Mathematik für Informatiker I

Andreas Griewank

Institut für Angewandte Mathematik
Humboldt Universität zu Berlin
griewank@math.hu-berlin.de

Wiss. Mitarbeiter:
Dr. Andrej Ponomarenko (andrej@math.hu-berlin.de)
Heinz Jürgen Lange (lange@math.hu-berlin.de)
Hannelore Wagner (wagnerha@math.hu-berlin.de)
Jan Riehme (riehme@math.hu-berlin.de)

10. Februar 2005

Literaturhinweise I

Donald E. Knuth,
Fundamental Algorithms. The art of computer programming. Vol I,II,III. Second Edition. Addison Wesley.
Absoluter Klassiker sehr umfangreich und mathematisch. Bill Gates hat mal jedem einen Job versprochen, der 80 % der Übungen lösen kann.

Peter Hartmann,
Mathematik für Informatiker. 3. überarbeitete Auflage, 2004, Vieweg.
Bei Lehmann's vorhanden, ca. 30 €
Gute Grundlage, äusserst lesbar, nicht unbedingt an Eliteuniversitäten orientiert. ISBN: 3-528-23181-5

Vélu Jacques,
1^{er} CYCLE. Méthodes mathématiques pour l´informatique. Cours et exercices corrigés. 3^{er} edition. Dunod, Paris, 1999.

Teil I

Algebraische Grundstrukturen

Literaturhinweise II

Guerino Mazzola, Gérard Milmeister, Jody Weissmann,
Comprehensive Mathematics for Computer Scientists 1, 2004, Springer.
Ziemlich axiomatisch und knapp geschrieben. Zweiter Band in Vorbereitung. Definitiv für höhere Ansprüche. Begleitender Kurs im Internet verfügbar. ca 30 €, ISBN: 3-540-20835-6

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest,
Introduction to Algorithms. 2nd ed. 2001. The MIT Press.
ca 60 €, ISBN: 0-262-53196-8

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein,
Algorithmen – Eine Einführung. 2004, Oldenbourg.
ca 70 €, ISBN: 3-486-27515-1

Zitate

It is generally very difficult to keep up with a field that is economically profitable.

Donald E. Knuth

Since, I myself profess to be a mathematician, it is my duty to mantain mathematical integrity as much as I can.

Donald E. Knuth

Definition A.2 (Verknüpfungseigenschaften)

Für Verknüpfungen $\circ$ zwischen Elementen einer Menge $\mathcal{M}$ betrachtet man die Eigenschaften:

(i)	$(a \circ b) \circ c = a \circ (b \circ c)$	**Assoziativität**
(ii)	$e \circ b = b \circ e = b$	**Neutrales bzw. Einselement**
(iii)	$a \circ b = b \circ a$	**Kommutativität**
(iv)	$a \circ b = e$	**Inverse Elemente**

Definition A.3 (Halbgruppe, Monoid, Gruppe)

$\mathcal{M}$ heißt

Halbgruppe falls (i) gilt

Monoid falls zudem (ii) gilt

Kommutativ falls zudem (iii) gilt

Gruppe falls zudem für jedes $a \in \mathcal{M}$ ein Inverses $b \in \mathcal{M}$ existiert, so daß (iv) gilt

A - 1 Algebraische Grundlagen

Beispiel A.1

`unsigned char` in Programmiersprachen (`C`, `C++`, Java, etc.)

$a \in \mathcal{B} \equiv \{0, 1, 2, 3, \ldots, 254, 255\}$

wobei $255 = 2^8 - 1 = m - 1$ mit m $\equiv 256$

Frage:

Welche Eigenschaften haben Verknüpfungen + und $*$ für sich allein und wie ist ihre Wechselwirkung?
Wie klassifiziert man die Struktur von $\mathcal{B}$ griffig?

Beispiel A.4 (Nichtkommutativer Monoid)

Alle Worte bzw Zeichenketten A^* über einem gegebenen Alphabet A, z.B. $\{0, 1\}$ oder $\{a, b, \cdots, z\}$ wobei + Konkatenation und e das Leere Wort sind, d.h

$$axz + yi = axzyi.$$

Beispiel A.5 (Kommutativer Monoid)

$\mathbb{N}_+ = \{1, 2, 3, \ldots\}$ Menge der positiven natürlichen Zahlen bzgl. $*$ mit neutralem Element 1.

Beispiel A.6 (Kommutative Gruppe)

$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$ Menge aller ganzen Zahlen bezüglich + mit neutralem Element e = 0 und inversem Element -a.

Warnung:

$\mathbb{Z}$ ist bezüglich $*$ keine Gruppe da im allgemein keine Reziproke (d.h. Kehrwerte) existieren, und ein solches für 0 auch nicht definiert werden kann. Allerdings ist $\mathbb{Z}$ ein Ring.

Definition A.7 (Ring)

Eine Menge $\mathcal{M}$ heisst Ring falls

(i) $\mathcal{M}$ ist kommutative Gruppe bezüglich Verknüpfung + mit $a+0=a$ und $a+(-a)=0$

(ii) $\mathcal{M}$ ist Halbgruppe bezüglich Verknüpfung $*$

(iii) $a*(b+c)=a*b+a*c$ **Distributivität**

(iv) $a*b=b*a$ **Kommutativität**

Falls nur (iv) nicht gilt nennt man $\mathcal{M}$ einen nichtkommutativen Ring.

Falls $\mathcal{M}$ bezüglich $*$ sogar ein Monoid ist, also ein multiplikatives Einselement besitzt, so heißt $\mathcal{M}$ ein Ring mit 1.

Lemma A.10 (Cartesisches Produkt)

Für zwei Ringe $\mathcal{R}$ und $\mathcal{S}$ bildet die Menge aller geordneten Paare

$$\mathcal{R}\times\mathcal{S}=\{(r,s)\ :\ r\in\mathcal{R},\ s\in\mathcal{S}\}$$

wiederrum einen Ring mit dem additiven Inversen $(-r,-s)$ und dem neutralen Elementen $(0_{\mathcal{R}},0_{\mathcal{S}})$.
Hierbei bezeichnen $0_{\mathcal{R}}$ und $0_{\mathcal{S}}$ die Nullelemente von $\mathcal{R}$ und $\mathcal{S}$.

Haben beide Ringe ein Einselemente $1_{\mathcal{R}}$ bzw. $1_{\mathcal{S}}$, so ist $(1_{\mathcal{R}},1_{\mathcal{S}})$ das Einselement von $\mathcal{R}\times\mathcal{S}$.

Beispiel A.8 (Kommutativer Ring mit 1)

Neben $\mathbb{Z}$ selbst auch $\mathbb{Z}[x]$ d.h. die Menge aller Polynome mit Koeffizienten in $\mathbb{Z}$ (siehe Abschnitt A2.4).

Beispiel A.9 (Nichtkommutativer Ring mit 1)

$\mathbb{Z}^{2\times 2}$ d.h. die Menge allen 2×2 Matrizen mit ganzahligen Elementen.

$$0=\begin{bmatrix}0&0\\0&0\end{bmatrix},\qquad 1=\begin{bmatrix}1&0\\0&1\end{bmatrix}$$

Definition A.11 (Körper)

Ein Ring $\mathcal{M}$ mit 1 heisst Körper falls $\mathcal{M}\backslash\{0\}$ eine Gruppe bezüglich $*$ bildet d.h. für alle $0\neq a\in\mathcal{M}$ ein Inverses Element $a^{-1}=1/a$ existiert.
Falls $\mathcal{M}$ als Ring nicht kommutativ ist, heisst er *Schiefkörper*.

Beispiel A.12 (Kommutativer Körper)

$$\mathbb{Q}=\{\frac{p}{q}:q\neq 0,(p,q)\in\mathbb{Z}^2\ \textit{teilerfrei}\}$$

Bemerkung:

Schiefkörper, d.h. nicht kommutative Körper, spielen im Allgemeinen keine grosse Rolle.

Wahre Menschen, die Sinn und Wahrheit suchen, studieren Mathematik, Informatik, Psychologie usw. Wenn wir bei IBM eine solche eher seltene Mischung von Mitarbeitern haben, müssen wir auch dementsprechend artgerechtes Management betreiben.

Gunter Dueck, IBM Global Services (N.D. 21.10.2004)

Beispiel A.15
$\mathbb{N}$ ist Teilmonoid von $\mathbb{Z}$.

Beispiel A.16
$\mathbb{Z}$ ist Unterring von $\mathbb{Q}$.

Beispiel A.17
$2\mathbb{Z} \equiv \{a \in \mathbb{Z} : a \textit{ ist gerade}\}$ ist Untergruppe von $\mathbb{Z}$.

Beispiel A.18
$3\mathbb{Z} \equiv \{a \in \mathbb{Z} : a \textit{ ist durch } 3 \textit{ teilbar}\}$ ist Untergruppe von $\mathbb{Z}$.

Beispiel A.19
$2\mathbb{Z} \cap 3\mathbb{Z} \equiv \{a \in \mathbb{Z} : a \textit{ ist durch } 6 \textit{ teilbar}\}$ ist Untergruppe von $\mathbb{Z}$.

A - 2 Algebraische Teilstrukturen

Definition A.13
Häufig hat eine Teilmenge $\mathcal{U} \subseteq \mathcal{M}$ einer Halbgruppe, eines Monoids, einer Gruppe, eines Ringes oder eines Körpers diesselben strukturellen Eigenschaften bezüglich der vorgegebenen Verknüpfungen. Sie heißt dann entsprechend Unter- oder Teil- Halbgruppe, Monoid, Gruppe, Ring oder Körper.

Lemma A.14 (*Schnittprinzip*)
Der Durchschnitt zweier Unterhalbgruppen, Untergruppen, Unterringe oder Unterkörper ist wiederum eine Unterhalbgruppe, Untergruppe, Unterring, Unterkörper usw.

Beispiel A.20
Geometrische Rotationen in der Ebene bilden eine kommutative Gruppe, die man mit $\mathcal{S}_1$ bezeichet. Links- oder Rechtsdrehungen um ein Vielfaches von 30 Grad bilden eine Untergruppe. Neutrales Element ist die Drehung um den Winkel Null.

Beispiel A.21
Drehungen eines physikalischen Körpers im dreidimensionalen Raum bilden eine nichtkommutative Gruppe. Davon bilden alle Drehungen um eine vorgegebene Achse wiederum eine Untergruppe, die kommutativ ist.

Bemerkung:
Unterstrukturen können stärkere Eigenschaften haben und insbesondere kommutativ sein, auch wenn dies für die Oberstruktur nicht gilt.

Warnung:
Lemma A.14 gilt nicht für Vereinigungen.
Der Schnitt von Ringen mit 1 braucht keine 1 zu haben.

Lemma A.23 (Abschluss in Halbgruppe)
Sei $\mathcal{U} \subset \mathcal{M}$ Teilmenge einer Halbgruppe $\mathcal{M}$ mit der Verknüpfung $*$. Dann besteht die Hülle $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ aus allen Elementen $u \in M$ der Form

$$u = a_1 * a_2 * \cdots * a_n \; = \; \prod_{i=1}^{n} a_i,$$

wobei $n \in \mathbb{N}$ und $a_i \in \mathcal{U}$ beliebig.

Definition A.22 (Hüllenbildung)

(i) Für ein beliebiges $\mathcal{U} \subset \mathcal{M}$ wird der Durchschnitt aller Halbgruppen bzw. Monoide, Gruppen, Ringe und Körper, die $\mathcal{U}$ als Untermenge enthaltenden, als Hülle $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ von $\mathcal{U}$ bezeichnet.

(ii) Die Element dieser Hülle $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ lassen sich als Ergebnis beliebiger Verknüpfungen und Inversionen von Elementen aus $\mathcal{U}$ darstellen.
Man bezeichnet $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ deshalb auch als den Abschluss von $\mathcal{U}$ bezüglich der vorhandenen Verknüpfungen.

Lemma A.24 (Abschluss in Gruppe)
Sei $\mathcal{U} \subset \mathcal{M}$ Teilmenge einer Gruppe $\mathcal{M}$ mit der Verknüpfung $+$ und $a - b = a + (-b)$. Dann besteht die Hülle $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ aus allen Elementen $u \in \mathcal{M}$ der Form

$$\begin{aligned} u &= a_1 + a_2 + \cdots + a_n &- \quad (b_1 + b_2 + \cdots + b_m) \\ &= \textstyle\sum_{i=1}^{n} a_i &- \quad \sum_{i=1}^{m} b_i, \end{aligned}$$

wobei $n, m \in \mathbb{N}$ und $a_i, b_i \in \mathcal{U}$ beliebig.

Lemma A.25 (Abschluss in Ring)

Sei $\mathcal{U} \subset \mathcal{M}$ Teilmenge eines Ringes $\mathcal{M}$ mit der Verknüpfungen $+$, $a - b = a + (-b)$ und $a * b$. Dann besteht die Hülle $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ *aus allen Elementen $u \in \mathcal{M}$ der Form*

$$\begin{aligned} u &= \pm a_{11} * a_{12} * \cdots * a_{1n_1} \pm a_{21} * a_{22} * \cdots * a_{1n_2} \ldots\ldots \\ &= \sum_{i=1}^{m} \pm \prod_{j=1}^{n_i} a_{ij}, \end{aligned}$$

wobei $m, n_i \in \mathbb{N}$ und $a_{ij} \in \mathcal{U}$ beliebig.

Beispiel A.26

Die natürlichen Zahlen $\mathbb{N}$ sind bezüglich der Addition nur ein Monoid (d.h. Halbgruppe) mit den neutralen Element 0. Um sie zu einer Gruppe zu erweitern, führt man für jedes Element $n \in \mathbb{N}$ ein mit $(-n)$ bezeichnetes neues Element ein, das gerade durch die Eigenschaft

$$(-n) + n = 0 = n + (-n)$$

gekennzeichnet ist. Mann muss dann "nur" noch zeigen, dass die Verknüpfung mit den neuen Elementen so definiert werden kann, dass die erhaltene Menge der ganzen Zahlen, nämlich $\mathbb{Z}$, wirklich eine Gruppe bezüglich + darstellt. Man erhält so die negativen Zahlen mit den bekannten Rechenregeln.

Beispiel A.27

Durch obige Konstruktion erhält man $\mathbb{Z}$, das bezüglich + und $*$ sogar ein Ring ist. Um $\mathbb{Z}$ noch zum Körper auszubauen, fügt man alle Quotienten a/b mit $a, b \in \mathbb{Z}$, teilerfrei hinzu und erhält die rationalen Zahlen $\mathbb{Q}$.

A - 3 Algebraische Erweiterungen

Bemerkung:

Häufig will man eine gegebene algebraische Struktur $\mathcal{M}$ so erweitern, dass sie bezüglich einer wünschenswerten Eigenschaft abgeschlossen ist. Dazu konstruiert man geeignet neue Elemente, so dass der erzielte Abschluss diese stärkere Eigenschaft hat.

Bemerkung:

Nicht alle Ringe lassen sich wie $\mathbb{Z}$ zu einem Körper erweitern. Das geht z.B nicht für die **unsigned char**s $\mathcal{B}$, da dort $32 * 8 = 0$ gilt.

Hätte 8 in irgendeiner Erweiterung einen Kehrwert 8^{-1}, so wurde folgen $32 = 32 * 8 * 8^{-1} = 0 * 8^{-1} = 0$ was offensichtlich inkonsistent wäre.

Definition A.28 (Integritätsbereich)

Ein Paar von Ringelementen $a, b \in \mathcal{M}$ heisst Nullteiler falls

$$a \neq 0 \neq b \quad \wedge \quad a * b = 0.$$

Ein Ring ohne Nullteiler heisst Integritätsbereich.

Satz A.29 (Nullteiler oder Inverse)

In einem endlichen Ring ist jedes Element $a \neq 0$ entweder selbst Nullteiler oder hat ein multiplikatives Inverses der Form $a^{-1} = a^k = a * \cdots * a$ für ein $k \in \mathbb{N}$.

Satz A.30 (Körpererweiterung)

Ein Ring $\mathcal{M}$ mit 1 kann dann und nur dann zu einem Körper erweitert werden, wenn er ein Integritätsbereich ist, d.h. keine Nullteiler besitzt.

Alle endlichen Integritätsbereiche sind selbst Körper.

Resultierende Zahlenhierarchie:

Monoid $\mathbb{N}$ Natürliche Zahlen

$\bigcap$ (Negativenbildung)

Ring $\mathbb{Z}$ Ganze Zahlen

$\bigcap$ (Quotientenbildung)

Körper $\mathbb{Q}$ Rationalen Zahlen

$\bigcap$ (Inf/Sup Bildung)

Körper $\mathbb{R}$ Reelle Zahlen

$\bigcap$ (Wurzelberechnung)

Körper $\mathbb{C} \simeq \mathbb{R} \times \mathbb{R}$ Komplexer Zahlen

$\bigcap$ (Mathemathischer Eifer)

Schiefkörper $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ Quaternionen

Bemerkung:

Quaternionen sind nützlich bei der Beschreibung von Positionen und Drehungen im Raum.