Kodierungstheorie
-Körper und Vektorräume-

Abschnitt: 3 bis 4

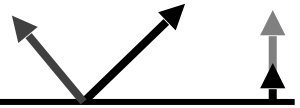
Von: Michel Carneiro Last

Inhaltsverzeichnis

Körper 

Endliche Körper 

ISBN-Code 

Vektorräume 

Körper

Körper

- Ein Körper (engl. field) ist eine Menge ***K***, mit den Operationen Addition und Multiplikation, wo folgende Bedingungen erfüllt sind:

$$Seien\ a, b, c\ \in K$$

1. (K, +) ist eine abelsche Gruppe

1.1 (Assoziativgesetzt)

$$a + (b + c) = (a + b) + c$$

1.2 (Kommutativgesetz)

$$a + b = b + a$$

1.3 (neutrales Elements)

$$Sei\ 0\ neutrales\ Element\ "+":$$
$$a + 0 = 0 + a = a$$

1.4 (Inverses Element)

$$Sei\ (-a)\ die\ Inverse\ von\ a\ so:$$
$$a + (-a) = (-a) + a = 0$$

2. (K\{0}, *) ist eine abelsche Gruppe

2.1 (Assoziativgesetzt)

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

2.2 (Kommutativgesetz)

$$a * b = b * a$$

2.3 (neutrales Elements)

$$Sei\ 1\ neutrales\ Element\ "*":$$
$$a * 1 = 1 * a = a$$

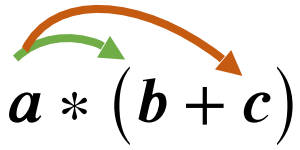
2.4 (Inverses Element)

$$Sei\ (1/a)\ die\ Inverse\ von\ a\ so:$$
$$a * \left(\frac{1}{a}\right) = \left(\frac{1}{a}\right) * a = 1$$

Körper

- Ein Körper (engl. field) ist eine Menge ***K***, mit den Operationen Addition und Multiplikation, wo folgende Bedingungen erfüllt sind:

  3.1 Distributivität



Körper – Lemma 3.1

- Seien a und b Elemente aus K, so gilt:
  i. $a * 0 = 0 \ \forall \ a \in K$
  ii. $a * b = 0 \ => \ a = 0 \, oder \, b = 0$

- Beweis:

$i) \ a * 0 = a(0 + 0) = a * 0 + a * 0$

$0 = a * 0 + (- a * 0) = a * 0 \ + a * 0 + (-a * 0) = a * 0 + 0 = a * 0$

$ii) \ Sei \ a \ \neq 0, \, dann \, ex. \, ein \, Inverse \, für \, a:$

$$\mathrm{b} = 1 * b = \left(a * \frac{1}{a} \right) * b = \frac{1}{a} * (a * b) = \frac{1}{a} * 0 = 0$$

Körper - Ring

- Ein **Körper** (engl. field) ist eine Menge ***K***, mit den Operationen Addition und Multiplikation, wo folgende Bedingungen erfüllt sind:

    1. (**K**, +) ist eine abelsche Gruppe

    2. (**K**\{0}, *) ist eine abelsche Gruppe

    3. Es gelten die Distributivgesetze

- Ein **Ring** (engl. ring) ist eine Menge ***R***, mit den Operationen Addition und Multiplikation, wo folgende Bedingungen erfüllt sind:

    1. (**R**, +) ist eine abelsche Gruppe

    2. (**R**\{0}, *) ist eine abelsche Halbgruppe mit Eins

        2.4 aber besitzt nicht unbedingt ein Inverses Element

    3. Es gelten die Distributivgesetze

Endliche Körper

Endliche Körper

- Wir bezeichnen einen endlichen Köper (Galoiskörper) einen Körper mit einer endlichen Anzahl an Elementen. Die Anzahl der Elemente eines endlichen Körpers ist immer eine Primzahlpotenz. Für jede Primzahl p und jede positive natürliche Zahl n existiert genau ein Körper mit p^n Elementen, der mit der Notation: F_{p^n}**, oder GF(**p^n**).**
- Es ist für n**=1** der Ring der Restklassen Z_{p^n} ganzer Zahlen „modulo“ p.

$Bsp.: Z_4,$ *also Z besitzt die Elemente* $0, 1, 2, 3$

1. (Z_4, +) ist eine abelsche Gruppe

1.1 (Assoziativgesetzt)
$klar$

1.2 (Kommutativgesetz)
$klar$

1.3 (neutrales Elements)
$klar$

1.4 (Inverses Element) als Beispiel 3 ?

$3 + x = 0 \Rightarrow x = 1$

2. (Z_4, *) ist eine abelsche Halbgruppe m.E.

2.1 (Assoziativgesetzt)
$klar$

2.2 (Kommutativgesetz)
$klar$

2.3 (neutrales Elements)
$klar$

2.4 (Inverses Element, nur manchmal)

$3 * x = 1 \Rightarrow x = 3$

Endliche Körper - Tipp

*	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

*	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Endliche Körper - Kongruenz

- Sei ***m*** eine festgelegte natürliche Zahl und seien a und b ganze Zahlen. So sagt man „a und b sind miteinander in Kongruenz“, wenn gilt:

- $(a - b) = m * k \quad , k \in \mathbb{Z}$

- Notation: $a \equiv b \ (\%\ \ m)$

- Beispiele:

$$3 \equiv 24 \ (\%\ \ 7)$$
$$(3 - 24) = -21 \Rightarrow -21 \% 7 = 0$$

$$15 \equiv 0 \ (\%\ \ 5)$$
$$(15 - 0) = 15 \Rightarrow 15 \% 5 = 0$$

$$13 \equiv -2 \ (\%\ \ 5)$$
$$(13 + 2) = 15 \Rightarrow 15 \% 5 = 0$$

$$25 \not\equiv 12 \ (\%\ \ 7)$$
$$(25 - 12) = 13 \Rightarrow 13 \% 7 = 6$$

Endliche Körper – Lemma 3.3

- Seien $a \equiv a' (\%\quad m)\ und\ b \equiv b'\ (\%\quad m)$, so gilt:

i) $a + b \equiv a' + b'\ (\%\quad m)$

ii) $ab \equiv a'b'\ (\%\quad m)$

Beweis:

i) *Es gilt* $m|(a-b)$ *und* $m|(a'-b')$

$\Rightarrow \boldsymbol{m|(a-b)+(a'-b')}$

$\Rightarrow \boldsymbol{m|a+a'-b-b'}$

$\Rightarrow \boldsymbol{m|(a+b)-(a'+b')}$

ii) *Es gilt* $m|(a-b)$ *und* $m|(a'-b')$

$\Rightarrow \boldsymbol{m|(a-b)*a' und (a'-b')*b}$

$\Rightarrow \boldsymbol{m|(a-b)*a'*(a'-b')*b}$

$\Rightarrow \boldsymbol{m|a*a'-b*a'+b*a'-b*d}$

$\Rightarrow \boldsymbol{m|a*a'-b*d}$

- Anmerkung:

Wenn

$a \equiv a' (\%\quad m)$ *gilt, dann gilt auch* $a^n \equiv a'^n (\%\quad m)$. *Wobei n eine natürliche Zahl ist.*

Alternativ:

i)

$\Rightarrow a = a' + ml\ und\ b = b' + mk,\quad l,k \in \mathbb{N}$

$\Rightarrow a + b = a' + b' + (l*m)m,\qquad l,k \in \mathbb{N}$

$\Rightarrow (a+b) = (a'+b') + (l*m)m,\qquad l,k \in \mathbb{N}$

ii)

$\Rightarrow a = a' + ml\ und\ b = b' + mk,\quad l,k \in \mathbb{N}$

$\Rightarrow\ a*b = (a' + ml)\ *\ (b' + mk),\quad l,k \in \mathbb{N}$

Endliche Körper

- Frage: Sind endliche Restklassenringe immer Körper?
- Antwort: Nicht immer. Allgemein hat Z_p immer eine Ring-Struktur. Ist p aber eine Primzahl, so ist $F_p = Z_p$ ein Körper.

Seien a und b Elemente aus K, so gilt:

i. $a * 0 = 0 \ \forall \ a \in K$

ii. $a * b = 0 \Rightarrow a = 0 \ oder \ b = 0$

- Beweis:
- $Sei\ p\ keine\ Primzahl,\ dann\ gilt:\ a * b = p,\ mit\ a\ und\ b\ als\ ganze\ Zahlen\ und\ kleines\ als\ p.$

$$\Rightarrow a * b \equiv 0(\%\ p),\ \ mit\ a \not\equiv 0(\mathrm{mod\ p})\ \text{und}\ b \not\equiv 0(\mathrm{mod}\ p)$$

$$\Rightarrow\ a * b = 0$$

- Kleines Beispiel:
  Z_4
- F_4

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

ISBN-Code

- Internationale Standardbuchnummer (ISBN) ist eine Nummer zur eindeutigen Kennzeichnung von Büchern und anderen selbstständigen Veröffentlichungen mit redaktionellem Anteil, wie beispielsweise Multimedia-Produkten und Software. (Quelle: Wikipedia.de)

- Aufbau:

ISBN-Code

0-19-859617-0

Die Prüfziffer, ist wie folgt definiert:

$$z_{10} = \sum_{i=1}^{9} i x_i (\%11), \quad wobei\ x_i\ die\ Einträge,\ der\ ISBN\ nummer\ entspricht$$

Also in unserem Beispiel:

$$(1 * 0 + 2 * 1 + 3 * 9 + 4 * 8 + 5 * 5 + 6 * 9 + 7 * 6 + 8 * 1 + 9 * 7)\ \%\ 11$$

=> $253\%\ 11 = 0$

Es gelten zwei wichtige Formeln:

$$\sum_{i=1}^{10} i x_i \equiv 0\ (\%\ 11)$$

$$z_{10} = \sum_{i=1}^{9} i x_i (\%11),$$

ISBN-Code – Warum das Ganze?

$$\sum_{i=1}^{10} i x_i \equiv 0 \ (\%\ 11)$$

- Der Code kann einzelnen fehlende Ziffern selber korrigieren:

Beispiel: Sei 0-201-1x-502-7 eine ISBN. Suchen x:

$$\Rightarrow\ 1*0+2*2+3*0+4*1+5*1+6*x+7*5+8*0+9*2+10*7=0$$

$$\Rightarrow\ 4+4+5+6*x+7*5+9*2+10*7=0$$

$$\Rightarrow\ 4+4+5+6*x+2+7+4=0$$

$$\Rightarrow\ 6*x+4=0$$

$$\Rightarrow x=\frac{-4}{6}=7*6^{-1}=7*2=14=3$$

ISBN-Code – Warum das Ganze?

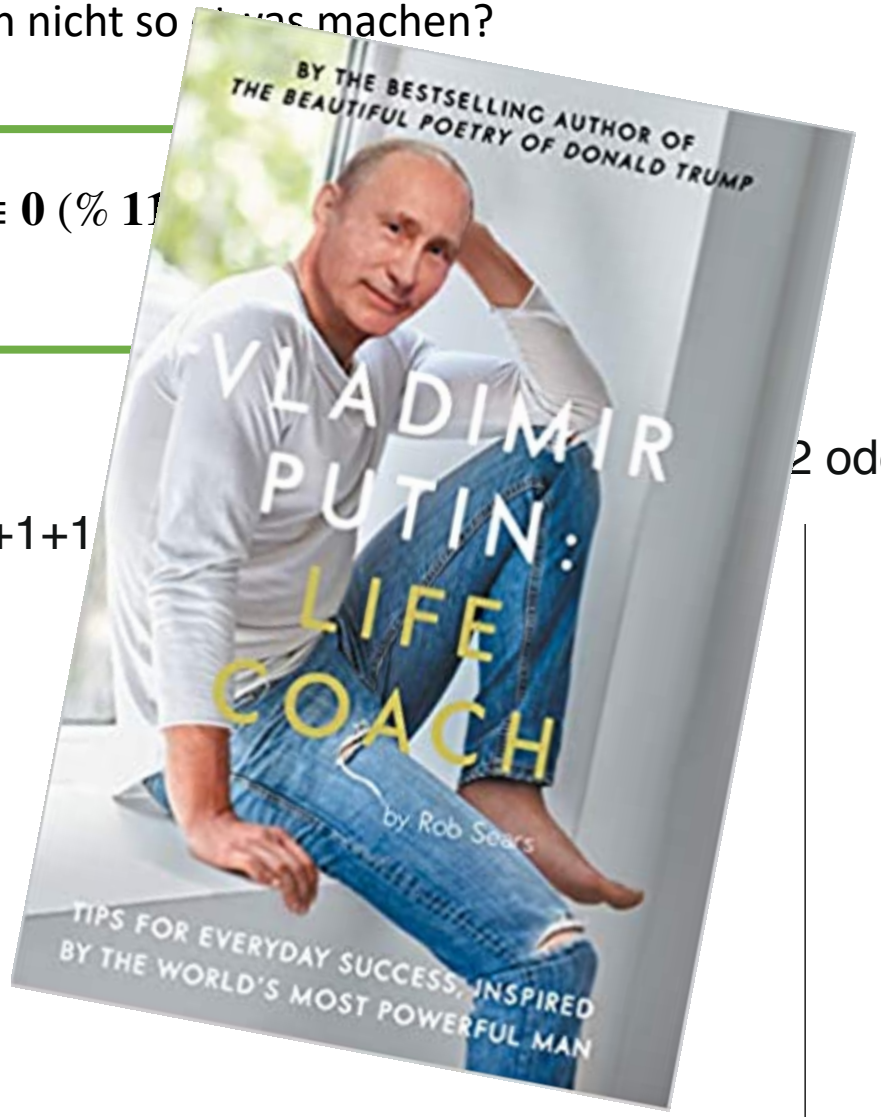
- Könnte man nicht so etwas machen?

$$\sum_{i=1}^{10} x_i \equiv 0 \ (\%\ 11$$

- Problem:

  => 3+5+5+1+1

  => …

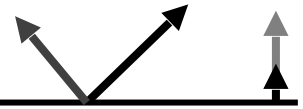


2 oder 3-55-1

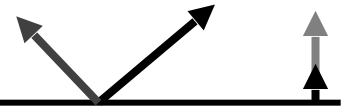
⇒ 1∗3 2 ≠5

⇒ 1 $= 2 = z_{10}$

Vektorräume



Vektorräume



- Sei K ein Körper. Ein Vektorraum über K ist eine abelsche Gruppe ***(V,+)***, zusammen mit einer Verknüpfung *: K x V -> V , so dass für alle $r, s \in K$ und alle $u, v \in V$ gilt:

a) $r * (u + v) = r * u + r * v$

b) $(r + s) * v = r * v + s * v$

c) $(r * s) * v = r * (s * v)$

d) $1 * v = v$

Elemente von V nennt man Vektoren. die Elemente von K nennt man Skalare; + heißt Vektoraddition, * heißt Skalarmultiplikation. Das Element 0 ∈ V nennt man Nullvektor.

Gestallt:

Sei K^nein Vektorraum und seien a und b Vektoren:

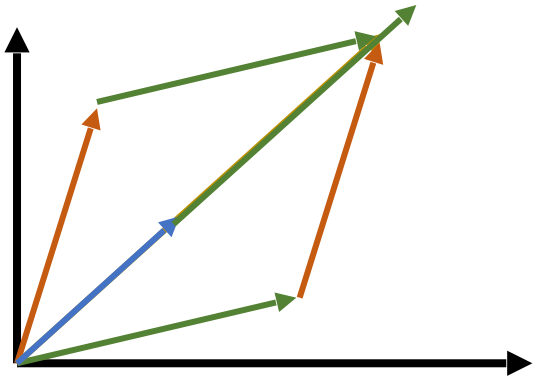
$a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$

Addition:

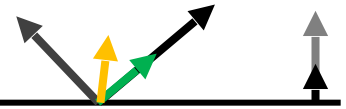
$$a + b = (a_1 + b_1, \ldots, a_n + b_n)$$

Multiplikation:

$$ra = (ra_1, \ldots, ra_n)$$



Vektorräume - Untervektorräume



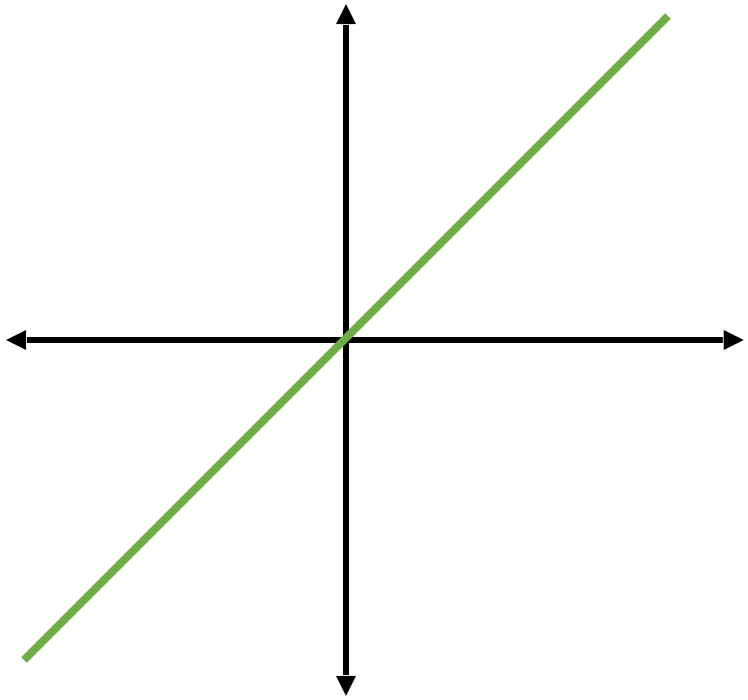
- Sei weiterhin K ein Körper. Ein Vektorraum über K ist eine abelsche Gruppe ***(V,+)***, zusammen mit einer Verknüpfung *: K x V -> V.
- Sei U eine Teilmenge von V ($U \subseteq V$), so dass U ein Vektorraum ist. Wir bezeichnen U als Untervektorraum von V, wenn gilt:

$Seien\ u, u' \in U\ und\ r\ \in K,\ dann\ gilt:$

a) $u * r \in U$

b) $u + u' \in U$

c) $0 \in U$



Vektorräume – Lineare Unabhängigkeit

- Unter einer Linearkombination von Vektoren versteht man eine Summe von Vektoren (Vektoraddition), wobei jeder Vektor noch mit einer reellen Zahl multipliziert wird. Als Ergebnis erhält man wieder einen Vektor.
- $Seien\ (\lambda_i)\ Skalare$ und $v_i \in V,\ mit\ i = 1 \ldots n\ so\ ist\ eine\ linearkombination\ wie\ folgt\ gegeben$:
- $\lambda_1 v_1 + \ldots + \lambda_n v_n = v$

- n Vektoren sind genau dann linear unabhängig, wenn sich der Nullvektor nur durch eine Linearkombination der Vektoren erzeugen lässt, in der alle Skalare 0 sind.

- $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0 \Rightarrow \ \forall(\lambda_i) = 0.$

Beispiel:

$$v_1 = \begin{pmatrix} 1 \\ 3 \end{pmatrix} v_2 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$$

$$\Rightarrow \lambda_1 * \begin{pmatrix} 2 \\ 4 \end{pmatrix} + \lambda_2 * \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\left(\begin{array}{cc|c} 1 & 2 & 0 \\ 3 & 4 & 0 \end{array}\right) \longrightarrow \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right)$$

$$\Rightarrow \lambda_1 = 0 \text{ und } \lambda_2 = 0$$

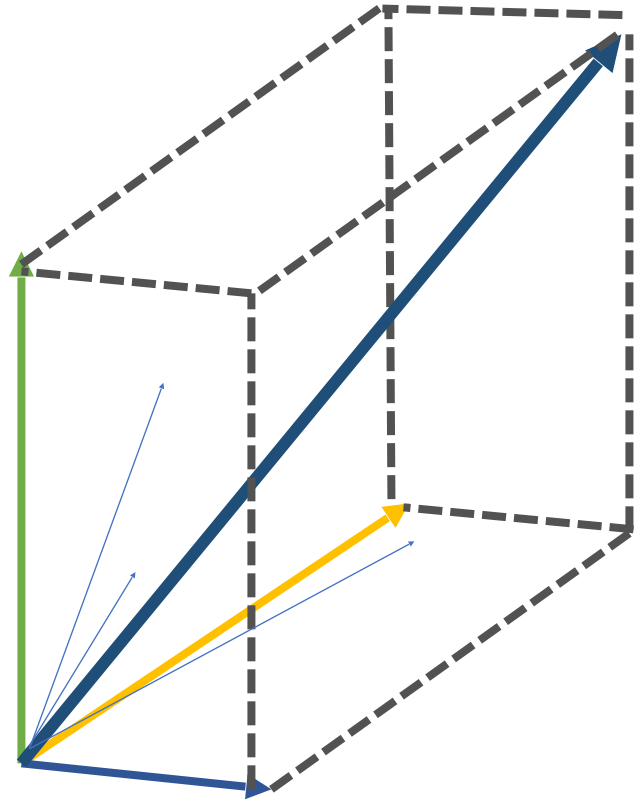
Vektorräume – Basis

- Seien (v_i) Vektoren von V, diese nennt man Basis von V, wenn diese linear unabhängig sind und V „erzeugen“.
- Das heißt:
  - Jeder Vektor v ∈ V lässt sich auf eindeutige Weise als Linearkombintation der Vektoren (v_i) schreiben.
  - Es ist ein minimales Erzeugendensystem
  - Es ist maximal linear unabhängig, d.h. der Span((v_i)) = dim(V)
- Standartbasis:

$$e_1 = \begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}, \ldots, e_n = \begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix} \quad , K^n$$

Beispiel: Dim(V)=3

$$\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \qquad \begin{pmatrix}1\\1/2\\(-3)\end{pmatrix} \qquad \begin{pmatrix}0\\0\\1\end{pmatrix}$$



Vielen Dank