ALGEBRA FÜR DIE INFORMATIK

Hans Opolka
TU Braunschweig
Institut für Analysis und Algebra
Pockelsstrasse 14
D - 38106 Braunschweig
e-mail: h.opolka@tu-bs.de

Inhaltsverzeichnis

Einleitung

Eine Aufgabe der Algebra besteht in der Untersuchung von *Rechenbereichen*. Rechenbereiche sind Mengen zusammen mit gewissen Vorschriften, sogenannten *Rechenvorschriften* oder *Rechenregeln*, die vorgeben, wie man aus vorgegebenen Elementen dieser Menge ein anderes Element dieser Menge bilden kann. Dabei werden diese Rechenvorschriften häufig durch konkrete Bedeutungen, die man den Elementen der zugrundeliegenden Menge, der sogenannten *Trägermenge*, eines Rechenbereichs geben kann, nahelegt.

Als Beispiel betrachten wir eine Menge mit 2 Elementen, etwa $X = \{0, 1\}$, die mit drei Rechenvorschriften, bezeichnet mit $'$, $\vee$ und $\wedge$, versehen ist; diese drei Rechenvorschriften seien mit Hilfe der folgenden Tabellen definiert:

	$'$
0	1
1	0

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

d.h. die Anwendung der Rechenregel $'$ auf 0 ergibt 1 und Anwendung von $'$ auf 1 ergibt 0; die Anwendung der Rechenregel $\vee$ auf $(0,0)$ ergibt 0, u.s.w.. Wir stellen fest, daß bei der Deutung des Elementes 0 als Wahrheitswert "falsch" und des Elementes 1 als Wahrheitswert "wahr" und bei Deutung der Rechenregeln $', \vee, \wedge$ durch "nicht", "oder" bzw. "und" die obigen Tabellen den bekannten Rechenoperationen der 2-wertigen Aussagenlogik entsprechen. Deshalb nennt man den Rechenbereich, der aus der Menge $X = \{0,1\}$ zusammen mit den Rechenregeln $', \vee, \wedge$ besteht, auch die *Algebra der Wahrheitswerte* und schreibt dafür gelegentlich $\mathbf{2} := (\{0,1\}, ', \vee, \wedge)$. Diese Algebra der Wahrheitswerte ist nur ein Beispiel einer ganzen Reihe von Rechenbereichen, die man *Boolesche Algebren* nennt und die in der Informatik von Bedeutung sind. Sie wurden nach dem englischen Logiker George Boole (1815-1864) benannt, der in einem grundlegenden Werk $[BL]$ gewisse Aspekte des Denkens unter formalen Gesichtspunkten untersucht hat. Ersetzt man die obige Rechenregel $\vee$ durch die Rechenregel $\dot{\vee}$, die in der Aussagenlogik dem "entweder oder" entspricht, also durch

$\dot{\vee}$	0	1
0	0	1
1	1	0

,

dann bildet die Menge $X = [0,1\}$ zusammen mit den Rechenoperatioen $\dot{\vee}$ und $\wedge$ den Rechenbereich, den man den (algebraischen) *Körper mit* 2 *Elementen* nennt und mit $\mathbb{F}_2$ bezeichnet; bei dieser Deutung entspricht $\dot{\vee}$ der Addition und $\wedge$ der Multiplikation in $\mathbb{F}_2$: $\mathbb{F}_2 = (\{0,1\}, \dot{\vee}, \wedge) = (\{0,1\}, +, \cdot)$.

Mit Hilfe dieses Körpers läßt sich ein endliches Modell für das folgende Axiomensystem angeben; vgl. $[KS]$, § 1:

Axiom A: Durch zwei verschiedene Punkte verläuft genau eine Gerade.

Axiom B: Zu einer gegebenen Gerade und zu einem gegebenen Punkt, der nicht auf dieser Gerade liegt, existiert genau eine Gerade, die durch diesen Punkt verläuft und die die gegebene Gerade nicht schneidet.

Axiom C: Es gibt drei Punkte, die nicht alle auf einer gemeinsamen Gerade liegen

Das endliche Modell, das dieses Axiomensystem realisiert, besteht aus vier Punkten A, B, C, D und aus den sechs Geraden AB, CD, AD, BC, AC, BD. Analytisch kann man es mit Hilfe des Körpers $\mathbb{F}_2$ wie folgt realisieren: Die vier Punkte A, B, C, D werden mit den vier Punkten der "endlichen Ebene" $\mathbb{F}_2 \times \mathbb{F}_2$ identifiziert:

$A = (0,0)$, $B = (0,1)$, $C = (1,0)$, $D = (1,1)$;

und die sechs Geraden mit den folgenden sechs linearen Gleichungen über $\mathbb{F}_2$:

AB: $1 \cdot X = 0$
CD: $1 \cdot X = 1$
AD: $1 \cdot X + 1 \cdot Y = 0$
BC: $1 \cdot X + 1 \cdot Y = 1$
AC: $1 \cdot Y = 0$
BD: $1 \cdot Y = 1$.

Der Körper $\mathbb{F}_2$ und auch andere Körper mit nur endlich vielen Elementen sind nicht nur für die Mathematik sondern auch für die Informatik, und hier insbesondere für die Codierungstheorie, von grundlegender Bedeutung.

In den nachfolgenden Abschnitten werden zunächst einzelne Rechenbereiche, die für die Informatik wichtig sind, durchgenommen und miteinander verglichen. Schließlich werden dann gemeinsame Merkmale von einigen dieser Rechenbereiche festgestellt und zum Anlaß genommen, einen "übergeordneten" Rechenbereich zu konstruieren, den man auch die *zugehörige Termalgebra* nennt.

Diese Aufzeichnungen erheben keinerlei Anspruch auf Originalität. Sie sollen grundlegende algebraische Begriffe, die für die Informatik von Bedeutung sind, vermitteln. Das Schwergewicht liegt dabei auf theoretischen Aspekten der Algebra. Für algorithmische Aspekte verweisen wir auf die entsprechenden Ausführungen in [KN]; außerdem wird zu algorithmischen Einzelaspekten weitere Literatur im Text angegeben. Teilweise geben die vorliegenden Aufzeichnungen Inhalte von Lehrveranstaltungen wieder, die ich an der TU Braunschweig durchgeführt habe. Den wissenschaftlichen Mitarbeitern F. Henningsen, G. Schwant, T. Riedel und der wissenschaftlichen Mitarbeiterin S. Rathjen, die dabei jeweils die entsprechenden Übungen durchgeführt haben, danke ich bei dieser Gelegenheit für ihre Mitarbeit und für nützliche Hinweise. Fehler und andere Unzulänglichkeiten können nicht ausgeschlossen werden und gehen selbstverständlich gänzlich zu meinen Lasten. Am Ende eines jeden Abschnittes wird die jeweils benutzte Literatur oder auch ergänzende und weiterführende Literatur angegeben.

Literatur zur Einleitung: [BB], [BL], [KN], [KS], [LS]

§ 1. **Mengen, Relationen und Abbildungen**

In diesem Abschnitt werden grundlegende Begriffe über Mengen, Relationen und Abbildungen besprochen. Dabei folgen wir weitgehend entsprechenden Darstellungen in [BB], [HM] und [LS].

Mengen werden beschrieben, indem ihre Elemente aufgezählt werden, etwa $M = \{a, b, c, ...\}$, oder indem ihre Elemente durch eine definierende Eigenschaft charkterisiert werden, etwa $M = \{x : x \text{ hat die Eigenschaft } E\}$. Dabei versuchen wir, Mengenbildungen, die zu Paradoxien oder Widersprüchen führen können, zu vermeiden; vgl. dazu die Bemerkungen weiter unten. Wir benutzen Standardbezeichnungen aus der sogenannten naiven Mengenlehre, vgl. z.B. [HM]:

$x \in A$: x ist Element von A; $x \notin A$: x ist nicht Element von A; $A \subset B$: A ist Teilmenge von B, d.h. wenn $x \in A$, dann ist $x \in B$; $A = B$: $A \subset B$ und $B \subset A$; $A \cup B := \{x : x \in A \text{ oder } x \in B\}$ ist die Vereinigung von A und B; $A \cap B := \{x : x \in A \text{ und } x \in B\}$ ist der Durchschnitt von A und B; für $A \subset B$ ist $B - A := \{x : x \in B \text{ und } x \notin A\}$ das Komplement von A in B; $A' := \{x : x \in U \text{ und } x \notin A\}$, wobei U eine A enthaltende Menge ist, ist das absolute Komplement von A; $A \times B := \{(a, b) : a \in A, b \in B\}$ ist das cartesische Produkt von A und B, bestehend aus allen geordneten Paaren $(a, b) := \{\{a\}, \{a, b\}\}$; $A \dot{\cup} B := (A \times \{0\}) \cup (B \times \{1\})$, wobei die Symbole 0 und 1 verschiedene Objekte bezeichnen, ist die disjunkte Vereinigung von A und B; $\emptyset$, die leere Menge, ist Teilmenge jeder Menge, also eindeutig bestimmt; für eine Menge A ist $\mathcal{P}(A)$ die Potenzmenge von A, d.h. die Menge aller Teilmengen von A.

Weitere Bezeichnungen sind:
$\mathbb{N} = \{1, 2, 3, ...\}$ = Menge aller natürlichen Zahlen
$\mathbb{N}_0 = \{0\} \cup \mathbb{N}$; $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$ = Menge aller ganzen Zahlen
$\mathbb{Q} = \{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}\}$ = Menge aller rationalen Zahlen
$\mathbb{R} = \{\sum_{n=0}^{\infty} a_n \cdot 10^{-n} : a_n \in \mathbb{Z}\}$ = Menge aller reellen Zahlen
$\mathbb{C} = \{a + b\sqrt{-1} : a, b \in \mathbb{R}\}$ = Menge aller komplexen Zahlen

Um Paradoxien und widersprüchliche Begriffsbildungen, die sich aus einem naiven Verständnis von Mengen ergeben, wie z.B. "die Menge aller Mengen" oder "die Menge aller Mengen, die sich nicht selbst als Element enthalten", zu vermeiden, hat es verschiedene Vorschläge und Theorien gegeben; zu dieser Thematik vgl. man die entsprechenden Texte und Ausführungen in [LS], pp. 33/34 oder in [LP], Chapter 2 sowie in der dort angegebenen Literatur. Für manche Begriffsbildungen, insbesondere im Zusammenhang mit Kategorien in §12 und mit algebraischen Systemen in §15, erweist es sich als günstig, den von A. Grothendieck stammenden Begriff des Universums zu benutzen; man vgl.dazu [$SGA4$], Exposé 1, Appendice: Univers (par N. Bourbaki), oder auch [SC], Teil I, 3, S. 15 und 16.

Definition Ein *Universum* ist eine Menge $\mathcal{U}$, die folgende Eigenschaften besitzt:
(1) Wenn $A \in \mathcal{U}$, dann ist $A \subset \mathcal{U}$
(2) Wenn $A, B \in \mathcal{U}$, dann ist $\{A, B\} \in \mathcal{U}$
(3) Wenn $A \in \mathcal{U}$, dann ist $\mathcal{P}(A) \in \mathcal{U}$
(4) Ist $J \in \mathcal{U}$ und existiert zu jedem $j \in J$ genau ein $U_j \in \mathcal{U}$, dann ist die Vereinigung $\cup_{j \in J} U_j \in \mathcal{U}$

Aus den in dieser Definition geforderten Eigenschaften von $\mathcal{U}$ ergibt sich, daß bei der Anwendung der oben genannten üblichen Operationen der Mengenlehre auf Elemente von $\mathcal{U}$ wiederum nur Elemente von $\mathcal{U}$ entstehen. Wir legen deshalb allen Betrachtungen ein fest gewähltes Universum zugrunde, d.h. wir fordern, daß alle betrachteten Mengen einem fest gewählten Universum angehören.

Wir besprechen zunächst grundlegende Sachverhalte und Resultate über Mengen, Relationen und Abbildungen und folgen dabei entsprechenden Darstellungen in $[BB]$, $[HM]$ und $[LS]$.

Definition Eine *Relation von einer Menge A zu einer Menge B* ist eine Teilmenge ρ von $A \times B$. Für $(a, b) \in \rho$ schreibt man auch $a\rho b$. Eine *Relation auf einer Menge A* ist eine Teilmenge von $A \times A$.

Beispiele (1) Die Gleichheitsrelation $=$ auf einer Menge A
(2) Die Relation $\leqq$ auf $\mathbb{R}$
(3) Der Einheitskreis $\subset \mathbb{R}^2$
(4) Verwandtschaft einer bestimmten Art

Definition Die zu einer Relation $\rho \subset A \times B$ gehörige *Relationsmatrix* ist die Matrix mit den Koeffizienten $r^{\rho}_{a,b}$, $(a, b) \in A \times B$, wobei $r^{\rho}_{a,b} = 1$, falls $a\rho b$, und $r^{\rho}_{a,b} = 0$ sonst.

Der $\rho \subset A \times B$ entsprechende *Relationsgraph* ist der gerichtete Graph, bei dem A und B durch disjunkte Mengen von Ecken dargestellt werden, und mit einer Kante von $a \in A$ nach $b \in B$ genau dann, wenn $a\rho b$ gilt.

Die folgende Definition ermöglicht das Rechnen mit Relationen.

Definition Für Relationen $\rho \subset A \times B$ und $\sigma \subset B \times C$ ist die *Verknüpfung von ρ und σ* die Relation $\rho\sigma \subset A \times C$, wobei $a\rho\sigma c$ per Definition genau dann gilt, wenn ein $b \in B$ existiert, so daß $a\rho b$ und $b\sigma c$ erfüllt sind. Die zu einer Relation $\rho \subset A \times B$ *inverse Relation* $\widetilde{\rho} \subset B \times A$ ist definiert durch die Eigenschaft, daß $b\widetilde{\rho}a$ genau dann gilt, wenn $a\rho b$ erfüllt ist.

Es gilt: $\widetilde{\rho\sigma} = \widetilde{\sigma}\widetilde{\rho}$.

Beweis $c\widetilde{\rho\sigma}a \Leftrightarrow a\rho\sigma c \Leftrightarrow$ Es existiert ein $b \in B$ mit $a\rho b$ und $b\sigma c \Leftrightarrow$ Es existiert ein $b \in B$ mit $c\widetilde{\sigma}b$ und $b\widetilde{\rho}a \Leftrightarrow c\widetilde{\sigma}\widetilde{\rho}a$.

Definition Eine *Abbildung von einer Menge A in eine Menge B - oder von A nach B* - ist eine Relation $f \subset A \times B$ mit den folgenden Eigenschaften:
(1) Für alle $a \in A$ existiert ein $b \in B$ mit $(a, b) \in f$
(2) Wenn afb und afb', dann gilt $b = b'$; d.h. die Relation f ist *rechtseindeutig.*

Aufgrund dieser Definition faßt man eine Abbildung f von A in B als eine Zuordnung auf, die jedem Element $a \in A$ genau ein Element $f(a) \in B$ zuordnet und deutet diesen Sachverhalt durch die Schreibweise $f : A \to B$, $a \longmapsto f(a)$, an. Zwei Abbildungen $f : A \xrightarrow{f} B$ und $g : B \xrightarrow{g} C$ lassen sich - als Relationen - zu einer Abbildung von A nach C verknüpfen. Aus naheliegenden Gründen schreiben wir für diese Verknüpfung $g \circ f$, also

$g \circ f := fg$, wobei $(g \circ f)(a) = g(f(a))$ für alle $a \in A$,

und nennen $g \circ f$ die *Verknüpfung* oder die *Komposition* von f mit g.

Definition Eine Abbildung $f : A \to B$ heißt *injektiv*, wenn für je zwei Elemente $a, a' \in A$ gilt: Wenn $f(a) = f(a')$, dann ist $a = a'$. Sie heißt *surjektiv*, wenn zu jedem $b \in B$ ein $a \in A$ existiert, so daß $b = f(a)$ gilt. Sie heißt *bijektiv*, wenn sie injektiv und surjektiv ist. Wir nennen

$$Bild(f) := \mathrm{Im}(f) := f(A) := \{f(a) : a \in A\}$$

auch das *Bild* der Abbildung f; und für $C \subset B$ heißt

$$f^{-1}(C) := \{a \in A : f(a) \in C\}$$

das *Urbild* von C unter f.

Eine Abbildung $f : A \to B$ ist also genau dann surjektiv, wenn $f(A) = B$ gilt; und genau dann injektiv, wenn für jedes $b \in B$ das Urbild $f^{-1}(\{b\})$ aus höchstens einem Element besteht.

Definition Die *identische Abbildung* oder *Identität* auf einer Menge A ist die Abbildung

$id = id_A : A \to A$, wobei $id_A(x) = x$ für alle $x \in A$.

Eine Abbildung $f : A \to B$ heißt *linksinvertierbar,* wenn eine linksinverse Abbildung $g : B \to A$ von f existiert, d.h. es gilt $g \circ f = id_A$; sie heißt *rechtsinvertierbar*, wenn eine rechtsinverse Abbildung $h : B \to A$ existiert, d.h. es gilt $f \circ h = id_B$; sie heißt *invertierbar*, wenn sie links- und rechtsinvertierbar ist.

Wenn $f : A \to B$ eine Abbildung ist, die eine linksinverse Abbildung $g : B \to A$ und eine rechtsinverse Abbildung $h : B \to A$ besitzt, dann gilt $g = h$; denn $g = g \circ id_B = g \circ (f \circ h) = (g \circ f) \circ h = id_A \circ h = h$. Außerdem gilt

(1.1) **Satz** *Sei $f : A \to B$ eine Abbildung. Dann gilt: f ist linksinvertierbar genau dann, wenn f injektiv ist; und f ist rechtsinvertierbar genau dann, wenn f surjektiv ist.*

Beweis: Sei $g : B \to A$ eine zu f linksinverse Abbildung und sei $f(a) = f(b)$ Dann gilt $g(f(a)) = a = g(f(b)) = b$. Also ist f injektiv. Sei f injektiv und sei $g : B \to A$ definiert durch $g(b) := a$, falls ein $a \in A$ mit $b = f(a)$ existiert, und sei $g(b) := \alpha$, wobei α irgendein Element aus A ist, andernfalls. g ist wohldefiniert, weil a wegen der Injektivität von f durch b eindeutig bestimmt ist. Nach Definition von g gilt $(g \circ f)(a) = g(f(a)) = a$. Es folgt $g \circ f = id_A$.

Sei $h : B \to A$ eine zu f rechtsinverse Abbildung und sei $b \in B$. Dann gilt $b = f(h(b))$, also $b \in Bild(f)$. Somit ist f surjektiv. Sei f surjektiv. Zu jedem $b \in B$ sei $a = a_b$ ein Element aus A mit $f(a) = b$. Definiere $h(b) := a_b$. Dann ist $h : B \to A$ eine zu f rechtsinverse Abbildung.

(1.2) **Folgerung** *Eine Abbildung ist genau dann bijektiv, wenn sie invertierbar ist.*

Definition Eine Relation $\rho \subset A \times A$ heißt
reflexiv: $\Leftrightarrow$ Für alle $a \in A$ gilt $a\rho a$
symmetrisch: $\Leftrightarrow$ Für alle $a, b \in A$ gilt: Aus $a\rho b$ folgt $b\rho a$
antisymmetrisch: $\Leftrightarrow$ Für alle $a, b \in A$ gilt: Aus $a\rho b$ und $b\rho a$ folgt $a = b$
transitiv: $\Leftrightarrow$ Für alle $a, b, c \in A$ gilt: Aus $a\rho b$ und $b\rho c$ folgt $a\rho c$

Definition Eine Relation $\rho \subset A \times A$ heißt *Aequivalenzrelation* auf A, wenn sie reflexiv, symmetrisch und transitiv ist.

Sei $\rho = \mathcal{E}$ eine Aequivalenzrelation auf A und für jedes $a \in A$ sei

$(a) := \{b \in A : a\mathcal{E}b\}$

die sogenannte *Aequivalenzklasse* von a. Sei

$A \setminus \mathcal{E} := \{(a) : a \in A\}$

die Menge aller Aequivalenzklassen oder die sogenannte Quotientenmenge von A modulo $\mathcal{E}$.

Es gilt: $(a) = (b) \Leftrightarrow a\mathcal{E}b$. Beweis: Aus der Gleichheit $(a) = (b)$ folgt unmittelbar $a\mathcal{E}b$. Gelte umgekehrt $a\mathcal{E}b$ und sei $c \in (a)$. Dann gilt $a\mathcal{E}c$, und wegen der Symmetrie der Relation $\mathcal{E}$ auch $c\mathcal{E}a$. Also gelten $c\mathcal{E}a$ und $a\mathcal{E}b$. Somit gilt wegen der Transitivität der Relation $\mathcal{E}$ auch $c\mathcal{E}b$, d.h. $c \in (b)$.

Beispiele (1) Die Gleichheitsrelation ist eine Aequivalenzrelation auf jeder Menge.
(2) Die Relation $A \times A$ ist eine Aequivalenzrelation auf jeder Menge A.
(3) Sei $A = L$ die Menge aller Geraden in der Ebene. Sei $\mathcal{E} \subset L \times L$ die Menge aller geordneten Paare (l, m) von Geraden l, m, die parallel sind. $\mathcal{E}$ ist eine Aequivalenzrelation auf L.
(4) Sei $A := \mathbb{N}_0 \times \mathbb{N}_0$ und sei $\mathcal{E} := \{((a, b), (c, d)) \in A \times A : a+d = b+c\}$. $\mathcal{E}$ ist eine Aequivalenzrelation auf A, und die Abbildung $A \setminus \mathcal{E} \to \mathbb{Z}$, $((a, b)) \longmapsto a - b$, ist bijektiv.
(5) Sei $m \in \mathbb{Z} \setminus \{0\}$ und $\mathcal{E} := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : m \text{ teilt } a - b\}$. $\mathcal{E}$ ist eine Aequivalenzrelation auf $\mathbb{Z}$.
(6) Sei $A := \mathbb{Z} \times (\mathbb{Z} - \{0\})$ und sei $\mathcal{E} := \{((a, b), (c, d)) \in A \times A : ad = bc\}$. $\mathcal{E}$ ist eine Aequivalenzrelation auf A, und die Abbildung $A \setminus \mathcal{E} \to \mathbb{Q}, ((a, b)) \mapsto \frac{a}{b}$, ist bijektiv.

Definition Eine *Partition* Π einer Menge A ist eine Menge $\{\pi_\alpha\}_{\alpha\in I}$ von nichtleeren Teilmengen π_α von A, die auch *Blöcke* genannt werden, so daß gilt:
(1) $A = \cup_{\alpha\in I}\pi_\alpha$
(2) Für alle $\alpha, \beta \in I$ gilt: Wenn $\pi_\alpha \cap \pi_\beta \neq \phi$, dann ist $\pi_\alpha = \pi_\beta$.

(1.3) **Satz** *Sei $\mathcal{E}$ eine Aequivalenzrelation auf einer nichtleeren Menge A. Dann ist $A \setminus \mathcal{E} = \{(a) : a \in A\}$ eine Partition von A. (Diese Partition bezeichnen wir mit $\Pi_\mathcal{E}$.)*

Beweis: Aus der Reflexivität von $\mathcal{E}$ folgt $a \in (a)$ für alle $a \in A$. Also ist $A = \cup_a(a)$, wobei a ein Repräsentatensystem der Aequivalenzklassen von $\mathcal{E}$ durchläuft. Sei $(a)\cap(b) \neq \phi$ und sei $c \in (a)\cap(b)$. Dann gilt $a\mathcal{E}c$ und $b\mathcal{E}c$. Wegen der Symmetrie von $\mathcal{E}$ daher auch $a\mathcal{E}c$ und $c\mathcal{E}b$. Und wegen der Transitivität von $\mathcal{E}$ gilt somit $a\mathcal{E}b$, also $(a) = (b)$.

(1.4) **Satz** *Sei $\Pi = \{\pi_\alpha\}_\alpha$ eine Partition einer nichtleeren Menge A. Dann existiert eine Aequivalenzrelation $\mathcal{E}$ auf A mit $\Pi_\mathcal{E} = \Pi$, nämlich*

$a\mathcal{E}b :\Leftrightarrow$ *a und b liegen in demselben Block von* Π.

Beweis: Daß $\mathcal{E}$ eine Aequivalenzrelation ist, ist leicht zu sehen. Außerdem gilt $A \setminus \mathcal{E} = \Pi$. Sei dazu $(a) \in A \setminus \mathcal{E}$ und sei π_a der zu a gehörige Block. Wir behaupten: $(a) = \pi_a$. Das beweisen wir so: Sei $b \in (a)$, also $a\mathcal{E}b$. Dann gilt $a \in \pi_a$ nach Definition von $\mathcal{E}$, also $b \in (a)$ und daher $\pi_a \subset (a)$. Es folgt $(a) = \pi_a$. Also gilt $A \setminus \mathcal{E} \subset \Pi$. Sei umgekehrt $\pi_a \in \Pi$. Wegen $\pi_\alpha \neq \phi$ existiert ein $a \in A$ mit $a \in \pi_a$. Mit einer ähnlichen Schlußweise wie oben zeigt man $\pi_\alpha = (a)$. Somit ist $A \setminus \mathcal{E} = \Pi$ nachgewiesen.

Definition Sei $\mathcal{E} \subset A \times A$ eine Aequivalenzrelation auf einer nichtleeren Menge A. Die Abbildung

$\pi : A \to A \setminus \mathcal{E}$, $a \to (a)$,

die jedem $a \in A$ die a entsprechende Aequivalenzklasse zuordnet, heißt die durch $\mathcal{E}$ definierte *Quotientenabbildung.*

Bemerkung Ist $f : A \to B$ eine Abbildung, dann wird durch

$a\mathcal{E}b :\Leftrightarrow f(a) = f(b)$

auf A eine Aequivalenzrelation $\mathcal{E} = \mathcal{E}_f$ definiert.

Definition Die aufgrund von (1.3) durch die obige Aequivalenzrelation $\mathcal{E}_f$ definierte Partition von A heißt auch die zu f gehörige *Kernpartition*; ihre Blöcke heißen auch die *Fasern* von f.

(1.5) **Satz** *Jede Abbildung $f : A \to B$ ist von der Form*

$f = \psi \circ \nu$

mit einer surjektiven Abbildung $\nu : A \to C$ *und einer injektiven Abbildung* $\psi : C \to B$.

Beweis: Setze $C := A \setminus \mathcal{E}_f$. $\nu := \pi : A \to C$ sei die entsprechende Quotientenabbildung und $\psi((a)) := f(a)$ für alle $(a) \in C$.

Mengen, Relationen und Abbildungen werden benutzt, um wichtige Konzepte in den Computerwissenschaften zu definieren. Als Beispiel erwähnen wir den Begriff des Automaten, vgl. z.B. [*LS*], Part Two, pp. 62-64.

Definition Ein *Automat* ist ein 5-Tupel $(S, X, Z, \delta, \lambda)$, bestehend aus nichtleeren Mengen S, X, Z und Abbildungen

$\delta : S \times X \to S, \quad \lambda : S \times X \to Z.$

S heißt die *Menge der Zustände* des Automaten
X heißt das *Eingabealphabet* des Automaten
Z heißt das *Ausgabealphabet* des Automaten
δ heißt die *Übergangsfunktion* des Automaten
λ heißt die *Ausgabefunktion* des Automaten

Später, in §3, wird ein Automat, der die Addition ganzer Zahlen im Binärsystem durchführen kann, besprochen.

Mit Hilfe von Abbildungen läßt sich auch eine *Verallgemeinerung des cartesischen Produkts* definieren: Seien X_i, $i \in I$, Mengen. Das cartesische Produkt

$\prod_{i \in I} X_i$

der X_i ist die Menge aller Abbildungen $f : I \to \cup_{i \in I} X_i$ mit $f(i) \in X_i$ für alle $i \in I$.
Außerdem kann man den Begriff der Folge mit Hilfe von Abbildungen definieren: Eine *Folge von Elementen einer nichtleeren Menge* X ist eine Abbildung $f : \mathbb{N}_0 \to X$.

Für die nachfolgenden Begriffsbildungen und Beispiele vgl. z.B. die entsprechenden Abschnitte in [*BB*] sowie in [*LS*].

Definition Eine nichtleere Menge P heißt *teilweise geordnet,* wenn auf P eine Relation $\leqq$ existiert, die reflexiv, antisymmetrisch und transitiv ist. In einer solchen teilweise geordneten Menge $(P, \leqq)$ bedeutet $x < y$, daß $x \leqq y$ und $x \neq y$. Mit $\geqq$ bezeichnen wir die zu $\leqq$ inverse Relation. $x > y$ bedeutet, daß $x \geqq y$ und $x \neq y$. Eine teilweise geordnete Menge $(P, \leqq)$ heißt *total geordnet*,

wenn je zwei Elemente $x, y \in P$ vergleichbar sind, d.h. wenn entweder $x \leqq y$ oder $y \leqq x$ gilt. Eine total geordnete Menge heißt auch *Kette.*

Beispiele (1) Sei M eine nichtleere Menge. Dann ist die Potenzmenge $\mathcal{P}(M)$ bezüglich der Inklusion $\subset$ eine teilweise aber i.a. keine total geordnete Menge.

(2) $\mathbb{N}_0$ ist bezüglich der Teilbarkeitsrelation eine teilweise aber keine total geordnete Menge.

(3) $\mathbb{N}_0$ ist bezüglich der üblichen Relation "kleiner gleich" $\leqq$ eine total geordnete Menge.

(4) Sei X eine nichtleere Menge und sei $\Pi(X)$ die Menge aller Partitionen von X. Für $\pi, \sigma \in \Pi(X)$ bedeute $\pi \leqq \sigma$, daß $(x)_\pi \subset (x)_\sigma$ für alle $x \in X$ gilt, d.h. daß für alle $x \in X$ der durch x definierte Block bezüglich π in dem durch x definierten Block bezüglich σ enthalten ist. $\Pi(X)$ ist bezüglich dieser Relation $\leqq$ eine teilweise geordnete Menge. (Für $\pi \leqq \sigma$ sagt man auch: π ist eine *Verfeinerung* von σ.)

Man kann teilweise geordnete Mengen $(P, \leqq)$ mit Hilfe von Diagrammen darstellen. Man sagt, daß ein $x \in P$ ein $y \in P$ überlagert, falls $x > y$ aber $x > z > y$ für kein $z \in P$ gilt. Das Diagramm von $(P, \leqq)$ ist ein gerichteter Graph mit einer Ecke für jedes Element aus P und einer Kante von y nach x, wenn y von x überlagert wird.

Definition (spezielle Elemente in teilweise geordneten Mengen) Sei $(P, \leqq)$ eine teilweise geordnete Menge und sei $X \subset P$ eine nichtleere Teilmenge.

(1) $y \in X$ heißt *minimal* (bzw. *maximal*), falls $x < y$ (bzw. $x > y$) für kein $x \in X$ gilt.

(2) $y \in X$ heißt *kleinstes* (bzw. *größtes*) Element, falls $y \leqq x$ (bzw. $y \geqq x$) für alle $x \in X$ gilt. (Ein kleinstes bzw. größtes Element in X ist eindeutig bestimmt.)

(3) $y \in P$ heißt *obere* (bzw. *untere) Schranke* von X, falls $y \geqq x$ (bzw. $y \leqq x$) für alle $x \in X$ gilt.

(4) $y \in P$ heißt *größte untere Schranke* (bzw. *kleinste obere Schranke)* von X, falls y das größte (bzw. kleinste) Element in der Menge aller unteren (bzw. oberen) Schranken von X ist.

In einer total geordneten Menge fallen die Begriffe "minimales Element" und "kleinstes Element" zusammen; ebenso "maximales Element" und "größtes Element"; in einer teilweise geordnete Mengen dagegen im allgemeinen nicht.

Sei $(P, \leqq)$ eine teilweise geordnete Menge. Die dazu *duale* teilweise geordnete Menge ist $(P, \geqq)$, wobei

$$x \geqq y \text{ in } (P, \geqq) :\Leftrightarrow y \leqq x \text{ in } (P, \leqq)$$

Der Graph von $(P, \geqq)$ entsteht durch "auf den Kopf stellen" des Graphen von $(P, \leqq)$.

Bemerkung (Dualitätsprinzip) Sei T ein Satz über alle teilweise geordneten Mengen. Dann ist auch $\widehat{T}$ ein Satz über alle teilweise geordneten Mengen.

Beweis: Angenommen, die Behauptung ist falsch. Dann existiert eine teilweise geordnete Menge $(P, \leqq)$, so daß die Aussage $\widehat{T}$ für $(P, \leqq)$ falsch ist. Dann ist $\widehat{\widehat{T}} = T$ eine Aussage für $(P, \geqq)$, die falsch ist; im Widerspruch zur Annahme.

Teilweise und total geordnete Mengen lassen sich offenbar bei der Organisation von Produktionsabläufen einsetzen.

Häufig benutzt wird das folgende Resultat aus der Mengenlehre; vgl. z.B. $[HM]$.

Satz ("Lemma von Zorn") *Eine teilweise geordnete Menge, in der jede total geordnete Menge eine obere Schranke besitzt, hat ein maximales Element.*

Die nachfolgenden Begriffe und Resultate aus der Mengenlehre werden ebenfalls in $[HM]$ behandelt. Wir erinnern jedoch zunächst daran, daß nach unserer anfangs getroffenen Vereinbarung alle betrachteten Mengen einem festen Universum angehören.

Definition Zwei Mengen A, B heißen *aequivalent*, wenn eine bijektive Abbildung $A \to B$ existiert. Für jede Menge A heißt die Menge aller zu A aequivalenten Mengen die *Cardinalität* oder die *Cardinalzahl* von A; sie wird mit $|A|$ bezeichnet. Mengen, die aequivalent zur Menge aller natürlichen Zahlen sind, heißen *abzählbar.*

Die Cardinalzahlen von endlichen Mengen heißen *endlich*, die nicht endlichen Cardinalzahlen heißen *unendlich* oder *transfinit.*

Definition Für je zwei Cardinalzahlen $a = |A|, b = |B|$ bedeute $a < b$: Es existiert eine injektive Abbildung $A \to B$, und es gibt keine Teilmenge von A, die aequivalent zu B ist.

Innerhalb eines geeigneten Axiomensystems der Mengenlehre läßt sich die folgende Aussage beweisen; vgl. $[HM]$.

Trichotomieprinzip *Für je zwei Cardinalzahlen a, b gilt genau eine der folgenden Aussagen: $a < b, b < a, a = b$.*

Dabei wird u.a. das sogenannte Auswahlaxiom, das auch in anderen Zusammenhängen eine wichtige Rolle spielt, benutzt; vgl. $[HM]$.

Auswahlaxiom *Für jede nichtleere Menge X existiert eine Abbildung $f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ mit $f(S) \in S$ für alle nichtleeren Teilmengen S von X.*

Eine Menge A heißt *abzählbar*, falls $|A| = |\mathbb{N}|$ gilt.

Man kann leicht zeigen, daß die Menge aller rationalen Zahlen abzählbar ist, indem man ihre Elemente mit natürlichen Zahlen in geeigneter Weise durchnumeriert. Hingegen hat der Begründer der Mengenlehre, Georg Cantor (1845-1918), gezeigt:

(1.6) **Satz** *Die Menge aller reellen Zahlen ist nicht abzählbar.*

Beweis (nach G. Cantor): Es reicht zu zeigen, daß das Intervall

$$[0,1) = \{x \in \mathbb{R} : 0 \leqq x < 1\}$$

nicht abzählbar ist. Cantor hat diese Aussage wie folgt bewiesen. Angenommen $[0,1)$ ist abzählbar. Dann kann man die Elemente aus $[0,1)$ in der folgenden Weise hinschreiben:

$$\begin{array}{l} a_1 = 0, a_{11}a_{12}a_{13}... \\ a_2 = 0, a_{21}a_{22}a_{23}... \\ a_3 = 0, a_{31}a_{32}a_{33}... \\ \vdots \quad \vdots \end{array}$$

Aus dem Dezimalbruch

$$c := 0, a_{11}a_{22}a_{33}...$$

bildet man den Dezimalbruch d, indem jede Ziffer a_{nn} aus c durch eine beliebige Ziffer b_n mit $b_n \neq a_{nn}$ und $b_n \neq 0$ ersetzt wird:

$$d := 0, b_1b_2b_3...$$

d ist verschieden von jedem a_n, weil der Dezimalbruch eines jeden a_n von dem Dezimalbruch für d in der n-ten Ziffer abweicht. Damit ist der Beweis beendet.

Das in dem vorstehenden Beweis benutzte Verfahren heißt aus naheliegenden Gründen das *Cantorsche Diagonalverfahren.*

Wie G. Cantor außerdem entdeckt hat, kann man mit Cardinalzahlen rechnen. Man definiert dazu für $a = |A|$, $b = |B|$

$$\begin{array}{l} a + b := \left|A \dot{\cup} B\right| \\ a \cdot b := |A \times B| \end{array}$$

$a^b := \left|A^B\right|$, wobei $A^B := \{f : B \to A \text{ Abbildung}\}$.

Es gelten dann die folgenden Rechenregeln, vgl. z.B. $[HM]$.

$a + (b + c) = (a + b) + x$
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
$a^{b+c} = a^b \cdot a^c$
$(a \cdot b)^c = a^c \cdot b^c$
$(a^b)^c = a^{bc}$

Sei A eine nichtleere Menge und für $S \subset A$ sei die Abbildung $\chi_S : A \to \{0, 1\}$ wie folgt definiert: $\chi_S(x) := 1$, falls $x \in S$, und $\chi_S(x) := 0$ sonst. χ_S heißt *charakteristische Funktion von* S. Es gilt, vgl. z.B. $[HM], [LS]$.

(1.7) **Satz** *Die Zuordnung* $S \to \chi_S$ *ist eine Bijektion zwischen der Potenzmenge* $\mathcal{P}(A)$ *einer nichtleeren Menge* A *und der Menge aller Abbildungen von* A *in* $\{0, 1$ *. Insbesondere gilt:* $|\mathcal{P}(A)| = 2^{|A|}$.

Beweis: Sei $f : A \to \{0, 1\}$ eine Abbildung. Dann gilt

$f = \chi_{S_f}$, wobei $S_f := \{x \in A : f(x) = 1\}$.

Daraus ergibt sich die Surjektivität.
Für Teilmengen $S, T \subset A$ sei $\chi_S = \chi_T$. Angenommen es existiert ein $x \in S \setminus T$. Dann ist $\chi_S(x) = 1 \neq 0 = \chi_T(x)$; Widerspruch ! Somit folgt auch die Injektivität.

Wir beweisen nun die folgende Beobachtung von G. Cantor.

(1.8) **Satz** *Zwischen einer nichtleeren Menge* A *und ihrer Potenzmenge* $\mathcal{P}(A)$ *gibt es keine bijektive Abbildung.*

Beweis (nach G. Cantor): Wir zeigen, daß keine Abbildung $f : A \to \mathcal{P}(A)$ surjektiv sein kann. Dazu definieren wir

$X := \{x \in A : x \notin f(x)\}$

und behaupten

$X \notin Bild(f)$.

Angenommen $X \in Bild(f)$. Dann existiert ein $x \in A$ mit $f(x) = X$. Also gilt

$x \in X = f(x) \Leftrightarrow x \notin f(x) = X$,

ein Widerspruch!

(1.9) **Folgerung** *Für jede Cardinalzahl a gilt $2^a > a$*

(1.10) **Folgerung** *Die Potenzmenge von $\mathbb{N}$ ist nicht abzählbar.*

Man kann also im Hinblick auf (1.7) nicht alle Abbildungen $\mathbb{N} \to \{0,1\}$ aufzählen.

Das *Kontinuumsproblem* besteht in der Frage, ob es zwischen $|\mathbb{N}_0|$ und $2^{|\mathbb{N}_0|}$ eine weitere Cardinalzahl gibt; vgl. dazu $[HM]$.

Zum Abschluß dieses Paragraphen wird die bereits im Zusammenhang mit Relationen benutzte intuitive Vorstellung von Graphen formalisiert; vgl. $[BB]$ und $[LS]$.

Definition Ein *Graph* ist ein Tripel (E, K, θ), wobei E eine Menge ist, deren Elemente *Punkte* oder *Ecken* genannt werden; wobei K eine Menge ist, deren Elemente *Verbindungen* oder *Kanten* heißen; und wobei

$\theta : K \to \{\{p,q\} : p,q \in E\}$

eine Abbildung ist. Für $k \in K$ heißt $\theta(k) = \{p,q\}$ das *Ende* von k. Ein Graph heißt *gerichtet*, wenn θ eine Abbildung ist, deren Bilder geordnete Paare sind, d.h. θ ist eine Abbildung von K nach $E \times E$. Eine Kante $k \in K$ heißt *Schleife*, falls $\theta(k) = (p,p)$ gilt.

Ein gerichteter Graph bestimmt eine Relation $\rho \subset E \times E$: Für alle $(p,q) \in E \times E$ gilt $p\rho q$ genau dann, wenn eine Kante $a \in K$ existiert, so daß $\theta(a) = (p,q)$. Umgekehrt definiert jede Relation $\rho \subset E \times E$ einen gerichteten Graphen $G(\rho) = (E, K(\rho), \theta)$ mit $K(\rho) = \{\overrightarrow{pq} : p \in E,\ q \in E,\ p\rho q\}$, und $\theta(\overrightarrow{pq}) = (p,q)$.

Aufgaben und Beispiele

(1) Schreiben Sie alle Elemente der Potenzmenge von $A = \{1,2,3\}$ hin.

(2) Es gilt $|\mathcal{P}(A)| = 2^{|A|}$, $\left|\mathcal{P}(X \dot\cup Y)\right| = |\mathcal{P}(X)| \cdot |\mathcal{P}(Y)|$:

(3) Gegeben seien die Mengen $A = \{1,2,3\}, B = \{a,b,c,d,e\}, C = \{\alpha,\beta,\gamma\}$ sowie die Relationen
$\sigma = \{(1,a),(1,b),(2,b),(3,c)\} \subset A \times B$,
$\rho = \{(\alpha,a),(\alpha,c),(\beta,d),(\gamma,b),(\gamma,d),(\gamma,e)\} \subset C \times B$.
Bestimmen Sie die Relation $\sigma\widetilde{\rho}$ sowie deren Relationsmatrix und zeichnen Sie den Relationsgraphen von $\sigma\widetilde{\rho}$.

(4) Sei $A = \{1,2,3\}, \rho := \{(1,1),(1,2),(2,1),(2,2)(2,3),(3,2),(3,3)\}$. $\rho \subset A \times A$ ist reflexiv, symmetrisch aber nicht transitiv; denn es ist $(1,2),(2,3) \in \rho, (1,3) \notin \rho$. Außerdem gilt $\rho^2 = A \times A$.

(5) Eine Relation ist genau dann sowohl symmetrisch als auch antisymmetrisch, wenn ihre Relationsmatrix eine Diagonalmatrix ist.

(6) (Vgl. $[BB]$, Chapter 2; $[LS]$, Chapters 1, 3) Die Menge $B = \{0,1\}$ sei versehen mit den wie folgt definierten Verknüpfungen + und ·:

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

Sei $M_1 = (r_{ij}^{(1)})$ eine $(\ell \times m)$- und sei $M_2 = (r_{ij}^{(2)})$ eine $(m \times n)$-Matrix mit Koeffizienten in B. Setze

$$M_1 M_2 := (\textstyle\sum_{k=1}^{m} r_{ik}^{(1)} \cdot r_{kj}^{(2)})_{1 \le i \le l, 1 \le k \le m}$$

wobei $\sum$ die Summe im Sinne der obigen Definition von + bezeichnet. Dann gilt: Sind A, B, C endliche Mengen und sind $\rho_1 \subset A \times B$, $\rho_2 \subset B \times C$ Relationen mit entsprechenden Relationsmatrizen $M(\rho_1)$, $M(\rho_2)$, dann ist

$$M(\rho_1)M(\rho_2) = M(\rho_1\rho_2).$$

(7) Sei $\Pi(X)$ die Menge aller Partitionen einer nichtleeren Menge X. Für π_1, $\pi_2 \in \Pi(X)$ bedeute $\pi_1 \le \pi_2$, daß $(x)_{\pi_1} \subset (x)_{\pi_2}$ für alle $x \in X$. Zeigen Sie, daß $(\Pi(X), \le)$ eine teilweise geordnete Menge ist.

(8) Auf der Menge aller reellen Zahlen $\mathbb{R}$ betrachte man die übliche totale Ordnungsrelation $\leqq$. Bestimmen Sie für die folgenden Teilmengen $X \subset \mathbb{R}$ jeweils, falls vorhanden, das kleinste und größte Element sowie die kleinste obere und größte untere Schranke:

(a) $X := \{\frac{1}{n} : n \in \mathbb{N}\}$ (b) $X := \{\frac{(-1)^n}{n} : n \in \mathbb{N}\}$

Lösung:

	(a)	(b)
kleinstes Element	existiert nicht	-1
größtes Element	1	$\frac{1}{2}$
größte untere Schranke	0	-1
kleinste obere Schranke	1	$\frac{1}{2}$

Literatur zu §1: $[BB]$, $[HM]$, $[LP]$, $[LS]$, $[SC]$, $[SGA4]$

§ 2. **Verbände und Boolesche Algebren**

In diesem Paragraphen werden grundlegende Begriffe und Resultate über Verbände und Boolesche Algebren besprochen. Dabei folgen wir vorwiegend entsprechenden Darstellungen in $[BB]$, $[GT]$ und $[LS]$.

Sei $(P, \leqq)$ eine teilweise geordnete Menge. Für $x, y \in P$ sei

$x \wedge y$ die größte untere Schranke von $\{x, y\}$, falls sie existiert

$x \vee y$ die kleinste obere Schranke von $\{x, y\}$, falls sie existiert.

Für $g := x \wedge y$ gilt

(1) $g \leqq x$, $g \leqq y$

(2) $h \leqq x$, $h \leqq y \Rightarrow h \leqq g$

$x \wedge y$ heißt auch *Durchschnitt von* x, y und $x \vee y$ heißt auch *Vereinigung* von x, y.

Definition Ein *Verband* ist eine teilweise geordnete Menge, in der je zwei Elemente einen Durchschnitt und eine Vereinigung besitzen.

Beispiele (1) Jede total geordnete Menge ist ein Verband mit

$a \wedge b = Min\{a, b\}$, $a \vee b = Max\{a, b\}$,

wobei Min bzw. Max bezüglich der gegebenen totalen Ordnungsrelation gebildet wird.

(2) Sei $\mathcal{P}(M)$ die Potenzmenge einer Menge M. Dann ist $(\mathcal{P}(M), \subset)$ ein Verband mit $A \wedge B = A \cap B$, $A \vee B = A \cup B$.

(3) $(\mathbb{N}_0, /)$ ist ein Verband, wobei a/b bedeutet: a teilt b. $a \wedge b$ ist der größte gemeinsame Teiler von a und b; $a \vee b$ ist das kleinste gemeinsame Vielfache von a und b. Vgl. dazu §3.

In einem Verband gelten die folgenden leicht zu beweisenden Rechenregeln

$x \wedge x = x$, $x \vee x = x$
$x \wedge (y \wedge z) = (x \wedge y) \wedge z$, $x \vee (y \vee z) = (x \vee y) \vee z$
$x \wedge y = y \wedge x$, $x \vee y = y \vee x$
$x \wedge (x \vee y) = x$, $x \vee (x \wedge y) = x$
$x \leqq y \Leftrightarrow x \wedge y = x \Leftrightarrow x \vee y = y$

Der in der nachfolgenden Definition gegebene Begriff der Booleschen Algebra entstand aus Untersuchungen von G. Boole $[BL]$.

Definition Eine *Boolesche Algebra* besteht aus einer Menge A zusammen mit zwei Abbildungen (Verknüpfungen)

$$\wedge, \vee : A \times A \to A,$$

einer Abbildung

$$' : A \to A$$

sowie mit zwei Elementen $0, 1 \in A$, so daß die folgenden Rechenregeln gelten:

$x \vee x = x$, $x \wedge x = x$
$x \vee (y \vee z) = (x \vee y) \vee z$, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$
$x \vee y = y \vee x$, $x \wedge y = y \wedge x$
$x \vee (x \wedge y) = x$, $x \wedge (x \vee y) = x$
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
$x \vee 0 = x$, $x \wedge 0 = 0$
$x \vee 1 = 1$, $x \wedge 1 = x$
$x \vee x' = 1$, $x \wedge x' = 0$

Es folgt:

Wenn $x \vee y = 1$ und $x \wedge y = 0$, dann ist $y = x'$
$(x \vee y)' = x' \wedge y'$
$(x \wedge y)' = x' \vee y'$.

Eine Boolesche Algebra schreiben wir manchmal auch in der Form $\mathfrak{A} = (A, \wedge, \vee, ', 0, 1)$.

Beispiele (a) Sei X eine nichtleere Menge. Dann ist die Potenzmenge $A = \mathcal{P}(X)$ von X zusammen mit $\wedge = \cap$ = Durchschnitt, $\vee = \cup$ = Vereinigung, $' =$ Komplement, $0 = \emptyset$, $1 = X$ eine Boolesche Algebra, die sogenannte *Boolesche Algebra der Potenzmenge von* X, geschrieben $(\mathcal{P}(X), \cap, \cup, ', \emptyset, X)$.

(b) Definiert man auf der Menge $\{0, 1\}$ zwei Verknüpfungen $\wedge, \vee : A \times A \to A$ sowie die Abbildung $' : A \to A$ durch

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$'$	
0	1
1	0

,

dann ist $(A, \wedge, \vee, ', 0, 1)$ eine Boolesche Algebra; die sogenannte *Boolesche Algebra der Wahrheitswerte*, weil bei der Interpretation von $\wedge$ durch "und", $\vee$ durch "oder", $'$ durch "nicht", 1 durch "wahr", 0 durch "falsch" diese Boolesche Algebra, die wir im Folgenden kurz mit **2** bezeichnen, dem Rechenbereich der elementaren Aussagenlogik entspricht.

(c) Die Boolesche Algebra der Wahrheitswerte induziert die Struktur einer Booleschen Algebra auch auf der Menge aller Abbildungen $\{0,1\}^X$ von einer nichtleeren Menge X in die Menge $\{0,1\}$, indem man die Verknüpfungen $\wedge, \vee$ sowie die Abbildung $'$ und die Elemente $\underline{0}$, $\underline{1}$ punktweise definiert, d.h.

$(f \wedge g)(x) := f(x) \wedge g(x)$
$(f \vee g)(x) := f(x) \vee g(x)$
$f'(x) := (f(x))'$
$\underline{0}(x) := 0$
$\underline{1}(x) := 1$

jeweils für alle $f, g \in \{0,1\}^X$ und für alle $x \in X$. Es folgt:

(2.1) **Satz** *Für die bijektive Abbildung*

$\chi : \mathcal{P}(X) \to \{0,1\}^X$, $S \mapsto \chi_S$,

wobei $\chi_S(x) := \begin{cases} 1, & \text{falls } x \in S \\ 0, & \text{falls } x \notin S \end{cases}$

aus (1.7) *gilt*

$\chi_{S \cap T} = \chi_S \wedge \chi_T$
$\chi_{S \cup T} = \chi_S \vee \chi_T$
$\chi_{S'} = \chi'_S$
$\chi_\emptyset = \underline{0}$
$\chi_X = \underline{1}$

jeweils für alle $S, T \subset X$; d.h. χ *ist im Sinne der folgenden Definition ein Isomorphismus von Booleschen Algebren.*

Definition Seien $\mathfrak{A} = (A, \wedge, \vee, ', 0, 1)$ und $\mathfrak{B} = (B, \curlywedge, \curlyvee, \urcorner, \underline{0}, \underline{1})$ Boolesche Algebren. Eine Abbildung $f : A \to B$ heißt *Morphismus* von der Booleschen Algebra $\mathfrak{A}$ in die Boolesche Algebra $\mathfrak{B}$, falls

$f(x \wedge y) = f(x) \curlywedge f(y)$
$f(x \vee y) = f(x) \curlyvee f(y)$
$f(x') = \urcorner f(x)$
$f(0) = \underline{0}$
$f(1) = \underline{1}$

jeweils für alle $x, y \in A$ gilt.
Ein injektiver bzw. surjektiver bzw. bijektiver Morphismus von Booleschen Algebren heißt *Monomorphismus* bzw. *Epimorphismus* bzw. *Isomorphismus*.

Definition Sei $(B, \wedge, \vee, ', 0, 1)$ eine Boolesche Algebra. Die Relation $\leqq$ auf B wird wie folgt definiert. Es gilt $a \leqq b$, wenn $a \wedge b = a$.

(2.2) **Satz** *Mit dieser Definition für* $\leqq$ *wird jede Boolesche Algebra* $(B, \wedge, \vee, ', 0, 1)$ *zu einem Verband.*

Beweis: Es reicht zu zeigen, daß $(B, \leqq)$ eine teilweise geordnete Menge ist. Wegen $a \wedge a = a$ gilt $a \leqq a$ für alle $a \in A$. Aus $a \leqq b$ und $b \leqq a$ folgt $a \wedge b = a$ und $b \wedge a = b$, also $a = b$ aufgrund der Kommutativität der Verknüpfung $\wedge$. Sei $a \leqq b$ und $b \leqq c$. Dann gilt $a \wedge b = a$, $b \wedge c = b$, also $a = a \wedge b = a \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c$, also $a = a \wedge c$, d.h. $a \leqq c$.

Wir ergänzen Beweise von bereits weiter oben erwähnten wichtigen Rechenregeln in Booleschen Algebren. Sei $\mathfrak{B} = (B, \wedge, \vee, ', 0, 1)$ eine Boolesche Algebra.

(2.3) **Bemerkung** Aus $p \wedge q = 0$ und $p \vee q = 1$ folgt $q = p'$.

Beweis: $q = 1 \wedge q = (p \vee p') \wedge q = (p \wedge q) \vee (p' \wedge q) =$

$= 0 \vee (p' \wedge q) = (p' \wedge p) \vee (p' \wedge q) = p' \wedge (p \vee q) = p' \wedge 1 = p'.$

(2.4) **Bemerkung** (Regeln von D'Morgan)

(a) $(p \vee q)' = p' \wedge q'$ (b) $(p \wedge q)' = p' \vee q'$

Beweis: (a) $(p \vee q) \vee (p' \wedge q') = ((p \wedge (q \vee q')) \vee q) \vee (p' \wedge q') =$

$= (p' \vee ((p \wedge (q \vee q')) \vee q)) \wedge (q' \vee ((p \wedge (q \vee q')) \vee q)) =$

$= (p' \vee (p \vee q)) \wedge (q' \vee (p \vee q)) = p' \vee (p \vee q) = 1.$

$(p \vee q) \wedge (p' \wedge q') = ((p \wedge p') \vee (q \wedge p')) \wedge q' = q \wedge p' \wedge q' = 0.$

Die behauptete Regel (a) folgt aus der vorangehenden Bemerkung (2.3).
(b) Aus (a) folgt mit p' an Stelle von p und q' an Stelle von q: $(p' \vee q')' = p'' \wedge q'' = p \wedge q$, also $p' \vee q' = (p \wedge q)'$, wegen $p'' = p$.

Boolesche Algebren finden Anwendung in der *Schaltalgebra*: Die Operation $\wedge$ bzw. $\vee$ in der Booleschen Algebra der Wahrheitswerte $\mathbf{2}$ interpretiert man als Hintereinanderschaltung bzw. als Parallelschaltung.

Definition Ein *Boolescher Term* in endlich vielen Unbestimmten (Symbolen) $X_1, X_2, ..., X_n$ wird rekursiv wie folgt definiert: Jedes X_i ist ein Boolescher Term; sind P, Q Boolesche Terme, so auch $P', P \wedge Q$ und $P \vee Q$.

Beispiel $((X_1 \wedge X_2) \vee X_3)' \wedge ((X_1 \vee X_2) \wedge X_3')$ ist ein Boolescher Term in den Symbolen X_1, X_2, X_3.

(2.5) **Hilfssatz** (Vgl. [BB], Chapter 5) *Zu jedem n-Tupel $(a_1, ..., a_n) \in \{0,1\}^n$ gibt es einen Booleschen Term t in n Unbestimmten $X_1, ..., X_n$, so daß gilt: $t(b_1, ..., b_n) = 1$ genau dann, wenn $b_1 = a_1, ..., b_n = a_n$.*

Beweis: $t := Y_1 \wedge ... \wedge Y_n$, wobei $Y_i := X_i$, falls $a_i = 1$, und $Y_i := X_i'$, falls $a_i = 0$, ist ein Term mit den gewünschten Eigenschaften.

(2.6) **Satz** (Vgl. [BB], Chapter 5) *Jede Abbildung $F : \{0,1\}^n \to \{0,1\}$ ist durch einen Booleschen Term beschreibbar, d.h. es existiert ein Boolescher Term $t(X_1, ..., X_n)$ in den Symbolen $X_1, ..., X_n$, so daß $F(a_1, ..., a_n) = t(a_1, ..., a_n)$ für alle $(a_1, ..., a_n) \in \{0,1\}^n$ gilt.*

Beweis**:** Für jedes n-Tupel von Argumenten, für den F den Wert 1 annimmt, konstruiere man einen Booleschen Term wie im vorangehenden Hilfssatz. Verbindet man diese Terme durch $\vee$, dann erhält man einen Term, der F beschreibt.

In der Sprechweise der Schaltalgebra kann man sagen, daß die "Vorgabe" (Abbildung) F durch einen "Schaltkreis" t (Boolescher Term) zu realisieren ist. Der Beweis des obigen Satzes (2.6) gibt ein Verfahren zur Konstruktion eines solchen Schaltkreises; dieses Verfahren ist natürlich im allgemeinen nicht optimal.

Beispiel $n = 2$

X_1X_2	F	$(X_1' \wedge X_2') \vee (X_1' \wedge X_2) \vee (X_1 \wedge X_2') = X_1' \vee X_2'$
0 0	1	1
0 1	1	1
1 0	1	1
1 1	0	0

Aufgaben und Beispiele

(1) (vgl. z.B. [GT], 10.1, 10.2, und auch [AMD], Chapter 1, Exercise 25) Sei $\mathfrak{B} = (B, \wedge, \vee, ', 0, 1)$ eine Boolesche Algebra. Wenn für $x, y \in B$ die Beziehung $y \leqq x$ gilt, d.h. wenn $x \wedge y = y$, so sagen wir auch, daß x das Element y *enthält.* $x \in B$ heißt *Atom* oder *minimales Element* von $\mathfrak{B}$, wenn $x \neq 0$ und wenn kein Element $y \in B$ existiert mit $0 < y < x$. $x \in B$ heißt *maximales Element* von $\mathfrak{B}$, wenn $x \neq 1$ und wenn kein $y \in B$ mit $x < y < 1$ existiert. Es gilt:

(a) Wenn $y \leqq x$ und $z \leqq x$, dann ist $y \vee z \leqq x$

(b) Ist $x \in B$ ein minimales Element, dann ist x' maximales Element; und umgekehrt

(c) Ist B endlich, dann hat $\mathfrak{B}$ maximale und minimale Elemente

(d) Sind x, y minimale Elemente von $\mathfrak{B}$, dann gilt $x \wedge y = 0$ oder $x = y$

(e) Gilt für zwei Elemente $x, y \in B$, daß $x > y$, dann enthält x ein Atom, das nicht in y enthalten ist.

(f) Ist B endlich, dann ist jedes Element x aus B von der Form $x_1 \vee ... \vee x_n$, wobei $x_1, ..., x_n$ die in x enthaltenen Atome von $\mathfrak{B}$ sind.

(g) Ist B endlich, dann ist jedes Element x aus B von der Form $x_1 \wedge ... \wedge x_m$, wobei $x_1, ..., x_m$ die maximalen Elemente von $\mathfrak{B}$ sind, die x enthalten.

(h) Ist B endlich und sind $x_1, ..., x_n$; $y_1, ..., y_m$ Atome von $\mathfrak{B}$, dann gilt $x_1 \vee ... \vee x_n = y_1 \vee ... \vee y_m$ genau dann, wenn $\{x_1, ..., x_n\} = \{y_1, ..., y_m\}$.

(i) Sei B endlich und sei X die Menge aller Atome von $\mathfrak{B}$. Sei $f : B \to \mathfrak{P}(X)$ die Abbildung, die $x \in B$ auf die Menge der in x enthaltenen Atome abbildet. Dann induziert f einen Isomorphismus von Booleschen Algebren

$$f : \mathfrak{B} \to (\mathcal{P}(X), \cap, \cup, ', \emptyset, X).$$

(2) Bestimmen Sie einen Booleschen Term, der die folgende Abbildung beschreibt:

$$F : \{0,1\}^4 \to \{0,1\},$$

$F(a_1, a_2, a_3, a_4) := 1$ genau dann, wenn $a_1 = a_2 = a_3 = a_4$

$F(a_1, a_2, a_3, a_4) := 0$ sonst.

(3) Sei die Abbildung $F : \{0,1\}^3 \to \{0,1\}$ durch die folgende Tabelle gegeben

x_1	x_2	x_3	$F((x_1, x_2, x_3))$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	1

Bestimmen sie einen Booleschen Term, der F beschreibt.

Lösung:. $F(x_1, x_2, x_3) = (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2' \wedge x_3') \vee (x_1' \wedge x_2 \wedge x_3) \vee (x_1' \wedge x_2' \wedge x_3')$

Bemerkung: Man kann diesen Ausdruck vereinfachen zu $F(x_1, x_2, x_3) = (x_2 \wedge x_3) \vee (x_2' \wedge x_3')$

Literatur zu §2: [AMD], [BB], [BL], [GT], [LS]

§ 3. **Ganze Zahlen und Polynome**

In diesem Abschnitt besprechen wir grundlegende Resultate über ganze Zahlen und Polynome in nur einer Unbestimmten mit Koeffizienten aus einem Körper und folgen dabei vorwiegend entsprechenden Darstellungen in [BA], [BB], [BM], [F], [$L1$], [$L2$], [LS], [LV], [SB].

(3.1) **Axiom** Jede nichtleere Teilmenge von $\mathbb{N}$ hat ein kleinstes Element.

(3.2) **Satz** *(*vollständige Induktion*) Angenommen für jede natürliche Zahl n ist eine Aussage $A(n)$ gegeben, und man kann beweisen:*
(1) *$A(1)$ ist wahr,*
(2) *Für alle $k \in \mathbb{N}$ gilt: Wenn $A(k)$ wahr ist, dann auch $A(k+1)$.*
Dann ist $A(n)$ für alle $n \in \mathbb{N}$ wahr.

Beweis: Sei $M := \{n \in \mathbb{N} : A(n) \text{ ist falsch}\}$. Zu zeigen ist: $M = \emptyset$. Angenommen $M \neq \emptyset$. Nach dem obigen Axiom (3.1) enthält M ein kleinstes Element n_0. Weil $A(1)$ nach Annahme (1) wahr ist, ist $n_0 \neq 1$, also $n_0 > 1$. Nach Wahl von n_0 ist $n_0 - 1 \notin M$. Also ist $A(n_0 - 1)$ wahr, und damit ist nach Annahme (2) auch $A(n_0)$ wahr. Also ist $A(n_0)$ wahr und falsch. Widerspruch !

Definition $a \in \mathbb{Z}$ heißt *teilbar durch* $b \in \mathbb{Z}$, falls ein $k \in \mathbb{Z}$ mit $a = k \cdot b$ existiert; a heißt auch ein *Vielfaches von* b. Wir schreiben auch b/a, wenn a ein Vielfaches von b ist.

(3.3) **Satz** *(*Teilbarkeit mit Rest*) Seien $m, n \in \mathbb{Z}$ mit $m > 0$ und $n \geqq 0$. Dann existieren $q, r \in \mathbb{N}_0$, so daß $n = qm + r$ und $0 \leqq r < m$. Durch diese Bedingungen sind q und r eindeutig bestimmt. r heißt Rest von n bei der Division durch m.*

Beweis: Wir beweisen die Aussage durch Induktion über n. Für $n = 0$ ist $q = r = 0$. Sei $n > 0$. Für $n < m$ ist $q = 0$ und $r = n$. Für $n \geqq m$ ist $0 \leqq n - m < n$. Nach Induktionsvoraussetzung existieren $q_1, r_1 \geqq 0$, so daß

$$
\begin{aligned}
&n - m = q_1 m + r_1 \text{ und } r_1 < m \\
&n = m + q_1 m + r_1 \\
&\quad = (1 + q_1)m + r_1 \\
&\quad = qm + r \text{ mit } q := 1 + q_1, r := r_1.
\end{aligned}
$$

Die Eindeutigkeit ergibt sich wie folgt: Sind

$$n = qm + r, 0 \leqq r < m; n = pm + s, 0 \leqq s < m$$

Darstellungen von n wie oben. Dann gilt

$$(p - q)m = r - s, 0 \leqq r - s < m.$$

Weil $r - s$ durch m teilbar ist, folgt $r - s = 0$, also $r = s$ und damit auch $p = q$.

(3.4) **Satz** *(g-adische* Ziffernentwicklung*) Sei $g \in \mathbb{N}, g > 1$. Dann besitzt jede natürliche Zahl a eine eindeutige Darstellung der Form*

$$a = c_0 + c_1 g + c_2 g^2 + ... + c_n g^n \quad \text{mit} \quad 0 \leqq c_m < g.$$

Diese Darstellung von a heißt die g-adische Entwicklung von a. Schreibweise: $(a)_g = c_n c_{n-1} ... c_0$.

Beweisskizze: Wir führen den Beweis durch Induktion über a. Für $a = 1$ gilt $n = a, c_0 = 1$. Sei $a > 1$ und sei die Behauptung schon bewiesen für $1, 2, ..., a-1$. Sei $g > 1$. Dann ist die Folge

$$g^0, g^1, g^2, ...$$

monoton steigend, und jede natürliche Zahl liegt zwischen zwei aufeinander folgenden Potenzen von g, d.h. es gibt ein $n \geqq 0$:

$$g^n \leqq a < g^{n+1}$$

Division mit Rest ergibt eine Darstellung der Form

$$a = c_n g^n + r \quad \text{mit} \quad 0 \leqq r < g^n.$$

Es ist $c_n > 0$, weil $c_n g^n = a - r > g^n - g^n = 0$. Es ist $c_n < g$, weil $c_n g^n \leqq a < g^{n+1}$. Für $r = 0$ gilt

$$a = 0 \cdot 0 \cdot g + ... + 0 \cdot g^{n-1} + c_n g^n.$$

Für $r > 0$ gilt wegen $r < g^n \leqq a$ nach Induktionsvoraussetzung

$$r = b_0 + b_1 g + ... + b_t g^t.$$

Dabei ist $b_t > 0, 0 \leqq b_m < g$ für $0 \leqq m \leqq t$. Außerdem ist $t < n$. Also

$$a = c_n g^n + r = b_0 + b_1 g + ... + b_t g^t + 0 \cdot g^{t+1} + ... + 0 \cdot g^{n-1} + c_n g^n.$$

Die Eindeutigkeit dieser Darstellung beweist man mit Hilfe der Eindeutigkeitsaussage in (3.3); vgl. dazu auch die entsprechenden Ausführungen in [LV].

Rechenbeispiel $2743 = 1 \cdot 7^4 + 0 \cdot 7^3 + 6 \cdot 7^2 + 6 \cdot 7^1 + 6 \cdot 7^0$, also $(2743)_7 = 10666$.

Nachfolgend wird ein Automat, mit dem die Addition ganzer Zahlen im Binärsystem durchgeführt werden kann, angegeben; vgl. dazu [LS], Part Two, p. 63.

Beispiel (Automat für die Addition ganzer Zahlen im Binärsystem)
$S = \{c, \overline{c}\}$; $\overline{c}$ heißt Anfangszustand
$X = \{\binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{1}\}$
$Z = \{0, 1\}$
Die Übergangs- und die Ausgabefunktion sind durch die folgenden Tabellen gegeben:

$\delta : S \times X \to S$	$\lambda : S \times X \to Z$
$\delta(\overline{c}, \binom{0}{0}) = \overline{c}$	$\lambda(\overline{c}, \binom{0}{0}) = 0$
$\delta(\overline{c}, \binom{0}{1}) = \overline{c}$	$\lambda(\overline{c}, \binom{0}{1}) = 1$
$\delta(\overline{c}, \binom{1}{0}) = \overline{c}$	$\lambda(\overline{c}, \binom{1}{0}) = 1$
$\delta(\overline{c}, \binom{1}{1}) = c$	$\lambda(\overline{c}, \binom{1}{1}) = 0$
$\delta(c, \binom{0}{0}) = \overline{c}$	$\lambda(c, \binom{0}{0}) = 1$
$\delta(c, \binom{0}{1}) = c$	$\lambda(c, \binom{0}{1}) = 0$
$\delta(c, \binom{1}{0}) = c$	$\lambda(c, \binom{1}{0}) = 0$
$\delta(c, \binom{1}{1}) = c$	$\lambda(c, \binom{1}{1}) = 1$

Wir testen diesen Automaten anhand eines Rechenbeispiels:

$$\begin{array}{rl} & 6 = 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 \\ + & 8 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 \\ \hline & 14 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 \end{array}$$

Eingabe	$\binom{0}{1}$	$\binom{1}{0}$	$\binom{1}{0}$	$\binom{0}{0}$			
Zustände	$\overline{c}$	$\overline{c}$	$\overline{c}$	$\overline{c}$	$\overline{c}$	=	Anfangszustand
Ausgabe	1	1	1	0			

Definition Ein *gemeinsamer Teiler* von $m, n \in \mathbb{Z} - \{0\}$ ist eine ganze Zahl $d \neq 0$ mit d/m und d/n. Ein *größter gemeinsamer Teiler* von $m, n \in \mathbb{Z} - \{0\}$ ist ein gemeinsamer Teiler $d > 0$ von m und n, der von jedem anderen gemeinsamen Teiler von m und n geteilt wird.

Ein größter gemeinsamer Teiler von $m, n \in \mathbb{Z} - \{0\}$ ist eindeutig bestimmt; Schreibweise $ggT(m, n)$.

Definition Eine nichtleere Teilmenge $J \subset \mathbb{Z}$ heißt *Untergruppe* von $\mathbb{Z}$, falls gilt: Wenn $x, y \in J$, dann ist auch $x - y \in J$.

Jede Untergruppe $J \subset \mathbb{Z}$ hat die Eigenschaft $J \cdot \mathbb{Z} \subset J$, wobei $J \cdot \mathbb{Z} := \{j \cdot m; j \in J, m \in \mathbb{Z}\}$.

Beispiel Seien $m_1, ..., m_s \in \mathbb{Z}$ und sei

$J := \{x_1 m_1 + ... + x_s m_s : x_1, ..., x_s \in \mathbb{Z}\}$.

Dann ist J eine Untergruppe von $\mathbb{Z}$, die mit

$J = (m_1, ..., m_s)$

bezeichnet wird und die *die von* $m_1, ..., m_s$ *erzeugte Untergruppe* genannt wird.

(3.5) **Satz** *Sei* $J \subset \mathbb{Z}$ *eine Untergruppe. Dann existiert ein* $d \in \mathbb{Z}, d \geqq 0$, *so daß* $J = (d)$

Beweis: Für $J = \{0\}$ ist $d = 0$. Sei $J \neq \{0\}$. Mit $n \in J$ gilt auch $-n = 0 - n \in J$. Also enthält J eine nazütliche Zahl. Sei d die kleinste natürliche Zahl in J; diese existiert nach dem Axiom vom kleinsten Element (3.1).

Behauptung: Es gilt $J = (d)$.

Beweis: Sei $n \in J$. Dann gilt aufgrund der Division mit Rest

$n = qd + r$ mit $0 \leqq r < d$.

Also $r = n - qd \in J$; denn es ist $n \in J$ und mit d auch $qd \in J$. Wegen $r < d$ folgt $r = 0$, also $n = qd$.

(3.6) **Satz** *Seien* $m_1, m_2 \in \mathbb{Z} - \{0\}$ *und sei* $d \in \mathbb{Z}, d > 0$, *so, daß* $(m_1, m_2) = (d)$ *(siehe (3.5)). Dann ist* $d = ggT(m_1, m_2)$. *Umgekehrt: Ist* $d = ggT(m_1, m_2)$, *dann gilt* $(m_1, m_2) = (d)$.

Beweis: Es gilt $m_1 = 1 \cdot m_1 + 0 \cdot m_2 \in (m_1, m_2) = (d)$, also ist d ein Teiler von m_1; ebenso zeigt man d/m_2. Somit ist d ein gemeinsamer Teiler von m_1 und m_2. Sei $e \neq 0$ ein gemeinsamer Teiler von m_1 und m_2, also $m_1 = h_1 e, m_2 = h_2 e$ mit $h_1, h_2 \in \mathbb{Z}$. Wegen $d \in (m_1, m_2)$ existieren $x_1, x_2 \in \mathbb{Z}$ mit

$$\begin{aligned} d &= x_1 m_1 + x_2 m_2 = x_1 h_1 e + x_2 h_2 e \\ &= (x_1 h_1 + x_2 h_2) e, \end{aligned}$$

also ist e ein Teiler von d.

Umgekehrt: Nach dem vorangehenden Satz existiert ein $d' > 0$ mit $(m_1, m_2) = (d')$. Also gilt nach dem bereits Bewiesenen: $d' = ggT(m_1, m_2)$. Wegen der Eindeutigkeit des ggT ist $(m_1, m_2) = (d)$.

Definition Der größte gemeinsame Teiler von endlich vielen ganzen Zahlen $m_1, ..., m_r \in \mathbb{Z} - \{0\}$ ist definiert durch

$ggT(m_1, ..., m_r) :=$ positives erzeugendes Element der Untergruppe

$(m_1, ..., m_r) \subset \mathbb{Z}$

Offensichtlich gilt

$(\star)$ $ggT(m_1, ..., m_r) = x_1 m_1 + ... + x_r m_r$

mit ganzen Zahlen $x_1, ..., x_r$.

(3.7) **Satz** *Die Gleichung*

$d = m_1 x_1 + ... + m_r x_r$

mit $d \in \mathbb{Z} - \{0\}; m_1, ..., m_r \in \mathbb{Z} - \{0\}$, *ist genau dann in ganzen Zahlen* $x_1, ..., x_r$ *lösbar, wenn* $ggT(m_1, ..., m_r)$ *die ganze Zahl* d *teilt.*

Beweis: Nach $(\star)$ gibt es ganze Zahlen $y_1, ..., y_r$, so daß

$ggT(m_1, ..., m_r) = y_1 m_1 + ... + y_r m_r$.

Sei $ggT(m_1, ..., m_r)$ ein Teiler von d, d.h. es gibt eine ganze Zahl k mit

$$\begin{aligned} d &= ggT(m_1, ..., m_r) \cdot k \\ &= y_1 k m_1 + ... + y_r k m_r. \end{aligned}$$

Mit $x_1 := y_1 \cdot k, ..., x_r := y_r \cdot k$ ist dann die gegebene Gleichung lösbar. Sei umgekehrt $d = m_1 x_1 + ... + m_r x_r$ lösbar in ganzen Zahlen $x_1, ..., x_r$, d.h. es gilt

$d \in (m_1, ..., m_r) = (ggT(m_1, ..., m_r))$.

Somit ist d ein Vielfaches von $ggT(m_1, ..., m_r)$.

Beispiel Die Gleichung $2 = 3x_1 + 6x_2$ ist nicht in ganzen Zahlen x_1, x_2 lösbar; denn $ggT(3, 6) = 3$ ist teilerfremd zu 2.

Für den ggT gelten die folgenden leicht zu beweisenden Rechenregeln:

(R1) Für alle ganzen Zahlen a, b, q ist $ggT(b, a) = ggT(b, a - bq)$.
(R2) Für $r \geqq 3$ gilt stets $ggT(a_1, ..., a_r) = ggT(ggT(a_1, ..., a_{r-1}), a_r)$.
(R3) Für alle $t \in \mathbb{N}_0$ gilt stets $ggT(ta_1, ..., ta_r) = t \cdot ggT(a_1, ..., a_r)$.
(R4) Für alle $a, b, c \in \mathbb{Z}$ mit $ggT(a, c) = 1$ gilt $ggT(ab, c) = ggT(b, c)$.

Die Division mit Rest erlaubt die schrittweise Bestimmung des ggT. Den entsprechenden Algorithmus, den wir jetzt erläutern, nennt man den *euklidischen Algorithmus.*

Gegeben seien natürliche Zahlen $a = a_0$ und $b = a_1$ mit $a_1 \leqq a_0$. Wir teilen a_0 durch a_1 mit Rest a_2 und erhalten

$$a_0 = a_1 q_1 + a_2 \quad \text{mit} \quad 0 \leqq a_2 < a_1;$$

sodann teilen wir a_1 durch a_2 mit Rest a_3 und erhalten

$$a_1 = a_2 q_2 + a_3 \quad \text{mit} \quad 0 \leqq a_3 < a_2$$

u.s.w., d.h. wir erhalten Folgen von ganzen Zahlen $(a_k)_{k=0,1,...}$, $(q_k)_{k=0,1,...}$ mit

$$a_{k-1} = a_k q_k + a_{k+1} \quad \text{mit} \quad 0 \leqq a_{k+1} < a_k.$$

Die Folge $a_0, a_1, a_2, ...$ ist strikt monoton fallend, und alle a_k sind nichtnegativ. Deshalb gibt es einen kleinsten Index n mit
$a_{n+1} = a_{n-1} - a_n q_n = 0$, d.h. $a_{n-1} = a_n q_n$. Es ist

$$\text{(nach (R1))} \quad a_n = ggT(a_n, 0) = ggT(a_n, a_{n-1} - a_n q_n) = ggT(a_n, a_{n-1}).$$

Außerdem gilt

$$\text{(nach (R1))} \quad ggT(a_k, a_{k+1}) = ggT(a_k, a_{k-1} - a_k q_k) = ggT(a_k, a_{k-1}).$$

Es folgt

$$a_n = ggT(a_0, a_1).$$

Den euklidischen Algorithmus stellen wir schematisch auch folgendermaßen dar:

$$\begin{array}{rcl} a_0 & = & a_1 q_1 + a_2 \\ a_1 & = & a_2 q_2 + a_3 \\ \vdots & & \vdots \\ a_{n-1} & = & a_n q_n \end{array}$$

d.h. an der n-ten Stelle tritt zum ersten Mal der Rest 0 auf. Dieser Algorithmus liefert auch eine explizite Darstellung des $ggT(a_0, a_1)$ in der Form

$d := ggT(a_0, a_1) = a_0x + a_1y$

mit $x, y \in \mathbb{Z}$; denn der n-te Schritt sieht in der Matrixform so aus:

$$\begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} a_{k+1} \\ a_k \end{pmatrix} = \begin{pmatrix} a_k \\ a_{k-1} \end{pmatrix} \text{ mit } 1 \leqq k \leqq n.$$

Das ergibt

$$\begin{pmatrix} a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} a_2 \\ a_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \begin{pmatrix} a_3 \\ a_2 \end{pmatrix} =$$
$$= \quad ... \quad = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} ... \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} \begin{pmatrix} 0 \\ a_n \end{pmatrix},$$

so daß also die Determinante der Matrix

$$M := \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} ... \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix}$$

gleich $(-1)^n \neq 0$ ist. M ist also invertierbar über $\mathbb{Z}$, und deshalb ist

$$M^{-1} \cdot \begin{pmatrix} a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ d \end{pmatrix}.$$

Durch Berechnung von M^{-1} erhält man $x, y \in \mathbb{Z}$ mit

$ggT(a_0, a_1) = a_0x + a_1y.$

Rechenbeispiel Zu bestimmen sind $d, x, y \in \mathbb{Z}$ mit

$d = ggT(3984007, 3980021) = 3984007 \cdot x + 3980021 \cdot y.$

Der euklidische Algorithmus liefert

$3984007 = 1 \cdot 3980021 + 3986$
$3980021 = 998 \cdot 3986 + 1993$
$3986 = 2 \cdot 1993,$

also

$d = 1993.$

Die Rechnung zeigt: $d = a_3 = 1993, q_1 = 1, q_2 = 998, q_3 = 2$. Also $M = E(1)E(998)E(2)$ mit $E(q) = \begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}$, also

$$M = \begin{pmatrix} 998 & 1997 \\ 999 & 1999 \end{pmatrix}.$$

Es gilt $\det(M) = -1$, also

$$M^{-1} = \begin{pmatrix} -1999 & 1997 \\ 999 & -998 \end{pmatrix},$$

und damit

$$1993 = 3984007 \cdot x + 3980021 \cdot y$$

mit

$x = -998$, $y = 999$.

Definition $v \in \mathbb{Z}$ heißt *kleinstes gemeinsames Vielfaches* der ganzen Zahlen $a_1, ..., a_r$; geschrieben $v = kgV(a_1, ..., a_r)$; falls v von allen a_i geteilt wird und falls jede ganze Zahl, die von allen a_i geteilt wird, von v geteilt wird.

(3.8) **Satz** (a) *Je r ganze Zahlen $a_1, ..., a_r$ haben ein kgV , das bis auf das Vorzeichen eindeutig bestimmt ist. Es ist gegeben durch*

$$\cap_{i=1}^{r}(a_i) = (kgV(a_1, ..., a_r)).$$

(b) *Für je zwei natürliche Zahlen a, b gilt*

$$ggT(a, b)kgV(a, b) = ab.$$

Beweis: (a) Wie bereits bewiesen (vgl. (3.5)) gibt es ein $v \in \mathbb{N}_0$ mit

$$\cap_{i=1}^{r}(a_i) = (v).$$

Wegen $v \in (a_i)$ für alle $i = 1, ..., r$ ist a_i ein Teiler von v für alle $i = 1, ..., r$. Ist w ein Vielfaches von a_i für alle $i = 1, ..., r$, dann gilt $w \in (a_i)$ für alle $i = 1, ..., r$, also $w \in \cap_{i=1}^{r}(a_i) = (v)$. Also ist v ein Teiler von w.

(b) Zu $d = ggT(a, b), v = kgV(a, b)$ existieren $a', b', a", b" \in \mathbb{N}_0$ sowie $x, y \in \mathbb{Z}$ mit

$$a = da', b = db', v = aa'' = bb'', d = ax + by.$$

Wegen $a/a'db', b/a'db'$ gilt nach Definition des kgV: $v/a'db'$, also $d \cdot v/da'db' = ab$. Andererseits ist $dv = (ax + by)v = (ax + by)(aa") = (ax + by)(bb") = ab(b"x + a"y)$, d.h. ab/dv.

Definition Eine *Primzahl* ist eine natürliche Zahl $p \neq 1$ mit den folgenden Eigenschaften: Ist p von der Form $p = mn$ mit $m, n \in \mathbb{N}$, dann ist $m = 1$ oder $n = 1$.

Die ersten Primzahlen sind $2, 3, 5, 7, 11, ...$

(3.9) **Satz** (Fundamentalsatz der elementaren Zahlentheorie) *Zu jeder natürlichen Zahl $n \geqq 2$ gibt es Primzahlen $p_1, ..., p_r$ (nicht notwendigerweise verschieden), so daß $n = p_1 ... p_r$. Diese Darstellung ist - bis auf die Reihenfolge der Faktoren - eindeutig.*

Die wesentliche Aussage dieses Satzes ist die Eindeutigkeitsaussage.

Beweis des Fundamentalsatzes: Zunächst beweisen wir die Existenz der Zerlegung durch Induktion über n. $n = 2$ ist eine Primzahl. Für $n > 2$ ist entweder n eine Primzahl, oder es gibt natürliche Zahlen $d, e > 1$ mit $n = d \cdot e$. Wegen $d, e < n$ folgt die Existenz der Zerlegung durch Anwendung der Induktionsannahme auf d und e.

Zum Beweis der Eindeutigkeit benutzen wir den folgenden Hilfssatz, der auf Euklid zurückgeht.

(3.10) **Hilfssatz** *Sei p eine Primzahl und seien m, n von 0 verschiedene ganze Zahlen. Wenn dann p ein Teiler von $m \cdot n$ ist, dann ist p ein Teiler von m oder von n.*

Beweis des Hilfssatzes: Angenommen p teilt mn aber nicht m, so daß also $ggT(p, m) = 1$. Gemäß (3.6) schreiben wir

$1 = ap + bm$ mit $a, b \in \mathbb{Z}$.

Es folgt

$n = n1 = apn + bmn$.

Wegen $mn = pc$ mit $c \in \mathbb{Z}$ folgt dann

$n = (an + bc)p$.

Also ist p ein Teiler von n.

Wir setzen nun den Beweis der Eindeutigkeitsaussage aus (3.3) fort: Wir nehmen dazu an, daß

$n = p_1 \cdot ... \cdot p_r = q_1 \cdot ... \cdot q_s$

mit Primzahlen $p_1, ..., p_r$; $q_1, ..., q_s$. Die Primzahl p_1 stimmt als Teiler von $q_1 \cdot ... \cdot q_s$ nach dem Hilfssatz mit einer Primzahl q_j überein. OE sei $p_1 = q_1$. Dann gilt

$p_2 \cdot ... \cdot p_r = q_2 \cdot ... \cdot q_s$,

u.s.w.

(3.11) **Satz** (Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis: Angenommen es gibt nur endlich viele Primzahlen $p_1 < ... < p_n$. Dann ist die Zahl

$P := p_1 \cdot ... \cdot p_n + 1$

durch keine der Primzahlen $p_1, ..., p_n$ teilbar, da bei Division von P durch p_i immer der Rest 1 bleibt. Also ist jede Primzahl p', die P teilt, größer als p_n. In der Faktorisierung von P gemäß dem Fundamentalsatz elementaren Zahlentheorie steht daher mindestens eine Primzahl $p' > p_n$.

Bei der Darstellung einer ganzen Zahl n als Produkt von Primzahlen ist es zweckmäßig, gleiche Faktoren zusammenfassen. Ordnet man die auftauchenden Primzahlen auch noch der Größe nach, so erhält man die sogenannte "kanonische Darstellung"

$n = \varepsilon \cdot \prod_{i=1}^{r} p_i^{n_i}$

mit Primzahlen $p_1 < p_2 < ... < p_r$, ganzen Zahlen $n_i \geq 0$ und $\varepsilon \in \{\pm 1\}$.
Jede rationale Zahl $\frac{m}{n}$ mit $m \in \mathbb{Z}, n \in \mathbb{Z} - \{0\}, ggT(m,n) = 1$, besitzt die kanonische Darstellung

$\frac{m}{n} = \varepsilon \cdot \prod_{i=1}^{r} p_i^{n_i}$

mit Primzahlen $p_1 < p_2 < ... < p_r$, ganzen Zahlen n_i und $\varepsilon \in \{\pm 1\}$.

Das Zerlegen einer ganzen Zahl in ihre Primfaktoren kann sehr schwierig sein. Bei der Überprüfung, ob eine gegebene Zahl Primzahl ist oder nicht, hilft der folgende Satz

(3.12) **Satz** *Sei $N > 1$ eine natürliche Zahl. Besitzt N keinen Primteiler $p \leqq \sqrt{N}$, dann ist N eine Primzahl.*

Beweis: Angenommen N ist keine Primzahl. Dann ist $N = xy$ mit $1 < x \leqq y < N$. Also ist $x^2 \leqq N$. Somit besitzt N Teiler, die $\leqq \sqrt{N}$ sind, also auch Primteiler $\leqq \sqrt{N}$.

Auch für Polynome in nur einer Unbestimmten mit Koeffizienten aus einem Körper ist eine Division mit Rest möglich, und viele Eigenschaften ganzer Zahlen, die auf der Division mit Rest beruhen, gelten analog für solche Polynome. Nachfolgend setzen wir den Körperbegriff, der erst in § 9 ausführlicher

behandelt wird, bereits voraus. Sei also K ein Körper, und für eine Unbestimmte X über K sei $K[X]$ die Menge aller Polynome in X mit Koeffizienten in K. Jedes $p(X) \in K[X]$ läßt sich also eindeutig in der Form

$$p(X) = a_0 + a_1X + ... + a_nX^n$$

mit $n \in \mathbb{N}_0$ und mit Koeffizienten $a_0, a_1, ..., a_n \in K$ darstellen. (Eine formale Definition von Polynomen wird in § 11 gegeben.) Wir definieren den Grad von p durch

$$grad(p) := n, \text{ falls } a_n \neq 0.$$

$p(X)$ ist das Nullpolynom genau dann, wenn alle Koeffizienten a_i gleich 0 sind. Der Grad des Nullpolynoms ist per Definition gleich $-\infty$.

(3.13) **Satz** *(*Division mit Rest für Polynome*) Seien* $p(X), s(X) \in K[X] \setminus K$ *mit* $grad(s(X)) \leqq grad(p(X))$. *Dann existieren* $q(X), r(X) \in K[X]$ *mit*

$$p(X) = q(X) \cdot s(X) + r(X)$$

mit $grad(r(X)) < grad(s(X))$ *oder* $r(X) =$ *Nullpolynom.*

Beweis: Setze $n := grad(p(X)), m := grad(s(X))$. Sei $p(X) = a_0 + a_1X + ... + a_nX^n, s(X) = b_0 + b_1X + ... + b_mX^m$. Wir beweisen die Behauptung durch Induktion über n. Für $n = 0$ ist die Behauptung klar. Sei also $n > 0$. Setze

$$p_1(X) := p(X) - c \cdot X^{n-m} \cdot s(X) \text{ mit } c := \tfrac{a_n}{b_m}.$$

Dann gilt $grad(p_1(X)) < n$. Nach Induktionsvoraussetzung gilt

$$p_1(X) = q_1(X) \cdot s(X) + r(X) \text{ mit } grad(r(X)) < m.$$

Es folgt

$$p(X) = (c \cdot X^{n-m} + q_1(X)) \cdot s(X) + r(X).$$

Rechenbeispiele

$$\begin{array}{l} (X^4 + 2X^2 + 3X + 1) : (2X^2 - X + 4) = \tfrac{1}{2}X^2 + \tfrac{1}{4}X + \tfrac{1}{8} \\ \underline{X^4 - \tfrac{1}{2}X^3 + 2X^2} \qquad\qquad\qquad\qquad \text{Rest } \tfrac{17}{8}X + \tfrac{1}{2} \\ \quad \tfrac{1}{2}X^3 + 3X + 1 \\ \quad \underline{\tfrac{1}{2}X^3 - \tfrac{1}{4}X^2 + X} \\ \qquad \tfrac{1}{4}X^2 + 2X + 1 \\ \qquad \underline{\tfrac{1}{4}X^2 - \tfrac{1}{8}X + \tfrac{1}{2}} \\ \qquad\quad \tfrac{17}{8}X + \tfrac{1}{2} \end{array}$$

Also

$$X^4+2X^2+3X+1 = (\tfrac{1}{2}X^2+\tfrac{1}{4}X+\tfrac{1}{8})(2X^2-X+4)+(\tfrac{17}{8}X+\tfrac{1}{2})$$

$$q(X) \quad \cdot \quad s(X) \quad + \quad r(X)$$

$$X^n-1 = (X^{n-1}+X^{n-2}+...+X+1)(X-1)$$

(3.14) **Folgerung** Sei $p(X) \in K[X] \setminus K$ und sei $a \in K$ eine Nullstelle von $p(X)$. Dann existiert ein $q(X) \in K[X]$ mit

$$p(X) = q(X)(X-a).$$

(3.15) **Folgerung** Jedes Polynom $p(X) \in K[X]$ hat höchstens $grad(p)$ Nullstellen in K.

Aufgaben und Beispiele

(1) **Definition durch Rekursion**: Für jedes $n \in \mathbb{N}$ ist eine Eigenschaft $p(n)$ definiert, wenn gilt:
(i) $p(1)$ ist definiert
(ii) Für alle $m \in \mathbb{N}$ gilt: Ist $p(m)$ definiert dann auch $p(m+1)$.

(2) **Peano-Axiome:** $\sigma : \mathbb{N} \to \mathbb{N}$ sei die sogenannte Nachfolger-Funktion, charakterisiert durch die *Peano-Axiome*:
(i) σ ist injektiv
(ii) Es existiert kein $n \in \mathbb{N}$ mit $\sigma(n) = 1$
(iii) Sei $S \subset \mathbb{N}$ so, daß
  (a) $1 \in S$
  (b) Wenn $n \in S$, dann ist $\sigma(n) \in S$.
Dann gilt $S = \mathbb{N}$.

(3) **Addition natürlicher Zahlen:** Für alle $m \in \mathbb{N}$ sei $\sigma^m : n \to m+n$ rekursiv wie folgt definiert:
(i) $m+1 = \sigma^m(1) = \sigma(m)$
(ii) $n+m+1 = \sigma^m(\sigma(n)) = \sigma(\sigma^m(n))$.
Durch diese beiden Festsetzungen ist $\sigma^m(n) = m+n$ für alle $n \in \mathbb{N}$ definiert; denn $\sigma^m(1)$ ist definiert, und mit $\sigma^m(n)$ ist auch $\sigma^m(\sigma(n)) = \sigma(\sigma^m(n))$ definiert, weil σ definiert ist.

(4) **Multiplikation natürlicher Zahlen:** Für alle $m \in \mathbb{N}$ sei $p_m : n \to n \cdot m$ rekursiv wie folgt definiert:
(i) $p_m(1) := m$
(ii) $p_m(\sigma(m)) := m + p_m(n) = \sigma^m(p_m(n))$.

(5) **Fibonacci-Folge** $u_1 := 1, u_2 := 2, u_n := u_{n-1} + u_{n-2}$ für $n \geqq 3$. Die so rekursiv definierte Folge heißt *Fibonacci-Folge*. Zeigen Sie:
$u_n \leqq (\frac{7}{4})^n$ für alle $n \in \mathbb{N}$.

Beweis durch Induktion über n. $n = 1 : 1 \leqq \frac{7}{4}$. $n = 2 : 2 \leqq (\frac{7}{4})^2$. $n + 2 \geqq 3 :$ $u_{n+2} = u_{n+1} + u_n$, also nach Induktionsvoraussetzung

$u_{n+2} \leqq (\frac{7}{4})^{n+1} + (\frac{7}{4})^n = (\frac{7}{4})^n(1 + \frac{7}{4})$

$\leqq (\frac{7}{4})^n(\frac{7}{4})^2 = (\frac{7}{4})^{n+2}$

denn $1 + \frac{7}{4} = \frac{11}{4} = \frac{44}{16}, (\frac{7}{4})^2 = \frac{49}{16}$.

(6) Die reelle Quadratwurzel aus einer ganzen Zahl ist entweder ganz oder irrational, d.h. nicht rational.

(7) Die reellen Zahlen $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, \sqrt{10}, ...$ sind irrational.

(8) Bestimmen Sie die 5-adische Darstellung von 6784

(9) Bestimmen Sie, wenn möglich, ganze Zahlen x, y, so daß

$3843 = 2136 \cdot x + 5097 \cdot y$

Lösung: $3843 = 2136 \cdot 71 - 5097 \cdot 29$,

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

$$\cdot \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} =$$

$$= \begin{pmatrix} 189 & 712 \\ 451 & 1699 \end{pmatrix}, \qquad \text{also}$$

$$M^{-1} = \begin{pmatrix} -1699 & 712 \\ 451 & -189 \end{pmatrix}, \text{ und somit}$$

$$M^{-1} \cdot \begin{pmatrix} 2136 \\ 5097 \end{pmatrix} = \begin{pmatrix} * \\ 3 \end{pmatrix}$$

$3 = 2136 \cdot 451 - 5097 \cdot 189$
$3843 = 3 \cdot 1281 = 2136 \cdot 451 \cdot 1281 - 5097 \cdot 189 \cdot 1281$

(10) Sei p eine Primzahl und sei $a \in \mathbb{Q} \setminus \{0\}$. Schreibe

$a = \varepsilon \cdot \prod_{i=1}^{r} p_i^{\alpha_i}$

mit paarweise verschiedenen Primzahlen p_i und mit $\alpha_i \in \mathbb{Z}, \varepsilon \in \{\pm 1\}$. Definiere $w_p(a) := \alpha_i$, falls $p = p_i$, $w_p(a) := 0$ sonst, $w_p(0) := \infty$. Auf diese Weise erhält man eine Abbildung

$w_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$,

die sogenannte p-adische Exponentenbewertung von $\mathbb{Q}$. Mit den Vereinbarungen

$\infty + \infty = \infty$, $z + \infty = \infty$ für alle $z \in \mathbb{Z}$,
$\infty > z$ für alle $z \in \mathbb{Z}$

gelten dann die folgenden Rechenregeln:

$w_p(a) = \infty$ genau dann, wenn $a = 0$
$w_p(ab) = w_p(a) + w_p(b)$ für alle $a, b \in \mathbb{Q}$
$w_p(a + b) \geqq Min\{w_p(a), w_p(b)\}$ für alle $a, b \in \mathbb{Q}$
$w_p(a + b) = Min\{w_p(a), w_p(b)\}$, falls $w_p(a) \neq w_p(b)$
$w_p(p) = 1$, $w_p(1) = 0$, $w_p(-a) = w_p(a)$

(11) Definiere für jede Primzahl p

$|a|_p := p^{-w_p(a)}$ für alle $a \in \mathbb{Q}$

und

$|a|_\infty := |a|$ für alle $a \in \mathbb{Q}$,

wobei $|a|$ der gewöhnliche Absolutbetrag von a ist. Dann gilt für alle $a \in \mathbb{Q}$:

$(\prod_{p \text{ Primzahl}} |a|_p) \cdot |a|_\infty = 1$.

(12) Bestimmen Sie für $K = \mathbb{R}$ und für $K = \mathbb{F}_2$ jeweils Polynome $q(X)$ und $r(X)$ aus $K[X]$, so daß

$X^5 + X + 1 = q(X) \cdot (X^2 + 1) + r(X)$

und $grad(r(X)) < 2$.

Lösung: Für $K = \mathbb{R} : q(X) = X^3 - X$, $r(X) = 2X + 1$
Für $K = \mathbb{F}_2 : q(X) = X^3 + X$, $r(X) = 1$.

(13) Finden Sie jeweils möglichst viele Teiler des Polynoms

$f(X) = X^6 - 2X^4 - X^2 + 2 \in K\,[X]$

in den Fällen $K = \mathbb{Q}$, $K = \mathbb{R}$ und $K = \mathbb{C}$.

Lösung: für $\mathbb{Q}$: $f(X) = (X-1)(X+1)(X^2-2)(X^2+1)$;
für $\mathbb{R}$: $f(X) = (X-1)(X+1)(X-\sqrt{2})(X+\sqrt{2})(X^2+1)$;
für $\mathbb{C}$: $f(X) = (X-1)(X+1)(X-\sqrt{2})(X+\sqrt{2})(X-i)(X+i)$

Teiler von f sind jeweils alle Produkte aus diesen Faktoren und deren skalare Vielfache.

Literatur zu §3: [BA], [BB], [BM], [DM], [F], [G], [$L1$], [$L2$], [LS], [LV], [SB]

§ 4. **Halbgruppen und Monoide**

In diesem Paragraphen behandeln wir Halbgruppen und Monoide und erwähnen ohne Beweise Zusammenhänge zwischen diesen Begriffen und formalen Sprachen und Automaten. Dabei folgen wir weitgehend entsprechenden Darstellungen in [GT], Chapter 11. Die wesentlichen Resultate stammen von S.C. Kleene [KL]. Einen Anstoß zur Untersuchung von Zusammenhängen zwischen formalen Sprachen und Automaten gab die einflußreiche Arbeit [TU] von A. Turing; vgl. dazu auch die Bemerkungen in [GT], Einleitung zu Kapitel 11. Selbstverständlich können und sollen die Ausführungen in diesem Paragraphen keine ausführliche Darstellung dieser Thematik ersetzen. Ausführliche Darstellungen findet man z.B. in [EB], [GB], [H], [HU], [KSA]. Zusammenhänge zwischen Algebra und formalen Sprachen werden auch in [CN] dargestellt.

Sei G eine Menge zusammen mit einer Verknüpfung, d.h. mit einer Abbildung

$G \times G \to G, (a,b) \to a \cdot b = ab.$

Die Verknüpfung heißt *assoziativ,* falls gilt

$(ab)c = a(bc)$ für alle $a, b, c \in G$.

Bemerkung Wenn eine Verknüpfung assoziativ ist, dann ist jedes endliche Produkt

$a_1 a_2 \cdot \ldots \cdot a_n$, $n \in \mathbb{N}$, $n \geqq 2$,

unabhängig von der Reihenfolge der Klammerung definierbar.

Definition Eine *Halbgruppe* ist eine Menge G zusammen mit einer assoziativen Verknüpfung $G \times G \to G$. Eine Halbgruppe heißt *Monoid*, falls ein sogenanntes neutrales Element $e \in G$ existiert, d.h. es gilt

$ae = a = ea$ für alle $a \in G$.

In einer Halbgruppe $G = (G, \cdot)$ definieren wir $a^1 := a$, $a^{n+1} := aa^n$ für alle $n \in \mathbb{N}$. Ist G ein Monoid, dann setzen wir $a^0 := e$.

Bemerkung: In einer Halbgruppe $G = (G, \cdot)$ gilt:

$$\begin{array}{l} a^m a^n = a^{m+n} = a^n a^m \\ \\ (a^m)^n = a^{mn} = (a^n)^m \end{array} \quad \text{jeweils für alle } a \in G \text{ und alle } m, n \in \mathbb{N}.$$

Definition Sei $M = (M, \cdot)$ ein Monoid. Ein *Teilmonoid* von M ist eine Teilmenge von M, die bezüglich der Verknüpfung in M ein Monoid ist. Jede Teilmenge $N \subset M$ *erzeugt* das Teilmonoid $\langle N \rangle = N^*$, das aus allen endlichen Produkten von Elementen aus N und e besteht.

Beispiele (1) Für jede nichtleere Menge X ist die Menge X^X aller Abbildungen $f : X \to X$ zusammen mit der Komposition $\circ$ von Abbildungen $(f, g) \to g \circ f$, ein Monoid, d.h. für alle $f, g \in X^X$ ist $g \circ f$ definiert durch $(g \circ f)(x) := g(f(x))$ für alle $x \in X$. Das neutrale Element ist die identische Abbildung $id = id_X : X \to X, id(x) = x$ für alle $x \in X$. Ähnlich ist X^X zusammen mit der Verknüpfung $(f, g) \to f\#g, (f\#g)(x) := f(g(x))$ für alle $x \in X$, ein Monoid mit dem neutralen Element id.

(2) Sei X eine nichtleere Menge und sei $\mathfrak{R}(X)$ die Menge aller Relationen auf X und sei $\cdot$ die in §1 definierte Verknüpfung von Relationen. Dann ist $(\mathfrak{R}(X), \cdot)$ ein Monoid mit dem neutralen Element, das der Relation "gleich" entspricht.

Wir erläutern nun die Rolle von Monoiden in der Theorie der formalen Sprachen und folgen dabei der Darstellung in [GT], Chapter 11, die, wie dort angemerkt wird, in wesentlichen Teilen auf [KSA] beruht. In der Theorie der formalen Sprachen geht man aus von einer nichtleeren endlichen Menge Σ, die das zugrunde gelegte *Alphabet der Sprache* genannt wird, und bildet daraus das Monoid Σ^*, das aus allen endlichen geordneten Folgen, d.h. geordneten Tupeln variabler endlicher Länge, von Elementen aus Σ sowie aus dem leeren Wort ϵ, das keinen Buchstaben enthält, besteht. Zwei solche Folgen x, y werden verknüpft, indem sie hintereinander geschrieben werden, d.h. $x \cdot y := xy$. Die Elemente aus Σ heißen *Buchstaben* und die Elemente aus Σ^* *Wörter*. Zwei Wörter aus Σ^* sind also genau dann gleich, wenn sie dieselben Buchstaben in derselben Reihenfolge enthalten. Das neutrale Element ist $\epsilon \in \Sigma^*$.

Beispiel $\Sigma = \{a, b\}$; $aababba \in \Sigma^*$

Definition Sei Σ eine nichtleere endliche Menge. Eine *formale Sprache über* Σ ist eine Teilmenge $L \subset \Sigma^*$.

Manchmal wird eine formale Sprache L über Σ als formale Reihe der folgenden Form geschrieben:

$L = \sum_{w \in \Sigma^*} (L, w)w,$

wobei $(L, w) := 1$, falls $w \in L$, und $(L, w) := 0$, falls $w \notin L$; dabei werden $0, 1$ als Elemente der in §2 eingeführten Booleschen Algebra der Wahrheitswerte $\mathbf{2} = B = (\{0, 1\}, \wedge, \vee, ', 0, 1)$ aufgefaßt. In diesem Zusammenhang schreibt man die Verknüpfungen $\wedge$ und $\vee$ in B auch in der folgenden Form: $\vee = +$, $\wedge = \cdot$, d.h. es ist $0+0 = 0, 1+0 = 0+1 = 1, 1+1 = 1, 00 = 0, 1 \cdot 0 = 0 \cdot 1 = 0, 1 \cdot 1 = 1$.

Beispiel $\Sigma = \{a.b\}$, $L = \{a, ab, b^2\} = a + ab + b^2$

Summe und Produkt formaler Sprachen über Σ sind wie folgt definiert

$U + V := \sum_{w \in \Sigma^*} ((U, w) + (V, w))w$

$UV := \sum_{s,t:w=st} (U, s)(V, t)w$

Die Wörter in $U + V$ bestehen also aus den Wörtern in $U \cup V$, und die Wörter in UV sind von der Form st, $s \in U$, $t \in V$.

Mit diesen Definitionen bilden alle formalen Sprachen über Σ eine Menge, in der Elemente addiert und multipliziert werden können; wir bezeichnen diese Menge mit

$B[[\Sigma]].$

Das neutrale Element in $B[[\Sigma]]$ bezüglich der Addition ist die sogenannte Nullsprache, d.h. alle (L, w) sind 0; und das Einselement ist ϵ, wobei $(\epsilon, w) = 1$, falls $w = \epsilon$, und $(\epsilon, w) := 0$, falls $w \neq \epsilon$. Die Elemente aus $B[[\Sigma]]$, die nur aus endlich vielen Summanden bestehen, heißen *Polynome.*

Bemerkungen (a) Für alle $U \in B[[\Sigma]]$ gilt

$U + U = U$
$U^* = \epsilon + U + U^2 + ...$
$(U^*)^* = U^*.$

Für $U = \{x\}$ schreiben wir auch

$x^* = U^*$
$x + y = \{x\} + \{y\}$
$x \cdot y = \{x\} \cdot \{y\}$.

Für die Schreibweise vereinbaren wir: * geht vor $\cdot$ und $\cdot$ geht vor $+$.

Definition Sei Σ eine nichtleere endliche Menge. Eine formale Sprache über Σ heißt *rational*, wenn sie aus ϵ und den Elementen aus Σ durch nur endlich viele Anwendungen von $+, \cdot$, und $*$ entsteht.

Bemerkung Nicht jede formale Sprache ist rational.

Zwischen formalen Sprachen und Automaten besteht ein Zusammenhang, den wir jetzt erläutern. Dazu erinnern wir zunächst an den Begriff des Automaten, vgl. §1: Ein Automat ist ein 5-Tupel $(S, X, Z, \delta, \lambda)$ mit nichtleeren Mengen S, X, Z und Abbildungen $\delta : S \times X \to S, \lambda : S \times X \to Z$; X heißt das Eingabealphabet, Z das Ausgabealphabet, δ die Übergangsfunktion, λ die Ausgabefunktion. Ein Automat $(S, X, Z, \delta, \lambda)$ heißt *endlich*, falls die Mengen S und X endlich sind.

Definition Man sagt, daß eine formale Sprache U von einem gegebenen endlichen Automaten $(S, X, Z, \delta, \lambda)$ *akzeptiert* bzw. *respektiert* wird, falls das Alphabet, über das die formale Sprache U gebildet wird, das Eingabealphabet X des Automaten ist und falls $p, q \in S$ existieren, so daß

$U =$ bzw. $U \subset \{w \in X^* : \delta(p, w) = q\}$;

dabei ist

$\delta(p, x_1 x_2 \cdots x_n) := \delta(\delta(p, x_1), x_2 \cdots x_n)$
$\delta(p, \epsilon) := p$

jeweils für alle $x_1, ..., x_n \in X$ und für alle $p \in S$.

Das Ausgabealphabet Z und die Ausgabefunktion λ des Automaten spielen in dieser Definition keine Rolle.

Beispiel $S := \{p, q\}$, $X := \{x, y, z\}$; $S \times X \xrightarrow{\delta} S$: $(p, x) \mapsto p$, $(p, y) \longmapsto q$, $(p, z) \mapsto p$, $(q, x) \mapsto q$, $(q, y) \mapsto p$, $(q, z) \mapsto q$. Einige formale Sprachen über X, die respektiert werden: $x^* : p \mapsto p$, $yx^* : p \mapsto q$, $z^* : q \mapsto q$, $x^* : q \mapsto q$. Offensichtlich wird die formale Sprache y^* nicht akzeptiert..

Für Beweise der folgenden für die Computerwissenschaften grundlegenden Resultate von Kleene verweisen wir auf [GT], Chapter 11.

(4.1) **Satz** *Die formalen Sprachen, die von einem endlichen Automaten akzeptiert werden, sind rational.*

(4.2) **Satz** *Jede rationale Sprache wird von einem geeigneten endlichen Automaten akzeptiert.*

Beispiel Sei $\Sigma := \{x\}$. Dann wird die formale Sprache $L := \{x\} \subset \Sigma^*$ von dem Automaten mit $S = \{p, q, r\}$, $X = \{x\}$ und $\delta : S \times X \to X$, $\delta(p, x) := q$, $\delta(q, x) := r$, $\delta(x, r) := r$ akzeptiert.

Aufgaben und Beispiele

(1) Geben Sie eine Halbgruppe an, die kein Monoid ist.

(2) Zeigen Sie: Für $\Sigma := \{x, y\}$ gilt in $B[[\Sigma]]$: $(x + y)^* = x^*(yx^*)^*$

(3) Bestimmen Sie die Zustandsmenge, die Eingabemenge und die Übergangsabbildung eines endlichen Automaten, der die über dem Alphabet $\{x, y\}$ definierten formalen Sprachen x^3y^*, y^*, y^*x^2 respektiert, der aber nicht x^* respektiert.

Literatur zu §4: [AB], [CN], [EB], [GB], [GT], [H], [HU], [KL], [KSA], [TU]

§ 5. **Permutationen**

In diesem Paragraphen besprechen wir grundlegende Eigenschaften von Permutationen und folgen dabei weitgehend entsprechenden Darstellungen in [BB], [BM], [GT] und vor allem in [R], Chapter 1.

Definition Sei X eine nichtleere Menge. Eine *Permutation* von X ist eine bijektive Abbildung $\alpha : X \to X$. Mit S_X bezeichnen wir die Menge aller Permutationen von X. Im Fall $X = \{1, 2, ..., n\}$ schreiben wir auch S_n statt S_X.

(5.1) **Bemerkung** Es gilt $|S_n| = n!$.

Beweis: Durch Induktion über n.

Gelegentlich schreiben wir Elemente $\alpha \in S_n$ auch in der Form

$$\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha(1) & \alpha(2) & ... & \alpha(n) \end{pmatrix}$$

(5.2) **Bemerkung** Die Komposition von Permutationen

$\circ : S_X \times S_X \to S_X, (\alpha, \beta) \to \alpha \circ \beta,$

hat die folgenden Eigenschaften:

(i) $\circ$ ist assoziativ, d.h. es gilt $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$ für alle $\alpha, \beta, \gamma \in S_X$
(ii) $\alpha \circ id = \alpha = id \circ \alpha$ für alle $\alpha \in S_X$
(iii) α^{-1} existiert für alle $\alpha \in S_X$

Im allgemeinen ist die Komposition von Permutationen nicht kommutativ:

Für $\alpha = \binom{1\ 2\ 3}{2\ 1\ 3}, \beta = \binom{1\ 2\ 3}{2\ 3\ 1} \in S_3$ gilt

$\alpha \circ \beta = \binom{1\ 2\ 3}{1\ 3\ 2}$, $\beta \circ \alpha = \binom{1\ 2\ 3}{3\ 2\ 1}$.

Definition Seien $i_1, ..., i_r \in \{1, 2, ..., n\}$ paarweise verschieden. Definiere $\alpha := (i_1, i_2, ..., i_r) := (i_1 i_2 ... i_r) \in S_n$ wie folgt:

$\alpha(i_1) = i_2, \alpha(i_2) = i_3, ..., \alpha(i_r) = i_1$
α läßt die $(n - r)$ Zahlen, die nicht zu $\{i_1, ..., i_r\}$ gehören, fest

$\alpha = (i_1 i_2 ... i_r)$ heißt *r-Zykel der Länge r*. Ein 2-Zykel heißt auch *Transposition.*

Beispiele $(15342) = \binom{1\ 2\ 3\ 4\ 5}{5\ 1\ 4\ 2\ 3}$

$(123) = (123) \circ (5) = \binom{1\ 2\ 3\ 4\ 5}{2\ 3\ 1\ 4\ 5}$

$\alpha = (12), \beta = (13425)$; dann ist

$(\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(3) = 3$
$(\alpha \circ \beta)(3) = \alpha(\beta(3)) = \alpha(4) = 4$
$(\alpha \circ \beta)(4) = \alpha(\beta(4)) = \alpha(2) = 1$
$(\alpha \circ \beta)(2) = \alpha(\beta(2)) = \alpha(5) = 5$
$(\alpha \circ \beta)(5) = \alpha(\beta(5)) = \alpha(1) = 2$,

also

$\alpha \circ \beta = (12) \circ (13425) = (134) \circ (25)$

$= \binom{1\ 2\ 3\ 4\ 5}{3\ 5\ 4\ 1\ 2}$.

Definition $\alpha, \beta \in S_X$ heißen *disjunkt*, wenn für alle $x, y \in X$ gilt:

$\alpha(x) \neq x \Rightarrow \beta(x) = x$
$\beta(y) \neq y \Rightarrow \alpha(y) = y.$

(5.3) **Satz** *Jedes $\alpha \in S_n$ ist entweder ein Zykel oder ein Produkt von paarweise disjunkten Zykeln.*

Beweis: Durch Induktion über die Anzahl k derjenigen Elemente aus der Menge $\{1, 2, ..., n\}$, die von $\alpha \in S_n$ bewegt werden. Für $k = 0$ ist $\alpha = id$. Also ist α insbesondere ein 1-Zykel. Sei $k > 0$. Dann existiert ein $i_1 \in \{1, 2, ..., n\}$ mit $\alpha(i_1) \neq i_1$. Definiere

$$i_2 := \alpha(i_1), i_3 := \alpha(i_2), ..., i_{r+1} := \alpha(i_r),$$

wobei r die kleinste natürliche Zahl mit $i_{r+1} \in \{i_1, ..., i_r\}$ ist.
Behauptung $\alpha(i_r) = i_1$.
Beweis: Andernfalls gilt $\alpha(i_r) = i_j$ für ein $j \geqq 2$. Aber $\alpha(i_{j-1}) = i_j$. Daraus folgt $i_r = i_{j-1}$, ein Widerspruch zur Wahl von r. Wir definieren $\sigma := (i_1, ..., i_r)$. Falls $r = n$, dann gilt $\alpha = \sigma$, d.h. α ist ein Zykel der Länge n. Falls $r < n$, dann setze

$$Y := \{1, 2, ..., n\} \backslash \{i_1, ..., i_r\}.$$

Es gilt: $\alpha(Y) = Y, \sigma(y) = y$ für alle $y \in Y$. Außerdem gilt:

$$\sigma_{|\{i_1,...,i_r\}} = \alpha_{|\{i_1,...,i_r\}}$$

Sei $\alpha' \in S_n$ so, daß $\alpha'_{|Y} = \alpha_{|Y}$ und daß α' die Menge $\{i_1, ..., i_r\}$ elementweise fest läßt. Dann sind σ und α' disjunkt, und es gilt

$$\alpha = \sigma \circ \alpha'.$$

α' bewegt weniger Punkte als α. Somit ist α' nach Induktionsannahme ein Produkt von paarweise disjunkten Zykeln und damit auch α.

(5.4) **Satz** *Sei $\alpha \in S_n$ und sei $\alpha = \beta_1 \circ ... \circ \beta_t$ eine vollständige Zerlegung in paarweise disjunkte Zykeln ("vollständig" heißt in diesem Zusammenhang, daß alle Ziffern vorkommen). Diese Zerlegung ist bis auf die Reihenfolge eindeutig.*

Beweis: Sei $i \in \{1, ..., n\}$ fest unter α. Dann enthält die Faktorisierung von α den Zykel (i) genau 1-mal. Deshalb reicht es, die Eindeutigkeit der in α vorkommenden Zykeln mit einer Länge $\geqq 2$ zu zeigen. Sei dazu $\alpha = \gamma_1 \circ ... \circ \gamma_s$ eine weitere vollständige Zerlegung in disjunkte Zykeln. Wenn i_1 von β_t bewegt wird, dann gilt

$$\beta_t^k(i_1) = \alpha^k(i_1) \text{ für alle } k.$$

Ein γ_j bewegt i_1 auch. OE sei $\gamma_j = \gamma_s$. Es gilt

$\gamma_s^k(i_1) = \alpha^k(i_1)$ für alle k,

also $\beta_t = \gamma_s$; denn $i_1 \in \{1, 2, ..., n\}$ ist ein beliebiges Element, das von β_t bewegt wird. Es folgt

$\gamma_1 \circ \gamma_2 \circ ... \circ \gamma_{s-1} = \beta_1 \circ ... \circ \beta_{t-1}$,

und die Behauptung ergibt sich induktiv.

(5.5) **Satz** *Jedes $\alpha \in S_n$ ist ein Produkt von Transpositionen. (Eine solche Zerlegung ist i.a. nicht eindeutig.)*

Beweis: Klar.

Definition $\alpha \in S_n$ heißt *gerade* bzw. *ungerade*, falls α als Produkt einer geraden bzw. ungeraden Anzahl von Transpositionen darstellbar ist.

Beispiel $\alpha = (123) = (13) \circ (12)$ ist gerade.

(5.6) **Hilfssatz** *Seien k, ℓ ganze Zahlen $\geqq 0$. Dann gilt*

$(ab)(ac_1...c_kbd_1...d_\ell) = (ac_1...c_k)(bd_1...d_\ell)$
$(ab)(ac_1...c_k)(bd_1...d_\ell) = (ac_1...c_kbd_1...d_\ell)$.

Beweis: Die linke Seite der ersten Gleichung bewirkt

$a \mapsto c_1 \mapsto c_1$
$c_i \mapsto c_{i+1} \mapsto c_{i+1}$ für alle $i < k$
$c_k \mapsto b \mapsto a$
$b \mapsto d_1 \mapsto d_1$
$d_j \mapsto d_{j+1} \mapsto d_{j+1}$ für alle $j < \ell$
$d_\ell \mapsto a \mapsto b$.

Und das bewirkt auch die rechte Seite.
Die zweite Gleichung folgt durch Multiplikation beider Seiten der ersten Gleichung mit (ab) von links.

Definition Für $\alpha \in S_n$ sei $\alpha = \beta_1 \circ ... \circ \beta_t$ eine vollständige Zerlegung in paarweise disjunkte Zykeln. Dann heißt

$\epsilon(\alpha) := sign(\alpha) := (-1)^{n-t}$

das *Vorzeichen* von α. Aiufgrund des obigen Satzes (5.4) ist

$\epsilon : S_n \to \{\pm 1\}$

eine wohldefinierte Abbildung, die sogenannte *Vorzeichenfunktion* oder *Signatur.*

Beispiel Ist $\tau \in S_n$ eine Transposition, dann bewegt τ zwei Ziffern i und j und läßt die restlichen $n-2$ Ziffern fest; also gilt $t = (n-2)+1 = n-1$ und damit

$$\epsilon(\tau) = (-1)^{n-t} = (-1)^{n-(n-1)} = -1.$$

(5.7) **Hilfssatz** *Ist $\beta \in S_n$ und τ eine Transposition, dann gilt*

$$\epsilon(\tau\beta) = -\epsilon(\beta)$$

Beweis: Sei $\tau = (ab)$ und sei $\beta = \gamma_1 \circ ... \circ \gamma_t$ eine vollständige Zerlegung in paarweise disjunkte Zykeln. Wenn a und b in demselben Zykel auftauchen, etwa in γ_1, dann gilt

$$\gamma_1 = (ac_1...c_k bd_1...d_\ell),\ k > 0, \ell > 0.$$

Nach (5.6) ist

$$\tau\gamma_1 = (ac_1...c_k) \circ (bd_1...d_\ell)$$
$$\tau\beta = (\tau\gamma_1) \circ \gamma_2 \circ ... \circ \gamma_t,$$

also

$$\epsilon(\tau\beta) = (-1)^{n-(t+1)} = (-1)^{n-1} \cdot (-1) = -\epsilon(\beta).$$

Wenn a und b in verschiedenen Zykeln

$$\gamma_1 = (ac_1...c_k) \quad \text{und} \quad \gamma_2 = (bd_1...d_\ell)$$

auftauchen, dann gilt nach (5.6)

$$\tau\beta = (\tau\gamma_1\gamma_2) \circ \gamma_3 \circ ... \circ \gamma_t$$
$$\tau \circ \gamma_1 \circ \gamma_2 = (ac_1...c_k bd_1...d_\ell).$$

Also hat die vollständige Faktorisierung von $\tau\beta$ einen Zykel weniger als β; somit gilt

$\epsilon(\tau \circ \beta) = (-1)^{n-(t-1)} = -\epsilon(\beta)$.

(5.8) **Satz** *Die Vorzeichenfunktion* $\epsilon : S_n \to \{\pm 1\}$ *hat die Eigenschaft* $\epsilon(\alpha \circ \beta) = \epsilon(\alpha)\epsilon(\beta)$ *für alle* $\alpha, \beta \in S_n$

Beweis: Sei $\alpha \in S_n$ und sei

$\alpha = \tau_1 \circ ... \circ \tau_m$

eine Faktorisierung von α als Produkt von Transpositionen mit minimalem m. Wir beweisen durch Induktion über m, daß

$\epsilon(\alpha \circ \beta) = \epsilon(\alpha)\epsilon(\beta)$ für alle $\beta \in S_n$.

Für $m > 1$ ist

$\tau_2 \circ ... \circ \tau_m$

ebenfalls eine Faktorisierung mit minimalem m; denn wenn $\tau_2 \circ ... \circ \tau_m = \sigma_1 \circ ... \circ \sigma_q$ mit Transpositionen σ_i und $q < m-1$, dann ist $\alpha = \tau_1 \circ \sigma_1 \circ ... \circ \sigma_q$ eine Faktorisierung von α mit kleinerer Länge als m. Also gilt

$$\begin{aligned}\epsilon(\alpha \circ \beta) &= \epsilon(\tau_1 \circ ... \circ \tau_m \circ \beta) = \text{(nach Hilfssatz (5.7))} \\ &= -\epsilon(\tau_2 \circ ... \circ \tau_m \circ \beta) = \text{(nach Induktionsannahme)} \\ &= -\epsilon(\tau_2 \circ ... \circ \tau_m)\epsilon(\beta) = \text{(nach Hilfssatz (5.7))} \\ &= \epsilon(\tau_1 \circ ... \circ \tau_m)\epsilon(\beta) = \\ &= \epsilon(\alpha)\epsilon(\beta).\end{aligned}$$

(5.9) **Folgerung** *Sei* $\alpha \in S_n$. *Dann gilt:* α *ist gerade genau dann, wenn* $\epsilon(\alpha) = +1$. α *ist ungerade genau dann, wenn* $\epsilon(\alpha) = -1$.

Aufgaben und Beispiele

(1) **Matrixdarstellung von Permutationen**: Für jedes $n \in \mathbb{N}$ sei

$$E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 1 \end{pmatrix} = (e_1, ..., e_n)$$

die Einheitsmatrix vom Grad n, geschrieben als Vektor der Spaltenvektoren

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} - i\text{-te Stelle}$$

Wir definieren eine Abbildung

$$P : S_n \to GL(n, \mathbb{Q}) \quad \text{durch} \quad P(\sigma) = (e_{\sigma(1)}, e_{\sigma(2)}, ..., e_{\sigma(n)}).$$

Zeigen Sie:
(a) P ist injektiv
(b) $P(\tau \circ \sigma) = P(\sigma)P(\tau)$ für alle $\sigma, \tau \in S_n$
(c) $\det(P(\sigma)) = \epsilon(\sigma) =$ Vorzeichen von $\sigma \in S_n$

(2) Bestimmen Sie eine vollständige Zerlegung in disjunkte Zykeln von

$$\sigma := \begin{pmatrix} 1234567 \\ 3641725 \end{pmatrix} \in S_7,$$

und bestimmen Sie das Vorzeichen von σ.

Lösung: $\sigma = (134)(26)(57), \epsilon(\sigma) = (-1)^{7-3} = +1$.

Literatur zu §5: $[BB]$, $[BM]$, $[GT]$, $[R]$

§ 6. **Gruppen**

In diesem Abschnitt besprechen wir grundlegende Eigenschaften von Gruppen und folgen dabei entsprechenden Darstellungen in Standardlehrbüchern der Algebra und der Gruppentheorie, insbesondere in $[R]$.

Definition Eine *Gruppe* ist ein Monoid $(G, \cdot)$, so daß zu jedem $a \in G$ ein Element $b \in G$ existiert mit

$$ab = e = ba,$$

wobei e das neutrale Element aus G ist.

b ist durch a eindeutig bestimmt und heißt das zu a *inverse Element*; es wird mit a^{-1} bezeichnet.

Eine Gruppe $(G, \cdot)$ heißt kommutativ oder abelsch, falls gilt

$$ab = ba$$

für alle $a, b \in G$.

Beispiele (1) Die Menge aller Permutationen einer nichtleeren Menge X ist bezüglich der Komposition von Abbildungen eine Gruppe $(S_X, \circ)$; vgl. § 5. Für $X = \{1, 2, ..., n\}$ wird diese Gruppe mit S_n bezeichnet. Im allgemeinen ist S_X nicht kommutativ; z.B. ist S_3 nicht kommutativ.

(2) $(\mathbb{Z}, +) =: \mathbb{Z}^+$ ist eine kommutative Gruppe.

(3) Für jedes $m \in \mathbb{N}$ ist $C_m := \{0, 1, ..., m-1\}$ bezüglich der wie folgt definierten Addition eine kommutative Gruppe

$a + b :=$ Rest von $a + b$ nach Division durch m.

Definition Sei $(G, \cdot)$ eine Gruppe. Eine nichtleere Teilmenge $S \subset G$ heißt *Untergruppe* von G, wenn gilt: Für alle $s, t \in S$ ist $st^{-1} \in S$.

Ist eine nichtleere Teilmenge $S \subset G$ auch Untergruppe von G, so schreiben wir $S \leqq G$.

Definition Sei $G = (G, \cdot)$ eine Gruppe und sei $X \subset G$ eine nichtleere Teilmenge. Dann ist $\langle X \rangle$ die kleinste Untergruppe von G, die X enthält. $\langle X \rangle$ heißt *die von X erzeugte Untergruppe von G.*

Bemerkung In der Situation der obigen Definition gilt $X = \cap U$, wobei der Durchschnitt über alle Untergruppen $U \leqq G$ mit der Eigenschaft $X \subset U$ erstreckt wird.

Definition Sei G eine Gruppe und sei $X \subset G$ eine nichtleere Teilmenge . Ein *Wort über X* ist ein Element $w \in G$ von der Form

$$w = x_1^{\epsilon_1} ... x_n^{\epsilon_n} \text{ mit } n \in \mathbb{N},\ x_i \in X,\ \epsilon_i \in \{\pm 1\}.$$

(6.1) **Satz** *Für jede Gruppe G und jede nichtleere Teilmenge $X \subset G$ besteht $\langle X \rangle$ aus allen Wörtern über X.*

Definition Eine Gruppe G heißt *zyklisch*, falls ein Element $a \in G$ mit $G = \langle \{a\} \rangle =: \langle a \rangle$ existiert.

Die Elemente einer zyklischen Gruppe $\langle a \rangle$ sind also von der Form a^i mit $i \in \mathbb{Z}$.

Definition Sei G eine Gruppe. Die *Ordnung eines Elementes* $a \in G$ ist definiert als die Cardinalität der von a erzeugten zyklischen Untergruppe:

$$ord(a) := |\langle a \rangle| .$$

(6.2) **Satz** *Sei G eine Gruppe und sei $a \in G$. Dann gilt: Wenn $ord(a)$ endlich ist, dann ist $ord(a)$ die kleinste natürliche Zahl m mit der Eigenschaft $a^m = e$.*

Beweis: Für $a = e$ ist $m = 1$. Sei $a \in G$, $a \neq e$. Dann existiert ein $k > 1$, so daß die Potenzen

$$e = a^0, a^1, a^2, ..., a^{k-1}$$

paarweise verschieden sind und $a^k = a^i$ für ein i mit $0 \leqq i \leqq k-1$ gilt.

Behauptung $a^k = e = a^0$.

Beweis: Wenn $a^k = a^i$ für ein $i \geqq 1$ ist, dann gilt $k - i \leqq k - 1$ und $a^{k-i} = e$, im Widerspruch dazu , daß die Potenzen $e, a, a^2, ..., a^{k-1}$ paarweise verschieden sind. Also ist k minimal mit der Eigenschaft $a^k = e$.

Behauptung $k = m$, d.h. $a = \{e, a, a^2, ..., a^{k-1}\}$.

Beweis: Offensichtlich gilt $\{e, a, a^2, ..., a^{k-1}\} \subset \langle a \rangle$. Sei $a^\ell \in \langle a \rangle$ und sei OE $k \leqq \ell$. Division mit Rest liefert $\ell = qk + r$ mit $0 \leqq r < k$. Dann ist

$$a^\ell = a^{qk} a^r = a^r,$$

weil $a^k = e$. Also ist $a^\ell = a^r \in \{e, a, a^2, ..., a^{k-1}\}$.

(6.3) **Satz** *Sei G eine endliche zyklische Gruppe der Ordnung n und sei d ein Teiler von n. Dann besitzt G eine eindeutige Untergruppe S der Ordnung d.*

Beweis: Sei a ein erzeugendes Element von G. Dann ist $\langle a^{n/d} \rangle$ eine zyklische Untergruppe der Ordnung d. S ist zyklisch, $S = \langle b \rangle$. Es gilt $b^d = e$ und $b = a^m$ für ein m. Also $md = nk$ für ein $k \in \mathbb{N}$, und dann

$$b = a^m = (a^{n/d})^k.$$

d ist ein Teiler von n. Also ist $\langle b \rangle \leqq \langle a^{n/d} \rangle$. Weil sowohl $\langle b \rangle$ als auch $\langle a^{n/d} \rangle$ die Ordnung d hat, gilt

$$\langle b \rangle = \langle a^{n/d} \rangle .$$

Definition Für jede natürliche Zahl m sei

$$\phi(m) := |\{i \in \mathbb{Z} : 0 \leqq i \leqq m-1, ggT(i,m) = 1\}|\,;$$

$\phi : \mathbb{N} \to \mathbb{N}$ heißt *Eulersche Funktion.*

(6.4) **Satz** *Sei G eine endliche zyklische Gruppe und sei $\mathcal{E}(G)$ die Menge aller erzeugenden Elemente von G. Dann gilt $|\mathcal{E}(G)| = \phi(|G|)$, wobei ϕ die Eulersche Funktion ist.*

Beweis: Sei $G = \langle a \rangle\,, |G| = n$. Dann gilt

$G = \langle a^k \rangle$ genau dann, wenn $ggT(k,n) = 1$.

Um diese Behauptung einzusehen, nehmen wir zunächst an, daß $G = \langle a^k \rangle$ ist. Angenommen es gibt eine natürliche Zahl d mit

$$k = d \cdot k_1, n = d \cdot k_2.$$

Also $k_2 < n$ und $(a^k)^{k_2} = a^{dk_1k_2} = a^{nk_1} = e$, und das steht im Widerspruch zu der Tatsache, daß die Ordnung von a^k gleich n ist.

Sei umgekehrt $ggT(k,n) = 1 = kx + ny$ mit $x, y \in \mathbb{Z}$. Angenommen es ist $a^{k\ell} = e$ mit $\ell < n$. Dann gilt

$$a^\ell = a^{(kx+ny)\ell} = a^{k\ell x} = e,$$

im Widerspruch dazu, daß a die Ordnung n hat.

Beispiele (a) Jede Gruppe von Primzahlordnung p zyklisch; denn jedes vom neutralen Element verschiedene Element einer solchen Gruppe hat ebenfalls die Ordnung p und erzeugt daher die Gruppe.

(b) Für jede natürliche Zahl m bilden die sogenannten m-ten *Einheitswurzeln* $(e^{2\pi i/m})^k, k = 0, 1, ..., m-1$; bezüglich der Multiplikation von komplexen Zahlen eine zyklische Gruppe der Ordnung m. Ihre Elemente liegen auf dem Einheitskreis und bilden die Ecken eines regulären m-Ecks. Die erzeugenden Elemente dieser Gruppe sind von der Form $(e^{2\pi i/m})^k$ mit $0 \leq k < m-1$ und $ggT(k,m) = 1$; sie heißen *primitive m-te Einheitswurzeln.*

Definition Seien $(G, \cdot), (H, \#)$ Halbgruppen. Eine Abbildung $f : G \to H$ heißt *Morphismus* oder *Homomorphismus*, falls

$$f(a \cdot b) = f(a) \# f(b) \quad \text{für alle} \quad a, b \in G.$$

(Die schreibtechnische Unterscheidung zwischen der Verknüpfung $\cdot$ in G und der Verknüpfung $\#$ in H wird häufig weggelassen.) Ein *Homomorphismus von Gruppen* ist ein Homomorphismus der zugrundeliegenden Halbgruppen.

(6.5) **Bemerkung** Sei $f : G \to G'$ ein Homomorphismus von Gruppen; sei e das neutrale Element in G und e' das neutrale Element in G'. Dann gilt

(i) $f(e) = e'$
(ii) $f(a^{-1}) = f(a)^{-1}$ für alle $a \in G$
(iii) $f(a^n) = f(a)^n$ für alle $a \in G$ und für alle $n \in \mathbb{Z}$.

Beweis: (i) $e = e \cdot e$ impliziert $f(e) = f(ee) = f(e)f(e)$, also $e' = f(e)^{-1}f(e) = f(e)^{-1}f(e)f(e) = f(e)$.
(ii) Für alle $a \in G$ gilt $aa^{-1} = e = a^{-1}a$, also $f(a)f(a^{-1}) = f(e) = e' = f(a^{-1})f(a)$, also $f(a^{-1}) = f(a)^{-1}$.
(iii) Klar nach Definition und (ii).

Beispiele (a) Die Vorzeichenfunktion $\epsilon : S_n \to \{\pm 1\}$ ist ein Homomorphismus von Gruppen, wobei $\{\pm 1\}$ die Gruppe mit der üblichen Multiplikation ist; siehe § 5, (5.8).
(b) Sei $(\mathbb{R}_{>0}, \cdot)$ die multiplikative Gruppe aller positiven reellen Zahlen und sei $(\mathbb{R}, +)$ die additive Gruppe aller reellen Zahlen. Dann sind $\log : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ und $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ - zueinander inverse - Homomorphismen von Gruppen.

Definition Ein Morphismus von Halbgruppen $f : G \to H$ heißt *Monomorphismus*, wenn er injektiv ist; *Epimorphismus*, wenn er surjektiv ist; *Isomorphismus*, wenn er bijektiv ist.

Beispiel Für jede natürliche Zahl $m \geqq 2$ ist die Abbildung

$$\mathbb{Z} \to C_m = \{0, 1, ..., m-1\},$$

die jeder ganzen Zahl den nach Division durch m entstehenden Rest zuordnet, ein Epimorphismus von Gruppen $(\mathbb{Z}, +) \to (C_m, +)$.

Definition Sei G eine Gruppe und sei $S \leqq G$ eine Untergruppe. Eine *Linkssnebenklasse von S in G* ist von der Form

$$tS := \{ts; s \in S\} \text{ mit } t \in G.$$

Eine *Rechtsnebenklasse von S in G* ist von der Form

$$St := \{st : s \in S\} \text{ mit } t \in G.$$

t heißt auch Repräsentant von tS bzw. St.

Beispiele (a) Sei G die Gruppe $(\mathbb{R}^2, +)$. Für $v \in \mathbb{R}^2$ sei $S := \{rv : r \in \mathbb{R}\}$; S ist eine Gerade. Für jedes $u \in \mathbb{R}^2$ ist $u + S$ die Gerade parallel zu S durch u.

(b) Sei G die Gruppe $(\mathbb{Z}, +)$. Für $m \in \mathbb{Z}$ sei $S := m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$. Für jedes $a \in \mathbb{Z}$ ist $a + S = \{k \in \mathbb{Z} : m \text{ teilt } k - a\}$.

(c) Sei G die symmetrische Gruppe S_3. Sei $\tau = (12)$ und $S := \langle\tau\rangle = \{1, \tau\}$. Die Rechtsnebenklassen von S in G sind

$$S = \{1, \tau\},\ S(123) = \{(123), (23)\}, S(132) = \{(132), (13)\}.$$

(6.6) **Definition und Satz** *Sei G eine Gruppe und sei $S \leqq G$ eine Untergruppe. Nennt man zwei Elemente $x, y \in G$ aequivalent bezüglich $S \leqq G$, wenn $x^{-1}y \in S$, dann erhält man auf diese Weise eine Aequivalenzrelation $\sim$ auf G, und die Aequivalenzklassen sind die Linksnebenklassen von S in G. Analoges gilt für die Rechtsnebenklassen von S in G.*

Beweis: $x \sim x$ für alle $x \in G$; denn $x^{-1}x = e \in S$, weil S als Untergruppe von G das neutrale Element aus G enthält. Sei $x \sim y$, d.h. $x^{-1}y \in S$. Dann enthält S als Untergruppe von G auch das Element $(x^{-1}y)^{-1} = y^{-1}x$, d.h. $y \sim x$. Sei $x \sim y$ und sei $y \sim z$. Mit $x^{-1}y$ und $y^{-1}z$ enthält S auch das Element $(x^{-1}y)(y^{-1}z) = (x^{-1}yy^{-1})z = x^{-1}z$, also gilt $x \sim z$.

(6.7) **Folgerung** *G ist die disjunkte Vereinigung der Linksnebenklassen von S in G, d.h.*

$$G = \dot{\bigcup_t} tS;$$

dabei wird die disjunkte Vereinigung erstreckt über ein Repräsentantensystem der Linksnebenklassen von S in G. Analoges gilt für die Rechtsnebenklassen von S in G.

Bemerkung Nach einem Resultat von P. Hall existiert zu einer gegebenen Untergruppe $S \leqq G$ ein gemeinsames Repräsentantensystem sowohl für die Menge der Rechts- als auch der Linksnebenklassen von S in G.

Definition Sei G eine Gruppe und sei $S \leqq G$ eine Untergruppe. Der *Index* $(G : S)$ von S in G ist definiert als die Cardinalität der Menge der Linksnebenklassen von S in G,

(6.8) **Satz** (Lagrange) *Sei G eine Gruppe. Für jede Untergruppe $S \leqq G$ gilt*

$$|G| = (G : S) \cdot |S|\,.$$

Beweis: Die Zuordnung $S \to tS, x \to tx$, ist eine bijektive Abbildung. Somit folgt die Behauptung aus der disjunkten Zerlegung von G in die Menge der Linksnebenklassen von S in G; vgl. (6.7).

(6.9) **Folgerung** *Wenn G endlich ist, dann ist für alle $a \in G$ die Ordnung von a ein Teiler von $|G|$.*

Beweis: Nach Definition ist die Ordnung von a gleich der Cardinalität der von a erzeugten Untergruppe, so daß die Behauptung aus dem obigen Satz von Lagrange folgt.

Definition Der *Exponent* $\exp(G)$ einer Gruppe G ist, falls sie existiert, die kleinste natürliche Zahl m, so daß $x^m = e$ für alle $x \in G$ gilt; und gleich ∞, falls eine solche natürliche Zahl m nicht existiert.

(6.10) **Satz** *Ist G eine endliche Gruppe, dann ist* $\exp(G)$ *ein Teiler von* $|G|$.

Beweis: Die Behauptung ergibt sich aus (6.8).

Definition Sei G eine Gruppe. Für Teilmengen $S, T \subset G$ sei

$$ST := \{st : s \in S, t \in T\}.$$

Wenn $S \leqq G$ eine Untergruppe ist und $T = \{t\}$, dann ist $ST = St$ eine Rechtsnebenklasse.

(6.11) **Satz** *Sei G eine endliche Gruppe und seien $S, T \leqq G$ Untergruppen. Dann gilt*

$$|ST| \cdot |S \cap T| = |S| \cdot |T|.$$

Beim Beweis greifen wir auf die folgende Beobachtung zurück.

Bemerkung Sei $f : A \to B$ eine Abbildung von Mengen. Nennt man zwei Elemente $x, y \in A$ aequivalent, wenn $f(x) = f(y)$, dann erhält man auf diese Weise eine Aequivalenzrelation auf A; denn die zugehörigen Aequivalenzklassen sind die Urbildmengen $f^{-1}(z)$ von Elementen $z \in B$.

Beweis von (6.11): Die Abbildung

$$\phi : S \times T \to ST, (s, t) \to st,$$

ist surjektiv. Also reicht es nach der obigen Bemerkung zu zeigen, daß für alle $x \in ST$

$$\left|\phi^{-1}(x)\right| = |S \cap T|$$

gilt. Dazu weisen wir nach, daß für alle $x \in sT, x = st$, Folgendes gilt

$\phi^{-1}(x) = \{(sd, d^{-1}t) : d \in S \cap T\}$.

Offensichtlich ist die rechte Seite in $\phi^{-1}(x)$ enthalten. Seien umgekehrt $(s,t),(\sigma,\tau) \in \phi^{-1}(x)$, d.h. $st = x = \sigma\tau$. Dann gilt $s^{-1}\sigma = t\tau^{-1} \in S \cap T$. Daraus folgt mit $d := s^{-1}\sigma = t\tau^{-1} : \sigma = s(s^{-1}\sigma) = sd, d^{-1}t = \tau t^{-1}t = \tau$.

Definition Sei G eine Gruppe. Eine Untergruppe $S \leqq G$ heißt *Normalteiler* oder *invariante Untergruppe*, falls $xSx^{-1} = S$ für alle $x \in G$ gilt. Ist eine Untergruppe $S \leqq G$ ein Normalteiler, dann schreiben wir $S \trianglelefteq G$.

Beispiele (a) Sei $f : G \to H$ ein Homomorphismus von Gruppen, dann ist das Bild von f, also

$Bild(f) := \mathrm{Im}(f) := f(G) := \{f(x) : x \in G\}$,

eine Untergruppe von H. Der Kern von f, also

$Kern(f) := \{x \in G : f(x) = e_H = \text{neutrales Element von } H\}$,

ist ein Normalteiler von G.
(b) Ist die Gruppe G kommutativ, dann ist jede Untergruppe von G ein Normalteiler von G.
(c) Sei G eine Gruppe. Für $a, b \in G$ heißt

$[a,b] := aba^{-1}b^{-1}$

der *Kommutator* von a und b. Man kann zeigen, daß die Menge aller Kommutatoren in G i.a. keine Untergruppe von G ist. Die Kommutatoruntergruppe G' von G ist die Untergruppe von G, die von allen Kommutatoren erzeugt wird; sie ist ein Normalteiler von G.

(6.12) **Satz und Definition** *Sei G eine Gruppe und sei $N \trianglelefteq G$ ein Normalteiler von G. Dann ist die Menge $G \setminus N$ aller Linksnebenklassen von N* bezüglich der Verknüpfung

$sN \cdot tN := stN$

eine Gruppe, die mit G/N bezeichnet wird und die Faktorgruppe von G nach N (oder modulo N) genannt wird.

Beweis: Die Normalteilereigenschaft wird zum Nachweis der Wohldefiniertheit der Verknüpfung benötigt: Sei nämlich $(sN, tN) = (s'N, t'N)$, d.h. $s^{-1}s' \in N$ und $t^{-1}t' \in N$. Dann ist $(st)^{-1}s't' = t^{-1}s^{-1}s't' = nt^{-1}t'$ mit einem Element $n \in N$ und $nt^{-1}t' \in N$; also $stN = s't'N$:
Das Nachrechnen der Gruppengesetze für die Verknüpfung bereitet keine Schwierigkeiten.

(6.13) **Satz** (Erster Isomorphiesatz) *Sei $f : G \to H$ ein Homomorphismus von Gruppen und sei $K := Kern(f)$. Dann ist K ein Normalteiler von G, und die Zuordnung $aK \to f(a)$ induziert einen Isomorphismus*

$$G/K \stackrel{\cong}{\to} Bild(f)$$

Beweis: Klar.

Definition Sei G eine Gruppe und seien H und K Untergruppen von G. $H \vee K$ sei die von $H \cup K$ erzeugte Untergruppe von G.

(6.14) **Hilfssatz** *Sei G eine Gruppe und seien $S, T \leqq G$ Untergruppen von G. Wenn dann S oder T normal ist, dann ist $ST = S \vee T = TS$.*

Beweis: $ST = \{st : s \in S, t \in T\}$. Es folgt $S \cup T \subset ST, TS \subset S \vee T$. Es reicht zu zeigen: ST, TS sind Untergruppen. Dann folgt nämlich $ST = S \vee T = TS$, weil $S \vee T$ nach Definition die kleinste Untergruppe ist, die $S \cup T$ enthält. Um zu zeigen, daß ST und TS Untergruppen sind, benutzen wir die Voraussetzung, daß $T \trianglelefteq G$ ein Normalteiler ist. Wenn $s_1t_1, s_2t_2 \in ST$, dann ist $(s_1t_1)(s_2t_2)^{-1} = s_1t_1t_2^{-1}s_2^{-1} = s_1(s_2^{-1}s_2)t_1t_2^{-1}s_2^{-1} = s_1s_2^{-1}t_3$ mit $t_3 \in T$, also $s_1s_2^{-1}t_3 \in ST$.

(6.15) **Satz** (Zweiter Isomorphiesatz) *Sei G eine Gruppe, seien $N, T \leqq G$ Untergruppen und sei N ein Normalteiler. Dann ist $N \cap T$ ein Normalteiler von T, und die Einschränklung der Abbildung $\nu : G \to G/N, x \to xN$, auf T induziert einen Isomorphismus*

$$T/(N \cap T) \stackrel{\cong}{\to} NT/N.$$

Beweis: $\nu' := \nu_{|T}$ ist ein Homomorphismus mit dem Kern $N \cap T$. Daraus ergibt sich, daß $N \cap T$ ein Normalteiler von T ist, und nach dem ersten Isomorphiesatz induziert ν' einen Isomorphismus $T/(N \cap T) \cong$Bild(ν'). Außerdem ist Bild(ν') die Menge aller Linksnebenklassen von N mit Repräsentanten in T, d.h. das Bild von ν' ist NT/N.

(6.16) **Satz** (Dritter Isomorphiesatz) *Sei G eine Gruppe und seien K, H Normalteiler von G mit $K \leqq H$. Dann ist H/K ein Normalteiler in G/K, und die Abbildung $f : G/K \to G/H, aK \to aH$, induziert einen Isomorphismus*

$$(G/K)/(H/K) \stackrel{\cong}{\to} G/H.$$

Beweis: Aufgrund der Voraussetzung $K \leqq H$ ist f wohldefiniert. Außerdem ist f nach Konstruktion surjektiv und hat den Kern H/K. Die Behauptung folgt aus dem ersten Isomorphiesatz.

(6.17) **Satz** (Korrespondenzsatz) *Sei G eine Gruppe und sei $K \trianglelefteq G$ ein Normalteiler. Sei $\nu : G \to G/K$ die Abbildung $x \to xK$. Dann ist die Zuordnung*

$S \to \nu(S)$

eine bijektive Abbildung zwischen der Menge aller Untergruppen $S \leqq G$ mit $K \leqq S$ und der Menge aller Untergruppen von G/K.

Beweis Klar.

(6.18) **Satz** *Sei $G = \langle a \rangle$ eine zyklische Gruppe mit dem erzeugenden Element a. Dann ist die Abbildung*

$f : (\mathbb{Z}, +) \to G,\ n \mapsto a^n$

ein surjektiver Homomorphismus von der additiven Gruppe $(\mathbb{Z}, +)$ in die Gruppe G. (Im Folgenden schreiben wir auch $\mathbb{Z}^+$ an Stelle von $(\mathbb{Z}, +)$.)

Beweis: Klar.

Wir diskutieren die Bedingungen $\mathrm{Kern}(f) = 0$ und $\mathrm{Kern}(f) \neq 0$ nacheinander.

1-ter Fall: $\mathrm{Kern}(f) = 0$. Dann ist f ein Isomorphismus $\mathbb{Z}^+ \stackrel{\cong}{\to} G$.

2-ter Fall: $\mathrm{Kern}(f) \neq \{0\}$. Sei d die kleinste natürliche Zahl im Kern von f. Wir behaupten, daß Kern $(f) = \langle d \rangle$. Sei dazu $m \in \mathrm{Kern}(f)$. Dann gilt $m = q \cdot d + r$ mit $r < d$. Es folgt $r = m - qd \in \mathrm{Kern}(f)$. Also $r = 0$ nach Wahl von d. Somit gilt $m = q \cdot d \in \langle d \rangle$.

Also induziert f nach dem ersten Isomorphiesatz einen Isomorphismus

$\mathbb{Z}^+/d\mathbb{Z}^+ \stackrel{\cong}{\to} G = \{e, a, a^2, ..., a^{d-1}\}$.

Wir formulieren das Ergebnis in dem folgenden Satz.

(6.19) **Satz** *Sei G eine zyklische Gruppe. Dann ist entweder G isomorph zu $\mathbb{Z}^+$, oder es existiert ein $d \in \mathbb{N}$, so daß G isomorph zu $\mathbb{Z}^+/d\mathbb{Z}^+$ ist.*

(6.20) **Satz** *Für alle natürlichen Zahlen n gilt*

$n = \sum_{d/n} \phi(d)$.

Beweis: Sei G eine Gruppe der Ordnung $n < \infty$, und für jede zyklische Untergruppe $C \leqq G$ sei $\mathcal{E}(C)$ die Menge ihrer erzeugenden Elemente. Dann gilt

$$G = \cup_{\substack{C \leqq G \\ C \text{ zyklisch}}} \mathcal{E}(C)$$

Sei nun G zyklisch. Nach (6.3) existiert zu jedem Teiler d von n genau eine zyklische Untergruppe C_d der Ordnung d. Also gilt

$n = |G| = \sum_{d/n} |\mathcal{E}(C_d)| = \sum_{d/n} \phi(d)$,

weil nach (6.4) $\phi(d) = |\mathcal{E}(C_d)|$.

(6.21) **Satz** *Sei G eine endliche Gruppe der Ordnung n. Dann gilt: G ist zyklisch genau dann, wenn zu jedem Teiler d von n höchstens eine zyklische Untergruppe von G der Ordnung d existiert.*

Beweis: Wenn G zyklisch ist, dann folgt die Behauptung aus (6.3).
Umgekehrt: Wegen

$$G = \dot{\bigcup}_{\substack{C \leqq G \\ C \text{ zyklisch}}} \mathcal{E}(C)$$

gilt

$$n = \sum_{\substack{C \leqq G \\ C \text{ zyklisch}}} |\mathcal{E}(C)|.$$

Aus der Voraussetzung folgt

$$\sum_{\substack{C \leqq G \\ C \text{ zyklisch}}} |\mathcal{E}(C)| \leqq \sum_{d/n} \phi(d).$$

Nach (6.20) gilt

$n = \sum_{d/n} \phi(d)$. Also

$$n = \sum_{\substack{C \leqq G \\ C \text{ zyklisch}}} |\mathcal{E}(C)| \leqq \sum_{d/n} \phi(d) = n.$$

Daraus folgt, daß zu jedem Teiler d von n eine zyklische Untergruppe der Ordnung d von G existiert. Insbesondere hat G eine zyklische Untergruppe der Ordnung $d = n$. Also ist C zyklisch.

Definition Seien $(G_1, \cdot), (G_2, \#)$ Gruppen. Dann ist $G_1 \times G_2$ bezüglich der Verknüpfung

$(x_1, x_2) \circ (y_1, y_2) := (x_1 \cdot y_1, x_2 \# y_2)$

eine Gruppe, das sogenannte *direkte Produkt von* $(G_1, \cdot)$ *mit* $(G_2, \#)$.

Beispiel $(\mathbb{Z}/2\mathbb{Z},+)\times(\mathbb{Z}\mathbb{Z}/3,+)\mathbb{Z}$ ist eine zyklische Gruppe der Ordnung 6.

Allgemeiner: Sind m,n teilerfremde natürliche Zahlen, dann ist $(\mathbb{Z}/m\mathbb{Z},+)\times(\mathbb{Z}/n\mathbb{Z},+)$ eine zyklische Gruppe der Ordnung mn.

(6.22) **Satz** *Jede endliche Untergruppe G der multiplikativen Gruppe eines Körpers K ist zyklisch.*

Zum Beweis von (6.22) benötigen wir den folgenden Hilfssatz:

(6.23) **Hilfssatz** *Sei G eine endliche abelsche Gruppe. Dann teilt die Ordnung jedes Elementes g von G das Maximum m der Ordnungen aller Elemente von G.*

Beweis des Hilfssatzes: Seien $ord(g)=\prod p^{\mu_p}, m=\prod p^{\nu_p}$ die Primzahlzerlegungen von $ord(g)$ und m. Sei $h\in G$ so, daß $m=ord(h)$. Angenommen $ord(g)$ ist kein Teiler von m. Dann gibt es eine Primzahl p mit $\mu_p>\nu_p$. Schreibt man $ord(g)=p^{\mu_p}n', m=p^{\nu_p}m'$, dann ist $ord(g^{n'})=p^{\mu_p}, ord(h^{\nu_p})=m'$, und es gilt $ggT(p^{\mu_p},m')=1$. Somit $ord(g^{n'}h^{\nu_p})=p^{\mu_p}m'>p^{\nu_p}m'=m$; Widerspruch!

Beweis von (6.22): Sei m das Maximum aller Ordnungen aller Elemente von G. Für alle $x\in G$ mit $ord(x)=m$ gilt $x^m-1=0$. Aufgrund von (6.23) ist $ord(g)$ für jedes $g\in G$ ein Teiler von m, so daß also $g^m-1=0$ gilt. Jedes $g\in G$ ist also Nullstelle des Polynoms $X^m-1\in K[X]$. Nach (3.15) hat dieses Polynom höchstens m Nullstellen in K. Somit gilt $|G|\le m=ord(g)\le|G|$, und damit $G=\langle g\rangle$.

Die beiden folgenden Sätze ergeben sich aus (9.30).

(6.24) **Satz** *Sei G eine abelsche Gruppe, die von endlich vielen Elementen erzeugt wird. Dann ist G isomorph zu einem direkten Produkt von zyklischen Gruppen.*

(6.25) **Satz** *Jede endliche abelsche Gruppe ist isomorph zu einem direkten Produkt von zyklischen Gruppen, deren jeweilige Ordnungen Primzahlpotenzen sind.*

Nun besprechen wir eine auf van der Waerden zurückgehende Konstruktion der freien Gruppe und folgen dabei der entsprechenden Darstellung in [R], Chapter 11.

Definition Sei F eine Gruppe und sei $X\subset F$ eine Teilmenge. Dann heißt F *freie Gruppe mit Basis* X, falls für jede Gruppe G und für jede Abbildung $f:X\to G$ genau ein Homomorphismus $\varphi:F\to G$ existiert, der f fortsetzt, d.h. für den $\varphi_{|X}=f$ gilt.

Sei X eine Menge und sei X^{-1} eine zu X disjunkte Menge, die zu X bijektiv ist und sei $X \to X^{-1}, x \mapsto x^{-1}$, irgendeine bijektive Abbildung. Sei außerdem X' eine einelementige Menge, die zu $X \cup X^{-1}$ disjunkt ist, etwa $X' = \{1\}$. Schreibe für $x \in X$ auch $x^1 := x, x^0 := 1$.

Definition Ein *Wort über* X ist eine geordnete Folge $w = (a_1, a_2, ...)$ mit $a_i \in X \cup X^{-1} \cup \{1\}$, so daß ab einem gewissen Index i alle a_j, $j \geq i$, gleich 1 sind. $(1, 1, ...)$ heißt das *leere Wort* und wird mit $\mathtt{1}$ bezeichnet.

Nichtleere Wörter w schreiben wir auch in der folgenden Form

$w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdot ... \cdot x_n^{\epsilon_n}$, $x_i \in X$, $\epsilon_i \in \{+1, -1, 0\}$, $\epsilon_n \in \{\pm 1\}$.

n heißt die *Länge* von w. Das leere Wort hat die Länge 0.

Definition Ein Wort w über X heißt *reduziert*, falls es leer ist oder falls $w = x_1^{\epsilon_1} \cdot ... \cdot x_n^{\epsilon_n}$ mit $x_i \in X$, $\epsilon_i \in \{\pm 1\}$, wobei x_i und x_i^{-1} für keinen auftauchenden Index i benachbart sind. Ein *Teilwort* von $w = x_1^{\epsilon_1} \cdot ... \cdot x_n^{\epsilon_n}$ ist von der Form $v = x_1^{\epsilon_1} \cdot ... \cdot x_j^{\epsilon_1}$ mit $1 \leq j \leq n$. Die *Multiplikation* $\circ$ *von Wörtern* ist wie folgt definiert:

$$(x_1^{\epsilon_1} \cdot ... \cdot x_n^{\epsilon_n}) \circ (y_1^{\epsilon_1} \cdot ... \cdot y_m^{\epsilon_m}) := x_1^{\epsilon_1} \cdot ... \cdot x_n^{\epsilon_n} y_1^{\epsilon_1} \cdot ... \cdot y_m^{\epsilon_m}.$$

Die *Multiplikation wu von reduzierten Wörtern (Juxtaposition)* w, u ist wie folgt definiert: wu ist das reduzierte Wort, das aus der obigen Multiplikation $w \circ u$ nach Reduktion entsteht.

Für reduzierte Wörter w, u gilt $wu = w'u''$, wobei $w = w'v$ mit einem Teilwort v von w, so daß v^{-1} ein Teilwort von u ist, etwa $u = v^{-1}u''$, und so daß $w'u''$ reduziert ist.

(6.26) **Satz** *Sei X eine nichtleere Menge. Dann existiert eine freie Gruppe F mit Basis X.*

Beweis: Sei F die Menge aller reduzierten Wörter über X. Wir zeigen mit einer Methode, die von van der Waerden stammt, daß F eine freie Gruppe mit Basis X ist, wenn man als Gruppenmultiplikation die Multiplikation von reduzierten Wörtern nimmt. Schwierigkeiten macht das Nachprüfen des Assoziativgesetzes. Diese Schwierigkeiten wurden von van der Waerden dadurch beseitigt, daß er jedem $x \in X$ die wie folgt definierten Permutationen

$$|x| : F \to F, \quad \left|x^{-1}\right| : F \to F$$

zuordnet: Für $\epsilon \in \{\pm 1\}$ ist $|x^\epsilon|\,(x_1^{\epsilon_1} \cdot ... \cdot x_n^{\epsilon_n}) := x^\epsilon x_1^{\epsilon_1} \cdot ... \cdot x_n^{\epsilon_n}$, falls $x^\epsilon \neq x_1^{-\epsilon_1}$, und $|x^\varepsilon|\,(x_1^{\varepsilon_1} \cdot ... \cdot x_n^{\varepsilon_n}) := x_2^{\epsilon_2} \cdot ... \cdot x_n^{\epsilon_n}$, falls $x^\epsilon = x_1^{-\epsilon_1}$. Es gilt

$$|x^{\epsilon}| \circ |x^{-\epsilon}| = id_F : F \to F$$

$$|x^{-\epsilon}| \circ |x^{\epsilon}| = id_F : F \to F.$$

Somit ist $|x^{\epsilon}|$ eine Permutation von F mit der inversen Permutation $|x^{-\epsilon}|$. Sei $\mathfrak{F}$ die Untergruppe der symmetrischen Gruppe S_F von F, die durch die zu X bijektive Menge $[X] := \{|x| : x \in X\}$ erzeugt wird. Wir behaupten: $\mathfrak{F}$ ist eine freie Gruppe mit Basis $[X]$. Um das einzusehen, bemerken wir zunächst, daß sich jedes $g \in \mathfrak{F}$ in eindeutiger Weise in der Form

$$g = |x_1^{\epsilon_1}| \circ |x_2^{\epsilon_2}| \circ ... \circ |x_n^{\epsilon_n}|$$

mit $\epsilon_i \in \{\pm 1\}$ so darstellen läßt, daß $|x^{\epsilon}|$ und $|x^{-\epsilon}|$ nie benachbart sind. Um nun zu zeigen, daß $\mathfrak{F}$ frei mit Basis $[X]$ ist, sei G eine Gruppe und sei $f : [X] \to G$ eine Abbildung. Definiert man für $g \in \mathfrak{F}$

$$\varphi(g) := \varphi(|x_1|^{\epsilon_1} \circ ... \circ |x_n|^{\epsilon_n}) := f(|x_1^{\epsilon_1}|) \cdot ... \cdot f(|x_n^{\epsilon_n}|);$$

dann ist dadurch eine Abbildung $\varphi : \mathfrak{F} \to G$ mit der Eigenschaft $\varphi_{|[X]} = f$ definiert.

Wir zeigen nun, daß φ ein Homomorphismus ist; daraus ergibt sich dann die Eindeutigkeit von φ mit der Eigenschaft $\varphi_{|[X]} = f$. Sind w, u reduzierte Wörter über $[X]$, dann gilt $\varphi(w \circ u) = \varphi(w)\varphi(u)$, wenn das Wort wu, das aus $w \circ u$ durch Weglassen der vertikalen Striche entsteht, reduziert ist. Im allgemeinen schreibe $w = w' \circ v, u = v^{-1} \circ u''$ wie in der Definition der Juxtaposition. Dann ist $\varphi(w) = \varphi(w')\varphi(v), \varphi(u) = \varphi(v^{-1})\varphi(u'') = \varphi(v)^{-1}\varphi(u'')$, weil $w' \circ v$ und $v^{-1} \circ u''$ reduziert sind. Also $\varphi(w)\varphi(u) = \varphi(w')\varphi(v)\varphi(v)^{-1}\varphi(u'')$. Andererseits gilt $\varphi(w \circ u) = \varphi(w' \circ u'') = \varphi(w')\varphi(u'')$, weil $w' \circ u''$ reduziert ist. Somit ist φ ein Homomorphismus. Die Abbildung $\rho : \mathfrak{F} \to F$, $|x_1^{\epsilon_1}| \circ ... \circ |x_n^{\epsilon_n}| \mapsto x_1^{\epsilon_1} ... x_n^{\epsilon_n}$ ist eine Bijektion mit der Eigenschaft $\rho([X]) = X$. Wir übertragen die Gruppenstruktur von $\mathfrak{F}$ mit Hilfe von ρ auf F und erkennen F als freie Gruppe mit Basis X. Damit ist der Beweis des Satzes beendet.

(6.27) **Folgerung** Jede Gruppe G ist Faktorgruppe einer freien Gruppe F.

Beweis: Sei X die Menge aller Elemente der Gruppe G und sei F die freie Gruppe mit Basis X. Die identische Abbildung $id : X \to G$ läßt sich zu einem Epimorphismus $\varphi : F \to G$ fortsetzen, so daß die Einbettung $X \hookrightarrow F$ gefolgt von φ mit $id : X \to G$ übereinstimmt.

Definition Sei X eine nichtleere Menge und sei Δ eine Menge von Wörtern über X. Eine Gruppe G hat *Erzeugende X und Relationen* Δ, falls G isomorph zu F/R ist, wobei F die freie Gruppe ,mit Basis X ist und wobei R die durch Δ erzeugte normale Untergruppe ist, d.h. R ist der Durchschnitt aller Normalteiler von F, die Δ enthalten. Das Paar (X, Δ) heißt auch *Presentation von G*; sind

dabei X und Δ endliche Mengen, so heißt (X, Δ) eine *endliche Presentation von* G.

Diese Konzeption geht auf W. van Dyck zurück.

Wir benutzen für $r \in \Delta$ auch die Bezeichnung $r = 1$ und für eine Präsentation (X, Δ) von G auch die Schreibweise $G = \langle X : r = 1 \text{ für alle } r \in R\rangle$, wobei man für $r = 1$ häufig auch dazu aequivalente Identitäten hinschreibt.

Beispiele (1) Sei $F = \langle x\rangle$ die freie Gruppe mit Bais $X = \{x\}$ Dann besitzt die zyklische Gruppe $(\mathbb{Z}/d\mathbb{Z}, +)$ der Ordnung d die Präsentation
$\langle x\rangle \,/\, \langle x^d\rangle$.
Eine Präsentation einer Gruppe ist nicht eindeutig bestimmt. So besitzt die zyklische Gruppe $(\mathbb{Z}/6\mathbb{Z}, +)$ der Ordnung 6 auch die Präsentation

$$\left\langle x, y : x^3 = 1, y^2 = 1, xyx^{-1}y^{-1} = 1\right\rangle.$$

(2) Die *Diedergruppe* D_{2n} der Ordnung $2n$ besitzt die Präsentation

$$\left\langle x, y : x^n = 1, y^2 = 1, yxy = x^{-1}\right\rangle.$$

(3) Die *Quaternionengruppe* Q_8 der Ordnung 8 besitzt die Präsentation

$$\left\langle x, y : x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1}\right\rangle.$$

(4) Die im Zusammenhang mit der Theorie der Zöpfe von E. Artin $[A1], [A2]$ eingeführte *Zopfgruppe* $\mathfrak{Z}_n$ besitzt die Präsentation

$$\left\langle \begin{array}{c} \sigma_1, ..., \sigma_{n-1} : \sigma_i\sigma_j = \sigma_j\sigma_i \text{ für alle } i, j \text{ mit } 1 \le i, j \le n-1 \\ \text{und } j \ne i \pm 1,\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ für alle } i \text{ mit } 1 \le i \le n-2 \end{array} \right\rangle.$$

(6.28) **Anwendung** Nachfolgend erläutern wir die Grundidee einer Anwendung der Gruppentheorie auf die Verschlüsselungstheorie, vgl. z.B. $[BBFR]$, $[GA]$, $[KA]$. Angenommen eine Person Y möchte eine geheim zu haltende Nachricht über einen öffentlich zugänglichen Kanal an eine Person X senden. Dazu wählt sie eine endlich präsentierte nichtkommutative Gruppe G, deren Elemente durch Wörter gegeben sind, und identifiziert die zu übermittelnde geheime Nachricht mit einem Element w aus G. Angenommen G besitzt Untergruppen A, B, die elementweise kommutieren, d.h. es gilt $gh = hg$ für alle $g \in A$ und alle $h \in B$. Unter solchen Paaren von Untergruppen wählen

die Personen X und Y ein Paar A, B aus und halten es geheim. Y wählt willkürlich zwei Elemente $a, b \in A$ und sendet das Element $awb \in G$ über den öffentlich zugänglichen Kanal an X. X wählt sodann willkürlich zwei Elemente $c, d \in B$ und sendet das Element $cawbd$ zurück an Y. Da die Untergruppen A, B nach Voraussetzung elementweise kommutieren, ist $cawbd = acwdb$. Y multipliziert jetzt das Element $cawbd$ von links mit a^{-1} und von rechts mit b^{-1} und erhält das Element cwd, das er an X zurücksendet. X multipliziert dieses Element von links mit c^{-1} und von rechts mit d^{-1} und erhält schließlich die geheime Nachricht w. Der Nutzen dieses Verfahrens liegt darin, daß die geheime Nachricht w selbst nicht gesendet wird, sondern lediglich veschlüsselte Formen von w, nämlich $awb, cawbd, cwd$. Offensichtlich hängt die Güte dieses Verschlüsselungsverfahrens entscheidend von der Wahl von G und den elementweise kommutierenden Untergruppen A und B ab. In diesem Zusammenhang hat man zeitweise Artinsche Zopfgruppen eingesetzt, dann aber auch andere Gruppen in Betracht gezogen.

Aufgaben und Beispiele

(1) Für $n \in \mathbb{N}$ sei $W_n := \{z \in \mathbb{C} : z^n = 1\}$. Zeigen Sie, daß W_n eine zyklische Gruppe der Ordnung n ist, und geben Sie alle erzeugenden Elemente von W_n an.

(2) Zeigen Sie, daß $\mathbb{R}^* \times \mathbb{R}$ mit der folgenden Verknüpfung eine Gruppe ist: $(a, b)(c, d) := (ac, ad + b)$.

(3) Sei M eine Menge. Zeigen Sie, daß die Potenzmenge $\mathcal{P}(M)$ bezüglich der Verknüpfung

$$S + T := (S \cup T) \setminus (S \cap T)$$

eine kommutative Gruppe vom Exponenten 2 ist.

(4) Gegeben seien die Gruppen $G := (\mathbb{R}, +)$ und $H := (\mathbb{C}^*, \cdot)$. Zeigen Sie, daß die Abbildung

$$f : \mathbb{R} \to \mathbb{C}^*, x \to f(x) := e^{2\pi i x},$$

ein Homomorphismus von Gruppen $G \to H$ ist. Bestimmen und skizzzieren Sie sowohl den Kern als auch das Bild von f. Was besagt der erste Isomorphiesatz der Gruppentheorie in der vorliegenden Situation?

(5) Sei G eine Gruppe, so daß zu jedem Element $g \in G$ eine natürliche Zahl n mit $g^n = e$ existiert. Dann gilt für jeden Homomorphismus $f : G \to \mathbb{C}^*$: $|f(g)| = 1$ für alle $g \in G$.

(6) Sei k ein Körper und für jedes $n \in \mathbb{N}$ sei

$GL(n,k) := \{A : A$ ist eine Matrix mit Koeffizienten in k, $\det(A) \neq 0\}$.

Zeigen Sie, daß $GL(n,k)$ bezüglich der Matrixmultiplikation eine Gruppe ist.

(7) Sei M eine Menge und sei G eine Gruppe. Zeigen Sie: Ist $f : M \to G$ eine bijektive Abbildung, dann gibt es auf M eine Gruppenstruktur, so daß f ein Isomorphismus von Gruppen ist.

(8) (Vgl. z.B. [F], Abschnitt 25) Sei d eine natürliche Zahl, die kein Quadrat ist, und sei $\mathcal{L} := \{(x,y) \in \mathbb{R}^2 : x > 0, x^2 - dy^2 = 1\}$. Definieren Sie auf $\mathcal{L}$ eine Gruppenstruktur, so daß die Gruppe $\mathcal{L}$ isomorph zur Gruppe $(\mathbb{R}, +)$ ist.

(Hinweise: $(x,y) \in \mathcal{L}$ identifiziere man mit der (2×2)-Matrix $\begin{pmatrix} x & dy \\ y & x \end{pmatrix}$ und nehme auf $\mathcal{L}$ die durch Matrixmultiplikation induzierte Verknüpfung. $\mathcal{L}$ ist geometrisch eine Hyperbel. Also benutzt man die Hyperbelfunktionen und definiert die Abildung

$(\mathbb{R}, +) \to \mathcal{L}, t \to (\cosh(t), \frac{1}{\sqrt{d}} \sinh(t))$.

Die Surjektivität sieht man so: $t := \log(x + y)$ für $y \geqq 0, t := \log(x - y)$ für $y < 0$. Dann gilt $t \mapsto (x,y)$.)

(9) Bestimmen Sie alle Elemente aus W_6, die W_6 erzeugen, und stellen Sie diese geometrisch dar.

(Erinnerung: $W_n := \{z \in \mathbb{C} : z^n = 1\}$ ist bezüglich der Multiplikation in $\mathbb{C}$ eine zyklische Gruppe der Ordnung n, die sogenannte Gruppe der n-ten Einheitswurzeln.)

Antwort:

$\frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}$ erzeugen $W_6 = \{+1, -1, \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}\}$.

(10) Sei $n \geqq 3$ und seien $\sigma, \tau \in S_n$ wie folgt definiert:

$$\sigma := \begin{pmatrix} 1 & 2 & \ldots & n \\ 2 & 3 & \ldots & 1 \end{pmatrix}, \tau := \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 1 & n & \ldots & 3 & 2 \end{pmatrix}.$$

Die von $\{\sigma, \tau\}$ erzeugte Untergruppe D_{2n} von S_n heißt Diedergruppe der Ordnung $2n$. Sie ist isomorph zur Symmetriegruppe eines regulären n-Ecks: σ erzeugt die Drehgruppe des n-Ecks, τ entspricht der Spiegelung des n-Ecks an einer Geraden.

Literatur zu §6: [A1], [A2], [BBFR], [BS], [F], [GA], [KA], [R]

§ 7. **Charaktere endlicher abelscher Gruppen und die endliche Fouriertransformation**

Die Grundidee dieses Abschnitts, die von C.F. Gauß (1777-1855) stammt, besteht darin, zu einer vorgegebenen natürlichen Zahl $N \geq 2$ den natürlichen Zahlen $k \in \{0, 1, ..., N-1\}$ die komplexen Zahlen $e^{2\pi ik/N}$ zuzuordnen. Damit wird das Rechnen mit Kongruenzen in das Rechnen mit komplexen Zahlen übersetzt. Es gilt nämlich $k \equiv k' \bmod N$ genau dann, wenn $e^{2\pi ik/N} = e^{2\pi ik'/N}$. Diese "Transformation" von natürlichen Zahlen in komplexe Zahlen ist Spezialfall eines Dualitätsprinzips, das viele Bereiche der Mathematik und des Denkens überhaupt durchzieht und das häufig zu neuen Erkenntnissen führt. Besonders eindrucksvoll kommt die Wirkungsweise dieses Prinzips nicht nur in der Zahlentheorie sondern auch in den Arbeiten von L. Euler (1707-1783) zur mathematischen Beschreibung von Schwingungen, in den Arbeiten von J.B.J. Fourier (1788-1830) zur mathematischen Beschreibung der Wärmeleitung sowie in der Quantenmechanik bei dem Übergang von der orts- zur impulsabhängigen Sichtweise zum Ausdruck. Die Transformation, die bei den genannten Beispielen angewandt wird, ist jeweils eine sogenannte Fouriertransformation. Wir behandeln in diesem Abschnitt eine endliche Version dieser Transformation, die für Teilbereiche der Informatik von großer Bedeutung ist. Dabei folgen wir weitgehend den entsprechenden Darstellungen in [AT]; [DMK], Chapter 4, insbesondere 4.5; [GT], Chapter 4.

Sei G eine endliche abelsche Gruppe.

Definition Ein *Charakter* von G ist ein Homomorphismus von G in die multiplikative Gruppe $\mathbb{C}^*$ von $\mathbb{C}$. Sei

$$\widehat{G} := Hom(G, \mathbb{C}^*)$$

die Menge aller Charaktere von G; $\widehat{G}$ ist eine Gruppe bezüglich der Verknüpfung

$(\chi \cdot \chi')(x) := \chi(x) \cdot \chi'(x)$ für alle $\chi, \chi' \in \widehat{G}$, für alle $x \in G$.

Das neutrale Element von $\widehat{G}$ ist die Abbildung

$\mathtt{1}\colon G \to \mathbb{C}^*, \mathtt{1}(x) := 1$ für alle $x \in G$;

$\mathbb{1}$ heißt auch der Einscharakter von G. Und die Gruppe $\widehat{G}$ heißt die *Charaktergruppe von* G.

(7.1) **Beispiel** Sei $G = \langle s \rangle$ zyklisch von der Ordnung n mit dem erzeugenden Element s. Dann ist

$$\chi : G \to \mathbb{C}^*,\ \chi(s) := e^{2\pi i/n},\ \chi(s^k) := \chi(s)^k,$$

ein erzeugendes Element von $\widehat{G}$; insbesondere ist $\widehat{G}$ zyklisch von der Ordnung n, und die Zuordnung $s \to \chi$ induziert einen Isomorphismus $G \cong \widehat{G}$.

(7.2) **Bemerkung** Ist $G \cong G_1 \times G_2$ isomorph zum direkten Produkt von abelschen Gruppen G_1 und G_2, dann ist die Abbildung

$$\widehat{G} \to \widehat{G_1} \times \widehat{G_2},\ \chi \to (\chi_{|G_1}, \chi_{|G_2})$$

ein Isomorphismus.

Beweis: Klar.

Nach (6.24) ist jede abelsche Gruppe isomorph zu einem direkten Produkt von zyklischen Gruppen. Aus (7.1) und (7.2) folgt also

(7.3) **Satz** *Es gibt einen Isomorphismus* $G \cong \widehat{G}$.

Ein Isomorphismus $G \cong \widehat{G}$ wie im vorstehenden Satz hängt insbesondere von der Wahl einer Basis von G und von der Auswahl entsprechender primitiver Einheitswurzeln ab. Man kann aber zeigen

(7.4) **Satz** *Die Abbildung* $G \to \widehat{\widehat{G}},\ x \to \underline{x} : \chi \to \chi(x)$, *ist ein basisunabhängiger Isomorphismus.*

Beweis: Wegen $|\ \widehat{\widehat{G}}\ | = |G|$ reicht es, die Injektivität zu zeigen. Dazu wiederum reicht es zu zeigen, daß zu jedem $x \in G - \{e\}$ein $\chi \in G$ mit$\chi(x) \neq 1$ existiert. Sei dazu $H := \langle x \rangle$. Sei $\psi \in \widehat{H}$ mit $\psi(x) \neq 1$, siehe (7.1). Nach dem nachfolgenden Satz existiert ein $\chi \in G$ mit $\chi_{|H} = \psi$, also insbesondere mit $\chi(x) \neq 1$.

(7.5) **Satz** *Für jede Untergruppe* $H \leqq G$ *ist die Restriktionsabbildung* $\widehat{G} \to \widehat{H}$ *surjektiv.*

Beweis: Durch Induktion über $(G : H)$. Für $G = H$ ist nichts zu zeigen. Sei $(G : H) > 1$ und sei $x \in G \setminus H$. Sei n die kleinste natürliche Zahl mit $x^n \in H$. Sei $\chi \in \widehat{H}$, $t := \chi(x^n)$. Sei $w \in \mathbb{C}^*$ so, daß $w^n = t$. (Ein solches w existiert, weil der Körper $\mathbb{C}$ nach dem Fundamentalsatz der Algebra algebraisch

abgeschlossen ist). Sei $H' := \langle H, x\rangle \leqq G$. Sei $h' \in H'$. Schreibe $h' = h \cdot x^a$ mit $h \in H$ und $a \in \mathbb{Z}$. Definiere

$\chi'(h') := \chi(h) \cdot w^a$.

Dann ist die dadurch definierte Abbildung $\chi' : H' \to \mathbb{C}^*$ ein Charakter von H' mit $\chi'_{|H} = \chi$. Es gilt $(G : H') < (G : H)$. Nach Induktionsannahme läßt sich χ' und damit χ zu einem Charakter von G fortsetzen.

(7.6) **Satz** *(*Orthogonalitätsrelationen*)*

(a) *Für alle* $\chi \in \widehat{G}$ *gilt:*

$\sum_{x\in G} \chi(x) = |G|$, falls $\chi = 1$, und $\sum_{x\in G} \chi(x) = 0$ sonst

(b) *Für alle* $x \in G$ *gilt:*

$\sum_{\chi\in \widehat{G}} \chi(x) = |G|$, falls $x = e$, und $\sum_{x\in G} \chi(x) = 0$ sonst

Beweis: Für $\chi = \mathtt{1}$ gilt offensichtlich $\sum_{x\in G} \chi(x) = |G|$. Sei $\chi \neq \mathtt{1}$. Dann existiert ein $y \in G$ mit $\chi(y) \neq 1$. Es gilt

$\chi(y) \cdot \sum_{x\in G} \chi(x) = \sum_{x\in G} \chi(yx) = \sum_{x\in G} \chi(x)$,

also

$(\chi(y) - 1) \cdot \sum_{x\in G} \chi(x) = 0$ und damit $\sum_{x\in G} \chi(x) = 0$.

(b) folgt aus (a) mit $G = \widehat{G}$ und (7.4).

Sei $N \geqq 2$ eine natürliche Zahl. Die N-te *Fouriermatrix* $\widetilde{F}(N)$ ist definiert durch

$\widetilde{F}(N) := (\frac{1}{\sqrt{N}} \exp(2\pi iab/N))_{0\leqq a,b\leqq N-1}$;

z.B.

$$\widetilde{F}(2) = \tfrac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\widetilde{F}(3) = \tfrac{1}{\sqrt{3}} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{2\pi i/3} & e^{4\pi i/3} \\ 1 & e^{4\pi i/3} & e^{2\pi i/3} \end{pmatrix}$$

Wir wollen zunächst $\widetilde{F}(N)$ als Matrix eines Endomorphismus $F(N)$ eines N-dimensionalen $\mathbb{C}$-Vektorraums erkennen.

Sei dazu $R_N = (\{0,1,2,...,N-1\},+,\cdot)$ der Rechenbereich, der als Trägermenge alle ganzen Zahlen zwischen 1 und N hat und bei dem + bzw. $\cdot$ die Addition bzw. Multiplikation modulo N ist; R_N ist ein Ring, vgl. § 9. Gelegentlich bezeichnen wir mit R_N^+ die kommutative Gruppe von R_N bezüglich der Addition, d.h. $R_N^+ = (\{0,1,...,N-1\},+)$. Sei $\mathcal{S}_N$ der $\mathbb{C}$-Vektorraum aller Abbildungen $f : R_N \to \mathbb{C}$ von R_N in $\mathbb{C}$. Addition und Skalarmultiplikation sind dabei punktweise definiert. Der folgende Satz ist leicht zu beweisen.

(7.7) **Satz** *Die charakteristischen Funktionen* $\chi_a := \chi_{\{a\}}, 0 \leqq a \leqq n-1$, *bilden eine Basis von* $\mathcal{S}_N$*; insbesondere gilt* $\dim_{\mathbb{C}} \mathcal{S}_N = N$. *Die* N*-te Fouriermatrix* $\widetilde{F}(N)$ *ist bezüglich dieser Basis von* $\mathcal{S}_N$ *die Matrix des Endomorphismus*

$F(N) : \mathcal{S}_N \to \mathcal{S}_N$,

$F(N)(f)(b) := \frac{1}{\sqrt{N}} \sum_{0 \leqq a \leqq N-1} f(a) e^{2\pi i a b/N}$

für alle $f \in \mathcal{S}_N$ *und für alle* b *mit* $0 \leqq b \leqq N-1$.

Der Endomorphismus $F(N)$ von $\mathcal{S}_N$ heißt die N*-te Fouriertransformation.*

Auf $\mathcal{S}_N$ definieren wir ein Skalarprodukt

$(\ , \ ) : \mathcal{S}_N \times \mathcal{S}_N \to \mathbb{C}, \ \ (f,g) := \sum_{0 \leqq a \leqq N-1} f(a)\overline{g(a)}$;

dabei bedeutet $\overline{z}$ die komplexe Konjugation einer komplexen Zahl z. Dadurch wird $\mathcal{S}_N$ zu einem unitären $\mathbb{C}$-Vektorraum, und die charakteristischen Funktionen χ_a, $a \in \{0,1,...,N-1\}$, bilden eine Orthogonalbasis von $\mathcal{S}_N$. Es gilt

$F(N)(f)(a) = \frac{1}{\sqrt{N}}(f, \lambda_a), f \in \mathcal{S}_N, \ \ a \in \{0,1,...,N-1\}$,

wobei $\lambda_a : R_N^+ \to \mathbb{C}^*$ der wie folgt definierte Homomorphismus ist:

$\lambda_a(b) := e^{-2\pi i a b/N}, \ \ b \in \{0,1,...,N-1\}$.

Außerdem gilt

$(\lambda_a, \lambda_b) = N$, falls $a = b$, und $(\lambda_a, \lambda_b) = 0$ sonst,

d.h. die λ_a, $a \in \{0,1,...,N-1\}$ bilden ebenfalls eine Orthogonalbasis von $\mathcal{S}_N$. Es ist

$F(N)(\chi_a) = \frac{1}{\sqrt{N}} \lambda_{-a}, F(N)(\lambda_a) = \sqrt{N} \cdot \chi_a$.

Daraus ergibt sich

$F(N)^2(\chi_a) = \chi_{-a}$ für alle $a \in \{0, 1, ..., N-1\}$,

also

$F(N)^4 = id.$

Außerdem gilt

$(F(N)(\chi_a), F(N)(\chi_b) = \frac{1}{N}(\lambda_{-a}, \lambda_{-b}) = 1,$ falls $a = b,$ und $= 0$ sonst.

Daraus ergibt sich

$(F(N)(\chi_a), F(N)(\chi_b)) = (\chi_a, \chi_b)$ für alle $a, b \in \{0, 1, ..., N-1\}$.

$F(N)$ ist also ein unitärer Endomorphismus von $\mathcal{S}_N$ von der Ordnung 4 und daher diagonalisierbar mit Eigenwerten $\{\pm 1, \pm i\}$. Um die Vielfachheiten dieser Eigenwerte zu bestimmen, folgen wir der Darstellung in $[AT]$ und bemerken zunächst, daß

$$F(N)^2 = \begin{pmatrix} 1 & 0 & \cdots & & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ \vdots & & & & \\ & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & & 0 \end{pmatrix}.$$

Das charakteristische Polynom von $F(N)^2$ ist daher

$(t-1)^{(N+1)/2}(t+1)^{(N-1)/2}$, falls N ungerade
$(t-1)^{(N+2)/2}(t+1)^{(N-2)/2}$, falls N gerade.

Die Eigenwerte von $F(N)^2$ sind Quadrate der Eigenwerte von $F(N)$. Daraus folgt: Ist

m_1 :=Anzahl der Eigenwerte von $\widetilde{F}(N)$, die gleich 1 sind
m_2 :=Anzahl der Eigenwerte von $\widetilde{F}(N)$, die gleich -1 sind
m_3 :=Anzahl der Eigenwerte von $\widetilde{F}(N)$, die gleich i sind
m_4 :=Anzahl der Eigenwerte von $\widetilde{F}(N)$, die gleich $-i$ sind,

dann ist

$m_1 + m_2 = \frac{N+1}{2}$, $m_3 + m_4 = \frac{N-1}{2}$; falls N ungerade ist
$m_1 + m_2 = \frac{N+2}{2}$, $m_3 + m_3 = \frac{N-2}{2}$; falls N gerade ist.

Außerdem gilt

$Spur(\widetilde{F}(N)) = (m_1 - m_2) + (m_3 - m_4)i.$

Schreibt man daher

$Spur(\widetilde{F}(N)) = \alpha + \beta i,$

so ist

$$\left.\begin{array}{c} \alpha = m_1 - m_2,\ \beta = m_3 - m_4 \\ \frac{N+1}{2} = m_1 + m_2,\ \frac{N-1}{2} = m_3 + m_4 \end{array}\right\} \text{falls } N \text{ ungerade ist.}$$

$$\left.\begin{array}{c} \alpha = m_1 - m_2,\ \beta = m_3 - m_4 \\ \frac{N+2}{2} = m_1 + m_2,\ \frac{N-2}{2} = m_3 + m_4 \end{array}\right\} \text{falls } N \text{ gerade ist}$$

Aus diesen Gleichungssystemen lassen sich m_1, m_2, m_3, m_4 durch N, α, β ermitteln. Um daher die Vielfachheiten der Eigenwerte von $\widetilde{F}(N)$ zu bestimmen, reicht es, die Spur von $\widetilde{F}(N)$ zu berechnen. Aus der Definition von $\widetilde{F}(N)$ folgt

$Spur(\widetilde{F}(N)) = \frac{1}{\sqrt{N}} \cdot \sum_{k=0}^{N-1} e^{2\pi i k^2/N} =: \frac{1}{\sqrt{N}} G(N).$

Wir haben also die sogenannte Gaußsche Summe $G(N)$ zu berechnen. Das geht nach G.L.J. Dirichlet wie folgt. Die Funktion $e(t) := e^{2\pi i t}, t \in \mathbb{R}$, hat die Periode 1. Sei

$f(t) := \sum_{k=0}^{N-1} e(\frac{(k+t)^2}{N}), 0 \leqq t \leqq 1$

Dann ist

$f(0) = f(1) = G(N) = \sum_{k=0}^{N-1} e(k^2/N).$

Ebenfalls mit f bezeichnen wir die periodisch mit Periode 1 auf ganz $\mathbb{R}$ fortgesetzte Funktion. Aus der Theorie der Fourier-Reihen folgt - im Sinne der gleichmäßigen Konvergenz:

$f(t) = \sum_{n=-\infty}^{\infty} a_n e(-nt).$

mit

$a_n = \int_0^1 f(t)e(nt)dt = \int_0^1 \sum_{k=0}^{N-1} e(\frac{(k+t)^2}{N})e(nt)dt.$

Es ist

$G(N) = f(0) = \sum_{n=-\infty}^{\infty} a_n$;

die ihrer Definition nach endliche Gaußsche Summe erscheint also hier als unendliche Reihe, die sich, wie wir sehen werden, leichter berechnen läßt. Es gilt

$a_n = \int_0^1 \sum_{k=0}^{N-1} e(\frac{(k+t)^2}{N})e(nt)dt$

$= \sum_{k=0}^{N-1} \int_0^1 e(\frac{(k+t)^2+Nnt}{N})dt$

$= \sum_{k=0}^{N-1} \int_0^1 e(\frac{(k+t+\frac{1}{2}Nn)^2}{N} - \frac{kNn+\frac{1}{4}N^2n^2}{N})dt$

Wegen $\frac{kNn}{N} \in \mathbb{Z}$ und weil $e(t)$ die Periode 1 hat, ist der letzte Ausdruck

$= \sum_{k=0}^{N-1} \int_0^1 e(\frac{(k+t+\frac{1}{2}Nn)^2}{N})e(-\frac{1}{4}Nn^2)dt$

$= e(-\frac{1}{4}Nn^2) \sum_{k=0}^{N-1} \int_0^1 e((k+t+\frac{1}{2}Nn)^2/N)dt.$

Die Substitution $\tau := k + t + \frac{1}{2}Nn$ ergibt

$= e(-\frac{1}{4}Nn^2) \sum_{k=0}^{N-1} \int_{k+\frac{1}{2}Nn}^{k+1+\frac{1}{2}Nn} e(\tau^2/N)dt$

$= e(-\frac{1}{4}Nn^2) \int_{\frac{1}{2}Nn}^{N+\frac{1}{2}Nn} e(\tau^2/N)dt.$

Also

$G(N) = \sum_{n=-\infty}^{\infty} a_n = \sum_{n=-\infty}^{\infty} e(-\frac{1}{4}Nn^2) \int_{\frac{1}{2}Nn}^{N+\frac{1}{2}Nn} e(\tau^2/N)dt.$

Für gerades n ist $\frac{1}{4}Nn^2 \in \mathbb{Z}$ und daher $e(-\frac{1}{4}Nn^2) = 1$. Für ungerades n ist $n^2 \equiv 1 \bmod 4$ und somit $e(-\frac{1}{4}Nn^2) = \eta$, wobei

$$\eta = \begin{cases} 1, & falls \;\; N \equiv 0 \bmod 4 \\ -i, & falls \;\; N \equiv 1 \bmod 4 \\ -1, & falls \;\; N \equiv 2 \bmod 4 \\ i, & falls \;\; N \equiv 3 \bmod 4 \end{cases}$$

Daraus ergibt sich

$$G(N) = \sum_{n\ gerade} \int_{\frac{1}{2}Nn}^{N+\frac{1}{2}Nn} e(\tau^2/N)d\tau + \sum_{n\ ungerade} \eta \int_{\frac{1}{2}Nn}^{N+\frac{1}{2}Nn} e(\tau^2/N)d\tau$$

$$= (1+\eta)\int_{-\infty}^{\infty} e(\tau^2/N)d\tau = (1+\eta)\sqrt{N}\int_{-\infty}^{\infty} e(t^2)dt$$

$$= (1+\eta)\sqrt{N}\int_{-\infty}^{\infty} \cos(2\pi t^2)dt + i\int_{-\infty}^{\infty} \sin(2\pi t^2)dt.$$

Die beiden letzten uneigentlichen Integrale können mit der folgenden Methode berechnet werden: Aus

$(G(1) = 1 = (1-i)\int_{-\infty}^{\infty} e(t^2)dt$

folgt

$\int_{-\infty}^{\infty} e(t^2)dt = \frac{1}{1-i} = \frac{1+i}{2}$,

also

$\int_{-\infty}^{\infty} \cos(2\pi t^2)dt = \int_{-\infty}^{\infty} \sin(2\pi t^2)dt = \frac{1}{2}$

Als Ergebnis erhalten wir also

(7.8) **Satz**

$$G(N) = \begin{cases} (1+i)\sqrt{N}, & falls \quad N \equiv 0 \mod 4 \\ \sqrt{N}, & falls \quad N \equiv 1 \mod 4 \\ 0, & falls \quad N \equiv 2 \mod 4 \\ i\sqrt{N} & falls \quad N \equiv 3 \mod 4 \end{cases}$$

Zusammenfassend erhält man einen vollständigen Überblick über die Eigenwerttheorie von $\widetilde{F}(N)$, vgl. $[AT]$.

(7.4) **Satz** *$\widetilde{F}(N)$ ist für alle $N \in N, N \geqq 2$, diagonalisierbar mit Eigenwerten $\in \{\pm 1, \pm i\}$. Sei m_1, m_2, m_3, m_4 die Vielfachheit des Eigenwertes $1, -1, i$ bzw. $-i$. Dann gilt*

N	m_1	m_2	m_3	m_4
$4m$	$m+1$	m	m	$m-1$
$4m+1$	$m+1$	m	m	m
$4m+2$	$m+1$	$m+1$	m	m
$4m+3$	$m+1$	$m+1$	$m+1$	m

Die Berechnung von

$\mathcal{F}(N)(f)(j) := \sum_{k=0}^{N-1} f(k)e^{2\pi ijk/N}$

in naiver Weise erfordert N^2 Operationen, wobei "Operation" eine komplexe Multiplikation gefolgt von einer komplexen Addition bedeutet. Für zusammengesetzte N, etwa $N = r_1 r_2$, kann man die Anzahl der Opeationen reduzieren. Die grundlegende Idee hierfür geht auf Cooley und Tukey zurück und ist wie folgt , vgl. $[CT]$ sowie die in der historischen Studie $[HJB]$ genannten Quellen. Schreibe

$j = j_1 r_1 + j_0;\ j_0 = 0, 1, ..., r_1 - 1;\ j_1 = 0, 1, ..., r_2 - 1$
$k = k_1 r_2 + k_0;\ k_0 = 0, 1, ..., r_2 - 1;\ k_1 = 0, 1, ..., r_1 - 1.$

Dann gilt mit $\mathcal{F} = \mathcal{F}(N)$ und $\epsilon_N = e^{2\pi i/N}$:

$$\mathcal{F}(f)(j) = \sum_{k=0}^{N-1} f(k)\epsilon_N^{jk} = \sum_{k_0} \sum_{k_1} f(k)\epsilon_N^{j_0 k_1 + r_2}\epsilon_N^{jk_0},$$

weil

$$\epsilon_N^{jk_1 r_2} = \epsilon_N^{j_0 k_1 r_2}.$$

Die innere Summe über k_1 hängt nur von j_0 und k_0 ab und kann als neue Funktion von j_0 und k_0 betrachtet werden:

$$g(j_0, k_0) := \sum_{k_1} f(k)\epsilon_N^{j_0 k_1 + r_2}.$$

Somit gilt

$$\mathcal{F}(f)(j) = \sum_{k_0} g(j_0, k_0)\epsilon_N^{jk_0}$$

Es gibt N Werte $g(j_0, k_0)$. Um g zu berechnen, benötigt man Nr_1 Operationen. Man benötigt Nr_2 Operationen, um $\mathcal{F}(f)$ aus g zu berechnen. Also braucht man insgesamt $N(r_1 + r_2)$ Operationen, um $\mathcal{F}(f)$ zu berechnen.

Diese Beobachtungen sind für "schnelles Rechnen" von großer Bedeutung, z.B. für die schnelle Multiplikation großer ganzer Zahlen, vgl. z.B. $[ST]$. Um das einzusehen, wählen wir $g \in \mathbb{N}_{\geq 2}$ und stellen zwei ganze Zahlen, $x, y > 0$ gemäß (3.4) bezüglich in der folgenden Form dar:

$$x = \sum_{n=0}^{S-1} x_n g^n,\ \ y = \sum_{m=0}^{T-1} y_m g^m,$$

wobei $x_n,\ y_m \in \{0, 1, ..., g-1\}$. Also gilt für das Produkt

$$z = xy = \sum_{n,m} x_n x_m g^{n+m} = \sum_k z_k g^k$$

mit

$z_k = \sum_{n+m=k} x_n x_m$.

Dabei müssen insgesamt ST Produkte berechnet werden. Mit Hilfe der endlichen Fouriertransformation und des obigen Algorithmus von Cooley und Tukey läßt sich dieser Rechenaufwand reduzieren. Wir schildern die dazu erforderliche grobe Idee und verweisen für die Einzelheiten auf [F], § 20, oder auf [WG]. Die obige Formel für z_k legt nahe, .die sogenannte Faltung $f * g$ von zwei Funktionen $f, g : R_N \to \mathbb{C}$ zu betrachten:

$(f * g)(k) := \sum_{0 \leqq n \leqq N-1} f(k-n)g(n)$

Es gilt

(7.10) **Satz** $F(f * g) = \sqrt{N} F(f) F(g)$

Beweis: Nach Definition gilt

$$F(f * g)(s) = \frac{1}{\sqrt{N}} \sum_{0 \leqq k \leqq N-1} (f * g)(k) \epsilon_N^{ks}$$

$$= \frac{1}{\sqrt{N}} \sum_{0 \leqq k,m \leqq N-1} f(k-m) g(m) \epsilon_N^{ks}$$

Substitution: $n := k - m$. Wenn - bei festem m - k alle Elemente aus R_N durchläuft, dann auch n. Also folgt

$$F(f * g)(s) = \frac{1}{\sqrt{N}} \cdot \sum_n \sum_m f(n) g(m) \epsilon_N^{(n+m)s}$$

$$= \frac{1}{\sqrt{N}} \cdot \sum_n f(n) \epsilon_N^{ns} \sum_m g(m) \epsilon_N^{ms}$$

$$= \sqrt{N} F(f) F(g).$$

(7.11) **Folgerung** $f * g = \sqrt{N} F^{-1}(F(f) \cdot F(g))$.

Das Faltungsprodukt von zwei Vektoren aus $\mathbb{C}^N$ benötigt insgesamt N^2 Multiplikationen von komplexen Zahlen, während das komponentenweise Produkt nur N Multiplikationen benötigt. Mit der Formel für die Faltung aus (7.11) kann man das Faltungsprodukt durch 3-malige Anwendung der Fouriertransformation auf das komponentenweise Produkt zurückführen. Indem man für N eine 2-Potenz wählt, erhält man unter Benutzung des weiter oben erläuterten Cooley-Tukey-Algorithmus ein Verfahren zur "schnellen Multiplikation" großer ganzer Zahlen; siehe dazu z.B. [F], § 20 oder [GT], Chapter 4.

In der Theorie der fehlerkorrigierenden Codes, vgl. z. B. $[MS]$, benutzt man die Elemente gewisser Teilmengen oder Untergruppen C einer gegebenen endlichen abelschen Gruppe V als Codewörter, die an einen Empfänger gesendet werden. Bei der Untersuchung solcher Untergruppen (Codes) $C \leq V$ studiert man insbesondere das Verhalten der charakteristischen Funktion χ_C unter einer endlichen Fouriertransformation, die in Abhängigkeit von einer Zerlegung von V in ein direktes Produkt von zyklischen Gruppen definiert ist. Wir definieren zunächst diese endliche Fouriertransformation und beschreiben ihre Wirkung auf χ_C; dabei folgen wir der entsprechenden Darstellung in $[DMK]$. In §14 geben wir dann eine kurze Einführung in die Theorie der fehlerkorrigierenden Codes und beschreiben die Rolle der endlichen Fouriertransformation in dieser Theorie.

Für gegebene natürliche Zahlen $N_1, ..., N_r$ sei

$$V = (R_{N_1} \times ... \times R_{N_r}, +, \cdot)$$

mit der komponentenweise definierten Addition und Multiplikation. Mit V^+ bezeichnen wir die V zugrunde liegende kommutative Gruppe. Sei $\mathcal{S}(V)$ der $\mathbb{C}-$Vektorraum aller Abbildungen $f : V \to \mathbb{C}$. Sei

$$\delta : V^+ \to \widehat{V^+} = Hom(V^+, \mathbb{C}^*)$$

der wie folgt definierte Isomorphismus

$$\delta(v)(w) := \exp(2\pi i v_1 w_1/N_1) \cdot ... \cdot \exp(2\pi i v_r w_r/N_r),$$

wobei $v = (v_1, v_2, ..., v_r), w = (w_1 w_2, ..., w_r) \in V$. Die endliche Fouriertransformation zu V oder V^+ ist die $\mathbb{C}$-lineare Abbildung

$$F_V : \mathcal{S}(V) \to \mathcal{S}(V), \;\; F_V(f)(w) := \frac{1}{|V|^{\frac{1}{2}}} \sum_{v \in V} \delta(w)(v) f(v).$$

Für eine Teilmenge $S \subset V$ sei

$$S^\perp := \{v \in V : \delta(v)(w) = 1 \text{ für alle } w \in S\};$$

$S^\perp$ ist eine Untergruppe von V^+. Sei χ_S sei die charakteristische Funktion von S.

(7.12) **Satz** *(*Poisson-Formel für endliche abelsche Grupppen*) Sei $C \leqq V^+$ eine Untergruppe. Dann gilt*

$$F_V(\chi_C) = \frac{|C|}{|V|^{\frac{1}{2}}} \chi_C$$

Dieses Resultat ist Spezielfall der sogenannten Poisson-Formel in der Integrationstheorie lokalkompakter Gruppe, vgl. dazu $[BK]$, p. 127. Ein direkter Beweis wird in $[DMK]$, Chapter 4, gegeben.

Beweis von (7.12): Nach Definition ist

$$F_V(\chi_C)(v) = \frac{1}{|V|^{\frac{1}{2}}} \cdot \sum_{w \in C} \delta(v)(w).$$

Für $v \in C^{\perp}$ ist die Einschränkung von $\delta(v)$ auf C ein nichttrivialer Charakter von C. Aufgrund der Orthogonalitätsrelationen (7.6) gilt daher

$$\sum_{w \in C} \delta(v)(w) = 0.$$

Die Behauptung folgt.

Einer Idee des Physikers R. Feynman folgend, vgl. $[FM1]$, $[FM2]$, $[FM3]$, versucht man, Computer zu bauen, die die Energiezustände von Atomen ausnutzen. Diese Computer nennt man Quantencomputer. In den entsprechenden informationstheoretischen Zusammenhängen spielt die endliche Fouriertransformation ebenfalls eine wichtige Rolle, und zwar in Form der sogenannten Quanten-Fouriertransformation, vgl. z.B. $[NC]$, 5; $[SH]$. Im Folgenden erläutern wir den Begriff der Quanten-Fouriertransformation und folgen dabei entsprechenden Ausführungen in $[NC]$, 5.

Sei $|0\rangle, ..., |N-1\rangle$ eine Orthogonalbasis des $\mathbb{C}$-Vektorraums $\mathcal{S}_N$ aller Funktionen $f : R_N^+ \to \mathbb{C}$ bezüglich des oben definierten hermiteschen Skalarprodukts $(\ ,\ ) : \mathcal{S}_N \times \mathcal{S}_N \to \mathbb{C}$. Die endliche Fouriertransformation $F(N) : \mathcal{S}_N \to \mathcal{S}_N$, angewandt auf $|j\rangle$, ist dann gegeben durch

$$F(N)(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle,$$

und $F(N)$, angewandt auf ein beliebiges Element $\sum_{j=1}^{N-1} x_j |j\rangle \in \mathcal{S}_N$, ist gegeben durch

$$F(N)(\sum_{j=0}^{N-1} x_j |j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k |k\rangle$$

mit

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k/N}$$

Sei nun $N = 2^n$. Schreibt man $j \in \{0, ..., 2^n - 1\}$ in binärer Form, vgl. (3.4), also

$$j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0 =: j_1 j_2 ... j_n$$

mit $j_i \in \{0, 1\}$ für $i = 1, ..., n$ und setzt man

$$0, j_\ell j_{\ell+1} ... j_m := \frac{j_\ell}{2} + \frac{j_{\ell+1}}{4} + ... + \frac{j_m}{2^{m-\ell+1}},$$

dann ist

$$F(2^n)(|j\rangle) = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} \, |k\rangle =$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi ij(\sum_{\ell-1}^{n} k_\ell 2^{-\ell})} \, |k_1 ... k_n\rangle$$

$$= \frac{(|0\rangle + e^{2\pi i 0, j_n}|1\rangle)(|0\rangle + e^{2\pi i o, j_{n-1} j_n}|1\rangle) ... (|0\rangle + e^{2\pi i 0, j_1 j_2 \cdots j_n}|1\rangle)}{2^{n/2}}$$

In dieser Form nennt man $F(2^n)$ die Quanten-Fouriertransformation. In Matrixform ist

$$F(2^n) = \frac{1}{2^{n/2}} (\otimes_{k=0}^{2^{n-1}} R_k) \text{ mit } R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix},$$

wobei das Tensorprodukt $A \otimes B$ von

$A \in Mat(m \times n, \mathbb{C})$ und $B \in Mat(m' \times n', \mathbb{C})$

wie folgt definiert ist:

$A \otimes B := (a_{ij}B)$, wenn $A = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$.

Die durch R_k definierten Operationen lassen sich auf einem Quantencomputer realisieren, und viele Rechnungen, die auf klassischen Computern nur mit exponentiellem Aufwand ablaufen, lassen sich mit Hilfe der Quanten-Fouriertransformation mit polynomialem Aufwand bewältigen; für Einzelheiten und Beispiele vgl. $[SH]$; $[NC]$, 5. Etwas formaler läßt sich die Quanten-Fouriertransformation also folgendermaßen beschreiben: Ist

$\beta : \mathcal{S}_{2^n} \to \mathcal{S}_2^{\otimes n}$, $|j\rangle \to |j\rangle \otimes ... \otimes |j_n\rangle$

der durch die Binärdarstellung definierte Isomorphismus zwischen $\mathcal{S}_{2^n}$ und dem n-fachen Tensorprodukt $\mathcal{S}_2^{\otimes n}$ von $\mathcal{S}_2$ mit sich selbst, dann ist die Quanten-Fouriertransformation derjenige $\mathbb{C}$-Vektorraumautomorphismus

$FQ(2^n) : \mathcal{S}_2^{\otimes n} \to \mathcal{S}_2^{\otimes n}$,

der das folgende Diagramm kommutativ ergänzt

$$\begin{array}{ccc} \mathcal{S}_{2^n} & \overset{F(2^n)}{\to} & \mathcal{S}_{2^n} \\ \beta \downarrow & & \downarrow \beta \\ \mathcal{S}_2^{\otimes n} & \overset{FQ(2^n)}{\to} & \mathcal{S}_2^{\otimes n} \end{array}$$

Für weitere Informationen in diesem Zusammenhang vgl. z.B. $[MN]$.

Andere Anwendungen der endlichen Fouriertransformation werden z.B. in $[TS]$ beschrieben.

Aufgaben und Beispiele

(1) Schreiben Sie die Fouriermatrizen $\widetilde{F}(4)$ und $\widetilde{F}(5)$ hin.

(2) Berechnen Sie die Spuren der Fouriermatrizen $\widetilde{F}(3)$ und $\widetilde{F}(5)$ ohne Benutzung von (7.8) oder (7.9).

(3) (Vgl. $[MF]$, Abschnitte 5 und 6) Für eine endliche abelsche Gruppe V sei $\mathcal{S}(V)^{F_V}$ der Untervektorraum von $\mathcal{S}(V)$, der aus allen $f \in \mathcal{S}(V)$ mit $F_V(f) = f$ besteht. Sei

$T_V : \mathcal{S}(V) \to \mathcal{S}(V)$

die durch

$T_V(f) := F_V(f) + F_V^2(f) + F_V^3(f) + f, \;\; f \in \mathcal{S}(N),$

definierte Abbildung. Zeigen Sie:

(a) $Bild(T_V) \subset \mathcal{S}(V)^{F_V}$

(b) Die Funktionen $T_V(\chi_v), v \in V$, wobei χ_v die charakteristische Funktion zu $v \in V$ bezeichnet, bilden ein Erzeugendensystem von $\mathcal{S}(V)^{F_V}$

(4) Zeigen Sie: $Spur(F_{\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}}) = -Spur(F_{\mathbb{Z}/3\mathbb{Z}}) \cdot Spur(F_{\mathbb{Z}/7\mathbb{Z}})$

(5) Bei der Analyse von Daten interpretiert man die Funktion $f \in \mathcal{S}_N$ bzw. den Vektor ihrer Werte $(f(0), f(1), ..., f(N-1))$ als Vektor von Meßdaten und ordnet der Funktion f ihr "Fourier-Bild" $\widetilde{\mathcal{F}}(N)(f)$ zu, wobei

$\widetilde{\mathcal{F}}(N)(f) : [0, N-1] \to \mathbb{C}$

die folgendermaßen definierte Funktion auf dem abgeschlossenen Intervall $[0, N-1]$ ist:

$\widetilde{\mathcal{F}}(N)(f)(x) := \sum_{k=0}^{N-1} f(k)e^{2\pi ixk/N}$ für alle $x \in [0, N-1]$.

$\mathcal{F}(N)(f)$ ist also die Einschränkung von $\widetilde{\mathcal{F}}(N)(f)$ auf $\{0,1,...,N-1\}$. Plotten Sie den Realteil von $\widetilde{\mathcal{F}}(3)(f)$ für $f(0) := 1$, $f(1) := 2$, $f(2) := 1$.

Das "Fourier-Bild" von $f \in \mathcal{S}(V)$ läßt sich auch im "mehrdimensionalen Fall"

$V = R_N \times R_N \times ... \times R_N$ (r-mal)

definieren; es ist die Funktion

$\widetilde{\mathcal{F}}_V(f) : [0, N-1]^r \to \mathbb{C}$:

$\widetilde{\mathcal{F}_V}(f)(x) := \sum_{v=(v_1,...,v_r)\in V} f(v)e^{2\pi i(x_1v_1+...+x_rv_r)/N}$

für alle $x = (x_1, ..., x_r) \in [0, N-1]^r$.

Literatur zu §7: $[AT]$, $[BK]$,$[CT]$, $[DM]$, $[DMK]$, $[F]$, $[FM1]$, $[FM2]$, $[FM3]$, $[G]$, $[GT]$, $[HJB]$, $[HS]$, $[HY]$, $[LPS]$, $[MF]$, $[MN]$, $[MS]$, $[NC]$, $[R]$, $[S]$, $[SH]$, $[ST]$, $[SW]$, $[T]$, $[TS]$, $[WG]$

.

§ 8. **Operationen von Gruppen auf Mengen**

In diesem Abschnitt besprechen wir grundlegende Tatsachen und Resultate über Operationen von Gruppen auf Mengen und folgen dabei entsprechenden Darstellungen in $[GT]$, Chapter 9 und $[R]$, Chapter 3.

Sei X eine nichtleere Menge und sei G eine Gruppe.

Definition *G operiert* (von links) *auf X* oder X ist *eine (Links-) G-Menge*, wenn eine Abbildung

$G \times X \to X, (g, x) \to gx$

mit den folgenden Eigenschaften existiert:

$(gh)x = g(hx)$, $ex = x$ jeweils für alle $g, h \in G$, $x \in X$.

Man beachte, daß die linke Seite der Gleichiung $(gh)x = g(hx)$ die Verknüpfung in G enthält, die rechte Seite dagegen nicht.

Wenn G auf X operiert, dann erhält man dadurch die folgende Abbildung T von G in die symmetrische Gruppe S_X von X:

$T : G \to S_X$, $g \to T_g$, $T_g(s) := gs$; $g \in G$, $s \in X$.

T ist ein Gruppenhomomorphismus.

Umgekehrt liefert jeder Gruppenhomomorphismus $T : G \to S_X$, $g \to T_g$, eine Operation von G auf X :

$G \times X \to X$, $(g, x) \to T_g(x)$.

Die folgende Aussage ist leicht zu beweisen.

(8.1) **Bemerkung** Die oben beschriebene Zuordnung zwischen der Menge aller Gruppenoperationen der Gruppe G auf der nichtleeren Menge X und der Menge aller Gruppenhomomorphismen von G in die symmetrische Gruppe S_X ist bijektiv.

(8.2) **Definition** *G operiert transitiv* auf X, wenn ein $z \in Z$ existiert, so daß zu jedem $x \in X$ ein $g \in G$ mit der Eigenschaft $x = gz$ existiert.

Beispiele von Gruppenoperationen (1) Seien $a \in \mathbb{Q}\backslash\{0, 1\}$ und $n \in \mathbb{N}, n \geqq 2$, vorgegeben. Sei $G := W_n := \{z \in \mathbb{C} : z^n = 1\}$ und $X := \{z \in \mathbb{C} : z^n - a = 0\}$. Dann ist $G \times X \to X$, $(g, z) \to g \cdot z$, eine Gruppenoperation. Diese Operation ist transitiv: Sei dazu $z \in X$. Dann gilt für alle $x \in X$:

$(\frac{x}{z})^n = \frac{x^n}{z^n} = \frac{a}{a} = 1$,

d.h. $g := \frac{x}{z} \in W_n = G$, also $x = g \cdot z$.
(2) Sei $G = (G, \cdot)$ eine Gruppe und $X = G$ die dieser Gruppe zugrundeliegende Menge. Dann operiert G auf X durch $G \times X \to X$, $(g, x) \to g \cdot x$, und der nach (8.1) zu dieser Operation gehörende Gruppenhomomorphismus $T : G \to S_X$ ist injektiv; es folgt: G ist isomorph zu einer Untergruppe von S_X.
(3) Sei $(G, \cdot)$ eine Gruppe und $X = G$. Dann operiert G auf X durch Konjugation:

$G \times X \to X$, $(g, x) \to gxg^{-1}$.

Für $x \in X$ heißt $\{gxg^{-1} : g \in G\} \subset G$ die *Konjugationsklasse von x*.

(8.3) **Definition und Satz** *Sei G eine Gruppe, die (von links) auf der nichtleeren Menge X operiert. Zwei Elemente $x, y \in X$ heißen aequivalent, wenn ein $g \in G$ existiert, so daß $y = gx$. Dadurch wird auf X eine Aequivalenzrelation definiert. Die entsprechenden Aequivalenzklassen heißen die Bahnen von G auf X. Sei $B(x) := \{gx : g \in G\}$ die Bahn des Elementes $x \in X$. Es gilt*

$X = \dot{\bigcup}_x B(x)$,

wobei x ein Repräsentantensystem der Bahnen durchläuft. Für $x \in X$ sei

$G_x := \{g \in G : gx = x\}$.

G_x ist eine Untergruppe von G, die sogenannte Stand- oder Fixgruppe oder Isotropiegruppe von x. Sei $G \setminus G_x$ die Menge aller Linksnebenklassen von G modulo G_x. Die Abbildung

$$G \setminus G_x \to B(x), gG_x \mapsto gx$$

ist bijektiv. Also erhält man dadurch eine bijektive Abbildung

$$X \xrightarrow{\sim} \dot{\bigcup_z} G \setminus G_z,$$

wobei z ein Repräsentantensystem der Bahnen durchläuft; insbesondere gilt

$|X| = \sum_z (G : G_z)$.

Beweis: Für alle $x \in X$ ist $x \sim x$, weil $ex = x$. Wenn $x \sim y$, also $y = gx$ mit einem $g \in G$, dann gilt $g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = ex = x$, also $y \sim x$. Wenn $x \sim y$ und $y \sim z$, dann existieren $g, h \in G$ mit $y = gx$ und $z = hy$, somit $z = h(gx) = (hg)x$, also $x \sim z$. Damit ist die angegebene Relation als Aequivalenzrelation nachgewiesen. Alle nachfolgenden Behauptungen sind ähnlich leicht zu beweisen.

Bemerkung Wenn eine Gruppe G auf der nichtleeren Menge X operiert, dann gilt für alle $x \in X$, $g \in G$:

$G_{gx} = gG_xg^{-1}$.

(8.4) **Satz** *("Lemma von Burnside") Sei G eine endliche Gruppe und sei X eine endliche G-Menge. Sei $G \setminus X$ die Menge der Bahnen. Dann gilt*

$$|G \setminus X| = \tfrac{1}{|G|} \cdot \sum_{t \in G} |X^t| = \tfrac{1}{|G|} \sum_{x \in X} |G_x| ,$$

wobei $X^t := \{x \in X : tx = x\}$.

Beweis: Sei $S := \{(s, x) \in G \times X : sx = x\}$. Für jedes $s \in S$ gilt dann

$$|\{(s, x) \in \{s\} \times X : sx = x\}| = |X^s| .$$

Also

$$|S| = \sum_{t \in G} |X^t| .$$

Andererseits gilt für jedes $x \in X$

$$|\{(s, x) \in G \times \{x\} : sx = x\}| = |G_x| .$$

Somit

$|S| = \sum_{x\in X} |G_x| = \sum_{\mathcal{O}\in G\setminus X} \sum_{y\in B(x)} |G_x| = (\text{weil } |\mathcal{O}| = (G : G_x))$

$= \sum_{\mathcal{O}\in G\setminus G} |\mathcal{O}| \cdot \left|\frac{G}{\mathcal{O}}\right| = |G \setminus X| \cdot |G| \,.$

Es folgt

$|G \setminus X| \cdot |G| = \sum_{t\in G} |X^t| = \sum_{x\in X} |G_x| \,.$

(8.5) **Folgerung** *Sei G eine endliche Gruppe und sei X eine endliche G-Menge, auf der G transitiv operiert. Wenn dann $|X| > 1$ ist, so existiert ein Element $t \in G$, das keine Fixpunkte hat, d.h. es gilt $|X^t| = 0$.*

Beweis: Wegen der Transitivität der Operation von G auf X gilt $|G \setminus X| = 1$. Nach dem Lemma von Burnside gilt also

$(\star)\quad 1 = \frac{1}{|G|} \sum_{t\in G} |X^t| \,.$

Für $t = e$ gilt nach Voraussetzung $|X^e| = |X| > 1$. Aus $(\star)$ folgt daher die Existenz eines Elementes $t \in G$ mit $|X^t| = 0$.

Sei X eine G-Menge und sei U eine weitere Menge. Definiere

$\mathcal{F} := \{f : f \text{ ist eine Abbildung von } X \text{ nach } U\}.$

Es gilt

$|\mathcal{F}| = |U|^{|X|} \,.$

G operiert wie folgt auf $\mathcal{F}$:

$s(f)(x) := f(s^{-1}(x)),\ \ s \in G,\ f \in \mathcal{F},\ x \in X.$

(8.6) **Satz** *Sei G eine endliche Gruppe und sei X eine endliche G-Menge: Sei U eine endliche Menge. Dann gilt*

$|G \setminus \mathcal{F}| = \frac{1}{|G|} \sum_{s\in G} |U|^{|\langle s\rangle\setminus X|} \,.$

Beweis: Die Behauptung ist gleichbedeutend mit der folgenden Identität:

$|G \setminus \mathcal{F}| = \frac{1}{|G|} \sum_{C} |C| \cdot |U|^{|\langle s_C\rangle\setminus X|} \,,$

wobei C alle Konjugationsklassen aus G durchläuft und wobei $\{s_C\}$ ein Repräsentantensystem für die Konjugationsklassen ist. (Erinnerung: $g, h \in G$ heißen konjugiert, wenn ein $s \in G$ existiert, so daß $g = shs^{-1}$.) Nach dem Lemma von Burnside gilt

$$|G \setminus \mathcal{F}| = \frac{1}{|G|} \sum_{s \in G} |\mathcal{F}^s| .$$

Die Bedingung $f(s^{-1}(x)) = f(x)$ für alle $x \in G$ impliziert

$$f(s^k(x)) = f(x) \quad \text{für alle} \quad k \in \mathbb{Z}, x \in X,$$

d.h. f ist konstant auf den Bahnen der Operation der von s erzeugten zyklischen Gruppe $\langle s \rangle$ auf X. Also gilt

$$|\mathcal{F}^s| = |U|^{|\langle s \rangle \setminus X|},$$

und damit die Behauptung.

Wir betrachten den folgenden Spezialfall:

$I = \{1, 2, ..., n\}$, $|U| = N$, $\mathcal{F} = \{f : I \to U\}$.

Sei $s \in S_n$ die Permutation $i \to (i + 1) \bmod n$. Dann gilt: $ord(s) = n$ und

(8.7) **Hilfssatz** $|\langle s \rangle \setminus \mathcal{F}| = \frac{1}{n} \sum_{d/n} \phi(d) \cdot N^{n/d}$,

wobei ϕ die Eulersche Funktion ist.

Beweis: Wir wenden den letzten Satz (8.6) auf die folgende Situation an: $X = I$, $G = \langle s \rangle$. Wenn $ggT(k, n) = 1$, dann ist die Anzahl der Bahnen der Operationen von $\langle s^k \rangle$ auf I gleich1. In jedem Fall gilt

$$ord(s^k) = d := \frac{n}{ggT(k,n)},$$

und die Anzahl der Bahnen der Operationen von $\langle s^k \rangle$ auf I ist $ggT(k, n) = \frac{n}{d}$. Außerdem gibt es $\phi(d)$ Elemente der Ordnung d. Die Behauptung folgt.

Als Anwendung betrachten wir die Operation der symmetrischen Gruppe auf der Menge aller Schaltfunktionen; vgl. z.B. [GT], Chapter 9. Sei dazu $I = \{1, 2, ..., n\}$ und sei

$$B(I) := \{x : I \to \{0, 1\}\}.$$

Definition Eine *Schaltfunktion* ist eine Abbildung

$f : B(I) \to \{0,1\}, x \to f(x)$.

Sei $\mathcal{S}(I)$ die Menge aller Schaltfunktionen. Es gilt

$|\mathcal{S}(I)| = 2^{|B(I)|} = 2^{2^n}$.

Die symmetrische Gruppe S_n operiert auf $B(I)$ wie folgt:

$\sigma(x)(i) := x(\sigma^{-1}(i))$, $i \in I$, $x \in B(I)$, $\sigma \in S_n$;

somit operiert S_n auf $\mathcal{S}(I)$ in der folgenden Weise:

$\sigma(f)(x) := f(\sigma^{-1}(x))$, $x \in B(I)$, $f \in \mathcal{S}(I)$, $\sigma \in S_n$.

Diese Begriffsbildungen beziehen sich auf einen Schaltkreis mit n Schaltern, die durch die Elemente aus $I = \{1, 2, ..., n\}$ repräsentiert werden. Die Elemente aus $B(I)$ betrachten wir als Vektoren

$B(I) \ni x = (x(1), x(2), ..., x(n))$ mit $x(i) \in \{0, 1\}$.

Die i-te Koordinate $x(i) \in \{0, 1\}$ entspricht der Schaltposition 0 ("aus") oder 1 ("ein") des i-ten Schalters. Der Wert $f(x)$ einer Schaltfunktion $f \in \mathcal{S}(I)$ an der Stelle $x = (x(1), x(2), ..., x(n))$ ist 0 ("Strom fließt nicht") oder 1 ("Strom fließt"). Je zwei Schaltfunktionen, die in derselben Bahn unter der Operation von S_n auf $\mathcal{S}(I)$ liegen, leisten in technischer Hinsicht dasgleiche. Aufgrund von (8.7) gilt

$$|S_n \setminus \mathcal{S}(I)| = \tfrac{1}{n!} \cdot \textstyle\sum_{\sigma \in S_n} 2^{|\langle\sigma\rangle \setminus B(I)|} =$$

$$= \tfrac{1}{n!} \cdot \textstyle\sum_C |C| \cdot 2^{|\langle\sigma_C\rangle \setminus B(I)|},$$

wobei C die Menge aller Konjugationsklassen von S_n durchläuft und wobei $\{\sigma_C\}$ ein Repräsentantensystem für die Konjugationsklassen ist. Außerdem gilt

$|\langle\sigma\rangle \setminus B(I)| = \frac{1}{|\langle\sigma\rangle|} \cdot \sum_{k=1}^{ord(\sigma)} 2^{|\langle\sigma^k\rangle \setminus I|}$

mit

$\left|\langle\sigma^k\rangle \setminus I\right|$ = Anzahl der Zykeln in σ^k.

Beispiel Wir berechnen im Fall $n = 3$ die Anzahl der Bahnen der Operation von S_3 auf $\mathcal{S}(I)$, $I = \{1, 2, 3\}$. Wir repräsentieren die Elemente aus $B(I)$ durch 3 Veränderliche x, y, z, die die Werte 0 und 1 annehmen können. S_3 permutiert diese 3 Veränderlichen x, y, z. $\mathcal{S}(I)$ hat $2^{2^3} = 256$ Elemente. Nach dem Lemma von Burnside ist

$|S_3 \setminus \mathcal{S}(I)| = \frac{1}{|S_3|} \cdot \sum_{\sigma \in S_3} |\mathcal{S}(I)^\sigma|$.

Es gilt $f \in \mathcal{S}(I)^\sigma$ genaun dann, wenn $\sigma(f) = f$. Aus $\sigma(f) = f$ folgt $(\tau\sigma\tau^{-1}\tau)(f) = \tau(f)$ für alle $\tau \in S_3$, und für alle $\tau \in S_3$ ist die Abbildung

$\mathcal{S}(I)^\sigma \to \mathcal{S}(I)^{\tau\sigma\tau^{-1}}, \ f \to \tau(f)$,

bijektiv. S_3 hat 3 Konjugationsklassen mit 1 bzw. 3 bzw. 2 Elementen; diese werden repräsentiert durch

$\{id\}$ bzw. (12) bzw. (123).

Eine Schaltfunktion f in der Fixmenge von (12) erfüllt die folgende Relation:

$f(x, y, z) = f(y, x, z)$,

und ist vollständig vollständig auf der folgenden Menge bestimmt:

$\{(1, 1, z), (1, 0, z), (0, 0, z)\}$, wobei $z \in \{0, 1\}$.

Also gilt $\left|\mathcal{S}(I)^{(12)}\right| = 2^6 = 64$. Ähnlich zeigt man

$\left|\mathcal{S}(I)^{(123)}\right| = 16$.

Es folgt

$|S_3 \setminus \mathcal{S}(I)| = \frac{1}{6}(256 + 3 \cdot 64 + 2 \cdot 16) = 80$.

Aufgaben und Beispiele

(1) Sei G eine Gruppe. Dann gibt es eine Menge X, so daß G isomorph zu einer Untergruppe von S_X ist.

(2) Sei G eine endliche Gruppe, die auf einer endlichen, nichtleeren Menge X operiert. Wenn G auf X transitiv operiert, dann ist $|X|$ ein Teiler von G.

(3) Sei G eine Gruppe, die auf einer endlichen, nichtleeren Menge X 1-fach transitiv operiert, d.h. für alle $(x, y) \in XxX$ existiert genau ein $g \in G$, so daß $y = gx$. Dann existiert auf X eine Gruppenstruktur, so daß für festes $x \in X$ die Abbildung $G \to X, g \to gx$, ein Isomorphismus von Gruppen ist.

(4) Sei G eine Gruppe, die auf einer nichtleeren Menge X operiert. Dann operiert G in der folgenden Weise auf der Potenzmenge $\mathcal{P}(X)$: $g(\phi) := \phi$, $g(A) := \{ga : a \in A\}$ für alle $g \in G$ und alle nichtleeren Teilmengen $A \subset X$. Im

Fall $X = \{1, 2, 3\}$ und der natürlichen Operation von $G = S_3$ auf X bestimme man die Anzahl der Bahnen der Operationen von G auf $\mathcal{P}(X)$.

Literatur zu §8: [BU], [GT], [P], [R]

§ 9. **Ringe, Körper und Moduln**

Ringe und Körper zählen zu den wichtigsten Rechenbereichen der Algebra. In diesem Abschnitt besprechen wir einige ihrer grundlegenden Eigenschaften, so wie sie in vielen der im Literaturverzeichnis genannten Standardlehrbüchern der Algebra dargestellt werden, vgl. z.B. [KU], [$L2$], [LL], [W], und beschreiben nach einigen zahlentheoretischen Folgerungen die sogenannte public-key Verschlüsselungsmethode; vgl. dazu [DH], [RSA] sowie den entsprechenden Abschnitt in [F].

Definition Ein *Ring* ist eine Menge R zusammen mit zwei Verknüpfungen (Abbildungen)

$+ : R \times R \to R$ (genannt "Addition")
$\cdot : R \times R \to R$ (genannt "Multiplikation")

so daß die folgenden Bedingungen erfüllt sind:

(1) $(a + b) + c = a + (b + c)$ für alle $a, b, c \in R$
(2) $a + b = b + a$ für alle $a, b \in R$
(3) Es existiert ein neutrales Element $0 \in R$ bezüglich der Addition, d.h. es gilt $a + 0 = 0 + a = a$ für alle $a, b \in R$
(4) Für alle $a \in R$ existiert ein Element $b = -a \in R$ mit $a+b = a+(-a) = 0$
(5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in R$
(6) $a \cdot (b + c) = a \cdot b + a \cdot c$ für alle $a, b, c \in R$
(7) $(b + c) \cdot a = b \cdot a + c \cdot a$ für alle $a, b, c \in R$

Für $a \cdot b$ schreibt man auch ab.

(1) und (5) heißen die Assoziativgesetze; (6) und (7) die Distributivgesetze. Ein Ring $R = (R, +, \cdot)$ heißt *kommutativ*, wenn $ab = ba$ für alle $a, b \in R$ gilt. Ein Einselement eines Ringes $R = (R, +, \cdot)$ ist ein Element $1 \in R$ mit $1 \neq 0$ und $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.

Ein Ring hat höchstens ein Einselement.

Eine *Einheit* eines Ringes R, der ein Einselement 1 besitzt, ist ein Element $u \in R$, so daß ein $v \in R$ mit $uv = 1 = vu$ existiert.

Bemerkung Sei $R = (R, +, \cdot)$ ein Ring mit Einselement 1. Die Menge R^* aller Einheiten von R bildet bezüglich der Multiplikation in R eine Gruppe, die sogenannte *Einheitengruppe* von R.

Ist also R ein kommutativer Ring mit 1 und $R^* = R - \{0\}$, dann ist R ein Körper.

Beispiele (1) Die Menge aller $(n \times n)$-Matrizen mit Koeffizienten in einem Ring R mit 1 bildet bezüglich der Addition und Multiplikation von Matrizen einen Ring $Mat(n \times n, R)$ mit $1 =$ Einheitsmatrix vom Grad n. Die Einheitengruppe von $Mat(n \times n, R)$ besteht aus allen invertierbaren $(n \times n)$-Matrizen mit Koeffizienten in R und wird mit $GL(n, R)$ bezeichnet; sie heißt auch die allgemeine lineare Gruppe vom Grad n über R.

(2) Die ganzen Zahlen $\mathbb{Z}$ bilden bezüglich der gewöhnlichen Addition und Multiplikatiopn einen kommutativen Ring mit Einselement 1; es gilt $\mathbb{Z}^* = \{\pm 1\}$.

(3 Ist K ein Körper, dann ist die Menge aller Polynome in der Unbestimmten X und mit Koeffiziuenten aus K ein kommutativer Ring $R = K[X]$ mit 1; es gilt $(K[X])^* = K^*$.

(4) Die komplexen Zahlen der Form $a + bi$ mit $a, b \in \mathbb{Z}$ bilden bezuüglich der Addition und Multiplikation von komplexen Zahlen einen kommutativen Ring mit Einselement, den sogenannten Ring der ganzen Gaußschen Zahlen $\mathbb{Z}\left[\sqrt{-1}\right]$; es gilt $(\mathbb{Z}\left[\sqrt{-1}\right])^* = \{\pm 1, \pm\sqrt{-1}\}$.

(5) Sei $m \geqq 2$ eine natürliche Zahl und $R_m = \{0, 1, 2, ..., m-1\}$. Für $a, b \in R_m$ sei $a + b$ bzw. $a \cdot b$ der Rest, der bei Division der Summe $a + b \in \mathbb{Z}$ bzw. des Produktes $a \cdot b \in \mathbb{Z}$ durch m übrig bleibt. Mit diesen Verknüpfungen wird R_m zu einem kommutativen Ring mit 1. Es ist leicht zu zeigen, daß $R_m^* = \{k \in Z : 0 \leqq k < m, ggT(k, m) = 1\}$ gilt. Insbesondere gilt: Ist $m = p$ eine Primzahl, dann ist $R_p^* = R_p - \{0\}$; also ist R_p ein Körper, den man auch mit $\mathbb{F}_p$ bezeichnet und den man den *Körper mit p Elementen* nennt.

Definition Sei R ein kommutativer Ring mit 1. $a \in R$ heißt *Nullteiler,* wenn ein $b \in R - \{0\}$ existiert, so daß $ab = 0$ gilt. Ist 0 der einzige Nullteiler in R, dann heißt R *nullteilerfrei* oder *Integritätsring.*

(9.1) **Satz und Definition** *Sei R ein Integritätsring. Nennt man (a, b), $(c, d) \in R \times (R - \{0\})$ aequivalent, wenn $ad = cb$, dann wird auf diese Weise auf $R \times (R - \{0\})$ eine Aequivalenzrelation definiert. Die Menge aller Aequivalenzklassen*

$$Q(R) = \{\tfrac{a}{b} : a \in R, b \in R - \{0\}\}$$

bilden bezüglich der nachfolgend definierten Verknüpfungen $+$ und $\cdot$ einen Körper, den sogenannten Quotientenkörper von R:

$$\tfrac{a}{b} + \tfrac{c}{d} := \tfrac{ad+bc}{bd}, \tfrac{a}{b} \cdot \tfrac{c}{d} := \tfrac{ac}{bd}.$$

Beweis: Alle Behauptungen sind leicht zu beweisen.

Definition Sei R ein Ring. Eine nichtleere Teilmenge $S \subset R$ heißt *Teilring* von R, wenn für alle $a, b \in S$ gilt: $a - b \in S, a \cdot b \in S$. Hat R ein Einselement 1, dann heißt eine nichtleere Teilmenge $S \subset R$ Teilring von R, wenn S zusätzlich zu den beiden obigen Eigenschaften das Einselement 1 enthält.

Definition Seien R_1, R_2 Ringe. Ein *Homomorphismus* von R_1 nach R_2 ist eine Abbildung $f : R_1 \to R_2$ mit

$$f(a+b) = f(a) + f(b), f(ab) = f(a)f(b)$$

für alle $a, b \in R_1$. Wenn R_1 und R_2 Einselemente besitzen, dann heißt ein Homomorphismus $f : R_1 \to R_2$ ein Homomorphismus von Ringen mit 1, wenn

$$f(1) = 1.$$

gilt. Sei $f : R_1 \to R_2$ ein Ringhomomorphismus. Dann heißt

$$Kern(f) := \{a \in R_1 : f(a) = 0\}$$

der Kern von R_1; $Kern(f)$ ist eine Untergruppe von R_1. Das Bild von f, also

$$Bild(f) := f(R_1) := \{f(a) := a \in R_1\},$$

ist ein Teilring von R_2.

Beispiel Sei m eine natürliche Zahl $\geqq 2$. Dann ist die Abbildung $f : \mathbb{Z} \to R_m$, die jedem $a \in \mathbb{Z}$ den Rest, der bei Division von a durch m übrig bleibt, zuordnet, ein Homomorphismus von Ringen mit 1. Der Kern von f ist $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$.

Definition Sei R ein Ring mit Einselement 1. Ein *Linksideal* bzw. *Rechtsideal* von R ist eine Teilmenge $I \subset R$ mit den folgenden Eigenschaften: Für alle $x, y \in I$ gilt $x - y \in I$ und für alle $x \in I$ und alle $a \in R$ gilt $ax \in I$ bzw. $xa \in I$. Ein *Ideal* oder *zweiseitiges Ideal* von R ist eine Teilmenge $I \subset R$, die sowohl Links- als auch Rechtsideal von R ist.

Bemerkungen (1) Der Kern jedes Homomorphismus von Ringen mit 1 ist ein zweiseitiges Ideal.

(2) Wenn ein zweiseitiges Ideal I eines Ringes R mit 1 das Einselement 1 enthält, dann gilt $I = R$; denn für alle $a \in R$ gilt $a = a \cdot 1 \in I$, also $R \subset I$. Es folgt: Ist k ein Körper und ist $I \subset k$ ein Ideal, dann ist $I = \{0\}$ oder $I = k$.

(3) Ist M eine Teilmenge eines Ringes R mit 1, dann ist die Menge RM aller endlichen Summen der Form $\Sigma_{i \in I} a_i m_i$ mit $a_i \in R$ und $m_i \in M$ ein Linksideal von R, das auch *das von M erzeugte Linksideal* genannt wird; analog definiert man *das von M erzeugte Rechtsideal* MR von R. Und für $M \subset R$ ist die Menge RMR aller endlichen Summen der Form $\Sigma_{i \in I} a_i m_i b_i$ mit $a_i \in R$, $b_i \in R$, $m_i \in M$ ein zweiseitiges Ideal von R, das sogenannte *von M erzeugte Ideal*, das manchmal auch in der Form (M) geschrieben wird.

Definition Ein kommutativer Ring R heißt *Hauptidealring*, wenn jedes Ideal von R mit nur einem Element erzeugbar ist

Wir werden später sehen, daß z. B. die Ringe $\mathbb{Z}$ und $k[X]$, wobei k ein Körper ist, Hauptidealringe sind.

(9.2) **Satz und Definition** *Sei R ein Ring und sei $I \subset R$ ein zweiseitiges Ideal. $a, b \in R$ heißen kongruent modulo I, geschrieben*

$$a \equiv b \bmod I,$$

falls $a-b \in I$. Auf diese Weise wird auf R eine Aequivalenzrelation definiert. Die Menge aller Aequivalenzklassen

$$R \setminus I = \{a + I : a \in R\}, a + I := \{a + x : x \in I\},$$

bildet bezüglich der nachfolgend definierten Verknüpfungen $+$ und $\cdot$ einen Ring, den sogenannten Faktorring von R modulo I, geschrieben R/I :

$$(a + I) + (b + I) := (a + b) + I, \ \ (a + I) \cdot (b + I) := ab + I.$$

Beweis: Der wesentliche Punkt ist die Wohldefiniertheit der Multiplikation. Sei dazu $(a+I, b+I) = (a'+I, b'+I)$. Dann gilt aufgrund der Idealeigenschaften von I :

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I,$$

also $(a + I) \cdot (b + I) = (a' + I) \cdot (b' + I)$.

Sei R ein Ring mit 1 und sei $I \subset R$ ein zweiseitiges Ideal. Dann ist die Abbildung

$$R \to R/I, a \to a + I,$$

ein surjektiver Homomorphismus von Ringen mit 1, der sogenannte *Restklassenhomomorphismus zu I*. Er hat den Kern I.

(9.3) **Satz** *(*Erster Isomorphiesatz für Ringe*) Sei $f : R_1 \to R_2$ ein Homomorphismus von Ringen. Dann wird durch die Zuordnung $a + Kern(f) \mapsto f(a)$ ein Isomorphismus von Ringen*

$$R_1/Kern(f) \xrightarrow{\cong} Bild(f).$$

definiert.

Beweis: Klar**.**

Definition Sei R ein kommutativer Ring mit 1. Ein Ideal $I \subsetneq R$ heißt Primideal, falls der Faktorring R/I nullteilerfrei ist. Ein Ideal $I \subsetneq R$ heißt maximal, falls kein Ideal $J \subset R$ mit $I \subsetneq J \subsetneq R$ existiert.

(9.4) **Satz** *Sei R ein kommutativer Ring mit 1 und sei $\mathfrak{a} \subsetneq R$ ein Ideal von R. Dann existiert ein maximales Ideal $\mathfrak{m}$ von R mit $\mathfrak{a} \subset \mathfrak{m}$.*

Beweis: Sei $\mathcal{S}$ die Menge aller Ideale $I \subsetneq R$ mit $\mathfrak{a} \subset I$. $\mathcal{S}$ ist eine bezüglich der Inklusion teilweise geordnete Menge, die $\mathfrak{a}$ enthält. Sei (I_j) eine Kette in $\mathcal{S}$ und sei

$$I := \cup_j I_j.$$

Dann ist $I \subset R$ ein Ideal. Es gilt $I \neq R$, weil $1 \notin I_j$ für alle j. Also gilt $I \in \mathcal{S}$, und I ist eine obere Schranke für die Kette (I_j). Also hat $\mathcal{S}$ nach dem Lemma von Zorn (vgl. §1) ein maximales Element. Daraus folgt die Behauptung..

(9.5) **Satz** *Sei R ein kommutativer Ring mit 1 und sei $I \subset R$ ein Ideal. Dann gilt: I ist maximal genau dann, wenn der Faktorring R/I ein Körper ist.*

Beweis: Sei R/I ein Körper. Angenommen es gibt ein Ideal $J \subset R$ mit $I \subsetneq J \subsetneq R$. Dann existieren Elemente $a \in J \setminus I$ und $b \in R$ mit $ab \equiv 1 \bmod I$. Es folgt:: $1 = -((ab-1) - ab) \in J$, also $R = J$; Widerspruch!
Sei umgekehrt $I \subset R$ maximal und sei $a \in R \setminus I$. Dann ist

$$J := (I, a) := \{\alpha x + \beta a : \alpha, \beta \in R, x \in I\}$$

ein Ideal mit $I \subsetneq J$; also gilt $J = R$. Somit existiert ein $\beta \in R$ mit

$$1 \equiv a\beta \bmod I,$$

d.h. a ist invertierbar modulo I. R/I ist also ein Körper.

(9.6) **Folgerung** Sei R ein kommutativer Ring mit 1. Jedes maximale Ideal von R ist ein Primideal.

(9.7) **Hilfssatz und Definition** *Sei R ein kommutativer Ring mit 1. Seien $I_1, ..., I_n$ Ideale von R. Dann sind auch der Durchschnitt*

$$\cap_{k=1}^{n} I_k$$

und die Summe

$$I_1 + ... + I_n := \{a_1 + ... + a_n : a_k \in I_k\}$$

Ideale von R.

Beweis: Klar.

Definition Seien R_1, R_2 Ringe. Dann wird das cartesische Produkt $R_1 \times R_2$ bezüglich der komponentenweise definierten Addition und Multiplikation zu einem Ring; $R_1 \times R_2$ heißt das direkte Produkt der Ringe R_1 und R_2.

Definition Sei R ein kommutativer Ring mit 1. Ideale $I_1, ..., I_n$ von R heißen teilerfremd, wenn

$$R = I_1 + I_2 + ... + I_n.$$

Der nachfolgende Satz ist von großer Bedeutung in der Ringtheorie.

(9.8) **Satz** *(*Chinesischer Restsatz*) Sei R ein kommutativer Ring mit* 1 *und seien $I_1, ..., I_n$ paarweise teilerfremde Ideale von R $(n \geqq 2)$. Dann ist der Ringhomomorphismus*

$$\begin{aligned} \alpha : R &\to R/I_1 \times R/I_2 \times ... \times R/I_n \\ a &\to (a + I_1, a + I_2, ..., a + I_n) \end{aligned}$$

surjektiv und hat den Kern $\cap_{k=1}^{n} I_k$.

Zum Beweis benötigen wir einige Hilfsmittel:

(9.9) **Hilfssatz** *Seien $I_1, ..., I_n \subset R$ Ideale und sei $P \subset R$ ein Primideal. Wenn dann $\cap_{j=1}^{n} I_j \subset P$, so gibt es ein $k \in \{1, 2, ..., n\}$ mit $I_k \subset P$.*

Beweis: Angenommen für alle $k \in \{1, ..., n\}$ existiert ein $a_k \in I_k \setminus P$. Dann ist $a_1 \cdot ... \cdot a_n \in \cap_{j=1}^{n} I_j \setminus P$, im Widerspruch zur Voraussetzung.

(9.10) **Hilfssatz** *Seien $I_1, I_2, ..., I_n$ paarweise teilerfremde Ideale von R. Dann sind die Ideale*

$$J_k := \cap_{\ell \neq k} I_\ell \quad (k = 1, 2, ..., n)$$

teilerfremd.

Beweis: Angenommen $J_1 + ... + J_n \neq R$. Dann existiert ein maximales Ideal $\mathfrak{m}$ von R mit $J_k \subset \mathfrak{m}$ für $k = 1, 2, ..., n$. Nach (9.9) gibt es ein $\ell \in \{1, 2, ..., n-1\}$ mit $I_\ell \subset \mathfrak{m}$. Wegen $J_\ell \subset \mathfrak{m}$ folgt aus (9.9) die Existenz eines $k \in \{1, ..., n\}, k \neq \ell$, mit $I_k \subset \mathfrak{m}$. Damit erhält man einen Widerspruch zur Teilerfremdheit von I_k und I_ℓ: $R = I_k + I_\ell \subset \mathfrak{m} \neq R$.

Beweis von (9.8): Die Aussage über den Kern von α folgt aus der Definition des Homomorphismus α.
Zum Beweis der Surjektivität von α bilden wir

$J_k := \bigcap_{\ell \neq k} I_\ell;\ \ k = 1, 2, ..., n.$

Die J_k sind nach dem letzten Hilfssatz (9.10) teilerfremd. Es besteht daher eine Gleichung der Form

$1 = \alpha_1 + \alpha_2 + ... + \alpha_n \ \ \text{mit} \ \ \alpha_k \in J_k, k = 1, 2, ..., n;$

und es gilt

$\alpha_k \equiv 1 \bmod I_k, \ \ \alpha_k \equiv 0 \bmod I_\ell \ \ \text{für} \ \ \ell \neq k.$

Sei nun

$(r_1 + I_1, ..., r_n + I_n) \in R/I_1 \times ... \times R/I_n$

vorgegeben. Setze

$r := \sum_{k=1}^{n} r_k \alpha_k.$

Dann gilt

$\alpha(r) = (r_1 + I_1, ..., r_n + I_n).$

Aus dem chinesischen Restsatz folgt aufgrund des ersten Isomorphiesatzes für Ringe (9.3):

(9.11) **Folgerung** α induziert einen Ringisomorphismus

$R/(\cap_{k=1}^{n} I_k) \cong R/I_1 \times ... \times R/I_n$

(9.12) **Beispiel** Sei $R = \mathbb{Z}$ und seien m_1, m_2 teilerfremde ganze Zahlen. Sei $I_k := m_k\mathbb{Z};\ \ k = 1, 2.$ Dann gilt $I_1 \cap I_2 = m_1 m_2 \mathbb{Z}$. Also ergibt sich aus dem chinesischen Restsatz

$\mathbb{Z}/m_1 m_2 \mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$

Es folgt

(9.13) **Satz** *Sei m eine natürliche Zahl $\geqq 2$ und sei*

$m = p_1^{\nu_1} \cdot ... \cdot p_r^{\nu_r}$

die Zerlegung von m in das Produkt von Primzahlpotenzen $p_i^{\nu_i}$ mit paarweise verschiedenen Primzahlen $p_i;\ \ i = 1, 2, ..., r$, gemäß dem Fundamentalsatz der elementaren Zahlentheorie (3.9). Dann gilt

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}$$

$$(\mathbb{Z}/m\mathbb{Z})^* = (\mathbb{Z}/p_1^{\nu_1}\mathbb{Z})^* \times ... \times (\mathbb{Z}/p_r^{\nu_r}\mathbb{Z})^*.$$

Eine ganze Zahl i mit $0 \leq i \leq m-1$ definiert im Restklassenring $\mathbb{Z}/m\mathbb{Z}$ genau dann eine Einheit $i+m\mathbb{Z}$, wenn $ggT(i,m) = 1$ gilt. Also gilt für die unter (6.4) definierte Eulersche Funktion ϕ :

$$\phi(m) = \phi(p_1^{\nu_1}) \cdot ... \cdot \phi(p_r^{\nu_r}).$$

Damit ist die Berechnung der Werte der Eulerschen Funktion auf den Fall einer Primzahlpotenz zurückgeführt, und dieser Fall wird in dem folgenden Satz behandelt:

(9.14) **Satz** *Sei p eine Primzahl und sei $\nu \in N$. Dann gilt*

$$\phi(p^\nu) = (p-1)p^{\nu-1}.$$

Beweis: Es ist $(\mathbb{Z}/p^\nu\mathbb{Z})^* = \{a \in \mathbb{Z}/p^\nu\mathbb{Z} : ggT(a,p) = 1\}$. Wir identifizieren $\mathbb{Z}/p^\nu\mathbb{Z}$ mit $\{a \in \mathbb{Z} : 0 \leqq a \leqq p^\nu - 1\}$. In der geordneten Folge der Zahlen $0, 1, ..., p^\nu - 1$ ist jedes p-te Element durch p teilbar, also

$$|(\mathbb{Z}/p^\nu\mathbb{Z})^*| = |\{a : 0 \leqq a \leqq p^\nu - 1\}| - p^{\nu-1} =$$

$$= p^\nu - p^{\nu-1} = (p-1)p^{\nu-1}.$$

Zusammengefaßt ergibt sich aus der Kenntnis der Primfaktorzerlegung von m also eine Formel für $\phi(m)$:

(9.15) **Satz** *Sei $m = p_1^{\nu_1} \cdot ... \cdot p_r^{\nu_r}$ die Primfaktorzerlegung von m. Dann gilt*

$$\phi(m) = \prod_{i=1}^{r}(p_i - 1)p_i^{\nu_i - 1}.$$

Wir notieren das folgende auf Euler zurückgehende Resultat, das sich durch Anwendung von (6.10) auf die Gruppe $G = (\mathbb{Z}/m\mathbb{Z})^*$ ergibt und das für den Fall "$m = p =$ Primzahl" von Fermat entdeckt wurde und in diesem Fall häufig "Kleiner Satz von Fermat" genannt wird.

(9.16) **Satz** *Für jede zu m teilerfremde ganze Zahl a gilt*

$$a^{\phi(m)} \equiv 1 \bmod m$$

Wir wollen nun die Struktur der Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^*$ in dem Fall untersuchen, daß $m = p^n$ Potenz einer Primzahl p ist. Für $n = 1$ ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper, weil wegen $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$ jedes von 0 verschiedene Element von

$\mathbb{Z}/p\mathbb{Z}$ bezüglich der Multiplikation invertierbar ist. Nach (6.22) ist daher die Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch.

Definition Jede ganze Zahl g mit der Eigenschaft, daß $\overline{g} := g + p\mathbb{Z}$ ein erzeugendes Element von $(\mathbb{Z}/p\mathbb{Z})^*$ ist, heißt *Primitivwurzel modulo p*. Ist g eine Primitivwurzel modulo p und ist $\overline{a} = a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$ ein beliebiges Element, dann existiert genau ein $i \in \{0, 1, ..., p-1\}$ mit $\overline{a} = \overline{g}^i$. i heißt der Index von a bezüglich g und wird mit $ind_{\overline{g}}(\overline{a})$ bezeichnet.

Bemerkung Es gilt $ind_{\overline{g}}(\overline{a}\overline{b}) = ind_{\overline{g}}(\overline{a}) + ind_{\overline{g}}(\overline{b})$ für alle $\overline{a}, \overline{b} \in (\mathbb{Z}/p\mathbb{Z})^*$, und die Abbildung

$$ind_{\overline{g}} : ((\mathbb{Z}/p\mathbb{Z})^*, \cdot) \to (\mathbb{Z}/p\mathbb{Z}, +)$$

ist ein Isomorphismus von der multiplikativen Gruppe $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ in die additive Gruppe $(\mathbb{Z}/p\mathbb{Z}, +)$ und läßt sich daher als *zahlentheoretischer Logarithmus zur Basis* $\overline{g}$ auffassen.

(9.17) **Satz** *Ist $p \neq 2$, dann ist die Gruppe $(\mathbb{Z}/p^n\mathbb{Z})^*$ zyklisch. Die Restklasse von $1 + p$ hat in $(\mathbb{Z}/p^n\mathbb{Z})^*$ die Ordnung p^{n-1}. Außerdem existiert eine Primitivwurzel modulo p, deren Restklasse in $(\mathbb{Z}/p^n\mathbb{Z})^*$ die Ordnung $p-1$ hat.*

Beweis: Durch vollständige Induktion beweist man, daß

$$(1+p)^{p^i} \equiv 1 + p^{i+1} \bmod p^{i+2}$$

für alle $i \in \mathbb{N}_0$ gilt. Es folgt

$$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \bmod p^n$$

$$(1+p)^{p^{n-1}} \equiv 1 \bmod p^n$$

Also hat die Restklasse von $1 + p$ die Ordnung p^{n-1}. Weil die Gruppe $(\mathbb{Z}/p^n\mathbb{Z})^*$ die Ordnung $(p-1)p^{n-1}$ besitzt, ist sie somit zyklisch. Genauer: Ist g eine Primitivwurzel modulo p, dann ist $g' := g^{p^{n-1}}$ ebenfalls eine Primitivwurzel modulo p. Außerdem gilt

$$g'^{p-1} \equiv g^{(p-1)p^{n-1}} \equiv 1 \bmod p^n$$

Es folgt, daß $(\mathbb{Z}/p^n\mathbb{Z})^*$ von $\overline{g'} \cdot \overline{(1+p)}$ erzeugt wird.

Für $p = 2$ gilt

$$(1+4)^{2^i} \equiv 1 + 2^{i+2} \bmod 2^{i+3}$$

für alle $i \in \mathbb{N}_0$. Es folgt

(9.18) **Satz** *Für $n \geq 3$ ist die Gruppe $(\mathbb{Z}/2^n\mathbb{Z})^*$ direktes Produkt der Untergruppen, die von der Restklasse von -1 und von 5 modulo 2^n erzeugt werden. Die Ordnung der Restklasse von 5 modulo 2^n ist gleich 2^{n-2}.*

(9.19) **Anwendung** (Sogenannte public-key-Verschlüsselung; vgl. $[DH]$, $[RSA]$, $[F]$) Man wählt nach dem Zufallsprinzip zwei sehr große Primzahlen p und q, hält p und q geheim aber macht das Produkt $r = p \cdot q$ bekannt. (r heißt "**Sendeschlüssel**"). Außerdem macht man auch eine ganze Zahl e mit $0 \leqq e < \phi(r)$ und $ggT(e, \phi(r)) = 1$ bekannt (e heißt "**Sendezahl**"). (Das Paar (r, e) heißt "**PK-Schlüssel**".) Eine Person, von der man eine Nachricht empfangen möchte, verwandelt die zu sendende Nachricht in eine Zahl x mit $0 \leqq x < r$ und $ggT(x, r) = 1$, und sendet

$$y \equiv x^e \bmod r, \;\; 0 \leqq y < r.$$

Um diese Nachricht zu entschlüsseln, berechnet man ein multiplikatives Inverses d von e modulo $\phi(r)$; das ist möglich, weil man die Zerlegung $r = p \cdot q$ und damit nach (9.15) $\phi(r) = (p-1)(q-q)$ kennt. Dann berechnet man

$$y^d \bmod r \equiv x^{ed} \bmod r \equiv x^{1+\phi(r)k} \bmod r \equiv x \bmod r \; ;$$

dabei folgt die letztgenannte Kongruenz aus $x^{\phi(r)} \equiv 1 \bmod r$, vgl. (9.16).

Beispiel $p = 3$, $q = 5$ (In der Praxis sind die Primzahlen p, q natürlich wesentlich größer zu wählen) Dann ist $r = 15, \phi(r) = (3-1)(5-1) = 8$. Sei $e = 3$. Gesendet wird

$$y \equiv x^3 \bmod 15 \equiv 8 \bmod 15.$$

Es ist

$$ggT(e, n\ \phi(r)) = ggT(3, 8) = 1 = 3 \cdot d + 8 \cdot f$$

mit $d = 3$, $f = -1$. Also gilt

$$x \bmod 15 \equiv y^d \bmod 15 \equiv 8^3 \bmod 15 \equiv 2 \bmod 15$$

Die entschlüsselte Nachricht ist also $2 \bmod 15$.

Die in diesem Verfahren enthaltene Methode ist inzwischen ausgebaut und weiterentwickelt worden. Für eine Übersicht über Anwendungen der Zahlentheorie und der arithmetischen Geometrie auf die Kryptographie vgl. z. B. $[FR]$ und die dort genannte Literatur.

Definition Sei R ein kommutativer Ring mit Einselement 1. $r \in R$ heißt *Teiler von* $s \in R$ oder s heißt *Vielfaches von* r, wenn ein Element $q \in R$ mit $s = qr$ existiert. Ist r ein Teiler von s, dann schreibt man r/s. $r, s \in R$ heißen *assoziiert*, wenn r/s und s/r. Sind r, s assoziiert, dann schreibt man $r \sim s$.

Bemerkung Die Relation "assoziiert" ist eine Aequivalenzrelation. Die Einheiten von R sind genau die zu 1 assoziierten Elemente von R.

(9.20) **Satz** *Sei R ein kommutativer nullteilerfreier Ring mit 1 (Integritätsring). Dann sind für $r, s \in R$ die folgenden Aussagen aequivalent*
(a) $r \sim s$
(b) *Es gibt eine Einheit $\varepsilon \in R^*$ mit $s = \varepsilon r$.*

Der Beweis ist leicht und wird hier nicht ausgeführt.
Bis auf weiteres sei R ein Integritätsring.

Definition $r \in R$ heißt *echter Teiler von* $s \in R$, wenn r ein Teiler von s ist und wenn $r \notin R^*$ und r nicht assoziiert zu s ist. $r \in R$ heißt *irreduziebel*, wenn $r \neq 0, r \notin R^*$ und wenn r keinen echten Teiler besitzt.

Beispiele (1) Die irreduziblen Elemente von $\mathbb{Z}$ sind die Zahlen εp, wobei $\varepsilon \in \{\pm 1\}$ und p eine Primzahl ist.
(2) Die irreduziblen Elemente im Polynomring $k[X]$, k Körper, sind die nichtkonstanten irreduziblen Polynome aus $k[X]$.

Definition Eine *Teilerkette in dem Integritätsring* R ist eine Folge $(r_n)_{n\in\mathbb{N}}$ von Elementen $r_n \in R$ mit r_{n+1}/r_n für alle $n \in \mathbb{N}$. Man sagt, daß in R der *Teilerkettensatz für Elemente* gilt, wenn für jede Teilerkette (r_n) aus R ein $n_0 \in \mathbb{N}$ existiert, so daß $r_{n+1} \sim r_n$ für alle $n \geq n_0$ gilt.

Beispiele (1) In $\mathbb{Z}$ gilt der Teilerkettensatz für Elemente
(2) In $k[X]$, k Körper, gilt der Teilerkettensatz für Elemente
(3) Gilt der Teilerkettensatz für Elemente in R so auch in $R[X]$

Die Beweise sind leicht.
Es gibt Integritätsringe, in denen der Teilerkettensatz für Elemente nicht gilt.

(9.21) **Satz** *Wenn in dem Integritätsring R der Teilerkettensatz für Elemente gilt, so läßt sich jede Nichteinheit $r \in R \setminus \{0\}$ als Produkt von endlich vielen irreduziblen Elementen darstellen.*

Beweis: Vorbemerkung: Sei M eine nichtleere Teilmenge von R. Dann existiert nach Voraussetzung ein $r \in M$ mit der folgenden Eigenschaft: Kein anderes Element von M ist ein echter Teiler von r. Angenommen nun es gibt eine Nichteinheit $r \in R \setminus \{0\}$, die nicht als Produkt von endlich vielen irreduziblen

Elementen dargestellt werden kann. Sei M die Menge all dieser Nichteinheiten. Nach der obigen Vorbemerkung gibt es ein $r \in M$, das kein anderes Element von M als echten Teiler besitzt. r ist nicht irreduzibel. Also gilt $r = r_1 r_2$ mit echten Teilern r_1, r_2 von r. Nach Wahl von r gilt $r_1, r_2 \notin M$. r_1 und r_2 sind also endliche Produkte von irreduziblen Elementen. Also ist auch r Produkt von endlich vielen irreduziblen Elementen. Widerspruch!

Definition Sei R weiterhin ein Integritätsring. $p \in R \setminus \{0\}$ heißt *Primelement*, wenn für alle $a, b \in R$ gilt: Aus p/ab folgt p/a oder p/b.

Beispiele (1) Die Primzahlen sind Primelemente von $\mathbb{Z}$
(2) Die nichtkonstanten irreduziblen Polynome aus $k[X]$, k Körper, sind Primelemente von $k[X]$.

Bemerkung Jedes Primelement ist irreduzibel.

Beweis $p = ab$ impliziert p/a oder p/b, also $a \sim p$ oder $b \sim p$.

(9.22) **Satz** *Seien $r, s \in R$ Produkte von Primelementen:*

$r = p_1 \cdot ... \cdot p_m, \;\; s = q_1 \cdot ... \cdot q_n$

mit Primelementen p_i, q_j. Dann gilt
(i) *Aus r/s folgt $m \leq n$*
(ii) *Ist r ein echter Teiler von s, dann ist $m < n$*
(iii) *Ist $r = s$, dann ist $m = n$ und, bei geeigneter Numerierung, $p_i \sim q_i$ für $i = 1, ..., m$*

Beweisskizze: Aus $p_1 \cdot ... \cdot p_m = q_1 \cdot ... \cdot q_m$ folgt p_1/q_1 oder $p_1/q_2 \cdot ... \cdot q_m$, also OE $p_1 \sim q_1$, und damit wegen der Nullteilerfreiheit $p_2 \cdot ... \cdot p_m \sim q_2 \cdot ... \cdot q_m$, u.s.w.

Definition Ein *ZPE-Ring* oder *faktorieller Ring* ist ein Integritätsring R mit der folgenden Eigenschaft: Jede Nichteinheit $r \in R \setminus \{0\}$ läßt sich als endliches Produkt von Primelementen darstellen.

(9.23) **Satz** *Sei R ein Integritätsring. Die folgenden Aussagen sind aequivalent*
(a) *R ist ein ZPE-Ring*
(b) *In R gilt der Teilerkettensatz für Elemente und jedes irreduzible Element von R ist Primelement*
(c) *In R gilt der Teilerkettensatz für Elemente und die folgende Bedingung ist erfüllt: Stellt man eine Nichteinheit $r \in R \setminus \{0\}$ auf zwei Weisen als Produkt von irreduziblen Elementen dar, dann treten in diesen Darstellungen gleich viele irreduzible Faktoren auf und bei geeigneter Numerierung sind entsprechende irreduzible Faktoren assoziiert*

Beweisskizze: Im wesentlichen bleibt zu zeigen, daß irreduzible Elemente unter der Voraussetzung (c) Primelemente sind. Sei dazu $p \in R$ irreduzibel und Teiler eines Produktes ab von Elementen $a, b \in R$. Dann existiert ein $h \in R$ mit $ab = ph$. Seien $a = p_1 \cdot ... \cdot p_m$, $b = p'_1 \cdot ... \cdot p'_n$ Darstellungen von a und b als Produkte von irreduziblen Elementen $p_1, ..., p_m$; $p'_1, ..., p'_n$. Dann ist

$$p_1 \cdot ... \cdot p_m \cdot p'_1 \cdot ... \cdot p'_n = ph$$

h ist eine Einheit oder ein endliches Produkt von irreduziblen Elementen. Aus (c) folgt, daß $p \sim p_i$ für ein $i \in \{1, ..., m\}$ oder $p \sim p'_j$ für ein $j \in \{1, ..., n\}$. Also gilt p/a oder p/b, d.h. p ist ein Primelement.

Bemerkung Sei R ein Integritätsring und seien $r, s \in R$. Dann gilt $(r) \subset (s)$ genau dann, wenn s/r. Also gilt $(r) = (s)$ genau dann, wenn $r \sim s$. Die Teilbarkeitsbedingung läßt sich also idealtheoretisch ausdrücken.

(9.24) **Satz** *Jeder nullteilerfreie Hauptidealring R ist ein ZPE-Ring.*

Beweis Wir zeigen, daß in R der Teilkettensatz für Elemente gilt und daß jedes irreduzioble Element ein Primelement ist. Sei dazu $(r_n)_{n \in \mathbb{N}}$ eine Teilerkette in R. Dann ist nach der vorstehenden Bemerking $(r_1) \subset (r_2) \subset ...$ eine aufsteigende Kette von Idealen. Die Vereinigung $I = \cup_{n \in \mathbb{N}}(r_n)$ all dieser Ideale ist ein Hauptideal (b). Somit $(r_n) \subset (b)$ für alle $n \in \mathbb{N}$, und es existiert ein n_0 mit $(b) \subset (r_{n_0})$, also $b \sim r_{n_0}$ und damit $r_{n+1} \sim r_n$ für alle $n \geq n_0$. In R gilt also der Teilerkettensatz für Elemente. Sei $r \in R$ ein irreduzibles Element, das ein Produkt ab mit $a, b \in R$ teilt. Angenommen $r \nmid a$ und $r \nmid b$. Das von r und a erzeugte Ideal (r, a) von R ist ein Hauptideal (c). Also c/r, d.h. $c \in R^*$ oder $c \sim r$. Wegen c/a ist $c \nsim r$. Somit $c \in R^*$ und damit $(r, c) = R$. Genauso zeigt man $(r, b) = R$. Man hat also Gleichungen der Form

$$1 = r_1 r + r_2 a = s_1 r + s_2 b$$

mit $r_1, r_2, s_1, s_2 \in R$. Es folgt

$$1 = 1 \cdot 1 = (r_1 s_1 r + r_1 s_2 b + r_2 s_1 a) r + r_1 s_2 ab$$

Somit $r \nmid ab$. Widerspruch!

Definition Ein Integritätsring R heißt *euklidischer Ring*, wenn eine Abbildung

$$h : R \setminus \{0\} \to \mathbb{N}_0 = \{0, 1, 2, ...\}$$

existiert, so daß gilt:

(i) Für alle $a, b \in R - \{0\}$ ist $h(ab) \geqq h(a)$

(ii) Für alle $a, b \in R - \{0\}$ existiert ein $c \in R$:

$h(a - bc) < h(b)$ oder $a = bc$.

Beispiele (1) $R = \mathbb{Z}$ ist ein euklidischer Ring mit $h(a) := |a|$ für alle $a \in \mathbb{Z} - \{0\}$.
(2) Ist K ein Körper, so ist $R = K[X]$ ein euklidischer Ring mit $h(f) := grad(f)$ für alle $f \in K[X]$, $f \neq 0$.
(3) $R = \mathbb{Z}\left[\sqrt[2]{-1}\right] = \{a + \sqrt{-1} := a, b \in \mathbb{Z}\}$ ist ein euklidischer Ring mit $h(a + b\sqrt{-1}) := a^2 + b^2$ für alle $a + b\sqrt{-1} \in R - \{0\}$.

Die nachfolgenden drei Sätze beweist man analog zum Fall $R = \mathbb{Z}$.

(9.25) **Satz** *In einem euklidischen Ring R existiert zu je endlich vielen Elementen $a_1, ..., a_s \in R$ ein größter gemeinsamer Teiler; jeder größte gemeinsame Teiler von $a_1, ..., a_s \in R$ ist von der Form*

$x_1a_1 + x_2a_2 + ... + x_na_n$ mit $x_i \in R$.

(9.26) **Satz** *Jeder euklidische Ring ist ein Hauptidealring.*

Definition Sei R ein Ring mit 1. Ein *R-Linksmodul* oder *Linksmodul über R* ist eine nichtleere Menge M zusammen mit Abbildungen

$+ : M \times M \to M$, $(a, b) \mapsto a + b$ (genannt "Addition")
$\cdot : R \times M \to M$, $(\alpha, a) \mapsto \alpha a$ (genannt "Skalarmultiplikation)

so daß gilt:

(i) M ist bezüglich $+$ eine kommuatative Gruppe. (Das neutrale Element in dieser Gruppe wird mit 0 bezeichnet. Das zu $a \in M$ inverse Element wird mit $-a$ bezeichnet.)

(ii) $(\lambda + \mu)a = \lambda a + \mu a$
$\lambda(a + b) = \lambda a + \lambda b$
$\lambda(\mu a) = (\lambda\mu)a$
$1a = a$

jeweils für alle $a, b \in M$ und alle $\lambda, \mu \in R$.

Ähnlich definiert man den Begriff *R-Rechtsmodul*.
Im Folgenden nennen wir einen R-Linksmodul oder Linlsmodul über R auch einfach *R-Modul* oder *Modul über R*.
Eine nichtleere Teilmenge $N \subset M$ eines R-Moduls M heißt *R-Untermodul* oder *R-Teilmodul* von M, falls für alle $a, b \in N$ gilt $a - b \in N$ und falls für alle $n \in N$, $\alpha \in R$ gilt $\alpha n \in N$.

Sei M ein R-Modul und sei N ein R-Untermodul. Auf der Faktorgruppe M/N bezüglich der durch + definierten Gruppenstruktur ist durch

$$R \times M/N \to M/N, \ \ (a, m+N) \mapsto am+N$$

eine Skalarmultiplikation definiert, und M/N wird so zu einem R-Modul, dem sogenannten *Faktormodul von M modulo N*.

Beispiele (1) R ist bezüglich der Multiplikation in R ein R-Modul
(2) Jedes Linksideal $\mathfrak{a} \subset R$ ist ein R-Untermodul von R; ist R kommutativ, dann ist der Faktorring $R/\mathfrak{a}$ ebenfalls ein R-Modul-
(3) Jede abelsche Gruppe $M = (M, +)$ ist bezüglich der auf M gegebenen Verknüpfung + und bezüglich der wie folgt definierten Skalarmultiplikation ein Modul über dem Ring $R = \mathbb{Z}$:

$$\mathbb{Z}\times M \to M, (\alpha, x) \mapsto \alpha x := \begin{cases} a + ... + a \ \ (\alpha \text{ Summanden, falls } \alpha \geq 0) \\ -\alpha - ... - \alpha \ \ (\ |\alpha| \text{ Summanden, falls } \alpha < 0) \end{cases}$$

(4) Sei $R = k[X]$ der Polynomring in nur einer Unbestimmten X über einem Körper k und sei V ein endlichdimensionaler k-Vektorraum. Sei $A : V \to V$ ein k-Endomorphismus von V. Dann wird V durch die wie folgt definierte Skalatmultiplikation zu einem R-Modul:

$$R \times V \to V, (p(X), v) \mapsto p(A)(v).$$

Definition Seien M, M' R-Moduln. Eine Abbildung $f : M \to M'$ heißt *R-Modulhomomorphismus*, wenn f bezüglich + ein Gruppenhomomorphismus ist und wenn $f(\alpha v) = \alpha f(v)$ für alle $\alpha \in R, v \in V$ gilt.

Bemerkung Ist $f : M \to M'$ ein $R-$Modulhomomorphismus, dann ist $\text{Kern}(f) := \{vM : f(v) = 0\}$ ein R-Untermodul von M und $\text{Bild}(f)$ ist ein R-Untermodul von M'; außerdem ist die Abbildung

$$M/\text{Kern}(f) \to \text{Bild}(f), \ \ v + \text{Kern}(f) \mapsto f(v)$$

ein R-Modulisomorphismus (= bijektiver R-Modulhomomorphismus). Neben diesem sogenannten "ersten Isomorphiesatz" gelten weitere Isomorphiesätze, die wir hier jedoch nicht besprechen.

Definition Sei $\{M_i : i \in I\}$ eine Familie von abelschen Gruppen $M_i = (M_i, +)$. Dann wird die Menge $\coprod_{i\in I} M_i$ aller Folgen der Form $(a_i)_{i\in I}$ mit $a_i \in M_i$ und $a_i \neq 0$ nur für endlich viele $i \in I$ durch komponentenweise Addition zu einer abelschen Gruppe, und sind die M_i R-Moduln, dann wird $\coprod_{i\in I} M_i$ durch die wie folgt definierte Skalarmultiplikation zu einem R-Modul

$R \times \coprod_{i\in I} M_i \to \coprod_{i\in I} M_i,\ \ (\alpha,(a_i)) \mapsto (\alpha a_i)$;

dieser R-Modul heißt die *direkte Summe der* M_i und wird auch mit

$\bigoplus_{i\in I} M_i$

bezeichnet.

Definition Sei M ein R-Modulund sei $S \subset M$ eine nichtleere Teilmenge. Eine *R-Linearkombination von Elementen aus* S ist eine Summe der Form $\sum_{x\in S} a_x x$, wobei $a_x \in R$ und $a_x \neq 0$ nur für endlich viele $x \in S$; die a_x, $x \in S$, heißen auch die *Koeffizienten* dieser Linearkombination. Die Menge $R\langle S\rangle$ aller Linearkombinationen von Elementen aus S ist ein R-Untermodul von M, der sogenannte *von S erzeugte R-Untermodul.* $S \subset M$ heißt *Erzeugendensystem von* M, falls $M = R\langle S\rangle$. Der R-Modul M heißt *endlich erzeugt*, wenn es eine endliche Teilmenge $S \subset M$ gibt, so daß $M = R\langle S\rangle$. Eine nichtleere Teilmenge $S \subset M$ heißt *linear unabhängig über* R, falls für jede Linearkombination $\sum_{x\in S} a_x x$ von Elementen aus S gilt: Wenn $\sum_{x\in S} a_x x = 0$, dann ist $a_x = 0$ für alle $x \in S$. Eine nichtleere Teilmenge $S \subset M$ heißt *linear abhängig*, wenn sie nicht linear unabhängig ist.

Ist $\{M_i : i \in I\}$ eine Familie von R-Untermoduln eines R-Moduls M und gilt für jedes $v \in M$

$v = \sum_{i\in I} v_i$

mit $v_i \in M_i$ und $v_i = 0$ für fast alle $i \in I$, dann schreibt man

$M = \sum_{i\in I} M_i$

und nennt M die *Summe der* M_i.

Bemerkung Ist der R-Modul M Summe der R-Untermoduln N, N' und gilt $N \cap N' = \{0\}$, dann ist $M = N \oplus N'$ die direkte Summe von N und N'.

Definition Eine nichtleere Teilmenge S eines R-Moduls M heißt eine *Basis von* M, wenn M von S erzeugt wird und wenn S linear unabhängig über R ist. Ein R-Modul M heißt *frei*, wenn M eine Basis besitzt oder wenn $M = \{0\}$.

Bemerkungen (1) Ist S eine Basis des R-Moduls M , dann läßt sich jedes Element in eindeutiger Weise als Linearkombination von Elementen aus S darstellen.

(2) Sei $\{x_i : i \in I\}$ eine Basis des R-Moduls M, sei N ein R-Modul und sei $\{y_i : i \in I\} \subset N$ eine Teilmenge. Dann existiert genau ein R-Modulhomomorphismus $f : M \to N$ mit $f(x_i) = y_i$ für alle $i \in I$.

Ist $R = k$ ein Körper, dann ist jeder k-Modul ein k-Vektorraum. Für entsprechende Resultate über k-Vektorräume verweisen wir auf die Anfängervorlesung über lineare Algebra.

Sei k ein kommutativer Ring und sei E ein k-Modul. Sei $End_k(E)$ der Ring aller k-linearen Abbildungen $E \to E$ (k-Endomorphismus von E). Sei R eine k-Algebra, d.h. R ist ein Ring zusammen mit einem Ringhomomorphismus $\alpha : k \to R$, so daß R durch die Abbildung $k \times R \to R$, $(a, x) \mapsto \alpha(a)x$, zu einem k-Modul wird. Eine *Darstellung von R auf E* ist ein Homomorphismus von k-Algebren $R \to End_k(E)$, d.h. ein Ringhomomorphismus $\rho : R \to End_k(E)$ mit der Eigenschaft $(\rho \circ \alpha)(a) = a \cdot id_E$ für alle $a \in k$, wobei $id_E : E \to E$ die identische Abbildung bezeichnet. Wir betrachten E in offensichtlicher Weise als $End_k(E)$-Modul; E ist also auch ein R-Modul vermöge der Abbildung $R \times E \to E$, $(x, v) \mapsto \rho(x)v =: xv$. Eine Untergruppe F der additiven Gruppe von E heißt *invarianter R-Untermodul von E* oder *invariant unter der Darstellung* $\rho : R \to End_k(E)$, falls $RF \subset F$ gilt, d.h. falls $xv \in F$ für alle $x \in R$ und alle $v \in F$. Die Darstellung ρ heißt *irreduzibel* oder *einfach,* wenn $E \neq \{0\}$ und wenn $\{0\}$ und E die einzigen invarianten R-Untermoduln von E sind. Die Darstellung ρ oder der R-Modul E heißen *vollständig reduzibel* oder *halbeinfach*, wenn E sich als direkte Summe von irreduziblen R-Untermoduln darstellen läßt, d.h. es gibt irreduzible R-Untermoduln $E_1, ..., E_m$ von E, so daß zu jedem $v \in E$ Elemente $v_1 \in E_1, ..., v_m \in E_m$ existieren, die durch v eindeutig bestimmt sind, und so daß $v = v_1 + ... + v_m$ gilt; wir schreiben in dieser Situation auch manchmal

$$E = E_1 \oplus ... \oplus E_m$$

Ist der R-Modul E von der Form $E = Rv =: (v)$ mit einem Element $v \in E$, dann heißt E auch *Hauptmodul* oder, genauer, *der von v erzeugte Hauptmodul,* und die Darstellung ρ heißt *Hauptdarstellung.* Ist $E = Rv$ ein Hauptmodul, dann bilden die Elemente $x \in R$ mit $xv = 0$ ein Linksideal $\mathfrak{a}$ von R, und die Zuordnung $R \to E$, $x \mapsto xv$, ergibt einen Isomorphismus von R-Moduln

$$R/\mathfrak{a} \xrightarrow{\cong} E;$$

dabei wird R als Modul über sich selbst und $R/\mathfrak{a}$ wegen $R\mathfrak{a} \subset R$ als Faktormodul aufgefaßt. Für $v_1, ..., v_n \in E$ bezeichne $(v_1, ..., v_n)$ den von $v_1, ..., v_n$ erzeugten R-Untermodul von E, d.h. die Menge aller Linearkombinationen der Form $x_1v_1 + ... + x_nv_n$ mit $x_1, ..., x_n \in R$. Wenn

$$E = E_1 \oplus ... \oplus E_s$$

eine direkte Summe von R-Teilmoduln $E_1, ..., E_s$ ist und wenn jeder dieser Teilmoduln E_i eine k-Basis B_i besitzt, dann ist $B = (B_1, ..., B_s)$ eine k-Basis von E. Für $\varphi \in R$, aufgefaßt als Endomorphismus von E, sei $\varphi_i : E_i \to E_i$ der entsprechende k-Endomorphismus von E_i, d.h. $\varphi_i = \varphi_{|E_i}$ ist die Einschränkung von φ auf E_i. Sei M_i die Matrix zu φ_i bezüglich der Basis B_i. Dann ist

$$M = \begin{pmatrix} M_1 & & 0 & \\ & M_2 & & \\ & & \ddots & \\ 0 & & & M_s \end{pmatrix}$$

die Matrix von φ bezüglich der Basis B von E. Die Matrizen $M_1, ..., M_s$ heißen auch die *Blöcke* der Matrix M. Sei $E' \subset E$ ein R-Untermodul. Angenommen E' besitzt eine k-Basis $v_1, ..., v_m$, die zu einer k-Basis $v_1, ..., v_m, v_{m+1}, ..., v_n$ von E ergänzt werden kann, so wie das im Fall eines Körpers k der Fall ist (Basisergänzungssatz der linearen Algebra). Für $\varphi \in R$ sei M' die Matrix zu $\varphi_{|E'}$. Dann ist die Matrix zu φ von der Form

$$\begin{pmatrix} M' & * \\ 0 & M" \end{pmatrix}$$

wobei die Matrix$\binom{*}{M"}$ durch Transposition aus der Matrix (c_{ji}) der Koeffizienten $c_{ji} \in k$, die in der Darstellung

$$\rho(\varphi)(v_j) = c_{j1}v_1 + ... + c_{jm}v_m + c_{j,m+1}v_{m+1} + ... + c_{mn}v_n,$$

$j = m+1, ..., n$, auftreten, entsteht. $M"$ ist auch die Matrix zur k-linearen Abbildung

$$E/E' \to E/E', v + E' \mapsto \rho(\varphi)(v) + E'$$

bezüglich der Basis $v_{m+1} + E', ..., v_{m+n} + E'$ des k-Faktormoduls E/E'.

Wir beschreiben nachfolgend die Struktur endlich erzeugter Moduln über nullteilerfreien Hauptidealringen und reproduzieren dabei fast wörtlich die entsprechende Darstellung in [*L2*], Chapter XV. Sei also R ein nullteilerfreier Hauptidealring. Sei F ein freier R-Modul mit Basis $(x_i)_{i \in I}$. Dann ist die Cardinalität von I eindeutig durch F bestimmt. Das erkennt man so: Ist $p \in R$ ein Primelement, dann ist nach einer obigen Bemerkung $R/(p)$ ein Körper und der Faktormodul F/pF ist ein Vektorraum über $R/(p)$, dessen Dimension mit der Cardinalität von I übereinstimmt.

Definition Die *Dimension eines freien R-Moduls* F ist die Cardinalität irgendeiner Basis von F.

(9.27) **Satz** *Sei F ein freier R-Modul endlicher Dimension und sei $M \subset F$ ein R-Untermodul. Dann ist M ebenfalls frei, und die Dimension von M ist nicht größer als die Dimension von F.*

Bemerkung Dieser Satz gilt auch ohne die Voraussetzung, daß F endliche Dimension besitzt.

Beweis von (9.27): Sei $x_1, ..., x_n$ eine Basis von F. Setze $M_r := M \cap (x_1, ..., x_r)$. M_1 ist ein Untermodul von (x_1), also $M_1 = (a_1 x_1)$ mit $a_1 \in R$. Somit ist M_1 entweder gleich $\{0\}$ oder frei von der Dimension 1. Nach Induktionsannahme ist M_r frei von der Dimension $\leq r$. Sei $A \subset R$ die Menge aller $a \in R$, so daß ein $x \in M$ von der Form

$$x = b_1 x_1 + ... + b_r x_r + a x_{r+1}$$

mit $b_1, ..., b_r \in R$ existiert. A ist ein Ideal von R. Sei $a_{r+1} \in R$ so, daß $A = (a_{r+1})$. Wenn $a_{r+1} = 0$, dann ist $M_{r+1} = M_r$, also ist M_{r+1} frei von der Dimension $\leq r + 1$. Wenn $a_{r+1} \neq 0$ ist, dann sei $w \in M_{r+1}$ so, daß der Koeffizient von w bezüglich x_{r+1} gleich a_{r+1} ist. Ist $x \in M_{r+1}$, dann ist der Koeffizient von x bezüglich x_{r+1} durch a_{r+1} teilbar. Also existiert ein $c \in R$, so daß $x - cw \in M_r$, also $x \in M_r + (w)$. Nach Konstruktion ist $M_r \cap (w) = 0$. Es folgt

$$M = M_r \oplus (w)$$

und damit die Behauptung.

(9.28) **Folgerung** Sei E ein endlich erzeugter R-Modul und $E' \subset E$ ein Untermodul. Dann ist E' ebenfalls ein endlich erzeugter R-Modul.

Beweis: Seien $v_1, ..., v_n$ erzeugende Elemente von E. Sei F ein freier R-Modul der Dimension n und sei $x_1, ..., x_n$ eine Basis von F (z.B. $F = R^n$ mit der Basis $(x_i)_{i=1,...,n}$ mit $x_i = (0, ..., 0, 1, 0, ..., 0)$, wobei die 1 an der i-ten Stelle steht). Die durch die Zuordnung $v_i \mapsto x_i$ definierte Abbildung $F \to E$ ist ein surjektiver R-Modulhomomorphismus. Das Urbild von E' in F unter dieser Abbildung ist ein Untermodul von F, der nach dem vorstehenden Satz frei von der Dimension $\leq n$ ist. Also ist E' endlich erzeugt.

Sei R ein nullteilerfreier Hauptidealring und sei E ein R-Modul. E heißt *Torsionsmodul*, wenn für alle $v \in E$ ein $a \in R - \{0\}$ existiert, so daß $av = 0$ ist. $v \in E$ heißt *Torsionselement*, wenn ein $a \in R - \{0\}$ existiert, so daß $av = 0$ ist. Ist E ein R-Modul, dann ist die Menge E_t aller Torsionselemente von E ein R-Untermodul von E, der sogenannte *Torsionsuntermodul* von E. Ist $E_t = \{0\}$, dann heißt E *torsionsfrei.*

(9.29) **Satz** *Sei E ein endlich erzeugter R-Modul. Dann ist der Faktormodul E/E_t frei. Außerdem existiert ein freier R-Untermodul von R , so daß $E = E_t \oplus F$, und die Dimension eines solchen freien Untermoduls von E ist eindeutig bestimmt.*

Beweis: Für $v \in E$ sei $\overline{v} := v + E_t$. Sei $v \in E$ so, daß ein $b \in R - \{0\}$ mit $b\overline{v} = \overline{0}$ exisitiert. Dann ist $bv \in E_t$. Also exisitiert ein $c \in R - \{0\}$, so daß $cbv = 0$. Also ist $v \in E_t$, d.h. $\overline{v} = \overline{0}$. Es folgt, daß E/E_t torsionsfrei ist.

Mit E ist auch E/E_t ein endlich erzeugter R-Modul. Sei M irgendein endlich erzeugter torsionsfreier R-Modul. Sei $y_1, ..., y_m$ ein Erzeugendensystem von M und sei $\{v_1, ..., v_n\} \subset \{y_1, ..., y_m\}$ eine maximale linear unabhängige Teilmenge. Für $y \in \{y_1, ..., y_m\}$ existieren Elemente $a, b_1, ..., b_n \in R$, die nicht alle 0 sind, so daß

$$ay + b_1v_1 + ... + b_nv_n = 0.$$

Aus der linearen Unabhängigkeit der $v_1, ..., v_n$ folgt $a \neq 0$. Also existiert zu jedem $j \in \{1, ..., m\}$ ein $a_j \in R - \{0\}$, so daß $a_jy_j \in (v_1, ..., v_n)$. Setze $a := a_1 \cdot ... \cdot a_m$. Dann ist $a \neq 0$ und $aM \subset (v_1, ..., v_n)$. Die Abbildung $M \to M$, $v \mapsto av$, ist ein injektiver Homomorphismus, dessen Bild in einem freien R-Modul enthalten ist, und dieses Bild ist isomorph zu M. Aus (9.27) folgt, daß M frei ist.

Um den in der Behauptung genannten freien R-Modul zu konstruieren, benötigen wir den folgenden Hilfssatz.

Hilfssatz *Seien E, E' R-Moduln. Sei E' frei. Sei $f : E \to E'$ ein Epimorphismus. Dann existiert ein freier Untermodul F von E, so daß die Einschränkung von f auf F ein Isomorphismus $F \cong E'$ ist und so daß $E = F \oplus Kern(f)$ gilt.*

Beweis: Sei $(v'_i)_{i \in I}$ eine Basis von E' und für jedes $i \in I$ sei $v_i \in E$ so, daß $f(v_i) = v'_i$. Sei F der von den v_i, $i \in I$, erzeugte Untermodul. Aus der linearen Unabhängigkeit der v'_i, $i \in I$, folgt die lineare Unabhängigkeit der v_i, $i \in I$. Also ist F frei. Zu jedem $v \in E$ existieren $a_i \in R$, $i \in I$, so daß

$$f(v) = \sum_{i \in I} a_i v'_i,$$

also $v - \sum_{i \in I}, a_i v_i \in Kern(f)$. Es folgt $E = Kern(f) + F$, und wegen $Kern(f) \cap F = \{0\}$ auch $E = Kern(f) \oplus F$. Der Hilfssatz ist damit bewiesen.

Um den Beweis von (9.29) zu Ende zu führen, wenden wir diesen Hilfssatz auf den Epimorphismus $E \to E/E_t$, $v \mapsto v + E_t$, an und erhalten $E = F \oplus E_t$. Die Dimension von F ist durch E eindeutig bestimmt, weil jedes F' mit der Eigenschaft $E = F' \oplus E_t$ isomorph zu E/E_t ist.

Sei E ein R-Modul, wobei R nach wie vor ein nullteilerfreier Hauptidealring ist. Für jedes $v \in E$ ist die Abbildung $R \to (v) = Rv$, $a \mapsto av$, ein R-Modulhomomorphismus. Dessen Kern R_a ist ein Ideal von R, das von einem Element $m \in R$ erzeugt wird; ein solches m heißt eine *Periode von v*. Ein Element $c \in R$ heißt *Exponent von E bzw. von $v \in E$*, wenn $c \cdot w = 0$ für alle $w \in E$ bzw. wenn $cv = 0$ gilt. Sei $p \in R$ ein Primelement und sei $E(p)$ der Untermodul von E, der aus allen Elementen aus E besteht, die eine Periode der Form p^r mit $r \in \mathbb{N}$ besitzen. Ein p-Untermodul von E ist ein Untermodul von $E(p)$. Sei

P ein Vertretersystem für die Klassen von assoziierten Primelementen von R. Ein R-Modul E heißt zyklisch, wenn ein $a \in R$ existiert, so daß E isomorph zu dem R-Modul $R/(a)$ ist; a heißt dann auch die *Ordnung von* E. Seien $r_1, ..., r_s$ natürliche Zahlen. Ein R-Modul E heißt *vom Typ* $(p^{r_1}, ..., p^{r_s})$ oder, wenn p fest gewählt ist, vom Typ $(r_1, ..., r_s)$, wenn E isomorph zum Produkt der zyklischen Moduln $R/(p^{r_1}), ..., R/(p^{r_s})$ ist.

(9.30) **Satz** *Sei $E \neq \{0\}$ ein endlich erzeugter R-Torsionsmodul. Dann gilt*

$$E = \oplus_{p \in P} E(p),$$

und es existieren eindeutig bestimmte natürliche Zahlen $1 \leq \nu_1 \leq ... \leq \nu_s$, so daß

$$E(p) \cong R/(p^{\nu_1}) \oplus ... \oplus R/(p^{\nu_s})$$

Beweis: Sei $a \in R$ ein Exponent für E. Schreibe $a = bc$ mit teilerfremden $b, c \in R$, und seien $x, y \in R$ so, daß

$$1 = xb + yc.$$

Für jedes $v \in E$ gilt dann

$$v = xbv + ycv.$$

Dann ist $xbv \in E_c$ wegen $cxbv = xbcv = xav = 0$. Ähnlich folgt $ycv \in E_b$. Somit ist $E = E_c + E_b$. Außerdem gilt $E_b \cap E_c = 0$. Also $E = E_c \oplus E_b$. Es folgt $E = \oplus_{p \in \mathfrak{P}} E(p)$.

Wir zeigen nun die behauptete Zerlegbarkeit von $E(p)$. Vorweg eine Definition: Elemente $y_1, ..., y_m$ eines R-Moduls heißen *unabhängig*, wenn aus dem Bestehen einer Relation der Form $a_1 y_1 + ... + a_m = 0$ mit $a_i \in R$ folgt; $a_i y_i = 0$

für $i = 1, 2, ..., m$. Gleichbedeutend damit ist die Aussage

$$(y_1, ..., y_m) = (y_1) \oplus ... \oplus (y_m)$$

Wir benötigen den folgenden Hilfssatz

Hilfssatz *Sei E ein R-Torsionsmodul vom Exponenten p^r mit $r \in \mathbb{N}$, wobei p ein Primelement von R ist. Sei $x_1 \in E$ ein Element mit der Periode p^r und sei $\overline{E} = E/(x_1)$. Seien $\overline{y_1}, ..., \overline{y_m} \in \overline{E}$ unabhängige Elemente. Dann exisitert zu jedem $\overline{y_i}$ ein Repräsentant $y_i \in E$, so daß die Perioden von y_i und $\overline{y_i}$ übereinstimmen. Außerdem sind die Elemente $x_1, y_1, ..., y_m$ unabhängig.*

Beweis: Sei p^n die Periode von $\overline{y_i} \in \overline{E}$. Sei $y \in E$ ein Repräsentant von $\overline{y} \in \overline{E}$. Dann ist $p^n y \in (x_1)$, also $p^n y = p^s c x_1$ mit $c \in R$, $p \nmid c$, $s \leq r$. Ist $s = r$,

dann hat y dieselbe Periode wie $\overline{y}$. Ist $s < r$, dann hat $p^s c x_1$ Periode p^{r-s}, also hat y Periode p^{n+r-s}. Da p^r ein Exponent für E ist, gilt $n + r - s \leq r$. Somit ist $n \leq s$ und $y - p^{s-n} \subset x_1$ ist ein Repräsentant für $\overline{y}$ mit Periode p^n. Sei y_i ein Repräsentant von $\overline{y_i}$ mit derselben Periode wie y_i. Wir zeigen, daß $x_1, y_1, ..., y_m$ unabhängig sind. Seien dazu $a, a_1, ..., a_m \in R$ so, daß

$$ax_1 + a_1 y_1 + ... + a_m y_m = 0.$$

Dann folgt

$$a_1 \overline{y_1} + ... + a_m \overline{y_m} = \overline{0}$$

Da $\overline{y_1}, ..., \overline{y_m} \in \overline{E}$ nach Voraussetzung unabhängig sind, folgt $a_i \overline{y_i}$ für $i = 1, ..., m$. Die Periode p^{r_i} von $\overline{y_i}$ teilt a_i. Somit $a_i y_i = 0$ für $i = 1, ..., m$ und damit $ax_1 = 0$. Der Hilfssatz ist bewiesen.

Um nun die behauptete Zerlegung für $E(p)$ zu erhalten, bemerken wir zunächst, daß $E(p)$ endlich erzeugt ist, also OE $E = E(p)$. Sei $x_1 \in E$ so, daß für dessen Periode p^{r_1} gilt: r_1 ist maximal; und sei $\overline{E} = E/(x_1)$. Behauptung: Die Dimension von $\overline{E_p}$ als Vektorraum über dem Körper R/pR ist echt kleiner als die Dimension des R-Moduls E_p. Beweis: Seien $\overline{y_1}, ..., \overline{y_m}$ R/pR-linear unabhängige Elemente aus $\overline{E_p}$. In (x_1) exisitert ein von $y_1, ..., y_m$ unabhängiges Element mit Periode p. Daher folgt aus dem vorstehenden Hilfssatz, daß $\dim E_p \geq m + 1$, also $\dim \overline{E_p} < \dim E_p$. Die behauptete Zerlegung von E folgt nun induktiv: Ist $\overline{E} \neq 0$, dann existieren Elemente $\overline{x_2}, ..., \overline{x_s} \in \overline{E}$ mit den jeweiligen Perioden $p^{r_2}, ..., p^{r_s}$, so daß $r_2 \geq ... \geq r_s$ Nach dem vorstehenden Hilfssatz exisitieren Repräsentanten $x_2, ..., x_r \in E$, so daß x_i Periode p^{r_i} besitzt und so daß $x_2, ..., x_r$ unabhängig sind. Nach Wahl von r_1 gilt $r_1 \geq r_2$. Die behauptete Zerlegung von $E = E(p)$ folgt. Die behauptete Eindeutigkeit der Folge $\nu_1, ..., \nu_s$ ergibt sich aus dem folgenden allgmeineren Resultat.

(9.31) **Satz** *Sei $E \neq \{0\}$ ein endlich erzeugter R-Torsionsmodul. Dann ist*

$$E \cong R/(q_1) \oplus ... \oplus R/(q_r)$$

mit von 0 verschiedenen Elementen $q_1, ..., q_r$, so daß $q_1/q_2/.../q_r$ und so daß die Folge der Ideale $(q_1), ..., (q_r)$ durch diese Eigenschaften eindeutig bestimmt ist.

Beweis: Aufgrund der bereits bewiesenen Behauptungen aus (9.30) gibt es Primelemente $p_1, ..., p_l \in R$ mit

$$E = E(p_1) \oplus ... \oplus E(p_l),$$

und zu jedem $i = 1, ..., l$ exisitert eine endliche Folge von natürlichen Zahlen $r_{i1} \leq r_{i2} \leq ...$ mit

$E(p_i) = R/(p_i^{r_{i1}}) \oplus R/(p_i^{r_{i2}}) \oplus ...$

Setze $q_i = p_1^{r_{1i}} p_2^{r_{2i}} ... p_l^{r_{li}}$. Dann ist

$R/(p_1^{r_{1i}}) \oplus R/(p_2^{r_{2i}}) \oplus ... \cong R/(q_i)$

Somit ergibt sich die behauptete Zerlegung

$E \cong R(q_1) \oplus R/(q_2) \oplus ... \oplus R/(q_r)$

mit $q_1/q_2/.../q_r$. Es bleibt die Eindeutigkeit der Idealfolge $(q_1), ..., (q_r)$ zu beweisen. Sei dazu $p \in R$ ein Primelement und sei $E = R/(pb)$ mit $b \in R \setminus \{0\}$. Dann ist E_p der Untermodul $bR/(pb) \subset E$, und der Kern des Homomorphismus

$R \to bR \to bR/(pb)$, $x \mapsto bx + (pb)$

ist (p), also

$R/(p) \cong bR/(pb)$.

Ist

$E \cong R/(q_1) \oplus ... \oplus R/(q_r)$,

dann folgt: $v = v_1 \oplus ... \oplus v_r \in E$, $v_i \in R/(q_i)$, gehört zu E_p genau dann, wenn $pv_i = 0$ für alle $i = 1, ..., r$. Somit ist E_p die direkte Summe derjenigen Untermoduln der $R/(q_i), i = 1, ..., r$, die jeweils gleich dem Kern des Homomorphismus $v \mapsto pv$ sind. Die Dimension des $R/(p)$-Vektorraums E_p ist gleich der Anzahl der $R/(q_i)$ mit p/q_i. Sei p ein Primelement, das q_1 und damit auch $q_2, ..., q_r$ teilt. Sei

$E = R/(q_1') \oplus ... \oplus R/(q_s')$

eine Zerlegung wie in der Behauptung des Satzes. Dann teilt p mindestens r der Elemente $q_1', ..., q_s'$, also $r \leq s$. Durch Vertauschen der Rollen von $q_1, ..., q_r$ und $q_1', ..., q_s'$ folgt auch $s \leq r$. Somit $r = s$ und p teilt $q_1', ..., q_r'$. Nach den obigen Bemerkungen gilt

$pE \cong R/(b_1) \oplus ... \oplus R/(b_r)$ mit $q_i = pb_i$,

insbesondere $b_1/b_2/.../b_r$. Induktiv erkennt man, daß die Nichteinheiten unter den $b_1, ..., b_r$ das von ihnen erzeugte Hauptideal eindeutig bestimmen. Die behauptete Eindeutigkeit folgt. Damit ist der Beweis von (9.31) beendet.

Definition Die Ideale $(q_1), ..., (q_r)$ in (9.31) heißen die *Invarianten von* E.

Als Folgerung aus (9.31) notieren wir den sogenannten *Elementarteilersatz.*

(9.32) **Satz** *Sei F ein freier Modul über dem nullteilerfreien Hauptidealring R und sei $M \subset F$, $M \neq \{0\}$, ein endlich erzeugter R-Untermodul. Dann exisitieren eine Basis B von F, Elemente $e_1, ..., e_r \in B$ und von 0 verschiedene Elemente $a_1, ..., a_r \in R$, so daß gilt*

(i) *Die Elemente $a_1e_1, ..., a_re_r$ bilden eine Basis von M über R*

(ii) *a_i teilt a_{i+1} für $i = 1, ..., r-1$*

Außerdem ist die Folge der Ideale $(a_1), ..., (a_r)$ durch die vorstehenden Bedingungen (i) *und* (ii) *eindeutig bestimmt.*

Für den Hauptidealring $R = \mathbb{Z}$ enthält (9.31) den sogenannten Hauptsatz über endlich erzeugte abelsche Gruppen. Ist k ein Körper und R der Hauptidealring $k[X]$ aller Polynome in nur einer Unbestimmten X mit Koeffizienten aus k, dann führt (9.31) zur sogenannten Jordanschen Normalform eines Endomorphismus $A : E \to E$ eines endlichdimensionalen k-Vektorraums E, indem man E vermöge der Abbildung

$$k[X] \times E \to E, (p(X), v) \mapsto p(A)(v)$$

als R-Modul auffaßt; für Einzelheiten vgl. [$L2$], XV, § 3.

Nachfolgend werden weitere Grundlagen über Körper zusammengestellt., die zum Teil auf L. Kronecker , E. Galois, K. Steinitz und E.H. Moore zurückgehen und die in vielen Lehrbüchern über Algebra behandelt werden, vgl. z.B. [KU]; [$L2$]; [R], Appendix VI; [W].

(9.33) **Hilfssatz** *Jedes Primideal $I \neq \{0\}$ in einem Hauptidealring R ist maximal.*

Beweis; Sei $Y \subset R$ ein Ideal mit der Eigenschaft $I \subsetneq J$. Seien $a, b \in R$ so, daß $I = (a)$, $J = (b)$. Schreibe $a = rb$ mit $r \in R$. Die Primidealeigenschaft von I impliziert $b \in I$ oder $r \in I$. $b \in I$ hat zur Folge, daß $J \subset I$, im Widerspruch zu $I \subset J, I \neq J$. Somit ist $r \in I$, also $r = sa$ mit einem Element $s \in R$. Es folgt: $a = rb = sab$, $a(1 - sb) = 0$, $1 = sb \in (b) = J$, $J = R$. Also ist I maximal.

(9.34) **Satz** (L. Kronecker) *Sei ein k Körper und sei $p(X) \in k[X]$ ein irreduzibles Polynom. Dann existiert ein Körper K, der einen zu k isomorphen Teilkörper k' und eine Nullstelle von $p(X) \in k'[X]$ enthält.*

Beweis: Sei $I = (p(X)) = k[X]\,p(X)$ das von $p(X)$ erzeugte Ideal von $k[X]$. Da $k[X]$ ein Hauptidealring ist, vgl. (3.13) und (9.21), und da $p(X)$ irreduzibel ist, ist der Faktorring $K := k[X]/I$ nach dem vorstehenden Hilfssatz (9.33) ein Körper. K enthält den zu k isomorphen Körper, der aus allen Restklassen der Form $a + I$ mit $a \in k$ besteht; und eine leichte Rechnung zeigt, daß $X + I \in K$ eine Nullstelle von $p(X)$ ist.

(9.35) **Folgerung** Sei k ein Körper und sei $f(X) \in k[X]$ ein Polynom vom Grad $n \geq 1$. Dann existiert ein Körper L, der einen zu k isomorphen Teilkörper enthält und so daß sich $f(X) \in L[X]$ als Produkt von Polynomen vom Grad 1 darstellen läßt. L enthält alle Nullstellen von $f(X)$.

Beweis: Für $n = 1$ ist die Behauptung klar. Für $n > 1$ gilt $f(X) = p(X)g(X)$ mit einem irreduziblen Polynom $p(X) \in k[X]$ und einem weiteren Polynom $g(X) \in k[X]$, vgl. (3.13). Nach (9.34) existiert ein Körper K, der einen zu k isomorphen Teilkörper k' und eine Nullstelle β von $p(X) \in k'[X]$ enthält. Somit gilt $p(X) = (X - \beta)h(X)$ mit $h(X) \in K[X]$, vgl. (3.14). Wegen $grad(h(X)g(X)) < n$ existiert ein Körper L, der K als Teilkörper enthält, so daß sich $h(X)g(X)$ und damit $f(X) = (X-\beta)h(X)g(X)$ als Produkt von Polynomen vom Grad 1 darstellen läßt.

Definition Sei k ein Körper und sei $f(X) \in k[X]$ ein Polynom vom Grad $n \geq 1$. Eine Körpererweiterung L/k, so daß sich $f(X) \in L[X]$ als Produkt von Polynomen vom Grad 1 darstellen läßt und der keinen echten k enthaltenden Teilkörper enthält, für den diese Aussage richtig ist, heißt *Zerfällungskörper* von $f(X)$

(9.36) **Satz** *Seien k, k' Körper und sei $\varphi : k \to k'$ ein Isomorphismus. Sei $f(X) \in k[X]$ und sei $\varphi(f)(X) \in k'[X]$ das Polynom, das durch Anwendung von φ auf die Koeffizienten von f entsteht. Sei K bzw. K' ein Zerfällungskörper von f bzw. f'. Dann läßt sich φ zu einem Isomorphismus $\widetilde{\varphi} : K \to K'$ fortsetzen.*

Beim Beweis dieses Satzes benutzen wir den folgenden Hilfssatz.

(9.37) **Hilfssatz** *Seien k, k' Körper und sei $\varphi : k \to k'$ ein Isomorphismus. Seien $F/k, F', k'$ Körpererweiterungen. Sei $f(X) \in f[X]$ irreduzibel und sei α eine Nullstelle von $f(X)$ in F und sei α' eine Nullstelle von $\varphi(f)(X)$ in F'. Dann läßt sich φ zu einem Isomorphismus $\widetilde{\varphi} : k(\alpha) \to k'(\alpha')$ fortsetzen.*

Beweis des Hilfssatzes: Durch $\widetilde{\varphi}(\alpha) := \alpha'$ ist eine Fortsetzung von α zu einem Isomorphismus $\widetilde{\varphi} : k(\alpha) \to k'(\alpha')$ definiert.

Beweis von (9.36): Für $(K : k) = 1$ zerfällt $f(X)$ über k in lineare Faktoren, und die Behauptung ist klar. Wir nehmen induktiv an, daß $(K : k) > 1$ und daß die Behauptung für alle Zerfällungskörper, die einen kleineren Grad als $(K : k)$ haben, richtig ist. Dann existieren ein Faktor $p(X) \in k[X]$ von $f(X)$ und eine Nullstelle $\alpha \in K$ von $p(X)$ mit $\alpha \notin k$. sowie eine Nullstelle $\alpha' \in K'$ von $\varphi(p)(X)$, $\alpha' \notin k'$. Nach dem vorstehenden Hilfssatz (9.37) existiert ein Isomorphismus $\widetilde{\varphi} : k(\alpha) \to k'(\alpha')$, der den Isomorphismus $\varphi : k \to k'$ fortsetzt. K bzw. K' ist ein Zerfällungskörper von $f(X) \in k(\alpha)[X]$ bzw. von $\varphi(f)(X) \in k'(\alpha')[X]$. Wegen $(K : k) = (K : k(\alpha))(k(\alpha) : k) > (K : k(\alpha))$ ergibt sich aus der Induktionsvoraussetzung, daß sich $\widetilde{\varphi} : k(\alpha) \to k'(\alpha')$ zu einem Isomorphismus $K \to K'$ fortsetzen läßt. Damit ist der Beweis von (9.36) beendet.

Die *Ableitung* eines Polynoms

$f(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^2$

mit Koeffizienten a_0,a_1,a_2,...,a_n aus einem Körper k ist das Polynom

$f'(X) := a_1 + 2a_2X + ... + na_nX^{n-1}$.

Für die Ableitung von Summen und Produkten von Polynomen gelten die aus der Analysis bekannten Regeln entsprechend.

(9.38) **Hilfssatz** *Sei k ein Körper, sei $f(X) \in k[X]$ und sei L ein Körper, der einen zu k isomorphen Teilkörper und alle Nullstellen von $f(X)$ enthält. Dann sind die folgenden Aussagen aequivalent:*
(a) *f hat keine mehrfachen Nullstellen in L*
(b) *$f(X)$ und $f'(X)$ sind in $L[X]$ teilerfremd.*

Beweis: Angenommen Aussage (a) ist falsch. Dann existiert ein $\beta \in L$, so daß $f(X) = (X-\beta)^2g(X)$, also $f'(X) = 2(X-\beta)g(X)+(X-\beta)^2g'(X)$. $(X-\beta)$ ist also ein Teiler von $f(X)$ und $f''(X)$. Sei umgekehrt Aussage (b) falsch, d.h. es existiert ein $\beta \in L$, so daß $(X-\beta)$ ein Teiler von $f(X)$ und $f'(X)$ in $L[X]$ ist, etwa $f(X) = (X-\beta)g(X)$, $f'(X) = (X-\beta)h(X) = (X-\beta)g'(X) + g(X)$. Dann ist $(X-\beta)$ ein Teiler von $g(X)$ und $(X-\beta)^2$ ist ein Teiler von $f(X)$. $f(X)$ hat also mehrfache Nullstellen in L, d.h. Aussage (a) ist falsch.

Definition Die *Charakteristik* eines Integritätsringes R ist, falls sie existiert, die kleinste natürliche Zahl m mit der Eigenschaft $ma = 0$ für alle $a \in R$. Existiert eine solche Zahl nicht, dann sagt man, daß R die Charakteristik 0 hat.

Die Charakteristik von R ist also diejenige nichtnegative ganze Zahl m, so daß m das Ideal $Kern(\rho)$ erzeugt, wobei $\rho : \mathbb{Z} \to R$ der durch $\rho(z) := z1$ definierte Ringhomomorphismus ist. Hat R eine von 0 verschiedene Charakteristik m, dann ist m eine Primzahl; denn ist $m = pq$ mit natürlichen Zahlen p, q, beide > 1, und ist $pqa = 0$ für alle $a \in R$, dann ist $pq1 = p1q1 = 0$, also $p1 = 0$ oder $q1 = 0$, somit $pa = 0$ für alle $a \in R$ oder $qa = 0$ für alle $a \in R$, im Widerspruch zur Minimalität von m. Aus dem ersten Isomorphiesatz für Ringe folgt: Wenn R die Charakteristik 0 hat, dann ist $\mathbb{Z}$ ein Teilring von R; und wenn R die Charakteristik $p > 0$ hat, dann ist $Kern(\rho) = p\mathbb{Z}$ und damit $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ein Teilring von R. Weiterhin folgt: Ist R ein Körper der Charakteristik 0, dann ist $\mathbb{Q}$ ein Teilkörper von R; und wenn R ein Körper der Charakteristik $p > 0$ ist, dann ist $\mathbb{F}_p$ ein Teilkörper von R. Der *Primkörper eines Körpers K* ist der Durchschnitt aller Teilkörper von K, die die Menge $\{0, 1\} \subset K$ enthalten. Aus den vorstehenden Überlegungen ergibt sich das folgende Resultat.

(9.39) **Satz** *Der Primkörper eines Körpers der Charakteristik 0 ist $\mathbb{Q}$; der Primkörper eines Körpers der Charakteristik $p > 0$ ist $\mathbb{F}_p$*

(9.40) **Hilfssatz** *Ist k ein Körper mit Charakteristik $m = p > 0$, dann gilt für alle $a, b \in k$ und alle $n \in \mathbb{N}$*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Beweis: Für $n = 1$ gilt nach der binomischen Formel

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

mit $\binom{p}{k} = \frac{p!}{(p-k)!k!}$. Für $0 < k < p$ ist $\binom{p}{k}$ durch p teilbar. Also gilt $(a+b)^p = a^p + b^p$. Die Behauptung folgt nun induktiv.

(9.41) **Satz** (E. Galois) *Zu jeder Primzahl p und jeder natürlichen Zahl n existiert ein Körper, der genau p^n Elemente enthält*

Beweis: Sei $q := p^n$. Sei L ein Körper, der einen zu $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ isomorphen Teilkörper und alle Nullstellen von $f(X) := X^q - X \in \mathbb{F}_p[X]$ enthält, und sei $M \subset L$ die Menge aller Nullstellen von $f(X)$, vgl. (9.35). Nach (3.15) hat $f(X)$ höchstens q Nullstellen, also $|M| \leq q$. Offensichtlich gilt $|M| = q$ genau dann, wenn $f(X)$ keine mehrfachen Nullstellen in L hat, und das ist nach (9.38) der Fall; denn $f(X) = X^q - X$ und $f'(X) = qX^{q-1} - 1 = -1$ sind teilerfremd. M ist ein Teilkörper von L. Daß M ein Teilring von L ist erkennt man leicht mit Hilfe von (9.40). Daß jedes von 0 verschiedene Element $\alpha \in M$ invertierbar ist, folgt aus der Gleichung $\alpha^{q-1} = \alpha\alpha^{q-2} = 1$.

(9.42) **Satz** (E.H. Moore) *Je zwei Körper, die jeweils p^n Elemente enthalten, sind isomorph.*

Beweis: Der Körper K enthalte genau $q = p^n$ Elemente. Da K^* eine endliche Gruppe der Ordnung $q-1$ ist, gilt nach (6.10) $\alpha^{q-1} = 1$ für alle $\alpha \in K^*$. Jedes $\beta \in K$ ist also Nullstelle von $X^q - X$. Ist K' ein weiterer Körper mit genau q Elementen, dann erhält man einen aufgrund von (9.37) einen Isomorphismus $K \cong K'$.

Aufgaben und Beispiele

(1) Zeigen Sie, daß im Ring $R = \mathbb{Z}$ jede additive Untergruppe ein Ideal ist.

(2) Zeigen Sie, daß im Ring $R = \mathbb{Z}$ ein Ideal $I \subset R$ genau dann maximal ist, wenn eine Primzahl p existiert, so daß $I = p\mathbb{Z}$ gilt.

(3) Sei $m \in \mathbb{N}, m \geqq 2$. Zeigen Sie: Der Faktorring $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist.

(4) Sei $R = \{a + b\sqrt{-1} : a, b \in \mathbb{Z}\}$. Zeigen Sie, daß R ein kommutativer Teilring von $\mathbb{C}$ ist. Zeigen Sie außerdem, daß

$$\mathfrak{a} := \{a + b\sqrt{-1} : a, b \in \mathbb{Z}; 3/a, 3/b\}$$

ein maximales Ideal von R ist.

(Hinweise für den letzten Teil dieser Aufgabe: Sei $\mathfrak{b} \subset R$ ein Ideal mit $\mathfrak{a} \subsetneq \mathfrak{b}$. Weil $\mathfrak{b}$ ein Ideal ist, existiert ein Element $r + s\sqrt{-1} \in \mathfrak{b}$ mit $3 \nmid r$ und $3 \nmid s$, also $3 \nmid (r^2 + s^2)$. $r^2 + s^2 = (r + s\sqrt{-1})(r - s\sqrt{-1}) \in \mathfrak{b}$, weil $r + s\sqrt{-1} \in \mathfrak{b}$ und weil $\mathfrak{b}$ ein Ideal ist. Setze $t := r^2 + s^2$. $1 = ggT(3, t) = ut + 3v$ mit $u, v \in \mathbb{Z}$. $ut \in \mathfrak{b}$, weil $t \in \mathfrak{b}$. $3 \in \mathfrak{a} \subset \mathfrak{b}$, also $3 \cdot v \in \mathfrak{b}$. Es folgt $1 \in \mathfrak{b}$. Also $\mathfrak{b} = R$.)

(5) (vgl. $[LM]$) Sei R ein kommutativer Ring mit Einselement und sei

$$K(R) := \{(x, y) \in R^2 : x^2 + y^2 = 1\}.$$

Zeigen Sie, daß $K(R)$ bezüglich der Verknüpfung

$$(x_1, y_1) + (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$$

eine Gruppe ist. Wieviele Elemente enthält $K(\mathbb{Z})$ bzw. $K(\mathbb{Z}/4\mathbb{Z})$?

Zeigen Sie außerdem: Ist $\phi : R \to S$ ein Homomorphismus von kommutativen Ringen mit Einselement, dann ist

$$\phi_K : K(R) \to K(S), \phi_K((x, y)) := (\phi(x), \phi(y)),$$

ein Gruppenhomomorphismus, und es gilt: Ist ϕ injektiv bzw. bijektiv, dann ist ϕ_K injektiv bzw. bijektiv.

(6) (vgl. $[AMD]$, Chapter 1, Exercise 26) Sei R der Ring aller stetigen Funktionen $f : [0, 1] \to \mathbb{R}$ bezüglich der punktweise erklärten Addition und Multiplikation als Verknüpfung.

(a) Für jedes $\alpha \in [0, 1]$ sei $\mathfrak{m}_\alpha := \{f \in R : f(\alpha) = 0\}$. Zeigen Sie, daß $\mathfrak{m}_\alpha$ ein maximales Ideal von R ist.

(b) Zeigen Sie, daß jedes maximale Ideal von R von der Form $\mathfrak{m}_\alpha$ für ein $\alpha \in [0, 1]$ ist.

(Hinweise: (a) $\mathfrak{m}_\alpha$ ist der Kern des surjektiven Ringhomomorphismus $R \to \mathbb{R}, f \to f(\alpha)$. Nach dem 1-ten Isomorphiesatz für Ringe gilt also $R/\mathfrak{m}_a \cong \mathbb{R}$. Also ist $R/\mathfrak{m}_\alpha$ ein Körper und somit $\mathfrak{m}_\alpha$ ein maximales Ideal von R.

(c) Sei $\mathfrak{m}$ ein maximales Ideal von R und sei

$$V := \{\alpha \in [0, 1] : f(\alpha) = 0 \text{ für alle } f \in \mathfrak{m}\}.$$

Annahme: $V = \phi$. Dann gilt: Für alle $\alpha \in [0, 1]$ existiert ein $f_\alpha \in \mathfrak{m}$ mit $f_\alpha(\alpha) \neq 0$. Aus der Stetigkeit von f_α folgt die Existenz einer evtl. einseitigen Umgebung U_α von α mit $U_\alpha \subset [0, 1]$ und $f_\alpha(x) \neq 0$ und alle $x \in U_\alpha$. Wegen

der Kompaktheit von $[0,1]$ gibt es unter den U_α endlich viele $U_{\alpha_1}...U_{\alpha_n}$ mit $[0,1] \subset \cup_{i=1}^{n} U_{\alpha_i}$. Sei

$$f := f_{\alpha_1}^2 + ... + f_{\alpha_n}^2.$$

Dann ist $f(x) \neq 0$ für alle $x \in [0,1]$, also $f \in R^*$ und damit $\mathfrak{m} = R$, ein Widerspruch zur Maximalität von $\mathfrak{m}$.

Also $V \neq \phi$. Sei $\alpha \in V$. Dann ist $\mathfrak{m} \subset \mathfrak{m}_\alpha$, also $\mathfrak{m} = \mathfrak{m}_\alpha$, weil $\mathfrak{m}$ maximal ist.

(7) (vgl. $[AMD]$, Chapter 1, Exercise 11) Ein kommutativer Ring A mit 1 heißt *Boolescher Ring*, falls $x^2 = x$ für alle $x \in A$ gilt. Zeigen Sie, daß in einem Booleschen Ring A die folgenden Aussagen gelten: $2x = 0$ für alle $x \in A$; jedes Primideal $\mathfrak{p}$ von A ist maximal, und $A/\mathfrak{p}$ ist ein Körper mit 2 Elementen.

(8) (vgl. $[AMD]$, Chapter 1, Exercise 24) Sei $L = (L, \wedge, \vee, ', 0, 1)$ eine Boolesche Algebra, vgl. § 2. Zeigen Sie, daß $A(L) := (L, +, \cdot)$ bezüglich der nachfolgend definierten Verknüpfung $+$ und $\cdot$ ein Boolescher Ring ist:

$a + b := (a \wedge b') \vee (a' \wedge b)$, $ab := a \wedge b$.

(9) (vgl. $[AMD]$, Chapter 1, Exercise 24) Sei A ein Boolescher Ring. Zeigen Sie:

(a) $(A, \leqq)$ ist bezüglich der nachfolgend definierten Ordnungsrelation $\leqq$ ein Verband (vgl. §2):

$a \leqq b$, fallls $a = ab$.

(b) Mit den Festsetzungen

$a \vee b := a + b + ab$, $a \wedge b := ab$, $a' := 1 - a$.

ist eine Boolesche Algebra $B(A) := (A, \wedge, \vee, ', 0, 1)$ definiert

(c) Die Zuordnung $A \mapsto B(A)$ eine bijektive Abbildung zwischen der Menge aller Booleschen Ringe und der Menge aller Booleschen Algebren, und es gilt: Sind $A, \widetilde{A}$ Boolesche Ringe und ist $f : A \to \widetilde{A}$ ein Homomorphismus von Ringen, dann ist $f : B(A) \to B(\widetilde{A})$ auch ein Morphismus von Booleschen Algebren; umgekehrt ist jeder Morphismus von Booleschen Algebren $g : B(A) \to B(\widetilde{A})$ auch ein Homomorphismen von Ringen $g : A \to \widetilde{A}$.

(10) Gegeben sind die Verschlüsselungszahl $r = 209$ und die Sendezahl $e = 7$. Entschlüsseln Sie mit dem public-key Verfahren die Nachricht $y \equiv 67 \bmod 209$.

Literatur zu §9: [AMD], [BB], [BM], [DH], [F], [FR], [G], [KS], [KU], [$L1$], [$L2$], [LL], [LM], [LS], [R], [RSA], [W]

§ 10. **Das quadratische Reziprozitätsgesetz**

In diesem Abschnitt besprechen wir ein überaus wichtiges Resultat der Zahlentheorie, das auch in der Informatik eine Rolle spielt, nämlich das quadratische Reziprozitätsgesetz. Dabei folgen wir weitgehend entsprechenden Ausführungen in [F], Abschnitt 11; [GT], Chapter 4, 4.3 und [$L3$], Chapter IV, §3. Der gegebene Beweis des quadratischen Reziprozitätsgesetzes ist einer der Beweise, die Gauß gegeben hat.

Definition Sei p eine ungerade Primzahl und sei a eine zu p teilerfremde ganze Zahl. Das *Legendre-Symbol* $\left(\frac{a}{p}\right)$ ist dann wie folgt definiert

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{falls } x^2 \equiv a \bmod p \text{ in } x \text{ ganzzahlig lösbar ist} \\ -1, & \text{sonst} \end{cases}$$

Im ersten Fall heißt a quadratischer Rest modulo p, im zweiten Fall quadratischer Nichtrest modulo p.

(10.1) **Satz** (Quadratisches Reziprozitätsgesetz) *Seien p, q verschiedene ungerade Primzahlen. Dann gilt*

(i) *Reziprozitätsformel* $\qquad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

(ii) *Erster Ergänzungssatz*
$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv 1 \bmod 4 \\ -1, & \text{falls } p \equiv 3 \bmod 4 \end{cases} = (-1)^{\frac{p-1}{2}}$$

(iii) *Zweiter Ergänzungssatz*
$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv 1, 7 \bmod 8 \\ -1, & \text{falls } p \equiv 3, 5 \bmod 8 \end{cases} = (-1)^{\frac{p^2-1}{8}}$$

(10.2) **Bemerkungen** (a) Wir ergänzen die Definition des Legendre-Symbols durch

$\left(\frac{a}{p}\right) := 0$, falls p ein Teiler von a ist

(b) Es gilt $\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$ für alle $k \in \mathbb{Z}$

(c) Wenn p eine ungerade Primzahl ist, dann ist $\mathbb{F}_p^*$ zyklisch von der Ordnung $p-1$. Der Kern des Homomorphismus von Gruppen

$$\mathbb{F}_p^* \to \mathbb{F}_p^*, x \longmapsto x^2,$$

hat die Ordnung 2. Das Bild dieses Homomorphismus ist $\mathbb{F}_p^{*^2}$ und hat die Ordnung $\frac{p-1}{2}$; denn

$$\mathbb{F}_p^{*^2} \cong \mathbb{F}_p^*/\text{Kern, also } \left|\mathbb{F}_p^{*^2}\right| = \frac{\left|\mathbb{F}_p^*\right|}{|\text{Kern}|} = \frac{p-1}{2}.$$

Es gibt also in $\mathbb{F}_p^*$ genauso viele Quadrate wie Nichtquadrate:

$$(\mathbb{F}_p^* : \mathbb{F}_p^{*^2}) = 2.$$

Für je zwei Elemente $\overline{a}, \overline{b}$ aus $\mathbb{F}_p^*$, die keine Quadrate sind, ist also das Produkt $\overline{a}\overline{b}$ ein Quadrat. Somit gilt

$$\left(\tfrac{ab}{p}\right) = \left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right).$$

(d) Für jede ungerade natürliche Zahl b mit der Primfaktorzerlegung

$$b = p_1 \cdot \ldots \cdot p_k$$

und für jede zu b teilerfremde ganze Zahl a definiert man das Jacobi-Symbol

$$\left(\tfrac{a}{b}\right) := \left(\tfrac{a}{p_1}\right) \cdot \ldots \cdot \left(\tfrac{a}{p_k}\right).$$

Für beliebige teilerfremde ungerade ganze Zahlen a, b gilt dann auch die Reziprozitätsformel

$$\left(\tfrac{a}{b}\right)\left(\tfrac{b}{a}\right) = (-1)^{\frac{1}{4}(a-1)(b-1)}$$

Wir benötigen

(10.3) **Eulersches Kriterium** Sei q eine Primzahl. Dann gilt für jede zu q teilerfremde ganze Zahl a

$$a^{\frac{q-1}{2}} \equiv \left(\tfrac{a}{q}\right) \bmod q.$$

Beweis: Nach (9.16) ist die Kongruenz $x^2 \equiv a \bmod q$ genau dann lösbar, wenn $a^{(q-1)/2} \equiv 1 \bmod q$ gilt.

Aus dem Eulerschen Kriterium folgt für $a = -1$:

$(-1)^{\frac{q-1}{2}} \equiv \left(\frac{-1}{q}\right) \bmod q$, also $(-1)^{\frac{q-1}{2}} = \left(\frac{-1}{q}\right)$,

und damit Aussage (ii) von (10.1).
Wir beweisen nun Aussage (iii) von (10.1). Es ist

$\left(\frac{(1+i)^2}{i}\right) = 2,$

also mit Hilfe des Eulerschen Kriteriums

$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv \left((1+i)^{p-1}/i^{\frac{p-1}{2}}\right) \bmod p$

$\equiv \left(1+i)^p/(i^{\frac{p-1}{2}}(1+i)\right) \bmod p$

$\equiv \frac{e^{p\pi i/4}+e^{-p\pi i/4}}{e^{\pi i/4}+e^{-\pi i/4}} \bmod p$

$\equiv \frac{\cos(\frac{p\pi}{4})}{\cos(\frac{\pi}{4})} \bmod p$

Daraus folgt

$$\left(\frac{2}{p}\right) = \frac{\cos(\frac{p\pi}{4})}{\cos(\frac{\pi}{4})} = \begin{cases} +1, & \text{falls } p \equiv \pm 1 \bmod 8 \\ -1, & \text{falls } p \equiv \pm 3 \bmod 8 \end{cases}$$

also

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Für den Beweis von Aussage (i) von (10.1) benötigen wir

(10.4) **Hilfssatz** *Für jede ungerade Primzahl p und jede natürliche Zahl n mit $ggT(n,p) = 1$ gilt*

$(\star) \quad \sum_{j=0}^{p-1} e^{2\pi i n j^2/p} = \left(\frac{n}{p}\right) \cdot \sum_{j=0}^{p-1} e^{2\pi i j^2/p}$

Beweis: Für $\left(\frac{n}{p}\right) = +1$ schreibe $n = m^2 \bmod p$. Dann ist

$\sum_{j=0}^{p-1} e^{2\pi i n j^2/p} = \sum_{j=0}^{p-1} e^{2\pi i (mj)^2/p} = \sum_{j=0}^{p-1} e^{2\pi i j^2/p}$.

Im Fall $\left(\frac{n}{p}\right) = -1$ schreibe

$(\star\star) \quad \sum_{j=0}^{p-1} e^{2\pi i j^2/p} = 1 + 2 \cdot \sum_r e^{2\pi i r/p},$

wobei r die von 0 verschiedenen quadratischen Reste modulo p durchläuft. Durchläuft s die von 0 verschiedenen quadratischen Nichtreste modulo p, dann gilt

$0 = \sum_{k=0}^{p-1} e^{2\pi ik/p} = 1 + \sum_r e^{2\pi ir/p} + \sum_s e^{2\pi is/p}$.

Also ergibt sich mit $(\star\star)$

$\sum_{j=0}^{p-1} e^{2\pi ij^2/p} = -1 - 2 \cdot \sum_s e^{2\pi is/p} = \left(\frac{n}{p}\right) \cdot \sum_{j=0}^{p-1} e^{2\pi inj^2/p}$.

Für jede natürliche Zahl N bezeichne F_N die N-te Fouriertransformation, vgl. § 7. Sei

$T_N := \sqrt{N} \cdot F_N, S_N := Spur(T_N)$,

also

$S_N = \sum_{j=0}^{N-1} e^{2\pi ij^2/N}$.

Das Ergebnis (7.8) läßt sich folgendermaßen schreiben, vgl. [$L3$], p.90:

$S_N = \frac{1+i^{-N}}{1+i^{-1}} \cdot \sqrt{N}$

Aus Formel $(\star)$ des obigen Hilfssatzes (10.4) folgt für verschiedene ungerade Primzahlen p, q :

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) S_p S_q = \sum_{k=0}^{q-1} \sum_{j=0}^{p-1} e^{2\pi i(\frac{qj^2}{p} + \frac{pk^2}{q})} =$

$= \sum_{\substack{j=0,1,\ldots,p-1 \\ k=0,1,\ldots,q-1}} e^{2\pi i \frac{(pk+qj)^2}{pq}} = S_{pq}$

Somit gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \frac{S_{pq}}{S_p S_q} = \begin{cases} -1 & \text{für } p, q \equiv 3 \bmod 4 \\ +1 & \text{sonst} \end{cases}$$

$$= (-1)^{\frac{(p-1)(q-1)}{4}},$$

also die Reziprozitätsformel (i) von (10.1).

Aufgaben und Beispiele

(1) Bestimmen Sie die Menge aller Primzahlen p, so daß die Kongruenz $5 \equiv x^2 \bmod p$ lösbar ist.

(2) Berechnen Sie das Jacobi-Symbol $\left(\frac{123}{917}\right)$.

(3) Zeigen Sie, daß für jede ganze Zahl d und jede ungerade Primzahl p die Anzahl der Lösungen der Kongruenz $x^2 \equiv d \bmod p$ gleich $1 + \left(\frac{d}{p}\right)$ ist.

Literatur zu §10: [BA], [DM], [F], [G], [GT], [$L3$]

§ 11. **Elementare Primzahltests und Faktorisierungsmethoden**

Für diesen Abschnitt benutzen wir insbesondere die entsprechenden Ausführungen in [F], den Übersichtsartikel [N] sowie die Arbeit [AKS].

Nach dem kleinen Satz von Fermat, vgl. (9.16), gilt

$$a^{p-1} \equiv 1 \bmod p$$

für jede Primzahl p und für jede zu p teilerfremde ganze Zahl a. Anders ausgedrückt:

$$\exp(\mathbb{Z}/p\mathbb{Z})^*/(p-1).$$

Einige zusammengesetzte Zahlen N haben ebenfalls die Eigenschaft

$$\exp(\mathbb{Z}/N\mathbb{Z})^*/(N-1);$$

diese Zahlen heißen *Carmichael-Zahlen*, benannt nach dem kanadischen Mathematiker Carmichael. Die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$. Weitere sind $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$. Es gilt jedoch die folgende Umkehrung des Eulerschen Krizeriums (10.3).

(11.1) **Satz** *Sei $N \geq 3$ eine ungerade natürliche Zahl. Für jede zu N teilerfremde ganze Zahl a gelte*

$$a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \bmod N$$

Dann ist N eine Primzahl.

Beweis: Angenommen N ist keine Primzahl. Aus der Voraussetzung folgt

$$a^{N-1} \equiv 1 \bmod N.$$

Also ist N eine Carmichael-Zahl. Um weiter zu schließen, beweisen wir zunächst den folgenden Hilfssatz über Carmichael-Zahlen.

(11.2) **Hilfssatz** *Eine ungerade zusammengesetzte Zahl $N \geq 3$ ist genau dann eine Carmichael-Zahl, wenn gilt*
(a) *N ist quadratfrei, d.h. N enthält keinen mehrfachen Primfaktor*
(b) *Für jeden Primfaktor p/N gilt $p-1/N-1$.*

Beweis von (11.2): Seien (a) und (b) erfüllt. Sei $N = p_1 p_2 ... p_n$ mit paarweise verschiedenen Primzahlen $p_1, ..., p_n$. Dann existiert nach dem chinesischen Restsatz, vgl. (9.12), ein Isomorphismus

$$(\mathbb{Z}/N\mathbb{Z})^* \cong (\mathbb{Z}/p_1\mathbb{Z})^* \times ... \times (\mathbb{Z}/p_n\mathbb{Z})^*;$$

eine zu N teilerfremde Zahl a entspricht bei diesem Isomorphismus einem n-Tupel $(a_1, ..., a_n)$ mit $p_i \nmid a_i$. Nach Voraussetzung gilt $p_i - 1/N - 1$ für $i = 1, ..., n$; also folgt

$$a_i^{N-1} \equiv 1 \bmod p_i \text{ für alle } i.$$

Daraus folgt $a^{N-1} \equiv 1 \bmod N$.
Sei umgekehrt N eine Carmichael-Zahl.
Zu (a): Ist N nicht quadratfrei, so gilt $N = p^e m$ mit einer Primzahl p und einem Exponenten $e \geq 2$ sowie einer zu p teilerfremden Zahl m. Sei g eine Primitivwurzel modulo p^e, d.h. $g + p^e\mathbb{Z}$ erzeugt die zyklische Gruppe $(\mathbb{Z}/p^e\mathbb{Z})^*$ Nach dem chinesischen Restsatz gibt es eine zu N teilerfremde Zahl a mit $a \equiv g \bmod p^e$ und $a \equiv 1 \bmod m$. Wäre $a^{N-1} \equiv 1 \bmod N$, dann wäre $a^{N-1} \equiv 1 \bmod p^e$, also $g^{N-1} \equiv 1 \bmod p^e$. Da g als Primitivwurzel modulo p^e die Ordnung $p^{e-1}(p-1)$ hat, folgt daraus $p^{e-1}(p-1)/N - 1$, insbesondere $p/N - 1$, im Widerspruch zu p/N.
Zu (b): Nach (a) ist N quadratfrei. Sei p ein Primteiler von N. Dann ist $N = pm$ mit einer zu p teilerfremden Zahl m. Dasselbe Argument wie bei (a), diesmal mit $e = 1$, zeigt: $p - 1/N - 1$.

Beweis von (11.1): Angenommen N ist keine Primzahl. Aus der Voraussetzung folgt durch Quadrieren $a^{N-1} \equiv 1 \bmod N$. Also ist N eine Carmichael-Zahl. Nach (11.2) gilt also $N = p_1 \cdot ... \cdot p_r$ mit paarweise verschiedenen ungeraden Primzahlen p_i, so daß $p_i - 1/N - 1$ für $i = 1, ..., r$. Wir benutzen den Isomorphismus aus (9.12)

$$\psi : (\mathbb{Z}/N\mathbb{Z})^* \xrightarrow{\cong} (\mathbb{Z}/p_1\mathbb{Z})^* \times ... \times (\mathbb{Z}/p_r\mathbb{Z})^*.$$

Sei $\overline{g} \in (\mathbb{Z}/p_1\mathbb{Z})^*$ ein erzeugendes Element und sei $\overline{b} \in (\mathbb{Z}/N\mathbb{Z})^*$ das Element mit

$$\psi(\overline{b}) = (\overline{g}, \overline{1}, ..., \overline{1}).$$

Dann gilt

$$\left(\tfrac{b}{N}\right) = \left(\tfrac{b}{p_1}\right) \cdot \ldots \cdot \left(\tfrac{b}{p_r}\right) = \left(\tfrac{g}{p_1}\right) = -1;$$

denn g ist modulo p_1 kein Quadrat. Wir unterscheiden zwei Fälle.

(i) $N-1$ ist ein geradzahliges Vielfaches von p_1-1. Dann ist $g^{\frac{N-1}{2}} \equiv 1 \bmod p_1$ und daher $b^{\frac{N-1}{2}} \neq \left(\tfrac{b}{N}\right) \bmod N$.

(ii) $N-1$ ist ein ungeradzahliges Vielfaches von p_1-1. Dann ist $g^{\frac{N-1}{2}} \equiv -1 \bmod p_1$ und daher $\psi(\overline{b}^{\frac{N-1}{2}}) = (\overline{-1}, \overline{1}, \ldots, \overline{1})$, also $b^{\frac{N-1}{2}} \neq \left(\tfrac{b}{N}\right) \bmod N$

(11.3) **Folgerung** *Sei $N \geq 3$ eine ungerade zusammengesetzte Zahl und sei A die Menge aller zu N teilerfremden $a, 0 < a < N$, mit $a^{(N-1)/2} \equiv \left(\tfrac{a}{N}\right) \bmod N$. Dann gilt $|A| \leq \frac{1}{2}\varphi(N)$.*

Beweis: Die Abbildung $\alpha : (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^*, x \mapsto x^{\frac{N-1}{2}} \cdot \left(\tfrac{x}{N}\right)$, ist ein Gruppenhomomorphismus, und es gilt $\mathrm{Kern}(\alpha) \neq (\mathbb{Z}/N\mathbb{Z})^*$. Also hat $\mathrm{Kern}(\alpha)$ mindestens den Index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$. Somit

$$|A| \leq \tfrac{1}{2} \left|(\mathbb{Z}/N\mathbb{Z})^*\right|.$$

Der Solovay-Strassen-Primzahltest: Gegeben sei eine ungerade Zahl N. Man wähle eine Zufallszahl a mit $2 \leq a \leq N$ und berechne das Jacobi-Symbol $\left(\tfrac{a}{N}\right)$.

Falls $\left(\tfrac{a}{N}\right) = 0$, sind a und N nicht teilerfremd, also ist N keine Primzahl.

Falls $\left(\tfrac{a}{N}\right) \neq 0$, berechne man $a^{\frac{N-1}{2}} \bmod N$ und überprüfe, ob

$$(\star) \quad a^{(N-1)/2} \equiv \left(\tfrac{a}{N}\right) \bmod N.$$

gilt. Falls dies nicht der Fall ist, ist N keine Primzahl. Ist dies der Fall, so ist man zwar nicht sicher, daß N Primzahl ist, aber nach obiger Folgerung ist bei zufälliger Wahl von a die Wahrscheinlichkeit dafür, daß $(\star)$ erfüllt ist, obwohl N keine Primzahl ist, nicht größer als $\frac{1}{2}$. Wiederholt man diesen Test k mal mit verschiedenen Zufallszahlen a, und ist jedes Mal die Konguenz $(\star)$ erfüllt, so ist die Wahrscheinlichkeit dafür, daß N keine Primzahl ist, nicht größer als $(\frac{1}{2})^k$.

Weitere Primzahltests werden z.B. in $[F]$ beschrieben.

Schon die Definition des Begriffs "Primzahl" führt zu einem Verfahren, von einer gegebenen natürlichen Zahl n festzustellen, ob sie Primzahl ist oder nicht: Man überprüft, ob n durch eine der natürlichen Zahlen m mit $m \leq \sqrt{n}$ teilbar ist. Dazu braucht man $0(\sqrt{n})$ Schritte. Ein gutes Verfahren jedoch sollte mit

einer Anzahl von Schritten auskommen, die polynomial in $\log_2(n)$ ist. Den Nachweis, daß ein solches Verfahren existiert, führten Massindra Agrawal, Neeraj Kayal und Nitin Saxena, vgl. $[AKS]$. Die Grundidee hierfür ist die folgende Verallgemeinerung des kleinen Satzes von Fermat, vgl. $[AKS]$.

Satz *Seien $a \in \mathbb{Z}, n \in \mathbb{N}, n \geq 2$ mit $ggT(a,n) = 1$. Dann gilt: n ist Primzahl genau dann, wenn die folgende Polynomkongruenz erfüllt ist:*

$$(X+a)^n \equiv (X^n + a) \bmod n.$$

Beweis: Für $0 < i < n$ ist der Koeffizient von X^i in $(X+a)^n - (X^n + a)$ gleich $\binom{n}{i} a^{n-i}$.

Angenommen n ist Primzahl. Dann gilt $\binom{n}{i} \equiv 0 \bmod n$ und daher ist für $0 < i < n$ der Koeffizient von X^i durch n teilbar.

Angenommen n ist keine Primzahl. Sei q ein Primteiler von n und sei q^k die höchste in n aufgehende q-Potenz. Dann ist q^k kein Teiler von $\binom{n}{q}$ und teilerfremd zu a^{n-q}. Also ist der Koeffizient von X^q nicht durch n teilbar, und die behauptete Polynomkongruenz ist nicht erfüllt.

Wie man mit Hilfe dieses Satzes zu einem Primzahltestverfahren der gewünschten Art kommt, wird in $[AKS]$ ausgeführt.

Die Grundidee für viele Faktorisierungsalgorithmen ist enthalten in dem folgenden **Faktorisierungsverfahren von Fermat**: Ist $N = ab$ eine zusammengesetzte ungerade Zahl, so sind auch a, b ungerade, und

$$x = \tfrac{a+b}{2},\ y = \tfrac{a-b}{2}$$

sind daher ganze Zahlen. Also ist

$$N = (x+y) \cdot (x-y) = x^2 - y^2$$

die Differenz zweier Quadrate. Wegen $y^2 \geq 0$ ist

$$x \geq \left\lceil \sqrt{N} \right\rceil.$$

Daraus ergibt sich der folgende Faktorisierungsalgorithmus

(1) Setze $x := \left\lceil \sqrt{N} \right\rceil$ und $z := x^2 - N$
(2) Ist z ein Quadrat, etwa $z = y^2$, dann erhält man die Faktorisierung

$$N = (x-y) \cdot (x+y).$$

Sonst setze $x_1 := x+1, z_1 := z + 2x + 1$ und wiederhole (2).

Rechenbeispiele (1) $N = 91$; $x = \left[\sqrt{91}\right] = 9, z = -10$; $x_1 := 10, z_1 = -10 + 18 + 1 = 9 = 3^2$; also $N = 91 = (x_1 - 3)(x_1 + 3) = 7 \cdot 13$

(2) $N = 209, x = \left[\sqrt{91}\right] = 14, z = x^2 - N = 196 - 209 = -13$; $x_1 = 14+1, z_1 := -13+28+1 = 16 = 4^2 = y^2$; also $N = 209 = (15-4)(15+4) = 11 \cdot 19$

(3) $N = 57, x = \left[\sqrt{57}\right] = 7, z = -8$; $x_1 = 8, z_1 = -8 + 2 \cdot 7 + 1 = 7$; $x_2 = 9, z_2 = 7 + 16 + 1 = 24$; $x_3 = 10, z_3 = 24 + 18 + 1 = 43$;$x_4 = 11, z_4 = 43 + 20 + 1 = 64 = y_4^2 = 8^2$; also $N = 57 = (11 - 8)(11 + 8) = 3 \cdot 19$.

Dieser Faktorisierungsalgorithmus ist Grundlage neuerer Faktorisierungsmethoden. Eine erste **Verbesserung** stammt **von Gauß und Legendre**. Hiernach genügt es, an Stelle von N ein natürliches Vielfaches $k \cdot N$ von N als Differenz von zwei Quadraten zu schreiben:

$$kN = x^2 - y^2 = (x + y)(x - y).$$

In dem Restklassenring $\mathbb{Z}/N\mathbb{Z}$ sind dann y und $\pm x$ Wurzeln von x^2. Hat N genau d verschiedene Primteiler, so gibt es in $\mathbb{Z}/N\mathbb{Z}$ genau 2^d verschiedene Wurzeln von x^2. Also ist die Wahrscheinlichkeit, daß $y \neq \pm x \bmod N$ und damit der $ggT(x-y, N)$ ein nichttrivialer Teiler von N ist, gleich $(2^d-2)/2^d$ und damit für $d \geq 2$ nicht kleiner als $1/2$. Man versucht also, Lösungen von $x^2 \equiv y^2 \bmod N$ mit $y \neq \pm x \bmod N$ zu finden. Das kann so geschehen: Man bestimmt ganze Zahlen $z_1, ..., z_m$, die modulo N Quadrate natürlicher Zahlen $x_1, ..., x_m$ sind:

$$z_i \equiv x_i^2 \bmod N, \quad i = 1, ..., m.$$

Diese $z_1, ..., z_m$ bestimmt man möglichst so, daß für eine Teilmenge $I \subset \{1, ..., m\}$ das Produkt der $z_i, i \in I$, Quadrat einer natürlichen Zahl y ist:

$$\prod_{i \in I} z_i = y^2.$$

Für $x := \prod_{i \in I} x_i$ ist dann $x^2 - y^2$ durch N teilbar.

Aufgaben und Beispiele

(1) Zeigen Sie: $N \in \mathbb{N}$ ist Primzahl genau dann, wenn für jede Primzahl p, die $N - 1$ teilt, eine ganze Zahl a existiert, so daß

$$a^{N-1} \equiv 1 \bmod N \quad \text{und} \quad a^{(N-1)/p} \neq 1 \bmod N$$

(2) Für $n \in \mathbb{N}$ sei $F(n) := 2^{2^n} + 1$. Zeigen Sie: $F(n)$ ist genau dann Primzahl, wenn

$$3^{(F(n)-1)/2} \equiv -1 \bmod F(n)$$

(3) Schreiben Sie 2456309 als Produkt von Primzahlen

.

Literatur zu § 11: [AKS], [DM], [F], [G], [N], [RL], [RSA]

§ 12. **Kategorien und Funktoren**

Der Begriff der Kategorie hat innerhalb der Mathematik und Informatik eine wichtige Ordnungsfunktion. Wir besprechen in diesem Paragraphen wichtige Grundbegriffe über Kategorien und folgen dabei weitgehend entsprechenden Darstellungen in [$L2$],Chapter I, 6 und [SC]. Bei der Einführung dieses Begriffes erinnern wir daran, daß wir, um Paradoxien und Widersprüche zu vermeiden, ein festes Universum $\mathcal{U}$ zugrunde legen, in dem jede der betrachteten Mengen als Element enthalten ist; vgl. §1. Eine *Klasse in bezug auf* $\mathcal{U}$ ist eine Teilmenge von $\mathcal{U}$. Mit diesen Festlegungen definieren wir jetzt den Begriff der Kategorie.

Definition Eine *Kategorie* $\mathfrak{A}$ besteht aus einer Klasse von *Objekten* $\mathcal{O}(\mathfrak{A})$, so daß für je zwei Objekte $A, B \in \mathcal{O}(\mathfrak{A})$ eine nur von A und B abhängige Menge $\mathcal{M}(A, B)$, genannt die *Menge von Morphismen von A nach B*, definiert ist, und so daß für je drei Objekte $A, B, C \in \mathcal{O}(\mathfrak{A})$ eine Abbildung, genannt *Verknüpfung*,

$$\mathcal{M}\ (B, C) \times \mathcal{M}(A, B) \to \mathcal{M}(A, C)$$

existiert, so daß die folgenden Axiome erfüllt sind:

(1) Für je vier Objekte $A, A', B, B' \in \mathcal{O}(\mathfrak{A})$ gilt: Wenn $\mathcal{M}(A, B) \cap \mathcal{M}(A', B') \neq \phi$, dann ist $A = A'$ und $B = B'$.

(2) Für alle $A \in \mathcal{O}(\mathfrak{A})$ existiert ein Morpismus $id \in \mathcal{M}(A, A)$, so daß für alle $B \in \mathcal{O}(\mathfrak{A})$ der Morphismus id Rechtsidentität für alle Elemente aus $\mathcal{M}(A, B)$ bzw. Linksidentität für alle Elemente aus $\mathcal{M}(B, A)$ ist, d.h. es gilt $f \circ id = f$ für alle $f \in \mathcal{M}(A, B)$ bzw. $id \circ f = f$ für alle $f \in \mathcal{M}(B, A)$.

(3) Die Verknüpfung $\circ$ ist assoziativ, d.h. für alle $A, B, C, D \in \mathcal{O}(\mathfrak{A})$ und für alle $f \in \mathcal{M}(A, B), g \in \mathcal{M}(B, C), h \in \mathcal{M}(C, D)$ gilt

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Beispiele (a) Die Kategorie $\mathfrak{R} : \mathcal{O}(\mathfrak{R})$ besteht aus den Mengen aus $\mathcal{U}$, $\mathcal{M}(A, B)$ = Menge aller Relationen von A zu B. $\circ$ = Verknüpfung von Abbildungen, id = Gleichheitsrelation.

(b) Die Kategorien $\mathfrak{S} : \mathcal{O}(\mathfrak{S})$ besteht aus den Mengen aus $\mathcal{U}$, $\mathcal{M}(A, B)$ = Menge aller Abbildungen von A nach B. $\circ$ = Verknüpfung von Abbildungen, id = identische Abbildung.

(c) Die Kategorie $\mathfrak{G}$: $\mathcal{O}(\mathfrak{G})$ besteht aus Gruppen, $\mathcal{M}(A, B)$ = Menge aller Gruppenhomomorphismen von A nach B.

(d) Die Kategorie $\mathcal{R}$: $\mathcal{O}(\mathfrak{R})$ besteht aus Ringen, $\mathcal{M}(A, B)$ = aller Ringhomomorphismen von A nach B

(e) G sei eine Gruppe. Die Kategorie $G-\mathfrak{S}:(G-\mathfrak{S})=$ Mengen aus $\mathcal{U}$ mit einer G-Operation. $\mathcal{M}(S,T)=$ Menge aller Abbildungen $f:S\to T$ mit der Eigenschaft $g(f(s))=f(g(s))$ für alle $s\in S, g\in G$.

Für eine Kategorie $\mathfrak{A}$ bezeichnen wir mit $\mathcal{M}(\mathfrak{A})$ die Menge aller Morphismen in $\mathfrak{A}$, und ein Morphismus $f\in\mathcal{M}(A,B)$ wird in der Form $f:A\to B$ geschrieben.

Definition Sei $\mathfrak{A}$ eine Kategorie. Ein Morphismus $f:A\to B$ in $\mathfrak{A}$ heißt Isomorphismus, wenn ein $g:B\to A$ existiert, so daß $g\circ f=id$ in $\mathcal{M}/A,A)$ und $f\circ g=id$ in $\mathcal{M}(B,B)$ gilt. Für $A=B$ heißt ein Isomorphismus $f:A\to A$ auch Automorphismus von A. Ein Morphismus $f:A\to A$ in $\mathfrak{A}$ heißt auch Endomorphismus von A.

Die Menge $End(A)$ aller Endomorphismen von $A\in\mathcal{O}(\mathfrak{A})$ ist bezüglich der Verknüpfung $\circ$ ein Monoid; die Menge $Aut(A)$ aller Automorphismen von $A\in\mathcal{O}(\mathfrak{A})$ ist bezüglich $\circ$ eine Gruppe.

Definition Seien $\mathfrak{A},\mathfrak{B}$ Kategorien. Ein *kovarianter* bzw. *kontravarianter Funktor* $F:\mathfrak{A}\to\mathfrak{B}$ von $\mathfrak{A}$ in $\mathfrak{B}$ ordnet jedem $A\in\mathcal{O}(\mathfrak{A})$ genau ein $F(A)\in\mathcal{O}(\mathfrak{B})$ und jedem Morpismus $f:A\to B$ in $\mathcal{M}(\mathfrak{A})$ genau einen Morphismus $F(f):F(A)\to F(B)$ in $\mathcal{M}(\mathfrak{B})$ zu, so daß gilt:

(1) Für alle $A\in\mathcal{O}(\mathfrak{A})$ ist $F(id_A)=id_{F(A)}$
(2) Für alle Morphismen $f:A\to B, g:B\to C$ in $\mathcal{M}(\mathfrak{A})$ ist $F(g\circ f)=F(g)\circ F(f)$ bzw. $F(g\circ f)=F(f)\circ F(g)$

Beispiele Sei $\mathfrak{A}$ eine Kategorie und sei $A\in\mathcal{O}(\mathfrak{A})$. Sei $\mathfrak{S}$ die Kategorie der Mengeneiner festen Stufe. Dann wird ein kovarianter Funktor $M_A:\mathfrak{A}\to\mathfrak{S}$ wie folgt definiert:

$M_A:\mathfrak{A}\to\mathfrak{S}$

$X\mapsto M_A(X):=M(A,X):=\{f:A\to X \text{ Abbildung}\},\ X\in\mathcal{O}(\mathfrak{A})$

$(X\xrightarrow{\phi}X')\mapsto(M_A(\phi):M(A,X)\to M(A,X')),\ \phi\in\mathcal{M}(\mathfrak{A})$

$$g\mapsto\phi\circ g$$

Sei $B\in\mathcal{O}(\mathfrak{A})$ ein weiteres Objekt. Dann wird ein kontravarianter Funktor $M^B:\mathfrak{A}\to\mathfrak{S}$ wie folgt definiert:

$M^B:\mathfrak{A}\to\mathfrak{S}$

$$Y \mapsto M^B(Y) := M(Y,B) = \{f : Y \to B \text{ Abbildung}\},\ Y \in \mathcal{O}(\mathfrak{A})$$

$$(Y' \xrightarrow{\phi} Y) \mapsto M^B(\phi) : M(Y,B) \to M(Y',B),\ \phi \in \mathcal{M}(\mathfrak{A})$$
$$f \to f \circ \phi$$

Diese Funktoren M_A und M^B heißen *Darstellungsfunktoren.*

Wir diskutieren nun unter funktoriellen Gesichtspunkten freie abelsche Gruppen. Sei S eine nichtleere Menge und sei

$$\mathbb{Z}(S) := \{\phi : S \to \mathbb{Z} \text{ Abbildung: } \phi(x) \neq 0 \text{ für nur endlich viele } x \in S\}.$$

$\mathbb{Z}(S)$ ist bezüglich der punktweise erklärten Addition und Skalarmultiplikation ein $\mathbb{Z}$-Modul, und die charakteristischen Funktionen χ_x, $x \in S$,

$$\chi_x(y) := \begin{cases} 1, & \text{falls } x = y \\ 0, & \text{falls } x \neq y \end{cases}$$

bilden eine $\mathbb{Z}$-Basis von $\mathbb{Z}(S)$.

Definition $\mathbb{Z}(S)$ heißt die *freie von S über $\mathbb{Z}$ erzeugte abelsche Gruppe.*

Jedes $\phi \in \mathbb{Z}(S)$ besitzt eine eindeutige Darstellung der Form

$$\phi = \textstyle\sum_{x \in S} \alpha_x \cdot \chi_x =: \sum_{x \in S} \alpha_x x \quad \text{mit} \quad \alpha_x = \phi(x).$$

Wir indentifizieren S vermöge der Abbildung $S \to \mathbb{Z}(S)$, $x \mapsto \chi_x$, mit einer Teilmenge von $\mathbb{Z}(S)$. Ist $\lambda : S \to S'$ eine Abbildung von nichtleeren Mengen, dann existiert ein Homomorphismus von Gruppen

$$\lambda_* = \mathbb{Z}(\lambda) : \mathbb{Z}(S) \to \mathbb{Z}(S'),$$

so daß das folgende Diagramm kommutiert

$$\begin{array}{ccc} S & \hookrightarrow & Z(S) \\ \lambda \downarrow & & \downarrow \lambda_* \\ S' & \hookrightarrow & Z(S') \end{array}$$

Die Zuordnungen

$$S \mapsto Z(S),\ \ \lambda \mapsto \lambda_*$$

definieren einen kovarianten Funktor von der Kategorie der Mengen in die Kategorie der Gruppen; dabei wird für die leere Menge $S = \phi$ unter $\mathbb{Z}(S)$ die triviale Gruppe verstanden.

Definition Sei $\mathfrak{C}$ eine Kategorie. Ein Objekt $P \in \mathcal{O}(\mathfrak{C})$ heißt *universell anziehend*, falls für alle $C \in \mathcal{O}(\mathfrak{C})$ genau ein Morphismus $C \to P$ existiert; und ein Objekt $P \in \mathcal{O}(\mathfrak{C})$ heißt *universell abstoßend*, falls für alle $C \in \mathcal{O}(\mathfrak{C})$ genau ein Morphismus $P \to C$ existiert.

Beispiel Sei S eine nichtleere Menge und sei $\mathfrak{A}$ die Kategorie der abelschen Gruppen. Sei $\mathfrak{A}(S)$ die folgende Kategorie: Die Objekte von $\mathfrak{A}(S)$ sind Abbildungen

$$f : S \to A \quad \text{mit} \quad A \in \mathcal{O}(\mathfrak{A}),$$

und die Morphismen $(f : S \to A) \to (f' : S \to A')$ sind Homomorphismen $\phi : A \to A'$, so daß $\phi \circ f = f'$. Sei $\mathbb{Z}(S)$ die freie abelsche Gruppe von S über $\mathbb{Z}$. Dann ist die Einbettung $S \hookrightarrow \mathbb{Z}(S)$, $s \to \chi_s$, ein universell abstoßendes Objekt in der Kategorie $\mathfrak{A}(S)$.

In nachfolgenden Abschnitten kommen weitere Beispiele von universellen Objekten vor.

Zum Schluß dieses Paragraphen besprechen wir Grothendieck-Gruppen und ihren Zusammenhang mit freien abelschen Gruppen.
Sei dazu $M = (M, +)$ ein kommutatives Monoid, so daß in M die folgende Kürzungsregel gilt:

$$x + z = y + z \Rightarrow x = y.$$

Das Monoid $M = (\mathbb{N}_0, +)$ erfüllt z.B. diese Bedingung.

(12.1) **Definition und Satz** *Zwei Elemente $(x, y), (x', y') \in M \times M$ heißen aequivalent, wenn $y + x' = x + y'$. Hierdurch wird auf $M \times M$ eine Aequivalenzrelation definiert.*

Beweis: $(x, y) \sim (x, y) : y + x = x + y$, weil M kommutativ ist.
$(x, y) \sim (x', y') \Longrightarrow (x', y') \sim (x, y) : y + x' = x + y' = y' + x = x' + y.$

$$(x, y) \sim (x', y') \sim (x", y") : \quad \left.\begin{array}{c} y + x' = x + y' \\ y' + x" = x' + y" \end{array}\right\} \Rightarrow$$
$$y + x' + x" = x + y' + x"$$
$$= x + x' + y"$$

$\Longrightarrow$(mit der Kürzungsregel) $y + x" = x + y"$, also $(x, y) \sim (x'', y'')$.

(12.2) **Satz und Definition** *Sei $(M \times M)/\sim$ die Menge aller Aequivalenzklassen der in (12.1) definierten Aequivalenzrelation. Die komponentenweise Addition definiert auf $(M \times M)/\sim$ die Struktur einer abelschen Gruppe. Diese Gruppe heißt die Grothendieckgruppe von M und wird mit $G(M)$ bezeichnet. Die Abbildung*

$M \to G(M), \;\; x \to (0, x),$

ist ein bijektiver Monoidhomomorphismus.

Beweis: Durch

$(x, y) + (x', y') := (x + x', y + y')$

ist eine Addition auf $(M \times M)/\sim$ wohldefiniert.
$(0, 0)$ ist das neutrale Element in $(M \times M)/\sim$.
$(x, y) + (y, x) = (0, 0)$, d.h. (y, x) ist das zu (x, y) inverse Element.

Beispiel $G((\mathbb{N}_0, +)) = (\mathbb{Z}, +)$

Nun zum Zusammenhang zwischen der Grothendieckgruppe und der freien abelschen Gruppe. Sei $(M, +)$ ein kommutatives Monoid, sei $\mathbb{Z}(M)$ die freie abelsche Gruppe von M über $\mathbb{Z}$ und sei $M \to \mathbb{Z}(M), x \to x$,die übliche Einbettung. Sei $B \leqq \mathbb{Z}(M)$ die Untergruppe, die von allen Elementen der Form

$[x + y] - [x] - [y]\,; x, y \in M$

erzeugt wird und sei

$K(M) := \mathbb{Z}(M)/B$

die entsprechende Faktorgruppe. Der folgende Satz ist leicht zu beweisen.

(12.3) **Satz** *Gilt für das Monoid $M = (M, +)$ die Kürzungsregel, dann ist die Abbildung*

$K(M) \to G(M), x + B \to (0, x)$

ein Isomorphismus von Gruppen.

Aufgaben und Beispiele

(1) Sei K ein Körper und sei $\mathfrak{V}_K$ die Kategorie der K-Vektorräumr. Für jeden K-Vektorraum V sei $V^* := Hom_K(V, K)$ der zu V duale K-Vektorraum. Jede K-liondeare Abbildung $f : V \to W$ von K-Vektorräumen induziert die duale K-lineare Abbildung $f^* : W^* \to V^*$, $f^*(\lambda)(v) := \lambda(f(v)), v \in V, \lambda \in W^*$. Zeigen Sie, daß die Zuordnungen $V \mapsto V^*, f \mapsto f^*$ einen kontravarianten Funktor $\mathfrak{V}_K \to \mathfrak{V}_K$ definieren.

(2) Jeder Kategorie $\mathfrak{C}$ wird wie folgt eine duale Kategorie $\mathfrak{C}^\circ$ zugeordnet: Die Objekte von $\mathfrak{C}^\circ$ sind die Objekte von $\mathfrak{C}$; für je zwei Objekte A, B von $\mathfrak{C}^\circ$ ist die Menge der Morphismen $\mathcal{M}(A, B)$ in $\mathfrak{C}^\circ$ per Definition die Menge $\mathcal{M}(B, A)$ in $\mathfrak{C}$; und die Komposition $f \circ g$ von zwei Morphismen in $\mathfrak{C}^\circ$ ist definiert als die Komposition $g \circ f$ in $\mathfrak{C}$. Es ist $\mathfrak{C}^{\circ\circ} = \mathfrak{C}$. Man erhält einen kontravarianten Funktor $\circ : \mathfrak{C} \to \mathfrak{C}^\circ$, incdem man jedem Objekt A von $\mathfrak{C}$ das Objekt A von $\mathfrak{C}^\circ$ und jedem Morphismus $f : A \to B$ in $\mathfrak{C}$ den Morphismus $f^\circ : B \to A$ in $\mathfrak{C}^\circ$ zuordnet.

(3) Sei $\mathfrak{S}$ die Kategorie der Mengen einer festen Stufe. Der kontravariante Funktor $\mathcal{P}\colon \mathfrak{S} \to \mathfrak{S}$ ordnet jeder Menge $A \in Ob(\mathfrak{S})$ ihre Potenzmenge $\mathcal{P}(A) \in Ob(\mathfrak{S})$ und jeder Mengenabbildung $f : A \to B$ mit $A, B \in Ob(\mathfrak{S})$ die Mengenabbildung $\mathcal{P}(f) : \mathcal{P}(B) \to \mathcal{P}(A)$, $X \mapsto f^{-1}(X) := \{x \in A : f(x) \in X\}$, zu. $\mathcal{P}$ respektiert die Operationen, die $\mathcal{P}(A)$ zu einer Booleschen Algebra machen.

(4) Sei $\mathfrak{A}$ eine Kategorie. Enthält die Menge der Morphismen $\mathcal{M}(A, B)$ für alle Objekte A, B von $\mathfrak{A}$ höchstens ein Element, dann heißt $\mathfrak{A}$ geordnet. Wenn für Objekte A, B einer geordneten Kategorie $\mathfrak{A}$ die Menge $\mathcal{M}(A, B)$ nicht leer ist, dann schreibt man $A \leq B$. Enthält die Menge $\mathcal{M}(A, B) \cup \mathcal{M}(B, A)$ für alle Objekte A, B von $\mathfrak{A}$ höchstens ein Element, dann heißt $\mathfrak{A}$ schwach geordnet. Enthält die Menge $\mathcal{M}(A, B) \cup \mathcal{M}(B, A)$ für alle Objekte genau ein Element, dann heißt $\mathfrak{A}$ streng geordnet. Jede teilweise bzw. total geordnete Menge ist eine schwach geordnete bzw. streng geordnete Kategorie.

Literatur zu § 12: [AD], [BW], [KS], [$L2$], [PI], [SC]

§ 13. **Monoide und Ringe**

In diesem Abschnitt beschreiben wir eine universelle Konstruktion mit Ringen und Monoiden und folgen dabei der entsprechenden Darstellung in [$L2$]. Sei dazu A ein kommutativer Ring mit Einselement 1.

Definition Eine A-Algebra ist ein A-Modul E zusammen mit einer A-bilinearen Abbildung $E \times E \to E$.

In diesem § 13 betrachten wir nur eine spezielle Art von Algebren, die wir jetzt beschreiben. Das Zentrum $Z(B)$ eines - nicht notwendigerweise kommutativen - Ringes B ist der Teilring

$Z(B) := \{b \in B : bx = xb \text{ für alle } x \in B\}$.

Sei $f : A \to B$ ein Ringhomomorphismus mit $f(A) \subset Z(B)$. Dann wird B auf folgende Weise zu einem A-Modul:

$A \times B \to B, (a, b) \to f(a)b$;

und die Ringmultiplikation

$B \times B \to B$

ist eine A-bilineare Abbildung. Somit ist B eine A-Algebra; wir sagen auch: $f : A \to B$ ist eine A-Algebra.

Sei G ein Monoid, dessen Verknüpfung wir multiplikativ schreiben: $G \times G \to G, (x, y) \to xy$. Sei e das neutrale Element von G.
Sei $\mathfrak{C}$ die folgende Kategorie: Die Objekte von $\mathfrak{C}$ sind die Tripel

(ϕ, f, B),

wobei $f : A \to B$ eine A-Algebra und wobei $\phi : G \to B$ ein Monoidhomomorphismus ist, d.h. es gilt

$\phi(xy) = \phi(x)\phi(y)$ für alle $x, y \in G$.

Die Morphismen von $\mathfrak{C}$ sind wie folgt definiert: Sind $(\phi, f, B), (\phi', f', B')$ Objekte von $\mathfrak{C}$, dann ist ein Morphismus

$(\phi, f, B) \to (\phi', f', B')$

ein Ringhomomorphismus

$h : B \to B'$,

so daß das folgende Diagramm kommutiert

$$\begin{array}{ccc} G & & \\ & \overset{\phi'}{\searrow} & \\ \phi\downarrow & & \\ B & \overset{h}{\to} & B' \\ f\uparrow & \overset{f'}{\nearrow} & \\ A & & \end{array} \quad .$$

Definition Eine freie (A, G)-Algebra oder eine freie G-Algebra über A ist ein universell abstoßendes Objekt in $\mathfrak{C}$

Im Folgenden konstruieren wir eine freie (A, G)-Algebra: Sei

$A[G] := \{\alpha : G \to A : \alpha(x) \neq 0 \text{ nur für endlich viele } x \in G\}$.

Die Addition in $A[G]$ wird über die Addition A^+ definiert Für $\alpha, \beta \in A[G]$ sei

$(\alpha \cdot \beta)(t) := \sum_{xy=t} \alpha(x)\beta(y)$ (das ist eine endliche Summe!)

Es ist $(\alpha \cdot \beta)(t) \neq 0$ nur für endlich viele t. Also ist $\alpha \cdot \beta =: \alpha\beta \in A[G]$. Die Ringaxiome sind erfüllt. Z.B. die Assoziativität:

$((\alpha\beta)\gamma)(t) = \sum_{xy=t}(\alpha\beta)(x)\gamma(y) =$

$= \sum_{xy=t}(\sum_{uv=x} \alpha(u)\beta(v))\gamma(y) =$

$= \sum_{xy=t}(\sum_{uv=x} \alpha(u)\beta(v)\gamma(y)) =$

$= \sum_{\substack{u,v,y \\ uvy=t}} \alpha(u)\beta(v)\gamma(y) =$

$= (\alpha(\beta\gamma))(t)$.

Das Einselement $\delta \in A[G]$ ist gegeben durch

$\delta(e) = 1, \delta(x) = 0$ für alle $x \in G - \{e\}$.

Es folgt nämlich: $\alpha = \delta\alpha = \alpha\delta$ für alle $\alpha \in A[G]$.

Für $a \in A, x \in G$ definieren wir $a \cdot x \in A[G]$ wie folgt:

$$(a \cdot x)(y) := \begin{cases} a, & \text{falls } y = x \\ 0, & \text{falls } y \neq x \end{cases}$$

Mit dieser Bezeichnung läßt sich jedes Element aus $A[G]$ eindeutig in der folgenden Form schreiben:

$\alpha = \sum_{x \in G} \alpha(x) \cdot x =: \sum_{x \in G} a_x \cdot x$.

$A[G]$ ist ein A-Modul mit der A-Basis $\{1 \cdot x\}_{x \in G}$. Die Multiplikation in $A[G]$ läßt sich mit dieser Schreibweise so darstellen:

$(\sum_{x \in G} a_x \cdot x)(\sum_{y \in G} b_y \cdot y) = \sum_{x,y \in G} a_x b_y xy$;

und die Addition so

$(\sum_{x\in G} a_x \cdot x) + (\sum_{x\in G} b_x \cdot x) = \sum_{x\in G}(a_x + b_x) \cdot x.$

Das Einselement $\delta \in A[G]$ ist in dieser Schreibweise gleich $1 \cdot e$. Sei $\phi_0 : G \to A[G]$ die Abbildung, die gegeben wird durch

$\phi_0(x) := 1 \cdot x.$

ϕ_0 ist ein multiplikativer Monoidhomomorphismus. Sei $f_0 : A \to A[G]$ die Abbildung $f_0(a) := a \cdot e$. f_0 ist ein Ringmonomorphismus.

Also: $A[G]$ ist eine A-Algebra mit G als Basis des A-Moduls $A[G]$.

(13.1) **Satz** $(\phi_0, f_0, A[G])$ *ist eine freie* (A, G)*-Algebra.*

Die Behauptung dieses Satzes folgt aus dem nachstehenden allgemeineren Resultat mit $B = A[G]$.

(13.2) **Satz** *Sei $f_0 : A \to B$ eine A-Algebra, sei G ein multiplikatives Teilmonoid von B und sei G eine A-Basis von B. Sei $f : A \to B$ eine weitere A-Algebra und sei $\phi : G \to C$ ein Monoidhomomorphismus. Dann existiert genau ein Ringhomomorphismus $h : B \to C$, so daß das folgende Diagramm kommutiert*

$$\begin{array}{ccc} B & \overset{h}{\to} & C \\ f_0 \uparrow & \nearrow_{f} & \\ A & & \end{array}$$

Außerdem ist $h_{|G} = \phi$.

Beweis: Für $x \in G$ und $a \in A$ schreibe

$a \cdot x = f_a(a)x.$

Jedes $\alpha \in A[G]$ hat eine eindeutige Darstellung der Form

$\alpha = \sum_{x\in G} a_x \cdot x \quad \text{mit} \quad a_x \in A.$

Es gibt genau einen Modulhomomorphismus $h : B \to C$, so daß obiges Diagramm kommutiert, nämlich

$h(\alpha) := \sum_{x\in G} f(a_x)\phi(x).$

Wir zeigen, daß h ein Ringhomomorphismus ist. Sei dazu $\beta = \sum_{y\in G} \beta_y y \in A[G]$. Dann gilt

$\alpha \cdot \beta = \sum_{z \in G} (\sum_{xy=z} a_x b_y) z$

und

$$\begin{aligned} h(\alpha \cdot \beta) &= \sum_z (\sum_{xy=z} a_x b_y) \phi(z) \\ &= \sum_z (\sum_{xy=z} f(a_x) f(b_y)) \phi(z) \\ &= h(\alpha) h(\beta). \end{aligned}$$

Wegen $h_{|G} = \phi$ ist $h(1) = 1$. Also ist h ein Ringhomomorphismus.

(11.3) **Satz** *Sei $\phi : G \to G'$ ein Monoidhomomorphismus und sei $f : A \to A'$ ein Homomorphismus von kommutativen Ringen mit 1. Dann existiert genau ein Ringhomomorphismus $h : A[G] \to A'[G']$, so daß das folgende Diagramm kommutiert*

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ \phi_0 \downarrow & & \downarrow \phi_0' \\ A[G] & \xrightarrow{h} & A'[G'] \\ f_0 \uparrow & & \uparrow f_0' \\ A & \xrightarrow{f} & A' \end{array}$$

Die Behauptung folgt aus dem vorangehenden Satz mit $C = A'[G'], \phi = \phi_0', f = f_0'$.

Ist Σ eine nichtleere Menge und $G = \Sigma^*$ das freie Monoid, das aus allen endlichen Folgen von Elementen aus Σ besteht und in dem zwei solche Folgen verknüpft werden, in dem sie hintereinander geschrieben werden und in dem das neutrale Element die leere Folge ist, dann heißt $A[G]$ die freie A-Algebra über Σ.

Mit Hilfe der obigen Begriffsbildungen lassen sich auch Polynome definieren.

Sei dazu S eine nichtleere Menge und sei $\mathbb{N}_0 = \{0, 1, 2, ...\}$. Wir betrachten $\mathbb{N}_0$ als Monoid bezüglich der Addition. Sei

$\mathbb{N}_0 \langle S \rangle := \{f : S \to \mathbb{N}_0 : f(x) \neq 0$ nur für endlich viele $x \in S\}$.

Für $x \in S$ und $i \in \mathbb{N}_o$ sei $x^i \in \mathbb{N}_0 \langle S \rangle$ wie folgt definiert:

$$x^i(y) := \begin{cases} i, & \text{falls } y = x \\ 0, & \text{falls } y \neq x \end{cases}.$$

Für $\phi, \psi \in \mathbb{N}_0 \langle S \rangle$ sei

$(\phi \cdot \psi)(x) := \phi(x) + \psi(x)$.

Dann ist $G = \mathbb{N}_0 \langle S \rangle$ bezüglich dieser Verknüpfung $(\phi, \psi) \to \phi \cdot \psi$ ein multiplikatives Monoid; das Einselement ist die 0-Funktion.

Jedes $\phi \in G$ läßt sich eindeutig in der folgenden Form schreiben:

$\phi = \sum_{x \in S} x^{\nu(x)}$,

wobei $\nu : S \to \mathbb{N}_0$ eine Abbildung ist mit der Eigenschaft, daß $\nu(x) \neq 0$ nur für endlich viele $x \in S$. Produkte von dieser Form heißen primitive Monome; wir benutzen dafür folgende Schreibweise

$M_{(\nu)}(S) := \prod_{x \in S} x^{\nu(x)}$.

Definition Sei A ein kommutativer Ring mit Einselement 1. Die Monoidalgebra

$A[G] := A[\mathbb{N}_0 \langle S \rangle]$

heißt die Polynomalgebra von S über A.

Jedes Element (= Polynom) aus $A[S] := A[G]$ läßt sich eindeutig in der folgenden Form darstellen:

$\sum_{(\nu)} a_{(\nu)} M_{(\nu)}(S) = \sum_{(\nu)} a_{(\nu)} \prod_{x \in S} x^{\nu(x)}$,

wobei $(\nu) \in \mathbb{N}_o \langle S \rangle$ und $a_{(\nu)} \neq 0$ nur für endlich viele (ν). Die primitiven Monome bilden also eine Basis von $A[G]$. Die $a_{(\nu)}$ heißen die Koeffizienten des Polynoms

Beispiel $S = \{X_1, ..., X_n\}$. Dann heißt

$A[S] =: A[X_1, ..., X_n] =: A[X]$

die Polynomalgebra in den Unbestimmten $X_1, ..., X_n$. Jedes Element aus $A[X_1, ..., X_n]$ läßt sich eindeutig in der folgenden Form darstellen:

$\sum_{(\nu)} a_{(\nu)} M_{(\nu)}(x) = \sum_{(\nu)} a_{(\nu)} X_1^{\nu_1} ... X_n^{\nu_n}$.

Aufgaben und Beispiele

(1) Sei B ein kommutativer Ring und sei $A \subset B$ ein Teilring. Die A-Algebra B heißt endlich erzeugt, wenn eine endliche Teilmenge $S \subset B$ mit $B = A[S]$ existiert. Zeigen Sie: Wenn B endlich erzeugt ist, dann existieren endlich viele Unbestimmte $X_1, ..., X_n$ über A und ein Ideal I im Polynomring $A[X_1, ..., X_n]$, so daß der Faktorring $A[X_1, ..., X_n]/I$ isomorph zu B ist.

Literatur zu § 13: [$L2$]

§ 14. **Fehlerkorrigierende Codes und ihre Gewichtspolynome**

Fehlerkorrigierende Codes treten in vielen technischen Zusammenhängen auf, z.B. bei der Sicherung von Daten, bei der Übertragung von Nachrichten, z.B. beim Senden von Satellitenaufnahmen,... . In diesem Abschnitt beschreiben wir die Grundlagen der Theorie der fehlerkorrigierenden Codes und folgen dabei den entsprechenden Darstellungen in [HS], [SW], [MS], [VL] und [T]. Die grundlegende Idee ist wie folgt. Die zu übertragende Information liegt in Form von endlichen Folgen von Symbolen (Zahlen oder Buchstaben), die einer vorgegebenen endlichen Menge, dem sogenannten Alphabet, angehören, vor. Das können z.B. Meßwerte sein, die ein Satellit im Weltraum ermittelt hat und die in endliche 0-1-Folgen gemäß der Binärdarstellung (vgl. (3.4)) verwandelt wurden; das zugrunde liegende Alphabet ist hier also die Menge $\{0, 1\}$, wobei bei der technischen Übertragung das Sysmbol 0 in ein kurzes und das Symbol 1 in ein langes Signal verwandelt wird. In einer endlichen Folge von Symbolen des Alphabets erscheint jedes Symbol mit derselben Wahrscheinlichkeit. Bei der technischen Übertragung einer solchen Folge treten häufig Störungen auf, die zur Folge haben, daß eventuell ein oder mehrere Symbole in andere Symbole aus dem Alphabet verwandelt werden. Das ist z.B. der Fall, wenn eine Satellitenaufnahme vom Satelliten in Form von 0-1 Folgen gesendet wird und Strahlungseinflüsse im Weltraum einen langen Signalton - für das Symbol 1 - in einen kurzen Signalton - für das Symbol 0 - verwandeln (oder umgekehrt). Allgemein spricht man bei einer solchen Umwandlung eines Symbols in ein anderes Symbol von einem Symbolfehler. Dabei geht man davon aus, daß Symbolfehler stets mit derselben Wahrscheinlichkeit auftreten. Ähnlich wie in der Umgangssprache, in der Fehler, die in einem langen Wort auftreten, leichter zu erkennen sind als Fahler, die in einem kurzen Wort auftreten, kann man auch in der Theorie der fehlerkorrigierenden Codes Fehler, die in einer langen Symbolfolge auftreten, leichter erkennen als solche, die in einer kurzen Symbolfolge auftreten. Durch Hinzufügen von redundanten Symbolen zu einer Symbolfolge läßt sich einerseits die Fehlerwahrscheinlichkeit bei der Decodierung von empfangenen Symbolfolgen verringern, andererseits erhöhen sich dadurch auch die Übertragungskosten. Die Aufgabe der Theorie der fehlerkorrigierenden Codes besteht darin, diese Problematik zufriedenstellend zu lösen.

Sei p eine Primzahl und $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen. Sei n eine natürliche Zahl. Ein *Code* bzw. ein *linearer Code der Länge n über $\mathbb{F}_p$* ist

eine Teilmenge bzw. ein Teilvektorraum des n-dimensionalen $\mathbb{F}_p$-Vektorraums $\mathbb{F}_p^n$. Die Elemente c eines Codes C heißen auch *Codewörter*. Auf $\mathbb{F}_p^n$ führt man den sogenannten *Hamming-Abstand* $d : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{N} \cup \{0\}$ ein: Für $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in \mathbb{F}_p^n$ ist $d(x, y)$ definiert als die Anzahl der Indizes i mit $1 \leq i \leq n$ und $x_i \neq y_i$. Die Abbildung d hat alle Eigenschaften einer Metrik, d.h. es gilt

(1) $d(x, x) = 0$ für alle $x \in \mathbb{F}_p^n$
(2) $d(x, y) = d(y, x)$ für alle $x, y \in \mathbb{F}_p^n$
(3) $d(x, y) \leq d(x, y) + d(y, z)$ für alle $x, y, z \in \mathbb{F}_p^n$

Definition Der *Minimalabstand eines* Codes $C \subset \mathbb{F}_p^n$ ist definiert durch

$$d := d(C) := Min\{d(x, y) : x, y \in C, x \neq y\}.$$

In dem in diesem Abschnitt zu besprechenden Modell gehen wir davon aus, daß ein Empfänger bei der Decodierung einer Nachricht ein empfangenes Wort c' aus $\mathbb{F}_p^n$ in ein Codewort $c \in C$ verwandelt, das im Sinne des Hamming-Abstands dem empfangenen Wort c' am nächsten liegt, d.h. $d(c', c)$ ist minimal. Durch diese Forderung ist c im allgemeinen nicht eindeutig bestimmt. Man trifft also bei der Decodierung eine Auswahl.

Definition Die *Informationsrate* eines Codes $C \subset \mathbb{F}_p^n$ ist

$$R := R(C) := \frac{\log_p(|C|)}{n}.$$

Ein (n, k, d)-Code C über $\mathbb{F}_p$ hat offensichtlich die Informationsrate $\frac{k}{n}$.

Aus obigen Bemerkungen über den Zusammenhang zwischen der Fehlerwahrscheinlichkiet bei der Decodierung und der Länge eines Codes ergibt sich einerseits, daß diese Fehlerwahrscheinlichkeit mit kleiner werdender Informationsrate abnimmt, daß es andererseits aber wünschenswert erscheint, Codes mit hoher Informationsrate und großem Minimalabstand zu konstruieren.

Definition C heißt (n, M, d)-Code über $\mathbb{F}_p$, falls C eine Teilmenge von $\mathbb{F}_p^n$ mit Cardinalität M und Minimalabstand d ist. C heißt (n, k)-Code über $\mathbb{F}_p$, wenn C ein k-dimensionaler Unterraum von $\mathbb{F}_p^n$ ist; C heißt dann auch linearer (n, k)-Code über $\mathbb{F}_p$. Hat ein linearer (n, k)-Code C den Minimalabstand d, dann heißt C auch (n, k, d)-Code über $\mathbb{F}_p$.

Definition Sei $f \in \mathbb{N}$ und sei C ein Code der Länge n über $\mathbb{F}_p$. Man sagt, daß der Code C höchstens f *Fehler korrigieren* kann, wenn gilt: Ist $a \in \mathbb{F}_p^n$ und ist $b \in C$ so, daß $d(a, b) \leq f$, dann ist $d(a, b') > f$ für alle $b' \in C$ mit $b' \neq b$.

Der folgende einfache Satz zeigt die Bedeutung des Minimalabstands für die fehlerkorrigierenden Eigenschaften eines Codes.

(14.1) **Satz** *Sei C ein Code der Länge n über $\mathbb{F}_p$ und sei $d = d(C)$ der Minimalabstand von C. Schreibt man $d = d(C) = 2e+1$ mit $e \in \mathbb{Q}$, dann kann der Code C höchstens $[e]$ Fehler korrigieren ($[e]$:= größte ganze Zahl $\leq e$).*

Beweis: Sei $a \in \mathbb{F}_p^n$. Angenommen es existieren verschiedene $b, b' \in C$ mit der jeweiligen Eigenschaft $d(a,b) \leq e$, $d(a,b') \leq e$. Anwendung der Dreiecksgleichung (3) und der Symmetrieeigenschaft (2) ergibt: $d(b,b') \leq d(b,a)+d(b',a) \leq e+e < 2e+1 = d$; das steht aber im Widerspruch dazu, daß $d = d(C)$ der Minimalabstand von C ist.

Definition Eine *Erzeugermatrix* G eines linearen (n,k)-Codes über $\mathbb{F}_p$ ist eine Matrix über $\mathbb{F}_p$, deren Zeilen aus k Basisvektoren von C bestehen.

Ist G eine Erzeugermatrix für den linearen (n,k)-Code C über $\mathbb{F}_p$, dann gilt also

$C = \{aG : a \in \mathbb{F}_p^k\}$.

Definition Zwei lineare Codes $C, C' \leq \mathbb{F}_p^n$ heißen *aequivalent,* wenn eine Permutation $s \in S_n$ existiert, so daß $C' = s(C)$. Dabei ist für alle $s \in S_n$: $s(C) := \{s(c) : x \in C\}$, und $s((a_1,...,a_n)) := (a_{s(1)},...,a_{s(n)})$ für alle $a \equiv (a_1,...,a_n) \in \mathbb{F}_p^n$.

Bis auf Aequivalenz hat also ein linearer (n,k)-Code C über $\mathbb{F}_p$ eine Erzeugermatrix G der Form $G = (E_k, P)$, wobei P eine $(k \times (n-k))$-Matrix und E_k die Einheitsmatrix vom Grad k ist. In dieser Situation werden die ersten k Symbole eines Codewortes aus C auch die *Informationssymbole* und die restlichen Symbole auch die *Prüfsymbole* genannt.

Definition Das *Gewicht* $w(x)$ von $x \in \mathbb{F}_p^n$ ist die Anzahl der von 0 verschiedenen Komponenten von x. Das *Minimalgewicht eines Codes* $C \subset \mathbb{F}_p^n$ ist das Minimum aller $w(x), x \in C, x \neq 0$.

(14.2) **Bemerkung** Ist C ein linearer Code, dann ist das Minimalgewicht gleich dem Minimalabstand von C.

Definition Sei C ein (n,k)-Code über $\mathbb{F}_p$. Der zu C duale Code $C^\perp$ ist definiert durch

$C^\perp := \{y \in \mathbb{F}_p^n : (x,y) = 0 \text{ für alle } x \in C\}$,

wobei für alle $x = (x_1,...,x_n), y = (y_1,...,y_n) \in \mathbb{F}_p^n$

$(x,y) := x_1y_1 + ... + x_ny_n$

$C^\perp$ ist ein linearer $(n, n-k)$-Code. Ein linearer Code C über $\mathbb{F}_p$ heißt selbstdual, wenn $C = C^\perp$.

Ist C ein Code der Länge n über $\mathbb{F}_p$, dann ist der *erweiterte Code* $\widetilde{C}$ definiert durch

$$\widetilde{C} := \{(c_1, ..., c_n, c_{n+1}) : (c_1, ..., c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}.$$

Beispiele (vgl. z.B. $[HS]$; $[MIH]$, Appendix 5)

(1) Der Code $\{(1,1,1,1,1),(0,0,0,0,0)\} \subset \mathbb{F}_2^5$ heißt der Wiederholungscode der Länge 5. Wenn die Nachricht $(0,1,0,0,1) \in \mathbb{F}_2^5$ empfangen wird, dann wird sie, entsprechend dem eingangs erläuterten Decodierungsprinzip, durch das im Sinne des Hamming Abstands am nächsten liegende Codewort, nämlich $(0,0,0,0,0)$, decodiert. Da der Minimalabstand von C gleich $5 = 2 \cdot 2 + 1$ ist, kann dieser Code 2 Fehler korrigieren. Die Informationsrate dieses Codes ist $1/5$.

(2) Der nach seinem Erfinder benannte Hamming-Code $C = H_7$ der Länge 7 wird wie folgt konstruiert. H_7 besteht aus allen 0-1 Folgen der Form

$(\epsilon_0, \epsilon_1, \epsilon_2, \epsilon_3, k_1, k_2, k_3)$ mit $k_i \in \{0,1\}$ und

$$k_1 = \epsilon_0 + \epsilon_2 + \epsilon_3$$
$$k_2 = \epsilon_0 + \epsilon_1 + \epsilon_3$$
$$k_3 = \epsilon_0 + \epsilon_1 + \epsilon_2$$

Die Elemente von H_7 sind also

0	0	0	0	0	0	0
0	0	0	1	1	1	0
0	0	1	0	1	0	1
0	0	1	1	0	1	1
0	1	0	0	0	1	1
0	1	0	1	1	0	1
0	1	1	0	1	1	0
0	1	1	1	0	0	0
1	0	0	0	1	1	1
1	0	0	1	0	0	1
1	0	1	0	0	1	0
1	0	1	1	1	0	0
1	1	0	0	1	0	0
1	1	0	1	0	1	0
1	1	1	0	0	0	1
1	1	1	1	1	1	1

Die Konstruktion zeigt: H_7 ist ein linearer $(7,4)-$Code über $\mathbb{F}_2$ mit Minimalabstand 3; er kann also 1 Fehler korrigieren und hat die Informationsrate $\frac{4}{7}$. Der Hamming-Code H_7 wurde benutzt, um gespeicherte Daten abzusichern.

(3) Als weiteres Beispiel eines Codes nennen wir den Golay-Code G_{24} und folgen dabei $[MIH]$, Appendix 5.

(14.3) **Satz** *Es existiert ein linearer* $(24, 12)$*-Code* $G_{24} \leq \mathbb{F}_2^{24}$ *mit Minimalabstand* 8*, so daß das Gewicht eines jeden von Null verschiedenen Codeworts aus* G_{24} *durch* 4 *teilbar ist. Außerdem enthält* G_{24} *den Vektor* $(1, 1, ..., 1) \in \mathbb{F}_2^{24}$*, dessen Komponenten nur aus Einsen bestehen.*

Wir beschreiben nachfolgend lediglich die in $[MIH]$, Appendix 5, angegebene Konstruktion von G_{24} und verweisen für die Beweise auf die dortigen Ausführungen. Sei dazu A die symmetrische (11×11)-Matrix über $\mathbb{F}_2$, deren 1-te Zeile

11101101000

ist und deren übrige Zeilen durch zyklische Permutation der Komponenten dieser ersten Zeile nach links entstehen. Sei B die symmetrische (12×12)-Matrix über $\mathbb{F}_2$, die aus A durch Hinzufügen der ersten Zeileund Spalte 011111111111 entsteht, also

$$B = \begin{pmatrix} 0 & 1 & 1 & . & . & . & 1 \\ 1 & & & & & & \\ 1 & & & & & & \\ . & & & A & & & \\ . & & & & & & \\ . & & & & & & \\ 1 & & & & & & \end{pmatrix}$$

Über $\mathbb{F}_2$ gilt $B^2 = BB^t = E_{12}$. Also ist B nichtsingulär, und je zwei Zeilen von B sind orthogonal bezüglich des Skalarproduktes $\mathbb{F}_2^{12} \times \mathbb{F}_2^{12} \to \mathbb{F}_2$, $(r, r') \mapsto \sum_{i=1}^{12} r_i r'_i$. Eine Erzeugermatrix für den Golay-Code ist (E_{12}, B). Dieser Code kann also 3 Fehler korrigieren und hat die Informationsrate $\frac{1}{2}$.

Definition Das sogenannte *vollständige Gewichtspolynom* eines linearen Codes $C \leq \mathbb{F}_p^n$ ist das wie folgt definierte Polynom

$W_C(x_0, ..., x_{p-1}) \in \mathbb{C}[x_0, ..., x_{p-1}]$

in den p Veränderlichen $x_0, ..., x_{p-1}$ (zum Begriff des Polynoms in mehreren Veränderlichen vgl. § 13):

$W_C(x_0, ..., x_{p-1}) := \sum_{v \in C} x_0^{w_0(v)} \cdot ... \cdot x_{p-1}^{w_{p-1}(v)}$

wobei für $v = (v_1, ..., v_n) \in \mathbb{F}_p^n$ und $k \in \{0, 1, ..., p-1\}$ mit $w_k(v)$ die Anzahl der Komponenten v_j von v mit der Eigenschaft $v_j \equiv k \bmod p$ bezeichnet wird. W_C ist ein homogenes Polynom vom Grad n. Wir beschreiben nachfolgend kurz

die Rolle, die dieses Polynom in der Codierungstheorie spielt und in welchem Zusammenhang es zur endlichen Fouriertransformation steht. Dazu übersetzen wir zunächst die Poisson-Formel für endliche abelsche Gruppen (7.12) in eine Identität für das Polynom $W_C(x_0, ..., x_{p-1})$. Für jedes $v = (v_1, ..., v_n) \in \mathbb{F}_p^n$ induziert die Zuordnung $\chi_v \mapsto x_0^{w_0(v)} \cdot ... \cdot x_{p-1}^{w_{p-1}(v)}$ durch $\mathbb{C}$-lineare Fortsetzung eine $\mathbb{C}$-lineare Abbildung

$$f : S(V) \to \mathbb{C}[x_0, ..., x_{p-1}].$$

Mit Hilfe von f wird die Poisson-Formel (7.12) zur sogenannten MacWilliams Identität für das vollständige Gewichtspolynom, vgl. z.B. [T]:

(14.4) **Satz** *Sei $C \leq \mathbb{F}_p^n$ ein linearer Code. Dann gilt für das Gewichtspolynom $W_C(x_0, ..., x_{p-1})$ die Identität*

$$W_C(y) = |C|\, W_{C^\perp}(x),$$

wobei

$$y = (y_0, ..., y_{p-1}) \text{ mit } y_j = \sum_{k=0}^{p-1} \exp(2\pi ikj/p) x_k$$

Wir betrachten den Fall $p = 2$ und benennen die Veränderlichen x_0, x_1 um: $x := x_0, y := x_1$. Dann wird

$$W_C(x_0, x_1) = W_C(x, y) = \sum_{u \in C} x^{n-w(u)} y^{w(u)},$$

wobei $w(u)$ das Gewicht von $u \in C$ bezeichnet. Bezeichnet A_r die Anzahl der Codewörter vom Gewicht r, dann ist also

$$W_C(x, y) = \sum_{r=0}^{n} A_r x^{n-r} y^r =$$

$$= x^n + A_{d(C)} x^{n-d(C)} y^{d(C)} + ...,$$

wobei $d(C)$ das Minimalgewicht von C bezeichnet. Die MacWilliams Identität (14.4) wird in dieser Situation zur Identität

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + y, x - y)$$

Sei $C \leq \mathbb{F}_2^n$ ein selbstdualer linearer Code, so daß das Gewicht jedes Codeworts durch 2 teilbar ist. Dann ergeben sich mit Hilfe der MacWilliams Identität:

(14.5) $W_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}) = W_C(x,y), \;\; W_C(x,-y) = W_C(x,y).$

Man kann diese Betrachtung auch so deuten: Das Polynom $W_C(x,y)$ ist invariant unter der Operation der Untergruppe G von $GL(2,\mathbb{C})$, die von den Matrizen

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

erzeugt wird; dabei ist für $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{C})$ und ein beliebiges Polynom $p(x,y)$ in zwei Veränderlichen mit Koeffizienten aus $\mathbb{C}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (p(x,y)) := p(ax+by, cx+dy)$$

Man weiß aus der Invariantentheorie, daß sich jedes Polynom $p(x,y)$ mit $A(p(x,y)) = p(x,y)$ für alle $A \in G$ als Polynom in x^2+y^2 und $x^2y^2(x^2-y^2)^2$ schreiben läßt. Insbesondere gilt diese Aussage also für das Gewichtspolynom $W_C(x,y)$; diese Beobachtung stammt von A.M.Gleason [GS]. Auch die folgende Aussage wurde von A.M. Gleason bewiesen, vgl. [GS].

(14.6) **Satz** *Sei $C \leq \mathbb{F}_2^n$ ein linearer selbstdualer Code, so daß das Gewicht jedes Codewortes durch 4 teilbar ist. Dann ist das vollständige Gewichtspolynom $W_C(x,y)$ in eindeutiger Weise als Polynom in den Gewichtspolynomen $W_{\widetilde{H}_7}(x,y)$ und $W_{G_{24}}(x,y)$ darstellbar, wobei $\widetilde{H}_7$ den erweiterten Hamming-Code der Länge 8 und G_{24} den Golay-Code der Länge 24 bezeichnet.*

Für eine ausführliche Darstellung dieser und anderer Resultate von Gleason und Verallgemeinerungen dieser Resultate, nebst der benötigten Aussagen aus der Invariantentheorie, vgl. [MS], Chapter 19.

Aufgaben und Beispiele

(1) Beweisen Sie, daß der Hamming-Abstand die genannten Eigenschaften einer Metrik besitzt.

(2) Schreiben Sie (evtl. unter Zuhilfenahme von [MIH], Appendix 5), einen ausführlichen Beweis für die Aussage (14.3) über die Konstruktion und die Eigenschaften des Golay-Codes G_{24}.

(3) Zeigen Sie, daß die Untergruppe von $GL(2,\mathbb{C})$, die von den Matrizen

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ und } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

erzeugt wird, isomorph zur Diedergruppe der Ordnung 16 ist.

(4) Zeigen Sie:

$W_{\tilde{H}_7}(x,y) = x^8 + 14x^4y^4 + y^8$

$W_{G_{24}}(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$

Literatur zu § 14: $[DM]$, $[GS]$, $[HS]$, $[MIH]$, $[MS]$, $[SW]$, $[T]$, $[VL]$

§ 15. **Algebraische Systeme**

In diesem Abschnitt beschreiben wir kurz und weitgehend ohne Beweise ein Schema, in das sich viele der bisher besprochenen algebraischen Strukturen einordnen lassen. Dabei folgen wir entsprechenden Darstellungen in $[AD]$, $[BS]$, $[BB]$, $[MC]$ und in $[LS]$. Insbesondere werden dabei Abschnitte aus $[BB]$, $[BS]$ und $[LS]$ übernommen.

Definition Ein *algebraisches System* ist ein Paar $\underline{A} = (A, \Omega)$, wobei A eine Menge ist und wobei Ω eine Menge von Operationen auf A ist, d.h. jedes $\omega \in \Omega$ ist eine Abbildung

$\omega : A^n \to A$

für ein von ω abhängiges $n = n(\omega) \in \mathbb{N}_0$. $n(\omega)$ heißt auch die *Stelligkeit* oder die *Dimension von* ω. Dabei sei $A^0 := \{\phi\}$ eine einelementige Menge; eine Abbildung $f : A^0 \to A$ definiert dann ein Element $f(\phi) \in A$ und wird mit diesem Element identifiziert.

Ist $\underline{A} = (A, \Omega)$ ein algebraisches System, so heißt $\underline{A}$ oder A auch Ω-*Algebra.*

Definition Eine *heterogene Algebra* $(\{A_i\}_{i\in I}, \Omega)$ besteht aus einer Familie von Mengen A_i, die durch die Elemente $i \in I$ induziert sind, und aus einer Menge Ω von Operationen, die in der folgenden Weise definiert sind: Zu jedem $\omega \in \Omega$ existieren genau ein $n = n(\omega) \in \mathbb{N}_0$ und ein $(n+1)$-Tupel $(i_1, ..., i_n, i_{n+1}) \in I^{n+1}$, so daß ω eine Abbildung der folgenden Form ist

$\omega : A_{i_1} \times ... \times A_{i_n} \to A_{i_{n+1}}$.

Beispiele (1) Jede Boolesche Algebra $(B, \wedge, \vee, ', 0, 1)$ ist ein algebraisches System $\underline{A} = (A, \Omega)$ mit $A = B$, $\Omega = \{\wedge, \vee, ', 0, 1\}$ mit $n(\wedge) = 2 = n(\vee)$, $n(') = 1$, $n(0) = 0 = n(1)$; dabei werden 0 und 1 als Abbildungen f bzw. $g : A^0 \to A$ gedeutet; d.h. $A^0 = \{\phi\}$, $f(\phi) = 0$, $g(\phi) = 1$.

(2) Jeder Ring $(R, +, -, \cdot, 0, 1)$ ist ein algebraisches System mit $A = R$, $\Omega = \{+, -, \cdot, 0, 1\}$.

(3) Jeder Automat $(S, X, Z; \delta, \lambda)$ ist eine heterogene Algebra.

Definition Sei $\underline{A} = (A, \Omega)$ ein algebraisches System. Man sagt, daß eine nichtleere Teimenge $B \subset A$ eine Ω-*Teilalgebra* ist, wenn B Ω-abgeschlossen ist, d.h. für alle $\omega \in \Omega$ ist das Bild der Einschränkung von ω auf B^n in B enthalten. $\underline{B} = (B, \Omega)$ heißt dann *die durch B definierte Teilalgebra.*

(15.1) **Satz** *Sei $\mathfrak{B}$ ein System von Teilalgebren des algebraischen Systems $\underline{A} = (A, \Omega)$. Dann definiert $\cap_{B \in \mathfrak{B}} B$ eine Ω-Teilalgebra von (A, Ω).*

Beweis: Für alle $\omega \in \Omega$ gilt: Wenn $x_1, ..., x_{n(\omega)} \in \cap_{B \in \mathfrak{B}} B$, dann ist $\omega(x_1, ..., x_{n(\omega)}) \in B$ für alle $B \in \mathfrak{B}$ und damit $\omega(x_1, ..., x_{n(\omega)}) \in \cap_{B \in \mathfrak{B}} B$.

Definition Sei $\underline{A} = (A, \Omega)$ ein algebraisches System. Sei $H \subset A$ eine nichtleere Teilmenge und sei

$\mathfrak{K} := \{B : \underline{B} = (B, \Omega)$ ist eine Teilalgebra von (A, Ω) mit $H \subset B\}$.

Nach dem vorstehenden Satz definiert

$[H] := \cap_{B \in \mathfrak{K}} B$

eine Teilalgebra $\underline{[H]}$ von (A, Ω), nämlich die - bezüglich der Inklusion - *kleinste Teilalgebra von (A, Ω)*, die H enthält. $\underline{[H]}$ heißt auch *die von H erzeugte Teilalgebra von (A, Ω)*. Wenn ein Element $a \in A$ existiert, so daß $\underline{A}$ gleich der von $H = \{a\}$ erzeugten Teilalgebra ist, dann heißt $\underline{A}$ *zyklisch.*

Definition Zwei algebraische Systeme $\underline{A} = (A, \Omega)$ und $\underline{A'} = (A', \Omega')$ heißen *ähnlich*, falls eine bijektive Abbildung $\Omega \xrightarrow{\alpha} \Omega'$ existiert, so daß $n(\alpha(\omega)) = n(\omega)$ für alle $\omega \in \Omega$ gilt. Ein *Morphismus* oder ein *Homomorphismus von ähnlichen algebraischen Systemen* $\underline{A} = (A, \Omega)$, $\underline{A'} = (A', \Omega')$ ist eine Abbildung

$f : A \to A'$,

so daß für alle $\omega \in \Omega$ und für alle $a_1, ..., a_{n(\omega)} \in A$ gilt

$f(\omega(a_1, ..., a_{n(\omega)})) = \omega'(f(a_1), ..., f(a_{n(\omega)}))$,

wobei $\omega' = \alpha(\omega)$ im Sinne der Ähnlichkeit zu ω gehört.

Bemerkungen (1) Die ähnlichen algebraischen Systeme zusammen mit den Morphismen bilden eine Kategorie. Damit sind insbesondere die Begriffe Epimorphismus, Monomorphismus und Isomorphismus von ähnlichen algebraischen

Systemen definiert. Z.B. ist $\log : (\mathbb{R}_{>0}, \cdot, 1) \to (\mathbb{R}, +, 0)$ ein Isomorphismus von ähnlichen algebraischen Systemen.

(2) Seien $\underline{A} = (A, \Omega)$, $\underline{B} = (B, \Omega')$ ähnliche algebraische Systeme und seien $f : \underline{A} \to \underline{B}$, $g : \underline{A} \to \underline{B}$ Morphismen. Dann definiert die Menge

$$A_0 := \{x \in A : f(x) = g(x)\}$$

eine Teilalgebra $\underline{A}_0 = (A_0, \Omega)$ von $\underline{A}$.

(3) Seien $\underline{A}$, $\underline{A}'$ zwei ähnliche algebraische Systeme und seien

$$f,\ g : \underline{A} \to \underline{A}'$$

zwei Morphismen. $\underline{A}$ werde erzeugt durch eine Teilmenge $X \subset A$. Wenn dann $f(x) = g(x)$ für alle $x \in X$, so ist $f = g$.

(15.2) **Satz** *Sei $\underline{A} = (A, \Omega)$ ein algebraisches System und sei $H \subset A$ eine nichtleere Teilmenge. Sei $S \subset A$ eine Teilmenge mit den folgenden Eigenschaften:*

(1) $H \subset S$

(2) *Für alle $\omega \in \Omega$ und für alle $x_1, ..., x_{n(\omega)} \in S$ ist $\omega(x_1, ..., x_{n(\omega)}) \in S$*

(3) *Alle Elemente aus S entstehen in der unter* (1) *und (2) beschriebenen Art und Weise.*

Dann ist $\underline{S} = (S, \Omega)$ eine Teilalgebra von $\underline{A}$, und es gilt $\underline{S} = \underline{[H]}$.

Beweis: $\underline{S} = (S, \Omega)$ ist nach (2) und (1) eine Teilalgebra von (A, Ω) mit $H \subset S$. $\underline{[H]}$ ist die kleinste Teilalgebra von $(A, \Omega$, die H enthält. Also gilt $\underline{[H]} \subset \underline{S}$.

Zu zeigen bleibt: $S \subset [H]$. Dazu definiere:

$$S_0 := H$$

$$S_{m+1} := S_m \cup \{x : x = \omega(x_1, ..., x_{n(\omega)}) \text{ für ein } \omega \in \Omega \text{ und für } x_1, ..., x_{n(\omega)} \in S_m\}.$$

Behauptung: $S_m \subset [H]$ für alle $m \in \mathbb{N}_0$

Beweis: Durch Induktion über m. Für $m = 0$ ist $S_0 = H \subset [H]$. Induktionsannahme: $S_m \subset [H]$. Sei $x \in S_{m+1}$. Dann ist $x \in S_m \subset H$ oder $x = \omega(x_1, ..., x_{n(\omega)})$ mit $x_1, ..., x_{n(\omega)} \in S_m \subset [H]$. Also ist $x \in [H]$, weil $\underline{[H]}$ eine Teilalgebra von $\underline{A}$ ist. Es folgt $S_{m+1} \subset [H]$.

Somit ist gezeigt: $\cup_{m=0}^{\infty} S_m \subset [H] \subset S$. Aus (3) folgt $S \subset \cup_{m=0}^{\infty} S_m$. Also ist

$S = \cup_{m=0}^{\infty} S_m$.

Weil $S_m \subset [H]$ für alle $m = 0, 1, ...,$ folgt $S \subset [H]$. Insgesamt also $\underline{S} = [\underline{H}]$.

Definition Eine *Kongruenzrelation* E auf einem algebraischen System $\underline{A} = (A, \Omega)$ ist eine Aequivalenzrelation E auf A, die die folgende Substitutions- oder Verträglichkeitseigenschaft erfüllt. Für alle $\omega \in \Omega$ gilt:

Wenn $a_i E b_i$ für $i = 1, ..., n(\omega)$, dann ist $\omega(a_1, ..., a_{n(\omega)}) E \omega(b_1, ..., b_{n(\omega)})$.

Benutzt man die zu E gehörige Partition von A, so läßt sich die in der Definition geforderte Bedingung auch so formulieren: Für alle $\omega \in \Omega$ gilt: Wenn $[a_i] = [b_i]$ für $i = 1, ..., n(\omega)$, dann ist $\left[\omega(a_1, ..., a_{n(\omega)})\right] = \left[\omega(b_1, ..., b_{n(\omega)})\right]$.

Beispiel Sei $\underline{A} = (\mathbb{Z}, +, -, \cdot, 0, 1)$ das durch den Ring der ganzen Zahlen definierte algebraische System. Sei $m \geqq 2$ eine natürliche Zahl. Nennt man zwei ganze Zahlen $a, b \in \mathbb{Z}$ aequivalent, wenn $a - b$ durch m teilbar ist, dann ist dadurch eine Kongruenzrelation auf $\underline{A}$ definiert.

(15.3) **Satz und Definition** (Existenz von Quotientenalgebren) *Sei* $\underline{A} = (A, \Omega)$ *ein algebraisches System und sei* E *eine Kongruenzrelation auf* A. *Dann gilt:*

(a) *Die Quotientenmenge* $A \setminus E$ *ist eine* $\overline{\Omega}$*-Algebra, die sogenannte Quotientenalgebra von* $\underline{A}$ *modulo* E, *wobei*

$\overline{\Omega} = \{\overline{\omega} : \omega \in \Omega\}$

$\overline{\omega}([a_1], ..., [a_n]) := [\omega(a_1, ..., a_n)]$, $n = n(\omega)$, $(a_1, ..., a_n) \in A^n$.

(b) *Die Abbildung* $\pi : A \to A \setminus E$, $a \to [a]$, *induziert einen Epimorphismus*

$\underline{A} \to \underline{A \setminus E}$.

Beweis: (a) $\overline{\omega}$ ist wohldefiniert: Seien dazu $(a_1, ..., a_n), (b_1, ..., b_n) \in A^n$ und sei $[a_i] = [b_i]$ für $i = 1, 2, ..., n$. Dann folgt aus der Voraussetzung, daß E eine Kongruenzrelation ist, für alle $\omega \in \Omega$ mit $n = n(\omega)$ die Identität

$[\omega(a_1, ..., a_n)] = [\omega(b_1, ..., b_n)]$.

Daraus folgt aufgrund der Definitioin von $\overline{\omega}$

$\overline{\omega}([a_1], ..., [a_n]) = \overline{\omega}([b_1], ..., [b_n])$.

(b) π ist nach Definition surjektiv. π ist auch ein Morphismus: Denn für alle $\omega \in \Omega$ mit $n = n(\omega)$ gilt

$\pi(\omega(a_1,..,a_n)) = [\omega(a_1,...,a_n)] = \overline{\omega}([a_1],...,[a_n]) = \overline{\omega}(\pi(a_1),...,\pi(a_n))$.

Definition Sei $f : (A,\Omega) \to (A',\Omega')$ ein Morphismus von ähnlichen algebraischen Systemen. Die *Kernrelation* von f ist

$Kern^{\sim}(f) := \{(a,b) \in A^2 : f(a) = f(b)\}$.

(15.4) **Satz** *$Kern^{\sim}(f)$ ist eine Kongruenzrelation auf $\underline{A} = (A,\Omega)$.*

Beweis: Daß $Kern^{\sim}(f)$ eine Aequivalenzrelation auf A ist, folgt unmittelbar aus der Definition. Sei $\omega \in \Omega$ und seien $(a_i,b_i) \in Kern^{\sim}(f)$ für $i = 1,2,...,n := n(\omega)$. Dann gilt mit $\omega' = \alpha(\omega)$:

$f(\omega(a_1,...,a_n)) = \omega'(f(a_1),...,f(a_n)) =$

$= \omega'(f(b_1),...,f(b_n)) = f(\omega(b_1,...,b_n))$.

Sei $\underline{A}/Kern^{\sim}(f)$ die zur Kernrelation von f gehörige Quotientenalgebra.

(15.5) **Satz** (Erster Isomorphiesatz) *Sei $f : (A,\Omega) \to (A',\Omega')$ ein Epimorphismus von ähnlichen algebraischen Systemen. Dann ist die Abbildung*

$g : \underline{A}/Kern^{\sim}(f) \to (A',\Omega')$, $g([a]) := f(a)$,

ein Isomorphismus.

Beweis: g ist nach Konstruktion und wegen der Surjektivität von f surjektiv. g ist auch injektiv; denn wenn $g([a]) = g([b])$, dann ist $f(a) = f(b)$, also $(a,b) \in Kern^{\sim}(f)$, d.h. $[a] = [b]$.

g ist auch ein Morphismus: Sei dazu $\omega \in \Omega$ mit $n = n(\omega)$ und seien $a_1,...,a_n \in A$. Dann gilt

$g(\overline{\omega}([a_1],...,[a_n]))$
$= g([\omega(a_1,...,a_n)])$ (weil $Kern^{\sim}(f)$ eine Kongruenzrelation ist)
$= f(\omega(a_1,...,a_n))$ (nach Definition von g)
$= \omega'(f(a_1),...,f(a_n))$ (weil f ein Morphismus ist)
$= \overline{\omega}((g([a_1]),...,g([a_n]))$ (nach Definition von g).

Beispiel Sei $\underline{A} = (\mathbb{Z},+,-,\cdot,0,1)$ der Ring der ganzen Zahlen, betrachtet als algebraisches System; und für eine natürliche Zahl $m \geqq 2$ sei $(\mathbb{Z}/m\mathbb{Z},+,-,\cdot,0,1)$ der entsprechende Restklassenring, ebenfalls betrachtet als algebraisches System. Sei $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, a \to a + m\mathbb{Z}$, die entsprechende Restklassenabbildung. Dann ist f ein Morphismus von algebraischen Systemen, und es gilt

$Kern^{\sim}(f) = \{(a,b) \in \mathbb{Z}^2 : m \text{ teilt } a - b\}$

$$= \{(a,b) \in \mathbb{Z}^2 : a - b \in Kern(f)\},$$

wobei

$Kern(f) = \{c \in \mathbb{Z} : f(c) = 0 \in \mathbb{Z}/m\mathbb{Z}\}$

der Kern des Ringhomomorphismus f ist.

Wir untersuchen nun einige spezielle Klassen von algebraischen Systemen und versuchen, diese zu klassifizieren; vgl. dazu $[BB]$.

Definition Eine *unitäre Algebra* ist ein algebraisches System der Form (S, f), wobei S eine nichtleere Menge ist und wobei $f : S \to S$ eine Abbildung ist.

Beispiele (1) $(\mathbb{N}_0, \tau), \tau(n) := n + 1$, heißt die *Peano-Algebra*
(2) $S := \underline{m} := \{1, 2, ..., m\}$, wobei $m \in \mathbb{N}$.

$$\sigma_m(k) := \begin{cases} k+1, & \text{falls } k \neq m \\ 1, & \text{falls } k = m \end{cases} .$$

(S, σ_m) heißt die *Uhr-Algebra.*

Sei (S, f) eine unitäre Algebra. Eine Teilmenge $T \subset S$ heißt f-abgeschlossen, falls gilt: Für alle $t \in T$ ist $f(t) \in T$, d.h. (T, f) ist eine Teilalgebra von (S, f). Die leere Menge $\emptyset$ und S selbst sind f-abgeschlossen.
In $(\underline{m}, \sigma_m)$ sind die einzigen σ_m-abgeschlossenen Teilmengen die leere Menge und die Menge $\underline{m}$ selbst. In $(\mathbb{N}_0, \tau)$ ist jede Menge der Form $\{k : k \geqq n\}$, wobei $n \in \mathbb{N}_0$ fest gewählt ist, τ-abgeschlossen.

Es sollen alle zyklischen unitären Algebren klassifiziert werden. Sei dazu (S, f) zunächst irgendeine unitäre Algebra und sei $a \in S$ ein festes Element. Definiere die Abbildung

$\theta : \mathbb{N}_0 \to S, \theta(n) := f^n(a) \quad (f^0(a) = a).$

θ ist ein Morphismus von unitären Algebren

$\theta : (\mathbb{N}_0, \tau) \to (S, f);$

denn

.
$\theta(\tau(n)) = \theta(n+1) = f^{n+1}(a) = f(f^n(a)) = f(\theta(n))$

für alle $n \in \mathbb{N}_0$. Somit gilt

(15.6) **Satz** *Sei (S, f) eine unitäre Algebra und sei $a \in S$. Dann existiert ein Morphismus*

$$\theta : (\mathbb{N}_0, \tau) \to (S, f)$$

mit $\theta(0) = a$. Ist (S, f) zyklisch und ist $a \in S$ ein erzeugendes Element, dann existiert ein Epimorphismus von algebraischen Systemen $(\mathbb{N}_0, \tau) \to (S, f)$ mit $0 \to a, 1 \to f(a)$. Also gilt

$$S = \{f^n(a) : n \in \mathbb{N}_0\}.$$

1-ter Fall: Alle $f^n(a)$ sind verschieden. Dann ist die Abbildung

$$(\mathbb{N}_0, \tau) \to (S, f), n \to f^n(a)$$

ein Isomorphismus.
2-ter Fall: Es gibt ein kleinstes p, so daß ein $k < p$ existiert mit $f^p(a) = f^k(a)$. Schreibe dann $p = k + m$. Durch Induktion über j folgt dann

$$f^{p+j}(a) = f^j(f^p(a)) = f^j(f^k(a)) = f^{k+j}(a)$$

für alle $j \in \mathbb{N}_0$. Also ist (S, f) isomorph zu $(U_m^k, \tau_{m,k})$, wobei

$$U_m^k = \{0, 1, ..., m + k - 1\}$$

$$\tau_{m,k}(j) := \begin{cases} j+1, & \text{falls } j \neq m+k-1 \\ 1, & \text{falls } j = m+k-1 \end{cases}$$

Es folgt

(15.7) **Satz** *Jede zyklische unitäre Algebra ist entweder isomorph zu $(\mathbb{N}_0, \tau)$ oder zu einer unitären Algebra der Form $(U_m^k, \tau_{m,k})$.*

Definition Eine *binäre Algebra* ist ein Paar (S, β), wobei S eine Menge ist und wobei $\beta : S \times S \to S$ eine Abildung ist. Eine binäre Algebra (S, β) heißt assoziativ, falls

$$\beta(x, \beta(y, z)) = \beta(\beta(x, y), z) \text{ für alle } x, y, z \in S;$$

sie heißt komutativ, falls

$$\beta(x, y) = \beta(y, x) \text{ für alle } x, y \in S.$$

Eine binäre assoziative Algebra (S, β) heißt auch Halbgruppe; eine Halbgruppe (S, β) heißt Monoid, falls ein Element $e \in S$ existiert, so daß gilt

$\beta(x, e) = x = \beta(e, x)$ für alle $x \in S$;

e heißt neutrales Element von (S, β).
Wenn β fest liegt, dann schreibt man auch

$\beta(x, y) = xy$.

Zu diesen Begriffsbildungen vgl. auch §4.
Beweise für die nachfolgenden Hilfssätze sind schnell erbracht.

(15.8) **Hilfssatz** *Sei (S, β) eine binäre Algebra, die ein linksneutrales Element e_ℓ besitzt, d.h. es gilt*

$\beta(e_\ell, x) = x$ *für alle* $x \in S$,

und auch ein rechtsneutrales Element e_r , d.h. es gilt

$\beta(x, e_r) = x$ *für alle* $x \in S$.

Dann sind e_ℓ und e_r jeweils eindeutig bestimmt und gleich einem (zweiseitigen) neutralen Element $e \in S$.

(15.9) **Hilfssatz** *Sei (S, β) eine binäre Algebra, die eine Linksnull 0_ℓ ($\beta(0_\ell, x) = 0_\ell$ für alle $x \in S$) und eine Rechtsnull 0_r ($\beta(x, 0_r) = 0_r$ für alle $x \in S$) besitzt. Dann sind beide eindeutig bestimmt und gleich einer zweiseitigen $0 \in S$.*

Beispiele Sei $(A, \wedge, \vee, ', 0, 1)$ eine Boolesche Algebra. Dann gilt: 0 ist das Nullelement für die binäre Algebra $(A, \wedge)$. 1 ist das neutrale Element für die binäre Algebra $(A, \wedge)$. 1 ist das Nullelement für die binäre Algebra $(A, \vee)$. 0 ist das neutrale Element für die binäre Algebra $(A, \vee)$.

Wir wollen zyklische Monoide klassifizieren.
Sei $\underline{M} = (M, \beta)$ ein Monoid; wir schreiben $\beta(a, b) = ab$ und $e = 1$. Für jedes $a \in M$ definieren wir die Potenzen a^n, $n \in \mathbb{N}_0$, rekursiv wie folgt

$a^0 := 1, a^1 := a, ..., a^{n+1} := a^n a$.

$\underline{M}$ ist zyklisch, falls ein $c \in M$ existiert, so daß jedes Element aus M von der Form c^n für ein $n \in \mathbb{N}_0$ ist. c heißt ein erzeugendes Element von M.

Beispiel $(\mathbb{N}_0, +, 0)$ ist ein zyklisches Monoid

(15.10) **Satz** *Sei ein M Monoid. Dann gilt $a^m a^n = a^{m+n}$ für alle $m, n \in \mathbb{N}_0$.*

Beweis: Sei $m \in \mathbb{N}_0$ fest. Für $n \in \mathbb{N}_0$ sei $P_m(n)$ die Aussage

Für alle $a \in M$ gilt $a^m a^n = a^{m+n}$

$P_m(0)$ ist wahr, weil $a^m a^0 = a^m 1 = a^m$ für alle $a \in M$. Sei $P_m(n)$ wahr. Dann gilt $a^m a^{n+1} = a^m(a^n a) = (a^m a^n)a = a^{m+n}a = a^{m+n+1}$ für alle $a \in M$.

(15.11) **Folgerung** Jedes zyklische Monoid ist kommutativ.

Sei C ein zyklisches Monoid mit dem erzeugenden Element c. Sei f_c die Abbildung

$f_c : C \to C, \ c^r \to c^{r+1}$.

Wenn alle c^r verschieden sind, dann gilt

$C \cong (\mathbb{N}_0, +, 0)$.

Wenn nicht, dann existiert ein kleinstes $s \in \mathbb{N}$, so daß

$c^s = c^m$ für ein $m < s$.

Also ist

$C = \{1, c, ..., c^{s-1}\}$,

insbesondere gilt $s = |C|$.
Durch Induktion über j folgt

$c^i c^j = c^{\varphi(i,j)}$ mit $\varphi(i,j) = i + j - kn$,

wobei $n = s - m$ und $k \in \mathbb{N}_0$ die kleinste ganze Zahl ist, so daß $k > (i + j - s)/n$. Insbesondere gilt: Wenn $i + j < s$, dann ist $k = 0$.
Es folgt

(15.12) **Satz** *Jedes unendliche zyklische Monoid C ist isomorph zu $(\mathbb{N}_0, +, 0)$. Jedes endliche zyklische Monoid mit s Elementen ist isomorph zu einem Monoid der Form $C_{m,n}$, wobei $m \in \mathbb{N}_0$ so ist, daß $m < s$, $n = s - m$ und*

$C_{m,n} = (\{1, c, ..., c^{s-1}\}, \cdot)$

$c^i c^j = c^{\varphi(i,j)}$, $\varphi(i,j) = i + j - kn$,

$k \in \mathbb{N}_0$ *die kleinste Zahl mit* $k > (i + j - s)/n$.

Also

$C_{m,n} = (\{0, 1, ..., s - 1\}, +)$,

wobei

$i + j = \varphi(i, j) + kn$.

Wie bereits weiter oben bemerkt, bilden die ähnlichen algebraischen Systeme eine Kategorie. Wir wollen nun ein universelles Objekt für eine mit dieser Kategorie zusammenhängende Kategorie von Abbildungen konstruieren.

Definition Gegeben seien
eine nichtleere Menge X (die Elemente aus X heißen Veränderliche oder Variable)
eine Menge $\mathfrak{F} \neq \emptyset$ mit $\mathfrak{F} \cap X = \emptyset$
eine Abbildung $t : \mathfrak{F} \to \mathbb{N}_0, \mathfrak{F}_n := t^{-1}(n)$ (die Elemente aus $\mathfrak{F}$ bzw. $\mathfrak{F}_n$ heißen Typen bzw. Typen der Dimension n)

Die *Menge der Terme vom Typ* $\mathfrak{F}$ *über* X, bezeichnet mit $T(X) = T(X, \mathfrak{F})$, ist der Durchschnitt aller Mengen Y mit den folgenden Eigenschaften

(1) $X \cup \mathfrak{F}_0 \subset Y$

(2) Sind $p_1, ..., p_n \in Y$ und ist $f \in \mathfrak{F}_n$, dann gehört die Zeichenfolge

$f(p_1, ..., p_n)$

zu Y.

Beispiele (1) $X = \{x, y, z\}; \mathfrak{F} = \mathfrak{F}_2 = \{\cdot\}; t : \mathfrak{F} \to \mathbb{N}_0, t(\cdot) = 2$. Dann gilt z.B.

x, y, z, $x \cdot y$, $y \cdot z$, $x \cdot (y \cdot z)$, $(x \cdot y) \cdot z \in T(X)$.

(2) $X = \{x, y, z\}$, $\mathfrak{F} = \mathfrak{F}_2 = \{+, \cdot\}$; $t : \mathfrak{F} \to \mathbb{N}_0$, $t(+) = 2 = t(\cdot)$. Dann gilt z.B.

x, y, z, $x \cdot (y + z)$, $(x \cdot y) + (x \cdot z) \in T(X)$.

Definition Sei $\mathfrak{F} \neq \emptyset$, sei $t : \mathfrak{F} \to \mathbb{N}_0$ eine Abbildung, $\mathfrak{F}_n := t^{-1}(n)$. Ein *algebraisches System vom Typ* $\mathfrak{F}$ ist ein Paar (A, Ω), wobei A eine nichtleere

Menge ist und wobei $\Omega \neq \emptyset$ eine Menge ist, so daß eine surjektive Abbildung $\tau : \mathfrak{F} \to \Omega$ mit der folgenden Eigenschaft existiert: Für alle $f \in \mathfrak{F}_n$ ist

$\tau(f) : A^n \to A$

eine n-stellige Operation.

Definition Sei p ein Term vom Typ $\mathfrak{F}$ über X und sei (A, Ω) ein algebraisches System vom Typ $\mathfrak{F}$. Für alle $n \in \mathbb{N}_0$ definiere $p^A \in \Omega$ mit $\dim(p^A) = n$ wie folgt:

(1) Ist p eine Variable - Schreibweise:

$p(x_1, ..., x_n) = p_i(x_1, ..., x_n)$ -,

dann sei

$p^A(a_1, ..., a_n) := p_i^A(a_1, ..., a_n) := a_i$.

(2) Ist p von der Form

$f(p_1(x_1, ..., x_n), ..., p_k(x_1, ..., x_n))$ mit $f \in \mathfrak{F}_k$,

dann sei

$p^A(a_1, ..., a_n) := \tau(f)(p_1^A(a_1, ..., a_n), ..., p_k^A(a_1, ..., a_n))$.

(15.13) **Satz** *Seien* $\underline{A} = (A, \Omega)$, $\underline{B} = (B, \Omega)$ *ähnliche algebraische Systeme vom Typ* $\mathfrak{F}$. *Dann gilt:*
(a) *Sei* p *ein Term vom Typ* $\mathfrak{F}$ *und sei* $n = \dim(p^A) = \dim(p^B)$. *Sei* θ *eine Kongruenzrelation auf* $\underline{A}$ *und seien* $(a_i, b_i) \in \theta$ *für* $i = 1, ..., n$. *Dann ist*

$(p^A(a_1, ..., a_n), p^B(b_1, ..., b_n)) \in \theta$.

(b) *Sei* p *ein Term vom Typ* $\mathfrak{F}$ *mit* $n = \dim(p^A) = \dim(p^B)$. *Sei* $\gamma : \underline{A} \to \underline{B}$ *ein Morphismus. Dann gilt*

$\gamma(p^A(a_1, ..., a_n)) = p^B(\gamma(a_1), ..., \gamma(a_n))$

für alle $a_1, ..., a_n \in A$.

(c) *Sei* $S \subset A$ *eine Teilmenge. Dann gilt: Die von* S *erzeugte Teilalgebra* $[\underline{S}]$ *ist von der folgenden Form:*

$[S] = \{p^A(a_1, ..., a_n) : p$ ist ein Term vom Typ $\mathfrak{F}$; $n \in \mathbb{N}_0; a_1, ..., a_n \in S\}$.

Beweis: Klar.

Definition Seien X und $\mathfrak{F}$ nichtleere Mengen mit $\mathfrak{F} \cap X = \emptyset$. Sei $T(X)$ die Menge aller Terme vom Typ $\mathfrak{F}$ über X. Die *Termalgebra vom Typ $\mathfrak{F}$ über X* ist das folgende algebraische System vom Typ $\mathfrak{F}$

$$\underline{T(X)} = (T(X), \Omega)$$

mit $\Omega = \{\tau(f) : f \in \mathfrak{F}\}$; dabei bedeutet $\tau(f)$, daß f als Operation auf $T(X)$ zu betrachten ist.

Offensichtlich gilt: $\underline{T(X)} = \underline{[X]}$.

Definition Sei $\mathfrak{K}$ eine Klasse von algebraischen Systemen vom Typ $\mathfrak{F}$ und sei $\underline{U(X)}$ ein algebraisches System vom Typ $\mathfrak{F}$, das durch X erzeugt wird. $\underline{U(X)}$

besitzt die *universelle Abbildungseigenschaft* für $\mathfrak{K}$ über X, falls für alle $\underline{A} \in \mathfrak{K}$ und für alle Abbildungen $\alpha : X \to A$ ein Morphismus $\beta : \underline{U(X)} \to \underline{A}$ existiert, der α fortsetzt. X heißt in diesem Fall eine *Menge von freien Erzeugenden von* $\underline{U(X)}$.

(15.14) **Hilfssatz** *$\underline{U(X)}$ habe die universelle Abbildungseigenschaft für die Klasse $\mathfrak{K}$ von algebraischen Systemen vom Typ $\mathfrak{F}$ über X. Dann gilt: Für alle $\underline{A} \in \mathfrak{K}$ und für alle Abbildungen $\alpha : X \to A$ existiert genau ein Morphismus $\beta : \underline{U(X)} \to \underline{A}$, der α fortsetzt.*

Beweis: $\underline{U}(X) = \underline{[X]}$, und β ist auf X eindeutig bestimmt.

(15.15) **Satz** *Seien $\underline{U_1(X_1)}$, $\underline{U_2(X_2)}$ algebraische Systeme mit der universellen Abbildungseigenschaft für eine Klasse $\mathfrak{K}$ von algebraischen Systemen vom Typ $\mathfrak{F}$ über X_1 bzw. X_2. Wenn dann $|X_1| = |X_2|$ gilt, dann existiert ein Isomorphismus*

$$\underline{U_1(X_1)} \cong \underline{U_2(X_2)}$$

Beweis: Jede Bijektion $f : X_1 \to X_2$ besitzt eine eindeutige Fortsetzung zu einem Isomorphismus $\underline{U_1(X_1)} \cong \underline{U_2(X_2)}$.

(15.16) **Satz** *Seien X und $\mathfrak{F}$ nichtleere Mengen mit $\mathfrak{F} \cap X = \emptyset$. Die Termalgebra $\underline{T(X)}$ vom Typ $\mathfrak{F}$ über X besitzt die universelle Abbildungseigenschaft für die Klasse aller algebraischen Systeme vom Typ $\mathfrak{F}$ über X.*

Beweis: Sei $\underline{A}$ ein algebraisches System vom Typ $\mathfrak{F}$ und sei $\alpha : X \to A$ eine Abbildung. Definiere

$$\beta : \underline{T(X)} \to \underline{A}$$

rekursiv durch

$\beta(x) := \alpha(x)$ für alle $x \in X$,

$\beta(f(p_1, ..., p_n)) := \tau(f)(f(p_1), ..., f(p_n))$

für alle $p_1, ..., p_n \in T(X)$ und alle $f \in \mathfrak{F}_n$. Dann gilt

$\beta(p(X_1, ..., X_n)) = p^A(\alpha(X_1), ..., \alpha(X_n)),$

und β ist ein Morphismus, der α fortsetzt.

Beispiel Die Peano-Algebra $(\mathbb{N}_0, \tau)$ hat die universelle Abbildungseigenschaft für die Klasse aller unitären Algebren über $X = \{x\}$, d.h. für die Klasse aller algebraischen Systeme vom Typ $\mathfrak{F} = \mathfrak{F}_1 = \{f\}$ über $X = \{x\}$.

Beweis: Sei $\underline{A} = (A, \gamma)$ eine unitäre Algebra. Sei :$\alpha : X \to A$ eine Abbildung. Sei

$\beta : \mathbb{N}_0 \to A, \beta(0) := \alpha(x), \beta(1) := \gamma^1(\alpha(x), ..., \beta(n) := \gamma^n(\alpha(x)).$

Dann ist $\beta : (\mathbb{N}_0, \gamma) \to (A, \gamma)$ ein Morphismus von algebraischen Systemen, der α fortsetzt:

$\beta(\tau(n)) = \beta(n + 1) = \gamma^{n+1}(\alpha(x)) = \gamma(\gamma^n(\alpha(x)) = \gamma(\beta(n)).$

Definition (Direkte Produkte von ähnlichen algebraischen Systemen) Sei $(\underline{A_i})_{i \in I}$ eine Familie von ähnlichen algebraischen Systemen vom Typ $\mathfrak{F}$. Das *direkte Produkt* dieser Familie ist das folgende algebraische System vom Typ $\mathfrak{F}$:

$\underline{A} := \prod_{i \in I} \underline{A_i} := (\prod_{i \in I} A_i, \Omega'),$

wobei für $f \in \mathfrak{F}_n$; $a_1, ..., a_n \in \prod_{i \in I} A_i$ gilt: Die i-te Koordinate $f^{\underline{A}}(a_1, ..., a_n)_i$ ist gleich $f^{\underline{A_i}}(a_{1,i}, ..., a_{n,i})$.

Definition Seien X und $\mathfrak{F}$ nichtleere Mengen mit $X \cap \mathfrak{F} = \emptyset$. Sei $\underline{T(X)}$ die Termalgebra vom Typ $\mathfrak{F}$ über X. Eine *Identität vom Typ $\mathfrak{F}$ über X* ist ein Ausdruck der Form

$p \approx q$, wobei $p, q \in \underline{T(X)}$.

Sei $Id(X)$ die Menge aller Identitäten vom Typ $\mathfrak{F}$ über X. Ein algebraisches System $\underline{A}$ vom Typ $\mathfrak{F}$ *erfüllt eine Identität* $p \approx q$ mit $p, q \in T(X)$, falls gilt:

$p^A(a_1, ..., a_n) = q^A(a_1, ..., a_n)$ für alle alle $a_1, ..., a_n \in A$;

in dieser Situation schreibt man auch

$\underline{A} : p \approx q$.

Eine Klasse $\mathfrak{K}$ von algebraischen Systemen vom Typ $\mathfrak{F}$ *genügt einer Identität* $p \approx q$ mit $p, q \in T(X)$, falls gilt

$\underline{A} : p \approx q$ für alle $\underline{A} \in \mathfrak{K}$;

in dieser Situation schreibt man auch

$\mathfrak{K} : p \approx q$.

Ist Σ eine Menge von Identitäten vom Typ $\mathfrak{F}$ über X, dann *erfüllt* $\mathfrak{K}$ *die Menge* Σ, falls gilt

$\mathfrak{K} : p \approx q$ für alle Identitäten $p \approx q$ aus Σ.

Sei Σ eine Menge von Identitäten vom Typ $\mathfrak{F}$ über X und sei $\mathcal{M}(\Sigma)$ die Klasse aller algebraischen Systrem $\underline{A}$, die Σ erfüllen. Eine Klasse $\mathfrak{K}$ von algebraischen Systemen vom Typ $\mathfrak{F}$ heißt eine *gleichungsdefinierte Klasse vom Typ* $\mathfrak{F}$, falls eine Menge von Identitäten Σ vom Typ $\mathfrak{F}$ existiert, so daß $\mathfrak{K} = \mathcal{M}(\Sigma)$ gilt. In dieser Situation heißt $\mathfrak{K}$ *gleichungsdefiniert oder axiomatisiert durch* Σ.

(15.17) **Satz** (G.Birkhoff) $\mathfrak{K}$ *ist eine gleichungsdefinierte Klasse vom Typ* $\mathfrak{F}$ *genau dann, wenn* $\mathfrak{K}$ *eine Varietät vom Typ* $\mathfrak{F}$ *ist, d.h.* $\mathfrak{K}$ *ist abgeschlossen unter der Bildung von Teilalgebren, Bildern von Morphismen und direkten Produkten.*

Für den Beweis dieses Satzes vgl. $[BS]$ oder $[AD]$, Chapter 5, 5D.

Aufgaben und Beispiele

(1) Sei $\underline{G} = (G, \cdot, e)$ eine Gruppe, betrachtet als algebraisches System ($\cdot$ = Verknüpfung in G, e = neutrales Element in G). Zeigen Sie:
(a) Die Menge aller Untergruppen von $\underline{G}$ bildet bezüglich der Inklusion einen Verband.
(b) Die Abbildung, die jeder Kongruenzrelation auf $\underline{G}$ die zugehörige Aequivalenzklasse des neutralen Elementes e zuordnet, ist eine Bijektion zwischen der Menge aller Kongruenzrelationen auf $\underline{G}$ und der Menge aller normalen Untzergruppen von $\underline{G}$.

(2) Sei (S, f) eine unitäre Algebra. Die Menge S sei endlich. Sei R die Relation

$R := \{(a, b) \in S \times S : \text{Es gibt ein } n \in \mathbb{N} \text{ mit } f^n(a) = b\}$.

Zeigen Sie, daß R reflexiv und transitiv ist. Zeigen Sie außerdem, daß (S, f) genau dann zyklisch ist, wenn ein $a \in S$ existiert, so daß $(a, b) \in R$ für alle $b \in S$ gilt.

(3) Sei $\underline{\mathbb{N}}_0 = (\mathbb{N}_0, \tau), \tau(n) := n + 1$, die sogenannte Peano-Algebra. Zeigen Sie, daß $\mathbb{N}_0$ die universelle Abbildungseigenschaft für die Klasse aller unitären Algebren über $\{0\}$ hat.

(4) Bestimmen Sie eine Menge von Variablen und einen Typ $\mathfrak{F}$, so daß die nachfolgende Zeichenfolge eine Identität vom Typ $\mathfrak{F}$ über X ist: $(x + y)^3 \approx (x^3 + y^3)$. Geben Sie außerdem ein nichtleeres algebraisches System vom Typ $\mathfrak{F}$ an, das diese Identität erfüllt.

Literatur zu § 15: $[AD]$, $[BB]$, $[BS]$, $[LS]$, $[MC]$

Literaturverzeichnis

$[AD]$ J. Adamek: Theory of mathematical structures, D. Reidel Publ. Comp., Dordrecht, 1983

$[AKS]$ M. Agrawal, N. Kayal, N. Saxena: Primes is in P, Annals of Math., 160, 2994, 781-793

$[AB]$ M.A. Arbib: Algebraic Theory of Machines, Languages and Semigroups, Academic Press, New York, 1968

$[A1]$ E. Artin: Theorie der Zöpfe, Abh. Mathem. Sem. d. Univ. Hamburg, 1925, 47-72

$[A2]$ E. Artin: Theory of braids, Annals of Math., 48, 1947, 101-126

$[AT]$ L. Auslander, R. Tolimieri: Is computing with the finite Fourier transform pure or applied mathematics, Bulletin AMS, 1, 1979, 847-897

$[AMD]$ M. Atiyah, I. MacDonald: Commutative Algebra, Addison Wesley, Reading, Mass., 1969

$[BA]$ A. Baker: A concise introduction to the theory of numbers, Cambridge University Press, 1984

$[BW]$ M. Barr, Ch. Wells: Category Theory for Computer Science, Prentice Hall, 1990

$[BB]$ G. Birkhoff, T.C. Bartee: Modern applied algebra, McGraw Hill, New York, 1969

$[BM]$ G. Birkhoff, S. MacLane: A survey of modern algebra, Macmillan, 1977

$[BBFR]$ G. Baumslag, Y. Brykhov, B. Fine, G. Rosenberger: Some cryptoprimitives in noncommutative algebraic cryptography, Aspects of infinite groups, pp. 26-44 in: Algebra discrete mathematics, 1, 2008

$[BL]$ G. Boole: An investigation of the laws of thought, Dover Publ., New York, 1951

$[BK]$ N. Bourbaki: Théories Spectrales, Chap. 1&2, Hermann, Paris, 1967

[BU] W. Burnside: The theory of groups of finite order, Cambridge, 1897

[BS] S. Burris, H.P. Sankappanavar: A course in universal algebra, Springer, GTM 78, New York, 1981

[CN] P.M. Cohn: Algebra and language theory, Bulletin London Math. Soc., 7, 1975, 1-29

[CT] J.W. Cooley, J.W. Tukey: An algorithm for the machine calculation of complex Fourier series, Mathematics of Computation, 19, 1965, 297-301

[DH] W. Diffie, M. Hellmann: New directions in cryptography, IEEE Trans. Inform. Theory, 22, 1976, 644-654

[DM] M. Demazure: Cours d'algebre, Cassini, Paris, 1997

[DMK] H. Dym, H.P. McKean: Fourier Series and Integrals, Academic Press, New York, 1972

[EB] S. Eilenberg: Automata, Languages and Machines I, II; Academic Press, New York, 1974

[$FM1$] R.P. Feynman: Quantum mechanical computers, Found. Physics, 16, 1986, 507-531

[$FM2$] R.P. Feynman: The Feynman lectures on computation; edited by A.J.G. Hey and R.W. Allen; Addison Wesley, Reading, Mass., 1996

[$FM3$] R.P. Feynman: Simulating physics with computers, Int. Journal of Theoretical Physics, 21, 1982, 467-488

[F] O. Forster: Algorithmische Zahlentheorie, Vieweg Verlag, Braunschweig, 1996

[FR] G. Frey: Duality theorems in arithmetic geometry and applications in data security, Institut für Experimentelle Mathematik, Universität Duisburg-Essen, 2007

[GA] D. Garber: Braid group cryptography, pp. 329-403; in: A. Jon Berrich, F.R. Cohen, E. Hamburg, Y.L. Wang, J. Wu: Braids, Int. Math. Sc., Singapore, 2010

[GT] L. Garding, T. Tambour: Algebra for Computer Science, Springer, New York, 1988

[G] C.F. Gauß: Disquisitiones Mathematicae, Leipzig 1801. Übersetzung von H. Maser, Berlin 1889; Nachdruck

[GB] A. Ginzburg: Algebraic theory of automata, Academic Press, New York, 1968

[GS] A.M. Gleason: Weight polynomials of self dual codes and the MacWilliams identities, Actes congrès international des mathémaciens, Nice, 1970, Tome 3, Gauthier-Villars, Paris, 1971, 211-215

[HM] P.R. Halmos: Naive Mengenlehre, Vandenhoeck & Ruprecht, Göttingen,1976

[H] M.A. Harrison: Introduction to Switching and Automata, McGrawHill, New York, 1965

[HJB] M.T. Heideman, D.H. Johnson, C.S. Burrus: Gauss and the History of the Fast Fourier Transform, Archive for the History of Exact Sciences, 34, 1985, 265-278

[HY] A.J.G. Hey (ed.): Feynman and computation, Exploring the limits of computers; Perseus books, Reading, Mass., 1999

[HS] F. Hirzebruch, N.-P. Skoruppa: Codierungstheorie und ihre Beziehung zu Geometrie und Zahlentheorie, MPI Preprint 88-6, Bonn, 1986

[HU] J.E. Hopcraft, J.D. Ullman: Introduction to Autmata Theory, Languages and Computation, Addison Wesley, Reading, Mass., 1979

[KA] D. Kahrobei, M. Anshel: Applications of group theory in cryptography, International Journal of pure and applied mathematics, 58, 2010, 21-23

[KL] S.C. Kleene: Representations of Events in Memory Nets and finite Automata, Princeton Univ. Studies, 1956, 3-40

[KN] D.E. Knuth: The Art of Computer Programming, Addison Wesley, Reading, Mass., 1969

[KS] A.I. Kostrikin, I.R. Šafarevič (eds.): Algebra I; I.R. Šafarevič: Basic notions of algebra, Springer Verlag, Berlin, 1990

[KSA] W. Kuich, A. Saloma: Semirings, Automata, Languages, Springer Verlag, Berlin, 1985

[KU] E. Kunz: Algebra, Vieweg Verlag, Braunschweig/Wiesbaden, 1991

[$L1$] S. Lang: Algebraic Structures, Addison Wesley, Reading, Mass., 1967

[$L2$] S. Lang: Algebra, Addison Wesley, Reading, Mass., 1972

[$L3$] S. Lang: Algebraic Number Theory, Second Edition, Springer Verlag, New York, 1994

[LM] F. Lemmermeyer: Kreise und Quadrate modulo p, Mathem. Semesterberichte, 47, 2000, 51-73

[LV] W.L. LeVeque: Topics in number theory I, II; Addison Wesley, Reading, Mass., 1956

[LP] R. Laubenbacher, D. Pengelley: Mathematical Expeditions, Chronicles by the Explorers, Springer Verlag, New York, 1999

[LS] J.D. Lipson: Elements of Algebra and Algebraic Computing, Addison Wesley, Reading, Mass., 1969

[LL] F. Lorenz, F. Lemmermeyer: Algebra 1, Körper und Galoistheorie, Spektrum Akademischer Verlag, Elsevier GmbH, München, 2007

[LPS] H.-K. Lo, S. Popescu, T. Spiller (eds.): Introduction to quantum computation and information, World Scientific, 1998

[MS] F.J. MacWilliams, N.J.A. Sloane: The theory of error correcting codes, North-Holland, Amsterdam, 1978

[MC] V.I. Malcev: Algebraic Systems, Springer Verlag, New York, 1973

[MF] N. Meyerhoff: Eigenwerttheorie der Fouriertransformation für endliche abelsche Gruppen, Diplomarbeit, TU Braunschweig, 2009

[MIH] J. Milnor, D. Husemoller: Symmetric bilinear forms, Berlin, Springer Verlag, 1973

[MN] Yu I. Manin: Classical computing, quantum computing and Shor's factoring algorithm; Sem. Bourbaki, 1998-1999, 862, Juni 1999, 375-404

[N] G. Nebe: Faktorisieren ganzer Zahlen, Jahresbericht der Deutschen Mathematiker Vereinigung, 102, 2000,1-14

[NC] M.A. Nielsen, I.L. Chuang: Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000

[PI] B.C. Pierce: Basis category theory for computer scientists, The MIT Press, Cambridge, Mass., 1991

[P] G. Polya: Kombinatorische Untersuchungen für Gruppen, Graphen und chemische Verbindungen, Acta Mathematica, 68, 1937, 145-264

[RL] H. Riesel: Prime Numbers and Computer methods for factorization, Birkhäuser Verlag, Basel, 1985

[RSA] R.L. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, Comm. ACM 21, 1978, 120-126

[R] J.J. Rotman: An introduction to the theory of groups, Springer, GTM 148, New York, 1995

[SB] A. Scholz, B. Schoeneberg: Einführung in die Zahlentheorie, Walter de Gruyter, Berlin, 1973

[ST] A. Schönhage, V. Strassen: Schnelle Multiplikation großer Zahlen, Computing 7, 1971, 281-283

[SC] H Schubert: Kategorien I, II; Springer Verlag, Berlin, 1970

[$SGA4$] Séminaire de Géometrie Algébrique du Bois Marie, dirigé par M. Artin, A. Grothendieck, J.L. Verdier; SGA 4, Springer Verlag, Berlin, LNM 270, 1972

[S] J.P. Serre: A course in Arithmetic, Springer Verlag, New York, 1973

[SW] C.E. Shannon, W. Weaver: The mathematical theory of communication, The University of Illinois Press, Urban; 1949

[SH] P.W. Shor: Quantum Computing, Documenta Nathematica, DMV, Extra Volume, ICM, I, 1998, 467-486

[ST] R. Solovay, V. Strassen: A fast Monte-Carlo test for primality, SIAM J. Comp., 6, 1977, 84-85

[TS] A. Terras: Fourier analysis on finite groups and applications, Cambridge University Press, Cambridge, 1999

[T] R. Tolimieri: The algebra of the finite Fourier transform and coding theory, Transactions of the AMS, 287, 1985, 253-273

[TU] A. Turing: On computable numbers with an application to the Entscheidungsproblem, Proc. London Math. Soc., Ser. 2, 42, 1936, 230-265; 43, 1937, 544-546

[VL] J.H. van Lint: Introduction to coding theory, Third Edition, Springer Verlag, Berlin, 1999

[W] B.L. van der Waerden: Algebra I, II; Springer Verlag, Berlin, 1971

[WG] S. Winograd: Arithmetic complexity of computations, CBMS-NSF Reg. Conf. Series in Applied Math., Philadelphia, 1980

Typeset with Scdientific Word 3.0 and LaTex

.