3. Vektorräume

(3.1) Def.: Ein Vektorraum über einem Körper K ist eine abelsche Gruppe $(V,+)$ zusammen mit einer Abbildung $K \times V \to V$, $(\alpha, v) \in K \times V \mapsto \alpha v$, so daß für alle $\alpha, \beta \in K$ und alle $v, w \in V$ gilt:

(i) $\alpha(\beta v) = (\alpha\beta)v \quad (=: \alpha\beta v)$
(ii) $(\alpha+\beta)v = (\alpha v) + (\beta v) \quad (=: \alpha v + \beta v)$
(iii) $\alpha(v+w) = (\alpha v) + (\alpha w) \quad (=: \alpha v + \alpha w)$
(iv) $1v = v$ (, wobei 1 das Einselement von K bezeichnet!)

Sprechweisen und Bezeichnungen:
"Punkt vor Strich" $\alpha v + \beta w := (\alpha v) + (\beta w)$, außerdem: $v - w := v + (-w)$
Vektorraum über einem Körper K = K-Vektorraum

Das neutrale Element von $(V,+)$ wird (zunächst) mit $\underline{0}$ bezeichnet, zur Unterscheidung vom neutralen Element 0 von $(K,+)$.

Elemente von V werden "Vektoren" (des Vektorraums V) genannt, Elemente des Körpers werden auch "Skalare" genannt.

Beispiele:

1) $K := \mathbb{R}$ und $V := \mathbb{R}^n$ mit den vor (1.15) eingeführten Operationen
$$(x_1,\ldots,x_n) + (y_1,\ldots,y_n) := (x_1+y_1,\ldots,x_n+y_n)$$
$$r(x_1,\ldots,x_n) := (rx_1,\ldots,rx_n).$$
In diesem Fall $\underline{0} = (0,\ldots,0)$
2) Allgemeiner: Sei K beliebiger Körper, $n \in \mathbb{N}$, $n \geq 1$. Dann können wir genau wie in Beispiel 1) die Menge
$$K^n = \{(x_1,\ldots,x_n) \mid x_1 \in K,\ldots,x_n \in K\}$$
zu einem Vektorraum über dem Körper K machen.
3) Sei I ein <u>homogenes</u> lineares Gleichungssystem mit m Gleichungen und n Unbekannten $x_1,\ldots,x_n$ und Koeffizienten $a_{11},\ldots,a_{mn}$ in K. Dann bildet die Lösungsmenge
$$L_I = \{x = (x_1,\ldots,x_n) \in K^n \mid x \text{ löst } I\}$$
mit den wie in 1) definierten Operationen einen K-Vektorraum, vgl. (1.15).
4) Sei $K := \mathbb{R}$, $M \neq \emptyset$ eine Menge und $V = \{f \mid f : M \to \mathbb{R}\}$.

Für $r \in \mathbb{R}$, $f, g \in V$ definieren wir $f + g \in V$ und $rf \in V$ durch

(a) $\forall x \in M : (f+g)(x) := f(x) + g(x)$
(b) $\forall x \in M : (rf)(x) := rf(x)$
Mit diesen Operationen ist V ein $\mathbb{R}$-Vektorraum (wobei $\underline{0} \in V$ die Abbildung ist, die jedes $x \in M$ auf $0 \in \mathbb{R}$ abbildet).

Wir beweisen exemplarisch, daß (3.1)(iii) gilt:
Seien $f, g \in V$, $r \in \mathbb{R}$. Zu zeigen ist:

$$(*) \qquad r(f+g) = rf + rg$$

Auf beiden Seiten von $(*)$ stehen Abbildungen von M nach $\mathbb{R}$. Wir haben also zu zeigen, daß für alle $x \in M$ gilt:

$$(r(f+g))(x) = (rf+rg)(x)$$

Wendet man auf beide Seiten (a) und (b) an (auf der linken Seite zunächst (b) dann (a)), so erhält man für die linke Seite

$$(r(f+g)(x)) \overset{\text{(b)}}{=} r((f+g)(x)) \overset{\text{(a)}}{=} r(f(x)+g(x))$$

und für die rechte Seite

$$(rf+rg)(x) \overset{\text{(a)}}{=} (rf)(x) + (rg)(x) \overset{\text{(b)}}{=} rf(x) + rg(x)$$

Schließlich gilt $r(f(x)+g(x)) = rf(x) + rg(x)$ aufgrund des Distributivgesetzes für die reellen Zahlen.

(3.2) Rechenregeln. Für alle $\alpha \in K$, $v \in V$ gilt

(i) $0v = \underline{0}$, $\alpha\underline{0} = \underline{0}$
(ii) $\alpha v = \underline{0} \Rightarrow \alpha = 0$ oder $v = \underline{0}$
(iii) $(-\alpha)v = \alpha(-v) = -(\alpha v) \quad (=: -\alpha v)$

Bew.:

(i) $0v = 0v + (v-v) = (0v+1v) - v = (0+1)v - v = 1 \cdot v - v = v - v = \underline{0}$
$\alpha\underline{0} = \alpha\underline{0} + (\alpha\underline{0} - \alpha\underline{0}) = \alpha(\underline{0}+\underline{0}) - \alpha\underline{0} = \alpha\underline{0} - \alpha\underline{0} = \underline{0}$
(ii) Sei $\alpha v = \underline{0}$ und $\alpha \neq 0 \overset{\text{(i)}}{\Rightarrow} \alpha^{-1}(\alpha v) = \underline{0} \Rightarrow (\alpha^{-1}\alpha)v = \underline{0} \Rightarrow 1v = \underline{0} \Rightarrow v = \underline{0}$
(iii) $(-\alpha)v + \alpha v = ((-\alpha)+\alpha)v = 0v \overset{\text{(i)}}{=} \underline{0} \Rightarrow (-\alpha)v = -(\alpha v)$
$\alpha(-v) + \alpha v = \alpha((-v)+v) = \alpha\underline{0} \overset{\text{(i)}}{=} \underline{0} \Rightarrow \alpha(-v) = -(\alpha v)$

(3.3) Def.: Sei V K-Vektorraum und $U \subseteq V$. U heißt Unter(vektor)raum von V, falls

(i) $U \neq \emptyset$
(ii) $v_1, v_2 \in U \Rightarrow v_1 + v_2 \in U$
(iii) $\alpha \in K$, $v \in U \Rightarrow \alpha v \in U$

(3.4) Folgerung: Sei V K-Vektorraum, $U \subseteq V$ Unterraum. Dann ist U (mit den von V auf U eingeschränkten Strukturen) ein K-Vektorraum.

Bew.: Sei U Unterraum.

(i) $\Rightarrow +$ ist innere Verknüpfung auf $U (\Rightarrow (G_1))$.
(ii) $\Rightarrow$ die Multiplikation mit Skalaren ist eine Abbildung $K \times U \to U$.

Wir zeigen: $(U,+)$ ist abelsche Gruppe: $v \in U \overset{\text{(ii)}}{\Rightarrow} (-1)v \in U \overset{(3.2)\text{(iii)}}{\Rightarrow} -v \in U$

$U \neq \emptyset \Rightarrow \exists v \in U \Rightarrow v$ und $-v \in U \overset{\text{(ii)}}{\Rightarrow} v + (-v) = \underline{0} \in V$
Daraus folgen $(G_2), (G_3)$ für $(U,+)$, (G_1) für $(U,+)$ folgt aus (G_1) für $(V,+)$. Die anderen Eigenschaften sind offensichtlich erfüllt.

Beispiele:

1) $\{0\}$ und V sind Unterräume von V
2) Ist $m < n$, so ist $K^m \times \{\underbrace{(0,\ldots,0)}_{(n-m)-\text{mal}}\} = \{(x_1,\ldots,x_n) \in K^n \mid x_{m+1} = \ldots = x_n = 0\}$ Unterraum von K^n
3) Ist I homogenes lineares Gleichungssystem für n Unbekannte mit Koeffizienten a_{ij} in K, so ist L_I Unterraum von K^n, vgl. (1.15).
4) $V = \{f \mid f : M \to \mathbb{R}\}$, vgl. Bsp. 4) nach (3.1). Zu festem $a \in M$ sei $U = \{f \in V \mid f(a) = 0\}$. Dann ist U Unterraum von V.

(3.5) Fakt. Ist V ein K-Vektorraum und $\mathcal{U}$ eine Menge von Unterräumen von K, so ist $W := \bigcap_{U \in \mathcal{U}} U$ Unterraum von V.

Bew.: $\forall U \in \mathcal{U} : \underline{0} \in U \Rightarrow \underline{0} \in W$
$v_1, v_2 \in W \Leftrightarrow \forall U \in \mathcal{U} : v_1, v_2 \in U \overset{(3.3)\text{(ii)}}{\Rightarrow} \forall U \in \mathcal{U} : v_1 + v_2 \in U \Leftrightarrow v_1 + v_2 \in W$
Ebenso: $\alpha \in K$, $v \in W \Rightarrow \alpha v \in W$.

(3.6) Def.: Sei V K-Vektorraum, $M \subseteq V$. $\mathcal{U}_M := \{U \mid U$ Unterraum von V mit $M \subseteq U\}$

Dann heißt $\operatorname{span}(M) := \bigcap_{U \in \mathcal{U}_M} U$ der von M aufgespannte (oder erzeugte) Unterraum. M heißt Erzeugendensystem von V, falls $\operatorname{span}(M) = V$ gilt. V heißt endlich erzeugt, falls es eine endliche Menge $M \subseteq V$ gibt mit $\operatorname{span}(M) = V$.

Bem.: (3.5) $\Rightarrow \operatorname{span}(M)$ ist Unterraum von V, der (bzgl. der Inklusion) kleinste, M enthaltende Unterraum.

Bsp.:

1) $M = \emptyset$ oder $M = \{\underline{0}\} \Rightarrow \operatorname{span}(M) = \{\underline{0}\}$
2) Ist M Unterraum von V, so $\operatorname{span}(M) = M$

(3.7) Satz. *Sei V K-Vektorraum, $\emptyset \neq M \subseteq V$. Dann gilt:*

$$\operatorname{span}(M) = \{v \in V \mid \exists k \in \mathbb{N}, \alpha_1,\ldots,\alpha_k \in K, v_1,\ldots,v_k \in M : v = \alpha_1 v_1 + \ldots + \alpha_k v_k\}$$

Bez.: $\alpha_1 v_1 + \ldots + \alpha_k v_k$ heißt eine Linearkombination der Vektoren $v_1, \ldots, v_k$.
abgekürzt: $\alpha_1 v_1 + \alpha_s v_2 + \ldots + \alpha_k v_k = \sum\limits_{i=1}^{k} \alpha_i v_i$

Bew.: Wir bezeichnen die Menge auf der rechten Seite des Gleichheitszeichens in (3.7) durch U_0.
1) Zeige U_0 ist Unterraum von V. Wegen $M \neq \emptyset$ gilt $U_0 \neq \emptyset$. Seien $v, w \in U_0$, $v = \alpha_1 v_1 + \ldots + \alpha_k v_k$, $w = \beta_1 w_1 + \ldots + \beta_j w_j$ mit $\alpha_1, \ldots, \beta_j \in K, v_1, \ldots, w_j \in M$. Dann gilt $v + w = \alpha_1 v_1 + \ldots + \alpha_k v_k + \beta_1 w_1 + \ldots + \beta_j w_j \in U_0$.

Sei $\alpha \in K, v = \sum\limits_{i=1}^{k} \alpha_i v_i \in U_0$ mit $v_i \in M$. Dann gilt

$$\alpha v = \alpha(\alpha_1 v_1 + \ldots + \alpha_k v_k) = \alpha(\alpha_1 v_1) + \ldots + \alpha(\alpha_k v_k) = (\alpha\alpha_1)v_1 + \ldots + (\alpha\alpha_k)v_k \in U_0.$$

(Kürzer: $\alpha \sum\limits_{i=1}^{k} \alpha_i v_i = \sum\limits_{i=1}^{k} \alpha\alpha_i v_i$).
Also ist U_0 ein M enthaltender Unterraum. Nach Definition (3.6) folgt $\mathrm{span}(M) \subseteq U_0$.
2) Zeige $U_0 \subseteq \mathrm{span}(M)$. Seien $v_1, \ldots, v_k \in M$, $\alpha_1, \ldots, \alpha_k \in K$. Da $\mathrm{span}(M)$ Unterraum ist, folgt nach (3.3)(iii): $\alpha_1 v_1 \in \mathrm{span}(M), \ldots, \alpha_k v_k \in \mathrm{span}(M)$, und nach (3.3)(ii) $\alpha_1 v_1 + \alpha_2 v_2 \in \mathrm{span}(M)$, $(\alpha_1 v_1 + \alpha_2 v_2) + \alpha_3 v_3 \in \mathrm{span}(M)$, u.s.w. bis

$$\alpha_1 v_1 + \ldots + \alpha_k v_k \in \mathrm{span}(M).$$

Also $U_0 \subseteq \mathrm{span}(M)$.

Bsp.: Betrachte K^n und $e_1 := (1, 0, \ldots, 0) \in K^n$, $e_2 := (0, 1, 0, \ldots, 0) \in K^n$, $\ldots$, $e_n = (0, \ldots, 0, 1) \in K^n$. Dann ist $M = \{e_1, \ldots, e_n\}$ Erzeugendensystem für K^n. Es genügt, $K^n \subseteq \mathrm{span}(M)$ zu zeigen. Ist $x = (x_1, \ldots, x_n) \in K^n$, so gilt $x = x_1 e_1 + x_2 e_2 + \ldots + x_n e_n \in \mathrm{span}(M)$.

(3.8) Def.: Die Vektoren $v_1, \ldots, v_k$ heißen <u>linear unabhängig</u>, falls gilt: Ist $\alpha_1 \in K, \ldots, \alpha_k \in K$ und $\alpha_1 v_1 + \ldots + \alpha_k v_k = \underline{0}$, so folgt $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$. Sonst heißen die Vektoren $v_1, \ldots, v_k$ linear abhängig. Eine Teilmenge M von V heißt linear unabhängig, falls gilt: Ist $k \in \mathbb{N}$ und sind $v_1, \ldots, v_k$ verschiedene Vektoren in M, so sind die $v_1, \ldots, v_k$ linear unabhängig. Sonst heißt M linear abhängig.

Bem.: $v_1, \ldots, v_k$ linear abhängig $\Leftrightarrow \exists \alpha_1, \ldots, \alpha_k \in K$ <u>nicht</u> <u>alle</u> $= 0$:

$$\alpha_1 v_1 + \ldots + \alpha_k v_k = \underline{0}$$

Bsp.:

1) $\underline{0} \in M \Rightarrow M$ linear abhängig. Denn: $1 \cdot \underline{0} = \underline{0}$.
2) $M = \{v\}$ linear unabhängig $\Leftrightarrow v \neq 0$. Denn: $\alpha v = \underline{0}, v \neq \underline{0} \overset{(3.2)(\text{ii})}{\Rightarrow} \alpha = 0$.
3) Sei $M \subseteq M' \subseteq V$. Dann: M linear abhängig $\Rightarrow M'$ linear abhängig
M' linear unabhängig $\Rightarrow M$ linear unabhängig

4) $e_1, \ldots, e_n$ sind linear unabhängig in K^n. Denn:
$x_1e_1 + \ldots + x_ne_n = (x_1, \ldots, x_n) = \underline{0} \Leftrightarrow x_1 = \ldots = x_n = 0$.

5) $V = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$. Die Funktion $x \to \sin x$ und $x \to \cos x$ sind linear unabhängig. Seien $r, s \in \mathbb{R}$ und $r \sin x + s \cos x = 0$ <u>für alle</u> $x \in \mathbb{R}$. Dann gilt das speziell für $x = 0$ und $x = \frac{\pi}{2}$, d.h.

$$\begin{aligned} r \underbrace{\sin 0}_{=0} + s \underbrace{\cos 0}_{=1} = 0 \qquad &\Rightarrow \quad s = 0 \\ r \underbrace{\sin\left(\frac{\pi}{2}\right)}_{=1} + s \underbrace{\cos\left(\frac{\pi}{2}\right)}_{=0} = 0 \quad &\Rightarrow \quad r = 0. \end{aligned}$$

(3.9) Fakt. Die Vektoren $v_1, \ldots, v_k$ seien linear unabhängig. Dann gilt:

$$\alpha_1v_1 + \ldots + \alpha_kv_k = \beta_1v_1 + \ldots + \beta_kv_k \Rightarrow \alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k$$

Bew.: Voraussetzung $\Rightarrow$ $(\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + \ldots + (\alpha_k - \beta_k)v_k = \underline{0}$
$\overset{\text{l. unabh.}}{\Rightarrow}$ $\alpha_1 - \beta_1 = 0, \ldots, \alpha_k - \beta_k = 0 \Rightarrow \alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k$.

(3.10) Def.: Eine Teilmenge M von V heißt <u>Basis von</u> V, falls M linear unabhängig und ein Erzeugendensystem von V ($\Leftrightarrow \operatorname{span}(M) = V$) ist.

Bsp.: $\{e_1, \ldots, e_n\} \subseteq K^n$ ist Basis von K^n, die "Standardbasis von K^n".

Eine Beispielrechnung zur linearen Unabhängigkeit von Vektoren:

Wir fragen, ob die Vektoren $(1,0,1), (0,1,1), (1,1,-1)$ im $\mathbb{R}$-Vektorraum $\mathbb{R}^3$ linear unabhängig sind. Dazu nehmen wir an, daß für die reellen Zahlen r, s und t gilt:

$$r(1,0,1) + s(0,1,1) + t(1,1,-1) = (0,0,0)$$

Die Vektoren sind linear unabhängig, wenn wir aus dieser Gleichung folgern können, daß $r = s = t = 0$ gilt, vgl. Def. (3.8). Die Gleichung ist äquivalent zum homogenen linearen Gleichungssystem

$$\begin{array}{rcl} r \qquad + t & = & 0 \quad | \; - \\ s + t & = & 0 \quad | \\ r + s - t & = & 0 \; \leftarrow| \end{array}$$

Wir lösen es nach dem Gaußschen Eliminationsverfahren:

$$\begin{array}{rcl} r \qquad + \; t & = & 0 \\ s + \; t & = & 0 \quad | \; - \\ s - 2t & = & 0 \; \leftarrow| \end{array}$$

$$\begin{array}{rcl} r \qquad + \; t & = & 0 \\ s + \; t & = & 0 \\ -\, 3t & = & 0 \end{array}$$

Aus der letzten Gleichung folgt $t = 0$, damit aus der vorletzten $s = 0$ und aus der ersten $r = 0$.

Vorsicht: Bezeichnet man im Körper $(\mathbb{Z}_3, +, \cdot)$ wie in Körpern üblich das 0-Element mit 0, das 1-Element mit 1 und das additive Inverse von 1 mit -1, so kann man die Vektoren $(1,0,1), (0,1,1), (1,1,-1)$ auch als Element des $\mathbb{Z}_3$-Vektorraums $(\mathbb{Z}_3)^3$ auffassen. In diesem sind sie linear abhängig, denn

$$(1,0,1) + (0,1,1) - (1,1,-1) = (0,0,0) \text{ in } (\mathbb{Z}_3)^3!$$

(3.11) Lemma. (i) $v \in \operatorname{span}(M) \Rightarrow \operatorname{span}(M \cup \{v\}) = \operatorname{span}(M)$
(ii) $v \in \operatorname{span}(M) \setminus M \Rightarrow M \cup \{v\}$ linear abhängig

Beweis von (i): $\operatorname{span}(M) \subseteq \operatorname{span}(M \cup \{v\})$ ist klar.
Sei $w \in \operatorname{span}(M \cup \{v\})$, $w = \alpha v + \sum_{j=1}^{l} \beta_j w_j$ mit $w_j \in M$.
$v \in \operatorname{span}(M) \Rightarrow v = \sum_{i=1}^{k} \alpha_i v_i \Rightarrow w = \sum_{i=1}^{k} (\alpha\alpha_i) v_i + \sum_{j=1}^{l} \beta_j w_j \in \operatorname{span}(M)$.

Beweis von (ii): (3.7) $\Rightarrow$ Es existiert $k \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_k \in K$, $v_1, \ldots, v_k \in M$: $v \stackrel{(*)}{=} \sum_{i=1}^{k} \alpha_i v_i$.

Wir können (mittels der Vektorraumaxiome) etwaige Summanden $\alpha_i v_i$ und $\alpha_j v_j$ mit $v_i = v_j$ zu $(\alpha_i + \alpha_j) v_i$ zusammenfassen und dann annehmen, daß alle $v_1, \ldots, v_k$ verschieden sind.
$v \notin M \Rightarrow v, v_1, \ldots, v_k$ sind alle verschieden.

$$(*) \Rightarrow 1 \cdot v - \sum_{i=1}^{k} \alpha_i v_i = 0 \Rightarrow M \cup \{v\} \text{ linear abhängig.}$$

(3.12) Satz. *Folgende Aussage über eine Teilmenge M von V sind äquivalent:*

(i) *M ist Basis*
(ii) *M ist linear unabhängig und jede echte Obermenge $M' \subseteq V$ von M ist linear abhängig. ("M ist eine maximale linear unabhängige Teilmenge von V.")*
(iii) *Es gilt* $\operatorname{span}(M) = V$ *und für jede echte Teilmenge M'' von M gilt:* $\operatorname{span}(M'') \neq V$. *("$M$ ist ein minimales Erzeugendensystem von V.")*

Bew.: $V = \{0\} \Leftrightarrow M = \emptyset$ ist Basis von V. Dann ist (3.12) klar. Es genügt also, den Fall $M \neq \emptyset$ zu betrachten.

1) (i) $\Rightarrow$ (ii): Es ist zu zeigen, daß jede echte Obermenge $M' \subseteq V$ von M linear abhängig ist. Sei $v \in M' \setminus M$. Wegen $\operatorname{span}(M) = V$ (M Basis!) gilt $v \in \operatorname{span}(M) \setminus M$. Nach (3.11)(ii) ist $M \cup \{v\}$ und damit auch $M' \supseteq M \cup \{v\}$ linear abhängig.
2) (ii) $\Rightarrow$ (iii). Wir zeigen zunächst, daß $\operatorname{span}(M) = V$ gilt. Sei $v \in V \setminus M$. Wegen (ii) ist $M \cup \{v\}$ linear abhängig. Es existieren also verschiedene $v_1, \ldots, v_k \in M$ und

$\alpha, \alpha_1, \ldots, \alpha_k \in K$, nicht alle $= 0$, mit

$$\alpha v + \sum_{i=1}^{k} \alpha_i v_i = \underline{0}$$

Da M linear unabhängig ist ((ii)!), gilt $\alpha \neq 0$. Also

$$v = \sum_{i=1}^{k} \left(\frac{-\alpha_i}{\alpha} \right) v_i \in \operatorname{span}(M)$$

Also $V \setminus M \subseteq \operatorname{span}(M)$, und damit: $V = \operatorname{span}(M)$.
Sei schließlich M'' eine echte Teilmenge von M, $v \in M \setminus M''$. Wäre $v \in \operatorname{span}(M'')$, so würde aus (3.11)(ii) folgen, daß $M'' \cup \{v\} \subseteq M$ linear abhängig ist, im Widerspruch dazu, daß M nach Voraussetzung ((ii)!) linear unabhängig ist.
Also $v \notin \operatorname{span}(M'')$ und deshalb $\operatorname{span}(M'') \neq V$.

3) (iii) $\Rightarrow$ (i). Zu zeigen ist, daß M linear unabhängig ist. Seien $v_1, \ldots, v_k$ verschiedene Elemente in M, $\alpha_1, \ldots, \alpha_k \in K$ und

$$\sum_{i=1}^{k} \alpha_i v_i = \underline{0}$$

wäre eines der α_i ungleich 0, z.B. $\alpha_1 \neq 0$, so folgt:

$$v_1 = \sum_{i=1}^{k} \left(\frac{-\alpha_i}{\alpha_1} \right) v_i \in \operatorname{span}\{v_2, \ldots, v_k\} \subseteq \operatorname{span}(M \setminus \{v_1\})$$

Wegen (3.11)(i) folgt $\operatorname{span}(M) = \operatorname{span}(M \setminus \{v_1\})$, also $\operatorname{span}(M \setminus \{v_1\}) = V$, im Widerspruch zu (iii).

(3.13) Satz. *Jeder Vektorraum besitzt eine Basis.*

Bem.: Wir zeigen sogar: Ist $M_0 \subseteq V$ linear unabhängig, so existiert eine M_0 enthaltende Basis von V.

Bew.: 1) Wir betrachten zunächst den Spezialfall, daß es ein endliches Erzeugendensystem, genannt M_1, von V gibt. Dann existiert das kleinste $n \in \mathbb{N}$, so daß es eine n-elementige Teilmenge von M_1 gibt, die V erzeugt. Sei M ein solches Erzeugendensystem. Dann folgt aus (3.12), daß M eine Basis von V ist. Zusätzlich gilt $M \subseteq M_1$.
2) Für den allgemeinen Fall benötigen wir folgendes

(3.14) Lemma von Zorn. Sei $\mathcal{M} \neq \emptyset$ eine Menge, deren Elemente Mengen sind. Gilt für jede Kette $\mathcal{K} \subseteq \mathcal{M}$, daß $\bigcup\limits_{M \in \mathcal{K}} M \in \mathcal{M}$ gilt, so existiert ein maximales Element in $\mathcal{M}$, d.h. ein $M \in \mathcal{M}$, so daß aus $M \subseteq M' \in \mathcal{M}$ folgt $M = M'$.

Dabei heißt eine Teilmenge $\mathcal{K}$ von $\mathcal{M}$ Kette, falls $\mathcal{K} \neq \emptyset$ und falls für je zwei Elemente $M_1, M_2 \in \mathcal{K}$ gilt:

$$(*) \qquad M_1 \subseteq M_2 \text{ oder } M_2 \subseteq M_1$$

Wir nehmen das Lemma von Zorn als Axiom der Mengenlehre hin und definieren in Abhängigkeit von einer gegebenen, linear unabhängigen Menge $M_0 \subseteq V$:

$$\mathcal{M} := \{M \mid M_0 \subseteq M \subseteq V, M \text{ linear unabhängig}\}$$

Wegen $M_0 \in \mathcal{M}$ gilt $\mathcal{M} \neq \emptyset$. Wir wollen die Voraussetzung von (3.14) nachweisen. Sei also $\mathcal{K}$ eine Kette in $\mathcal{M}$. Dann gilt $M_0 \subseteq \bigcup\limits_{M \in \mathcal{K}} M$ und es bleibt zu zeigen, daß $\bigcup\limits_{M \in \mathcal{K}} M$ linear unabhängig ist.

Seien $v_1, \ldots, v_k$ verschiedene Vektoren in $\bigcup\limits_{M \in \mathcal{K}} M$. Dann existieren $M_1, \ldots, M_k \in \mathcal{K}$ mit $v_1 \in M_1, \ldots, v_k \in M_k$. Wegen $(*)$ existiert eine der Mengen $M_1, \ldots, M_k$, sagen wir M_j, die die anderen enthält. Dann sind $v_1, \ldots, v_k$ verschiedene Elemente in M_j und damit linear unabhängig (, da $M_j \in \mathcal{M}$ linear unabhängig ist). Also $\bigcup\limits_{M \in \mathcal{K}} M \in \mathcal{M}$. Nach (3.2) ist ein maximales Element von $\mathcal{M}$, das nach (3.14) existiert, eine M_0 enthaltende Basis von V.

Wichtig: Es gibt im allgemeinen sehr viele Basen eines Vektorraumes. Sie haben aber alle "gleich viele" Elemente, siehe (3.16). Zum Beispiel bilden zwei Vektoren $v = (a, b)$, $w = (c, d)$ des $\mathbb{R}^2$ genau dann eine Basis des $\mathbb{R}^2$, wenn $ad - bc \neq 0$ (, was "meistens" der Fall ist!).

Bemerkung: Die "Lösung eines homogenen linearen Gleichungssystems", d.h. das Auffinden einer Parameterdarstellung des Lösungsraums, besteht gerade darin, eine Basis dieses Lösungsraums zu finden.

(3.15) Austauschlemma. Sei $B = \{v_1 \ldots, v_n\}$ eine Basis von V mit n Elementen und $w \in V \setminus \{0\}$. Dann existiert $j \in \{1, \ldots, n\}$, so daß $B' = (B \setminus \{v_j\}) \cup \{w\}$ Basis von V ist.

Bew.: Wegen $\operatorname{span}(B) = V$ existieren $\alpha_1, \ldots, \alpha_n \in K$, so daß

$$(*) \qquad w = \sum_{i=1}^{n} \alpha_i v_i$$

gilt. Da $w \neq 0$ ist, existiert ein j, $1 \leq j \leq n$ mit $\alpha_j \neq 0$. Wir zeigen, daß für jedes solche j gilt: $B' = (B \setminus \{v_j\}) \cup \{w\} = \{v_1, \ldots, v_{j-1}, v_{j-1}, \ldots, v_n, w\}$ ist Basis.

Zunächst gilt $v_j \in \operatorname{span}(B')$, da aus $(*)$ folgt

$$v_j = \frac{1}{\alpha_j}\left(w - \sum_{\substack{i=1 \\ i \neq j}}^{n} \alpha_i v_i\right) = \frac{1}{\alpha_j} w + \sum_{\substack{i=1 \\ i \neq j}}^{n} \left(\frac{-\alpha_i}{\alpha_j}\right) v_i$$

und die rechte Seite ist eine Linearkombination von Elementen von B'.

Nach (3.11)(i) folgt

$$\operatorname{span}(B') \overset{(3.11)(\mathrm{i})}{=} \operatorname{span}(B' \cup \{v_j\}) = \operatorname{span}(B \cup \{w\}) \overset{(3.11)(\mathrm{i})}{=} \operatorname{span}(B) = V,$$

d.h. B' ist Erzeugendensystem von V. Um die lineare Unabhängigkeit von B' zu zeigen, nehmen wir an, daß für $\beta \in K$, $\beta_1, \ldots, \beta_{j-1}, \beta_{j+1}, \ldots, \beta_n \in K$ gilt:

$$(**) \qquad \beta w + \sum_{\substack{i=1 \\ i \neq j}}^{n} \beta_i v_i = \underline{0}$$

Mit $(*)$ folgt

$$\beta \sum_{i=1}^{n} \alpha_i v_i + \sum_{\substack{i=1 \\ i \neq j}}^{n} \beta_i v_i = \underline{0},$$

also

$$\beta \alpha_j v_j + \sum_{\substack{i=1 \\ i \neq j}}^{n} (\beta \alpha_i + \beta_i) v_i = \underline{0}.$$

Da $B = \{v_1, \ldots, v_n\}$ linear unabhängig ist, folgt aus der vorangehenden Gleichung $\beta \alpha_j = 0$ und $\beta \alpha_i + \beta_i = 0$ für alle $i \neq j$. Da wir j so gewählt hatten, daß $\alpha_j \neq 0$ ist, folgt $\beta = 0$ und daraus $\beta_i = 0$ für alle $i \neq j$. Damit haben wir gezeigt, daß in $(**)$ alle Koeffizienten β und β_i für $i \neq j$ gleich 0 sind, d.h. B' ist linear unabhängig.

(3.16) Austauschsatz von Steinitz. *Sei $B = \{v_1, \ldots, v_n\}$ eine Basis von V mit n Elementen und seien $w_1, \ldots, w_m$ m linear unabhängige Vektoren in V. Dann gilt*

(i) $m \leq n$
(ii) *Es gibt $(n - m)$ Vektoren in B, bei geeigneter Numerierung $v_{m+1}, \ldots, v_n$, so daß $\{w_1, \ldots, w_m, v_{m+1}, \ldots, v_n\}$ eine Basis von V ist.*

Speziell gilt: Jede Basis von V hat n Elemente.

Bew.: Induktion nach m.
1) $m = 1$. $\underline{0} \neq w_1 \in V \Rightarrow V \neq \{0\} \Rightarrow n \geq 1 = m \Rightarrow$ (i). (ii) folgt aus (3.15).
2) $m > 1$. Induktionsvoraussetzung: (i) und (ii) gelten für $m - 1$. Seien $w_1, \ldots, w_m$ linear unabhängig gegeben. Die Induktionsvoraussetzung impliziert: $(m-1) \leq n$ und es existieren $n - m + 1$ Vektoren in B, o.E. $v_m \ldots, v_n$, so daß $\{w_1, \ldots, w_{m-1}, v_m \ldots, v_n\}$ eine Basis von V ist.

Zeige (i): $m \leq n$. Sonst gilt nach der vorangehenden Überlegung $m - 1 = n$ und die Menge $\{w_1, \ldots, w_{m-1}\}$ ist Basis von V ($n - m + 1 = 0!$), im Widerspruch zur Voraussetzung, daß $\{w_1, \ldots, w_m\}$ linear unabhängig ist. Das beweist $m \leq n$.

Zeige (ii): Wir wollen in der Basis $\{w_1, \ldots, w_{m-1}, v_m, \ldots, v_n\}$ eines der v_i, $m \leq i \leq n$, gegen w_m "austauschen" und zwar so, daß wieder eine Basis entsteht.

Da $\text{span}\{w_1, \ldots, w_{m-1}, v_m, \ldots, v_n\} = V$ gilt, existieren $\alpha_1, \ldots, \alpha_n \in K$, so daß

$$w_m = \alpha_1 w_1 + \ldots + \alpha_{m-1} w_{m-1} + \alpha_m v_m + \ldots + \alpha_n v_n$$

gilt. Da $\{w_1, \ldots, w_m\}$ linear unabhängig ist, existiert ein $j \in \{m, \ldots, n\}$ mit $\alpha_j \neq 0$. Wir können annehmen, daß $j = m$ ist. Wendet man das Austauschlemma (3.15) (vgl. auch den Anfang des Beweises von (3.15)!) auf $w := w_m$ und die Basis $\{w_1, \ldots, w_{m-1}, v_m, \ldots, v_n\}$ an, so folgt, daß $\{w_1, \ldots, w_m, v_{m+1}, \ldots, v_n\}$ eine Basis von V ist. Das beweist (ii).

(3.17) Def.: Ist V endlich erzeugter Vektorraum, so heißt die Anzahl der Elemente einer ($\Rightarrow$ jeder) Basis von V die <u>Dimension</u> <u>von</u> V (abgekürzt: $\dim V$).

Ist V nicht endlich erzeugt, so setzen wir $\dim V := \infty$.

Beispiele:

1) $V = \{\underline{0}\} \Leftrightarrow \dim V = 0$ (mit Basis $M = \emptyset$)
2) Für den K-Vektorraum K^n gilt: $\dim(K^n) = n$
   Begründung: Die Standardbasis $\{e_1, \ldots, e_n\}$ von K^n hat n Elemente.
3) $V = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$, vgl. Bsp. 4) nach (3.1). Für diesen $\mathbb{R}$-Vektorraum gilt $\dim V = \infty$, vgl. Blatt 6, Aufgabe 4(b).

Bem.: V endlich erzeugt $\Leftrightarrow$ V endlich-dimensional.

(3.18) Folgerungen. Sei V Vektorraum, $\dim V = n < \infty$. Dann gilt:

(i) Ist $M \subseteq V$ linear unabhängig, so gilt $\#M \leq n$, und es gilt $\#M = n$ genau dann, wenn M Basis von V ist.
(ii) Ist $M \subseteq V$ Erzeugendensystem von V, so gilt $\#M \geq n$, und es gilt $\#M = n$ genau dann, wenn M Basis von V ist.
(iii) Ist $U \subseteq V$ Unterraum, so gilt $\dim U \leq \dim V$. Jede Basis von U ist in einer Basis von V enthalten. Es gilt genau dann $\dim U = \dim V$, wenn $U = V$ gilt.

Lösung von Blatt 5, Aufgabe 3: Sei U Unterraum des $\mathbb{R}^2$ mit $\{(0,0)\} \neq U \neq \mathbb{R}^2$. Dann existiert $v \in \mathbb{R}^2 \setminus \{(0,0)\}$, so daß $U = \{rv \mid r \in \mathbb{R}\}$.

Bew.: Es gilt $0 < \dim U < 2 = \dim(\mathbb{R}^2)$, also $\dim U = 1$. Sei $\{v\}$ Basis von $U \Rightarrow$ Beh.

Beweis von (3.18):

(i) (3.16)(i) $\Rightarrow \#M \leq n$. Speziell: Ist $\#M = n$, so ist M (im Sinne von (3.12)!) eine maximale linear unabhängige Teilmenge, also nach (3.12) eine Basis.
(ii) Analog zu (i).
(iii) Ist B' Basis von U, so ist B' als Teilmenge von V linear unabhängig, also $\dim U = \#B' \leq n = \dim V$ nach (i). Aus (3.16)(ii) folgt, daß B' in einer Basis von V enthalten ist. Gilt $\dim U = \dim V$, so ist nach (i) jede Basis B' von U auch Basis von V, d.h. $U = \text{span}(B') = V$.

(3.19) Def.: Seien U_1, U_2 Unterräume eines Vektorraums V. Dann heißt der Unterraum

$$U_1 + U_2 := \operatorname{span}(U_1 \cup U_2)$$

die Summe von U_1 und U_2. Gilt $U_1 \cap U_2 = \{\underline{0}\}$, so nennt man $\operatorname{span}(U_1 \cup U_2)$ die direkte Summe von U_1 und U_2 und schreibt

$$\operatorname{span}(U_1 \cup U_2) =: U_1 \oplus U_2$$

Bsp.: Für $0 < m < n$ gilt: $K^n = (K^m \times \{\underline{0}\}) \oplus (\{\underline{0}\} \times K^{n-m})$

(3.20) Fakt. (i) $U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$
(ii) Gilt $U_1 \cap U_2 = \{0\}$, so existieren für jedes $v \in U_1 \oplus U_2$ genau zwei Vektoren $u_1 \in U_1$, $u_2 \in U_2$, so daß $v = u_1 + u_2$ gilt.

Bsp.: 1) $V = \mathbb{R}^2$, U_1, U_2 Unterräume der Dimension 1, $U_1 \neq U_2$. Dann: $U_1 \cap U_2 = \{(0,0)\}$, $U_1 \oplus U_2 = \mathbb{R}^2$.
2) $V = \mathbb{R}^3$, $U_1 \neq U_2$ Unterräume der Dimension 2. Dann: $\dim(U_1 \cap U_2) = 1$, $U_1 + U_2 = \mathbb{R}^3$.

Beweis: Die Menge $\{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$ ist Unterraum (!), der U_1 und U_2 enthält, also $\operatorname{span}(U_1 \cup U_2) \subseteq \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$, vgl. Def. (3.6).
Die Inklusion $\{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\} \subseteq \operatorname{span}(U_1 \cup U_2)$ ist klar!

Gilt $v = u_1 + u_2 = u_1' + u_2'$ mit $\{u_1, u_1'\} \subseteq U_1$, $\{u_2, u_2'\} \subseteq U_2$, so folgt

$$u_1 - u_1' = u_2' - u_2 \in U_1 \cap U_2 = \{\underline{0}\}, \text{ also } u_1 = u_1', u_2 = u_2'.$$

(3.21) Lemma.

(i) Ist U Unterraum von V, so existiert ein Unterraum W von V, so daß $U \cap W = \{\underline{0}\}$ und $U \oplus W = V$ gilt.
(W heißt ein zu U komplementärer Unterraum)
(ii) Sind U_1, U_2 Unterräume von V mit $U_1 \cap U_2 = \{0\}$, so gilt

$$\dim(U_1 \oplus U_2) = \dim U_1 + \dim U_2.$$

Bem.: Im allgemeinen gibt es sehr viele zu U komplementäre Unterräume. Beispiel: Es sei $U = \mathbb{R} \times \{0\} \subseteq \mathbb{R}^2$ und es sei $v = (v_1, v_2) \in \mathbb{R}^2$ und $v_2 \neq 0$. Dann ist $W = \operatorname{span}\{v\}$ zu U komplementär.

Bew.: (i) Ergänze eine Basis B' von U nach (3.18)(iii) zu einer Basis B von V und setze $W := \operatorname{span}(B \setminus B')$.
(ii) Für $i = 1, 2$ seien B_1, B_2 Basen von U_1, U_2. Aus $U_1 \cap U_2 = \{0\}$ folgt $B_1 \cap B_2 = \emptyset$. Wir zeigen, daß $B_1 \cup B_2$ Basis von $U_1 \oplus U_2$ ist ($\Rightarrow \dim(U_1 \oplus U_2) = \#(B_1 \cup B_2) = \#B_1 + \#B_2 = \dim U_1 + \dim U_2$). Wegen (3.20)(i) ist $B_1 \cup B_2$ Erzeugendensystem von $U_1 \oplus U_2$. Um zu zeigen, daß $B_1 \cup B_2$ linear unabhängig ist, sei

$$\sum_{i=1}^{k} \alpha_i v_i + \sum_{j=1}^{l} \beta_j w_j = \underline{0},$$

wobei $\alpha_1, \dots, \beta_l \in K$, $v_1, \dots, v_k$ verschiedene Elemente von B_1, $w_1, \dots, w_l$ verschiedene Elemente von B_2 sind. Dann folgt

$$\sum_{i=1}^{k} \alpha_i v_i = \sum_{j=1}^{l} (-\beta_j) w_j \in U_1 \cap U_2.$$

Wegen $U_1 \cap U_2 = \{0\}$ folgt

$$\sum_{i=1}^{k} \alpha_i v_i = \underline{0} = \sum_{j=1}^{l} (-\beta_j) w_j.$$

Da B_1 und B_2 beide linear unabhängig sind, folgt aus den vorangehenden Gleichungen $\alpha_1 = \ldots = \alpha_k = 0$ und $\beta_1 = \ldots = \beta_l = 0$. Das beweist die lineare Unabhängigkeit von $B_1 \cup B_2$.

Bem.: (3.21)(ii) gilt – richtig interpretiert – auch für den Fall, daß U_1 oder U_2 unendlich-dimensional sind. Für den Rest des Kapitels werden wir aber $\underline{\dim V < \infty}$ voraussetzen.

(3.22) Dimensionssatz. *Seien U_1, U_2 Unterräume eines Vektorraums V. Dann gilt*

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

Bew.: $U_1 \cap U_2 =: U_{12}$. Nach (3.21)(i) existieren Unterräume W_1(von $U_1 \Rightarrow$ von V) und W_2, so daß $U_1 = U_{12} \oplus W_1$ und $U_2 = U_{12} \oplus W_2$ gilt. Dann folgt

$$(*) \qquad U_1 + U_2 = (U_{12} \oplus W_1) \oplus W_2$$

Denn einerseits läßt sich jedes Element $v \in U_1 + U_2$ als

$$v = u_1 + u_2 = u_{12} + w_1 + u'_{12} + w_2 = (u_{12} + u'_{12}) + w_1 + w_2$$

mit $u_1 \in U_1$, $u_2 \in U_2$, $u_{12}, u'_{12} \in U_{12}$, $w_1 \in W_1$ und $w_2 \in W_2$ schreiben und andererseits gilt $(U_{12} \oplus W_1) \cap W_2 = U_1 \cap (U_2 \cap W_2) = U_{12} \cap W_2 = \{\underline{0}\}$.

Nach (3.21)(ii) folgt aus $(*)$: $\dim(U_1 + U_2) = \dim U_{12} + \dim W_1 + \dim W_2$, und aus $U_1 = U_{12} \oplus W_1$, $U_2 = U_{12} \oplus W_2$:

$$\begin{aligned} \dim U_1 &= \dim U_{12} + \dim W_1 \\ \dim U_2 &= \dim U_{12} + \dim W_2 \end{aligned}$$

Subtrahiert man diese beiden Gleichungen von der vorangehenden, so folgt

$$\dim(U_1 + U_2) - \dim U_1 - \dim U_2 = -\dim U_{12}$$

oder

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim U_{12},$$

wie behauptet.

Bez.: Ein Unterraum $H \subseteq V$ heißt <u>Hyperebene</u>, falls $\dim H = \dim V - 1$ gilt.

(3.23) Folgerung. Ist $U \subseteq V$ Unterraum, $H \subseteq V$ Hyperebene, so gilt entweder

$$\dim(U \cap H) = \dim U - 1$$

$$\text{oder} \quad U \subseteq H (\Leftrightarrow U = U \cap H \Leftrightarrow \dim(U \cap H) = \dim U).$$

Bew.: Aus (3.22) folgt

$$(*) \qquad \dim(U \cap H) = \dim U + (\dim V - 1) - \dim(U + H).$$

Gilt $\dim(U + H) < \dim V$, so folgt aus (3.18)(iii) angewendet auf $H \subseteq U + H$, daß $H = U+H$, d.h. $U \subseteq H$ gilt. Gilt $\dim(U+H) = \dim V$, so folgt aus $(*)$: $\dim(U \cap H) = \dim U - 1$.

(3.24) Lemma. Ist K ein Körper und sind $a_1, \ldots, a_n \in K$ nicht alle $= 0$, so ist der Lösungsraum $L_I \subseteq K^n$ der Gleichung

$$I \qquad a_1 x_1 + \ldots + a_n x_n = 0$$

eine Hyperebene in K^n.

Bew.: Sei etwa $a_j \neq 0$. Dann folgt durch Auflösen von I nach x_j:

$$L_I = \{x = (x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} \left(-\frac{a_i}{a_j}\right) x_i\}.$$

Wir definieren für $i \neq j$ die Vektoren $v_i = e_i - \frac{a_i}{a_j} e_j \in K^n$. Dann gilt

$$L_I = \operatorname{span}\{v_i \mid i \in \{1, \ldots, n\} \setminus \{j\}\}.$$

Da die Vektoren $v_i, i \neq j$, linear unabhängig sind (!), folgt $\dim L_I = n - 1$.

(3.25) Satz. Sei K ein Körper und

$$I \quad \begin{array}{ccccc} a_{11} & x_1 + \ldots + & a_{1n} & x_n & = 0 \\ \vdots & & \vdots & & \vdots \\ a_{k1} & x_1 + \ldots + & a_{kn} & x_n & = 0 \end{array}$$

ein homogenes lineares Gleichungssystem mit $a_{ij} \in K$ für $1 \leq i \leq k$, $1 \leq j \leq n$. Dann gilt $\dim L_I \geq n - k$.

Beweis: Induktion nach k.
$k = 1$: Nach (3.24) ist der Lösungsraum $L_I \subseteq K^n$ einer einzigen linearen Gleichung $(n-1)$-dimensional, es sei denn, alle Koeffizienten der Gleichung sind 0 (und in diesem Fall gilt $L_I = K^n$). In jedem Fall gilt $\dim L_I \geq n - 1$.

$k > 1$: Es sei I' das Gleichungssystem, das aus den ersten $(k-1)$ Gleichungen von I besteht, und I_k sei die k'te (=letzte) Gleichung von I. Dann gilt

$$L_I = L_{I'} \cap L_{I_k}$$

Die Induktionsvoraussetzung besagt: $\dim L_{I'} \geq n - k + 1$. Sind alle Koeffizienten von I_k gleich 0, so gilt $L_{I_k} = K^n$, also $L_I = L_{I'}$ und damit $\dim L_I = \dim L_{I'} \geq n - k + 1 > n - k$. Sind nicht alle Koeffizienten von I_k gleich 0, so ist L_{I_k} nach (3.24) eine Hyperebene.
Dann folgt aus (3.23), angewendet auf $U = L_{I'}$, $H = L_{I_k}$:
$\dim L_I = \dim(L_{I'} \cap L_{I_k}) \geq \dim(L_{I'}) - 1 \geq n - k$.

Bez.: Eine Teilmenge A von V heißt <u>k-dimensionaler</u> <u>affiner</u> <u>Unterraum</u>, falls es ein $v \in V$ und einen k-dimensionalen Unterraum $U \subseteq V$ gibt, so daß $A = \{v + u \mid u \in U\} =: v + U$ gilt. Ist $k = 1$, so nennt man A eine affine Gerade, ist $k = 2$, eine affine Ebene und ist $k = \dim V - 1$, eine affine Hyperebene.

Bem.: Ein affiner Unterraum A von V ist genau dann ein Unter(vektor)raum von V, wenn $\underline{0} \in A$ gilt. Sind v_0, $v_1 \in V$ und sind U_0, U_1 Unterräume von V, so gilt $v_0 + U_0 = v_1 + U_1$ genau dann, wenn $U_0 = U_1$ und $v_1 - v_0 \in U_0$ gilt.

(3.26) Folgerung. Sei K ein Körper und I ein inhomogenes lineares Gleichungssystem mit k Gleichungen für n Unbekannte. Dann gilt entweder $L_I = \emptyset$ oder L_I ist ein affiner Unterraum von K^n der Dimension $\geq n - k$. Insbesondere besitzt I höchstens dann genau eine Lösung (d.h. $\#L_I = 1$), wenn $k \geq n$ gilt.

Bew.: Die Behauptung folgt durch Kombination von (1.6) mit (3.25).

Bem.: Die Aussagen von (3.25) und (3.26) kann man auch direkt mit dem Gaußschen Eliminationsverfahren einsehen.

Exkurs: Fehlerkorrigierende Codes

Lit.: MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes, North-Holland, Amsterdam 1978.
van Lint, J.H.: Introduction to Coding Theory (3. Aufl.), Springer 1999.

Problem: bei der Übermittlung von Daten entstehen Fehler. Gesucht ist eine Methode, die die (meisten) Fehler automatisch korrigiert.

Daten $\overset{\text{Kodierung}}{\longrightarrow}$ endl. Folge der Länge n von $0,1$ $\overset{\text{Übermittlung}}{\longrightarrow}$ fehlerhafter Folge von $0,1$ $\overset{\text{automat. Fehlerkorrektur}}{\longrightarrow}$ ursprüngl. Folge von $0,1$ $\overset{\text{Dekodierung}}{\longrightarrow}$ ursprüngl. Daten.

Das kann nur funktionieren, wenn bei der Kodierung nur spezielle Folgen von $0,1$ ("die Wörter des Codes") verwendet werden.

Mathematische Formulierung:

$$\{0,1\}^n = \{(x_1, \ldots, x_n) \mid x_1 \in \{0,1\}, \ldots, x_n \in \{0,1\}\}$$

Folgen von $0,1$ der Länge n, z.B. $(0,1,0,1,0,1,0) \in \{0,1\}^7$

Hamming-Abstand d von Elementen $x, y \in \{0,1\}^n$

$$d(x,y) = \#\{i \mid 1 \leq i \leq n \text{ und } x_i \neq y_i\} \quad (\Rightarrow d(x,y) \in \{0, \ldots, n\})$$

Dabei wird mit $\#M$ die Anzahl der Elemente einer Menge M bezeichnet.

Bsp.: $(n = 4)$ $x = (0,0,1,1)$, $y = (0,1,1,0) \Rightarrow d(x,y) = 2$.

Eigenschaften von d: $\forall x, y, z \in \{0,1\}^n$ gilt:

(i) $d(x,y) \geq 0$ und $d(x,y) = 0 \Leftrightarrow x = y$

(ii) $d(x,y) = d(y,x)$ ("Symmetrie")
(iii) $d(x,y) \leq d(x,z) + d(z,y)$ ("Dreiecksungleichung")

(i)-(iii) $\Leftrightarrow$ "d ist Abstandsfunktion"

Zu $x \in \{0,1\}^n$, $t \in \mathbb{N}$ sei

$$B(x,t) = \{y \in \{0,1\}^n \mid d(x,y) \leq t\}$$

der (d-)Ball um x vom Radius t.

Bem.: $B(x,1)$ enthält genau $(n+1)$ Elemente.

(E1) Def.:

(i) Ein Code der Länge n ist eine Teilmenge $C \neq \emptyset$ von $\{0,1\}^n$.
(ii) Ein Code C heißt t-fehlerkorrigierend $\Leftrightarrow$
Ist $x \in C, y \in C, x \neq y$, so gilt $B(x,t) \cap B(y,t) = \emptyset$.

Idee: Sei C t-fehlerkorrigierender Code. Als kodierte Nachrichten sind nur "Codewörter" $x \in C$ erlaubt.

$$x \in C \overset{\text{Übermittlung}}{\longrightarrow} \overline{x} \in \{0,1\}^n \overset{\text{automat. Korrektur}}{\longrightarrow} \overline{\overline{x}} \in C \text{ so, daß } d(\overline{x}, \overline{\overline{x}}) \text{ minimal.}$$

Dann: Ist $d(x, \overline{x}) \leq t$, so gilt $\overline{\overline{x}} = x$, da es nur ein $x \in C$ mit $d(\overline{x}, x) \leq t$ gibt.
D.h.: Sind bei der Übermittlung höchstens t Fehler aufgetreten, so ordnet die automatische Fehlerkorrektur der fehlerhaften Nachricht $\overline{x}$ das ursprüngliche Codewort x zu.

Bem.: 1) $C \subseteq \{0,1\}^n$ ist t-fehlerkorrigierend $\Leftrightarrow$ Ist $x \in C$, $y \in C$ und $x \neq y$, so gilt $d(x,y) \geq 2t+1$ (Dreiecksungleichung!)
2) $C \subseteq \{0,1\}^n$ 1-fehlerkorriegierend $\Rightarrow \#C \cdot (n+1) \leq 2^n (= \#\{0,1\}^n)$

Problem: Zeitaufwand Fehlerkorrektur $\approx \#C \cdot n \approx 2^n$

Lineare Codes

$\{0,1\}^n$ ist Vektorraum über dem Körper $\{0,1\} = \mathbb{Z}_2$

(E2) Def. $C \subseteq \{0,1\}^n$ heißt linearer Code $\Leftrightarrow$ C ist Unterraum von $\{0,1\}^n$
($\Leftrightarrow \underline{0} \in C$ und $\forall x, y \in C : x + y \in C$)

Sei $p \in \mathbb{N}$ und $n := 2^p - 1$ (z.B. $p = 5, n = 31 \Rightarrow 2^n = 3^{31} = 2 \cdot (2^{10})^3 = 2 \cdot (1024)^3 \approx 2 \cdot 10^9$)

Seien $v_1, \ldots, v_n$ die von $\underline{0} \in \{0,1\}^p$ verschiedenen Elemente von $\{0,1\}^p$ und $F : \{0,1\}^n \to \{0,1\}^p$ definiert durch

$$F(x_1, \ldots, x_n) = x_1 v_1 + x_2 v_2 + \ldots + x_n v_n \in \{0,1\}^p$$

Dann gilt für alle $x, y \in \{0,1\}^n : F(x+y) = F(x) + F(y)$.

Daraus folgt: $C := \{x \in \{0,1\}^n \mid F(x) = \underline{0}\}$ ist Unterraum (=linearer Code).

C heißt der n'te Hammingcode.

(E3) Satz. *Der n'te Hammingcode ist ein 1-fehlerkorrigierender Code der Länge n*

$$\text{mit } \#C = \frac{2^n}{n+1} (\text{“}C \text{ ist perfekt”})$$

Bew.: Seien $x, y \in C$, $x \neq y$. Zu zeigen: $d(x,y) \geq 3$

$$x, y \in C \Rightarrow \quad (*) \quad (x_1 - y_1)v_1 + \ldots + (x_n - y_n)v_n = \underline{0}.$$

Wegen $x \neq y$ existiert ein $i \in \{1, \ldots, n\} : x_i \neq y_i$. Dann $(x_i - y_i)v_i = v_i \neq \underline{0}$.
Wegen $(*)$ existiert ein $j \neq i$ mit $x_j \neq y_j$, also $(x_j - y_j)v_j = v_j$. Wenn alle anderen Komponenten von x und y übereinstimmten, so wäre $(*)$ die Gleichung

$$v_i + v_j = \underline{0}$$

Da in $\mathbb{Z}_2$ $1+1=0$ gilt, gilt $v+v=\underline{0}$ für alle $v \in \{0,1\}^n$. D.h. aus $v_i + v_j = \underline{0}$, folgt $v_i = v_j$, im Widerspruch dazu, daß die v_i alle verschieden sind. Also gibt es mindestens eine weitere Komponente, in der x und y nicht übereinstimmen, d.h. $d(x,y) \geq 3$, wie behauptet.

Ist $x \in \{0,1\}^n$ und $F(x) \neq \underline{0}$, so gilt $F(x) = v_i$ für ein $i \in \{1, \ldots, n\}$.
Daraus folgt $F(x - e_i) = F(x) - F(e_i) = \underline{0}$, d.h. $x - e_i \in C$ und $d(x, x - e_i) = 1$.
Also $\bigcup_{x \in C} B(x,1) = \{0,1\}^n$ und damit $\#C \cdot (n+1) = 2^n$.

Algorithmus zur Korrektur <u>eines</u> Fehlers:

Sei $\overline{x} \in \{0,1\}^n$ die empfangene Nachricht. Berechne $F(\overline{x}) \in \{0,1\}^p$.

$$\begin{array}{lcl} F(\overline{x}) = \underline{0} & \Rightarrow & \overline{\overline{x}} := \overline{x} \\ F(\overline{x}) = v_i & \Rightarrow & \overline{\overline{x}} := \overline{x} + e_i \end{array}$$

Zeitaufwand $\approx n^2 p$ $(= 31^2 \cdot 5 \approx 5 \cdot 10^3) \ll 2^n \approx 2 \cdot 10^9)$