

Zahlentheorie und Matrizenrechnung

Jahrgang 4 - Semester 2 - Schularbeit 4

Markus Reichl

12. Juni 2017

Inhaltsverzeichnis

1	Zahlentheorie	2
1.1	Einführung	2
1.1.1	Kongruenz	2
1.2	Square and Multiply	2
1.3	Kodierung und Dekodierung	3
1.3.1	Cäsar	3
1.3.2	RSA	3
2	Matrizenrechnung	5
2.1	Grundlagen Vektoren	5
2.1.1	Typen	5
2.1.2	Rechenregeln	6
2.2	Grundlagen Matrizen	7
2.2.1	Rechenregeln	8
2.2.2	Determinanten	10
2.3	Gauß Algorithmus	12
2.4	Grafik im 2-dimensionalen Raum	14
2.4.1	Anwendung	15

1 Zahlentheorie

1.1 Einführung

Es sei x mit $x \in \mathbb{N}$ eine beliebige natürliche Zahl mit $n \geq 2$ mit $n \in \mathbb{N}$. Dann gelte:

$$x = q * n + r$$

n ... Modul

q ... $\text{int}(x/n)$, $q \in \mathbb{N}$

r ... Nicht negativer Rest

Die Kurzschreibweise zur Berechnung von r lautet

$$r = x \bmod n \hat{=} r = x - n * q$$

Für Modulo n existieren genau n Restklassen

$$\{0, 1, 2, \dots, n - 1\}$$

1.1.1 Kongruenz

2 natürliche Zahlen sind kongruent, wenn diese denselben, nicht negativen, Rest haben.

$$a \equiv b \rightarrow a \% n = b \% n$$

Regeln

Kongruenzen können multipliziert werden

$$a \equiv b \text{ und } c \equiv d \rightarrow a * c \equiv b * d$$

Kongruenzen können zu gleichen Potenzen erhöht werden

$$a \equiv b \rightarrow a^k \equiv b^k$$

1.2 Square and Multiply

Bei dieser Methode wird der Exponent in 2er Potenzen zerlegt.

Bsp.: $9^{23} \bmod 7$

$$9^{23} = 9^{16} * 9^4 * 9^2 * 9$$

$$9 \equiv 2$$

Die Potenzregel kann angewandt werden um die weiteren Potenzen zu bestimmen.

$$9^2 \equiv 2^2 = 4$$

$$9^4 \equiv 2^4 = 16 \equiv 2$$

$$9^{16} \equiv 2^4 = 16 \equiv 2$$

Anhand der Faktorregel können nun die Kongruenzen als Faktoren eingesetzt werden.

$$9^{23} \equiv 2 * 4 * 2 * 2 = 32$$

$$9^{23} \equiv 4$$

1.3 Kodierung und Dekodierung

Symmetrisch Gleicher Schlüssel für Ver- und Entschlüsselung Bsp.: Cäsar

Asymmetrisch Verschiedene Schlüssel für Ver- und Entschlüsselung Bsp.: RSA

1.3.1 Cäsar

	B	R	A	V	O	
	↓↑	↓↑	↓↑	↓↑	↓↑	
	02	18	01	22	15	
+(c % 27)	↓↑	↓↑	↓↑	↓↑	↓↑	+27 - (c % 27)
	10	26	11	03	23	
	↓↑	↓↑	↓↑	↓↑	↓↑	
	J	Z	I	C	W	

1.3.2 RSA

1. A wählt 2 Primzahlen p, q als **Private Key**
2. A wählt eine Zahl e (Encrypt), welche teilerfremd¹ zu $(p - 1) * (q - 1)$ ist
3. A veröffentlicht seinen **Public Key** bestehend aus der Zahl e und dem Produkt n aus

$$n = p * q$$

4. B möchte eine Nachricht an A senden und wandelt diese in eine Zahl um. Diese Zahl wird in x gleich lange Blöcke zerlegt. Die resultierende Nachricht y lautet

$$y = x^e \mod n$$

5. A berechnet den Private Key d (Decrypt) aus

$$d = \frac{1 + k(p - 1)(q - 1)}{e} \quad k \in \mathbb{N}$$

6. A erhält die Nachricht y und ermittelt x aus

$$x = y^d \mod n$$

¹ Zwei natürliche Zahlen sind teilerfremd, wenn es keine natürliche Zahl außer Eins gibt, welche beide Zahlen teilt.

Bsp.: "BRAVO"

1. B möchte die Nachricht "BRAVO" an A senden und findet dafür den Public Key

$$n = 1147 \text{ mit } e = 29$$

2. Zur Verschlüsselung wird die Nachricht in Zahlen umgewandelt und in gleich lange Blöcke unterteilt. Der letzte Block wird an der rechten Seite mit 0 aufgefüllt.

B	R	A	V	O
↓	↓	↓	↓	↓
02	18	01	22	15
↓	↓	↓	↓	↙
021	801	221	500	

3. Nun werden die einzelnen Blöcke anhand des Public Keys kodiert. Diesmal werden zu kurze Blöcke an der linken Seite mit 0 aufgefüllt.

$$y_n = x_n^e \mod n$$

021	801	221	500
↓	↓	↓	↓
003	533	628	535

4. A empfängt die Nachricht und nutzt seinen Private Key $p = 31, q = 37$ und findet den Schlüssel d aus

$$d = \frac{1 + k(p-1)(q-1)}{e}$$

k wird dabei in natürlichen Schritten gesteigert, bis d ganzzahlig ist. Hier bei $k = 4$.

$$d = \frac{1 + 4 * 30 * 36}{29} = 149$$

5. A erhält nun die Nachricht x aus

$$x_n = y_n^d \mod n$$

Zu kurze Blöcke werden von links aufgefüllt.

003	533	628	535		
↓	↓	↓	↓		
021	801	221	500		
↓	↓	↓	↓	↘	
02	18	01	22	15	00
↓	↓	↓	↓	↓	↓
B	R	A	V	O	-

2 Matrizenrechnung

2.1 Grundlagen Vektoren

Vektoren sind gerichtete Größen, definiert durch ihren Betrag und ihre Länge. Sie geben also keine Punkte, sondern eine Richtung an.

$$\vec{a} = \begin{pmatrix} a_x \\ a_y \end{pmatrix}$$

a_x ... Schaft

a_y ... Spitze

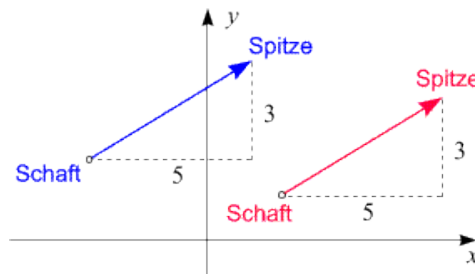


Abbildung 1: Vektoren im \mathbb{R}^2

2.1.1 Typen

Einheitsvektor Vektoren mit der Länge 1 werden als Einheitsvektoren oder auch normierte Vektoren bezeichnet.

$$\vec{a}_E = \frac{\vec{a}}{|\vec{a}|}$$

Inverser Vektor Ein Vektor ist invertiert wenn \vec{a} und $-\vec{a}$ gleich lang aber entgegengesetzt gerichtet sind.

$$\vec{a} = \begin{pmatrix} a_x \\ a_y \end{pmatrix} \rightarrow -\vec{a} = \begin{pmatrix} -a_x \\ -a_y \end{pmatrix}$$

Ortsvektor Ein Vektor vom Ursprung $O(0|0)$ zu einem bestimmten Punkt.

$$\overrightarrow{OP} = \begin{pmatrix} P_x \\ P_y \end{pmatrix}$$

Normalvektor Zwei Vektoren sind aufeinander normal, wenn deren x und y-Koordinaten vertauscht sind und ein Vorzeichen geändert wird.

$$\vec{a} \perp \vec{b} \text{ wenn } \vec{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \text{ und } \vec{b} = \begin{pmatrix} -a_2 \\ a_1 \end{pmatrix} \text{ oder } \vec{b} = \begin{pmatrix} a_2 \\ -a_1 \end{pmatrix}$$

2.1.2 Rechenregeln

Betrag Die Länge eines Vektors ist als dessen Betrag definiert. Dieser kann über den Satz des Pythagoras hergeleitet werden.

$$|\vec{a}| = \sqrt{a_x^2 + a_y^2}$$

Addition und Subtraktion Vektoren werden addiert oder subtrahiert indem deren Elemente nach Zeile addiert bzw. subtrahiert werden.

$$\begin{pmatrix} a_x \\ a_y \end{pmatrix} \pm \begin{pmatrix} b_x \\ b_y \end{pmatrix} = \begin{pmatrix} a_x \pm b_x \\ a_y \pm b_y \end{pmatrix}$$

Skalare Multiplikation Vektoren werden mit Zahlen multipliziert, indem jedes Element einzeln mit dem Faktor multipliziert wird.

$$\begin{pmatrix} a_x \\ a_y \end{pmatrix} * b = \begin{pmatrix} a_x * b \\ a_y * b \end{pmatrix}$$

Skalarprodukt zweier Vektoren Das Skalarprodukt zweier Vektoren ist von der Länge der Vektoren und dem eingeschlossenen Winkel abhängig.

$$\vec{a} * \vec{b} = |\vec{a}| * |\vec{b}| * \cos(\varphi)$$

$$\varphi = \sphericalangle(\vec{a}, \vec{b})$$

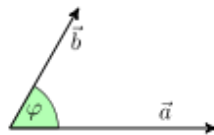


Abbildung 2: Skalarprodukt

Berechnet wird dieses aus

$$\begin{pmatrix} a_x \\ a_y \end{pmatrix} * \begin{pmatrix} b_x \\ b_y \end{pmatrix} = a_x * b_x + a_y * b_y$$

Das Skalarprodukt zweier Vektoren ist genau dann 0, wenn gilt $\cos(\varphi) = 0$ ^I, oder der Betrag eines Vektors 0 ist. In diesem Fall sind die Vektoren zueinander orthogonal.

^I Dies ist sowohl bei 90, als auch bei 270 Grad der Fall

2.2 Grundlagen Matrizen

Eine Matrix vom Typ $(m \times n)$ ist ein Schema aus m Zeilen und n Spalten.

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

a_{mn} ... Element der Matrix

m ... Zeile

n ... Spalte

Zeilenvektor Eine Matrix mit nur einer Zeile.

$$(1 \times 3) \rightarrow A \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

Spaltenvektor Eine Matrix mit nur einer Spalte.

$$(3 \times 1) \rightarrow A \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

Skalar Eine einzelne Zahl kann auch als eine Matrix mit einer Zeile und einer Spalte gesehen werden. Eine solche Matrix nennt man einen Skalar.

$$(1 \times 1) \rightarrow A = 1$$

Quadratische Matrix Die Anzahl der Zeilen ist gleich der Anzahl der Spalten ($m = n$).

$$(2 \times 2) \rightarrow A \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

Diagonalmatrix Alle Elemente außerhalb der Hauptdiagonale sind gleich 0.

$$(3 \times 3) \rightarrow A \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

Einheitsmatrix Alle Elemente der Hauptdiagonale sind gleich 1 und jene außerhalb 0.

$$(3 \times 3) \rightarrow A \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Transponierte Matrix Zeilen und Spalten einer Matrix werden vertauscht. Dabei wird jede Zeile zu einer Spalte.

$$A \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \rightarrow A^T \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$

Symmetrische Matrix Jede Diagonale einer Matrix enthält nur ein Element. Es gilt $A = A^T$.

$$(3 \times 3) \rightarrow A \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix}$$

2.2.1 Rechenregeln

Addition und Subtraktion Die Addition 2er Matrizen A und B ist nur dann definiert, wenn diese vom selben Typen sind ($A_m = B_m$ und $A_n = B_n$).

$$A + B = C \rightarrow A_{mn} \pm B_{mn} = C_{mn}$$

$$A \begin{pmatrix} a_{11} & a_{21} \\ a_{21} & a_{22} \end{pmatrix} \pm B \begin{pmatrix} b_{11} & b_{21} \\ b_{21} & b_{22} \end{pmatrix} = C \begin{pmatrix} a_{11} \pm b_{11} & a_{21} \pm b_{21} \\ a_{21} \pm b_{21} & a_{21} \pm b_{22} \end{pmatrix}$$

Skalare Multiplikation Jedes Element einer Matrix wird mit dem Faktor multipliziert.

$$A \begin{pmatrix} a_{11} & a_{21} \\ a_{21} & a_{22} \end{pmatrix} * b = C \begin{pmatrix} b * a_{11} & b * a_{21} \\ b * a_{21} & b * a_{22} \end{pmatrix}$$

Multiplikation von Matrizen C ist als Produkt von $A * B$ nur dann definiert wenn gilt

$$A(m \times p) \quad \text{und} \quad B(p \times n)$$

Damit ist C eine $(m \times n)$ Matrix definiert als

$$C_{mn} = \sum_{i=1}^p a_{mi} * b_{in}$$

ACHTUNG! Die Multiplikation von Matrizen ist NICHT kommutativ!

$$A \cdot B \neq B \cdot A$$

Beispiel

$$A \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} B \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$$

Zur Berechnung der Matrix $C = A \cdot B$ ist es sinnvoll, die Matrizen versetzt nebeneinander zu schreiben, diese Methode nennt man auch Falk'sches Schema.

Falk'sches Schema

				B	1	2	
					3	4	
					5	6	
					↓	↓	
A							
1	2	3	→	c_{11}	c_{12}	$c_{11} = 1 * 1 + 2 * 3 + 3 * 5 = 22$	
4	5	6	→	c_{21}	c_{22}	$c_{12} = 1 * 2 + 2 * 4 + 3 * 6 = 28$	
7	8	9	→	c_{31}	c_{32}	$c_{21} = 4 * 1 + 5 * 3 + 6 * 5 = 49$	
						$c_{22} = 4 * 2 + 5 * 4 + 6 * 6 = 64$	
						$c_{31} = 7 * 1 + 8 * 3 + 9 * 5 = 76$	
						$c_{32} = 7 * 2 + 8 * 4 + 9 * 6 = 100$	

$$A \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \cdot B \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} = C \begin{pmatrix} 22 & 28 \\ 49 & 64 \\ 76 & 100 \end{pmatrix}$$

2.2.2 Determinanten

Definition

‘Eine Determinante ist eine Zahl, die einer quadratischen Matrix zugeordnet ist. Man kann die Determinante jeder allgemeinen Matrix vom Typ $(m \times m)$ bestimmen“ [1]

Eigenschaften

- Die Determinante einer Matrix A ist gleich jener der transponierten Matrix A^T .

$$|A| = |A^T|$$

- Der Wert einer Determinante ist unabhängig von der Entwicklungszeile / -spalte.
- Eine Determinante ist gleich Null, wenn einer der folgenden Fälle zutrifft:
 - eine Zeile / Spalte besteht aus lauter Nullen
 - zwei Zeilen / Spalten sind gleich
 - eine Zeile / Spalte ist eine Linearkombination anderer Zeilen/Spalten
- Vertauscht man eine gerade Anzahl an Zeilen / Spalten ändert sich das Vorzeichen der Determinante.
- Multipliziert man eine Zeile / Spalte mit einer Zahl, wird die Determinante ebenfalls multipliziert.
- Die Determinante des Produktes zweier Matrizen entspricht dem ihrer Determinanten.

$$|A \cdot B| = |A| \cdot |B|$$

Berechnung

2×2 (Diagonalen) Die Determinante einer Matrix 2×2 entspricht dem Produkt der Hauptdiagonale abzüglich des Produktes der Nebendiagonale.

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = a * d - b * c$$

3×3 (Regel von Sarrus) Bei dieser Regel werden zu Beginn die ersten beiden Spalten noch einmal neben die Determinante geschrieben.

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \rightarrow \begin{array}{ccc|cc} a & b & c & a & b \\ d & e & f & d & e \\ g & h & i & g & h \end{array}$$

Jetzt bildet man die Produkte der Elemente der drei Diagonalen, welche von links oben nach rechts unten verlaufen. Diese Produkte werden addiert.

$$a * e * i + b * f * g + c * d * h$$

Von dieser Menge werden nun die Produkte der Elemente der drei Diagonalen, welche von links unten nach rechts oben verlaufen, abgezogen.

$$-g * e * c - h * f * a - i * d * b$$

Die Formel zur Berechnung einer 3×3 Determinante lautet also wie folgt.

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - gec - hfa - idb$$

2.3 Gauß Algorithmus

Ein lineares Gleichungssystem in n Gleichungen und n Unbekannten ist als Matrix genau dann eindeutig lesbar wenn $|A| \neq 0$ gilt.

Als Beispiel ist folgendes lineares Gleichungssystem in 3 Gleichungen und 3 Unbekannten gegeben. Dieses wird anschließend in einer Koeffizientenmatrix tabellarisch dargestellt.

$$\begin{array}{lllll} \text{I} & x & +2y & +3z & = 2 \\ \text{II} & x & +y & +z & = 2 \\ \text{III} & 3x & +3y & +z & = 0 \end{array}$$

Koeffizientenmatrix

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

Multiplikation Zeilen dürfen beliebig multipliziert und dividiert werden.

Addition / Subtraktion Zeilen dürfen voneinander addiert und subtrahiert werden.

Ziel des Gauß Algorithmus ist es nun anhand der Rechenregeln alle Werte über oder unter der Hauptdiagonalen auf 0 zu bringen.

$$\begin{array}{c} \downarrow \\ \begin{pmatrix} \times & \times & \times \\ 0 & \times & \times \\ 0 & 0 & \times \end{pmatrix} = \begin{pmatrix} \times \\ \times \\ \times \end{pmatrix} \end{array}$$

Durch dieses Verfahren wird pro Zeile eine steigende Zahl an Koeffizienten gleich 0, wodurch deren Variablen eliminiert werden.

Die häufigste Vorgehensweise ist dabei die erste Spalte der ersten Zeile auf 1 zu bringen und anschließend die Zeile mit einer konstanten zu multiplizieren, um diese von der nächsten Zeile abziehen zu können.

$$\begin{array}{c}
 \downarrow \\
 II - I \rightarrow \begin{pmatrix} 0 & -1 & -2 \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix} \\
 III - 3 * I \rightarrow \begin{pmatrix} 0 & -3 & -8 \end{pmatrix} = \begin{pmatrix} -6 \end{pmatrix} \\
 \downarrow \\
 \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & -3 & -8 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ -6 \end{pmatrix} \\
 \downarrow \\
 III - 3 * II \rightarrow \begin{pmatrix} 0 & 0 & -2 \end{pmatrix} = \begin{pmatrix} -6 \end{pmatrix}
 \end{array}$$

Die neue Matrix kann nun einfach weiter verwendet werden. So kann die 2. Spalte der 3. Zeile auf 0 gebracht werden, indem die 2. Zeile mit 3 multipliziert, von der 3. Zeile abgezogen wird.

$$\begin{array}{c}
 \downarrow \\
 \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & 0 & -2 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ -6 \end{pmatrix} \\
 \downarrow \\
 \begin{array}{rcll}
 \text{I} & x & +2y & +3z & = 2 \\
 \text{II} & & -y & -2z & = 0 \\
 \text{III} & & & -2z & = -6
 \end{array} \\
 \downarrow \\
 z = 3, \quad y = -6, \quad x = 5
 \end{array}$$

2.4 Grafik im 2-dimensionalen Raum

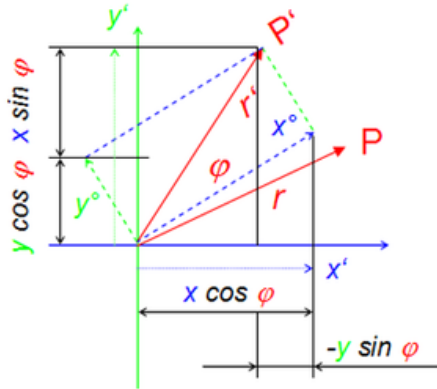


Abbildung 3: Drehung im \mathbb{R}^2

Gegeben sei ein Punkt $P(x|y)$ in einem Koordinatensystem. Dieser Punkt soll um den Ursprung $(0|0)$ um den Winkel φ gedreht werden.

$$P(x|y) \quad x = r * \sin(\alpha)$$

$$y = r * \cos(\alpha)$$

$$P'(x'|y') \quad x' = r * \sin(\alpha + \varphi)$$

$$y' = r * \cos(\alpha + \varphi)$$

↓

Additionstheorem

$$\sin(\alpha \pm \beta) = \sin(\alpha) * \cos(\beta) \pm \cos(\alpha) * \sin(\beta)$$

$$\cos(\alpha \pm \beta) = \cos(\alpha) * \cos(\beta) \pm \sin(\alpha) * \sin(\beta)$$

↓

$$P'(x'|y') \quad x' = r * \sin(\alpha) * \cos(\varphi) + r * \cos(\alpha) * \sin(\varphi)$$

$$y' = r * \cos(\alpha) * \cos(\varphi) - r * \sin(\alpha) * \sin(\varphi)$$

↓

$$P'(x'|y') \quad x' = x * \cos(\varphi) + y * \sin(\varphi)$$

$$y' = y * \cos(\varphi) - x * \sin(\varphi)$$

↓

$$P' \begin{pmatrix} x' \\ y' \end{pmatrix} = D \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix} * P \begin{pmatrix} x \\ y \end{pmatrix}$$

Drehmatrix

Beschreibt eine Drehung um den Ursprung um den Winkel φ .

$$D = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

Spiegelungsmatrix

Beschreibt die Spiegelung an einer Geraden, durch den Ursprung mit der Steigung φ .

$$Sp = \begin{pmatrix} \cos(2\varphi) & \sin(2\varphi) \\ \sin(2\varphi) & -\cos(2\varphi) \end{pmatrix}$$

Streckungsmatrix

Beschreibt eine Streckung um S_x in x-Richtung und um S_y in y-Richtung.

$$St = \begin{pmatrix} S_x & 0 \\ 0 & S_y \end{pmatrix}$$

2.4.1 Anwendung

1. Verschieben des Ankerpunktes zum Ursprung.

$$A' = A - \overrightarrow{OB}$$

2. Matrix anwenden durch Multiplikation.

$$A'' = D \cdot A \quad A'' = Sp \cdot A \quad A'' = St \cdot A$$

3. Zurückschieben um den Ortsvektor des Ankerpunktes.

$$A''' = A + \overrightarrow{OB}$$

Literatur

[1] <http://www.mathe-online.at/materialien/klaus.berger/files/Matrizen/determinante.pdf>

[2] <https://de.wikipedia.org/wiki/Skalarprodukt>

Abbildungsverzeichnis

1	http://www.mathe-online.at/mathint/vect1/grafiken/vektor1.gif	5
2	https://de.wikipedia.org/wiki/Skalarprodukt#/media/File:Dot-product-3.3.svg	6
3	http://systemdesign.ch/wiki/Drehung	14