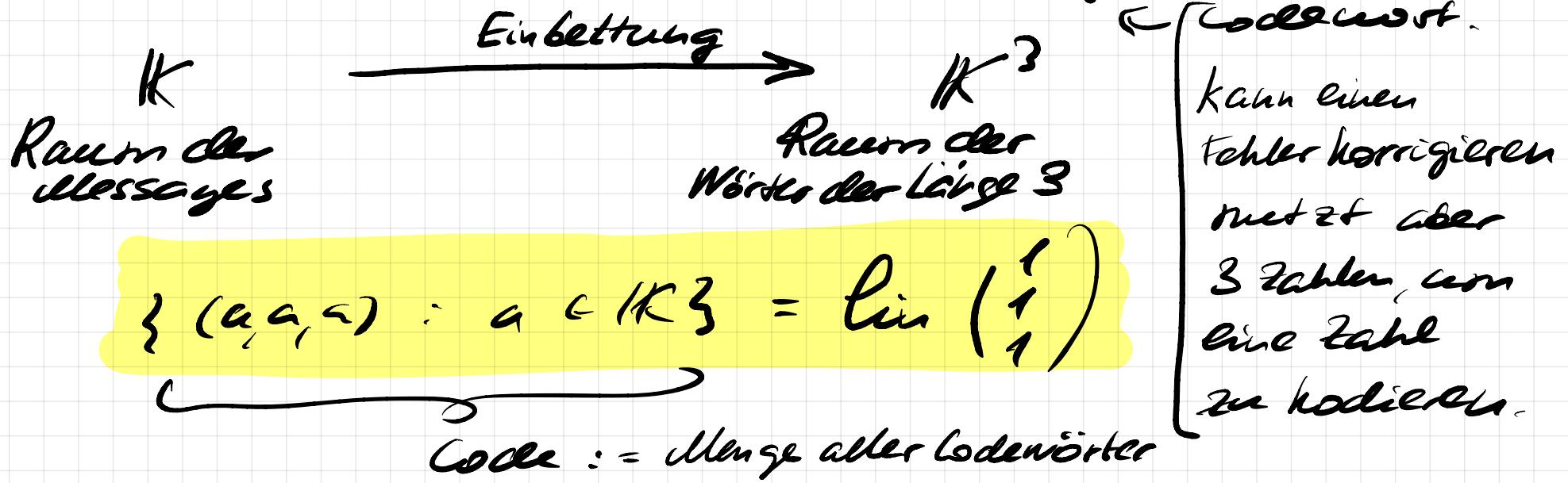


Bsp. Teaser zur Kodierungstheorie

Alice und Bob kommunizieren durch ein verschüttetes Kanal. Eine Möglichkeit.

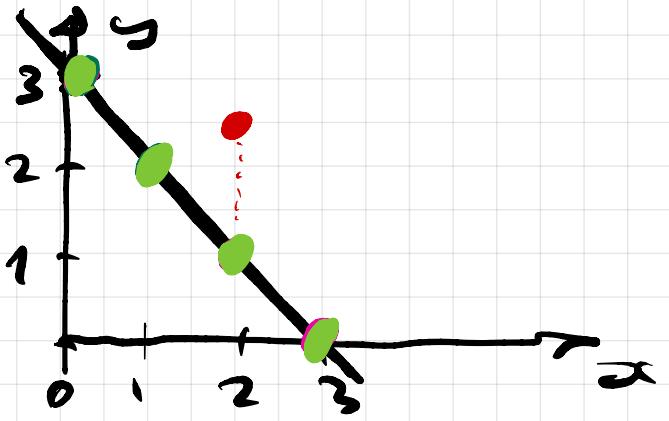
Message $a \in K \mapsto$ Codeword $(a, a, a) \in K^3$



Können wir besser kodieren? Wir probieren es...

Situation: Alice schickt Zahlen $a, b \in K$ an Bob.
Wir können uns vorstellen, dass Alice eine Gerade mit der Gleichung $y = a \cdot x + b$ an Bob schickt.

Nehmen wir als Beispiel die Message (a, b) mit $a = -1$
 $b = 3$



Alice schickt die Werte von $a x + b$ an den Stellen $x = 0, 1, 2, 3$ an Bob als das Codewort.

Das Codewort ist

$$\begin{pmatrix} b \\ ax+b \\ 2ax+b \\ 3ax+b \end{pmatrix}$$

(Im Bild: $\begin{pmatrix} 3 \\ 2 \\ 1 \\ 0 \end{pmatrix}$)

→ Rauschen

$$\begin{pmatrix} 3 \\ 2 \\ 25 \\ 0 \end{pmatrix}$$

$K = R$ zur Illustrationszweck.

$$\left\{ \begin{array}{l} a = 3 \\ a+b = 2 \\ 2a+b = 2.5 \\ 3a+b = 0 \end{array} \right.$$

Dann kann man nur sukzessiv ausprobieren, eine der 4 Gleichungen rauszulassen.

Wenn man "die koppelte Gleichung" durchsetzt ist die Lösungsmenge leer. Wenn man die koppelte Gleichung rauslässt, erhält man genau eine Lösung (a, b) .

Was ist die Menge aller Codewörter?

$$\left\{ \underbrace{\begin{pmatrix} a & b \\ a+b & 2a+b \\ 2a+b & 3a+b \end{pmatrix}}_{\text{lin}} : a, b \in K \right\} = \text{lin} \left(\begin{pmatrix} 1 & 0 \\ 1 & 2 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right).$$

$$a \cdot \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} + b \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Es ist ein 2-dimensionaler Raum innerhalb eines 4-dimensionalen Raums.

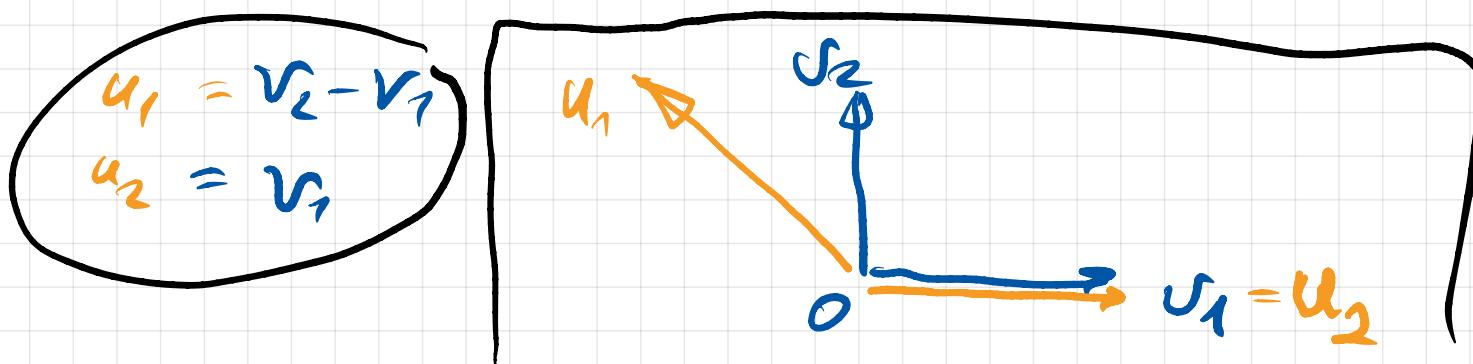
Wir können die Kodierungsmatrix ändern, ohne die Orte der Code-Wörter zu ändern.

$$(a, b) \in \mathbb{K}^2 \rightarrow \begin{pmatrix} (b-a) \cdot x + a \\ x = 0, 1, 2, 3 \end{pmatrix} = \begin{pmatrix} a \\ b \\ 2b-a \\ 3b-2a \end{pmatrix}$$

$$\text{lin} \left(\begin{pmatrix} 1 \\ 0 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} \right) = \text{lin} \left(\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right)$$

$\Downarrow \quad \Downarrow$

$\Downarrow u_1 \quad \Downarrow u_2 \quad \Downarrow v_1 \quad \Downarrow v_2$



Die Daten sind heutzutage digital. Daher können wir bei einer digitalen Kommunikation $K = \mathbb{F}$ nicht nutzen. Wir können endliche Körper nutzen, z.B. \mathbb{Z}_5 , dann $\alpha \in \mathbb{Z}_5$ hat man $[0], [1], [2], [3]$, die alle unterschiedlich sind. Aber in der Praxis nutzt man in so einer Situation andere Körper.

d.h. nutzt z.B. Körper mit 256 Elementen (das entspricht einem Byte). Ich zeige als Beispiel wie \mathbb{F}_4 , der Körper aus 4 Elementen, umgefasst werden kann.

$$\mathbb{F}_4 = \{0, 1, \omega, \overbrace{\omega}^{1+\omega}\}$$

// // // //
 00 10 01 11

In \mathbb{F}_4 deklarieren wir : $1+1=0$.

$$\omega^2 + \omega + 1 = 0$$

$$\omega(\omega+1) = \omega^2 + \omega = -1 = 1.$$

Innerhalb von Ringen und Körpern findet man noch eine weitere abstrakte Struktur...



Def Eine Gruppe ist eine Struktur $(G, *)$ mit einer Verknüpfung $*: G \times G \rightarrow G$, welche die folgenden Gesetze erfüllt:

- Es gibt ein $e \in G$, mit $a * e = e * a = a$ für alle $a \in G$
(dieses Element ist notwendigerweise eindeutig).
- $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$.
- Zu jedem $x \in G$ gibt es ein $y \in G$ mit $x * y = y * x = e$
(Dieses y zu x ist eindeutig, notwendigerweise.
Bezeichnung $y = \bar{x}$.)

eine Gruppe mit der kommutativen Verknüpfung,
d.h. mit $a * b = b * a$ für alle $a, b \in G$,
nennt man kommutativ oder Abelsch.

Die Gruppenverknüpfung wird oft als \circ (nach L) bezeichnet. In diesem Fall bezeichnet man e oft als 1.

$$a \cdot 1 = 1 \cdot a = a$$

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

$$a \cdot \bar{a} = \bar{a} \cdot a = 1$$

Bei abelschen Gruppen wird die Gruppenverknüpfung oft als + bezeichnet. Und dann schreibt man entsprechend $0 - a$ an:

$$\begin{aligned} a + 0 &= 0 + a = a \\ a + (b+c) &= (a+b)+c \\ a + b &= b + a \\ a + (-a) &= (-a)+a = 0 \end{aligned}$$

$(\mathbb{Q}, +)$
Abelsche
Gruppe

Bemerkung: Innerhalb eines Körpers $(K, +, \cdot)$
findet man zwei besondere Gruppen:

$(IK, +)$ Abelsche Gruppe

$(K \setminus \{0\}, \cdot)$ Abelsche Gruppe

Bem.: \mathbb{Z}_n in SageMath : IntegerModRing(n)

R = IntegerModRing(5)

M = matrix(R, [(0, 1, 3), (1, 1, 2), (2, 1, 1), (3, 1, 0)])

$$\left[\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 1 & 2 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \end{array} \right]$$



$$\begin{cases} b = 3 \\ a + b = 2 \\ 2a + b = 1 \\ 3a + b = 0 \end{cases}$$

SageMath
numerical

echelon-form
 $\in \mathbb{Z}_5$

$$\left[\begin{array}{cc|c} 1 & 0 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right]$$



$$\begin{cases} a = [4] \\ b = [3] \\ [0] = [0] \\ [0] = [0] \end{cases}$$

Lösungssammlung
über

Mit einem Kaputten Codewort.

$$\left[\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 1 & 2 \\ 2 & 1 & 4 \\ 3 & 1 & 0 \end{array} \right]$$

$$\begin{cases} b = 3 \\ a + b = 2 \\ 2a + b = 4 \\ 3a + b = 0 \end{cases}$$

SageMath

numerical

echelon-form
 $\in \mathbb{Z}_5$

$$\left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{array} \right]$$

$$\begin{cases} a = 0 \\ b = 0 \\ 0 = 1 \\ 0 = 0 \end{cases}$$

2.

Vektorräume

2.1

Der allgemeine Begriff eines Vektorraums

Def.

Für einen Körper $(K, +, \cdot)$ ist ein Vektorraum V über K eine Struktur mit den folgenden Eigenschaften:

V hat eine Addition $+ : V \times V \rightarrow V$

und eine so genannte eine Skalarmultiplikation

$\cdot : K \times V \rightarrow V$

derart, dass $(V, +)$ eine Abelsche Gruppe

bildet und darüber hinaus die folgenden Gesetze gelten:

$$(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$$

$$\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$$

$$(\alpha \cdot \beta) \cdot v = \alpha \cdot (\beta \cdot v)$$

$$1 \cdot v = v$$

für alle $\alpha, \beta \in K$
und alle $u, v \in V$

$(V, +)$ ist eine abelsche Gruppe heißt:

$$\left. \begin{array}{l} v + 0 = v \\ u + v = v + u \\ (u + v) + w = u + (v + w) \\ u + (-u) = 0 \end{array} \right\} \text{Für alle } u, v, w \in V$$

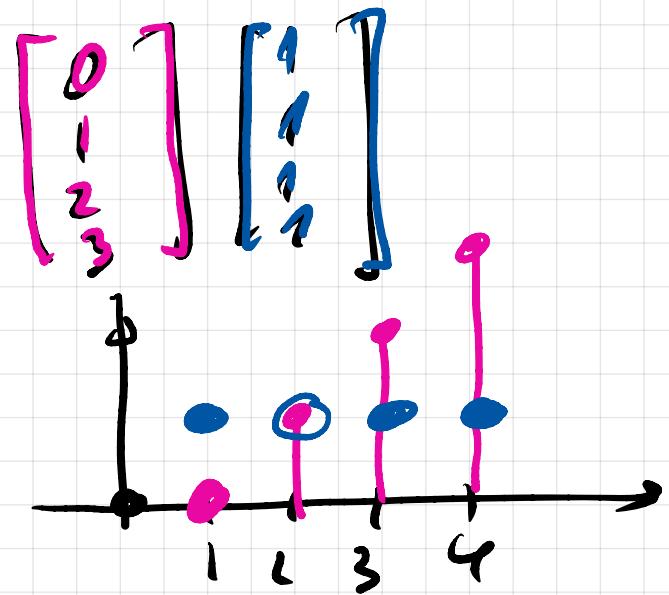
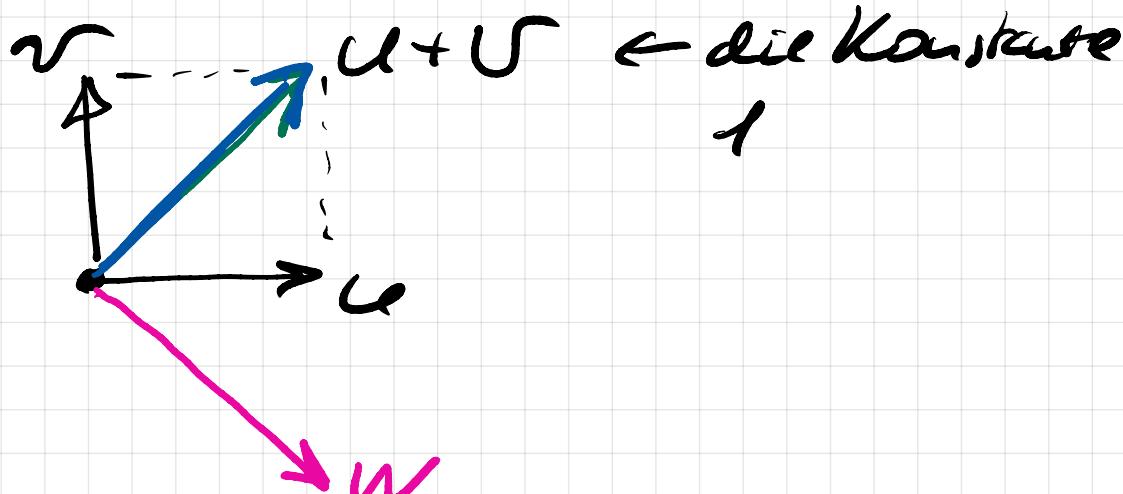
0 hier ist der Nullvektor.

Bsp. \mathbb{K}^n ist ein "konkreter" Vektorraum.

- $V = \{ \text{Funktionen von } \mathbb{R} \text{ nach } \mathbb{R} \} = \mathbb{R}^{\mathbb{R}}$

$$\cos 2x = \underbrace{\cos^2 x}_{w} - \underbrace{\sin^2 x}_{v}$$

$$w = u - v$$



Definieren wir lineare Abhangigkeit und
Unabhangigkeit werden in V genauso erfuhrt
wie in K^u .

Bsp. für abstrakte Argumentation

Wie zeigt man, dass \mathbb{C} einen Vektorraum (VR)

$\forall v \quad 0 \cdot v = 0$ für alle $v \in V$ gilt.
Zoll \oplus Vektor.

$$0 \cdot v = (0+0) \cdot v = 0 \cdot v + 0 \cdot v \Rightarrow$$

$$0 \cdot v = 0 \cdot v + 0 \cdot v \quad \text{Da } (V, +) \text{ Abelsche}$$

Gruppe ist hat man zu jedem $a \in V$

dies $-a$ mit $a + (-a) = 0$

$$\Rightarrow 0 \cdot v + (-0 \cdot v) = (0 \cdot v + 0 \cdot v) + (-0 \cdot v)$$

$$\Rightarrow 0 = (0 \cdot v + 0 \cdot v) + (-0 \cdot v)$$

$$\Rightarrow 0 = 0 \cdot v + (0 \cdot v + (-0 \cdot v))$$

$$\Rightarrow 0 = 0 \cdot v + 0$$

$$\Rightarrow 0 = 0 \cdot v$$

Ein weiteres ähnliches Beispiel:

Wie zeigen $(-1) \cdot v = -v$ für alle $v \in V$.

$-v$ ist der Vektor mit der Eigenschaft $v + (-v) = 0$

Wir zeigen, dass $(-1) \cdot v$ genau dieser Vektor ist:

$$\begin{aligned} v + (-1) \cdot v &= 1 \cdot v + (-1) \cdot v = (1 + (-1)) \cdot v \\ &= 0 \cdot v = 0. \end{aligned}$$

2.2. Untervektorräume

Def Für einen VR V heißt $W \subseteq V$ ein Untervektorraum (UVR) von V , wenn folgendes gilt:

- $0 \in W$
- $u, v \in W \Rightarrow u + v \in W$
- $\alpha \in K, u \in W \Rightarrow \alpha \cdot u \in W$

Bem. Ein UVR W von V ist stets ein VR bzgl. der Einschränkung der Verknüpfungen $+ : V \times V \rightarrow V$ und $\cdot : K \times V \rightarrow V$ auf W . Diese Einschränkungen sind wohldefiniert.

Bsp. aus der Kodierungstheorie

Wir schicken zu 4 bits: $a, b \in \mathbb{Z}_2$

unser Körper ist \mathbb{Z}_2 . Eine Möglichkeit wäre

(a, b, a, b, a, b) als Codewort zu senden.

Dann ist $\{(a, b, a, b, a, b) : a, b \in \mathbb{Z}_2\}$

ein Untervektorraum von \mathbb{Z}_2^6 .

Eine andere Möglichkeit:

$(a, b, a, b, a+b)$

Der Code (die Menge der Codewörter)

ist der Untervektorraum

$\{(a, b, a, b, a+b) : a, b \in \mathbb{Z}_2\}$.