Inhaltsverzeichnis

Abbildungsverzeichnis

Ende des SS 2015

0 Der Vektorraum $\mathbb{R}^n$

$n \in \mathbb{N} \quad \mathbb{R}^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_1 \in \mathbb{R} \right\}$

Spaltenvektoren der Länge n : $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = (a_1, \ldots, a_n)^t$

$a_1, \ldots, a_n$ *Komponente* der Spaltenvektoren.

Wie bei Matrizen:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}$$

(Multiplikation entspricht der Matrizenmultiplikation und ist nicht möglich falls $n > 1$)

Multiplikation eines Spaltenvektors mit einer Zahl (*Skalar*)

$$a \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} aa_1 \\ \vdots \\ aa_n \end{pmatrix}$$

Addition+Abbildung : $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$

$\mathbb{R}^n$ mit Addition und Multiplikation mit Skalaren : $\mathbb{R}$-*Vektorraum*

Die Vektoren im $\mathbb{R}^1 (= \mathbb{R})$, $\mathbb{R}^2$ und $\mathbb{R}^3$ entsprechen Punkten auf der Zahlengerade, Ebene, dreidimensionalen Raums. Punkte des $\mathbb{R}^2, \mathbb{R}^3$ lassen sich identifizieren mit, *Ortsvektoren* Pfeile mit Beginn in 0 (Komp = 0) und Ende im entsprechenden Punkt

Addition von Spaltenvektoren entspricht der Addition von Ortsvektoren entsprechend der Parallelogrammregel. Multiplikation mit Skalaren a :

Streckung (falls $|a| > 1$)

Stauchung (falls $0 \geq |a| \geq 1$)

Richtungspunkt, falls $a < 0$

Abbildung 1: Ein Vektor dargestellt durch seinen Ortsvektor

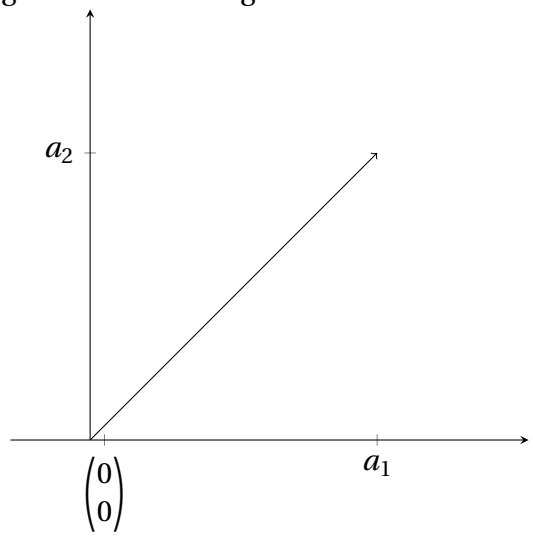
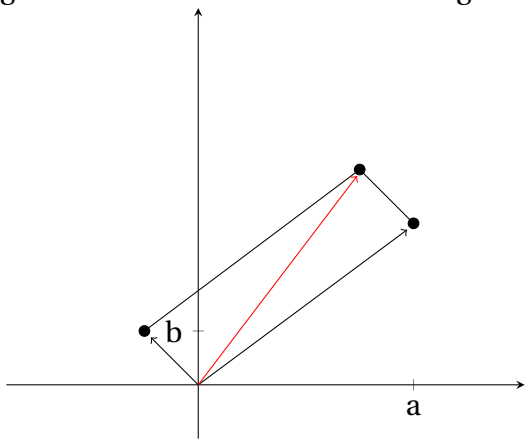


Abbildung 2: Vektoraddition durch Parallelogrammbildung



0.1 Satz (Rechenregeln in $\mathbb{R}^n$)

Seien $u, v, w \in \mathbb{R}^n, a, b \in \mathbb{R}$ Dann gilt:

a)

(1.1) $u+(v+w)=(u+v)+w$

(1.2) $v+0=0+v=v$, wobei 0 *Nullvektor*

(1.3) $v+-v=0$

(1.4) $u+v=v+u$

(2.1) $(a+b)v=av+bv$

(2.2) $a(u+v)=au+av$

(2.3) $(a\cdot b)v=a(bv)$

(2.4) $1v=v$

$\mathbb{R}^n$ kommutative Gruppe

b) $0\cdot v=0$ und $a\cdot 0=0$
Beweis folgt aus entsprechenden Rechenregeln in 0

0.2 Definition

Eine nicht-leere Teilmenge $\mathcal{U}\supset\mathbb{R}^n$ heißt *Unterraum* (oder *Teilraum* von $\mathbb{R}^n$), falls gilt:

(1) $\forall u_1, u_2\in\mathcal{U}: u_1+u_2\in\mathcal{U}$ (Abgeschlossenheit bezüglich +)

(2) $\forall u\in\mathcal{U}\,\forall a\in\mathbb{R}: au\in\mathcal{U}$ (Abgeschlossenheit bezüglich Mult. mit Skalaren)

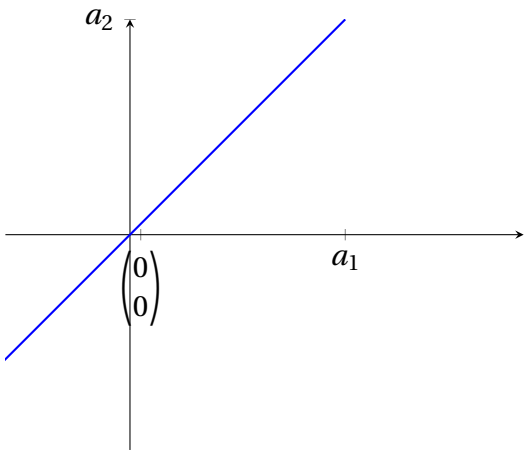
$\mathcal{U}$ enthält Nullvektor {0} Unterraum von $\mathbb{R}^n$ (Nullraum)
$\mathbb{R}^n$ ist Unterraum von $\mathbb{R}$

0.3 Beispiele

a) $0\neq v\in\mathbb{R}^2$ $G=\{av: a\in\mathbb{R}\}$ ist Unterraum von $\mathbb{R}^n$ $(a_1v, a_2v \in G, (a_1+a_2)v\in G$ 2.1 in 0.2 $av\in G, b\in\mathbb{R}(ba)v\in G)$

G = Ursprungsgerade durch $\begin{pmatrix}0\\0\end{pmatrix}$ und v = $\begin{pmatrix}a_1\\a_2\end{pmatrix}$ $n=2$:

Abbildung 3: Gerade dargestellt durch Vektoren



b) $v, w \in \mathbb{R}^n$
$E = \{av + bw : a, b \in \mathbb{R}\}$ ist Unterraum von $\mathbb{R}^n$
$v = o, w = o : E = \{o\}$
$v \neq o \quad w \notin \{av : a \in \mathbb{R}\}$
$E = \mathbb{R}^2$ $n = 3$: Ebene durch $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ und durch v, w
Ist $w \in \{av : a \in \mathbb{R}\}$, so ist $E = G$ (aus a))

c) $v, w \neq o$
$G' = \{w + av : a \in \mathbb{R}\}$
$[v \in G' \Leftrightarrow \exists a \in \mathbb{R} : w + av \in o \Leftrightarrow \exists a \in \mathbb{R} : w = (-a)v \in G]$

0.4 Satz

Seien $\mathcal{U}_1, \mathcal{U}_2$ Unterräume von $\mathbb{R}^n$

a) $\mathcal{U}_1 \cap \mathcal{U}_2$ ist Unterraum von $\mathbb{R}^n$

b) $\mathcal{U}_1 \cup \mathcal{U}_2$ ist im Allgemeinen KEIN Unterraum von $\mathbb{R}^n$

c) $\mathcal{U}_1 + \mathcal{U}_2 := \{u_1 + u_2 : u_1 : \mathcal{U}_1, u_2 : \mathcal{U}_2\}$ (Summe von $\mathcal{U}_1$ und $\mathcal{U}_2$) ist Unterraum von $\mathbb{R}^n$.

d) $\mathcal{U}_1 \subseteq \mathcal{U}_1 + \mathcal{U}_2 \quad \mathcal{U}_2 \subseteq \mathcal{U}_1 + \mathcal{U}_2$ und $\mathcal{U}_1 + \mathcal{U}_2$ ist der kleinste Unterraum von $\mathbb{R}^n$, der $\mathcal{U}_1$ und $\mathcal{U}_2$ enthält. (d.h ist w Unterraum von $\mathbb{R}^n$ mit $\mathcal{U}_1, \mathcal{U}_2 \in w$, so $\mathcal{U}_1 + \mathcal{U}_2 \subseteq W$)

Beweis. a) ✓
b) c) □

0.5 Beispiel

a) **??**b) $G_1 = \{av : a \in \mathbb{R}\}$
$G_2 = \{aw : a\}$
$G_1 + G_2 = E$

b) $\mathbb{R}^3$

$$E_1 = \left\{ r \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + s \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} : r, s \in \mathbb{R} \right\}$$

$$= \left\{ \begin{pmatrix} r \\ 0 \\ s \end{pmatrix} : r, s \in \mathbb{R} \right\}$$

$$E_2 = \left\{ t \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + u \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

$$= \left\{ \begin{pmatrix} u \\ t+u \\ u \end{pmatrix} \right\}$$

$E_1 + E_2$ Unterräume von $\mathbb{R}^3$ (10.3.b)
$E_1 \cap E_2 = ?$

$$v \in E_1 \cap E_2 \Leftrightarrow v = \begin{pmatrix} r \\ 0 \\ s \end{pmatrix} = \begin{pmatrix} u \\ t+u \\ u \end{pmatrix} \Leftrightarrow r = u, t+u = 0, s = u$$

$$E_1 \cap E_2 = \left\{ \begin{pmatrix} u \\ 0 \\ u \end{pmatrix} : u \in \mathbb{R} \right\}$$

$$= \left\{ u \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} : u \in \mathbb{R} \right\}$$

$E_1 + E_2 = ?$

$E_1 + E_2 = \mathbb{R}^3$, denn :

Es gilt sogar:

$\mathbb{R}^3 = E_1 + G_2$, wobei

$$G_2 = \left\{ t \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} : t \in \mathbb{R} \right\} \subseteq E_@$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = x \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} z \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + y \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ 0 \\ z \end{pmatrix} + \begin{pmatrix} 0 \\ y \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = (x-y) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + (z-y) \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + y \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} x-y \\ 0 \\ z-y \end{pmatrix} + \begin{pmatrix} y \\ y \\ y \end{pmatrix}$$

0.6 Definition

a) $v_1, \ldots, v_m \in \mathbb{R}^n, a_1, \ldots a_m \in \mathbb{R}$

Dann heißt $a_1 v_1 + \ldots + a_m v_m = \sum_{i=1}^{m} a_i v_i$

Linearkombination von $v_1, \ldots, v_m$ (mit Koeffizienten $a_1, \ldots, a_m$).

[Zwei formal verschiedene Linearkombinationen der gleichen $v_1, \ldots, v_m$ können den gleichen Vektor darstellen

$$1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} + 3 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} + 2 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \end{pmatrix}]$$

b) Ist $M \subseteq R^n$, so ist der von M *erzeugte* (oder *aufgespannte*) Unterraum $\langle M \rangle_{\mathbb{R}}$ (oder $\langle M \rangle$) die Menge aller (endlichen) Linearkombinationen, die man mit Vektoren aus M bilden kann.

$$\langle M \rangle_{\mathbb{R}} = \left\{ \sum_{i=1}^{n} a_i v_i : n \in \mathbb{N}, a_i \in \mathbb{R}, v_i \in M \right\} \text{ falls } M \neq \varnothing$$

$\langle \varnothing \rangle_{\mathbb{R}} := \{\varnothing\}$
$M = \{v_1, \dots v_m\}$, so

0.7 Beispiel

a) $e_i = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \in \mathbb{R}^n$

$\langle e_1, \dots e_n \rangle = \mathbb{R}^n$

$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 e_1 + x_2 e_2 + \dots + x_n e_n$

b) $\mathcal{U} = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \right\rangle_{\mathbb{R}}$

Ist $\mathcal{U} = \mathbb{R}^3$?

Für welche $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$ gibt es geeignete Skalare $a, b, c \in \mathbb{R}$ mit $a \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + b \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} +$

$c \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}$?

$$\begin{array}{rrrl} a & +3b & +2c & = x \\ 2a & +2b & +3c & = y \\ 3a & +b & +4c & = z \end{array}$$

LGS für die Unbekannten a, b, c mit variabler rechter Seite : Gauß

$$\begin{pmatrix} 1 & 3 & 2 & x \\ 2 & 2 & 3 & y \\ 3 & 1 & 4 & z \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & 2 & x \\ 2 & -4 & -1 & y-2x \\ 0 & -8 & -2 & z-3x \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & 3 & 2 & x \\ 0 & 1 & \frac{1}{4} & \frac{2x-y}{4} \\ 0 & 0 & 0 & x-2y+z \end{pmatrix}$$

LGS ist lösbar $\Leftrightarrow x-2y+z=0$.

Dass heißt $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathcal{U} \Leftrightarrow x-2y=z=0$

$$\mathcal{U} = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : x-2y+z=0, x,y,z \in \mathbb{R} \right\}$$

$$= \left\{ \begin{pmatrix} x \\ y \\ -x+2y \end{pmatrix} : x,y \in \mathbb{R} \right\}$$

$$\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \in \mathcal{U}$$

Lösungen des LGS: c frei wählen, b, a ergeben sich, (falls $x-2y+z=0$) z.B $c=0, b=\frac{1}{2}x-\frac{1}{4}y, a=x-3b=-\frac{1}{2}x+\frac{3}{4}y$

Ist $x-2y+z=0$, so ist

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \left(-\tfrac{1}{2}x+\tfrac{3}{4}y\right)\begin{pmatrix} x \\ y \\ z \end{pmatrix} + \left(\tfrac{1}{2}x-\tfrac{1}{4}y\right)\begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \frac{5}{4}\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$$

$$\mathcal{U} = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \right\rangle_{\mathbb{R}}$$

$$\begin{array}{llll} 6x^2 & -3xy & +y^3 & =5 \\ 7x^3 & +3x^2y^2 & -xy & =7 \end{array}$$

0.9 Definition

$v_1, \ldots, v_n \in \mathbb{R}^n$ heißen *linear abhängig.* falls $a_1, \ldots, a_n \in \mathbb{R}$ existieren, *nicht alle = 0*, mit $a_1 v_1 + \ldots + a_n v_n = 0$.
Gibt es solche Skalare nicht, so heiSSen $v_1, \ldots, v_m$ *linear unabhängig* (d.h. aus $a_1 v_1 \ldots a_n v_n = 0 folgt a_1 = \ldots = a_n = 0$).
(Entsprechend $\{v_1 \ldots v_n\}$ linear abhängig/linear unabhängig)
Per Definition : $\varnothing$ is linear unabhängig.

0.10 Beispiel

a) σ + v $\in \mathbb{R}^n$ Dann ist v linear unabhängig:
Zu zeigen : Ist av = $\sigma \Rightarrow a = 0$
Sei $v \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ Da $v \neq \sigma$,
existiert mindestens ein i mit $b_i \neq 0$.
Angenommen $\sigma v = \begin{pmatrix} 0b_1 \\ \vdots \\ 0b_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \sigma$.
Dann $ab_i = 0$ Da $b_i \neq 0$, folgt a = 0.
σ ist linear abhängig:

$$1 \cdot \sigma = \sigma$$

b) $v_1 = \sigma . v_2 \ldots, v_m$ ist linear abhängig :
$\sigma = 1 \cdot \sigma + 0 \cdot v_2 + \ldots + 0 \cdot v_m$

c) $v, w \in \mathbb{R}^n$
$v \neq \sigma \neq w$
① v,w sind linear abhängig $\Leftrightarrow$
②$v \in \langle w \rangle_{\mathbb{R}} \Leftrightarrow$
③$w \in \langle v \rangle_{\mathbb{R}} \Leftrightarrow$
④$\langle v \rangle_{\mathbb{R}} = \langle w \rangle_{\mathbb{R}}$
①

v, w linear abhängig $\rightarrow \exists a_1, a_2 \in \mathbb{R}$, nicht beide = 0, $a_1 v + a_2 w = \sigma$. Dann beide $(a_1, a_2) \neq 0$
$a_1 v = -a_2 w \mid \cdot \frac{1}{a_1}$
$v = -\frac{-a_2}{-a_1} w \in \langle w \rangle_{\mathbb{R}}$②
②
$v \in \langle w \rangle_{\mathbb{R}}$ dass heißt $v = aw$ für ein $a \in \mathbb{R}$ Dann $a \neq 0$, da $v \neq \sigma$. $w = \frac{1}{a} \cdot v \in \langle v \rangle_{\mathbb{R}}$③
③
$w = bv$ für ein $b \in \mathbb{R} b \neq 0$,da $w \neq \sigma$.
$aw \in \langle w \rangle_{\mathbb{R}} \Rightarrow aW = (ab)v \in \langle v \rangle_{\mathbb{R}}$
$\langle w \rangle_{\mathbb{R}} \subseteq \langle v \rangle_{\mathbb{R}}$
$w = \frac{1}{b} w$ Dann analog $\langle v \rangle \mathbb{R} \subseteq \langle w \rangle_{\mathbb{R}}$
Also $\langle v \rangle \mathbb{R} = \langle w \rangle_{\mathbb{R}}$④
④
$v \in \langle v \rangle_{\mathbb{R}} = \langle w \rangle_{\mathbb{R}}$, dass heißt.
$v = a \cdot w$ für ein $a \in \mathbb{R}$
$a \cdot v + (-a) w = \sigma \Rightarrow v, w$ sind linear abhängig ①

d) $e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \in \mathbb{R}^n$

$e_1, \ldots, e_n$ sind linear unabhängig.

$$\sigma = a_1 e_1 + \ldots a_n e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_2 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow a_1 = a_2 = \ldots = a_n = 0$$

e) $\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}-3\\1\end{pmatrix},\begin{pmatrix}6\\2\end{pmatrix}$ sind linear abhängig $\mathbb{R}^2$:

Gesucht sind alle $a_i, b_i \in \mathbb{R}$ mit $a\cdot\begin{pmatrix}1\\2\end{pmatrix}+b\cdot\begin{pmatrix}-3\\1\end{pmatrix}+c\cdot\begin{pmatrix}6\\2\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$

Führt auf LGS für a,b,c:

$\begin{pmatrix}1 & -3 & 6 & 0\\ 2 & 1 & 2 & 0\end{pmatrix} \rightarrow \begin{pmatrix}1 & -3 & 6 & 0\\ 0 & 7 & -10 & 0\end{pmatrix}$

c ist frei wählbar

f) $\begin{pmatrix}1\\2\\3\end{pmatrix},\begin{pmatrix}3\\2\\1\end{pmatrix},\begin{pmatrix}2\\3\\4\end{pmatrix}$ sind linear abhängig in $\mathbb{R}^3$,

10.8b) : $\frac{5}{4}\begin{pmatrix}1\\2\\3\end{pmatrix}+\frac{1}{4}\begin{pmatrix}3\\2\\1\end{pmatrix}+(-1)\begin{pmatrix}2\\3\\4\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}$

0.11 Satz

Seien $v_1,\ldots,v_n \in \mathbb{R}^n$

a) $v_1,\ldots,v_m$ sind linear abhängig ①

$\Leftrightarrow \exists i \ldots v_i = \sum_{\substack{j=1\\ j\neq i}}^{m} b_j v_j$ ②

$\Leftrightarrow \exists i : \langle v_1,\ldots,v_m\rangle_{\mathbb{R}} = \langle v_1,\ldots v_{i-1}, v_{i+!},\ldots,v_m\rangle_{\mathbb{R}}$ ③

b) $v_1,\ldots,v_m$ sind linear unabhängig $\Leftrightarrow$ Jedes $v \in \langle v_1,\ldots,v_m\rangle_{\mathbb{R}}$ lässt sich auf *genau eine* Weise als Linearkombination von $v_1,\ldots,v_m$ schreiben.

c) Sind $v_1,\ldots,v_m$ linear unabhängig und es existiert $v \in \mathbb{R}^n mit v \neq \langle v_1,\ldots,v_m\rangle_{\mathbb{R}}$ dann sind auch $v_1,\ldots,v_m, v$ linear unabhängig

Beweis. a) ① $\Rightarrow$ ②

$v_1,\ldots v_m$ sind linear abhängig

$\Rightarrow \exists a_1,\ldots,a_m$ nicht alle = 0,

$a_a v_i + \ldots + a_m v_m = 0$

Sei $a_i \neq 0$

$$a_i v_i = \sum_{\substack{j=1 \\ j\neq i}}^{m} -a_j v_j$$

$$v_i = \sum_{\substack{j=1 \\ j\neq i}}^{m} -\frac{a_j}{a_i} v_j \ ②$$

② $\Rightarrow$ ③

Klar : $\langle v_1, \dots v_{i-1}, v_{i+1}, v_m \rangle_{\mathbb{R}} \subseteq \langle v_1, \dots, v_m \rangle_{\mathbb{R}}$

Zeige $\supseteq$ $v = \langle v_1, \dots, v_m \rangle_{\mathbb{R}}$, d.h

$$v = \sum_{j=1}^{m} a_j v_j = \sum_{\substack{j=1 \\ j\neq i}}^{m} a_j v_j + a_i \Big(\sum_{\substack{j=1 \\ j\neq i}}^{m} b_j v_j \Big) = \sum_{\substack{j=1 \\ j\neq i}}^{m} (a_j + a_i b_j) v_j \in \langle v_1, \dots v_{i-1}, v_{i+1} \dots, v_m \rangle_{\mathbb{R}} ②$$

③ $\Rightarrow$ ①

$v_i \in \langle v_1 \dots v_m \rangle_{\mathbb{R}} = \langle v_1 \dots v_{i-1}, v_{i+1}, \rangle_{\mathbb{R}}$, dass heißt es existiert

$a_1, \dots a_{i-1}, a_{i+1}, \dots a_m \in \mathbb{R}$ mit

$$v_i = \sum_{\substack{j=1 \\ j\neq i}}^{m} a_j v_j$$

$\Rightarrow \sigma = a_1 + v_1 + \dots + a_{i-1} v_{i-1} + (-1) v_i + a_{i+1} v_{i+1} + \dots a_m v_m$ $v_1 \dots v_m$ linear abhängig □

0.12 Satz

Sind $v_i, \dots, v_{n+1} \in \mathbb{R}^n$, so

sin $v_i, \dots, v_{n+1}$ linear abhängig.

(Insbesondere ist $m > n$ und $v_i, v_m \in \mathbb{R}^n$, so sind $v_1, \dots, v_m$ linear abhängig)

Beweis. Suche alle $a_1, \dots, an+1 \in \mathbb{R}$ mit $a_i v_1 + \dots a_{n+1} v_{n+1} = \begin{pmatrix} 0 \\ \dots \\ 0 \end{pmatrix}$

Führt zu LGS für $a_1, \dots, a_{n+1}$ mit Koeffizientenmatrix $(v_1, \dots, v_2, \dots, v_{n+1}) = A$

Frage : Hat $A \cdot \begin{pmatrix} a_i \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^n$ nicht triviale Lösung?

Gauß :

$$\left(A\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}\longrightarrow\right)$$ □

0.13 Definition

Sei $\mathcal{U}$ ein Unterraum von $\mathbb{R}^n$
$B \subseteq \mathcal{U}$ heißt Basis von $\mathcal{U}$ falls:

(1) $\langle B\rangle_{\mathbb{R}} = U$

(2) B ist linear unabhängig

($\mathcal{U} = \{\sigma\}, B = \varnothing$)

0.14 Beispiel

a) $e_1, \ldots, e_n$ ist Basis von $\mathbb{R}^n$ (kanonische Basis)

$$e_1 = \begin{pmatrix}0\\ \vdots\\ 1\\ 0\\ 0\end{pmatrix} \leftarrow i$$

$$\begin{pmatrix}a_i\\ \vdots\\ a_n\end{pmatrix} = \sum_{i=1}^{n} a_i e_i$$

b) $\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}3\\2\end{pmatrix}$ ist Basis von R^2:

Sei $\begin{pmatrix}x\\y\end{pmatrix} \in R^2$. Gesucht: $a, b \in \mathbb{R}$ mit $a\begin{pmatrix}1\\2\end{pmatrix} + b\begin{pmatrix}3\\2\end{pmatrix} = \begin{pmatrix}x\\y\end{pmatrix}$

LGS mit variabler rechter Seite

$$\begin{aligned} 1a \quad +3b \quad &= x \\ 2a \quad +2b \quad &= y \end{aligned}$$

Gauß:

$\begin{pmatrix} 1 & 3 & x \\ 2 & 2 & y \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & x \\ 0 & -4 & y-2x \end{pmatrix}$

Eindeutige Lösung: $b = -\frac{1}{4}y + \frac{1}{2}x \quad a = x - 3b = x + \frac{3}{4}y - \frac{3}{2}x = -\frac{1}{2}x + \frac{3}{4}y$

z.B $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = -\frac{1}{2}\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 3 \\ 2 \end{pmatrix} \mathbb{R}^2 \left\langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix} \right\rangle$

$\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ sind linear unabhängig nach 0.10c)

$\left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix} \right\}$ Basis.

c) $\mathcal{U} = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \right\rangle_{\mathbb{R}}$

$\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = \frac{5}{4}\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$

$\mathcal{U} = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \right\rangle_{\mathbb{R}}$

$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$ linear unabhängig (0.10c))

$\left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \right\}$ Basis von $\mathcal{U}$

0.15 Satz

Jeder Unterraum $\mathcal{U}$ des $\mathbb{R}^n$ besitzt eine Basis.

Beweis. Ist $\mathcal{U} = \{\sigma\}$,so $b = \emptyset$.
Sei also $\mathcal{U} \neq \{\sigma\}$.

v_1 ist linear unabhängig.
$\langle v_1 \rangle_{\mathbb{R}} \subseteq \mathcal{U}$.
Ist $\mathcal{U} = \langle v_1 \rangle_{\mathbb{R}}$, so ist $\{v_1\}$ Basis von $\mathcal{U}$
Ist $\langle v_1 \rangle_{\mathbb{R}} \subsetneq \mathcal{U}$.
Sei $v_2 \in \mathcal{U} \setminus \langle v_1 \rangle_{\mathbb{R}}$.
Nach 0.11c) ist $\{v_1, v_2\}$ linear unabhängig. Ist $\rangle v_1, v_2\rangle = \mathcal{U}$, so ist $\{v_1.v_2\}$ Basis von $\mathcal{U}$.
Ist $\langle v_1, v_2 \rangle_{\mathbb{R}} \subsetneq U$ so wähle v_3 usw.
Es existiert $m \neq n$ mit $\langle v_1, \dots v_m \rangle_{\mathbb{R}} = \mathcal{U}$ und $v_1 \dots, v_m$ sind linear unabhängig.
(Denn noch 0.12 gibt es im $\mathbb{R}^n$ keine n+1 linear unabhängige Vektoren) □

0.16 Satz

Je zwei Basen B_1, B_2 eines Unterraums $\mathcal{U}$ des $\mathbb{R}^n$ enthalten die gleiche Anzahl von Vektoren $|B_1| = |B_2|$.
Insbesondere:
Je zwei Basen des $\mathbb{R}^n$ enthalten n Vektoren

0.17 Definition

Ist $\mathcal{U}$ Unterraum von $\mathbb{R}^n$, B Basis von $\mathcal{U}$, $|B| = m$.
Dann ist m die *Dimension* von $\mathcal{U}$, $\dim(u) = m$.
$\dim(\mathbb{R}^n) = n$, $\dim(\mathcal{U}) \neq n$.

0.18 Satz (Basisergänzungssatz)

Sei $\mathcal{U}$ Unterraum der $\mathbb{R}^n$, $M \subseteq \mathcal{U}$ eine Menge m linear unabhängiger Vektoren.
Dann lässt sich M zu einer Basis von $\mathcal{U}$ ergänzen.

Beweis. Analog zu 0.15 □

0.19 Korollar

Ist $\mathcal{U}$ Unterraum des $\mathbb{R}^n$ und $\dim(\mathcal{U}) = n$, dann ist $\mathcal{U} = \mathbb{R}^n$

Beweis. Sei B Basis von $\mathcal{U}$, also $|B| = n$.
Nach 0.18 (dort mit $\mathcal{U} = \mathbb{R}^n, M = B$) lässt sich B zu Basis B' von $\mathbb{R}^n$ ergänzen.
$\dim(\mathbb{R}^n) = n \Rightarrow |B'| = n$.
Also B = B'
$\mathbb{R}^n = \langle B' \rangle_{\mathbb{R}} = \langle B \rangle_{\mathbb{R}} = \mathcal{U}$ □

0.20 Definition

Ist $\mathcal{U}$ Unterraum von $\mathbb{R}^n$, B = $(u_1 \ldots, u_m)$ eine geordnete Basis von $\mathcal{U}$. Nach 0.11b), lässt sich jeder Vektorraum $\mathcal{U} = \langle B \rangle_{\mathbb{R}}$ *eindeutig* als Linearkombination

$$\mathcal{U} = \sum_{i=1}^{m} a_i u_i \quad , a_i \in \mathbb{R}$$

schreiben.
$(a_1 \ldots, a_m)$ heißen *Koordinaten* von u bzgl. der Basis B.

0.21 Beispiele

a) B$(e_1 \ldots, e_m)$ kanonische Basis von $\mathbb{R}^n$.

Koordinaten von $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n$ bzgl. B:

$(a_1 \ldots, a_n)$ *kartesische* Koordinaten. (*Rene Descartes, 1596-1650*)

Anfang des WS 2015/16

1 Algebraische Strukturen

13.10.2015

1.1 Definition

Sei $X \neq \varnothing$. Eine *Verknüpfung* auf X ist :

$$\begin{cases} X \times X & \longrightarrow X \\ (a,b) & \longrightarrow a \star b \end{cases}$$ ('Produkt' von a und b)

$\star$ ist Platzhalter für andere Verknüpfungssymbole, die in speziellen Beispielen auftreten können.

1.2 Beispiele

a) Addition + und Multiplikation $\cdot$ sind Verknüpfungen auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ Multiplikation ist *keine* Verknüpfung auf der Menge der negativen ganzen Zahlen.

b) Division ist keine Verknüpfung auf $\mathbb{N}$. Division ist Verknüpfung auf $\mathbb{Q}\backslash\{Q\}, \mathbb{R}\backslash\{0\}, \mathbb{C}\setminus\{0\}$

c) $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ $(n \in \mathbb{N})$
$a \oplus b := (a+b) \mod n \in \mathbb{Z}_n$
$a \circledcirc b := (a \cdot b) \mod n \in \mathbb{Z}_n$
Verknüpfungen auf $\mathbb{Z}_n$
$n = 7$: $5 \circledcirc 6 = 2$
$5 \oplus 6 = 4$
$n = 2$: $\mathbb{Z}_n = \{0, 1\}$
$0 \oplus 0 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1, 1 \oplus 1 = 0$
$\circledcirc = \cdot$

d) M Menge, X = Menge aller Abbildungen $M \longrightarrow M$. Verknüpfung auf X: Hintereinanderausführung von Abbildungen: $\circ$
$(f,g) : M \longrightarrow M$, So $f \circ g : M \to M$
$(f \circ g)(m) = f(g(m)) \in M, m \in M$
Im Allgemeinen ist $g \circ f \neq f \circ g$

e) $X = \{0,1\}$
2-stellige Aussagen, Junktoren wie $\wedge, \vee$, XOR , $\Rightarrow, \Leftrightarrow$ heißen Verknüpfungen auf X. 0 entspricht f, 1 entspricht w
$0 \vee 0 = 0, 1 \vee 0 = 1, 0 \vee 1 = 1, 1 \vee 1 = 1$
$0 \wedge 0 = 0, 0 \wedge 1 = 0, 1 \wedge 0 = 0, 1 \wedge 1 = 1$ (= 'Multiplikation')
0 XOR 0 = 0, 1 XOR 0 = 1, 0 XOR 1 = 1, 1 XOR 1 = 0 (= Addition mod 2)

f) $X = M_n(\mathbb{R})$ = Menge der $n \times n$- Matrizen über $\mathbb{R}$.
Matrizenaddition ist Verknüpfung auf X
Matrizenmultiplikation ist Verknüpfung auf X.

g) M Menge, X, Menge aller endlichen Folgen von Elementen aus M ('Wörter' über M)
Verknüpfung: Hintereinanderausführung zweier Folgen (Konkatenation)
$M = \{0,1\} w_1 = 1101 w_2 = 001$
$w_1 w_2 = 110111$
$w_2 w_1 = 0011101$

1.3 Definition

Sei $X \neq 0$ eine Menge mit Verknüpfung $\star$.

a) X, genauer $(X, \star)$ ist *Halbgruppe*, falls $(a \star b) \star c = a \star (b \star c)$ für alle $a, b, c \in X$. (*Assoziativgesetz*)

b) $(X, \star)$ heißt *Monoid*, falls $(X, \star)$ Halbgruppe ist und ein $e \in X$ existiert mit $e \star a = a$ und $a \star e = a$ für alle $a \in X$. e heißt *neutrales Element* (später, e ist eindeutig bestimmt)

c) Sei $(X, \star)$ ein Monoid. Ein Element $a \in X$ heißt *invertierbar*, falls $b \in X$ existiert (abhängig von a) mit $a \star b = b \star a = e$. b heißt *inverses Element* (das *Inverse*) zu a. (später: wenn b existiert, so ist es eindeutig bestimmt)

d) Monoid $(X, \star)$ heißt *Gruppe*, falls jedes Element in X bezüglich $\star$ invertierbar ist.

e) Halbgruppe, Monoid, Gruppe $(X, \star)$ bezüglich kommutativ (oder *abelsch*) falls $a \star b = b \star a$ für alle $a, b \in X$ (Kommutativgesetz)
(Nach: Abel, 1802-1829)

14.10.2015

1.4 Bermerkung

In Halbgruppe liefert jede sinnvolle Klammerung eines Produktes mit endlich vielen Faktoren das gleiche Element.

(n = 4)

$$(a\star(b\star c))\star d \underset{\text{AG}^1}{=} ((a\star b)\star c)\star d \underset{\text{AG}^1}{=} (a\star b)\star(c\star d) \underset{\text{AG}^1}{=} a\star(b(c\star d)) \underset{\text{AG}^1}{=} a\star((b\star c)\star d)$$

Klammern werden daher meist weggelassen
$a^n = \underbrace{a\star\ldots\star a}_{n\in\mathbb{R}}$ "Potenzen eindeutig definiert"

1.5 Proposition

a) In einem Monoid $(X, \star)$ ist das neutrale Element eindeutig bestimmt

b) Ist $(X, \star)$ Monoid und ist $a \in X$ invertierbar, so ist das Inverse zu a eindeutig bestimmt. Bezeichnung: a^{-1}

c) Ist $()X, \star$ Monoid und wenn $a, b \in X$ invertierbar sind, so auch $a \star b$.
$(a \star b)^{-1} = b^{-1} \star a^{-1}$

d) Die Menge der invertierbaren Elemente in einem Monoid $(X, \star)$ bilden bezüglich $\star$ eine Gruppe.

Beweis. a) Angenommen: $e_!, e_2$ sind neutrale Elemente. Dann:

$$e_1 = e_1 \star e_2 = e_1 \star e_2 = e_2 \qquad \lightning$$

[1] Assoziativgesetz

b) Angenommen a hat 2 inverse Elemente b_1, b_2 also.

$$a \star b_1 = e, b_2 \star a = e$$
$$b_1 = e \star b_1 = (b_2 \star a) \star b_1 = b_2 \star (a \star b_1) = b_2 \star e = b_2 \qquad \lightning$$

c)
$$(a \star b) \star (b^{-1} \star a^{-1}) = a \star (b \star b^{-1}) \star a^{-1} = a \star e \star a^{-1} = e$$

Analog: $(b^{-1} \star a^{-1}) \star (a \star b) = e$
Also: $(a \star b)^{-1} = b^{-1} \star a^{-1}$
d) $\mathscr{I}$ = Menge der inversen Elemente in $(X, \star)$,
$e \in \mathscr{I}$, dann $e \star e = e$, dass heißt $e^{-1} = e, \star$ ist Verknüpfung auf $\mathscr{I}$. Zu zeigen: $a, b \in \mathscr{I} \Rightarrow a \star b \in \mathscr{I}$ Folgt aus c).
Assozativgesetz gilt in $\mathscr{I}$, $a \in \mathscr{I} \Rightarrow a^{-1} \in \mathscr{I}$, denn $(a^{-1})^{-1} = a$ □

Bemerkung: Multiplikation mit a^{-1} macht Multiplikation mit a (Verknüpfung) rückgängig.

1.6 Beispiel

a) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Halbgruppen bezüglich +
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind bezüglich + Monoide mit neutralen Element 0.
$\mathbb{N} = \{1, 2, \ldots\}$ ist kein Monoid bezüglich +, aber $\mathbb{N}_0$.
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Gruppen bezüglich +. Inverses Element zu $a : -a$
$\mathbb{N}$ ist keine Gruppe bezüglich +, Inverse Elemente in $\mathbb{N}_0 : \{0\}$,

b) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Monoide bezüglich $\cdot$ (neutrales Element 1). Keine Gruppen (in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ist 0 nicht invertierbar).
$\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ Gruppen.
Invertierbare Elemente in $\mathbb{Z} ::$ $\underset{\substack{\uparrow \\ \text{Eigenes Inverses}}}{\{1, -1\}}$ ← Gruppe bezüglich $\cdot$

c) M Menge.
X = Menge aller Abbildungen $M \longrightarrow M$ mit Hintereinanderausführung $\circ$ als

Verknüpfung.
Monoid, neutrales Element. id_M
$f \circ id_M = f = id_M \circ f$
$id_M(m) = m$ für alle $m \in M$.
Invertierbar sind genau die bijektiven Abbildungen $M \longrightarrow M$, Inverse = Umkehrabbildung.
$f : M \longrightarrow M$ bijektiv
$f \circ f^{-1} = f^{-1} \circ f = id_M$
'Proposition' on page 21 d): Die bijektive n Abbildung, $M \longrightarrow M$ bilden bezüglich $\circ$ eine Gruppe

d) M = Menge z.B $\{0,1\}$, x Menge aller endlichen Folgen über m.Halbgruppe mit Verknüpfung Konkatenation . Nimmt man die leere Folge mit hinzu, ist es das neutrale Element. Dann: Monoid.

e) $M_n(\mathbb{R})$ Menge der Matrizen über $\mathbb{R}$.
Addition: neutrales Element $0 - Matrix$, Inverse zu A ist -A. (M,Addition) ist Gruppe
Multiplikation: $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ Halbgruppe mit neutralem Element I_m

f) $n \in \mathbb{N}$ $\mathbb{Z}_n = \{0, \ldots, n-1\}$ Verknüpfung $\oplus$
$a \oplus b = a + b \mod n$
$(\mathbb{Z}_n, \oplus)$ ist Gruppe.
Assoziativgesetz: $a, b, c \in \mathbb{Z}_n$

$$
\begin{aligned}
(a \oplus b) \oplus c &= (a + b \mod n) \mod n \\
&\underset{\text{Mathe I}}{=} ((a+b)+c) \mod n \\
&= (a + (b + c)) \mod n \\
&\underset{\text{Mathe I}}{=} (a + (b + c \mod n)) \mod n \\
&= (a + (b \oplus c)) \mod n \\
&= (a \oplus (b \oplus c))
\end{aligned}
$$

0 ist neutrales Element bezüglich $\oplus$
0 ist sein eigenes Inverse.
$1 \leq i \leq n$ $n - i \in \mathbb{Z}_n$ Inverses zu i
$i \oplus (n - i)$

$= (i + (n - i)) \mod n = n \mod n = 0$

g) $n \in \mathbb{N}, \mathbb{Z}_0$ Verknüpfung $\circledcirc$ $n > 1$
$a \circledcirc b = a \cdot b \mod n$
$(\mathbb{Z}_n \circledcirc)$ *ist Monoid*
Assoziativgesetz wie bei $\oplus$.
1 ist neutrales Element bei $\circledcirc$ Keine Gruppe bezüglich $\circledcirc$, denn 0 hat kein Inverses

1.7 Satz

Sei $n \in \mathbb{N}, n > 1$

a) Die Elemente in $(\mathbb{Z}_n, \circledcirc)$, die invertierbar bezüglich $\circledcirc$ sind, sind genau diejenigen $a \in \mathbb{Z}_n$ mit $\text{ggT}(a, n) = 1$.
Für solche a bestimmt man das Inverse folgendermaßen:
Bestimme $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot n = 1$ (Erweiterter Euklidischer Algorithmus)
Dann ist $a^{-1} = s \mod n$

b) $\mathbb{Z}_n{}^* := \{a \in \mathbb{Z}_n : \text{ggT}(a, n) = 1\}$ ist Gruppe bezüglich $\circledcirc$.
$|\mathbb{Z}_n{}^*| =: \varphi(n)$ *Euler'sche φ-Funktion* (Leonard Euler 1707-1783)

c) Ist p eine Primzahl so ist $(\mathbb{Z}_p \setminus 0, \circledcirc)$ eine Gruppe. *Beweis* folgt aus b)

Beweis. a) Angenommen $a \in \mathbb{Z}_n$ invertierbar bezüglich $\circledcirc$
D.h es existiert $b \in Z_n$ mit $a \circledcirc b = 1$
$a \cdot b \mod n = 1$, d.h es existiert $k \in \mathbb{Z}$ mit $a \cdot b = 1 + k \cdot n, 1 = a \cdot b - k \cdot n$
Sei d =ggT$(a.n)$:

$d \mid a \quad \Rightarrow d \mid a \cdot b$
$d \mid n \quad \Rightarrow d \mid k \cdot n$
$\Rightarrow \quad d \mid a \cdot b \quad -k \cdot n = 1$
$\Rightarrow \quad d = 1 \quad ggT(a, n) = 1.$

Umgekehrt sei $a \in \mathbb{Z}_n$ mit $\text{ggT}(a, n) = 1$
EEA liefert $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot n = 1$.

$$
\begin{array}{lll}
 & (s \mod n) \circledcirc a & = ((s \mod n) \cdot a) \mod n \\
\underset{\text{Mathe I}}{=} & (s \cdot a) \mod n & = (1 - t \cdot n) \mod n \\
= & (1 - \underbrace{(t \cdot n) \mod n}_{=0}) \mod n & = 1 \mod n = 1
\end{array}
$$

b) 'Proposition' on page 21 d) □

1.8 Beispiel

$n = 24$, $a = 7$ ist invertierbar in $(Z_{24}, \circledcirc)$

EEA:

$$1 = (-2) \cdot 24 + 7 \cdot 7$$

$$a^{-1} = 7 \mod 24 = 7 = a$$

1.9 Beispiel

Sei $M = \{1, \ldots, n\}$

Die Menge der bijektiven Abbildungen auf M (*Permutationen*) bilden nach 1.6c) eine Gruppe bezüglich Hintereinanderausführung $\circ$.

Bezeichnung: S_n *systematische Gruppe von Grad n*

Es ist $|S_n| = n!$ (Mathe I)

$$\text{z.B} : \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \pi$$

$$\varrho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$$

$$\varrho^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\varrho \circ \varrho^{-1} = id$$

$$\pi \circ \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\varrho \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

S_n ist für $n \geq 3$ nicht abelsch (nicht kommutativ)

1.10 Satz (Gleichungslösen in Gruppen)

Sei $(G,\cdot)$ eine Gruppe $a,b \in G$ (in allgemeinen Gruppen schreibt man Verknüpfungen oft als $\cdot$ statt $\star$, oft auch ab statt $a \cdot b$)

a) Es gibt genau ein $x \in G$ mit $ax = b$ (nämlich $x = a^{-1}b$) ["Teilen durch" a von links = Multiplikation von links mit a^{-1}]

b) Es gibt genau ein $y \in G$ mit $ya = b$ (nämlich $y = ba^{-1}$)

c) Ist $ax = bx$ für ein $x \in G$, so ist $a = b$
Ist $ya = yb$ für ein $y \in G$, so ist $a = b$

Beweis. a) Setze $x = a^{-1}b \in G$.
$a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1})b = a \cdot b = b$ Eindeutigkeit : Sei $x \in G$ mit $ax = b$
Multiplikation beide Seiten mit a^{-1},
$x = (a^{-1}a)x = a^{-1}b$

b) analog
c) $ax = bx$ Multiplikation mit x^{-1} Dann a= b □

1.11 Beispiel

a) Suche Permutation $\xi \in S_3$ mit $\varrho \circ \xi = \pi$ (vgl. 1.9). 'Satz (Gleichungslösen in Gruppen)' on page 26a):

$$\xi = \varrho^{-1} \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

b) 1.10c) gilt in Monoiden, die keine Gruppen sind, im Allgemeinen nicht:
Beispiel: $(\mathbb{Z}_0, \circledcirc)$
$2 \circledcirc 3 - 0 = 3 \circledcirc 3$, aber $2 \neq 4$

1.12 Definition

a) $R \neq \varnothing$ Menge mit 2 Verknüpfungen + und $\cdot$ heißt *Ring*, falls

(1) $(R,+)$ ist kommutative Gruppe (neutrales Element: 0, *Nullelement*, Inverses zu a : $-a$ $\quad b+(-a)=:b-a$)

(2) $(R,\cdot)$ ist Halbgruppe

(3) $(a+b)\cdot c = a\cdot c = a\cdot c + b\cdot c$ und $a\cdot(b+c) = a\cdot b + a\cdot c$ $\quad$ ($\cdot$ vor $+$) *Distributivgesetz*

b) Ring R heißt *kommutativer Ring* falls $(R,\cdot)$ kommutative Halbgruppe ist.

c) Ring R heißt *Ring mit Eins*, falls $(R,\cdot)$ Monoid, neutrales Element $1 \neq 0$ (*Einselement, Eins*)

1.13 Beispiele

a) $(\mathbb{Z},+,\cdot)$ ist kommutativer Ring mit 1, invertierbare Elemente bezüglich $\cdot$ sind 1 und -1.

b) $(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$ sind kommutative Ringe mit Eins.
Alle Elemente $\neq 0$ sind invertierbar bezüglich $\cdot$

c) $n \in \mathbb{N}, n > 1$.
$\mathbb{Z}_n = \{0,\ldots,n-1\}$
$(\mathbb{Z}_N, \oplus, \circledcirc)$ ist kommutativer Ring mit Eins:
Wegen 'Beispiel' on page 22 f),g) sind nur die Distributivgesetz zu zeigen:

$$
\begin{aligned}
& (a \oplus b) \circledcirc c = ((a \oplus b)\cdot c) \mod n \\
= \quad & ((a+b) \mod n)\cdot c) \mod n \\
\underset{\text{Mathe I}}{=} \quad & ((a+b)\cdot) \mod n \\
= \quad & (a\cdot c + b\cdot c) \mod n \\
\underset{\text{Mathe I}}{=} \quad & ((a\cdot c) \mod n + (b\cdot c) \mod n) \mod n \\
= \quad & a \circledcirc c \oplus b \circledcirc c
\end{aligned}
$$

d) $M_n(\mathbb{R})$, $n\times n$-Matrizen über $\mathbb{R}$, mit Matrizenaddition + und, Multiplikation $\cdot$ ist Ring mit Eins.
(Folgt aus Rechenregeln für Matrizen, Mathe II) Eins : E_n $\quad n\times n$-Einheitsmatrix
Für $n \geq 2$ ist $M_n(\mathbb{R})$ kein kommutativer Ring

1.14 Proposition

Sei $(R,+,\cdot)$ ein Ring. Dann gilt für alle $a,b \in R$.

a) $0 \cdot a = a \cdot 0 = 0$

b) $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$

c) $(-a)\cdot(-b) = a\cdot b$

Beweis.

a) $0\cdot a = (0+0)\cdot a \underset{\text{DG}^2}{=} 0\cdot a + 0\cdot a$
Addiere auf beiden Seiten $-(0\cdot a)$
$0 = 0\cdot a + 0 = 0\cdot a$

b) $(-a)\cdot b + ab = ((-a)+a)\cdot b = 0\cdot b \underset{\text{a)}}{=} 0$
$\Rightarrow (-a)\cdot b = -(ab)$ Analog $a\cdot(-b) = -(ab)$

c) $(-a)\cdot(-b) \underset{\text{b)}}{=} -(a\cdot(-b)) \underset{\text{b)}}{=} -(-(a\cdot b)) = a\cdot b$

□

1.15 Bemerkung

a) In einem Ring mit Eins sind 1 und -1 bezüglich $\cdot$ invertierbar.
$1\cdot 1 = 1 \quad (1^{-1} = 1)$
$(-1)\cdot(-1) = 1$ (1.14c)), dass heißt. $(-1)^{-1} = -1$
0 Ist nie bezüglich Multiplikation invertierbar, denn $0\cdot a = 0 \neq 1$. 1.14a)

b) Es kann sein dass $1 = -1$ gilt. Zum Beispiel:
$(\mathbb{Z}_2, \oplus, \circledcirc)$ $1 \oplus 1 = 0$ $1 = -1$

1.16 Definition

Ein kommutativer Ring $(R,+,\cdot)$ mit Eins heißt *Körper*, wenn jedes Element $\neq 0$ bezüglich Multiplikation invertierbar ist.

[2] Distributivgesetz

1.17 Beispiel

a) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper, $\mathbb{Z}$ nicht.

b) $(\mathbb{Z}_n, \oplus, \circledcirc)$ ist genau dann ein Körper, wenn n eine Primzahl.
$\mathbb{Z}_n$ ist kommutativer Ring mit 1.
'Beispiele' on page 27c: Die invertierbaren Elemente in $\mathbb{Z}_n$ sind alle $a \in \mathbb{Z}_n$ mit $\text{ggT}(a, n) = a$

1.18 Proposition (Nullteilerfreiheit in Körpern)

Ist K ein Körper, $a, b \in K$, mit $a \cdot b = 0$, so ist $a = 0$ oder $b = 0$

Beweis.
Sei $a \cdot b = 0$ Angenommen $a \neq 0$. Dann existiert $a^{-1} \in K$
$0 \underset{\text{1.14a)}}{=} a^{-1} \cdot 0 \underset{\text{Vor.}}{=} a^{-1}(a \cdot b) = (a^{-1} \cdot a) \cdot b = b$ □

Beispiel: $R = (\mathbb{Z}_6, \oplus, \circledcirc)$
$2 \circledcirc 3 = 0 \qquad 2 \neq 0, 3 \neq 0$

1.19 Definition

Sei K ein Körper,

a) Ein (Formales) *Polynom* über K ist ein Ausdruck $f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i$ wobei $n \in \mathbb{N}_0, a_i \in K$. (Manchmal $f(x)$ statt f, +-Zeichen hat zunächst nichts mit einer Addition zu tun. a_i *Koeffizienten* von f
Ist $a_i = 0$ so kann man in der Schreibweise von f $0 \cdot x^i$ auch weglassen.
Statt $a_0 x^0$ schreibt man a_o, statt $a_1 x^1$ schreibt man $a_1 x$. Sind alle $a_i = 0$, so $f = 0$, *Nullpolynom* .
Ist $a_i = 1$, so schreibt man x^i statt $1x^i$

b) Zwei Polynome f und g sind *gleich*, wenn *entweder* $f = 0$ und $g = 0$ *oder* $f \neq 0$ und $g \neq 0$
d.h $f = \sum_{i=0}^{n} a_i x^i, a_n \neq 0$

$g = \sum_{i=0}^{m} a_i x^i, b_m \neq 0$
und $n = m$ und $a_i = b_i$ für $i = 0...n$

c) Menge aller Polynome über K. $K[x]$
Wir wollen $K[x]$ zu einem Ring machen. Wie?
Beispiel: $f = 3x^2 + 2x + 1$,
$g = 5x^3 + x^2 + x \in Q[x]$
$f + g = 5x^3 + 4x^2 + 3x + 1$
$f \cdot g = (3^x + 2x + 1) \cdot (5x^3 + x^2 + x)$
$= 15x^5 + 10x^4 + 5x^3 + 3x^4 + 2x^3 + x^2 + 3x^2 + 2x^2 + x$
$= 15x^5 + 13x^4 + 10x^3 + 3x^2 + x$

27.10.2015

1.20 Satz und Definition

K Körper. $K[x]$ wird zu einem kommutativen Ring mit Eins durch folgenden Verknüpfungen.
$f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{m} b_i x_i$ so
$f + g \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$
$f \cdot g = \sum_{i=0}^{n+m} c_i x^i$, wobei $c_i = \sum_{j=0}^{i} a_j b_{i-j}$ (Faltungsprodukt)
In beiden Fällen sind Koeffizienten a_i mit $i > n$ bzw. b_i mit $i > m$ gleich 0 zu setzen. Das Einselement ist 1 $(= 1x^0)$
Das Nullelement ist das Nullpolynom.
$-f = \sum_{i=0}^{n} (-a_i) x^i$
$(K[x], +, \cdot)$ heißt *Polynomring* in einer Variable *Beweis:* Nachrechnen

1.21 Bemerkung

a) $f = \sum_{i=0}^{n} a^i x^i \in K[x]$, $a \in K \subseteq K[x]$
$a \cdot f = \sum_{i=0}^{n} (a \cdot a_i) x^i$

$$x \cdot f = \sum_{i=0}^{n} a_i x^{i+1} = a_n x^{n+1} + \ldots + a_0 x$$

b) Das $+-$ Zeichen in der Definition der Polynome entspricht genau der Addition der *Monome* $a_i x^i$.
$(a_0 x^0 \underset{\substack{\uparrow \\ \text{Add. aus 1.20}}}{+} a_1 x^1) = a_0 x^0 \underset{\substack{\uparrow \\ \text{+ aus 1.19}}}{+} a_1 x^1$

1.22 Definition

Sei $0 \neq f \in k[x], f = \sum_{i=0}^{n} a_i x^i, a_n \neq 0$.
Dann heißt n der *Grad* in f, $\text{Grad}(f) = n$
$\text{Grad}(0) := -\infty$
$\text{Grad}(f) := 0$:*Konstante Polynome* $=\neq 0$

1.23 Satz

Sei K ein Körper, $f, g \in K[x]$.
Dann ist $\text{Grad}(f \cdot g) = \text{Grad}(f) + \text{Grad}(g)$
(Konvention: $-\infty + n = n + (-\infty) = (-\infty + \infty)$,
Sei $f \neq 0$ und $g \neq 0$
$f = \sum_{i=0}^{n} a_i x^i, a_n \neq 0, n = \text{Grad}(f)$
$g = \sum_{i=0}^{m} b_i x^i, b_m \neq 0, m = \text{Grad}(g)$
Koeffizienten von x^{n+m} in $f \cdot g$: $a_n b_m \underset{1.18}{\neq} 0$

1.24 Korollar

Sei K ein Körper

a) Genau die konstanten Polynome $\neq 0$ sind in $K[x]$ bezüglich $\cdot$ invertierbar
Insbesondere ist $K[x]$ *kein* Körper

b) Sind $f, g \in K[x]$ mit $f \cdot g = 0$, so ist $f = 0$ oder $g = 0$ (Nullteilerfreiheit in $K[x]$)

c) Sind $f, g_1, g_2 \in K[x]$ mit $f \cdot g_1$ und ist $f \neq 0$, so ist $g_1 = g_2$

Beweis.

a) Sei $f \in K[x]$ invertierbar bezüglich $\cdot$. Dann ist $f \neq 0$ und es existiert $g \in K[x]$ mit $f \cdot g = 1$.
Mit 1.23:
$0 = \text{Grad}(1) = \text{Grad}(f \cdot g)$
$= \text{Grad}(f) + \text{Grad}(1)$.
Also: $\text{Grad}(f) = 0 (= \text{Grad}(g))$
Dass heißt f ist konstantes Polynom.
Ist umgekehrt $f = a \in L, a \neq 0$, so $f^{-1} = a^{-1} \in K$

b) Folgt aus 1.23:

$$-\infty = \text{Grad}(0) = \text{Grad}(f \cdot g)$$
$$= \text{Grad}(f) + \text{Grad}(g)$$

$\Rightarrow$ $\text{Grad}(f) = -\infty$ oder $\text{Grad}(g) = -\infty$, d.h $f = 0$, oder $g = 0$

c) $fg_1 = fg_2$
$\Rightarrow 0 = fg_1 - fg_2 \qquad = f \cdot (g_1 - g_2)$
Da $f \neq 0$, folgt mit b)
$g_1 - g_2 = 0$, d.h $g_1 = g_2$

□

1.25 Bemerkung

a) Jedem Polynom $f = \sum_{i=0}^{n} a_i x^i \in K[x]$
kann man eine Funktion $K \to K$ zuordnen. $a \in K \longmapsto f(a) = \sum_{i=0}^{n} a_i a^i \in K$
(Polynomfunktion aus Analysis $K = \mathbb{R}$)
Aufgrund der Definition von Addition/Multiplikation von Polynomen gilt:
$(f + g)(a) = f(a) + g(a)$
$(f \cdot g)(a) = f(a) \cdot g(a)$
Es kann passieren, dass zwei verschiedene Polynome die gleiche Funktion beschreiben.

Z.B $K = \mathbb{Z}_2 = \{0,1\}$
$f = x^2, g = x$
$f \neq g$
$f(1) = 1 = g(1)$
$f(0) = -g(0)$
Über unendlichen Körpern passiert das nicht (später)

b) Schnelle Berechnung von $f(a)$:
$f = a_0 + a_1 x + \ldots + a_n x^n$
$f(a) = a_0 + a(a(a_1 + a(a_2 + \ldots + a(a_{n-1} + aa_n)))$

Horner-Schema

1.26 Definition

K Körper, $f, g \in K[x]$
f *teilt* g $(f \mid g)$ falls $q \in K[x]$ existiert mit $g = q \cdot f$ (Falls $g \neq 0 \mod f \mid g$, so ist $\text{Grad}(f) \leq \text{Grad}(g)$ nach 'Satz' on page 31)

1.27 Satz

K Körper, $0 \neq f \in K[x], g \in K[x]$
Dann existiert eindeutig bestimmte Polynome q, r

(1) $$g = q \cdot f + r$$

(2) $$\text{Grad}(r) < \text{Grad}(f)$$

(Beweis WHK, Satz 4.69) *Division mit Rest*

1.28 Beispiel

28.10.2015

a) $g = x^4 + 2x^3 - x + 2, f = 3x^2 - 1, f, g \in Q[x]$

$$\left(x^4 + 2x^3 - x + 2\right) : \left(3x^2 - 1\right) = \tfrac{1}{3}x^2 + \tfrac{2}{3}x + \tfrac{1}{9} + \frac{-\frac{1}{3}x + \frac{19}{9}}{3x^2 - 1}$$

$$\begin{array}{r}
-x^4 \quad + \frac{1}{3}x^2 \\
\hline
2x^3 + \frac{1}{3}x^2 - x \\
-2x^3 \quad + \frac{2}{3}x \\
\hline
\frac{1}{3}x^2 - \frac{1}{3}x + 2 \\
-\frac{1}{3}x^2 \quad + \frac{1}{9} \\
\hline
-\frac{1}{3}x + \frac{19}{9}
\end{array}$$

b) $g = x^4 - x^2 + 1 \quad f = x^2 + x \quad f, g \in \mathbb{Z}_3[x]$

$$\begin{array}{l}
x^4 + 3x^3 + 1 : x^2 + x = x^2 + 2x \\
-\underline{\left(x^4 + x^3\right)} \\
\qquad 2x^3 + 2x^2 + 1 \\
\qquad -\underline{\left(2x^3 + 2x^2\right)} \\
\qquad\quad 1 \leftarrow r
\end{array}$$

1.29 Korollar

K Körper, $a \in K$.
$f \in K[x]$ ist genau dann durch $(x-a)$ teilbar, wenn $f(a) = 0$ (d.h a ist Nullstelle von f)
$[f = g \cdot (x-a), q \in K[x]]$

Beweis.
Falls $x - a \mid f$, so existiert $q \in K[x]$ mit $f \underset{1.25}{=} q(x-a)$.
Dann $f(a) = q(a) \cdot \underbrace{(a-a)}_{=0} = 0$.
Umgekehrt: Angenommen $f(a) = 0$. Division mit Rest von f durch $x - a$:
$f = q \cdot (x-a) r, q, r \in K[x]$
$\text{Grad}(r) < \text{Grad}(x-a) = 1, r \in K$
Zeige: $r = 0$.
$r = f - q \cdot (x-a)$

Setze $a \in K$ ein.
$r \underset{1.25}{=} f(a) - q(a) \cdot (a-a) = 0 - 0 = 0$
$f = q \cdot (x-a)$ □

1.30 Definition

K Körper $a \in K$ heißt*m-fache Nullstelle* von $f \in K[x]$, falls $(x-a)^m \mid f$ und $(x-a)^{m+1} \nmid f$.
Dass heißt $f = q \cdot (x-a)^m$ und $q(a) \neq 0$

1.31 Beispiel

$x^5 + x^4 + 1 \in \mathbb{Z}_3[x]$
In Z_3 hat f die Nullstelle 1
'Korollar' on page 34: $x - 1 (= x + 2)$ teilt f
Dividiere f durch $x - 1$:
$f = (x^4 + 2x^3 + 2x + 2) \cdot (x-1)$

1.32 Satz

K Körper, $f \in K[x]$, Grad$(f) = n \geq 0$ (dass heißt $f \neq 0$).
Dann hat f höchstens n Nullstellen in K (einschließend Vielfachheit). Genauer:
Sind $a_1, \ldots, a_k$ die verschiedenen Nullstellen von f, so ist
$f = g \cdot (x-a_1)^{m_1} \cdot \ldots \cdot (x-a_k)^{m_k}$, m_i Vielfachheiten der Nullstellen a_i, g hat keine Nullstelle in K6

Beweis. Durch Induktion nach n.
$n = 0$: $f = a_0 \neq 0$, ohne Nullstelle.✓.
Sei $n > 0$. Behauptung sei richtig für alle Polynome von Grad $< n$.
Hat f keine Nullstellen, $g = f$✓
Hat f Nullstellen $a_1 \ldots, a_k, k \geq 1$
so $f = q \cdot (x-a_1)^{m-1}$ (nach Definition) $q(a_1) \neq 0$.
Grad$(q) \underset{1.23}{=} n - m_1 \underset{m_1 > 0}{<} n$
Wir zeigen:

q hat genau die Nullstellen $a_2,\dots,a_k$ mit Vielfachheiten $m_2,\dots,m_k$.
Klar: Jede Nullstelle von q ist Nullstelle von f, Dass heißt q hat höchstens Nullstellen $a_2,\dots,a_k$.
Diese Nullstellen hat q mit Vielfachheit $0 \geq n_i \geq m_i$, denn $(x-a_i)^{m_i} | q \Rightarrow (x-a_i)^{n_i} \mid f$
Sei $i \in \{2,\dots,k\}$. Es ist $f = s\cdot(x-a_i)^{m_i}, s \in K[x], s(a_i) \neq 0$
$q = q_1\cdot(x-a_i)^{n_i}, q_1 \in K[x], q(a_i) \neq 0, \qquad ((x-a_i)^0 = 1)$
$f = q_1(x-a_1)^{n_i}\cdot(x-a_1)^{m_1}$ 'Korollar' on page 31c):
$s(x-a_i)^{m_i-n_i} = q_1\cdot(x-a_1)^{m_1}$
Ist $m_i > n_i$, so ist $m_i - n_i > 0$
$0 = s(a_i)(a_i-a_i)^{m_i-n_i} = q(a_i)(a_i-a_i) \neq 0E$
Dass heißt $.n_i = m_i.i, 2\dots,k$
$q = g(x-a_2)^{m_2}\dots(x-a_k)^{m_k}$, g ohne Nullstelle in K
$f = g(x-a_1)^{m_2}\cdots(x-a_2)^{m_1}$ (Nach Induktionsvorsaussetzung) □

1.33 Korollar

K Körper, $f,g \in K[x], m = \max(\text{Grad}(f), \text{Grad}(g)$
Gibt es $m+1$ Elemente $a_1,\dots,a_{m+1} \in K$, paarweise verschieden, mit $f(a_i) = g(a_i), i = 1,\dots,m+1$ so $f = g$.
Insbesondere: Ist K unendlich ,$f,g \in K[x]$ mit $f(a) = g(a)$ für alle $a \in K$, so ist $f = g$

Beweis. $f-g \in K[x], \text{Grad}(f-g) \leq m$.
$f-g$hat $m+1$ Nullstellen $a_1,\dots a_{m+1}$
1.32 $f-g = 0, f = g$ □

1.34 Bemerkung

Über $\mathbb{Q},\mathbb{R},\mathbb{Z}_p$($p$ Primzahl) gibt es Polynome beliebig hohen Grades ohne Nullstellen
Über $\mathbb{Q},\mathbb{R}$: $(x^2+1)^m$ hat Grad$(2m)$, keine Nullstellen in $\mathbb{Q},\mathbb{R}$
über $\mathbb{Z}_p$ z.B $(x^p-x+1)^m$ hat Grad pm, ohne Nullstellen (ohne Beweis)

1.35 Fundamentalsatz der Algebra

Ist $f \in \mathbb{C}[x], f \neq 0$ so ist $(f = a_n x^n + \ldots + a_0)$
$f = a_n(x-c_1)^{m_1} \ldots (x-c_k)^{m_k}, a_n.c_i, \ldots, c_k \in \mathbb{C}$ (Nullstellen mit Vielfachen m_1, m_2)
$m_1 + \ldots + m_k = \text{Grad}(f)$
$\text{Grad}(f) = n$ f hat n Nullstellen (einschließend Vielfachheit)

Index