

1. systematische Lösung mit dem Euklidischen Algorithmus:

$$\begin{array}{r}
 13 = 1 \cdot 8 + 5 \\
 5 = 1 \cdot 13 - 1 \cdot 8 \\
 \hline
 8 = 1 \cdot 5 + 3 \\
 3 = 8 - 1 \cdot 5 = 8 - (13 - 8) = 2 \cdot 8 - 13 \\
 \hline
 5 = 1 \cdot 3 + 2 \\
 2 = 5 - 3 = 13 - 8 - (2 \cdot 8 - 13) = 2 \cdot 13 - 3 \cdot 8 \\
 \hline
 3 = 1 \cdot 2 + 1 \\
 1 = 3 - 2 = (2 \cdot 8 - 13) - (2 \cdot 13 - 3 \cdot 8) = 5 \cdot 8 - 3 \cdot 13
 \end{array}$$

Die letzte Gleichung bedeutet gerade

$$\bar{1} = \bar{8} \cdot \bar{5}$$

in  $\mathbb{Z}/13\mathbb{Z}$ . D.h.  $\bar{5}$  ist das gesuchte multiplikative Inverse.

2. Die Basiswechselabbildung  $S$  ist die Abbildung, welche die neuen Basisvektoren (in der alten Basis ausgedrückt) als Spalten enthält. Wir haben hier also:

$$S = \begin{pmatrix} -1 & 1 & 0 \\ 1 & 1 & 1 \\ -2 & 1 & -1 \end{pmatrix}.$$

Die Matrix der Abbildung  $A$  bzgl. der neuen Basis ist dann

$$S^{-1}AS = ?$$

Wir müssen dazu die Matrix  $S$  invertieren, was am effizientesten mit dem Gaussverfahren geht:

$$\begin{array}{ccc|ccc}
 -1 & 1 & 0 & 1 & 0 & 0 \\
 1 & 1 & 1 & 0 & 1 & 0 \\
 -2 & 1 & -1 & 0 & 0 & 1 \\
 \hline
 -1 & 1 & 0 & 1 & 0 & 0 \\
 0 & 2 & 1 & 1 & 1 & 0 \\
 0 & -1 & -1 & -2 & 0 & 1 \\
 \hline
 1 & -1 & 0 & -1 & 0 & 0 \\
 0 & 1 & 1 & 2 & 0 & -1 \\
 0 & 2 & 1 & 1 & 1 & 0 \\
 \hline
 1 & -1 & 0 & -1 & 0 & 0 \\
 0 & 1 & 1 & 2 & 0 & -1 \\
 0 & 0 & -1 & -3 & 1 & 2
 \end{array}$$

$$\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 0 & -1 \\ 0 & 0 & 1 & 3 & -1 & -2 \end{array}$$

$$\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 1 \\ 0 & 0 & 1 & 3 & -1 & -2 \end{array}$$

$$\begin{array}{ccc|ccc} 1 & 0 & 0 & -2 & 1 & 1 \\ 0 & 1 & 0 & -1 & 1 & 1 \\ 0 & 0 & 1 & 3 & -1 & -2 \end{array}$$

Daher:

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

An dieser Stelle sollte man überprüfen, dass tatsächlich  $S \cdot S^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$  gilt, und man sich also nicht verrechnet hat. Damit ist

$$S^{-1}AS = \begin{pmatrix} -2 & 1 & 1 \\ -1 & 1 & 1 \\ 3 & -1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 & -1 \\ 4 & -1 & -3 \\ -2 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 & 0 \\ 1 & 1 & 1 \\ -2 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

3.

$$\det \begin{pmatrix} 9 & 8 & 7 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix} = 0$$

4. Der Schnitt der beiden Untervektorräume  $U_1 \cap U_2$  ist die Menge der Vektoren in  $\mathbb{R}^4$  in dem *beide* der definierenden Gleichungen gelten. Wir haben also

$$U_1 \cap U_2 = \left\{ \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} \in \mathbb{R}^4 \left| \begin{pmatrix} 3 & 4 & -1 & 1 \\ 2 & 1 & 5 & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = 0 \right. \right\}.$$

Der gesuchte Raum ist also der Kern der Matrix

$$\begin{pmatrix} 3 & 4 & -1 & 1 \\ 2 & 1 & 5 & -1 \end{pmatrix}.$$

Um diesen zu bestimmen, wenden wir das Gaußverfahren auf diese Matrix an:

$$\begin{pmatrix} 3 & 4 & -1 & 1 \\ 2 & 1 & 5 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 4 & -1 & 1 \\ 0 & -5 & 17 & -5 \end{pmatrix}$$

(wir haben die zweite Zeile mit 3 multipliziert und dann zweimal die erste abgezogen.)  
 Diese Matrix hat Zeilenstufenform. Die ersten beiden Spalten sind nun offensichtlich die Pivotspalten und die restlichen zwei sind freie Parameter. Wir vereinfachen weiter:

$$\begin{pmatrix} 15 & 20 & -5 & 5 \\ 0 & -5 & 17 & -5 \end{pmatrix}$$

$$\begin{pmatrix} 15 & 0 & 63 & -15 \\ 0 & -5 & 17 & -5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & \frac{21}{5} & -1 \\ 0 & 1 & -\frac{17}{5} & 1 \end{pmatrix}$$

Wir bekommen nun durch Rückwärtseinsetzen:

$$\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = z \cdot \begin{pmatrix} -\frac{21}{5} \\ \frac{17}{5} \\ 1 \\ 0 \end{pmatrix} + w \cdot \begin{pmatrix} 1 \\ -1 \\ 0 \\ 1 \end{pmatrix}$$

D.h. eine Basis des Schnittes ist (wir multiplizieren noch den ersten Vektor mit 5) gegeben durch die Vektoren:

$$\begin{pmatrix} -21 \\ 17 \\ 5 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ 1 \end{pmatrix}.$$

Beachten Sie, dass eine Basis keineswegs eindeutig ist! Wenn Sie zwei linear unabhängige Vektoren gefunden haben, die die beiden Gleichungen oben erfüllen, dann ist Ihr Ergebnis richtig.

5. Die Vereinigung zweier Untervektorräume ist (im Gegensatz zu Ihrem Schnitt) im allgemeinen kein Untervektorraum. Gegenbeispiel:

$$U_1 = \mathbb{R} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \subset \mathbb{R}^2$$

und

$$U_2 = \mathbb{R} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \subset \mathbb{R}^2$$

sind die beiden Koordinatenachsen des  $\mathbb{R}^2$ . Ihre Vereinigung enthält sowohl den Vektor  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  als auch den Vektor  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ . Wäre  $U_1 \cup U_2$  ein Untervektorraum müsste er z.B. auch den Vektor

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

enthalten. Dies ist offensichtlich nicht der Fall.

6. (a) Hierfür gibt es zwei Lösungsmöglichkeiten:

**Erste Lösungsmöglichkeit:**

Wende das Gaussverfahren auf die Matrix

$$\begin{pmatrix} 1 & 5 & 9 & 1 \\ 2 & 6 & 10 & 0 \\ 3 & 7 & 11 & 0 \\ 4 & 8 & 12 & 1 \end{pmatrix}$$

an:

$$\begin{pmatrix} 1 & 5 & 9 & 1 \\ 0 & -4 & -8 & -2 \\ 0 & -8 & -16 & -3 \\ 0 & -12 & -24 & -3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 5 & 9 & 1 \\ 0 & -4 & -8 & -2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 5 & 9 & 1 \\ 0 & -4 & -8 & -2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Diese Matrix hat Zeilenstufenform und offensichtlich sind die 1., 2. und 4. Spalte Pivotspalten. D.h. dass der 1., 2. und 4. der *ursprünglichen* Vektoren zusammen eine Basis bilden, also die Vektoren

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 5 \\ 6 \\ 7 \\ 8 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

**Zweite Lösungsmöglichkeit:**

Wende das Gaussverfahren auf die (transponierte) Matrix

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

an:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -4 & -8 & -12 \\ 0 & -8 & -16 & -24 \\ 0 & -2 & -3 & -3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -4 & -8 & -12 \\ 0 & 0 & 0 & 0 \\ 0 & -2 & -3 & -3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -4 & -8 & -12 \\ 0 & -2 & -3 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -2 & -4 & -6 \\ 0 & -2 & -3 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -2 & -4 & -6 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Die Zeilen dieser Matrix bilden nun eine Basis des aufgespannten Raumes, also

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 3 \end{pmatrix}.$$

Beachten Sie wieder, dass eine Basis keineswegs eindeutig ist! Nur die Anzahl der Vektoren darin ist eindeutig bestimmt.

(b) Um die Vektoren zu einer Basis des  $\mathbb{R}^4$  zu ergänzen, nehmen wir zum Beispiel die Vektoren der ersten Lösung und ergänzen Sie zu einem Erzeugendensystem des  $\mathbb{R}^4$ , indem wir eine bekannte Basis (die Standardbasis!) des  $\mathbb{R}^4$  hinzufügen:

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 5 \\ 6 \\ 7 \\ 8 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Wir werden die Rechnung hier nicht wiederholen. Wie oben bekommt man, dass die ersten 4 Spalten Pivotspalten sind, d.h.

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 5 \\ 6 \\ 7 \\ 8 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

ist eine Basis des  $\mathbb{R}^4$ .

7. Es ist kein allgemeiner Algorithmus bekannt, um einen Erzeuger einer Gruppe  $(\mathbb{Z}/p\mathbb{Z})^*$  zu finden ( $p$  eine Primzahl). Die Wahrscheinlichkeit ist allerdings recht hoch, dass ein zufällig ausgewähltes Element ein Erzeuger ist. In unserem Fall hat die Gruppe  $\mathbb{Z}/5\mathbb{Z}$  überhaupt nur 4 Elemente (entsprechen den Zahlen zwischen 0 und 4, die zu 5 teilerfremd sind, also 1,2,3,4). Versuchen wir  $\bar{2}$ : Die Potenzen sind

$$\bar{2}^1 = \bar{2} \quad \bar{2}^2 = \bar{4} \quad \bar{2}^3 = \bar{3} \quad \bar{2}^4 = \bar{1}.$$

Damit ist klar, dass  $\bar{2}$  ein erzeugendes Element ist und die Abbildung

$$\begin{aligned} \mathbb{Z}/4\mathbb{Z} &\rightarrow (\mathbb{Z}/5\mathbb{Z})^* \\ x &\mapsto \bar{2}^x \end{aligned}$$

ist also ein Isomorphismus. Als Wertetabelle

$$\begin{array}{c|c|c|c} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \hline \bar{1} & \bar{2} & \bar{4} & \bar{3} \end{array}$$

bzw. das Inverse, wie gefordert, als Abbildung  $(\mathbb{Z}/5\mathbb{Z})^* \rightarrow \mathbb{Z}/4\mathbb{Z}$ :

$$\begin{array}{c|c|c|c} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \hline \bar{0} & \bar{1} & \bar{3} & \bar{2} \end{array}$$

*Zusatz:* Das einzige andere erzeugende Element in diesem Fall ist  $\bar{3}$ . Es führt auf den Isomorphismus:

$$\begin{array}{c|c|c|c} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \hline \bar{1} & \bar{3} & \bar{4} & \bar{2} \end{array}$$

bzw. das Inverse, wie gefordert, als Abbildung  $(\mathbb{Z}/5\mathbb{Z})^* \rightarrow \mathbb{Z}/4\mathbb{Z}$ :

$$\begin{array}{c|c|c|c} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \hline \bar{0} & \bar{3} & \bar{1} & \bar{2} \end{array}$$

8. Wir berechnen

$$H \cdot c = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Dies ist die 1. Spalte von  $H$ , d.h. das 1. Bit muss korrigiert werden. Anschliessend streichen wir die letzten 4 Prüfbits und erhalten:

$$(0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1)^T$$

als dekodierten Vektor.

9. Wir berechnen zunächst die Jacobi-Matrix

$$\left( \frac{d}{dx} f(x, y) \quad \frac{d}{dy} f(x, y) \right) = (2 \cdot x + 6 \cdot y + 92; \quad 3 \cdot y^2 + 6 \cdot x + 3)$$

und die Hesse-Matrix

$$\begin{pmatrix} \frac{d^2}{(dx)^2} f(x, y) & \frac{d}{dx} \frac{d}{dy} f(x, y) \\ \frac{d}{dy} \frac{d}{dx} f(x, y) & \frac{d^2}{(dy)^2} f(x, y) \end{pmatrix} = \begin{pmatrix} 2 & 6 \\ 6 & 6 \cdot y \end{pmatrix}$$

Die Extremstellen sind die Nullstellen der Jacobi-Matrix. Um diese zu bestimmen, lösen wir die erste Gleichung nach  $x$  auf und erhalten:

$$x = -3 \cdot y - 46$$

Eingesetzt in die zweite Gleichung:

$$3 \cdot y^2 + 6 \cdot (-3 \cdot y - 46) + 3 = 0$$

vereinfacht

$$y^2 - 6 \cdot y - 91 = 0.$$

Die Lösung mit quadratischer Ergänzung oder "p, q-Formel" ergibt:

$$y_1 = -7 \quad y_2 = 13.$$

und daher

$$x_1 = -25 \quad x_2 = -85.$$

Die Hesse-Matrix an den entsprechenden Punkten ist

$$\begin{pmatrix} 2 & 6 \\ 6 & -42 \end{pmatrix} \quad \begin{pmatrix} 2 & 6 \\ 6 & 78 \end{pmatrix}$$

Die zweite Matrix erfüllt das Kriterium für Positiv-Definitheit, da

$$2 > 0 \quad 2 \cdot 78 - 36 > 0$$

Der Punkt  $(x_2, y_2)$  ist also ein lokales Minimum.

Die erste Matrix erfüllt das Kriterium nicht, da

$$2 \cdot (-42) - 36 < 0.$$

Auch ihr Negatives erfüllt das Kriterium nicht. Der Punkt  $(x_1, y_1)$  ist also ein Sattelpunkt.

10. Wir führen den Euklidischen Algorithmus durch:

$$\begin{array}{r} X^2 + X + 1 \quad : X^2 + 1 = 1 \\ X^2 \quad \quad \quad + 1 \\ \hline +X \end{array}$$

Also:

$$X = (X^2 + X + 1) - (X^2 + 1).$$

$$\begin{array}{r} X^2 + 1 : X = X \\ \hline X^2 + 1 \end{array}$$

Also:

$$\begin{aligned} 1 &= (X^2 + 1) - X \cdot X = (X^2 + 1) - ((X^2 + X + 1) - (X^2 + 1)) \cdot X \\ &= -X \cdot (X^2 + X + 1) + (X + 1)(X^2 + 1). \end{aligned}$$

11. Wir kombinieren die 1 aus 9 und 10, z.B. mit dem Euklidischen Algorithmus, oder indem wir raten:

$$1 = 10 - 9.$$

d.h.  $10 \equiv 0 \pmod{9}$  und  $10 \equiv 1 \pmod{9}$ , sowie  $-9 \equiv 0 \pmod{10}$  und  $-9 \equiv 1 \pmod{10}$ . Daher bekommen wir eine Lösung durch

$$x = 10 \cdot 10 + 9 \cdot (-9) = 19.$$

Sie ist eindeutig modulo  $9 \cdot 10 = 90$  bestimmt.

12. Es handelt sich um eine Spiegelung an der Achse, die vom Vektor  $\begin{pmatrix} \cos(\alpha/2) \\ \sin(\alpha/2) \end{pmatrix}$  aufgespannt wird. Beweis:

$$\begin{aligned} \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix} \cdot \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix}. \end{aligned}$$

Die Matrix vertauscht also die Vektoren  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  und  $\begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix}$ , daher bleibt der Vektor

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix} = c \begin{pmatrix} \cos(\alpha/2) \\ \sin(\alpha/2) \end{pmatrix}$$

fest (und damit auch  $\begin{pmatrix} \cos(\alpha/2) \\ \sin(\alpha/2) \end{pmatrix}$ ). Hier ist  $c$  eine reelle Konstante, die wir auch ausrechnen könnten, indem wir die Länge des Vektors auf der linken Seite bestimmen.

Die Matrix vertauscht auch die Vektoren  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  und  $\begin{pmatrix} -\sin(\alpha) \\ \cos(\alpha) \end{pmatrix}$  und multipliziert diese mit -1. Daher wird auch der Vektor (welcher auf dem vorigen senkrecht steht)

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} -\sin(\alpha) \\ \cos(\alpha) \end{pmatrix} = c' \begin{pmatrix} -\sin(\alpha/2) \\ \cos(\alpha/2) \end{pmatrix}$$

mit -1 multipliziert. Und damit auch  $\begin{pmatrix} -\sin(\alpha/2) \\ \cos(\alpha/2) \end{pmatrix}$ .