Script generated by TTT

Title: Meixner: ZUE_DS_WS2014 (21.01.2015)

Date: Wed Jan 21 16:59:43 CET 2015

Duration: 90:01 min

Pages: 45

WS 2014/15

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Bungartz)

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2014WS/ds/uebung/

21. Januar 2015

ZÜ XIV

Übersicht:

1. Übungsbetrieb	Fragen, Probleme?
2. Quiz:	Rechnen modulo n
3. Thema	Euklidischer Algorithmus
4. Vorbereitung	von Blatt 13

1. Fragen, Anregungen?

Aktuelle Fragen?

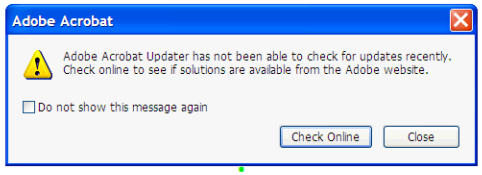
Anmeldungen zur Klausur unbedingt nachholen!!

2. Quiz: Rechnen modulo n

Wir rechnen im Ring $Z_6 = (\mathbb{Z}_6, +_6, \cdot_6)$.

in 3 Minuten,

Wieviel ist:



Wir rechnen im Ring $Z_6 = (\mathbb{Z}_6, +_6, \cdot_6)$ in 3 Minuten, schriftlich!.
Im Folgenden lassen wir den Index 6 in den Bezeichnungen $+_6, \cdot_6$ weg.

Wieviel ist:

$$\begin{array}{llll} 1 \cdot 1 = \_\_\_| & 2 \cdot 2 = \_\_\_| & 3 \cdot 3 = \_\_\_| & (-3) = \_\_\_ \\ 1 - 2 = \_\_\_| & 2 \cdot (-5) = \_\_\_| & 5^{-1} = \_\_\_| & (-3) \cdot 3 = \_\_\_ \\ (1-2)^3 = \_\_\_| & 2 \cdot (1-5) = \_\_\_| & (-1)^{-1} = \_\_\_| & (-4) \cdot (-4) = \_\_\_ \end{array}$$

?

Zusatzfrage: Besitzt 2 ein multiplikatives Inverses 2^{-1} ?

Wir rechnen im Ring $Z_6 = (\mathbb{Z}_6, +_6, \cdot_6)$ in 3 Minuten, schriftlich!.
Im Folgenden lassen wir den Index 6 in den Bezeichnungen $+_6, \cdot_6$ weg.

Wieviel ist:

$$\begin{array}{llll} 1 \cdot 1 = \_\_\_| & 2 \cdot 2 = \_\_\_| & 3 \cdot 3 = \_\_\_| & (-3) = \_\_\_ \\ 1 - 2 = \_\_\_| & 2 \cdot (-5) = \_\_\_| & 5^{-1} = \_\_\_| & (-3) \cdot 3 = \_\_\_ \\ (1-2)^3 = \_\_\_| & 2 \cdot (1-5) = \_\_\_| & (-1)^{-1} = \_\_\_| & (-4) \cdot (-4) = \_\_\_ \end{array}$$

?

Zusatzfrage: Besitzt 2 ein multiplikatives Inverses 2^{-1} ?

Lösung:

Wir rechnen in $\mathbb{Z}_6$.

$$\begin{array}{llll} 1 \cdot 1 = \underline{1}| & 2 \cdot 2 = \underline{4}| & 3 \cdot 3 = \underline{3}| & (-3) = \underline{3} \\ 1 - 2 = \underline{5}| & 2 \cdot (-5) = \underline{2}| & 5^{-1} = \underline{5}| & (-3) \cdot 3 = \underline{3} \\ (1-2)^3 = \underline{5}| & 2 \cdot (1-5) = \underline{4}| & (-1)^{-1} = \underline{5}| & (-4) \cdot (-4) = \underline{4} \end{array}$$

!

Es gibt kein multiplikatives Inverses von 2, denn 2 ist ein Nullteiler (zu welchem co-Nullteiler?)

3. Thema: Euklidischer Algorithmus

3.1 Beispiel

Aufgabe:
Berechnen Sie den größen gemeinsamen Teiler der ganzen Zahlen 53 und 36 und stellen Sie den ggT als Linearkombination dar wie folgt:

$$a \cdot 53 + b \cdot 36 = \mathrm{ggT}(53, 36)\,.$$

Lösung:
Man berechnet mit Hilfe des erweiterten Euklidischen Algorithmus ganze Zahlen a, b, so dass gilt

$$a \cdot 53 + b \cdot 36 = 1\,.$$

Wir führen den Euklidischen Algorithmus aus wie folgt.

$$\begin{aligned}
r_0 &= 53\,,\\
r_1 &= 36\,,\\
r_2 &= 53 \bmod 36 &&= r_0 - 1 \cdot r_1 &&= 17\,,\\
r_3 &= 36 \bmod 17 &&= r_1 - 2 \cdot r_2 &&= 2\,,\\
r_4 &= 17 \bmod 2 &&= r_2 - 8 \cdot r_3 &&= 1\,.
\end{aligned}$$

Es folgt

$$\mathrm{ggT}(53, 36) = 1\,.$$

Nun führen wir die Erweiterung des Euklidischen Algorithmus z.B. in der Form der Rückeinsetzung aus.

$$\begin{aligned}
1 &= r_4\\
&= r_2 - 8r_3 &&= r_2 - 8(r_1 - 2r_2)\\
&= -8r_1 + 17r_2 &&= -8r_1 + 17(r_0 - r_1)\\
&= 17r_0 - 25r_1\,.
\end{aligned}$$

Es folgt $17r_0 - 25r_1 = 1$, mithin, für $a = 17$ und $b = -25$,

$$a \cdot 53 + b \cdot 36 = 1\,.$$

Aus der Gleichung folgt:

Das Inverse von 36 modulo 53 ist $(-25) \bmod 53 = 28$.

Wir führen den Euklidischen Algorithmus aus wie folgt.

$$\begin{aligned}
r_0 &= 53\,,\\
r_1 &= 36\,,\\
r_2 &= 53 \bmod 36 &&= r_0 - 1 \cdot r_1 &&= 17\,,\\
r_3 &= 36 \bmod 17 &&= r_1 - 2 \cdot r_2 &&= 2\,,\\
r_4 &= 17 \bmod 2 &&= r_2 - 8 \cdot r_3 &&= 1\,.
\end{aligned}$$

Es folgt

$$\mathrm{ggT}(53, 36) = 1\,.$$

Nun führen wir die Erweiterung des Euklidischen Algorithmus z.B. in der Form der Rückeinsetzung aus.

$$\begin{aligned} 1 &= r_4 \\ &= r_2 - 8r_3 && = r_2 - 8(r_1 - 2r_2) \\ &= -8r_1 + 17r_2 && = -8r_1 + 17(r_0 - r_1) \\ &= 17r_0 - 25r_1\,. \end{aligned}$$

Es folgt $17r_0 - 25r_1 = 1$, mithin, für $a = 17$ und $b = -25$,

$$a \cdot 53 + b \cdot 36 = 1\,.$$

Aus der Gleichung folgt:

Das Inverse von 36 modulo 53 ist $(-25) \bmod 53 = 28$.

3.2 Formalisierung und Verallgemeinerung

In gewissen kommutativen Ringen $R = (S, +, \cdot, 0, 1)$ stellt sich der erweiterte Euklidische Algorithmus zur Berechnung des größten gemeinsamen Teilers $\mathrm{ggT}(a, b)$ zweier Elemente $a \in S$ und $b \in S$ dar als eine iterierte Transformation (Matrixmultiplikation) Q_i angewandt auf Δ_{i-1} wie folgt mit $r_0 = a$ und $r_1 = b$.

$$\begin{aligned} \Delta_0 &= \begin{pmatrix} a \\ b \end{pmatrix} \\ \Delta_i &= \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = Q_i \Delta_{i-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} \\ &= \begin{pmatrix} r_i \\ r_{i-1} - q_i r_i \end{pmatrix} \qquad \text{für alle} \quad i = 1, 2, \ldots, n \in \mathbb{N}\,. \end{aligned}$$

Dabei werden die Quotienten q_i so gewählt (geschätzt), dass die Δ_i mit wachsendem i in einem gewissen Sinn stets echt kleiner werden.

Eine Berechnung wird beendet, wenn die Folge der Δ_i maximale Länge besitzt, d. h. wenn kein Quotient existiert, der die Bildung eines noch kleineren Restes erlaubt.

Zur Bemessung der Größe von Elementen eines Ringes dient beispielweise im Ring der ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0, 1)$ die Betragsfunktion.
In Polynomringen wird der Grad eines Polynoms verwendet.

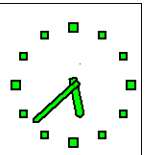
Die Berechnung setzt voraus,
dass der Faktor q_i gefunden werden kann!

Dies setzt z.B. voraus, dass r_{i-1} in gewissem Sinne „größer“ ist als r_i.

Falls umgekehrt r_i in gewissem Sinne „größer“ ist als r_{i-1}, dann fügt man eine Vertauschung ein in Gestalt einer Vertauschungsmatrix.
Wir haben dann

$$\begin{pmatrix} r_{i-1} \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}.$$

Dies ist ein Schritt einer „Division“.



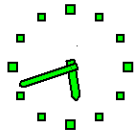
Die Berechnung setzt voraus,
dass der Faktor q_i gefunden werden kann!

Dies setzt z.B. voraus, dass r_{i-1} in gewissem Sinne „größer“ ist als r_i.

Falls umgekehrt r_i in gewissem Sinne „größer“ ist als r_{i-1},
dann fügt man eine Vertauschung ein in Gestalt einer Vertauschungsmatrix.
Wir haben dann

$$\begin{pmatrix} r_{i-1} \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} .$$

Dies ist ein Schritt einer „Division“.



4. Vorbereitung auf TA Blatt 11

4.1 VA 1

Man zeige:

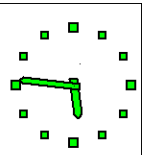
$$2^{16} \bmod 3 = 1, \quad 2^{33} \bmod 3 = 2, \quad 2^{1600} \bmod 3 = 1 .$$

Lösung

$$2^{16} \bmod 3 = (2^2)^8 \bmod 3 = (4 \bmod 3)^8 \bmod 3 = 1^8 \bmod 3 = 1 .$$

$$2^{33} \bmod 3 = ((2^{16})^2 \cdot 2) \bmod 3 = 1 \cdot 2 \bmod 3 = 2 .$$

$$2^{1600} \bmod 3 = (2^{16})^{100} \bmod 3 = 1 \bmod 3 = 1 .$$

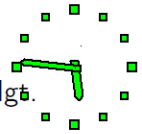


4.2 VA 2, Euklidischer Algorithmus

Wir betrachten im Folgenden den Ring $(\mathbb{Z}, +, \cdot, 0, 1)$
der ganzen Zahlen.

1. Zeigen Sie für alle entsprechenden i

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(r_i, r_{i+1}) .$$



Die Matrixmultiplikation liefert eine Linearkombination wie folgt.

$$\Delta_i = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i-1} - q_i r_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} .$$

Da die Matrix $Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$ invertierbar ist mit

$$Q_i^{-1} = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} ,$$

haben die Komponentenpaare der Δ_i für alle i die gleichen Teiler.
w.z.b.w.

Die Matrixmultiplikation liefert eine Linearkombination wie folgt.

$$\Delta_i = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i-1} - q_i r_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} .$$

Da die Matrix $Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$ invertierbar ist mit

$$Q_i{}^{-1} = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} ,$$

haben die Komponentenpaare der Δ_i für alle i die gleichen Teiler.
w.z.b.w.

Berechnung:

Wir rechnen im Ring der ganzen Zahlen.

Im Euklidischen Algorithmus für den Ring ganzer Zahlen zur Berechnung des $\mathrm{ggT}(a, b)$ werden die Quotienten q_i durch ganzzahlige Division bestimmt.

$$q_i = r_{i-1} \operatorname{div} r_i .$$

Abweichend davon könnte man aber auch grob schätzen.

Für die Linearkombination $r_{i+1} = r_{i-1} - q_i r_i$ folgt dann

$$r_{i+1} = r_{i-1} \bmod r_i .$$

Die Berechnung wird beendet, wenn $r_{n+1} = 0$ eintritt für irgendein $n \in \mathbb{N}$.

Berechnung:

Wir rechnen im Ring der ganzen Zahlen.

Im Euklidischen Algorithmus für den Ring ganzer Zahlen zur Berechnung des $\mathrm{ggT}(a, b)$ werden die Quotienten q_i durch ganzzahlige Division bestimmt.

$$q_i = r_{i-1} \operatorname{div} r_i .$$

Abweichend davon könnte man aber auch grob schätzen.

Für die Linearkombination $r_{i+1} = r_{i-1} - q_i r_i$ folgt dann

$$r_{i+1} = r_{i-1} \bmod r_i .$$

Die Berechnung wird beendet, wenn $r_{n+1} = 0$ eintritt für irgendein $n \in \mathbb{N}$.

Berechnung (Fortsetzung):

$$\begin{aligned} r_0 &= 10800 , \\ r_1 &= 122 , \\ r_2 &= 10800 \bmod 122 = 64 , \\ r_3 &= 122 \bmod 64 = 58 , \\ r_4 &= 64 \bmod 58 = 6 , \\ r_5 &= 58 \bmod 6 = 4 , \\ r_6 &= 6 \bmod 4 = 2 , \\ r_7 &= 4 \bmod 2 = 0 . \end{aligned}$$

Ergebnis: $\mathrm{ggT}(10800, 122) = r_6 = 2.$

3. Berechnen Sie mit dem erweiterten Euklidischen Algorithmus ganze Zahlen m, n, so dass gilt

$$m \cdot 10800 + n \cdot 122 = \mathrm{ggT}(10800, 122) \qquad \text{(Linearkombination)}.$$

Ein äußerst wichtiger nächster Schritt besteht darin, den größten gemeinsamen Teiler r_6 von a und b als Linearkombination von $a = r_0$ und $b = r_1$ zu bestimmen.

Dies geschieht mit dem *erweiterten Euklidischen Algorithmus* wie folgt.

Der erweiterte Euklidische Algorithmus lässt sich als Matrixmultiplikation wie folgt darstellen:

$$\begin{pmatrix} r_n \\ r_{n+1} \end{pmatrix} = Q_n \cdot Q_{n-1} \cdot \ldots \cdot Q_2 \cdot Q_1 \cdot \begin{pmatrix} a \\ b \end{pmatrix}.$$

Nun führen wir die Erweiterung des Euklidischen Algorithmus z.B. in der Form der Rückeinsetzung aus.

$$\begin{aligned} 1 &= r_4 \\ &= r_2 - 8r_3 && = r_2 - 8(r_1 - 2r_2) \\ &= -8r_1 + 17r_2 && = -8r_1 + 17(r_0 - r_1) \\ &= 17r_0 - 25r_1\,. \end{aligned}$$

Es folgt $17r_0 - 25r_1 = 1$, mithin, für $a = 17$ und $b = -25$,

$$a \cdot 53 + b \cdot 36 = 1\,.$$

Aus der Gleichung folgt:

Das Inverse von 36 modulo 53 ist $(-25) \bmod 53 = 28$.

Wir führen den Euklidischen Algorithmus aus wie folgt.

$$\begin{aligned} r_0 &= 53\,, \\ r_1 &= 36\,, \\ r_2 &= 53 \bmod 36 && = r_0 - 1 \cdot r_1 && = 17\,, \\ r_3 &= 36 \bmod 17 && = r_1 - 2 \cdot r_2 && = 2\,, \\ r_4 &= 17 \bmod 2 && = r_2 - 8 \cdot r_3 && = 1\,. \end{aligned}$$

Es folgt

$$\mathrm{ggT}(53, 36) = 1\,.$$

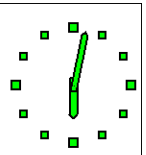
Die Matrizen P_k enthalten die Koeffizienten der jeweiligen Linearkombinationen. Man berechnet diese Koeffizienten gleichzeitig mit den r_k durch sukzessive Berechnung von

$$P_k = Q_k \cdot P_{k-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \cdot \begin{pmatrix} m_{k-1} & n_{k-1} \\ m_k & n_k \end{pmatrix}.$$

Es gelten die folgenden Gleichungen.

$$\begin{aligned} q_k &= r_{k-1} \operatorname{div} r_k\,, \\ r_{k+1} &= r_{k-1} \bmod r_k\,, \\ m_{k+1} &= m_{k-1} - q_k \cdot m_k\,, \\ n_{k+1} &= n_{k-1} - q_k \cdot n_k\,, \\ r_k &= m_k \cdot a + n_k \cdot b\,. \end{aligned}$$

Wir führen die Auswertung der Formeln von Hand aus mit Buchführung in einer Tabelle.

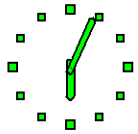


k	r_{k-1}	r_k	q_k	m_{k-1}	m_k	n_{k-1}	n_k
$k=1$	10800	122	88	1	0	0	1
$k=2$	122	64	1		1		-88
$k=3$	64	58	1		-1		89
$k=4$	58	6	9		2		-177
$k=5$	6	4	1		-19		1682
$k=6$	4	2	2		21		-1859
$k=7$	2	0			-61		5400

Ergebnis:

$$m_6 \cdot a + n_6 \cdot b = 21 \cdot 10800 + (-1859) \cdot 122 = 2\,.$$

Wir führen die Auswertung der Formeln von Hand aus mit Buchführung in einer Tabelle.

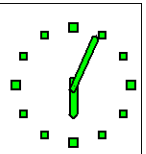


k	r_{k-1}	r_k	q_k	m_{k-1}	m_k	n_{k-1}	n_k
$k=1$	10800	122	88	1	0	0	1
$k=2$	122	64	1		1		-88
$k=3$	64	58	1		-1		89
$k=4$	58	6	9		2		-177
$k=5$	6	4	1		-19		1682
$k=6$	4	2	2		21		-1859
$k=7$	2	0			-61		5400

Ergebnis:

$$m_6 \cdot a + n_6 \cdot b = 21 \cdot 10800 + (-1859) \cdot 122 = 2\,.$$

Die Matrizen P_k enthalten die Koeffizienten der jeweiligen Linearkombinationen. Man berechnet diese Koeffizienten gleichzeitig mit den r_k durch sukzessive Berechnung von



$$P_k = Q_k \cdot P_{k-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \cdot \begin{pmatrix} m_{k-1} & n_{k-1} \\ m_k & n_k \end{pmatrix}\,.$$

Es gelten die folgenden Gleichungen.

$$\begin{aligned} q_k &= r_{k-1} \operatorname{div} r_k\,, \\ r_{k+1} &= r_{k-1} \bmod r_k\,, \\ m_{k+1} &= m_{k-1} - q_k \cdot m_k\,, \\ n_{k+1} &= n_{k-1} - q_k \cdot n_k\,, \\ r_k &= m_k \cdot a + n_k \cdot b\,. \end{aligned}$$

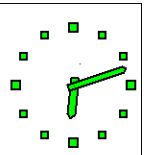
Wir führen die Auswertung der Formeln von Hand aus mit Buchführung in einer Tabelle.

k	r_{k-1}	r_k	q_k	m_{k-1}	m_k	n_{k-1}	n_k
$k=1$	10800	122	88	1	0	0	1
$k=2$	122	64	1		1		-88
$k=3$	64	58	1		-1		89
$k=4$	58	6	9		2		-177
$k=5$	6	4	1		-19		1682
$k=6$	4	2	2		21		-1859
$k=7$	2	0			-61		5400

Ergebnis:

$$m_6 \cdot a + n_6 \cdot b = 21 \cdot 10800 + (-1859) \cdot 122 = 2\,.$$

4.3 VA 3, Abstrakte Ringe, elementare Eigenschaften

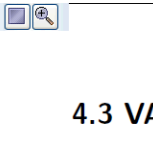


1. Man zeige:
   In einem beliebigen Ring $(R, \oplus, \odot, 0, 1)$ gelten die folgenden Gleichungen.

$$a \odot 0 \;=\; 0 \odot a \;=\; 0\,, \qquad\qquad a \odot b \;=\; (-a) \odot (-b)\,.$$

Bemerkung 1: Das Inverse eines Elements x bezüglich der Operation $\oplus$ wird mit $-x$ bezeichnet.

Bemerkung 2: Da a und b beliebige Elemente aus R sind, schreiben wir die Gleichungen ohne Allquantoren.
Natürlich darf man auch $\forall a, b$ ergänzen.



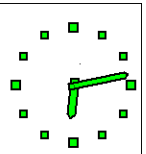
4.3 VA 3, Abstrakte Ringe, elementare Eigenschaften

1. Man zeige:
   In einem beliebigen Ring $(R, \oplus, \odot, 0, 1)$ gelten die folgenden Gleichungen.

$$a \odot 0 \;=\; 0 \odot a \;=\; 0\,, \qquad\qquad a \odot b \;=\; (-a) \odot (-b)\,.$$

Bemerkung 1: Das Inverse eines Elements x bezüglich der Operation $\oplus$ wird mit $-x$ bezeichnet.

Bemerkung 2: Da a und b beliebige Elemente aus R sind, schreiben wir die Gleichungen ohne Allquantoren.
Natürlich darf man auch $\forall a, b$ ergänzen.



Beweis:

1. Gleichung(en): $a \odot 0 \;=\; 0 \odot a \;=\; 0\,.$

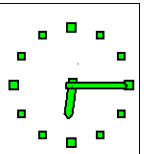
- Es gilt

$$a \odot 0 = a \odot (0 \oplus 0) = (a \odot 0) \oplus (a \odot 0)\,.$$

Daraus folgt mit additiver Kürzungsregel $a \odot 0 = 0$.

Da die Kommutativität der Multiplikation nicht vorausgesetzt wurde, müssen wir $0 \odot a = 0$ gesondert beweisen.

Dies folgert man aber analog wie vorhin.



2. Geben Sie zwei nichtkommutative Ringe an.

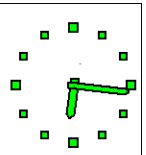
Lösung:

Man nehme die Ringe der $n \times n$-Matrizen für verschiedene $n \geq 2$.

Für die Matrixmultiplikation mit $n = 2$ gilt beispielsweise

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

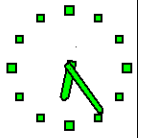
Was erhält man bei Rechnung modulo 2 ?



4.4 VA 4

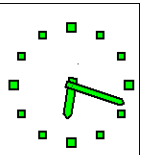
Die Menge der Permutationen der Teilmenge $\{1, 2, 3, 4\}$ der natürlichen Zahlen bildet zusammen mit der Komposition $\circ$ von Abbildungen die Gruppe $\mathcal{S}_4$. Das neutrale Element der Gruppe sei id. Wir betrachten die in Zyklusschreibweise gegebenen Permutationen

$$p = (1\ 2)(3)(4) \qquad \text{und} \qquad q = (1)(2)(3\ 4)\,.$$



Seien $r = p \circ q$ und $U = \{id, p, q, r\}$.

1. Geben Sie die $\circ$-Verknüpfungstafel für die Elemente aus U an.
2. Beweisen Sie, dass die Menge U mit jedem Element $x \in U$ auch sein Inverses x^{-1} enthält (mit $x \circ x^{-1} = id$).
3. Aus den obigen Aussagen folgt, dass U eine Untergruppe von $\mathcal{S}_4$ ist. Ist die Gruppe U zyklisch ? Beweis!

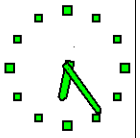


4.4 VA 4

Die Menge der Permutationen der Teilmenge $\{1, 2, 3, 4\}$ der natürlichen Zahlen bildet zusammen mit der Komposition $\circ$ von Abbildungen die Gruppe $\mathcal{S}_4$. Das neutrale Element der Gruppe sei id. Wir betrachten die in Zyklusschreibweise gegebenen Permutationen

$$p = (1\ 2)(3)(4) \qquad \text{und} \qquad q = (1)(2)(3\ 4)\,.$$

ZÜ DS
©Dr. Werner Meixner
4.4 VA 4
27/33



4.4 VA 4

Die Menge der Permutationen der Teilmenge $\{1, 2, 3, 4\}$ der natürlichen Zahlen bildet zusammen mit der Komposition $\circ$ von Abbildungen die Gruppe $\mathcal{S}_4$. Das neutrale Element der Gruppe sei id. Wir betrachten die in Zyklusschreibweise gegebenen Permutationen

$$p = (1\ 2)(3)(4) \qquad \text{und} \qquad q = (1)(2)(3\ 4)\,.$$

ZÜ DS
©Dr. Werner Meixner
4.4 VA 4
27/33

Einige Hilfsrechnungen:

$(p \circ p)(1) = p(p(1)) = p(2) = 1,$
$(p \circ p)(2) = p(p(2)) = p(1) = 2,$
$(p \circ p)(3) = p(p(3)) = p(3) = 3,$
$(p \circ p)(4) = p(p(4)) = p(4) = 4.$

Analog für $q \circ q$.

Es gelten $p \circ p = id$ und $q \circ q = id$.

$$p \circ q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad q \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Daraus folgt $p \circ q = q \circ p$.

Einige Hilfsrechnungen:

$(p \circ p)(1) = p(p(1)) = p(2) = 1,$
$(p \circ p)(2) = p(p(2)) = p(1) = 2,$
$(p \circ p)(3) = p(p(3)) = p(3) = 3,$
$(p \circ p)(4) = p(p(4)) = p(4) = 4.$

Analog für $q \circ q$.

Es gelten $p \circ p = id$ und $q \circ q = id$.

$$p \circ q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad q \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Daraus folgt $p \circ q = q \circ p$.

ZÜ DS
©Dr. Werner Meixner
29/33

1. Geben Sie die $\circ$-Verknüpfungstafel für die Elemente aus U an.

Lösung

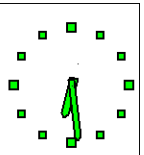
$\circ$	id	p	q	r
id	id	p	q	r
p	p	id	r	q
q	q	r	id	p
r	r	q	p	id

2. Beweisen Sie, dass die Menge U mit jedem Element $x \in U$ auch sein Inverses x^{-1} enthält (mit $x \circ x^{-1} = id$).

Lösung

Für jedes Element $x \in U$ gilt $x^2 = id$.

Damit ist jedes Element zu sich selbst invers.

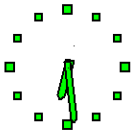


3. Aus den obigen Aussagen folgt, dass U eine Untergruppe von $\mathcal{S}_4$ ist.
   Ist die Gruppe U zyklisch ? Beweis!

Lösung

Nein!

Wäre die Gruppe zyklisch, dann müsste sie ein Element der Ordnung 4 enthalten.



Viel Erfolg bei der Endterm!!