§3 Polynomfunktionen

Sei K ein Körper. In Kapitel 1, §4, haben wir zu $A \in M_n(K)$ die Minimalgleichung $\mu_A \colon K \to K$ definiert $\rightsquigarrow$ "polynomiale" Gleichung für Eigenwerte. — Allgemein:

Definition 3.1. Sei K Körper und $V = \mathrm{Abb}(K, K)$.

Für $i \in \mathbb{N}_0$ definieren wir die Funktion $p_i \in V$ durch $p_i(x) := x^i$ für alle $x \in K$. (Für $i = 0$ ist $p_0(x) = x^0 = 1$ für alle $x \in K$.) Für $n \in \mathbb{N}_0$ heißt dann

$$P_n(K) := \langle p_0, p_1, \ldots, p_n \rangle_K \subseteq K$$

der Vektorraum der ***Polynomfunktionen*** vom Grade $\leqslant n$ über K.

Ist also $f \in P_n(K)$, so gibt es $a_0, a_1, \ldots, a_n \in K$ mit

(∗) $$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \qquad \text{für alle } x \in K.$$

Sei $\hat{P}_n(K)$ die Menge aller $f \in P_n(K)$, so dass (∗) gilt mit $a_n \neq 0$. (Dies ist kein Teilraum von $P_n(K)$!) Schließlich: Es gilt $P_0(K) \subseteq P_1(K) \subseteq P_2(K) \subseteq \ldots$, und

$$P(K) := \langle \{p_i \mid i \in \mathbb{N}_0\} \rangle_K = \bigcup_{n \geqslant 0} P_n(K)$$

ist der Vektorraum aller Polynomfunktionen über K.

Frage: Sind $\{p_0, p_1, \ldots, p_n\}$ linear unabhängig ? Im Allgemeinen NEIN !

Sei z.B. $K = \mathbb{F}_2$ und $f(x) = x + x^2$ für alle $x \in K$, also $f = p_1 + p_2$. Dann ist $f(0) = 0$ und $f(1) = 1 + 1 = 0$, also $f(x) = 0$ für alle $x \in K$, d.h., $p_1 + p_2 = \underline{0}$.

Damit sind $\{p_1, p_2\}$ in diesem Fall linear abhängig.

Ziel dieses (kurzen) Abschnittes: Klärung dieser Frage.

Lemma 3.2 (Horner–Schema)

Sei $n \geqslant 1$ und $f \in \hat{P}_n(K)$, d.h., es gibt $a_0, a_1, \ldots, a_n \in K$ mit $a_n \neq 0$ und $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ für alle $x \in K$. Sei $c \in K$ fest und definiere rekursiv wie folgt Elemente in K:

$$b_{n-1} := a_n, \qquad b_{n-2} := a_{n-1} + b_{n-1}c, \qquad b_{n-3} := a_{n-2} + b_{n-2}c,$$
$$\ldots, \qquad b_1 := a_2 + b_2 c, \qquad b_0 := a_1 + b_1 c, \qquad r := a_0 + b_0 c.$$

Sei $g \in \hat{P}_{n-1}(K)$ definiert durch $g(x) := b_0 + b_1 x + b_2 x^2 + \ldots + b_{n-1}x^{n-1}$ für alle $x \in K$. Dann gilt $f(x) = (x - c)g(x) + r$ für alle $x \in K$. Insbesondere also $f(c) = r$.

Beweis. Im Wesentlichen einfaches Nachrechnen. Für $x \in K$ gilt:

$$(x-c)g(x) = (x-c)\sum_{i=0}^{n-1} b_i x^i = \sum_{i=0}^{n-1} b_i x^{i+1} - \sum_{i=0}^{n-1} b_i c x^i = \sum_{i=1}^{n} b_{i-1} x^i - \sum_{i=0}^{n-1} b_i c x^i$$

$$= \underbrace{b_{n-1}}_{=a_n} x^n - \underbrace{b_0 c}_{r-a_0} + \sum_{i=1}^{n-1} \underbrace{(b_{i-1} - b_i c)}_{=a_i} x^i = f(x) - r. \qquad \square$$

Bemerkung. Rechnet man $c, c^2, \ldots, c^n$ aus und dann $f(c) = a_0 + a_1 c + \ldots + a_n c^n$, so braucht man insgesamt n Additionen und $2n-1$ Multiplikationen. Benutzt man Horner-Schema, so benötigt man auch n Additionen, aber nur n Multiplikationen !

Sei zum Beispiel $f(x) = -3 - 11x + 5x + 2x^3$ und $c = 2$, wobei $K = \mathbb{Q}$.

Horner-Schema:

$$\begin{array}{r|cccc} f: & 2 & 5 & -11 & -3 \\ c=2: & \downarrow & +2\cdot 2 = 4 & +2 \cdot 9 = 18 & +2 \cdot 7 = 14 \\ \hline g: & 2 & 9 & 7 & \boxed{11} \end{array}$$

Dann ist $g(x) = 2x^2 + 9x + 7$ und $r = f(2) = 11$. — Nachrechnen:

$(x-2)(2x^2+9x+7) = 2x^3 + 9x^2 + 7x - 4x^2 - 18x - 14 = f(x) - 11$.

Folgerung 3.3

Sei $n \geqslant 1$ und $f \in \hat{P}_n(K)$. Dann hat f höchstens n Nullstellen in K.
(Eine Nullstelle von f ist ein Element $c \in K$ mit $f(c) = 0$.)

Beweis. (Vollständige Induktion nach n.) Für $n = 1$ ist $f(x) = a_0 + a_1 x$ mit $a_1 \neq 0$. Also gibt es genau $n = 1$ Nullstelle, nämlich $c = -a_0 a_1^{-1}$. Sei nun $n \geqslant 2$ und Aussage bereits gezeigt für alle $g \in \hat{P}_{n-1}(K)$. Sei $f \in \hat{P}_n(K)$. Annahme: es gibt paarweise verschiedene $c_1, \ldots, c_{n+1} \in K$ mit $f(c_i) = 0$ für $1 \leqslant i \leqslant n+1$. Nach Lemma 3.2 gibt es ein $g \in \hat{P}_{n-1}(K)$ mit $f(x) = (x - c_{n+1})g(x)$ für alle $x \in K$. Nach Induktionsannahme hat also g höchstens $n-1$ Nullstellen. Für $1 \leqslant i \leqslant n$ gilt dann aber $0 = f(c_i) = (c_i - c_{n+1})g(c_i)$. Wegen $c_i \neq c_{n+1}$ folgt also $g(c_i) = 0$ für $1 \leqslant i \leqslant n$, d.h., g hat n Nullstellen, Widerspruch. □

Folgerung 3.4

Sei $n \geqslant 1$ und K Körper mit $|K| > n$. Dann sind $(p_0, p_1, \ldots, p_n)$ linear unabhängig.

Beweis. Seien $s_0, s_1, \ldots, s_n \in K$ mit $s_0 p_0 + s_1 p_1 + \ldots + s_n p_n = \underline{0}$.
Annahme: es gibt ein i mit $s_i \neq 0$. Sei dann $m := \max\{i \mid s_i \neq 0\}$; also:

$(*) \qquad s_0 p_0 + s_1 p_1 + \ldots + s_m p_m = \underline{0}$ mit $m \leqslant n$ und $s_m \neq 0$.

Setze $f(x) := s_0 + s_1 x + s_2 x^2 + \ldots + s_m x^m$ für alle $x \in K$. Dann ist $f \in \hat{P}_m(K)$ und mit $(*)$ folgt $f(x) = 0$ für alle $x \in K$. Nach Folgerung 3.3 hat f aber höchstens $m \leqslant n$ Nullstellen, also folgt $|K| \leqslant m \leqslant n$, Widerspruch. $\square$

Satz 3.5

Sei $n \geqslant 1$ und K Körper mit $|K| > n$. Dann lässt sich jedes $f \in P_n(K)$ auf eindeutige Weise schreiben als $f = a_0 p_0 + a_1 p_1 + \ldots + a_n p_n$ mit $a_i \in K$.
D.h., gilt $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ für alle $x \in K$, so sind die Koeffizienten a_i eindeutig bestimmt.

Beweis. Haben bereits am Anfang des Abschnittes gesehen, dass $P_n(K) = \langle p_0, p_1, \ldots, p_n \rangle_K$ gilt. Nach Folgerung 3.4 sind $(p_0, p_1, \ldots, p_n)$ linear unabhängig. Eindeutigkeit der Darstellung folgt also aus Lemma 2.7. $\square$

Beispiel 3.6

Seien $x_1, \ldots, x_n \in K$ paarweise verschieden. Dann ist die sogenannte ***Vandermonde-Matrix***

$$V(x_1, \ldots, x_n) := \begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{bmatrix} \in M_n(K) \quad \text{invertierbar.}$$

Beweis. Wir zeigen, dass das homogene lineare Gleichungssystem mit Matrix $V := V(x_1, \ldots, x_n)$ nur die Lösung 0_n hat. Sei also $c \in K^n$ mit Komponenten $c_0, c_1, \ldots, c_{n-1} \in K$ und so dass $Vc = 0_n$ gilt. Dann ist für $1 \leqslant i \leqslant n$ die i-te Komponente von $Vc = 0_n$ gegeben durch: $\quad c_0 + c_1 x_i + c_2 x_i^2 + \ldots + c_{n-1} x_i^{n-1} = 0.$ Definieren wir also $f \in P_{n-1}(K)$ durch $f(x) := c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1}$ für alle $x \in K$, so hat f die n Nullstellen $x_1, \ldots, x_n$. Nehmen wir an, nicht alle c_i sind gleich 0. Setzen wir $m := \max\{i \mid c_i \neq 0\}$, so ist also $f \in \hat{P}_m(K)$. Nach Folgerung 3.3 kann dann f aber höchstens $m \leqslant n-1$ Nullstellen haben, Widerspruch. $\square$

§4 Basis und Dimension

Voraussetzung wie üblich: V Vektorraum über beliebigem Körper K.

Definition 4.1. Sei S eine beliebige Teilmenge von V.

(a) Ist S endlich und $S \neq \varnothing$, so sei $n := |S| \geqslant 1$ und $S = \{v_1, \dots, v_n\}$. Dann heißt S ***linear unabhängig*** (l.u.), wenn das Tupel $(v_1, \dots, v_n)$ l.u. ist (siehe Definition 2.6).

(b) Ist $|S| = \infty$, so heißt S l.u., wenn jede endliche Teilmenge l.u. ist (siehe (a)).
(Die leere Menge $S = \varnothing$ wird auch als l.u. definiert.)

(c) S heißt eine ***Basis*** von V, wenn S l.u. ist und $V = \langle S \rangle_K$ gilt.

Haben bereits mehrere Beispiele in §2, §3 gesehen:

- Sei $V = K^n$ (Spaltenvektoren). Dann ist $B = \{e_1, \dots, e_n\}$ eine Basis, wobei e_i die Einheitsvektoren in Beispiel 2.1 sind.
- Sei $V = P_n(K)$ (Polynomfunktionen vom Grad $\leqslant n$) mit $|K| > n \geqslant 1$. Dann ist $B = \{p_0, p_1, \dots, p_n\}$ eine Basis, siehe §3. Hier $p_i(x) = x^i$ für $x \in K$.

Hauptsatz 4.2. (Basissatz) Sei V e.e. (endlich erzeugt). Dann gilt:

(a) Es gibt eine Basis von V mit endlich vielen Elementen.
Genauer: Ist $S \subseteq V$ beliebige Teilmenge mit $V = \langle S \rangle_K$, so gibt es eine endliche Teilmenge $B \subseteq S$, so dass B eine Basis von V ist.

(b) Sind B_1, B_2 zwei beliebige Basen von V, so gilt $|B_1| = |B_2| < \infty$.
Also: Je zwei Basen von V haben gleich viele Elemente.

Beweis. (a) Nach Voraussetzung gibt es $v_1, \ldots, v_n \in V$ mit $V = \langle v_1, \ldots, v_n \rangle_K$. Sei nun $S \subseteq V$ mit $V = \langle S \rangle_K$. Dann gibt es $w_1, \ldots, w_m \in S$ mit $v_i = \sum_{j=1}^m a_{ij} w_j$ mit $a_{ij} \in K$. Also gilt $v_1, \ldots, v_n \in \langle w_1, \ldots, w_m \rangle_K$ und damit auch $V = \langle w_1, \ldots, w_m \rangle_K$, d.h., wir können eine endliche Teilmenge $S' \subseteq S$ finden mit $V = \langle S' \rangle_K$. Sei nun $B \subseteq S'$ mit $|B'|$ minimal and so dass $V = \langle B \rangle_K$ gilt. (Der Fall $B = S'$ ist hier natürlich erlaubt und möglich.) Behauptung: B ist eine Basis von V. Dazu müssen wir nur noch zeigen, dass B l.u. ist. Ist $B = \varnothing$, so ist dies klar nach Definition 4.1.

Sei nun $|B| = d \geqslant 1$ und schreibe $B = \{b_1, \ldots, b_d\}$. Wäre das Tupel $(b_1, \ldots, b_d)$ l.a., so gäbe es nach Lemma 2.9 ein $j \in \{1, \ldots, d\}$ mit

$$V = \langle b_1, \ldots, b_d \rangle_K = \langle b_1, \ldots, b_{j-1}, b_{j+1}, \ldots, b_d \rangle_K .$$

D.h., V könnte auch mit einer Teilmenge von S mit $d-1$ Elementen erzeugt werden, Widerspruch zur Minimalität von $|B| = d$. Also ist $B = \{b_1, \ldots, b_d\}$ l.u.

(b) In (a) haben wir eine endliche Basis B gefunden; sei $|B| = d \geqslant 0$. Ist $d = 0$, so ist $V = \{0_V\}$ und die Aussage klar. Sei nun $d \geqslant 1$ und B_1 eine weitere Basis. Folgerung 2.10: Wegen $V = \langle B \rangle_K$ gilt $m \leqslant d$ für jedes m-Tupel von l.u. Vektoren in V. Also folgt auch $|B_1| \leqslant d$. Analog: Wegen $V = \langle B_1 \rangle_K$ und weil B l.u. ist, gilt auch $|B| = d \leqslant |B_1|$. Also schließlich $|B_1| = d = |B|$. $\square$

Definition 4.3

Ist V e.e., so haben nach Hauptsatz 4.2 alle Basen die gleiche endliche Anzahl von Elementen. Ist B eine dieser Basen, so heißt $\dim V := |B|$ die ***Dimension*** von V. Ist V nicht e.e., so setzen wir $\dim V := \infty$.

Beispiel 4.4

(a) $\dim V = 0 \Leftrightarrow V = \langle\varnothing\rangle_K = \{0_V\}$; $\quad \dim V = 1 \Leftrightarrow V = Kv$ für ein $0_V \neq v \in V$.

(b) $\dim K^n$, denn $B = \{e_1, \ldots, e_n\}$ ist eine Basis von K^n.

Allgemeiner: $\dim K^{m\times n} = mn$, denn $B = \{E_{ij}^{(m,n)} \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$ ist eine Basis von $K^{m\times n}$ (siehe Kapitel 1, Bemerkung 1.11).

(c) Ist $|K| > n$, so $\dim P_n(K) = n+1$, denn $B = \{p_0, p_1, \ldots, p_n\}$ ist eine Basis.

(d) Sei X Menge mit $|X| = \infty$. Dann ist $\dim \mathrm{Abb}(X,K) = \infty$, denn die Menge $\{f_y \mid y \in X\}$ ist l.u., siehe Beispiel 2.12(b).

Bemerkung 4.5

Ist V nicht e.e., so gilt weiterhin, dass V eine Basis besitzt und je zwei Basen gleichmächtig sind. Der allgemeine Beweis benutzt das ***Auswahlaxiom*** (§6, Kap. 0) und ist nicht konstruktiv. Betrachte als Beispiel den $\mathbb{Q}$-Vektorraum $\mathbb{R}$. Nach Beispiel 2.13 ist dieser nicht e.e., also $\dim \mathbb{R} = \infty$. Es gibt eine Basis — aber niemand weiss, wie so eine Basis konkret aussieht !

Satz 4.6. Sei V e.e. und $n = \dim V$.

Sei $B = \{v_1, \dots, v_n\}$ Basis von V. Nach Lemma 2.7 lässt sich jedes $v \in V$ eindeutig schreiben als $v = \sum_{i=1}^n x_i v_i$ mit $x_i \in K$. Dann heißt

$$M_B(v) := \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in K^n$$ der ***Koordinatenvektor*** von v (bezüglich B).

Die Abbildung $\kappa_B \colon V \to K^n$, $v \mapsto M_B(v)$, ist ein Vektorrraum-Isomorphismus.

Beweis. Wegen $V = \langle B \rangle_K$ lässt sich jedes $v \in V$ wie oben schreiben; wegen B l.u. ist die Darstellung eindeutig (siehe Lemma 2.7). Also ist $\kappa_B \colon V \to K^n$ bijektiv. Man rechnet sofort nach, dass κ_B linear ist. Umkehrabbildung:

$$\psi_B \colon K^n \to V, \qquad \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \mapsto \sum_{i=1}^n x_i v_i.$$

□

Beispiel 4.7

(a) Sei V e.e. und $n = \dim V$. Dann gilt $|V| = |K^n|$ (gleiche Mächtigkeit).

Denn sei B eine Basis von V. Nach Satz 4.6 erhalten wir einen Isomorphismus $\kappa_B \colon V \to K^n$. Insbesondere ist κ_B bijektiv, also $|V| = |K^n|$.

- Ist also $|K| = \infty$, so gilt auch $|V| = \infty$.
- Ist p Primzahl und $K = \mathbb{F}_p$ Körper mit p Elementen, so folgt $|V| = |\mathbb{F}_p^n| = p^n$.

(b) Sei $X = \{x_1, \dots, x_n\}$ endliche Menge mit $|X| = n \geqslant 1$. Nach Beispiel 1.3(c) ist $V = \mathcal{P}(X)$ ein $\mathbb{F}_2$-Vektorraum mit Addition $S + T := (S \cup T) \setminus (S \cap T)$ (symmetrische Differenz). Sei $v_i := \{x_i\} \in V$ für $1 \leqslant i \leqslant n$. Dann ist

$$B := \{v_1, \dots, v_n\} \text{ eine Basis von } V.$$

Denn sei $Y \subseteq X$ beliebige Teilmenge, $Y = \{x_{i_1}, \dots, x_{i_r}\}$ mit $1 \leqslant i_1 < \dots < i_r \leqslant n$. Dann hat Y die eindeutige Darstellung $Y = \{x_{i_1}\} \cup \dots \cup \{x_{i_r}\} = v_{i_1} + \dots + v_{i_r}$.

Also folgt $\dim V = n$ und damit nach (a) auch $|\mathcal{P}(X)| = |V| = 2^n$.

Lemma 4.8. Gegeben seien $v, v_1, \ldots, v_n \in V$, wobei $n \geqslant 1$.

Ist $(v_1, \ldots, v_n)$ l.u. und $v \notin \langle v_1, \ldots, v_n \rangle_K$, so ist auch $(v_1, \ldots, v_n, v)$ l.u.

Beweis. (Kontraposition.) Setze $v_{n+1} := v$; sei $(v_1, \ldots, v_n, v_{n+1})$ linear abhängig. Dann gibt es nach Lemma 2.9 ein $j \in \{1, \ldots, n+1\}$ mit $v_j \in \langle v_1, \ldots, v_{j-1} \rangle_K$. Ist $j \leqslant n$, so gibt es $s_1, \ldots, s_{j-1} \in K$ mit $v_j = s_1 v_1 + \ldots + s_{j-1} v_j$, also

$$s_1 v_1 + \ldots + s_{j-1} v_{j+1} + (-1) s_j + 0 \cdot v_{j+1} + \ldots + 0 \cdot v_n = 0,$$

d.h., $(v_1, \ldots, v_n)$ ist l.a. Ist $j = n+1$, so gilt $v = v_{n+1} \in \langle v_1, \ldots, v_n \rangle_K$. $\square$

Satz 4.9. Sei V e.e. und $n := \dim V < \infty$.

Sei $B = \{v_1, \ldots, v_n\}$ eine Teilmenge mit n Elementen.

(a) Ist $V = \langle B \rangle_K$, so ist B eine Basis.

(b) Ist B l.u., so ist B eine Basis.

Beweis. (a) Wegen $V = \langle B \rangle_K$ gibt es nach Hauptsatz 4.2(a) eine Basis $B' \subseteq B$. Nach Hauptsatz 4.2(b) gilt dann $\dim V = n = |B'|$, also muss $B' = B$ sein.

(b) Sei $v \in V$ beliebig. Wäre $v \notin \langle B \rangle_K$, dann $(v_1, \dots, v_n, v)$ l.u. nach Lemma 4.8, Widerspruch zu Folg. 2.10. Also ist $v \in \langle B \rangle_K$. Da v beliebig, folgt $V = \langle B \rangle_K$. $\square$

Beispiel 4.10. Gegeben sei eine quadratische Matrix $A \in M_n(K)$.

Für $1 \leqslant j \leqslant n$ sei $\quad v_j := \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{bmatrix} \in K^n \quad$ die j-te Spalte von A.

Dann sind folgende Aussagen äquivalent:

(a) Die Menge $B := \{v_1, \dots, v_n\}$ ist eine Basis von $V = K^n$.

(b) Das Tupel $(v_1, \dots, v_n)$ ist linear unabhängig.

(c) Das homogene lineare Gleichungssystem mit Matrix A hat nur die Lösung 0_n.

(d) A ist invertierbar.

(e) Mit dem Gauß-Algorithmus gilt $A \to I_n$.

(Nach Satz 4.9(b) gilt “(a) $\Leftrightarrow$ (b)”; nach Beispiel 2.8 gilt “(b) $\Leftrightarrow$ (c)”; nach Kapitel 1, Satz 3.7, gilt “(c) $\Leftrightarrow$ (d) $\Leftrightarrow$ (e)”.)

Satz 4.11. Sei V e.e. und $n = \dim V$.

Sei $U \leqslant V$ ein Teilraum. Dann ist auch U e.e. und es gilt $\dim U \leqslant n$.
Ist $U \subsetneqq V$, so gilt auch $\dim U < n$.

Beweis. Ist $U = \{0_V\}$, so ist nichts zu zeigen. Sei nun $U \neq \{0_V\}$.
Nehmen wir an, U ist nicht e.e.
Sei $0_V \neq v_1 \in U$. Dann ist (v_1) l.u. und $\langle v_1 \rangle_K \subsetneqq U$ (weil U nicht e.e.). Wähle $v_2 \in V \setminus \langle v_1 \rangle_K$. Nach Lemma 4.8 ist (v_1, v_2) l.u. und $\langle v_1, v_2 \rangle_K \subsetneqq U$ (wieder weil U nicht e.e.). Wähle $v_3 \in U \setminus \langle v_1, v_2 \rangle_K$. Dann ist (v_1, v_2, v_3) l.u. und $\langle v_1, v_2, v_3 \rangle_K \subsetneqq U$.
Wir fahren auf diese Weise fort, bis wir ein l.u. Tupel $(v_1, v_2, \ldots, v_{n+1})$ mit $v_i \in U$ erhalten. Aber $\dim V = n$, also Widerspruch zu Folgerung 2.10.
Also ist U e.e.; sei $d := \dim U < \infty$. Eine Basis von U ist eine l.u. Teilmenge von V, also gilt $d \leqslant n$ (wieder nach Folgerung 2.10). Ist $d = n$, so ist Basis von U auch Basis von V (siehe Satz 4.9), also $U = V$. $\square$

Satz 4.12 (Basisergänzungssatz). Sei V e.e. und $n = \dim V \geqslant 1$.

Sei $d \geqslant 0$ und $S = \{v_1, \ldots, v_d\} \subseteq V$ l.u. (also $S = \varnothing$ falls $d = 0$).
Nach Folgerung 2.10 gilt $d \leqslant n$. Ist $d = n$, so ist S eine Basis von V (siehe Satz 4.9). Ist $d < n$, so gibt es $n - d$ Vektoren $v_{d+1}, \ldots, v_n \in V$, so dass $B := \{v_1, \ldots, v_d, v_{d+1}, \ldots, v_n\}$ eine Basis von V ist.

Beweis. Sei $d < n$. Dann ist $\langle S \rangle_K \subsetneqq V$ (sonst wäre S eine Basis mit weniger als n Elementen). Also gibt es ein $v \in V$ mit $v \notin \langle S \rangle_K$.
Setze $v_{d+1} := v$. Nach Lemma 4.8 ist dann $S' := \{v_1, \ldots, v_d, v_{d+1}\}$ wiederum l.u.
Ist $d + 1 < n$, so wiederholen wir obiges Argument mit S' anstelle von S. Es gibt dann also ein $v' \in V$ mit $v' \notin \langle S' \rangle_K$.
Setze $v_{d+2} := v'$. Dann ist wiederum $S'' := \{v_1, \ldots v_d, v_{d+1}, v_{d+2}\}$ l.u.
Ist $d + 2 < n$, so wiederholen wir obiges Argument mit S'' anstelle von S'.

Nach insgesamt $n - d$ Wiederholungen finden wir $v_{d+1}, \ldots, v_n \in V$, so dass $\{v_1, \ldots, v_d, v_{d+1}, \ldots, v_n\}$ l.u., also eine Basis ist. $\square$

Hauptsatz 4.13. (Kern-Bild-Dimensionsformel)

Seien V und W Vektorräume über K und $\varphi\colon V \to W$ eine lineare Abbildung.
Ist V e.e., so sind auch Kern(φ) und Bild(φ) e.e., und es gilt

$$\dim V = \dim \mathrm{Kern}(\varphi) + \dim \mathrm{Bild}(\varphi).$$

Beweis. Da Kern$(\varphi) \leqslant V$ Teilraum und V e.e. ist, folgt aus Satz 4.11, dass auch Kern(φ) e.e. ist. Seien $v_1, \ldots, v_n \in V$ so dass $V = \langle v_1, \ldots, v_n \rangle_K$ gilt. Aus Lemma 2.4 folgt dann Bild$(\varphi) = \langle \varphi(v_1), \ldots, \varphi(v_n) \rangle_K$, also ist auch Bild$(\varphi)$ e.e.

Sei nun $n = \dim V$ und $d = \dim \mathrm{Kern}(\varphi)$; dann ist $d \leqslant n$.

Ist $d = n$, so ist $V =$ Kern(φ) (siehe Satz 4.9), also $\varphi(v) = 0_W$ für alle $v \in V$.
Damit folgt Bild$(\varphi) = \{0_W\}$ und die Dimensionsformel gilt.

Sei nun $d < n$. Sei $\{v_1, \ldots, v_d\}$ eine Basis von Kern(φ). Nach Satz 4.12 gibt es $v_{d+1}, \ldots, v_n \in V$, so dass $\{v_1, \ldots, v_d, v_{d+1}, \ldots, v_n\}$ eine Basis von V ist.

Behauptung: $\{\varphi(v_{d+1}), \ldots, \varphi(v_n)\}$ ist eine Basis von Bild(φ).

(Dann folgt auch $\dim$ Bild$(\varphi) = n - d = \dim V - \dim$ Kern(φ) und wir sind fertig.)

Dazu: Weil $V = \langle v_1, \ldots, v_n \rangle_K$ gilt und $\varphi(v_1) = \ldots = \varphi(v_d) = 0_W$, folgt

$$\text{Bild}(\varphi) = \langle \varphi(v_1), \ldots, \varphi(v_n) \rangle_K = \langle \varphi(v_{d+1}), \ldots, \varphi(v_n) \rangle_K .$$

Also ist $\{\varphi(v_{d+1}), \ldots, \varphi(v_n)\}$ ein Erzeugendensystem für Bild(φ).

Wir müssen noch zeigen, dass das Tupel $\big(\varphi(v_{d+1}), \ldots, \varphi(v_n)\big)$ l.u. ist.

Dazu seien $s_{d+1}, \ldots, s_n \in K$ mit

$$0_W = s_{d+1}\varphi(v_{d+1}) + \ldots + s_n\varphi(v_n) = \varphi\big(s_{d+1}v_{d+1} + \ldots + s_n v_n\big).$$

Dann ist $s_{d+1}v_{d+1} + \ldots + s_n v_n \in$ Kern(φ), also gibt es $s_1, \ldots, s_d \in K$ mit

$$s_{d+1}v_{d+1} + \ldots + s_n v_n = s_1 v_1 + \ldots + s_n v_d.$$

Damit erhalten wir eine Linearkombination

$$s_1 v_1 + \ldots + s_n v_d - s_{d+1}v_{d+1} - \ldots - s_n v_n = 0_W.$$

Weil das Tupel $(v_1, \ldots, v_n)$ l.u. ist, folgt $s_1 = \ldots = s_n = 0$,

also insbesondere $s_{d+1} = \ldots = s_n = 0$. $\square$

Beispiel 4.14

Seien V, W e.e. Vektorräume über K und $\varphi\colon V \to W$ eine lineare Abbildung.

- Ist φ bijektiv, dann gilt $\dim V = \dim W$.

(Denn in diesem Fall ist Bild$(\varphi) = W$ und Kern$(\varphi) = \{0_V\}$, also $\dim V = \dim$ Kern$(\varphi) + \dim$ Bild$(\varphi) = \dim W$; siehe Satz 4.13.) Außerdem folgt:

- Ist $n = \dim V$ und $B = \{v_1, \ldots, v_n\}$ eine Basis von V, so ist $\{\varphi(v_1), \ldots, \varphi(v_n)\}$ eine Basis von W.

(Denn $W =$ Bild$(\varphi) = \langle\varphi(v_1), \ldots, \varphi(v_n)\}$ und die Aussage folgt aus Satz 4.9(a).)

- Ist $\dim V = \dim W$ so gilt: $\quad \varphi$ bijektiv $\quad\Leftrightarrow\quad \varphi$ injektiv $\quad\Leftrightarrow\quad \varphi$ surjektiv.

(Denn: Ist φ bijektiv, so ist φ natürlich injektiv und surjektiv.
Nun betrachte $\dim W = \dim V = \dim$ Kern$(\varphi) + \dim$ Bild(φ). Ist φ injektiv, so $\dim$ Kern$(\varphi) = 0$, also $\dim$ Bild$(\varphi) = \dim W$, d.h., φ auch surjektiv. Ist φ surjektiv, so $\dim W = \dim$ Bild(φ), also $\dim$ Kern$(\varphi) = 0$, d.h., φ auch injektiv.)

Satz 4.15. Seien $U_1, U_2 \leqslant V$ e.e. Teilräume.

(a) Dann ist $U_1 \times U_2$ e.e. und $\dim(U_1 \times U_2) = \dim U_1 + \dim U_2$.

(b) $\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$.

Beweis. (a) Sei B_1 Basis von U_1 und B_2 Basis von U_2. In Aufgabe 12.2 wird gezeigt, dass $B := \{(b, 0_{U_2}) \mid b \in B_1\} \cup \{(0_{U_1}, b) \mid b \in B_2\}$ Basis von $U_1 \times U_2$ ist.
Also $\dim(U_1 \times U_2) = |B| = |B_1| + |B_2| = \dim U_1 + \dim U_2$.

(b) Sei $U := U_1 + U_2 \leqslant V$. Betrachte die lineare Abbildung

$$\varphi\colon U_1 \times U_2 \to V, \qquad (u_1, u_2) \mapsto u_1 + u_2.$$

Dann ist $\text{Bild}(\varphi) = U$ und $\text{Kern}(\varphi) = \{(u, -u) \mid u \in U_1 \cap U_2\}$; siehe Satz 1.13.
Mit Satz 4.13 folgt also $\dim U = \dim(U_1 \times U_2) - \dim \text{Kern}(\varphi)$. Die Abbildung

$$\psi\colon U_1 \cap U_2 \to \text{Kern}(\varphi), \qquad u \mapsto (u, -u),$$

ist linear und bijektiv, also folgt mit Beispiel 4.14 auch $\dim(U_1 \cap U_2) = \dim \text{Kern}(\varphi)$.
Damit erhalten wir insgesamt

$$\dim U = \dim(U_1 \times U_2) - \dim \text{Kern}(\varphi) \overset{(a)}{=} \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2). \qquad \square$$

Kapitel 3: Lineare Abbildungen, Matrizen und Polynome

§1 Der Rang einer Matrix

Voraussetzung wie üblich: V Vektorraum über beliebigem Körper K.

Wir wenden nun die Ergebnisse des letzten Kapitels auf Matrizen und lineare Gleichungssysteme an. Gegeben sei eine beliebige Matrix $A \in K^{m \times n}$.

- Sei $\mathsf{SR}(A) \subseteq K^m$ der Spaltenraum von A.
  Dann heißt $\dim \mathsf{SR}(A)$ der ***Spaltenrang*** von A.
- Sei $\mathsf{ZR}(A) \subseteq K^n$ der Zeilenraum von A.
  Dann heißt $\dim \mathsf{ZR}(A)$ der ***Zeilenrang*** von A.

Was wir bereits wissen (siehe §2):

Betrachte die lineare Abbildung $\varphi_A \colon K^n \to K^m$, $v \mapsto Av$. Dann ist

$$\mathsf{SR}(A) = \mathsf{Bild}(\varphi_A) = \{Av \mid v \in K^n\} \text{ und}$$
$$\mathsf{Kern}(\varphi_A) = N(A) := \{v \in K^n \mid Av = 0_m\}.$$

Also folgt mit Kern-Bild-Dimensionsformel: $\boxed{n = \dim N(A) + \dim \mathsf{SR}(A).}$

Bemerkung 1.1. Wie oben sei $A^{m\times n}$ gegeben.

Nach Kapitel 1, §2, ändert sich die Lösungsmenge $N(A) = \{x \in K^n \mid Ax = 0_m\}$ nicht bei elementaren Zeilenumformungen. Sei $A' \in K^{m\times n}$ in Zeilenstufenform und $A \to A'$ (Gauß-Algorithmus). Dann folgt also

$$\dim \mathsf{SR}(A) = n - \dim N(A) = n - \dim N(A') = \dim \mathsf{SR}(A').$$

d.h., der Spaltenrang ändert sich nicht bei elementaren Zeilenumformungen.

Beispiel 1.2. Wir betrachten das Beispiel aus Kapitel 1, §2:

$$A = \begin{bmatrix} 0 & 0 & 2 & 2 & 0 & 2 \\ 2 & 4 & 2 & 6 & 0 & 4 \\ 3 & 6 & 0 & 6 & 1 & 4 \end{bmatrix} \quad \to \quad A' = \begin{bmatrix} 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Also $r = 3$ Stufen; Pivots $j_1 = 1$, $j_2 = 3$, $j_3 = 5$; freie Variablen x_2, x_4, x_6.

Zugehöriges homogenes Gleichungssystem:
$$\begin{aligned} x_1 + 2x_2 + 2x_4 + x_6 &= 0 \\ x_3 + x_4 + x_6 &= 0 \\ x_5 + x_6 &= 0 \end{aligned}.$$

Damit ist $N(A) = N(A') = \{v(x_2, x_4, x_5) \mid x_2, x_4, x_6 \in \mathbb{Q}$ beliebig$\}$, wobei

$$v(x_2,x_4,x_5) := \begin{bmatrix} -2x_2 - 2x_4 - x_6 \\ x_2 \\ -x_4 - x_6 \\ x_4 \\ -x_6 \\ x_6 \end{bmatrix} \qquad \left(\text{System :} \quad \begin{aligned} \color{blue}{x_1} + 2x_2 + 2x_4 + x_6 &= 0 \\ \color{blue}{x_3} + x_4 + x_6 &= 0 \\ \color{blue}{x_5} + x_6 &= 0 \end{aligned}\right)$$

Wie erhält man eine Basis für $N(A)$? Dazu bemerken wir, dass $v(x_2,x_4,v_6) = x_2 v(1,0,0) + x_4 v(0,1,0) + x_6 v(0,0,1)$ gilt, mit

$$v(\color{blue}{1},0,0) := \begin{bmatrix} -2 \\ \color{blue}{1} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \qquad v(0,\color{blue}{1},0) := \begin{bmatrix} -2 \\ 0 \\ -1 \\ \color{blue}{1} \\ 0 \\ 0 \end{bmatrix}, \qquad v(0,0,\color{blue}{1}) := \begin{bmatrix} -1 \\ 0 \\ -1 \\ 0 \\ -1 \\ \color{blue}{1} \end{bmatrix}.$$

Behauptung: $v(1,0,0), v(0,1,0), v(0,0,1)$ sind l.u. Denn sind $s_1, s_2, s_3 \in \mathbb{Q}$, so ist $s_1 v(1,0,0) + s_2 v(0,1,0) + s_3 v(0,0,1) = v(s_1,s_2,s_3)$, wobei die 2. Komponente dieses Spaltenvektors gleich s_1 ist, die 4. Komponente gleich s_2 und die 6. Komponente gleich s_3. Gilt also $v(s_1,s_2,s_3) = 0_6$, so folgt $s_1 = s_2 = s_3 = 0$.