Kapitel 8

Algebraische Strukturen

Verständnisfragen

Sachfragen

1. Was ist eine algebraische Operation?
2. Was ist eine Halbgruppe?
3. Nennen Sie Beispiele für Halbgruppen!
4. Was ist eine Gruppe?
5. Nennen Sie Beispiele für Gruppen!
6. Was ist eine abelsche Gruppe?
7. Nennen Sie Beispiele für abelsche Gruppen!
8. Nennen Sie Gruppen, die nicht abelsch sind!
9. Nennen Sie Beispiele für endliche Gruppen!
10. Ist $(\mathbb{Z}_n \setminus \{0\}, \odot)$ immer eine Gruppe?
11. Was ist eine Untergruppe?
12. Was ist ein Homomorphismus?
13. Was ist der Kern eines Homomorphismus?
14. Was ist das Bild eines Homomorphismus?
15. Wann ist ein Homomorphismus injektiv?
16. Was ist ein Isomorphismus?
17. Haben Kern und Bild eines Homomorphismus eine algebraische Struktur?
18. Was ist die Klein'sche Vierergruppe? Warum wurde Sie eingeführt?
19. Was ist ein Ring?
20. Nennen Sie Beispiele für Ringe und für Ringe mit Einselement!

21. Was ist ein Körper?
22. Was ist ein Nullteiler? Nennen Sie Beispiele!
23. Gibt es Ringe mit Nullteilern, die trotzdem kein Körper sind?
24. Wie ist ein Polynom über einem Körper definiert?
25. Wie werten Sie Polynome auf dem Computer aus?
26. Beschreiben Sie die Addition, Multiplikation und Division von Polynomen!
27. Vergleichen Sie einen Polynomring und den Ring der ganzen Zahlen!
28. Was ist ein Linearfaktor?
29. Beschreiben Sie die Linearfaktorzerlegung eines Polynoms!
30. Wie kann die Polynomdivision über $\mathbb{Z}_2$ zur Fehlererkennung in der Kanalcodierung verwendet werden?
31. Was ist eine Bool'sche Algebra?
32. Nennen Sie Beispiele von Bool'schen Algebren!
33. Ist in einer Bool'schen Algebra eine Teilordnung definiert?

Methodenfragen

1. Nachweisen können, dass eine Menge mit einer gegebenen Operation eine Halbgruppe, eine Gruppe oder eine abelsche Gruppe ist.
2. Nachweisen können, dass eine Teilmenge einer Gruppe eine Untergruppe darstellt.
3. Elementare Eigenschaften in einer Gruppe nachweisen können.
4. Nachweisen können, dass eine Abbildung ein Homomorphismus ist.
5. Den Kern und das Bild eines Homomorphismus bestimmen können.
6. Nachweisen können, dass ein Homomorphismus ein Isomorphismus ist.
7. Isomorphismen zwischen zwei gegebenen Gruppen mit gleicher Anzahl von Elementen finden können.
8. Nachweisen können, dass eine Menge mit zwei gegebenen algebraischen Operationen ein Ring oder ein Körper ist.
9. Die Polynomarithmetik in einem gegebenen Körper durchführen können.
10. Die Polynomarithmetik implementieren können.
11. Die Fehlererkennung mit Hilfe von Polynomen an Beispielen durchführen können.
12. Nachweisen können, dass eine Menge mit zwei gegebenen algebraischen Operationen und einer unären Operation eine Bool'sche Algebra ist.

Übungsaufgaben

1. Weisen Sie die Gruppeneigenschaften der Mengen $\{-1,1\} \subset \mathbb{Z}$ und $\{1,-1,i,-i\} \subset \mathbb{C}$ mit der Multiplikation als algebraische Operation nach!

   Lösung:
   Zuerst zu $M_1 = \{1,-1\}$.

   Die Multiplikation ist abgeschlossen, denn es ist $1 \cdot 1 = (-1) \cdot (-1) = 1 \in M_1$ und $(-1) \cdot 1 = 1 \cdot (-1) = -1 \in M_1$.

   Das Assoziativgesetz ist erfüllt:

   $$1 \cdot ((-1) \cdot 1) = -1 = (1 \cdot (-1)) \cdot 1 = 1 \cdot (1 \cdot (-1)) = (1 \cdot 1) \cdot (-1);$$
   $$(-1) \cdot ((-1) \cdot 1) = 1 = ((-1) \cdot (-1)) \cdot 1 = (-1) \cdot (1 \cdot (-1) = ((-1) \cdot 1) \cdot (-1).$$

   Das neutrale Element ist 1, wie in $\mathbb{Z}$. Das inverse Element für -1 ist -1 selbst wegen $(-1) \cdot (-1) = 1$. Als ist $(M_1, \cdot)$ eine Gruppe der Ordnung 2. Sie ist auch abelsch, wie Sie beim Nachweis der Abgeschlossenheit ganz oben bereits sehen.

   $M_2 = \{1,-1,i,-i\}$.

   Die Multiplikation ist abgeschlossen. Für die Elemente 1 und -1 erhalten Sie die gleichen Ergebnisse wie in M_1. Es ist $i \cdot i = -1$, so war die imaginäre Einheit gerade definiert. $i \cdot (-i) = (-i) \cdot i = 1$.

   $1 \cdot a = a$ und $(-1) \cdot a = -a$ für alle $a \in M_2$, damit ist die Abgeschlossenheit nachgewiesen; und auch die Existenz des neutralen Elements e ist bewiesen.

   Bleibt die Frage nach einem inversen Element für jedes $a \in M_2$ ungleich 1 zu beantworten. Das inverse Element zu -1 ist wieder -1 selbst, wie in M_1. Das inverse Element zu i ist $-i$, denn es gilt $i \cdot (-i) = 1$; inverses Element zu $-i$ ist i.

   M_2 ist abelsch, wie die bisher betrachteten Verknüpfungen beweisen. $(M_2, \cdot)$ ist eine Gruppe der Ordnung 4; fasst man M_1 ist eine Untergruppe von M_2.

2. Weisen Sie nach, dass für Gruppen $(G_1, \circ)$ und $(G_2, \bullet)$ das kartesische Produkt $G_1 \times G_2$ mit der algebraischen Operation $(x_1, y_1) \diamond (x_2, y_2) = (x_1 \circ x_2, y_1 \bullet y_2)$ eine Gruppe ist!

   Lösung:
   Die definierte Abbildung $\diamond$ ist eine algebraische Operation, denn da $x_1 \circ x_2 \in G_1$ und $y_1 \bullet y_2 \in G_2$ gilt ist auch

   $$(x_1, y_1) \diamond (x_2, y_2) = (x_1 \circ x_2, y_1 \bullet y_2) \in G_1 \times G_2.$$

   Das Assoziativgesetz ist erfüllt, da dies in den einzelnen Komponenten erfüllt ist:

   $$\begin{aligned}(x_1, y_1) \diamond ((x_2, y_2) \diamond (x_3, y_3)) &= (x_1 \circ (x_2 \circ x_3), y_1 \circ (y_2 \circ y_3)) \\ &= ((x_1 \circ x_2) \circ x_3, (y_1 \bullet y_2) \bullet y_3) \\ &= ((x_1, y_1) \diamond (x_2, y_2)) \diamond (x_3, y_3).\end{aligned}$$

   Das neutrale Element ist (e_1, e_2), falls e_1 das neutrale Element in G_1 und e_2 das in G_2 ist:

   $$(x, y) \diamond (e_1, e_2) = (x \circ e_1, y \bullet e_2) = (x, y).$$

   Die inversen Elemente sind gegeben als kartesisches Produkt der inversen Elemente:

   $$(x, y) \diamond (x^{-1}, y^{-1}) = (x \circ x^{-1}, y \bullet y^{-1}) = (e_1, e_2).$$

3. Beweisen Sie, dass für eine Gruppe $(G, \circ)$ und $a, b, c \in G$ $ab = ac \Rightarrow b = c$ gilt!

   Lösung:
   In einer Gruppe gibt es zu a ein Element a^{-1}, sodass $a \circ a^{-1} = e$ ist, wenn e das neutrale Element kennzeichnet.

   Dann gilt

   $$\begin{aligned} & a \circ b = a \circ c \\ \Leftrightarrow\ & a^{-1} \circ a \circ b = a^{-1} \circ a \circ c \\ \Leftrightarrow\ & e \circ b = e \circ c \\ \Leftrightarrow\ & b = c \end{aligned}$$

   Als Widerspruchsbeweis:

   Angenommen, es gibt zwei Elemente $b \neq c$ mit $a \circ b = a \circ c \Rightarrow b = c$. Dann gilt

   $$b = a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) = c,$$

   ein Widerspruch.

4. Bestimmen Sie alle Gruppen mit $n \leq 3$ Elementen durch Aufstellen der Verknüpfungstabellen!

   Lösung:
   Sie müssen das neutrale Element wählen und für die restlichen Elemente entscheiden, wie die inversen Elemente aussehen. In jeder Zeile und jeder Spalte muss jedes Element genau einmal auftreten, da die inversen Elemente und auch das neutrale Element eindeutig bestimmt sind.

   Dann bleibt für $n = 2$ und auch für $n = 3$ nur eine Möglichkeit übrig, nämlich die Tabellen 8.1 und 8.2.

$\circ$	e	a
e	e	a
a	a	e

Tabelle 8.1: Die Verknüpfungstabelle der Gruppe der Ordnung 2

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tabelle 8.2: Die Verknüpfungstabelle der Gruppe der Ordnung 3

5. Weisen Sie nach, dass die folgenden 6 Funktionen von $\mathbb{R} \setminus \{0, 1\}$ nach $\mathbb{R} \setminus \{0, 1\}$ mit der Komposition als algebraische Operation eine Gruppe bilden: $\iota(x) = x$, $\rho(x) = 1 - \frac{1}{x}$, $\sigma(x) = \frac{1}{1-x}$, $\alpha(x) = 1 - x$, $\beta(x) = \frac{x}{x-1}$ und $\gamma(x) = \frac{1}{x}$.

   Lösung:
   Die Verkettung ist abgeschlossen auf der Menge $\{\iota, \rho, \sigma, \alpha, \beta, \gamma\}$, beispielsweise gilt

   $$(\rho \circ \alpha)(x) = 1 - \frac{1}{\alpha(x)} = 1 - \frac{1}{1-x} = \beta(x).$$

   Die Verkettung ist immer assoziativ.

   Die Funktion ι ist das neutrale Element, es gilt immer $f \circ \iota = \iota \circ f = f$, was Sie nachrechnen können.

   α, β und γ sind zu sich selbst invers, es gilt beispielsweise

   $$(\beta \circ \beta)(x) = \frac{\beta(x)}{\beta(x) - 1} = \frac{x}{x - (x-1)} = x.$$

ρ^{-1} ist durch σ gegeben wegen

$$(\rho \circ \sigma)(x) = 1 - \frac{1}{\frac{1}{1-x}} = 1 - (1-x) = x.$$

Das inverse Element σ^{-1} ist ρ wegen

$$(\sigma \circ \rho)(x) = \frac{1}{1-\rho(x)} = \frac{1}{1-(1-\frac{1}{x})} = x.$$

In Tabelle 8.3 finden Sie die komplette Verknüpfungstafel; Sie erkennen darin auch, dass die Gruppe nichtabelsch ist; beispielsweise ist $\gamma \circ \sigma = \alpha$ und $\sigma \circ \gamma = \beta$.

$\circ$	ι	ρ	σ	α	β	γ
ι	ι	ρ	σ	α	β	γ
ρ	ρ	σ	ι	β	γ	α
σ	σ	ι	ρ	γ	α	β
α	α	γ	β	ι	σ	ρ
β	β	α	γ	ρ	ι	σ
γ	γ	β	α	σ	ρ	ι

Tabelle 8.3: Die Verknüpfungstafel zu Aufgabe 6

6. Weisen Sie nach, dass für das gleichschenklige Dreieck in Abbildung 8.1 die folgenden Abbildungen eine Gruppe mit der Verkettung als algebraische Operation bilden: I, die Identität, R, die Rotation im Uhrzeigersinn um den Inkreismittelpunkt, die N auf L, L auf M und M auf N abbildet; S, die entgegengesetzte Rotation gegen den Uhrzeigersinn, und A, B, C die Spiegelungen um die Achsen LX, MY und NZ.

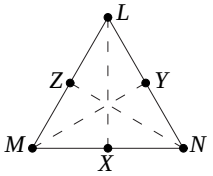

Abbildung 8.1: Ein gleichschenkliges Dreieck für Aufgabe 6

Lösung:
Die 6 Elemente stellen die möglichen Symmetrien dar; zwei Drehungen um jeweils 120° um den Inkreismittelpunkt, die Drehung um 0°, also die Identität und die drei Spiegelungen. Solche Symmetriegruppen sind der Ursprung der Gruppentheorie, man kann auch für andere geometrische Objekte wie beispielsweise das Quadrat, Fünfeck oder den Tetraeder oder Hexaeder entsprechende Symmetriegruppen bilden.

Die Verkettung der Operationen ist abgeschlossen, denn es gilt beispielsweise

$$R(L) = N, R(M) = L, R(N) = M,$$
$$A(L) = L, A(M) = N, A(N) = M,$$
$$A \circ R(L) = A(N) = M, A \circ R(M) = A(L) = L, A \circ R(N) = A(M) = N.$$

Dann ist offensichtlich $A \circ R = C$. Analog können Sie nachweisen, dass $R \circ A = B$. Die Komposition von Abbildungen ist immer assoziativ, in Tabelle 8.4 finden Sie alle 36 möglichen Verknüpfungen.

Die Gruppe ist nicht abelsch, auch das können Sie in der Tabelle ablesen, beispielsweise ist $A \circ R = C$ und $R \circ A = B$.

$\circ$	I	R	S	A	B	C
I	I	R	S	A	B	C
R	R	S	I	B	C	A
S	S	I	R	C	A	B
A	A	C	B	I	S	R
B	B	A	C	R	I	S
C	C	B	A	S	R	I

Tabelle 8.4: Die Verknüpfungstafel für Aufgabe 6

7. Weisen Sie nach, dass die Abbildung $A : (\mathbb{C} \setminus \{0\}, \cdot) \to (\mathbb{C} \setminus \{0\}, \cdot)$ mit $A(z) = |z|$ und $L : (\mathbb{R} \setminus \{0\}, \cdot) \to (\mathbb{R}, +)$ mit $L(x) = \mathrm{ld}\,(x^2)$ Homomorphismen sind. Bestimmen Sie den Kern und das Bild der Homomorphismen!

   Lösung:
   Sowohl in $\mathbb{R}$ als auch in $\mathbb{C}$ gilt $|x_1 \cdot x_2| = |x_1| \cdot |x_2|$.
   $N(A) = \{0\}$; $R(A) = \{z \in \mathbb{C} \mid Im(z) = 0, Re(z) \geq 0\}$.
   Auch L ist ein Homomorphismus, denn mit den Rechenregeln für den Logarithmus gilt

$$\begin{aligned} L(x \cdot y) &= \mathrm{ld}\,((xy)^2) \\ &= \mathrm{ld}\,(x^2 y^2) \\ &= \mathrm{ld}\,(x^2) + \mathrm{ld}\,(x^2) \\ &= L(x) + L(y). \end{aligned}$$

   L ist nicht injektiv, denn es gilt $L(x) = L(-x)$, der Kern ist gegeben durch $N(L) = \{1, -1\}$. L ist aber surjektiv, Urbilder für ein $y \in \mathbb{R}$ sind $x = \pm\sqrt{2^y}$; also ist $R(L) = \mathbb{R}$.

8. Ist $(M, \circ)$ eine Gruppe und $x \in M$. Die *Konjugation* ist durch $\gamma_x : M \to M, \gamma_x(n) = x \circ n \circ x^{-1}$ definiert. Weisen Sie nach, dass γ_x ein Isomorphismus und die Menge aller Konjugationen eine Untergruppe von $S(M)$ ist!

   Lösung:
   Eine Konjugation ist ein Homomorphismus, denn es gilt

$$\begin{aligned} \gamma_x(m_1 \circ m_2) &= x \circ (m_1 \circ m_2) \circ x^{-1} \\ &= x \circ m_1 \circ m_2 \circ x^{-1} \\ &= x \circ m_1 \circ x^{-1} \circ x \circ m_2 \circ x^{-1} \\ &= \gamma_x(m_1) \circ \gamma_x(m_2). \end{aligned}$$

   Es ist $N(\gamma_x) = \{e\}$, also ist eine Konjugation injektiv:

$$\begin{aligned} \gamma_x(m) = e &\Leftrightarrow x \circ m \circ x^{-1} = e, \\ &\Leftrightarrow m \circ x^{-1} = x^{-1} \circ e \\ &\Leftrightarrow m \circ x^{-1} = x^{-1} \\ &\Leftrightarrow m = x^{-1} \circ x \\ &\Leftrightarrow m = e. \end{aligned}$$

   Das Urbild für ein $m \in M$ ist $n = x^{-1} \circ m \circ x$:

$$\gamma_x(n) = x \circ x^{-1} \circ m \circ x \circ x^{-1} = m.$$

Jetzt zur Untergruppeneigenschaft:

Die Identität ist eine Konjungation, mit $x = e$. Die Abgeschlossenheit folgt aus

$$(\gamma_x \circ \gamma_y)(n) = x \circ y \circ n \circ y^{-1} \circ x^{-1} = \gamma_{x \circ y}(n).$$

Für jede Konjugation ist die Inverse gegeben durch $\gamma_x^{-1} = \gamma_{x^{-1}}$; also ist die Menge aller Konjugationen eine Untergruppe von $S(M)$.

9. Weisen Sie nach, dass die Gruppen aus Aufgabe 5 und 6 isomorph sind!

Lösung:
Die Notation in den Tabellen 8.3 und 8.4 wurde schon so gewählt, dass man die Isomorphie direkt ablesen kann. Die Isomorphie F ist definiert durch

$$F(I) = \iota, F(R) = \rho, F(S) = \sigma, F(A) = \alpha, F(B) = \beta, F(C) = \gamma.$$

Eine weitere, zu diesen beiden Gruppen isomorphe Gruppe ist gegeben durch die sechs 2×2 Matrizen

$$i = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), r = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right), s = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right),$$
$$a = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), b = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), c = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right),$$

wenn die Matrixarithmetik mit modularer Arithmetik in $\mathbb{Z}_2$ durchgeführt wird. Auch hier ist die Isomorphie schon durch die Bezeichnungen gegeben. Und zu S_3, der Gruppe der Permutationen auf der Menge $\{0, 1, 2\}$ finden Sie ebenfalls leicht eine Isomorphie!

10. Weisen Sie die Rechenregeln eines Rings in Satz 8.8 nach!

Lösung:
$\forall a \in R\, a \cdot 0 = 0 \cdot a = 0$:

Es ist $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, denn im Ring R ist das Distributivgesetz erfüllt. $(R, +)$ ist eine abelsche Gruppe, dort ist das neutrale Element der Addition eindeutig bestimmt, also ist $0 \cdot a = 0$. Analog beweisen Sie $a \cdot 0 = 0$.

$\forall a, b \in R\, (-a) \cdot b = -a \cdot b = a \cdot (-b)$:

Aus $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$ folgt $(-a) \cdot b = -a \cdot b$. Analog ergibt sich $a \cdot (-b) = -a \cdot b$.

$\forall a, b \in R\, (-a) \cdot (-b) = a \cdot b$:

Mit den eben nachgewiesenen Regeln ist $(-a) \cdot (-b) = -(a \cdot (-b)) = a \cdot b$.

11. Weisen Sie für den Körper mit vier Elementen und den Verknüpfungstafeln 8.7 und 8.8 auf Seite 208 die Distributivgesetze nach!

Lösung:
Die Additionstabelle 8.8 ist symmetrisch bezüglich der Diagonale. Das neutrale Element ist 0. $(R, +)$ eine abelsche Gruppe.

Die Multiplikationstablle 8.7 zeigt, dass 1 das neutrale Element der Multiplikation ist. Das Assoziativgesetz ist ebenfalls erfüllt, was Sie exemplarisch nachprüfen sollten. Also ist $(R, \cdot)$ eine Halbgruppe.

Bleibt das Distributivgesetz zu überprüfen. Auch das nur exemplarisch, interessant sind nur die Fälle, bei denen die Klammer nicht mit 0 oder 1 multipliziert werden. Es ist beispielsweise

$$a \cdot (1 + b) = a \cdot a = b, a \cdot 1 + a \cdot b = a + 1 = b$$

und

$$(b + 1) \cdot a = a \cdot a = b, b \cdot a + 1 \cdot a = 1 + a = b.$$

Tabelle 8.5: Eine Addition?

$\diamond$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Tabelle 8.6: Eine Multiplikation?

$\times$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

12. Definieren die Verknüpfungstafeln 8.5 und 8.6 für die Menge $\{a,b,c,d\}$ einen Körper?

    Lösung:
    Die Tabellen definieren zwei abelsche Gruppen, bleibt, die Distributivgesetze zu überprüfen. Es gilt $c \times (c \diamond d) = c \neq c \times c \diamond c \times d = a$.

    Also lautet die Antwort *Nein*.

13. Ist in den Körpern $\mathbb{Z}_5$ und $\mathbb{Z}_7$ die Gleichung $x^2 = 2$ lösbar? Wenn ja, wie sieht die Lösung aus?

    Lösung:
    In $\mathbb{Z}_7$ hat die Gleichung die beiden Lösungen $x = 3, x = 4$, denn es gilt $3 \cdot 3 = 9 \equiv 2 \bmod 7$ und $16 \equiv 2 \bmod 7$. In $\mathbb{Z}_5$ existiert keine Lösung.

14. Berechnen Sie Summe und Produkt der Polynome $p(x) = x^6 + x^3 - 1$ und $q(x) = x^4 + x^3 + x$ über $\mathbb{R}$, $\mathbb{Z}_3$ und $\mathbb{Z}_2$!

    Lösung:
    Die Summen: Über $\mathbb{R}$ und $\mathbb{Z}_3$: $(p+q)(x) = x^6 + x^4 + 2x^3 + x - 1$; über $\mathbb{Z}_2$ $(p+q)(x) = x^6 + x^4 + x - 1$.

    Die Produkte: Über $\mathbb{R}$ und $\mathbb{Z}_3$: $(p \cdot q)(x) = x^{10} + x^9 + 2x^7 + x^6 - x^3 - x$, über $\mathbb{Z}_2$: $(p \cdot q)(x) = x^{10} + x^9 + x^6 - x^3 - x$.

15. Dividieren Sie das Polynom $p_1(x) = x^5 - 1$ mit Rest durch $q_1(x) = x^3 - 1$ und $p_2(x) = -144 - 23x^2 + 2x^4$ durch $q_2(x) = -24 - 6x + 4x^2 + x^3$.

    Lösung:
    $r_1(x) = x^2$, $s_1(x) = x^2 - 1$ und $r_2(x) = 2x - 8$, $s_2(x) = 9x^2 + 48x - 336$. ???

16. Berechnen Sie die Linearfaktorzerlegung des Polynoms $x^6 - 4x^4 - 4x^2 + 16$ über den Körpern $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$!

    Lösung:
    Nur über $\mathbb{C}$ zerfällt das Polynom in Linearfaktoren:

    $$p(x) = (x-2)(x+2)(x-\sqrt{2})(x+\sqrt{2})(x-i\sqrt{2})(x+i\sqrt{2}).$$

17. Setzen Sie die Matrix $\left(\begin{smallmatrix} 3 & -5 \\ 2 & 1 \end{smallmatrix}\right)$ als Variable x in das Polynom $x^2 + 2x + 5$ ein! Setzen Sie in das gleiche Polynom die Zahl 3 ein und berechnen Sie das Ergebnis in $\mathbb{Z}$ und $\mathbb{Z}_5$!

    Lösung:
    $\left(\begin{smallmatrix} 0 & -30 \\ 12 & -2 \end{smallmatrix}\right)$, in $\mathbb{Z}$: 20, in $\mathbb{Z}_5$: 0.

18. Zeigen Sie, dass alle Elemente aus $\mathbb{Z}_6$, wenn Sie diese in das Polynom $p(x) = x^3 - x$ einsetzen, als Ergebnis 0 ergeben. Welche Eigenschaft von $\mathbb{Z}_6$ verursacht dies?

    Lösung:
    Es gilt immer $x^3 = x$.

19. Implementieren Sie in der objektorierten Programmiersprache Ihrer Wahl eine Klasse, die Polynome und die Polynomarithmetik, insbesondere die Polynomdivision, zur Verfügung stellt!

Lösung:

```
//-------------------------------------------------------------
// vlPolynom.java
// Implementierung von Polynomen und der Polynomarithmetik
// über den reellen Zahlen (Datentyp double).
// -------------------------------------------------------------
// Autor:           Manfred Brill
// Letzte Änderung: 22. 06. 2004
//-------------------------------------------------------------
public class vlPolynom {

    public vlPolynom() {
        degree = 0;
        a = new double[1];
        a[0] = 0.0;
    }

    //! Konstruktor mit Grad, ohne Koeffizienten
    public vlPolynom(int n) {
        a = new double[n+1];
        degree = n-1;
        for (int i=0; i<=degree; i++) a[i]=0.0;
    }

    //! Konstruktor mit Grad und Feld mit Koeffizienten
    public vlPolynom(int n, double[] c) {
        a = new double[n+1];
        degree = n-1;
        for (int i=0; i<=degree; i++) a[i] = c[i];
    }

    //! Kopierkonstruktor
    public vlPolynom(vlPolynom copy) {
        a = new double[copy.getDegree()+1];
        degree = copy.getDegree();

        for (int i=0; i<=degree; i++) a[i] = copy.getCoefficient(i);
    }

    //! Grad zurückgeben
    public int getDegree() {
        return degree;
    }

    //! Grad setzen
    public void setDegree(int n) {
        degree=n;
    }

    //! Koeffizienten setzen
    public void setCoefficients(int n, double c[]) {
        degree = n-1;
        a = new double[n];
```

```
        for (int i=0; i<=degree; i++) a[i] = c[i];
    }

    //! Koeffizient i setzen
    public void setCoefficient(int i, double c) {
        a[i] = c;
    }
    //! Koeffizienten abfragen
    public void getCoefficients(double c[]) {
        for (int i=0; i<=degree; i++) c[i] = a[i];
    }

  //! i-ter Koeffizient abfragen
  public double getCoefficient(int i) {
        return a[i];
  }

  //! Auswerten des Polynoms
  public double eval(double x) {
        double value;

        value = a[degree+1];
        for (int i=degree; i>=0; i--) {
            value = x*value + a[i];
        }
        return value;
  }

  //! Polynom-Addition
  public void add(vlPolynom p) {

        int i, maxdegree, mindegree, d;

        d = p.getDegree();

        if (this.degree >= d) {
            for (i=0; i<=d; i++) a[i] += p.getCoefficient(i);
        }
        else {
            double help[] = new double[degree+1];

            for (i=0; i<=degree; i++) help[i] = a[i];
            // Grad vergrößern und Koeffizienten neu anlegen

            a = new double[d+1];

            for (i=0; i<=degree; i++) a[i] = help[i] + p.getCoefficient(i);

            for (i=degree+1; i<=d; i++) a[i] = p.getCoefficient(i);
            degree = d;
        }
    }

    //! Polynom-Multiplikation
    /** Voraussetzung: q[m] != 0;
     *  Wird zur Zeit nicht überprüft!
     */
    public void divide(vlPolynom q, vlPolynom s, vlPolynom r) {
```

```
        int i, j, m = q.getDegree();

        double ahelp[] = new double[degree+1], qc[] = new double[m+1],
               sc[] = new double[degree - m+1], rc[] = new double[m];

        // Koeffizienten kopieren
        for (i=0; i<= degree; i++)
             ahelp[i] = a[i];
        q.getCoefficients(qc);

        for (i=degree-m; i>= 0; i--) {
            sc[i] = ahelp[m+i]/qc[m];
            for (j=m+i-1; j>=i; j--)
                ahelp[j] -= sc[i]*qc[j-i];
        }

        for (i=0; i<= m-1; i++)
            rc[i] = ahelp[i];

        s.setCoefficients(degree-m+1, sc);
        r.setCoefficients(m, rc);
    }

    //! Polynom-Multiplikation
    public vlPolynom multiply(vlPolynom q) {
         int i, j, pd, qd, deg, min;
         double sum;

         qd = q.getDegree();
         deg = degree+qd;

         vlPolynom result = new vlPolynom(deg+1);

         for (i=0; i<=deg; i++) {
            sum = 0.0;
            if (i > degree)
                min = degree;
            else
                min = i;

            for (j=0; j<=i; j++) {
                min = i-j;
                if (j <= degree && i-j <= qd)
                      sum += a[j]*q.getCoefficient(i-j);
            }
            result.setCoefficient(i, sum);
         }
         return result;
     }

    public void print() {
        System.out.println("Ausgabe einer Instanz der Klasse vlPolynom");
        System.out.println("Grad des Polynoms: " + degree);

        for (int i=0; i <= degree; i++) {
            System.out.println("Index " + i + ": " + a[i]+" ");
        }
    }
```

```
    private int degree;
    private double a[];
}
```

20. Zeigen Sie, dass die Menge $\mathbb{B} = \{n \in \mathbb{N} \mid n|105\}$ mit $\boxdot = \text{ggT}$, $\boxplus = \text{kgV}$, $\mathbf{0} = 1$, $\mathbf{1} = 105$ und $\diagdown x$ als größtes Element $y \in \mathbb{B}$ mit $\text{ggT}(x, y) = 1$ eine Boolesche Algebra ist! Finden Sie eine Potenzmenge $\mathbb{P}(M)$, die zu $\mathbb{B}$ isomorph ist!

Lösung:
Die Primzahlfaktorisierung von 105 ist gegeben durch $105 = 3 \cdot 5 \cdot 7$. Also ist

$$\mathbb{B} = \{1, 3, 5, 7, 15, 21, 35, 105\}.$$

Die Axiome aus Definition 8.13 müssen nachgerechnet werden.

- $x \boxplus \mathbf{0} = x$, $x \boxdot \mathbf{1} = 1$:

Es ist $x \boxplus \mathbf{0} = \text{kgV}(x, 1) = x$. Die Aussage für die Multiplikation ist ebenfalls erfüllt, denn es gilt $x \boxdot \mathbf{1} = \text{ggT}(x, 105) = x$, denn jedes $x \in \mathbb{B}$ ist ein Teiler von 105.

- $x \boxplus \diagdown x = \mathbf{1}$, $x \boxdot \diagdown x = \mathbf{0}$:

Nach der Definition ist $\diagdown x = \frac{105}{x}$. Dann gilt

$$x \boxplus \diagdown x = \text{kgV}(x, \frac{105}{x})0 = \frac{x \cdot \frac{105}{x}}{1} = 105 = \mathbf{1}.$$

Es gilt

$$x \boxdot \diagdown x = \text{ggT}(x, \frac{105}{x}) = 1 = \mathbf{0}.$$

In $\mathbb{B}$ sind die komplementären Teiler relativ prim!

- $(x \boxplus y) \boxplus z = x \boxplus (y \boxplus z)$, $(x \boxdot y) \boxdot z = x \boxdot (y \boxdot z)$:

Es ist $\text{ggT}(\text{ggT}(x, y), z) = \text{ggT}(x, \text{ggT}(y, z))$ und $\text{kgV}(\text{kgV}(x, y), z) = \text{kgV}(x, \text{kgV}(y, z))$. Diese Aussagen wurden nicht im Kapitel über Zahlentheorie bewiesen; aber das sollte nicht schwer fallen. Man könnte beispielsweise einen Widerspruchsbeweis führen!

- $x \boxplus y = y \boxplus x$, $x \boxdot y = y \boxdot x$:

Es ist $\text{ggT}(x, y) = \text{ggT}(y, x)$ und $\text{kgV}(x, y) = \text{kgV}(y, x)$.

- $x \boxplus (y \boxdot z) = x \boxplus y \boxdot x \boxplus z$, $x \boxdot (y \boxplus z) = x \boxdot y \boxplus x \boxdot z$:

Auch dies ist wieder auf Grund von zahlentheoretischen Aussagen erfüllt:

$$\text{kgV}(x, \text{ggT}(y, z)) = \text{ggT}(\text{kgV}(x, y), \text{kgV}(x, z)),$$
$$\text{ggT}(x, \text{kgV}(y, z)) = \text{kgV}(\text{ggT}(x, y), \text{ggT}(x, z)).$$

$\mathbb{B}$ hat wie oben angegeben 8 Elemente. Dann ist diese Boolsche Algebra isomorph zu einer Algebra mit einer Potenzmenge $\mathbb{P}(M)$ einer Menge mit $|M| = 3$, beispielsweise $M = \{a, b, c\}$. Diese Boolsche Algebra ist dann gegeben durch $(\mathbb{P}(M), \cup, \cap, \setminus, \emptyset, M)$.

21. Ersetzen Sie in Aufgabe 20 die Zahl 105 durch eine Primzahl und suchen Sie eine dazu isomorphe Boolesche Algebra!

Lösung:
Die Trägermenge enthält nur 2 Elemente, die 1 und die Primzahl selbst. Diese Boolsche Algebra ist isomorph zur kleinst möglichen Boolschen Algebra mit zwei Elementen.

22. Beweisen Sie die De Morgan'sche Regel in einer Booleschen Algebra aus Satz 8.17 und die Absorptionsregel $\forall\, x, y \in \mathbb{B}\ x \boxdot (x \boxplus y) = x$ aus Satz 8.16!

Lösung:
Zuerst überlegen wir uns, dass das Element y mit $x \boxplus y = \mathbf{1} \wedge x \boxdot y = \mathbf{0}$ eindeutig bestimmt ist als $y = \diagdown x$.

Sind x und y beliebige Elemente der Algebra $\mathbb{B}$, die die Behauptung erfüllen, dann gilt

$$y = y \boxplus \mathbf{0} = y \boxplus x \boxdot \diagdown x = (y \boxplus x) \boxdot (y \boxplus \diagdown x).$$

und

$$(y \boxplus x) \boxdot (y \boxplus \diagdown x) = \mathbf{1} \boxdot (y \boxplus \diagdown x) = (y \boxplus \diagdown x).$$

Genauso gilt

$$\diagdown x = \diagdown x \boxplus \mathbf{0} = \diagdown x \boxplus x \boxdot \diagdown y.$$

Dann ist

$$\diagdown x \boxplus x \boxdot y = (\diagdown x + x) \boxdot (\diagdown x \boxplus y) = (x \boxplus \diagdown x) \boxdot (y \boxplus \diagdown x) = \mathbf{1} \boxdot (y \boxplus \diagdown x) = (y \boxplus \diagdown x).$$

Dann folgt aber insgesamt $y = \diagdown x$.

Es wird nur die erste de Morgan'sche Regel bewiesen, die zweite folgt analog. Es ist

$$\begin{aligned}(x \boxplus y) \boxplus (\diagdown x \boxdot \diagdown y) &= ((x \boxplus y) \boxplus \diagdown x) \boxdot ((x \boxplus y) \boxplus \diagdown y) \\ &= (\mathbf{1} \boxplus y) \boxdot (x \boxplus \mathbf{1}) = \mathbf{1}.\end{aligned}$$

und

$$\begin{aligned}(x \boxplus y) \boxdot ((\diagdown x \boxdot \diagdown y) &= ((x \boxdot \diagdown x) \boxdot \diagdown y) \boxplus (\diagdown x \boxdot (y \boxdot \diagdown y)) \\ &= (\diagdown y \boxdot \mathbf{0}) \boxplus (\diagdown x \boxdot \mathbf{0}) = \mathbf{0}.\end{aligned}$$

Dann ist mit der Überlegung zu Beginn der Lösung $\diagdown(x \boxplus y) = \diagdown x \boxdot \diagdown y$.

Die Absorptionsregel $\forall\, x, y \in \mathbb{B}\ x \boxdot (x \boxplus y) = x$:

$$x \boxdot (x \boxplus y) = (x \boxplus \mathbf{0}) \boxdot (x \boxplus y) = x \boxplus \mathbf{0} \boxdot y = x \boxplus y \boxdot \mathbf{0} = x \boxplus \mathbf{0} = x.$$

23. Weisen Sie nach, dass in einer Booleschen Algebra $x \leq y \Leftrightarrow x \boxplus y = y$ und $x \leq y \Leftrightarrow \diagdown y \leq \diagdown x$ gelten.

Lösung:
Aus $x \boxplus y = y$ folgt

$$x \boxdot y = x \boxdot (x \boxplus y) = x$$

mit dem Absorptionsgesetz aus Satz 8.16. Dann ist $x \leq y$.

$x \leq y$ ist äquivalent zu $x \boxdot y = x$. Dann folgt

$$x \boxplus y = (x \boxdot y) \boxplus y = y,$$

wieder mit Satz 8.16.

Die Aussage $x \leq y \Leftrightarrow \diagdown y \leq \diagdown x$ folgt mit den de Morgan'schen Regeln in Satz 8.17 und der eben bewiesenen Äquivalenz:

$$x \leq y \Leftrightarrow x \boxdot y = x \Leftrightarrow x \boxplus y = y \Leftrightarrow \diagdown(\diagdown x \boxdot \diagdown y) = y \Leftrightarrow \diagdown y \boxdot \diagdown x = \diagdown y.$$