Westfälische
Wilhelms-Universität
Münster

Fachbereich 10
Mathematik und
Informatik

Skript Lineare Algebra II.

Mitschrift der Vorlesung „Lineare Algebra II.“ von Prof. Dr. Arthur Bartels

Jannes Bantje

23. Oktober 2015

Aktuelle Version verfügbar bei

GitHub

https://github.com/JaMeZ-B/latex-wwu

GitHub ist eine Internetplattform, auf der viele OpenSource-Projekte gehostet werden. Diese Plattform nutzen wir zur Zusammenarbeit, also findet man hier neben den PDFs auch die TEX-Dateien. Außerdem ist über diese Plattform auch direktes Mitarbeiten möglich, siehe nächste Seite.

sciebo die Campuscloud

https://uni-muenster.sciebo.de/public.php?service=files&t=965ae79080a473eb5b6d927d7d8b0462

Sciebo ist ein Dropbox-Ersatz der Hochschulen in NRW, der von der Uni Münster in leitender Position auf Basis der OpenSource-Software Owncloud aufgebaut wurde. Wenn man auf den Link klickt, kann man die Freigabe zum eigenen Speicher hinzufügen und hat dann immer automatisch die aktuellste Version.

Bittorrent Sync

B6WH2DISQ5QVYIRYIEZSF4ZR2IDVKPN3I

BTSync ist ein peer-to-peer Dateisynchronisations-Tool. Dabei werden die Dateien nur auf den Computern der Teilnehmer an einer Freigabe gespeichert. Ein RasPi ist permanent online, sodass stets die aktuellste Version verfügbar ist. `Clients` gibt es für jedes Betriebssystem. Zugang ist über das obige „Secret“ bzw. den QR-Code möglich.

Vorlesungshomepage

http://wwwmath.uni-muenster.de/reine/u/topos/lehre/SS2013/LineareAlgebra2/index.html

Hier ist ein Link zur offiziellen Vorlesungshomepage.

Vorwort — Mitarbeit am Skript

Dieses Dokument ist eine Mitschrift aus der Vorlesung „Lineare Algebra II., SoSe 2013“, gelesen von Prof. Dr. Arthur Bartels. Der Inhalt entspricht weitestgehend dem Tafelanschrieb. Für die Korrektheit des Inhalts übernehme ich keinerlei Garantie! Für Bemerkungen und Korrekturen – und seien es nur Rechtschreibfehler – bin ich sehr dankbar. Korrekturen lassen sich prinzipiell auf drei Wegen einreichen:

- Persönliches Ansprechen in der Uni, Mails an `j.bantje@wwu.de` (gerne auch mit annotieren PDFs) oder Kommentare auf `https://github.com/JaMeZ-B/latex-wwu`.

- *Direktes* Mitarbeiten am Skript: Den Quellcode poste ich auf GitHub (siehe oben), also stehen vielfältige Möglichkeiten der Zusammenarbeit zur Verfügung: Zum Beispiel durch Kommentare am Code über die Website und die Kombination Fork + Pull Request. Wer sich verdient macht oder ein Skript zu einer Vorlesung, die ich nicht besuche, beisteuern will, dem gewähre ich gerne auch Schreibzugriff.

  Beachten sollte man dabei, dass dazu ein Account bei `github.com` notwendig ist, der allerdings ohne Angabe von persönlichen Daten angelegt werden kann. Wer bei GitHub (bzw. dem zugrunde liegenden Open-Source-Programm „`git`“) – verständlicherweise – Hilfe beim Einstieg braucht, dem helfe ich gerne weiter. Es gibt aber auch zahlreiche empfehlenswerte Tutorials im Internet.[1]

- *Indirektes* Mitarbeiten: TeX-Dateien per Mail verschicken.

  Dies ist nur dann sinnvoll, wenn man einen ganzen Abschnitt ändern möchte (zB. einen alternativen Beweis geben), da ich die Änderungen dann per Hand einbauen muss! Ich freue mich aber auch über solche Beiträge!

[1] zB. `https://try.github.io/levels/1/challenges/1`, ist auf Englisch, aber dafür interaktives LearningByDoing

Inhaltsverzeichnis

1. Isometrien

1.1. Definition

Sei $(V, \langle\,|\,\rangle)$ ein euklidischer oder unitärer Vektorraum. Ein Endomorphismus $f : V \to V$ heißt eine **Isometrie**, falls für alle $v \in V$ gilt:

$$\|f(v)\| = \|v\|$$

1.2. Satz

$$f \text{ Isometrie} \iff \forall v, w \in V \text{ gilt } \langle f(v) \mid f(w)\rangle = \langle v \mid w\rangle \quad (\star)$$

Beweis
Gilt $(\star)$ so folgt

$$\|f(v)\|^2 = \langle f(v) \mid f(v)\rangle \underset{(\star)}{=} \langle v \mid v\rangle = \|v\|^2$$

Da $\|f(v)\|, \|v\| \geqslant 0$ folgt $\|f(v)\| = \|v\|$. Sei nun umgekehrt f eine Isometrie. Für $v, w \in V$ gilt dann

$$\langle f(v+w) \mid f(v+w)\rangle = \langle v+w \mid v+w\rangle$$

Also

$$\langle f(v) \mid f(v)\rangle + \langle f(v) \mid f(w)\rangle + \langle f(w) \mid f(v)\rangle + \langle f(w) \mid f(w)\rangle = \langle v \mid v\rangle + \langle v \mid w\rangle + \langle w \mid v\rangle + \langle w \mid w\rangle$$

Wegen $\langle f(v) \mid f(v)\rangle = \langle v \mid v\rangle$ und $\langle f(w) \mid f(w)\rangle = \langle w \mid w\rangle$ folgt

$$\langle f(v) \mid f(w)\rangle + \langle f(w) \mid f(v)\rangle = \langle v \mid w\rangle + \langle w | v\rangle$$

Ist V euklidisch so $\langle f(v) \mid f(w)\rangle = \langle f(w) \mid f(v)\rangle$ und $\langle v \mid w\rangle = \langle w \mid v\rangle$ und es folgt $\langle f(v) \mid f(w)\rangle = \langle v \mid w\rangle$. Ist V unitär so folgt nur

$$\mathrm{Re}\,\langle f(v) \mid f(w)\rangle = \mathrm{Re}\,\langle v \mid w\rangle$$

Es gilt aber auch $\langle f(v+iw) \mid f(v+iw)\rangle = \langle v+iw \mid v+iw\rangle$. Damit folgt analog zu ($\diamondsuit$)

$$\langle f(v) \mid if(w)\rangle + \langle i(fw) \mid f(v)\rangle = \langle v \mid iw\rangle + \langle iw \mid v\rangle$$

Also

$$\begin{aligned} -i\,\langle f(v) \mid f(w)\rangle + i\,\langle f(w) \mid f(v)\rangle &= -i\,\langle v \mid w\rangle + i\,\langle w \mid v\rangle \\ \langle f(v) \mid f(w)\rangle - \langle f(w) \mid f(v)\rangle &= \langle v \mid w\rangle - \langle w \mid v\rangle \end{aligned}$$

Es folgt $\mathrm{Im}\,\langle f(v) \mid f(w)\rangle = \mathrm{Im}\,\langle v \mid w\rangle$ $\square$

1.3. Bemerkung

Sei $e_1, \ldots, e_n$ eine Orthonormalbasis von V und $f \in \mathrm{End}(V)$. Dann ist f genau dann eine Isometrie, wenn gilt

$$\langle f(e_i) \,|\, f(e_j)\rangle = \delta_{ij} \qquad \text{für } i, j = 1, \ldots, n$$

1.4. Satz

Sei $B = (e_1, \ldots, e_n)$ eine Orthonormalbasis und $f \in \mathrm{End}(V)$. Sei $A = m_B^B(f)$ Dann gilt:

$$f \text{ ist Isometrie} \iff A \cdot \overline{A}^t = I_n$$

Beweis
Es ist $A = (a_{ij})$ mit $a_{ij} = \langle f(e_j) \mid e_i \rangle$ da $f(e_j) = \sum_{i=1}^n \langle f(e_j) \mid e_i \rangle e_i$ ist. Sei f eine Isometrie. Dann

$$A \cdot \overline{A}^t = \left(\sum_{j=1}^n \langle f(e_j) \mid e_i \rangle \overline{\langle f(e_j) \mid e_k \rangle} \right)_{ik} =: (b_{ik})_{ik}$$

Da f eine Isometrie ist, ist $f(B) = f(e_1), \ldots, f(e_n)$ auch eine Orthonormalbasis und es folgt

$$\begin{aligned} b_{ik} &= \sum_{j=1}^n \langle f(e_j) \,|\, e_i \rangle \langle e_k \mid f(e_j) \rangle \\ &= \langle \sum_{j=1}^n \langle e_k \mid f(e_j) \rangle f(e_j) \,|\, e_i \rangle \\ &= \langle e_k \mid e_i \rangle = \delta_{ki} \end{aligned}$$

Sei $A \cdot \overline{A}^t = I_n$. Dann ist auch $\overline{A}^t \cdot A = I_n$ und wir erhalten für alle i, k

$$\sum_{j=1}^n \overline{\langle f(e_i) \mid e_j \rangle} \langle f(e_k) \mid e_j \rangle = \delta_{ik}$$

Es folgt

$$\begin{aligned} \langle f(e_k) \mid f(e_i) \rangle &= \langle \sum_{j=1}^n \langle f(e_k) \mid e_j \rangle e_j \mid \sum_{j=1}^n \langle f(e_i) \mid e_j \rangle e_j \rangle \\ &= \sum_{j=1}^n \langle f(e_k) \mid e_j \rangle \overline{\langle f(e_i) \mid e_j \rangle} \\ &= \delta_{ik} \end{aligned}$$

□

1.5. Korollar

Ist f eine Isometrie eines endlich dimensionalen euklidischen oder unitären Vektorraums, so ist

$$|\det f| = 1$$

Beweis
Sei B Orthonormalbasis von V, $A = m_B^B(f)$. Dann

$$\det f = \det A = \det A^t = \overline{\det \overline{A}^t}$$

Nach 1.4 folgt

$$\det f \cdot \overline{\det f} = \det A \cdot \det \overline{A}^t = \det(A \cdot \overline{A}^t) = \det(I_n) = 1$$

Also $|\det f| = 1$ □

1.6. Lemma

Sei V euklidischer oder unitärer Vektorraum. Seien $f, g : V \to V$ Isometrien

a) $f \circ g$ ist eine Isometrie

b) f ist injektiv $\Rightarrow$ surjektiv, wenn $\dim V < \infty$

c) Ist f bijektiv, so ist auch f^{-1} eine Isometrie

Insbesondere bilden die Isometrien eine Gruppe, falls $\dim V < \infty$

Beweis

a) $\|f \circ g(v)\| \underset{f \text{ Isometrie}}{=} \|g(v)\| \underset{g \text{ Isometrie}}{=} \|v\|$

b) Sei $f(v) = 0 \implies \|v\| = \|f(v)\| = \|0\| = 0 \to v = 0$

c) $\|f^{-1}(v)\| = \|f\left(f^{-1}(v)\right)\| = \|v\|$

$\square$

1.7. Definition

(i) Sei V eine endlich dimensionaler euklidischer Vektorraum

$$O(V) := \{f \in \operatorname{End}(V) \mid f \text{ Ist Isometrie}\}$$

heißt die **orthogonale Gruppe** von V. Die Untergruppe

$$SO(V) := \{f \in O(V) \mid \det f = 1\}$$

heißt die **spezielle orthogonale Gruppe** von V. Ist $V = \mathbb{R}^n$ mit dem Standard-Skalarprodukt, so schreiben wir auch $O(n) := O(\mathbb{R}^n)$ bzw $SO(n) := SO(\mathbb{R}^n)$

(ii) Sei V eine endlich dimensionaler unitärer Vektorraum

$$U(V) := \{f \in \operatorname{End}(V) \mid f \text{ ist Isometrie}\}$$

heißt die **unitäre Gruppe** von V. Die Untergruppe

$$SU(V) := \{f \in U(V) \mid \det f = 1\}$$

heißt die **spezielle unitäre Gruppe** von V. Ist $V = \mathbb{C}^n$ mit dem Standard-Skalarprodukt, so schreiben wir auch $U(n) := U(\mathbb{C}^n)$ bzw $SU(n) := SU(\mathbb{C}^n)$

1.8. Bemerkung

Wegen 1.3 ist $O(n)$ die Menge der Matrizen deren Spalten eine Orthonormalbasis von $\mathbb{R}^n$ (mit Standardskalarprodukt) bilden. $U(n)$ ist die Menge der Matrizen deren Spalten eine Orthonormalbasis von $\mathbb{C}^n$ (mit Standardskalarprodukt) bilden.

1.9. Beispiel

$$O(2) = \left\{ \begin{pmatrix} a & -\varepsilon b \\ b & \varepsilon a \end{pmatrix} \middle| a^2 + b^2 = 1, \varepsilon \in \{\pm 1\} \right\}$$

$$SO(2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a^2 + b^2 = 1 \;\; a, b \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \middle| \varphi \in [0, 2\pi) \right\}$$

1.10. Bemerkung

$D(\varphi) := \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$ wirkt als Drehung um den Winkel φ um den Nullpunkt auf $\mathbb{R}^2$.

1.11. Beispiel

Sei

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in O(2) \setminus SO(2)$$

S wirkt als Spiegelung an der Achse e_1. Es ist $S^2 = I_2$. Es gilt $O(2) = SO(2) \cup SO(2) \cdot S$. Jedes Element in $SO(2) \cdot S$ ist eine Spiegelung.

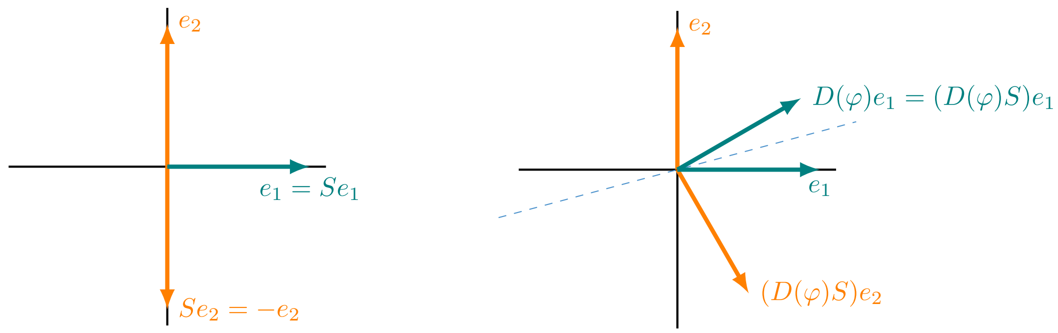


Abbildung 1: Veranschaulichung von Elementen in $SO(2) \cdot S$

1.12. Lemma

Sei $f : V \to V$ eine Isometrie.

(i) Ist λ ein Eigenwert von f so gilt $|\lambda| = 1$

(ii) Ist $U \leqslant V$ mit $f(U) = U$ so gilt $f(U^\perp) \subseteq U^\perp$

Beweis

(i) Sei v ein Eigenvektor zum Eigenwert λ. Dann

$$\|v\| = \|f(v)\| = \|\lambda \cdot v\| = |\lambda| \cdot \|v\|$$

$v \neq 0 \Rightarrow \|v\| \neq 0$. Also $|\lambda| = 1$. □

(ii) Sei $v \in U^\perp$. Zu zeigen:$\forall u \in U : \langle f(v) \,|\, u \rangle = 0$.
Sei $u \in U$. Da $U = f(U)$ gibt es $u' \in U$ mit $f(u') = u$. Also

$$\langle f(v) \,|\, u \rangle = \langle f(v) \,|\, f(u') \rangle \underset{(1.2)}{=} \langle v \,|\, u' \rangle \underset{v \in U^\perp}{=} 0$$

□

1.13. Satz

Sei V ein endlichen dimensionaler unitärer Vektorraum. Dann sind alle $f \in U(V)$ diagonalisierbar[1].

[1] $\exists$ Basis B mit $m_B^B(f)$ Diagonalmatrix oder $\exists$ Basis B aus EV von f

Beweis

(vgl. 15.5 LinA I) Induktion nach $n := \dim V$. Induktionsanfang: $n = 0$ $\surd$
Induktionsschritt: $n - 1 \mapsto n$
Nach dem Fundamentalsatz der Algebra hat χ_f eine Nullstelle und f damit einen Eigenvektor v. Sei $U := \langle v \rangle^\perp$. Dann $\dim U = n - 1$. Wegen (1.12) (i) ist$\langle f(v) \rangle = \langle v \rangle$. Aus (1.12) (ii) folgt $f(U) \subseteq U$. Weiter ist $f_0 := f|_U : U \to U$ eine Isometrie. Induktionsannahme $\Rightarrow$ $\exists$ Basis aus Eigenvektoren B_0 für f_0. Dann ist $B = \{v\} \cup B_0$ eine Basis aus Eigenvektoren für f. $\square$

Bemerkung

In (1.13) gibt es sogar eine Orthonormalbasis aus Eigenvektoren für f.

1.14. Bemerkung

Ist V ein endlich dimensionaler euklidischer Vektorraum so sind nicht alle $f \in O(V)$ diagonalisierbar. $f \in O(2)$ ist genau dann diagonalisierbar wenn $f \in \{\pm I_2\}$ oder f eine Spiegelung ist.

Aber es existiert eine Orthonormalbasis von f mit

$$m_B^B(f) = \begin{pmatrix} \boxed{D(\varphi_1)} & & & & & \\ & \boxed{D(\varphi_2)} & & & & \\ & & \ddots & & & \\ & & & \boxed{D(\varphi_i)} & & \\ & & & & \boxed{I_n} & \\ & & & & & \boxed{-I_n} \end{pmatrix}$$

2. Volumen und Determinante

2.1. Definition

Sei V ein $\mathbb{R}$-Vektorraum, $v_1, \ldots, v_r \in V$ Dann heißt

$$P(v_1, \ldots, v_r) := \left\{ \sum_{i=1}^{r} t_i v_i \,\middle|\, t_i \in [0,1] \right\}$$

der von $v_1, \ldots, v_r$ aufgespannte **Parallelotop**. Ist $v_1, \ldots, v_r$ linear unabhängig, so heißt $P(v_1, \ldots, v_r)$ r**-dimensional**.

2.2. Bemerkung

$$P(v_1, \ldots, v_r) \subseteq \langle v_1, \ldots, v_r \rangle = \mathcal{L}(\{v_1, \ldots, v_r\})$$

2.3. Beispiel

(i) $V = \mathbb{R}^n$, $P(e_1, \ldots, e_n) = \left\{ \begin{pmatrix} t_1 \\ \cdot \\ t_n \end{pmatrix} \,\middle|\, t_i \in [0,1] \right\}$

(ii) $P(e_1, e_2)$ Quadrat der Kantenlänge 1.

(iii) $P(e_1, e_2, e_3)$ Würfel der Kantenlänge 1.

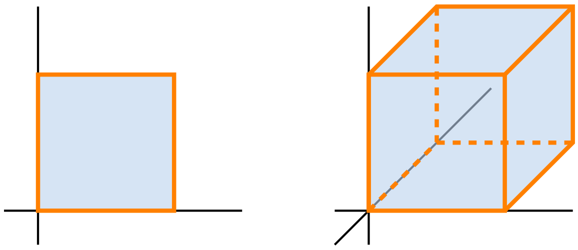


Abbildung 2: einfache Parallelotope in $\mathbb{R}^2$ bzw. $\mathbb{R}^3$

(iv) $P(v_1, v_2)$

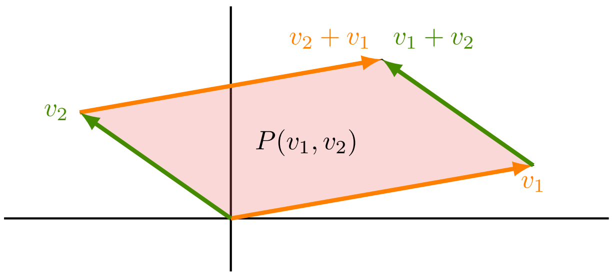


Abbildung 3: Parallelotop von Nicht-Standardvektoren in $\mathbb{R}^2$

2.4. Frage

Was ist das Volumen eines n-dimensionalen Parallelotops in $\mathbb{R}^n$? In anderen $\mathbb{R}$-Vektorraum?
Es sollte gelten:

(1) $\mathrm{Vol}_{\mathbb{R}^n}\left(P(e_1,\dots,e_n)\right) = 1$

(2) $\mathrm{Vol}_{\mathbb{R}^n}\left(P(\lambda_1 e_1,\dots,\lambda_n e_n)\right) = \lambda_1 \cdots \lambda_n$

(3) $v_1,\dots,v_n$ linear abhängig $\Longrightarrow \mathrm{Vol}_{\mathbb{R}^n}(v_1,\dots,v_n) = 0$

(4) Mit $U := \langle v_1,\dots,v_{n-1}\rangle$

$$\mathrm{Vol}_{\mathbb{R}^n}\left(P(v_1,\dots,v_n)\right) = \mathrm{Vol}_U\left(P(v_1,\dots,v_{n-1})\right)\|v_n - P_U(v_n)\|$$

wobei $P_U : V \to U$ die orthogonale Projektion ist.

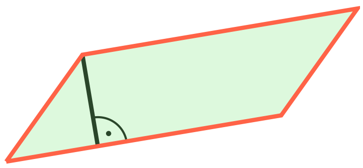


Abbildung 4: Veranschaulichung von 2.4((4))

2.5. Beispiel

$$\mathrm{Vol}_{\mathbb{R}^n}(P(v_1,\dots,v_i+v_i',v_{i+1},\dots,v_n)) = ?$$

$\mathrm{Vol}_{\mathbb{R}^2}(P(v_1,v_2)) + \mathrm{Vol}_{\mathbb{R}^2}(P(v_1,v_2')) = \mathrm{Vol}_{\mathbb{R}^2}(P(v_1,v_2+v_2'))$
Aber: $\mathrm{Vol}_{\mathbb{R}^2}(P(v_1,v_2+\hat{v}_2)) = \mathrm{Vol}_{\mathbb{R}^2}(P(v_1,v_2)) - \mathrm{Vol}_{\mathbb{R}^2}(P(v_1,\hat{v}_2))$

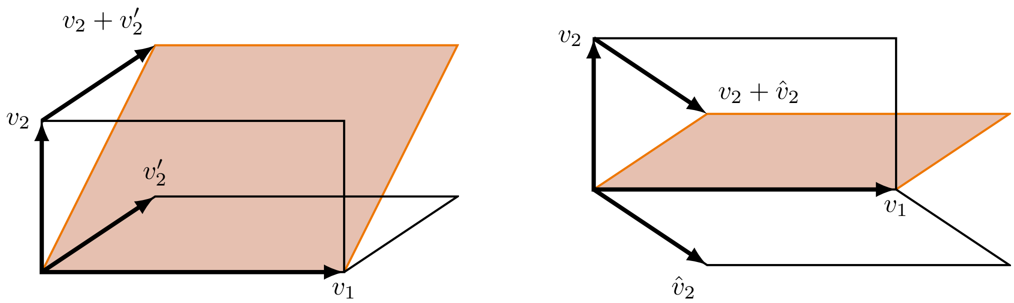


Abbildung 5: Veranschaulichung von Beispiel 2.5

2.6. Definition

Sei V ein n-dimensionaler euklidischer Vektorraum. Sei $P = P(v_1,\dots,v_n)$ ein n-dimensionales Parallelotop in V. Sei $(e_1,\dots,e_n)$ eine Orthonormalbasis von V und $f : V \to V$ linear mit $f(e_i) = v_i$. Wir definieren

$$\mathrm{Vol}(P) := |\det f|$$

Wir werden sehen, dass dies nicht von der Wahl der Orthonormalbasis abhängt. Offensichtlich sind ((1)) - ((3)) aus 2.4 erfüllt.

2.7. Lemma

Sei V ein n-dimensionaler euklidischer Vektorraum. Seien $v_1, \dots, v_n \in V$ und $B = (e_1, \dots, e_n)$ und $B' = (e'_1, \dots, e'_n)$ zwei Orthonormalbasen. Seien $f, f' : V \to V$ mit $f(e_i) = v_i = f'(e'_i)$. Dann gilt

$$|\det f| = |\det f'|$$

Beweis
Sei $\varphi \in O(V)$ mit $\varphi(e_i) = e'_i$. Dann $f = f' \circ \varphi$. Also

$$\det f = \det(f' \circ \varphi) = \det f' \cdot \det \varphi$$

Da φ eine Isometrie ist, gilt $|\det \varphi| = 1$. Es folgt $|\det f| = |\det f'|$ □

2.8. Satz

Sei V ein euklidischer Vektorraum, $\dim V = n$. Sei $P = P(v_1, \dots, v_n)$ ein n-dimensionaler Parallelotop in V. Sei $U := \langle v_1, \dots, v_{n-1} \rangle$. Dann ist

$$\mathrm{Vol}_V(P) = \mathrm{Vol}_U(P(v_1, \dots, v_{n-1})) \cdot \|v_n - P_U(v_n)\|$$

wobei $P_U : V \to U$ die orthogonale Projektion[2] von V auf U ist.

Beweis
Sei $B = (e_1, \dots, e_n)$ eine Orthonormalbasis von V so, dass $B' = (e_1, \dots, e_{n-1})$ eine Orthonormalbasis von U ist. Sei $f \in \mathrm{End}(V)$ mit $f(e_i) = v_i$. Also

$$\mathrm{Vol}_V(P) = |\det f| \qquad \mathrm{Vol}_U(P(v_1, \dots, v_{n-1})) = |\det f|_U|$$

Es ist

$$m_B^B(f) = \begin{pmatrix} & & & \langle f(e_n) \,|\, e_1 \rangle \\ & m_{B'}^{B'}(f|_U) & & \langle f(e_n) \,|\, e_2 \rangle \\ & & & \vdots \\ 0 & \cdots & 0 & \langle f(e_n) \,|\, e_n \rangle \end{pmatrix}$$

Also

$$\det f = (\det f|_U) \cdot \langle f(e_n) \,|\, e_n \rangle$$
$$\|v_n - P_U(v_n)\| = \left\| \sum_{i=1}^{n} \langle v_n \,|\, e_i \rangle e_i - \sum_{i=1}^{n-1} \langle v_n \,|\, e_i \rangle e_i \right\| = \|\langle v_n \,|\, e_n \rangle e_n\| = |\langle v_n \,|\, e_n \rangle| = |\langle f(e_n) \,|\, e_n \rangle|$$

2.9. Bemerkung

Sei V ein euklidischer Vektorraum, $\dim V = n$. Sei $f \in \mathrm{End}(V)$. Dann gilt für jeden Parallelotop $P = P(v_1, \dots, v_n)$ mit $f(P) = P\big(f(v_1), \dots, f(v_n)\big)$

$$\mathrm{Vol}_V\left(f(P)\right) = |\det f| \cdot \mathrm{Vol}_V(P)$$

[2] $U \leqslant V$, V eukl. VR , $\dim V < \infty$, Bild$P_U = U$, $P_U \circ P_U = P_U$, $P_U(v)$ ist der Vektor in U mit minimalem Abstand zu V , Formel: $P_U(v) = \sum_{i=1}^{r} \langle v \,|\, e_i \rangle e_i$ wobei $e_1, \dots, e_r$ ONB von U

3. Quotientenräume

3.1. Lemma

Seien $f : U \to V$, $\varphi : U \to W$ lineare Abbildungen wobei f surjektiv sei. Genau dann gibt es eine lineare Abbildung $\phi : V \to W$ mit $\varphi = \phi \circ f$, wenn $\operatorname{Kern} f \subseteq \operatorname{Kern} \varphi$ ist.

Beweis
Gilt $\phi \circ f = \varphi$ so ist $\operatorname{Kern} f \subseteq \operatorname{Kern} \varphi$. Sei umgekehrt $\operatorname{Kern} f \subseteq \operatorname{Kern} \varphi$. Sei $v \in V$. Dann ist φ auf den Urbildern von v konstant: Ist $f(u) = v = f(u')$ so gilt $u - u' \in \operatorname{Kern} f \subseteq \operatorname{Kern} \varphi$. Also $\varphi(u - u') = 0 \Rightarrow \varphi(u) = \varphi(u')$. Da außerdem f surjektiv ist, gibt es eine eindeutige Abbildung $\phi : V \to W$ mit $\phi(v) = \varphi(u)$ für alle $u \in U, v \in V$ mit $f(u) = v$. Insbesondere $\varphi = \phi \circ f$.

$$\begin{tikzcd} U \arrow[r, "\varphi"] \arrow[d, "f"'] & W \\ V \arrow[ur, "\phi"'] & \end{tikzcd}$$

ϕ ist linear
Seien $v, v' \in V$. Wähle $u, u' \in U$ mit $f(u) = v$, $f(u') = v'$. Dann ist auch $f(u + u') = v + v'$. Daher

$$\phi(v + v') = \varphi(u + u') = \varphi(u) + \varphi(u') = \phi(v) + \phi(v')$$

Genauso $\phi(\lambda v) = \lambda\phi(v)$. □

3.2. Bemerkung

Sei $f : U \to V$ linear und surjektiv. Sei $L := \operatorname{Kern} f$. Dann nennen wir f eine **Quotientenabbildung** zum Unterraum L von U. Durch $u \sim u' :\Leftrightarrow f(u) = f(u')$ wird eine Äquivalenzrelation auf U erklärt; es gilt

$$u \sim u' \Leftrightarrow u - u' \in \operatorname{Kern} f = L$$

Die Äquivalenzklassen sind die Urbilder von Vektoren aus V und haben die Form

$$u + L := \{u + l \,|\, l \in L\}$$

Eine Teilmenge dieser Form heißt ein **affiner Unterraum** von U mit **Richtung** L.

3.3. Defintion

Sei L ein Unterraum von U. Die Äquivalenzklassen von $u \sim u' :\Leftrightarrow u - u' \in L$ sind die affinen Unterräume von U mit Richtung L. Die Menge aller Äquivalenzklassen, also die Menge aller affinen Unterräume von U mit Richtung L, bezeichnen wir mit U/L. Sei $p : U \to U/L$ die Quotientenabbildung mit $p(u) = u + L$.

3.4. Lemma

Es gibt genau eine Vektorraumstruktur auf U/L, so dass $p : U \to U/L$ linear wird. Es gilt dann

$$(u + L) + (u' + L) = (u + u') + L \qquad \lambda(u + L) = \lambda u + L$$

Beweis
Da p linear sein soll muss gelten:

$$(u_1 + L) + (u_2 + L) = (u_1 + u_2) + L$$
$$\lambda(u + L) = (\lambda u) + L$$

Damit folgt die Eindeutigkeit. Wir müssen zeigen, dass $(*)$ und $(\#)$ wohldefiniert sind. Zu $(\#)$: Sei $u' + L = u + L$ und $\lambda \in \mathbb{K}$. Wir müssen zeigen: $\lambda u' + L = \lambda u + L$. Da $u' + L = u + L$ ist $u \in u' + L$. Also gibt es $l \in L$ mit $u = u' + l$. Also $u - u' \in L$. Dann auch $\lambda u - \lambda u' \in L$ und damit $\lambda u + L = \lambda u' + L$. $(*)$ genauso.
Die Vektorraumaxiome für U/L folgen leicht aus denen für U. □

3.5. Definition

Mit dieser Vektorraumstruktur heißt U/L der **Quotientenvektorraum** von U durch L.

3.6. Bemerkung

$p(l) = 0 + L$

Der Kern der Projektion $p : U \to U/L$ ist L. Es gibt also zu jedem Unterraum L von U eine surjektive Abbildung mit Kern L. Alternativ könnte man ein Komplement K zu L wählen $U = L \oplus K$ und $p : U \to K$ mit $p(l + k) = k$ betrachten. Diese Alternative ist aber nicht kanonisch, sie erfordert die Wahl von K.

Ist zum Beispiel $f \in \mathrm{End}(U)$ mit $f(L) \subseteq L$, gibt es nicht immer ein Komplement K von L mit $f(K) \subseteq K$. Andererseits induziert f mit $f(L) \subseteq L$ eine lineare Abbildung $F : U/L \to U/L$ mit $F(u + L) = f(u) + L$. Wegen $f(L) \subseteq L$ ist diese wohldefiniert.

3.7. Definition

Seien $L_0 \subseteq U_0$, $L_1 \subseteq U_1$ Unterräume und $f : U_0 \to U_1$ linear mit $f(L_0) \subseteq L_1$. Dann heißt

$$F : U_0/L_0 \to U_1/L_1 \text{ mit } F(u + L_0) := f(u) + L_1$$

die von f **induzierte Abbildung**. F ist wohldefiniert, da $f(L_0) \subseteq L_1$ und linear, da f linear ist.

3.8. Lemma

Seien $L_0 \subseteq U_0, L_1 \subseteq U_1$ Unterräume, $f : U_0 \to U_1$ linear mit $f(L_0) \subseteq L_1$

i) F ist die eindeutige bestimmte lineare Abbildung $F : U_0/L_0 \to U_1/L_1$ für die $F \circ p_0 = p_1 \circ f$ ist, also Abb. 6 kommutiert.

$$\begin{tikzcd}
L_0 \arrow[r, hook] \arrow[d, "f|_{L_0}"'] & U_0 \arrow[r, "p_0"] \arrow[d, "f"'] & U_0/L_0 \arrow[d, "F"] \\
L_1 \arrow[r, hook] & U_1 \arrow[r, "p_1"] & U_1/L_1
\end{tikzcd}$$

Abbildung 6: Kommutierendes Diagramm zu Lemma 3.8

ii) Sind $f|_{L_0} : L_0 \to L_1$ und $F : U_0/L_0 \to U_1/L_1$ bijektiv, so ist auch f bijektiv.

Beweis

i) folgt aus (3.1)

ii) Seien $f|_{L_0}$ und F bijektiv.

f **ist injektiv:** Sei $f(u) = 0$. Dann

$$F\big(p_0(u)\big) = p_1\big(f(u)\big) = p_1(0) = 0$$

Da F bijektiv ist, ist $p_0(u) = 0$. Also $u \in \operatorname{Kern} p_0 = L_0$. Nun ist $f|_{L_0}(u) = f(u) = 0$. Da $f|_{L_0}$ bijektiv ist, folgt $u = 0$.

f **ist surjektiv** Sei $u_1 \in U_1$. Da F surjektiv ist, gibt es $u_0 + L_0 \in U_0/L_0$ mit $F(u_0 + L_0) = u_1 + L_1$. Da $F(u_0 + L_0) = f(u_0) + L_1$ also $u_1 - f(u_0) \in L_1$. Da $f|_{L_0}$ surjektiv ist, gibt es $l_0 \in L_0$ mit $f(l_0) = u_1 - f(u_0)$. Es folgt

$$f(l_0 + u_0) = f(l_0) + f(u_0) = u_1 - f(u_0) + f(u_0) = u_1$$

□

3.9. Satz

Sei $f : V \to W$ linear. Seien $0 = V_0 \subseteq V_1 \subseteq \ldots \subseteq V_r = V$ und $0 = W_0 \subseteq W_1 \subseteq \ldots \subseteq W_r = W$ mit $f(V_i) \subseteq W_i$ für $i = 0, \ldots, r$. Sei $f_i : {}^{V_i}/_{V_{i-1}} \to {}^{W_i}/_{W_{i-1}}$ die durch $f|_{V_i}$ induzierte Abbildung für $i = 1, \ldots, r$.
Sind alle f_i Isomorphismen, so ist auch f ein Isomorphismus.

Beweis
Induktion nach r mittels (3.8) ii)

3.10. Definition

Sei $f \in \mathrm{End}(U)$. Ein Unterraum $L \leqslant U$ mit $f(L) \subseteq L$ heißt f**-stabil** oder f**-invariant**. Es wird dann ein Endomorphismus $F \in \mathrm{End}({}^{U}/_{L})$ induziert.

4. Polynome

4.1. Definition

Sei K ein Körper. Ein formaler Ausdruck der Form

$$p = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

mit $a_n, \ldots, a_0 \in K$ heißt ein **Polynom** mit Koeffizienten in K. Die Menge aller Polynome wird mit $K[X]$ bezeichnet.

Ist $a_n \neq 0$ so sagen wir: p hat den **Grad** $d(p) := n$ und den **Leitkoeffizienten** $l(p) := a_n$. Polynome mit $a_i = 0$ für $i \geqslant 1$ heißen **konstant**. Für das Nullpolynom $0 := (0 \cdot x^n)$ setzen wir $d(0) := -\infty$ und $l(0) := 0$. Ist $l(p) = 1$ so heißt p **normiert** .

4.2. Bemerkung

Durch

$$\lambda \mapsto p(\lambda) := a_n \lambda^n + a_{n-1} \lambda^{n-1} + \ldots + a_1 \lambda + a_0$$

wird eine Abbildung $f_p : K \to K$ definiert. Es gibt aber Beispiele ($K = \mathbb{F}_2, p = X^2 + X$) in denen $p \neq 0$ aber $f_p = 0$. Also sollte man zwischen dem Polynom p und der zugehörigen Funktion f_p unterscheiden.

4.3. Bemerkung

$$0 \cdot X^n = 0$$

4.4. Bemerkung

Durch

$$\left(\sum_{k=0}^{n} a_k X^k\right) + \left(\sum_{k=0}^{n} b_k X^k\right) := \sum_{k=0}^{n} (a_k + b_k) X^k$$

und

$$\left(\sum_{k=0}^{n} a_k X^k\right) \cdot \left(\sum_{l=0}^{m} b_l X^l\right) := \sum_{j=0}^{n+m} \left(\sum_{k+l=j} a_k \cdot b_l\right) X^j$$

wird $K[X]$ zu einem kommutativen Ring. Das Einselement ist das konstante Polynom 1, das Nullelement ist das Nullpolynom 0.

Beispiel
$K = \mathbb{Q}$.

$$(x^2 + x + 4) \cdot (x + 3) = x^3 + 4x^2 + 7x + 12$$

4.5. Bemerkung

Es gelten:

$$\begin{aligned} d(p \cdot q) &= d(p) + d(q) \\ l(p \cdot q) &= l(p) \cdot l(q) \\ d(p + q) &\leqslant \max\{d(p), d(q)\} \end{aligned}$$

4.6. Lemma

$K[X]$ ist nullteilerfrei, d.h. aus $p \cdot q = 0$ folgt $p = 0$ oder $q = 0$.

Beweis

$$p \cdot q = 0 \Longrightarrow -\infty = d(p \cdot q) = d(p) + d(q)$$

$\Rightarrow d(p) = -\infty$ oder $d(q) = -\infty \quad \Rightarrow p = 0$ oder $q = 0$ □

4.7. Division mit Rest

Für $f, g \in K[X], g \neq 0$ gibt es eine eindeutige Darstellung $f = q \cdot g + r$ mit $d(r) < d(g)$.

Beweis
Eindeutigkeit: Sei $f = q_0 g + r_0 = q_1 g + r_1$, $d(r_0), d(r_1) < d(g)$.

$$\Rightarrow (q_0 - q_1)g = r_1 - r_0 \quad d(r_1 - r_0) < d(g)$$

Es folgt $d(q_0 - q_1) = d(r_1 - r_0) = -\infty$, da $d(g) \neq 0$. Also $q_0 = q_1$ und $r_1 = r_0$.

Existenz: Per Induktion nach $d(f)$. Ist $d(f) < d(g)$ so setze $q = 0, r = f$. Sei also $f = aX^{n+k} + \ldots,\ g = bX^n + \ldots$ mit $k \geqslant 0$. Dann hat $f - \frac{a}{b}X^k g$ einen kleineren Grad als f und es gibt per Induktion q_0, r_0 mit $d(r_0) < d(g)$ und

$$\left(f - \frac{a}{b}x^k g\right) = q_0 \cdot g + r_0$$

Dann

$$f = \underbrace{\left(q_0 + \frac{a}{b}x^k\right)}_{:=q} g + r_0$$

Also $f = q \cdot g + r$. □

4.8. Beispiel

schriftliche Division

$$(x^3 - 2x^2 - 4x + 8) = (x^2 + x - 2) \cdot (x - 3) + (x + 2)$$

4.9. Korollar

Ist $\alpha \in K$ eine **Nullstelle** von $p \in K[X]$, d.h. $p(\alpha) = 0$, so gilt

$$p = q \cdot (X - \alpha) \quad \text{mit } q \in K[X]$$

Beweis
Division mit Rest: $p = q(X - \alpha) + r$ mit $d(r) < 1$, also $r \in K$ konstant. Mit Einsetzen folgt

$$0 = p(\alpha) = q(\alpha) \cdot (\alpha - \alpha) + r = r$$

Beispiele:

- $\alpha = 2$ ist Nullstelle von $x^3 - 2x^2 - 4x + 8 = (x + 2)(x - 2)^2$

$$(x^3 - 2x^2 - 4x + 8) : (x - 2) = x^2 - 4 = (x + 2)(x - 2)$$

- $\alpha = \sqrt{2}$ ist Nullstelle von $x^3 + x^2 - 2x - 2 \in \mathbb{R}[K]$

4.10. Bemerkung

Ein Körper K heißt **algebraisch abgeschlossen**, wenn jedes nicht konstante Polynom $p \in K[X]$ eine Nullstelle in K hat. Es folgt dann, dass jedes Polynom ein Produkt von **Linearfaktoren** $(x - \alpha_i)$ und einem konstanten Polynom ist:

$$p = l(p)(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$$

wobei α_i die Nullstellen von p (mit Vielfachheit!) sind. Man sagt p zerfällt in Linearfaktoren.

4.11. Der Euklid'sche Algorithmus

Seien $f_1, f_2 \in K[X]$, beide ungleich 0, mit $d(f_2) \leqslant d(f_1)$. Wiederholte Division mit Rest liefert:

$$\begin{aligned} f_1 &= q_1 \cdot f_2 + f_3 \qquad & d(f_3) < d(f_2) \\ f_2 &= q_2 \cdot f_3 + f_4 \qquad & d(f_4) < d(f_3) \\ f_{n-1} &= q_{n-1} \cdot f_n \end{aligned}$$

Da $d(f_i)$ fällt, muss irgendwann der Rest Null auftreten und der Algorithmus endet.

1)

$$\begin{aligned} 420 &= 33 \cdot 12 + 24 \\ 33 &= 24 \cdot 1 + 9 \\ 24 &= 9 \cdot 2 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= \boxed{3} \cdot 2 \end{aligned}$$

2)

$$\begin{aligned} x^3 - 2x^2 - 4x + 8 &= \big(x^2 + x - 2\big)(x-3) + (x-2) \\ x^2 + x - 2 &= \boxed{(x+2)}(x-1) \end{aligned}$$

4.12. Definition

Sei R ein kommutativer Ring. Seien $r, s \in R$. Wir sagen r teilt s (in Zeichen: $r \mid s$), wenn es $q \in R$ gibt mit $q \cdot r = s$.

4.13. Satz

Seien f_1, f_2 und $d := f_n$ wie in (4.11). Dann gelten:

a) $d \mid f_1$ und $d \mid f_2$

b) Gilt für $g \in K[X]$ $g \mid f_1$ und $g \mid f_2$, so gilt auch $g \mid d$

c) Es gibt $p_1, p_2 \in K[X]$ mit $d = p_1 f_1 + p_2 f_2$

Beweis

a) Es gilt $d \mid f_k$, $d \mid f_{k-1} \Rightarrow d \mid f_{k-2}$. Induktiv folgt, (4.11) aufsteigend, $d \mid f_1$ und $d \mid f_2$

b) Es gilt $g \mid f_k$ und $g \mid f_{k+1} \Longrightarrow g \mid f_{k+2}$. Induktiv folgt, (4.11) absteigend, $g \mid f_n = d$

c) Sei $f_k = v_k f_1 + u_k f_2$ und $f_{k+1} = v_{k+1} f_1 + u_{k+1} f_2$. Dann folgt

$$\begin{aligned} f_{k+2} &= f_k - q_k f_{k+1} \\ &= v_k f_1 + u_k f_2 - q_k v_{k+1} f_1 - q_k u_{k+1} f_2 \\ &= (v_k - q_k v_{k+1}) f_1 + (u_k - q_k u_{k+1}) f_2 \end{aligned}$$

Induktiv, (4.11) absteigend, folgt die Behauptung:

$$\begin{aligned} d &= f_n = p_1 f_1 + p_2 f_2 \\ p_1 &= v_{n-2} - q_{n-2} v_{n-1} \\ p_2 &= u_{n-2} - q_{n-2} u_{n-1} \end{aligned}$$

□

4.14. Bemerkung

Wegen a) und b) nennen wir d einen **größten gemeinsamen Teiler**(ggT) von f_1 und f_2. Er ist eindeutig bis auf Multiplikation mit einem konstanten Polynom ungleich 0.

4.15. Definition

Ein nichtkonstantes Polynom f heißt **irreduzibel**, wenn für jede Faktorisierung $f = g \cdot h$ in $K[X]$ gilt g oder h ist konstant.

die konstanten Polonome sind die Einheiten des Polynomrings

4.16. Satz

Sei f irreduzibel und es gelte $f \mid g \cdot h$. Dann gilt $f \mid g$ oder $f \mid h$.

Beweis

Angenommen $f \nmid g$. Da f irreduzibel ist, ist dann 1 der ggT von f und g. Mit (4.13) c) $\Rightarrow \exists p, q \in K[X]$ mit

$$1 = p \cdot f + q \cdot g$$

Dann $1 \cdot h = h \cdot p \cdot f + h \cdot q \cdot g$. Da $f \mid h \cdot p \cdot f$ und $f \mid h \cdot q \cdot g = q \cdot g \cdot h$ folgt $f \mid h$. □

4.17. Bemerkung

In nullteilerfreien kommutativen Ringen heißen Elemente $p \in R, p \neq 0, p \notin R^\times = \left\{v \in R \,\middle|\, \exists v^{-1} \in R : 1 = v \cdot v^{-1}\right\}$ mit der Eigenschaft $(p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b)$ auch **prim**. ($R^\times$ ist die Menge aller Einheiten auf R)
Wegen (4.16) sind irreduzible Polynome prim.

4.18. Primfaktorzerlegung in $K[X]$

Jedes nichtkonstante Polynom f besitzt eine bis auf die Reihenfolge der Faktoren eindeutige Produktzerlegung als

$$f = a \cdot p_1 \dots p_k \qquad a = l(f),\ l(p_i) = 1,\ p_1, \dots, p_k \text{ irreduzibel}$$

Beweis

Existenz: Eine Produktzerlegung von f kann nicht mehr als $d(f)$ nicht-konstante Faktoren haben. In einer Zerlegung mit maximaler Faktorzahl sind daher alle nichtkonstanten Faktoren irreduzibel. Durch Multiplikation geeigneter Konstanten erreichen wir, dass sie alle normiert sind.

Eindeutigkeit Seien $f = a \cdot p_1 \cdot \ldots \cdot p_k = a \cdot q_1 \cdot \ldots \cdot q_l$ zwei solche Zerlegungen. Da $p_1 \mid f$ folgt mit (4.13), dass es ein j gibt mit $p_1 \mid q_j$. Da q_j irreduzibel ist und p_1 und q_j normiert sind, folgt $p_1 = q_j$. Die Eindeutigkeit folgt nun per Induktion. □

4.19. Definition

Sei $f \in \mathrm{End}_K(V)$ und

$$p = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 = \sum_{k=0}^{n} a_k X^k \in K[X]$$

Dann setzen wir

$$p(f) := a_n f^n + a_{n-1} f^{n-1} + \ldots + a_1 f + a_0 \,\mathrm{id}_V = \sum_{k=0}^{n} a_k f^k \in \mathrm{End}_K(V)$$

4.20. Bemerkung

$$\begin{aligned}(p+q)(f) &= p(f) + q(f)\\ (p \cdot q)(f) &= p(f) \cdot q(f)\\ (c)(f) &= c \cdot \mathrm{id}_V \qquad c \in K[X] \text{ konstant}\end{aligned}$$

4.21. Definition

Sei R ein Ring.

$$\begin{aligned}R[X] &:= \left\{ \sum_{k=0}^{n} r_k X^k \,\middle|\, n \in \mathbb{N}, r_0, \ldots, r_n \in R \right\}\\ R[\![X]\!] &:= \left\{ \sum_{k=0}^{\infty} r_k X^k \,\middle|\, r_0, \ldots, r_n \in R \right\}\\ R[X, X^{-1}] &:= \left\{ \sum_{k=-m}^{n} r_k X^k \,\middle|\, n, m \in \mathbb{N}, r_{-m}, r_{-m+1}, \ldots, r_n \in R \right\}\\ R[\![X]\!][X^{-1}] &:= \left\{ \sum_{k=-m}^{\infty} r_k X^k \,\middle|\, m \in \mathbb{N}, r_{-m}, r_{-m+1}, \ldots, r_n \in R \right\}\end{aligned}$$

werden durch die Multiplikation und Addition aus (4.4) zu Ringen.

$R[X]$	Polynomring über R
$R[\![X]\!]$	Ring der formalen Potenzreihen
$R[X, X^{-1}]$	Ring der Laurent-Polynome
$R[\![X]\!][X^{-1}]$	Ring der formalen Laurent-Reihen

4.22. Bemerkung

$$\left\{ \sum_{k=-\infty}^{\infty} r_k x^k \,\middle|\, r_k \in R \text{ für } k \in \mathbb{Z} \right\}$$

wird nicht durch (4.4) zu einem Ring. Die Multiplikation aus (4.4) ist nicht sinnvoll.

5. Normalformen

5.1. Erinnerung

Matrizen $A_1, A_2 \in K^{n\times n}$ heißen ähnlich (bzw. konjugiert), wenn es $S \in GL(n,K)$ gibt mit $A_1 = SA_2S^{-1}$. Endomorphismen $f_1, f_2 \in \operatorname{End}(V)$ heißen konjugiert, wenn es $\varphi \in GL(V)$ gibt mit $f_1 = \varphi f_2 \varphi^{-1}$.

Sind B_1 und B_2 zwei endliche Basen von V, so sind f_1 und f_2 genau dann konjugiert, wenn $A_1 := m_{B_1}^{B_1}(f_1)$ und $A_2 := m_{B_2}^{B_2}(f_2)$ konjugiert sind. Insbesondere sind $m_{B_1}^{B_1}(f_1)$ und $m_{B_2}^{B_2}(f_2)$ konjugiert.

5.2. Normalformenproblem

Für Matrizen bezüglich Konjugation:

(1) Bestimmung aller Äquivalenzklassen bezüglich Konjugation (=Konjugationsklassen) auf $\mathbb{K}^{n\times n}$.

(2) Bestimmung eines ausgezeichneten (möglichst einfachen) Elements in jeder Konjugationsklasse. Ein solches Element nennen wir dann die **Normalform** für die Konjugationsklasse.

(3) Bestimmung von **Invarianten** für Konjugationsklassen.

(im Bezug auf die Äquivalenz von Matrizen ist dies recht simpel)

5.3. Beispiel

i) $\det : K^{n\times n} \to K$ und $\operatorname{Sp} : K^{n\times n} \to K$ und $\operatorname{rg} : K^{n\times n} \to \mathbb{N}$ sind Invarianten für Konjugationsklassen: Sind A und B konjugiert, so gilt $\det A = \det B$ und $\operatorname{Sp} A = \operatorname{Sp} B$.

ii) Die Menge der Eigenwerte ist ebenfalls invariant unter Konjugation: Ist A_1 konjugiert zu A_2, so gilt
$$\{\lambda \mid \lambda \text{ ist Eigenwert zu } A_1\} = \{\lambda \mid \lambda \text{ ist Eigenwert zu } A_2\}$$

5.4. Bemerkung

Die Invarianten aus (5.3) sind nicht stark genug, um alle Konjugationsklassen zu unterscheiden: $0 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ und $N = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ sind nicht konjugiert, obwohl $\operatorname{Sp} 0 = \operatorname{Sp} N = 0$, $\det 0 = \det N = 0$ und sowohl 0 als auch N nur 0 als Eigenwert haben. (Aber: $\operatorname{rg} = 0 \neq 1 = \operatorname{rg} N$)

5.5. Konjugationsklassen in $\mathbb{C}^{2\times 2}$

Sei $A \in \mathbb{C}^{2\times 2}$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, besitzt A mindestens einen Eigenwert λ. Wir unterscheiden zwei Fälle:

1) A besitzt zwei verschiedene Eigenwerte $\lambda \neq \mu$. Dann ist A diagonalisierbar und damit konjugiert zu $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$. In diesem Fall bestimmt die Menge der Eigenwerte die Konjugationsklasse von A.

2) A besitzt nur λ als Eigenwert: Ergänze einen Eigenvektor v zu einer Basis $B = (v, w)$ von $\mathbb{C}^{2\times 2}$. Dann ist A konjugiert zu $A' := m_B^B(A) = \left(\begin{smallmatrix} \lambda & \alpha \\ 0 & \beta \end{smallmatrix}\right)$. Da β eine Nullstelle des charakteristischen Polynoms ist, ist β ein Eigenwert. Also $\beta = \lambda$. Also auch $A' = \left(\begin{smallmatrix} \lambda & \alpha \\ 0 & \lambda \end{smallmatrix}\right)$.

   Es ergeben sich zwei Unterfälle:

   a) $\alpha = 0$. Dann $A' = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right) = \lambda \cdot I_2$. Da $\lambda \cdot I_2 = S(\lambda \cdot I_2)S^{-1}$ für alle $S \in GL(2,\mathbb{C})$ folgt $A = \lambda \cdot I_2$ und die Konjugationsklasse von A besteht genau aus A.

b) $\alpha \neq 0$. Ist $\lambda \neq 0$, so sei $w' = w - \frac{\alpha}{\lambda} v$. Ist $\lambda = 0$, so sei $w' = \frac{w}{\alpha}$. Mit $B' = (v, w')$ gilt:

$$m_{B'}^{B'}(A) = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

Also ist A konjugiert zu $\left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$.

5.6. Bemerkung

Man kann (5.5) so zusammenfassen: $A, B \in \mathbb{C}^{2\times 2}$ sind genau dann konjugiert wenn:

(i) Eigenwert A = Eigenwert B

(ii) A ist genau dann diagonalisierbar, wenn B diagonalisierbar ist.

Die Matrizen $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$ mit $\lambda, \mu \in \mathbb{C}$ sind die Normalformen für Konjugationsklassen in $\mathbb{C}^{2\times 2}$. Im ersten Fall ist diese Normalform für $\lambda \neq \mu$ nicht ganz eindeutig da $\left(\begin{smallmatrix} \lambda & \\ & \mu \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} \mu & \\ & \lambda \end{smallmatrix}\right)$

5.7. Beispiel

$$\begin{aligned}
\det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= 1 = \det \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
\mathrm{Sp} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= 2 = \mathrm{Sp} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
\mathrm{rg} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= 2 = \mathrm{rg} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
\text{EW von } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \{1\} = \text{ EW von } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

Aber $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ sind nicht konjugiert. (warum?)

6. Charakteristisches Polynom

6.1. Bemerkung

Die Determinante $\det : K^{n\times n} \to K$ lässt sich durch dieselbe Formel wie über einen Körper auch für Matrizen über einen kommutativen Ring erklären: $\det_R R^{n\times n} \to R$. Es gilt:

(i) $\det_R(I_n) = 1$

(ii) $\det_R(A \cdot B) = \det_R A \cdot \det_R B$

analog: $\det A$ *ist eine Einheit*

(iii) $A \in R^{n\times n}$ ist invertierbar $\iff$ $\det_R A \in R$ ist invertierbar.

6.2. Definition

Sei $A \in K^{n\times n}$. Dann ist $(X \cdot I_n - A) \in K[X]^{n\times n}$. Das Polynom

$$\chi_A := \det_{K[X]}(X \cdot I_n - A) \in K[X]$$

heißt das **charakteristische Polynom** von A. χ_A ist ein normiertes Polynom vom Grad n.

6.3. Bemerkung

Es gilt für $\lambda \in K$

$$\chi_A(\lambda) = \det_K(\lambda \cdot I_n - A) \in K$$

Insbesondere gilt: Die Eigenwerte von A sind genau die Nullstellen von χ_A.

6.4. Bemerkung

Sei $A \in K^{n\times n}, S \in GL(n,K)$. Die charakteristischen Polynome konjugierter Matrizen stimmen überein:

$$\begin{aligned}\chi_{SAS^{-1}} = \det_{K[X]}\left(X \cdot I_n - SAS^{-1}\right) = \det_{K[X]}\left(SXI_nS^{-1} - SAS^{-1}\right) &= \det_{K[X]}\left(S \cdot (X \cdot I_n - A)S^{-1}\right)\\ &= \det_K S \cdot \det_{K[X]}(X \cdot I_n - A) \cdot \det_K S^{-1}\\ &= \det_{K[X]}(X \cdot I_n - A) = \chi_A\end{aligned}$$

6.5. Definition

Sei V ein endlich dimensionaler Vektorraum. Sei $f \in \operatorname{End}(V)$ und B eine Basis von V. Dann hängt $\chi_f := \chi_{m_B^B(f)}$ nur von f und nicht von der Wahl von B ab und heißt das charakteristische Polynom von f.

6.6. Bemerkung

Die Nullstellen von χ_f sind genau die Eigenwerte von f.

6.7. Bemerkung

Ist $A = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, so

$$\chi_A = \det_{K[X]} \begin{pmatrix} (x-\lambda_1) & & \\ & (x-\lambda_2) & \\ & & (x-\lambda_n) \end{pmatrix} = (x-\lambda_1) \cdot \ldots \cdot (x-\lambda_n)$$

Insbesondere zerfällt χ_A in Linearfaktoren. Es gilt: Die Dimension von $V(\lambda) = \{v \in K^n \mid A \cdot v = \lambda \cdot v\}$ (Eigenraum zum Eigenwert λ) ist genau die Vielfachheit von $(x - \lambda)$ in χ_A.

6.8. Satz

Sei $A \in K^{n \times n}$. Dann sind äquivalent:

(1) A ist diagonalisierbar.

(2) $\chi_A = (x-\lambda_1)^{n_1} \ldots (x-\lambda_k)^{n_k}$, $\lambda_i \neq \lambda_j$ für $i \neq j$, zerfällt in Linearfaktoren und es gilt: $\dim V(\lambda_i) = n_i$ für $i = 1, \ldots, k$.

Beweis

(1) $\Rightarrow$ (2) folgt aus (6.7) und (6.4)

(2) $\Rightarrow$ (1) [3] Es ist $n = \text{Grad}\, \chi_A = \sum_{i=1}^k n_i$. Es ist immer $V(\lambda_1) + \ldots + V(\lambda_k) = V(\lambda_1) \oplus \ldots \oplus V(\lambda_k)$. Also $\dim(V(\lambda_1) \oplus \ldots \oplus V(\lambda_k)) = \sum_{i=1}^k n_i = n = \dim V$. Es folgt

$$V = V(\lambda_1) \oplus \ldots \oplus V(\lambda_k) \qquad \square$$

6.9. Beispiel

Sei $A = \left(\begin{smallmatrix} \lambda_1 & 0 \\ * & \lambda_n \end{smallmatrix}\right)$ eine untere Dreiecksmatrix. Dann ist $\chi_A = (x-\lambda_1) \cdot \ldots \cdot (x-\lambda_n)$.

6.10. Satz

Sei $f \in \operatorname{End}(V)$, $\dim(V) < \infty$. Dann sind äquivalent:

(1) χ_f zerfällt in Linearfaktoren

(2) Es existiert eine Basis B, so dass $m_B^B(f)$ eine untere Dreieckmatrix ist.

Beweis

(2)$\Rightarrow$(1) siehe (6.9)

(1)$\Rightarrow$(2) Sei $\chi_f = (x-\lambda_1) \ldots (x-\lambda_n)$. Sei b ein Eigenvektor zum Eigenwert λ_1. Dann ist $U := \langle b \rangle$ f-invariant. Sei $F : {}^{V}\!/_{U} \to {}^{V}\!/_{U}$ von f induziert. Dann zerfällt auch χ_F als Faktor von χ_f auch in Linearfaktoren. Per Induktion nach $\dim V$ gibt es eine Basis $\overline{B} = (b_1 + U, \ldots, b_{n-1} + U)$ von ${}^{V}\!/_{U}$, so dass $m_{\overline{B}}^{\overline{B}}(F)$ eine untere Dreiecksmatrix ist. Dann ist $B = (b_1, \ldots, b_{n-1}, b)$ die gesuchte Basis:

$$m_B^B(f) = \begin{pmatrix} m_{\overline{B}}^{\overline{B}}(F) & 0 \\ * - * & \lambda \end{pmatrix} \qquad \square$$

[3] Wiederholung LA I: $\operatorname{End}(V) \ni f$ diagonalisierbar $\Leftrightarrow \bigoplus_{\lambda \in \Lambda} V(\lambda) = V$

6.11. Satz

Sei $f \in \mathrm{End}(V)$, $\dim(V) < \infty$. Sei U ein f-invarianter Unterraum von V. Sei $f|_U : U \to U$ die Einschränkung von f auf U und $F : {}^V/_U \to {}^V/_U$ durch f induziert. Dann gilt:

$$\chi_f = \chi_{f|_U} \cdot \chi_F$$

Beweis
Wir ergänzen eine Basis $B_0 = (b_1, \ldots, b_k)$ von U zu einer Basis $B = (b_1, \ldots, b_k, b_{k+1}, \ldots, b_n)$ von V. Dann

$$m_B^B(f) = \begin{pmatrix} m_{B_0}^{B_0}(f|_U) & * \\ 0 & m_{B_1}^{B_1}(F) \end{pmatrix}$$

wobei $B_1 = (b_{k+1} + U, \ldots, b_n + U)$ die von $b_{k+1}, \ldots, b_n$ induzierte Basis von ${}^V/_U$ ist. Es folgt

$$\begin{aligned} \chi_f &= \det\bigl(X \cdot I_n - m_B^B(f)\bigr) = \det \begin{pmatrix} X \cdot I_k - m_{B_0}^{B_0}(f|_U) & -* \\ 0 & X \cdot I_{n-k} - m_{B_1}^{B_1}(F) \end{pmatrix} \\ &= \det_{K[X]}\Bigl(X \cdot I_k - m_{B_0}^{B_0}(f|_U)\Bigr) \cdot \det_{K[X]}\Bigl(X \cdot I_{n-k} - m_{B_1}^{B_1}(F)\Bigr) \\ &= \chi_{f|_U} \cdot \chi_F \end{aligned}$$

□

6.12. Lemma

Sei $f \in \mathrm{End}(V)$ und $v \in V$. Dann ist der Unterraum $L(v, f) := \langle v, f(v), f^2(v), \ldots \rangle$ f-invariant.

Beweis
Für $w = \sum_{i=0}^n \lambda_i f^i(v) \in L(v, f)$ ist

$$f(w) = f\left(\sum_{i=0}^n \lambda_i f^i(v)\right) = \sum_{i=0}^n \lambda_i f^{i+1}(v) \in L(v, f)$$

□

6.13. Definition

$f \in \mathrm{End}(V)$ heißt **zyklisch**, falls es $v \in V$ gibt mit $V = L(v, f)$.

6.14. Lemma

Sei $f \in \mathrm{End}(V)$ und $v \in V$. Sei $n = \dim L(v, f) < \infty$. Dann gilt:

(1) $B = \bigl(v, f(v), \ldots, f^{n-1}(v)\bigr)$ ist eine Basis von $L(v, f)$.

(2) Ist $f^n(v) = \sum_{i=0}^{n-1} \lambda_i f^i(v)$, so ist

$$m_B^B(f|_{L(v,f)}) = \begin{pmatrix} 0 & & & \lambda_0 \\ 1 & \ddots & & \lambda_1 \\ & \ddots & 0 & \vdots \\ & & 1 & \lambda_{n-1} \end{pmatrix}$$

und $\chi_f = X^n - \lambda_{n-1} X^{n-1} - \ldots - \lambda_1 X - \lambda_0$

Beweis

(1) Sei k minimal mit $f^k(v) \in \langle v, \dots, f^{k-1}(v)\rangle =: U$. Dann ist U f-invariant und daher $f^l(v) \in U$ für alle l. Also $L(v,f) = U$. Da k minimal ist, ist $v, f^1, \dots, f^{k-1}$ linear unabhängig. Es folgt $k = n$ und die Behhauptung. □

(2) Die behauptete Gestalt von $m_B^B(f|_{L(v,f)})$ folgt direkt aus der Definition. Die Formel für χ_f folgt mit der Entwicklung der ersten Spalte und Induktion. □

6.15. Definition

Ein Endomorphismus $f \in \mathrm{End}(V)$ heißt **nilpotent**, wenn es $N \in \mathbb{N}$ gibt mit $f^N = 0$

6.16. Bemerkung

Ist in (6.14)(2) $V = L(v,f)$ und $f^n(v) = 0$, dann ist f nilpotent (mit $n = N$) und $\chi_f = x^n$

Beispiel
$A \in K^{n\times n}$ A^N =0

(1) $A = 0$ $N = 1\surd$

(2)

$$\begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix} = \begin{pmatrix} 0 & & & 0 \\ 0 & \ddots & & \\ & \ddots & \ddots & \\ * & & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix}^n = 0$$

untere (bzw. obere) Dreiecksmatrizen mit 0 auf der Diagonalen sind nilpotent.

(3) A nilpotent, $S \in GL(n,k)$ und $A^N = 0$. Dann

$$(SAS^{-1})^N = SAS^{-1} \cdot SAS^{-1} \cdot \ldots \cdot SAS^{-1} = SA^N S^{-1} = 0$$

6.17. Definition

Sei $f \in \mathrm{End}(V)$ nilpotent. Das kleinste $k \in \mathbb{N}$ mit $f^k(v) = 0$ heißt die **Stufe** von v bezüglich f.

6.18. Lemma

Sei $f \in \mathrm{End}(V)$ nilpotent und $v \in V$ von maximaler Stufe bezüglich f. Ist $V \neq L(v,f)$ so gibt es $u \in V \setminus L(v,f)$ mit $f(u) = 0$.

Beweis
Sei $x \in V \setminus L(v,f)$. Da f nilpotent ist, gibt es ein minimales k mit $f^k(x) \in L(v,f)$. Indem wir x durch $f^{k-1}(x)$ ersetzen, erhalten wir $x \in V \setminus L(v,f)$ mit $f(x) \in L(v,f)$. Da $L(v,f) = \langle v, f(v), f^2(v), \dots\rangle$ gibt es $\lambda \in K$ und $y \in L(v,f)$ mit $f(x) = \lambda v + f(y)$. Es folgt $f^k(x) = \lambda f^{k-1}(v) + f^k(y)$.

Sei nun k die Stufe von v. Da k die maximale Stufe ist, folgt $f^k(x) = 0 = f^k(y)$. Es folgt $\lambda f^{k-1}(v) = 0$. Da k die Stufe von v ist, ist $f^{k-1}(v) \neq 0$. Also $\lambda = 0$. Es folgt $f(x) = f(y)$, also $u = x - y \in \mathrm{Kern}\, f$. Da $x \notin L(v,f)$, $y \in L(v,f)$ folgt $u = x - y \notin L(v,f)$. □

6.19. Satz

Sei $\dim V < \infty$, $f \in \mathrm{End}(V)$ nilpotent. Sei $v \in V$ von maximaler Stufe bezüglich f. Dann besitzt $L(v, f)$ ein f-invariantes Komplement.

Beweis
Sei U ein maximaler f-invarianter Unterraum von V mit $U \cap L(v, f) = \{0\}$. Sei $F \in \mathrm{End}(V/U)$ mit $F(v + U) = f(v) + U$. Dann ist $\overline{v} := v + U$ ein Vektor maximaler Stufe bezüglich F.
Annahme: $L(\overline{v}, F) \subsetneq V/U$. Dann gibt es nach (6.18) $\overline{u} \in V/U$ mit $\overline{u} \in V/U \setminus L(\overline{v}, F)$ mit $F(\overline{u}) = 0$. Sei $u \in V$ mit $\overline{u} = u + U$. Dann $f(u) \in U$, da $F(\overline{u}) = 0$. Insbesondere ist $U^+ := \langle U, u\rangle$ f-invariant.
Wegen $\overline{u} \in V/U \setminus L(\overline{v}, F)$ und $U \cap L(v, f) = 0$ ist auch $U^+ \cap L(v, f) = 0$ (Denn: $\lambda u + \tilde{u} \in L(v, f)$, $\lambda \in K, \tilde{u} \in U$)

$$\Rightarrow \lambda u \in L(\overline{v}, F) \Rightarrow \lambda = 0 \to \tilde{u} \in L(v, f) \cap U = 0$$

↯ zur Maximalität von U. Es folgt $L(\overline{v}, F) = V/U (\star)$.
Wir müssen nur zeigen: $V = U + L(v, f)$
Sei nun $w \in V$. Wegen $(\star)$ gibt es $\lambda_0, \dots, \lambda_n \in K$ mit

$$\begin{aligned} w + U &= (\lambda_0 v + U) + (\lambda_1 f(v) + U) + \ldots + (\lambda_n f^n(v) + U) \\ &= \underbrace{\Big(\lambda_0 v + \lambda_1 f(v) + \ldots + \lambda_n f^n(v)\Big)}_{=: x \in L(v,f)} + U \end{aligned}$$

Aus $w + U = x + U$ folgt $w - x \in U$. Also $w = (w - x) + x \in U + L(v, f)$. □

6.20. Satz

Sei $f \in \mathrm{End}(V)$ nilpotent und $\dim V < \infty$. Dann gibt es eine Zerlegung $V = V_1 \oplus \ldots \oplus V_r$ in f-invariante zyklische Unterräume $V_i = L(v_i, f)$.

Beweis
Induktion nach $\dim V$. Induktionsschritt: (6.19) □

6.21. Lemma

Sei $f \in \mathrm{End}(V)$ nilpotent und $\dim V = n$. Dann gilt $f^n = 0$.

Beweis
Sei N minimal mit $f^N = 0$. Betrachte

$$0 = \mathrm{Kern}\, f^0 \subseteq \mathrm{Kern}\, f^1 \subseteq \mathrm{Kern}\, f^2 \subseteq \ldots \subseteq \mathrm{Kern}\, f^N = V$$

Wegen de Minimalität von N ist $\mathrm{Kern}\, f^{N-1} \subsetneq \mathrm{Kern}\, f^N$.
Angenommen: $\mathrm{Kern}\, f^i = \mathrm{Kern}\, f^{i+1}$. Dann folgt auch $\mathrm{Kern}\, f^{i+1} = \mathrm{Kern}\, f^{i+2}$: Sei $v \in \mathrm{Kern}\, f^{i+2} \Longrightarrow f(v) \in \mathrm{Kern}\, f^{i+1} = \mathrm{Kern}\, f^i$. Also

$$f^{i+1}(v) = f^i(f(v)) = 0 \Rightarrow v \in \mathrm{Kern}\, f^{i+1}$$

Da $\mathrm{Kern}\, f^{N-1} \subsetneq \mathrm{Kern}\, f^N$ folgt:

$$0 = \mathrm{Kern}\, f^0 \subsetneq \mathrm{Kern}\, f^1 \subsetneq \mathrm{Kern}\, f^2 \subsetneq \ldots \subsetneq \mathrm{Kern}\, f^N = V$$

Es folgt $0 < \dim \mathrm{Kern}\, f < \dim \mathrm{Kern}\, f^2 < \ldots < \dim \mathrm{Kern}\, f^N = \dim V = n$. Daher $N \leqslant n$. □

6.21.1. Bemerkung

i) Sei $f \in \mathrm{End}(V)$ nilpotent und zyklisch mit $V = L(v, f)$ und $\dim V = n$. Für die Basis $B = (v, f(v), \ldots, f^{n-1}(v))$ gilt dann

$$m_B^B(f) = \begin{pmatrix} 0 & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}$$

ii) Sei $f \in \mathrm{End}(V)$ nilpotent, $\dim V < \infty$. Mit (6.20) folgt: $\exists$ Basis B mit

$$m_B^B(f) = \begin{pmatrix} \boxed{\begin{matrix} 0 & & \\ 1 & \diagdown & \\ & \diagdown 1 & 0 \end{matrix}} & & \\ & \diagdown & \\ & & \boxed{\begin{matrix} 0 & & \\ 1 & \diagdown & \\ & \diagdown 1 & 0 \end{matrix}} \end{pmatrix}$$

Die Kästen heißen **Jordankästen**. Sie entsprechen genau den V_i aus (6.20).

6.22. Definition

Eine Matrix $A = (a_{ij}) \in K^{n \times n}$ heißt eine **strikte obere Dreiecksmatrix**, wenn $a_{ij} = 0$ für $i \leqslant j$. „$\leqslant$" !!!

6.23. Bemerkung

Ist $A \in K^{n \times n}$ eine strikte obere Dreiecksmatrix, so gilt $A^n = 0$ (siehe auch 6.16 Beispiel)

6.24. Satz

Sei $f \in \mathrm{End}(V)$, $\dim V = n < \infty$. Dann sind äquivalent:

(1) f ist nilpotent

(2) $\exists$ Basis B, so dass $m_B^B(f)$ eine strikte untere Dreiecksmatrix ist.

(3) $\chi_f = X^n$

Beweis

(1)⇒(2): (6.21.1) ii))

(2)⇒(1): (6.23)

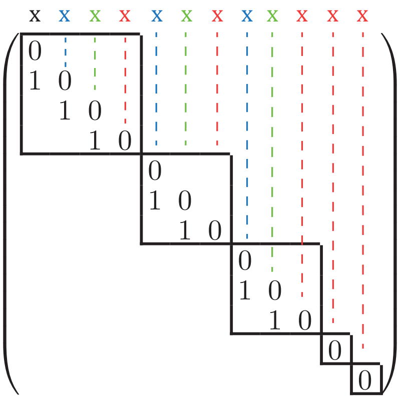
(2)⇒(3): Sei $m_B^B(f)$ eine strikte untere Dreiecksmatrix. Dann $\chi_f = \det_{K[X]}\left(X \cdot I_n - m_B^B(f)\right) = X^n$

(3)⇒(2): Ist $\chi_f = X^n$, so zerfällt χ_f insbesondere in Linearfaktoren. Nach (6.10) gibt es eine Basis B so dass $m_B^B(f) = \left(\begin{smallmatrix} \lambda_1 & 0 \\ * & \lambda_n \end{smallmatrix}\right)$ eine untere Dreiecksmatrix ist. Es ist

$$X^n = \chi_f = \chi_{m_B^B(f)} = \det_{K[X]} \begin{pmatrix} x - \lambda_1 & & 0 \\ & \diagdown & \\ -* & & x - \lambda_n \end{pmatrix} = (x - \lambda_1) \ldots (x - \lambda_n)$$

Also ist $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$ $\square$

Abbildung 7: Beispiel eines nilpotenten Endomorphimus



$$
\begin{aligned}
\operatorname{Kern} f &= \text{Eigenraum zum Eigenwert } 0 \\
&= \langle xxxxx \rangle \\
\operatorname{Kern} f^2 &= \langle xxxxxxxx \rangle \\
\operatorname{Kern} f^3 &= \langle xxxxxxxxxxx \rangle \\
\operatorname{Kern} f^4 &= \langle xxxxxxxxxxxx \rangle
\end{aligned}
$$

7. Die Jordansche Normalform

7.1. Bemerkung

Sei $f \in \operatorname{End}(V)$ und $\lambda \in K$ ein Eigenwert von f. Für $t \in \mathbb{N}$ sei $V^t(\lambda) := \operatorname{Kern}(f - \lambda \operatorname{id})^t$. Dann ist

$$0 = V^0(\lambda) \subseteq V^1(\lambda) \subseteq V^2(\lambda) \subseteq V^3(\lambda) \subseteq \dots$$

$$W_\lambda := \bigcup_{t=0}^{\infty} V^t(\lambda)$$

heißt der **verallgemeinerte Eigenraum** von f zum Eigenwert λ. Ist $\dim V < \infty$, so gibt es ein minimales $k \geqslant 1$ mit $V^l(\lambda) = V^k(\lambda)$ für alle $l \geqslant k$. Dann $W_\lambda = V^k(\lambda)$.

7.2. Lemma

W_λ ist f-invariant. λ ist der einzige Eigenwert von $f|_{w_\lambda}$

Beweis
Da $(f - \lambda) \circ f = f \circ (f - \lambda)$ ist auch $(f - \lambda)^t \circ f = f \circ (f - \lambda)^t$. Ist $v \in V^t(\lambda)$, so ist

$$(f - \lambda)^t\big(f(v)\big) = f\big(\underbrace{(f - \lambda)^t(v)}_{=0 \text{ da } v \in V^t(\lambda)}\big) = 0 \quad \Longrightarrow f(v) \in V^t(\lambda)$$

Es sind also sogar alle $V^t(\lambda)$ f-invariant. Sei nun μ ein Eigenwert von $f|_{W_\lambda}$, also $f(w) = \mu \cdot w$ mit $w \in W_\lambda, w \neq 0$. Dann $(f - \lambda)(w) = (\mu - \lambda) \cdot w$ und damit $(f - \lambda)^t(w) = (\mu - \lambda)^t \cdot w$. Da $w \in W_\lambda$ gibt es k mit $(f - \lambda)^k(w) = 0$. Es folgt

$$0 = (\mu - \lambda)^k(w) \overset{w \neq 0}{\Longrightarrow} (\mu - \lambda)^k = 0 \Rightarrow \mu - \lambda = 0 \Rightarrow \mu = \lambda \qquad \square$$

7.3. Satz

Sei $f \in \mathrm{End}(V)$, $\dim V < \infty$, λ ein Eigenwert von f. Sei $f_\lambda := f|_{W_\lambda}$. Dann existiert eine Basis B von W_λ mit

$$m_B^B(f_\lambda) = \begin{pmatrix} \boxed{\begin{matrix} \lambda & & \\ 1 & \ddots & \\ & \ddots 1 & \lambda \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} \lambda & & \\ 1 & \ddots & \\ & \ddots 1 & \lambda \end{matrix}} \end{pmatrix}$$

Beweis
$g := (f_\lambda - \lambda)$ ist auf W_λ nilpotent, da $W_\lambda = \mathrm{Kern}(f-\lambda)^k$ für ein geeignet großes k. Nach (6.21.1) (i) gibt es eine Basis B, so dass $m_B^B(g)$ die obige Form mit $\lambda = 0$ hat. Nun ist $m_B^B(f_\lambda) = m_B^B(g+\lambda) = m_B^B(g) + m_B^B(\lambda) = m_B^B(g) + \lambda \cdot I_n$ mit $n = \dim W_\lambda$. Also

$$m_B^B(f_\lambda) = \begin{pmatrix} \boxed{\begin{matrix} 0 & & \\ 1 & \ddots & \\ & \ddots 1 & 0 \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} 0 & & \\ 1 & \ddots & \\ & \ddots 1 & 0 \end{matrix}} \end{pmatrix} + \begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix} = \begin{pmatrix} \boxed{\begin{matrix} \lambda & & \\ 1 & \ddots & \\ & \ddots 1 & \lambda \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} \lambda & & \\ 1 & \ddots & \\ & \ddots 1 & \lambda \end{matrix}} \end{pmatrix}$$ □

7.4. Lemma

Sei $f \in \mathrm{End}(V)$, $\dim V < \infty$. Sei λ ein Eigenwert von f. Dann teilt $(X-\lambda)^k$ genau dann das charakteristische Polynom χ_f, wenn $k \leqslant \dim W_\lambda$.

Beweis
Sei $F : V/W_\lambda \to V/W_\lambda$ von f induziert. Nach (6.11) gilt: $\chi_f = \chi_{f|_{W_\lambda}} \cdot \chi_F$. Wegen (7.3) ist $\chi_{f|_{W_\lambda}} = (X-\lambda)^n$ mit $n = \dim W_\lambda$. Insbesondere gilt $\chi_f = (X-\lambda)^n \cdot \chi_F$.

Es bleibt zu zeigen: $(X-\lambda) \nmid \chi_F$, also $\chi_F(\lambda) \neq 0$. Angenommen doch: $\chi_F(\lambda) = 0$. Dann ist λ Eigenwert von F. Sei $\overline{v} = v + W_\lambda \in V/W_\lambda$ ein zugehöriger Eigenvektor. Also $f(v) + W_\lambda = F(\overline{v}) = \lambda\overline{v} = \lambda v + W_\lambda$. Also auch $w := f(v) - \lambda v \in W_\lambda$. Sei nun $k \in \mathbb{N}$ mit $(f-\lambda)^k(w') = 0 \, \forall w' \in W_\lambda$. Insbesondere $(f-\lambda)^k(w) = 0$. Dann ist

$$(f - \lambda\,\mathrm{id})^{k+1}(v) = (f-\lambda\,\mathrm{id})^k(w) = 0 \qquad \text{also } v \in W_\lambda$$

Es folgt $\overline{v} = v + W_\lambda = 0$ ↯ zu $\overline{v}$ ist Eigenvektor (also $\neq 0$) □

7.5. Lemma

Sei $f \in \mathrm{End}(V)$, $\dim V < \infty$. Sei Λ die Menge der Eigenwerte von f. Für alle $\lambda \in \Lambda$ gilt dann:

$$W_\lambda \cap \sum_{\substack{\mu \in \Lambda \\ \mu \neq \lambda}} W_\mu = 0$$

Beweis
Wähle n_μ mit $W_\mu = \operatorname{Kern}(f-\mu)^{n_\mu}$. Da $(X-\lambda)^{n_\lambda}$ und $\prod_{\mu\neq\lambda,\mu\in\Lambda}(X-\mu)^{n_\mu}$ teilerfremd sind, gibt es Polynome $p_1, p_2 \in K[X]$ mit

$$1 = p_1 \cdot (X-\lambda)^{n_\lambda} + p_2 \prod_{\substack{\mu\neq\lambda\\ \mu\in\Lambda}} (X-\mu)^{n_\mu}$$

Es folgt (durch Einsetzen von f).

$$\mathrm{id} = \underbrace{p_1(f)\circ(f-\lambda\,\mathrm{id})^{n_\lambda}}_{=:f_1} + \underbrace{p_2(f)\circ\prod_{\mu\neq\lambda,\mu\in\Lambda}(f-\mu\,\mathrm{id})^{n_\mu}}_{=:f_2}$$

Es ist $f_1(w) = 0\,\forall w\in W_\lambda = \operatorname{Kern}(f-\lambda)^{n_\lambda}$. Da $(f-\mu)(f-\mu') = (f-\mu')(f-\mu)$ gilt $f_2(w) = 0$ für alle $w \in \sum_{\mu\neq\lambda,\mu\in\Lambda} W_\mu$. Es folgt $W_\lambda \cap \sum_{\mu\neq\lambda} W_\mu = 0$, da $f_1 + f_2 = \mathrm{id}$. □

7.6. Satz

Sei $f\in\operatorname{End}(V)$, $\dim V < \infty$. Sei Λ die Menge der Eigenwerte von f. Weiter zerfalle χ_f in Linearfaktoren. Dann gilt

$$V = \bigoplus_{\lambda\in\Lambda} W_\lambda \;,\quad \chi_f = \prod_{\lambda\in\Lambda}(X-\lambda)^{n_\lambda} \qquad \text{mit } n_\lambda = \dim W_\lambda$$

Beweis
Es ist $\chi_f = \prod_{\lambda\in\Lambda}(X-\lambda)^{m_\lambda}$ für geeignete $m_\lambda \geqslant 1$. Wegen (7.4) ist $m_\lambda = n_\lambda = \dim W_\lambda$. Wegen (7.5) ist $\sum_{\lambda\in\Lambda} W_\lambda = \bigoplus_{\lambda\in\Lambda} W_\lambda$. Da

$$\dim V = d(\chi_f) = \sum_{\lambda\in\Lambda} n_\lambda = \dim \bigoplus_{\lambda\in\Lambda} W_\lambda$$

folgt $V = \bigoplus_{\lambda\in\Lambda} W_\lambda$. □

7.7. Jordansche Normalform

Sei $f\in\operatorname{End}(V)$, $\dim V<\infty$. χ_f zerfalle in Linearfaktoren. Dann gibt es eine Basis B von V mit

$$m_B^B(f) = \begin{pmatrix} \boxed{K_1} & & & \\ & \boxed{K_2} & & \\ & & \ddots & \\ & & & \boxed{K_r} \end{pmatrix}$$

wobei jedes $K_i = \boxed{\begin{matrix} \lambda_i & & \\ 1 & \ddots & \\ & \ddots\,1 & \lambda_i \end{matrix}}$ ein Jordankasten ist. Jeder Eigenwert taucht mindestens einmal als Eigenwert eines der K_i auf.

Beispiel

$$A = \begin{pmatrix} 2 & 1 & 0\\ 0 & 2 & 0\\ 0 & 4 & 2\end{pmatrix} \qquad \chi_A = \det_{K[X]}\begin{pmatrix} X-2 & -1 & 0\\ 0 & X-2 & 0\\ 0 & -4 & X-2\end{pmatrix} = (X-2)^3$$

Mögliche Jordansche Normalform für A:

$$J_1 = \begin{pmatrix} 2 & & \\ 1 & 2 & \\ & 1 & 2 \end{pmatrix} \qquad J_2 = \begin{pmatrix} 2 & & \\ 1 & 2 & \\ & & 2 \end{pmatrix} \qquad J_3 = \begin{pmatrix} 2 & & \\ & 2 & \\ & & 2 \end{pmatrix}$$

Eigenraum von J_1 zum Eigenwert 2 hat die Dimension: $\dim \operatorname{Kern}(2I_3 - J_1) = \dim \operatorname{Kern} \begin{pmatrix} 0 & & \\ -1 & 0 & \\ & -1 & 0 \end{pmatrix} = 1$

Eigenraum von J_2 zum Eigenwert 2 hat die Dimension: $\dim \operatorname{Kern}(2I_3 - J_2) = \dim \operatorname{Kern} \begin{pmatrix} 0 & & \\ -1 & 0 & \\ & & 0 \end{pmatrix} = 2$

Also ist J_2 die Jordansche Normalform von A.

Frage

Seien $A, B \in K^{n \times n}$ mit $\chi_A = \chi_B$ $\forall$ Eigenwerte λ ist $\dim V_\lambda(A) = \dim V_\lambda(B)$. Sind dann A und B konjugiert? (bzw. sind die Jordanschen Normalformen gleich)

Nein! Betrachte $A = \begin{pmatrix} 2 & & & \\ 1 & 2 & & \\ & & 2 & \\ & & 1 & 2 \end{pmatrix}$ und $B = \begin{pmatrix} 2 & & & \\ 1 & 2 & & \\ & 1 & 2 & \\ & & & 2 \end{pmatrix}$ Es gilt

$$(B - 2 \cdot I_4)^2 = \begin{pmatrix} 0 & 0 & 0 & \\ 0 & 0 & 0 & \\ 1 & 0 & 0 & \\ & & & 0 \end{pmatrix} \neq 0 \qquad \text{aber} \qquad (A - 2 \cdot I_4)^2 = \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & & 0 & \\ & & 1 & 0 \end{pmatrix}^2 = 0$$

7.8. Proposition

Seien $f, g \in \operatorname{End}(V)$ mit $fg = gf$. Dann gilt

$$(f+g)^n = \sum_{k=0}^{n} \binom{n}{k} f^k g^{n-k}$$

Beweis

Für die Binomialkoeffizienten

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!}, & \text{falls } 0 \leqslant k \leqslant n \\ 0, & \text{sonst} \end{cases}$$

gilt $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. Die Aussage folgt per Induktion:

$$\begin{aligned} (f+g)^{n+1} = (f+g) + (f+g)^n = (f+g) \sum_{k=0}^{n} \binom{n}{k} f^k g^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} f^{k+1} g^{n-k} + \sum_{k=0}^{n} \binom{n}{k} f^k gn - k + 1 \\ &= \sum_{k=0}^{n+1} \binom{n}{k-1} f^k g^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} f^k g^{n+1-k} \\ &= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k} \right) f^k g^{n+1-k} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} f^k g^{n+1-k} \end{aligned}$$

$\square$

7.9. Jordan-Chevalley-Zerlegung

Sei $f \in \operatorname{End}(V), \dim V < \infty$, χ_f zerfalle in Linearfaktoren. Dann gibt es eine eindeutige Zerlegung $f = h + n$ mit

1) h ist diagonalisierbar
2) n ist nilpotent
3) $hn = nh$

Beweis
Existenz: folgt aus (7.7)

Eindeutigkeit: Behauptung: Für $\lambda \in K$ gilt $(\star)$ $W_\lambda(f) = V_\lambda(h)$. Sei $v \in V_\lambda(h)$, also $h(v) = \lambda v$. Dann gilt:

$$(h+n-\lambda)^N(v) = \big(n+(h-\lambda)\big)^N(v) = \sum_{k=0}^{N} \binom{N}{k} n^k (h-\lambda)^{N-k}(v) \overset{h(v)=\lambda v}{=} n^N \cdot (h-\lambda)^0(v) = n^N(v)$$

Da n nilpotent ist, gibt es ein N mit $n^N = 0$. Es folgt $(f-\lambda)^N(v) = (h+n-\lambda)^N(v) = 0$ für dieses N. Also $v \in W_\lambda(f)$. Da

$$\bigoplus_{\lambda\in\Lambda} W_\lambda(f) = V \underset{h \text{ diagonalisierbar}}{=} \bigoplus_{\lambda\in\Lambda} V_\lambda(h)$$

folgt nun aus $V_\lambda(h) \subseteq W_\lambda(f)$ schon $V_\lambda(h) = W_\lambda(f)$. Sei nun $f = h' + n'$ eine zweite Zerlegung mit 1)-3). Dann

$$V_\lambda(h) = W_\lambda(f) = V_\lambda(h') \quad \text{wegen } (\star)$$

Da h und h' diagonalisierbar sind, folgt $h = h'$. Dann folgt auch $n = f - h = f - h' = n'$. $\square$

7.10. Definition

Ein Endomorphismus der Form $f = \operatorname{id} + n$ mit n nilpotent heißt **unipotent**.

7.11. Bemerkung

Ist $f = \operatorname{id} + n$ unipotent mit $n^N = 0$, so ist f invertierbar mit

$$f^{-1} = \operatorname{id} - n + n^2 - n^3 + \ldots = \sum_{k=0}^{\infty} (-n)^k = \sum_{k=0}^{N-1} (-n)^k$$

7.12. Multiplikative Jordan-Chevalley-Zerlegung

Sei $f \in GL(V), \dim V < \infty$, χ_f zerfalle in Linearfaktoren. Dann gibt es eine eindeutige Faktorisierung $f = h \cdot u$ mit

1) h ist diagonalisierbar
2) u ist unipotent
3) $h \cdot u = u \cdot h$

Beweis
Sind h, n wie in (7.9) so erfüllt $(h, u = \operatorname{id} + n)$ 1) - 3) aus (7.12). Erfülle h, u 1) - 3) aus (7.12) so erfüllen $(h, u - \operatorname{id})$ 1) - 3) aus (7.9).

8. Das Minimalpolynom

8.1. Erinnerung

Sei $f \in \mathrm{End}(V)$ zyklisch mit $V = L(v, f)$. Ist $n = \dim V$ so ist $B = \big(v, f(v), \ldots, f^{n-1}(v)\big)$ eine Basis von V und ist $f^n(v) = \sum_{i=0}^{n-1} \lambda_i f^i(v)$ so ist $\chi_f = X^n - \lambda_{n-1}X^{n-1} - \ldots - \lambda_0$. (vergleiche 6.14)

8.2. Lemma

In der Situation von (8.1) gilt: $\chi_f(f)(v) = 0$

Beweis

$$\chi_f(f)(v) = f^n(v) - \lambda_{n-1}f^{n-1}(v) - \ldots - \lambda_0 f^0(v) = 0 \qquad \square$$

8.3. Satz von Cayley-Hamilton

Sei $f \in \mathrm{End}(V), \dim V < \infty$. Dann ist $\chi_f(f) = 0$

Beweis
Sei $v \in V$. Sei f_0 die Einschränkung von f auf den f-invarianten Unterraum $U := L(v, f)$. Dann ist $\chi_{f_0}(f)v = \chi_{f_0}(f_0) = 0$ wegen (8.2). Sei $F : {}^{V}\!/_{U} \to {}^{V}\!/_{U}$ von f induziert. Dann $\chi_f = \chi_{f_0} \cdot \chi_F = \chi_F \cdot \chi_{f_0}$. Es folgt

$$\chi_f(f)(v) = \Big(\chi_F(f) \cdot \chi_{f_0}(f)\Big)(v) = \chi_F(f) \cdot \Big(\chi_{f_0}(f)(v)\Big) = 0$$

Also $\chi_f(f)(v) = 0$ für alle $v \in V$. $\square$

8.4. Satz

Sei $f \in \mathrm{End}(V), \dim V < \infty$. Dann gibt es ein eindeutiges normiertes Polynom $p \in K[X]$ minimalen Grades mit $p(f) = 0$. Es gilt $p \mid \chi_f$.

Beweis
Existenz: folgt aus Cayley-Hamilton

Eindeutigkeit: Ist $q \in K[X]$ ein zweites normiertes Polynom mit $q(f) = 0$. Ist $d(p) = d(q)$, so ist $d(p-q) < d(p) = d(q)$. Da $(p-q)(f) = 0$ ist, folgt $p - q = 0$ wegen der Minimalität von $d(p)$.

Division mit Rest liefert $\chi_f = l \cdot p + r$ mit $d(r) < d(p)$. Da $r(f) = \chi_f(f) - l(f)p(f) = 0$ ist folgt mit der Minimalität von $d(p)$ wieder $r = 0$. $\square$

8.5. Definition

p aus (8.4) heißt das **Minimalpolynom** von f. Wir bezeichnen es mit p_f.

8.6. Lemma

$p_f(\lambda) = 0 \iff \lambda$ ist Eigenwert von f.

Beweis
Ist λ eine Nullstelle von p_f so ist λ auch eine Nullstelle von χ_f (da $p_f \mid \chi_f$) und damit ein Eigenwert von f. Ist umgekehrt λ ein Eigenwert von f mit Eigenvektor v, so folgt mit $p_f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$

$$0 = p_f(f)(v) = \sum_{k=0}^{n} a_k f^k(v) = \sum_{k=0}^{n} a_k \lambda^k \cdot v = p_f(\lambda) \cdot v$$

Da $v \neq 0$ ist, folgt $p_f(\lambda) = 0$. □

8.7. Lemma

Ist f diagonalisierbar, so ist

$$p_f = \prod_{\lambda \text{ Eigenwert von } f} (X - \lambda)$$

Beweis
Sei q die rechte Seite von (⋆). Wegen (8.6) teilt q das Minimalpolynom p_f. Es bleibt zu zeigen $q(f) = 0$. Sei v ein Eigenvektor von f zum Eigenwert λ. Schreibe $q = q_0(X - \lambda)$. Dann

$$q(f)(v) = q_0(f)\big(\underbrace{(f - \lambda)(v)}_{=0}\big) = 0$$

Da f diagonalisierbar ist, gibt es eine Basis von V aus Eigenvektoren von f. Nun wirkt $q(f)$ trivial auf dieser Basis. Damit folgt $q(f) = 0$. □

8.8. Lemma

Sei $f \in \mathrm{End}(V)$, $\dim V < \infty$. Weiter sei $p_f = (X - \lambda_1) \cdot \ldots \cdot (X - \lambda_n)$ das Produkt von paarweise verschiedenen Linearfaktoren. Dann ist f diagonalisierbar.

Beweis
Mit Division mit Rest erhalten wir mit einem festen i

$$\prod_{j \neq i} (X - \lambda_j) = q_i \cdot (X - \lambda_i) + c_i \qquad c_i \in K, q_i \in K[X]$$

da die λ_j paarweise verschieden sind, ist $c_i \neq 0$. Es folgt für $v \in V$

$$c_i v = \underbrace{\prod_{j \neq i} (f - \lambda_j)(v)}_{v_i} - \underbrace{(f - \lambda i) q_i(f)(v)}_{w_i}$$

Es ist $v_i \in \mathrm{Kern}(f - \lambda_i)$, da $0 = p_f(f) = \prod_j (f - \lambda_j)$. Weiter ist $w_i \in \mathrm{Bild}(f - \lambda_i)$. Es gilt also

$$\begin{aligned} V &= \mathrm{Kern}(f - \lambda_i) \oplus \mathrm{Bild}(f - \lambda_i) \\ &= V_{\lambda_i} \oplus \mathrm{Bild}(f - \lambda_i) \end{aligned}$$

Sei $U := \bigoplus_i V_{\lambda_i} \subseteq V$. Wegen (⋆) ist die von $(f - \lambda_i)$ induzierte Abbildung auf V/U surjektiv. Also induziert auch $0 = (f - \lambda_1) \cdot \ldots \cdot (f - \lambda_n)$ eine surjektive Abbildung auf V/U. Es folgt $V/U = \{0\}$. Also $V = U = \bigoplus_i V_{\lambda_i}$ und f ist diagonalisierbar. □

8.9. Satz

Sei $f \in \operatorname{End}(V)$, $\dim V < \infty$. Dann ist f genau dann diagonalisierbar, wenn p_f ein Produkt von paarweise verschiedenen Linearfaktoren ist.

Beweis
(8.7) und (8.8)

8.10. Beispiel

Sei $J = \boxed{\begin{matrix} \lambda & & \\ 1 & \ddots & \\ & \ddots\, 1 & \lambda \end{matrix}}$ ein Jordankasten der Größe n. Dann gilt $p_J = (X-\lambda)^n$

Beweis

Es ist $\chi_J = (X-\lambda)^n$. Da $p_J \mid \chi_J$ ist $p_J = (X-\lambda)^k$ mit $k \leqslant n$. Da $(J-\lambda) = \boxed{\begin{matrix} 0 & & \\ 1 & \ddots & \\ & \ddots\, 1 & 0 \end{matrix}}$ ist leicht zu sehen, dass $(J-\lambda)^k \neq 0$ für $k < n$. Es folgt $p_J = (X-\lambda)^n$. □

8.11. Satz

Sei

$$A = \begin{pmatrix} \boxed{J_1} & & \\ & \ddots & \\ & & \boxed{J_n} \end{pmatrix}$$

wobei jedes J_i ein Jordankasten mit λ_i auf der Diagonalen ist. Für jeden Eigenwert λ von A sei n_λ die Größe des größten Jordankasten zum Eigenwert λ. Dann gilt:

$$p_A = \prod_{\lambda \text{ EW}} (X-\lambda)^{n_\lambda}$$

Beweis
Folgt mit (8.10) □

8.12. Lemma

Sei $p \in K[X]$ und B eine endliche Basis von V. Für $f \in \operatorname{End}(V)$ gilt $p\big(m_B^B(f)\big) = m_B^B\big(p(f)\big)$

Beweis
$m_B^B : \operatorname{End}(V) \to K^{n\times n}$ ist linear und verträglich mit Komposition. Ist $p = \sum_{k=0}^n a_k X^k$ so folgt:

$$p\big(m_B^B(f)\big) = \sum_{k=0}^n a_k \big(m_B^B(f)\big)^k = \sum_{k=0}^n a_k \cdot m_B^B(f^k) = m_B^B\left(\sum_{k=0}^n a_k f^k\right) = m_B^B\big(p(f)\big)$$ □

8.13. Korollar

$p_f = p_{m_B^B(f)}$

Beweis
(8.12) □

8.14. Bemerkung

Zu $f \in \mathrm{End}(V), A \in K^{n\times n}$ sind die Einsetzungshomomorphismen

$$\Phi_f : K[X] \to \mathrm{End}(V) \quad, \Phi_f(p) := p(f)$$
$$\Phi_A : K[X] \to K^{n\times n} \quad, \Phi_A(p) := p(A)$$

Ringhomomorphismen. Ebenso ist $m_B^B : \mathrm{End}(V) \to K^{n\times n}$ ein **Ringhomomorphismus**. Nach (8.12) kommutiert das Diagramm

$$\begin{tikzcd} K[X] \arrow[r, "\Phi_f"] \arrow[dr, bend right, "\Phi_{m_B^B(f)}"'] & \mathrm{End}(V) \arrow[d, "m_B^B"] \\ & K^{n\times n} \end{tikzcd}$$

8.15. Bemerkung

$\mathrm{Bild}(\Phi_f) \subseteq \mathrm{End}(V)$ und $\mathrm{Bild}(\Phi_A) \subseteq K^{n\times n}$ sind kommutative Unterringe von $\mathrm{End}(V)$ bzw. $K^{n\times n}$

8.16. Satz

Sei $f \in \mathrm{End}(V)$, $\dim V < \infty$. Das charakteristische Polynom χ_f zerfalle in Linearfaktoren. Sei Λ die Menge der Eigenwerte von f. Für $\lambda \in \Lambda$ sei $d_{\lambda,k} := \dim \mathrm{Kern}(f-\lambda)^k$ und $d_{\lambda,0} := 0$. Sei $j_{\lambda,k}$ die Anzahl der $k \times k$ Jordankästen zum Eigenwert λ. Dann gilt:

$$j_{\lambda,k} = 2 \cdot d_{\lambda,k} - (d_{\lambda,k+1} + d_{\lambda,k-1})$$

Beweis

Sei $J = \begin{pmatrix} \boxed{J_1} & & \\ & \ddots & \\ & & \boxed{J_n} \end{pmatrix}$ die Jordan-Normalform zu f. Dann gilt

$$(J-\lambda)^k = \begin{pmatrix} (J_1-\lambda)^k & & \\ & \ddots & \\ & & (J_n-\lambda)^k \end{pmatrix}$$

Also ist $d_{\lambda,k} = \sum_{i=1}^n \dim \mathrm{Kern}(J_i - \lambda)^k$. Ist J_i ein $l \times l$ Jordankasten zum Eigenwert μ, so gilt

$$\dim \mathrm{Kern}(J_i-\lambda)^k = \begin{cases} 0, & \text{falls } \lambda \neq \mu \\ \min\{k,l\}, & \text{falls } \lambda = \mu \end{cases}$$

Es folgt:

$$d_{\lambda,1} = \sum_{l=1}^{\dim V} j_{\lambda,l}$$
$$d_{\lambda,2} = \sum_{l=1}^{\dim V} j_{\lambda,l} + \sum_{l=2}^{\dim V} j_{\lambda,l}$$
$$\dots$$
$$d_{\lambda,k} = d_{\lambda,k-1} + \sum_{l=k}^{\dim V} j_{\lambda,l} \Longrightarrow d_{\lambda,k} - d_{\lambda,k-1} = \sum_{l=k}^{\dim V} j_{\lambda,l}$$

Also ist

$$2 \cdot d_{\lambda,k} - (d_{\lambda,k+1} + d_{\lambda,k-1}) = (d_{\lambda,k} - d_{\lambda,k-1}) - (d_{\lambda,k+1} - d_{\lambda,k}) = \sum_{l=k}^{\dim V} j_{\lambda,l} - \sum_{l=k+1}^{\dim V} j_{\lambda,l} = j_{\lambda,k} \quad \square$$

9. Euklidische Ringe und Hauptidealringe

9.1. Definition

Sei R ein kommutativer Ring. Eine Teilmenge $I \subset R$ heißt **Ideal** falls gilt:

i) $I \subseteq R$ ist eine Untergruppe bezüglich $+$

ii) $\forall a \in I, \forall r \in R : r \cdot a \in I$

9.2. Beispiele

i) $I = R$, $I = \{0\} \subseteq R$

ii) Sei $R = \mathbb{Z}$, $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}$ ist ein Ideal

iii) Sei $R = \mathbb{Z}$, n fest. $n\mathbb{Z} = \{n \cdot z \mid z \in \mathbb{Z}\} \subseteq \mathbb{Z}$ ist ein Ideal

iv) $I = \left\{\sum_{k=1}^{n} a_k X^k \,\middle|\, a_k \in 2\mathbb{Z}\right\} \subseteq \mathbb{Z}[X]$ ist ein Ideal

9.3. Definition

$u \in R$ heißt **Einheit**, falls es ein $r \in R$ gibt, so dass $u \cdot r = 1$. Die Einheiten eines Ringes bilden eine Gruppe $R^{\times}$.

9.4. Lemma

Sei $I \subset R$ ein Ideal. Dann sind äquivalent:

(i) $I = R$

(ii) $1 \in I$

(iii) I enthält eine Einheit

Beweis

(i)⇒(ii) klar

(ii)⇒(iii) klar

(iii)⇒(i) $I \subseteq R$ per Definition. Also nu $R \subseteq I$ zu zeigen:
Sei $r \in R$ und u die Einheit in I. Dann ist $r = (r \cdot u^{-1}) \cdot u \in I$ □

9.5. Bemerkung

$\{0\}$ und K sind die einzigen Ideale des Körpers K.

9.6. Definition

Seien $a_1, \dots, a_n \in R$. Mit $(a_1, \dots, a_n)$ bezeichnen wir das kleinste Ideal von R, das $a_1, \dots, a_n$ enthält. Also

$$(a_1, \dots, a_n) := \bigcap_{I \subset R, a_1, \dots, a_n \in I} I$$

$(a_1, \dots, a_n)$ heißt das von $a_1, \dots, a_n$ erzeugte Ideal.

Bemerkung

$$(a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} r_i a_i \,\middle|\, r_i \in R \right\}$$

9.7. Definition

Ideale, die von einem Element erzeugt werden, heißen **Hauptideale**

9.8. Definition

Ein **Integritätsring** R ist ein kommutativer nullteilerfreier Ring. Ein Integritätsring heißt **Hauptidealring** (HIR), wenn alle Ideale Hauptideale sind.

Beispiel
Jeder Körper ist ein Hauptidealring.

9.9. Definiton

Ein Integritätsring heißt **euklidscher Ring**, wenn es eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}$ mit folgenden Eigenschaften gibt $\forall a, b \in R, b \neq 0 \;\; \exists q, r \in R : a = qb + r, \delta(r) < \delta(b)$ oder $r = 0$. δ heißt dann eine **Gradfunktion**

9.10. Beispiel

(i) $\mathbb{Z}$ ist ein euklidscher Ring ($\delta(n) := |n|$)

(ii) $K[X]$ ist ein euklidscher Ring ($\delta(p) := d(p)$ vgl. 4.7)

9.11. Satz

Euklidsche Ringe sind Hauptidealringe.

Beweis
Sei $I \subseteq R$ ein Ideal. Ist $I = \{0\}$, so ist nichts mehr zu tun. Sei also $\{0\} \neq I$. Wähle $b \in I \setminus \{0\}$ so, dass $\delta(b)$ minimal ist. Behauptung: $I = (b)$

„$\subseteq$“: Sei $a \in I$. Dann ist $a = qb + r$ mit $r = 0$ oder $\delta(r) < \delta(b)$. Da $r = a - qb \in I$ ist und $\delta(b)$ minimal war, folgt $\delta(r) \geqslant \delta(b)$ $\lightning$. Also $r = 0$. Es folgt $a = q \cdot b$, also $a \in (b)$

„$\supseteq$“: klar, da $b \in I$ $\square$

9.12. Definition

Sei R ein Integritätsring. Sei $p \in R, p \neq 0, p \notin R^\times$

(i) p heißt **irreduzibel,** falls $p = a \cdot b \quad a, b \in R \Rightarrow a \in R^\times$ oder $b \in R^\times$

(ii) p heißt **prim**, falls : $p \mid a \cdot b \quad a, b \in R \Rightarrow p \mid a$ oder $p \mid b$

9.13. Lemma

Ist p prim, so ist p irreduzibel

Beweis
Sei $p = a \cdot b$, p prim $\Rightarrow p \mid a$ oder $p \mid b$. oBdA $p \mid a$. D.h. $\exists u \in R$, so dass $p \cdot u = a$. Daraus folgt $p = ab = pub \Leftrightarrow p - pub = 0 \Rightarrow p(1 - ub) = 0 \xrightarrow{\text{nullteilerfrei}} 1 - ub = 0$, also $ub = 1$. Also ist b eine Einheit. □

9.14. Satz

Sei R ein Hauptidealring. Dann gilt: p ist prim $\iff$ p irreduzibel

Beweis
„$\Rightarrow$“: 9.13

„$\Leftarrow$“: Sei p irreduzibel. Seien $a, b \in R$ mit $p \mid a \cdot b$, $p \nmid a$. Zu zeigen: $p \mid b$.

Dazu R Hauptidealring, d.h. $\exists d \in R$ mit $(a, p) = (d)$. Also $\exists c \in R$ mit $p = c \cdot d$. Da p irreduzibel ist, muss $c \in R^\times$ oder $d \in R^\times$ gelten. Angenommen $c \in R^\times$. Dann ist $d = c^{-1}p$. Wegen $a \in (d)$ gibt es nun $f \in R$ mit $a = f \cdot d \Rightarrow a = fc^{-1}p \Rightarrow p \mid a$ ↯ zur Vorraussetzung.

Also muss $d \in R^\times$ gelten. Also $(d) = R = (a, p)$. Also gibt es $r, s \in R$ mit $1 = ra + sp \Rightarrow b = rab + spb \Rightarrow p \mid b$ □

9.15. Satz

Sei R ein Hauptidealring. Dann lässt sich jedes $a \in R$, $a \neq 0$, $a \notin R^\times$ als ein Produkt von endlich vielen Primelementen aus R schreiben.

Beweis (mit 9.16)
Wir nennen $a \in R, a \neq 0$, $a \notin R^\times$ "gut", falls es das Produkt von endlich vielen Primelementen ist. Angenommen $a \in R \setminus \{0\} \cup R^\times$ ist nicht "gut". Dann ist a nicht prim, also nach (9.14) auch nicht irreduzibel. Also $a = a_1 b_1$ für $a_1, b_1 \notin R^\times$. Dann ist entweder a_1 nicht gut oder b_1. Sei o.B.d.A also a_1 nicht gut. $\rightsquigarrow$ Folge $a_1 a_2, \ldots, b_1 b_2, \ldots \in R \setminus R^\times$ mit $a_i = a_{i+1} b_{i+1}$ ($a = a_0$). Also $(a) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$. Wegen (9.16) $\exists N$ mit $(a_N) = (a_{N+1}) = (a_N b_N)$. Also $\exists u \in R$ mit $a_N = a_N b_N u$. Da R nullteilerfrei ist folgt $b_N u = 1 \Rightarrow b_N \in R^\times$ ↯ □

9.16. Lemma

Sei R ein Hauptidealring. Sei $I_1 \subseteq I_2 \subseteq \ldots$ eine aufsteigende Folge von Idealen in R. Dann gibt es eine $N \in \mathbb{N}$ so dass $I_n = I_N \forall n \geqslant N$.

Beweis
Definiere $I := \bigcup_{n=1}^\infty I_n$ ist ein Ideal. Also $\exists a \in R$ mit $I = (a)$. Sei $a \in I_N$. Es folgt

$$I = (a) \subseteq I_N \subseteq I_n \subseteq I_{n+1} \subseteq \ldots \subseteq I$$

Also $I_N = I_n \forall n \geqslant N$. □

9.17. Eindeutige Primfaktorzerlegung in Hauptidealringen

Sei R ein Hauptidealring.

1) Jedes $a \in R$, $a \neq 0$, $a \notin R^\times$ ist das Produkt von endlich vielen Primelementen $a = p_1 \cdot \ldots \cdot p_N$
2) Ist $p_1 \cdot \ldots \cdot p_N = q_1 \cdot \ldots \cdot q_M$ mit p_i, q_j prim, so gilt $N = M$ und es gibt $u_1, \ldots, u_N \in R^\times$ so dass (nach Umnummerierung) $p_i = q_i u_i$

Beweis

1) (9.15)

2) per Induktion nach N.

$N = 1$ $\surd$

$N-1 \mapsto N$ • Ist $p_1 \cdot \ldots \cdot p_N = q_1 \cdot \ldots \cdot q_M$ mit p_i, q_i prim, so gilt insbesondere $p_1 \mid q_1 \cdot \ldots \cdot q_M$

- Da p_1 prim, folgt o.B.d.A. $p_1 \mid q_1 \Rightarrow cp_1 = q_1$.
- Da q_1 prim (und somit irreduzibel) ist, folgt $p_1 = u_1 q_1$ mit $u_1 \in R^\times$.

Also ist

$$q_1 \cdots q_m = p_1 \cdots p_N = q_1 u_1 p_2 \cdots p_N \overset{R \text{ nullteilerfrei}}{\Longrightarrow} q_2 \cdots q_M = u_i p_2 \cdots p_M \overset{\text{I.V.}}{\Rightarrow} \text{Beh.}$$ □

9.18. Definition

Der Ring

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

heißt Ring der **Gaußschen Zahlen**.

9.19. Lemma

$\mathbb{Z}[i]$ ist ein Euklidischer Ring (und damit ein Hauptidealring).

Beweis

- $\mathbb{Z}[i]$ ist Integritätsring, definiere $N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ mit $a + ib \mapsto a^2 + b^2 = |a + ib|^2$. Damit ist N multiplikativ. Sei nun $z, \zeta \in \mathbb{Z}[i], \zeta \neq 0$. Zu zeigen: $\exists q, r \in \mathbb{Z}[i]$ mit $z = q\zeta + r$ und $r = 0$ oder $N(r) < N(\zeta)$. Es gilt
  - $\zeta \in \mathbb{C}^\times \Rightarrow z \cdot \zeta^{-1} \in \mathbb{C}$
  - Für benachbarte $f, g \in \mathbb{Z}[i]$ ist $|f - g| \leqslant \sqrt{2}$

  Also gibt es zu $h \in \mathbb{C}$ eine Gaußsche Zahl q mit $|h - q| \leqslant \frac{1}{\sqrt{2}} = \frac{1}{2}\sqrt{2}$
- Wähle so ein $q \in \mathbb{Z}[i]$ für $h = z \cdot \zeta^{-1}$ und setze $r := z - q \cdot \zeta \in \mathbb{Z}[i]$. Dann ist $z = q \cdot \zeta + r$ und

$$|r| = |z - q\zeta| = |\zeta| \cdot \underbrace{\left|z\zeta^{-1} - q\right|}_{\leqslant \frac{1}{\sqrt{2}} < 1} \leqslant |\zeta|$$

  mit $\zeta \neq 0$ folgt $N(r) < N(\zeta)$ □

9.20. Lemma

a) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

b) Ist $c \in \mathbb{Z}[i]$ mit $N(c) = |c|^2 = 1$, so ist $c \in \mathbb{Z}[i]^\times$

Beweis

a) „$\supseteq$“: klar
„$\subseteq$“: Sei $u \in \mathbb{Z}[i]^\times$. Dann ist $1 = N(1) = N(uu^{-1}) = N(u) \cdot N(u^{-1})$. Dann ist $N(u) = 1$. Sei $u = a + ib$, also $1 = a^2 + b^2 \Rightarrow$ Behauptung

b) schon erledigt □

9.21. Satz

Die einzige ganzzahlige Lösung der Gleichung $x^2+1=y^3$ ist $x=0, y=1$.

Beweis
Seien $x,y\in\mathbb{Z}$ mit $x^2+1=y^3$. Ist $x=0$ folgt $y=1$. Die Annahme $x=\pm1$ führt zu $y^3=2$, was in $\mathbb{Z}$ nicht lösbar ist. Also können wir $x\notin\{0,\pm1\}$ annehmen.

i) Betrachte $y^3=x^2+1=(x+i)(x-i)$ in $\mathbb{Z}[i]$. Da $x\neq 0$ ist $x+1, x-1\notin\mathbb{Z}[i]^\times$. (siehe 9.20)

ii) Behauptung: Ist c ein gemeinsamer Teiler von $x+i$ und $x-i$ ist, so ist c bereits eine Einheit.

N multiplikativ

Beweis: Ist $c \mid x+i \;\wedge\; c \mid x-i$, so ist auch $c \mid (x+i)-(x-i)=2i$. Wegen $N(2i)=4$, muss $N(c)\in\{1,2,4\}$ gelten. Ist $N(c)=1$ so folgt mit (9.20) $c\in\mathbb{Z}[i]^\times$. Ist also $N(c)=4$, so ist

$N(a+bi)=a^2+b^2$	1	2	3	4
$a+bi$	$\pm1,\pm i$	$\pm1+i,\pm1-i$	/	$\pm2,\pm2i$

Tabelle 1: Lösungen für $N(a+bi)\in\{1,2,3,4\}$

$c=\pm2$ oder $\pm2i$, so folgt $c\nmid x+1$ in $\mathbb{Z}[i]$. $\lightning$

Ist $N(c)=2$ folgt $c\in\{\pm1+i,\pm1-i\}\Rightarrow c=1+i$ bis auf Muliplikation mit einer Einheit. Es folgt

$$1+i \mid (x+i)(x-i)=y^3 \overset{(\star)}{\Longrightarrow} 1+i\mid y \Rightarrow (1+i)^3 \mid y^3=(x+i)(x-i)\overset{\text{PFZ}}{=}(p_1\cdots p_N)(q_1\cdots q_M)$$

zu $(\star)$: $1+i$ ist prim in $\mathbb{Z}[i]$, da aus $1+i=z_1z_2$ folgt $0=N(1+i)=N(z_1)\cdot N(z_2)\Rightarrow$ o.B.d.A $N(z_1)=1$ also $z_1\in\mathbb{Z}[i]^\times$

$$\Longrightarrow\quad (1+i)(1+i)(1+i)\cdot(r_1+r_k)=(p_1\cdots p_N)(q_1\cdots q_M)$$

Es folgt $(1+i)^2=2i \mid x+i$ oder $(1+i)^2=2i\mid(x-i)\Rightarrow 2\mid x+i$ oder $2\mid x-i$ $\lightning$

Also kann c nur noch eine Einheit sein.

iii) Die Primfaktorzerlegung liefert

$$y^3=(t_1\cdots t_L)^3=t_1t_1t_1\cdots t_2t_2t_2=x^2+1=(x+i)(x-i)$$

mit Behauptung ii)) folgt nach Umnummerierung $(x+i)=t_1^3\cdots t_\nu^3$ und $x-i=t_{\nu+1}^3\cdots t_L^3$. Also existieren $a,b\in\mathbb{Z}$ mit $(x+i)=(a+ib)$.

Hieraus ergibt sich wie folgt ein Widerspruch;

$$(x+i)=(a+bi)^3=(a^3-3ab^2)+(3a^2b-b^3)i$$

Also $b(3a^2-b^2)=1\Rightarrow b=\pm1$ und $3a^2=2$ $\lightning$ zu $a\in\mathbb{Z}$. Oder: $3a^2=0\Rightarrow a=0\Rightarrow x=0$ $\lightning$ zur Annahme. Also ist $x=0, y=1$. □

Anmerkung: Der Beweis ist in den Vorlesungsnotizen etwas kürzer, da dort die Primfaktorzerlegung weniger formal durchgeführt wird. Die Notizen zu diesem Kapitel befinden sich HIER

10. Tensorprodukte

10.1. Wiederholung

Seien V, W und U K-Vektorräume. Eine Abbildung $\varphi : V \times W \to U$ heißt **bilinear** falls gilt:

(1) $\varphi(v + v', w) = \varphi(v, w) + \varphi(v', w)$, $\varphi(\lambda v, w) = \lambda \cdot \varphi(v, w)$

(2) $\varphi(v, w + w') = \varphi(v, w) + \varphi(v, w')$, $\varphi(v, \lambda w) = \lambda \cdot \varphi(v, w)$

Den K-Vektorraum aller solchen Abbildungen bezeichnen wir mit $\mathrm{Hom_{bi}}(V \times W, U)$.

10.2. Definition

Seien V, W K-Vektorräume. Ein Vektorraum $V \otimes W$ zusammen mit einer bilinearen Abbildung $\phi : V \times W \to V \otimes W$ heißt **Tensorprodukt** von V mit W falls folgende **universelle Eigenschaft** erfüllt ist:

Das Tensorprodukt ermöglicht das Zurückführen bilinearer Abbildungen auf lineare Abbildungen

Zu jeder bilinearen Abbildung $\varphi : V \times W \to U$ gibt es eine eindeutige lineare Abbildung $f_\varphi; V \otimes W \to U$ so dass $\varphi = f_\varphi \circ \phi$

$$\begin{tikzcd} V \times W \arrow[r, "\varphi"] \arrow[d, "\phi"'] & U \\ V \otimes W \arrow[ur, dashed, "f_\varphi"'] & \end{tikzcd}$$

10.3. Bemerkung

Durch die universelle Eigenschaft wird das Tensorprodukt bis auf kanonischen Isomorphismus eindeutig festgelegt:

Sei $\tilde{\phi} : V \times W \to V \tilde{\otimes} W$ ein zweites Tensorprodukt. Indem wir die universelle Eigenschaft zweimal anwenden erhalten wir kanonische Abbildungen

$$\begin{tikzcd} V \times W \arrow[r, "\tilde{\phi}"] \arrow[d, "\phi"'] & V \tilde{\otimes} W \\ V \otimes W \arrow[ur, dashed, "f_{\tilde{\phi}}"'] & \end{tikzcd} \qquad \begin{tikzcd} V \times W \arrow[r, "\phi"] \arrow[d, "\tilde{\phi}"'] & V \otimes W \\ V \tilde{\otimes} W \arrow[ur, dashed, "f_\phi"'] & \end{tikzcd}$$

Nun können wir die Eindeutigkeit in der universellen Eigenschaft anwenden und erhalten

$$\begin{tikzcd} V \times W \arrow[r, "\tilde{\phi}"] \arrow[d, "\tilde{\phi}"'] & V \tilde{\otimes} W \\ V \tilde{\otimes} W \arrow[ur, dashed, "\mathrm{id} = f_\phi \circ f_{\tilde{\phi}}"'] & \end{tikzcd} \qquad \begin{tikzcd} V \times W \arrow[r, "\phi"] \arrow[d, "\phi"'] & V \otimes W \\ V \otimes W \arrow[ur, dashed, "\mathrm{id} = f_{\tilde{\phi}} \circ f_\phi"'] & \end{tikzcd}$$

Als ist f_ϕ der gesuchte kanonische Isomorphismus. □

10.4. Bemerkung

$\varphi \mapsto f_\varphi$ definiert einen Isomorphismus $\mathrm{Hom_{bi}}(V \times W, U) \xrightarrow{\cong} \mathrm{Hom}(V \otimes W, U)$. Sein Inverses ist durch $f \mapsto f \circ \phi$ definiert. Um $\mathrm{Hom_{bi}}(V \times W, U)$ zu verstehen, genügt es also $V \otimes W$ zu verstehen. Ein Vorteil ist nun, dass $V \otimes W$ unabhängig von U ist. Wir müssen aber die Existenz des Tensorprodukts noch nachweisen!

10.5. Definition

Sei $\mathfrak{M}$ eine beliebige Menge. Mit $K[\mathfrak{M}]$ bezeichnen wir den K-Vektorraum aller formalen Summen $\sum_{x\in\mathfrak{M}} \lambda_x \cdot x$ mit $\lambda_x \in K$ und $|\{x \mid \lambda_x \neq 0\}| < \infty$.

10.6. Bemerkung

Sei $x \in \mathfrak{M}$. Sei $\sigma(x) := \sum_{y\in\mathfrak{M}} \delta_{x,y} y$. Dies definiert eine Abbildung $\sigma : \mathfrak{M} \to K[\mathfrak{M}]$. Nun ist $\sigma(x), x \in \mathfrak{M}$ eine Basis von $K[\mathfrak{M}]$. Oft wird σ ignoriert und man schreibt kurz $\sigma(x) = x$.

10.7. Konstruktion von $V \otimes W$

Betrachte $K[V \times W]$. Wir erhalten $\sigma : V \times W \to K[V \times W]$, aber diese Abbildung ist (noch) nicht bilinear. Um dies zu korrigieren betrachten wir den folgenden Unterraum:

$$R := \langle \begin{matrix} (v+v',w)-(v,w)-(v',w), & (\lambda v,w)-\lambda(v,w), \\ (v,w+w')-(v,w)-(v,w'), & (v,\lambda w)-\lambda(v,w) \end{matrix} \mid v,v' \in V \quad w,w' \in W \quad \lambda \in K \rangle$$

und definieren $V \otimes W := {}^{K[V\times W]}/_{R}$ und $\phi(v,w) := (v,w) + R$. Nach Definition von R ist ϕ bilinear.

Üblicherweise schreibt man $v \otimes w$ für $(v,w) + R = \phi(v,w)$. Mit dieser Schreibweise gelten dann:

$$\begin{matrix} (v+v')\otimes w = v\otimes w + v'\otimes w & (\lambda v)\otimes w = \lambda(v\otimes w) \\ v\otimes(w+w') = v\otimes w + v\otimes w' & v\otimes(\lambda w) = \lambda(v\otimes w) \end{matrix}$$

10.8. Nachweis der universellen Eigenschaft für $V \otimes W$

Sei $\varphi : V \times W \to U$ bilinear. Da $V \times W$ eine Basis von $K[V \times W]$ ist, gibt es eine eindeutige lineare Abbildung $\hat{f} : K[V \times W] \to U$ mit $\hat{f}_\varphi((v,w)) = \varphi(v,w) \in U$, die also $\varphi : V \times W \to U$ fortsetzt. Da φ bilinear ist, liegt R im Kern von $\hat{f}$ und wir erhalten eine induzierte lineare Abbildung $f_\varphi : V \otimes W \to U$ mit $f_p(v \otimes w) = \varphi(v,w)$. Dies ist die eindeutige lineare Abbildung mit $f_\varphi \circ \phi = \varphi$ $\square$

10.9. Satz

Seien V, W K-Vektorräume mit Basen A, B. Dann bilden die $a \otimes b$, $a \in A$, $b \in B$ eine Basis von $V \otimes W$.

Beweis
Nach Konstruktion ist $\{v \otimes w \mid v \in V, w \in W\}$ ein Erzeugendensystem von $V \otimes W$. Seien $v \in V$ und $w \in W$ beliebig. Ist $v = \sum_{a\in A} \lambda_a \cdot a$, $w = \sum_{b\in B} \lambda_b \cdot b$ mit $\lambda_a, \lambda_b \in K$, so ist

$$v \otimes w = \left(\sum_{a\in A} \lambda_a \cdot a\right) \otimes \left(\sum_{b\in B} \lambda_b \cdot b\right) = \sum_{\substack{a\in A\\ b\in B}} \lambda_a \cdot \lambda_b (a \otimes b)$$

Daher ist auch $\{a \otimes b \mid a \in A, b \in B\}$ ein Erzeugendensystem. Sei nun $\sum_{a\in A, b\in B} (\lambda_{a,b}) a \otimes b = 0 \in V \otimes W$. Seien $a_0 \in A$, $b_0 \in B$ beliebig. Dann gibt es $\alpha_0 \in \mathrm{Hom}(V,K), \beta_0 \in \mathrm{Hom}(W,K)$ mit $\alpha_0(a) = \delta_{a_0,a}$, $\beta_0(b) = \delta_{b_0,b}$ für $a \in A$, $b \in B$. Nun ist $\varphi : V \times W \to K$ mit $\varphi(v,w) = \alpha_0(v) \cdot \beta_0(w)$ bilinear. Es gibt also eine lineare Abbildung $f_\varphi : V \otimes W \to K$ $f_\varphi(v \otimes w) = \alpha(v) \cdot \beta(w)$ $\forall v \in V, w \in W$. Insbesondere gilt

$$f_\varphi(a \otimes b) = \begin{cases} 1, & \text{falls } a = a_0, b = b_0 \\ 0 & \text{sonst} \end{cases}$$

für $a \in A, b \in B$. Es folgt

$$0 = f_\varphi(0) = f_\varphi\left(\sum_{\substack{a\in A\\ b\in B}} (\lambda_{a,b}) \cdot a \otimes b\right) = \sum_{\substack{a\in A\\ b\in B}} \lambda_{a,b} f_\varphi(a\otimes b) = \lambda_{a_0,b_0}$$

Da a_0 und b_0 beliebig waren, folgt $\lambda_{a,b} = 0$ für alle $a \in A, b \in B$. Damit ist $\{a \otimes b \,|\, a \in A, b \in B\}$ linear unabhängig. □

10.10. Bemerkung

Sei K ein Unterkörper von L. Dann ist L insbesondere ein K-Vektorraum. Zu einem K-Vektorraum V betrachte nun das Tensorprodukt $L \otimes_K V$. Dann wird $L \otimes_K V$ durch

$$L \times L \otimes_K V \to L \otimes_K V \qquad (\lambda, l \otimes v) \mapsto (\lambda \cdot l) \otimes v$$

zu einem L-Vektorraum. Wir bezeichnen ihn oft mit $V_L := L \otimes_K V$.

10.11. Lemma

Sei K ein Unterkörper von L. Sei B eine Basis des K-Vektorraums V. Dann ist $\{1 \otimes b \,|\, b \in B\}$ eine Basis von V_L.

Beweis
Sei $v \in V$. Dann ist $v = \sum_{b\in B} k_b \cdot b$ für geeignete $k_b \in K$. Für $l \in L$ gilt dann

$$l \otimes v = l \otimes \sum_{b\in B} k_b \cdot b = \sum_{b\in B} l \cdot k_b \cdot (1 \otimes b)$$

Da V_L von allen $l \otimes v$ erzeugt wird, ist daher $\{1 \otimes b \,|\, b \in B\}$ ein Erzeugendensystem von V_L.

Sei $\sum_{b\in B} l_b(1 \otimes b) = 0$. Sei $b_0 \in B$ beliebig. Sei $\beta_0 \in \mathrm{Hom}_K(V, K)$ mit $\beta_0(b) = \delta_{b_0,b}$ für $b \in B$. Nun ist $\varphi : L \times V \to L$ mit $\varphi(l, v) = l \cdot \beta(v)$ K-bilinear. Daher gibt es $f_\varphi \in \mathrm{Hom}_K(V_L, L)$ mit $f_\beta(l \otimes v) = l \cdot \beta(v)$. Wegen $f_\varphi(1 \otimes b) = \delta_{b_0,b}$

$$f_\varphi(l \cdot (l' \otimes v)) = f_\varphi(l' \cdot l \otimes v) = (l \cdot l') \cdot \beta(v) = l'(l \cdot \beta(v)) = l' \cdot f_\varphi(l \otimes v)$$

ist f_φ sogar L-linear. Es folgt

$$0 = f_\varphi(0) = f_\varphi\left(\sum_{b\in B} l_b(1 \otimes b)\right) = \sum_{b\in B} l_b f_\varphi(1 \otimes b) = l_{b_0}$$

Also ist $l_b = 0$ für alle b und $\{1 \otimes b \,|\, b \in B\}$ L-linear unabhängig. □

10.12. Bemerkung

Sei K ein Unterkörper von L. Ist $f : V \to W$ eine K-lineare Abbildung, so gibt es eine eindeutige L-lineare Abbildung $f_L : V_L \to W_L$ mit $f_L(l \otimes v) := l \otimes f(v)$.

Ist $g : W \to U$ eine weitere K-lineare Abbildung, so gilt $(g \circ f)_L = g_L \circ f_L$. Weiter ist $(\mathrm{id}_V)_L = \mathrm{id}_{(V_L)}$. (Man sagt auch, dass $(V \mapsto V_L, f \mapsto f_L)$ ein **Funktor** von der Kategorie der K-Vektorräume in die Kategorie der L-Vektorräume ist.)

10.13. Bemerkung

Sei K ein Unterkörper von L. Sei B eine endliche K-Basis dese K-Vektorraums V. Sei $B_L = \{1 \otimes b \,|\, b \in B\}$ die zugehörige L-Basis von V_L. Ist $f \in \mathrm{End}_K(V)$, so gilt

$$K^{n\times n} \ni m_B^B(f) = m_{B_L}^{B_L}(f_L) \in L^{n\times n}$$

10.14. Bezeichnung

Sei K ein Unterkörper von L und V ein K-Vektorraum. Indem wir $v = 1 \otimes v$ schreiben, können wir V als Teilmenge von V_L auffassen. Dann wird V zu einem K-Untervektorraum von V_L. Es gilt $l \cdot v = l \otimes v$ für $l \in L, v \in V$.

10.15. Beispiel

Sei V ein $\mathbb{R}$-Vektorraum

i) Jeder Vektor $\omega \in V_{\mathbb{C}}$ lässt sich dann eindeutig schreiben als $\omega = x + iy$ mit $x, y \in V$

ii) Durch $\omega = x + iy \mapsto \overline{\omega} := x - iy$ wird ein $\mathbb{R}$-linearer(!) Endomorphismus von $V_{\mathbb{C}}$ definiert. Es gilt $V = \{\omega \in V_{\mathbb{C}} \,|\, \omega = \overline{\omega}\}$. Weiter ist für $\omega = x + iy$ $x = \frac{\omega + \overline{\omega}}{2}$ und $y = \frac{\omega - \overline{\omega}}{2i}$

iii) Es gilt $\overline{\alpha\omega} = \overline{\alpha} \cdot \overline{\omega}$ für $\omega \in V_{\mathbb{C}}, \alpha \in \mathbb{C}$. Man sagt, $\omega \mapsto \overline{\omega}$ ist $\mathbb{C}$-**antilinear**.

iv) Ist $f : V \to W$ $\mathbb{R}$-linear, so wird $f_{\mathbb{C}} : V_{\mathbb{C}} \to W_{\mathbb{C}}$ festgelegt durch

$$f_{\mathbb{C}}(x + iy) = f(x) + if(y) \qquad \text{für } x, y \in V$$

Es gilt dann $f_{\mathbb{C}}(\overline{\omega}) = \overline{f_{\mathbb{C}}(\omega)}$.

11. Die Jordansche Normalform über $\mathbb{R}$

11.1. Lemma

Sei $p = c_n X^n + c_{n-1} X^{n-1} + \ldots + c_0 \in \mathbb{R}[X]$.

(i) Für $\lambda \in \mathbb{C}$ gilt $p(\lambda) = 0 \iff p(\overline{\lambda}) = 0$.

(ii) Ist $p = g \cdot f$ mit $0 \neq g \in \mathbb{R}[X], f \in \mathbb{C}[X]$, so ist $f \in \mathbb{R}[X]$.

(iii) Ist p irreduzibel , so ist $d(p) \leqslant 2$.

Beweis

(i)

$$\begin{aligned} p(\overline{\lambda}) &= c_n \overline{\lambda}^n + c_{n-1} \overline{\lambda}^{n-1} + \ldots + c_0 \\ &= \overline{c_n} \overline{\lambda^n} + \overline{c_{n-1}} \overline{\lambda^{n-1}} + \ldots + \overline{c_0} \\ &= \overline{(c_n \lambda^n + c_{n-1} \lambda^{n-1} + \ldots + c_0)} = \overline{p(\lambda)} = 0 \end{aligned}$$

(ii) Division mit Rest in $\mathbb{R}[X]$ liefert: $p = gq + r$ mit $r, q \in \mathbb{R}[X], d(r) < d(g)$. Daher $g \cdot f = p = g \cdot q + r$. Also $r = g(f - q)$. Da $g \neq 0$ und der $d(r) < d(g)$, folgt $f - q = 0$ also $f = q \in \mathbb{R}[X]$. $d(p \cdot q) = d(p) + d(q)$

(iii) Angenommen $d(p) \geqslant 3$. Sei $\lambda \in \mathbb{C}$ eine Nullstelle von p. Da p irreduzibel über $\mathbb{R}[X]$ ist, ist $\lambda \notin \mathbb{R}$. Da $\lambda \neq \overline{\lambda}$ und $\lambda, \overline{\lambda}$ Nullstellen von p sind, gilt $(X - \lambda)(X - \overline{\lambda}) \mid p$ in $\mathbb{C}[X]$. Da

$$(X - \lambda)(X - \overline{\lambda}) = X^2 - (\underbrace{\lambda + \overline{\lambda}}_{\in \mathbb{R}})X + \underbrace{\lambda \overline{\lambda}}_{\in \mathbb{R}}$$

gilt wegen (ii) $(X - \lambda)(X - \overline{\lambda}) \mid p$ schon in $\mathbb{R}[X]$. $\lightning$ zu p irreduzibel und $d(p) \geqslant 3$ $\square$

11.2. Bemerkung

Die normierten irreduziblen Polynome $p \in \mathbb{R}[X]$ sind genau

(i) $X - a, \quad a \in \mathbb{R}$

(ii) $(X - a)^2 + b^2, \quad a, b \in \mathbb{R}\ b > 0$

11.3. Satz

Sei $f \in \operatorname{End}_K(V), \dim_K V < \infty$. Sei $p_f = g \cdot h \in K[X]$ mit g, h teilerfremd und normiert. Dann gilt:

(i) $\operatorname{Kern} g(f) = \operatorname{Bild} h(f), \operatorname{Kern} h(f) = \operatorname{Bild} g(f)$

(ii) $V = \operatorname{Kern} g(f) \oplus \operatorname{Kern} h(f)$

(iii) $\operatorname{Kern} g(f)$ und $\operatorname{Kern} h(f)$ sind f-invariant

(iv) Für $f_g := f|_{\operatorname{Kern} g(f)}, f_h = f|_{\operatorname{Kern} h(f)}$ gilt $p_{f_g} = g, p_{f_h} = h$.

Beweis
Da g und h teilerfremd sind, gibt es $\alpha, \beta \in K[X]$ mit $1 = \alpha g + \beta h$. Insbesondere $\mathrm{id}_V = \alpha(f)g(f) + \beta(f)h(f)$.

(i) Sei also $v = h(f)(w) \in \operatorname{Bild} h(f)$ mit $w \in V$. Dann gilt

$$g(f)(v) = g(f)\big(h(f)(w)\big) = (g \cdot h)(f)(v) = p_f(f)(v) = 0$$

Also $v \in \operatorname{Kern} g(f)$.

Sei nun $v \in \operatorname{Kern} g(f)$.

$$v = \alpha(f)\underbrace{g(f)(v)}_{=0} + \beta(f)h(f)(v) = \beta(f)h(f)(v) = h(f)\beta(f)(v) \in \operatorname{Bild} h(f)$$

Es folgt $\operatorname{Kern} g(f) = \operatorname{Bild} h(f)$. Genauso folgt $\operatorname{Kern} h(f) = \operatorname{Bild} g(f)$. □

(ii) Sei $v \in V$. Dann

$$\begin{aligned} v = \alpha(f)g(f)(v) + \beta(f)h(f)(v) &= g(f)\alpha(f)(v) + h(f)\beta(f)(v) \\ &\in \operatorname{Bild} g(f) + \operatorname{Bild} h(f) = \operatorname{Kern} h(f) + \operatorname{Kern} g(f) \end{aligned}$$

Sei $v \in \operatorname{Kern} h(f) \cap \operatorname{Kern} g(f)$. Dann

$$v = \alpha(f)\underbrace{g(f)(v)}_{=0} + \beta(f)\underbrace{h(f)(v)}_{=0} = 0$$

Also $V = \operatorname{Kern} h(f) + \operatorname{Kern} g(f)$ und $\operatorname{Kern} h(f) \cap \operatorname{Kern} g(f) = \{0\}$. Damit $V = \operatorname{Kern} g(f) \oplus \operatorname{Kern} h(f)$. □

(iii) Wegen $g(f) \cdot f = f \cdot g(f)$ ist $\operatorname{Kern} g(f)$ f-invariant. Sei $v \in \operatorname{Kern} g(f)$. Dann $g(f)(f(v)) = f(g(f)(v)) = 0$. Also $f(v) \in \operatorname{Kern} g(f)$. Genauso ist $\operatorname{Kern} h(f)$ f-invariant.

(iv) Für $v \in \operatorname{Kern}(f)$ gilt $g(f_g)(v) = g(f)(v) = 0$. Also $g(f_g) = 0$. Es folgt (mit Division mit Rest) $p_{f_g} \mid g$. Ebenso $p_{f_h} \mid h$. Für $v \in \operatorname{Kern} g(f)$ gilt

$$\big(p_{f_h} \cdot p_{f_g}\big)(f)(v) = \big(p_{f_h} \cdot p_{f_g}\big)(f_g)(v) = p_{f_h}(f_g) \cdot p_{f_g}(f_g)(v) = 0$$

Genauso gilt für $v \in \operatorname{Kern} h(f)$: $\big(p_{f_h} \cdot p_{f_g}\big)(f)(v) = 0$

Da $V = \operatorname{Kern} g(f) \oplus \operatorname{Kern} h(f)$ folgt $\big(p_{f_h} \cdot p_{f_g}\big)(f)(v) = 0$ für alle $v \in V$. Also $\big(p_{f_h} \cdot p_{f_g}\big)(f) = 0$. Daher $p_f \mid p_{f_h} \cdot p_{f_g}$. Also $p_{f_h} \cdot p_{f_g} \mid g \cdot h = p_f$ und $p_f \mid p_{f_h} \cdot p_{f_g}$. Daher $p_{f_h} \cdot p_{f_g} = p_f = g \cdot h$. Da g, h normiert sind und $p_{f_h} \mid h, p_{f_g} \mid g$ folgt auch

$$p_{f_h} = h \quad \text{und} \quad p_{f_g} = g$$ □

11.4. Proposition

Sei V ein $\mathbb{R}$-Vektorraum. Sei $W \subseteq V_{\mathbb{C}}$ ein $\mathbb{C}$-Unterraum. Sei $\overline{W} := \{\overline{w} \mid w \in W\}$. Sei $w_1, \ldots, w_n$ $\mathbb{C}$-Basis von W. Sei für $i = 1, \ldots, n$ $x_i := \frac{w_i + \overline{w_i}}{2}$ und $y_i = \frac{w_i - \overline{w_i}}{2i}$. Ist $V_{\mathbb{C}} = W \oplus \overline{W}$ so ist $x_1, y_1, \ldots, x_n, y_n$ eine $\mathbb{R}$-Basis von V.

Beweis
$\overline{w}_1, \ldots, \overline{w}_n$ ist eine $\mathbb{C}$-Basis von $\overline{W}$. Es folgt

$$2n = \dim_{\mathbb{C}} W + \dim_{\mathbb{C}} \overline{W} = \dim_{\mathbb{C}} V_{\mathbb{C}} = \dim_{\mathbb{R}} V$$

Es genügt nun zu zeigen, dass $x_1, y_1, \ldots, x_n, y_n$ ein $\mathbb{R}$-Erzeugendensystem von V ist. Sei $v \in V$. Da $w_1, \overline{w}_1, \ldots, w_n, \overline{w}_m$ eine $\mathbb{C}$-Basis von $V_{\mathbb{C}} = W \oplus \overline{W}$ ist, gibt es daher $\alpha_1, \beta_1, , \ldots, \alpha_n, \beta_n \in \mathbb{C}$ mit

$$\begin{aligned} v &= \alpha_1 w_1 + \beta_1 \overline{w}_1 + \ldots + \alpha_n w_n + \beta_n \overline{w}_n \\ \Rightarrow v &= \overline{v} = \overline{\alpha}_1 \overline{w}_1 + \overline{\beta}_1 w_1 + \ldots + \overline{\alpha}_n \overline{w}_n + \overline{\beta}_n w_n \end{aligned}$$

Es folgt, da $w_1, \overline{w}_1, \ldots, w_n, \overline{w}_n$ $\mathbb{C}$-Basis von $V_{\mathbb{C}}$ ist, gilt $\alpha_i = \overline{\beta}_i$ für $i = 1, \ldots, n$

$$\Rightarrow v = \underbrace{(\alpha_1 + \overline{\alpha}_1)}_{\in \mathbb{R}} \underbrace{\frac{w_1 + \overline{w}_1}{2}}_{=x_1} + \underbrace{i(\alpha_1 - \overline{\alpha}_1)}_{\in \mathbb{R}} \underbrace{\frac{w_1 - \overline{w}_1}{2i}}_{=y_1} + \ldots + \underbrace{(\alpha_n + \overline{\alpha}_n)}_{\in \mathbb{R}} \underbrace{\frac{w_n + \overline{w}_n}{2}}_{=x_n} + \underbrace{i(\alpha_n - \overline{\alpha}_n)}_{\in \mathbb{R}} \underbrace{\frac{w_n - \overline{w}_n}{2i}}_{=y_n}$$

□

11.5. Notation

Sei $p = \alpha_N X^n + \alpha_{n-1} X^{n-1} + \ldots + \alpha_1 X + \alpha_0 \in \mathbb{C}[X]$. Dann setzen wir

$$\overline{p} := \overline{\alpha_n} X^n + \overline{\alpha_{n-1}} X^{n-1} + \ldots + \overline{\alpha_1} X + \overline{\alpha_0}$$

Es gilt $p = \overline{p} \iff p \in \mathbb{R}[X]$.

11.6. Lemma

Sei V ein $\mathbb{R}$-Vektorraum, $\dim_{\mathbb{R}} V < \infty$, $f \in \operatorname{End}_{\mathbb{R}}(V)$. Dann ist $p_{f_{\mathbb{C}}} = p_f$.

Beweis
Sei $w = x + iy \in V_{\mathbb{C}}$, $x, y \in V$. Dann ist

$$(p_f(f_{\mathbb{C}}))(w) = p_f(f_{\mathbb{C}})(x + iy) = p_f(f_{\mathbb{C}})(x) + i \cdot p_f(f_{\mathbb{C}})(y) = p_f(f)(x) + i \cdot p_f(f)(y) = 0$$

Es folgt $p_{f_{\mathbb{C}}} \mid p_f$. Sei $p_{f_{\mathbb{C}}} = \alpha_n \lambda^n + \alpha_{n-1} \lambda^{n-1} + \ldots + \alpha_1 \lambda + \alpha_0$. Für $w = x + iy$ gilt

$$\overline{p_{f_{\mathbb{C}}}}(w) = \sum_{k=0}^{n} \overline{\alpha_k} f_{\mathbb{C}}^n(w) = \sum_{k=0}^{n} \overline{\alpha_k \overline{f_{\mathbb{C}}^n(\overline{w})}} = \overline{p_{f_{\mathbb{C}}}(f_{\mathbb{C}})(\overline{w})} = 0$$

Es folgt $\overline{p_{f_{\mathbb{C}}}} = p_{f_{\mathbb{C}}}$. Also $p_{f_{\mathbb{C}}} \in \mathbb{R}[X]$. Wegen $p_{f_{\mathbb{C}}}(f_{\mathbb{C}}) = 0$ ist auch $p_{f_C}(f) = 0$. Es folgt weiter $p_f \mid p_{f_{\mathbb{C}}}$. Also $p_f = p_{f_{\mathbb{C}}}$. □

11.7. Proposition

Sei V ein $\mathbb{R}$-Vektorraum. $\dim V < \infty$, $f \in \operatorname{End}_{\mathbb{R}}(V)$. Sei $p_f = \left((X-a)^2 + b^2\right)^N$ mit $a, b \in \mathbb{R}, b > 0$. Dann gibt es eine Basis $B = (x_1, y_1, \ldots, x_n, y_n)$ von V mit

$$m_B^B(f) = \begin{pmatrix} A & & & \\ D_1 & \ddots & & \\ & \ddots & \ddots & \\ & & D_{n-1} & A \end{pmatrix} \qquad \text{mit } A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad D_i = \{I_2, 0\}$$

Beweis
Sei $\alpha = a + bi \in \mathbb{C}$. Dann ist $p_{f_\mathbb{C}} = p_f = (X-\alpha)^N(X-\overline{\alpha})^N$. Da $b > 0$ ist, ist $\alpha \neq \overline{\alpha}$. Daher sind $(X-\alpha)^N$ und $(X-\overline{\alpha})^N$ teilerfremd. Es folgt mit (11.3)

$$V_\mathbb{C} = \mathrm{Kern}(f_\mathbb{C}-\alpha)^N \oplus \mathrm{Kern}(f_\mathbb{C}-\overline{\alpha})^N$$

Sei $W := \mathrm{Kern}(f_\mathbb{C}-\alpha)^N$ und $f_W := f_\mathbb{C}\big|_W$. Dann ist $p_{f_W} = (X-\alpha)^N$ nach (11.3). Daher ist α der einzige Eigenwert von f_W. Jordannormalform für $f_W \Rightarrow$ Es existiert eine Basis $w_1, \ldots, w_n$ von W mit

$$m_B^B(f) = \begin{pmatrix} \alpha & & & \\ \delta_1 & \ddots & & \\ & \ddots & \ddots & \\ & & \delta_n & \alpha \end{pmatrix} \qquad \text{mit } \delta_1, \ldots, \delta_n \in \{0,1\}$$

Also $f_\mathbb{C}(w_j) = \alpha w_j + \delta_j w_{j+1}$. Für $w = x + iy \in V_\mathbb{C}$ mit $x, y \in V$ gilt

$$(f_\mathbb{C}-\overline{\alpha})(\overline{w}) = f_\mathbb{C}(\overline{w}) - \overline{\alpha w} = \overline{f_C(w)} - \overline{\alpha w} = \overline{(f_\mathbb{C}-\alpha)(w)}$$

Es folgt $(f_\mathbb{C}-\overline{\alpha})^N(\overline{w}) = \overline{(f_\mathbb{C}-\alpha)^N(w)}$. Daher ist $\overline{W} = \mathrm{Kern}(f_\mathbb{C}-\overline{\alpha})^N$. Damit ist $V_\mathbb{C} = W \oplus \overline{W}$ und wir können (11.4) anwenden:
Setze: $x_j := \frac{w_j + \overline{w}_j}{2}$, $y_j := \frac{w_j - \overline{w}_j}{2i}$. Dann ist $B = x_1, y_1, \ldots, x_n, y_n$ eine Basis von V. Es ist

$$\begin{aligned} f(x_j) = f_\mathbb{C}\left(\frac{w_j + \overline{w}_j}{2}\right) = \frac{1}{2}\Big(f_\mathbb{C}(w_j) + \overline{f_\mathbb{C}(w_j)}\Big) &= \frac{1}{2}(\alpha w_j + \delta_j w_{j+1} + \overline{\alpha w}_j + \delta_j \overline{w}_{j+1}) \\ &= \frac{1}{2}(a w_j + ibw_j + a\overline{w}_j - ib\overline{w}_j) + \delta_j\left(\frac{w_{j+1} + \overline{w_{j+1}}}{2}\right) \\ &= a\frac{(w_j + \overline{w}_j)}{2} + ib\frac{w_j - \overline{w}_j}{2} + \delta_j x_{j+1} \\ &= a\frac{(w_j + \overline{w}_j)}{2} - b\frac{w_j - \overline{w}_j}{2i} + \delta_j x_{j+1} \\ &= ax_j - by_j + \delta_j x_{j+1} \end{aligned}$$

Genauso rechnet man aus $f(y_j) = b_j x_j + a y_j + \delta_j y_{j+1}$. □

11.8. Definition

Eine reelle Matrix der Gestalt

$$\begin{pmatrix} A & & & \\ I_2 & A & & \\ & & \ddots & \\ & & I_2 & A \end{pmatrix} \qquad \text{mit } A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \text{mit } a, b \in \mathbb{R},\ \ b > 0$$

heißt **verallgemeinerter Jordankasten**.

11.9. Satz

Sei $f \in \mathrm{End}(V)$, $\dim V < \infty$. Dann gibt es eine Basis B von V, so dass

$$m_B^B(f) = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_n \end{pmatrix}$$

wobei jedes J_j ein Jordankasten oder verallgemeinerter Jordankasten ist.

Beweis
Sei $p_f = q_1^{k_1} \cdot \ldots \cdot q_N^{k_N}$ die Primfaktorzerlegung. Sei $V_j := \operatorname{Kern} q_j(f)^{k_j}$. Wegen (11.3) sind die V_j f-invariant und

- $V = V_1 \oplus \ldots \oplus V_N$
- $p(f|_{V_j}) = q_j^{k_j}$

Nach (11.2) ist jedes q_j entweder ein Linearfaktor oder $q_j = (X - a_j)^2 + b_j$ mit $a_j, b_j \in \mathbb{R}, b > 0$. Ist q_j ein Linearfaktor, so können wir die übliche Jordansche Normalform auf $f_j := f|_{V_j}$ anwenden und erhalten eine Basis B_j von V_j so dass $m_{B_j}^{B_j}(f_j)$ aus Jordankästen besteht. Andernfalls können wir (11.7) anwenden und erhalten eine Basis B_j von V_j für die $m_{B_j}^{B_j}(f_j)$ aus verallgemeinerten Jordankästen besteht. Also ist $B = B_1 \cup \ldots \cup B_N$ die gesuchte Basis. $\square$

12. Der Dualraum

12.1. Definition

Sei V ein K-Vektorraum. Dann heißt $V^* := \mathrm{Hom}_K(V, K)$ der **Dualraum** von V.

12.2. Lemma

Sei $B = (b_1, \dots, b_n)$ eine Basis von V. Sei für $i = 1, \dots, n$ $\beta_i : V \to K$ die eindeutig bestimmte lineare Abbildung mit $\beta_i(b_j) = \delta_{ij}$ für alle $j = 1, \dots, n$. Dann ist $B^* = (\beta_1, \dots, \beta_n)$ eine Basis von V^*.

Beweis
B^* **ist linear unabhängig:** Sei $\lambda_1\beta_1 + \ldots + \lambda_n\beta_n = 0$ mit $\lambda_1, \dots, \lambda_n \in K$. Dann gilt

$$0 = (\lambda_1\beta_1 + \ldots + \lambda_n\beta_n)(b_j) = \lambda_1\beta_1(b_j) + \ldots + \lambda_n\beta_n(b_j) = \lambda_j$$

Also $\lambda_1 = \ldots = \lambda_n = 0$.

B^* **ist ein EZS:** Sei $\varphi \in V^*$. Betrachte $\sum_{i=1}^n \varphi(b_i) \cdot \beta_i$. Dann gilt für $j = 1, \dots, n$

$$\left(\sum_{i=1}^n \varphi(b_i)\beta_i\right)(b_j) = \sum_{i=1}^n \varphi(b_i)\beta_i(b_j) = \varphi(b_j)$$

Also $\varphi = \sum_{i=1}^n \varphi(b_i)\beta_i$. □

<u>Bemerkung:</u> Sei $\dim V < \infty$, $B = b_1, \dots, b_n$ Basis und $B^* = \beta_1, \dots, \beta_n$ die duale Basis. Dann gilt

(i) $\forall \varphi \in V^* : \varphi = \sum_{i=1}^n \varphi(b_i)\beta_i$

(ii) $\forall v \in V : v = \sum_{i=1}^n \beta_i(v) b_i$

12.3. Definition

B^* aus (12.2) heißt die **duale Basis** zu B.

12.4. Korollar

Ist $\dim V < \infty$, so sind V und V^* isomorph.

12.5. Bemerkung

Der Isomorphismus $V \cong V^*$ aus (12.4) ist nicht kanonisch.

12.6. Bemerkung

Ist B eine unendliche Basis von V, also $\dim v = \infty$, so kann man B^* wie in (12.2) definieren. B^* ist dann linear unabhängig, aber kein Erzeugendensystem für V^*. Ist $\dim V = \infty$, so sind V und V^* nicht isomorph. (Übung)

12.7. Definition

Sei $f : V \to W$ linear. Dann heißt die durch $f^*(\varphi) := \varphi \circ f$ definierte lineare Abbildung $f^* : W^* \to V^*$ die zu f **duale Abbildung.**

$$V \xrightarrow{f} W \xrightarrow{\varphi} K$$

12.8. Proposition

(1) Für $f, g \in \mathrm{Hom}(V, W)$ gilt $(f+g)^* = f^* + g^*$ *$f \mapsto f^*$ linear*

(2) Für $\lambda \in K, f \in \mathrm{Hom}(V, W)$ gilt $(\lambda f)^* = \lambda f^*$

(3) Für $f \in \mathrm{Hom}(V, W)$, $g \in \mathrm{Hom}(W, U)$ gilt $(g \circ f)^* = f^* \circ g^*$

Beweis

(1) Sei $\varphi \in W^*$. Dann

$$(f+g)^*(\varphi) = \varphi \circ (f+g) = \varphi \circ f + \varphi \circ g = f^*(\varphi) + g^*(\varphi) = (f^* + g^*)(\varphi)$$

Also $(f+g)^* = f^* + g^*$.

(2) Sei $\varphi \in W^*$. Dann

$$(\lambda f)^*(\varphi) = \varphi \circ (\lambda f) = \lambda \ \ \varphi \circ f = \lambda f^*(\varphi)$$

Also $(\lambda f)^* = \lambda(f^*)$.

(3) Sei $\varphi \in U^*$. Dann gilt

$$(f^* \circ g^*)(\varphi) = f^*(g^*(\varphi)) = f^*(\varphi \circ g) = (\varphi \circ g) \circ f = \varphi \circ (g \circ f) = (g \circ f)^*(\varphi)$$

Also $(g \circ f)^* = f^* \circ g^*$. □

12.9. Proposition

Sei B eine endliche Basis von V und $f \in \mathrm{End}(V)$. Dann gilt

$$m_{B^*}^{B^*}(f^*) = \left(m_B^B(f)\right)^t$$

Beweis

Sei $m_B^B(f) = (a_{ij})$. Die definierenden Gleichungen für die a_{ij} sind

$$f(b_j) = \sum_{i=1}^{n} a_{ij} b_i$$

Zu zeigen: Für $j = 1, \dots, n$ ist $f^*(\beta_k) = \sum_{i=1}^{n} a_{ki}\beta_i$. Es ist

$$f^*(\beta_k)(b_j) = \beta_k(f(b_j)) = \beta_k\left(\sum_{i=1}^{n} a_{ij} b_i\right) = a_{kj}$$

und

$$\left(\sum_{i=1}^{n} a_{ki}\beta_i\right)(b_j) = \sum_{i=1}^{n} a_{ki}\beta_i(b_j) = a_{kj}$$ □

12.10. Lemma

Sei V ein euklidischer Vektorraum mit $\dim V < \infty$. Definiere $\phi_V : V \to V^*$ durch $\phi_V(v)(w) := \langle v \mid w \rangle$. Dann ist ϕ ein kanonischer Isomorphismus

Beweis
Wegen $\dim V = \dim V^*$ genügt es zu zeigen, dass ϕ_V injektiv ist. Sei $v \in V$ mit $\phi_V(v) = 0$. Dann ist

$$0 = \phi_V(v)(v) = \langle v \mid v \rangle = \|v\|^2$$

Also $v = 0$. □

12.11. Bemerkung

a) Der Isomorphismus ϕ_V ist kanonisch, er hängt nicht von Wahlen ab.

b) Ist B eine Orthonormalbasis von V, so bildet ϕ_V die Basis B auf die zugehörige duale Basis B^* ab.

12.12. Bemerkung

Ist V ein unitärer Vektorraum, so wird durch $\phi(v)(w) := \langle w \mid v \rangle$ eine Abbildung $\phi : V \to V^*$ definiert, sie ist aber $\mathbb{C}$-antilinear.

12.13. Proposition

Sei $f : V \to W$ eine lineare Abbildung zwischen endlich dimensionalen euklidischen Vektorräumen. Dann gibt es eine eindeutig bestimmte lineare Abbildung $f^\# : W \to V$ mit

$$\langle f(v) \mid w \rangle_W = \langle v \mid f^\#(w) \rangle_V$$

für alle $v \in V, w \in W$. Die gleiche Aussage gilt auch für endlich dimensionale unitäre Vektorräume.

Beweis
Eindeutigkeit: Ist $f^{\tilde{\#}}$ eine zweite solche Abbildung so gilt für alle $v \in V, w \in W$

$$\langle v \mid f^\#(w) - f^{\tilde{\#}}(w) \rangle = \langle v \mid f^\#(w) \rangle - \langle v \mid f^{\tilde{\#}}(w) \rangle = \langle f(v) \mid w \rangle - \langle f(v) \mid w \rangle = 0$$

Also $f^\#(w) = f^{\tilde{\#}}(w)$.

Existenz: Sei B eine Orthonormalbasis von V. Definiere $f^\#(w) := \sum_{b \in B} \langle f(b) \mid w \rangle b$. Dann gilt für $b_0 \in B, w \in W$

$$\langle b_0 \mid f^\#(w) \rangle = \sum_{b \in B} \langle b_0 \mid \langle f(b) \mid w \rangle b \rangle = \sum_{b \in B} \langle f(b) \mid w \rangle \langle b_0 \mid b \rangle = \langle f(b_0) \mid w \rangle$$

Es folgt $\langle v \mid f^\#(w) \rangle = \langle f(v) \mid w \rangle \ \ \forall v \in V, w \in W$. □

Bezeichnung
$f^\#$ heißt der zu f **adjungierte Homomorphismus**.

12.14. Lemma

Seien U, V, W endlich dimensionale euklidische Vektorräume

1) Für $f_1, f_2 : V \to V$ gilt $(f_1 + f_2)^\# = f_1^\# + f_2^\#$
2) Für $f : U \to V$ $\lambda \in \mathbb{R}$ gilt $(\lambda \cdot f)^\# = \lambda f^\#$ $\quad (= \overline{\lambda} f^\#)$ im unitären Fall
3) Für $f : U \to V$, $g : V \to W$ gilt $(g \circ f)^\# = f^\# \circ g^\#$
4) Für $f : U \to V$ gilt $(f^\#)^\# = f$

Beweis

1) Übung
2) Übung
3) Es genügt zu zeigen, dass $\langle u \,|\, f^\# \circ g^\#(w) \rangle = \langle u \,|\, (g \circ f)^\#(w) \rangle$ für alle $u \in U, w \in W$ gilt:
$$\langle u \,|\, f^\#(g^\#(w)) \rangle = \langle f(u) \,|\, g^\#(w) \rangle = \langle (g \circ f)(u) \,|\, w \rangle = \langle u \,|\, (g \circ f)^\#(w) \rangle$$
4) Zu zeigen: $\forall u \in U, v \in V$ gilt $\langle f(u) \,|\, v \rangle = \langle (f^\#)^\#(u) \,|\, v \rangle$
$$\langle f(u) \,|\, v \rangle = \langle u \,|\, f\#(v) \rangle = \langle f^\#(v) \,|\, u \rangle = \langle v \,|\, (f^\#)^\#(u) \rangle = \langle (f^\#)^\#(u) \,|\, v \rangle \qquad \square$$

12.15. Proposition

Seien V, W endlich dimensionale euklische Vektorräume. Sei $f : V \to W$ linear. Dann gelten
$$f^\# = \phi_V^{-1} \circ f^* \circ \phi_W \quad \text{und} \quad f^* = \phi_V \circ f^\# \circ \phi_W^{-1}$$

Beweis

ϕ_V und ϕ_W sind Isomorphismen. Es genügt also zu zeigen, dass

$$\begin{tikzcd}
V \arrow[d, "\phi_V"'] & W \arrow[l, "f^\#"'] \arrow[d, "\phi_W"] \\
V^* & W^* \arrow[l, "f^*"']
\end{tikzcd}$$

kommutiert. Sei $w \in W$. Wir zeigen: $\forall v \in V$ ist $\phi_V(f^\#(w))(v) = f^*(\phi_W(w))(v)$.

$$\begin{aligned}
\phi_V\Big(f^\#(w)\Big)(v) &= \langle f^\#(w) \,|\, v \rangle &&= \langle w \,|\, f(v) \rangle \\
f^*\Big(\phi_W(w)\Big)(v) &= \phi_W(w)\Big(f(v)\Big) &&= \langle w \,|\, f(v) \rangle
\end{aligned} \qquad \square$$

12.16. Bemerkung

Oft wird sowohl für die adjungierte als für die duale Abbildung die Notation f^* benutzt und so werden wir es auch halten. (12.15) sagt, dass für endlich dimensionale euklidische Vektorräume die adjungierte und die duale Abbildung bis auf die kanonischen Isomorphismen ϕ_V und ϕ_W übereinstimmen.

12.17. Bemerkung

Ist V ein endlich dimensionaler unitärer oder euklidischer Vektorraum und $f \in \mathrm{End}(V)$, so gilt

f ist selbstadjungiert $\iff f = f^*$

f ist Isometrie $\iff \forall v{:}\|f(v)\| = \|v\| \iff \forall v,w \in V{:}\langle f(v) \,|\, f(w) \rangle = \langle v \,|\, w \rangle \iff f^* = f^{-1}$

12.18. Lemma

Sei V ein endlich dimensionaler unitärer oder euklidischer Vektorraum. Sei $f \in \mathrm{End}(V)$ und B eine Orthonormalbasis von V. Dann gilt

$$m_B^B(f^*) = \overline{m_B^B(f)^t}$$

Beweis
(Übung)

13. Normale Endomorphismen

In diesem Kapitel ist V immer ein endlich dimensionaler euklidischer oder unitärer Vektorraum. Sei $K = \mathbb{R}$ oder $\mathbb{C}$ entsprechend.

13.1. Definition: Normaler Endomorphismus

$f \in \operatorname{End}(V)$ heißt **normal** falls $f^* \circ f = f \circ f^*$.

13.2. Beispiel

Isometrien und selbstadjungierte Endomorphismen sind normal. Siehe (12.17)

13.3. Lemma

$f \in \operatorname{End}(V)$ ist genau dann normal, wenn

$$\langle f(v) \,|\, f(w) \rangle = \langle f^*(v) \,|\, f^*(w) \rangle \qquad \text{für alle } v, w \in V$$

Beweis
Folgt aus

$$\begin{aligned} \langle f(v) \,|\, f(w) \rangle &= \langle f^* f(v) \,|\, w \rangle \\ \langle f^*(v) \,|\, f^*(w) \rangle &= \langle f f^*(v) \,|\, w \rangle \end{aligned}$$

□

13.4. Lemma

Sei $f \in \operatorname{End}(V)$ normal. Dann gilt

(i) $\operatorname{Kern} f = \operatorname{Kern} f^*$

(ii) Für $v \in V, \lambda \in K$ sind äquivalent
   a) v ist Eigenvektor von f zum Eigenwert λ.
   b) v ist Eigenvektor von f^* zum Eigenwert $\overline{\lambda}$

Beweis
(i) Für $v \in V$ ist $\|f(v)\|^2 = \langle f(v) \,|\, f(v) \rangle \overset{13.3}{=} \langle f^*(v) \,|\, f^*(v) \rangle = \|f^*(v)\|^2$. Also $f(v) = 0 \iff f^*(v) = 0$

(ii) Es ist $(\lambda - f)^* = (\overline{\lambda} - f^*)$ und mit f ist auch $\lambda - f$ normal. Für $v \in V$ folgt

$$\text{a)} \iff v \in \operatorname{Kern}(\lambda - f) \overset{\text{(i)}}{\iff} v \in \operatorname{Kern}(\overline{\lambda} - f^*) \iff \text{b)}$$

□

13.5. Lemma

Sei $f \in \operatorname{End}_K(V)$. Sei $U \leqslant V$. Dann ist U genau dann f-invariant, wenn $U^\perp$ f^*-invariant ist.

Beweis
Sei U f-invariant. Sei $w \in U^\perp$. Für alle $u \in U$ gilt dann

$$\langle f^*(w) \,|\, u \rangle = \langle \underset{\in U^\perp}{w} \,|\, \underset{\in U}{f(u)} \rangle = 0$$

Also $f^*(w) \in U^\perp$. Damit ist $U^\perp$ f^*-invariant. Wegen $(f^*)^* = f$ und $(U^\perp)^\perp = U$ gilt auch die Umkehrung. □

13.6. Lemma

Sei $f \in \operatorname{End}_K(V)$ normal und $U \leqslant V$ invariant unter f und f^*. Dann $U^\perp$ auch invariant unter f und f^*. Weiter ist $f^*\big|_U = \big(f\big|_U\big)^*$ und $f^*\big|_{U^\perp} = \big(f\big|_{U^\perp}\big)^*$. Insbesondere sind auch $f|_U$ und $f|_{U^\perp}$ normal.

Beweis
Für $u, u' \in U$ ist

$$\langle (f\big|_U)^* u \,|\, u' \rangle = \langle u \,|\, f\big|_U(u') \rangle = \langle u \,|\, f(u') \rangle = \langle f^*(u) \,|\, u' \rangle = \langle f^*\big|_U(u) \,|\, u' \rangle$$

Also $\big(f\big|_U\big)^* = f^*\big|_U$. Genauso folgt $\big(f\big|_{U^\perp}\big)^* = f^*\big|_{U^\perp}$. □

13.7. Spektralsatz

normale Endomorphismen sind diagonalisierbar, wenn χ_f zerfällt

Sei $f \in \operatorname{End}_K(V)$ ein Endomorphismus, dessen charakteristisches Polynom über K vollständig in Linearfaktoren zerfällt. Dann sind äquivalent:

(i) f ist normal

(ii) Es gibt eine Orthonormalbasis aus Eigenvektoren von f

Beweis
(i)⇒(ii): per Induktion nach $n := \dim_K V$.

$n = 0$: Klar

$n - 1 \mapsto n$: Da χ_F zerfällt, gibt es einen Eigenwert $\lambda \in K$ für f. Sei $e_1 \in V$ ein zugehöriger Eigenvektor mit $\|e_1\| = 1$. Betrachte $V = \langle e_1 \rangle \oplus \langle e_1 \rangle^\perp$. $\langle e_1 \rangle$ ist f-invariant. Sei $v \in \langle e_1 \rangle^\perp$. Dann gilt

$$\langle f(v) \,|\, e_1 \rangle = \langle v \,|\, f^*(e_1) \rangle \overset{\text{13.4 ii)}}{=} \langle v \,|\, \overline{\lambda} e_1 \rangle = \lambda \langle v \,|\, e_1 \rangle = 0$$

Also $f(v) \in \langle e_1 \rangle^\perp$. Daher ist $\langle e_1 \rangle^\perp$ f-invariant. Es folgt

$$\chi_f = \chi_{(f|_{\langle e_1 \rangle})} \cdot \chi_{\left(f|_{\langle e_1 \rangle^\perp}\right)}$$

Wegen (13.5) und (13.6) ist auch $f\big|_{\langle e_1 \rangle^\perp}$ normal, da $\chi_{\left(f|_{\langle e_1 \rangle^\perp}\right)}$ dann auch in Linearfaktoren zerfällt. Daher gibt es nach Induktionsannahme eine Orthonormalbasis $e_2, \ldots, e_n$ von $\langle e_1 \rangle^\perp$ aus Eigenvektoren von $f\big|_{\langle e_1 \rangle^\perp}$. Insgesamt ist $e_1, \ldots, e_n$ die gesuchte Orthonormalbasis.

(ii)⇒(i): Sei B eine Orthonormalbasis aus Eigenvektoren von f. Dann ist $m_B^B(f)$ eine Diagonalmatrix. Wegen (12.18) ist auch

$$m_B^B(f^*) = \overline{m_B^B(f)^t}$$

eine Diagonalmatrix. Es folgt

$$m_B^B(f \circ f^*) = m_B^B(f) \cdot m_B^B(f^*) = m_B^B(f^*) \cdot m_B^B(f) = m_B^B(f^* \circ f)$$

und damit auch $f \circ f^* = f^* \circ f$. □

14. Moduln

14.1. Definition

Sei R ein Ring. Ein R**-Modul** ist eine Menge M zusammen mit zwei Abbildungen

$$\begin{aligned} M \times M \to M, &\quad (v,w) \mapsto v+w \\ R \times M \to M, &\quad (r,v) \mapsto r \cdot w \end{aligned}$$

Dabei müssen folgende Axiome erfüllt sein:

(i) $(M,+)$ ist eine abelsche Gruppe

(ii) $\forall r \in R, v,w \in M : r(v+w) = rv + rw$

(iii) $\forall r,s \in R, v \in M : (r+s)v = rv + sv$

(iv) $\forall r,s \in R, v \in M : (r \cdot s) \cdot v = r \cdot (s \cdot v)$

(v) $\forall v \in M : 1_R \cdot v = v$

14.2. Beispiel

(1) K ein Körper: K-Modul = K-Vektorraum

(2) $\mathbb{Z}$-Modul = abelsche Gruppe

(3) $I \subseteq R$ ist R-Modul $\iff$ I Ideal

(4) Sei V ein K-Vektorraum, $f \in \operatorname{End}_K(V)$. Dann wird V zu einem $K[X]$-Modul durch:

$$p \cdot v := p(f)(v)$$

(5) $R^n = \left\{ \left(\begin{smallmatrix} x_1 \\ \vdots \\ x_n \end{smallmatrix} \right) \middle| x_i \in R \right\}$ mit

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \qquad r \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} rx_1 \\ \vdots \\ rx_n \end{pmatrix}$$

ist ein R-Modul. $e_1 = \left(\begin{smallmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{smallmatrix} \right), e_2 = \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{smallmatrix} \right), \ldots, e_n = \left(\begin{smallmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{smallmatrix} \right)$ heißt **Standardbasis von** R^n

14.3. Definition

Eine Teilmenge U eines R-Moduls M heißt ein **Untermodul**, falls gilt:

(i) $\forall r, w \in U : v + w \in U$

(ii) $\forall v \in U, r \in R : r \cdot v \in U$

(iii) $U \neq \emptyset$

14.4. Definition

Sei $U \leqslant V$ ein Untermodul. Dann heißt ${}^{V}\!/\!{}_{U} := \{v + U \mid v \in V\}$ der **Quotientenmodul** von V nach U. Er wird durch $(v+U)+(v'+U) := (v+v')+U$ und $r \cdot (v+U) := (r \cdot v)+U$ zu einem R-Modul. Dabei steht $v+U$ für die Menge $\{v+u \mid u \in U\}$. Dies ist auch die Äquivalenzklasse von v bezüglich $x \sim y :\Leftrightarrow x - y \in U$. Es gilt $v + U = v' + U \iff v - v' \in U$.

14.5. Beispiel

Ist $I \subseteq R$ ein Ideal in R, so ist ${}^{R}\!/\!{}_{I}$ ein R-Modul. (Ist R kommutativ oder ist I ein **zweiseitiges Ideal**, so ist ${}^{R}\!/\!{}_{I}$ ein Ring mit $(r+I)\cdot(s+I) = r \cdot s + I$)

14.6. Definition

Sei M ein R-Modul und $S \subseteq M$ eine Teilmenge. Dann heißt

$$\langle S \rangle_R = \langle S \rangle = \mathcal{L}(S) := \left\{ \sum_{i=1}^{n} r_i s_i \,\middle|\, r_1, \ldots, r_n \in R \;\; s_1, \ldots, s_n \in S \right\}$$

der von S **erzeugte** Untermodul. Ist $\langle S \rangle = M$ so heißt S ein **Erzeugendensystem**. Besitzt M ein endliches Erzeugendensystem, so heißt M **endlich erzeugt**. Wird M von einem Element erzeugt, so heißt M **zyklisch**.

14.7. Beispiel

Ist $I \subseteq R$ ein Ideal, so erzeugt $1 + I$ den R-Modul ${}^{R}\!/\!{}_{I}$. Insbesondere ist ${}^{R}\!/\!{}_{I}$ zyklisch.

14.8. Beispiel

${}^{\mathbb{Z}}\!/\!{}_{n\mathbb{Z}}$ wird als $\mathbb{Z}$-Modul von $1 + n\mathbb{Z}$ erzeugt. Für jedes $k \in \mathbb{Z}$ mit $n \mid k$ ist $k(1 + n\mathbb{Z}) = 0$. Insbesondere ist $1 + n\mathbb{Z}$ keine „Basis" für ${}^{\mathbb{Z}}\!/\!{}_{n\mathbb{Z}}$.

14.9. Definition

Eine Abbildung $f : M \to N$ zwischen R-Moduln heißt R-**linear**, falls:

(i) $\forall r \in R, v \in M : f(r \cdot v) = r \cdot f(v)$

(ii) $\forall v, w \in M : f(v + w) = f(v) + f(w)$

$\mathrm{Bild}(f) := \{f(v) \mid v \in M\} \subseteq N$ ist ein Untermodul.
$\mathrm{Kern}(f) := \{v \mid f(v) = 0\} \subseteq M$ ist ein Untermodul.

14.10. Bemerkung

$\mathrm{Bild}\, f = N \iff f$ surjektiv. $\mathrm{Kern}\, f = 0 \iff f$ injektiv

14.11. Definition

Sei $f : M \to N$ R-linear.

$$\mathrm{Koker}(f) := {}^{N}\!/\!{}_{\mathrm{Bild}(f)}$$

heißt der **Kokern** von f. Es gilt $\mathrm{Koker}(f) = 0 \iff f$ surjektiv.

14.12. Lemma

Ein R-Modul M ist genau dann endlich erzeugt, wenn es $n \in N$ und eine surjektive R-lineare Abbildung $f : R^n \to M$ gibt.

Beweis
Ist $f : R^n \to M$ surjektiv, so ist $f(e_1), \dots, f(e_n)$ ein Erzeugendensystem von M. Ist umgekehrt $s_1, \dots, s_n$ ein Erzeugendensystem von M, so definiert

$$f\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \sum_{i=1}^{n} x_i \cdot s_i$$

eine surjektive R-lineare Abbildung $f : R^n \to M$. □

14.13. Definition

R-Module M und N heißen **isomorph**, falls es eine R-lineare bijektive Abbildung $f : M \to N$ gibt. (So eine Abbildung heißt ein Isomorphismus). Wir schreiben $M \cong N$, falls M und N isomorph sind.

14.14. Bemerkung

(i) Nicht jeder endlich erzeugte R-Modul ist isomorph zu R^n für geeignetes n (Beispiel: $\mathbb{Z}/n\mathbb{Z}$ als $\mathbb{Z}$-Modul).

Nicht jedes endlich erzeugte R-Modul besitzt eine Basis

(ii) Es gibt Ringe R mit $R^n \cong R^m$ aber $n \neq m$.

14.15. Definition

Eine **kurze exakte Folge** von R-Moduln besteht aus R-linearen Abbildungen $M_0 \overset{i}{\hookrightarrow} M_1 \overset{p}{\twoheadrightarrow} M_2$ wobei

(i) i injektiv ist

(ii) $\operatorname{Bild} i = \operatorname{Kern} p$

(iii) p surjektiv ist.

Bemerkung:

(i) Ist $M_1 = M_0 \oplus M_2$, so ist $M_0 \hookrightarrow M_0 \oplus M_2 \to M_2$ $x \mapsto (x, 0)$, $(x, y) \mapsto y$

(ii) Beispiel $\mathbb{Z} \overset{\cdot 2}{\hookrightarrow} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$

(iii) oft schreibt man $0 \to M_0 \to M_1 \to M_2 \to 0$

14.16. Lemma

Sei $M_0 \overset{i}{\hookrightarrow} M_1 \overset{p}{\twoheadrightarrow} M_2$ eine kurze exakte Folge von R-Moduln. Sind M_0 und M_2 endlich erzeugt, so ist auch M_1 endlich erzeugt.

Beweis
Seien $\{s_1, \dots, s_n\} \subseteq M_2$ und $\{t_1, \dots, t_m\} \subseteq M_0$ Erzeugendensysteme. Da p surjektiv ist, gibt es $\{\tilde{s}_1, \dots, \tilde{s}_n\} \subseteq M_1$ mit $p(\tilde{s}_i) = s_i$ für $i = 1, \dots, n$. Zu zeigen: $\{\tilde{s}_1, \dots, \tilde{s}_n, i(t_1), \dots, i(t_m)\} \subseteq M_1$ ist ein Erzeugendensystem. Sei $v \in M_1$. Dann $p(v) = \sum_{i=1}^n r_i \cdot s_i$. Es ist

$$P\left(v - \sum_{i=1}^n r_i \cdot \tilde{s}_i\right) = p(v) - p\left(\sum_{i=1}^n r_i \cdot \tilde{s}_i\right) = p(v) - \sum_{i=1}^n r_i \cdot s_i = 0$$

Also $v - \sum_{i=1}^n r_i \tilde{s}_i \in \operatorname{Kern} p = \operatorname{Bild} i$. Sei $w \in M_0$ mit $i(w) = v - \sum_{i=1}^n r_i \tilde{s}_i$. Nun ist $w = \sum_{j=1}^m r'_j t_j$

$$\Rightarrow v = i(w) + \sum_{i=1}^n r_i \tilde{s}_i = \sum_{j=1}^m r'_j i(t_j) + \sum_{i=1}^n r_i \tilde{s}_i$$ □

14.17. Satz

Sei R ein Hauptidealring und $U \leqslant R^n$ ein Untermodul. Dann ist U endlich erzeugt.

Beweis
Induktion nach n:

n=0: Klar

n=1: Untermoduln von R sind genau die Ideale. Da R ein Hauptidealring ist, wird jedes Ideal von einem Element erzeugt.

n $\mapsto$ n+1: Sei $U \leqslant R^{n+1}$. Betrachte $p : R^{n+1} \twoheadrightarrow R$ mit $p(x_1, \dots, x_{n+1}) := x_{n+1}$. Wir erhalten eine kurze exakte Folge.

$$\begin{array}{rcc} R^n \cong \operatorname{Kern} p \hookrightarrow & R^{n+1} \overset{p}{\twoheadrightarrow} & R \\ & \cup\!| \qquad & \cup\!| \\ U \cap \operatorname{Kern} p \hookrightarrow & U \quad \twoheadrightarrow & p(U) \end{array}$$

dann ist auch eine kurze exakte Folge. Nach Induktionsvorraussetzung bzw. dem Fall $n = 1$ sind $U \cap \operatorname{Kern} p$ und $p(U)$ endlich erzeugt. Mit 14.16 folgt, dass U endlich erzeugt ist. □

14.18. Satz

Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es eine R-lineare Abbildung $f : R^m \to R^n$ mit $M \cong \operatorname{Koker}(f) = R^n/\operatorname{Bild} f$.

Beweis
Da M endlich erzeugt ist, folgt mit (14.12): $\exists p : R^n \twoheadrightarrow M$ surjektiv. Nun ist $\operatorname{Kern} p \subseteq R^n$ endlich erzeugt. Mit (14.12) folgt wieder: $\exists \tilde{f} : R^m \twoheadrightarrow \operatorname{Kern} p$ surjektiv. Wir erhalten also $f : R^m \to R^n$ mit $\operatorname{Bild} f = \operatorname{Kern} p$. Nun ist f die gesuchte Abbildung. Ein Isomorphismus

$$\operatorname{Koker}(f) = R^n/\operatorname{Bild} f = R^n/\operatorname{Kern}(p) \underset{\ni x + \operatorname{Kern}(p) \mapsto p(x)}{\to} M$$

wird von p induziert. □

14.19. Bemerkung

Sei $f: R^m \to R^n$ linear mit $f(e_j) = \begin{pmatrix} a_{ij} \\ \vdots \\ a_{nj} \end{pmatrix} = \sum_{i=1}^n a_{ij} e_i$. Dann gilt

$$f\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \sum_{j=1}^m x_j f(e_j) = \sum_{j=1}^m \sum_{i=1}^n x_j a_{ij} e_i = \sum_{i=1}^n \left(\sum_{j=1}^m x_j a_{ij} \right) \cdot e_i$$

Insbesondere werden R-lineare Abbildungen $R^m \to R^n$ durch $n \times m$-Matrizen über R beschrieben: $\mathrm{Hom}_R(R^m, R^n) \cong R^{n \times m}$

14.20. Elementarmatrizen

I) für $i \neq j, r \in R$

$$E(i,j;r) := \in R^{n \times m}$$

hier fehlen noch die Matrizen …

II) Für $i \neq j$

$$T(i,j) := \in R^{n \times m}$$

III) Für $i \in \{1, \dots, n\}, u \in R^\times$

$$E(i;u) := \in R^{n \times m}$$

Wie über Körper sind diese Elementarmatrizen **invertierbar** und entsprechen elementaren Zeilen- bzw. Spaltenumformungen.

14.21. Lemma

Seien $f_0, f_1 : R^m \to R^n$ R-linear und $\alpha : R^m \to R^m$ und $\beta : R^n \to R^n$ Isomorphismen mit $\beta \circ f_0 = f_1 \circ \alpha$. Dann gilt

$$\mathrm{Koker}\, f_0 \cong \mathrm{Koker}\, f_1$$

Beweis

$R^m \xrightarrow{f_0} R^n \to \mathrm{Koker}\, f_0 = {}^{R^n}\!/_{\mathrm{Bild}\, f_0}$ $R^m \xrightarrow{f_1} R^n \to \mathrm{Koker}(f_1) = {}^{R^n}\!/_{\mathrm{Bild}\, f_1}$ Definiere $h : {}^{R^n}\!/_{\mathrm{Bild}\, f_0} \to$

$$\begin{tikzcd}
R^m \arrow[r, "f_0"] \arrow[d, "\alpha"] & R^n \arrow[r] \arrow[d, "\beta"] & \mathrm{Koker}(f_0) = {}^{R^n}\!/_{\mathrm{Bild}\, f_0} \\
R^m \arrow[r, "f_1"] & R^n \arrow[r] & \mathrm{Koker}(f_1) = {}^{R^n}\!/_{\mathrm{Bild}\, f_1}
\end{tikzcd}$$

Abbildung 8: Diagramm zum Beweis von (14.21)

${}^{R^n}\!/_{\mathrm{Bild}\, f_1}$ durch $h(v + \mathrm{Bild}\, f_0) := \beta(v) + \mathrm{Bild}\, f_1$. Wegen

$$\beta(\mathrm{Bild}\, f_0) = f_1(\mathrm{Bild}(\alpha)) \subseteq \mathrm{Bild}\, f_1$$

ist dies wohldefiniert. Für $w + \mathrm{Bild}\, f_1$ ist $h(\beta^{-1}(w) + \mathrm{Bild}\, f_0) = w + \mathrm{Bild}\, f_1$, also h surjektiv. Ist $v + \mathrm{Bild}\, f_0$ mit $h(v + \mathrm{Bild}\, f_0) = 0$ so gilt: $\exists w \in R^m$ mit $\beta(v) = f_1(w)$. Dann $f_0(\alpha^{-1}(w)) = \beta^{-1}(f_1(w)) = v$. Also $v \in \mathrm{Bild}\, f_0 \Rightarrow v + \mathrm{Bild}\, f_0 = 0$. Damit ist h auch injektiv. $\square$

14.22. Korollar

Seien $A_0, A_1 \in R^{n\times m}$. Geht A_1 aus A_0 durch elementare Umformungen (Zeilen und Spalten) hervor, so gilt

$$\mathrm{Koker}\, A_0 \cong \mathrm{Koker}\, A_1$$

Beweis
(14.20) + (14.21) □

14.23. Satz

Sei R ein euklidischer Ring. Sei $A \in R^{n\times m}$. Dann gibt es eine Matrix

$$B = \begin{pmatrix} b_1 & & & 0 \\ & \ddots & & \\ & & b_k & \\ 0 & & & 0 \end{pmatrix}$$

die aus A durch Zeilen- und Spaltenumformungen hervorgeht. Weiter können wir erreichen: $b_1 \mid b_2$, $b_2 \mid b_3, \ldots b_{k-1} \mid b_k$.

Beweis
Sei oBdA $A \neq 0$. Sei $\mathfrak{M}$ die Menge aller Matrizen, die durch Zeilen- und Spaltenumformungen aus A hervorgehen und deren Eintrag an der Stelle $(1,1)$ nicht 0 ist. Sei $B_1 \in \mathfrak{M}$ so dass $b_1 := (1,1)$-Eintrag von B_1 von minimalem Grad ist. Dann teilt b_1 alle Einträge der ersten Zeile und der ersten Spalte, denn andernfalls könnten wir Division mit Rest und Zeilen/Spaltenumformungen benutzen um eine Matrix in $\mathfrak{M}$ zu finden, deren $(1,1)$-Eintrag von kleinerm Grad als b_1 ist. Durch weitere Umformungen finden wir nun

$$\begin{pmatrix} b_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B_1' & \\ 0 & & & \end{pmatrix} \in \mathfrak{M}$$

Indem wir das gleiche Verfahren auf B_1' anwenden, finden wir $\begin{pmatrix} b_1 & & \\ & b_2 & \\ & & B_2' \end{pmatrix} \in \mathfrak{M}$. Die Minimalität von b_1 impliziert $b_1 \mid b_2$. Induktiv folgt die Behauptung. □

14.24. Bemerkung

Bis auf Multiplikation mit Einheiten sind die b_i in (14.23) eindeutig.

14.25. Satz

Sei R ein euklidischer Ring und M ein endlich erzeugtes R-Modul. Dann gibt es $N \in \mathbb{N}_0$ und $a_1, \ldots, a_k \in R \setminus (\{0\} \cup R^\times)$ mit

$$M \cong R^N \oplus R/(a_1) \oplus \ldots \oplus R/(a_k) \quad \text{und} \quad a_1 \mid a_2, a_2 \mid a_3, \ldots, a_{k-1} \mid a_k$$

Beweis
Nach (14.18) gibt es $f : R^m \to R^n$ mit $M \cong \operatorname{Koker} f$. Nach (14.19) wird f durch $A \in R^{n\times m}$ beschrieben, also $M \cong \operatorname{Koker} A$. Wegen (14.22) und (14.23) können wir annehmen, dass

$$A = \begin{pmatrix} a_1 & & & 0 \\ & \ddots & & \\ & & a_k & \\ 0 & & & 0 \end{pmatrix}$$

ist. Dann ist $\operatorname{Koker} A \cong R/(a_1) \oplus \ldots \oplus R/(a_k) \oplus R^{n-k}$. Ist $a_i = 0$, so $R/(a_i) \cong R$. Ist $a_i \in R^\times$, so $R/(a_i) = 0$. Daher können wir annehmen, dass $a_i \notin \{0\} \cup R^\times$ für alle i. □

14.26. Beispiel

Sei $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ definiert durch $f(n+6\mathbb{Z}) := (n+2\mathbb{Z}, n+3\mathbb{Z})$. Ist $n+6\mathbb{Z} \in \operatorname{Kern} f$, so folgt $2 \mid n$ und $3 \mid n$, also $6 \mid n$. Daher ist f injektiv. Da $|\mathbb{Z}/6\mathbb{Z}| = 6 = 2 \cdot 3 = |\mathbb{Z}/2\mathbb{Z}| \cdot |\mathbb{Z}/3\mathbb{Z}|$ ist f auch surjektiv, also

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

14.27. Klassifikationssatz für endlich erzeugte $\mathbb{Z}$-Moduln

Sei M ein endlich erzeugtes $\mathbb{Z}$-Modul. Dann

$$M \cong \mathbb{Z}^d \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/q_l\mathbb{Z}$$

wobei die q_i Primzahlpotenzen sind. Weiter sind d und l eindeutig. Die q_i sind bis auf Umnummerierung auch eindeutig.

14.28. Proposition

Sei R ein Hauptidealring und $c = a \cdot b$ wobei a und b teilerfremd sind. Dann $R/(c) \cong R/(a) \oplus R/(b)$

Beweis
Betrachte $f : R/(c) \to R/(a) \oplus R/(b)$ mit $f\big(r + (c)\big) = \big(r + (a), r + (b)\big)$. Wie in Beispiel (14.26) ist f injektiv. Betrachte das Ideal $I = \{ra + sb \,|\, r, s \in R\}$. Da R ein Hauptidealring ist, ist $I = (x)$ für ein geeignetes $x \in I$. Da $a, b \in I$ teilt dann x sowohl a als auch b. Da a und b teilerfremd sind, ist x eine Einheit und $I = R$. Also gibt es $r, s \in R$ mit $1 = ra + sb$. Nun ist

$$\begin{aligned} f\big(ra + (c)\big) &= \big(ra + (a), ra + (b)\big) = (0, 1) \\ f\big(sb + (c)\big) &= \big(sb + (a), sb + (b)\big) = (1, 0) \end{aligned}$$

Also $f\big(xra + ysb + (c)\big) = \big(y + (a), x + (b)\big)$. Damit ist f auch surjektiv. □

A. Ausblick in die Algebra

A.1. Fundamentalsatz der Algebra

Jedes Polynom $p \in \mathbb{C}[X]$, $d(p) \geqslant 1$ hat eine Nullstelle.
Problem Finde die Nullstelle!
Beispiel: $X^2 + aX + b = (X + \frac{a}{2})^2 - \frac{a^2}{4} + b$ Nullstelle mit pq-Formel

A.2. Definition

$\rightsquigarrow$ *Minimalpolynom von α*

$\alpha \in \mathbb{C}$ heißt **algebraisch** (über $\mathbb{Q}$), falls es $p \in \mathbb{Q}[X], p \neq 0$ gibt mit $p(\alpha) = 0$.
Beispiel für algebraische Zahlen: $\frac{3}{7}, \sqrt{2}, \sqrt{\sqrt[3]{7} + 25\sqrt[7]{3}}$
Können wir alle algebraischen Zahlen so hinschreiben?

A.3. Definition

Sei $p \in \mathbb{Q}[X], p \neq 0$ irreduzibel. Sei $K \subseteq \mathbb{C}$ der kleinster Körper der alle Nullstellen von p enthält. Sei

$$\mathrm{Gal}(p) := \{\sigma : K \to K \text{ ist Körperautomorphismus}\}$$

A.4. Satz

Die Nullstellen von p lassen sich durch Wurzeln beschreiben $\iff$ $\mathrm{Gal}(p)$ ist auflösbar.

A.5. Konstruktion mit Zirkel und Lineal

Winkelteilung möglich, Winkeldreiteilung nicht möglich
Quadratur des Kreises ?

B. Fragestunde

B.1. Sind Linearfaktoren immer irreduzibel?

Sei $R = K[X]$. $p = X - \alpha$ $\alpha \in K$. $p = a \cdot b$ $d(p) = 1 \iff d(a) + d(b) = 1$. Also $d(a) = 0$ oder $d(b) = 0 \Rightarrow a \in K^\times$ oder $b \in K^\times$. Also sind Linearfaktoren irreduzibel

B.2. Beispiel $\mathbb{Z}[X]$

$2X - 2$ ist nicht irreduzibel. $2X - 2 = 2(X - 1)$

Index

Die Seitenzahlen *sind mit Hyperlinks zu den entsprechenden Seiten versehen, also anklickbar*

Abbildungsverzeichnis