2 Ringe

Wir haben gesehen, dass $\mathbb{Z}_n$ (also die Restklassen in $\mathbb{Z}$ modulo n) „fast“ einen Körper bilden. Wie nennt man denn sowas, und gibt es dazu noch weitere Beispiele?

Definition 2.1. Eine Menge $(r, +, \cdot)$ mit zwei Operationen $+$ und $\cdot$ heisst ein *Ring*, wenn die beiden Operationen allen Körperaxiomen genügen ausser vii) und viii). Ist auch viii) erfüllt (Kommutativität der Multiplikation), so sprechen wir von einem *kommutativen Ring*.

Bemerkung: vii) betrifft die Existenz von multiplikativen Inversen.

Beispiele:

(1) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring.

(2) $(\mathbb{Z}_n, +, \cdot)$ ist für jedes $n > 1$ ein kommutativer Ring.

(3) Jeder Körper $(k, +, \cdot)$ ist sowieso ein kommutativer Ring.

(4) Die Paare $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m$ bilden einen kommutativen Ring durch die Definitionen

$$(a, b) + (c, d) := (\underset{\substack{\nearrow \\ + \text{ in } \mathbb{Z}_n}}{a + c}, \underset{\substack{\uparrow \\ + \text{ in } \mathbb{Z}_m}}{b + d}) \quad \text{und} \quad (a, b) \cdot (c, d) := (\underset{\substack{\nearrow \\ \cdot \text{ in } \mathbb{Z}_n}}{a \cdot c}, \underset{\substack{\uparrow \\ \cdot \text{ in } \mathbb{Z}_m}}{b \cdot d})$$

Wer spielt die Rollen von 0 und 1??

Einige Aufgaben dazu:

1. Ist für Primzahlen p $\mathbb{Z}_p \times \mathbb{Z}_p$ ein Körper?

2. Was hat das mit einem Computerspiel zu tun, bei welchem das Raumschiff am linken Bildrand wieder hereinkommt, wenn es rechts über den Rand hinausdriftet (analog oben und unten)? Der Bildschirm habe 1024×800 Pixel ...

3. Wir haben uns $\mathbb{Z}_8$ vorgestellt als die Ecken eines regulären 8-Ecks, die entstehen, wenn man die Zahlengerade geeignet zu einem Kreis biegt.

Wie hat man sich $\mathbb{Z}_8 \times \mathbb{Z}_5$ vorzustellen?!

4. Basteln Sie sich ein Modell von $\mathbb{Z}_8 \times \mathbb{Z}_5$!

5. Die Idee, die von $\mathbb{Z}_n$ zu $\mathbb{Z}_n \times \mathbb{Z}_m$ führte, lässt sich verallgemeinern ... wie?

6. Bilden $\mathbb{Q}_7$ und $\mathbb{R}_7$ ähnlich wie $\mathbb{Z}_7$ einen Ring oder gar einen Körper?

7. Kennen Sie Geräte, welche mod 12, mod 24 oder z. B. mod 10 000 rechnen? Welche? Weitere Beispiele?

Alle Beispiele von Ringen, die wir bis jetzt betrachtet haben, waren kommutativ. Gibt es überhaupt nicht-kommutative Ringe??

Wir müssen jetzt einigen Aufwand betreiben, um solche Beispiele zu konstruieren. Sie haben aber in Theorie und Praxis eine grosse Bedeutung: Es geht um das Rechnen mit *Matrizen.*

Definition 2.2. Sei $(r, +, \cdot)$ ein Ring. Dann nennen wir eine rechteckige Anordnung von $n \cdot m$ Elementen aus r eine Matrix M $(n, m \in \mathbb{N})$. M hat dann n Zeilen und m Spalten. Man schreibt auch $M = (a_{ij})$, wobei der Index i von 1 bis n und der Index j von 1 bis m laufen soll.

Beispiele:

① $(r, +, \cdot) = (\mathbb{R}, +, \cdot)$

$\begin{pmatrix} 1 & 2.9 & -3 \\ 5 & 2 & 0 \end{pmatrix}$ ist eine 2×3-Matrix über $\mathbb{R}$ $(a_{23} = 0,\ a_{21} = 5)$

$\begin{pmatrix} 3.8 \\ -5 \\ 7 \end{pmatrix}$ ist eine 3×1-Matrix über $\mathbb{R}$
($n \times 1$-Matrizen heissen auch *Vektoren*)

$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9.1 \end{pmatrix}$ ist eine 3×3-Matrix über $\mathbb{R}$ $(a_{23} = 6,\ a_{32} = 8)$

$\begin{pmatrix} 1 & 5.2 \\ 2 & \pi \\ 3 & -9 \end{pmatrix}$ ist eine 3×2-Matrix über $\mathbb{R}$ $(a_{32} = -9,\ a_{23}$ gibt es nicht)

② $(r, +, \cdot) = \mathbb{Z}_5$

$\begin{pmatrix} 1 & 2 & 0 \\ 4 & 3 & 1 \end{pmatrix}$ ist eine 2×3-Matrix über $\mathbb{Z}_5$

$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 0 & 1 \end{pmatrix}$ ist eine 3×2-Matrix über $\mathbb{Z}_5$

③ $(r, +, \cdot) = \mathbb{Z}_6$ (kein Körper)
genau so wie bei $\mathbb{Z}_5$

Bemerkung: Matrizen sind also rechteckige Anordnungen von Zahlen aus einem ganz bestimmten Ring. Die Anzahl der Zeilen und Spalten ist immer eine natürliche Zahl ≥ 1.

In der Informatik würde man von einem 2d-Array sprechen.

Definition 2.3. Die Menge aller $n \times m$-Matrizen über einem Ring r bezeichnen wir mit $\mathbb{M}^{n\times m}(r)$ oder einfach mit $\mathbb{M}^{n\times m}$, wenn klar ist, auf welche Zahlen man sich bezieht.

Wir definieren nun für diese Matrizen ebenfalls eine Addition und eine Multiplikation.

Definition 2.4. Es seien $A = (a_{ij})$ und $B = (b_{ij})$ Matrizen aus $\mathbb{M}^{n\times m}(r)$. Dann ist die Addition von A und B definiert durch

$$[A + B]_{ij} = a_{ij} + b_{ij}$$

Bemerkung: Das i-j-te Element der Summe erhalten wir einfach, indem wir das i-j-te Element der ersten Matrix mit dem i-j-ten Element der zweiten Matrix addieren.

Beispiel:

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

Lemma 2.5. Diese Addition in $\mathbb{M}^{n\times m}(r)$ ist assoziativ und kommutativ. Es existiert ein Neutralelement und jede Matrix besitzt ein additives Inverses.

Die Axiome i) – iv) sind also erfüllt.

Beweis: Banal. Benutzt wird, dass r selber ein Ring ist. □

Nun könnte man ganz entsprechend eine Multiplikation in $\mathbb{M}^{n\times m}(r)$ einführen, und es würde dadurch auch ein Ring entstehen. Eine komponentenweise Multiplikation von a_{ij} mit b_{ij} hat aber nirgends eine vernünftige Anwendung! Dagegen ist eine komplizierter definierte Multiplikation von Matrizen von **grosser** Bedeutung. Diese studieren wir jetzt und erhalten damit auch ein ganz wichtiges Beispiel von einem nicht-kommutativen Ring.

Definition 2.6. Sei $A \in \mathbb{M}^{n\times m}(r)$ und $B \in \mathbb{M}^{m\times p}(r)$. Dann definieren wir $C = A \cdot B$ mit $C \in \mathbb{M}^{n\times p}(r)$ durch

$$c_{ik} = \sum_{j=1}^{m} a_{ij} \cdot b_{jk}$$

Salopp gesagt multipliziert man also die „i-te Zeile von A“ mit der „k-ten Spalte von B“, um das Element c_{ik} des Produkts C zu erhalten.

Beispiele:

① $$\begin{pmatrix} 1 & 2 & 3 \\ -4 & 1 & 5 \\ 0 & 7 & 2 \\ 5 & -1 & 7 \end{pmatrix} \cdot \begin{pmatrix} -2 & 5 \\ 1 & 3 \\ 4 & 2 \end{pmatrix} = \begin{pmatrix} 12 & 17 \\ 29 & -7 \\ 15 & 25 \\ 17 & 36 \end{pmatrix}$$

Es ist z. B. $29 = -4 \cdot (-2) + 1 \cdot 1 + 5 \cdot 4$, $29 = c_{21}$

② $$\begin{pmatrix} 2 & 3 & -4 & 1 \\ 5 & 7 & 6 & 0 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ -3 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} -8 \\ 11 \end{pmatrix}$$

③ $$\begin{pmatrix} 1 & -5 \\ 2 & 6 \\ 3 & 1 \\ 4 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 3 & 1 & 5 \\ -2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 10 & -2 & -19 & -10 \\ -12 & 12 & 26 & 28 \\ -2 & 10 & 7 & 18 \\ 0 & 12 & 4 & 20 \end{pmatrix}$$

Es ist $26 = c_{23}$, $26 = 2 \cdot 1 + 6 \cdot 4$

④ Noch ein Beispiel über dem Zahlkörper $\mathbb{Z}_7$:

$$\begin{pmatrix} 6 & 2 & 3 \\ 1 & 5 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ 1 & 4 \end{pmatrix}$$

Es ist $c_{22} = 4$, $4 = 1 \cdot 2 + 5 \cdot 4 + 4 \cdot 6$

Welche Rechengesetze gelten nun für diese Matrix-Multiplikation?

Als erstes stellen wir fest, dass diese Multiplikation im Allgemeinen **nicht kommutativ** ist: In unseren Beispielen ① und ② lässt sich das Produkt in der umgekehrten Reihenfolge der Faktoren gar nicht bilden! Und bei den Beispielen ③ und ④ resultiert eine Matrix mit ganz anderen Kantenlängen.

Ist wenigstens das Produkt von quadratischen Matrizen kommutativ? Das folgende Beispiel zerstört auch diese Hoffnung:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 & -1 \\ -2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 7 & -3 \end{pmatrix}$$

$$\begin{pmatrix} 5 & -1 \\ -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 6 \\ -2 & -4 \end{pmatrix}$$

Feststellung: Die Matrix-Multiplikation ist im Allgemeinen nicht kommutativ.

Ganz allgemein gilt hingegen

Lemma 2.7. Die Matrix-Multiplikation ist assoziativ. Existiert das Produkt $(A \cdot B) \cdot C$, so existiert auch $A \cdot (B \cdot C)$ und die beiden Produkte sind identisch.

Beweis: Sei also $A \in \mathbb{M}^{n \times m}$, $B \in \mathbb{M}^{m \times p}$ und $C \in \mathbb{M}^{p \times q}$, wobei alle Zahlen aus demselben Ring r stammen sollen. Dann existiert $A \cdot B$ und $(A \cdot B) \cdot C$, aber auch $B \cdot C$ und $A \cdot (B \cdot C)$. Das Ergebnis ist in beiden Fällen eine Matrix aus $\mathbb{M}^{n \times q}$. Dass die beiden Matrizen identisch sind, liesse sich mit grossem Schreibaufwand elementar beweisen. Diesen Aufwand wollen wir uns ausnahmsweise einmal ersparen. □

Überprüfen Sie aber die Assoziativität der Matrix-Multiplikation am folgenden Beispiel:

$$A = \begin{pmatrix} 1 & 3 & -2 \\ 2 & 4 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 2 \\ 3 & 0 \\ 1 & 5 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 3 & 0 & -2 \\ 5 & -1 & 2 & 1 \end{pmatrix}$$

Berechnen Sie $A \cdot B$ und $(A \cdot B) \cdot C$, sowie $B \cdot C$ und $A \cdot (B \cdot C)$.

Lemma 2.8. Die Matrix-Multiplikation ist distributiv. Ist $A \in \mathbb{M}^{n \times m}$ und sind $B, C \in \mathbb{M}^{m \times p}$ und $D \in \mathbb{M}^{p \times q}$, so gilt

i) $A \cdot (B + C) = A \cdot B + A \cdot C$

ii) $(B + C) \cdot D = B \cdot D + C \cdot D$

Beweis: Die Rechnungen sind hier nicht so aufwendig, weil die Addition der Matrizen einfach ist:

i) $$[A \cdot (B + C)]_{ik} = \sum_{j=1}^{m} a_{ij} \cdot (b_{jk} + c_{jk}) = \sum_{j=1}^{m} a_{ij} \cdot b_{jk} + \sum_{j=1}^{m} a_{ij} \cdot c_{jk}$$
$$= [A \cdot B]_{ik} + [A \cdot C]_{ik} = [A \cdot B + A \cdot C]_{ik}$$

ii) Der Beweis von ii) lässt sich ganz ähnlich führen. □

Nun können wir uns der Frage zuwenden, welche Mengen von Matrizen durch die Addition und Multiplikation selber zu einem Ring werden. Damit zu allen Elementen A und B auch die Produkte $A \cdot B$ und $B \cdot A$ existieren, **müssen** wir uns auf Mengen von **quadratischen** Matrizen beschränken.

Nach Lemma 2.7 und Lemma 2.8 ist nur noch die Frage offen, ob es auch ein multiplikatives Neutralelement gibt in $\mathbb{M}^{n \times n}(r)$.

Lemma 2.9. Es sei E die $n \times n$-Matrix mit $e_{ij} = 1$ für $i = j$ und $e_{ij} = 0$ für $i \neq j$. Dann gilt für alle $A \in \mathbb{M}^{n \times n}$ $E \cdot A = A$ und $A \cdot E = A$.

Beweis: Weil die Multiplikation nicht kommutativ ist, müssen wir zwei Beweise führen:

$$(E \cdot A)_{ik} = \sum_{j=1}^{n} e_{ij} \cdot a_{jk} = e_{ii} \cdot a_{ik} = 1 \cdot a_{ik} = a_{ik}$$

Also gilt $E \cdot A = A$. Genau so folgt $A \cdot E = A$. □

Bemerkung: Man nennt E auch die „Einheitsmatrix“. Bei den Rechnern der Firma TI können Sie die $n \times n$-Matrix E bequem erzeugen mit dem Befehl „identity(n)“.

Beispiel: „identity(4)“ liefert die Matrix E der Kantenlänge 4

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Korollar 2.10. Sei r ein Ring. Dann bilden die Elemente von $\mathbb{M}^{n\times n}(r)$ bezüglich der komponentenweisen Addition und der eben definierten Matrix-Multiplikation ebenfalls einen Ring. Für $n > 1$ ist dieser Ring nicht kommutativ.

Beweis: Lemma 2.5, Lemma 2.7, Lemma 2.8 und Lemma 2.9 sowie das Beispiel zweier Matrizen $A, B \in \mathbb{M}^{2\times 2}(\mathbb{Z})$ mit $A \cdot B \neq B \cdot A$. □

Im Ring $\mathbb{Z}_n$ haben wir die Frage untersucht, welche Elemente ein multiplikatives Inverses haben und wie man dieses effizient berechnen kann.

Diese Frage stellen wir uns auch für $\mathbb{M}^{n\times n}(r)$, wo r ein Ring ist. Da der Ring der Matrizen aber nicht kommutativ ist, ist einiges ein bisschen komplizierter.

Definition 2.11. Sei $A \in \mathbb{M}^{n\times n}(r)$. A heisst invertierbar, wenn es Matrizen B und C in $\mathbb{M}^{n\times n}(r)$ gibt, so dass gilt $A \cdot B = E$ und $C \cdot A = E$.

A muss also durch Multiplikation sowohl von links als auch von rechts auf die Einheitsmatrix überführt werden können. Immerhin gilt

Lemma 2.12. A sei eine invertierbare Matrix in $\mathbb{M}^{n\times n}(r)$. Dann gilt

$$(A \cdot B = E \text{ und } C \cdot A = E) \implies B = C$$

Beweis: $B = E \cdot B = (C \cdot A) \cdot B = C \cdot (A \cdot B) = C \cdot E = C$ □

Wir müssen also nicht zwischen der linksinversen und der rechtsinversen Matrix unterscheiden, und zu jeder invertierbaren Matrix A gibt es also eine Matrix B mit $A \cdot B = E$ und $B \cdot A = E$. Wir zeigen noch, dass diese inverse Matrix B eindeutig bestimmt ist:

Lemma 2.13. Es sei A eine invertierbare Matrix in $\mathbb{M}^{n\times n}(r)$, und für $B \in \mathbb{M}^{n\times n}(r)$ gelte $A \cdot B = E$ und $B \cdot A = E$. Dann gilt für alle Matrizen C und D aus $\mathbb{M}^{n\times n}(r)$

i) $A \cdot C = E \implies C = B$

ii) $D \cdot A = E \implies D = B$

Beweis: $A \cdot C = E \implies C = E \cdot C = (B \cdot A) \cdot C = B \cdot (A \cdot C) = B \cdot E = B$
$D \cdot A = E \implies D = D \cdot E = D \cdot (A \cdot B) = (D \cdot A) \cdot B = E \cdot B = B$ □

Ist A invertierbar, so ist die inverse Matrix $B = A^{-1}$ zu A eindeutig bestimmt, und wegen $A \cdot B = E$ und $B \cdot A = E$ ist auch die inverse Matrix B invertierbar , und es ist $B^{-1} = A$, also $(A^{-1})^{-1} = A$.

Der Vollständigkeit halber zeigen wir noch, dass auch das Produkt von invertierbaren Matrizen wieder eine invertierbare Matrix ist:

Lemma 2.14. Sind A und B invertierbare Matrizen in $\mathbb{M}^{n\times n}(r)$, so sind auch $A \cdot B$ und $B \cdot A$ invertierbar.

Beweis: Es ist $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$ nach der folgenden Rechnung:

$$(A \cdot B) \cdot (B^{-1} \cdot A^{-1}) = A \cdot (B \cdot B^{-1}) \cdot A^{-1} = A \cdot E \cdot A^{-1} = A \cdot A^{-1} = E$$ □

Wir betrachten nun den Spezialfall, wo der zugrundeliegende Ring ein Körper ist. In einem Körper sind ja lineare Gleichungen mit **einer** Unbekannten eindeutig lösbar (Lemma 1.3). Wir zeigen nun, was die Matrizen von $\mathbb{M}^{n\times n}(k)$ mit den linearen Gleichungssystemen der Art „n Gleichungen für n Unbekannte“ zu tun haben.

Gegeben sei ein Gleichungssystem, der zugrundeliegende Zahlkörper k sei $\mathbb{R}$:

$$\begin{aligned} \text{I} \quad & y - z = 5 \\ \text{II} \quad & 2x + 5y + 4z = 7 \\ \text{III} \quad & x + 2y + 3z = 2 \end{aligned}$$

Das Gleichungssystem kann in Matrix-Form geschrieben werden als

$$\begin{pmatrix} 0 & 1 & -1 \\ 2 & 5 & 4 \\ 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 5 \\ 7 \\ 2 \end{pmatrix}$$

oder abgekürzt $$A \cdot X = V$$

Dieses Gleichungssystem ist genau dann eindeutig lösbar, wenn die Matrix A ein multiplikatives Inverses hat. Existiert A^{-1} mit $A^{-1} \cdot A = E$, so gilt

$$\begin{aligned} A^{-1} \cdot (A \cdot X) &= A^{-1} \cdot V \\ (A^{-1} \cdot A) \cdot X &= A^{-1} \cdot V \\ E \cdot X &= A^{-1} \cdot V \end{aligned}$$

also $$\underline{X = A^{-1} \cdot V}$$

Dringend gewünscht sind also zwei Methoden: Eine erste, mit der man entscheiden kann, ob eine Matrix $A \in \mathbb{M}^{n\times n}(k)$ invertierbar ist, und eine zweite, mit der man die inverse Matrix A^{-1} gegebenenfalls auch berechnen kann.

Carl Friedrich Gauss, der „Fürst der Mathematiker“, hat ein Verfahren angegeben, welches gleich beides leistet. Falls A^{-1} existiert, liefert es die inverse Matrix und gleichzeitig auch noch die Lösung des Gleichungssystems.

Wir starten mit $A \,|\, E \,|\, V$, vertauschen Zeilen und bilden Linearkombinationen einer Zeile mit Vielfachen von einer andern. Schliesslich erhalten wir $E \,|\, A^{-1} \,|\, X$:

①	I	0	1	−1	1	0	0	5
	II	2	5	4	0	1	0	7
	III	1	2	3	0	0	1	2
②	III	1	2	3	0	0	1	2
	I	0	1	−1	1	0	0	5
	II − 2 · III	0	1	−2	0	1	−2	3

③	I − 2 · II	1	0	5	−2	0	1	−8
	II	0	1	−1	1	0	0	5
	II − III	0	0	1	1	−1	2	2
④	I − 5 · III	1	0	0	−7	5	−9	−18
	II + III	0	1	0	2	−1	2	7
	III	0	0	1	1	−1	2	2

Prüfen Sie die folgenden Behauptungen:

$$A^{-1} = \begin{pmatrix} -7 & 5 & -9 \\ 2 & -1 & 2 \\ 1 & -1 & 2 \end{pmatrix} \quad \text{und} \quad X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -18 \\ 7 \\ 2 \end{pmatrix}$$

Gelingt es links die Matrix E herzustellen, dann hat das Gleichungssystem genau eine Lösung, und das Verfahren liefert uns A^{-1} und die Lösung X.

Ein Beweis, dass der Gauss-Algorithmus immer korrekt entscheidet, findet sich im Skriptum LinAlg_03.

In den TI - Taschenrechnern ist der Gauss-Algorithmus mit dem Befehl rref(m) implementiert, wo m eine Matrix ist:

① $\begin{bmatrix} 0 & 1 & -1 & 1 & 0 & 0 & 5 \\ 2 & 5 & 4 & 0 & 1 & 0 & 7 \\ 1 & 2 & 3 & 0 & 0 & 1 & 2 \end{bmatrix} \longrightarrow$ m

② rref(m) liefert die Matrix

$$\begin{bmatrix} 1 & 0 & 0 & -7 & 5 & -9 & -18 \\ 0 & 1 & 0 & 2 & -1 & 2 & 7 \\ 0 & 0 & 1 & 1 & -1 & 2 & 2 \end{bmatrix}$$

Nebenbei: m^{-1} liefert für eine Matrix m auch ihre Inverse.

Gelingt es rref( ) oder dem Gauss-Algorithmus nicht, vorne die Matrix E zu bilden, dann existiert A^{-1} nicht und das Gleichungssystem hat nicht eine eindeutige Lösung, sondern es gibt keine oder viele Lösungen. Welcher dieser beiden Fälle vorliegt, lässt sich ebenfalls am Ergebnis des Gauss-Algorithmus ablesen.

Lässt man bei ① die Einheitsmatrix (also die Spalten 4, 5 und 6) weg, so liefert der Gauss-Algorithmus immer noch die Lösung des Gleichungssystems, aber nicht mehr die inverse Matrix.

Zum Abschluss berechnen wir noch die inverse Matrix zu A in $\mathbb{M}^{3\times 3}(\mathbb{Z}_7)$:

$$A = \begin{pmatrix} 2 & 0 & 5 \\ 1 & 3 & 4 \\ 6 & 1 & 2 \end{pmatrix} \in \mathbb{M}^{3\times 3}(\mathbb{Z}_7)$$

①

I	2	0	5	1	0	0
II	1	3	4	0	1	0
III	6	1	2	0	0	1

②

II	1	3	4	0	1	0
$\mathrm{I}+5\cdot\mathrm{II}$	0	1	4	1	5	0
$\mathrm{II}+\mathrm{III}$	0	4	6	0	1	1

③

$\mathrm{I}+\mathrm{III}$	1	0	3	0	2	1
II	0	1	4	1	5	0
$\mathrm{III}+3\cdot\mathrm{II}$	0	0	4	3	2	1

④

$\mathrm{I}+\mathrm{III}$	1	0	0	3	4	2
$\mathrm{II}-\mathrm{III}$	0	1	0	5	3	6
$2\cdot\mathrm{III}$	0	0	1	6	4	2

Es ist $$A^{-1} = \begin{pmatrix} 3 & 4 & 2 \\ 5 & 3 & 6 \\ 6 & 4 & 2 \end{pmatrix}$$

Kontrollieren Sie unsere Rechnung mit dem TR. Verwenden Sie die Funktion $\mathrm{mod}\,(\mathrm{a}\cdot\mathrm{b},\ 7)$, wo $\mathrm{a} = A$ und $\mathrm{b} = A^{-1}$.

Aufgaben:

1. Schreiben Sie das folgende Gleichungssystem in der Sprache der Matrizen, also in der Form $A \cdot X = V$:

$$\begin{aligned} -w + 3x - 2y + z &= 17 \\ w + 2x - 3y - 4z &= 10 \\ 3w - x + 4y + 2z &= 21 \\ 2w - 5x + y + 3z &= 15 \end{aligned}$$

a) Lösen Sie das Gleichungssystem von Hand mit dem Gauss-Algorithmus und bestimmen Sie gleichzeitig die inverse Matrix A^{-1}.

b) Machen Sie dasselbe mit dem TR und dem Befehl rref( ).

c) Geben Sie A und V in den TR ein. Lassen Sie A^{-1} mit der Kehrwertfunktion berechnen und bestimmen Sie die Lösung X des Systems durch $X = A^{-1} \cdot V$.

2. a) Lassen Sie sich z. B. durch mod(randmat(4,4),7) → m zufällige Matrizen aus $\mathbb{M}^{n\times n}(\mathbb{Z}_7)$ erzeugen.

b) Prüfen Sie, ob die erzeugte Matrix m invertierbar ist, indem Sie m^{-1} berechnen lassen.

c) m ist invertierbar, wenn die Zahl det(m) verschieden von 0 ist.
(Mitteilung ohne Beweis)

d) Programmieren Sie eine Funktion matinver(m,p), welcher Sie eine Matrix übergeben können und die Ihnen (falls sie existiert!) die inverse Matrix m^{-1} in $\mathbb{M}^{n\times n}(\mathbb{Z}_p)$ zurückgibt.

3. Berechnen Sie von Hand die inverse Matrix zu A in $\mathbb{Z}_{11}$:

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

Prüfen Sie zuerst mit mod(det(a),11), ob die Determinante von A auch verschieden ist von null.

Version 2.01, vom Nov 2012

Ausgearbeitet von Martin Gubler, Kantonsschule Frauenfeld, anno 1999

Mit LaTeX in eine lesbare Form gebracht von Alfred Hepp im Juni 2011