Anwendung: Teilbarkeitsregeln im Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $2 \mid \alpha_n\alpha_{n-1}...\alpha_0$*?* (In Worten: teilt 2 die Zahl $\alpha_n\alpha_{n-1}...\alpha_0$)?
Die Antwort wissen Sie seit der Schule (die Zahl ist gerade g.d.w. die letze Ziffer 0,2,4,6, oder 8 ist); jetzt werden wir diese Antwort beweisen; die Methode erlaubt es uns, Teilbarkeitsregeln für beliebige Zahl selber zu konstruieren.
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $2 \mid a - 0$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 2}{+} ... \overset{\text{mod } 2}{+} [\alpha_0 \cdot 1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 2}{+} ... \overset{\text{mod } 2}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 2}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 2}{+} ... \overset{\text{mod } 2}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 2}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n \cdot 0 + ... + \alpha_1 \cdot 0 + \alpha_0 \cdot 1] = [\alpha_0].$$

Antwort: $[\alpha_n\alpha_{n-1}...\alpha_0] = [0] \iff [\alpha_0] = [0]$ in $\mathbb{Z}_2$
Antwort umformulieren: $\alpha_n\alpha_{n-1}...\alpha_0$ ist g.d. durch 2 teilbar, wenn α_0 durch 2 teilbar ist.

Frage: $3 \mid \alpha_n\alpha_{n-1}...\alpha_0$*?*

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	$\vdots$

Deswegen:

$$
\begin{aligned}
& [\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 + \alpha_0 \cdot 1] \\
= & [\alpha_n] \overset{\text{mod } 3}{\cdot} [10^n] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
= & [\alpha_n] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
= & [\alpha_n + ... + \alpha_1 + \alpha_0].
\end{aligned}
$$

Antwort: $\alpha_n\alpha_{n-1}...\alpha_0$ *ist g.d. durch 3 teilbar, wenn* $\alpha_n + \alpha_{n-1} + ... + \alpha_0$ *durch 3 teilbar ist.*

Frage: $4 \mid \alpha_n\alpha_{n-1}...\alpha_0$? *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_4$?

Ausrechnen 10^k in $\mathbb{Z}_4$:

k	$[10^k]$ in $\mathbb{Z}_4$
0	$[1]$
1	$[2]$
2	$[2] \overset{\text{mod } 4}{\cdot} [2] = [0]$
3	$[2] \overset{\text{mod } 4}{\cdot} [0] = [0]$
$\vdots$	$\vdots$
$n \geq 3$	$[2] \overset{\text{mod } 4}{\cdot} [0] = 0$

Antwort: $\alpha_n\alpha_{n-1}...\alpha_0$ *ist g.d. durch 4 teilbar, wenn* $2 \cdot \alpha_1 + \alpha_0$ *durch 4 teilbar ist.*

Bsp. 16 *ist durch 4 teilbar, da* $2 \cdot 1 + 1 \cdot 6 = 8$ *durch 4 teilbar ist.*

$$
\begin{aligned}
&[\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 \cdot \alpha_0 \cdot 1] \\
&= [\alpha_n] \overset{\text{mod } 4}{\cdot} [10^n] \overset{\text{mod } 4}{+} ... \overset{\text{mod } 4}{+} [\alpha_1] \overset{\text{mod } 4}{\cdot} [10] \overset{\text{mod } 4}{+} [\alpha_0] \overset{\text{mod } 4}{\cdot} [1] \\
&= [\alpha_n] \overset{\text{mod } 4}{\cdot} [0] \overset{\text{mod } 4}{+} ... \overset{\text{mod } 4}{+} [\alpha_1] \overset{\text{mod } 4}{\cdot} [2] \overset{\text{mod } 4}{+} \alpha_0 \overset{\text{mod } 4}{\cdot} [1] \\
&= [2 \cdot \alpha_1 + \alpha_0].
\end{aligned}
$$

Frage: $7 \mid \alpha_n\alpha_{n-1}...\alpha_0$?

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Bsp. 938748033764775430564 9 ist durch 7 teilbar, weil

$$1 \cdot 9 + 3 \cdot 4 + 2 \cdot 6 - 1 \cdot 5 - 3 \cdot 0 - 2 \cdot 3$$
$$+1 \cdot 4 + 3 \cdot 5 + 2 \cdot 7 - 1 \cdot 7 - 3 \cdot 4 - 2 \cdot 6$$
$$+1 \cdot 7 + 3 \cdot 3 + 2 \cdot 3 - 1 \cdot 0 - 3 \cdot 8 - 2 \cdot 4$$
$$+1 \cdot 7 + 3 \cdot 8 + 2 \cdot 3 - 1 \cdot 9 - 3 \cdot 0 - 2 \cdot 0$$
$$= 42$$ durch 7 teilbar ist.

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 teilbar,* wenn (in $\mathbb{Z}_7$)

$$10^0 \cdot \alpha_0 + 10^1 \cdot \alpha_1 + 10^2 \cdot \alpha_2 + 10^3 \cdot \alpha_3 + 10^4 \cdot \alpha_4 + 10^5 \cdot \alpha_5 + ... +$$
$$10^{6k} \cdot \alpha_{6k} + 10^{6k+1} \cdot \alpha_{6k+1} + 10^{6k+2} \cdot \alpha_{6k+2} + 10^{6k+3} \cdot \alpha_{6k+3} + 10^{6k+4} \cdot \alpha_{6k+4} +$$
$$10^{6k+5} \cdot \alpha_{6k+5} + ... \overset{\text{in } \mathbb{Z}_7}{=} \alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5$$
$$+ ... + \alpha_{6k} + 3\alpha_{6k+1} + 2\alpha_{6k+2} - \alpha_{6k+3} - 3\alpha_{6k+4} - 2\alpha_{6k+5} + ...$$

gleich Null (in $\mathbb{Z}_7$) ist; also wenn das, was rechts steht, durch 7 teilbar ist.

Zu Hause:

Teilbarkeitsregel für 37. Hinweis: $37 \mid 999 = 1000 - 1$.

Mit diesen Methoden kann man mehrere Zahlentheoretische Aufgaben lösen

BspAufgabe: Z.z.: $27 \mid 10^n + 18n - 1$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \cdot [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] = [27] = [0]$,

Für $n = 3k + 2$ ist

$[10^{3k+2} + 18 \cdot (3 \cdot k + 2) - 1] = [-8 + 18 \cdot 2 - 1] = [27] = [0]$. □

Def. *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grösste Zahl* $m \in \mathbb{N}$ *s.d.* $m \mid a$ *und* $m \mid b$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *teilerfremd.*

Satz A5 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt: Es gibt* $n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst die folgende

Hilfsaussage: $ggT(a,b) = ggT(a-b,b)$. $\quad (*)$

Tatsächlich, $\begin{array}{l} x \mid a \\ k_1 x = a \end{array}$ und $\begin{array}{l} x \mid b \\ k_2 x = b \end{array} \Rightarrow \begin{array}{l} x \mid a-b \\ (k_1 - k_2)x = a - b, \end{array}$

also die Menge

$A := \{\text{alle gem. Teiler von } a, b\}$ ist eine Teilmenge von

$B := \{\text{alle gem. Teiler von } a-b, b\}$ (d.h., $A \subseteq B$).

Analog gilt:

$\begin{array}{l} x \mid a-b \\ k_1 x = a - b \end{array}$ und $\begin{array}{l} x \mid b \\ k_2 x = b \end{array} \Rightarrow \begin{array}{l} x \mid b \\ (k_1 + k_2)x = b, \end{array}$

also die Menge

$A := \{\text{alle gem. Teiler von } a, b\}$ enthält alle Elemente von

$B := \{\text{alle gem. Teiler von } a-b, b\}$ (d.h., $A \supseteq B$).

Also, $A = B$, und die grössten Elemente der Mengen sind ebenfalls gleich.

Satz A5 *Seien $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. Dann gilt: Es gibt $n, m \in \mathbb{Z}$ s.d. $na + mb = ggT(a, b)$.*

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion in $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a, b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a, b)$.

Ist $a = b$, so ist die Aussage offensichtlich: $1 \cdot a + 0 \cdot b = ggT(a, b)$.

Angenommen, $a \neq b$, oBdA sei $a > b$. Nach (IV) und Hilfsaussage gibt es n, m_1 s.d. $n \cdot (a - b) + m_1 \cdot b = ggT(a - b, b) \overset{(*)}{=} ggT(a, b)$. Also,

$$na + \underbrace{(m_1 - n)}_{m} b = ggT(a, b),$$

□

Def. Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Bemerkung. Die Gruppe $(\mathbb{K} \setminus \{0\}, \cdot)$ ist automatische abel'sch, weil „$\cdot$“ kommutativ ist.

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Sazt A6. $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir mit 0 bezeichen;

(R2) die Multiplikation „$\cdot$" ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz, d. h. für alle $a, b, c \in \mathbb{K}$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$.

Beweis $\Longleftarrow$: Angenommen: q ist eine Primzahl. Z.z.: $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist ein Körper. $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist ein kommutativer Ring. Z.z.: $(\mathbb{Z}_q \setminus \{[0]\}, \overset{\text{mod } q}{\cdot})$ ist eine Gruppe.
(G1) ist nach Definition des Rings erfüllt, siehe (R2).
(G2) [1] ist ein neutrales Element bzgl. $\overset{\text{mod } q}{\cdot}$.
(G3) Z.z. Für jeden $[a] \neq [0]$ gibt es ein n mit $[n \cdot a] = [1]$. Da q eine Primzahl ist, ist $ggT(q, a) \in \{1, q\}$. Ist $ggT(q, a) = q$, so $q \vdots a$, also $[a] = [0]$. Ist $ggT(q, a) = 1$, so gibt es nach Satz A5 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann $[1] = [m \cdot q + n \cdot a] = [n \cdot a]$ (d.h., n ist ein inverses Element zu a). Offensichtlich, ist $[n] \neq [0]$. (G3) ist bewiesen.
Daraus folgt auch, dass die Operation „$\cdot$" wohldefiniert ist: wenn $[a] \neq [0]$ und $[b] \neq [0]$ sind, ist $[a] \cdot [b]$ ebenfalls nicht 0. In der Tat, wir nehmen n mit $[n] \cdot [a] = [1]$. Ist $[a] \cdot [b] = [0]$, so ist $\underbrace{[n] \cdot [a]}_{[1]} \cdot [b] = [n] \cdot [0]$;
daraus folgt dass $[b] = [0]$ was uns ein Widerspruch gibt. □

Satz A6. $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis $\Longrightarrow$. Z.z.: ist $\mathbb{K}$ eine Körper, so ist q eine Primzahl. Sei $q = m \cdot n$, wobei $n \neq q$,. Dann ist $[q] = [m \cdot n]$, also $[0] = [m] \overset{\text{mod } q}{\cdot} [n]$. Dann gilt: $[0] \overset{\text{Lemma A4}}{=} [0] \overset{\text{mod } q}{\cdot} ([n]^{-1}) = [m] \overset{\text{mod } q}{\cdot} [n] \overset{\text{mod } q}{\cdot} ([n]^{-1}) = [m]$, also $[m] = [0]$, also $m = q$. □

Bitte üben

Was ist $[2]^{-1}$ in $\mathbb{Z}_5$?
Antwort: $[3]$, weil $[3] \cdot [2] = [6] = [1]$.

Wiederholung: (Hauptdefinition aus Vorl. 3:) Vektorraum ist eine Menge V mit zwei Abbildungen $+ : V \times V \to V$, $\circ : \mathbb{R} \times V \to V$ s.d. die folgende Eigenschaften erfüllt sind (für alle $u, v, w \in V$, $\lambda, \mu \in \mathbb{R}$).

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

II $u + v = v + u$

III Es existiert ein $\vec{0} \in V$, s. d. $\vec{0} + v = v$

IV Es existiert ein $-v \in V$, s. d. $-v + v = \vec{0}$

V $(\lambda\mu)v = \lambda(\mu v)$

VI $(\lambda + \mu)v = (\lambda v + \mu v)$

VII $\lambda(u + v) = \lambda u + \lambda v$

VIII $1v = v$

Def. Sei $(\mathbb{K}, +, \cdot)$ ein Körper. Eine Menge V mit Abbildungen
$+ : V \times V \to V$
$\circ : \mathbb{K} \times V \to V$
heißt ein Vektorraum über $\mathbb{K}$, falls die folgende Eigenschaften erfüllt sind (für alle $u, v, w \in V$, $\lambda, \mu \in \mathbb{K}$).

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

II $u + v = v + u$

III Es existiert ein $\vec{0} \in V$, s. d. $\vec{0} + v = v$

IV Für jedes $v \in V$ es existiert ein $-v \in V$, s. d. $-v + v = \vec{0}$

V $(\lambda\mu)v = \lambda(\mu v)$

VI $(\lambda + \mu)v = (\lambda v + \mu v)$

VII $\lambda(u + v) = \lambda u + \lambda v$

VIII $1v = v$ (Wobei 1 das neutrale Element in $(\mathbb{K}, \cdot)$ ist.)

Am Anfang des Kurses haben wir in Beweisen nur Eigenschaften I–VIII benutzt. Deswegen sind alle Aussagen, die wir in diesen Vorlesungen bewiesen haben, auch für Vektorräume über beliebigen Körpern gültig (und die Beweise für beliebige Körper wiederholen buchstäblich die Beweise für $\mathbb{K} = \mathbb{R}$). Das war auch ein Grund, warum ich das Wort „Skalare“ statt „reelle Zahlen“ benutzt habe – der einzige Unterschied ist jetzt, dass skalare Elemente aus $\mathbb{K}$ sind.
Das betrifft u.a.: Allgemeine Theorie von Vektorräumen, Untervektorräumen, Basis, Dimension, lineare Abbildungen, Matrizen, Determinante, Behandlung linearer Gleichungssysteme, Eigenwerte, Eigenvektoren, Diagonalisierbarkeit.
Es gibt auch Aussagen, die tatsächlich einige Eigenschaften von $\mathbb{R}$ verwenden und deswegen nicht über einem beliebigen Körper richtig sind (wir haben aber diese Aussagen noch nicht gehabt:
Bsp. In jedem Vektorraum über $\mathbb{R}$ gilt: Ist $v \neq \vec{0}$, so ist $v + v \neq \vec{0}$.
Diese Aussage ist aber falsch in den Vektorräumen über $\mathbb{Z}_2$:
In der Tat: $v + v \overset{VI}{=} (1 + 1)v = 2v = 0v = \vec{0}$.

$\mathbb{K}-$Vektorraum $\mathbb{K}^n$

Bsp. Sei $(\mathbb{K}, \cdot, +)$ ein Körper. $\mathbb{K}^n = \underbrace{\mathbb{K} \times ... \times \mathbb{K}}_{n \quad \text{Stuck}}$ ist die Menge von $n-$Tupeln $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ mit den Operationen $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$,

$\lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$ – dasselbe wir früher; die Elemente x_i, y_i und λ liegen jetzt in $\mathbb{K}$.

Rechnen Sie bitte selbst

- In $(\mathbb{Z}_5)^3$ addieren Sie $\begin{pmatrix}1\\2\\3\end{pmatrix}$ und $\begin{pmatrix}4\\4\\2\end{pmatrix}$.

  Antwort: $\begin{pmatrix}1\\2\\3\end{pmatrix} + \begin{pmatrix}4\\4\\2\end{pmatrix} = \begin{pmatrix}5\\6\\5\end{pmatrix} \overset{\text{in } \mathbb{Z}_5}{=} \begin{pmatrix}0\\1\\0\end{pmatrix}$.

- Berechnen Sie $\det \begin{pmatrix}4 & 3\\3 & 1\end{pmatrix} \in Mat(2,2,\mathbb{Z}_5)$.

  Antwort: $\det \begin{pmatrix}4 & 3\\3 & 1\end{pmatrix} = 4 - 9 \overset{\text{in } \mathbb{Z}_5}{=} 4 + 1 = 5 = 0$.

- Finden Sie den Eigenvektor zum Eigenwert 0 von $\begin{pmatrix}4 & 3\\3 & 1\end{pmatrix} \in Mat(2,2,\mathbb{Z}_5)$.

  Antwort: Dazu müssen wir das System $\begin{pmatrix}4 & 3\\3 & 1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}4x & +3y\\3x & +\ y\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$ lösen, z.B. mit Gauss-Algorithmus. Substrahiere Zeile_1 von Zeile_2 und ersetze 4 mit -1 und 3 mit -2 in Zeile_1 ergibt $\begin{pmatrix}-x & -2y\\-x & -2y\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$. Dann ist jeder Vektor $\begin{pmatrix}x\\y\end{pmatrix}$ mit $x = -2y$ eine Lösung. Also ist $\begin{pmatrix}-2\\1\end{pmatrix}$ ein Eigenvektor. Um sicher zu gehen kann man nachrechnen: $\begin{pmatrix}4 & 3\\3 & 1\end{pmatrix}\begin{pmatrix}-2\\1\end{pmatrix} = \begin{pmatrix}-8+3\\-6+1\end{pmatrix} \overset{\text{in } \mathbb{Z}_5}{=} \begin{pmatrix}0\\0\end{pmatrix}$

Satz 11 (Hauptsatz der linearen Algebra) *Zwei endlichdimensionale Vektorräume über einem Körper sind genau dann isomorph, wenn sie gleiche Dimension haben.*

Bitte üben

Satz 11 (Hauptsatz der linearen Algebra) *Zwei endlichdimensionale Vektorräume über einem Körper sind genau dann isomorph, wenn sie gleiche Dimension haben.*

Frage: Gibt es einen Vektorraum, der aus 2 Punkten besteht? JA! Für $\mathbb{K} = \mathbb{Z}_2$ ist $\mathbb{K}^1$ ein Vektorraum; Anzahl von Punkten in $\mathbb{K}^1$ ist 2.

Frage. Gibt es einen Vektorraum, der aus 4 Punkten besteht? JA! Für $\mathbb{K} = \mathbb{Z}_2$ ist $\mathbb{K}^2 = (\mathbb{Z}_2)^2$ ein Vektorraum; Anzahl von Punkten in $\mathbb{K}^2$ ist die Anzahl von $2-$Zeiligen Vektoren mit sodass Einträge in der 2-Elemetiger Menge $\mathbb{Z}_2$ ist, also 4.

Noch eine Frage für Sie: Gibt es einen Vektorraum, der aus 6 Punkten besteht? Nein; ist aber nicht trivial (in dem Fall muss $\mathbb{K}$ endlich sein; man kann zeigen, dass $\#\ \mathbb{K}$ ein Primzahlpotenz ist; und deswegen muss die Anzahl von Elementen in einem endlichen Vektorraum Primzahlpotenz sein und kann deswegen nicht 6 sein.