

Formale Grundlagen der Informatik

WiSe 2007/08 in Trier

Henning Fernau

Universität Trier

fernau@informatik.uni-trier.de

Formale Grundlagen der Informatik

Gesamtübersicht

1. Rechnen: Gesetze und Regeln
2. Zählen und Würfeln: Kombinatorik und Wahrscheinlichkeitsrechnung
3. Modellieren und Formalisieren: Keine Angst vor Formalismen
4. Warum stimmt das eigentlich ? Beweisverfahren
5. Herangehen an Aufgaben aus Informatik und Mathematik

Organisatorisches

Vorlesung heute 8.15 bis 11.30 im HS 11 (mit Pause)

an den folgenden Tagen: 8.45 bis 12.00 (mit Pause)

12-14 Uhr: Gelegenheit zur Gruppenarbeit zu ausgewählten Übungen

parallel dazu: 13.30-14.15 **Sprechstunde**: Wir fünf sind im HS 11 für Sie da.

(Große) Übung 14-16 Uhr, d.h.: 14.15-15.45 (Gulan, Raible, Bakman, Schlecht)

Am Abend überdenken Sie bitte den Stoff; sie erhalten auch Gelegenheit zu weiteren Übungen.

An den folgenden Tagen stehen Ihnen Studierende (Bakman, Schlecht) von 8.00 bis 8.45 für Fragen hier zur Verfügung. Dann werden auch die Übungen vom letzten Abend angesprochen. **(Kleine) Übung**

(Weitere Unterrichtsformen: praktische Übungen, Seminare)

Hinweis: HZ 202, 203 und 204 stehen von 12-18 Uhr zu Ihrer Verfügung !

Organisatorisches: Der erste Tag (heute)

Vorlesung 8.15 bis 11.30 im HS 11 (mit Pause)

11.30 werden Sie vom Fachschaftsrat Informatik “abgeholt” (Mensa, Gebäudeführung)

13.30-14.15 **Sprechstunde** im HS 11 (Fragen bitte ?)

(Große) Übung 14.15-15.45 (Gulan, Raible, Bakman, Schlecht)

Fachschaftsratsprechstunde 15.45-16.45 im H 508

Achtung: Die Mensa schließt während der “vorlesungsfreien Zeit” um 13.30.

Ziele / Gründe

Viele Studierende haben Schwierigkeiten mit formalen Denkweisen.

Schule und Uni liegen in Mathematik und Informatik oft weit auseinander:
Unterrichtsstil / -form, Tempo, Abstraktionsgrad.

~> (leider) sehr hohe “Schwundquote” in der Informatik

Dieser Vorkurs soll hier Abhilfe schaffen.

Probleme beim Studium ?!

Sprechen Sie mit uns:

Studierende gleicher Semester, Studierende höherer Semester, Fachschaftsrat, Fachstudienberater, Verwaltung, Assistenten, Professoren

Wir sind für Sie da!

Unterschätzen Sie nicht die Fächer und den Arbeitsaufwand:

zwei Stunden Infor-Mathe-matikvorlesung bedeutet stets mindestens denselben Zeitaufwand “im stillen Kämmerlein” (plus Bearbeitung der Übungen).

Besuchen Sie Vorlesungen und Übungen persönlich.

Schieben Sie Lücken nicht “auf die lange Bank”.

Gestehen Sie sich Schwierigkeiten ein. Jede(r) hat sie.

Fachstudienberatung: Probleme beim Studium ?!

Lassen Sie es gar nicht erst dazu “richtig” kommen...

Fachstudienberatung: Norbert Müller, H417;
reguläre Sprechstunde: Di 9:00-11:00, Fr 9:00-11:00

Einführungsveranstaltung zum Bachelor Informatik:

Mo, 22.10., 8:15-10:00, Raum HS 13, Campus II

Gruppen/Einzel-Beratung:

Mo, 22.10., 14:00-16:00, Raum H 417, Campus II

Di, 23.10., 9:00-11:00, Raum H 417, Campus II

Bei der Einführungsveranstaltung werden u.a. auch angesprochen:
(scheinbare) Überschneidungen im Stundenplan, mögliche Anwendungsfächer...

Ein Kaufhausproblem



Zwei Kaufhausleiter streiten sich:

A: Bei mir ist der Kunde noch König: Meine 20% Rabatt gibt es selbstverständlich auf den Gesamtpreis der Ware, also einschließlich der (vereinfacht) 15% Mehrwertsteuer.

B: Papperlapapp! Warum sollte der Kunde noch Steuern mit zahlen auf einen Preis, der eh nachher reduziert wird? Bei mir wird erst rabattiert und dann die Mehrwertsteuer dazugerechnet.

Bei wem sollten wir ein rabattiertes, vor Steuern für 100 Euro ausgewiesenes Modell erwerben ?

Ein Kaufhausproblem — Herangehensweise

Lesen wir die Aufgabe genau durch. Was sind die wesentlichen Punkte?

Rechnen wir das Beispiel für A und B aus.

Was fällt auf?

Ist das Zufall? Wir prüfen weitere Beispiele.

Wie können wir die Aufgabenstellung verallgemeinern?

Was ist der eigentliche Grund für unsere Beobachtungen?

Rechengesetze I

Eine binäre Verknüpfung \circ (z.B.: $\circ = +$ oder $\circ = \cdot$) heißt *kommutativ* genau dann, wenn für alle a, b gilt

$$a \circ b = b \circ a$$

Beispiele

Als Verknüpfungen auf den reellen Zahlen sind Addition und Multiplikation kommutativ, siehe das Kaufhausbeispiel.

Anschaulich ist das Parallelogramm bei der Vektoraddition, welches die Kommutativität dieser Operation versinnbildlicht.

Die Subtraktion und Division sind hingegen nicht kommutativ, denn es ist z. B.

$$2 - 3 = -1 \quad \neq \quad 1 = 3 - 2.$$

Auch die Potenz ist nicht kommutativ, da z. B.

$$2^3 = 8 \quad \neq \quad 9 = 3^2$$

gilt.

Fabel vom klugen Wolf und den neun dummen Wölfen

ein mathematischer Lehrtext aus der Zeit Mitte des 3. Jahrtausends v. Chr. (es gibt wohl auch kaum ältere Schultexte), den die Schüler einer Schule in Sumer, einem sogenannten Tafelhaus, abschreiben mussten. Er behandelt das Kommutativgesetz der Addition.

Es brechen zehn Wölfe in einen Schafpferch ein und stehlen zehn Schafe.

Der kluge Wolf schlägt vor zu teilen, und zwar gerecht.

Die neun anderen Wölfe, vor Fressgier ganz dumm, fragen, was das bedeute.

Der kluge Wolf schlägt vor, so zu teilen, dass immer zehn herauskommt.

“Ihr neun Wölfe bekommt ein Schaf, dann seid ihr zusammen zehn. Ich und neun Schafe — macht ebenfalls zehn. Stimmt das etwa nicht?”

“Stimmt genau.” sagen die neun Wölfe und stürzen sich auf das Schaf, das ihnen der kluge Wolf hinschiebt.

Sie fressen, während der schlaue Wolf die anderen neun Schafe wegschleppt.

Didaktik

Mathematik “bei den Alten” (ausschließlich) anhand von **Beispielen**.

Das ist sehr anschaulich, aber auch sehr langatmig.

Auch Schulmathematik arbeitet oft vom Konkreten zum Abstrakten.

Mathematik hat historisch gesehen immer so gearbeitet.

Vorteile der Abstraktion:

Konzentration auf das Wesentliche / Erkenntnis des Wesentlichen

Möglichkeit einer sehr kompakten, aber “ungeschichtlichen” Darstellung von Mathematik.

~> Uni-Mathematik ist sehr viel konzentrierter als Schulmathematik.

~> Ihre implizite und ständige Aufgabe: Spezialisieren Sie, was Ihnen zu abstrakt erscheint, durch geeignete, selbst gewählte Beispiele.

Wenn Sie das nicht können, haben Sie den Stoff nicht verstanden.

Rechengesetze II

Eine binäre Verknüpfung \circ heißt *assoziativ* genau dann, wenn für alle a, b, c gilt

$$a \circ (b \circ c) = (a \circ b) \circ c$$

Beispiele

Als Verknüpfungen auf den reellen Zahlen sind Addition und Multiplikation assoziativ, z.B.:

$$(2 + 3) + 7 = 5 + 7 = 12 \quad = \quad 2 + (3 + 7) = 2 + 10 = 12.$$

Die Subtraktion und Division sind hingegen nicht assoziativ, denn es ist z. B.

$$2 - (3 - 1) = 0 \quad \neq \quad (2 - 3) - 1 = -2.$$

Auch die Potenz ist nicht assoziativ, da z. B.

$$2^{(2^3)} = 2^8 = 256 \quad \neq \quad 64 = 4^3 = (2^2)^3$$

gilt.

Rechengesetze III

Distributivgesetze geben an, wie sich zwei Verknüpfungen, zum Beispiel Multiplikation (\cdot) und Addition ($+$), bei der Auflösung von Klammern zueinander verhalten. Man unterscheidet linksdistributiv und rechtsdistributiv:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad (\text{linksdistributiv})$$

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad (\text{rechtsdistributiv})$$

Beispiele bei reellen Zahlen:

$$6 \cdot 16 = 6 \cdot (10 + 6) = 6 \cdot 10 + 6 \cdot 6 = 60 + 36 = 96$$

$$5 \cdot (7 + 3) = 5 \cdot 10 = 50 = 5 \cdot 7 + 5 \cdot 3 = 35 + 15 = 50$$

Weitere Beispiele für Distributivgesetze

Für reelle Zahlen a, b, c gilt:

$$a \cdot (b - c) = a \cdot b - a \cdot c \quad (\text{linksdistributiv})$$

$$(a - b) \cdot c = a \cdot c - b \cdot c \quad (\text{rechtsdistributiv})$$

Aufgaben:

Kennen Sie weitere Beispiele ?

Kennen Sie Paare von Verknüpfungen, bei denen die Distributivgesetze nicht gelten ?

Wieso folgt für die reellen Zahlen die Rechts- aus der Linksdistributivität ?

Anwendungen der Rechengesetze

Kopfrechentricks:

$$25 \cdot 19 = ??$$

$$25 \cdot 19 = 25 \cdot (20 - 1) = 25 \cdot 20 - 25 \cdot 1 = 500 - 25 = 475$$

$$36 + 55 + 64 + 33 + 12 = ??$$

$$36 + 55 + 64 + 33 + 12 = (36 + 64) + (55 + (33 + 12)) = 100 + 100 = 200$$

In der Schulalgebra bezeichnet man die Verwendung des Distributivgesetzes zur Umwandlung einer Summe in ein Produkt als *Ausklammern* oder Herausheben. Der umgekehrte Rechenschritt wird als *Ausmultiplizieren* bezeichnet.

Gelten diese Rechengesetze auch auf Rechnern ?

Zahldarstellungen

TAB. 86 MEMOIRE DE L'ACADEMIE ROYALE
DES NOMBRES.

bres entiers au-dessous du double du plus haut degré. Car icy, c'est comme si on disoit, par exemple, que 111 ou 7 est la somme de quatre, de deux & d'un. Et que 1101 ou 13 est la somme de huit, quatre & un. Cette propriété sert aux Essayeurs pour peser toutes fortes de masses avec peu de poids, & pourroit servir dans les monnoyes pour donner plusieurs valeurs avec peu de pieces.

Cette expression des Nombres étant établie, sert à faire tres-facilement toutes fortes d'operations.

Pour l'Addition par exemple.

$$\begin{array}{r} 110 \parallel 6 \\ 111 \parallel 7 \\ \hline 1101 \parallel 13 \end{array} \quad \begin{array}{r} 101 \parallel 5 \\ 1011 \parallel 11 \\ \hline 10000 \parallel 16 \end{array} \quad \begin{array}{r} 1110 \parallel 14 \\ 10001 \parallel 17 \\ \hline 11111 \parallel 31 \end{array}$$

Pour la Soustraction.

$$\begin{array}{r} 1101 \parallel 13 \\ 111 \parallel 7 \\ \hline 110 \parallel 6 \end{array} \quad \begin{array}{r} 10000 \parallel 16 \\ 1011 \parallel 11 \\ \hline 101 \parallel 5 \end{array} \quad \begin{array}{r} 11111 \parallel 31 \\ 10001 \parallel 17 \\ \hline 1110 \parallel 14 \end{array}$$

Pour la Multiplication.

$$\begin{array}{r} 11 \parallel 3 \\ 11 \parallel 3 \\ \hline 11 \parallel 3 \\ 1001 \parallel 9 \end{array} \quad \begin{array}{r} 101 \parallel 5 \\ 11 \parallel 3 \\ \hline 101 \parallel 5 \\ 1111 \parallel 15 \end{array} \quad \begin{array}{r} 101 \parallel 5 \\ 101 \parallel 5 \\ \hline 101 \parallel 5 \\ 11001 \parallel 25 \end{array}$$

Pour la Division.

$$\begin{array}{r} 15 \parallel 2211 \\ 3 \parallel 2221 \end{array} \quad \begin{array}{r} 101 \parallel 5 \\ 21 \end{array}$$

Et toutes ces operations sont si aisées, qu'on n'a jamais besoin de rien essayer ni deviner, comme il faut faire dans la division ordinaire. On n'a point besoin non-plus de rien apprendre par cœur icy, comme il faut faire dans le calcul ordinaire, où il faut sçavoir, par exemple, que 6 & 7 pris ensemble font 13; & que 5 multiplié par 3 donne 15, suivant la Table d'une fois un est un, qu'on appelle Pythagorique. Mais icy tout cela se trouve & se prouve de source, comme l'on voit dans les exemples précédens sous les signes \odot & \ominus .

Das *Dualsystem* (*Zweiersystem*, *Binärsystem*), also das Stellenwertsystem mit der Grundzahl (Basis) Zwei, wurde von Gottfried Wilhelm Leibniz 1703 in seinem Artikel "Explication de l'Arithmétique Binaire" vollständig beschrieben.

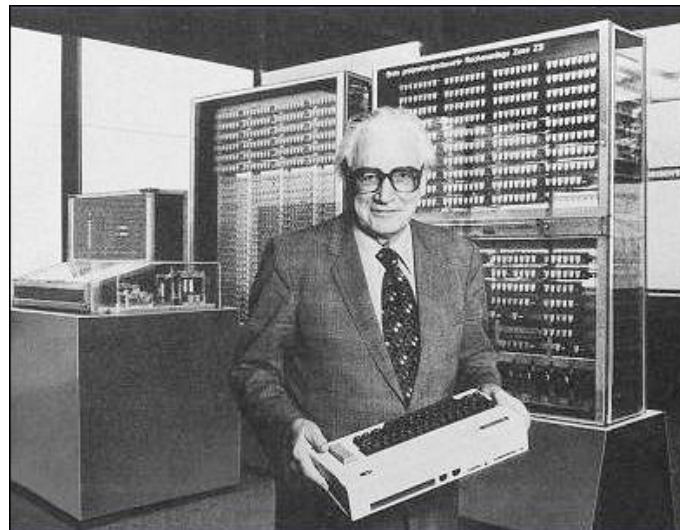
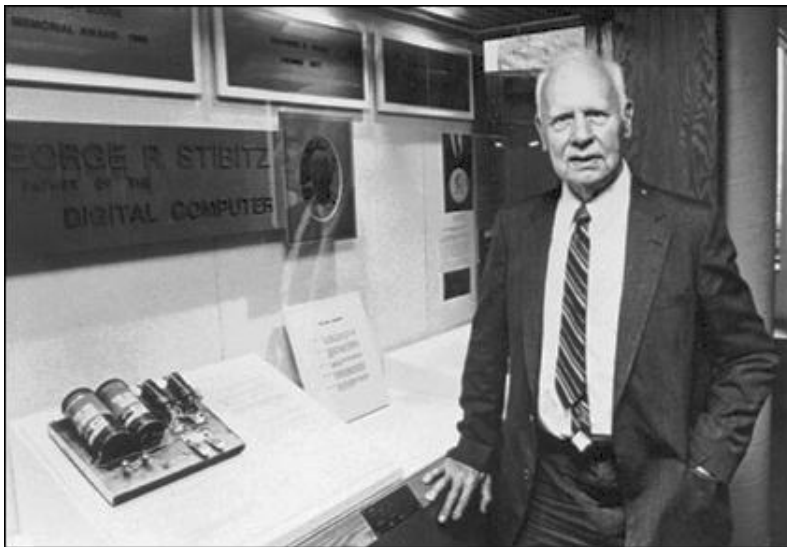
Die Bedeutung für Rechenanlagen erkannte 1854 George Boole.

Umgesetzt wurden diese Ideen von George Stibitz (Modell K, 1937) und Konrad Zuse (Z3, 1941).

Stibitz und Zuse: Pioniere der Informatik

Quelle: <http://www.kerryr.net/index.htm> mit der Warnung:

This is an Australian site, and written in Australian English. Any resemblance to American or Euro English is purely coincidental.



Dualsystem: Umwandlungen

Vom Dualsystem ins Dezimalsystem

Um eine Dualzahl in die entsprechende Dezimalzahl umzurechnen, werden alle Ziffern jeweils mit ihrem Stellenwert (entsprechende Zweierpotenz) multipliziert und dann addiert.

Beispiel:

$$1010_{(2)} = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 1 \cdot 2^3 + 1 \cdot 2^1 = 8 + 2 = 10_{(10)}$$

Vom Dezimalsystem ins Dualsystem

Es gibt mehrere Möglichkeiten der Umrechnung ins Dualsystem. Im Folgenden ist die Divisionsmethode (Modulo-Methode) am Beispiel $41_{(10)}$ beschrieben:

$$\begin{array}{r} 41 : 2 = 20 \text{ Rest } \mathbf{1} \\ 20 : 2 = 10 \text{ Rest } \mathbf{0} \\ 10 : 2 = 5 \text{ Rest } \mathbf{0} \\ 5 : 2 = 2 \text{ Rest } \mathbf{1} \\ 2 : 2 = 1 \text{ Rest } \mathbf{0} \\ 1 : 2 = 0 \text{ Rest } \mathbf{1} \end{array} \left| \begin{array}{l} \uparrow \\ \\ \\ \\ \\ \end{array} \right.$$

Die entsprechende Dualzahl ergibt sich durch Notation der errechneten Reste von unten nach oben: $101001_{(2)}$.

Dualzahlen in der elektronischen Datenverarbeitung

Darstellung von *Festkommazahlen* oder *ganzen Zahlen*.

Negative Zahlen werden vor allem als Zweierkomplement dargestellt, welches nur im positiven Bereich der Dualzahlendarstellung entspricht.

Um näherungsweise *rationale* oder gar *reelle Zahlen* darzustellen, werden vorzugsweise Gleitkommadarstellungen verwendet, bei der die Zahl normalisiert und in Mantisse und Exponent aufgeteilt wird. Diese beiden Werte werden dann in Form von Dualzahlen gespeichert.

Zweierkomplement

Beispielhafte Umwandlung der negativen Dezimalzahl -4 ins Zweierkomplement:

1. Vorzeichen ignorieren und ins Binärsystem umrechnen: $4_{(10)} = 00000100_{(2)}$.

2. Invertieren, da negativ: 11111011_2 .

3. Eins addieren, da negativ: $11111011_2 + 00000001_2 = 11111100_2$.

Mit n Bits lassen sich Zahlen von -2^{n-1} bis $+2^{n-1} - 1$ darstellen; bei 8 Bit: $-128_{(10)}$ bis $+127_{(10)}$.

Negative Zahlen erkennt man an der Eins als höchstwertigem Bit.

Addition und Subtraktion benötigen keine Fallunterscheidung.

Die Subtraktion wird auf eine Addition zurückgeführt.

$$-4 + 3 = -1 \text{ führt zu}$$

$$\begin{array}{r} 11111100 \\ + 00000011 \\ = 11111111 \end{array}$$

$$+4 - 4 = 0 \text{ führt zu}$$

$$\begin{array}{r} 00000100 \\ + 11111100 \\ = (1) 00000000 \end{array}$$

$$\text{Problem: Überlauf: } +4 + 127 = +131$$

$$\begin{array}{r} 00000100 \\ + 01111111 \\ = 10000011 \end{array}$$

Einfache Aufgaben

Berechnen Sie $63 - 55$, indem Sie:

- (1) Die Dezimalzahlen 63 und 55 (systematisch) ins Zweiersystem umrechnen,
- (2) sich einen geeigneten Zahlbereich aussuchen, um im Folgenden “verlustfrei” im Zweiersystem rechnen zu können,
- (3) das Zweierkomplement von der ins Zweiersystem verwandelten Zahl 55 ausrechnen,
- (4) diese dann (im Zweiersystem) zu der unter (2) ins Zweiersystem umgewandelten Zahl 63 addieren und schließlich
- (5) das Ergebnis wieder (systematisch) ins Zehnersystem umrechnen.

Rechengesetze auf Rechnern (speziell: Ganzzahlarithmetik, Typ “integer”)

Kommutativität ✓

Assoziativität $(4 + 127) + (-4)$ liefert (zwischen durch) Überlauf, $4 + (127 + (-4))$ zeigt diese Schwierigkeit nicht.

Distributivität $(1 + 127) \cdot (-1)$ liefert (zwischen durch) Überlauf, $(-1) + (-127)$ zeigt diese Schwierigkeit nicht.

Untersuchen Sie:

(Wann) Kann man Überlauf bei Zwischenergebnissen ignorieren ?

Informieren Sie sich genauer über Gleitkomma-Arithmetik.

Welche Rechengesetze gelten hier (nicht) und warum ?

Speziell: In welcher Reihenfolge sollte man eine Reihe von Gleitkommazahlen addieren, will man ein möglichst genaues Ergebnis erzielen (und warum) ?!

Weitere Zahlssysteme

Das Zweiersystem kommt einer elektronischen Realisierung sehr entgegen: an vs. aus.

Es gab (und gibt) aber auch alternative Vorschläge.

Der zweithäufigst umgesetzte (!) betrifft das *balancierte Ternärsystem*:

Satz: Jede ganze Zahl lässt sich darstellen als $\sum_{i=0}^k a_i 3^i$ mit $a_i \in \{-1, 0, 1\}$.

Beispiel: $2 = 1 \cdot 3^1 + (-1)3^0$, $-2 = (-1) \cdot 3^1 + 1 \cdot 3^0$.

Aufgaben:

Finden Sie weitere Beispiele !

Wie kann man in diesem System addieren, negieren, subtrahieren ?

Rechengesetze IV

Für eine Verknüpfung \circ heißt e *neutrales Element* gdw. $x \circ e = e \circ x = x$ für alle x gilt.

0 ist neutrales Element der Addition, 1 ist neutrales Element der Multiplikation. Daher heißen neutrale Elemente manchmal auch Nullelemente oder auch Einselemente.

Für eine Verknüpfung \circ mit neutralem Element e heißt y *inverses Element* von x gdw. $y \circ x = x \circ y = e$ gilt.

Jede reelle Zahl hat ein additives Inverses, oft *Gegenzahl* genannt.
Jede reelle Zahl x außer der Null hat ein multiplikatives Inverses x^{-1} .

Begriffserklärung



Auf Georg Cantor geht folgende Definition für Mengen (Mannigfaltigkeiten) zurück:

Eine *Menge* ist eine Zusammenfassung bestimmter, wohlunterschiedlicher Dinge unserer Anschauung oder unseres Denkens, welche *Elemente* der Menge genannt werden, zu einem Ganzen.

Beispiel: \emptyset : die *leere Menge*

Schulkasse (als Menge von Schülerinnen und Schülern)

$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$: die Menge der natürlichen Zahlen

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$: die Menge der ganzen Zahlen

\mathbb{Q} : die Menge der rationalen Zahlen

\mathbb{R} : die Menge der reellen Zahlen

Warnung vor naivem Zugang: “Menge aller Mengen”

Elementrelation; Mengengleichheit

Um auszudrücken, dass x ein Element der Menge M ist, schreiben wir: $x \in M$ und sprechen aus: x *liegt in* M .

Für das Gegenteil schreibt man kurz: $x \notin M$.

Endliche Mengen kann man durch vollzählige Aufzählung ihrer Elemente beschreiben, z.B. eine Schulklasse durch Auflistung der SchülerInnen.

$M = \{\text{Martin, Michael, Carla, } \dots \}$ (bitte ergänzen, bis alle höchstens 50 Elemente aufgezählt sind ;-)

Zwei Mengen M_1 und M_2 sind *gleich*, i.Z.: $M_1 = M_2$, gdw.:
 $x \in M_1$ genau dann, wenn $x \in M_2$.

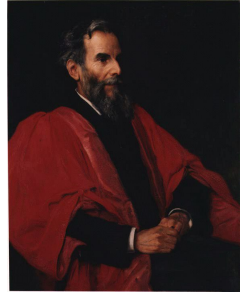
Teilmengen und Obermengen

N heißt *Teilmenge* von M ($N \subseteq M$) gdw. M heißt *Obermenge* von N ($M \supseteq N$) gdw. jedes Element $x \in N$ liegt auch in M .

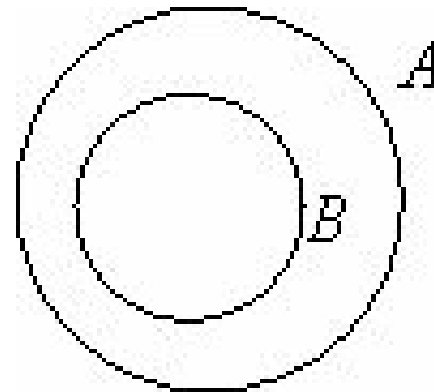
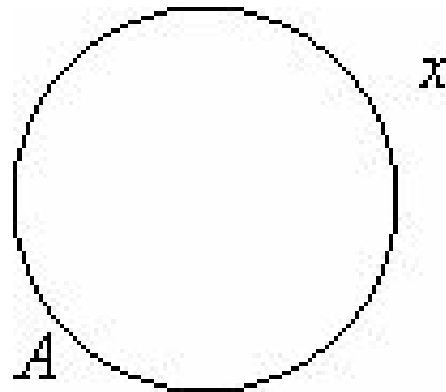
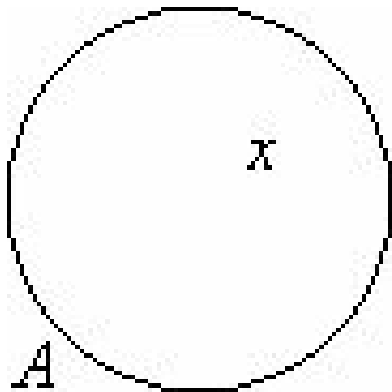
Gilt $N \subseteq M$ und $N \neq M$, so sprechen wir auch von einer *echten Teilmenge* und schreiben $N \subset M$.

Beispiel: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

Satz: $N = M$ gdw. sowohl $N \subseteq M$ als auch $M \subseteq N$.



Venn-Diagramme

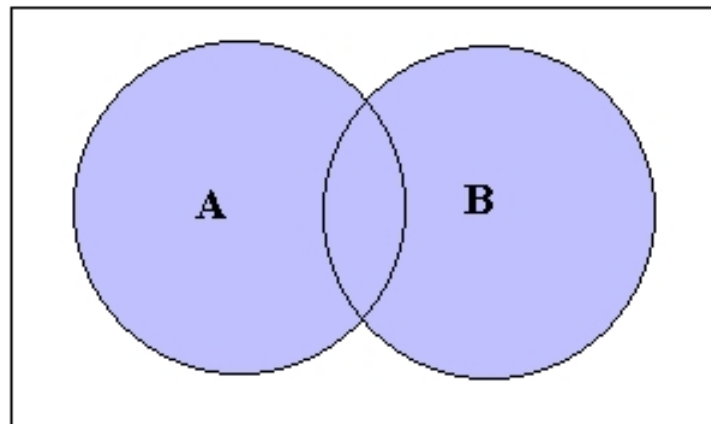


Problem: Uneinheitliche Beschriftung

Mengenalgebra: Vereinigung

Es seien A, B Mengen. Die Gesamtheit der Elemente, die zu A oder auch zu B gehören, wird als *Vereinigung* von A und B bezeichnet;

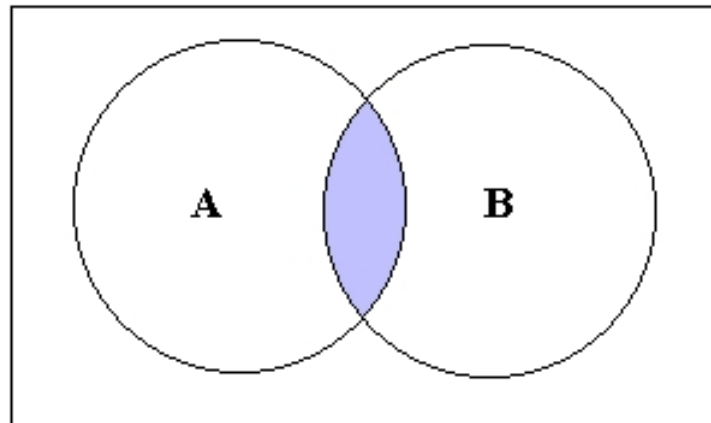
Schreibweise: $A \cup B$



Venn-Diagramm:

Mengenalgebra: Durchschnitt

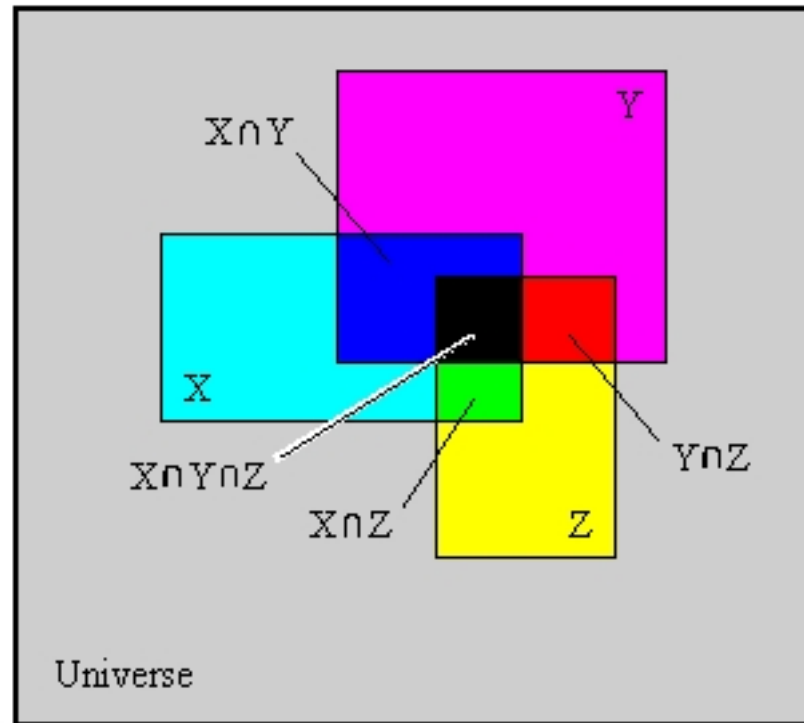
Es seien A, B Mengen. Die Gesamtheit der Elemente, die sowohl zu A als auch zu B gehören, wird als *Durchschnitt* von A und B bezeichnet;
Schreibweise: $A \cap B$



Venn-Diagramm:

A und B heißen *disjunkt* oder *fremd* gdw. $A \cap B = \emptyset$.

Venn-Diagramme: Zusammenfassung



Mengenalgebra: Aussagen

Satz: $A \cap B \subseteq A \subseteq A \cup B$; $A \cap B \subseteq B \subseteq A \cup B$.

Satz: $A \cup A = A \cap A = A$.

Satz: $A \cup B = B \cup A$; $A \cap B = B \cap A$. (Kommutativität)

Satz: $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$. (Assoziativität)

Satz: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$; $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.
(Distributivität)

Aufgabe: Machen Sie sich sämtliche Aussagen an “möglichst allgemeinen” Beispielen klar.

Jetzt werden wir noch etwas kompakter in der Darstellung

Eine *Halbgruppe* ist eine Struktur (H, \circ) , wobei \circ eine assoziative Verknüpfung auf der Menge H ist.

Diese Formulierung soll auch die *Abgeschlossenheit* beinhalten, d.h., wenn $a, b \in H$, so auch $(a \circ b) \in H$.

Lemma: In einer Halbgruppe gibt es höchstens ein neutrales Element.

Beweis: Wenn die Aussage falsch wäre, so gäbe es zwei Elemente e_1 und e_2 , die die Eigenschaft eines neutralen Elements erfüllen. Daher gilt:

$$e_1 = e_1 \circ e_2 = e_2 \circ e_1 = e_2.$$

Dies widerspricht der Annahme.

Dies ist ein Beispiel für einen *Widerspruchsbeweis*.

Eine Struktur (M, \circ, e) ist ein *Monoid* gdw. (M, \circ) eine Halbgruppe ist und e ein neutrales Element von \circ ist.

Beispiele

Es sei \mathbb{N} die Menge der natürlichen Zahlen, d.h.:

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}.$$

Hinweis: \mathbb{N} umfasst “im Wesentlichen” alle auf Rechnern tatsächlich behandelbaren Objekte; insbesondere “reelle Zahlen” sind Fiktion.

Beispiel: $(\mathbb{N}, \max, 0)$ ist ein Monoid.

Beispiel: $(\mathbb{N}, +, 0)$ ist ein Monoid.

Beispiel: (\mathbb{N}, \min) ist eine Halbgruppe ohne neutrales Element. Man könnte allerdings ein neutrales Element zu \mathbb{N} künstlich hinzufügen. Nennen wir es ∞ , so bildet $(\mathbb{N} \cup \{\infty\}, \min, \infty)$ ein Monoid.

Endliche Monoide

Ein Monoid (M, \circ, e) heißt endlich gdw. $|M| < \infty$.

Endliche Monoide kann man gut mit einer *Verknüpfungstafel* angeben.

Beispiel: Betrachte $M = \mathbb{Z}_m = \{0, 1, \dots, m-1\}$ mit der Addition $+$ modulo m als Verknüpfung. Für $m = 3$ ergibt sich folgende Tafel:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Konvention: “Zeile mal Spalte” (egal bei Kommutativität)

Ablezen von Eigenschaften anhand einer Verknüpfungstafel

Da die mit der 0 indizierte Zeile bzw. Spalte die Grundelemente in der “richtigen Reihenfolge” aufzählt, ist 0 das neutrale Element von $+$.

Die Abgeschlossenheit ist offenbar (warum?),

und die Assoziativität kann man durch erschöpfende Analyse aller Fälle nachrechnen, z.B.:

$$(1 + 2) + 2 = 0 + 2 = 2 = 1 + 1 = 1 + (2 + 2).$$

Mengenoperationen als Halbgruppenoperationen

Es sei X eine Menge. Dann bezeichnet 2^X *Potenzmenge* von X , d.i. die Menge der Teilmengen von X .

Beispiel: Ist $X = \{0, 1, 2\}$, so ist $2^X = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, X\}$.

Satz: Für jede Menge X sind

$$(2^X, \cup, \emptyset)$$

und

$$(2^X, \cap, X)$$

Monoide.

Abbildungen

Es seien X, Y nicht-leere Mengen.

Eine **Abbildung** (oder **Funktion**) $f : X \rightarrow Y$ ist eine Vorschrift, die jedem Element aus X höchstens ein Element aus Y zuordnet.

In dieser Vorlesung werden Abbildungen stets **total** sein, d.h., jedem Element aus X wird genau ein Element aus Y zugeordnet.

In diesem Sinne ist dann Y^X die Menge aller Abbildungen von X nach Y .

Hintereinanderausführung von Abbildungen

Sind $f : X \rightarrow Y$ und $g : Y \rightarrow Z$ Abbildungen, so ordnet

ihre **Hintereinanderausführung** (oder **Komposition**) $g \circ f : X \rightarrow Z$

(beachte das "Vertauschen" von g und f in der Schreibweise)

einem $x \in X$ dasjenige Element $z \in Z$ zu, das sich durch $z = g(f(x))$ ergibt, i.Z.: $g \circ f : X \rightarrow Z, x \mapsto g(f(x))$.

Satz: $(X^X, \circ, \text{id}_X)$ ist ein Monoid, wobei $\text{id}_X(x) = x$ für alle $x \in X$ gilt (**Identität**).

Zur Quellenlage

Vieles finden Sie natürlich heutzutage im Internet.

Vorsicht: Noch mehr als bei Gedrucktem gilt: Nicht alles, was im Internet steht, ist deshalb richtig. Seien Sie ein kritischer Leser.

Das Internet ist zudem auch schlechter zitierbar: Auf welche Version eines Wikipedia-Artikels beziehe ich mich ?!

Immer noch besser: die gute alte Bibliothek, siehe Führung

Speziell:

F. L. Bauer: Trits and Trytes—Ein früher ternärer Computer in der Sowjetunion. Informatik Spektrum 30 (2007), 279–284.

J. Mason, L. Burton, K. Stacey: Mathematisch denken; Mathematik ist keine Hexerei. Oldenbourg Verlag, 4. Auflage, 2006.