, faktorisiert $G/\mathrm{Stab}_G(m)$ mit einer Bijektion $\overline{\varphi}_m$, die offensichtlich G-äquivariant ist. □

Der Bahnensatz besagt:

$${}^{G}/_{\mathrm{Stab}_G(m)} \cong M \not\cong Gm \text{ wenn } M \text{ nicht transitiv}$$

→ Sonderfall des Homomorphiesatzes!

Beweis zu 8.1.20:
(Alternative)
Seien M, N zwei G-Mengen und $f : M \to N$ eine G-äquivariante Abbildung.

(i) G operiert auf $M/\sim_f$ durch

$$\begin{aligned}G \times {}^{M}/_{\sim_f} &\longrightarrow {}^{M}/_{\sim_f},\\ (g,\ [m]_f) &\longmapsto [gm]_f\end{aligned}$$

(wohldefiniert, da f G-äquivariant ist). G operiert außerdem auf $f(M)$ durch

$$\begin{aligned}G \times f(M) &\longrightarrow f(M),\\ (g, n) &\longmapsto gn\end{aligned}$$

und $M/\sim_f \underset{G}{\cong} f(M)$ vermöge

$$\varphi : {}^{M}/_{\sim_f} \longrightarrow f(M),\ [m]_f \longmapsto f(m)$$

nach dem Homomorphiesatz für Mengen, wobei φ durch die Definition über f auch G-äquivariant ist.

(ii) Es gilt $[m] = f^{-1}(\{f(m)\})$. Ist M eine transitive G-Menge, so gilt: $f^{-1}(\{n\}) = \mathrm{Stab}_G(n)\,m$ für $m \in f^{-1}(m)$, da $\mathrm{Stab}_G(f(m))\,m = \{g \in G \mid f(gm) = f(m)\}\,m = [m]_f = f^{-1}(\{f(m)\})$.

(iii) Sei Ω eine G-Menge. Dann ist $\forall \omega \in \Omega : M/\mathrm{Stab}_G(\omega) \underset{G}{\cong} G\omega$ vermöge

$$\psi_\omega : G \longrightarrow \Omega,\ g \longmapsto g\omega$$

Es ist $\psi_\omega(G) = G\omega$, und ψ_ω ist G-äquivariant.
Nach (ii) ist jedes Element $[g]_{\psi_\omega} \in G/\sim_{\psi_\omega}$ ist von der Form $g\,\mathrm{Stab}_G(\omega)$ (Linksnebenklasse zu $\mathrm{Stab}_G(\omega)$).
Damit ist $G/\sim_{\psi_\omega} = G/\mathrm{Stab}_G(\omega)$. Und mit (i) folgt jetzt: $G/\mathrm{Stab}_G(\omega) \underset{G}{\cong} G\omega$.

□

In anderen Worten: Alle transitiven G-Mengen findet man „in der Gruppe“ wieder.

$$\begin{aligned} G \times G/U &\longrightarrow G/U\,, \\ (g, hU) &\longmapsto ghU \end{aligned}$$

Gegeben G, $U \leq G$, SUCHE G-Menge M und $m \in M$ mit $\mathrm{Stab}_G(m) = U$.
ANTWORT: $M := G/U$, $m := U$.
Wäre $n := gU$: $\mathrm{Stab}_G(n) = \mathrm{Stab}_G(gm) = g\underbrace{\mathrm{Stab}_G(m)}_{=U}g^{-1} = gUg^{-1}$
$\Rightarrow G/U \underset{G}{\cong} G/gUg^{-1}$

Korollar 8.1.21:

Die Gruppe G operiere auf der Menge M. Sei $m \in M$ mit $|Gm| < \infty$. Dann gilt: Die Länge der Bahn ist gleich dem Index des Stabilisators:

$$|Gm| = [G : \mathrm{Stab}_G(m)] := \left|G/\mathrm{Stab}_G(m)\right|$$

und falls $|G| < \infty$, dann gilt:

$$|Gm| = \frac{|G|}{|\mathrm{Stab}_G(m)|}$$

Dies gibt uns eine Strategie, wie wir Mengenmächtigkeiten, aber auch Gruppenordnungen bestimmen können.

Beispiel 8.1.22: BESTIMMUNG DER ORDNUNG DER GENERELLEN LINEAREN GRUPPE

Sei $\mathbb{F}_q$ ein Körper mit $q = p^a$ Elementen (p prim).

$$\mathrm{GL}_n(\mathbb{F}_q) = \left\{X \in \mathbb{F}_q^{n\times n} \,\middle|\, \det X \neq 0\right\}$$

Dann gilt:

$$\begin{aligned} \left|\mathrm{GL}_n(\mathbb{F}_q)\right| &= q^{\binom{n}{2}}(q^{n-1}-1)\cdots(q-1) \\ &= (q^n-1)(q^n-q)\cdots\left(q^n-q^{n-1}\right) \end{aligned}$$

Vgl.: $|\mathrm{S}_n| = n! = \underbrace{(n-0)}_{n}(n-1)\cdots\underbrace{(n-(n-1))}_{1}$
Frappierende Analogie! Man kann es als eine Art „Grenzwertproblem“ sehen:
Die S_n wäre die $\mathrm{GL}_n(K)$, wenn K ein einelementiger Körper wäre (den es nicht gibt).

Beweis zu 8.1.22:
$\mathrm{GL}_n(\mathbb{F}_q)$ operiert auf $\mathbb{F}_q^{n\times 1} \setminus \{0\}$ transitiv. Denn: $V \mapsto W$? Ergänze V zu Basis $V = V_1, V_2, \ldots, V_n$ und W zu Basis $W = W_1, W_2, \ldots, W_n$, bilde Basisvektor auf Basisvektor ab $\Rightarrow$ bijektive Abbildung.

$$\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}\left(\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}\right) = \left\{\left(\begin{array}{c|c} 1 & *\cdots* \\ \hline 0 & \\ \vdots & X \\ 0 & \end{array}\right) \,\middle|\, *\cdots* \in \mathbb{F}_q^{1\times(n-1)},\ X \in \mathrm{GL}_{n-1}(\mathbb{F}_q)\right\}$$

$$\Rightarrow \mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(e_1) = \left|\mathbb{F}_q^{1\times(n-1)}\right| \cdot \left|\mathrm{GL}_{n-1}(\mathbb{F}_q)\right| = q^{n-1} \cdot \left|\mathrm{GL}_{n-1}(\mathbb{F}_q)\right|$$

Nach dem Bahnensatz 8.1.20 und 8.1.21

$$\Rightarrow \left|\mathrm{GL}_n(\mathbb{F}_q)\right| = \left|\mathrm{GL}_n(\mathbb{F}_q)\,e_1\right| \cdot \left|\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(e_1)\right| = (q^n-1)\cdot q^{n-1}\left|\mathrm{GL}_{n-1}(\mathbb{F}_q)\right|$$

und beachte, dass $\left|\mathrm{GL}_1(\mathbb{F}_q)\right| = q-1$ (invertierbare Elemente im Körper). □

Beispiel 8.1.A2: VGL.:

(1) S_n operiert transitiv auf $\underline{n}$. ($G = \mathrm{S}_n$, $M = \underline{n}$, $m = n$)

$$|\mathrm{S}_n| = |\mathrm{S}_n m| \cdot \left|\mathrm{Stab}_{\mathrm{S}_n}(m)\right| = n \cdot |\mathrm{S}_{n-1}|$$

(2) Definiere $\binom{\underline{n}}{k} := \mathrm{Pot}_k(\underline{n}) = \{X \subseteq \underline{n} \mid |X| = k\}$. GESUCHT: $\binom{n}{k} := \left|\binom{\underline{n}}{k}\right|$
ANTWORT: S_n operiert auf $\underline{n}$ transitiv und daraufhin auf $\binom{\underline{n}}{k}$ ebenfalls transitiv, und zwar elementweise. $G = \mathrm{S}_n$, $M = \binom{\underline{n}}{k}$, $m = \underline{k}$.

$$|G| = |Gm| \cdot |\mathrm{Stab}_G(m)|$$
$$n! = \left|\binom{\underline{n}}{k}\right| \cdot \underbrace{\left|\mathrm{Stab}_{\mathrm{S}_n}(\underline{k})\right|}_{\left|\mathrm{S}_k \times \mathrm{S}_{\underline{n}\setminus\underline{k}}\right| = |\mathrm{S}_k \times \mathrm{S}_{n-k}| = |\mathrm{S}_k| \cdot |\mathrm{S}_{n-k}| = k! \cdot (n-k)!}$$
$$\overset{\cdot|\mathrm{Stab}\ldots|}{\Longrightarrow} \binom{n}{k} = \left|\binom{\underline{n}}{k}\right| = \frac{n!}{k!(n-k)!}$$

Übung 8.1.Ü3: GAUSSSCHER BINOMIALKOEFFIZIENT

Sei $\mathscr{U}\left(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q\right) := \left\{X \mid X \leq_{\mathbb{F}_q} \mathbb{F}_q^{n\times 1}\right\}$ die Menge der $\mathbb{F}_q$-Teilräume von $\mathbb{F}_q^{n\times 1}$ und

$$\mathscr{U}_k\left(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q\right) := \left\{X \leq_{\mathbb{F}_q} \mathbb{F}_q^{n\times 1} \mid \mathrm{Dim}_{\mathbb{F}_q} X = k\right\}$$

die Menge der k-dimensionalen Teilräume, mit $q := p^m$, p prim, $n, m \in \mathbb{N}$, $k \in \mathbb{Z}_{\geq 0}$. Dann ist

$$\left|\mathscr{U}_k\left(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q\right)\right| = \frac{\left|\mathrm{GL}_n(\mathbb{F}_q)\right|}{\left|\mathrm{GL}_k(\mathbb{F}_q)\right| \cdot \left|\mathrm{GL}_{n-k}(\mathbb{F}_q)\right| \cdot q^{k(n-k)}} =: \begin{bmatrix} n \\ k \end{bmatrix}_q$$

der **Gaußsche Binomialkoeffizient**.

Beweis:
$\mathrm{GL}_n(\mathbb{F}_q)$ operiert transitiv auf $\mathbb{F}_q^{n\times 1} \setminus \{0\}$ durch Linksmultiplikation. Daher operiert $\mathrm{GL}_n(\mathbb{F}_q)$ auch transitiv auf $\mathscr{U}_k\left(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q\right)$, nämlich elementweise durch:

$$\begin{aligned} \mathrm{GL}_n(\mathbb{F}_q) \times \mathscr{U}_k\left(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q\right) &\longrightarrow \mathscr{U}_k\left(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q\right), \\ (g, \langle B\rangle) &\longmapsto \langle gB\rangle \end{aligned}$$

wobei B eine geordnete Basis des jeweiligen $\mathbb{F}_q^{n\times 1}$-Teilraums ist und $\mathrm{GL}_n(\mathbb{F}_q)$ komponentenweise durch Linksmultiplikation auf den Basisvektoren $B_i \in \mathbb{F}_q^{n\times 1} \setminus \{0\}$ operiert.
Es ist

$$\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(\langle e_1, e_2, \ldots, e_k\rangle) = \left\{g \in \mathrm{GL}_n(\mathbb{F}_q) \mid g\langle e_1, \ldots, e_k\rangle = \langle e_1, \ldots, e_k\rangle\right\}$$

also alle invertierbaren Matrizen, die angewandt auf alle Basisvektoren immer noch den gleichen Teilraum erzeugen, d.h. jeder Basisvektor wird auf einen Basisvektor einer weiteren Basis B' vom gleichen TR abgebildet. Diese Eigenschaft, dass Basen auf Basen abgebildet werden, haben aber genau die bijektiven linearen Abbildungen.

$$\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(\langle e_1, \ldots, e_k\rangle) = \left\{\begin{pmatrix} A & * \\ 0 & B \end{pmatrix} \middle| A \in \mathrm{GL}_k(\mathbb{F}_q),\ B \in \mathrm{GL}_{n-k}(\mathbb{F}_q),\ * \in \mathbb{F}_q^{k\times(n-k)}\right\}$$

A ist der Anteil der Matrix, der die Vektoren $e_1, \ldots, e_k$ auf andere Basisvektoren abbildet, B bildet andere Vektoren als $e_1, \ldots, e_k$ beliebig bijektiv ab, und $*$ sidn beliebige Körperelemente zum „Auffüllen“. Und damit:

$$\left|\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(\langle e_1, \ldots, e_k\rangle)\right| = \underbrace{\left|\mathrm{GL}_k(\mathbb{F}_q)\right|}_{\text{Mglk. für } A} \cdot \underbrace{\left|\mathrm{GL}_{n-k}(\mathbb{F}_q)\right|}_{\text{Mglk. für } B} \cdot \underbrace{q^{k(n-k)}}_{\text{Mglk. für } *}$$

Nach Folgerung 8.1.21 des Bahnensatzes bzgl. der transitiven $\mathrm{GL}_n(\mathbb{F}_q)$-Menge $\mathscr{U}_k(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q)$, wobei $\mathrm{GL}_n(\mathbb{F}_q)$ endlich ist mit

$$\left|\mathrm{GL}_n(\mathbb{F}_q)\right| = \prod_{i=1}^{n}\left(q^n - q^{i-1}\right) < \infty$$

nach Bsp. 8.1.22, gilt nun also:

$$\left|\mathscr{U}_k(\mathbb{F}_q^{n\times 1}, \mathbb{F}_q)\right| = \left|\mathrm{GL}_n(\mathbb{F}_q)\langle e_1, \ldots, e_k\rangle\right| = \frac{\left|\mathrm{GL}_n(\mathbb{F}_q)\right|}{\left|\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(\langle e_1, \ldots, e_k\rangle)\right|} = \begin{bmatrix} n \\ k \end{bmatrix}_q$$

□

Übung 8.1.Ü4:

$\mathrm{GL}_n(\mathbb{F}_q)$ operiert auf $\mathbb{F}_q^{n\times n}$ durch Konjugation. Die Bahnen sind genau die Ähnlichkeitsklassen von Matrizen, von denen wir eine Parametrisierung im vorherigen Kapitel kennengelernt haben.
Der Stabilisator einer Matrix A ist $\mathrm{C}_{\mathrm{GL}_n(\mathbb{F}_q)}(A) := \mathrm{C}_{\mathbb{F}_q^{n\times n}}(A)^*$, die Einheitengruppe des Zentralisators von A, auch **Zentralisator von A in $\mathrm{GL}_n(\mathbb{F}_q)$** genannt. Der Index der Gruppe gibt an, wie viele Matrizen zu A ähnlich sind. Der Fall $n = 2,\ q = 2$ kann wie folgt zusammengefasst werden:

μ_A	χ_A	Vertreter	$\left\lvert\mathrm{C}_{\mathrm{GL}_n(\mathbb{F}_q)}(A)\right\rvert$	Anzahl
x	x^2	$\begin{pmatrix}0&0\\0&0\end{pmatrix}$	6	1
$x+1$	$(x+1)^2$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	6	1
x^2	x^2	$\begin{pmatrix}0&0\\1&0\end{pmatrix}$	$2 = \left\lvert\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}\right\}\right\rvert$	3
$(x+1)^2$	$(x+1)^2$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$2 = \ldots''$	3
$x(x+1)$	$x(x+1)$	$\begin{pmatrix}1&0\\0&0\end{pmatrix}$	$1 = \left\lvert\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}\right\rvert$	6
x^2+x+1	x^2+x+1	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$3 = \left\lvert\left\{\begin{pmatrix}0&1\\1&1\end{pmatrix}^i \middle\vert\ i \in \underline{3}\right\}\right\rvert$	2

Übung 10.4:

Für den Fall $n = 3,\ q = 2$ gilt: Nach 8.1.22 ist $|\mathrm{GL}_3(\mathbb{F}_2)| = \left(2^3-1\right)\left(2^2-2\right)\left(2^3-2^2\right) = 7\cdot 6\cdot 4 = 168$.

μ_A	χ_A	Vertreter (JNF)	$\left\lvert\mathrm{C}_{\mathrm{GL}_3(\mathbb{F}_2)}(A)\right\rvert$	Anzahl
x^3	x^3	M_{x^3}	4	$\frac{168}{4} = 42$
	x^2	$\mathrm{Diag}(0, \mathrm{M}_{x^2})$	8	21
	x	0	168	1
$(x+1)\left(x^2+x+1\right)$	$(x+1)\left(x^2+x+1\right)$	$\mathrm{Diag}(1, \mathrm{M}_{x^2+x+1})$	3	56
$x^2(x+1)$	$x^2(x+1)$	$\mathrm{Diag}(1, \mathrm{M}_{x^2})$	2	84
	$x(x+1)$	$\mathrm{Diag}(0,0,1)$	6	28
$x(x+1)^2$	$x(x+1)^2$	$\mathrm{Diag}\left(0, \mathrm{M}_{(x+1)^2}\right)$	2	84
	$x(x+1)$	$\mathrm{Diag}(0,1,1)$	6	28
$x\left(x^2+x+1\right)$	$x\left(x^2+x+1\right)$	$\mathrm{Diag}(0, \mathrm{M}_{x^2+x+1})$	3	56
x^3+x^2+1	x^3+x^2+1	$\mathrm{M}_{x^3+x^2+1}$	7	24
x^3+x+1	x^3+x+1	M_{x^3+x+1}	7	24
$(x+1)^3$	$(x+1)^3$	$\mathrm{M}_{(x+1)^3}$	4	42
	$(x+1)^2$	$\mathrm{Diag}\left(1, \mathrm{M}_{(x+1)^2}\right)$	8	21
	$x+1$	I_3	168	1

8.1.d Zykel, Zykelschreibweise und Zykelzähler

Bemerkung 8.1.23: ZYKEL

(1) Sei M eine Menge und $a_1,\dots,a_k \in M$ genau k paarweise verschiedene Elemente. Dann heißt

$$(a_1,\dots,a_k): M \longrightarrow M,$$
$$a \longmapsto \begin{cases} a & a \notin \{a_1,\dots,a_k\} \\ a_{i+1} & a = a_i \text{ mit } i \in \underline{k-1} \\ a_1 & a = a_k \end{cases}$$

ein **Zykel** der Länge k (oder kurz: k-Zykel).
Es gilt $(a_1,\dots,a_k) \in \mathrm{S}_M$ und $(a_1,\dots,a_k) = (a_2,a_3,\dots,a_k,a_1) = (a_k,a_1,\dots,a_{k-1})$ und $(a_1,\dots,a_k)^{-1} = (a_k,\dots,a_1) = (a_1,a_k,\dots,a_2)$.
Ein 1-Zykel entspricht immer der Identität, ein 2-Zykel heißt **Transposition**, da es beim Abbilden nur zwei Elemente tauscht.

(2) Disjunkte Zykel kommutieren miteinander.
D.h. $(a_1,\dots,a_k)\circ(b_1,\dots,b_l) = (b_1,\dots,b_l)\circ(a_1,\dots,a_k)$ falls $\{a_1,\dots,a_k\}\cap\{b_1,\dots,b_l\} = \emptyset$.

(3) Jedes $f \in \mathrm{S}_M$ lässt sich als Produkt disjunkter Zykeln schreiben, falls M endlich ist. Diese Schreibweise ist eindeutig bis auf Reihenfolge der Zykel.
Die Anzahl und Länge der einzelnen Zykeln in der Zerlegung heißt der **Zykeltyp** von f.

Beweis zu 8.1.23:

(1) Trivial.

(2) Trivial.

(3) Dies zeigen wir mit einem Algorithmus, der u.a. die Bahnen der zyklischen Untergruppe $\langle f\rangle \leq \mathrm{S}_M$ auf M konstruiert.

EINGABE: $f \in \mathrm{S}_M$

ALGORITHMUS:

(0) Setze $N := M$.

(1) Solange $N \neq \emptyset$, wähle $a \in N$ und finde das kleinste k mit $f^k(a) = a$.
Dann ist $z_a := \left(a, f(a), f^2(a), \dots, f^{k-1}(a)\right)$ ein Zykel.

(2) Ersetze N durch $N \setminus \left\{a, f(a), f^2(a), \dots, f^{k-1}(a)\right\}$, solange $N \neq \emptyset$ und gehe zu (1).

AUSGABE: Menge der disjunkten Zykel z_a. Ihr Produkt ist f.

EINDEUTIGKEIT: Die in jedem Schritt (1) erzeugten Zykeln z_a stellen jeweils eine Bahn $\langle f\rangle a \subseteq M$ dar. Hätte man eine Zykelzerlegung, die ein Zykel mit Elementen aus einer Bahn enthält, aber min. eines der Elemente aus der Bahn fehlt, so muss dieser Fehler korrigiert werden, um das korrekte Bild von f herzustellen, indem das Urbild des fehlenden Elements und das fehlende Element in einem neuen Zykel dazugehangen wird. Dann ist die Zerlegung aber nicht mehr disjunkt. Die Zerlegung über Bahnen ist also die einzige disjunkte Zerlegung, und die Bahnen sind bis auf Vertreterwahl eindeutig.

□

Beispiel 8.1.24:

$$f := \begin{array}{c|ccccc} n & 1 & 2 & 3 & 4 & 5 \\ f(n) & 2 & 4 & 5 & 1 & 3 \end{array} = (1,2,4)\circ(3,5)$$

Außerdem:

$$(1,2,3,4,5)(2,3,4,5) = (1,2,4)(3,5)$$

denn: Nehme 1, bilde sie vom rechten Zykel aus ab. Der rechte Zykel bewegt 1 nicht, also bleibt es 1. Der linke Zykel bildet 1 auf 2 ab. Das Ergebnis ist also 2. $\Rightarrow (1,2\ \ldots$
Nehme 2. Der rechte Zykel bildet 2 auf 3 ab. Der linke Zykel bildet 3 auf 4 ab.
Das Ergebnis ist also 4. $\Rightarrow (1,2,4\ \ldots$
Nehme 4. Das Ergebnis ist 1. $\Rightarrow (1,2,4)\ldots$
Nehme 3. Usw...

Daraus folgt außerdem: $\underline{5}/_{\langle f\rangle} = \{\langle f\rangle m \mid m \in \underline{5}\} = \{\{1,2,4\},\{3,5\}\}$

Bemerkung 8.1.25:

Für ein Zykel $\pi = (a_1,\ldots,a_k)$ gilt $\operatorname{sign}(\pi) = (-1)^{k-1}$, da

$$\pi = \underbrace{(a_2,a_3)(a_3,a_4)\cdots(a_{k-1},a_k)(a_1,a_k)}_{k-1 \text{ Transpositionen}}$$

da $\operatorname{sign}((a,b)) = -1$.

Als nächstes: Konjugationsoperationen in S_M.

Übung 8.1.Ü5:

Konjugation erhält den Zykeltyp, genauer:

$$\sigma(a_1,\ldots,a_k)\sigma^{-1} = (\sigma(a_1),\ldots,\sigma(a_k)) \ \forall \sigma \in \mathrm{S}_M$$

Beweis:
Sei $m \in M$ und $n := \sigma^{-1}(m)$, d.h. $m = \sigma(n)$.

FALL 1: $n \notin \{a_1,\ldots,a_k\}$: Dann ist $(a_1,\ldots,a_k)(n) = n$, und somit folgt:

$$\left(\sigma\circ(a_1,\ldots,a_k)\circ\sigma^{-1}\right)(m) = \sigma\left((a_1,\ldots,a_k)\left(\sigma^{-1}(m)\right)\right) = \sigma((a_1,\ldots,a_k)(n)) = \sigma(n) = m$$

FALL 2: $n = a_i$ für ein $i \in \underline{k}$. Dann ist $(a_1,\ldots,a_k)(n) = a_{i+1}$ (bzw. a_1, falls $i = k$, substituiere entsprechend im Folgenden), und somit folgt:

$$\left(\sigma\circ(a_1,\ldots,a_k)\circ\sigma^{-1}\right)(m) = \sigma\left((a_1,\ldots,a_k)\left(\sigma^{-1}(m)\right)\right) = \sigma((a_1,\ldots,a_k)(n)) = \sigma(a_{i+1})$$

$$\Rightarrow \left(\sigma\circ(a_1,\ldots,a_k)\circ\sigma^{-1}\right)(m) = \left\{\begin{array}{ll} m & m \notin \{\sigma(a_1),\ldots,\sigma(a_k)\} \\ \sigma(a_{i+1}) & m = \sigma(a_i) \text{ für } i \in \underline{k-1} \\ \sigma(a_1) & m = \sigma(a_k) \end{array}\right\} \overset{\text{Def.}}{=} (\sigma(a_1),\ldots,\sigma(a_k))$$

(Dass der Zykeltyp auch bei mehreren disjunkten Zykeln gleich bleibt, ist klar, da $\sigma^{-1}\circ\sigma = \mathrm{id}_M$. Siehe auch im Beweis von 8.1.26.) □

Satz 8.1.26: Zykelzähler

Für $\pi \in \mathrm{S}_n$ sei $a_i(\pi)$ die Anzahl der Zykel der Länge i in einer disjunkten Zykelzerlegung von π und

$$a(\pi) := (a_1(\pi), \ldots, a_n(\pi))$$

der **Zykelzähler**.

Es gilt: $\pi, \rho \in \mathrm{S}_n$ sind konjugiert $\Leftrightarrow a(\pi) = a(\rho)$.
Der Zykelzähler ist eine trennende Invariante der Operation von S_n auf sich per Konjugation.

Dies ist „äquivalent" zu Elementarteilertheorie/Jordan über dem „Körper mit einem Element" – viel einfacher als die Operation von GL_n auf GL_n!

Beweis zu 8.1.26:

(1) Konjugation erhält den Zykelzähler, denn:

Seien $\pi, \sigma \in \mathrm{S}_n$ mit $\pi = (\alpha_1, \ldots, \alpha_k)(\beta_1, \ldots, \beta_l)\cdots$ in disjunkter Zykelzerlegung. Dann ist

$$\sigma\pi\sigma^{-1} = \sigma(\alpha_1, \ldots, \alpha_k)\underbrace{\sigma^{-1}\sigma}_{=\mathrm{id}_{\underline{n}}}(\beta_1, \ldots, \beta_l)\underbrace{\sigma^{-1}\sigma}_{=\mathrm{id}_{\underline{n}}}\cdots$$

$$\overset{8.1.Ü5}{=} (\sigma(\alpha_1), \ldots, \sigma(\alpha_k))(\sigma(\beta_1), \ldots, \sigma(\beta_l))\cdots$$

Der Zykeltyp ist gleich. Insbesondere hat sich also der Zykelzähler nicht geändert.

(2) Umgekehrt: Sei $a(\pi) = a(\rho)$. Ordnet man bei beiden Operationen die Zykel aus der disjunkten Zykelzerlegung der Länge nach, so stehen im folgenden Schema die Zykel gleicher Länge untereinander:

$$\pi = (\alpha_1, \ldots, \alpha_k)(\beta_1, \ldots, \beta_l)\cdots$$
$$\rho = (\alpha'_1, \ldots, \alpha'_k)(\beta'_1, \ldots, \beta'_l)\cdots$$

in disjunkter Zykelzerlegung. Dann definiere nach Übung 8.1.5 $\sigma \in \mathrm{S}_n$ durch

$$\alpha_i \mapsto \alpha'_i,\ \beta_j \mapsto \beta'_j, \ldots$$

für $i \in \underline{k}$, $j \in \underline{l}$ usw. Dann ist $\sigma\pi\sigma^{-1} = \rho$. □

Übung 8.1.Ü6:

Jedes $a \in \mathbb{Z}^n_{\geq 0}$ mit $\sum_{i=1}^n i a_i = n$ kommt als Zykelzähler eines Elements von S_n vor.

Wie viele Konjugiertenklassen hat S_6?

Beispiel 8.1.27: KONJUGATION IN S_n

(1) Gegeben seien

$$\pi := (1,2)(3,4,5,6,7)(8,9)$$
$$\rho := (9,4)(1,2,3,7,6)(5,8)$$

in S_9. SUCHE ein $\sigma \in S_9$ mit $\sigma\pi\sigma^{-1} = \rho$. LÖSUNG:

$$\sigma = (1,\ 9,\ 8,\ 5,\ 3)(2,\ 4)(6,\ 7)$$

σ ist nicht eindeutig! Nach Umschreiben in $\rho = (5,8)(1,2,3,7,6)(9,4)$ erhält man $\sigma = (1,5,7)(2,8,9,4,3)$ als eine weitere Lösung.

BEACHTE: Die Lösungen bilden eine Nebenklasse nach $C_{S_9}(\pi) = \{\sigma \in S_9 \mid \sigma\pi\sigma^{-1} = \pi\}$. Man sieht leicht: Die Elemente von $C_{S_9}(\pi)$ entsprechen den Möglichkeiten, eine disjunkte Zykelzerlegung von π kompatibel unter die gegebene disjunkte Zykelzerlegung von π zu schreiben. Also ist $|C_{S_9}(\pi)| = 2 \cdot 2^5 \times 5$.

(2) Bestimme den Zentralisator $C_{S_{10}}((1,2,3))$. LÖSUNG:

$$\begin{aligned} C_{S_{10}}((1,2,3)) &= \{\pi \in S_{10} \mid \pi(1,2,3)\pi^{-1} = (1,2,3)\} \\ &= \{\pi \in S_{10} \mid (\pi(1),\pi(2),\pi(3)) = (1,2,3)\} \end{aligned}$$

Also ist $\pi = (1,2,3)^i \rho$ mit $\rho \in S_{10}$ und $\rho(j) = j\ \forall j \in \underline{3}$, kurz: $C_{S_{10}}((1,2,3)) = \langle(1,2,3)\rangle \times \underbrace{S_{\underline{10}\setminus\underline{3}}}_{\cong S_7}$

8.1.e Anzahl der Bahnen des Stabilisators

Bemerkung 8.1.28:

Die Gruppe G operiere auf M und N.

(1) G operiert auf $M \times N$ durch

$$\begin{aligned} G \times (M \times N) &\longrightarrow M \times N, \\ (g,(m,n)) &\longmapsto (gm, gn) \end{aligned}$$

Diese Operation heißt **Diagonaloperation**.

(2) Ist die Operation auf M transitiv, dann gibt es eine Bijektion zwischen der Menge der Bahnen von G auf $M \times N$ und der Menge der Bahnen von $\mathrm{Stab}_G(m)$ auf N für jedes feste $m \in M$.
Genauer: Die Abbildung

$$\begin{aligned} G\backslash(M \times N) &\longrightarrow \mathrm{Stab}_G(m)\backslash N, \\ G(m,n) &\longmapsto \mathrm{Stab}_G(m)n \end{aligned}$$

ist eine Bijektion.

Beweis zu 8.1.28:

(1) trivial (Operationsaxiome).

(2) Wir zeigen, dass die Abbildung wohldefiniert ist: Wegen der Transitivität von G auf M ist jede Bahn von G auf $M \times N$ von der Form $G(m,n) = \{(gm,gn) \mid g \in G\}$. Gilt $G(m,n) = G(m,n')$ für ein $n \in N$, so sind offenbar n und n' in derselben Bahn unter $\mathrm{Stab}_G(m)$:

$$\begin{aligned} &(gm,gn) = (hm,hn') \\ \Leftrightarrow\ &(h^{-1}gm, h^{-1}gn) = (m,n') \\ \Leftrightarrow\ &h^{-1}g \in \mathrm{Stab}_G(m) \wedge n' = (h^{-1}g)n \end{aligned}$$

Offenbar ist die Abbildung surjektiv (trifft jede Bahn). Die Injektivität folgt wegen

$$\mathrm{Stab}_G(m)n = \mathrm{Stab}_G(m)n' \Leftrightarrow G(m,n) = G(m,n')$$

Also haben wir eine Bijektion.

□

Beispiel 8.1.29:

Sei $\mathcal{V}$ ein e.e. K-VR. Dann operiert $G := \mathrm{GL}(\mathcal{V})$ auf $\mathcal{V} \setminus \{0\}$ transitiv.
Der Stabilisator eines Vektors $\mathcal{V} \in \mathcal{V} \setminus \{0\}$ hat dann jedes Vielfache $\neq 0$ von V wieder als Bahn, sowie die Menge aller Vektoren, die linear unabhängig von V sind.
Die Bahnen von $\mathrm{GL}(\mathcal{V})$ auf $(\mathcal{V} \setminus \{0\}) \times (\mathcal{V} \setminus \{0\})$ sind also durch $\{(V, aV) \mid V \neq 0\}$ mit $a \in K$ und $\{(V,W) \mid V, W \text{ linear unabhängig}\}$ gegeben.

In Matrizen: $\mathcal{V} = K^{n\times 1}$, $G = \mathrm{GL}_n(K)$, Operation durch Linksmultiplikation. Der Stabilisator des ersten Standardbasisvektors $E_1 = (\mathrm{I}_n)_{-,1}$ ist

$$\mathrm{Stab}_G(E_1) = \left\{ \left(\begin{array}{c|c} 1 & a \\ \hline 0 & \\ \vdots & A \\ 0 & \end{array} \right) \middle| a \in K^{1\times(n-1)},\ A \in \mathrm{GL}_{n-1}(K) \right\}$$

und hat die folgenden Bahnen auf $\mathcal{V}$: $\{aE_1\}$ für $a \in K \setminus \{0\}$ und $\mathcal{V} \setminus \{aE_1 \mid a \in K\}$.

Beispiel 8.1.30:

Sei $\mathcal{V}$ ein e.e. K-VR. Dann operiert $G = \mathrm{GL}(\mathcal{V})$ auf $\mathcal{V}^* := \mathrm{Hom}(\mathcal{V}, K)$ (**Dualraum** von $\mathcal{V}$) linear und treu durch

$$\begin{aligned} G \times \mathcal{V}^* &\longrightarrow \mathcal{V}^*, \\ (g, \varphi) &\longmapsto \varphi \circ g^{-1} \end{aligned}$$

Der Stabilisator eines $\varphi \in \mathcal{V}^* \setminus \{0\}$ operiert auf jeder Faser $\varphi^{-1}(\{a\})$ mit $a \in K$, also auf jeder Restklasse nach $\mathrm{Kern}\,\varphi$.
Das Studium der Operationen von $\mathrm{Stab}_G(\varphi)$ auf $\varphi^{-1}(\{1\})$ heißt **affine Geometrie** und wird im nächsten Kapitel ausführlich behandelt.

In Matrizen: $\mathcal{V} = K^{n\times 1}$, $G = \mathrm{GL}_n(K)$ Die Operation auf $K^{1\times n}$, die bekanntlich $\mathrm{Hom}(K^{n\times 1}, K)$ entspricht, ist gegeben durch:

$$\begin{aligned} G \times K^{1\times n} &\longrightarrow K^{1\times n}, \\ (g, Z) &\longmapsto Zg^{-1} \end{aligned}$$

Der Stabilisator des letzten Standardbasisvektors $Z_n := (\mathrm{I}_{n,-}) = (0, \ldots, 0, 1)$ ist

$$\mathrm{Stab}_G(Z_n) := \left\{ \left(\begin{array}{c|c} A & a \\ \hline 0 & 1 \end{array} \right) \middle| a \in K^{(n-1)\times 1},\ A \in \mathrm{GL}_{n-1}(K) \right\}$$

Die Operation dieser Gruppe auf

$$\varphi^{-1}(\{1\}) = \left\{ \begin{pmatrix} S \\ \hline 1 \end{pmatrix} \middle| S \in K^{(n-1)\times 1} \right\} \text{ mit } \varphi \begin{pmatrix} V_1 \\ \vdots \\ V_n \end{pmatrix} := Z_n \begin{pmatrix} V_1 \\ \vdots \\ V_n \end{pmatrix} = V_n$$

wird also die affine Geometrie sein. Man beachte:

$$\left(\begin{array}{c|c} A & a \\ \hline 0 & 1 \end{array} \right) \begin{pmatrix} S \\ \hline 1 \end{pmatrix} = \begin{pmatrix} AS + a \\ \hline 1 \end{pmatrix}$$

8.2 Homomorphismen und Normalteiler

Definition 8.2.1: Gruppenhomomorphismus

Seien G, H Gruppen. Eine Abbildung $\varphi : G \to H$ heißt **Gruppenhomomorphismus**, wenn

$$\varphi(\underbrace{g_1 g_2}_{\in G}) = \underbrace{\varphi(g_1)\varphi(g_2)}_{\in H} \quad \forall g_1, g_2 \in G$$

Beispiel 8.2.2:

$G \circlearrowright M$. Dann ist

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{S}_M, \\ g &\longmapsto (m \mapsto gm) \end{aligned}$$

ein Gruppenhomomorphismus.

Ist $M = \mathcal{V}$ ein K-VR, so ist die Operation genau dann linear, wenn $\operatorname{Bild}\varphi \overset{!}{\subseteq} \mathrm{GL}(\mathcal{V}) \leq \mathrm{S}_{\mathcal{V}}$ liegt.

Definition 8.2.3: Normalteiler

Eine Untergruppe $U \leq G$ mit $gUg^{-1} = U \ \forall g \in G$ (Fixpunkt bzgl. Konjugationsoperation auf der Menge der Untergruppen) heißt **Normalteiler** (NT) von G, und wir schreiben $U \trianglelefteq G$.

Satz 8.2.4: Bild und Kern

Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist $\operatorname{Bild}\varphi := \{\varphi(g) \mid g \in G\}$ eine Untergruppe von H und $\operatorname{Kern}\varphi := \{g \in G \mid \varphi(g) = 1_H\}$ ein Normalteiler von G.

Beweis zu 8.2.4:
Für $n \in \operatorname{Kern}\varphi,\ g \in G$ gilt:

$$\varphi\left(gng^{-1}\right) = \varphi(g)\underbrace{\varphi(n)}_{=1_H}\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1_H$$

also ist $gng^{-1} \in \operatorname{Kern}\varphi$. □

Beispiel 8.2.5: Konkrete Beispiele für Normalteiler

(1) Ist G eine beliebige Gruppe, so sind $\{1\}$ und G Normalteiler von G, die „trivialen Normalteiler".

(2) $\operatorname{sign} : \mathrm{S}_n \to (\{\pm 1\}, \cdot)$ ist ein Gruppenhomomorphismus. Der Kern ist also ein Normalteiler (vom Index 2) von S_n, die sogenannte **alternierende Gruppe** $\mathrm{A}_n := \operatorname{Kern}(\operatorname{sign})$ vom Grad n. Ihre Elemente heißen **gerade Permutationen**. (Dies ist wieder ein Fall des „Körpers mit einem Element" analog der speziellen linearen Gruppe.)

(3) $\det : \mathrm{GL}_n(K) \to K^* := (K \setminus \{0\}, \cdot)$ ist ein Gruppenhomomorphismus für jeden Körper K. Also ist $\operatorname{Kern}\det$ ein Normalteiler von $\mathrm{GL}_n(K)$. Dieser wird mit $\mathrm{SL}_n(K) := \{g \in \mathrm{GL}_n(K) \mid \det g = 1\}$ bezeichnet und heißt die **spezielle lineare Gruppe** vom Grad n.

(4) Sei $U \leq G$. Dann ist $\operatorname{Core}(U) := \bigcap_{g \in G} gUg^{-1}$ der größte Normalteiler von G, der in U enthalten ist. Es gilt: $\operatorname{Core}(U) = \operatorname{Kern}\left(G \overset{\varphi}{\longmapsto} \mathrm{S}_{G/U}\right)$.

(5) In einer Abelschen Gruppe ist jede Untergruppe ein Normalteiler. $(gUg^{-1} = gg^{-1}U = U)$

Bemerkung 8.2.6:

Eine Untergruppe $N \leq G$ ist genau dann ein Normalteiler, wenn sie Vereinigung von Konjugiertenklassen von Elementen ist.

Beweis zu 8.2.6:
N ist genau dann ein Normalteiler von G, wenn sich die Konjugationsoperation von G auf N einschränken lässt (d.h. auf N abgeschlossen ist – ganze Konjugationsklassen müssen also immer in N liegen). □

Übung 8.2.Ü1: Normalteiler symmetrischer Gruppen

Alle Normalteiler von symmetrischen Gruppen vom Grad 3 und 4 sind

$$\mathrm{S}_3 \trianglerighteq \mathrm{A}_3 \trianglerighteq \{1\} \quad \text{und} \quad \mathrm{S}_4 \trianglerighteq \mathrm{A}_4 \trianglerighteq \mathrm{V}_4 \trianglerighteq \{1\}$$

wobei $\mathrm{V}_4 := \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.

Beweis:
Betrachte zunächst die Konjugiertenklassen von S_4 (Bahnen von $\mathrm{S}_4 \circlearrowright \mathrm{S}_4$ durch Konjugation).
Diese sind nach Übung 8.1.Ü5:

Vertreter	Länge der Bahn	
$\mathrm{id}_{\underline{4}}$	1	
$(1,2)$	$\binom{4}{2} = 6$	(alle Mglk., zweielementige Zykeln ohne Reihenfolge zu wählen)
$(1,2)(1,2)$	$\frac{6}{2} = 3$	(erstes Zykel gibt zweites vor, Reihenfolge egal $\rightarrow : 2$)
$(1,2,3)$	$2 \cdot \binom{4}{2} = 8$	(zwei Mglk. für 3er-Zykel, 4 Möglichkeiten für 3 Elemente aus $\underline{4}$)
$(1,2,3,4)$	$\frac{4!}{4} = 6$	($4!$ mgl. Reihenfolgen, aber jeder Zykel hat 4 verschiedene Darstellungen)

Außerdem gilt: $|\mathrm{S}_4| = 4! = 24 = 2^3 \cdot 3$, d.h. nach dem Satz von Lagrange 8.1.7 muss jede Untergruppe von S_4 eine Ordnung von $2, 3, 4, 6, 12$ oder 24 haben. Die $\mathrm{id}_{\underline{4}}$ muss in jeder Untergruppe enthalten sein.
Zunächst natürlich die trivialen Untergruppen, die auch die trivialen Normalteiler sind: S_4 selbst und $\{\mathrm{id}_{\underline{4}}\}$.
Nach Bemerkung 8.2.6 sind mögliche Kandidaten für Normalteiler also:

- 1: $\{\mathrm{id}_{\underline{4}}\} \cup \mathrm{S}_4(1,2)(3,4)$ mit Ordnung 4
- 2: $\{\mathrm{id}_{\underline{4}}\} \cup \mathrm{S}_4(1,2)(3,4) \cup \mathrm{S}_4(1,2,3)$ mit Ordnung 12

wobei $\mathrm{S}_4 m$ die Bahn unter der Konjugationsoperation von S_4 auf sich selbst sei.
Es ist

- $\mathrm{S}_4(1,2)(3,4) = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$
- $\mathrm{S}_4(1,2,3) = \{(1,2,3), (1,3,2), (2,3,4), (2,4,3), (1,3,4), (1,4,3), (1,2,4), (1,4,2)\}$

Damit folgt: Der zweite Kandidat, mit Ordnung 12, ist A_4, ein Normalteiler auch nach 8.2.5.(2).
Der erste Kandidat ist $\mathrm{V}_4 := \{\mathrm{id}_{\underline{4}}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, eine Gruppe (ggf. Multiplikationstabelle aufstellen zum Nachprüfen) und somit auch Untergruppe und Normalteiler nach 8.2.6.
Somit sind die Normalteiler von S_4 genau S_4, A_4, V_4 und $\{1\}$. □

Übung 11.3:

Sei G eine Gruppe. Dann gilt:

(1) $\varphi : G \to G,\ g \mapsto g^{-1}$ ist Automorphismus $\Leftrightarrow G$ Abelsch.
(2) $\varphi : G \to G,\ g \mapsto g^2$ ist Endomorphismus $\Leftrightarrow G$ Abelsch.
(3) $M \trianglelefteq N \trianglelefteq G \not\Rightarrow M \trianglelefteq G$

Beweis:

(1) Durch Gruppenaxiome gilt zunächst: φ ist bijektiv. Seien $a, b \in G$ beliebig. Es gilt:

$$\begin{aligned}
&\varphi(ab) \overset{!}{=} \varphi(a)\varphi(b) \text{ (Gruppenhomomorphismuseigenschaft)}\\
&\Leftrightarrow (ab)^{-1} = a^{-1}b^{-1}\\
&\Leftrightarrow (ab)^{-1} = (ba)^{-1}\\
&\Leftrightarrow \varphi(ab) = \varphi(ba)\\
&\Leftrightarrow ab = ba \text{ (Abelsche Gruppeneigenschaft)}
\end{aligned}$$

$\Rightarrow \varphi$ ist Gruppenhomomorphismus auf G genau dann, wenn G Abelsch ist.

(2) Seien $a, b \in G$ beliebig. Es gilt:

$$\begin{aligned}
&\varphi(ab) \overset{!}{=} \varphi(a)\varphi(b)\\
&\Leftrightarrow (ab)^2 = a^2b^2\\
&\Leftrightarrow abab = aabb \qquad \| \cdot_L a^{-1} \ \| \cdot_R b^{-1}\\
&\Leftrightarrow ba = ab
\end{aligned}$$

(3) Intuitiv ist dies klar: Wenn M unter Konjugation mit Elementen aus $N \subseteq G$ invariant bleibt, kann es trotzdem Elemente in G (genauer: $G \setminus N$) geben, die M unter Konjugation variieren.

Betrachte $U := \{\mathrm{id}_4, (1,2)(3,4)\} \leq \mathrm{V}_4$ (da $(1,2)(3,4)$ selbstinvers): V_4 ist Abelsch (siehe Übung 8.2.Ü1), damit ist $U \trianglelefteq \mathrm{V}_4$ ein NT.

Aber in Übung 8.2.Ü1 wurde bereits gezeigt, dass U *kein* Normalteiler von S_4 ist, V_4 hingegen schon.

Somit kann i.A. aus $M \overset{U}{\trianglelefteq} N \overset{\mathrm{V}_4}{\trianglelefteq} G \overset{\mathrm{S}_4}{}$ nicht $M \overset{U}{\trianglelefteq} G \overset{\mathrm{V}_4}{}$ folgen.

□

Satz 8.2.7: VORBEREITUNG ZUM HOMOMORPHIESATZ

Sei N ein Normalteiler von G. Dann bildet die Menge der Linksnebenklassen $G/N = \{gN \mid g \in G\}$ eine Gruppe unter vertreterweise Multiplikation:

$$\begin{aligned}
G/N \times G/N &\longrightarrow G/N,\\
(gN, hN) &\longmapsto ghN
\end{aligned}$$

Beweis zu 8.2.7:

Es ist klar, dass wir eine Gruppe vorliegen haben, sobald die Verknüpfung wohldefiniert ist. Zur Wohldefiniertheit: Sei $g' = gm \in gN$, $h' = hm \in hN$. Dann gilt:

$$(g'h')N = (gmhm)N = (gh)\underbrace{(h^{-1}mh)n}_{\substack{m\in N,\ n\in N,\\ h^{-1}mh\in N \text{ weil NT}}} N = ghN$$

□

Beispiel 8.2.8:

Die $\mathrm{S}_3 = \mathrm{Stab}_{\mathrm{S}_4}(4)$ ist *kein* Normteiler von S_4.
Dies kann man auf mehrere Arten nachvollziehen. Zum Einen haben wir in Übung 8.2.Ü1 alle Normalteiler konstruiert. S_3 ist keine Vereinigung von Konjugiertenklassen, denn

$$\pi \mathrm{S}_3 \pi^{-1} = \pi\, \mathrm{Stab}_{\mathrm{S}_4}\, \pi^{-1} = \mathrm{Stab}_{\mathrm{S}_4}(\pi(4)) \neq \mathrm{S}_3$$

für einige π, z.B. $\pi = (1,4)$.
Zum Anderen bilden die Linksnebenklassen $\mathrm{S}_4/\mathrm{S}_3 = \{\mathrm{S}_3, a\mathrm{S}_3, a^2\mathrm{S}_3, a^3\mathrm{S}_3\}$ mit $a = (1,2,3,4)$ keine Gruppe. Es ist z.B. $(a\mathrm{S}_3)^2 = \{ahag \mid g, h \in \mathrm{S}_3\} = \mathrm{S}_4$.

Bemerkung 8.2.9: Wichtige Eigenschaft von Normalteilern

Eine Untergruppe N ist genau dann ein Normalteiler von G, wenn $gN = Ng \ \forall g \in G$ (d.h. Links- und Rechtsnebenklassen stimmen überein). Dies wird oft auch als Definition von NT verwendet.

Insbesondere sind Untergruppen N vom Index 2 immer Normalteiler, denn

$$N \dot\cup gN = G = N \dot\cup Ng$$

also $gN = G \setminus N = Ng$.

Definition 8.2.10: Einfache Gruppen

Eine Gruppe $G \neq \{1\}$ heißt **einfach**, falls G und $\{1\}$ die einzigen Normalteiler von G sind.

Übung 8.2.Ü2:

Die zyklische Gruppe der Ordnung n

$$\mathrm{C}_n := \left(\mathbb{Z}/n\mathbb{Z}, +\right)$$

ist genau dann einfach, wenn n prim ist (d.h. sie keine nicht-trivialen Untergruppen hat).

Es gibt einige Ordnungen, in denen es *nur* die zyklische Gruppe gibt (Sylowsätze, → Algebra).

Übung 8.2.Ü3:

A_5 ist einfach. (A_4 ist nicht einfach, denn $\mathrm{V}_4 \trianglelefteq \mathrm{A}_4$.)

Die Klassifikation aller endlichen einfachen Gruppen war ein „Desaster“. In 150 Jahren Arbeit wurde die genaue Klassifikation nie komplett dokumentiert. Die Klassifikation besteht hauptsächlich aus A_n und Gruppen vom Lie-Typ.

$$\mathrm{Z}\left(\mathrm{SL}_n\left(\mathbb{F}_q\right)\right) \trianglelefteq \mathrm{SL}_n\left(\mathbb{F}_q\right) \trianglelefteq \mathrm{GL}_n\left(\mathbb{F}_q\right) \rightsquigarrow \mathrm{PSL}_n\left(\mathbb{F}_q\right) := \mathrm{SL}_n\left(\mathbb{F}_q\right) \Big/ \mathrm{Z}\left(\mathrm{SL}_n\left(\mathbb{F}_q\right)\right)$$

(P für „projektiv“) – das $\mathbb{F}_q$-Analogon zu A_n über dem „einelementigen Körper“.

Hauptsatz 8.2.11: Homomorphiesatz für Gruppen

(1) Ist G eine Gruppe, $N \trianglelefteq G$, dann bildet die Menge G/N der (Links-)Nebenklassen eine Gruppe mit vertreterweiser Multiplikation:

$$gN \cdot hN := ghN \ \forall g \in G$$

und der **natürliche Epimorphismus**

$$\nu := \nu_N : G \longrightarrow G/N, \quad g \longmapsto gN$$

ist ein surjektiver Gruppenhomomorphismus (Gruppenepimorphismus) mit $\operatorname{Kern} \nu = N$.

(2) Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so ist $\operatorname{Kern}\varphi$ ein Normalteiler von G und $\operatorname{Bild}\varphi$ eine Untergruppe von H. Weiter definiert

$$\tilde{\varphi} : G/\operatorname{Kern}\varphi \longrightarrow H, \quad g\operatorname{Kern}\varphi \longmapsto \varphi(g)$$

einen Monomorphismus und φ faktorisiert, d.h.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle \nu_{\operatorname{Kern}\varphi}}\searrow & & \nearrow{\scriptstyle \tilde{\varphi}} \\ & G/\operatorname{Kern}\varphi & \end{array}$$

kommutiert, d.h. $\varphi = \tilde{\varphi} \circ \nu_{\operatorname{Kern}\varphi}$.
Insbesondere sind $G/\operatorname{Kern}\varphi$ und $\operatorname{Bild}\varphi \leq H$ isomorph.

Beweis zu 8.2.11:

(1) Dies ist Satz 8.2.7.

(2) Genauso wie beim Homomorphiesatz für Mengen zeigt man, dass $\tilde{\varphi}$ wohldefiniert ist:

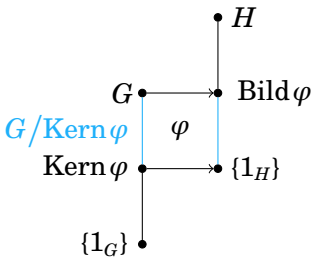
$$\varphi\left(g\operatorname{Kern}\varphi\right) = \varphi(g)\varphi\left(\operatorname{Kern}\varphi\right) = \varphi(g)\cdot = \varphi(g)$$

Es bleibt die Homomorphieeigenschaft von $\tilde{\varphi}$ zu überprüfen. Setze $N := \operatorname{Kern}\varphi$, und seien $g, h \in G$. Dann gilt:

$$\tilde{\varphi}(gNhN) = \tilde{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \tilde{\varphi}(gN)\tilde{\varphi}(hN)$$

Dass ν_N ein Epi ist, wissen wir bereits. Dass die Komposition $\tilde{\varphi} \circ \nu_N = \varphi$ ist, ist trivial (fast Definition von $\tilde{\varphi}$).

□

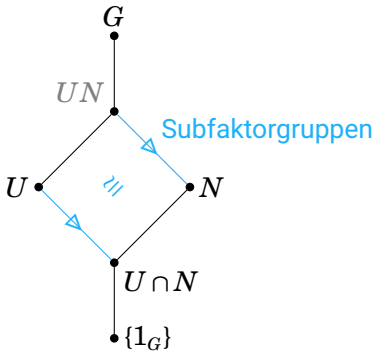


Satz 8.2.12: Noetherscher Isomorphiesatz

Sei N ein Normalteiler von G und $U \leq G$. Dann ist

$$UN \leq G \text{ und } N \cap U \trianglelefteq U$$

(wobei $UN := \{un \mid u \in U,\ n \in N\}$) und es gilt $UN/N \cong U/U \cap N$.



Beweis zu 8.2.12:

Wichtiger Beweis! *(Prüfungsfrage)*

Wegen $UN = NU$ folgt $UN \leq G$. Offenbar ist N auch NT in UN, da es in G ein NT ist, und somit ist

$$\begin{aligned} \mu : U &\longrightarrow UN/N \,, \\ u &\longmapsto uN \end{aligned}$$

ein Homomorphismus, sogar ein Epimorphismus mit $\operatorname{Kern}\mu = U \cap N$ und $\operatorname{Bild}\mu = UN/N$.
Wende jetzt Homomorphiesatz an. □

Definition 8.2.13: Semidirektes Produkt

Eine Gruppe G heiß (internes) **semidirektes Produkt**, falls es einen Normalteiler $N \trianglelefteq G$ und eine Untergruppe $U \leq G$ gibt mit

(1) $NU = G$

(2) $N \cap U = \{1\}$

Wir schreiben $G = N \rtimes U$ („Stab“ auf Seite der Untergruppe).

Beispiel 8.2.14:

$\mathrm{S}_4 = \mathrm{V}_4 \rtimes \mathrm{S}_3$, wobei es egal ist, welche der 4 Untergruppen S_3 in S_4 gewählt wird. Beachte, dass alle Elemente $\neq 1_{\mathrm{S}_4} = \mathrm{id}_{\underline{4}}$ in V_4 keine Fixpunkte auf $\underline{4} = \{1,2,3,4\}$ haben, also ist $\mathrm{V}_4 \cap \mathrm{S}_3 = \{1\}$.

Übung 8.2.Ü4:

$\mathrm{V}_4\mathrm{S}_3 = \mathrm{S}_4$

Beispiel 8.2.15: AFFINE GRUPPE

Die **affine Gruppe** ist definiert durch

$$\begin{aligned}\mathrm{Aff}_n(K) &:= \left\{ \left(\begin{array}{c|c} A & a \\ \hline 0 & 1 \end{array} \right) \middle| a \in K^{n\times 1},\ A \in \mathrm{GL}_n(K) \right\} \leq \mathrm{GL}_{n+1}(K) \\ &= „K^{n\times 1}“ \rtimes „\mathrm{GL}_n(K)“ \text{ (eigentlich andere NT/Untergruppe, die man damit identifizieren kann)}\end{aligned}$$

Dabei ist

$$„K^{n\times 1}“ := \left\{ \left(\begin{array}{c|c} \mathrm{I}_n & a \\ \hline 0 & 1 \end{array} \right) \middle| a \in K^{n\times 1} \right\} \text{ mit } \left(\begin{array}{c|c} \mathrm{I}_n & a \\ \hline 0 & 1 \end{array} \right) \left(\begin{array}{c|c} \mathrm{I}_n & b \\ \hline 0 & 1 \end{array} \right) = \left(\begin{array}{c|c} \mathrm{I}_n & a+b \\ \hline 0 & 1 \end{array} \right)$$

(d.h. Gruppenmultiplikation verhält sich wie die *Addition* der Vektoren $a \in K^{n\times 1}$!)
der Kern des Gruppenhomomorphismus

$$\begin{aligned}&\mathrm{Aff}_n(K) \longrightarrow \mathrm{GL}_n(K), \\ &\left(\begin{array}{c|c} A & a \\ \hline 0 & 1 \end{array} \right) \longmapsto A\end{aligned}$$

und

$$„\mathrm{GL}_n(K)“ := \left\{ \left(\begin{array}{c|c} A & 0 \\ \hline 0 & 1 \end{array} \right) \middle| A \in \mathrm{GL}_n(K) \right\}$$

Bemerkung 8.2.16:

In einem semidirekten Produkt $G = N \rtimes U$ hat jedes Element g eine eindeutige Darstellung als $g = nu$ mit $n \in N,\ u \in U$.

Beweis:
$un = u'n' \Leftrightarrow \underbrace{u^{-1}u'}_{\in U} = \underbrace{n\left(n'\right)^{-1}}_{\in N} = 1$ (weil Schnitt {1}). □

Es gilt $(n_1u_1)(n_2u_2) = \big(\underbrace{n_1}_{\in N}\ \underbrace{u_1n_2\overbrace{u_1^{-1}}^{=1}}_{\in N}\big)(\underbrace{u_1u_2}_{\in U})$ für $n_1, n_2 \in N,\ u_1, u_2 \in U$.

9 Geometrie

9.1 Affine Geometrie

9.1.a Der affine Raum

Definition 9.1.1: Affine Räume

Sei $\mathcal{V}$ ein K-VR.
Ein **affiner Raum** über $\mathcal{V}$ ist eine nicht-leere Menge $\mathscr{A}$, genannt **Punktmenge**, auf der $\mathcal{V}$ scharf transitiv operiert. Da $\mathcal{V}$ als Gruppe Abelsch ist, ist „scharf transitiv“ = „treu und transitiv“.
Der VR $\mathcal{V}$ wird als **Translationsraum** von $\mathscr{A}$ bezeichnet, kurz $\mathcal{V} = \mathcal{T}(\mathscr{A})$.

Genauer: Ein affiner Raum ist ein Tripel $(\mathscr{A}, \mathcal{V}, \tau)$, wobei

$$\begin{aligned}\tau : \mathcal{V} \times \mathscr{A} &\longrightarrow \mathscr{A},\\ (V, P) &\longmapsto \tau_V(P)\end{aligned}$$

eine scharf transitive Operation von $\mathcal{V} \circlearrowright \mathscr{A}$, wobei die Abbildung

$$\tau_V : \mathscr{A} \to \mathscr{A},\ P \mapsto \tau_V(P) := \tau(V, P)$$

Translation um den Vektor V von $\mathscr{A}$ heißt.

Bezeichnung: Oft schreiben wir $V + P$ oder $P + V$ anstelle von $\tau(V, P) = \tau_V(P)$.
Diese Schreibweise darf *nicht* implizieren, dass $\mathscr{A} = \mathcal{V}$ ist!

Jeder VR $\mathcal{V}$ ist ein affiner Raum mit Translationsraum $\mathcal{V}$, aber dieses Modell ($\mathscr{A} = \mathcal{V} = \mathcal{T}(\mathscr{A})$) hat den Nachteil, dass man nicht zwischen Punkten und Vektoren unterscheidet. Daher bevorzugen wir ein besseres Modell:

Beispiel 9.1.2: Affiner Standardraum

Ist $\widetilde{\mathcal{V}}$ ein K-VR mit nicht verschwindender Linearform $\varphi : \widetilde{\mathcal{V}} \to K$, so setze

$$\mathcal{V} := \operatorname{Kern} \varphi \text{ und } \mathscr{A}(\varphi) := \varphi^{-1}(\{1\})$$

Dann ist $(\mathscr{A}(\varphi), \mathcal{V}, \tau)$ mit

$$\begin{aligned}\tau :\ \mathcal{V} \times \mathscr{A}(\varphi) &\longrightarrow \mathscr{A}(\varphi),\\ (V, P) &\longmapsto V + P\end{aligned}$$

ein affiner Raum.
$\mathscr{A}(\varphi)$ ist ein Modell des VRs, in dem das Nullelement keine besondere Rolle mehr hat!
Wir sehen speziell für $\widetilde{\mathcal{V}} = K^{(n+1)\times 1}$ und $\varphi \in \left(K^{(n+1)\times 1}\right)^*$ die Projektion auf die letzte Komponente:

$$\mathscr{A}_n(K) := \mathscr{A}(\varphi) = \left\{ \begin{pmatrix} X \\ 1 \end{pmatrix} \middle| X \in K^{n\times 1} \right\}$$

und nennen ihn den ***n*-dimensionalen affinen Standardraum**. Sein Translationsraum ist

$$\mathcal{T}(\mathscr{A}_n(K)) = \left\{ \begin{pmatrix} X \\ 0 \end{pmatrix} \middle| X \in K^{n\times 1} \right\}$$

was wir mit $K^{n\times 1}$ identifizieren.

Bemerkung 9.1.3:

Sei $\mathscr{A}$ ein affiner Raum über dem K-VR $\mathcal{V}$.

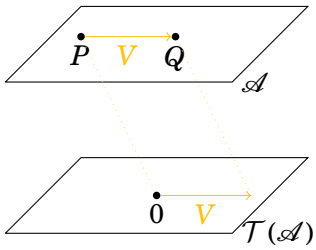
(1) Für jeden Punkt $P_0 \in \mathscr{A}$ ist

$$\begin{aligned} \mathcal{V} &\longrightarrow \mathscr{A}, \\ V &\longmapsto \tau_V(P_0) = P_0 + V \end{aligned}$$

eine Bijektion.

(2) Für jedes Paar $(P,Q) \in \mathscr{A}^2$ gibt es genau einen Vektor $V \in \mathcal{V}$ mit $\tau_V(P) = Q$. Wir bezeichnen ihn mit $V =: \overrightarrow{PQ}$ als „**Richtungsvektor** von P nach Q".

Beweis zu 9.1.3:
Spezialfall von 8.1.12. □



Übung 9.1.Ü1:

Sei K ein Körper, $\mathcal{V}$ ein K-VR, $\mathscr{A}$ ein affiner Raum über $\mathcal{V}$. Seien $P,Q,P',Q',R \in \mathscr{A}$. Dann gilt:

(1) $\overrightarrow{QP} = -\overrightarrow{PQ}$

(2) $\overrightarrow{QR} = \overrightarrow{PR} - \overrightarrow{PQ}$

(3) $\overrightarrow{PQ} = \overrightarrow{P'Q'} \Leftrightarrow \overrightarrow{PP'} = \overrightarrow{QQ'}$

Beweis:

(1) Es gilt per Def.: $Q + \overrightarrow{QP} = P \quad \| + \left(-\overrightarrow{QP}\right)$ (+ ist hier die *Translation*!)

$$\begin{aligned} &\Leftrightarrow Q + \overrightarrow{QP} + \left(-\overrightarrow{QP}\right) = P + \left(-\overrightarrow{QP}\right) \\ &\Leftrightarrow Q + \underbrace{\left(\overrightarrow{QP} + \left(-\overrightarrow{QP}\right)\right)}_{\text{Addition in } \mathcal{V}} = P + \left(-\overrightarrow{QP}\right) \\ &\Leftrightarrow Q + 0_{\mathcal{V}} = P + \left(-\overrightarrow{QP}\right) \\ &\Leftrightarrow Q = P + \left(-\overrightarrow{QP}\right) \\ &\Leftrightarrow \overrightarrow{PQ} = -\overrightarrow{QP} \text{ per Def.} \\ &\Leftrightarrow -\overrightarrow{PQ} = \overrightarrow{QP} \end{aligned}$$

(2) Es gilt: $Q + \overrightarrow{QR} = R$
$P + \overrightarrow{PR} = R$

$$P + \overrightarrow{PQ} = Q$$

$$\Rightarrow Q - \overrightarrow{PQ} = P \text{ (wobei für } A \in \mathscr{A},\ V \in \mathcal{V} \text{ hier gelte: } A + (-V) =: A - V)$$

$$\Rightarrow Q - \overrightarrow{PQ} = R - \overrightarrow{PR} \quad \| + \overrightarrow{PR}$$

$$\Leftrightarrow Q - \overrightarrow{PQ} + \overrightarrow{PR} = R - \overrightarrow{PR} + \overrightarrow{PR}$$

$$\Leftrightarrow Q + \underbrace{\left(-\overrightarrow{PQ} + \overrightarrow{PR}\right)}_{\text{Addition in } \mathcal{V}} = R + \underbrace{\left(-\overrightarrow{PR} + \overrightarrow{PR}\right)}_{= 0_{\mathcal{V}}}$$

$$\Leftrightarrow Q + \left(\overrightarrow{PR} - \overrightarrow{PQ}\right) = R$$

$$\Rightarrow \overrightarrow{QR} = \overrightarrow{PR} - \overrightarrow{PQ} \text{ per Def.}$$

(3) Es gilt per Def.:

$$P + \overrightarrow{PQ} = Q; \qquad P + \overrightarrow{PP'} = P';$$
$$P' + \overrightarrow{P'Q'} = Q'; \quad Q + \overrightarrow{QQ'} = Q'$$

Nach (1) ist

$$\begin{aligned} \overrightarrow{P'Q'} &= \overrightarrow{PQ'} - \overrightarrow{PP'} && \text{(Ia)} \\ &= \overrightarrow{QQ'} - \overrightarrow{QP'} && \text{(Ib)} \\ \overrightarrow{PQ} &= \overrightarrow{P'Q} - \overrightarrow{P'P} && \text{(IIa)} \\ &= \overrightarrow{Q'Q} - \overrightarrow{Q'P} && \text{(IIb)} \end{aligned}$$

Betrachte

$$\begin{aligned} & \overrightarrow{PQ} && = && \overrightarrow{P'Q'} && \| - \overrightarrow{P'Q'} \\ \Leftrightarrow & \underbrace{\overrightarrow{PQ}}_{\text{(IIa)}} && - && \underbrace{\overrightarrow{P'Q'}}_{\text{(Ib)}} && = 0_{\mathcal{V}} \\ \Leftrightarrow & \underbrace{\overrightarrow{P'Q} - \overrightarrow{P'P}}_{} && - && \underbrace{\overrightarrow{QQ'} + \overrightarrow{QP'}}_{} && = 0_{\mathcal{V}} \\ \Leftrightarrow & \underbrace{\overrightarrow{P'Q} - \overrightarrow{P'Q}}_{} && - && \underbrace{\overrightarrow{PP'} - \overrightarrow{QQ'}}_{} && = 0_{\mathcal{V}} \quad \| + \overrightarrow{QQ'} \\ \Leftrightarrow & 0_{\mathcal{V}} && - && \overrightarrow{P'P} = \overrightarrow{QQ'} \\ \Leftrightarrow_{(1)} & && && \overrightarrow{PP'} = \overrightarrow{QQ'} \end{aligned}$$

□

Definition 9.1.4: Affine Teilräume

Sei $(\mathscr{A}, \mathcal{V}, \tau)$ ein affiner Raum über dem K-VR $\mathcal{V}$. Eine Teilmenge $\mathscr{A}' \subseteq \mathscr{A}$ heiß **affiner Teilraum** von $\mathscr{A}$, falls ein Teilvektorraum $\mathcal{W} \leq \mathcal{V}$ existiert, sodass $\left(\mathscr{A}', \mathcal{W}, \tau|_{\mathcal{W} \times \mathscr{A}'}\right)$ ein affiner Raum über $\mathcal{W}$ ist.

Bemerkung 9.1.5:

Sei $\mathscr{A}$ ein affiner Raum über $\mathcal{V} := \mathcal{T}(\mathscr{A})$.

(1) Der Translationsraum eines affinen TR $\mathscr{A}'$ von $\mathscr{A}$ ist eindeutig bestimmt.

$$\mathcal{T}(\mathscr{A}') = \left\{ \overrightarrow{PQ} \,\middle|\, P, Q \in \mathscr{A}' \right\}$$

(2) Zu jedem $\mathcal{W} \leq \mathcal{V}$ und jedem Punkt $P \in \mathscr{A}$ gibt es genau einen affinen TR $\mathscr{A}'$ von $\mathscr{A}$ mit $P \in \mathscr{A}'$ und Translationsraum $\mathcal{T}(\mathscr{A}) = \mathcal{W}$, nämlich $\mathscr{A}' = P + \mathcal{W} = \mathcal{W} + P$.

Beweis zu 9.1.5:

(1) folgt sofort aus 9.1.3: $\overrightarrow{PQ}$ ist der *eindeutige* Vektor mit $P+V=Q$.

(2) Ganz offensichtlich operiert $\mathcal{W}$ auf $P+\mathcal{W}$ durch τ, und zwar transitiv. Dass diese Operation scharf transitiv ist, vererbt sich dadurch, dass $\mathcal{W} \leq \mathcal{V}$ und $\mathcal{V} \circlearrowright \mathscr{A} \supseteq P+\mathcal{W}$ scharf transitiv.
Damit ist $P+\mathcal{W}$ ein affiner Raum mit $\mathcal{T}(P+\mathcal{W})=\mathcal{W}$ und $P \in P+\mathcal{W}$ (nämlich für $P+0_{\mathcal{V}}$).

□

Bemerkung 9.1.6: Affines Erzeugnis

Der Schnitt affiner TRe eines affinen Raums $\mathscr{A}$ ist entweder *leer* oder wieder ein affiner TR.
Sind $\mathscr{A}_i$ $(i \in I \subseteq \mathbb{N})$ affine TRe von $\mathscr{A}$ und $P \in \bigcap_{i\in I} \mathscr{A}_i$, so ist

$$\bigcap_{i\in I} \mathscr{A}_i = P + \bigcap_{i\in I} \mathcal{T}(\mathscr{A}_i) = \left\{ \tau_V(P) = P+V \;\middle|\; V \in \bigcap_{i\in I} \mathcal{T}(\mathscr{A}_i) \right\}$$

Ist $\emptyset \neq M \subseteq \mathscr{A}$ eine Teil*menge*, so sei das **affine Erzeugnis** von M der kleinste affine TR, der M enthält: $\langle M \rangle_{\mathrm{a}} := \bigcap_{\substack{\mathscr{A}' \leq \mathscr{A} \\ M \subseteq A'}} \mathscr{A}'$

9.1.b Affine Abbildungen

Definition 9.1.7: Affine Abbildung

Seien $\mathscr{A}, \mathscr{A}'$ affine Räume über den K-VRen $\mathcal{V}=\mathcal{T}(\mathscr{A})$ und $\mathcal{V}'=\mathcal{T}(\mathscr{A}')$.
Die Abbildung $f: \mathscr{A} \to \mathscr{A}'$ heißt **affine Abbildung**, falls eine lineare Abbildung $\overline{f}: \mathcal{V} \to \mathcal{V}'$ existiert mit

$$\overrightarrow{f(P)f(Q)} = \overline{f}\left(\overrightarrow{PQ}\right) \quad \forall P,Q \in \mathscr{A}$$

Die lineare Abbildung $\overline{f}$ heißt auch der **lineare Anteil** von f.

vgl. Polynom:

$p(x) = \boxed{a_0} + \boxed{a_1 x} + \cancel{a_2 x^2 + \ldots}$

konst. Anteil linearer Anteil

Affine Geometrie

Lineare Algebra

Bemerkung 9.1.8:

Seien $\mathscr{A}, \mathscr{A}'$ affine Räume mit Translationsvektorraum $\mathcal{V}=\mathcal{T}(\mathscr{A})$ und $\mathcal{V}'=\mathcal{T}(\mathscr{A}')$. Sei $P_0 \in \mathscr{A}$ fest gewählt.

(1) Jede affine Abbildung $f: \mathscr{A} \to \mathscr{A}'$ ist eindeutig festgelegt durch $f(P_0)$ und ihrem linearen Anteil $\overline{f}: \mathcal{V} \to \mathcal{V}'$.
Ist nämlich $f(P_0) =: Q_0 \in \mathscr{A}'$, so ist für einen beliebigen Punkt $P \in \mathscr{A}$ und $V := \overrightarrow{P_0P} \in \mathcal{V}$ (sodass $\tau_V(P_0)=P$):

$$\overrightarrow{Q_0 f(P)} = \overrightarrow{f(P_0)f(P)} = \overline{f}\left(\overrightarrow{P_0P}\right) = f(V)$$

d.h. $f(P) = f(P_0) + \overline{f}(V)$ (man weiß also, wie man *jeden* Punkt P ausrechnet.)

(2) Für jeden Punkt $Q_0 \in \mathscr{A}'$ und jede lineare Abbildung $\varphi: \mathcal{V} \to \mathcal{V}'$ gibt es genau eine affine Abbildung $f: \mathscr{A} \to \mathscr{A}'$ mit $f(P_0)=Q_0$ und $\overline{f}=\varphi$, nämlich $f(P) = Q_0 + \overline{f}\left(\overrightarrow{P_0P}\right)$.

Übung 9.1.Ü2: Translationen

Translationen sind affine Abbildungen, deren linearer Anteil die Identität des Translationsraumes ist. Sie sind auch die einzigen Abbildungen eines affinen Raumes mit dieser Eigenschaft.

Beispiel 9.1.9: Affine Abbildungen von $\mathscr{A}_n(K)$

Wähle $P_0 := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \hline 1 \end{pmatrix} \in \mathscr{A}_n(K)$.

Die affine Abbildung f mit linearen Anteil ${}^{\mathcal{S}}\overline{f}^{\mathcal{S}}$ (bzgl. der Standardbasis $\mathcal{S}$ von $K^{n\times 1}$) und

$$f(P_0) = Q_0 = \begin{pmatrix} b_1 \\ \vdots \\ b_n \\ \hline 1 \end{pmatrix}$$

ist gegeben durch Matrixmultiplikation mit $\left(\begin{array}{c|c} A & b \\ \hline 0 & 1 \end{array}\right)$.

Satz 9.1.10:

Seien $\mathscr{A}, \mathscr{A}', \mathscr{A}''$ affine Räume über K-VRen.

(1) Kompositionen affiner Abbildungen sind affin.
Genauer: Sind $f : \mathscr{A} \to \mathscr{A}'$, $f' : \mathscr{A}' \to \mathscr{A}''$ affine Abbildungen, so ist

$$f' \circ f : \mathscr{A} \longrightarrow \mathscr{A}''$$

wieder affin, mit $\overline{f' \circ f} = \overline{f'} \circ \overline{f}$.

(2) Ist $f : \mathscr{A} \to \mathscr{A}'$ affin und bijektiv, so ist $f^{-1} : \mathscr{A}' \longrightarrow \mathscr{A}$ ebenfalls affin mit $\overline{f^{-1}} = \overline{f}^{-1}$.
Man sagt, dass f ein **affiner Isomorphismus** ist.
Insbesondere ist

$$\mathrm{Aff}(\mathscr{A}) := \{f : \mathscr{A} \to \mathscr{A} \mid f \text{ affin und bijektiv}\} \leq \mathrm{S}_{\mathscr{A}}$$

eine Gruppe, genannt die **affine Gruppe** von $\mathscr{A}$, und

$$\begin{aligned} \mathrm{Aff}(\mathscr{A}) &\longrightarrow \mathrm{GL}(\mathcal{T}(\mathscr{A})), \\ f &\longmapsto \overline{f} \end{aligned}$$

ist ein Gruppenhomomorphismus.

(3) Ist $f : \mathscr{A} \to \mathscr{A}'$ affin und $\mathscr{A}''$ ein affiner TR von $\mathscr{A}$, so ist $f(\mathscr{A}'')$ ein affiner TR von $\mathscr{A}'$, mit $\mathcal{T}(f(\mathscr{A}'')) = \overline{f}(\mathcal{T}(\mathscr{A}''))$.

(4) Ist $f : \mathscr{A} \to \mathscr{A}'$ affin und $\mathscr{A}''$ ein affiner TR von $\mathscr{A}'$, so ist $f^{-1}(\mathscr{A}'')$ leer oder ein affiner TR von $\mathscr{A}$ mit $\mathcal{T}\left(f^{-1}(\mathscr{A}'')\right) = \overline{f}^{-1}(\mathcal{T}(\mathscr{A}''))$.

Beweis zu 9.1.10:

(1) Für $P, Q \in \mathscr{A}$ ist

$$\begin{aligned} \overrightarrow{(f' \circ f)(P)(f' \circ f)(Q)} &= \overrightarrow{f'(f(P))f'(f(Q))} \\ &= \overline{f'}\left(\overrightarrow{f(P)f(Q)}\right) = \overline{f'}\left(\overline{f}\left(\overrightarrow{PQ}\right)\right) = \left(\overline{f' \circ f}\right)\left(\overrightarrow{PQ}\right) \end{aligned}$$

□

(2) Wegen der Identifikation nach Wahl eines Punktes von $\mathscr{A}$ mit $\mathcal{T}(\mathscr{A})$ und $\mathscr{A}'$ mit $\mathcal{T}(\mathscr{A}')$ ist klar, dass $\overline{f}: \mathcal{T}(\mathscr{A}) \to \mathcal{T}(\mathscr{A}')$ bijektiv ist. Zeige nun noch, dass $\overrightarrow{f^{-1}(P')f^{-1}(Q')} = \overline{f}^{-1}\left(\overrightarrow{P'Q'}\right)\ \forall P', Q' \in \mathscr{A}'$. Dies ist äquivalent dazu, dass $\overline{f}\left(\overrightarrow{f^{-1}(P')f^{-1}(Q')}\right) \underset{(1)}{=} \overrightarrow{P'Q'}$.

□

Satz 9.1.11: Affine Dimension

Zwei affine Räume $\mathscr{A}$ und $\mathscr{A}'$ sind isomorph genau dann, wenn $\operatorname{Dim}\mathcal{T}(\mathscr{A}) = \operatorname{Dim}\mathcal{T}(\mathscr{A}')$ ist.
Sei $\operatorname{Dim}\mathscr{A} := \operatorname{Dim}\mathcal{T}(\mathscr{A})$ die **Dimension des affinen Raumes** $\mathscr{A}$.
Insbesondere ist $\mathscr{A}$ affin isomorph zu $\mathscr{A}_n(K)$ für $n = \operatorname{Dim}\mathscr{A}$. Ein affiner Isomorphismus $\mathscr{A} \to \mathscr{A}_n(K)$ heißt **affines Koordinatensystem** (→ Descartes).

Beweis zu 9.1.11:
Ist $f: \mathscr{A} \to \mathscr{A}'$ ein affiner Isomorphismus, so ist $\overline{f}: \mathcal{T}(\mathscr{A}) \to \mathcal{T}(\mathscr{A}')$ ein VR-Isomorphismus, also $\operatorname{Dim}\mathcal{T}(\mathscr{A}) = \operatorname{Dim}\mathcal{T}(\mathscr{A}')$.
Umgekehrt sei $\varphi: \mathcal{T}(\mathscr{A}) \to \mathcal{T}(\mathscr{A}')$ ein VR-Isomorphismus. Offenbar ist für jeden festen, aber beliebigen Punkt $P_0 \in \mathscr{A}$ die Abbildung

$$\mathscr{A} \longrightarrow \mathcal{T}(\mathscr{A}),\ P \mapsto \overrightarrow{P_0P}$$

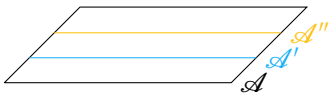
ein affiner Isomorphismus.
Dieser Isomorphismus ist gegeben durch $P \mapsto P'_0 + \varphi\left(\overrightarrow{P_0P}\right)$, wobei $P'_0 \in \mathscr{A}'$ beliebig, aber fest gewählt. □

Somit ist die Dimension eine **affine Invariante**.

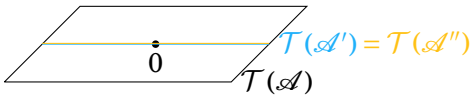
Definition 9.1.12: Parallelität

Sei $\mathscr{A}$ ein affiner Raum über dem K-VR $\mathcal{T}(\mathscr{A})$ mit affinen Teilräumen $\mathscr{A}', \mathscr{A}''$.

(1) Die TRe heißen **parallel**, falls $\mathcal{T}(\mathscr{A}') = \mathcal{T}(\mathscr{A}'')$.
(2) Die TRe heißen **schwach parallel**, falls $\mathcal{T}(\mathscr{A}') \subset \mathcal{T}(\mathscr{A}'')$ oder $\mathcal{T}(\mathscr{A}'') \subset \mathcal{T}(\mathscr{A}')$.
(3) Die TRe heißen **windschief**, wenn $\mathscr{A}' \cap \mathscr{A}'' = \emptyset$ und $\mathcal{T}(\mathscr{A}') \cap \mathcal{T}(\mathscr{A}'') = \{0\}$.



← parallel



Übung 9.1.Ü3:

Sei $\mathscr{A}$ ein affiner Raum über dem K-VR $\mathcal{V}$.

(1) Parallelität ist eine Äquivalenzrelation auf allen affinen Teilräumen von $\mathscr{A}$.
(2) Eine Äquivalenzklasse der Parallelität mit zugehörigem TR $\mathcal{W} \leq \mathcal{T}(\mathscr{A})$ bildet einen affinen Raum $\mathscr{A}/\mathcal{W} \subseteq \mathcal{U}_{\mathscr{A}}$ mit Translationsraum $\mathcal{V}/\mathcal{W}$. Man nennt ihn auch den **Bahnenraum** von $\mathscr{A}$ mod $\mathcal{W}$. Beachte: $\mathcal{V}$ operiert zwar auch transitiv auf $\mathscr{A}/\mathcal{W}$, aber nicht treu, außer bei $\mathcal{W} = \{0\}$.

Beweis:
(1) Dass Parallelität auf $\mathcal{U}_{\mathscr{A}} := \{\mathscr{A}' \mid \mathscr{A}' \leq \mathscr{A}\}$ eine Äquivalenzrelation ist, ist offensichtlich, da Gleichheit eine Äquivalenzrelation ist.

(2) Intuitiv ist dies klar – durch die Translationen außerhalb von $\mathcal{W}$ wechselt man zwischen parallelen TRen, transitiv und eindeutig.

Definiere für $\mathscr{A}' \leq \mathscr{A}$ mit $\mathcal{T}(\mathscr{A}') = \mathcal{W} \leq \mathcal{V}$ die Operation

$$\begin{aligned} \tau: \quad & \mathcal{V}/\mathcal{W} \times \mathscr{A}/\mathcal{W} \longrightarrow \mathscr{A}/\mathcal{W}, \\ & ((V+\mathcal{W}), \mathcal{P}) \longmapsto \mathcal{P} + (V+\mathcal{W}) := \{P + V + W \mid P \in \mathcal{P},\ W \in \mathcal{W}\} \end{aligned}$$

Dies ist eine Operation, denn für beliebige $\mathcal{P} \in \mathscr{A}/\mathcal{W}$ gilt:

- $\mathcal{P} + \mathcal{W} = \mathcal{P} + \mathcal{T}(\mathcal{P}) = \mathcal{P}$, da $\mathcal{T}(\mathcal{P})$ auf $\mathcal{P}$ per Def. transitiv operiert. $\Rightarrow \mathcal{P} + (0_{\mathcal{V}} + \mathcal{W}) = \mathcal{P}$

Damit kann die Operation vereinfacht werden: $\mathcal{P} + (V+\mathcal{W}) = \{P + V \mid P \in \mathcal{P}\}$

- Mit $V+\mathcal{W},\ V'+\mathcal{W} \in \mathcal{V}/\mathcal{W}$ ist

$$\mathcal{P} + (V+\mathcal{W}) + (V'+\mathcal{W}) = \{P+V \mid P \in \mathcal{P}\} + (V'+\mathcal{W}) = \left\{P' + V' \,\middle|\, P' \in \{P+V \mid P \in \mathcal{P}\}\right\} = \left\{P + V + V' \,\middle|\, P \in \right.$$

- Die Wohldefiniertheit ist klar, da in Faktorräumen gilt: Ist $V+\mathcal{W} = V'+\mathcal{W}$, so ist $V = V' + W$ für ein $W \in \mathcal{W}$, und wie im ersten Punkt gezeigt ist dieses W für die Operation irrelevant.

Seien nun $\mathcal{P}, \mathcal{Q} \in \mathscr{A}/\mathcal{W}$, $P \in \mathcal{P}$, $Q \in \mathcal{Q}$ beliebig. Da $P + \overrightarrow{PQ} = Q$, gilt:

$$P + \left(\overrightarrow{PQ} + \mathcal{W}\right) = \left\{P + \overrightarrow{PQ} + W \,\middle|\, W \in \mathcal{W}\right\} = \{Q + W \mid W \in \mathcal{W}\}$$

wieder, da $\mathcal{W}$ auf $\mathcal{Q}$ transitiv operiert.

$\Rightarrow \mathcal{P} + \left(\overrightarrow{PQ} + \mathcal{W}\right) = \mathcal{Q} \Rightarrow \mathcal{V}/\mathcal{W}$ operiert *transitiv* auf $\mathscr{A}/\mathcal{W}$.

Außerdem: Seien auch $P' \in \mathcal{P}$, $Q' \in \mathcal{Q}$. $\Rightarrow P' = P + W_1$, $Q' = Q + W_2$ für jeweils ein *eindeutiges* $W_1, W_2 \in \mathcal{W}$, da $\mathcal{W}$ auf auf $\mathcal{P}$ und $\mathcal{Q}$ scharf transitiv operiert (Satz 8.1.12).

Es ist $P' + \overrightarrow{P'Q'} = Q'$

$$\begin{aligned} &\Leftrightarrow P + W_1 + \overrightarrow{P'Q'} = Q + W_2 \\ &\Leftrightarrow P + \left(\overrightarrow{P'Q'} + W_1 - W_2\right) = Q \\ &\Rightarrow \overrightarrow{PQ} = \overrightarrow{P'Q'} + W_1 - W_2, \text{ da die Richtungsvektoren eindeutig sind} \\ &\Rightarrow \overrightarrow{PQ} + \mathcal{W} = \overrightarrow{P'Q'} + \mathcal{W}, \text{ d.h. Richtungsvektoren in } \mathcal{V}/\mathcal{W} \text{ sind eindeutig} \end{aligned}$$

$\Rightarrow$ Nach 8.1.12, (2)$\Rightarrow$(1), folgt: $\mathcal{V}/\mathcal{W}$ operiert scharf transitiv auf $\mathscr{A}/\mathcal{W}$.

Damit ist $\mathscr{A}/\mathcal{W}$ ein affiner Raum mit $\mathcal{T}\left(\mathscr{A}/\mathcal{W}\right) = \mathcal{V}/\mathcal{W}$.

□

Übung 9.1.Ü4:

Seien $\mathcal{U}, \mathcal{W} \leq \mathcal{V}$ und

$$\begin{aligned} \varphi: \mathscr{A} &\longrightarrow \mathscr{A}/\mathcal{U} \times \mathscr{A}/\mathcal{W}, \\ P &\longmapsto (P+\mathcal{U}, P+\mathcal{W}) \end{aligned}$$

Dann gilt:

(1) φ ist eine affine Abbildung.

(2) φ ist injektiv $\Leftrightarrow \mathcal{U} \cap \mathcal{W} = \{0\}$.

(3) φ ist surjektiv $\Leftrightarrow \mathcal{U} + \mathcal{W} = \mathcal{V}$.

Beweis:

(1) $\mathscr{A}/\mathcal{U} \times \mathscr{A}/\mathcal{W}$ ist affiner Raum mit

- $\mathcal{T}\left(\mathscr{A}/\mathcal{U} \times \mathscr{A}/\mathcal{W}\right) = \mathcal{V}/\mathcal{U} \oplus \mathcal{V}/\mathcal{W}$
- $(Q+\mathcal{U}, Q'+\mathcal{W}) + \left(\overline{U}, \overline{W}\right) := ((Q+U)+\mathcal{U}, (Q'+W)+\mathcal{W})$

und es gilt:

$$\begin{aligned}\overrightarrow{\varphi(P)\varphi(Q)} &= \overrightarrow{(P+\mathcal{U}, P+\mathcal{W})(Q+\mathcal{U}, Q+\mathcal{W})} \\ &= \left(\overrightarrow{PQ}+\mathcal{U},\ \overrightarrow{PQ}+\mathcal{W}\right) \\ &= \overline{\varphi}\left(\overrightarrow{PQ}\right)\end{aligned}$$

$$\begin{aligned}\overline{\varphi}: \mathcal{V} &\longrightarrow \mathcal{V}/\mathcal{U} \oplus \mathcal{V}/\mathcal{W}, \\ V &\mapsto (V+\mathcal{U}, V+\mathcal{W})\end{aligned}$$

(2) φ injektiv $\overset{9.1.8}{\iff}$ $\overline{\varphi}$ injektiv $\Leftrightarrow \operatorname{Kern}\overline{\varphi} = \{0\} = \mathcal{U} \cap \mathcal{W} = \{0\}$.

(3) φ surjektiv $\overset{9.1.8}{\iff}$ $\overline{\varphi}$ surjektiv $\Leftrightarrow \mathcal{U} + \mathcal{W} = \mathcal{V}$.

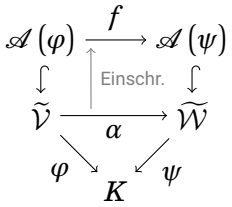
□

Bemerkung 9.1.13:

Parallelität und schwache Parallelität bleiben unter affinen Abbildungen erhalten. Die Eigenschaft, windschief zu sein, bleibt unter mindestens injektiven affinen Abbildungen erhalten.

Beispiel 9.1.14:

Seien $\widetilde{\mathcal{V}}$, $\varphi \in \widetilde{\mathcal{V}}^* = \operatorname{Hom}(\widetilde{\mathcal{V}}, K)$, $\mathcal{V} := \operatorname{Kern}\varphi$ und $\mathscr{A}(\varphi) := \varphi^{-1}(\{1\})$ wie in Beispiel 9.1.2.
Entsprechend nehmen wir einen zweiten affinen Raum mit weiteren Daten $\widetilde{\mathcal{W}}$, $\psi \in \widetilde{\mathcal{W}}^*$, $\mathcal{W} := \operatorname{Kern}\psi$, $\mathscr{A}(\psi) := \psi^{-1}(\{1\})$.
Dann ist eine affine Abbildung $f : \mathscr{A}(\varphi) \to \mathscr{A}(\psi)$ nichts anderes als die Einschränkung einer linearen Abbildung $\alpha : \widetilde{\mathcal{V}} \to \widetilde{\mathcal{W}}$, welche $\mathscr{A}(\varphi)$ in $\mathscr{A}(\psi)$ abbildet, d.h. $\psi \circ \alpha = \varphi$.
Wir haben also das kommutative Diagramm



Übung 9.1.Ü5:

α legt f eindeutig fest und umgekehrt.

Beweis zu 9.1.14:

(1) Sei B eine Basis von $\mathcal{V} = \operatorname{Kern}\varphi \leq \widetilde{\mathcal{V}}$, $a, b \in \widetilde{\mathcal{V}}/\mathcal{V}$; $\varphi(a) = a' \neq 0$, $\varphi(b) = b' \neq 0$ in K.

$$\Rightarrow \varphi\left(\frac{a'}{b'} \cdot b\right) = \frac{a'}{b'}\varphi(b) = a' = \varphi(a)$$

$$\Rightarrow \varphi\left(\frac{a'}{b'}b - a\right) = 0 \Rightarrow \frac{a'}{b'}b - a \in \operatorname{Kern}\varphi$$

$$\Rightarrow \frac{a'}{b'}b = a + \lambda_1 B_1 + \cdots + \lambda_k B_k$$

$$\Rightarrow \frac{a'}{b'}b = a + \lambda_1 B_1 + \cdots + \lambda_k B_k$$

$$\Rightarrow b \in \langle a \rangle + \langle B \rangle$$

$$\Rightarrow \widetilde{\mathcal{V}} = \langle a \rangle + \mathcal{V}$$

Man sagt auch, der Kern hat **Kodimension** 1: 1 Vektor fehlt, um ganz $\widetilde{\mathcal{V}}$ zu erzeugen.

Sei $\alpha : \widetilde{\mathcal{V}} \to \widetilde{\mathcal{W}},\ a \mapsto f(a),\ B_i \mapsto \overline{f}(B_i)$. α ist linear, da sie auf einer Basis definiert ist.

- $V \in \mathscr{A}(\varphi) \subseteq \widetilde{\mathcal{V}} \Rightarrow V = a + b,\ b \in \mathcal{T}(\mathscr{A}(\varphi)) = \mathcal{V}$

$$\Rightarrow f(V) = f(a) + \overline{f}(b) = \alpha(a) + \alpha(b) = \alpha(V)$$
$$\Rightarrow \psi(f(V)) = \psi(\alpha(V)) = \underbrace{\psi(f(a))}_{\in \mathscr{A}(\psi)} + \psi\Big(\underbrace{\overline{f}(b)}_{\in \widetilde{\mathcal{W}}}\Big) = 1 + 0 = 1$$

- $V \in \widetilde{\mathcal{V}} \Rightarrow V = \lambda a + b',\ b' \in \mathcal{V} \Rightarrow \psi(\alpha(V)) = \lambda \cdot 1 = \varphi(V)$

(2) „⇒“: Klar: $f = \alpha\big|_{\mathscr{A}(\varphi)} \Rightarrow f$ eindeutig durch α definiert.

„⇐“:
- $a + 0 \in \mathscr{A}(\varphi)$
  $\Rightarrow \alpha'(a + 0) = f(a + 0) = f(a) = \alpha(a)$
- $\alpha'(a) + \alpha'(b) = \alpha'(a + b) = f(a + b) = f(a) + \overline{f}(b) = \alpha'(a) + \overline{f}(b),\ b \in B$ (Basis)
  $\Rightarrow \alpha'(b) = \overline{f}(b) = \alpha(b)$
  $\Rightarrow \alpha = \alpha'$ (weil Basis α komplett definiert)

□

Wichtiger Spezialfall: AFFINE GRUPPE

$\mathrm{Aff}(\mathscr{A}_n(K))$ kann mit der Matrixgruppe

$$\mathrm{Aff}_n(K) := \left\{ \left(\begin{array}{c|c} A & t \\ \hline 0 & 1 \end{array}\right) \middle| A \in \mathrm{GL}_n(K),\ t \in K^{n\times 1} \right\} \leq \mathrm{GL}_{n+1}(K)$$

identifiziert werden, die durch Linksmultiplikation auf

$$\mathscr{A}_n(K) = \left\{ \left(\begin{array}{c} X \\ \hline 1 \end{array}\right) \middle| X \in K^{n\times 1} \right\}$$

operiert. Man beachte, dass $\mathrm{Aff}_n(K)$ bereits als Stabilisator eines Kovektors (d.h. eines Vektors im Dualraum, auch Funktional genannt) in Beispiel 8.1.30 und als semidirektes Produkt in Beispiel 8.2.15 vorkam.

Bemerkung 9.1.15:

In $\mathrm{Aff}_n(K)$ gelten:

$$\left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array}\right)\left(\begin{array}{c|c} b & t \\ \hline 0 & 1 \end{array}\right) = \left(\begin{array}{c|c} ab & as+t \\ \hline 0 & 1 \end{array}\right)$$
$$\left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array}\right)^{-1} = \left(\begin{array}{c|c} a^{-1} & -a^{-1}t \\ \hline 0 & 1 \end{array}\right)$$
$$\left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array}\right)\left(\begin{array}{c|c} \mathrm{I}_n & s \\ \hline 0 & 1 \end{array}\right)\left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array}\right)^{-1} = \left(\begin{array}{c|c} \mathrm{I}_n & as \\ \hline 0 & 1 \end{array}\right)$$
$$\text{denn } \left(\begin{array}{c|c} a & a+st \\ \hline 0 & 1 \end{array}\right)\left(\begin{array}{c|c} a^{-1} & -a^{-1}t \\ \hline 0 & 1 \end{array}\right) = \left(\begin{array}{c|c} \mathrm{I}_n & -\cancel{aa^{-1}}t + as + t \\ \hline 0 & 1 \end{array}\right)$$

Der Homomorphismus „linearer Anteil nehmen“ ist hier gegeben durch

$$\mathrm{Aff}_n(K) \longrightarrow \mathrm{GL}_n(K),\ \left(\begin{array}{c|c} a & t \\ \hline 0 & 1 \end{array}\right) \longmapsto a$$

9.1.c Das Invarianzprinzip der affinen Geometrie

Bemerkung 9.1.16:

$\mathrm{Aff}(\mathscr{A})$ operiert transitiv auf dem affinen Raum $\mathscr{A}$ und hat genau zwei Bahnen auf $\mathscr{A} \times \mathscr{A}$.

Beweis zu 9.1.16:

$\mathcal{T}(\mathscr{A}) \leq \mathrm{Aff}(\mathscr{A})$ operiert scharf transitiv auf $\mathscr{A}$ per Def., also insbesondere transitiv und somit auch $\mathrm{Aff}(\mathscr{A})$.

$$\mathscr{A} \simeq \mathrm{Aff}(\mathscr{A}) / \mathrm{GL}(\mathcal{T}(\mathscr{A}))$$

Ist $P_0 \in \mathscr{A}$, so ist der Stabilisator $\mathrm{Stab}_{\mathrm{Aff}(\mathscr{A})}(P_0) \cong \mathrm{GL}(\mathcal{T}(\mathscr{A}))$ vermöge dem Gruppenisomorphismus

$$\mathrm{Stab}_{\mathrm{Aff}(\mathscr{A})} \ni f \mapsto \left(\overline{f} : \overrightarrow{P_0 P} \mapsto \overrightarrow{P_0 f(P)}\right) \in \mathrm{GL}(\mathcal{T}(\mathscr{A}))$$

Also hat $\mathrm{Stab}_{\mathrm{Aff}(\mathscr{A})}(P_0)$ zwei Bahnen auf $\mathscr{A}$, nämlich $\{P_0\}$, $\mathscr{A} \setminus \{P_0\}$. □

In unserem Standardmodell kann man ohne Einschränkung annehmen, dass $P_0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \hline 1 \end{pmatrix}$ ist.

$$\mathrm{Stab}_{\mathrm{Aff}(\mathscr{A})}(P_0) = \left\{ \left(\begin{array}{c|c} a & 0 \\ \hline 0 & 1 \end{array} \right) \middle| a \in \mathrm{GL}_n(K) \right\}$$

Bei der Operation auf Tripeln bekommen wir die ersten geometrischen Invarianten:

Definition 9.1.17: KOLLINEARITÄT

(1) $P \in \mathscr{A}^n$ heißt **affin unabhängig**, falls für jeden affinen Raum $\mathscr{A}'$ über K und jedes Tupel $Q \in (\mathscr{A}')^n$ eine affine Abbildung $f : \mathscr{A} \to \mathscr{A}'$ existiert mit $f \circ P = Q$, d.h. $f(P_i) = Q_i \ \forall i \in \underline{n}$.
Ein maximal affin unabhängiges System in $\mathscr{A}$, d.h. das ganz $\mathscr{A}$ erzeugt, heißt **affine Basis**.

(2) P heißt **kollinear**, falls $\mathrm{Dim}\langle P \rangle_{\mathrm{a}} \leq 1$, und **komplanar**, falls $\mathrm{Dim}\langle P \rangle_{\mathrm{a}} \leq 2$.

Bemerkung 9.1.18:

Für $P \in \mathscr{A}^n$ sind folgende Aussagen äquivalent:

(1) P ist affin unabhängig.

(2) $\mathrm{Dim}\langle P \rangle_{\mathrm{a}} = n - 1$

(3) $\left(\overrightarrow{P_n P_1}, \ldots, \overrightarrow{P_n P_{n-1}}\right) \in \mathcal{T}(\mathscr{A})^{n-1}$ ist linear unabhängig.

(4) Die affine Abbildung

$$\begin{aligned} f : \quad & \mathscr{A}_{n-1}(K) \longrightarrow \langle P \rangle_{\mathrm{a}} \leq \mathscr{A}, \\ & \widetilde{E}_i := \begin{pmatrix} E_i \\ \hline 1 \end{pmatrix} \longmapsto P_i, \\ & \widetilde{E}_n := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \hline 1 \end{pmatrix} \longmapsto P_n \end{aligned}$$

definiert einen affinen Isomorphismus.

Beweis zu 9.1.18:

VORBEMERKUNG: Es gilt $\mathcal{T}(\langle P \rangle_{\mathrm{a}}) = \left\langle \overrightarrow{P_n P_1}, \ldots, \overrightarrow{P_n P_{n-1}} \right\rangle$.

(1)⇒(4): Es liegt eine affine Abbildung vor mit $f\left(\widetilde{E}_n\right) = P_n$ und $\overline{f} : K^{(n-1)\times 1} \to \mathcal{T}(\langle P \rangle_{\mathrm{a}}) \leq \mathcal{T}(\mathscr{A}) =: \mathcal{V}$, $E_i \mapsto \overrightarrow{P_n P_1}$.
Aus der Definition der affinen Unabhängigkeit von P erhält man eine affine Abbildung $\mathscr{A} \to \mathscr{A}_{n-1}(K)$, die P_i auf $\widetilde{E}_i$ abbildet. Die Einschränkung dieser zweiten Abbildung auf $\langle P \rangle_{\mathrm{a}}$ liefert das Inverse, d.h. es liegt ein affiner Isomorphismus vor.

(4)⇒(2): Die Dimension ist eine Invariante unter affinen Isomorphismen.

(2)⇒(3): Es ist $n-1=\operatorname{Dim}\langle P\rangle_a=\operatorname{Dim}\mathcal{T}(\langle P\rangle_a)=\left\langle\overrightarrow{P_nP_1},\dots,\overrightarrow{P_nP_{n-1}}\right\rangle$.

(3)⇒(1): Sei $\mathscr{A}'$ irgendein affiner Raum über dem K-VR $\mathcal{V}'$ und $Q\in(\mathscr{A}')^n$. Es existiert eine lineare Abbildung $\varphi:\mathcal{V}\to\mathcal{V}'$ mit $\varphi\left(\overrightarrow{P_nP_1}\right):=\overrightarrow{Q_nQ_1}$. Also gibt es genau eine affine Abbildung $f:\mathscr{A}\to\mathscr{A}'$ mit $\overline{f}=\varphi$ und $f(P_n)=Q_n$. Für diese gilt offenbar $f(P_i)=Q_i\ \forall i\in\underline{n}$.

□

Übung 12.1:

Sei K ein Körper und $(\mathscr{A},\mathcal{V},\tau),(\mathscr{A}',\mathcal{V}',\tau')$ affine Räume.

(1) Sei $f:\mathscr{A}\to\mathscr{A}'$ eine affine Abbildung. Dann gilt $\forall P\in\mathscr{A},\ V\in\mathcal{V}:f(P+V)=f(P)+\overline{f}(V)$.

(2) Die Abbildung f in 9.1.17.(2) ist eindeutig.
GENAUER: Sei $P\in\mathscr{A}^{n+1}$ eine **affine Basis**, d.h. P ist affin unabhängig und $\langle P\rangle_a=\mathscr{A}$. Sei $Q\in(\mathscr{A}')^{n+1}$. Per Definition existiert eine affine Abbildung $f:\mathscr{A}\to\mathscr{A}$ mit $f\circ P=Q$. Diese Abbildung ist eindeutig.

(3) Für allgemeine $X\in\mathscr{A}$ kann $f(X)$ leicht mit der Basis ausgerechnet werden.

Beweis:

(1) Seien $P\in\mathscr{A},\ V\in\mathcal{V}$ beliebig. Es gilt per Def.:

$$\overrightarrow{f(P)f(P+V)}=\overline{f}\left(\overrightarrow{P(P+V)}\right)\qquad(*)$$
$$\Rightarrow f(P)+\overrightarrow{f(P)f(P+V)}=f(P+V)$$
$$\overset{(*)}{\iff} f(P)+\overline{f}\left(\overrightarrow{P(P+V)}\right)=f(P+V)$$

und ganz offensichtlich ist $\overrightarrow{P(P+V)}=V$, daher: $\Rightarrow f(P)+\overline{f}(V)=f(P+V)$. □

(2) Es gilt nach Bemerkung 9.1.18:

- $\operatorname{Dim}\langle P\rangle_a=\operatorname{Dim}\mathscr{A}=\operatorname{Dim}\mathcal{V}=n+1-1=n$
- $\left(\overrightarrow{P_{n+1}P_1},\overrightarrow{P_{n+1}P_2},\dots,\overrightarrow{P_{n+1}P_n}\right)\in\mathcal{V}^n$ ist linear unabhängig.

$\Rightarrow\left(\overrightarrow{P_{n+1}P_1},\overrightarrow{P_{n+1}P_2},\dots,\overrightarrow{P_{n+1}P_n}\right)$ ist Basis von $\mathcal{V}$.

Es gilt für $i\in\underline{n}$: $f(P_i)=f\left(P_{n+1}+\overrightarrow{P_{n+1}P_i}\right)\overset{(1)}{=}f(P_{n+1})+\overline{f}(P_{n+1}P_i)=Q_i$.

$\Rightarrow\overline{f}\left(\overrightarrow{P_{n+1}P_i}\right)=\overrightarrow{f(P_{n+1})Q_i}=\overrightarrow{Q_{n+1}Q_i}$

Eine lineare Abbildung ist durch das Bild von Basisvektoren eindeutig definiert. Nach 9.1.3 ist $\overrightarrow{Q_{n+1}Q_i}$ eindeutig. $\Rightarrow\overline{f}$ ist eindeutig.

$f(P_{n+1})=Q_{n+1}$ ist nach Voraussetzung bereits eindeutig. Nach 9.1.8 ist damit f eindeutig.

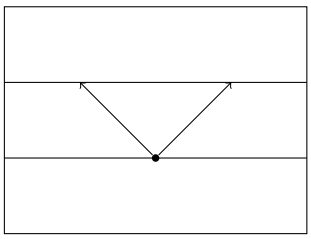
(3) Es ist $X=P_{n+1}+\overrightarrow{P_{n+1}X}$, wobei $\overrightarrow{P_{n+1}X}=\sum_{i=1}^{n}x_i\overrightarrow{P_{n+1}P_i}$ mit $x\in K^n$ (Basiszerlegung).

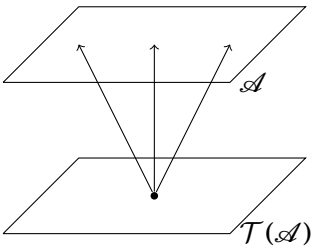
$$\Rightarrow f(X)=f(P_{n+1})+\overline{f}\left(\overrightarrow{P_{n+1}X}\right)=Q_{n+1}+\sum_{i=1}^{n}x_i\overline{f}\left(\overrightarrow{P_{n+1}P_i}\right)=Q_{n+1}+\sum_{i=1}^{n}x_i\overrightarrow{Q_{n+1}Q_i}.$$

□

Bemerkung 9.1.19:

Ist $\mathscr{A}=\varphi^{-1}(\{1\})\subseteq\widetilde{\mathcal{V}}$ für $\varphi\in\widetilde{\mathcal{V}}^*$, so ist $P\in\mathscr{A}^n$ affin unabhängig, genau dann, wenn P als Tupel in $\widetilde{\mathcal{V}}$ betrachtet linear unabhängig ist.
Die affinen Basen von $\mathscr{A}$ sind also genau die Basen von $\widetilde{\mathcal{V}}$, die in $\mathscr{A}\subseteq\widetilde{\mathcal{V}}$ enthalten sind.





Bemerkung 9.1.20:

(1) Affine Abhängigkeit von Tupeln bleibt erhalten unter Bildern affiner Abbildungen.

(2) Affine Unabhängigkeit von Tupeln bleibt unter injektiven affinen Abbildungen erhalten.

Beweis zu 9.1.20:
Folgt sofort aus 9.1.18. □

Satz 9.1.21:

Sei $\mathscr{A}$ ein affiner Raum über einem e.e. K-VR. Dann operiert $\mathrm{Aff}(\mathscr{A})$ scharf transitiv auf der Menge aller affinen Basen von $\mathscr{A}$.
(Vgl.: GL operiert scharf transitiv auf der Menge der K-VR-Basen)
Letztere bilden eine der Bahnen der Operation von $\mathrm{Aff}(\mathscr{A})$ auf $\mathscr{A}^{n+1}$, mit $n = \mathrm{Dim}\,\mathscr{A}$.

Beweis zu 9.1.21:
Folgt sofort aus 9.1.11 und 9.1.18. □

Satz 9.1.22:

(1) $\mathrm{Aff}(\mathscr{A})$ operiert transitiv auf der Menge $\mathscr{A}^3_{\text{generisch}}$ der affin unabhängigen Tripel in $\mathscr{A}^3$ (nicht entartete Dreicke, entartet = „zu einer Linie entartet"), falls $\mathrm{Dim}\,\mathscr{A} \geq 2$. d.h. *alle* Dreicke sind affin kongruent!

(2) Eine trennende Invariante für die Operation von $\mathrm{Aff}(\mathscr{A})$ auf der Menge

$$\mathscr{A}^3_{\text{spez}} := \{P = (P_1, P_2, P_3) \mid P_1 \neq P_2,\ P \text{ kollinear}\}$$

ist das **Teilverhältnis.** Dabei ist das Teilverhältnis $\mathrm{TV}(P_1, P_2, P_3)$ definiert als das eindeutige $a \in K$ mit $\overrightarrow{P_1P_3} = a\overrightarrow{P_1P_2}$.

Beweis zu 9.1.22:

(1) Wir können o.B.d.A. in $\mathscr{A} = \mathscr{A}(\varphi) = \varphi^{-1}(\{1\}) \subseteq \widetilde{\mathcal{V}}$ arbeiten.

Offenbar hat $\widetilde{\mathcal{V}}$ eine Basis $B \in \mathscr{A}^{n+1}$ und jedes affin unabhängige Tripel $P \in \mathscr{A}^3$ kann seinerseits zu einer Basis $\widehat{P} \in \mathscr{A}^{n+1}$ von $\widetilde{\mathcal{V}}$ ergänzt werden.

Es genügt z.z., dass $f \in \mathrm{Aff}(\mathscr{A})$ existiert mit $f(B_1, B_2, B_3) = P$. Dies ist klar, denn ein solches f wird induziert von der eindeutigen linearen Abbildung, die B auf $\widehat{P}$ abbildet. (Spezialfall vom vorherigen Satz)

(2) Dass eine Invariante vorliegt, ist klar aus der Definition einer affinen Abbildung. Um z.z., dass sie die Bahnen trennt, gehen wir von der Situation des Beweises von (1) aus mit Basis B. Sei $P \in \mathscr{A}^3_{\text{spez}}$ mit Teilverhältnis $a \in K$.

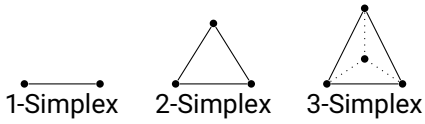
Es genügt z.z., dass ein $f \in \mathrm{Aff}(\mathscr{A})$ existiert mit $f((B_1, B_2, \ldots, B_1 + a(B_2 - B_1))) = P$.

Zu diesem Zweck ergänzt man (P_1, P_2) zu einer Basis $\widehat{P} \in \mathscr{A}^{n+1}$ von $\widetilde{\mathcal{V}}$. Die lineare Abbildung, die B auf $\widehat{P}$ abbildet, induziert durch Einschränkung auf $\mathscr{A} \subseteq \widetilde{\mathcal{V}}$ einen gewünschten affinen Automorphismus. □

Aus dem letzten Beweis erhalten wir eine Folgerung, die eine anschauliche Darstellung der affinen Gruppe $\mathrm{Aff}(\mathscr{A})$ liefert:

Korollar 9.1.23:

Sei $\operatorname{Dim}\mathscr{A} = n$. Dann operiert $\operatorname{Aff}(\mathscr{A})$ transitiv auf $\mathscr{A}^k_{\text{generisch}} := \{P \in \mathscr{A}^k \mid P \text{ affin unabhängig}\}$, der Menge der affin unabhängigen Tupel ($(k-1)$-Simplizes) für $k \notin \underline{n+1}$. Im Fall $k = n+1$ ist der Stabilisator eines solchen Tupels trivial, d.h. in diesem Fall ist die Operation scharf transitiv.



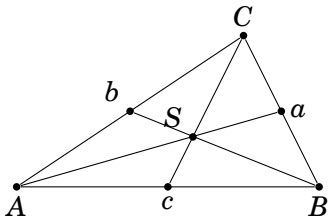
Verallgemeinerung der nicht-entarteten Dreiecke.

„nicht-ägyptische Pyramide“

Wir wollen jetzt als Beispiel einen geometrischen Satz beweisen:

Satz 9.1.24: Seitenhalbierendensatz (Descartes)

Sei K ein Körper mit $6 \cdot 1 \neq 0 \in K$, $\mathscr{A}$ ein affiner Raum über K und $(A,B,C) \in \mathscr{A}^3_{\text{generisch}}$.



Dann schneiden sich die Seitenhalbierenden des nicht-entarteten Dreiecks (A,B,C) in einem Punkt S, sodass das Teilverhältnis $\operatorname{TV}(A,a,S) = \frac{2}{3}$, wobei a der Mittelpunkt der Seite (C,B) ist.

Beweis zu 9.1.24:

Zunächst einmal definieren wir die Seitenhalbierenden:

$$s_a := \langle A, a\rangle_{\mathrm{a}}$$
$$s_b := \langle B, b\rangle_{\mathrm{a}}$$
$$s_c := \langle C, c\rangle_{\mathrm{a}}$$

wobei $a := B + \frac{1}{2}\overrightarrow{BC}$, $b := A + \frac{1}{2}\overrightarrow{AC}$ und $c := A + \frac{1}{2}\overrightarrow{AB}$ ist.
Um zu rechnen, wählen wir Koordinaten für die Eckpunkte (A,B,C) des Dreiecks, also einen affinen Isomorphismus

$$f : \langle A,B,C\rangle_{\mathrm{a}} \longrightarrow \mathscr{A}_2(K)$$

definiert durch

$$f(A) := \begin{pmatrix} 0 \\ 0 \\ \hline 1 \end{pmatrix},\ f(B) := \begin{pmatrix} 2 \\ 0 \\ \hline 1 \end{pmatrix},\ f(C) := \begin{pmatrix} 0 \\ 2 \\ \hline 1 \end{pmatrix}$$

Ein solcher Isomorphismus existiert per Definition, da (A,B,C) affin unabhängig sind. Es genügt, den Satz für das Bild unter f zu zeigen, da die Aussage invariant unter affinen Isomorphismen ist. Dann ergeben sich die Fußpunkte

$$f(a) = f\left(B + \frac{1}{2}\overrightarrow{BC}\right) = f(B) + \frac{1}{2}f\left(\overrightarrow{BC}\right) = \begin{pmatrix} 1 \\ 1 \\ \hline 1 \end{pmatrix}$$

$$f(b) = \begin{pmatrix} 0 \\ 1 \\ \hline 1 \end{pmatrix},\ f(c) = \begin{pmatrix} 1 \\ 0 \\ \hline 1 \end{pmatrix}$$

Die Seitenhalbierenden sind dann

$$f(s_a) = \left\{ f(A) + \alpha \overline{f}\left(\overrightarrow{Aa}\right) = \begin{pmatrix} \alpha \\ \alpha \\ \hline 1 \end{pmatrix} \middle| \alpha \in K \right\}$$
$$f(s_b) = \left\{ \begin{pmatrix} 2-2\beta \\ \beta \\ \hline 1 \end{pmatrix} \middle| \beta \in K \right\}$$
$$f(s_c) = \left\{ \begin{pmatrix} \gamma \\ 2-2\gamma \\ \hline 1 \end{pmatrix} \middle| \gamma \in K \right\}$$

Um den Schnittpunkt $\{S\} = s_a \cap s_b \cap s_c$ zu berechnen, suchen wir $\alpha, \beta, \gamma \in K$ mit

$$\begin{pmatrix} \alpha \\ \alpha \\ \hline 1 \end{pmatrix} = \begin{pmatrix} 2-2\beta \\ \beta \\ \hline 1 \end{pmatrix} = \begin{pmatrix} \gamma \\ 2-2\gamma \\ \hline 1 \end{pmatrix}$$

Lösen des LGS (nur erste beiden Zeilen wichtig) ergibt:

$$\alpha = \beta = \gamma = \frac{2}{3} \Rightarrow f(S) = \begin{pmatrix} \frac{2}{3} \\ \frac{2}{3} \\ \hline 1 \end{pmatrix}$$

Das Teilverhältnis ergibt sich als

$$\mathrm{TV}(A,a,S) = \mathrm{TV}(f(A), f(B), f(C)) = \frac{2}{3} = \mathrm{TV}(B,b,S) = \mathrm{TV}(C,c,S)$$

□

Zum Beweis des nächsten Satzes benötigen wir sogenannte **Streckungen**, also affine Abbildungen der Form

$$\begin{aligned} \mathscr{A} &\longrightarrow \mathscr{A}, \\ P &\longmapsto P_0 + a\overrightarrow{P_0P} \end{aligned}$$

wobei der feste Punkt $P_0 \in \mathscr{A}$ das **Streckzentrum** und das $a \in K^*$ der **Streckfaktor** ist.

Übung 9.1.Ü6:

(1) Je zwei Streckungen sind konjugiert in $\mathrm{Aff}(\mathscr{A})$ genau dann, wenn sie denselben Streckfaktor haben.

(2) Die Streckungen zusammen mit den Translationen bilden einen Normalteiler in $\mathrm{Aff}(\mathscr{A})$, der zur Matrixgruppe

$$\left\{ \left(\begin{array}{c|c} a\mathrm{I}_n & t \\ \hline 0 & 1 \end{array} \right) \middle| a \in K^*,\ t \in K^{n\times 1} \right\}$$

isomorph ist.

Beweis:
Sei $\mathrm{Dim}\,\mathscr{A} =: n \in \mathbb{N}$.

$$\Rightarrow \mathscr{A} \cong \mathscr{A}_n(K)$$
$$\Rightarrow \mathrm{Aff}(\mathscr{A}) \underset{\Phi}{\cong} \mathrm{Aff}_n(K)$$
$$f \circ g \mapsto \Phi(g) \cdot \Phi(g)$$

$$G := \langle \{\text{Streckungen, Translationen}\} \rangle \leq \mathrm{Aff}(\mathscr{A})$$
$$M := \left\{ \left(\begin{array}{c|c} a\mathrm{I}_n & t \\ \hline 0 & 1 \end{array} \right) \middle| \, a \in K^*,\ t \in K^{n\times 1} \right\}$$
$$\varphi : G \longrightarrow M,$$
$$\left(S : \mathscr{A} \to \mathscr{A},\ P \mapsto P_0 + s\overrightarrow{P_0P} \right) \longmapsto \left(\begin{array}{c|c} s\mathrm{I}_n & 0 \\ \hline 0 & 1 \end{array} \right),$$
$$(T : \mathscr{A} \to \mathscr{A},\ P \mapsto P + t) \longmapsto \left(\begin{array}{c|c} \mathrm{I}_n & t \\ \hline 0 & 1 \end{array} \right)$$
$$\varphi(T \circ S) = \varphi(T) \cdot \varphi(S)$$
$$\varphi(S \circ T) = \varphi(S) \cdot \varphi(T)$$

φ bijektiv.
NORMALTEILER:

$$\left(\begin{array}{c|c} a & b \\ \hline 0 & 1 \end{array} \right) \cdot \left(\begin{array}{c|c} s\mathrm{I}_n & t \\ \hline 0 & 1 \end{array} \right) \cdot \left(\begin{array}{c|c} a & b \\ \hline 0 & 1 \end{array} \right)^{-1}$$
$$= \left(\begin{array}{c|c} as\mathrm{I}_n & at+b \\ \hline 0 & 1 \end{array} \right) \left(\begin{array}{c|c} -a^{-1} & -a^{-1}b \\ \hline 0 & 1 \end{array} \right)$$
$$= \left(\begin{array}{c|c} b\mathrm{I}_n & t' \\ \hline 0 & 1 \end{array} \right) \in M$$

$\mathrm{Aff}_n(K)$ operiert durch Konjugation auf M.
$\Rightarrow M$ ist Vereinigung von Konjugiertenklassen.
$\Rightarrow M \trianglelefteq \mathrm{Aff}(K)$
$\Rightarrow \varphi^{-1}(M) = G$, und ein Isomorphismus bildet NT auf NT ab.
$\Rightarrow G \trianglelefteq \mathrm{Aff}(\mathscr{A})$

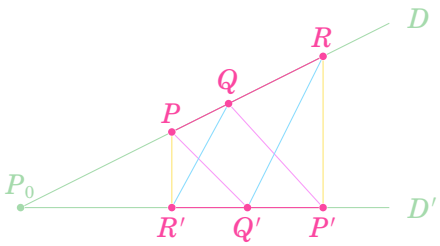
Seien $S, S' : \mathscr{A} \to \mathscr{A}$ Streckungen. S, S' seien konjugiert, d.h. $\exists f : f \circ S \circ f^{-1} = S'$.

$$\Leftrightarrow \varphi(f) \cdot \varphi(S) \cdot \varphi\left(f^{-1}\right) = \varphi\left(S'\right)$$
$$\Leftrightarrow \left(\begin{array}{c|c} A & t \\ \hline 0 & 1 \end{array} \right) \left(\begin{array}{c|c} S\mathrm{I}_n & 0 \\ \hline 0 & 1 \end{array} \right) \left(\begin{array}{c|c} A^{-1} & -A^{-1}t \\ \hline 0 & 1 \end{array} \right) = \left(\begin{array}{c} S' \end{array} \right)$$
$$\Leftrightarrow \left(\begin{array}{c|c} S\mathrm{I}_n & t - St \\ \hline 0 & 1 \end{array} \right) = \left(\begin{array}{c|c} S'\mathrm{I}_n & 0 \\ \hline 0 & 1 \end{array} \right)$$
$$\Leftrightarrow S = S' \wedge t = St$$
$$\Leftrightarrow S = S' \wedge t = 0$$

□

Satz 9.1.25: SATZ VON PAPPOS

Seien $\mathrm{Dim}\,\mathscr{A} = 2$ und D, D' zwei Geraden in $\mathscr{A}$ (d.h. 1-dimensionale TRe) mit 6 verschiedenen Punkten $P, Q, R \in D$, $P', Q', R' \in D'$, von denen keiner in $D \cap D'$ ist.



Gilt • $\langle P, Q' \rangle_a \parallel \langle Q, P' \rangle_a$ und • $\langle Q, R' \rangle_a \parallel \langle R, Q' \rangle_a$, dann gilt • $\langle P, R' \rangle_a \parallel \langle R, P' \rangle_a$.

Beweis zu 9.1.25:

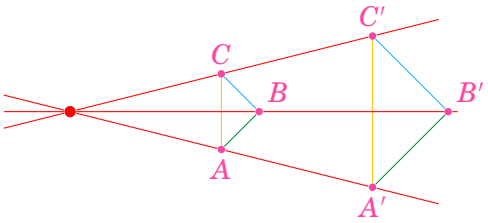
Wir betrachten zunächst den Fall, dass D und D' sich schneiden. Dann sei $\{P_0\} = D \cap D'$ und f_1 die Streckung mit Zentrum P_0, die P in $Q = P_0 + a\overrightarrow{P_0P}$ überführt, und f_2 die Streckung mit Zentrum P_0, Streckfaktor a', die Q nach R überführt.
Es gilt: $Q' = \tau_V(P)$, also $f_1(Q') = f_1(\tau_V(P)) = \tau_{aV}(f_1(P)) = \tau_{aV}(Q) \overset{!}{=} P'$ und analog $f_2(R') = Q'$.
Dann ist $(f_2 \circ f_1)(P) = R$ und $(f_1 \circ f_2)(R') = P'$.
Da der lineare Anteil von $f_2 \circ f_1$ gleich dem von $f_1 \circ f_2$ ist, gleich $b\mathrm{id}_V = aa'\mathrm{id}_V$, $b \in K^*$, gilt $b\overrightarrow{PR'} = \overrightarrow{RP'}$ und somit $\langle P, R' \rangle_a \parallel \langle R, P' \rangle_a$.
Falls D und D' sich nicht schneiden, arbeitet man mit Translationen, denn dann sind D und D' parallel. □

Satz 9.1.26: Satz von Desargues

Seien (A,B,C) und $(A',B',C') \in \mathscr{A}^3_{\text{generisch}}$ zwei nicht-entartete Dreiecke, die keine Eckpunkte gemeinsam haben, und

- $\langle A,B \rangle_a \parallel \langle A',B' \rangle_a$
- $\langle B,C \rangle_a \parallel \langle B',C' \rangle_a$
- $\langle A,C \rangle_a \parallel \langle A',C' \rangle_a$

Dann schneiden sich die drei Geraden $\langle A,A' \rangle_a$, $\langle A,A' \rangle_a$, $\langle A,A' \rangle_a$ in einem gemeinsamen Punkt, oder sie sind parallel.



Beweis zu 9.1.26:
Da die beiden Dreiecke nicht entartet sind, erzeugen sie einen drei- oder zweidimensionalen affinen Raum.
Wir betrachten also zunächst nur den ersten Fall.
Also sei (A,B,C,A') nicht komplanar. Dann können wir affine Koordinaten

$$\kappa : \langle A,B,C,A' \rangle_a \longrightarrow K^{3\times 1}$$

so wählen, dass $\kappa(A) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \kappa(B) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \kappa(C) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \kappa(A') = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.
Wegen der Parallelität der Seiten folgt durch kurze Rechnung

$$\kappa(B') = \begin{pmatrix} a \\ 0 \\ 1 \end{pmatrix}, \kappa(C') = \begin{pmatrix} 0 \\ a \\ 1 \end{pmatrix}$$

für ein $a \in K$.
Da (A',B',C') nicht kollinear ist, folgt $a \neq 0$. Im Falle $a = 1$ sind die drei Geraden parallel. Andernfalls schneiden sie sich im Punkt mit den Koordinaten $\begin{pmatrix} 0 \\ 0 \\ \frac{1}{1-a} \end{pmatrix}$. □

10 Multilineare Algebra

10.1 Tensorprodukte von Moduln

„Tensor“ ist hier das Zauberwort. Ursprünglich aus Ingenieurswissenschaften, quadratische Matrizen, die lange vor den tatsächlichen Matrizen existierten, wurden sie für die Mathematik besonders relevant durch Einsteins Allgemeine Relativitätstheorie.
Sei R ein kommutativer Ring und K ein Körper.

Definition 10.1.1: Tensorprodukt

Seien M, N, T Moduln über R.

(1) Eine Abbildung

$$\Phi : M \times N \longrightarrow T$$

heißt **biliear**, falls $\forall a, b \in R,\ V, V' \in M,\ W, W' \in N$ gilt:

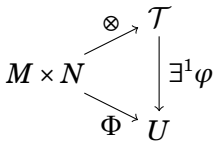
- $\Phi(aV + bV', W) = a\Phi(V, W) + b\Phi(V', W)$
- $\Phi(V, aW + bW') = a\Phi(V, W) + b\Phi(V, W')$

(2) $(\otimes, \mathcal{T})$ heißt **Tensorprodukt** (TP) von M und N, falls gilt:

(a)
$$\begin{aligned} \otimes : M \times\ N &\longrightarrow \mathcal{T}, \\ (V,\ W) &\longmapsto V \otimes W \end{aligned}$$

ist bilinear.

(b) Für jeden R-Modul U und jede bilieare Abbildung $\Phi : M \times N \to U$ existiert *genau eine* lineare Abbildung $\varphi : \mathcal{T} \to U$, sodass das Diagramm



kommutiert, d.h. $\Phi(V, W) = \varphi(V \otimes W)$.
Man sagt, das Tensorprodukt ist eine **universelle bilineare Abbildung**.

Übung 13.3: Tensorprodukte

(1) Seien $a, b \in \mathbb{N},\ g := \mathrm{ggT}(n, m)$. Dann ist

$$\begin{aligned} \otimes :\ \mathbb{Z}/n\mathbb{Z} \times\ \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/g\mathbb{Z}, \\ (a + n\mathbb{Z},\ b + m\mathbb{Z}) &\longmapsto ab + g\mathbb{Z} \end{aligned}$$

ein Tensorprodukt.

(2) Fasse $\mathbb{Q}$ als $\mathbb{Z}$-Modul auf. Dann ist

$$\begin{aligned} \otimes : \mathbb{Q} \times \mathbb{Q} &\longrightarrow \mathbb{Q}, \\ (r,\ s) &\longmapsto rs \end{aligned}$$

ein Tensorprodukt.

Beweis:

(1) $\otimes$ ist offensichtlich bilinear auf $\mathbb{Z}$.

Wohldefiniertheit:

Seien $\overline{a} = \overline{\alpha} \in \mathbb{Z}/n\mathbb{Z}$ und $\overline{b} = \overline{\beta} \in \mathbb{Z}/m\mathbb{Z}$.

$\Rightarrow a = \alpha + kn$ und $b = \beta + lm$ für $k, l \in \mathbb{Z}$.

$$\begin{aligned} \Rightarrow \overline{a} \otimes \overline{b} &= \left(\overline{a} + \overline{kn}\right) \otimes \left(\overline{\beta} + \overline{lm}\right) \\ &= \overline{a} \otimes \overline{\beta} + \overline{a} \otimes \overline{lm} + \overline{kn} \otimes \overline{\beta} + \overline{kn} \otimes \overline{lm} \\ &= \left(\alpha\beta + g\mathbb{Z}\right) + (\alpha lm + g\mathbb{Z}) + \left(kn\beta + g\mathbb{Z}\right) + (knlm + g\mathbb{Z}) \\ &= \alpha\beta + g\mathbb{Z} + \overline{0} + \overline{0} + \overline{0} \\ &= \alpha\beta + g\mathbb{Z} = \overline{\alpha} \otimes \overline{\beta} \end{aligned}$$

Universelle Eigenschaft:

Sei $\Phi : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathcal{U}$ bilinear, wobei $\mathcal{U}$ ein $\mathbb{Z}$-Modul ist.

Setze $\varphi : \mathbb{Z}/g\mathbb{Z} \to \mathcal{U}$, $\overline{a} \mapsto \Phi\left(\overline{1}, \overline{a}\right)$. φ ist offensichtlich linear, und es gilt:

$$\begin{aligned}\varphi\left(\overline{a} \otimes \overline{b}\right) = \varphi(ab + g\mathbb{Z}) &= \Phi\left(\overline{1}, \overline{ab}\right) \\ &= a\Phi\left(\overline{1}, \overline{b}\right) \\ &= \Phi\left(\overline{a}, \overline{b}\right)\end{aligned}$$

EINDEUTIGKEIT:

Sei $\varphi' : \mathbb{Z}/g\mathbb{Z} \to \mathcal{U}$ eine weitere lineare Abbildung mit $\varphi' \circ \otimes = \Phi$. Dann gilt:

$$\varphi'(\overline{a}) = \varphi'\left(\overline{1} \otimes \overline{a}\right) = \Phi\left(\overline{1}, \overline{a}\right) = \varphi(\overline{a})$$

$\Rightarrow \varphi = \varphi'$

(2) Wieder ist $\otimes$ ganz klar bilinear.

Sei $\Phi : \mathbb{Q} \times \mathbb{Q} \to \mathcal{U}$ bilinear mit $\mathcal{U}$ als beliebigem $\mathbb{Z}$-Modul.

Definiere $\varphi : \mathbb{Q} \to \mathcal{U}$, $a \mapsto \Phi(1, a)$. φ ist klar linear, und analog dem ersten Beispiel ist $\varphi \circ \otimes = \Phi$, sowie eindeutig.

□

Bemerkung 10.1.2: KRONECKER-PRODUKT

Sei $A \in R^{m \times n}$ und $B \in R^{o \times p}$. Das **Kronecker-Produkt** von den Matrizen A und B ist definiert durch

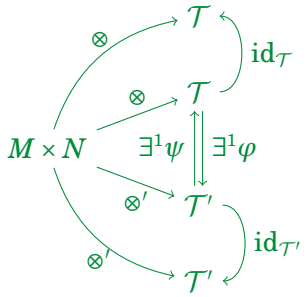
$$A \otimes B := \begin{pmatrix} A_{1,1}B & \cdots & A_{1,n}B \\ \vdots & \ddots & \vdots \\ A_{m,1}B & \cdots & A_{m,n}B \end{pmatrix}$$

Dann ist $\otimes : R^{m \times n} \times R^{o \times p} \to R^{mo \times np}$ sicher bilinear. Ist dieses Produkt universell, also ein Tensorprodukt?

Bemerkung 10.1.3:

Falls ein Tensorprodukt von M und N existiert, dann ist es bis auf eindeutige Isomorphie eindeutig.

Beweis zu 10.1.3:



$\psi \circ \varphi : \mathcal{T} \to \mathcal{T} \Rightarrow \psi \circ \varphi = \mathrm{id}_{\mathcal{T}}$

$\varphi \circ \psi : \mathcal{T}' \to \mathcal{T}' \Rightarrow \varphi \circ \psi = \mathrm{id}_{\mathcal{T}'}$

„abstract nonsense" – Kategorientheorie

□

In Worten: Seien $(\otimes, \mathcal{T})$ und $(\otimes', \mathcal{T}')$ Tensorprodukte der R-Moduln M und N. Dann haben wir eine lineare Abbildung $\varphi : \mathcal{T} \to \mathcal{T}'$ mit $V \otimes W$ für alle $V \in M$, $W \in N$ und eine lineare Abbildung $\psi : \mathcal{T}' \to \mathcal{T}$ mit $V \otimes W = \psi(V \otimes' W)$. Also hat die Komposition $\varphi \circ \psi : \mathcal{T}' \to \mathcal{T}'$ die Eigenschaft $V \otimes' W = \left(\varphi \circ \psi\right)(V \otimes' W)$ für alle $V \in M$, $W \in N$ ebenso wie die Identität $\mathrm{id}_{\mathcal{T}'}$ von $\mathcal{T}'$. Also ist $\varphi \circ \psi = \mathrm{id}_{\mathcal{T}'}$. Analog $\psi \circ \varphi = \mathrm{id}_{\mathcal{T}}$. D.h. φ und ψ sind invers zueinander – also Isomorphismen. □

Bemerkung 10.1.4:

Ist $M = \langle m_1, \ldots, m_s \rangle$ und $N = \langle n_1, \ldots, n_s \rangle$, so ist jede bilineare Abbildung

$$\Phi : M \times B \longrightarrow U$$

eindeutig bestimmt durch alle $\Phi(m_i, n_i)$.

Bemerkung 10.1.5:

Das Kronecker-Produkt ist ein Tensorprodukt.
Genauer: $(\otimes, K^{mo \times np})$ ist ein Tensorprodukt von $K^{m \times n}$ und $K^{o \times p}$.

Beweis zu 10.1.5:
Eine bilineare Abbildung Φ ist festgelegt durch die Bilder von (B, C), wobei B und C die Basisvektoren von je einer Basis der beiden Ausgangsvektorräume durchlaufen.

z.B. $K^{2\times 2} = \left\langle \begin{pmatrix} 1 & \cdot \\ \cdot & \cdot \end{pmatrix}, \begin{pmatrix} \cdot & 1 \\ \cdot & \cdot \end{pmatrix}, \begin{pmatrix} \cdot & \cdot \\ 1 & \cdot \end{pmatrix}, \begin{pmatrix} \cdot & \cdot \\ \cdot & 1 \end{pmatrix} \right\rangle$
$\Phi\left(\sum b_i B_i, \sum c_j C_j\right) = \sum b_i c_j \Phi\left(B_i, C_j\right)$

Im vorliegenden Fall kann man die Standardbasis nehmen. Aber dann bilden die Kronecker-Produkte $B \otimes C$ eine Basis von $K^{mo \times np}$, nämlich auch wieder die Standardbasis bei geeigneter Anordnung.
Also ist doch

$$\varphi : B \otimes C \longrightarrow \Phi(B, C)$$

eine lineare Abbildung festgelegt, die unser Diagramm zum Kommutieren bringt. Es ist klar, dass wir keine andere Wahl für φ haben.
Für Moduln über R mit freien EZS statt Basis geht der Beweis analog. □

Damit ist die Existenz und Eindeutigkeit für Tensorprodukte von endlich-dimensionalen VRen bewiesen (sogar für freie Moduln von endlichem Rang).

Bemerkung 10.1.6:

Sind $\mathcal{V}, \mathcal{W}$ zwei K-VRe der Dimension n und m, so heißt das Tensorprodukt $\mathcal{V} \otimes \mathcal{W}$ die Dimension nm.
Genauer: Ist $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$ und $C \in \mathcal{W}^m$ eine Basis von $\mathcal{W}$, so ist

$$B \otimes C := (B_1 \otimes C_1, B_1 \otimes C_2, \ldots, B_1 \otimes C_m, B_2 \otimes C_1, \ldots, B_n \otimes C_m) \in (\mathcal{V} \otimes \mathcal{W})^{nm}$$

eine Basis von $\mathcal{V} \otimes \mathcal{W}$.

Bemerkung 10.1.7:

Seien M, N zwei R-Moduln. Dann existiert bis auf Isomorphie genau ein Tensorprodukt.
Dieses wird mit $(\otimes, M \otimes N)$ bezeichnet.

Beweis zu 10.1.7:
Eindeutigkeit wissen wir bereits aus 10.1.3.

Zur Existenz: Sei F der freie R-Modul mit Basis $M \times N$, d.h.

$$F = \left\{ \sum_{(m,n) \in M \times N} a_{(m,n)}(m,n) \;\middle|\; a_{(m,n)} \in R,\ a_{(m,n)} \neq 0 \text{ nur für endlich viele Paare } (m,n) \right\}$$

Setze $F \geq B = \langle (rm_1 + m_2,\ sn_1 + n_2) - rs(m_1, n_1) - r(m_1, n_2) - s(m_2, n_1) - (m_2, n_2) \rangle$.

Behauptung: Ist $F/B =: \mathcal{T}$, so ist

$$\otimes : M \times N \longrightarrow \mathcal{T},$$
$$(m,n) \longmapsto (m,n) + B =: \nu((m,n)) \text{ (natürlicher Epimorphismus } F \to T)$$

ein Tensorprodukt.

- $\otimes$ ist bilinear nach Konstruktion, sprich nach Definition von B.
- $\otimes$ hat die universelle Eigenschaft:
  Ist U ein R-Modul und $\psi : M \times N \to U$ bilinear, so gibt es genau einen R-Modulhomomorphismus

  $$\varphi : F \longrightarrow U \text{ mit } \varphi|_{M \times N} = \psi$$

  da F frei auf $M \times N$ ist.

  Aus der Bilinearität von ψ folgt, dass $B \leq \operatorname{Kern} \varphi$. Somit induziert φ eine lineare Abbildung $\mathcal{T} \to U$ mit der gewünschten Eigenschaft $(\overline{\varphi})$.

□

Beispiel 10.1.8:

(1) $R = \mathbb{Z}$ (HIB), $M = \mathbb{Z}/2\mathbb{Z} = \langle a \rangle$, $N = \mathbb{Z}/3\mathbb{Z} = \langle b \rangle$.
Hier ist $M \otimes N = \{0\}$. Denn jede bilineare Abbildung $\Phi : M \times N \to U$, insbesondere das Tensorprodukt, muss folgendes erfüllen:

$$\begin{aligned}\Phi(a,b) &= 3\Phi(a,b) - 2\Phi(a,b) \\ &= \Phi(a,3b) - \Phi(2a,b) \\ &= 0 - 0 = 0\end{aligned}$$

(2) $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z} = \langle a \rangle$, $N = \mathbb{Z}/4\mathbb{Z} = \langle c \rangle$.
Dann ist $M \otimes N \cong M = \mathbb{Z}/2\mathbb{Z}$, denn jede bilineare Abbildung (insbesondere das TP)

$$\Phi : M \times N \longrightarrow U$$

ist eindeutig bestimmt durch

$$\Phi(a,c) =: u$$

Es ist $2u = \Phi(2a,c) = 0$.
Umgekehrt definiert

$$\Phi : M \times N \longrightarrow \mathbb{Z}/2\mathbb{Z},$$
$$(a,\ c) \longmapsto 1 + 2\mathbb{Z}$$

eine bilineare Abbildung.

Wir haben noch eine unmittelbare Konsequenz der Definition: Die Existenz von Tensorprodukten von linearen Abbildungen.

Satz 10.1.9:

Seien $\mathcal{V},\mathcal{V}',\mathcal{W},\mathcal{W}'$ vier K-VRe mit linearen Abbildungen $\alpha:\mathcal{V}\to\mathcal{V}'$, $\beta:\mathcal{W}\to\mathcal{W}'$. Dann gilt:

(1) Es gibt genau eine lineare Abbildung

$$\alpha \underset{\text{Hom}}{\otimes} \beta: \mathcal{V} \underset{1}{\otimes} \mathcal{W} \longrightarrow \mathcal{V}' \underset{2}{\otimes} \mathcal{W}'$$

mit $\left(\alpha \underset{\text{Hom}}{\otimes} \beta\right)(V \underset{1}{\otimes} W) = \alpha(V) \underset{2}{\otimes} \beta(W)$ für alle $V,V' \in \mathcal{V}$, $W,W' \in \mathcal{W}$.

(2) Sind B,B',C,C' Basen von $\mathcal{V},\mathcal{V}',\mathcal{W},\mathcal{W}'$ respektive in der Reihenfolge, so gilt:

(3)
$$^{B'\otimes C'}\left(\alpha \underset{\text{Hom}}{\otimes} \beta\right)^{B\otimes C} = \underbrace{{}^{B'}\alpha^{B} \otimes {}^{C'}\beta^{C}}_{\text{Kronecker-Produkt}}$$

$$\otimes : \operatorname{Hom}(\mathcal{V},\mathcal{V}') \times \operatorname{Hom}(\mathcal{W},\mathcal{W}') \longrightarrow \operatorname{Hom}(\mathcal{V}\otimes\mathcal{V}',\ \mathcal{W}\otimes\mathcal{W}'),$$
$$(\alpha,\beta) \longmapsto \alpha\otimes\beta$$

ist ein Tensorprodukt, insbesondere ist $\operatorname{Hom}(\mathcal{V},\mathcal{V}')\otimes\operatorname{Hom}(\mathcal{W},\mathcal{W}') \cong \operatorname{Hom}(\mathcal{V}\otimes\mathcal{V}',\ \mathcal{W}\otimes\mathcal{W}')$.
$\alpha\otimes\beta \mapsto \alpha \underset{\text{Hom}}{\otimes} \beta$ ist ein Isomorphismus, falls die betroffenen VRe endlich-dimensional sind.

Beweis zu 10.1.9:

(1) Offenbar ist

$$\mathcal{V}\times\mathcal{W} \longrightarrow \mathcal{V}'\otimes\mathcal{W}',$$
$$(V,W) \longmapsto \alpha(V)\otimes\beta(W)$$

bilinear. Mit der Definition des TP folgt die Behauptung.

(2) Sei ${}^{B'}\alpha^{B} =: M$, ${}^{C'}\beta^{C} =: N$. Dann ist

$$\begin{aligned}(\alpha\otimes\beta)(B_i\otimes C_j) &= \alpha(B_i)\otimes\beta(C_j)\\ &= \left(\sum_k M_{k,i}B'_k\right)\otimes\left(\sum_l N_{l,j}C'_l\right)\\ &= \underbrace{\sum_k\sum_l M_{k,i}N_{l,j}B'_kC'_l}_{\text{Kronecker-Produkt}}\end{aligned}$$

(3) Die Existienz ist (1). Die Isomorphie ist (2).

□

Offenbar kann man $K\otimes\mathcal{W}$ mit $\mathcal{W}$ identifizieren, indem $k\otimes W$ mit kW für $k\in K$ und $W\in\mathcal{W}$ identifiziert wird. Dies funktioniert genauso für R-Moduln:

$$R\otimes M \xrightarrow{\sim} M,$$
$$r\otimes m \longmapsto rm$$

$$\Psi:\operatorname{Hom}(R,M)\xrightarrow{\sim} M,$$
$$\varphi \longmapsto \varphi(1)$$

$$\Psi(r\varphi) = (r\varphi+\varphi')(1) = r\varphi(1)+\varphi'(1) = r\Psi(\varphi)+\Psi(\varphi')$$
$$0 = \Psi(\varphi) = \varphi(1) \Rightarrow \varphi(r) = r\varphi(1) = 0$$

$$\varphi_m : R \longrightarrow M,$$
$$1 \longmapsto m,$$
$$r \longmapsto rm$$

Dann bekommen wir eine wichtige Folgerung, wobei mit $\mathcal{V}^*$ wie üblich der Dualraum $\operatorname{Hom}(\mathcal{V},K)$ bezeichnet wird:

Korollar 10.1.10:

$\mathcal{V}^* \otimes \mathcal{W} \cong \mathrm{Hom}(\mathcal{V}, \mathcal{W})$, genauer:

$$\otimes : \mathcal{V}^* \times \mathcal{W} \longrightarrow \mathrm{Hom}(\mathcal{V}, \mathcal{W}),$$
$$(\varphi,\ W) \longmapsto (V \mapsto \varphi(V)W)$$

ist ein Tensorprodukt.

Beweis zu 10.1.10:

$\mathcal{V}^* \otimes \mathcal{W} \cong \mathrm{Hom}(\mathcal{V}, K) \otimes \mathrm{Hom}(K, \mathcal{W}) \cong \mathrm{Hom}(\mathcal{V} \otimes K,\ K \otimes \mathcal{W}) \cong \mathrm{Hom}(\mathcal{V}, \mathcal{W})$ (natürlicher Isomorphismus; nicht basisabhängig!) □

Bemerkung 10.1.11: KONSTANTENERWEITERUNG

Sei K ein Teilkörper eines Körpers F und $\mathcal{V}$ ein K-VR. Dann ist $\mathcal{V}_F := F \otimes \mathcal{V}$ ein F-VR, die sogenannte **Konstantenerweiterung** mit

$$a(b \otimes V) := (ab) \otimes V \ \forall a, b \in F,\ V \in \mathcal{V}$$

Zusätzlich gilt:

(1) Ist $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$, so ist

$$1 \otimes B := (1 \otimes B_1, \ldots, 1 \otimes B_n) \in \mathcal{V}_F^n$$

eine F-Basis von $\mathcal{V}_F$.

(2) Ist $\mathcal{W}$ ein weiterer K-VR und $\varphi : \mathcal{V} \to \mathcal{W}$ linear über K, so ist $\mathrm{id}_F \otimes \varphi : \mathcal{V}_F \to \mathcal{W}_F$ linear über F. Ist $C \in \mathcal{W}^m$ eine K-Basis von $\mathcal{W}$, so ist

$${}^{1\otimes C}\left(\mathrm{id}_F \otimes \varphi\right)^{1\otimes B} = {}^{B}\varphi^{C}$$

(3) Die beiden F-VRe $\mathrm{Hom}(\mathcal{V}, \mathcal{W})_F$ und $\mathrm{Hom}(\mathcal{V}_F, \mathcal{W}_F)$ werden identifiziert, indem man $a \otimes \varphi$ für $a \in F$ und $\varphi \in \mathrm{Hom}(\mathcal{V}, \mathcal{W})$ mit $\widetilde{a} \otimes \varphi$ identifiziert, wobei $\widetilde{a}$ die Skalierung

$$\widetilde{a} : F \to F,\ b \mapsto ab$$

bezeichnet.

Beweis zu 10.1.11:

(0) z.z. $\mathcal{V}_F =: F \otimes \mathcal{V}$ ist F-VR. Seien $a, b, \alpha, \beta \in F,\ V, W \in \mathcal{V}$.

- $(F \otimes \mathcal{V}, +)$ Abelsche Gruppe, da K-Modul.
- $(\alpha + \beta)(a \otimes V) = (\alpha + \beta)a \otimes V = (\alpha a + \beta a) \otimes V = \alpha(a \otimes V) + \beta(a \otimes V)$
- $\alpha(a \otimes V + b \otimes W) = (\alpha a) \otimes V + (\alpha b) \otimes W = \alpha(a \otimes V) + \alpha(b \otimes W)$
- $(\alpha\beta)(a \otimes V) = (\alpha\beta a) \otimes V = \alpha((\beta a) \otimes V) = \alpha(\beta(a \otimes V))$
- $1(a \otimes V) = (1a \otimes V) = a \otimes V$

$\Rightarrow F$-VR. □

(1) Sei $B \in \mathcal{V}^n$ eine K-Basis von $\mathcal{V}$ und $\mathrm{Dim}_K \mathcal{V} = n$.
Es ist $\mathcal{V}_F := F \otimes \mathcal{V} \cong F \otimes K^{n\times 1} \cong (F \otimes K)^n \cong \mathbb{F}^{n\times 1}$, damit ist $\mathrm{Dim}_F \mathcal{V}_F = n$.
Sei $1 \otimes B := (1 \otimes B, \ldots, 1 \otimes B_n)$. Hat n linear unabhängige Elemente, erzeugt es $\mathcal{V}_F$?
Sei $a \otimes \mathcal{V} \in \mathcal{V}_F$.

$$\Rightarrow a \otimes \mathcal{V} = a \otimes \left(\sum_i \lambda_i B_i\right) = \sum_i a\lambda_i (1 \otimes B_i)$$

$\Rightarrow 1 \otimes B$ ist EZS

$\Rightarrow$ Basis.

(2)
- LINEAR: $\mathrm{id}_F \otimes \varphi : \mathcal{V}_F \to \mathcal{W}_F,\ a \otimes V \mapsto a \otimes \varphi(V)$. Es gilt:

$$\begin{aligned}(\mathrm{id}_F \otimes \varphi)\left(\alpha(a \otimes V) + \beta(b \otimes V')\right) &= \left(\alpha a \otimes \varphi(V)\right) + \left(\beta b \otimes \varphi(V')\right) \\ &= \alpha\left((\mathrm{id}_F \otimes \varphi)(V)\right) + \beta\left((\mathrm{id}_F \otimes \varphi)(V')\right)\end{aligned}$$

- DARSTELLUNGSMATRIX: Seien $B_i \in B,\ C_i \in C$ Basen von $\mathcal{V}, \mathcal{W}$.

$$\varphi(B_j) = \lambda_{1,j} C_1 + \cdots + \lambda_{n,j} C_n,\ \lambda_{i,j} \in K$$

$$\begin{aligned}(\mathrm{id}_F \otimes \varphi)(1 \otimes B_j) &= \mathrm{id}_F(1) \otimes \varphi(B_j) \\ &= 1 \otimes \left(\sum_i \lambda_{i,j} C_i\right) \\ &= \sum_i \lambda_{i,j} \underbrace{(1 \otimes C_i)}_{\text{Basisvektor von } \mathcal{W}}\end{aligned}$$

$$\Rightarrow 1 \otimes C\,(\mathrm{id}_F \otimes \varphi)^{1 \otimes B} = (\lambda_{i,j})_{i,j} = {}^C\varphi^B$$

(3) Zunächst z.z.:

$$\begin{aligned}\Phi : F \times \mathrm{Hom}(\mathcal{V}, \mathcal{W}) &\longrightarrow \mathrm{Hom}(\mathcal{V}_F, \mathcal{W}_F), \\ (a, \quad \varphi) &\longmapsto \widetilde{a} \otimes \varphi\end{aligned}$$

ist ein Tensorprodukt.
Sei $\mathrm{Dim}\,\mathcal{V} =: n,\ \mathrm{Dim}\,\mathcal{W} =: m$.

- Für $\lambda \in K,\ a, b \in F,\ \varphi, \psi \in \mathrm{Hom}(\mathcal{V}, \mathcal{W})$ gilt:

$$\begin{aligned}\Phi(\lambda a + b, \varphi) &= \widetilde{\lambda a + b} \otimes \varphi = \left(\lambda \widetilde{a} + \widetilde{b}\right) \otimes \varphi = \lambda \widetilde{a} \otimes \varphi + \lambda \widetilde{b} \otimes \varphi \\ &= \lambda \Phi(a, \varphi) + \lambda \Phi(b, \varphi)\end{aligned}$$

-

$$(a, \lambda\varphi + \psi) = \widetilde{a} \otimes \lambda\varphi + \psi = \lambda\left(\widetilde{a} \otimes \varphi\right) + \lambda\left(\widetilde{a} \otimes \psi\right) = \lambda\Phi(a, \varphi) + \lambda\Phi(a, \psi)$$

$\Rightarrow \Phi$ bilinear.

- UNIVERSELLE EIGENSCHAFT: Basis von $\mathrm{Hom}(\mathcal{V}_F, \mathcal{W}_F)$ ist gegeben durch die Funktionen

$$\begin{aligned}(\pi_F)_{i,j} : \mathcal{V}_F &\longrightarrow \mathcal{W}_F, \\ 1 \otimes B_i &\longmapsto 1 \otimes C_j, \\ 1 \otimes B_k &\longmapsto 0 \text{ falls } k \neq i\end{aligned}$$

mit $i \in \underline{n},\ j \in \underline{m}$, wobei $B_1, \ldots, B_n$ eine Basis von $\mathcal{V}$ ist und $C_1, \ldots, C_m$ eine Basis von $\mathcal{W}$.
Basis von $\mathrm{Hom}(\mathcal{V}, \mathcal{W})$ ist analog gegeben durch die Funktionen

$$\begin{aligned}\pi_{i,j} : \mathcal{V} &\longrightarrow \mathcal{W}, \\ B_i &\longmapsto C_j, \\ B_k &\longmapsto 0 \text{ falls } k \neq i\end{aligned}$$

$\Rightarrow (\pi_F)_{i,j} = \widetilde{1} \otimes \pi_{i,j}$
Konstruiere T auf Basis von $\mathrm{Hom}(\mathcal{V}_F, \mathcal{W}_F)$:
Sei $\varphi_F \in \mathrm{Hom}(\mathcal{V}_F, \mathcal{W}_F)$, d.h.

$$\begin{aligned}\varphi_F : \mathcal{V}_F &\longrightarrow \mathcal{W}_F, \\ 1 \otimes B_i &\longmapsto \sum_{j=1}^{m} a_{i,j} \cdot 1 \otimes C_j\end{aligned}$$

φ_F ist durch die Bilder der Basen $1 \otimes B_i$ definiert.

$$\Rightarrow \varphi_F = \sum_{i,j} a_{i,j} (\pi_F)_{i,j} = \sum_{i,j} \left(\widetilde{a_{i,j}} \otimes \pi_{i,j}\right)$$

Sei

$$T : \mathrm{Hom}(\mathcal{V}_F, \mathcal{W}_F) \longrightarrow M,$$
$$\varphi_F \longmapsto \sum_{i,j} \varphi(a_{i,j}, \pi_{i,j})$$

$$T \circ \Phi(a, \varphi) = T(\widetilde{a} \otimes \varphi) = T\left(\widetilde{a} \otimes \left(\sum_{i,j} a_{i,j} \cdot \pi_{i,j}\right)\right)$$
$$= T\left(\sum_{i,j} (a \cdot a_{i,j}) \otimes \pi_{i,j}\right)$$
$$= \sum_{i,j} \psi(a \cdot a_{i,j}, \pi_{i,j})$$
$$= \sum_{i,j} a_{i,j} \psi(a, \pi_{i,j})$$
$$= \sum_{i,j} \psi(a, a_{i,j} \pi_{i,j})$$
$$= \psi(a, \varphi)$$

T ist linear und eindeutig. Damit ist Φ ein Tensorprodukt.
Daraus folgt die Behauptung.

□

10.2 Die Tensoralgebra

Definition 10.2.1:

Seien $\mathcal{V}_i$ für $i \in \underline{n}$ und $\mathcal{W}, \mathcal{T}$ seien K-VRe.
Eine Abbildung

$$\Psi : \bigtimes_{i=1}^{n} \mathcal{V}_i \longrightarrow \mathcal{W}$$

heißt **multilinear**, falls sie in jeder Komponente linear ist. $(\otimes, \mathcal{T})$ heißt **(mehrfaches) Tensorprodukt** der $\mathcal{V}_i$s, falls $\mathcal{T}$ ein K-VR ist,

$$\otimes : \bigtimes_{i=1}^{n} \mathcal{V}_i \longrightarrow \mathcal{T},$$
$$(V_1, \ldots, V_n) \longmapsto V_1 \otimes \cdots \otimes V_n$$

multilinear ist, und für jede multilineare Abbildung $\Psi : \bigtimes_{i=1}^{n} \mathcal{V}_i \to \mathcal{W}$ in einem beliebigen K-VR $\mathcal{W}$ genau eine lineare Abbildung $\varphi : \mathcal{T} \to \mathcal{W}$ mit $\Psi(V_1, \ldots, V_n) = \varphi(V_1 \otimes \cdots \otimes V_n)$ $\forall V_i \in \mathcal{V}_i$, $i \in \underline{n}$.

Satz 10.2.2:

Bis auf Isomorphie gibt es genau ein TP $(\otimes, \mathcal{T})$ von $(\mathcal{V}_1, \ldots, \mathcal{V}_n)$. Dieses wird mit $\mathcal{V}_1 \otimes \cdots \otimes \mathcal{V}_n$ bezeichnet.

Beweis zu 10.2.2:
Der Beweis für den Fall $n = 2$ in 10.1.5 bzw. 10.1.7 überträgt sich, wenn man die offensichtliche Identität von Kronecker-Produkten von Matrizen beachtet: Für beliebige Matrizen gilt:

$$(A \otimes B) \otimes C = A \otimes (B \otimes C)$$

□

Korollar 10.2.3:

$$\begin{array}{ccccc} (\mathcal{V}_1 \otimes \mathcal{V}_2) \otimes \mathcal{V}_3 & \cong & \mathcal{V}_1 \otimes \mathcal{V}_2 \otimes \mathcal{V}_3 & \cong & \mathcal{V}_1 \otimes (\mathcal{V}_2 \otimes \mathcal{V}_3) \\ 2\times\ (n=2) & & 1\times\ (n=3) & & 2\times\ (n=2) \\ (V_1 \otimes V_2) \otimes V_3 & \rightleftarrows & V_1 \otimes V_2 \otimes V_3 & \rightleftarrows & V_1 \otimes (\otimes V_2 \otimes V_3) \end{array}$$

ist multilinear für alle $V_i \in \mathcal{V}_i\ \forall i \in \underline{3}$.

Definition 10.2.4: Tensoralgebra

Sei $\mathcal{V}$ ein K-VR. Setze $\mathcal{V}^{\otimes 0} := \mathrm{T}^0\mathcal{V} := K \cdot 1$ ein eindimensionaler K-VR mit Basis (1) und $\mathcal{V}^{\otimes n} := \mathrm{T}^n\mathcal{V} := \otimes^n \mathcal{V}$ für $n > 0$. Die **Tensoralgebra** $\mathrm{T}\mathcal{V}$ ist definiert durch

$$\mathrm{T}\mathcal{V} := \bigoplus_{i \in \mathbb{Z}_{\geq 0}} \mathrm{T}^i\mathcal{V}$$

mit der bilinearen Multiplikation

$$\underbrace{(V_1 \otimes \cdots \otimes V_n)}_{\in \mathrm{T}^n\mathcal{V}} \otimes \underbrace{(W_1 \otimes \cdots \otimes W_m)}_{\in \mathrm{T}^m\mathcal{V}} := \underbrace{V_1 \otimes \cdots \otimes V_n \otimes W_1 \otimes \cdots \otimes W_m}_{\in \mathrm{T}^{n+m}\mathcal{V}}$$

für alle $V \in \mathcal{V}^n$, $W \in \mathcal{V}^m$ und $1X = X = X1\ \forall X \in \mathrm{T}\mathcal{V}$.

Für die Tensoralgebra können wir nicht nur zeigen, dass sie eine Algebra ist, sondern dass sie sogar eine universelle Eigenschaft erfüllt, ähnlich wie das TP selbst.

Satz 10.2.5:

(1) $\mathrm{T}\mathcal{V}$ ist eine assoziative K-Algebra mit Eins.

(2) Ist A eine andere assoziative Algebra mit Einselement und $\varphi : \mathcal{V} \to A$ eine lineare Abbildung, so gibt es genau einen Algebrenhomomorphismus $\overline{\varphi} : \mathrm{T}\mathcal{V} \to A$, der φ fortsetzt.

Beweis zu 10.2.5:

(1) Zeige, dass die Multiplikation wohldefiniert ist. Klar:

$$\begin{aligned} \mathrm{T}^n\mathcal{V} \times \mathrm{T}^m\mathcal{V} &\longrightarrow \mathrm{T}^{n+m}\mathcal{V}, \\ (X, Y) &\longmapsto X \otimes Y \end{aligned}$$

ist bilinear, sogar ein Tensorprodukt. Also ist die Multiplikation auf $\mathrm{T}^n\mathcal{V} \times \mathrm{T}^m\mathcal{V}$ wohldefiniert und bilinear. Dies wird bilinear auf ganz $\mathrm{T}\mathcal{V}$ fortgesetzt, was wegen der Struktur von $\mathrm{T}\mathcal{V}$ als direkte Summe wohldefiniert ist. Offenbar ist dieses Produkt assoziativ, sodass wir eine K-Algebra mit Eins erhalten.

$$\underbrace{V'' \otimes W'' + V' \otimes W' + \underbrace{V \otimes W}_{\substack{\text{Tensoren nicht immer von der Form} \\ \text{(zerlegbare Tensoren)}}}}_{\text{manchmal auch von dieser}} \in \mathcal{V} \otimes \mathcal{W}$$

(2) Klar: Soll $\overline{\varphi}$ ein Homomorphismus für Algebren mit Eins sein, so muss $\overline{\varphi}(1) = 1 \in A$ und

$$\overline{\varphi}(V_1 \otimes \cdots \otimes V_m) = \varphi(V_1) \cdots \varphi(V_m)\ \forall V \in \mathcal{V}^n$$

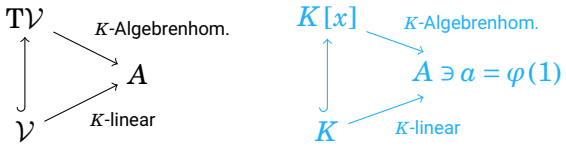
sein. Offenbar ist aber

$$\begin{aligned} \mathcal{V}^n &\longrightarrow A, \\ V &\longmapsto \varphi(V_1) \cdots \varphi(V_n) \end{aligned}$$

multilinear, sodass $\overline{\varphi}|_{\mathrm{T}^n\mathcal{V}}$ wohldefiniert ist.

Da $\mathrm{T}\mathcal{V}$ direkte Summe der $\mathrm{T}^n\mathcal{V}$ ist, folgt die Behauptung.

□



$\Rightarrow K[x] \cong \mathrm{T}K$

Aber $K[x_1,\ldots,x_n] \ncong \mathrm{T}K^n$ falls $n > 1$, da $v \otimes w \neq w \otimes v$ (Symmetrie nicht gefordert).

10.3 Alternierende Tensoren und die Grassmann-Algebra

Definition 10.3.1: Alternierendes Produkt

Seien $\mathcal{V}, \mathcal{W}$ zwei K-VRe.

(1) Eine multilineare Abbildung

$$\Psi : \mathcal{V}^k \longrightarrow \mathcal{W}$$

heißt alternierend, falls $\Psi(V) = 0 \ \forall V \in \mathcal{V}^k$, für die $i, j \in \underline{k},\ i \neq j$ existieren mit $V_i = V_j$.

(2) $(\wedge, \mathcal{T})$ heißt **äußeres k-faches Produkt** von $\mathcal{V}$ oder **alternierendes k-faches Tensorprodukt**, falls $\mathcal{T}$ ein K-VR ist,

$$\begin{aligned} \wedge : \mathcal{V}^k &\longrightarrow \mathcal{T}, \\ V &\longmapsto V_1 \wedge \cdots \wedge V_k \end{aligned}$$

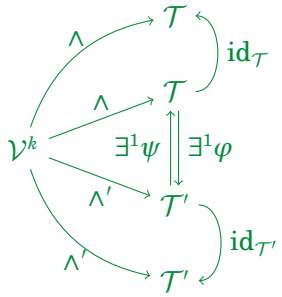
eine alternierende multilineare Abbildung ist und für jeden weiteren K-VR $\mathcal{W}$ und jede weitere alternierende multilineare Abbildung $\Psi : \mathcal{V}^k \to \mathcal{W}$ genau eine lineare Abbildung $\psi : \mathcal{T} \to \mathcal{W}$ existiert mit

$$\Psi(V) = \psi(V_1 \wedge \cdots \wedge V_k) \ \forall V \in \mathcal{V}^k$$

Übung 10.3.Ü1:

Falls ein alternierendes Tensorprodukt existiert, so ist es eindeutig bis auf eindeutige Isomorphie.

Beweis:



□

Satz 10.3.2:

Sei $\mathcal{V}$ ein e.e. K-VR. Es existiert bis auf eindeutige Isomorphie genau ein äußeres k-faches Produkt $(\wedge, \mathcal{T})$. Wir bezeichnen es mit $\bigwedge^k \mathcal{V} := \mathcal{T}$.

Beweis zu 10.3.2:

Falls $\mathcal{T}$ existiert, sollte es nach Def. der Tensorpotenz ein epimorphes Bild von $\mathrm{T}^k\mathcal{V}$ sein. Ist $\varepsilon : \mathrm{T}^k\mathcal{V} \to \mathcal{T}$ dieser Epimorphismus, so gilt sicherlich:

$$V_1 \otimes \cdots \otimes V_k \in \operatorname{Kern} \varepsilon$$

sobald $V_i = V_j$ ist für ein Paar (i,j) mit $i \neq j$.
Dies führt uns zu folgendem Ansatz: Setze

$$\mathcal{T} := \left(\mathrm{T}^k \mathcal{V}\right) \Big/ \mathcal{U}$$

wobei $\mathcal{U}$ von allen $V_1 \otimes \ldots V_k$ mit $V \in \mathcal{V}^k$ für ein Paar (i,j) mit $i \neq j$ erzeugt wird.
Es folgt sofort:

$$\begin{aligned} \wedge : \mathcal{V}^k &\longrightarrow \mathcal{T}, \\ V &\longmapsto V_1 \wedge \cdots \wedge V_k := V_1 \otimes \cdots \otimes V_k + \mathcal{U} \end{aligned}$$

ist multilinear und alternierend.
Wir wissen: $\mathcal{U} \subseteq \operatorname{Kern} \varepsilon$, z.z. $U = \operatorname{Kern} \varepsilon$.
Wir überprüfen die Universalität: Sei $\Psi : \mathcal{V}^k \to \mathcal{W}$ multilinear und alternierend. Dann, nach Def. des Tensorproduktes, haben wir eine eindeutige lineare Abbildung $\alpha : \mathrm{T}^k \mathcal{V} \to \mathcal{W}$ mit

$$\Psi(V) = \alpha(V_1 \otimes \cdots \otimes V_k) \ \forall V \in \mathcal{V}^k$$

Da Ψ alternierend ist, folgt $U \leq \operatorname{Kern} \alpha$. Also faktorisiert α über dem natürlichen Epimorphismus $\varepsilon : \mathrm{T}^k \mathcal{V} \longrightarrow \mathcal{T}$ d.h. es existiert eine eindeutige lineare Abbildung $\psi : \mathcal{T} \to \mathcal{W}$ mit $\psi \circ \varepsilon = \alpha$, d.h. mit $\Psi(V) = \psi(V_1, \wedge \cdots \wedge V_k)$.
□

Beispiel 10.3.3:

(1) Sei $k > \operatorname{Dim} \mathcal{V}$, dann ist $\bigwedge^k \mathcal{V} = \{0\}$.
Denn, sei $\Psi : \mathcal{V}^k \to \mathcal{W}$ alternierend, so ist jedes $V \in \mathcal{V}^k$ linear abhängig und somit $\Psi(V) = 0$.

(2) $\bigwedge^1 \mathcal{V} \cong \mathcal{V}$

(3) Sei $n = \operatorname{Dim} \mathcal{V}$. Dann gilt: $\operatorname{Dim} \bigwedge^n \mathcal{V} = 1$.
Genauer: Ist $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$, so ist $(B_1 \wedge \cdots \wedge B_n)$ eine Basis von $\bigwedge^n \mathcal{V}$.
Andere Sichtweise: In LA1 hatten wir gezeigt, dass der VR der alternierenden Multilinearformen eindimensional ist, genauer von „einer“ Determinante (nach Basiswahl) erzeugt.

Satz 10.3.4:

Sei $\operatorname{Dim} \mathcal{V} = n$. Dann gilt $\operatorname{Dim} \bigwedge^k \mathcal{V} = \binom{n}{k}$.
Genauer: Sei $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$. Für jede k-elementige Teilmenge $I \subseteq \underline{n}$ mit Elementen $i_1 < i_2 < \cdots < i_k$. Sei $B_I := B_{i_1} \wedge \cdots \wedge B_{i_k}$. Dann ist $\left(B_I \,\middle|\, I \subseteq \underline{n},\ |I| = k\right)$ eine Basis von $\bigwedge^k \mathcal{V}$ der Mächtigkeit $\binom{n}{k}$.

Beweis zu 10.3.4:

(1) DIE B_I ERZEUGEN $\bigwedge^k \mathcal{V}$: Zur Vorbereitung betrachte

$$V_1 \wedge \cdots \wedge V_k = \operatorname{sign}(\sigma) W_1 \wedge \cdots \wedge W_k \ \forall V \in \mathcal{V}^k,\ \sigma \in \mathrm{S}_k,\ W = V \circ \sigma$$

(Tupel permutieren). Dies folgt sofort für Transpositionen, und da diese Transpositionen S_k erzeugen, folgt dies auch für alle $\sigma \in \mathrm{S}_k$.
Dan nun klar ist, dass $\bigwedge^k \mathcal{V}$ von Elementen der Form

$$B_{a(1)} \wedge \cdots \wedge B_{a(k)}$$

erzeugt wird, wobei $a : \underline{k} \to \underline{n}$ eine beliebige Abbildung ist, folgt die Erzeugung aus der Multilinearität, der Umsortierungseigenschaft (tausche Element mit Transpositionen, kostet nur ein Vorzeichen) oben und der offensichtlichen Tatsache, dass

$$B_{a(1)} \wedge \cdots \wedge B_{a(k)} = 0$$

ist, falls a nicht injektiv ist.
Einschränkung der Bedingungen an a: injektiv und ordnungserhaltend ($x < y \Rightarrow a(x) < a(y)$), dann ist man genau bei Basis B_I.

(2) LINEARE UNABHÄNGIGKEIT: Sei $\sum a_I B_I = 0$ für gewisse $a_I \in K$, $I \subseteq \underline{n}$, $|I| = k$. Sei nun $J \subseteq \underline{n}$, $|J| = k$. Um $a_J = 0$ zu zeigen, betrachte:

$$\begin{aligned} \pi_J : \quad & \mathcal{V} \longrightarrow \langle B_i \mid i \in J \rangle, \\ & \sum_{i=1}^{n} a_i B_i \longmapsto \sum_{j \in J} a_j B_j \end{aligned}$$

und sei $\det$ die Determinante von $\langle B_i \mid i \in J \rangle$ bzgl. $(B_i)_{i \in J}$. Dann ist

$$\begin{aligned} \Psi_J : \mathcal{V}^k & \longrightarrow K, \\ V & \longmapsto \det(\pi_J(V_1), \ldots, \pi_J(V_k)) \end{aligned}$$

multilinear und alternierend.

Nach Definition des äußeren Produkts haben wir eine eindeutige lineare Abbildung

$$\psi_J : \bigwedge^k \mathcal{V} \longrightarrow K \text{ mit } \Psi_J(V) = \psi_J(V_1 \wedge \cdots \wedge V_k) \ \forall V \in \mathcal{V}^k$$

Klar: $\psi_J = \delta_{IJ} := \begin{cases} 1 & I = J \\ 0 & I \neq J \end{cases}$

Wende ψ_J auf $\sum a_I B_I$ und erhalte

$$0 = \psi_J\left(\sum a_I B_I\right) = \sum a_I \psi_J(B_I) = \sum a_I \delta_{IJ} = a_J$$

□

Korollar 10.3.5:

Ein k-Tupel $V \in \mathcal{V}^k$ ist genau dann linear abhängig, wenn $V_1 \wedge \cdots \wedge V_k = 0$ gilt.

Beweis zu 10.3.5:

„⇒“: hatten wir schon (Determinante).

„⇐“: durch Kontraposition aus 10.3.4.

□

Bisher war $\wedge$ nur eine alternierende multilineare Abbildung. Wir wollen uns überlegen, dass man $\wedge$ auch als Verknüpfung auffassen kann, und dabei alle äußeren Potenzen zu einem größeren Ganzen zusammenfassen kann. → Grassmann-Algebra, analog zur Tensoralgebra:

Definition 10.3.6: GRASSMANN-ALGEBRA

Sei $\operatorname{Dim} \mathcal{V} = n$ und $\bigwedge^0 \mathcal{V} = K \cdot 1$ ein 1-dimensionaler VR. Man setzt

$$\bigwedge \mathcal{V} := \bigoplus_{k=0}^{n} \bigwedge^k \mathcal{V}$$

und definiert eine Multiplikation auf $\bigwedge \mathcal{V}$, indem man die durch

$$\begin{aligned} \wedge_{k,l} : \quad & \bigwedge^k \mathcal{V} \times \bigwedge^l \mathcal{V} \longrightarrow \bigwedge^{k+l} \mathcal{V}, \\ & (V_1 \wedge \cdots \wedge V_k, W_1 \wedge \cdots \wedge W_l) \longmapsto V_1 \wedge \cdots \wedge V_k \wedge W_1 \wedge \cdots \wedge W_l \end{aligned}$$

definierten bilinearen Abbildungen zu einer bilinearen Abbildung

$$\wedge : \bigwedge \mathcal{V} \times \bigwedge \mathcal{V} \longrightarrow \bigwedge \mathcal{V}$$

zusammensetzt. $(\bigwedge \mathcal{V}, \wedge)$ heißt die **äußere Algebra** oder **Grassmann-Algebra** von $\mathcal{V}$.

Es gilt $\operatorname{Dim} \bigwedge = \sum \operatorname{Dim} \bigwedge^k \mathcal{V} = \sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Jetzt haben wir die komplette Analogie Mengenlehre ↔ lineare Algebra.

Index

Symbol- und Abkürzungsverzeichnis

$\mathscr{A}^k_{\text{generisch}}$	Menge der affin unabhängigen k-Tupel im affinen Raum $\mathscr{A}$
$\mathscr{A}^k_{\text{spez}}$	Menge der kollinearen k-Tupel im affinen Raum $\mathscr{A}$
$\mathrm{Aff}(\mathscr{A})$	affine Gruppe vom affinen Raum $\mathscr{A}$, Gruppe der affinen Automorphismen
$\mathrm{Ann}_R(M)$	Annihilator des R-Moduls M
$\mathrm{Ann}_R(m)$	Annihilatorideal vom R-Modulelement m
$\mathrm{Aut}_\alpha(\mathcal{V})$	Menge der α-Automorphismen im VR $\mathcal{V}$
χ_φ	charakteristisches Polynom des K-VR-Endomorphismus φ
$\mathcal{B}(\mathcal{V})$	Menge aller Basen des K-Vektorraums $\mathcal{V}$
δ_{ij}	Kronecker-Delta, $\delta_{ij} := \begin{cases} 1 & \text{wenn } i = j \\ 0 & \text{wenn } i \neq j \end{cases}$
$\mathrm{End}(M)$	Menge der Endomorphismen, also strukturerhaltenden Selbstabbildungen, auf der algebraischen Struktur M
$\mathrm{End}_R(M)$	Endomorphismenring des R-Moduls M
$\exp(X)$	Exponentialfunktion/Exponentialreihe
G/U	Menge der Linksnebenklassen der Untergruppe U in Gruppe G
$M/\sim$	Menge aller Äquivalenzklassen der Äquivalenzrelation $\sim$ auf M
M/U	Faktormodul von M nach U
$\mathrm{Fr}_R(A)$	freier R-Modul auf A
$\langle M \rangle_{\mathrm{a}}$	affines Erzeugnis der Teilmenge M eines affinen Raumes
$\langle V \rangle_\alpha$	Erzeugnis vom K-Vektor V bzgl. Endomorphismus α, $\langle V \rangle_\alpha := K[\alpha](V)$
$\langle V \rangle_A$	Erzeugnis von $V \in K^{n\times 1}$ bzgl. $A \in K^{n\times n}$, $\langle V \rangle_A := K[A]V$
$\langle X \rangle$	Erzeugnis von X
$\mathrm{ggT}(a,b)$	größter gemeinsamer Teiler von a und b
$\mathrm{GL}_n(K)$	Generelle lineare Gruppe über dem Körper K, d.h. Menge der invertierbaren Matrizen von $K^{n\times n}$
$\mathrm{GL}_n(R)$	Generelle lineare Gruppe über dem Ring R, d.h. $(R^{n\times n})^*$
$K(x)$	Körper der rationalen Funktionen in einer Variablen über dem Körper K
$K(x_1,\ldots,x_n)$	Körper der rationalen Funktionen über dem Körper K
$K[\alpha]$	Menge der Endomorphismen, die durch Einsetzen vom Endomorphismus α in alle Polynome in $K[x]$ entsteht, $K[\alpha] = \{p(\alpha) \mid p \in K[x]\}$
$K[[x]]$	formaler Potenzreihenring über dem Körper K
$K[A]$	Menge der Matrizen, die durch Einsetzen von $A \in K^{n\times n}$ in alle Polynome in $K[x]$ entsteht, $K[A] := \{p(A) \mid p \in K[x]\}$
$K[x]$	Polynomring über dem Körper K
κ_g	Konjugationsautomorphismus von g, $\kappa_g(h) := ghg^{-1}$
$\mathrm{kgV}(a,b)$	kleinstes gemeinsames Vielfaches von a und b
$[G:U]$	Index der Untergruppe U in Gruppe G (Anzahl der Linksnebenklassen)
$\mathfrak{X}(A)$	charakteristische Matrix zur Matrix $A \in K^{n\times n}$

A_n	alternierende Gruppe vom Grad n
$\mathrm{C}_G(m)$	Zentralisator von $m \in G$ (Stabilisator unter Konjugation)
C_m	die zyklische Gruppe der Ordnung $m \in \mathbb{Z}_{\geq 0}$; $\mathrm{C}_m := \left(\mathbb{Z}/m\mathbb{Z}, +\right)$
$\mathrm{C}_{\mathrm{End}(\mathcal{V})}(\varphi)$	Zentralisatoralgebra von $\varphi \in \mathrm{End}(\mathcal{V})$
$\mathrm{C}_{K^{n\times n}}(A)$	Zentralisatoralgebra der Matrix $A \in K^{n\times n}$
$\mathrm{E}_a(\varphi)$	Eigenraum des Eigenwerts a vom Endomorphismus φ
$\mathrm{Hom}_R(M,N)$	Menge der R-Modulhomomorphismen von M nach N
I_n	Einheitsmatrix der Größe $n \times n$ (mit $(\mathrm{I}_n)_{i,j} = \delta_{ij}$)
$\mathrm{J}_m(p)$	Jordan-Block vom Polynom p der Größe m
M_A	VR $K^{n\times 1}$ aufgefasst als $K[x]$-Modul vermöge $(p(x), V) \mapsto p(A)V$ für $A \in K^{n\times n}$
N_d	Matrix in $K^{d\times d}$ mit nur einer 1 in der oberen linken Ecke, sonst Nullen
$\mathrm{S}(A)$	Spaltenraum erzeugt von den Spalten der Matrix A
$\mathrm{T}(M)$	Torsionsmodul des Moduls M
$\mathrm{T}\mathcal{V}$	Tensoralgebra des VRs $\mathcal{V}$
$\mathrm{T}^n\mathcal{V}$	n-faches Tensorprodukt des VRs $\mathcal{V}$ mit sich selbst
$\mathrm{U}_{(a,b)}$	$:= \begin{pmatrix} s & t \\ -\frac{b}{d} & \frac{a}{d} \end{pmatrix}$ mit $d := \mathrm{ggT}(a,b)$ und s,t sodass $d = sa + tb$ (Bézout-Identität).
$\mathrm{Z}(G)$	Zentrum von G
M_p	Begleitmatrix zum Polynom p
S_n	symmetrische Gruppe über n Elementen (Ordnung $n!$)
S_M	symmetrische Gruppe über der Menge M (bijektive Selbstabbildungen)
$\mu_{\varphi,V}$	Minimalpolynom des VR-Endomorphismus φ bzgl. Vektor V
μ_φ	Minimalpolynom des K-VR-Endomorphismus φ
$\mathbb{N}$	Natürliche Zahlen ohne 0
$\mathbb{N}_0$	Natürliche Zahlen mit 0, $= \mathbb{Z}_{\geq 0}$
ν_U	natürlicher Epimorphismus von einem Modul M in den Faktormodul M/U
$\mathrm{ord}\, a$	Ordnung des Gruppenelements a
$\mathrm{ord}\, G$	Ordnung der Gruppe G (Anzahl der Elemente)
$\overline{m}$	Restklasse von m
$\mathrm{Pot}(M)$	Potenzmenge der Menge M (Menge aller Teilmengen)
$\mathrm{Pot}_n(M)$	Menge aller n-elementigen Teilmengen von M
$\mathrm{PRF}(A)$	primäre rationale Form der Matrix A
$\mathrm{Quot}(R)$	Quotientenkörper des Rings R
$\mathrm{Rang}(A)$	torsionsfreier Rang der Matrix A über einem Ring
$G\backslash M$	Menge der Bahnen zu der G-Menge M
$\mathrm{RKF}(A)$	rationale kanonische Form der Matrix A
$\sim_f$	Bildgleichheitsäquivalenzrelation der Abbildung f ($x \sim_f y :\Leftrightarrow f(x) = f(y)$)

$\sim_G$	Bahngleichheitsäquivalenzrelation auf der G-Menge M
$\mathrm{SL}_n(K)$	spezielle lineare Gruppe vom Grad n über dem Körper K
$\mathrm{Stab}_G(m)$	Stabilisator von G-Mengen-Element m
$\underline{n}$	Standardmenge n; $\underline{n} := \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$
$\mathcal{V}^*$	Dualraum des VRs $\mathcal{V}$
$\mathcal{V}^{\otimes n}$	n-faches Tensorprodukt des VRs $\mathcal{V}$ mit sich selbst
$\widehat{g}$	induzierte Abb. einer Gruppenoperation; $\widehat{g} : M \to M,\ m \mapsto gm$ für die G-Menge M und $g \in G$.
${}_R R$	regulärer R-Modul
$a \mid b$	a teilt b
$a \sim b$	a ist assoziiert zu b
A^{tr}	transponierte Matrix A (an der Diagonale gespiegelt)
$f^{-1}(\{y\})$	Faser von $y \in \mathrm{Bild}\, f$; d.h. Menge der Urbilder $f^{-1}(\{y\}) := \{x \mid f(x) = y\}$
$G \circlearrowright M$	Gruppe G operiert auf Menge M
$I \trianglelefteq R$	I ist ein Ideal des Rings R
$I_1 + I_2$	Summe der Ideale I_1, I_2
$M \cong_R N$	M ist R-Modul-isomorph zu N
$M \leq N$	M ist Teilmodul von N
$M \dot{\cup} N$	die Vereinigung von M und N ist disjunkt
$M \oplus N$	direkte Summe der Moduln M und N
$M \otimes N$	das Tensorprodukt von den Moduln M und N
$M \underset{G}{\cong} N$	die G-Mengen M und N sind ähnlich
$N \rtimes U$	semidirektes Produkt von NT N und Untergruppe U
$N \trianglelefteq G$	N ist Normalteiler von G
N^M	Menge der Abbildungen von M nach N
R^*	Einheitengruppe von R (Menge der invertierbaren Elemente in der algebraischen Struktur R)
$U \leq G$	U ist Untergruppe von Gruppe G
DGL	Differentialgleichung
e.e.	endlich erzeugt (von endlicher Dimension, bzw. Erzeugnis einer endlichen Menge)
EZS	Erzeugendensystem
HIB	Hauptidealbereich
IB	Integritätsbereich
kmE.	kommutativ mit Eins (bzgl. Ring)
MinPoly	Minimalpolynom
NT	Normalteiler
SNF	Smith-Normalform
TP	Tensorprodukt
TR	Teilraum
VR	Vektorraum
ÄR	Äquivalenzrelation