Von Caesar zu Matrizen – Drehungen und Spiegelungen

Hannes Stoppel & Benjamin Rott; Gladbeck und Köln

Illustrationen von W. Zettlmeier

II/B

Abb. 1: Schon Gaius Julius Caesar (13. Juli 100 v. Chr. – 15. März 44 v. Chr.) verwendete Verschlüsselungsalgorithmen

Klasse: 11–13

Dauer: 4–7 Stunden

Inhalt: Drehungen und Spiegelung mithilfe von Matrizen beschreiben und diesen Formalismus anwenden, um Aufgaben aus der Kryptografie zu lösen;

Erläuterung kryptografischer Verfahren

Umgang mit dem Bogenmaß üben

Feststellen, dass für die Verknüpfung von Drehungen und Spiegelungen das Kommutativgesetz nicht gilt

Ihr Plus: Der Beitrag dient als Einstieg in die Matrizenrechnung und bietet eine interessante Anwendung von Drehungen und Spiegelungen als linearen Abbildungen. Die Reihe eignet sich zur Festigung des Umgangs mit dem Bogenmaß.

Codierung und Decodierung spielen seit weit über tausend Jahren eine große Rolle – oft im militärischen Bereich, spätestens seit **Online-Banking** und verschlüsselten Smartphone-Nachrichten auch im heutigen täglichen Leben. Bereits Julius Caesar verschlüsselte Nachrichten. Das Verfahren von Caesar lässt sich mithilfe von Matrizen mathematisch beschreiben. Hiermit ergibt sich eine Möglichkeit, Nachrichten rechnerisch zu ver- und zu entschlüsseln. Außerdem lässt sich dieses Verfahren dann mit geringem Aufwand variieren und so deutlich sicherer gestalten.

II/B

Didaktisch-methodische Hinweise

In dieser Unterrichtssequenz geht es um die Beschreibung von **Drehungen** und **Spiegelungen** durch **Matrizen**. Hierbei zeigt sich eine Brücke zwischen der Geometrie und der Algebra. Auf diese Art lassen sich einerseits Berechnungen mit bestimmten Matrizen geometrisch beschreiben. Andererseits lassen sich geometrische Operationen durch Berechnungen bzw. Abbildung darstellen. Bei Drehungen und Spiegelungen und damit bei den Berechnungen mit entsprechenden Matrizen erkennt man, dass entgegen typischer Rechenoperationen mit Zahlen *nicht* das Kommutativgesetz gilt.

Mithilfe der Unterrichtssequenz lässt sich die Rechnung im **Bogenmaß** festigen. Als Nebeneffekt ergibt sich eine Erkundung der **Modulo-Rechnung** auf anschauliche Art. Außerdem können **Sicherheitsstandards verschiedener Kryptosysteme** erkundet und diskutiert werden.

Vorbereitung zur Binnendifferenzierung

Laminieren Sie die **Tipp-Karten** zu den Arbeitsblättern und legen Sie sie auf dem Lehrerpult aus. Tipps auf den Aufgabenblättern sollten Ihren Schülern zur Verfügung stehen, da sie zur Lösung der entsprechenden Aufgaben nötig sind. Die zusätzlichen Tippkarten hingegen sind als Hilfe für leistungsschwächere Schüler gedacht, die ansonsten mit den Aufgaben nicht zurechtkommen würden.

Kopieren Sie die **Tabellen 1 bis 8 (CD-ROM 72)** so, dass sie für die Schüler in ausreichender Zahl vorhanden sind. Sollten sämtliche Aufgaben ausschließlich in der Schule bearbeitet werden, so reicht es aus, Tabellen für jede Gruppe einmal zu kopieren. Um Kopien zu sparen, können Ihre Schüler die Tabellen 1 bis 4 auch abzeichnen.

Einzelarbeit, Partnerarbeit oder Gruppenarbeit?

Die folgende Tabelle gibt die möglichen Arbeitsformen an. Hierbei bedeuten

e: Einzelarbeit, p: Partnerarbeit, g: Gruppenarbeit.

Ferner ist in dieser Tabelle notiert, ob der Einsatz eines dynamischen Geometriesystems (**DGS**) zur Lösung von Aufgaben notwendig ist. DGS oder Grafik-Taschenrechner (**GTR**) sowie Computer-Algebra-Systeme (**CAS**) lassen sich sinnvoll in weiteren Aufgaben einsetzen. Da GTR oder CAS häufig – wenngleich unter Umständen nur über das Handy – zur Verfügung stehen und die Schüler die Medien hiermit frei wählen können, wurde hierauf nicht an jeder Stelle hingewiesen.

Material	**M 1**	**M 2**		**M 3**		**M 5**			**M 6**	**M 7**		**M 8**	
Aufgabe	1	1	2	1	2	1	2	3		1	2	1	2
Arbeitsform	e	e	e	e	e	g	e	p	e	e	e	g	g
DGS nötig				x						x	x		

Abb. 2: Übersicht der Arbeitsformen im Beitrag

Basteltipp

Auf **CD-ROM 72** finden Sie eine Bastelvorlage für die Caesar-Scheibe. Drucken Sie sie auf etwas festerem Karton aus.

II/B

Auf einen Blick

Teil I: Drehungen kann man mit Matrizen beschreiben

Material	Thema	Stunde
M 1	**Es dreht sich um Caesar – ein einfaches Verfahren** Einstieg: das Caesar-Verfahren kennenlernen	1./2.
M 2	**Caesar im Koordinatensystem – Rechnen modulo 31** Die Buchstaben der Scheibe Koordinaten zuorden Rechnen modulo 31	
M 3	**Caesar mit virtueller Scheibe – mit Drehmatrizen arbeiten** Die Wirkung von Drehmatrizen kennenlernen	3.
M 4	**Exkurs: Drehung mithilfe von Matrizen** Definition einer Drehmatrix	HA
M 5	**Wie sicher ist das Verfahren? – Übungsaufgaben** Anhand von Übungen erkennen, dass man das Caesar-Verfahren leicht entschlüsseln kann	4.

Teil II: Auch Spiegelungen lassen sich mit Matrizen beschreiben

Material	Thema	Stunde
M 6	**Es spiegelt sich wieder – die Caesar-2-Codierung** Das Caesar-Verfahren durch zusätzliche Spiegelung verbessern	5./6.
M 7	**Die Spiegelung mithilfe von Matrizen** Auch die Spiegelung lässt sich durch eine Matrix beschreiben	
M 8	**Spiegelung mithilfe von Matrizen – Übungsaufgaben** Das Gelernte durch Übungsaufgaben vertiefen	7.

Hilfe für leistungsschwache Schüler

Material	Thema	Stunde
M 9	**Tippkarten** Hilfe für leistungsschwache Schüler	

Minimalplan

Wenn Sie wenig Zeit haben, beschränken Sie sich auf **Teil I**, das einfache Caesar-Verfahren und die Drehmatrizen. Den **Exkurs** zu Drehmatrizen lesen die Schüler als Hausaufgabe.

Sollten Ihre Schüler bereits mit der Multiplikation von Matrizen und Vektoren vertraut sein, können Sie auf das Exkurs-Arbeitsblatt „Drehung mithilfe von Matrizen“ verzichten.

II/B

M 1 Es dreht sich um Caesar – ein einfaches Verfahren

Das Thema „Verschlüsselung“ ist nicht erst seit E-Mails und Online-Banking, sondern schon lange wichtig. Nicht zuletzt im militärischen Bereich sollten Nachrichten, die möglicherweise abgefangen wurden, vom Feind nicht gelesen werden können. Vor ca. 2000 Jahren hat der damalige Feldherr Julius G. Caesar ein Verfahren zur Verschlüsselung ge-nutzt, das heutzutage nach ihm benannt ist. Dieses wird im Folgenden näher betrachtet

Allgemein lässt sich der Verlauf in einem Codierungs-System darstellen durch:

$$\text{Klartext} \xrightarrow{\text{Schlüssel}} \text{Geheimtext} \xrightarrow{\text{Inverser Schlüssel}} \text{Klartext}$$

Man benötigt hierbei

Klartextalphabet, *Geheimtextalphabet*,

Menge der Schlüssel,

Verschlüsselung, *Entschlüsselung*.

© ViewApart/iStock/Getty Images Plus

Abb. 3: Schon Gaius Julius Caesar (13. Juli 100 v. Chr. – 15. März 44 v. Chr.) verwendete Verschlüsselungsalgorithmen.

Bei der Caesar-Verschlüsselung wird jeder Buchstabe um einen vorher festgelegten Wert „verschoben“. Wählt man zum Beispiel eine Verschiebung um drei Buchstaben, wird aus jedem A ein D, aus jedem B ein E und so weiter. Wenn man einen Text auf diese Weise verschlüsselt, wird er unlesbar. Nur wenn man weiß, um wie viel die jeweiligen Buchstaben verschoben wurden und das Ganze rückgängig macht, kann man den Geheimtext lesen.

Aufgabe

a) Wenn man sich nicht aufschreiben möchte, welche Buchstaben bei der Ver- und Entschlüsselung einander zugeordnet werden, oder wenn man nicht immer Buchstaben vor- bzw. rückwärtszählen möchte, kann man sich mit einer sog. **Caesar-Scheibe** behelfen. Eine solche Scheibe besteht eigentlich aus zwei Scheiben, die alle Buchstaben des Alphabets und ein paar weitere Zeichen enthalten und gegeneinander verdreht werden können (siehe Abb. 4).

Beschreiben Sie das Caesar-System zunächst anschaulich unter Zuhilfenahme der Caesar-Scheibe.

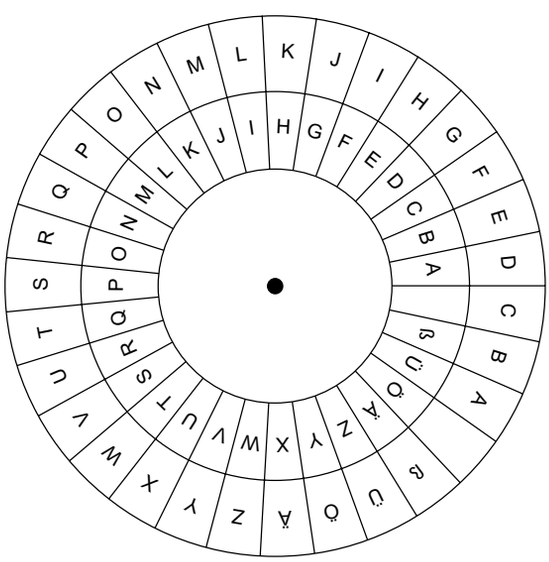

Abb. 4: Die Caesar-Scheibe: Klartextbuchstaben: innen; Geheimtextbuchstaben: außen

b) Falls Sie mit dem Verfahren noch nie gearbeitet haben, verschlüsseln Sie nun ein Wort (z. B. „CAESAR“) zunächst mit dem in der Abbildung 4 eingestellten Schlüssel und dann mit einem beliebig gewählten Schlüssel (d. h. durch Verdrehen der äußeren Scheibe in eine andere feste Zuordnung der Buchstaben, die später auch als Zahl zwischen 0 und 30 abgekürzt wird). Jemand anderes soll versuchen, das Wort zu entschlüsseln.

c) Tragen Sie Ihre Beschreibung in Tabelle 1 ein.

Tipp Tabelle 1 gibt Ihnen Ihr Lehrer.

M 3 Caesar mit virtueller Scheibe – mit Drehmatrizen arbeiten

Mithilfe von Matrizen lässt sich eine **Drehung** mathematisch beschreiben. Wenn wir also eine Matrix (die Drehung) auf einen Vektor (einen Buchstaben) anwenden, erhalten wir einen anderen Vektor (den verschlüsselten Buchstaben).

Aufgabe 1

a) Wenden Sie folgende Matrizen auf die Ortsvektoren der Punkte $(1|0), (0|1), (-1|0)$ und $(0|-1)$ von Punkten des Einheitskreises an.

(1) $A_{\frac{\pi}{2}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$,

(2) $A_{\pi} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$,

(3) $A_{\frac{3\pi}{2}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Beschreiben Sie die Wirkung der Multiplikation auf die Ortsvektoren

$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

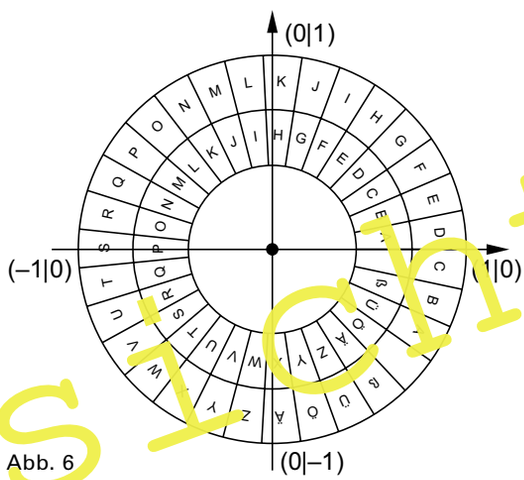

Abb. 6

Machen Sie sich dies an Abb. 6 oder an einem Modell der Caesar-Scheibe deutlich.

Die Matrizen wurden mit Indizes (z. B. „π“) bezeichnet. Können Sie anhand Ihrer Beobachtungen begründen, warum diese Indizes sinnvoll gewählt wurden?

Tipp 1 Im Bogenmaß entspricht π einem Winkel von $180°$.

Tipp 2 Eine Matrix, durch die sich eine Drehung beschreiben lässt, nennt man Drehmatrix.

Überprüfen Sie Ihre Vermutung durch die Anwendung der Matrizen auf die Ortsvektoren zu den Punkten aus Tabelle 4 (**CD-ROM 72**). Stellen Sie dabei die Drehungen mithilfe einer DGS grafisch dar.

b) Mit den Punkten $(1|0)$ und $(0|1)$ sollen Drehungen von Hand oder mithilfe einer DGS durch Matrizen dargestellt werden.

Mithilfe welcher Matrix lässt sich eine Drehung beschreiben? Führen Sie dies für die Winkel $\frac{1}{8}\pi$ und $\frac{5}{9}\pi$ durch.

Überprüfen Sie Ihr Verfahren mithilfe der Ergebnisse aus Aufgabenteil a).

Wie wir gesehen haben, lassen sich Codierungen mithilfe von Matrizen durchführen. Das Codieren reicht jedoch nicht aus, man muss die empfangene Nachricht auch decodieren, um den Text lesen zu können. Für uns bedeutet dies, die Drehung umzukehren.

Aufgabe 2

Bestimmen Sie die Umkehrung einer Drehung um den Winkel α.

M 5 Wie sicher ist das Verfahren? – Übungsaufgaben

Auf den letzten Aufgabenblättern wurden Verfahren entwickelt, mit denen Drehungen mithilfe von Matrizen durchgeführt und – als Drehung in entgegengesetzter Richtung bzw. als Ergänzungsdrehung zu 360° – rückgängig gemacht werden können. Um solche Drehungen auf das Codieren und Decodieren zu übertragen, müssen wir berücksichtigen, dass die Drehungen auf das Alphabet einzuschränken sind. Wir betrachten also Drehungen um ein ganzzahliges Vielfaches von $\frac{360°}{31}$.

Abb. 7: Verschlüsseln am PC

Nach dem Leerzeichen kommen wir wieder zurück zum **A**. Dazu verwenden wir die Koordinaten der zu den Buchstaben gehörenden Punkte in den **Tabellen 4 bis 7** (**CD-ROM 72**) und wenden eine Drehung auf sie an.

Aufgabe 1

a) Definieren Sie sich eine Matrix, um die Codierung nach Caesar durch Verdrehen um fünf Buchstaben gegen den Uhrzeigersinn zu beschreiben. Codieren und decodieren Sie damit unter Anwendung digitaler Medien (beispielsweise GeoGebra) das Wort

HALLO.

Führen Sie die Codierung für verschiedene Verdrehungen durch.

Wie lässt sich der allgemeine Fall einer Verdrehung um k Buchstaben durch eine Matrix beschreiben?

Notieren Sie die Verschlüsselung und die Entschlüsselung in Tabelle 2 (**CD-ROM 72**).

b) Codieren und decodieren Sie

CAESAR.

Erklären Sie Schritte und Schwierigkeiten der Codierung und Decodierung am Bild eines Einheitskreises.

c) Diskutieren und beheben Sie die in Teil b) entdeckten Probleme in kleinen Gruppen mit Ihren Mitschülern. Ergänzen Sie Tabelle 2 um entsprechende Schritte in der Verschlüsselung und der Entschlüsselung.

Aufgabe 2

Der folgende Text wurde mit dem Caesar-Verfahren verschlüsselt. Bestimmen Sie den Schlüssel. Entschlüsseln Sie hiermit den folgenden Text:

UNRLQÜIDßITWJLTNW

Aufgabe 3

Diskutieren Sie die Sicherheit des Codier- und Decodierverfahrens nach Caesar bezüglich des „Knackens“ einer Nachricht durch fremde Personen. Werfen Sie hierbei auch einen Blick auf die Häufigkeit von Buchstaben in der deutschen Sprache.

Tipp Häufigkeitsanalysen beziehen sich immer auf längere Texte.

II/B

M 7 Die Spiegelung mithilfe von Matrizen

Der Schritt der Caesar-2-Codierung ist umständlich an einer Scheibe machbar und schwer vorstellbar. Hilfreich wäre es, ähnlich wie Drehungen auch Spiegelungen mithilfe von Matrizen untersuchen zu können. Dafür müssen wir uns zunächst anschauen, wie **Matrizen von Spiegelungen an Ursprungsgeraden** aussehen.

Zunächst elementare Beispiele: Weil sich beliebige Vektoren als Linearkombination der Basisvektoren

$$v_1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + v_2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

darstellen lassen, betrachten wir wie in **M 3**, Aufgabe 1, Spiegelungen der Basisvektoren.

Aufgabe 1

Erklären Sie mithilfe von Spiegelachsen an Skizzen oder mithilfe digitaler Medien (z. B. GeoGebra) die Wirkungen der durch die folgenden Matrizen beschriebenen Abbildungen auf die Vektoren $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Verwenden Sie ggf. die Abbildung 9 unten.

(1) $A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, (2) $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, (3) $C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Verfahren Sie analog zu Aufgabe 1 a) von Material **M 3**, mit den Matrizen A, B und C.

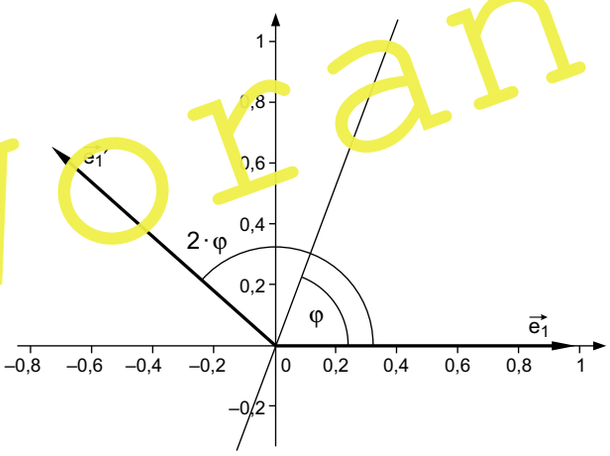

Abb. 9: Bilder der Standardvektoren unter einer Spiegelung;

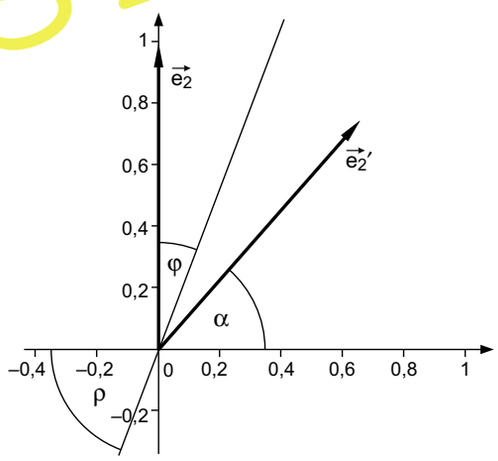

Abb. 10: Der Winkel φ bezeichnet jeweils den Winkel zwischen dem zu spiegelnden Vektor und der Spiegelachse.

Aufgabe 2

Weisen Sie mithilfe obiger Abb. 10 nach, dass die Spiegelung eines Punktes an der Ursprungsgeraden, die mit der x-Achse bzw. der y-Achse den Winkel φ bzw. ϱ einschließt, durch die Matrix

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

beschrieben wird. $\vec{e}_1'$ und $\vec{e}_2'$ bezeichnen dabei die Bilder der Vektoren $\vec{e}_1$ und $\vec{e}_2$ unter der Spiegelung.

M 9 Tippkarten (zum Ausschneiden und Laminieren)

Tipp **zu M 3, Aufgabe 1, Teil a):**

Jeder Vektor $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ lässt sich mithilfe der Vektoren

$\vec{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $\vec{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ durch

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = v_1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + v_2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = v_1 \cdot \vec{e}_1 + v_2 \cdot \vec{e}_2$$

mit den Skalare (= Zahlen) v_1 und v_2 notieren. Daher reicht es aus, sich auf die Vektoren $\vec{e}_1$ und $\vec{e}_2$ zu beschränken.

Tipp **zu M 3, Aufgabe 2:**

Beachten Sie, dass das Bild des Vektors $\vec{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ nach der Drehung in der linken Spalte und das Bild des Vektors $\vec{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ nach der Drehung in der rechten Spalte der Matrix abgelesen werden können.

Tipp 1 **zu M 5, Aufgabe 1:**

Benutzen Sie die Punkte aus Tabelle 1 als zu Buchstaben gehörende Vektoren.

Tipp 2 **zu M 5, Aufgabe 2:**

Es macht Sinn, an bestimmten Stellen in Dezimalzahlen umzurechnen.

Tipp 3 **zu M 5, Aufgabe 2, Teil c):**

Berücksichtigen Sie das Vorzeichen der zweiten Komponente des codierten Vektors.

Lösungen und Tipps zum Einsatz

M 1 Es dreht sich um Caesar – ein einfaches Verfahren

II/B

Viele kennen das Verfahren zur Caesar-Codierung, bei dem Buchstaben einer Nachricht (des Klartexts) mithilfe einer einfachen Regel verschlüsselt werden. Es entsteht auf diese Weise ein auf den ersten Blick unlesbarer Buchstabensalat (der Geheimtext). Mit Kenntnis des verwendeten Schlüssels kann man die Nachricht dann einfach wieder entschlüsseln und lesen. Beim Caesar-Verfahren, das nachweislich schon vom römischen Feldherren Gaius Julius Caesar verwendet wurde, werden die Buchstaben immer um einen festen Wert gegeneinander „verschoben“. Beispielsweise wird beim Verschieben um drei Buchstaben aus dem Klartextbuchstaben A ein D, aus B ein E und so weiter.

Allerdings ist dieses Verfahren relativ einfach zu „knacken“ und bietet keine große Sicherheit für die verschlüsselten Daten. Daher wird im Folgenden, nach einer kurzen Vorstellung des Caesar-Verfahrens, ein etwas aufwendigeres, dafür aber deutlich sichereres Verfahren erarbeitet.

Algebraisch kann man das Caesar-Verfahren als **Addition** interpretieren, wobei man sich die 26 Buchstaben des Alphabets (inklusive der Umlaute Ä, Ö und Ü und ß) und (in diesem Fall ein) Leerzeichen von 0 bis 30 durchnummeriert denkt und in diesem Beispiel immer drei addiert. Am Ende der Skala fängt man – wie bei einer Uhr (nach 12 Uhr kommt 1 Uhr) – wieder von vorne an, man rechnet also modulo 31.

...	Q	R	S	T	U	V	W	X	Y	Z	Ä	Ö	Ü	ß		A	B
...	T	U	V	W	X	Y	Z	A	Ö	Ü	ß		A	B	C	D	E

Abb.11: Die Caesar-Verschlüsselung

Die Tabelle zeigt, dass man diese Verschlüsselung auch als Verschieben zweier Stäbe gegeneinander und damit geometrisch als **Translation** auffassen kann. Das Entschlüsseln funktioniert so, dass man die zuvor gewählte Zahl von den Geheimtextbuchstaben abzieht bzw. um denselben Betrag in die entgegengesetzte Richtung verschiebt.

Möchte man per Hand einen Text mit diesem Verfahren (evtl. sogar mit wechselnden Verschiebungen) ver- bzw. entschlüsseln, ist es hilfreich, sich entsprechende Stäbe zu basteln. Noch einfacher wird das Verfahren, wenn man sich eine sog. **Chiffrierscheibe** bastelt: zwei Scheiben mit den Buchstaben (und Zeichen), die gegeneinander verdreht werden können. Auch diese Umsetzung der Verschlüsselung kann man mathematisch beschreiben, am besten geometrisch mit **Drehungen**. Möchte man dazu einen Computer bzw. Taschenrechner verwenden, ist es günstig, die Drehung als Anwendung von Drehmatrizen aufzufassen. Dies führt dann zur Codierung und Decodierung mithilfe von (2×2)-Matrizen.

An diesem Beispiel – gerade wenn man sich erst entsprechende Scheiben bastelt (Vorlagen auf **CD-ROM 72**) und anschließend die Drehung rechnerisch nachvollzieht – kann man den Einsatz von (zweidimensionalen) Drehmatrizen sehr gut nachvollziehen und seine Rechnungen händisch sehr einfach kontrollieren.

Auf den ersten Blick ist die **Anwendung von Matrizen** ein wenig komplizierter und aufwendiger als eine **Modulo-Addition**. Wenn man allerdings erst einmal Matrizen eingeführt hat (und mit ihnen vertraut ist), lässt sich die Verschlüsselung relativ einfach erweitern – beispielsweise um **Spiegelungen** –, wodurch sie deutlich schwieriger zu knacken ist. Dies ist wichtig, denn die Caesar-Verschlüsselung lässt sich alleine durch **systematisches Probieren** entschlüsseln.