Lineare Algreba 1

Noah J. Zimmermann

supervised by

x

Wintersemester 2016/17

Inhaltsverzeichnis

Gruppen, Ringe und Körper

•

Verknüpfung

- def: M Menge . Eine Verknüpfung (innere Verknüpfung) auf M ist eine Abbildung $* : M \times M \to M$
  Normalerweise schreiben wir anstelle von $*(a, b) = a * b$

- Beispiele:
  $+ : \mathbb{R} \times \mathbb{R}, (a, b) \mapsto a + b$
  $\times : \mathbb{R} \times \mathbb{R}, (a, b) \mapsto a \times b$

Monoid Ein Monoid ist ein Tupel $(M, *)$, bestehend aus einer Menge M und einer Verknüpfung $* : M \times M \to M$ welche folgenden Bedingungen erfüllt:
(M1) Die Verknüpfung ist assoziativ, d.h. für alle $a, b, c \in M$ ist

$$a * (b * c) = (a * b) * c$$

(M2) Es ex. ein neutrales Element e in M, d.h. ein Element $e \in M$ mit

$$e * a = a = a * e$$

für alle $a \in M$

- Beispiele:
  (a) $(\mathbb{N}_0, +), (\mathbb{Z}, +)$ sind Monoide (neutrales Element : 0)
  (b) $(\mathbb{N}, +)$ ist kein Monoid (es ex. kein neutrales Element)
  (c) $(\mathbb{N}, \times), (\mathbb{Z}, \times)$ sind Monoide (neutrales Element : 1)

- Bemerkung:

  $(M, *)$ ist ein Monoid, dann gibt es genau ein neutrales Element.

  Beweis:
  Existenz per Definition.
  Eindeutigkeit: Seien $e, \tilde{e} \in M$ neutrale Elemente
  $\rightarrow e = e * \tilde{e} = \tilde{e}$

  q.e.d.

Inverses $(M, *)$ Monoid mit neutralem Element e , $a \in M$ Ein Element $b \in M$ heißt ein Inverses zu a genau dann wenn ($\leftrightarrow$) $a * b = e = b * a$

- Beispiel:
  In $(\mathbb{Z}, +)$ -2 ein Inverses zu 2 , denn : $2 + (-2) = 0 = (-2) + 2$
  In $(\mathbb{N}_0, +)$ existiert kein Inverses zu 2 , denn es existiert kein $n \in \mathbb{N}_0 : 2+n = 0 = n+2$

- Bemerkung:
  $(M, *)$ Monoid mit neutralem Element e , $a \in M$
  Besitzt a ein Inverses, dann ist dieses eindeutig bestimmt.

- Beweis:
  Seien $b, \tilde{b}$ Inverse zu a

  $\rightarrow b = e * b = \underbrace{(\tilde{b} * a)}_{e} * b = \tilde{b} * \underbrace{(a * b)}_{e} = \tilde{b}$

Gruppe DEF: Eine Gruppe ist ein Tupel $(G, *)$, bestehend aus einer Menge G und einer Verknüpfung $* : G \times G \to G$, so dass gilt:
(G1) (G, *) ist ein Monoid
(G2) Jedes Element aus G besitzt ein Inverses
In diesem Fall schreiben wir a' für das eindeutig bestimmte (siehe Beweis oben) Inverse eines Elementes $a\ inG$

- Beispiel:
  (a) $(\mathbb{Z}, +)$ ist eine Gruppe, denn : $(\mathbb{Z}, +)$ ist ein monoid, und für alle $a \in \mathbb{Z}$ ist $-a$ das inverse $E!$:
  $a + (-a) = 0 = (-a) + a$

  (b) $(\mathbb{Z}, \times)$ ist keine Gruppe, denn das Element $2 \in \mathbb{Z}$ hat kein Inverses

  (c) $(\mathbb{Q}\ 0, \times)$ ist eine Gruppe, denn $(\mathbb{Q}\ 0, \times)$ ist ein Monoid (mit neutr El. 1), und für jedes $E!a \in \mathbb{Q}\backslash\{0\}$ ex. ein $b \in \mathbb{Q}\backslash\{0\}$ mit $a \times b = 1 = b \times a$, nämlich $b = \frac{1}{a}$

Wichtige Bemerkungen bezüglich Gruppen $(G, *)$ Gruppe mit neutralem Element e , $a, b, c \in G$ Dann gilt :
(a) (Kürzungsregel) $a * b = a * c \to b = c$
$a * c = b * c \to a = b$
(b) $a * b = e \to b = a'$
(c) $(a')' = a$

(d) (Regel von Hemd und Jacke) $(a * b)' = b' * a'$

- Beweise :

(a) Sei $a * b = a * c \Rightarrow a' * (a * b) = a' * (a * c)$
$\Rightarrow ASS. \underbrace{(a' * a)}_{e} * b = \underbrace{(a' * a)}_{e} * c$
$\Rightarrow e * b = e * c \Rightarrow b = c$
andere Regel analog

(b) aus (a): $a * b = e = a * a' \Rightarrow (a)b = a'$
(c) Es ist $a * a' = e = a' * a$, d.h. a ist invers zu $a' \Rightarrow (a')' = a$
(d) Es ist $(a * b) * (b' * a') = a * \underbrace{(b * b')}_{e} * a' = a * a' = e \Rightarrow (b)(b' * a') = (a * b)'$

q.e.d.

Abelsch / Kommutativ

- Ein Monoid $(M, *)$ heißt abelsch, wenn für alle $a, b \in M$ gilt:

$$a * b = b * a$$

Symmetrische Gruppe

- Sei M eine Menge, dann ist $S(M) = \{f : M \to M | \textit{ f ist bijektiv}\}$. Dann ist $(S(M), \circ)$ eine symmetrische Gruppe und diese beinhaltet nun alle bijektiven Abbildungen auf sich selbst.

- Beweis, dass dies eine Gruppe ist.
  (1) Da die Komposition von zwei bijektiven (bzw. surjektiven oder injektiven) Funktionen wieder bijektiv ist, gilt

$$f, g \in S(M) \Rightarrow f \circ g \in S(M)$$

  (2) Die Assoziativität von Kompositionen ist bereits gezeigt
  (3) Das neutrale Element ist die id_M da gilt $id_m \circ f = f = f \circ id_m$

(4) Es wurde bereits gezeigt und es macht auch intuitiv Sinn, dass jede bijektive Abbildung (folgt aus $f \in S(M)$) eine Umkehrabbildung f^{-1} besitzt.

- **Kommentar:** $f : M \to N \wedge |M| = |N| \Leftrightarrow$ f ist bijektiv

Weiterführung Symmetrische Gruppen

- $S_n := S(\{1, ..., n\}) = \{\pi\{1, ..., n\} \mapsto \{1, ..., n\}\} | \pi$ ist bijektiv $\}$
  π **ist hier einfach ein beliebiger Name für eine Abbildung**
  $(S_n, \circ)$ heißt die symmetrische Gruppe auf n Ziffern.
  Elemente aus S_n heißen Permutationen

$$\pi = \begin{cases} 1 \ 2 \ ... \ n \\ \pi(1) \ \pi(2) \ ... \ \pi(n) \end{cases}$$

- Symmetrische Gruppen sind nicht abelsch! Dies ist leicht an einem Beispiel zu sehen (Vorlesung La 8.11.2016 / Bsp. 5.16)

Restklassen / Modulo

- Uhren funktionieren in einem Modulo Prinzip, wo verständlich ist, dass 22 Uhr + 7 h = 5 Uhr ist. Dieses Konzept will man nun verallgemeinern.

- Bem.5.17 $n \in \mathbb{N}$ Dann ist durch, DEF:

$$a \sim b \Leftrightarrow \text{ Es ex. } q \in \mathbb{Z} : a - b = qn$$

eine Äquivalenzrelation auf $\mathbb{Z}$ gegeben.
Anstelle von $a \sim b$ schreiben wir auch $a \equiv b(modn)$ (ä kongruent b modulo n ") Man

meine damit, dass a in Relation zu b ist, wenn die Differenz ein vielfaches von n ist.
Beispiel:

$$11 \equiv 5(mod 3) = 11 - 5 = 6 = 3 * 2 = q \times n$$

Dazugehörige Äquivalenzklassen = Restklassen

- $$\overline{a} := \{b \in \mathbb{Z} | b \equiv a(mod n)\} = a + n\mathbb{Z} := \{a + nq | q \in \mathbb{Z}\}$$

  heißt also die Restklasse von a modulo n
  Die Menge aller Restklassen modulo n wird $\mathbb{Z}/_n\mathbb{Z}$ bezeichnet ("$\mathbb{Z}$ modulo $\mathbb{Z}$")
  Es ist $\mathbb{Z}/_n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{n-1}\}$
  ((n-1) weil bei der 0 angefangen wird zu zählen). Die Restklassen sind natürlich alle verschieden.

- Die dazugehörige Äquivalenzrelation kann leicht bewiesen werden, indem man die Eigenschaften durchgeht.

- Die Äquivalenzklase ist wie folgt gegeben:

$$\begin{aligned} \{b \in \mathbb{Z} \,|b \equiv a(mod\ n)\} &:= \{b \in \mathbb{Z} \,|\textit{Es existiert ein } q \in \mathbb{Z} : b - a = qn\} \\ &:= \{b \in \mathbb{Z} \,|\textit{Es existiert } \ q \in \mathbb{Z} mit b = a + qn\} \qquad (1) \\ &:= a + n\mathbb{Z} \end{aligned}$$

Fortsetzung zu Restklassen

- $\mathbb{Z}/_n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{n-1}\}$ gilt denn, ist $a \in \mathbb{Z}$ beliebig, so liefert Division mit Rest durch n:
  $\exists q, r \in \mathbb{Z}$ mit $a = qn + r, 0 \leq r < n$
  $\Rightarrow a - r = qn \Rightarrow a \equiv r$ (mod n) $\Rightarrow \overline{a} = \overline{r}$

- Dies sagt uns quasi nur, dass jede beliebige Zahl in einem Modulo System zu einer dieser $\{\overline{0}, \overline{1}, \overline{n-1}\}$ Äquivalenzklassen korrespondiert.

Beispiele zu Restklassen

- $n = 3 : a \equiv b(\text{ mod } 3) \Leftrightarrow$ Es ex. $q \in \mathbb{Z}$ mit $a - b = 3q$
  z.B.: $11 \equiv 5$ (mod 3) , denn $11 - 5 = 6 = 2 * 3$

- Beispiele für Restklassen (Äquivalenzklassen)

  $\overline{0} = \{a \in \mathbb{Z} |\ a \equiv 0(\textit{mod } 3)\} = \{a \in \mathbb{Z} |\ \textit{Es ex. ein } q \in \mathbb{Z} : a = 3q\} = 3\mathbb{Z} = \{..., -9, -6, -3, 0, 3, 6...\}$

  $\overline{1} = \{a \in \mathbb{Z} |\ a \equiv 1(\textit{mod } 3)\} = \{a \in \mathbb{Z} |\ \textit{Es ex. ein } q \in \mathbb{Z} : a-1 = 3q\} = 1+3\mathbb{Z} = \{...-5, -2, 1, 4, 7, ..$

  Demnach gilt dann auch für (mod 3) : $\overline{0} = \overline{3}$

Wichtige Bemerkung 5.19

- Man definiere eine Verknüpfung (Addition) auf $\mathbb{Z}/_n\mathbb{Z}$ wie folgt :
  Für $\overline{a}, \overline{b} \in \mathbb{Z}/_n\mathbb{Z}$ setzen wir $\overline{a}, \overline{b} := \overline{a + b}$ Damit ist $(\mathbb{Z}/_n\mathbb{Z}, +)$ eine abelsche Gruppe.
  Da diese Verknüpfung nun Verteter verwendet, müssen wir uns davon überzeugen, dass dies keinen Einfluss auf das Ergebnis hat (z.B. $3 \equiv 5$ (mod 3))

Gruppenhomomorphismus

- **Disclaimer:** Eigentlich wird der spezifische Homomorphismus benannt (Vektorraumhomormorphismus, Gruppenhomomorphismus, etc.), jedoch wird er meistens weglassen, wenn klar ist, was der Kontext ist und nur mit Homomormphismus benannt.

- Zwei Gruppen $(G, *), (H, *_2), \varphi : G \to H$ Abb.

- φ heißt ein Gruppenhomomorphismus DEF Für alle $a, b \in G$ gilt:

$$\varphi(a * b) = \varphi(a) *_2 \varphi(b)$$

- φ heißt ein Gruppenisomorphismus DEF φ ist ein bijektiver Gruppenhomomorphismus

- Dies ist ein simples Konzept, deshalb hier Beispiele:
  (a) $\varphi : \mathbb{Z} \to \mathbb{Z}, a \mapsto 2a$ ist ein Gruppenhomo. von $(\mathbb{Z}, +)$nach $(\mathbb{Z}, +)$, denn :
  $\varphi(a + b) = 2(a + b) = 2a + 2b = \varphi(a) + \varphi(b)$ für alle $a, b \in \mathbb{Z}$

  (b) $n \in \mathbb{N}$ Dann ist $\varphi : \mathbb{Z} \to \mathbb{Z}/_n\mathbb{Z}, a \mapsto \overline{a}$ ist ein Gruppenhomo. von
  $(\mathbb{Z}, +)$ nach $(\mathbb{Z}/_n\mathbb{Z}, +)$, denn:
  Für alle $a, b \in \mathbb{Z}$ ist $\varphi(a + b) = \overline{a + b} = \overline{a} + \overline{b} = \varphi(a) + \varphi(b)$
  Jedoch kein Gruppenisomorphismus, denn φ ist nicht injektiv
  ($\varphi(0) = \overline{0} = \overline{n} = \varphi(n)$, jedoch $n \neq 0$ das n ist hier modulo n)

  (c) **Gegenbeispiel** $\varphi : \mathbb{Z} \to \mathbb{Z}, a \mapsto a + 1$ ist **kein** Gruppenhomomorphismus von
  $(\mathbb{Z}, +)$ nach $(\mathbb{Z}, +)$, denn :
  $\varphi(2 + 6) = \varphi(8) = 9$, aber $\varphi(2) + \varphi(6) = 3 + 7 = 10$

Eigenschaften des Gruppenhomomorphismus

- $(G, *), (H, *_2)$ Gruppen mit neutralen Elementen e_G bzw. e_H , $\varphi : G \to H$ ist ein Gruppenhomo.
  Dann gilt:
  (a) $\varphi(e_G) = e_H$
  Beweis: $e_G *_2 \varphi(e_G) = \varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) * \varphi(e_G)$ wir kürzen nun die ganz linke und ganz rechte Gleichung er halten $\varphi(e_G) = e_H$, was zu zeigen war.

q.e.d.

(b) Für alle $a \in G$ ist $\varphi(a') = \varphi(a)'$ (hierbei bezeichnet ' das Inverse)
Beweis:

Aus (a) wissen wir : $\varphi(e_G) = e_H$ und die Definition von dem Inversen ist $a * a' = e$, wo e das neutrale Element ist
(denke $2 * \frac{1}{2} = 1$)
Zu zeigen: $\varphi(a) *_2 \varphi(a') = e_H$ Dies impliziert nämlich, dass $\varphi(a')$ das Inverse zu einem $\varphi(a)$ ist, da es das neutrale Element von H wiedergibt.
$e_H = \varphi(e_G) = \varphi(a * a') = \varphi(a) *_2 \varphi(a')$

q.e.d.

(c) Ist φ ein Gruppenisomorphismus, dann ist $\varphi^- 1 : H \to G$ ebenfalls ein Gruppenisomorphismus
$(G, *), (H, *_2)$ heißen isomorph DEF es ex. ein Gruppenisomorph $\varphi : G \to H$ Wir schreiben dann $(G, *) \tilde{=} (H, *_2)$

Ringe (6)

- Def: Ein Ring ist ein Tripel $(R, +, *)$, bestehend aus einer Menge R und zwei Verknüpfungen
  1. + : $R \times R \to R, (a, b) \mapsto a + b$ genannt Addition
  2. * : $R \times R \to R, (a, b) \mapsto a * b$ genannt Multiplikation

  Diese sollen den folgenden Bedingungen genügen:
  (R1) $(R, +)$ ist eine abelsche Gruppe
  (R2) $(R, *)$ ist ein Monoid (keine Gruppe unbedingt, da noch kein inverses Element vorhanden)
  (R3) Es gelten die Distributivgesetze,d.h. für alle $a, b, c \in R$ ist
  $a * (b + c) = ab + ac$

Ein Ring heißt kommutativ *DEF* die Multiplikation ist kommutativ, d.h. $a * b = b * a$ für alle $a, b \in R$

- Anmerkungen:
  Es gilt * vor Strich.
  Das neutrale Element bzgl. "+"bezeichnen wir mit 0_R (Nullelement), für Multiplikation 1_R (Einselement)
  Inverses zu + ist -. Zu Multiplikation a^-1
  Man schreibt häufig auch R Ring, anstatt $(R, +, *)$

- R Ring. Dann gilt:
  (a) $0_R * a = 0_R = a * 0_R$ für alle $a \in R$
  (b) $a * (-b) = -ab = (-a) * b$ für alle $a, b \in R$
  (c) Ist $R \neq 0$, dann ist $1_R \neq 0_R$ Dies bedeutet, dass in einem Ring (nicht Nullring) das neutrale Element ungleich dem Nullelement ist.

  Beweis:
  (a) zz.: $0_R * a = 0_R$
  $0_R + 0_R * a = 0_R * a = (0_R * 0_R) * a = 0_R * a + 0_R * a =$ ***kürzen*** $0_R * a$
  (b) $0_R =$ ***siehe (a)*** $0_R * b = (a + (-a)) * b = a * b + (-a) * b \xrightarrow{kuerzen} -ab = (-a) * b = -ab$
  (c) Beweis durch Kontraposition,d.h. zu zeigen: $1_R = 0_R \rightarrow R = 0$
  Für jedes $a \in R$ ist $a = a * 1_R = a * 0_R = 0_R$ (Vergleiche (a) und Definition von neutralem bzw. Einselement)

- Beispiele:
  (a) $(\mathbb{Z}, +, *)$ ist ein kommutativer Ring (b) Nullring $(\{0\}, +, *)$ mit $0 + 0 = 0$, $0 * 0 = 0$ ist ein kommutativer Ring (hier ist Nullelement = Einselement = 0). Wir bezeichnen den Nullring kurz mit 0.

Der Ring $(\mathbb{Z}/_n\mathbb{Z}, +, *)$

- Beweis, dass dies ein kommutativer Ring ist:
  (1) Multiplikation ist wohldefiniert (vgl. Vertreterunabhängigkeit von Modulo Rechnung (5.18))
  (2) Multiplikation ist assoziativ (Beweis durch simples Ausklammern und mithilfe von Assoziativgesetz in $\mathbb{Z}$)
  (3) Existenz eines Einselements $\overline{1} * \overline{a} = \overline{a} = \overline{a} * \overline{1}$
  (4) Multiplikation ist kommutativ
  (5) $(\mathbb{Z}/_n\mathbb{Z}, +)$ ist eine abelsche Gruppe
  (6) Distributivgesetz (folgt ebenfalls aus $\mathbb{Z}$)

- Ist also vom Ring $\mathbb{Z}/_n\mathbb{Z}$ die Rede, ist dieser gemeint.

Integritätsbereich bzw. Ring

- *DEF* ist ein kommutativer Ring $(R, +, *)$ mit $R \neq 0$ in dem gilt: Für alle $a, b \in R$ gilt: $a * b = 0_R \rightarrow a = 0_R$ *oder* $b = 0_R$ bzw. äquivalent zu $a \neq 0_R$ und $b \neq 0_R \rightarrow a * b \neq 0_R$

- Beispiel:
  $\mathbb{Z}/_3\mathbb{Z}$ ist ein Integritätsbereich, $\mathbb{Z}/_4\mathbb{Z}$ ist kein Integritätsbereich, denn

$$\overline{2} * \overline{2} = \overline{4} = \overline{0}, \textit{aber } \overline{2} \neq \overline{0}$$

- Bemerkung: $n \in \mathbb{N}$, dann sind äquivalent:
  (1) $\mathbb{Z}/_n\mathbb{Z}$ ist ein Körper
  (2) n ist eine Primzahl

Körper

- Ein Körper ist ein kommutativer Ring $(K, +, *)$, in dem gilt:
  $K \neq 0$ und jedes Element $a \in K, a \neq 0$ besitzt ein Inverses in K bzgl. "* ", d.h.
  es existiert $b \in K$ mit $a * b = 1_K$. Wir setzen $K^*K\backslash\{0\}$

- Beispiel:
  (1) $(\mathbb{R}, +, *)$, $(\mathbb{Q}, +, *)$ sind Körper (2) $\mathbb{Z}/_3\mathbb{Z}$ ist ein Körper (3) $\mathbb{Z}/_4\mathbb{Z}$ ist kein Körper.
  Wäre es ein Körper, dann müsste gelten :
  Es ex. $\overline{a} \in \mathbb{Z}/_4\mathbb{Z} : \overline{2} * \overline{a} = \overline{1}$ (vgl. inverses und neutrales Element)
  Dieses existiert jedoch nicht.

Eigenschaften von Körpern

(1) $0_K \neq 1_K$ folgt aus den Eigenschaften von Ringen
(2) K ist ein Integritätsbereich
(3) $(K*, \times)$ ist eine abelsche Gruppe mit neutralem Element 1_K

- Beweis:
  (2) $K \neq 0$ nach Definition. Seien $a, b \in K$ sodass $a * b = 0_K$
  Nach der Definition eines Integritätsbereiches ist nun zu zeigen, dass wenn $a * b = 0_K$, dann muss mindestes a oder b null sein.

$$b = 1_K * b = (a^-1 * a) * b = a^-1 * (a * b) = a^-1 * 0_K = 0_K$$

  Inbesondere gilt also: $a = 0$ oder $b = 0$
  (3) siehe LA Notizen 13.11 oder VL 10.11.2016

- $\mathbb{Z}/_n\mathbb{Z}$ ist ein Körper und n ist eine Primzahl sind äquivalente Aussagen

- sei p eine Primzahl. Man nennt $\mathbb{F} := \mathbb{Z}/_p\mathbb{Z}$ auch den endlichen Körper mit p Elementen.

Def 6.14 Charakteristik eines Rings

- R Ring

$$\text{char}(R) := \begin{cases} 0, \textit{ falls } 1_R + ...1_R \neq 0_R \quad \forall n \in \mathbb{N} \\ min\{n \in \mathbb{N} |\ 1_R + ...1_R = 0_R\} \end{cases}$$

Somit ist n die Charakteristik des Ringes und beschreibt wie oft man das Einselement miteinander addieren muss, um das Nullelement zu kriegen (meist gar nicht möglich).

- Beispiel:
1. $\textit{char}(\mathbb{Z}) = \textit{char}(\mathbb{Q}) = \textit{char}(\mathbb{R})$ 2. $\textit{char}(\mathbb{Z}/n\mathbb{Z}) = n$, denn

$$\overline{1} + \overline{1} + \overline{1} + ... + \overline{1} = \overline{n} = \overline{0}$$

- Bemerkung 6.16

Wenn R ein Integritätsbereich ist, dann ist char(R) = 0 oder char(R) ist eine Primzahl. (Beweis, siehe Ordner)

- Bemerkung 6.17

Das gleiche gilt für Körper, da jeder Körper nach Definition ein Integritätsbereich ist (siehe 6.11 und 6.16).

Polynome

- Sei K ein Körper.
  Ein Polynom in der Variablen t über K ist ein Ausdruck der Form:

$$\sum_{k=0}^{n} a_k \times t^k = f$$

  mit $n \in \mathbb{N}_0$ (das heißt insbesondere nur endliche Summanden), fehlende Summanden setzen wir =0; die a_k heißen die Koeffizienten von f

- $$deg(f) := \begin{cases} -\infty & f = 0 \\ max k \in \mathbb{N}_0 |\ a_k \neq 0 & f \neq 0 \end{cases}$$

  nennen wir Grad von f. Der Leitkoeffizient heißt $l(f) := a_d eg(f)$. f heißt normiert, falls der Leitkoeffizient 1 ist.

  Zwei Polynome sind identisch, wenn der Grad gleich ist und jeder einzelne Koeffizient gleich ist.

- Beispiel:

$$f = \frac{3}{4}x^2 - 7x \in \mathbb{Q}[x] \Rightarrow deg(f) = 2\ l(f) = \frac{3}{4}$$

  f ist demnach nicht normiert

- Multiplikation und Addition von Polynomen:
  K Körper $f, g \in K[t],\ \sum_{k=0}^{n} a_k \times t^k = f,\ \sum_{k=0}^{g} b_k \times t^k = g$

  Man setze $r := max\{m, n\}$, also den maximalen Grad beider Funktionen

  $$f + g = (a_r + b_r)t^r + ... + (a_1 + b_1)t + (a_0 + b_0)$$

  $$f * g = c_n + mt^n + m + ... + c_1 * t + c_0$$

  wo

  $$c_k := \sum_{i+j=k} a_i b_j$$

  Man multipliziert sie einfach nach den ganz normalen Rechenregeln.. Und damit bilden sie einen Ring, den kommutativen Polynomring. Allgemein ist jedoch nicht jeder Ring bezüglich der Multiplikation kommutativ!

- Bemerkung 5 7.4
  K Körper $f, g \in K[t]$

  1. $deg(f + g) \leq max\{deg(f), deg(g)\}$
  2. $deg(fg) = deg(f) + deg(g)$

- Bemerkung 7.5
  K Körper, dann ist $K[t]$ ein Integritätsbereich.
  Anmerkung: $K[t]$ ist aber kein Körper, da es kein inverses zu zum Beispiel t gibt, da negative Exponenten nicht zulässig sind (sprich $\frac{1}{t} = t^{-1}$)

- Satz 7.6:
  Polynomdivision (Konstruktive Herleitung)
  K Körper, $f, g \in K[t],\ g \neq 0$

Dann ex. eindeutig bestimme Polynome $q, r \in K[t]$ mit

$$f = qg + r$$

und es gilt zusätzlich $deg(r) < deg(g)$

Def. 7.8 Nullstellen

- Sei $f \in K[t]$

- x heißt Nullstelle von $f \Leftrightarrow f(x) = 0$

- Bemerkung: $f \in K[t]$ und x sei eine Nullstelle von f, dann gibt es in $K[t]$ ein eindeutig bestimmtes Polynom q mit $f = (t - x)q$
  Es gilt $deg(q) = deg(f) - 1$

  Jede Nullstelle eines Polynoms kann als Linearfaktor ausgeklammert werden. q stellt dann den "Rest"des Polynoms dar.

- Folgerung 7.10
  $f \in K[t], K$ Körper, $f \neq 0$ $n := deg(f)$

  Dann besitzt f in K höchstens n Nullstellen.

def: 7.11

- $f \in K[t], K$ Körper, $f \neq 0$, $\lambda \in K$

$$\mu(f, \lambda) := max\{e \in \mathbb{N}_0 | \textit{ Es ex. ein } g \in K[t] \ f = (t - \lambda)^e \times g \ \}$$

  heißt die Vielfachheit der Nullstelle λ von f.

- Weiterhin zur Vielfachheit
  Es gilt, $\mu(f, \lambda) = 0$ dann ist Lambda keine Nullstelle von f. Dies ist offensichtlich, da ja sonst lambda als Linearfaktor ausgeklammert werden könnte und dann wäre die Vielfachheit 1

$$\mu(f, \lambda) = 1$$

  Die Vielfachheit von Lambda gibt an, wie oft der Linearfaktor von Lambda in f vorkommt.
  Gibt es mehrere verschiedene Nullstellen $x_1, x_2, ..., x_n \in K$ und ist $e_i = \mu(f, x_i)$ I indiziert hier unsere x_n, dann existiert ein Polynom
  $g \in K[t]$ mit

$$f = (t - x_1)^{e_1} \times ... \times (t - x_n)^{e_n} \times g$$

  und den Eigenschaften, dass g in K keine Nullstelle besitzt und dass

$$deg(g) = deg(f) - (e_1 + ... + e_n)$$

  Man zieht also in diesem Verfahren von dem originalen Polynomgrad f die ganzen Linearfaktorengrade ab (bzw. die Vielfachheit dieser, falls diese mehrfach vorkommen bzw. !). Man definiert die Differenz als das Polynom g.

  Der beste Fall, ist dass das Polynom komplett in Linearfaktoren zerfällt, dann ist der Grad von $deg(g) = 0$. Wir sagen das auch für den Fall, dass $n = 0$, sprich, dass das Polynom konstant ist, also keine t Potenzen enthält und ungleich dem Nullpolynom ist.

  Als Gegenbeispiel, in den reelen Zahlen ist dies nicht immer der Fall, da manche Polynome keine Nullstellen haben und sich somit nicht als Linearfaktoren ausklammern lassen, somit ist unser Differenzpolynom $deg(g) \neq 0$.

Fundamentalsatz der Algebra

- Jedes Polynom $f^{\in}\mathbb{C}[t]$ mit $deg(f)^{\geq}1$ besitzt eine Nullstelle.

- Damit folgt, dass wenn $f^{\in}\mathbb{C}[t]$ und f nicht das Nullpolynom ist, dass f in Linearfaktoren zerfällt.
- Der Beweis ähnelt dem Beweis zur Linearfaktorerzerlegung. Man beginnt mit der IA mit dem konstantem Polynom. Dann sei die Aussage bewiesen für alle Polynome mit einem kleinerem Grad als $deg(f)$. Man weiß nach dem FS der Algreba, dass mindestens eine Nullstelle existiert. Man klammert die aus und nun hat man ein Polynom mit einem kleineren Grad als $deg(f)$ und unsere IV greift.

def: 7.14

- f induziert eine Abbildung
$$\tilde{f} : K \to K, x \mapsto f(x)$$
Man nennt die Abbildung $\tilde{f}$ die Polynomfunktion zum Polynom f

Die Polynomfunktion ordnet also dem Polynom ihr Element zu.

Beispielsweise induziert $f = t^2 \in K[t]$ die Abbildung

$$\tilde{f} : K \to K, x \to f(x) = x^2$$

- Bsp: Die Polynomfunktion und das Polynom sind **nicht** gleich.
Sei $f = t^2 + t \in \mathbb{F}_2[t]$
Dann ist $f(\overline{0}) = \overline{0}^2 + \overline{0} = \overline{0}$, $f(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{0}$

d.h. $\tilde{f} : \mathbb{F} \to \mathbb{F}$ ist die Nullabbildung, aber f ist nicht das Nullpolynom.

Bem. 7.16 Sei K ein Körper mit unendlich vielen Elementen

Man ordnet nun jedem Polynom, was so eine Polynomfunktion induziert so eine Polynomfunktion $\sim$ zu. Bei unendlich vielen Elementen ist diese injektiv und somit ist jede von diesen Tilde Polynomfunktionen eindeutig.

Dann ist die Abbildung $\tilde{f} : K[t] \to Abb(K, K) := \{g : K \to K \textit{ Abbildung } \}$ injektiv

- dies gilt jedoch nur für unendliche Körper!

Vektorräume

- K sei stets ein Körper

§8 Vektorräume

def: 8.1

- Ein K-Vektorraum ist ein Tripel $(V, +, *)$ bestehend aus einer Menge V, einer Verknüpfung der Addition

$$+ : V \times V \to V, (v, w) \mapsto v + w$$

und einer äußeren Verknüpfung der skalaren Multiplikation (äußere Verknüpfung, da ein Element des Körpers K mit einem Vektor aus der Menge V multipliziert wird). Zahlen des Körpers sind dabei Skalare, da sie die Vektoren ßkalieren"

$$\times \ : K \times V \to V, (\lambda, v) \mapsto \lambda * v$$

Folgende Bedingungen müssen erfüllt sein:

(V1) $(V, +)$ ist eine abelsche Gruppe
(V2) Die skalare Multiplikation ist in folgender Weise mit den anderen Verknüpfungen auf V und K verträglich:

Für alle $x, y \in K, v, w \in V$ ist

$$(x + y) * v = xv + yv$$

$$x(v + w) = xv + xw$$

$$x(y * v) = (xy) * v$$

$$1 * v = v$$

Bedeutet: Distributivität, Assoziativität, Einselement
Die Kommutativität der Multiplikation folgt, wenn der Körper über dem der Vektorraum liegt kommutativ ist. (was er ja zwinged nach unser Definition ist, nur gibt es in der allg. Mathematik auch nicht kommutative, sogenannte schiefe Körper)

beispiele für VR: (1) $\mathbb{C}$ ist ein $\mathbb{R} - VR$
Die Addition ist wie gewohnt definiert.
Die skalare Multiplikation:

$$\times : \mathbb{R} \times \mathbb{C} \to \mathbb{C}, \lambda * (a + bi) := \lambda a + \lambda bi$$

(2) $K[t]$ Polynomring über K in der Variablen t wird zum K-VR durch die reguläre Addition von Polynomen und der skalaren Multiplikation wie folgt:

$$\times : K * K[t] \to K[t], \lambda * (a_n t^n + ... + a_0) := \lambda a_n + t^n ...$$

Bemerkung 8.3 Sei V ein K-VR Vektorraum, dann gilt:

(a) $0_K * v = 0_V$ für alle $v \in V$

(b) $\lambda * 0_V$ für alle $\lambda \in K$

(c) $\lambda * v = 0_V \Rightarrow \lambda = 0_K$ oder $v = 0_V$

(d) $(-1_K) * v = -v$ für alle $v \in V$

Untervektorraum

- V ist ein K-VR und $U \subset V$
  Dann müssen folgende Bedingungen erfüllt sein:

  (U1) $U \neq 0$
  (U2) $v, w \in U \Rightarrow v + w \in U$ Man nennt dies abgeschlossen bzgl. Addition
  (U3) $v \in U, \lambda \in K \Rightarrow \lambda * v \in U$ (d.h. U ist abgeschlossen bzgl. skal. Mult.)

Bemerkung 8.5

- V K-VR, $U \subset V$
  Dann sind äquivalent

  (i) U ist UVR (Untervektorraum) von V

  (ii) Addition und skal. Mult. auf dem V induzieren durch Einschränkung auf U Verknüpfungen. Einschränkungen deshalb, weil wir diese kleinere Teilmenge haben und nur auf dieser jetzt die Verknüpfungen definieren, und somit die Menge V einschränken. Darum muss man aber auch aufpassen, ob diese wohldefiniert (abgeschlossen sind, da es ja sein kann, dass das Bild außerhalb von U liegt.

  $$+ : U \times U \to U$$
  $$\times : K \times U \to U$$

  bzgl. dieser Verknüpfungen ist U ein K-VR

Anmerkung Nun folgt aus diesem Beweis, dass $0_V = 0_U \in U$ und somit können wir die Indizes einfach weglassen.

Weitere Beispiele zu Untervektorräumen in dem Ordner Handschriftliche Beweise oder in der VL vom 22.11.2016

Anmerkung V K-VR, dann sind 0 und V triviale UVR von V
0 ist abgeschlossen, da es ja nur Vektor + Vektor abgeschlossen ist per Addition. Und Nullvektor + Nullvektor bleibt Nullvektor.
Man nennt den ersten Fall auch den Nullvektorraum oder nur Nullraum.

Bemerkung 8.7 V K-VR, I sei eine Indexmenge, $(U_i)_{i \in I}$ (einfach nur eine Menge von Untervektorräumen und wir indizieren die einfach durch mit der Menge der Zahlen in I) , d.h. für jedes Index ($i \in I$) ist ein UVR von V gegeben

Sei unsere Menge beispielsweise $I = \{1, 2\}$, dann haben wir U_1, U_2

Dann ist $U := \cap U_i$ (also der Durschnitt aller dieser durchindizierten Mengen) ein UVR von V.

Der Durschnitt von UVRs von V ist wieder ein UVR.

Die Vereinigung von UVRs ist meistens **kein UVR**, da sie bzgl. der Verknüpfungen oft nicht abgeschlossen ist.

Def. 8.9

- V sei ein K-VR, $(v_1, ..., v_r)$ ist eine **endl. Familie** von Vektoren aus V

Die Lineare Hülle

$$lin((v_1, ..., v_r)) := \{a_1 * v_1 + ... + a_r * v_r |\ a_1, ..., a_r \in K\}$$

heißt die **lineare Hülle** oder das Erzeugnis der Familie $v_1, ..., v_r$, $v \in V$ heißt Linearkombination von

$$\begin{aligned} v_1, ..., v_r \Leftrightarrow v \in \textit{Lin}((v_1, ..., v_r)) \\ \Leftrightarrow \textit{ Es ex. } a_1, ..., a_r \in K \textit{ mit } v = a_1 * v_1 + ... + a_r * v_r \end{aligned} \tag{2}$$

Andere Notationen für Lin: span(...), <...> ,

In anderen Worten, die lineare Hülle sind einfach alle möglichen Vielfachen des Vektors. Die Menge

$$x \in K, v \in V\ Lin((v)) = x * v |\ x \in \mathbb{K}$$

Grafisch gesehen ist es dann nur die Ërweiterung des Vektorsïn eine Gerade.

Bsp. 8.10 (a) Beispielsweise kann man sich überlegen, dass alle Linearen Hüllen der Einheitsvektoren den K^n bilden, da ja jeder Punkt dargestellt werden kann (sozusagen, hätte man dann in R^3 3 Lineare Hüllen, welche die Achsen bilden)
Weiterhin sollte man sich klar machen, dass dieses Summenzeichen dafür steht, dass es ja all diese möglichen Kombinationen der Richtungen sein können und somit alle möglichen Punkte getroffen werden können.

Man nennt einen dieser Einheitsvektoren $e_i := (\ \underbrace{0, 0, 1, 0}_{\textit{i-te Stelle eine 1}}\ )$

$$
\begin{aligned}
\textit{Lin}\left((e_1,...,e_n)\right) &= \{a_1 * e_1 + ... + a_n * e_n |\ a_1,...,a_n \in K\} \\
&= \{(a_1,0,...,0) + (0,a_2,0,0...0)...(0,0...,a_n) | a_1,...,a_n \in K\} \\
&= \{(a_1,...a_n) | a_1,...,a_2 \in K\} \\
&= K^n
\end{aligned}
\tag{3}
$$

Anmerkung Die Lineare Hülle ist also nichts weiter als ein Vektorraum aller möglichen Linearkombinationen der Vektoren (wie dimensional die auch aussehen mögen). Linearkombination bedeutet, erreichbar durch Summen und Produkte.

Def. 8.11 Diese Definition soll nun den Begriff der Linearen Hülle auf **unendliche Familien** von Vektoren anwenden, im Gegensatz zu den vorher angesprochenen endlichen Familien.

Da unendliche Summen problematisch in der Algebra sind, werden diese kategorisch vermieden und dieses fast alle bewahrt uns davor.

V K-VR, $(v_i)_{i\in I}$ Familie von Vektoren aus V

$$\textit{Lin}((v_i)_{i\in I}) := \{\sum_{i\in I} a_i v_i |\ a_i \in K \textbf{ für alle } i \in I, a_i = 0 \textit{ für fast alle } i \in I\}$$

heißt die lineare Hülle (das Erzeugnis) der Familie v_i

Hierbei bedeutet "$a_i = 0$ "für fast alle $i \in I$: Es gibt nur endlich viele $i \in I$ mit $a_i \neq 0$

d.h. die auftretenden Summen sind endliche Summen

Falls die Indexmenge $I = \not\emptyset$, setzen wir $\textit{Lin}((v_i)_{i\in\not\emptyset}) := \{0\}$

Da nun fast alle Faktoren null sind, ist es nicht wirklich eine unendlich Summe, denn die Vielfachen, die nicht 0 sind, sind ja endlich.

Anmerkung Lin = Lineare Hülle

Ein Element $v \in V$ ist genau dann in $\mathit{Lin}((v_i)_{i\in I})$ enthalten, wenn es eine endl. Teilmenge
$\{i_1, ..., i_r\} \subset I$ und Elemente $(a_i)_1, ..., (a_i)_r \in K$ gibt mit der Eigenschaft:

$$v = (a_i)_1(v_i)_1 + ... + (a_i)_r(v_i)_r$$

Insbesondere ist $\mathit{Lin}((v_i)_{i\in I}) = \cup_{X\subset I \text{ finite}} \mathit{Lin}((v_i)_{i\in I})$

Bedeutet nur, dass ein Vektor in dieser linearen Hülle enthalten ist, falls man ihn durch eine endliche Summe von Linearkombination darstellen kann. Beispielsweise ist der Vektor $(3, 3) \in \mathit{Lin}[(1, 0), (0, 1)]$, da der Vektor doch auf jeden Fall, als eine Linearkombinationen dieser Linearen Hülle dargestellt werden kann.

- Bsp:
  $V = K[t]$ ist ein K- Vektorraum

  Es ist Lin$((t^n)_{n\in\mathbb{N}_0})$. Nach Definition:

$$\text{Lin}((t^n)_{n\in\mathbb{N}_0}) = \{\sum_{i\in I} a_i t^i |\ a_i \in K \textbf{ für alle } i \in \mathbb{N}_0, a_i = 0 \textit{ für fast alle } i \in \mathbb{N}_0\}$$

  Erneut, hier sind ja dann alle Vielfachen von diesen t^n Potenzen drin, praktisch alle Polynome. Damit bildet man ja dann den Polynomkörper $K[t]$

- Bemerkung 8.13

  V K-VR, $(v_i)_{i\in I}$ Familie von Vektoren aus V

  Dann gilt
  a) $\mathit{Lin}((v_i)_{i\in I})$ ist ein UVR von V
  b) Ist $U \subset V$ ein UVR mit $v_i \in U$ für alle $i \in I$, dann ist

  $$\mathit{Lin}((v_i)_{i\in I}) \subset U$$

  d.h. $\mathit{Lin}((v_i)_{i\in I})$ ist das bzgl. " $\subset$ " (also bezüglich Inklusion geordnet), das kleinste Element der Menge derjenigen UVr von V, die alle $v_i, i \in I$ enthalten.
  c)

  $$\mathit{Lin}((v_i)_{i\in I}) = \cap U$$

  Der Durchschnitt von allen UVR von V, wo alle $v_i \in U$ für alle $i \in I$ enthalten sind, also alle Vektoren.

Notation dazu: Ist $M \subset V$, dann setzen wir $Lin(M) := \mathit{Lin}((m)_{m\in M})$. Falls man nicht direkt eine Familie nimmt, sondern eine Menge, kann man wieder aus der Menge eine Familie kreieren, indem wir einfach alle Elemente der Menge in diese Familie aufnehmen. Nach 8.13 ist dies der kleinste UVR, der alle Vektoren enthält, hier also alle $m \in M$.

Der Vorteil von Familien gegenüber Mengen, ist dass Elemente mehrfach vorkommen können. Darüber hinaus kann man bei Familien auch über eine Reihenfolge sprechen, was sinnvoll im Kontext der Vektoren sein kann. Zum Beispiel bei der späteren Betrachtung von Basen. Da ist die Position des Vektors in der Familie relevant.

Lineare Unabhängigkeit

V K-VR, $(v_i)_{i \in I}$ Familie von Vektoren aus V
$(v_1, ..., v_r)$ endliche Familie von Vektoren ist **linear unabhängig** DEF$\lambda_1, ..., \lambda_r \in K$ mit $\lambda_1 * v_1, ..., \lambda_r * v_r = 0$, dann folgt

$$\lambda_0 = ... = \lambda_r = 0$$

Mit anderen Worten der Nullvektoren lässt sich nur auf triviale Weise aus der Familie $(v_1, ..., v_r)$ linear kombinieren.
$(v_1, ..., v_r)$ endliche Familie von Vektoren ist **linear abhängig**, wenn sie nicht linear unabhängig ist.

Lineare Unabhängigkeit verallgemeinert für Familien lautet dann wie folgt:
$((v_i)_{i \in I})$ Fam. von Vektoren aus V
$((v_i)_{i \in I})$ heißt linear unabhängig DEF Jede endl. Teilfamilie (also jede mögliche Kombination von Vektoren aus dieser Familie ist lin. unabhängig, d.h. für jede endliche Teilmenge $J \subset I$ ist $((v_i)_{i \in J})$ linear unabhängig

Nochmal zur Verdeutlichung hier ausführlich:
$((v_i)_{i \in I})$ heißt **linear abhängig** DEF $((v_i)_{i \in I})$ ist nicht lin. unabhängig

$\Leftrightarrow$ Es ex. eine endl. Teilfamilie $((v_i)_{i \in J})$, die lin. abh. ist

$\Leftrightarrow$ Es gibt eine endl. Teilmenge $J = \{i_1, ..., i_r\} \subset I$, $\lambda_1, ..., \lambda_r \in K$ mit
$(\lambda_1, ..., \lambda_r) \neq (0, ..., 0)$ und $\lambda_1 * v_1, ..., \lambda_r * v_r = 0$

Für Mengen analog

Man sagt häufig einfach, dass die Vektoren selbst linear unabhängig sind und lässt Begriffe wie Mengen und Familien weg

- Anmerkung: Die leere Hülle ist linear unabhängig (wurde so definiert)

Bem.8.16 V K-VR, $(v_i)_{i\in I}$ Familie von Vektoren aus V
Dann sind äquivalent:

(i) $(v_i)_{i\in I}$ ist lin. unabhängig (ii) Jeder Vektor $v \in \mathit{Lin}(v_i)_{i\in I}$ lässt sich in eindeutiger Weise aus Vektoren der Familie $(v_i)_{i\in I}$ linear kombinieren

Bem. 8.17 (a) ist $v \in V$, dann gilt: (v) linear unabhängig DEF$v \neq 0$
(b) Gehört der Nullvektor zu einer Familie, dann ist sie linear abhängig
(c) Kommt der gleiche Vektor in einer Familie mehrfach vor, so ist sie linear abhängig
(d) Ist $r \geq 2$, so gilt: Die Familie $(v_1, ..., v_r)$ von Vektoren aus V ist linear abh. DEF
Es ex. ein $i \in \{1, ..., r\}$, sodass v_i Linearkomb. von $v_1, ..., v_{i-1}, v_{i+1}, ..., v_r$ ist.
Dies ist also ein lineares Abhängigkeitskriterium für Familien von Vektoren mit mehr als einem Vektor.

In anderen Worten: Der Vektor v_i lässt sich als Linearkombination der Vektoren der Familie ohne den Vektor v_i selbst darstellen.

Basis und Dimensionen

In diesem Abschnitt sei V stets ein K-VR.

Def. 9.1: $(v_i)_{i\in I}$ Familie von Vektoren aus V
$(v_i)_{i\in I}$ heißt ein Erzeugendensystem (ES) von V DEF
$\mathit{Lin}(v_i)_{i\in I} =: V$ heißt endlich erzeugt DEF
(d.h. es ex. eine endliche Familie $(v_1, ..., v_n)$ von Vektoren aus V mit $V = \mathit{Lin}(v_1, ..., v_n)$

$(v_i)_{i\in I}$ heißt eine Basis von V DEF $(v_i)_{i\in I}$ ist ein lin. unabh. ES von V

Ist B(Basis)$= (v_1, ..., v_n)$ eine endliche Basis von V, dann heißt n die Länge von B.

Ein Erzeugendensystem ist also einfach eine Familie von Vektoren aus V, mit denen es möglich ist alle Vektoren aus dem Vektorraum zu erzeugen (d.h. als Linearkombination darzustellen.
Sind alle Vektoren in diesem Erzeugendensystem linear unabhängig, dann nennt man diese Familie eine Basis.

- Das Buch (Tutorium, LA und ANA 1) gibt gute Beispiele , z.B. für $\mathbb{R}^{\not\vdash}$ ist die Basis zum Beispiel

$$(1, 0, 0), (0, 1, 0), (0, 0, 1)$$

Diese Vektoren, die wir mit $e_1, ...e_2$ etc. bezeichnet hatte, die immer 0 bis auf die i-te Stelle waren, bilden dann immer die Standardbasis des $\mathbb{K}^n$ oder auch kanonische Basis.

Es gibt aber natürlich unendlich viele Basen, da ja auch

$$(2, 0, 0), (0, 3, 0), (0, 0, 4)$$

eine Basis ist.

Satz 9.3 $V \neq 0, B = (v_1, ..., v_n)$ ist eine endl. Familie von Vektoren aus V

Dann sind äquivalent:

(i) B ist eine Basis von V, d.h. ein lin. unabh. Erzeugersystem von V

(ii) B ist ein unverkürzbares ES von V, d.h. B ist ein ES und für jedes $r \in \{1, ..., n\}$ ist $(v_1, ..., v_{-1}, v_{r+1}, ..., v_n)$ kein ES von V mehr.

Intuitiv folgt dies einfach aus der oben genannten Erklärung

(iii) Zu jedem $v \in V$ gibt es eindeutig bestimmte $\lambda_1, ..., \lambda_n \in K$ mit

$$v = \lambda_1 v_1 + ... + \lambda_n v_n$$

(iv) Eine Erweiterung der Aussage (ii), jeder additionelle Vektor der mit der Familie vereinigt wird, macht diese linear abhängig

B ist unverlängerbar linear unabhängig, d.h. B ist linear unabh. und für jedes $v \in V$ ist die Familie $(v_1, ..., v_n, v)$ linear abhängig

Satz 9.4 (Basisauswahlsatz)

Besitzt V ein endliches ES $(v_1, ..., v_n)$, dann kann man aus diesem eine Basis auswählen, d.h. es gibt eine Teilemenge von $(v_1, ..., v_n)$, die eine Basis von V ist.

Inbesondere besitzt also jeder endlich erzeugte Vektorraum eine Basis.

Beweis: Entferne einfach aus dem ES solange Elemente, bis die resultierende Familie ein unverkürzbares ES und somit nach 9.3 eine Basis von V ist.

Folgerung 9.5 Jeder endlich erzeugte K-VR besitzt eine Basis von endlicher Länge (Länge ist die Anzahl der Vektoren der Basis)

Satz 9.6 Austauschlemma

V endl. erz K-VR, $B = (v_1, ..., v_r)$ von V, $\lambda_1, ..., \lambda_r \in K$
$w = \lambda_1 v_1 + ... + \lambda_r v_r$
Dann gilt: Ist $k \in \{1, ..., r\}$ mit $\lambda_k \neq 0$, dann ist

$$B' := (v_1, ..., v_{k-1}, w, v_{k+1}, ..., v_r)$$

ebenfalls eine Basis von V (d.h. man kann v_k gegen w austauschen).

Satz 9.7 Austauschsatz

V endl. en K-VR, $(w_1, ..., w_n)$ lin. unabh. Familie in V
Dann gilt:

(a) Ist $B = (v_1, ..., v_r)$ eine Basis von V, dann ist $r \geq n$

Hier einmal die Erklärung dafür. $(w_1, ..., w_n)$ ist einfach eine bel. unabh. Familie in dem Vektorraum. Dies hat noch nichts mit der Basis zu tun. Stellt man sich aber nun $\mathbb{R}^{\nVdash}$ vor, dann realisiert man, dass man keine lin. unabh. Familie von Vektoren finden kann, die mehr als 3 Vektoren enthält. Warum nicht? Weil jede Basis ja die Länge 3 hat! Und jede Basis ist unverlängerbar lin. unabhängig. Würde es also so eine Familie mit 4 Vektoren geben, die lin. abhängig sind, dann ist die Basis entweder kein komplettes ES, da ja ein Teil nicht dargestellt werden kann (Widerspruch) oder man müsste den 4. Vektor noch zu der Basis hinzufügen, was aber ebenfalls ein Widerspruch zur Unverlängerbarkeit ist. Dass bedeutet :

Jede linear unabhängige Familie kann nur höchstens die gleiche Länge haben wie die Basis.

(b) Es gibt Indizes $i_1, ..., i_n \in \{1, .., r\}$ derart, dass man aus der Basis $B = (v_1, ..., v_r)$ von V nach Austausch von v_{i_1} gegen w_1 etc. wieder eine Basis von V erhält.
Nummeriert man B so um, dass $i_1 = 1$ etc., bedeutet dies, dass

$$B' := (w_1, ..., w_n, v_n + 1, ..., v_r)$$

eine Basis von V ist.

Hieraus folgt dann auch das Recht, Vektoren in Basen umzuformulieren.

Folgerung 9.8 Aus dem Austauschlemma und dem Austauschsatz folgt:

(a) Ist V endlich erzeugt, dann ist jede Basis von V von endlicher Länge, und je zwei Basen von V haben dieselbe Länge.
(b) Ist V nicht endlich erzeugt, dann existiert für V keine Basis von endlicher Länge.

Definition 9.9 Dimension

$$dim_k V := \begin{cases} r, \textit{ falls V endlich erzeugt, r Länge einer und somit jeder Basis von V} \\ \infty \textit{ falls V nicht endlich erzeugt} \end{cases}$$

heißt die Dimension von V über K. Ist die Dimension von V $\in \mathbb{N}_0$ dann heißt V endlich dimensional.
Nach 9.8. ist dieser Begriff wohldefiniert, also egal wie die Basis aussieht, irgendeine Bezeichnung endlich oder unendlich dimensional passt.

Folgerung 9.11 V endlichdimensional K-VR, $U \subset V$ UVR von V

(a) U ist endlichdimensional
(b) $dim_k U \leq dim_k V$
(c) Es ist $U = V \Leftrightarrow dim_k U = dim_k V$

Basisergänzungssatz V endlichdim K-VR, $(u_1, ..., u_n)$ lin. unabh. Familie in V
Dann ex. $u_{n+1}..., u_r \in V \;\; r = dim\, V$, sodass
$B = (u_1, ..., u_n, u_{n+1}..., u_r)$ eine Basis von V ist.

Das bedeutet, mann kann jede linear unabhängige Familie in V zu einer Basis ergänzen.