KAPITEL III

Algebraische Grundstrukturen

1. Halbgruppen, Monoide und Gruppen

Wir haben in den ersten beiden Kapiteln gewisse Gesetze kennengelernt, wie etwa das Assoziativgesetz oder das Kommutativgesetz, die bei so unterschiedlichen Strukturen, wie der Mengenalgebra oder der Addition bzw. Multiplikation von Zahlen eine Rolle spielen. In diesem Kapitel werden die allgemeinen Eigenschaften solcher Gesetze studiert. Wir werden sehen, daß diese Gesetze in sehr vielen mathematischen Objekten auftreten und daß sie auch bei Strukturen, die für die Informatik wichtig sind, eine ganz wesentliche Rolle spielen.

Definition 1.1. Sei G eine Menge. Eine (binäre) *Operation* oder *Verknüpfung* in G ist eine Abbildung $\gamma : G \times G \longrightarrow G$. Das Bild $\gamma((a,b))$ eines Paares $(a,b) \in G \times G$ wird je nach Kontext bezeichnet mit

$$a \cdot b,\ a + b,\ ab,\ a \cap b,\ a \cup b,\ a - b,$$

d.h. statt des vorangestellten Funktionszeichens (*Präfix*notation oder *umgekehrte polnische Notation*) $\gamma((a,b))$ oder einfach $\gamma(a,b)$ verwendet man gewöhnlich ein zwischen die zwei Argumente a

und b gestelltes Funktionszeichen (*Infix*notation). Ein nachgestelltes Funktionszeichen, z.B. $ab+$, wird auch *Postfix*notation oder *polnische Notation* genannt.

Definition 1.2. Sei $\circ : G \times G \ni (a,b) \mapsto a \circ b \in G$ eine Operation. Für die Operation gilt das

(1) *Assoziativ*gesetz: $\Longleftrightarrow \forall a,b,c \in G[(a \circ b) \circ c = a \circ (b \circ c)]$.
(2_l) Gesetz vom *linksneutralen Element* $:\Longleftrightarrow \exists e_l \in G \forall a \in G[e_l \circ a = a]$;
(2_r) Gesetz vom *rechtsneutralen Element* $:\Longleftrightarrow \exists e_r \in G \forall a \in G[a \circ e_r = a]$;
(3_l) Gesetz vom *linksinversen Element* (falls ein linksneutrales Element e_l existiert): $\Longleftrightarrow \forall a \in G \exists a' \in G[a' \circ a = e_l]$;
(3_r) Gesetz vom *rechtsinversen Element* (falls ein rechtsneutrales Element e_r existiert): $\Longleftrightarrow \forall a \in G \exists a'' \in G[a \circ a'' = e_r]$;
(4) *Kommutativ*gesetz: $\Longleftrightarrow \forall a,b \in G[a \circ b = b \circ a]$.

Übung: Formulieren Sie das Assoziativgesetz in Postfixnotation. Warum werden dabei keine Klammern benötigt?

Das Assoziativgesetz kann natürlich auch bei mehr als drei Faktoren eingesetzt werden und gestattet auch dann beliebiges Umklammern. Das kann auch formal bewiesen werden. Man kann daher bei der Produktbildung die Klammern völlig fortlassen.

Definition 1.3. Eine Menge G zusammen mit einer Operation $\gamma : G \times G \longrightarrow G$ heißt

(1) *Halbgruppe*: $\Longleftrightarrow$ (1) gilt;
(2) *Monoid* : $\Longleftrightarrow$ (1), (2_l) und (2_r) gelten;
(3) *Gruppe*: $\Longleftrightarrow$ (1), (2_l), (2_r), (3_l) und (3_r) gelten;
(4) *kommutative* oder *abelsche* Gruppe : $\Longleftrightarrow$ (1), (2), (3) und (4) gelten.

Beispiele 1.4. a) $(\mathbb{N},+)$ ist eine Halbgruppe, aber kein Monoid.
b) $(\mathbb{N},\cdot)$ ist ein Monoid, aber keine Gruppe.

c) Die Menge $G := \mathrm{Abb}(M, M)$ der Abbildungen von M in sich zusammen mit der Komposition $\circ$ von Abbildungen ist ein Monoid, aber keine Gruppe.
d) Die Menge der bijektiven Abbildungen $f : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ wird mit der Komposition $\circ$ von Abbildungen wegen I. 2.22 eine Gruppe S_n, die sogenannte *symmetrische Gruppe* oder *Permutationsgruppe*.
e) $(\mathbb{Z}, +)$ ist eine kommutative Gruppe.
f) $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ zusammen mit der Multiplikation ist eine kommutative Gruppe.
g) $\mathbb{R}$ zusammen mit der Multiplikation ist ein Monoid, aber keine Gruppe.
h) Die Potenzmenge $\mathcal{P}(M)$ einer Menge M zusammen mit dem Durchschnitt $\cap$ ist ein Monoid, aber keine Gruppe.
i) Wenn G und H Halbgruppen (Monoide, Gruppen) sind, dann ist auch $G \times H$ eine Halbgruppe (ein Monoid, eine Gruppe) mit der „komponentenweisen“ Multiplikation $(g, h) \cdot (g', h') = (gg', hh')$. Im Falle von Monoiden ist dann (e_G, e_H) das neutrale Element. Im Falle von Gruppen ist (g^{-1}, h^{-1}) das inverse Element von (g, h).
j) Bei Halbgruppen (Monoiden, Gruppen) mit nur endlich vielen Elementen kann man die Verknüpfung auch in Form einer Tabelle, genannt *Verknüfungstafel* oder *Multiplikationstafel* angeben. Das folgende ist ein Beispiel für eine Multiplikationstafel einer Gruppe $G = \{e, a, b\}$ mit drei Elementen:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Übung: Man zeige, daß für eine Halbgruppe (Monoid, Gruppe) G und eine Menge I auch die Menge $\mathrm{Abb}(I, G) = \prod_I G = G^I$ mit der „komponentenweisen“ Multiplikation eine Halbgruppe (Monoid, Gruppe) bildet.

Bemerkung 1.5. In einem Monoid gibt es nur ein linksneutrales Element e_l und ein rechtsneutrales Element e_r und diese sind gleich. Es ist nämlich $e_l = e_l \circ e_r = e_r$. Wir sprechen dann einfach vom *neutralen Element*.
Wenn in einer Halbgruppe die Gesetze (b_l) und (c_l) erfüllt sind, so sind auch (b_r) und (c_r) erfüllt und die Links- und Rechtsinversen a' bzw. a'' eines Elements a sind eindeutig bestimmt und stimmen überein. Sei nämlich $a'a = e_l$ und $\tilde{a}a' = e_l$, dann ist $aa' = e_l(aa') = (\tilde{a}a')(aa') = \tilde{a}((a'a)a') = \tilde{a}(e_l a') = \tilde{a}a' = e_l$. Weiter ist $ae_l = a(a'a) = (aa')a = e_l a = a$. Also ist e_l auch rechtsneutrales Element und a' auch Rechtsinverses von a. Ist $a'a = e$ und $a\bar{a} = e$, so ist $a' = a'e = a'a\bar{a} = e\bar{a} = \bar{a}$. Damit sind linksinverse und rechtsinverse Elemente von a gleich und eindeutig bestimmt. Wir sprechen dann einfach vom *inversen Element* a' von a. Das inverse Element von a' ist a, denn $aa' = e$. Das inverse Element von ab ist $b'a'$, denn $b'a'ab = b'eb = b'b = e$. Wenn die Operation durch $a \cdot b, ab, a * b$ oder $a \circ b$ bezeichnet wird, schreibt man für das Inverse von a gewöhnlich a^{-1}. Wenn die Operation durch $a + b$ bezeichnet wird, schreibt man für das Inverse $-a$ oder $(-a)$.

Bei konkreten Beispielen, wie z.B. der Gruppe $(\mathbb{R}, +)$, ist man oft geneigt, auch *unendliche Summen* zu bilden und sie wie die endlichen Summen zu behandeln. Das ist jedoch prinzipiell nicht möglich. Wir können die Summe oder das Produkt von genau zwei Elementen bilden. Durch Iteration können wir die Addition bzw. Multiplikation auch auf Familien von n Elementen ausdehnen, wobei $n \in \mathbb{N}$ ist, so daß Ausdrücke der Form $a_1 + a_2 + \ldots + a_n$ sinnvoll sind. Es ist aber keine unendliche Summe (Produkt) mit diesen Mitteln definierbar. Die bei reellen Zahlen definierbaren unendlichen Summen und Produkte leben von der Konvergenz von Folgen von endlichen Teilsummen (-produkten). Die meisten Reihen konvergieren nicht. Und selbst wenn sie konvergieren, kann man z.B. das Kommutativgesetz nicht unbeschränkt verwenden. Hier spielt eine zusätzliche Struktur der reellen Zahlen,

die Norm oder der Absolutbetrag, eine wesentliche Rolle.

Definition 1.6. Sei A eine Menge und A^* die Menge aller endlichen Folgen in A

$$A^* := \{(\alpha, n) | n \in \mathbb{N}_\circ \wedge \ \alpha : \{1, \ldots, n\} \longrightarrow A\}.$$

A^* heißt auch *Kleene Abschluß* von A. A heißt *Alphabet*, die Elemente $a \in A$ *Buchstaben*, die Elemente von A^* *Wörter*. Eine beliebige Menge von Wörtern über einem Alphabet A wird in der Informatik auch *Sprache* genannt. Die Verknüpfung in A^* ist definiert durch

$$\circ : A^* \times A^* \ni ((a_1, \ldots, a_m), (b_1, \ldots, b_n)) \mapsto (a_1, \ldots, a_m, b_1, \ldots, b_n) \in A^*$$

oder genauer

$$\circ : A^* \times A^* \ni ((\alpha, m), (\beta, n)) \mapsto (\gamma, m + n) \in A^*$$

mit

$$\gamma(i) := \begin{cases} \alpha(i) & \text{für } 1 \leq i \leq m, \\ \beta(i - m) & \text{für } m < i \leq m + n. \end{cases}$$

Lemma 1.7. $(A^*, \circ)$ *ist ein Monoid, genannt das* (*intern*) freie von A erzeugte *Monoid.*

BEWEIS. Wir schreiben statt $(a_1, \ldots, a_m)$ einfach $a_1 \ldots a_m$. Dann ist $a_1 \ldots a_m \circ b_1 \ldots b_n = a_1 \ldots a_m b_1 \ldots b_n$ und

$$(a_1 \ldots a_m \circ b_1 \ldots b_n) \circ c_1 \ldots c_r = a_1 \ldots a_m b_1 \ldots b_n \circ c_1 \ldots c_r = a_1 \ldots a_m b_1 \ldots b_n c_1 \ldots c_r = a_1 \ldots a_m \circ (b_1 \ldots b_n \circ c_1 \ldots c_r).$$

Das neutrale Element ist $(\emptyset, 0)$ mit $\emptyset : \emptyset \longrightarrow A$ leere Abbildung. Dabei fassen wir $\{1, \ldots, 0\}$ als leere Menge auf. Die leere endliche Folge $(\emptyset, 0)$ in A^* oder das *leere Wort* wird oft auch mit ϵ bezeichnet. Offenbar gilt $\epsilon a_1 \ldots a_n = a_1 \ldots a_n = a_1 \ldots a_n \epsilon$. □

Definition 1.8. Sei $(G, \circ)$ eine Halbgruppe und $A \subset G$ eine Teilmenge. Wir definieren eine Teilmenge $\bar{A} \subset G$ durch

$$\bar{A} := \{a_1 \circ \ldots \circ a_m | m \in \mathbb{N} \wedge \ a_1, \ldots, a_m \in A\}.$$

Wenn $(G, \circ)$ ein Monoid ist, dann definiert man

$$\bar{A} := \{a_1 \circ \ldots \circ a_m | m \in \mathbb{N}_\circ \wedge \ a_1, \ldots, a_m \in A\},$$

wobei im Falle $m = 0$ das leere Produkt das neutrale Element e sei. Wenn $(G, \circ)$ eine Gruppe ist, dann definiert man

$$\bar{A} := \{a_1^{\epsilon_1} \circ \ldots \circ a_m^{\epsilon_m} | m \in \mathbb{N}_\circ \wedge \ a_i \in A \wedge \ \epsilon_i \in \{1, -1\}\}.$$

Man läßt also bei der Produktbildung als Faktoren auch Inverse von Elementen aus A zu. $\bar{A}$ heißt die von A *erzeugte* Menge in G. Wenn $G = \bar{A}$, dann heißt G von A *erzeugt*.

Man spricht von den Mengen der Form $\bar{A}$ auch als durch A von „innen“ erzeugt, weil alle ihre Elemente einzeln aus A konstruiert werden. In 1.12 werden wir auch eine Methode kennen lernen, wie man die Menge $\bar{A}$ von „außen“ erzeugen kann.

Definition 1.9. Eine Teilmenge $B \subset G$ in einer Halbgruppe, einem Monoid oder einer Gruppe $(G, \circ)$ heißt

(1) *Unterhalbgruppe*, wenn $\forall a, b \in B[a \circ b \in B]$;
(2) *Untermonoid*, wenn B Unterhalbgruppe ist und $e \in B$ gilt;
(3) *Untergruppe*, , wenn $\forall a, b \in B[a \circ b \in B \wedge \ a^{-1} \in B]$ und wenn $B \neq \emptyset$.

Eine Untergruppe ist insbesondere ein Untermonoid, weil auch $e = a \circ a^{-1} \in B$ gilt. Wir sagen auch, daß B unter der Bildung von Produkten, des neutralen Elements bzw. von Inversen *abgeschlossen* ist. Eine Unterhalbgruppe (-monoid, -gruppe) ist selbst eine Halbgruppe (Monoid, Gruppe).

Lemma 1.10. *Sei $(G, \circ)$ eine Halbgruppe, ein Monoid oder eine Gruppe und sei $A \subset G$ eine Teilmenge. Dann ist die von A*

erzeugte Menge $\bar{A}$ die kleinste Unterhalbgruppe (-monoid bzw. -gruppe), die A enthält.

BEWEIS. $\bar{A}$ ist so definiert, daß es unter der Multiplikation (bzw. $e \in \bar{A}$, bzw. Inversenbildung) von $(G, \circ)$ abgeschlossen ist. Es ist daher $\bar{A}$ eine Unterhalbgruppe (-monoid, -gruppe). Ist aber $B \subset G$ eine Unterhalbgruppe (-monoid, -gruppe) mit $A \subset B$, so gilt auch $\bar{A} \subset B$; also ist $\bar{A}$ kleinste Unterstruktur von G mit $A \subset \bar{A}$. □

Satz 1.11. *Seien $(G, \circ)$ eine Halbgruppe (Monoid, Gruppe) und seien B_i, $i \in I$ Unterhalbgruppen (-monoide, -gruppen). Dann ist $\bigcap_{i \in I} B_i$ wieder Unterhalbgruppe (-monoid, -gruppe).*

BEWEIS. Wenn jedes der B_i unter der Multiplikation ($1 \in B_i$, Inversenbildung) abgeschlossen ist, dann auch der Durchschnitt $\bigcap B_i$. □

Satz 1.12. *Sei $(G, \circ)$ eine Halbgruppe (Monoid, Gruppe) und $A \subset G$ eine Teilmenge. Dann ist*

$$\bar{A} = \bigcap \{B \subset G | B \text{ Unterstruktur } \wedge \ A \subset B\}.$$

BEWEIS. Da $\bar{A}$ unter den zugelassenen B ist, gilt „$\supset$“. Da der Durchschnitt wieder eine Unterstruktur ist, die A enthält, und da $\bar{A}$ kleinste solche Unterstruktur ist, gilt „$\subset$“. □

Die Erzeugung von $\bar{A}$ muß man als eine Erzeugung von „außen“ auffassen. Der Mechanismus der Gewinnung der einzelnen Elemente aus A wird nicht angegeben. Man erhält mit dieser Methode zwar sehr schnell die Existenz des gewünschten Objekts. Die Methode ist aber nicht konstruktiv, weil man keinen Überblick über alle Unterhalbgruppen (-monoide, -gruppen) hat, die A umfassen. Man kann einzelne Elemente von $\bar{A}$ nicht angeben. Im Falle von komplizierteren algebraischen Gebilden ist es jedoch oft sehr schwer, die Konstruktion der Elemente explizit anzugeben. Das war schon für Gruppen komplizierter, als für Monoide.

Dann entwickelt die Methode der Durchschnittsbildung erst ihre ganze Kraft.

2. Homomorphismen

Nachdem wir nun erste Beispiele und Eigenschaften von gewissen algebraischen Strukturen kennen, folgt nun die Einführung von Abbildungen, die mit der gegebenen Struktur verträglich sind, sogenannten Homomorphismen.

Definition 2.1. Seien $(G, \circ)$ und $(H, \cdot)$ Halbgruppen (Monoide, Gruppen). Eine Abbildung $f : G \longrightarrow H$ heißt ein *Homomorphismus* von

(1) Halbgruppen, wenn $\forall g_1, g_2 \in G[f(g_1 \circ g_2) = f(g_1) \cdot f(g_2)]$,
(2) Monoiden, wenn $\forall g_1, g_2 \in G[f(g_1 \circ g_2) = f(g_1) \cdot f(g_2)]$, und $f(e_G) = e_H$, (wobei $e_G \in G$ und $e_H \in H$ die neutralen Elemente sind),
(3) Gruppen, wenn $\forall g_1, g_2 \in G[f(g_1 \circ g_2) = f(g_1) \cdot f(g_2)]$.

Lemma 2.2. *Ist $f : G \longrightarrow H$ ein Homomorphismus von Gruppen, so gilt $f(e_G) = e_H$ und $\forall g \in G[f(g^{-1}) = f(g)^{-1}]$.*

BEWEIS. $f(e_G) \cdot f(e_G) = f(e_G \circ e_G) = f(e_G) \Longrightarrow h \cdot h = h$ für $h = f(e_G)$. $\Longrightarrow h = h^{-1} \cdot h \cdot h = h^{-1} \cdot h = e_H \Longrightarrow f(e_G) = e_H$. $f(g)^{-1} \cdot f(g) = e_H = f(e_G) = f(g^{-1} \circ g) = f(g^{-1}) \circ f(g) \Longrightarrow f(g)^{-1} = f(g^{-1})$. □

Lemma 2.3. *Seien G, H, K Halbgruppen (Monoide, Gruppen) und $f : G \longrightarrow H, f' : H \longrightarrow K$ Homomorphismen. Dann ist auch $f'f : G \longrightarrow K$ ein Homomorphismus. Weiter ist $\mathrm{id}_G : G \longrightarrow G$ ein Homomorphismus.*

BEWEIS. $(f'f)(g_1 \cdot g_2) = f'(f(g_1) \cdot f(g_2)) = (f'f)(g_1) \cdot (f'f)(g_2)$ und $(f'f)(e_G) = f'(e_H) = e_K$. □

Definition 2.4. Ein Homomorphismus $f : G \longrightarrow H$ heißt *Isomorphismus*, wenn es einen Homomorphismus $f' : H \longrightarrow G$ so

gibt, daß $ff' = \mathrm{id}_H$ und $f'f = \mathrm{id}_G$. Wenn es einen Isomorphismus $f : G \longrightarrow H$ gibt, dann heißen G und H *isomorph*, in Zeichen $G \cong H$.

Bemerkung 2.5. Isomorphe Objekte sind für alle mathematischen Betrachtungen als gleichwertig anzusehen. Man kann nämlich die Verknüpfung von zwei Elementen auch durch die Verknüpfung der entsprechenden Elemente im dazu isomorphen Objekt ausdrücken, d.h. für einen Isomorphismus $f : G \longrightarrow H$ und $a, b \in G$ gilt

$$a \cdot b = f^{-1}(f(a) \cdot f(b)).$$

Ist $f : G \longrightarrow H$ ein bijektiver Homomorphismus, so ist f ein Isomorphismus, denn für die eindeutig bestimmte Umkehrabbildung $f^{-1}H \longrightarrow G$ gilt $f^{-1}(h_1 \cdot h_2) = f^{-1}(ff^{-1}(h_1) \cdot ff^{-1}(h_2)) = f^{-1}f(f^{-1}(h_1) \cdot f^{-1}(h_2)) = f^{-1}(h_1) \cdot f^{-1}(h_2)$ und $f^{-1}(e_H) = e_G$.

Lemma 2.6. *Wenn $f : G \longrightarrow H$ ein Homomorphismus ist, dann ist* $\mathrm{Bi}(f)$ *eine Unter-Halbgruppe (-Monoid, -Gruppe) von H.*

Beweis. Seien $h_1, h_2 \in \mathrm{Bi}(f)$. Dann gibt es $g_1, g_2 \in G$ mit $f(g_1) = h_1, f(g_2) = h_2$. Da f ein Homomorphismus ist, ist $h_1 \cdot h_2 = f(g_1) \cdot f(g_2) = f(g_1 \cdot g_2) \in \mathrm{Bi}(f)$. Im Monoidfall ist außerdem $e_H = f(e_G) \in \mathrm{Bi}(f)$. Ist schließlich f ein Homomorphismus von Gruppen, dann ist $h^{-1} = f(g)^{-1} = f(g^{-1}) \in \mathrm{Bi}(f)$. □

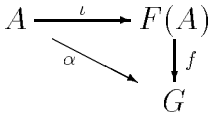
Beispiel 2.7. Ein wichtiges Beispiel für einen Isomorphismus ist die Exponential-Abbildung oder e-Funktion. Die reellen Zahlen bilden unter der Addition eine Gruppe $(\mathbb{R}, +)$. Weiter bildet die Menge $\mathbb{R}_+$ der positiven reellen Zahlen unter der Multiplikation eine Gruppe $(\mathbb{R}_+, \cdot)$. Die Funktionalgleichung für die Exponentialfunktion $\exp(a + b) = \exp(a) \cdot \exp(b)$ besagt genau daß diese Abbildung ein Homomorphismus ist. Da sie bijektiv ist, ist sie ein Isomorphismus. Die Umkehrabbildung ist ebenfalls ein Isomorphismus und genügt der Gleichung $\log(a \cdot b) = \log(a) + \log(b)$.

Man merke sich zudem, daß die Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}_+, \cdot)$ zueinander isomorph sind.

3. Freie Halbgruppen, Monoide und Gruppen

Eine besonders nützliche Art von Strukturen sind die freien Strukturen. Man kennt sie (bis auf Isomorphie), wenn man nur ihre erzeugenden Elemente kennt. Sie erlauben es auch, besonders einfach Homomorphismen in andere Strukturen zu konstruieren. Allerdings geht ihre Definition von einer besonderen Eigenschaft aus, die sie haben, einer sogenannten universellen Eigenschaft. Daher ist ihre Definition nicht ganz leicht verständlich. Erst nach dem Beweis ihrer Existenz (und Eindeutigkeit) kann man diese Eigenschaft besser verstehen.

Definition 3.1. Sei A eine Menge. Eine Halbgruppe (Monoid, Gruppe) $F(A)$ zusammen mit einer Abbildung $\iota : A \longrightarrow F(A)$ heißt eine (extern) *freie Halbgruppe (Monoid, Gruppe)*, wenn zu jeder Halbgruppe (Monoid, Gruppe) G und zu jeder Abbildung $\alpha : A \longrightarrow G$ genau ein Homomorphismus $f : F(A) \longrightarrow G$ existiert, so daß

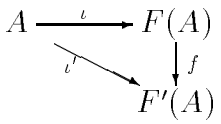


kommutiert.

Bemerkung 3.2. Die Abbildung ι ist immer injektiv, so daß man A als Teilmenge von $F(A)$ auffassen kann. Dann bedeutet die obige Definition, daß sich jede beliebige Zuordnung α von Elementen aus G zu den Elementen aus A auf genau eine Weise zu einem Homomorphismus von $F(A)$ nach G fortsetzen läßt und daß jeder Homomorphismus $f : F(A) \longrightarrow G$ schon vollständig durch die Werte bestimmt ist, die er auf Elementen aus A annimmt.

Satz 3.3. (1) *Ist $F(A)$ mit $\iota : A \longrightarrow F(A)$ eine freie Halbgruppe (Monoid, Gruppe), so ist ι injektiv.*

(2) *Sind $F(A)$ und $F'(A)$ mit $\iota : A \longrightarrow F(A)$ und $\iota' : A \longrightarrow F'(A)$ freie Halbgruppen (Monoide, Gruppen), so gibt genau einen Homomorphismus $f : F(A) \longrightarrow F'(A)$ mit*



kommutativ (d.h. $f\iota = \iota'$) und f ist ein Isomorphismus.

BEWEIS. (1) $\{1, -1\}$ mit der Multiplikation ist eine Gruppe (Halbgruppe, Monoid). Sei $\iota : A \longrightarrow F(A)$ nicht injektiv. Dann gibt es $a, b \in A$ mit $\iota(a) = \iota(b)$ und $a \neq b$. Wir definieren $\alpha : A \longrightarrow \{1, -1\}$ durch $\alpha(c) = \begin{cases} 1 & c \neq a \\ -1 & c = a \end{cases}$. Dann ist $1 = \alpha(b) = f\iota(b) = f\iota(a) = \alpha(a) = -1$, ein Widerspruch. Also ist ι injektiv.

(2) Die erste Aussage, daß genau ein Homomorphismus f mit $f\iota = \iota'$ existiert, ist die Definition einer freien Halbgruppe (Monoid, Gruppe). Ebenso gibt es (genau) einen Homomorphismus $f' : F'(A) \longrightarrow F(A)$ mit $f'\iota' = \iota$. Damit ist $ff'\iota' = \iota' = \mathrm{id}_{F'(A)}\,\iota'$, also $ff' = \mathrm{id}_{F'(A)}$, weil $(F'(A), \iota')$ frei ist, und es ist $f'f\iota = \iota = \mathrm{id}_{F(A)}\,\iota$, also $f'f = \mathrm{id}_{F(A)}$, weil $(F(A), \iota)$ frei ist. Also ist f ein Isomorphismus. □

Wir haben schon in 1.7 freie Monoide kennengelernt, jedoch nicht durch die oben gegebene Abbildungseigenschaft. Diese Abbildungseigenschaft beweisen wir im folgenden Satz. Ebenso geben wir hier die Konstruktion einer freien Halbgruppe an. Die Konstruktion einer freien Gruppe ist schwieriger. Da wir sie später nicht benötigen, wollen wir diese Konstruktion auch hier nicht angeben.

Satz 3.4. (1) *Sei A eine Menge. Dann ist A^* zusammen mit der Einbettung von A in A^* freies Monoid.*
(2) *Sei A eine Menge. Dann ist $A^* \setminus \{\varepsilon\}$ zusammen mit der Einbettung von A in $A^* \setminus \{\varepsilon\}$ freie Halbgruppe.*

BEWEIS. (1) Sei $\alpha : A \longrightarrow G$ eine Abbildung in ein Monoid G. Wir definieren $f : A^* \longrightarrow G$ durch $f(a_1 \dots a_n) := \alpha(a_1) \cdot \ldots \cdot \alpha(a_n)$ für $n \geq 1$ und $f(\varepsilon) := e_G$. (Wir definieren das 0-fache Produkt von Elementen in G als e_G.) f ist eine wohldefinierte Abbildung, weil durch jedes Element $a_1 \dots a_n \in A^*$ die Komponenten $a_1, \dots, a_n \in A$ eindeutig stimmt sind. Sie werden benötigt, um den Wert $f(a_1 \dots a_n)$ zu beschreiben. Es ist f ein Homomorphismus, denn $f(a_1 \dots a_n \circ b_1 \dots b_r) = \alpha(a_1) \cdot \ldots \cdot \alpha(a_n) \cdot \alpha(b_1) \cdot \ldots \cdot \alpha(b_r) = f(a_1 \cdot \ldots \cdot a_n) \cdot f(b_1 \cdot \ldots \cdot b_r)$ und $f(\varepsilon) = e_G$. Weiter ist $f\iota(a) = f(a) = \alpha(a)$, also $f\iota = \alpha$. Um die Eindeutigkeit von f mit $f\iota = \alpha$ zu zeigen, sei $f' : A^* \longrightarrow G$ ein Homomorphismus mit $f'\iota = \alpha$. Dann ist $f'(a_1 \dots a_n) = f'(a_1 \circ \ldots \circ a_n) = f'(a_1) \cdot \ldots \cdot f'(a_n) = f'\iota(a_1) \cdot \ldots \cdot f'\iota(a_n) = \alpha(a_1) \cdot \ldots \cdot \alpha(a_n) = f(a_1 \dots a_n)$. Weiter ist $f'(\varepsilon) = e_G = f(\varepsilon)$. Also gilt $f' = f$.
(2) Der Beweis verläuft ebenso wie in Teil (1). Allerdings müssen alle Referenzen zu $\varepsilon \in A^*$ fortgelassen werden. □

Man kann auch zeigen, daß es zu jeder Menge A eine freie Gruppe $\iota : A \longrightarrow F(A)$ gibt. Die Konstruktion ist jedoch wesentlich komplizierter. Wir haben eine solche Konstruktion daher hier nicht mit aufgenommen.

Beispiele 3.5. (1) $(\mathbb{N}, +)$ ist freie Halbgruppe über $A = \{1\}$.
(2) $(\mathbb{N}_0, +)$ ist freies Monoid über $A = \{1\}$.
(3) $(\mathbb{Z}, +)$ ist freie Gruppe über $A = \{1\}$.

4. Kongruenzrelationen und Restklassen

Wir haben gesehen, daß die freien Strukturen besonders günstige Eigenschaften haben. Wir kennen jedoch Beispiele von Halbgruppen, Monoiden bzw. Gruppen, die nicht frei sind. Wir werden

in diesem Abschnitt zeigen, daß sich alle solchen Objekte zumindest mit Hilfe von freien Objekten beschreiben lassen. Dazu führen wir zunächst eine allgemeine Konstruktion der Restklassenbildung ein, wie wir sie bei der Bildung von Äquivalenzklassen in ähnlicher Weise auch schon früher kennengelernt haben. Der sogleich einzuführende Begriff der Kongruenzrelation spielt für Halbgruppen (Monoide, Gruppen) dieselbe Rolle, wie der Begriff der Äquivalenzrelation für Mengen. Insbesondere werden wir Partitionen nach einer Kongruenzrelation bilden und einen Faktorisierungssatz beweisen.

Definition 4.1. Sei G eine Halbgruppe (Monoid, Gruppe). Eine Teilmenge $R \subset G \times G$ heißt *Kongruenzrelation*, wenn R eine Äquivalenzrelation und eine Unter-Halbgruppe (-Monoid, -Gruppe) von $G \times G$ ist. Dabei ist die Multiplikation auf $G \times G$ komponentenweise definiert: $(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$.

Übung: Sei G eine Gruppe. Sei $R \subset G \times G$ eine Kongruenzrelation für die *Halb*gruppe G. Man zeige, daß R dann auch eine Kongruenzrelation für die Gruppe G ist.
(Hinweis: Ist $(g, h) \in R$, so auch $(h, g), (h^{-1}, h^{-1})$ und (g^{-1}, g^{-1}). Dann ist $(h^{-1}, h^{-1})(h, g)(g^{-1}, g^{-1}) = (g^{-1}, h^{-1}) \in R$.)

Satz 4.2. *Wenn $R \subset G \times G$ eine Kongruenzrelation auf G ist, dann trägt G/R genau eine Struktur einer Halbgruppe (Monoid, Gruppe), so daß die Restklassenabbildung $\nu : G \longrightarrow G/R$ ein Homomorphismus ist.*

Beweis. Im Halbgruppenfall definieren wir eine Operation auf G/R durch das kommutative Diagramm

$$\begin{array}{ccc} G \times G & \xrightarrow{\nu \times \nu} & G/R \times G/R \\ & \searrow^{\alpha} & \downarrow f \\ & & G/R \end{array}$$

mit $\alpha(g, h) := \overline{g \cdot h}$. Die Abbildung f existiert und ist eindeutig bestimmt, weil für $(g, g'), (h, h') \in R$ auch $(g, g') \cdot (h, h') = (g \cdot h, g' \cdot h') \in R \subset G \times G$ gilt. Ist also $g \sim g'$ und $h \sim h'$, so ist

$g \cdot h \sim g' \cdot h'$, also $\overline{g \cdot h} = \overline{g' \cdot h'}$ und damit $\alpha(g,h) = \alpha(g',h')$ Wir schreiben die Multiplikation $f(\overline{g},\overline{h})$ als $\overline{g} \cdot \overline{h}$, also gilt $\overline{g} \cdot \overline{h} = \overline{g \cdot h}$. Die Multiplikation $f : G/R \times G/R \longrightarrow G/R$ ist assoziativ wegen $\overline{g} \cdot (\overline{h} \cdot \overline{k}) = \overline{g} \cdot (\overline{h \cdot k}) = \overline{g \cdot (h \cdot k)} = \overline{(g \cdot h) \cdot k} = \overline{(g \cdot h)} \cdot \overline{k} = (\overline{g} \cdot \overline{h}) \cdot \overline{k}$. Weiter ist die Restklassenabbildung $\nu : G \longrightarrow G/R$ ein Homomorphismus wegen $\nu(g \cdot h) = \overline{g \cdot h} = \overline{g} \cdot \overline{h} = \nu(g) \cdot \nu(h)$. Schließlich ist f eindeutig dadurch festgelegt, daß ν ein Homomorphismus ist, denn $f(\overline{g},\overline{h}) = f(\nu(g),\nu(h)) =$ (da ν ein Homomorphismus ist) $\nu(g \cdot h) = \overline{g \cdot h}$. Im Falle von Monoiden kommt das neutrale Element $e \in G$ hinzu. Wegen $\overline{e} \cdot \overline{g} = \overline{e \cdot g} = \overline{g}$ und $\overline{g} \cdot \overline{e} = \overline{g \cdot e} = \overline{g}$ ist $\overline{e}$ neutrales Element in G/R. Weiter ist $\nu(e) = \overline{e}$. Im Falle von Gruppen kommen inverse Elemente hinzu. Es ist $\overline{g^{-1}} \cdot \overline{g} = \overline{g^{-1} \cdot g} = \overline{e} = \overline{g \cdot g^{-1}} = \overline{g} \cdot \overline{g^{-1}}$, also ist $\overline{g^{-1}}$ invers zu $\overline{g}$ und G/R damit eine Gruppe. □

Beispiele 4.3. (1) In $\mathbb{N}$ ist die Partition

$$\bar{1} = \{1\}, \bar{2} = \{2\}, \bar{3} = \{n \in \mathbb{N} | n \geq 3\}$$

von einer Kongruenzrelation abgeleitet, denn in

$$R = \{(r,s) | r,s \geq 3 \vee r = s\}$$

gilt $(r,s) + (r',s') = (r + r', s + s') \in R$, wie man durch Nachrechnen sofort sieht. Dann hat $\mathbb{N}/R$ die folgende Verknüpfungstafel:

$+$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{3}$
$\bar{2}$	$\bar{3}$	$\bar{3}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{3}$	$\bar{3}$

(2) Sei $n \in \mathbb{N}_0$ fest gewählt. In $\mathbb{Z} \times \mathbb{Z}$ sei $R := \{(r,s) \in \mathbb{Z} \times \mathbb{Z} | \exists q \in \mathbb{Z}[q \cdot n = r - s]\}$. Man sieht leicht, daß R eine Kongruenzrelation (bzgl. der Addition von $\mathbb{Z}$) ist. Die Kongruenzklassen $\mathbb{Z}/R$ sind $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ im Falle $n > 0$ und $\{\bar{0}, \pm\bar{1}, \pm\bar{2}, \pm\bar{3}, \ldots\}$ für $n = 0$. Die Ver-

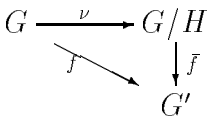
knüpfungstafel für $n > 0$ ist wegen $\bar{r} + \bar{s} = \overline{r+s}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\ldots$	$\overline{n-1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\ldots$	$\overline{n-1}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\ldots$	$\overline{0}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\overline{n-1}$	$\overline{n-1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\ldots$	$\overline{n-2}$

Im Falle $n = 0$ ist R die Gleichheitsrelation auf $\mathbb{Z}$ und $\mathbb{Z}/R \cong \mathbb{Z}$ (als Gruppen). In diesem Beispiel schreiben wir auch $(n) := R$ und damit $\mathbb{Z}/(n)$ für $n > 0$ bzw. $\mathbb{Z}/(0) \cong \mathbb{Z}$. Die hier betrachtete Äquivalenzrelation (n) ist die in Beispiel I. 4.2 (3) betrachtete.
Die Äquivalenzrelation (n) ist auch eine Kongruenzrelation bezüglich der Multiplikation auf $\mathbb{Z}$. $\mathbb{Z}$ ist dann ein Monoid. Die Verknüpfungstafel für $n = 6$ ist wegen $\bar{r} \cdot \bar{s} = \overline{r \cdot s}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Satz 4.4. (Faktorisierungssatz oder Homomorphiesatz) *Sei $f : G \longrightarrow G'$ ein Homomorphismus von Halbgruppen (Monoiden, Gruppen) und R eine Kongruenzrelation in G. Wenn für alle $(a,b) \in R$ gilt $f(a) = f(b)$, dann gibt es genau einen Homomorphismus $\bar{f} : G/R \longrightarrow G'$, so daß*



kommutiert.

BEWEIS. Nach I. 4.9 existiert genau eine Abbildung $\bar{f}$ mit $\bar{f}\nu = f$. Wir zeigen daher nur, daß $\bar{f}$ ein Homomorphismus ist. Da ν nach 4.2 ein Homomorphismus ist gilt $\bar{f}(\bar{a}\cdot\bar{b}) = \bar{f}(\nu(a)\cdot\nu(b)) = \bar{f}(\nu(a\cdot b)) = (\bar{f}\nu)(a\cdot b) = f(a\cdot b) = f(a)\cdot f(b) = (\bar{f}\nu)(a)\cdot(\bar{f}\nu)(b) = \bar{f}(\bar{a})\cdot\bar{f}(\bar{b})$ und im Falle von Monoiden $\bar{f}(\bar{e}) = (\bar{f}\nu)(e) = f(e) = e$. □

Der vorstehende Satz ist das allgemeine und einzige Hilfmittel, um einen Homomorphismus $\bar{f} : G/R \longrightarrow G'$ zu definieren. Wenn man einen solchen Homomorphismus konstruieren soll, so muß man zunächst einen Homomorphismus $f : G \longrightarrow G'$ konstruieren und dann die Voraussetzungen des Satzes erfüllen. Wir wollen das an einigen Beispielen studieren.

Beispiele 4.5. (1) Definiert die folgende Angabe einen Homomorphismus:

$$\mathbb{Z}/(6) \ni \bar{n} \mapsto \bar{n} \in \mathbb{Z}/(3)?$$

Hier ist eine Eigenheit der Notation der Restklassen besonders zu beachten. Es ist $\bar{0} \in \mathbb{Z}/(6)$ die Menge $\bar{0} = \{0, \pm 6, \pm 12, \pm 18, \dots\}$. Weiter ist $\bar{0} \in \mathbb{Z}/(3)$ eine gänzlich andere Menge, nämlich $\bar{0} = \{0, \pm 3, \pm 6, \pm 9, \dots\}$. Der Leser möge sich die Elemente $\bar{1} \in \mathbb{Z}/(6)$ und $\bar{1} \in \mathbb{Z}/(3)$ in entsprechender Schreibweise klarmachen. Bei Verwendung der Schreibweise $\bar{n}$ muß also immer klar sein, in welcher Menge dieses Element liegen soll. Wir sind insbesondere mit der obigen Angabe weit von einer identischen Abbildung entfernt.
Die wichtigste Frage ist jedoch, ob die oben angegebene Zuordnung oder Relation eine (wohldefinierte) Abbildung ist. Es können nämlich verschiedene Zahlen $n \in \mathbb{Z}$ gleiche Elemente $\bar{n} \in \mathbb{Z}/(6)$ bestimmen, z.B. $\bar{1} = \bar{7}$. Wir haben also zwei verschiedene Repräsentanten für $\bar{1}$, nämlich 1 und 7. Dann muß man überprüfen, daß in jedem solchen Fall die Bilder $\bar{n} \in \mathbb{Z}/(3)$ nicht von der besonderen Wahl

des Repräsentanten n für $\bar{n}$ abhängt. Also ist der Faktorisierungssatz einzusetzen. Das geschieht so:
Die Abbildung $\alpha := \nu_3 : \mathbb{Z} \longrightarrow \mathbb{Z}/(3)$ (die Restklassenabbildung) ist nach 4.2 ein Homomorphismus. Für $R = (6)$ ist $(n, r) \in R$ genau dann, wenn $n - r = q \cdot 6$ für ein $q \in \mathbb{Z}$. Dann gilt aber $\alpha(n) = \nu_3(n) = \nu_3(r + q \cdot 6) = \nu_3(r + 2q \cdot 3) = \nu_3(r) = \alpha(r)$. Also gibt es genau einen Homomorphismus $f : \mathbb{Z}/(6) \longrightarrow \mathbb{Z}/(3)$ mit $f\nu_6 = \nu_3$, d.h. mit $f(\bar{n}) = \nu_3(n) = \bar{n}$, also der gewünschte Homomorphismus.
Wie sind wir nun gerade auf den Homomorphismus $\alpha := \nu_3$ gekommen. Da das Dreieck

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\nu} & \mathbb{Z}/(6) \\ & \searrow^{\alpha} & \downarrow f \\ & & \mathbb{Z}/(3) \end{array}$$

kommutieren soll, muß, falls f überhaupt existiert, $\alpha = f\nu$ sein. Dann ergibt sich aber $\alpha(n) = f\nu_6(n) = f(\bar{n}) = \bar{n} = \nu_3(n)$.

(2) Definiert die folgende Angabe einen Homomorphismus:

$$\mathbb{Z}/(6) \ni \bar{n} \mapsto \bar{n} \in \mathbb{Z}/(4)?$$

Wieder setzen wir den Faktorisierungssatz ein. Als Homomorphismus $\alpha : \mathbb{Z} \longrightarrow \mathbb{Z}/(4)$ müssen wir wie zuvor $\alpha = \nu_4$ wählen. Für $(n, r) \in (6)$, also $n = r + q \cdot 6$ ist $\nu_4(n) = \nu_4(r)$ oder $(n, r) \in (4)$ zu zeigen, also müssen wir prüfen, ob $n - r$ auch durch 4 teilbar ist, wenn es durch 6 teilbar ist. Das ist offenbar nicht der Fall und liefert und schon ein Gegenbeispiel. In $\mathbb{Z}/(6)$ ist $\bar{6} = \bar{0} = \{0, \pm 6, \pm 12, \pm 18, \dots\}$. Aber in $\mathbb{Z}/(4)$ ist $\bar{6} = \{2, -4, 6, -8, 10, \dots\} \neq \{0, \pm 4, \pm 8 \pm 12, \dots\} = \bar{0}$, also kann die angegebene Relation keine Abbildung sein, weil ein Element $\bar{6} = \bar{0} \in \mathbb{Z}/(6)$ zwei verschiedene Bilder $\bar{6} \neq \bar{0}$ in $\mathbb{Z}/(4)$ hat.

(3) Definiert die folgende Angabe einen Homomorphismus:

$$\mathbb{Z}/(3) \ni \bar{n} \mapsto \overline{n^3} \in \mathbb{Z}/(3)?$$

Der Homomorphismus $\alpha : \mathbb{Z} \longrightarrow \mathbb{Z}/(3)$ muß die Abbildung $\alpha(n) = \overline{n^3}$ sein. Das ist tatsächlich ein Homomorphismus, denn

$$\alpha(n+r) = \overline{(n+r)^3} = \overline{n^3 + 3n^2r + 3nr^2 + r^3}$$

und

$$\alpha(n) + \alpha(r) = \overline{n^3} + \overline{r^3} = \overline{n^3 + r^3}.$$

Die beiden rechten Seiten der Gleichungen stimmen überein, weil $n^3 + 3n^2r + 3nr^2 + r^3 - n^3 - r^3 = (n^2r + nr^2) \cdot 3$. Ist weiterhin $n \sim r$, d.h. $n - r = q \cdot 3$, so ist $n^3 = (r + q \cdot 3)^3 = r^3 + (r^2q \cdot 3 + rq^2 \cdot 9 + q^3 \cdot 9) \cdot 3$, also $\alpha(n) = \overline{n^3} = \overline{r^3} = \alpha(r)$. Damit sind die Voraussetzungen des Faktorisierungssatzes erfüllt.
Tatsächlich kann man leicht nachrechnen, daß die gegebene Abbildung sogar die identische Abbildung ist.

Satz 4.6. *Sei $f : G \longrightarrow G'$ ein Homomorphismus von Halbgruppen (Monoiden, Gruppen). Dann ist die zu f gehörige Äquivalenzrelation $a \sim b :\Longleftrightarrow f(a) = f(b)$ (vgl. I. 4.3) eine Kongruenzrelation.*

BEWEIS. Sei $R \subset G \times G$ die gegebene Äquivalenzrelation. Seien $(a,b), (a',b') \in R$. Dann ist $f(a \cdot a') = f(a) \cdot f(a') = f(b) \cdot f(b') = f(b \cdot b)$, also auch $(a \cdot a', b \cdot b') \in R$. Ebenso ist im Monoidfall $(e,e) \in R$, weil R eine Äquivalenzrelation ist. Schließlich ist im Falle von Gruppen mit $(a,b) \in R$ auch $(a^{-1}, b^{-1}) \in R$, denn $f(a^{-1}) = f(a)^{-1} = f(b)^{-1} = f(b^{-1})$. □

Bemerkung 4.7. Mit der Konstruktion von G/R erhält man eine Bijektion zwischen der Menge aller Kongruenzrelationen in G und der Menge aller möglichen Restklassenobjekte G/R, d.h. der Menge aller Partitionen von G, die die Struktur einer Halbgruppe

(Monoid, Gruppe) so tragen, daß $\nu : G \longrightarrow G/R$ ein Homomorphismus wird (vgl. I. 4.7). Die Aussagen von I. 4.10 übertragen sich sinngemäß. Insbesondere ist $\mathrm{Bi}(f)$ eine Unter-Halbgruppe (-Monoid, -Gruppe) für einen Homomorphismus $f : G \longrightarrow G'$, und die von $\nu : G/R \longrightarrow G'$ induzierte Abbildung $\nu' : G/R \longrightarrow \mathrm{Bi}(f)$ ist ein Isomorphismus, wobei R die zu f gehörige Kongruenzrelation ist.

Definition 4.8. Sei G eine Halbgruppe (Monoid, Gruppe), die von einer Menge A erzeugt wird. Dann gibt es nach 3.1 genau einen Homomorphismus $f : F(A) \longrightarrow G$, der die Inklusion $\alpha : A \longrightarrow G$ fortsetzt. Eine *Relation für G bzgl. A* ist ein Paar (w_1, w_2) in $F(A) \times F(A)$ mit $f(w_1) = f(w_2)$. Die Menge der Relationen für G bezüglich A bezeichnen wir mit $R_G(A) := \{(w_1, w_2) \in F(A) \times F(A) | f(w_1) = f(w_2)\}$.

Folgerung 4.9. *Die Menge der Relationen für G bezüglich A ist eine Kongruenzrelation auf $F(A)$.*

Beweis. $R_G(A)$ ist die Kongruenzrelation, die durch den Homomorphismus $f : F(A) \longrightarrow G$ induziert wird. □

Satz 4.10. *Jede Halbgruppe (Monoid, Gruppe) ist isomorph zu einem Objekt $F(A)/R$, wobei R eine Kongruenzrelation ist.*

Beweis. Sei A eine Erzeugendenmenge von G. Eine solche existiert immer, z.B. $A = G$. Es gibt aber im allgemeinen sehr viel kleinere Erzeugendenmengen für G. Sei $R := R_G(A)$. Wir definieren einen surjektiven Homomorphismus $f : F(A) \longrightarrow G$ durch das kommutative Diagramm

$$\begin{array}{ccc} A & \xrightarrow{\iota} & F(A) \\ & \searrow^{\alpha} & \downarrow f \\ & & G, \end{array}$$

wobei $\alpha : A \longrightarrow G$ die Inklusionsabbildung ist. Da $A \subset \mathrm{Bi}(f)$ und $\mathrm{Bi}(f)$ nach 2.6 eine Unter-Halbgruppe (-Monoid, -Gruppe)

von G ist, ist nach 1.10 $G = \bar{A} \subset \mathrm{Bi}(f) \subset G$, also $\mathrm{Bi}(f) = G$ und damit f surjektiv.
Dann induziert $f : F(A) \longrightarrow G$ nach I. 4.9 und I. 4.10 (3) einen bijektiven Homomorphismus $\bar{f} : F(A)/R \longrightarrow G$, so daß

$$\begin{array}{ccc} F(A) & \xrightarrow{\nu} & F(A)/R \\ & \searrow^{f} & \downarrow \bar{f} \\ & & G \end{array}$$

kommutiert, denn $\bar{f}(\overline{w_1} \cdot \overline{w_2}) = \bar{f}(\overline{w_1 \cdot w_2}) = \bar{f}\nu(w_1 \cdot w_2) = f(w_1 \cdot w_2) = f(w_1) \cdot f(w_2) = \bar{f}\nu(w_1) \cdot \bar{f}\nu(w_2) = \bar{f}(\overline{w_1}) \cdot \bar{f}(\overline{w_2})$.
Im Falle von Monoiden gilt zusätzlich $\bar{f}(\bar{\varepsilon}) = f(\varepsilon) = e$. □

Bemerkung 4.11. Zur Darstellung einer Halbgruppe (Monoid, Gruppe) G in der Form $F(A)/R$ genügt es also, eine Erzeugendenmenge A für G und eine Erzeugendenmenge B für $R \subset F(A) \times F(A)$ anzugeben. Gibt man eine Menge A und eine Teilmenge $B \subset F(A) \times F(A)$ vor, so kann man daraus eine kleinste Kongruenzrelation $R \subset F(A) \times F(A)$ mit $B \subset R$ bilden durch $R := \bigcap\{S \subset F(A) \times F(A) | S \text{ Kongruenzrelation} \wedge A \subset S\}$. Damit definieren A und B eine Halbgruppe (Monoid, Gruppe) $F(A)/R$ durch *Erzeugende* A und *Relationen* B.

5. Restklassengruppen

Bei den Gruppen hängt die Restklassenbildung mit gewissen Untergruppen mit einer ganz besonderen Eigenschaft zusammen, die man normale Untergruppen nennt. Genauer gibt es eine Bijektion zwischen allen normalen Untergruppen einer Gruppe G und allen Kongruenzrelationen auf G. Die etwas unhandlichen Kongruenzrelationen lassen sich also durch einfachere normale Untergruppen erzetzen. Auch die Faktorgruppen oder Restklassengruppen lassen sich damit einfacher beschreiben.

Definition 5.1. Eine Untergruppe H einer Gruppe G heißt *Normalteiler* (oder *normale Untergruppe*), wenn

$$\forall g \in G, h \in H \exists h' \in H[gh = h'g].$$

Bemerkung 5.2. Äquivalent dazu ist, daß für alle $g \in G$ gilt $gHg^{-1} = \{ghg^{-1}|h \in H\} \subset H$ oder daß für alle $g \in G$ gilt $gH = Hg$.
Die Bedingung läßt sich besonders einfach für abelsche (kommutative) Gruppen G erfüllen, es ist nämlich $gh = hg$ für alle $h \in H$ und alle $g \in G$. Zu g und h kann man also immer $h \in H$ wählen, um die Bedingung für die Normalität zu erfüllen. Es gilt also: jede Untergruppe einer abelschen Gruppe ist eine normale Untergrppe.

Satz 5.3. *Sei G eine Gruppe. Die Zuordnungen*

$$\mathcal{P}(G) \ni H \mapsto R \in \mathcal{P}(G \times G)$$

mit $R := \{(a,b)|ab^{-1} \in H\}$ und

$$\mathcal{P}(G \times G) \ni R \mapsto H \in \mathcal{P}(G)$$

mit $H := \{ab^{-1}|(a,b) \in R\}$ definieren eine Bijektion zwischen der Menge der Normalteiler H von G und der Menge der Kongruenzrelationen R auf G.

Beweis. 1. Behauptung: Wenn H ein Normalteiler ist, dann ist $R := \{(a,b)|ab^{-1} \in H\}$ eine Kongruenzrelation.
Beweis: R ist reflexiv, weil $a \cdot a^{-1} = e \in H$ für alle $a \in G$ gilt. Ist $(a,b),(b,c) \in R$, so ist $a \cdot b^{-1}, b \cdot c^{-1} \in H$, also auch $a \cdot c^{-1} = (a \cdot b^{-1}) \cdot (b \cdot c^{-1}) \in H$. Also ist $(a,c) \in R$ und R damit transitiv. Ist $(a,b) \in R$, so ist $a \cdot b^{-1} \in H$, also $b \cdot a^{-1} = (b^{-1})^{-1} \cdot a^{-1} = (a \cdot b^{-1})^{-1} \in H$ und damit $(b,a) \in R$. Daher ist R eine Äquivalenzrelation. Bisher haben wir nur verwendet, daß H eine Untergruppe von G ist. Seien jetzt $(a,b),(c,d) \in R$. Dann ist $a \cdot b^{-1}, c \cdot d^{-1} \in H$ und damit $(a \cdot c) \cdot (b \cdot d)^{-1} = a \cdot c \cdot d^{-1} \cdot b^{-1} = a \cdot h \cdot b^{-1} = h' \cdot a \cdot b^{-1} \in H$, wobei $h = c \cdot d^{-1} \in H$ und $a \cdot h = h' \cdot a$, weil H ein Normalteiler ist. Damit ist auch $(a \cdot c, b \cdot d) \in R$. Nach der Übung im Anschluß an 4.1 ist R damit eine Kongruenzrelation.
2. Behauptung: Wenn R eine Kongruenzrelation ist, dann ist $H := \{ab^{-1}|(a,b) \in R\}$ ein Normalteiler.

Beweis: H ist eine Untergruppe von G. Wegen $(e,e) \in R$ ist $e = e \cdot e^{-1} \in H$.
Ist $x = a \cdot b^{-1} \in H$ mit $(a,b) \in R$, so ist auch $(b,a) \in R$, also $x^{-1} = (a \cdot b^{-1})^{-1} = b \cdot a^{-1} \in H$.
Seien schließlich $x = a \cdot b^{-1}$ und $y = c \cdot d^{-1}$ in H mit $(a,b),(c,d) \in R$. Dann ist auch $(a,b) \cdot (b^{-1},b^{-1}) \cdot (c,d) \cdot (d^{-1},d^{-1}) = (a \cdot b^{-1} \cdot c \cdot d^{-1}, b \cdot b^{-1} \cdot d \cdot d^{-1}) = (a \cdot b^{-1} \cdot c \cdot d^{-1}, e) \in R$, also $x \cdot y = a \cdot b^{-1} \cdot c \cdot d^{-1} \cdot e^{-1} \in H$.
Sei schließlich $x \in H$ und $c \in G$. Sei $x = a \cdot b^{-1}$ mit $(a,b) \in R$, so ist auch $(c,c) \cdot (a,b) \cdot (b^{-1},b^{-1}) \cdot (c^{-1},c^{-1}) = (c \cdot a \cdot b^{-1} \cdot c^{-1}, c \cdot b \cdot b^{-1} \cdot c^{-1}) = (c \cdot a \cdot b^{-1} \cdot c^{-1}, e) \in R$, also $y := c \cdot a \cdot b^{-1} \cdot c^{-1} \in H$. Zu $x = a \cdot b^{-1}$ und c ist damit ein $y \in H$ gefunden mit $y \cdot c = c \cdot a \cdot b^{-1} \cdot c^{-1} \cdot c = c \cdot a \cdot b^{-1} = c \cdot x$. Damit ist H ein Normalteiler.
3. Behauptung: Die Hintereinanderausführung $H \mapsto R \mapsto H'$ ist die Identität.
Beweis: Es seien also

$$R := \{(a,b) | ab^{-1} \in H\} \quad \text{und} \quad H' := \{ab^{-1} | (a,b) \in R\}.$$

Wir zeigen $H = H'$. Sei $x \in H'$. Dann ist $x = ab^{-1}$ für ein $(a,b) \in R$. Für (a,b) gilt aber $ab^{-1} \in H$, also ist $x \in H$ und damit $H' \subset H$. Ist umgekehrt $h \in H$, so ist $(h,e) \in R$ und damit $h = he^{-1} \in H'$, also auch $H \subset H'$.
4. Behauptung: Die Hintereinanderausführung $R \mapsto H \mapsto R'$ ist die Identität.
Beweis: Es seien also

$$H := \{ab^{-1} | (a,b) \in R\} \quad \text{und} \quad R' := \{(a,b) | ab^{-1} \in H\}.$$

Wir zeigen $R = R'$. Sei $(a,b) \in R$. Dann ist $ab^{-1} \in H$ und daher $(a,b) \in R'$, also $R \subset R'$. Sei $(a,b) \in R'$. Dann gilt $ab^{-1} \in H$, also gibt es $(c,d) \in R$ mit $cd^{-1} = ab^{-1}$. Wegen $(b,b),(d^{-1},d^{-1}) \in R$ folgt $(a,b) = (ab^{-1}b,b) = (cd^{-1}b,b) = (c,d)(d^{-1},d^{-1})(b,b) \in R$, also $(a,b) \in R$ und damit auch $R' \subset R$. □

Bemerkung 5.4. Man schreibt nun auch $G/H := G/R$. Die Kongruenzklassen $\overline{a}$ lassen sich schreiben als $\overline{a} = \{b \in G | (b,a) \in$

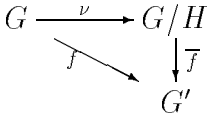
$R\} = \{b|\exists h \in H[b \cdot a^{-1} = h]\} = \{b|\exists h \in H[b = h \cdot a]\} = H \cdot a = a \cdot H$. Die Verknüpfung in G/H ist $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ oder $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$.

Definition 5.5. Sei H ein Normalteiler von G. Die Gruppe

$$G/H = \{a \cdot H | a \in G\}$$

heißt *Restklassengruppe* oder *Faktorgruppe von G modulo H.*

Satz 5.6. (Faktorisierungs- oder Homomorphiesatz für Gruppen) *Sei $f : G \longrightarrow G'$ ein Homomorphismus von Gruppen und H ein Normalteiler in G. Wenn $f(H) = \{e_{G'}\}$, dann gibt es genau einen Homomorphismus $\overline{f} : G/H \longrightarrow G'$, so daß*



kommutiert.

BEWEIS. Nach I. 4.9 existiert $\overline{f}$ eindeutig als Abbildung, wenn für alle $a, b \in G$ mit $(a, b) \in R$ gilt $f(a) = f(b)$. Aber wenn $(a, b) \in R$ ist, dann ist $a \cdot b^{-1} \in H$, also $f(a \cdot b^{-1}) = e_{G'}$ und damit $f(a) = f(b)$, denn $f(a) \cdot f(b)^{-1} = f(a \cdot b^{-1}) = e_{G'}$. Da die Multiplikation in G/H auf den Repräsentanten durchgeführt wird, gilt (wie im Beweis von 4.2) $\overline{f}(\overline{a} \cdot \overline{b}) = \overline{f}(\overline{a \cdot b}) = \overline{f}\nu(a \cdot b) = f(a \cdot b) = f(a) \cdot f(b) = \overline{f}\nu(a) \cdot \overline{f}\nu(b) = \overline{f}(\overline{a}) \cdot \overline{f}(\overline{b})$, also ist $\overline{f}$ ein Homomorphismus. □

Beispiele 5.7. (1) Sei $n \in \mathbb{N}$. Dann ist

$$S_n := \{\{1, \ldots, n\} \longrightarrow \{1, \ldots, n\} | a \text{ bijektiv } \}$$

unter der Verknüpfung von Abbildungen eine Gruppe (I. 2.22). S_n heißt *symmetrische Gruppe* oder *Permutationsgruppe*. Nach (II. 4.6) ist S_n eine Gruppe mit $n!$ Elementen. S_n hat Erzeugende

$$\begin{pmatrix} 1, 2, 3, \ldots, n \\ 2, 1, 3, \ldots, n \end{pmatrix} \text{ und } \begin{pmatrix} 1, 2, 3, \ldots, n \\ 2, 3, 4, \ldots, 1 \end{pmatrix}.$$

Eine andere Erzeugendenmenge ist $\{\sigma_i\} \subset S_n$ für $i = 1, \ldots, n-1$ mit

$$\sigma_i(k) := \begin{cases} i+1, & \text{für } k = i, \\ i, & \text{für } k = i+1, \\ k, & \text{sonst.} \end{cases}$$

Die σ_i heißen *Transpositionen.*
Die σ_i erfüllen die Relationen $\sigma_i\sigma_j = \sigma_j\sigma_i$ für $i < j-1$ und $1 \leq i, j \leq n-1$, und $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ für $1 \leq i \leq n-2$, und $\sigma_i^2 = \mathrm{id}$ für $1 \leq i \leq n-1$. Man kann S_n auch darstellen als $F(\{\sigma_1, \ldots, \sigma_{n-1}\})/R$, wobei R die von den Relationen $(\sigma_i\sigma_j, \sigma_j\sigma_i), (\sigma_i\sigma_{i+1}\sigma_i, \sigma_{i+1}\sigma_i\sigma_{i+1})$ und $(\sigma_i\sigma_i, \varepsilon)$ erzeugte Kongruenzrelation ist.

(2) Die Untergruppe $A_n \subset S_n$ mit $A_n = \{s_1 \cdot \ldots \cdot s_{2t} | t \in \mathbb{N}_0 \wedge s_i \in \{\sigma_1, \ldots, \sigma_{n-1}\}\}$ heißt Gruppe der *geraden Permutationen.* Man kann zeigen, daß $A_n \subset S_n$ ein Normalteiler ist und daß $A_n \neq S_n$ gilt ($n \geq 2$). Dann hat S_n/A_n genau 2 Elemente $\overline{\mathrm{id}}$ und $\overline{\sigma_1}$, denn für $s_1 \cdot \ldots \cdot s_t \in S_n$ gilt $s_1 \cdot \ldots \cdot s_t \sim \mathrm{id}$ ($s_1 \cdot \ldots \cdot s_t \cdot \mathrm{id}^{-1} \in A_n$), wenn t gerade ist, und $s_1 \cdot \ldots \cdot s_t \sim \sigma_1$ ($s_1 \cdot \ldots \cdot s_t \cdot \sigma_1 \in A_n$), wenn t ungerade ist. Dabei seien die s_i Transpositionen. Es genügt Elemente der Form $s_1 \cdot \ldots \cdot s_t$ zu betrachten, weil $s_i = s_i^{-1}$ gilt. Die Multiplikationstafel muß daher

$\cdot$	$\overline{\mathrm{id}}$	$\overline{\sigma_1}$
$\overline{\mathrm{id}}$	$\overline{\mathrm{id}}$	$\overline{\sigma_1}$
$\overline{\sigma_1}$	$\overline{\sigma_1}$	$\overline{\mathrm{id}}$

sein. Die Abbildung $\overline{f} : S_n/A_n \longrightarrow \{1, -1\}$ mit $\overline{f}(\overline{\mathrm{id}}) = 1, \overline{f}(\overline{\sigma_1}) = -1$ ist ein Isomorphismus, wenn man $\{1, -1\}$ als Gruppe mit der gewöhnlichen Multiplikation auffaßt:

$\cdot$	1	-1
1	1	-1
-1	-1	1

.

Der Homomorphismus $S_n \xrightarrow{\nu} S_n/A_n \xrightarrow{\overline{f}} \{1,-1\}$ heißt *Signatur* oder *Vorzeichen*: sgn $:= \overline{f}\nu$. Eine Permutation $\tau \in S_n$ heißt *gerade*, wenn sie sich als Produkt einer geraden Anzahl von Transpositionen schreiben läßt. Sonst heißt sie *ungerade*. $\tau \in S_n$ ist genau dann gerade, wenn $\operatorname{sgn}(\tau) = 1$ gilt.

Satz 5.8. (Cayley) *Sei G eine endliche Gruppe. Dann gibt es eine Untergruppe U einer Permutationsgruppe S_n, zu der G isomorph ist.*

BEWEIS. Habe G genau n Elemente und sei

$$G = \{e = a_1, \ldots, a_n\}.$$

Jedem $a \in G$ ordnen wir die Permutation $\sigma_a : \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$ zu mit $a \cdot a_i = a_{\sigma_a(i)}$. Offenbar gibt es zu jedem Index i genau einen Index $\sigma_a(i)$ mit $a \cdot a_i = a_{\sigma_a(i)}$. Daher ist σ_a eine Abbildung. Die Umkehrabbildung von σ_a ist $\tau := \sigma_{a^{-1}}$, denn $a_i = a^{-1} \cdot a \cdot a_i = a^{-1} \cdot a_{\sigma_a(i)} = a_{\tau(\sigma_a(i))}$ und $a_i = a \cdot a^{-1} \cdot a_i = a \cdot a_{\varepsilon(i)} = a_{\sigma_a(\tau(i))}$, also gilt $\tau(\sigma_a(i)) = i = \sigma_a(\tau(i))$. Damit ist σ_a bijektiv, also eine Permutation. Wir haben somit eine Abbildung $\sigma : G \ni a \mapsto \sigma_a \in S_n$ definiert. Wegen $a_{\sigma_{a\cdot b}(i)} = (a \cdot b) \cdot a_i = a \cdot b \cdot a_i = a \cdot a_{\sigma_b(i)} = a_{\sigma_a(\sigma_b(i))}$ ist $\sigma_{a\cdot b} = \sigma_a \circ \sigma_b$, also ist σ ein Homomorphismus. Schließlich ist σ injektiv, denn aus $\sigma_a = \sigma_b$ folgt $a = a\cdot e = a\cdot a_1 = a_{\sigma_a(1)} = a_{\sigma_b(1)} = b \cdot a_1 = b$ Sei $U := \operatorname{Bi}(\sigma)$. Dann ist U eine Untergruppe von S_n und der eingeschränkte Homomorphismus $\sigma' : G \longrightarrow \operatorname{Bi}(\sigma) = U$ bijektiv, also ein Isomorphismus. □

Definition 5.9. (1) Sei G eine endliche Gruppe. Die Anzahl der Elemente von G heißt *Ordnung* von G.

(2) Sei $a \in G$ ein Element einer beliebigen Gruppe. Wenn es ein kleinstes $n \in \mathbb{N}$ gibt mit $a^n = a \cdot \ldots \cdot a(n\text{-mal}) = e$, dann heißt n die *Ordnung* von a. Gibt es kein solches n, so sagen wir, daß die Ordnung von a unendlich ist.

Man beachte, daß dieser Begriff einer Ordnung nichts zu tun hat mit dem Begriff einer geordneten Menge.

Bemerkung 5.10. Wenn es ein $n \in \mathbb{N}$ mit $a^n = e$ gibt, so gibt es auch ein kleinstes solches n, da $\mathbb{N}$ wohlgeordnet ist. Wir betrachten jetzt ein Element $a \in G$ in einer endlichen Gruppe. Wenn $a^r = a^s$ ist und $r < s$, so ist $a^{s-r} = e$, denn $a^{s-r} = a^{s-r}a^r(a^s)^{-1} = a^s(a^s)^{-1} = e$.

Wir betrachten die Folge $a, a^2, a^3, a^4, \ldots$. Die Elemente können nicht alle paarweise verschieden sein, denn sie liegen in G und G ist endlich. Sei nun s die kleinste Zahl, so daß ein r mit $1 \leq r < s$ existiert mit $a^r = a^s$. Sei $n := s-r$. Dann ist $a^n = e$, die Elemente $a, a^2, \ldots, a^n$ sind alle paarweise verschieden (denn $n = s-r < s$, weil $r \geq 1$). Damit ist n die Ordnung von a. Für $t > n$ gibt es eindeutig bestimmte q und r mit $t = qn + r$ und $0 \leq r < n$. Dann ist $a^t = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r$. Also ist $\{a, a^2, \ldots, a^n\} = \{a, a^2, \ldots, a^n, a^{n+1}, \ldots\}$. Weiter ist $a^i \cdot a^{n-i} = a^n = e$ für $1 \leq i < n$, d.h. alle Elemente in $\{a, a^2, \ldots, a^{n-1}\}$ haben ihr inverses Element ebenfalls in dieser Menge. Insgesamt ist damit $U = \{a, a^2, \ldots, a^n\}$ eine Untergruppe der Ordnung n, die von *a erzeugte zyklische Untergruppe* von G.

Wir haben damit allgemein bewiesen, daß ein Element der Ordnung n eine Untergruppe der Ordnung n erzeugt. Hat das Element a unendliche Ordnung (in einer unendlichen Gruppe G), so hat die von a erzeugte Untergruppe $\overline{\{a\}}$ ebenfalls unendlich viele Elemente.

Man beachte, daß es in einer unendlichen Gruppe Elemente endlicher Ordnung geben kann. In $(\mathbb{R} \setminus \{0\}, \cdot)$ hat z.B. (-1) die Ordnung 2.

Satz 5.11. (Lagrange) *In einer endlichen Gruppe G ist die Ordnung jeder Untergruppe U ein Teiler der Ordnung der Gruppe. Insbesondere ist die Ordnung jedes Elements ein Teiler der Ordnung der Gruppe.*

BEWEIS. Wir definieren auf G eine Partition $G/U := \{aU | a \in G\}$, wobei $aU := \{au | u \in U\}$. Wegen $e \in U$ gilt $a \in aU$, also ist $\bigcup_{a \in G} aU = G$. Sei $c \in aU \cap bU$. Dann ist $c = au_1 = bu_2$, also $a = bu_2u_1^{-1} \in bU$ und $au = bu_2u_1^{-1}u \in bU$. Damit ist $aU \subset bU$ und analog $bU \subset aU$, d.h. $aU = bU$. Damit ist gezeigt, daß G/U eine Partition ist. Zwischen aU und U gibt es eine bijektive Abbildung $aU \ni x \mapsto a^{-1}x \in U$, denn wenn $x = au$, dann ist $a^{-1}x = a^{-1}au = u \in U$. Die Umkehrabbildung ist $U \ni u \mapsto au \in aU$. Daher haben alle Klassen aU der Partition gleich viele Elemente, etwa r Elemente. Da $G = \bigcup aU$ eine Vereinigung von s paarweise disjunkten Mengen ist, hat G genau $s \cdot r$ Elemente, also ist r, die Ordnung von U, ein Teiler der Ordnung von G. □

Bemerkung 5.12. Wir wissen zunächst nicht, wieviele paarweise verschiedene (und damit auch disjunkte) Mengen der Form aU wir haben. Es können a und b verschieden sein, und es kann trotzdem $aU = bU$ gelten. Da aber G endlich ist, können nur endlich viele (oben s) solche Klassen auftreten.

Bemerkung 5.13. Bezeichnen wir $U\backslash G := \{Ua | a \in G\}$, so ist dies ebenfalls eine Partition von G. Die Partitionen $U\backslash G$ und G/U sind im allgemeinen verschieden. Es gilt $U\backslash G = G/U$ genau dann, wenn U ein Normalteiler ist. Wir beachten dazu die Definition 5.1. Damit ist nur zu zeigen, daß $aU = Ub$ impliziert $aU = Ua$. Aber aus $aU = Ub$ folgt $a \in Ub$ und damit wie oben $Ub = Ua$.

6. Ringe und Körper

Bei den Mengen von Zahlen, etwa den ganzen oder den komplexen Zahlen, haben wir Beispiele gefunden, bei denen zwei verschiedene Verknüpfungen, z.B. die Addition und die Multiplikation, auftreten. Die beiden Verknüpfungen erfüllen Eigenschaften, die nur mit beiden Verknüpfungen gemeinsam ausgedrückt werden können, wie das Assoziativgesetz. Wir werden daher jetzt die Axiome dieser Beispiele betrachten und sie verallgemeinern.

Definition 6.1. Ein *Ring* ist ein Tripel $(R, +, \cdot)$ mit folgenden Eigenschaften

(1) $(R, +)$ ist eine abelsche Gruppe,
(2) $(R, \cdot)$ ist eine Halbgruppe,
(3) Es gelten die Distributiv-Gesetze

$$\forall a, b, c, \in R[\quad a \cdot (b + c) = a \cdot b + a \cdot c \wedge \\ (a + b) \cdot c = a \cdot c + b \cdot c \ ]$$

(wobei die Multiplikation stärker bindet (also Präzedenz hat), als die Addition: $a \cdot b + c = (a \cdot b) + c$).

Ein Ring $(R, +, \cdot)$ heißt *Ring mit Einselement* oder *unitärer Ring*, wenn $(R, \cdot)$ ein Monoid ist. Ein Ring heißt *kommutativer Ring*, wenn $(R, \cdot)$ kommutativ ist. Ein Ring heißt *nullteilerfrei*, wenn gilt: $\forall a, b \in R[a \cdot b = 0 \Longrightarrow a = 0 \vee b = 0]$. Wir schreiben im folgenden das *Produkt* $a \cdot b$ auch als ab. Das neutrale Element von $(R, +)$ wird mit *Null* oder 0 bezeichnet. Das neutrale Element von $(R, \cdot)$ für einen unitären Ring wird mit Eins oder 1 bezeichnet. Die Verknüpfungen $+ : R \times R \longrightarrow R$ bzw. $\cdot : R \times R \longrightarrow R$ heißen *Addition* bzw. *Multiplikation*. Das Inverse eines Elements $a \in R$ unter der Addition wird mit $-a$ oder $(-a)$ bezeichnet, unter der Multiplikation (falls es existiert) mit a^{-1}.

Lemma 6.2. *(Rechengesetze in Ringen) Seien* $a, b \in R$. *Dann gilt*

(1) $0a = a0 = 0$,
(2) $(-ab) = (-a)b = a(-b)$,
(3) $(-a)(-b) = ab$,
(4) $(-a) = (-1)a$.
(5) *Wenn* $0 = 1$, *dann ist* $R = \{0\}$.

BEWEIS. (1) Es ist $0a = (0 + 0)a = 0a + 0a$. Durch Subtrahieren von $0a$ (Addieren von $(-0a)$) erhält man $0 = 0a$. Analog ergibt sich $0 = a0$.
(2) Es ist $ab + (-a)b = (a + (-a))b = 0b = 0$, also ist $(-a)b = (-ab)$ invers zu ab. Analog ist $a(-b) = (-ab)$.

(3) Es ist $(-a)(-b) = (-a(-b)) = (-(-ab)) = ab$.
(4) Es ist $(-1)a = (-1a) = (-a)$.
(5) Sei $0 = 1$ und $a \in R$. Dann ist $a = 1a = 0a = 0$. □

Definition 6.3. Seien R und S Ringe und $f : R \longrightarrow S$ eine Abbildung. f heißt *Homomorphismus von Ringen*, wenn

$$\forall a, b \in R[f(a + b) = f(a) + f(b) \wedge f(a \cdot b) = f(a) \cdot f(b)].$$

Seien R und S unitäre Ringe und $f : R \longrightarrow S$ eine Abbildung. f heißt *Homomorphismus von unitären Ringen*, wenn $f : R \longrightarrow S$ ein Homomorphismus von Ringen ist und gilt $f(1) = 1$.

Beispiele 6.4. (1) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind unitäre kommutative Ringe. $(\mathbb{N}_0, +, \cdot)$ ist kein Ring, weil $(\mathbb{N}_0, +)$ keine Gruppe ist.

(2) Sei $n \in \mathbb{N}_0$ fest gewählt. Dann ist $\mathbb{Z}/(n)$ mit der Addition und Multiplikation der Kongruenzklassen definiert durch Addition und Multiplikation der Repräsentanten wie in 4.3(2)

$$\overline{r} + \overline{s} = \overline{r + s}, \qquad \overline{r} \cdot \overline{s} = \overline{rs}$$

ein unitärer kommutativer Ring. Wegen 4.2 und 4.3(2) sind nur die Distributivgesetze zu prüfen:

$$\overline{r} \cdot (\overline{s} + \overline{t}) = \overline{r} \cdot (\overline{s + t}) = \overline{r(s + t)} = \overline{rs + rt} = \overline{rs} + \overline{rt} = \overline{r} \cdot \overline{s} + \overline{r} \cdot \overline{t}$$

und analog

$$(\overline{r} + \overline{s}) \cdot \overline{t} = \overline{r} \cdot \overline{t} + \overline{s} \cdot \overline{t}.$$

(3) Restklassentests: Sei $\alpha : \mathbb{N} \longrightarrow \mathbb{Z}$ eine Abbildung, deren Bild eine endliche Teilmenge $X \subset \mathbb{Z}$ ist und für die gilt $\forall r \in \mathbb{N}[\overline{\alpha(r)} = \overline{r}]$, wobei die Restklassen in $\mathbb{Z}/(n)$ für ein festes $n \in \mathbb{Z}$ betrachtet werden. Dann gilt $\overline{\alpha(r + s)} = \overline{\alpha(r) + \alpha(s)}$ und $\overline{\alpha(r \cdot s)} = \overline{\alpha(r) \cdot \alpha(s)}$, denn $\overline{\alpha(r + s)} = \overline{r + s} = \overline{\alpha(s)} = \overline{\alpha(r) + \alpha(s)}$ und $\overline{\alpha(r \cdot s)} = \overline{r \cdot s} = \overline{r} \cdot \overline{s} = \overline{\alpha(r)} \cdot \overline{\alpha(s)} = \overline{\alpha(r) \cdot \alpha(s)}$. Diese Formeln gestatten eine Überprüfung von Additions- und Multiplikationsaufgaben, indem man $\alpha(r \cdot s)$ und $\alpha(r) \cdot \alpha(s)$ vergleicht. Diese müssen kongruent modulo n sein. Da X eine endliche Menge

ist, sind diese Kongruenzen leicht zu überprüfen. Wenn der vermeintliche Wert des Produktes $r \cdot s$ unter α nicht kongruent zu $\alpha(r) \cdot \alpha(s)$ ist (letzteres Produkt ist leichter zu berechnen, evtl. aufgrund einer expliziten Multiplikationstabelle auf X), so ist bei der Berechnung von $r \cdot s$ ein Fehler aufgetreten. Analoges gilt für Summen.

(4) Die Abbildung $\beta : \mathbb{N} \longrightarrow \mathbb{Z}$ sei die sogenannte Quersumme (der Dezimaldarstellung), d.h. $\beta(a_r \cdot 10^r + a_{r-1}10^{r-1} + \ldots + a_1 \cdot 10 + a_0) := a_0 + a_1 + \ldots + a_{r-1} + a_r$. Dann ist $10^i \equiv 1 \mod 9$, weil $10 \equiv 1 \mod 9$, und damit $a_i \cdot 10^i \equiv a_i \mod 9$ und $a_r \cdot 10^r + \ldots + a_0 \equiv a_r + \ldots + a_0 \mod 9$. Also ist $\overline{\beta(r)} = \overline{r}$ für alle $r \in \mathbb{N}$. Sei α die iterierte Quersummenbildung $\alpha(r) = \beta \ldots\ldots \beta(r)$, so oft iteriert, bis eine einstellige Zahl herauskommt. Dann gilt $\overline{\alpha(r)} = \overline{\beta \ldots \beta(r)} = \ldots = \overline{\beta(r)} = \overline{r}$. Außerdem hat α das Bild $\{0, 1, 2, \ldots, 9\} = X$. In X sind 2 Zahlen a und b genau dann kongruent modulo 9, wenn sie gleich sind oder 0 und 9 sind. Die *Neunerprobe* für die Multiplikation natürlicher Zahlen ergibt sich damit: die iterierte Quersumme des Produkts $r \cdot s$ stimmt mit der Quersumme des Produkts der iterierten Quersummen der einzelnen Faktoren überein, es sei denn, daß sich Resultate 0 und 9 ergeben.

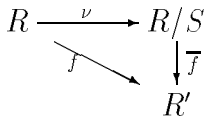
(5) Die Abbildung $\beta : \mathbb{Z} \longrightarrow \mathbb{Z}$ sei die sogenannte alternierende Quersumme, d.h. $\beta(a_r \cdot 10^r + \ldots + a_0) = (-1)^r a_r + (-1)^{r-1} a_{r-1} + \ldots + a_0$ auf $\mathbb{N}$ und $\beta(-r) := -\beta(r)$. Wegen $-10 \equiv 1 \mod 11$ ergibt sich wie zuvor $\beta(r) \equiv r \mod 11$. Sei α die iterierte alternierende Quersumme (stationär unter weiterer Quersummenbildung). Dann ist $\overline{\alpha(r)} = \overline{r}$ für alle $r \in \mathbb{N}$ und die Bildmenge von α ist $X = \{-9, -8, -7 \ldots, 0, 1, 2, \ldots, 9\}$. Wieder gilt eine entsprechende *Elferprobe* für Summen und Produkte: $\alpha(r \cdot s) \equiv \alpha(\alpha(r) \cdot \alpha(s)) \mod 11$.

(6) Schneidet man bei der Binärdarstellung einer natürlichen Zahl alle vorderen Stellen, bis auf die letzten 8 Stellen ab: $\alpha(a_r \cdot 2^r + \ldots + a_1 \cdot 2 + a_0) = a_7 \cdot 2^7 + \ldots + a_1 \cdot 2 + a_0$ mit $a_i \in \{0, 1\}$, so gilt wieder $\alpha(2^8) \equiv 0 \mod 2^8$, also $\overline{\alpha(r)} = \overline{r}$ in $\mathbb{Z}/(256)$.

Die Bildmenge von α ist $X = \{0, \ldots, 255\}$. Damit ist X sogar ein vollständiges Repräsentantensystem für $\mathbb{Z}/(256)$ und es gilt $\alpha(\alpha(r) \cdot \alpha(s)) = \alpha(r \cdot s)$, d.h. den Repräsentanten von $\overline{r} \cdot \overline{s}$ in X findet man durch Bestimmung des Repräsentanten in X von $\overline{r \cdot s}$. Diese besonders einfache Bildung der Restklassen und Repräsentanten ist die Grundlage für die Rechenoperationen in CPUs z.B. in 8 Bit-Registern. Addition und Multiplikation kann man wie bei natürlichen Zahlen durchführen und dann die höherwertigen Stellen (die Überträge) fortlassen. Dann erhält man die Rechenregeln eines Ringes, z.B. $\mathbb{Z}/(256)$.

Definition 6.5. Ein *Körper* ist ein kommutativer Ring, bei dem die von 0 verschiedenen Elemente bei der Multiplikation eine Gruppe bilden.

Bemerkung 6.6. Sei R ein unitärer Ring. Eine *Kongruenzrelation* (R, R, S) (mit $S \subset R \times R$) auf R ist eine Äquivalenzrelation auf R, so daß S ein Unterring von $R \times R$ ist, d.h. sowohl eine Untergruppe von $(R \times R, +)$ als auch ein Untermonoid von $(R \times R, \cdot)$. Dann bilden die Äquivalenzklassen R/S wieder einen unitären Ring und $\nu : R \longrightarrow R/S$ ist ein Ringhomomorphismus. Weiter gilt der Faktorisierungssatz für unitäre Ringe: eine eindeutige Faktorisierung $\overline{f}$ existiert mit



falls für alle $(r, r') \in S$ gilt $f(r) = f(r')$.
Ähnlich wie wir bei Gruppen Kongruenzrelationen durch normale Untergruppen $H \subset G$ beschrieben haben, können wir im Falle von unitären Ringen Kongruenzrelationen durch zweiseitige Ideale $I \subset R$ beschreiben. Dabei heißt eine Teilmenge $I \subset R$ ein zweiseitiges Ideal, wenn I eine Untergruppe von $(R, +)$ ist und für alle $r \in R$ und $i \in I$ gilt $ri, ir \in R$. Aus einem zweiseitigen Ideal $I \subset R$ gewinnt man eine Kongruenzrelation durch $S := \{(r, r') \in R | r - r' \in I\}$ und umgekehrt erhält man aus

einer Kongruenzrelation S auf R ein zweiseitiges Ideal durch $I := \{r - r' | (r, r') \in S$. Man schreibt dann auch $R/S =: R/I$. Die Elemente in R/I sind von der Form $r + I = \{r + i | i \in I$. Die Addition und Multiplikation auf R/I ist definiert durch $(r + I) + (r' + I) := (r + r') + I$ und $(r + I) \cdot (r' + I) := r \cdot r' + I$. Das gilt wegen $\overline{r} + \overline{r'} = \overline{r + r'}$ und $\overline{r} \cdot \overline{r'} = \overline{r \cdot r'}$.

Satz 6.7. *Für $n \in \mathbb{N}_0$ ist $\mathbb{Z}/(n)$ genau dann ein Körper, wenn n eine Primzahl ist.*

BEWEIS. Sei $p = n$ eine Primzahl. Die Elemente von $\mathbb{Z}/(p)$ sind $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$. Sei $0 < k < p$. Dann gibt es $a, b \in \mathbb{Z}$ mit $ak + bp = 1$, weil k und p teilerfremd sind. Damit ist $\overline{a} \cdot \overline{k} = \overline{ak} + \overline{b} \cdot \overline{p} = \overline{ak + bp} = \overline{1}$, denn $\overline{p} = \overline{0}$ in $\mathbb{Z}/(p)$, also ist $\overline{a}$ invers zu $\overline{k}$ und damit $\mathbb{Z}/(p)$ ein Körper.
Sei jetzt n keine Primzahl. Ist $n = 0$, so ist $\overline{2} \neq \bar{0}$. Wäre $\overline{2}$ invertierbar, etwa $\overline{1} = \overline{2} \cdot \overline{a}$, so wäre $1 \equiv 2a \mod 0$, also $2a = 1$ in $\mathbb{Z}$. Das ist aber nicht möglich. Ist $n = 1$, so hat $\mathbb{Z}/(1)$ genau ein Element. Aber $\mathbb{Z}/(1) \forall \{\overline{0}\} = \emptyset$ kann keine Gruppe sein. Ist schließlich $n > 1$, so muß n ein Produkt sein: $n = ab$, mit $1 < a < n$, sonst wäre es eine Primzahl. Dann ist $\overline{0} = \overline{n} = \overline{a} \cdot \overline{b}$, aber $\overline{a} \neq \overline{0}$ und $\overline{b} \neq 0$. Wäre $\overline{c} \cdot \overline{a} = \overline{1}$, so wäre $\overline{0} = \overline{c} \cdot \overline{0} = \overline{c} \cdot \overline{a} \cdot \overline{b} = \overline{1} \cdot \overline{b} = \overline{b}$ im Widerspruch zu $\overline{b} \neq 0$. □

Beispiele 6.8. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper, jedoch nicht $\mathbb{N}$ und $\mathbb{Z}$.

Bemerkung 6.9. Sei R ein unitärer Ring und X eine Menge. Dann ist $\mathrm{Abb}(X, R) = \{\alpha : X \longrightarrow R | \alpha$ Abbildung$\}$ ein Ring mit den Operationen

$$(\alpha + \beta)(x) := \alpha(x) + \beta(x), \qquad (\alpha \cdot \beta)(x) := \alpha(x) \cdot \beta(x).$$

Es übertragen sich die algebraischen Eigenschaften von R auf $R^X = \mathrm{Abb}(X, R)$. So ist z.B. die Eins in R^X gegeben durch $\alpha(x) = 1$ für alle $x \in X$. Ist R ein Körper, so ist R^X kein Körper, denn $\alpha \neq 0$ bedeutet nicht, daß $\alpha(x) \neq 0$ für alle $x \in X$(dann könnte man $\alpha^{-1}(x) = \alpha(x)^{-1}$ definieren), sondern nur, daß es mindestens ein $x \in X$ gibt mit $\alpha(x) \neq 0$. Wenn dann aber für

ein weiteres $y \in X$ gilt $\alpha(y) = 0$, dann läßt sich α^{-1} an der Stelle y nicht sinnvoll definieren.

Definition 6.10. Sei $\mathbb{K}$ der Körper $\mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$. Die Menge $\mathbb{K}[x] := \{\alpha : \mathbb{K} \longrightarrow \mathbb{K} | \exists a_0, \ldots, a_n \in \mathbb{K} \forall b \in \mathbb{K}[\alpha(b) = a_n b^n + \ldots + a_1 b + a_0\}]$ ist ein Unterring von $\mathbb{K}$ und heißt *Ring der Polynom(-funktionen)* auf $\mathbb{K}$. Wir schreiben $\sum_{i=0}^{n} a_i x^i = a_n x^n + \ldots + a_1 x + a_0 := \alpha$, wenn $\alpha(b) = a_n b^n + \ldots + a_1 b + a = 0$ für alle $b \in \mathbb{K}$. Die Addition ist gegeben durch $\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$, die Multiplikation durch $\sum_{i=0}^{m} a_i x^i \cdot \sum_{j=0}^{n} b_j x^j = \sum_{k=0}^{m+n} \sum_{i=0}^{k} a_i b_{k-i} x^k$, wie man leicht nachrechnet.

Bemerkung 6.11. Außer den genannten Körpern $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ und $\mathbb{Z}/(p)$ (p Primzahl) gibt es noch viele weitere. Insbesondere gibt es einen endlichen Körper mit n Elementen genau dann, wenn n von der Form p^r mit einer Primzahl p ist. Die endlichen Körper mit p^r Elementen heißen auch *Galois-Felder* $GF(p^r)$. Sie werden insbesondere in der Codierungstheorie verwendet.

7. Boolesche Ringe und Algebren

Auch in der Potenzmenge einer Menge haben wir zwei Verknüpfungen betrachtet, den Durchschnitt $\cap$ und die Vereinigung $\cup$. Sie erfüllen etwas andere Gesetze, als wir sie für Ringe und Körper kennengelernt haben. Diese Gesetze sind jedoch besonders wichtig, weil man sie nicht nur in Potenzmengen findet, sondern auch bei Ausdrücken mit logischen Verknüpfungszeichen.

Definition 7.1. Sei $(A, \cup, \cap, ')$ ein Quadrupel mit einer Menge A, binären Operationen $\cup : A \times A \longrightarrow A$ und $\cap : A \times A \longrightarrow A$ und einer 1-stelligen Operation $' : A \longrightarrow A$. Das Quadrupel $(A, \cup, \cap, ')$ heißt eine *Boolesche Algebra*, wenn für alle $a, b, c \in A$ gelten:

(1) $(a \cup b) \cup c = a \cup (b \cup c)$, $\qquad (a \cap b) \cap c = a \cap (b \cap c)$,
(2) $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$,
$\quad a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$,
(3) $a \cup b = b \cup a$, $\qquad a \cap b = b \cap a$,

(4) es gibt ein Element $0 \in A$, so daß für alle $a \in A$ gilt $0 \cup a = a$,
(5) es gibt ein Element $1 \in A$, so daß für alle $a \in A$ gilt $1 \cap a = a$,
(6) $a \cup a' = 1, \qquad a \cap a' = 0.$

Beispiele 7.2. (1) $\mathcal{P}(A)$, die Potenzmenge einer Menge A, zusammen mit der gewöhnlichen Vereinigung $\cup$, dem gewöhnlichen Durchschnitt $\cap$ und der Komplementbildung $B' := A \setminus B$ ist eine Boolesche Algebra.
(2) $\{0,1\} = B$ mit $a \cup b = \max(a,b)$ und $a \cap b = \min(a,b)$ ist eine Boolesche Algebra.
(3) $\mathcal{P}(A)$ mit $B \cup C$ = Durchschnitt (!) von B und C, $B \cap C$ = Vereinigung von B und C und $B' = A \setminus B$ ist eine Boolesche Algebra.

Satz 7.3. *Für eine Boolesche Algebra* $(A, \cup, \cap, ')$ *und Elemente* $a, b \in A$ *gelten*

(1) *das Nullelement* 0 *und das Einselement* 1 *sind eindeutig bestimmt,*
(2) $a \cap b = 0 \wedge a \cup b = 1 \Longrightarrow a' = b$,
(3) $a'' = a$,
(4) $0' = 1,\ 1' = 0$,
(5) $a \cup a = a = a \cap a$,
(6) $a \cup 1 = 1, a \cap 0 = 0$,
(7) $a \cup (a \cap b) = a, \qquad a \cap (a \cup b) = a$,
(8) $(a \cup b)' = a' \cap b', (a \cap b)' = a' \cup b'$.

Beweis. (1) $(A, \cup, 0)$ und $(A, \cap, 1)$ sind Monoide.
(2) $a' = a' \cup 0 = a' \cup (a \cap b) = (a' \cup a) \cap (a' \cup b) = 1 \cap (a' \cup b) = a' \cup b$. Vertauscht man die Rollen von a' und b, so erhält man $b = a' \cup b$, also $a' = b$.
(3) $a' \cup a = 1$ und $a' \cap a = 0$ impliziert nach (2) $a'' = a$.
(4) Wegen $1 \cap 0 = 0$ und $1 \cup 0 = 1$ und (2) folgt $0' = 1$. Aus (3) folgt $0 = 0'' = 1'$.

(5) $a \cup a = (a \cup a) \cap 1 = (a \cup a) \cap (a \cup a') = a \cup (a \cap a') = a \cup 0 = a$. Weiter ist $a \cap a = (a \cap a) \cup 0 = (a \cap a) \cup (a \cap a') = a \cap (a \cup a') = a \cap 1 = a$.
(6) $a \cup 1 = a \cup a \cup a' = a \cup a' = 1$ und $a \cap 0 = a \cap a \cap a' = a \cap a' = 0$.
(7) $a \cup (a \cap b) = (a \cup a) \cap (a \cup b) = a \cap (a \cup b)$. Wir weisen jetzt $a \cup (a \cap b) = a''$ nach. Es ist $a \cup (a \cap b) \cup a' = 1 \cup (a \cap b) = 1$ und $(a \cup (a \cap b)) \cap a' = (a \cap (a \cup b)) \cap a' = 0 \cap (a \cup b) = 0$, also ist nach (2) und (3) $a \cup (a \cap b) = a'' = a$.
(8) Es ist $(a' \cap b') \cup a \cup b = (a' \cup a \cup b) \cap (b' \cup a \cup b) = (1 \cup b) \cap (1 \cup a) = 1 \cup 1 = 1$ und $a' \cap b' \cap (a \cup b) = (a' \cap b' \cap a) \cup (a' \cap b' \cap b) = (0 \cap b') \cup (0 \cap a') = 0 \cup 0 = 0$. Damit und mit (2) folgt $(a \cup b)' = a' \cap b'$. Weiter folgt $(a \cap b)' = (a'' \cap b'')' = (a' \cup b')'' = a' \cup b'$. □

Definition 7.4. Ein Ring R heißt ein *Boolescher Ring*, wenn gilt $\forall r \in R[r^2 = r]$.

Satz 7.5. *Sei R ein Boolescher Ring. Dann ist R kommutativ, und es gilt $\forall r \in R[r + r = 0]$.*

BEWEIS. Für $r, s \in R$ ist $r + s = (r + s)^2 = r^2 + rs + sr + s^2 = r + rs + sr + s \Longrightarrow rs + sr = 0$. Für $s = r$ folgt $r + r = r^2 + r^2 = 0$. Damit ist $r = -r$ und auch $rs = -rs$. Aus $rs + sr = 0$ folgt nun $rs = sr$. □

Satz 7.6. (1) *Sei $(A, \cup, \cap, ')$ eine Boolesche Algebra. Dann ist $(A, +, \cdot)$ ein Boolescher Ring mit*

$$\begin{aligned} r + s &:= (r \cap s') \cup (r' \cap s) \quad (= r \triangle s), \\ r \cdot s &:= r \cap s. \end{aligned}$$

(2) *Sei $(A, +, \cdot)$ ein Boolescher Ring. Dann ist $(A, \cup, \cap, ')$ eine Boolesche Algebra mit*

$$\begin{aligned} r \cup s &:= r + s + r \cdot s, \\ r \cap s &:= r \cdot s, \\ r' &:= 1 + r. \end{aligned}$$

BEWEIS. (1) 1. $(a + b) + c = (((a \cap b') \cup (a' \cap b)) \cap c') \cup (((a \cap b') \cup (a' \cap b))' \cap c) = (a \cap b' \cap c') \cup (a' \cap b \cap c') \cup ((a' \cup b) \cap (a \cup b') \cap c) =$ (durch

Auflösen des rechten Ausdrucks) $(a\cap b'\cap c')\cup(a'\cap b\cap c')\cup(a'\cap b'\cap c)\cup(a\cap b\cap c)$ und ebenso wegen der Symmetrie des Ausdrucks $a+(b+c)=(a\cap b'\cap c')\cup(a'\cap b\cap c')\cup(a'\cap b'\cap c)\cup(a\cap b\cap c)$.
2. $a+b=b+a$, weil Vereinigung und Durchschnitt kommutativ sind.
3. $a+0=(a\cap 0')\cup(a'\cap 0)=(a\cap 1)\cup 0=a$, also existiert ein neutrales Element.
4. $a+a=(a\cap a')\cup(a'\cap a)=0$, also existieren inverse Elemente.
5. $(A,\cdot)$ ist ein Monoid.
6. $(a+b)\cdot c=((a'\cap b)\cup(a\cap b'))\cap c=(a'\cap b\cap c)\cup(a\cap b'\cap c)=(a\cap c\cap(b'\cup c'))\cup((a'\cup c')\cap b\cap c)=(a\cap c\cap(b\cap c)')\cup((a\cap)'\cap b\cap c)=a\cdot c+b\cdot c$. Damit ist A ein Ring. Wegen $a\cap a=a=a\cdot a$ ist A ein Boolescher Ring.
(2) 1. $a\cup b=a+b+a\cdot b=b+a+b\cdot a=b\cup a$.
2. $(a\cup b)\cup c=(a+b+ab)+c+(a+b+ab)c=a+b+c+ab+ac+bc+abc=a+(b+c+bc)+a(b+c+bc)=a\cup(b\cup c)$.
3. $0\cup a=0+a+0a=a$.
4. $a\cup a'=a+a'+aa'=a+1+a+a+a=1$ und $a\cap a'=a(1+a)=a+a=0$.
5. $(A,\cap,1)$ ist trivialerweise ein kommutatives Monoid.
6. $a\cap(b\cup c)=a(b+c+bc)=ab+ac+abc=ab+ac+abac=(a\cap b)\cup(a\cap c)$ und $a\cup(b\cap c)=a+bc+abc=a+ab+ab+ac+bc+abc+ac+abc+abc=(a+b+ab)(a+c+ac)=(a\cup b)\cap(a\cup c)$. □

Bemerkung 7.7. Tatsächlich erhält man wechselseitig aus den Strukturen der Booleschen Algebra und des Booleschen Ringes und beim zweimaligen Übergang die alten Strukturen zurück. Es ist nämlich $a+b+ab=(((a\cap b')\cup(a'\cap b))\cap(a\cap b))\cup(((a\cap b')\cup(a'\cap b))'\cap a\cap b)=((1\cap(a\cup b)\cap(a'\cup b')\cap 1)\cap(a'\cup b'))\cup((1\cap(a\cup b)\cap(a'\cup b')\cap 1)'\cap a\cap b)=((a\cup b)\cap(a'\cup b'))\cup(((a'\cap b')\cup(a\cap b))\cap a\cap b)=(a'\cap b)\cup(a\cap b')\cup(a'\cap b'\cap a\cap b)\cup(a\cap b\cap a\cap b)=(a'\cap b)\cup(a\cap b')\cup(a\cap b)=(a'\cap b)\cup(a\cap(b'\cup b))=(a'\cap b)\cup a=(a'\cup a)\cap(a\cup b)=1\cap(a\cup b)=a\cup b$.
Weiter ist $(a\cap b')\cup(a'\cap b)=a(1+b)+(1+a)b+a(1+b)(1+a)b=a+ab+b+ab+ab+ab+ab+ab=a+b$. Schließlich ist

$1 + a = (1' \cap a) \cup (1 \cap a') = (0 \cap a) \cup a' = 0 \cup a' = a'$.

Bemerkung 7.8. Boolesche Algebren und Boolesche Ringe sind algebraische Strukturen. Es lassen sich Kongruenzrelationen und Restklassenstrukturen bilden. Der Faktorisierungssatz gilt. Jede Boolesche Algebra läßt sich als Restsklassenalgebra einer freien Booleschen Algebra darstellen, insbesondere durch Erzeugende und Relationen. Wenn A eine Boolesche Algebra ist, dann ist auch $\mathrm{Abb}(X, A) = A^X$ eine Boolesche Algebra mit komponentenweisen Operationen.

Man weiß viel über die Struktur von Booleschen Algebren. Besonders im endlichen Fall kann man diese Struktur vollständig beschreiben. Wir geben hier den entsprechenden Satz zur Information an, ohne allerdings den Beweis durchzuführen.

Satz 7.9. *Jede endliche Boolesche Algebra ist isomorph zur Booleschen Algebra auf der Potenzmenge $\mathcal{P}(M)$ einer endlichen Menge M. Sie ist außerdem isomorph zu einer Booleschen Algebra der Form B^n, wobei $B = \{0, 1\}$ die Struktur einer Booleschen Algebra wie in Beispiel 7.2 (2) trägt.*

Definition 7.10. Sei A eine Boolesche Algebra. Eine Abbildung $f \in \mathrm{Abb}(A^n, A)$ aus der Booleschen Algebra $\mathrm{Abb}(A^n, A)$ heißt *Boolesche Funktion* mit Werten in A. Wir schreiben $f = f(x_1, \ldots, x_n)$.
Die Booleschen Funktionen $x_i : A \times \ldots \times A \ni (a_1, \ldots, a_n) \mapsto a_i \in A$ heißen *Projektionen* (oder *Variable*), die Booleschen Funktionen $A \times \ldots \times A \ni (a_1, \ldots, a_n) \mapsto b \in A$ für festes $b \in A$ *konstante Abbildungen*. Da sie in der Booleschen Algebra $\mathrm{Abb}(A^n, A)$ liegen, kann man die kleinste von den Konstanten $b \in A$ und den Variablen $x_1, \ldots, x_n$ (mit $\cup$, $\cap$, $'$) erzeugte Boolesche Unteralgebra $A[x_1, \ldots, x_n] \subset \mathrm{Abb}(A^n, A)$ bilden. $A[x_1, \ldots, x_n]$ heißt Boolesche Algebra der *Polynomfunktionen*.

Bemerkung 7.11. Die freie Boolesche Algebra über den Erzeugenden $X_1, \ldots, X_n$ mit Konstanten A ist $A[X_1, \ldots, X_n]$, die

Algebra der formalen Ausdrücke, die mit Elementen $a \in A$, $X_1, \ldots, X_n, \cup, \cap$ und $'$ gebildet werden können modulo den Relationen für Boolesche Algebren, heißt Boolesche Algebra der *Polynome* über A. Die Abbildung $X_i \mapsto x_i$ induziert einen Homomorphismus von Booleschen Algebren

$$A[X_1, \ldots, X_n] \longrightarrow A[x_1, \ldots, x_n].$$

Man unterscheidet daher Polynome und Polynomfunktionen.

Satz 7.12. (1) *Zu jeder Booleschen Polynomfunktion*

$$f : A^n \longrightarrow A$$

gibt es genau eine disjunktive Normalform

$$f(x_1, \ldots, x_n) = \bigcup_{(i_1, \ldots, i_n)} a_{i_1, \ldots, i_n} \cap x_1^{i_1} \cap \ldots \cap x_n^{i_n}$$

mit $i_j \in \{1, -1\}$, *wobei* $x_i^1 = x_i$ *und* $x_i^{-1} = x_i'$ *sei.*

(2) *Zu jeder Booleschen Polynomfunktion* $f : A^n \longrightarrow A$ *gibt es genau eine* konjunktive Normalform

$$f(x_1, \ldots, x_n) = \bigcap_{(i_1, \ldots, i_n)} a_{i_1, \ldots, i_n} \cup x_1^{i_1} \cup \ldots \cup x_n^{i_n}$$

mit $i_j \in \{1, -1\}$.

Beweis. Wir beweisen lediglich Teil (1) des Satzes. Zunächst weisen wir die Existenz einer disjunktiven Normalform nach. Wenn eine Polynomfunktion f gegeben ist, so wenden wir eventuell mehrfach die Gleichungen von Satz 7.3 (2) an, um die Bildung des Komplements auf die einzelnen Konstanten oder Variablen zu ziehen. Dann verwenden wir das Distributivgesetz 7.1 (2) i), um den Durchschnitt $\cap$ nach innen auf die einzelnen Konstanten und Variablen zu ziehen. Wegen der Kommutativität und 7.3 (3) erhalten wir einen Ausdruck wie in der disjunktiven Normalform, jedoch ist es möglich, daß nicht alle Terme $a_{i_1, \ldots, i_n} \cap x_1^{i_1} \cap \ldots \cap x_n^{i_n}$ mit allen Variablen $x_1, \ldots, x_n$ auftreten. In diesem Falle bekommt man die fehlenden Variablen x_i, indem

man den entsprechenden Ausdruck mit $1 = x_i \cup x_i'$ schneidet und den obigen Prozeß wiederholt. Zuletzt fasse man Ausdrücke mit gleichen Komponenten $x_1^{i_1} \cap \ldots \cap x_n^{i_n}$ zusammen, indem man die zugehörigen Konstanten $a_{i_1,\ldots,i_n}$ und $b_{i_1,\ldots,i_n}$ in A vereinigt. Das ergibt die gewünschte Normalform.
Um die Eindeutigkeit der disjunktiven Normalform zu zeigen, wählen wir ein n-Tupel $(k_1, \ldots, k_n)$ und setzen wir in

$$f(x_1, \ldots, x_n) = \bigcup a_{i_1,\ldots,i_n} \cap x_1^{i_1} \cap \ldots \cap x_n^{i_n}$$

Argumente $I_1, \ldots, I_n$ ein mit

$$I_j = \begin{cases} 1, \text{ falls } k_j = 1, \\ 0, \text{ falls } k_j = -1. \end{cases}$$

Dann verschwinden alle Terme der disjunktiven Normalform, bis auf den Term zum Index $(k_1, \ldots, k_n)$. Wir erhalten damit $f(I_1, \ldots, I_n) = a_{k_1,\ldots,k_n}$. Man kann also aus f allein die „Koeffizienten“ der disjunktiven Normalform erhalten. Diese ist damit eindeutig.
Hinweis zur Gewinnung der Koeffizienten $a_{i_1,\ldots,i_n}$ in den Normalformen aus der gegebenen Polynomfunktion. Es ist durch Einsetzen ersichtlich, daß für

$$I_j = \begin{cases} 1, \text{ falls } i_j = 1, \\ 0, \text{ falls } i_j = -1, \end{cases}$$

in der disjunktiven Normalform gilt $a_{i_1,\ldots,i_n} = f(I_1, \ldots, I_n)$. In der konjunktiven Normalform setze man

$$I_j = \begin{cases} 0, \text{ falls } i_j = 1, \\ 1, \text{ falls } i_j = -1, \end{cases}$$

ein und erhält $a_{i_1,\ldots,i_n} = f(I_1, \ldots, I_n)$. □

Beispiel 7.13. Die disjunktive Normalform von $(x_1 \cup x_2) \cap (x_1 \cap x_2')$ ist $1 \cap x_1 \cap x_2'$, weil $f(0,0) = f(0,1) = f(1,1) = 0$ und

$f(1,0) = 1$ ist. Tatsächlich ist

$$(x_1 \cup x_2) \cap (x_1 \cap x_2') = (x_1 \cap x_1 \cap x_2') \cup (x_2 \cap x_1 \cap x_2' = \\ (x_1 \cap x_2') \cup 0 = x_1 \cap x_2' = 1 \cap x_1 \cap x_2'.$$

Boolesche Polynome stellen eine besonders einfache Klasse von Booleschen Funktionen dar. In einem Spezialfall fallen diese beiden Begriffe jedoch sogar zusammen. Wir formulieren hier nur den entsprechenden Satz ohne Beweis.

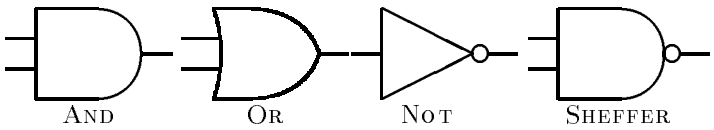
Satz 7.14. *Ist* $B = \{0,1\}$*, so ist jede Boolesche Funktion in* $\mathrm{Abb}(B^n, B)$ *ein Boolesches Polynom.*

Bemerkung 7.15. (über Gatter) Eine (technische Realisierung einer) Booleschen Funktion $f : B^n \longrightarrow B$ mit $B = \{0,1\}$ heißt ein Gatter.

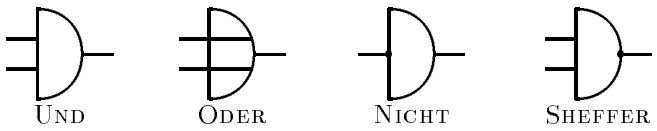
$f(x_1, \ldots, x_n) = x_1 \cap x_2 \cap \ldots \cap x_n$	heißt UND-Gatter,
$f(x_1, \ldots, x_n) = x_1 \cup x_2 \cup \ldots \cup x_n$	heißt ODER-Gatter,
$f : B \longrightarrow B$ mit $f(x) = x'$	heißt NICHT-Gatter oder Inverter,
$f(x_1, \ldots, x_n) = (x_1 \cap x_2 \cap \ldots \cap x_n)'$	heißt NAND-Gatter,
$f(x_1, \ldots, x_n) = (x_1 \cup x_2 \cup \ldots \cup x_n)'$	heißt NOR-Gatter,
$f(x_1, x_2) = (x_1 \cup x_2)' = x_1 \downarrow x_2$	heißt Pierce-Gatter,
$f(x_1, x_2) = (x_1 \cap x_2)' = x_1 \mid x_2$	heißt Sheffer-Gatter.

Die zugehörigen Gatter-Symbole sind:

US Norm:



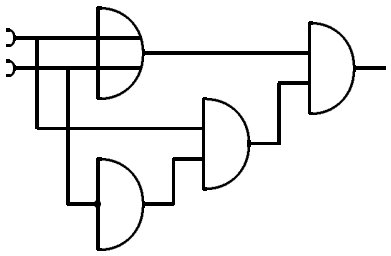
Deutsche Norm:



Eine Parallelschaltung von Eingängen von Gattern wird als doppelte Anwendung derselben Variablen angesehen, z.B. sind mit $(f(x_1, x_2), g(x_1, x_3))$ zwei Eingänge x_1 der beiden Gatter f und g parallel geschaltet.
Eine Serienschaltung von Gattern wird als Einsetzen einer Funktion in eine andere Funktion angesehen. So ist z.B.

$$(x_1 \cup x_2) \cap (x_1 \cap x_2')$$

realisierbar durch die folgende Zusammenschaltung von Gattern



Da jede Boolesche Funktion in $\mathrm{Abb}(B^n, B)$ eine Polynomfunktion ist, läßt sie sich durch Gatter darstellen. Die Sheffer-Operation stellt alle Booleschen Funktionen dar, denn sei $a \setminus b = (a \cap b)$. Dann gelten

$$\begin{aligned} x_1' &= (x_1 \cap x_1)' = x_1|x_1, \\ x_1 \cap x_2 &= ((x_1 \cap x_2)' \cup (x_1 \cap x_2)')' = (x_1|x_2)|(x_1|x_2), \\ x_1 \cup x_2 &= ((x_1 \cap x_1)' \cup (x_2 \cap x_2)')' = (x_1|x_1)|(x_2|x_2). \end{aligned}$$

Ebenso lassen sich alle Gatter in eindeutiger Weise mit Hilfe der disjunktiven bzw. konjunktiven Normalform darstellen.