Zusammenfassung Algebra

Bachelorstudium Informatik HSZ-T

Benjamin Bütikofer

3. Juli 2012

Inhaltsverzeichnis

1. Aussagen, Junktoren und Quantoren

1.1. Aussagen

Die Person X hat Übergewicht	Aussageform	Es kommen eine oder mehrere Variablen frei vor.
Esel haben lange Ohren	Aussage (wahr)	Es kann einen Wahrheitswert (wahr/falsch) zugeordnet werden.

1.2. Junktoren

$=:$	ist definiert als	
$\neg A$	**nicht** A	Ist genau dann wahr, wenn A falsch ist
$A \wedge B$	A **und** B	Ist genau dann wahr, wann A und B wahr sind
$A \vee B$	A **oder** B	Ist genau dann wahr, wann A oder B oder beide wahr sind
$A \Rightarrow B$	A **impliziert** B	Ist genau dann wahr, wenn $\neg A \vee B$ wahr ist
$A \Leftrightarrow B$	A ist **äquivalent** mit B	$A \Rightarrow B$ und $B \Rightarrow A$ ist wahr

a	b	$a \wedge b$	$a \vee b$	$a \Rightarrow b$	$a \Leftrightarrow b$
w	w	w	w	w	w
w	f	f	w	f	f
f	w	f	w	w	f
f	f	f	f	w	w

Tab. 1.3.: Wahrheitstabelle zu den Junktoren

1.2.1. Gültige Äquivalenzen

1. Doppelte Negation: $\neg\neg A \Leftrightarrow A$

2. Kommutativität: $A \wedge B \Leftrightarrow B \wedge A$ und $A \vee B \Leftrightarrow B \vee A$
3. Assoziativität: $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$ und $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$
4. Distributivität: $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ und $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
5. DeMorgan: $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ und $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$

1.3. Quantoren

$\forall A(x)$	Für alle x gilt, sie haben die Eigenschaft A
$\forall \in K A(x)$	Für alle x aus K gilt, sie haben die Eigenschaft A
$\exists A(x)$	Es gibt (min.) ein x mit der Eigenschaft A
$\exists \in K A(x)$	Es gibt (min.) ein x aus K welches die Eigenschaft A besitzt.

1.3.1. Vertauschungsregeln

unbeschränkte Quantoren	$\forall x A(x) \Leftrightarrow \neg\exists x \neg A(x)$
beschränkte Quantoren	$\forall x \in K A(x) \Leftrightarrow \neg\exists x \in K \neg A(x)$
unbeschränkte Quantoren	$\forall x \in K A(x) \Leftrightarrow \forall x(x \in K \Rightarrow A(x)$
unbeschränkte Quantoren	$\exists x \in K A(x) \Leftrightarrow \exists x(x \in K \wedge A(x))$

1.3.2. Wichtige formale Ausdrücke

Alle geraden Zahlen	$\exists_y \in \mathbb{N} : 2y = x$
Alle ungeraden Zahlen	$\forall_y \in \mathbb{N} : 2y \neq x$
Es gibt eine nat. Zahl > 5	$\exists_x \in \mathbb{N} : x > 5$
Es gibt unendlich viele n	$\forall_x \in \mathbb{N} : (\exists_y \in \mathbb{N} : (x < y))$
Jede Zahl > 5 erfüllt die Eigenschaft E(x)	$\forall_x(x > 5 \Rightarrow E(x))$
Es gibt genau ein n mit der Eigenschaft E(x)	$\exists_x E(x) \wedge \forall_{x,y}(E(x) \wedge E(y) \Rightarrow x = y)$
Min. eine gerade Zahl hat die Eigenschaft E(x)	$\exists_x \in \mathbb{N}(\exists_y \in \mathbb{N} \vert 2y = x \Rightarrow E(x))$

Es gibt mehrere $\mathbb{P}$ mit der Eigenschaft E(x)	$\exists_{x,y}(x \in \mathbb{P} \wedge y \in \mathbb{P} \wedge E(x) \wedge E(y) \wedge x \neq z)$
$x = y$	$\forall_z(z \in X \Leftrightarrow z \in Y)$
$x = y$	$(x \subset y) \wedge (y \subset x)$
$x \subset y$	$\forall_z(z \in X \Rightarrow z \in Y)$

2. Mengen

2.1. Allgemein

Eine Menge ist die Zusammenfassung von (mathematischen) Objekten zu einem neuen Ganzen, welches für sich selbst genommen wieder ein mathematisches Objekt darstellt. Weiter gelte das *Prinzip der extensionalen Gleichheit*, welches wie folgt lautet:

Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente enthalten.

$A \in B$	A ist Element von B	
$A \subset B$	A ist Teilmenge von B	Jedes Element von A kommt in B vor
$A \subseteq B$	echte Teilmenge	Wenn $A \subset B$ und $A \neq B$ ist
$A \cap B$	Schnittmenge	Alle Elemente die zu A sowie zu B gehören
$A \cup B$	Vereinigungsmenge	Alle Elemente die zu A oder zu B oder zu beiden gehören
$A \setminus B$	Differenzmenge	Alle Elemente die zu A aber nicht zu B gehören
$\emptyset$	Leeremenge	
$\wp(A)$	Potenzmenge	$\wp(A) := \{x \mid x \subset A\}$

2.2. Rechenregeln

1. Kommutativität der Vereinigung und des Schnittes:

$$A \cup B = B \cup A \text{ und } A \cap B = B \cap A$$

2. Assoziativität:

$$A \cap (B \cap C) = (A \cap B) \cap C \text{ und } A \cup (B \cup C) = (A \cup B) \cup C)$$

3. Distributivität:

$$A \cap (B \cup C)?(A \cap B) \cup (A \cap C) \text{ und } a \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

4. Idempotenz:

$$A \cap A = A \text{ und } A \cup A = A$$

5. De Morgan

$$(C \setminus A) \cap (C \setminus B) = C \setminus (A \cup B) \text{ und } (C \setminus A) \cup (C \setminus B) = C \setminus (A \cap B)$$

2.3. Mengenbildung

2.3.1. Leeremenge

Die Leeremenge ist Teilmenge von jeder Menge da jedes Element der Leermenge Teil jeder Menge ist.

2.3.2. Vereinigung

Ist A eine Menge von Mengen, dann definieren wir die *Vereinigung* $\bigcup A$ von A als die Menge, welche alle Dinge enthält die ein Element eines Elementes von A sind.

$$x \in \cup A \Leftrightarrow \exists Y \in A(x \in Y).$$

A ist eine Menge von Mengen:

$$\cup A = \{x | \forall_X \in A(x \in X)\}$$
$$\cup\{A, B, C\} = A \cup B \cup C = \{x | x \in A \vee x \in B \vee x \in C\}$$
$$X \cup Y = \{x | x \in Y \vee x \in X\}$$

2.3.3. Schnittmenge

Ist A eine nicht leere Menge von Mengen, dann definieren wir die Schnittmenge $\bigcap A$ von A, als die Menge die alle Dinge enthält, die ein Element von jedem Element von A sind.

$$x \in \cap A \Leftrightarrow \forall Y \in A(x \in Y).$$

2.3.4. Potenzmenge

die Potenzmenge von A ist die Menge aller Teilmengen inkl. der Leerenmenge von A.
$\wp(\emptyset) = \{\emptyset\} \neq \emptyset$
$\wp(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$
$\wp(A) \cup \wp(B) \subset \wp(A \cup B)$

3. Relationen und Funktionen

3.1. Begriffe

3.1.1. Tupel

Ein Tupel ist ein primitives Objekt. Zwei Tupel sind genau dann identisch wenn in beiden Tupeln das gleiche steht: **Beispiel:** Die geordneten Paare (x, y) und (y, z) sind genau dann gleich wenn $x = y = z$ gilt.

3.1.2. Kartesisches Produkt

Das Kreuzprodukt zweier Mengen: A = 0,1,2, B = s,t. AxB = (0,s), (0,t), (1,s), (1,t), (2,s), (2,t) . Das Kreuzprodukt zweier Mengen ist wieder eine Menge und zwar eine Menge aus allen Kombinationsmöglichkeiten von Elementen aus der ersten Menge und der zweiten Menge in Tupelschreibweise geschrieben. Kann auch in einer Matrix geschrieben werden.

3.2. Relationen

3.2.1. Definition

Seien A und B zwei Mengen. Die Teilmenge R des Kreuzprodukts AxB heisst Relation zwischen A und B. $R \subset A \times B$.
Eine Relation $R \subset A \times A$ heisst Relation auf A. Sind A und B beliebige Mengen, so nennen wir eine Teilmenge $R \subset A \times B$. eine *Relation* zwischen A und B. Sind $a \in A$ und $b \in B$, so sagen wir, dass a in Relation R zu b steht falls $(a, b) \in R$ ist. Steht a in Relation R zu b so schreiben wir auch aRb oder $a \sim_R b$.

3.2.2. Reflexiv

$\forall_a A(a) : a \sim a \in R$. Jedes Element aus A steht zu sich selbst in Relation.

- Die Kleiner-Gleich-Relation auf den reellen Zahlen ist reflexiv, da stets $x \leq x$ gilt. Sie ist darüber hinaus eine Totalordnung. Gleiches gilt für die Relation $\geq$.
- Die gewöhnliche Gleichheit auf den reellen Zahlen ist reflexiv, da stets $x = x$ gilt. Sie ist darüber hinaus eine Äquivalenzrelation.
- Die Teilmengenbeziehung $\subseteq$ zwischen Mengen ist reflexiv, da stets $A \subseteq A$ gilt. Sie ist darüber hinaus eine Halbordnung.

Um Reflexivität zu beweisen, ein Element auswählen und die Relation auf's erste Element anwenden. Wenn die Aussage wahr ist, steht das Element mit sich selbst in Beziehung.

3.2.3. Symmetrisch

$\forall_{a,b} A : a \sim b \Rightarrow b \sim a \in R \Rightarrow (b, a) \in R$
Für alle a, b von A gilt wenn a zu b in Relation steht, dann steht auch b zu a in Relation.
Wenn Person a in der selben Reihe sitzt wie Person b, sitzt Person b auch in der selben Reihe wie Person a. **Beispiel:** $R = \{(0,1),(0,0),(2,1),(1,0),(1,2)\}$ Gleichheit, Ungleichheit. => Wenn die Relation umgekehrt werden kann und sie immer noch gilt.

3.2.4. Asymmetrisch

$\forall_{a,b} A : a \sim b \Rightarrow \neg(b \sim a)$. Für alle a, b aus A gilt: a ist symmetrisch zu b aber b ist nicht symmetrisch zu a. Wenn A **grösser als** B ist, ist B **nicht grösser als** A. Eine Asymmetrie ist immer auch Antisymmetrisch, da die Voraussetzung falsch ist (Implikation).

3.2.5. Antisymmetrisch

$\forall_{a,b} A : a \sim b \wedge b \sim a \Rightarrow a = b$. Wenn a zu b in Relation steht und b zu a, dann ist a = b.
Beispiel: Wenn a Vorfahre von b ist und b Vorfahre von a, dann sind a und b die gleiche Person.
$\leq, \geq$ sowie die Teilbarkeitsrelation $x|y$

3.2.6. Transitiv

$\forall_{a,b,c} A : a \sim b \wedge b \sim c \Rightarrow a \sim c$. Wenn a in Relation zu b steht und b in Relation zu c, dann steht auch a zu c in Relation.
Beispiel: $<, >, =, \subset, A \Rightarrow BundB \Rightarrow C, = A \Rightarrow C$
$R = \{(a, b), (b, a)\}$ = nicht transitiv!
$R = \{(a, b), (b, a), (a, a), (b, b)\}$ = transitiv!

3.2.7. Äquivalenzrelation

Eine Relation die reflexiv, symmetrisch und transitiv ist, heisst Äquivalenzrelation.
Eine Äquivalenzklasse sind die disjunkten Mengen der Äquivalenzrelation, also alle Mengen, die zwar die gleiche Eigenschaft haben, ansonsten aber nichts miteinander gemeinsam haben (zb. alle binären Zahlen mit der gleichen Anzahl der Ziffer 1).

3.2.8. Halbordnung

Die Relation R wird als Halbordnung bezeichnet, falls sie transitiv, reflexiv sowie antisymmetrisch ist.
$A \subset B$: Bei zwei Mengen, muss nicht zwingenderweise eine Menge eine Teilmenge der anderen sein.

3.2.9. Totalordnung

Gilt zusätzlich zur *Halbordnung* noch für alle $a, b \in A$ stets $a \sim b \vee b \sim a$ so ist R eine *Ordnung* auf A. => transitiv, irreflexiv und antisymmetrisch.

3.2.10. Beispiele

$=$	reflexiv, transitiv, symmetrisch, antisymmetrisch, ist eine Äquivalenzrelation
$\geq, \leq$	reflexiv, transitiv, antisymmetrisch, ist eine Totalordnung
$<, >$	asymmetrisch, transitiv, nicht antisymmetrisch, nicht relativ, nicht total

3.3. Funktionen

3.3.1. Allgemein

Eindeutige zweiteillige Relationen. Eine beliebige Teilmenge $f \subset X \times Y$, $f : x \to y$.

- Domain: A, $f(x)$, dom, Urbild, Definitionsbereich
- Image: B, y, Im(...), Bild, Zielmenge, Wertebereich

3.3.2. Injektiv

Injektivität oder **Linkseindeutigkeit** besagt, dass jedes Element der Zielmenge **höchstens** einmal als Funktionswert angenommen wird. Kein Wert der Zielmenge wird mehrfach angenommen. Dabei darf die Domain kleiner als die Zielmenge sein.
$\forall_{x,y} \in dom(F) : (F(x) = F(y) \Rightarrow x = y)$

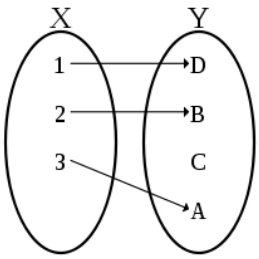

Abb. 3.1.: Injektivität

3.3.3. Surjektiv

Surjektivität oder **Rechtstotalität** bedeutet, dass jedes Element der Zielmenge mindestens einmal als Funktionswert angenommen wird, also mindestens ein Urbild hat. Jedes Element von Y wird angenommen. $F : x \to y$

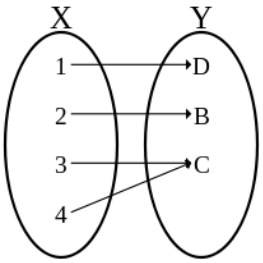

Abb. 3.2.: Surjektivität

$F : \mathbb{N} \to \mathbb{N} : F(n) = n^2$ injektiv, nicht surjektiv
$G : \mathbb{R} \to \mathbb{R} : G(x) = x^2$ nicht injektiv, nicht surjektiv
$F : X \to Y$: jedes Element von y wird erreicht auch: $im(F) = y$

3.3.4. Bijektiv

Eine Funktion ist bijektiv (oder *umkehrbar eindeutig auf* oder *eineindeutig auf*), wenn sie sowohl injektiv (kein Wert der Zielmenge wird mehrfach angenommen) als auch surjektiv (jeder Wert der Zielmenge wird angenommen) ist. Insgesamt heißt das, es findet eine vollständige Paarbildung zwischen den Elementen von Definitionsmenge und Zielmenge statt. Nur Bijektionen behandeln ihren Definitionsbereich und ihren Wertebereich symmetrisch, sodass eine bijektive Funktion immer eine Umkehrfunktion hat bzw. invertierbar ist. "Für jedes A gibt es ein B".

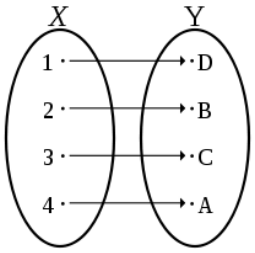

Abb. 3.3.: Bijektivität

$$\begin{aligned} F \circ G \circ H &= F(G(H(x))) \\ &= F \circ (G \circ H) \\ &= (F \circ G) \circ H \end{aligned}$$

$G \circ F : x \to z$ und $G \circ F(x) := G(F(X))$.
$(x, y) \in F = F(x) = y$.

3.3.5. Äquivalenzklassen

Ist A eine Menge und $\sim$ eine Äquivalenzrelation auf A, dann sind folgende Aussagen äquivalent:

1. $\sim$ ist eine Äquivalenzrelation auf A
2. Es gibt eine Funktion $F : A \to \wp(A)$, so dass für alle $x, y \in A$

$$x \sim y \Leftrightarrow F(x) = F(y)$$

   gilt.

Ist F eine Funktion wie in 2., dann ist das eine Äquivalenzklasse von $\sim$.

Beispiel Schüler, die alle in der gleichen Reihe sitzen, haben als ihre Äquivalenzklasse diese Reihe.

3.3.6. Umkehrabbildung

$$h(-z) = z$$
$$h^{-1}(z) = -z$$

4. Natürliche Zahlen

4.1. Die grundlegende Struktur der natürlichen Zahlen

Definition:

1. Jede natürliche Zahl k hat genau einen Nachfolger $N(k)$.
2. 0 ist kein Nachfolger aber alle anderen natürlichen Zahlen sind Nachfolger von genau einer natürlichen Zahl.
3. Ist $X \subset \mathbb{N}$ mit $0 \in X$ eine Menge von natürlichen Zahlen mit der Eigenschaft, dass für jedes Element k von X auch $N(k)$ zu x gehört, dann ist $X = \mathbb{N}$.

Die letzte der oben genannten Eigenschaften wird das Prinzip der vollständigen Induktion gennant.

4.1.1. Vollständige Induktion

Zu Beweisen:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Induktionsverankerung

$$\text{für n=1: } \sum_{i=1}^{1} i = 1 = \frac{2}{2} = \frac{1 \cdot 2}{2} = \frac{1(1+1)}{2}$$

Induktionsschritt: Für $n \to n+1$
Induktionsannahme:

$$\sum_{i=1}^{n+1} i = \frac{(n+1)((n+1)+1)}{2}$$

$$\begin{aligned}
\sum_{i=1}^{n+1} i &= \sum_{i=1}^{n} i + (n+1) \\
&=^{iA} \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n(n+1)}{2} + \frac{2n(n+1)}{2} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2} \\
\sum_{i=1}^{n+1} i &= \frac{(n+1)((n+1)+1)}{2}
\end{aligned}$$

4.2. Rekursive Definitionen

Ist M eine beliebige Menge und $g : M \to M$ sowie $c \in M$, dann gibt es eine eindeutig bestimmte Funktion $f : \mathbb{N} \to M$ welche die Gleichungen

$$\begin{aligned}
f(0) &= c \\
f(k+1) &= f(g(k))
\end{aligned}$$

erfüllt.

4.3. Die algebraische Struktur der natürlichen Zahlen

Siehe Skript, Seite 32.

5. Ganze Zahlen

Seinen x, y ganze Zahlen. Es gilt $x < y$ genau dann wenn es eine natürliche Zahl $n > 0$ mit der Eigenschaft $x + n = y$ gibt.

5.1. Teilbarkeit

Sind $x, y \in \mathbb{Z}$ ganze Zahlen so sagen wir, dass x *eine Teiler von* y ist falls es ein $k \in \mathbb{Z}$ gibt mit $xk = y$. Wir schreiben in diesem Fall $x|y$. Es gilt also:

$$x|y :\Leftrightarrow \exists k \in \mathbb{Z}(y = xk)$$

Die Teilbarkeitsrelation ist transitiv, d. h. wenn für beliebige ganze Zahlen x, y, z folgt aus $x|y$ und $y|z$ stets auch $x|z$.

Beispiel

$$\begin{aligned} x \in T(0) &\Leftrightarrow x|0 \\ &\Leftrightarrow \exists_k \in \mathbb{Z}(kx = 0) \end{aligned}$$

Funktioniert für jedes x, da jedes x ein Teiler von Null ist.

Definition: Zwei ganze Zahlen heissen *teilerfremd* wenn *ggT(x,y)*=1 gilt.
Seien $x, y \in \mathbb{Z}$ teilerfremd, dann gibt es ganze Zahlen k, k' so, dass

$$1 = kx + k'y$$

gilt.

Definition Sind $x, y, z \in \mathbb{Z}$, dann sind folgende Aussagen äquivalent:

$$x|y \wedge x|z$$
$$x|y0 \wedge x|(y - z)$$

Beweis: Seite 44 im Skript.

5.2. Primzahlen

Folgende Aussagen sind für $p \in \mathbb{N}$ äquivalent:

1. $\forall n, m \in \mathbb{N}(p|nm \Rightarrow p|n \vee p|m)$ und $p \neq 1$
2. $T(p) = \{1, p\}$ und $p \neq 1$
3. $|T(p)| = 2$

Weiter gilt:
Mit Ausnahme der Zahl 2 sind alle Primzahlen p ungerade und jede ganze Zahl die nicht $-1, 1$ ist, wird durch eine Primzahl geteilt.

5.2.1. Primfaktorzerlegung

Vorgehen: Die gegebene Zahl Modulo die kleinste, noch nicht getestete Primzahl. Falls der Rest 0 ist, weiter mit dem Ergebins, ansonsten die nächst grössere Primzahl verwenden.
Beispiel: pfz(45)

$$\begin{aligned}
45 &\mod 2 = 1 \rightarrow \text{ Rest ungleich 0, nächste Primzahl} \\
45 &\mod 3 = 0 \rightarrow 3 \cdot 15 = 45 \\
15 &\mod 3 = 0 \rightarrow 3 \cdot 5 = 15 \\
5 &\mod 3 = 2 \rightarrow \text{ Rest ungleich 0, nächste Primzahl} \\
5 &\mod 5 = 0 \rightarrow 1 \cdot 5 = 5
\end{aligned}$$

Daraus folgt, die Primfaktoren für 45 heissen: $3^2 \cdot 5^1$
Um die Anzahl Primfaktoren zu bestimmen wird nur die Anzahl unterschied-

licher Basen gezählt und nicht die Anzahl der Faktoren. **45 hat demzufolge zwei Primfaktoren!**

5.3. Modulare Arithmetik

5.3.1. Chinesischer Restsatz

Beispiel Gegeben:

$$x \equiv_4 3 \; ; \; x \equiv_5 2 \; ; \; x \equiv_9 1$$

1. Teiler des Teilsystems bestimmen

$$\begin{aligned} x &\equiv_4 3 \\ x &\equiv_5 2 \\ 4 &= 2 \cdot 2 + 0 \\ 5 &= 1 \cdot 5 + 0 \end{aligned}$$

somit gilt:

$$\begin{aligned} 0 &= 4 - 2 \cdot 2 \\ &= 4 - 2(5 - 4) \end{aligned}$$

Algorithmus:

$$an_1 + bn_2 = 1$$

$$x := y_1 bn_2 + y_2 an_1$$

6. Algebraische Strukturen

Eine algebraische Struktur ist eine Menge von Mengen (die der Struktur zugrundeliegenden Mengen) die jeweils mit einer oder mehreren (meist binären) Verknüpfung versehen sind.

6.1. Grundstrukturen

6.1.1. Halbgruppen, Gruppen und Monoide

Definition Eine Struktur $(G, \cdot)$ bestehend aus einer Menge G und einer Verknüpfung $\cdot : G \times G \to G$ heisst:

1. **Halbgruppe**, falls $\cdot$ assoziativ d.h. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ist.
2. **Monoid**, falls $(G, \cdot)$ eine Halbgruppe ist und ein neutrales Element $e \in G$ existiert.
3. **Gruppe**, falls $(G, \cdot)$ ein Monoid (mit neutralem Element e) ist und für alle $a \in G$ ein $b \in G$ existiert, so dass $a \cdot b = b \cdot a = e$ gilt.
4. **kommutative Gruppe**, falls $(G, \cdot)$ eine Gruppe und $\cdot$ kommutativ ist.

Bemerkung In einer Gruppe $(M, \cdot)$ besitzt jedes Element $a \in G$ ein eindeutig bestimmtes inverses Element (dies kann auch a selbst sein), wir bezeichnen dieses mit a^{-1}. Offensichtlich gilt für jedes $a \in G$ auch $(a^{-1})^{-1} = a$.

6.1.2. Unterstukturen

Eine unter $\cdot$ abgeschlossene Teilmenge $\bigcup$ nennen wir Unterstruktur. Für sie gelten die selben Regeln wie für die normalen Strukturen. Folgerung: Jede (Halb-) Gruppe besitzt eine kleinste Unter(halb)gruppe und jeder Monoid besitzt einen kleinsten Untermonoid, die eine gegebene Teilmenge der (Halb-) Gruppe bzw. des Monoids enthalten.

6.1.3. Die Morphismen von (Halb-) Gruppen und Monoiden

- Ein **(Halb-) Gruppenhomomorphismus** von der (Halb-) Gruppe $(G, \cdot)$ in die (Halb-) Gruppe $(G', \circ)$ ist eine Abbildung $f : G \to G'$, so dass für alle $a, b \in G$

  $$f(a \cdot b) = f(a) \circ f(b)$$

  gilt.

- Ein **Monoidhomomorphismus** vom Monoid $(M, \cdot)$ in den Monoid $(M', \circ)$ ist eine Abbildung $f : M \to M'$, so dass für alle $a, b \in M$

  $$f(a \cdot b) = f(a) \circ f(b)$$

  gilt, und ausserdem wird das neutrale Element von $(M, \cdot)$ aus das neutrale Element von $(M', \circ)$ abgebildet.

Injektive[1] Homomorphismen nennen wir **Monomorphismen**, surjektive[2] **Epimorphismen** und bijektive[3] **Isomorphismen**.

Bemerkung Nicht jeder Halbgruppenhomomorphismus zwischen Monoiden ist auch ein Monoidhomomorphismus. Des weiteren gilt, dass wenn $f : (G, \cdot) \to (G', \star)$ und $h : (G', \star) \to (G'', \bullet)$ Homomorphismen von Gruppen oder Halbgruppen oder Monoiden sind, dann ist auch $h \circ f : (G, \cdot) \to (G'' \to \bullet)$ ein entsprechender Homomorphismus.
Wenn eine Gruppe $(\mathbb{Z}, +)$ auch einen Halbgruppenhomomorphismus (Assoziativ) ist, ist sie auch ein Gruppenhomomorphismus!

[1] Injektiv: Jedes Element in der Abbildung wird nur einmal erreicht
[2] Surjektiv: Es gibt Punkte in der Abbildung die mehrmals erreicht werden können
[3] Bijektiv: Es findet eine vollständige Paarbildung zwischen der Definitions- und Zielmenge statt

6.1.4. Ringe und Körper

Definition Eine Struktur $(R, +, \cdot)$ heisst Ring, wenn folgende Bedingungen erfüllt sind:

1. $(R, +)$ ist eine kommutative[4] Gruppe
2. $(R, \cdot)$ ist eine Halbgruppe
3. Es gilt das Distributivgesetz, d. h. für alle Elemente r, s, t des Rings gelten:
   a) $r \cdot (s + t) = (r \cdot s) + (r \cdot t)$
   b) $(r + s) \cdot t = (r \cdot t) + (s \cdot t)$

Die Beweise zu den Rechenregeln sind in den Notizen zu finden.

Beispiel

Ringe	Keine Ringe
$(\mathbb{Z}, +, \cdot)$	$(\mathbb{N}, +, \cdot)$, da + auf $\mathbb{N}$ nicht kommutativ ist
$(\mathbb{Z}_{/n}, +, \cdot)$	
$(\{0\}, +, \cdot)$	

Nullteiler

Definition Ein Nullteiler ist eine Zahl, welche nicht 0 ist, und mit einer anderen Zahl multipliziert 0 ergibt.
Es sei $(R, +, \cdot)$ ein Ring

1. Ein Element $(r \in R)$ heisst rechter Nullteiler in R, falls ein $s \in R$ 0 existiert mit $sr = 0$.
2. Ein Element $(r \in R)$ heisst linker Nullteiler in R, falls ein $s \in R$ 0 existiert mit $rs = 0$.
3. Ein Element $(r \in R)$ heisst Nullteiler in R, falls ein r sowohl linker- als auch rechter Nullteiler in R ist.
4. Der Ring $(R, +, \cdot)$ heisst Integritätsring, wenn:
   a) Die Verknüpfung $\cdot$ kommutativ ist.
   b) $0 \in R$ ist der einzige Nullteiler in R

[4]Kommutativ: Reihenfolge egal; $a + b = b + a$

Integritätsring

Ein Integritätsring ist ein nullteilerfreier kommutativer Ring mit einem Einselement (neutrales Element).

Beispiel für Integritätsringe:

- $\mathbb{Z}$
- Jeder Körper ist ein Integritätsring. Ausserdem ist jeder endliche Integritätsring ein endlicher Körper.
- Ein Polynomring ist ein Integritätsring, wenn die Koeffizienten aus einem Integritätsring stammen.
- Der Restklassenring $\mathbb{Z}_{/n}$ ist genau dann ein Integritätsring, sogar ein Körper, wenn n eine Primzahl ist.

Bemerkung In einem Integritätsring R gilt stets $1 \neq 0$. $1 = 0$ gilt nur in einem Nullring [5]. Ein Nullring ist jedoch kein Integritätsring, da 0 kein Nullteiler von 0 ist.

[5] $(\{0\}, +, \cdot)$

Anhang

A. Algorithmen in pseudo Code

A.1. Grösster gemeinsamer Teiler

Algorithmus zur ggT Berechnung (Pseudo Code):

```
1 ggt(m,n) {
2   if (n==0)
3     return m;
4   else
5     return ggt(n, m%n);
6 }
```

A.2. Kleinstes gemeinsames Vielfaches

```
1 kgv(m,n) {
2     o = ggt(m,n);
3     p = (m * n) / o;
4     return p;
5 }
```

A.3. Euklidischer Algorithmus

Beispiel: $99x \cdot 78y = ggt(99, 78)$

$$
\begin{aligned}
99 &= 1 \cdot 78 + 21 \\
78 &= 3 \cdot 21 + 15 \\
21 &= 1 \cdot 15 + 6 \\
15 &= 2 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0
\end{aligned}
$$

3 ist ein Teiler von 6 und damit der gesuchte grösste gemeinsame Teiler von 99 und 78. Nun kann man diese Gleichungen rückwärts lesen und den Rest jeweils als Differenz der beiden anderen Terme darstellen. Setzt man diese Restdarstellungen rekursiv ineinander ein, so ergeben sich verschiedene Darstellungen des letzten Restes 3:

$$
\begin{aligned}
3 &= 15 - 2 \cdot 6 \\
&= 15 - 2 \cdot (21 - 1 \cdot 15) && = 3 \cdot 15 - 2 \cdot 21 \\
&= 3 \cdot (78 - 3 \cdot 21) - 2 \cdot 21 && = 3 \cdot 78 - 11 \cdot 21 \\
&= 3 \cdot 78 - 11 \cdot (99 - 1 \cdot 78) && = 14 \cdot 78 - 11 \cdot 99
\end{aligned}
$$

Somit ist $x = -11$ und $y = 14$ die gesuchte Lösung.

A.4. Primfaktorzerlegung

```
1 pfz(n) {
2   pz=2;
3   if(n % pz) {
4     print(pz)
5     pfz(n/pz)
6   } else {
7     pz = getNextPrime(pz++)
8   }
9 }
```

A.5. Primpotenz finden

Java Code:

```
1  public static boolean isPrimePower(int n) {
2    int nold = n;
3    for (int i = 2; i <= n; i++) {
4      if (isPrime(i)) {
5        while (n % i == 0) {
6          n = n / i;
7          if (n == 1) {
8            return true;
9          }
10       }
11     }
12     n = nold;
13   }
14   return false;
15 }
```