Script **generated by TTT**

Title: Meixner: test2 (21.11.2012)

Date: Wed Nov 21 17:46:17 CET 2012

Duration: 89:52 min

Pages: 48

WS 2012/13

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2012WS/ds/uebung/

21. November 2012

---

1. Übungsbetrieb

1.1 Fragen und Probleme zum Übungsbetrieb

Bemerkung:

1. Die ZÜ unterstützt die Vorbereitung.
2. Die Folien der ZÜ liefern das vollständige Material für die Bearbeitung der Vorbereitungsaufgaben zu Hause.
3. Die ZÜ wird aufgezeichnet. Das ersetzt nicht die Anwesenheit.

Weitere Fragen?

---

2. Tipps

Neu: Zu jedem Übungsblatt wird es in Zukunft ein

Informationsblatt mit Hin.Ti's

geben, d. h. Hinweise und Tipps für eine erfolgreiche Lösung der Hausaufgaben.

Empfehlung:

- Versuchen Sie zunächst einige Minuten lang, ohne Hilfestellung auszukommen, und verwenden Sie die Tipps erst dann, wenn Sie nicht weiter kommen.
- Prüfen Sie abschließend, ob die Hinweise zu Ihrer Lösung passen.

3. Quiz:

3.1 Rechnen modulo n

Wir rechnen in $\mathbb{Z}_6$ in 3 Minuten, schriftlich!

Wieviel ist:

?

3. Quiz:

3.1 Rechnen modulo n

Wir rechnen in $\mathbb{Z}_6$ in 3 Minuten, schriftlich!

Wieviel ist:

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

?

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

Lösung:

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

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

!

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

e05.pdf - Adobe Acrobat Professional
File Edit View Document Comments Forms Tools Advanced Window Help
16 / 153 170%

Lösung:

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

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

!

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

ZÜ DS
©Dr. Werner Meixner
6/51

4. Thema: Konzepte der Abstraktion

4.1 Isomorphismus

Ein Isomorphismus vergleicht Bereiche,
die bis auf Bezeichnungsänderung identisch sind.

Ein Isomorphismus etabliert dadurch einen abstrakten Standpunkt,
von dem aus Dinge als im Wesentlichen gleich erscheinen,
d.h. eine gleiche Gestalt haben,
insbesondere unabhängig von den Bezeichnungen.

Berühmte Beispiele: Die Kardinalzahlen des Zählens (nach Cantor).

4.2 Homomorphismus

Mit einem Homomorphismus betrachtet man
eine Struktur unter einem gewissen abstrakten Aspekt.

Die Vertauschbarkeit wird benutzt um komplexe Operationen
durch einfachere Operationen zu ersetzen.

Beispiel 1: Wenn man die ganzen Zahlen unter dem Aspekt
„gerade Zahl“ bzw. „ungerade Zahl“ betrachtet, dann wird diese
Betrachtung durch den folgenden Homomorphismus etabliert.

$$f : \mathbb{Z} \ni x \mapsto (x \bmod 2) \in \mathbb{Z}_2 .$$

Beispiel 2: Wenn man die Zeit in Tagen mit je 24 Stunden zählt,
dann wird das modelliert durch den Homomorphismus

$$f : \mathbb{Z} \ni x \mapsto (x \bmod 24) \in \mathbb{Z}_{24} .$$

Bemerkung:
Man beachte die Darstellung der ganzen Zahlen durch die
Komponenten Fortschritt (Tage) und Wiederholung (24 Stunden).

Die Tage mit festgehaltener Uhrzeit
durchschreiten eine Restklasse
zur Untergruppe der durch 24 teilbaren Stundenzahlen.

Die Uhrzeit durchläuft zyklisch wiederholt die 24 Stunden.

4.3 Abstraktion durch Algebren

Unterschiedliche Rechenstrukturen werden durch Algebren auf
einen

gemeinsamen Nenner

gebracht und sind dann in gewisser Weise gleich.

Auch dadurch wird eine Abstraktion geleistet.

4.4 Äquivalenzrelationen

Äquivalenzrelation:

Eine binäre Relation $R \subseteq M \times M$, die reflexiv, transitiv und symmetrisch ist.

Äquivalenzklasse $[x]_R$ einer Äquivalenzrelation R mit Repräsentant x:

Die Menge A aller y, die in Relation $(y, x) \in R$ sind, i.Z. $A = [x]_R$.

Partition:

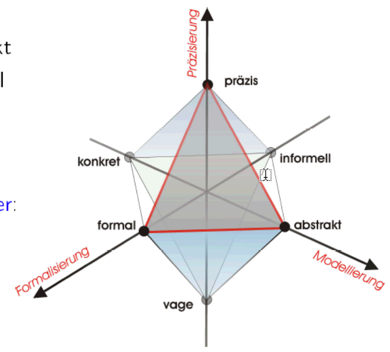
Menge aller Äquivalenzklassen einer Äquivalenzrelation = „Überdeckung einer Menge durch eine Menge von disjunkten Mengen"

Erinnerung an ZÜ 1:

Wissenschaftliche Schulung und Entwicklung
vollzieht sich im Spannungsfeld folgender Begriffspaare:

- vage — präzis
- konkret — abstrakt
- informell — formal

Darstellung im Oktaeder:



5. Vorbereitung auf TA Blatt 6

5.1 VA 1, Permutationen und Zyklen

Sei M eine endliche Menge und $z = (a_0, a_1, \ldots, a_{|M|-1})$ ein $|M|$-Tupel mit paarweise verschiedenen $a_i \in M$.

Dann ist die Abbildung

$$\pi_z : M \to M \text{ mit } \pi_z(a_i) = a_{(i+1) \bmod |M|)}$$

ein *Zyklus* der Länge $|M|$ mit *Basis* M und *Darstellung* z.

Für jeden Zyklus π bezeichne $M(\pi)$ die Basis von π.

Man kann π_z als zyklische Nachfolgerbildung in M auffassen.

5. Vorbereitung auf TA Blatt 6

5.1 VA 1, Permutationen und Zyklen

Sei M eine endliche Menge und $z = (a_0, a_1, \ldots, a_{|M|-1})$ ein $|M|$-Tupel mit paarweise verschiedenen $a_i \in M$.

Dann ist die Abbildung

$$\pi_z : M \to M \text{ mit } \pi_z(a_i) = a_{(i+1) \bmod |M|)}$$

ein *Zyklus* der Länge $|M|$ mit *Basis* M und *Darstellung* z.

Für jeden Zyklus π bezeichne $M(\pi)$ die Basis von π.

Man kann π_z als zyklische Nachfolgerbildung in M auffassen.

ZÜ DS ©Dr. Werner Meixner 5.1 VA 1, Permutationen und Zyklen 13/51

1. Wie viele Darstellungen
besitzt ein Zyklus der Länge 3?

Welchen Zyklus
stellt $z = (4, 1, 3, 2)$ dar und welche Basis hat der Zyklus?

Welche verschiedenen Darstellungen
hat ${\pi_z}^3$?

Ist ${\pi_z}^4$ ein Zyklus ?

Lösung:

Bemerkung:
Für Operationen f über einer Menge M, d.h. $f : M \to M$, gibt es die mehrfache Hintereinanderausführung der Operation f mit entsprechenden Schreibweisen. Es gilt

$$f^2 = f \circ f, \quad \text{und allgemein} \quad f^{n+1} = f \circ f^n \quad \forall n \in \mathbb{N},$$

d. h. für alle $n \in \mathbb{N}$ und $x \in M$

$$f^{n+1}(x) = f(f^n(x)), \quad \text{insbesondere } f^2(x) = f(f(x)).$$

Wie viele Darstellungen besitzt ein Zyklus der Länge 3?

Antwort: 3.

Begründung:
Sei π ein Zyklus der Länge 3 mit Basis $M(\pi) = \{a, b, c\}$. Für jede Darstellung $z = (a_1, a_2, a_3)$ von π gilt

$$a_1 \in M, \quad a_2 = \pi(a_1), \quad a_3 = \pi^2(a_1) = \pi(a_2).$$

Damit gibt es genau die folgenden drei Darstellungen

$$z_1 = (a, \pi(a), \pi^2(a)), \quad z_2 = (b, \pi(b), \pi^2(b)), \quad z_3 = (c, \pi(c), \pi^2(c)).$$

Welchen Zyklus stellt $z = (4, 1, 3, 2)$ dar und
welche Basis hat der Zyklus?

Antwort:

Die Basis von $z = (4, 1, 3, 2)$ ist $M_z = \{1, 2, 3, 4\}$.

Für den dargestellten Zyklus $\pi_z : M \to M$ gilt

$$\pi_z(1) = 3, \quad \pi_z(2) = 4, \quad \pi_z(3) = 2, \quad \pi_z(4) = 1.$$

Welche verschiedenen Darstellungen hat ${\pi_z}^3$?

Antwort:

Es gilt

$$\begin{aligned}
{\pi_z}^3(1) &= {\pi_z}^2(\pi_z(1)) = {\pi_z}^2(3) = \pi_z(\pi_z(3)) = \pi_z(2) = 4\,,\\
{\pi_z}^3(2) &= {\pi_z}^2(\pi_z(2)) = {\pi_z}^2(4) = \pi_z(\pi_z(4)) = \pi_z(1) = 3\,,\\
{\pi_z}^3(3) &= {\pi_z}^2(\pi_z(3)) = {\pi_z}^2(2) = \pi_z(\pi_z(2)) = \pi_z(4) = 1\,,\\
{\pi_z}^3(4) &= {\pi_z}^2(\pi_z(4)) = {\pi_z}^2(1) = \pi_z(\pi_z(1)) = \pi_z(3) = 2\,.
\end{aligned}$$

${\pi_z}^3$ ist ein Zyklus mit genau den folgenden 4 Darstellungen.

$z_1=(1,4,2,3)\,,\quad z_2=(2,3,1,4)\,,\quad z_3=(3,1,4,2)\,,\quad z_4=(4,2,3,1)\,.$

Ist ${\pi_z}^4$ ein Zyklus?

Antwort: Nein!

Begründung:
Es gilt

$$\begin{aligned}
{\pi_z}^4(1) &= \pi_z({\pi_z}^3(1)) = 1\,,\\
{\pi_z}^4(2) &= \pi_z({\pi_z}^3(2)) = 2\,,\\
{\pi_z}^4(3) &= \pi_z({\pi_z}^3(3)) = 3\,,\\
{\pi_z}^4(4) &= \pi_z({\pi_z}^3(4)) = 4\,.
\end{aligned}$$

${\pi_z}^4$ ist kein Zyklus, weil $|\{(\pi^4)^n(1)\,|\,n \in \mathbb{N}\}| = 1 \neq 4\,.$

Tatsächlich ist ${\pi_z}^4$ gleich der Identität id.

Zyklen ρ, σ heißen *disjunkt*, falls $M(\rho) \cap M(\sigma) = \emptyset$ gilt, d. h., falls deren Basismengen disjunkt sind.

Eine Menge Z von paarweise disjunkten Zyklen heißt *Zyklenpartition*.

Dabei bildet die Menge der Basismengen

$$P_Z = \{M(\pi)\,;\,\pi \in Z\}$$

eine Mengenpartition der Vereinigung der Basismengen

$$M(Z) = \bigcup_{\pi \in Z} M(\pi)\,.$$

Wir sagen, dass Z eine Zyklenpartition der Menge $M(Z)$ ist.

2. Welche Basis haben die Zyklen zu
$z_1 = (2,5),\ z_2 = (1),\ z_3 = (5,4,3,2,1)$?
Geben Sie eine extensionale Darstellung der Abbildungen π_{z_i} an!
Warum ist $Z = \{\pi_{z_1}, \pi_{z_2}, \pi_{z_3}\}$ keine Zyklenpartition von $[5]$?

Geben Sie eine extensionale Darstellung der Abbildungen π_{z_i} an!

Antwort:

Es gilt mit Auflistung der Funktionswerte

$$\pi_{z_1}(2) = 5\,,\quad \pi_{z_1}(5) = 2\,.$$

$$\pi_{z_2}(1) = 1\,.$$

$$\pi_{z_3}(1) = 5\,,\quad \pi_{z_3}(2) = 1\,,\quad \pi_{z_3}(3) = 2\,,\quad \pi_{z_3}(4) = 3\,,\quad \pi_{z_3}(5) = 4\,.$$

Warum ist $Z = \{\pi_{z_1}, \pi_{z_2}, \pi_{z_3}\}$ keine Zyklenpartition von $[5]$?

Antwort:

Offenbar sind die Zyklen nicht paarweise disjunkt.

Für die Basismengen gilt z. B. $M(\pi_{z_1}) \cap M(\pi_{z_3}) \neq \emptyset$.

Sei Z eine Zyklenpartition von $[n]$. Dann ist eine bijektive Abbildung $f_Z : [n] \to [n]$ gegeben für alle $i \in [n]$ durch

$$f_Z(i) = \pi(i), \quad \text{falls} \quad i \in M(\pi) \text{ und } \pi \in Z\,.$$

3. Zyklenpartitionen werden häufig durch eine Folge $z_1 z_2 \ldots z_k$ von Zyklusdarstellungen z_i definiert, wobei die Reihenfolge der z_i in der Folge keine Rolle spielt.

   Sei $Z = (4,5,1)(3)(2)$ eine Zyklenpartition.

   Beschreiben Sie die Abbildung f_Z extensional!

Lösung:

Für f_Z gilt mit Auflistung der Funktionswerte

$$f_Z(1) = 4\,,\quad f_Z(2) = 2\,,\quad f_Z(3) = 3\,,\quad f_Z(4) = 5\,,\quad f_Z(5) = 1\,.$$

4. Eine Funktion f sei gegeben durch die folgende Matrixdarstellung.

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

Berechnen Sie
$\{f^i(2)\,;\, i \in \mathbb{N}\}$, $\{f^i(3)\,;\, i \in \mathbb{N}\}$, $\{f^i(5)\,;\, i \in \mathbb{N}\}$!

Bestimmen Sie eine *Zyklendarstellung* von f,
d. h. eine Zyklenpartition Z von $[9]$,
so dass $f(i) = f_Z(i)$ für alle $i \in [9]$ gilt!

Lösung:

Durch Auswertung von $f_Z^i(x)$ erhält man

$$\{f_Z^i(2)\,;\, i \in \mathbb{N}\} = \{1, 8, 4, 2\}, \quad (1)$$
$$\{f_Z^i(3)\,;\, i \in \mathbb{N}\} = \{6, 9, 3\}, \quad (2)$$
$$\{f_Z^i(5)\,;\, i \in \mathbb{N}\} = \{7, 5\}. \quad (3)$$

Wir bezeichnen die Mengen in den Gleichungen (1), (2) und (3) entsprechend mit M_1, M_2 bzw. M_3. Dann definiert f je einen Zyklus f_i auf den Basismengen M_1, M_2 und M_3 mit den entsprechenden Darstellungen

$$z_1 = (1, 8, 4, 2), \quad z_2 = (6, 9, 3) \quad \text{bzw.} \quad z_3 = (7, 5).$$

Zyklenpartition bzw. Zyklendarstellung von f:

$$Z = (1, 8, 4, 2)\,(6, 9, 3)\,(7, 5).$$

5.2 VA 2, Abstrakte Ringe, elementare Eigenschaften

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

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

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. Gleichung: $a \odot b \;=\; (-a) \odot (-b)\,.$

- Es gilt

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

Daraus folgt $\quad -(a \odot b) = a \odot (-b)$.

Analog folgt $\quad -(a \odot b) = (-a) \odot b$.

Damit erhalten wir

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

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 ?

5.3 VA 3, Abstrakte Ringe, weitere Eigenschaften

Beweisen Sie:

1. Es gibt bis auf Isomorphie genau einen Ring $R = (S, \oplus, \odot, 0, 1)$ mit drei Elementen, d. h. $S = \{0, 1, a\}$.

   Insbesondere also muss R isomorph sein zum Ring $(\mathbb{Z}_3, +_3, \cdot_3, 0, 1)$.

Erinnerung: Sei $R = (S, \oplus, \odot, 0,)$ ein Ring. Nach Vorlesung ist $(S, \oplus, 0)$ eine abelsche Gruppe mit neutralem Element 0 und $(S, \odot, 1)$ ist ein Monoid mit neutralem Element 1. Außerdem gelten die beidseitigen Distributivgesetze. Für Ringe mit mehr als einem Element gilt stets $1 \neq 0$. Der Ring ist kommutativ, falls die Multiplikation kommutativ ist.

Beweis:

Eine Gruppe mit 3 Elementen ist notwendigerweise zyklisch, denn die Ordnung eines Elements ungleich dem Neutralen kann, nach dem Satz von Lagrange, nicht 2 sein, weil dann 2 Teiler der Gruppenordnung 3 sein müsste.

Jedes Element ungleich dem neutralen Element erzeugt die Gruppe. Die Verknüpfungstafel für $\oplus$ lautet deshalb wie folgt.

$\oplus$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

Dass diese Verknüpfungstafel eine Gruppe definiert, ergibt sich aus der Isomorphie zu $(\mathbb{Z}_3, +_3)$.

Auch die Verknüpfungstafel für die Multiplikation ergibt sich zwingend wegen

$$a \odot a = (1 \oplus 1) \odot (1 \oplus 1) = 1 \oplus 1 \oplus 1 \oplus 1 = 1$$

wie folgt:

$\odot$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Dass alle Ringaxiome erfüllt sind, zeigt man wiederum mithilfe der Isomorphie auf den Ring $(\mathbb{Z}_3, +_3, \cdot_3, 0,)$.

Es folgt, dass R ein Ring ist.

Die Eindeutigkeit von R ist eine Konsequenz der Herleitung, denn die Verknüpfungstafeln hatten sich zwingend ergeben.

Beweis:

R ist genau dann ein Körper, wenn $(S \setminus \{0\}, \odot,)$ eine kommutative Gruppe ist.

Zum Beweis genügt der Hinweis auf die Isomorphie mit $(\mathbb{Z}_3, +_3, \cdot_3, 0, 1)$, weil $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ bekanntlich ein Körper ist, wenn n eine Primzahl ist.

Wir geben aber auch einen direkten Beweis an, wie folgt.

Direkter Beweis:

Wir streichen aus der Verknüpfungstafel die Zeile bzw. Spalte der Multiplikation mit 0 und erhalten.

$\odot$	1	a
1	1	a
a	a	1

Offenbar definiert die Multiplikation eine Gruppe.
Sie ist isomorph zu $(\mathbb{Z}_2, +_2)$.

Definition:

Es heiße $y \in S \setminus \{0\}$ *co*-Nullteiler von $x \in S \setminus \{0\}$, falls $x \odot y = 0$.

Beispiel: In $\mathbb{Z}_8$ sind $2, 4, 6$ *co*-Nullteiler von 4.

3. Sei t_x die Anzahl der *co*-Nullteiler eines Ringelementes $x \in S \setminus \{0\}$ eines endlichen, kommutativen Ringes $(S, \oplus, \odot, 0, 1)$.

   Dann ist $t_x + 1$ ein Teiler der Anzahl $n = |S|$ aller Ringelemente.

Da $N_x \cup \{0\}$ eine additive Untergruppe von $(S, \oplus)$ ist,
gilt nach dem Satz von Lagrange,
dass $t_x + 1 = |N_x \cup \{0\}|$ ein Teiler von $|S|$ ist,
w.z.b.w.

Bemerkung:

Die Konsequenz der Aussage in dieser Teilaufgabe ist, dass
jeder endliche kommutative Ring,
dessen Anzahl von Elementen eine Primzahl ist,
notwendigerweise auch ein Körper ist!

5.4 VA 4, direkte Produkte von Ringen

Eine allgemeine Methode zur Konstruktion von
Algebren B aus gegebenen Algebren A_1 und A_2 ist
die Bildung von *direkten Produkten*.

Seien $A_1 = (S_1, \circ_1)$ und $A_2 = (S_2, \circ_2)$, dann ist das direkte
Produkt von A_1 und A_2 definiert als

$$A_1 \times A_2 = (S_1 \times S_2, \circ_1 \times \circ_2)$$

mit dem direkten Produkt $\circ_1 \times \circ_2$ der komponentenweisen
Verknüpfungen, so dass also für alle $x_1, y_1 \in S_1, x_2, y_2 \in S_2$ gilt

$$(x_1, x_2)(\circ_1 \times \circ_2)(y_1, y_2) = (x_1 \circ_1 y_1, x_2 \circ_2 y_2)\,.$$

5.4 VA 4, direkte Produkte von Ringen

Eine allgemeine Methode zur Konstruktion von
Algebren B aus gegebenen Algebren A_1 und A_2 ist
die Bildung von *direkten Produkten*.

Seien $A_1 = (S_1, \circ_1)$ und $A_2 = (S_2, \circ_2)$, dann ist das direkte
Produkt von A_1 und A_2 definiert als

$$A_1 \times A_2 = (S_1 \times S_2, \circ_1 \times \circ_2)$$

mit dem direkten Produkt $\circ_1 \times \circ_2$ der komponentenweisen
Verknüpfungen, so dass also für alle $x_1, y_1 \in S_1, x_2, y_2 \in S_2$ gilt

$$(x_1, x_2)(\circ_1 \times \circ_2)(y_1, y_2) = (x_1 \circ_1 y_1, x_2 \circ_2 y_2)\,.$$

1. Seien $(\mathbb{Z}_2, +_2)$ und $(\mathbb{Z}_3, +_3)$ die additiven Gruppen der ganzen Zahlen modulo 2 bzw. modulo 3. Dann ist das direkte Produkt $(\mathbb{Z}_2 \times \mathbb{Z}_3, +_2 \times +_3)$ eine kommutative Gruppe.

   Stellen Sie die Verknüpfungstafel auf für das direkte Produkt

$$+_2 \times +_3 .$$

Lösung:

$+_{2,3}$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(1,1)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$	$(0,0)$
$(0,2)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$	$(0,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,1)$	$(1,2)$	$(0,0)$	$(1,1)$	$(0,2)$
$(0,1)$	$(0,1)$	$(1,2)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$
$(1,2)$	$(1,2)$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$

Lösung:

Die additive Gruppe $(\mathbb{Z}_6, +_6)$ ist zyklisch.

Damit ist die Gruppe $(\mathbb{Z}_2 \times \mathbb{Z}_3, +_2 \times +_3)$ genau dann isomorph zu $(\mathbb{Z}_6, +_6)$, wenn sie ebenfalls zyklisch ist.

Sei $x = (1,1)$. Dann gilt

$$2x = (0,2),\ 3x = (1,0),\ 4x = (0,1),\ 5x = (1,2),\ 6x = (0,0).$$

Daraus folgt, dass $\mathrm{ord}(x) = 6$, d.h. die Gruppe ist zyklisch und damit isomorph zu $(\mathbb{Z}_6, +_6)$.

Lösung:

$\cdot_{2,3}$	$(0,0)$	$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(0,0)$	$(0,0)$					
$(1,1)$		$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$(0,2)$		$(0,2)$	$(0,1)$	$(0,0)$	$(0,2)$	$(0,1)$
$(1,0)$		$(1,0)$	$(0,0)$	$(1,0)$	$(0,0)$	$(1,0)$
$(0,1)$		$(0,1)$	$(0,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,2)$		$(1,2)$	$(0,1)$	$(1,0)$	$(0,2)$	$(1,1)$

Lösung:

$\cdot_6 \cong \cdot_{2,3}$	$0 \cong (0,0)$	$1 \cong (1,1)$	$2 \cong (0,2)$	$3 \cong (1,0)$	$4 \cong (0,1)$	$5 \cong (1,2)$
$0 \cong (0,0)$	$(0,0)$					
$1 \cong (1,1)$		$(1,1)$	$(0,2)$	$(1,0)$	$(0,1)$	$(1,2)$
$2 \cong (0,2)$		$(0,2)$	$4 \cong (0,1)$	$(0,0)$	$(0,2)$	$(0,1)$
$3 \cong (1,0)$		$(1,0)$	$(0,0)$	$3 \cong (1,0)$	$(0,0)$	$(1,0)$
$4 \cong (0,1)$		$(0,1)$	$(0,2)$	$(0,0)$	$4 \cong (0,1)$	$(0,2)$
$5 \cong (1,2)$		$(1,2)$	$(0,1)$	$(1,0)$	$(0,2)$	$1 \cong (1,1)$

Eine Ergänzung und Überprüfung der roten Einträge in der Tabelle zeigt eine Übereinstimmung mit der multiplikativen Halbgruppe des Ringes $\mathbb{Z}_6$.