Ergänzung zu Kapitel 1 (Zahlenmengen)

im Skript „Hinweise zur Mathematik I und II“
(Stand 29.01.2015)

Einige Grundbegriffe der allgemeinen Mengenlehre

Obwohl für Ingenieure, Wirtschaftswissenschaftler, Informatiker und andere der Schwerpunkt der Mathematik im Einsatz von – teilweise auch recht anspruchsvollen – Rechenverfahren liegt, ist die Kenntnis einiger weniger theoretischer Grundlagen dennoch hilfreich. Hierzu gehört die **Mengenlehre**, da viele der praktischen Verfahren hieraus entwickelt werden. Hier nochmals die von ***Georg Cantor***, einem Mitbegründer der Mengenlehre, gegebene Definition:

> Def.: Eine Menge ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen. Die Objekte heißen Elemente der Menge.

Für unsere Zwecke sind diese Objekte - auch Elemente - genannt, fast immer Zahlen, doch allgemein können sie unterschiedlichste Inhalte annehmen. Nicht zwingend, aber oft sinnvoll ist es, wenn die Objekte wenigstens ein gemeinsames Merkmal haben. Sie lassen sich aufzählen, wie etwa für

$$A = \{\text{FRA UAS},\ \text{HS AB},\ \text{HS DA},\ \text{Uni FFM}\}$$
$$B = \{\text{Algebra},\ \text{BWL},\ \text{Englisch},\ \text{Analysis}\}\ ,$$

oder verbal beschreiben wie in

$$C = \{\text{alle Hochhäuser Frankfurts, die höher als 100 Meter sind}\}\ ,$$

oder durch eine Formelangabe wie in

$$D = \{x \mid\ x = 2n+1,\ n \in N\}$$ (Menge aller positiven ungeraden Zahlen),

oder als Bestandteil einer schon definierten Menge wie in

$$E = \{E \subset C, \text{ ohne Hochhäuser über 150 Meter Höhe}\}$$

E ist dann eine **Teilmenge** von C. Die Menge E könnte auch C selbst sein, etwa wenn es in Frankfurt keine Hochhäuser über 150 Meter Höhe gäbe.

Gehört ein Element x zur Menge M, schreibt man

$x \in M$, andernfalls $x \notin M$.

Ist z. B. x= HS AB, dann gilt $x \in A$, aber $x \notin D$.

Objekte kommen in einer Menge nur einfach vor, die Reihenfolge ist beliebig.

Da „unsere“ Mengenobjekte fast überwiegend Zahlen sind, wird jetzt mit Zahlenmengen fortgefahren. Doch begegnet man für den praktischen Gebrauch auch Mengen mit anderen Objekten, z. B. bei Programmiersprachen in der Form

- von **Feldern** (array) für Objekte mit gemeinsamen Merkmalen
- oder sogar solchen für Objekte mit unterschiedlichen Merkmalen wie in **Listen** (list), **Tabellen** (table) oder **Zellenfeldern** (cell arrays).

Zwei besondere Mengen sind

- die **leere Menge** $\emptyset$, die kein Element enthält
- die Potenzmenge P(M), die alle Teilmengen von M einschließlich der leeren Menge enthält.

Weitere Eigenschaften und Operationen:

Kardinalzahl: Dies ist die Anzahl der Elemente in einer endlichen Menge A und wird als |A| geschrieben. Z.B. hat die Potenzmenge einer Menge A mit n Elementen die Kardinalzahl $|A|=2^n$ (bitte an einem Beispiel nachprüfen).

Gleichheit: Die Mengen A und B sind genau dann gleich, wenn sie die gleichen Elemente enthalten.

Kartesisches Produkt A X B zweier Mengen A und B: Die Menge aller geordneten Paare (a,b) mit

$a \in A \quad , \quad b \in B \quad .$

Ein Beispiel ist etwa die durch eine Funktion y=f(x) gegebene Punktemenge des zugehörigen Graphen. Aber Vorsicht: Bei der Paarbildung kommt es auf die Reihenfolge an, also darauf, welche Elemente links und welche rechts stehen! A X B wird im Allgemeinen nicht gleich B X A sein.

Durchschnitt $C=A \cap B$ zweier Mengen A und B: Die Menge aller Elemente, die sowohl in A als auch in B enthalten sind. Wenn die Elemente von A und B vollkommen verschieden sind, ist $C=\emptyset$.

Vereinigung $C=A \cup B$ zweier Mengen A und B: Die Menge aller Elemente, die entweder in A oder in B enthalten sind.

Differenz $C=A \setminus B$ zweier Mengen A und B: Die Menge der Elemente von A ohne die Elemente von B. Falls A = B, so ist $C=A \setminus B=\emptyset$.

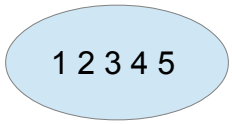
Komplement : $C = A \setminus B$ zweier Mengen A und B, wenn $A \subset B$: Ein Sonderfall der Differenz.

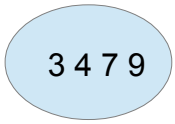
Für Mengen gelten das

- **Kommutativgesetz**
- **Assoziativgesetz**
- **Distributivgesetz**

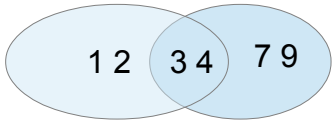
Diese Gesetze spielen u.a. auch eine Rolle in der Stochastik, also bei der Behandlung von Zufallsobjekten. Z. B. lässt sich darüber die Wahrscheinlichkeit der Paarbildung von Objekten beschreiben, etwa im – mehr theoretischen und unterhaltsamen – Fall der Wahrscheinlichkeit der Bildung von Tanzpaaren. Die Frage, wie hoch die Wahrscheinlichkeit ist, dass ein Paar im Startzustand nach zufälliger Zuordnung wieder aufeinandertrifft, wird durch die **Derangement-Berechnung** oder die **Subfakultäten** nach dem **Inklusions-Exklusions-Prinzip** beantwortet (wird detailliert). Eine nützliche Anwendung ist etwa bei der Bestimmung der Fehlerwahrscheinlichkeit für übertragene Bits in der digitalen Nachrichtentechnik mit dem Soft-Decision-Verfahren gegeben.

Die Mengenoperationen lassen sich anschaulich durch Venn-Diagramme als Flächen darstellen. die sich durchdringen können. Beispiel: Wenn A = { 1, 2, 3, 4, 5} und B = {3, 4 , 7 ,9} , also

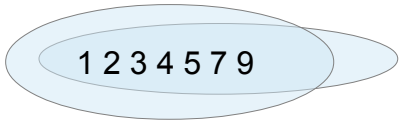
A: 

B: 

dann ist $C = A \cap B = \{3\ \ 4\}$



oder $C = A \cup B = \{1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 7\ \ 9\}$



usw.

Operationen mit Elementen von Mengen und algebraische Strukturen

Zwischen den Elementen von Zahlenmengen (und auch für einige Nichtzahlenmengen) sind Rechenoperationen, so genannte Verknüpfungen, möglich, die sich aber – abhängig von der jeweiligen Menge – nicht beliebig durchführen lassen. So kann man natürliche Zahlen innerhalb ihres Definitionsbereiches zwar ohne Einschränkung addieren und multiplizieren, nicht jedoch subtrahieren und dividieren. Bei der Arbeit mit mehr als einem Element ist darüber hinaus noch die Reihenfolge der Verknüpfungsoperationen zu beachten.

Halbgruppe

- Es ist eine innere Verknüpfung a+b = c oder a··b = d definiert, z. B. 1+2 = 3 oder 2··3 = 6.
- Es gilt das Assoziativgesetz (a+b)+c = a+(b+c) oder (a··b)··c=a··(b··c).

Mit diesen Festlegungen können einige bekannte Mengen bereits auf ihre Halbgruppeneigenschaft überprüft werden. So ist die Menge der natürlichen Zahlen N = {0, 1, 2, 3, 4,..} bezüglich Addition und Multiplikation eine Halbgruppe, nicht aber bezüglich der Subtraktion und Division. Die ganzen Zahlen Z = {..., -3, -2, -1, 0, 1, 2, 3 , 4,..} hingegen bilden auch für die Subtraktion eine Halbgruppe. Viele Verknüpfungen führen auf Elemente mit besonderen Eigenschaften, es sind dies die inversen und die neutralen Elemente. Bei den ganzen Zahlen Z gibt es bezüglich der Addition zu jedem positiven Element auch ein negatives, wobei die Verknüpfung selbst das Element 0 ergibt, also z. B. 2+(-2) = 0. "0" ist also ein neutrales Element, darüber hinaus sogar das einzige. Nun kann eine weitere algebraische Struktur definiert werden:

Gruppen spielen eine Rolle bei Codes zur Datenfehlerbeseitigung (Codewörter bilden eine Gruppe). Die Menge, welche eine Gruppe darstellt, hat die Eigenschaft einer Halbgruppe, zusätzlich existieren aber noch:

- ein neutrales Element und
- zu jedem Element a ein inverses Element a_{inv}.

Auch hier lassen sich wieder bekannte oder weniger bekannte Mengen auf die Gruppeneigenschaften prüfen. So ist z. B. (Z;+), d. h. die Menge der ganzen Zahlen bezüglich der Addition, eine Gruppe. Für die Multiplikation gilt dies nicht, da es in Z hierfür keine inversen Elemente gibt. Dies ist jedoch etwa für die Menge Q der rationalen Zahlen der Fall, da zu jedem Element a auch das inverse Element $a_{inv}=\frac{1}{a}$ besteht und die Multiplikation $a\cdot\left(\frac{1}{a}\right)=1$ das neutrale Element "1" erbringt, wenn man die Zahl "0" ausnimmt.

Demnach ist (Q\{0};·), d. h. die Menge der rationalen Zahlen ohne das Element "0" bezüglich der Multiplikation eine Gruppe. Gilt für die Verknüpfung auch das kommutative Gesetz $a\cdot b=b\cdot a$, so nennt man diese Gruppe eine kommutative oder **Abelsche Gruppe**.

Wenn in einer Menge nicht nur eine Verknüpfung, sondern deren zwei definiert sind, kommen weitere algebraische Strukturen hinzu.

Ringe treten z. B. im Zusammenhang mit Codes zur Datenfehlerbeseitigung auf (Polynomringe über Erweiterungskörpern) und besitzen folgende Eigenschaften:

- Die Menge ist bezüglich der Addition eine kommutative Gruppe.
- Die Menge ist bezüglich der Multiplikation eine Halbgruppe.
- Es gelten für alle Elemente die distributiven Gesetze
  $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$.

Die Menge der ganzen Zahlen bildet demnach nicht nur eine Gruppe, sondern einen Ring.

Gilt in einem Ring, dass das Ergebnis einer Multiplikation nur dann Null ist, wenn wenigstens einer der beiden Faktoren selbst den Wert Null hat, dann bezeichnet man ihn als "**nullteilerfrei**". Gilt für die Verknüpfungen weiterhin noch das Kommutativgesetz und ist das neutrale Element der Multiplikation die "1", so liegt ein **Integritätsring** vor. Für die ganzen Zahlen trifft dies zu, da unter anderem keine gleichzeitig von 0 verschiedenen Elemente existieren, für die $a \bullet b = 0$ wäre. Es gibt aber im Rahmen der weiteren Betrachtungen Mengen, die keine Nullteilerfreiheit aufweisen.

Restklassenmengen sind von zentraler Bedeutung. Sie entstehen, wenn man in der Menge der ganzen Zahlen bei jedem Element und/oder bei jeder Verknüpfung die Modulo n-Operation durchführt (Abkürzung: MOD n). Dabei zieht man von jeder Zahl oder jedem Ergebnis einer Addition bzw. Multiplikation solange die Zahl n ab (oder addiert die inverse Zahl (-n)), bis ein Rest kleiner als n übrig bleibt. Die Menge der so gebildeten Zahlen ist endlich (mit der so genannten Ordnung n) und erfüllt die genannten Ringeigenschaften.

Eine Restklassenmenge z. B. $Z_5 = \{0, 1, 2, 3, 4\}$ wird aus allen ganzen Zahlen MOD 5 gebildet. Anhand einer Tabelle lassen sich hier alle möglichen Multiplikationsergebnisse aufstellen, da es sich um eine endliche Menge mit 5 Elementen handelt, die in $5 \cdot\cdot 5 = 25$ verschiedenen Kombinationen multipliziert werden können. Bei geschachtelten Verknüpfungen entstehen dabei zwar auch Zwischenergebnisse, welche größer als 5 sind. Die Modulo 5-Operation kann man dann aber entweder bei jedem Teilergebnis oder zum Schluss anwenden. Beispiele:

$(2 \cdot 4) \cdot 3$ MOD 5	$= 8 \cdot 3$ MOD 5	
	= 24 MOD 5	= 4
oder	= (8 MOD 5) · (3 MOD 5) MOD 5	
	$= 3 \cdot 3$ MOD 5	
	= 9 MOD 5	= 4
oder	= (2 MOD 5 · 4 MOD 5) · 3 MOD 5	
	$= (2 \cdot 4) \cdot 3$ MOD 5	
	$= 8 \cdot 3$ MOD 5	= 4

und so weiter. Die Tabelle 2-1 für die Multiplikation aller Elemente paarweise untereinander sieht dann so aus:

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tabelle 2-1: *Paarweise Multiplikation aller Elemente im Z_5*

Man erkennt, dass die Restklassenmenge Z_5 nullteilerfrei ist. Bei Z_6 trifft dies hingegen nicht zu, wie Tabelle 2-2 zeigt. Z_6 bildet also keinen Integritätsring.

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Tabelle 2-2: *Paarweise Multiplikation aller Elemente im Z_6*

Generell sind Restklassenmengen aus ganzen Zahlen immer nur dann nullteilerfrei, wenn man die Restklassenbildung über MOD n mit Primzahlen n durchführt. Verständlich wird das aus der Definition der Primzahlen:

> Primzahlen sind alle natürlichen Zahlen, die sich ohne Rest nur durch 1 und sich selbst teilen lassen, also 2, 3, 5, 7, 11, 13, ... usw. Sie können demnach nicht in ganzzahlige Faktoren zerlegt werden.

Körper ist ein zentraler Begriff, z. B. auch für alle Codierungsverfahren: Wenn eine Menge einen Ring bildet und zusätzlich bezüglich der Multiplikation eine Gruppe darstellt, also zu jedem Element a (außer a=0) ein inverses Element a_{inv} existiert, so dass $a \cdot a_{inv} = a \cdot \left(\frac{1}{a}\right) = 1$ gilt, so stellt diese Menge einen Körper dar.

Für die Menge der ganzen Zahlen trifft dies nicht zu (Warum?), wohl aber für die Menge Q der rationalen Zahlen. Aber auch spezielle Restklassenringe sind Körper, nämlich alle, die aus der Modulo-Bildung bezüglich einer Primzahl hervorgegangen sind, wie z. B. Z_3, Z_5 usw. Dies erscheint vielleicht erstaunlich, da man bei Betrachtung der Tabelle 2-1 zunächst gar keine inversen Elemente erkennt. Aus dem Alltag ist man nur mit Bruchzahlen als inversen Elementen vertraut, die Definition des inversen Elements bezüglich der Multiplikation lässt aber auch ganzzahlige Inverse zu. Es muss nur gelten $a \cdot\cdot a_{inv} = 1$. Das trifft im Beispiel gemäß Tabelle 2-1 etwa für $2 \cdot\cdot 3$ MOD 5 = 1 zu. Also ist 3 das inverse Element zu 2. Da jedes Element außer 0 ein Inverses besitzt, ist die Restklassenmenge Z_5 demnach nicht nur ein Ring, sondern ein Körper.

Bildet eine Menge einen kommutativen Ring und gibt es darin eine Untergruppe zur Additionsgruppe, dann ist diese Untergruppe ein **Ideal**, wenn alle paarweisen Produkte zwischen den Elementen des Ringes und der Untergruppe wiederum Elemente der Untergruppe sind. Ein Beispiel:

Die Menge der ganzen Zahlen ist ein kommutativer Ring. Die Additionsgruppe hierin ist in diesem Fall die Menge selbst, mit "0" als neutralem Element. Es gilt ja, dass jedes Element mit jedem

beliebigen anderen (oder mit sich selbst) addiert werden kann und dabei wieder ein Element der Menge entsteht. Inverse Elemente (-a), zu ihren Partnerelementen a addiert, bringen als Ergebnis das neutrale Element "0". Bei den natürlichen Zahlen trifft dies z. B. aber nicht zu.

Eine Untermenge wären etwa alle geraden Zahlen {... -6, -4, -2, 0, 2, 4, 6...}. Jede paarweise Addition ergibt wieder ein Element der Untermenge selbst, also ist die Untermenge auch eine Gruppe mit "0" als neutralem Element. Aber auch dann, wenn diese Untermenge mit einem beliebigen Element aus der Menge der ganzen Zahlen multipliziert wird, entstehen nur Elemente, die ebenfalls ausschließlich in der Untermenge enthalten sind:

$2 \cdot \{...-6, -4, -2, 0, 2, 4, 6...\} = \{... -12, -8, -4, 0, 4, 8, 12, ...\}.$

Für die ungeraden Zahlen stimmt dies nicht, da die Addition zweier ungerader Zahlen immer eine gerade Zahl ergibt und die Ergebnismenge nicht in der Untermenge enthalten wäre.

Allgemein sind Ideale aus dem Ring der ganzen Zahlen die Teilmengen, die durch Multiplikation einer natürlichen Zahl n mit der Menge der ganzen Zahlen entstehen. Für n = 7 etwa ist

$$7 \cdot \{..., -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ...\}$$
$$= \{..., -35, -28, -21, -14, -7, 0 ,7, 14, 21, 28, 35, ...\},$$

da die Gruppeneigenschaft vorliegt und die Multiplikation des Ideals mit einer beliebigen ganzen Zahl wieder auf eine Teilmenge des Ideals führt. Verwendet man bei dem oben angegebenen Beispiel als Element der ganzen Zahlen etwa -8, so erhält man

$$-8 \cdot \{ ...,-35, -28, -21, -14, -7, 0, 7, 14, 21, 28, ...\}$$
$$= \{..., -280, -208, -168, -112, -56, 0, 56, 112, 168, 280,...\}$$

und damit eine Teilmenge der Untergruppe.

Primideale sind z. B. beim Ring der ganzen Zahlen solche Ideale, zu deren Erzeugung als Multiplikator n eine Primzahl gewählt wurde.

Bisher wurden nur Zahlen betrachtet. Der Elementbegriff bei Mengen ist aber ganz abstrakt, weshalb auch ganz andere Elementtypen einbezogen werden können. Allerdings scheinen nur wenige für einen praktischen Gebrauch interessant zu sein.

Solche Elemente können auch Polynome sein. Es ist aus technischen Gründen sinnvoll, die Werte der Koeffizienten und der Polynom-Variablen auf ganze Zahlen zu beschränken. Genau genommen sind sogar nur ganze Zahlen MOD n interessant.

Z. B. gibt es einen Ring von Polynomen über einem endlichen Körper, etwa Z_2. Die Koeffizienten (und gegebenenfalls x) haben dann nur die Werte 0 oder 1. Wählt man ein **irreduzibles**, d. h. ein nicht weiter in Polynome kleineren Grades zerlegbares Polynom, z. B. $f(x) = x^2 + x^1 + 1$ (es entspricht in dieser Eigenschaft der Primzahl aus den Zahlenmengen), so bilden alle Polynome MOD f(x) eine endliche Menge von "Restpolynomen", die wieder die Ringeigenschaften aufweisen. Algebraische Körpererweiterungen sind ein zentraler Begriff für Codes zur Datenfehlerbeseitigung (Nullstellen von irreduziblen Polynomen über endlichen Körpern).