Kapitel 1

Grundlagen

Medaillon aus Archimedes:
Werke, ed. J. Torelli. 1792

δος μοι που στω
και κινησω την γην.

Gib mir einen Punkt, wo ich stehen kann,
und ich werde die Erde aus den Angeln heben.

Archimedes von Syrakus (∼287–212 v.u.Z.),
mathematisches Jahrtausendgenie und eines der ersten Opfer der Mathematik („Noli perturbare circulos meos“).

Wir wollen in diesem Paragraphen einige Werkzeuge kennenlernen, die wir brauchen, um unsere Aussagen und Beweise so fassen zu können, daß sie den heutzutage üblichen wissenschaftlichen Standards genügen. Dabei geht es hier nur um „Sprechweisen“ (Nomenklatur). Die Prinzipien des Schließens werden beileibe nicht erschöpfend dargestellt (das bleibt der Disziplin der mathematischen Logik überlassen und ist nichts für Anfänger!), die Probleme der Axiomatik der Mengenlehre werden nur angerissen.

Erst seit Mitte des vorigen Jahrhunderts bemühen sich die Mathematiker um eine exakte Grundlegung ihrer Wissenschaft (Boole, Frege, Hilbert, Russell, Gödel, ...), wohl infolge der Erschütterungen, die die Entdeckung der Nichteuklidischen Geometrien nach sich zog. Seither hat die Mathematik auch ihren Charakter geändert. Aus einer Disziplin von Zahl und Raum wurde sie zur Theorie der Strukturen – zu einer Wissenschaft, die aus vorgegebenen Axiomen Folgerungen zieht.

Demgemäß wird heutzutage in mathematischen Vorlesungen der Stoff nach der axiomatischen Methode (vgl. S. 12 ff) präsentiert, wenn auch gewöhnlich nicht voll formalisiert. Ersteres fasziniert und verwirrt Anfänger bzw. -innen gleichermaßen. Daher sind einige Warnungen angebracht.

Das axiomatische Vorgehen erweckt den Eindruck, als ob jede mathematische Disziplin (z.B. die Lineare Algebra) eine Kette aus Definitionen und Sätzen sei und als ob die Mathematiker in ihren Schöpfungen weitestgehend „frei“ seien. So gibt es die Meinung, daß die platonische Auffassung von Mathematik (wonach mathematische Gegebenheiten außerhalb der menschlichen Vorstellung existieren, also vom menschlichen Geist entdeckt werden und nicht von ihm erschaffen) durch die moderne Entwicklung obsolet geworden sei.

Wenn jedoch logisches Denken und mathematisches Schließen nichts anderes als unter dem Anpassungsdruck der Evolution erworbene Fähigkeiten der menschlichen Spezies sind, so löst sich der sonst so gerne unversöhnlich aufgebaute Gegensatz „entdecken – schaffen“ (Platonismus – Nominalismus) auf und gleichzeitig löst sich das Rätsel, warum die vom Menschen „geschaffene“ Mathematik sich so wundervoll zur Beschreibung der Welt eignet, warum Mathematik sich anwenden läßt.

Die immer wieder prinzipiell gestellte Frage nach der Anwendbarkeit moderner mathematischer Theorien erhält somit eine überraschend einfache Antwort: Der Selektionsdruck der Evolution hat der Spezies Mensch mit der Fähigkeit zu Logik und Mathematik offensichtlich ein sehr gut an die Realität angepaßtes Vermögen beschert, und mit dem Erschaffen mathematischer Realität erfolgt daher eben nichts anderes als das Wiederentdecken zugrundeliegender Realität.

Oft können wir den Realitätsbezug einer mathematischen Theorie erst relativ spät nach ihrer Ausformulierung erkennen (Die Geschichte zeigt uns viele interessante Beispiele: Nichteuklidische Geometrien, Gruppentheorie, Theorie der endlichen Körper, Tensorkalkül, Knotentheorie, Primzahltheorie). Die Beschäftigung mit Primzahlen zum Beispiel – insbesondere die Frage nach großen Primzahlen – galt lange Zeit als eine Disziplin für Sonderlinge, bis sie im letzten Viertel unseres Jahrhunderts große Relevanz erlangte: Abgesehen davon, daß man neue Generationen von Superrechnern gern auch insoweit testet, daß man den Rekord für die größte bekannte Primzahl zu brechen sucht[1], sind große Primzahlen heute in der Kryptologie für gewisse sehr sichere Verschlüsselungsverfahren wichtig – zur heutigen Zeit der Kommunikation in globalen Netzwerken von vitalem Interesse für die Wirtschaft.

Da es die Aufgabe der Informatiker ist, Prozesse des logischen Schließens, Algorithmen und Datenstrukturen auf Maschinen zu implementieren, ist für sie natürlich jegliche Art von Mathematik von Interesse. Dennoch gibt es einen Grundkanon dessen, was ein Naturwissenschaftler heutzutage an Mathematik kennengelernt haben sollte.

Was die Präsentation von Mathematik in Gestalt des Schemas „Axiome, Definitionen, Theoreme, ... “ angeht, so darf diese Darstellungsform nicht für das Ganze gehalten werden. Definieren heißt begrenzen, ausgrenzen, aussondern oder „feststellen“ (letzteres durchaus in des Sinnes wörtlicher Bedeutung). Der Verstand setzt also – um einmal bei der platonischen Sichtweise zu bleiben – in der Welt mathematischer Sachverhalte Fixpunkte so, wie der Bergsteiger Eisen in den Fels schlägt. Die gesetzten Haltepunkte (Axiome, Definitionen, Theoreme, ...) sind bis zu einem bestimmten Grade eine willkürliche Auswahl aus der Gesamtheit aller Möglichkeiten. Wo ich meine Eisen einschlage, ist in gewissem Sinne willkürlich, erfolgt aber angepaßt an die mathematische Topographie. Die Eindimensionalität der Zeit erweckt den Eindruck einer Kette. In Wirklichkeit entsteht ein (vieldimensionales) Netz von Fixpunkten (den Knotenpunkten) und Relationen (den Fäden des Netzes), das über das mathematische Substratum gelegt wird (relationaler Beziehungszusammenhang).

Das durch die axiomatische Methode gelieferte Bild ist also ein Teilbild der mathematischen Wirklichkeit, wie es durch das Netz mit seinen Knotenpunkten geliefert wird. Wir präsentieren einen historisch gewachsenen Kanon. Schließlich halten sich die Bergsteiger gewöhnlich auch an die von den Vorgängern eingeschlagenen Eisen. Wichtig ist es, möglichst viel in dem Netz herumzuwandern (das Bergsteigen zu üben!).

[1]Mersenne-Primzahl z.B. $2^{3021377} - 1$.
Info http://www.utm.edu/research/primes/largest.html

1.1 Mathematische Logik

Die formale Logik befaßt sich mit **Aussagen** (das sind deklarierende, sinntragende Zeichenfolgen, die eine Bedeutung, den sog. **Wahrheitswert**, tragen) – mit ihrer Struktur und mit dem Umgang mit ihnen (Schlußregeln). In der zweiwertigen Logik kommt jeder Aussage entweder der Wahrheitswert W (wahr) oder F (falsch) zu (Kontradiktion, tertium non datur). Diese Auffassung entspricht auch der klassischen Logik, wie sie etwa im Organon des Aristoteles (384–322 v.u.Z.) oder – noch pointierter – in den Werken der megarisch-stoischen Schule niedergelegt ist.

Beispiele für Aussagen:

1. Jeder Vogel kann fliegen. F

2. $3^2 + 4^2 = 5^2$ W

3. $4^2 + 5^2 = 6^2$ F

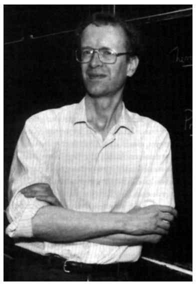
4. Wenn n eine natürliche Zahl größer als 2 ist, so gibt es kein Tripel x, y, z ganzrationaler, von Null verschiedener Zahlen mit $x^n + y^n = z^n$. (Satz von Fermat-Wiles) [2] W

5. Jede von 2 verschiedene gerade natürliche Zahl ist Summe zweier Primzahlen. (Goldbachsche Vermutung) W?F?

Der Wahrheitswert der letzten Aussage ist nicht bekannt.[3] Dennoch wird in der zweiwertigen Logik davon ausgegangen, daß „im Grunde“ feststeht, ob die Aussage wahr oder falsch ist. Keine Aussagen sind z.B. Fragen oder Befehle.

---

[2] Diese (erst im Nachlaß gefundene) Aussage wurde von Pierre de Fermat (1601-65) auf den Rand seines Diophant-Exemplars notiert mit dem Zusatz, er habe einen wahrhaft wundervollen Beweis dafür gefunden, aber der Rand sei dafür zu klein. Es war eine Sensation, als Andrew Wiles (⋆1953) diese sog. große Fermatsche Vermutung endlich 1994 beweisen konnte (publiziert in Ann. of Math. 41 (1995)). Die Akademie der Wissenschaften zu Göttingen verwaltete für einen für die Lösung 1906 ausgesetzten Preis von 100000 Goldmark (3 Mio. DM nach heutiger Kaufkraft), der nach Abwertungen jetzt noch mit 75000 DM valutierte und am 27.06.1997 überreicht wurde.



Andrew Wiles

[3] Bisher bewiesen: ... als Summe von höchstens 67 Primzahlen darstellbar.

Es gibt auch Bestrebungen, mehrwertige Logiken zu entwickeln.[4] Versuche, diese Logiken praktisch anzuwenden, waren bisher haupsächlich im Falle der **Fuzzy-Logik** erfolgreich. (In der Fuzzy-Logik arbeitet man statt mit zwei diskreten Wahrheitswerten W, F mit einem ganzen Kontinuum gewichteter Wahrheitswerte.)[5]

Für den konkret forschenden Mathematiker oder Naturwissenschaftler ist aber die Zweckmäßigkeit das entscheidende Kriterium. Daher wird Mathematik immer noch nahezu ausschließlich nach der zweiwertigen Logik betrieben.

Der einfachste Part der formalen Logik ist der sogenannte **Aussagenkalkül.**[6] Hier werden neben den Aussagen auch **Aussagenvariable** behandelt. Die Aussagenvariablen sind Statthalter für beliebige Aussagen, die an Stelle der Variablen eingesetzt werden können; so, wie in

$$x^2 - y^2 = (x + y)(x - y)$$

für die arithmetischen Variablen x, y jede beliebige reelle Zahl eingesetzt werden kann. Aussagenvariable und/oder Aussagen können durch Verwendung von Junktoren zu **Ausdrücken (Formeln, Aussagenverbindungen)** kombiniert werden, welche ihrerseits mittels Junktoren weiter verknüpft weden können. Die **Junktoren**[7] (Verknüpfungszeichen) werden folgendermaßen über Wahrheitstafeln eingeführt:

Seien A, B Formeln.

---

[4] Erste Versuche 1920 von Lukasiewicz. Vgl. J.B. Rosser - A.R. Turquette: Many valued logics. Amsterdam 1952. Anwendung der dreiwertigen Logik auf die Quantenmechanik zuerst 1944 durch Hermann Reichenbach, der die in der Quantentheorie auftretende Unbestimmtheit durch den Wahrheitswert „unbestimmt“ zu beschreiben suchte. Jedoch scheint das nicht hinreichend allgemein, da die Wahrscheinlichkeitsrechnungen der Quantentheorie nicht zu 3 diskreten Wahrheitswerten passen. Wiederum vertrat U. Blau die Meinung, daß nur eine dreiwertige Logik unserem intuitiven Denken gerecht werden kann (Papiere zur Linguistik 4, 1973: Dreiwertige Sprachanalyse und Logik, 1974).

[5] Jedoch nutzt z.B. das Computeralgebra-System Maple die dreiwertige Logik mit dem dritten Wahrheitswert FAIL, der zurückgegeben wird, wenn eine Prozedur das Problem nicht vollständig lösen kann.

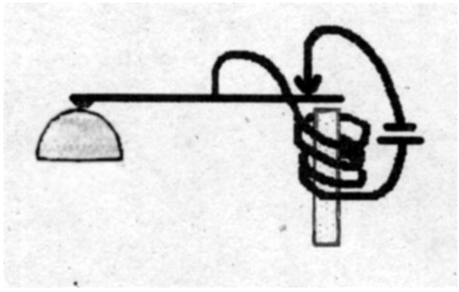
[6] Das Wort Kalkül rührt von „calculi“ her, der lat. Bezeichnung für Rechensteinchen. Ein Kalkül erfordert, daß die Zeichenfolgen eindeutig erkannt und gemäß den Regeln des Kalküls mechanisch verarbeitet werden können.

[7] Einige Junktoren treten in Programmiersprachen als Operatoren auf. Z.B. in C: $\neg$ als `!`, $\wedge$ als `&&`, $\vee$ als `||`.

<table>
<tr><th>Bezeichnung</th><th>Zeichen</th><th>Wahrheitstafel</th><th>Sprechweise</th></tr>
<tr><td>Negation</td><td>$\neg A$</td><td>$\begin{array}{c|c} A & \neg A \\ \hline W & F \\ F & W \end{array}$</td><td>Non A; A gilt nicht; es ist nicht wahr, daß A gilt.</td></tr>
<tr><td>schwache Disjunktion; einschließendes (schwaches) Oder</td><td>$A \vee B$</td><td>$\begin{array}{cc|c} A & B & A \vee B \\ \hline W & W & W \\ W & F & W \\ F & W & W \\ F & F & F \end{array}$
Kurzform: $\begin{array}{c|cc} \vee & W & F \\ \hline W & W & W \\ F & W & F \end{array}$</td><td>$A$ gilt oder B gilt oder beides gilt; A oder B oder beides.</td></tr>
<tr><td>strenge Disjunktion; ausschließendes Oder</td><td>$A \sqcup B$</td><td>$\begin{array}{c|cc} \sqcup & W & F \\ \hline W & F & W \\ F & W & F \end{array}$</td><td>Entweder A oder B.</td></tr>
<tr><td>Konjunktion</td><td>$A \wedge B$</td><td>$\begin{array}{c|cc} \wedge & W & F \\ \hline W & W & F \\ F & F & F \end{array}$</td><td>$A$ gilt und B gilt; A und B.</td></tr>
<tr><td>logische Äquivalenz</td><td>$A \leftrightarrow B$</td><td>$\begin{array}{c|cc} \leftrightarrow & W & F \\ \hline W & W & F \\ F & F & W \end{array}$</td><td>Mit A gilt auch B und umgekehrt; genau wenn A, so B; A dann und nur dann, wenn B; A ist hinreichend und notwendig für B.</td></tr>
<tr><td>Implikation</td><td>$A \to B$</td><td>$\begin{array}{c|cc} \to & W & F \\ \hline W & W & F \\ F & W & W \end{array}$</td><td>Wenn A, so B; mit A ist auch B wahr; A ist hinreichend für B; B ist notwendig für A; A höchstens dann, wenn B.</td></tr>
</table>

Achtung: Bei $A \to B$ braucht B nicht aus A ableitbar zu sein, wenn dies auch die oft benutzte Sprechweise „Aus A folgt B" zu suggerieren scheint!

Die Implikation ist auch sehr zu unterscheiden vom Kausalzusammenhang. Betrachten wir das Modell einer Klingel, die Aussagen A: „Es fließt Strom.", B: „Der Magnet unterbricht durch Anziehung der Metallzunge den Stromkreis." sowie die durch das Modell offensichtlich als richtig erwiesenen Aussagen:



1. Wenn Strom fließt, so unterbricht der Magnet durch Anziehung der Metallzunge den Stromkreis.
2. Wenn der Magnet durch Anziehung der Metallzunge den Stromkreis unterbricht, so fließt kein Strom.

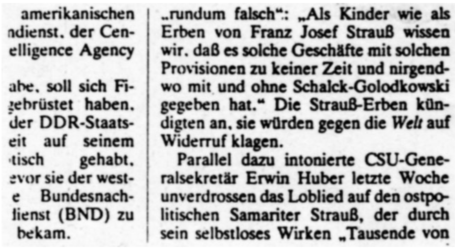
Also würde gelten $A \to B$ und $B \to \neg A$ und somit (siehe unten modus Barbara) $A \to \neg A$. Demnach wäre die Aussage falsch, im Widerspruch zur Realität.

Sie haben den Fehler natürlich sofort bemerkt! Es handelt sich hier um Ursache und Wirkung. Diese beziehen sich auf Vorgänge, die in der Zeit ablaufen. Das „wenn ... so" bedeutet also keine Gleichzeitigkeit wie bei der logischen Implikation.

In der Mathematik verwenden wir die Junktoren präzise so, wie oben definiert. Es gibt sicherlich Unterschiede zwischen dem Sprachgebrauch im täglichen Leben und dem in der mathematischen Logik. Einige Beispiele:

1. Jemand erbittet von seinem Freund, welcher jede Woche an genau einem Nachmittag in der Werkstatt seines Vaters mithilft, als Freundschaftsdienst die dringend nötige Behebung eines Defekts am Auto und fragt ihn: „Wann bist Du wieder in der Werkstatt?" Antwort: „Ich bin heute oder morgen oder übermorgen dort." Wird diese Antwort im Alltagsleben als wahr angesehen werden, wenn der Antwortende im Augenblick der Antwort schon genau weiß, daß er zu keinem anderen Zeitpunkt als morgen in der Werkstatt sein wird?
2. Eine Erbengemeinschaft gab der Öffentlichkeit gegenüber folgende Stellungnahme ab:

„Als Kinder wie als Erben von Franz Josef Strauß wissen wir, daß es solche Geschäfte mit solchen Provisionen zu keiner Zeit und nirgendwo mit und ohne Schalck-Golodkowski gegeben hat.“ Zeugt diese Verlautbarung nun von logischem Unvermögen oder von bewußtem Mißbrauch der Sprache zum Zwecke der Verschleierung des Sinns der Aussage?


amerikanischen ndienst, der Centelligence Agency abe, soll sich Fi- gebrüstet haben, der DDR-Staats- eit auf seinem tisch gehabt, evor sie der west- e Bundesnach- lienst (BND) zu bekam.

„rundum falsch“: „Als Kinder wie als Erben von Franz Josef Strauß wissen wir, daß es solche Geschäfte mit solchen Provisionen zu keiner Zeit und nirgendwo mit und ohne Schalck-Golodkowski gegeben hat.“ Die Strauß-Erben kündigten an, sie würden gegen die *Welt* auf Widerruf klagen.

Parallel dazu intonierte CSU-Generalsekretär Erwin Huber letzte Woche unverdrossen das Loblied auf den ostpolitischen Samariter Strauß, der durch sein selbstloses Wirken „Tausende von

Ausriß aus Der Spiegel 34/1991, p.19

3. Es fällt ohne streng formale Betrachtungsweise schwer, die Aussage „Wenn der Imperator nicht sterblich ist, so ist der Imperator sterblich.“ als wahr anzusehen.

Übrigens stand und steht die Definition der Implikation über die von uns abgedruckte Wahrheitstafel seit eh und je im Kreuzfeuer der Kritik von Philosophen und Logikern. Anlaß zur Kritik bildete unter anderem auch die Zeitabhängigkeit des Wahrheitswertes der folgenden Aussage: „Wenn Daniela lustig ist, so ist sie nicht lustig.“ (Zu allen Zeiten, zu denen Daniela lustig ist, ist die Aussage falsch. Zu den Zeiten, zu denen Daniela nicht lustig ist, ist sie wahr!) Möglicherweise erlaubt es unser Implikationsbegriff auch nicht, gewisse Probleme adäquat zu behandeln. In einer zweiwertigen Logik muß die Implikation jedoch notwendig so definiert werden, denn von den 2^4 kombinatorischen Möglichkeiten für die Wahrheitstafeln kommt unsere Wahl dem, was intuitiv als Implikation angesehen wird, am nächsten.

Eine Formel, die stets den Wahrheitswert W hat, heißt eine **Tautologie**. Durch Einsetzen aller möglichen Wahrheitswerte für A, B, C sind die folgenden Ausdrücke leicht als Tautologien zu verifizieren:

(Dabei gilt folgende **Rangfolge der Junktoren**: $\neg$ bindet stärker als $\vee$, $\wedge$, und letztere binden stärker als $\rightarrow$, $\leftrightarrow$. Von dieser Konvention abweichende Bindungen werden durch Klammern realisiert.)

1. $A \vee \neg A$ (**Tertium non datur**. Schlechter Name, der erst mit der folgenden Tautologie Sinn macht.)
2. $\neg(A \wedge \neg A)$ (**Gesetz vom Widerspruch, Kontradiktion**)
3. $(A \rightarrow B) \wedge (B \rightarrow C) \rightarrow (A \rightarrow C)$ (**Syllogismus, Modus Barbara**)
4. $A \leftrightarrow \neg(\neg A)$ (**Gesetz der doppelten Negation**)

5. $(A \to B) \leftrightarrow (\neg B \to \neg A)$ (**Gesetz der Kontraposition**)
6. $A \wedge (A \to B) \to B$ (**Modus ponendo ponens**)
7. $A \wedge \neg A \to B$ (**Ex falso quodlibet, Duns-Scotus-Regel**)
8. $(A \to A \wedge \neg A) \to \neg A$ (**Reductio ad absurdum**)
9. $\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$ (**De Morgansche Gesetze**)
10. $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$

Übung: Welche der folgenden drei Formeln sind Tautologien?

$$A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C) \quad ,$$
$$(\neg B \to A \wedge \neg A) \to B \quad ,$$
$$(A \wedge \neg B \to C \wedge \neg C) \leftrightarrow (A \to B) \quad .$$

Die beiden folgenden Tautologien zeigen, daß wir eigentlich nur die beiden Junktoren $\neg$ und $\vee$ benötigen:

$$(A \to B) \leftrightarrow \neg A \vee B \quad ,$$

$$A \wedge B \leftrightarrow \neg(\neg A \vee \neg B) \quad .$$

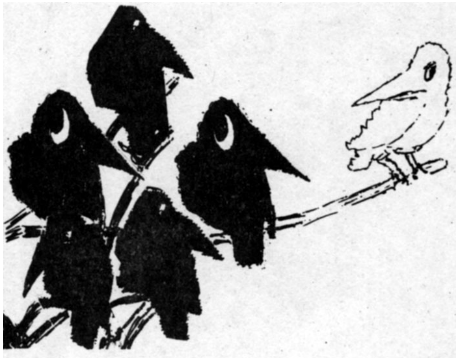
Bemerkung: Definitionen erfolgen mit Hilfe der logischen Äquivalenz nach dem Schema Definiendium (Das neu zu Definierende) $:\leftrightarrow$ Definiens (Die definierende Aussage). Der Doppelpunkt wird auf die Seite des Definiendums geschrieben (Beispiel: Definitionen 1.1, S.17). Steht jedoch ausdrücklich „Definition:“ davor, so wird auch öfter salopper „... heißt ..., wenn ...“ statt „... heißt ..., genau wenn ...“ formuliert.

Der Aussagenkalkül ist noch sehr grob; denn er regelt nur die Verknüpfung von Aussagen zu Formeln. Er befaßt sich aber überhaupt nicht mit der Feinstruktur der Aussagen, wie es sogar schon in der Aristotelischen Logik zu finden ist. Typische „Aussagen“ sind doch: „Alle Menschen sind sterblich.“, „7 ist eine Primzahl.“, „$\pi < 5$“, aber auch „Für alle $x \in \mathbb{R}$, $x > 0$, existiert $y \in \mathbb{R}$ mit $x = y^2$ “.

Daher wird der Aussagenkalkül zum sog. **(engeren) Prädikatenkalkül** erweitert, der den Umgang mit speziellen sprachlichen Gebilden regelt.

Aussageformen oder **Aussagefunktionen** sind Gebilde vom Typ „x ist ein Rabe“, kurz geschrieben als $R(x)$, „x ist schwarz“, kurz geschrieben als $S(x)$. (Das sind keine Aussagen, da es keinen Sinn macht, von Wahr oder Falsch zu reden.) x heißt eine **Individualvariable**, R heißt eine **Prädikatsvariable**.

Zu den Verknüpfungen des Aussagenkalküls kommen noch zwei **Quantoren** hinzu: $\bigvee$ und $\bigwedge$ (oft auch als $\exists$ bzw. $\forall$ geschrieben). $\bigvee\limits_x R(x)$ ist eine Schreibweise für „Es gibt ein x mit dem Prädikat R", also für „Es gibt ein x so, daß gilt: x ist ein Rabe." $\bigvee$ (bzw. $\exists$) heißt **Partikularisator**. Analog wird der **Generalisator** $\bigwedge$ (bzw. $\forall$) „für alle " gebraucht.



$\bigwedge_x [R(x) \to S(x)]$???

Drei wichtige gültige Formeln des Prädikatenkalküls sind:

$$\neg \bigwedge_x P(x) \leftrightarrow \bigvee_x \neg P(x) \quad ,$$

$$\neg \bigvee_x P(x) \leftrightarrow \bigwedge_x \neg P(x) \quad ,$$

$$\bigvee_x \bigwedge_y P(x,y) \to \bigwedge_y \bigvee_x P(x,y) \quad .$$

Übung: Machen Sie sich die Formeln anhand von Beispielen klar, insbesondere auch, daß die letzte Formel keine Äquivalenz ist (Wichtig später für das Verständnis des Unterschiedes zwischen Konvergenz und gleichmäßiger Konvergenz).

Vielbenutzte Quantoren der Sprache, wie „für fast alle", „für die meisten", …, werden hingegen in der klassischen mathematischen Logik nicht verwandt. Die bei den Quantoren stehenden Individualvariablen heißen **gebundene Variablen**, während die anderen Individualvariablen **freie Variablen** heißen.[8] Prädikate können natürlich mehrere Individualvariablen auf-

[8]Der engere Prädikatenkalkül wird oft erweitert, indem auch gebundene Prädikatsvariablen zugelassen werden, z.B. zwecks Definition der Gleichheit $a = b :\leftrightarrow \bigwedge\limits_x F(a) = F(b)$ (Gleichheit im Sinne universeller Vertretbarkeit). Jedoch hat Bernays eine für die Zwecke der Mathematiker hinreichende axiomatische Einführung der Zermelo-Fraenkelschen Mengenlehre auf der Basis des engeren Prädikatenkalküls mit ι-Symbol gegeben.

weisen, geschrieben dann als $P(x_1, x_2, \ldots, x_n)$.
Beispiel: $K(x, y)$ für „x ist kleiner als y“.

Ein Problem des Prädikatenkalküls liegt darin, daß ein entsprechendes Universum von Individuen vorausgesetzt wird, auf die sich die Aussagenvariablen beziehen. Wenn das Universum aus endlich vielen Individuen besteht, geht der Prädikatenkalkül nicht über die Aussagenlogik hinaus.

1.2 Die axiomatische Methode

Eine **formale mathematische Theorie** ist ein geeigneter logischer Kalkül (meist der engere Prädikatenkalkül mit dem Begriff der Identität (d.i. Gleichheit im Sinne universeller Vertretbarkeit), eventuell noch mit dem ι-Symbol[9]), der durch spezielle Symbole für besondere Individuen, Prädikate oder Aussageformen erweitert ist[10], zusammen mit sogenannten **Axiomen**, in denen diese Symbole vorkommen. (Vgl. G.T. Kneebone: Mathematical Logic and the foundations of mathematics. London 1963.) Ferner muß festgelegt werden, welche Formeln **einschlägig** (wohlgebildet) sind und welche **Ableitungsregeln** angewendet werden dürfen.

Seien $P_1, P_2, \ldots, P_n$ einschlägige Aussagen der formalen Theorie, die sog. **Prämissen** oder **Voraussetzungen**, und sei B eine zu beweisende **Behauptung**.

(i) Ein **formaler (direkter) Beweis** für das **Theorem**:
„Mit $P_1, P_2, \ldots, P_n$ gilt auch B“ besteht aus einer Folge (gewöhnlich untereinander geschriebener) einschlägiger Formeln $F_1, F_2, \ldots, F_k$ mit $F_k = B$, wobei jede Formel F_i eine Prämisse oder ein Axiom ist oder aus vorhergehenden Formeln F_j $(j < i)$ durch Anwendung einer der Ableitungsregeln entstanden ist.

(ii) Ein **formaler indirekter Beweis** für den obigen Satz beginnt mit n Zeilen mit den Prämissen $P_1, P_2, \ldots, P_n$. In der $(n+1)$-ten Zeile steht $\neg B$. Dann folgen weitere Beweiszeilen, die wie bei einem formalen direkten Beweis, also eventuell unter Verwendung vorheriger Zeilen, entstanden sind. Sobald einmal zwei Zeilen mit den Formeln Z und $\neg Z$ aufgetreten sind (**Widerspruch**), ist der indirekte Beweis vollendet ($\neg B$ kann nicht wahr sein).

[9] Wenn eine Eigenschaft E durch ein Prädikat $P(x)$ dargestellt wird, so bedeutet $\iota_x P(x)$ „das Individuum mit der Eigenschaft E“

[10] Im Axiomensystem der Mengenlehre sind zum Beispiel $\in$ und $\{\ :\ \}$ solche Symbole.

Beispiel (für einen indirekten Beweis):
Behauptung: $\sqrt{2}$ ist nicht rational (Aussage B).
Annahme: $\sqrt{2} = \frac{a}{b}$ (a, b ganzrational; Bruch sei durchgekürzt).
Dann ist $a^2 = 2b^2$, a also gerade, d.h. $a = 2c$. Mithin ist $4c^2 = 2b^2$, also auch b gerade. Also ist $\frac{a}{b}$ nicht durchgekürzt. Widerspruch! $\square$

Als **Beispiel** für eine formale mathematische Theorie führen wir 4 Axiome und 2 Ableitungsregeln ein, mit denen Hilbert und Ackermann den Aussagenkalkül formalisierten.

Axiome:

(i) $\neg(A \vee A) \vee A$

(ii) $\neg A \vee (A \vee B)$

(iii) $\neg(A \vee B) \vee (B \vee A)$

(iv) $\neg(\neg A \vee B) \vee (\neg(C \vee A) \vee (C \vee B))$

Ableitungsregeln:

(I) Von zwei Formeln F_1 und $F_1 \to F_2$ darf zur Formel F_2 übergegangen werden, symbolisch geschrieben:

$$\frac{\begin{array}{l} F_1 \\ F_1 \to F_2 \end{array}}{F_2}$$

(Modus ponendo ponens)

(II) Für jede Variable, die in einer gegebenen Formel auftritt, ist folgende Substitution zulässig: X wird überall, wo es auftritt, durch eine beliebige, aber festgewählte, einschlägige Formel F ersetzt, geschrieben: $F|X$. (Substitutionsregel)

Zunächst ist es sicher nützlich, die Implikation mittels der Definition $(A \to B) :\leftrightarrow \neg A \vee B$ einzuführen und die Formeln der Axiome in einer „anschaulicheren“ Version zu schreiben: (i) $A \vee A \to A$, (ii) $A \to A \vee B$, (iii) $A \vee B \to B \vee A$, (iv) $(A \to B) \to (C \vee A \to C \vee B)$. Die Substitution $\neg C|C$ in (iv) zeigt die Gültigkeit von $(A \to B) \to ((C \to A) \to (C \to B))$ und (I) zweimal hierauf angewendet liefert die so formal deduzierte Ableitungsregel

$$\frac{\begin{array}{l} C \to A \\ A \to B \end{array}}{C \to B}$$

(Modus Barbara)

Als Beispiele für formale Beweise mögen die Deduktion des „tertium non datur“ und des Satzes von der doppelten Negation dienen:

Satz: $A \vee \neg A$
Beweis:

1. $A \to A \vee A$ — (ii) und $A|B$
2. $A \vee A \to A$ — (i)
3. $A \to A$ — Modus Barbara
4. $\neg A \vee A$ — Definition von $\to$
5. $\neg A \vee A \to A \vee \neg A$ — (iii) und (II)
6. $A \vee \neg A$ — (I) bezügl. 4. und 5.

Satz: $A \leftrightarrow \neg\neg A$
Beweis:

1. Ann.: $\neg((A \to \neg\neg A) \wedge (\neg\neg A \to A))$
2. $\neg\neg(\neg(A \to \neg\neg A) \vee \neg(\neg\neg A \to A))$ — (Definition von $\wedge$)
3. $A \vee \neg A$ — voriger Satz
4. $\neg A \vee \neg\neg A$ — $\neg A|A$ in voriger Zeile
5. $A \to \neg\neg A$ — Definition von $\to$
6. $\neg A \to \neg\neg\neg A$ — $\neg A|A$ in voriger Zeile
7. $(A \vee \neg A) \to (A \vee \neg\neg\neg A$ — $\neg A|A$, $\neg\neg\neg A|B$, $A|C$ in (iv) und (I)
8. $A \vee \neg\neg\neg A$ — (I)
9. $\neg\neg\neg A \vee A$ — (iii) mit Substitution und (I)
10. $\neg\neg A \to A$ — Definition von $\to$
11. $\neg(A \to \neg\neg A) \vee \neg(\neg\neg A \to A)$ — (I) bezogen auf 2. Zeile und letzte Zeile mit entsprechender Substitution
12. $(A \to \neg\neg A) \to \neg(\neg\neg A \to A)$ — Definition von $\to$
13. $\neg(\neg\neg A \to A)$ — (I)

14. Widerspruch zur Aussage 3 Zeilen höher! □

Während die Beweisführung im ersten Satz voll formalisiert ist, sind beim Beweis des zweiten Satzes für die Etablierung einer neuen Zeile bisweilen mehrere Beweisschritte zusammengefaßt. Formale Beweise zu führen ist schrecklich umständlich und mühsam, auch werden sie für unseren menschlichen Verstand eher undurchsichtig. Die Situation erinnert an die Unterschiede, die zwischen der korrekten Beschreibung eines Algorithmus in freier Sprache (erster Schritt beim Programmieren) und dem vollständigen Quell-Code eines Computerprogramms bestehen. Bei formalen Beweisen muß im Prinzip ein Computer prüfen können, ob die Beweise richtig sind. Die praktizierenden Mathematiker begnügen sich mit einer teilweisen Formalisierung – weit weniger als in unserem zweiten Beispiel. Es wird zwar gefordert, daß die mathematische Theorie voll formalisierbar ist, um die Verwendung der Anschauung und die darin liegenden Gefahren auszuschalten, jedoch werden meistens die Ableitungsregeln nicht vollständig formuliert und auch unbewußt angewandt.

Der Stand der Dinge auf dem Gebiet der Computerbeweise ist folgender: Zwar können Computer aus den Prämissen mit Hilfe der Ableitungsregeln neue gültige Formeln in Hülle und Fülle produzieren, aber zu der behaupteten Formel zu gelangen ist nicht so einfach, da Computer ja keine Intuition besitzen. Jedoch ist es dem Computerprogramm EQP (equational power) von Mc Cune in Argonne (Illinois, USA) 1997 gelungen zu beweisen, daß eine Menge, auf der folgende Axiome für die beiden Verknüpfungen $\vee$ und $\neg$ gelten

(i) $A \vee B \leftrightarrow B \vee A \quad ,$

(ii) $(A \vee B) \vee C \leftrightarrow A \vee (B \vee C) \quad ,$

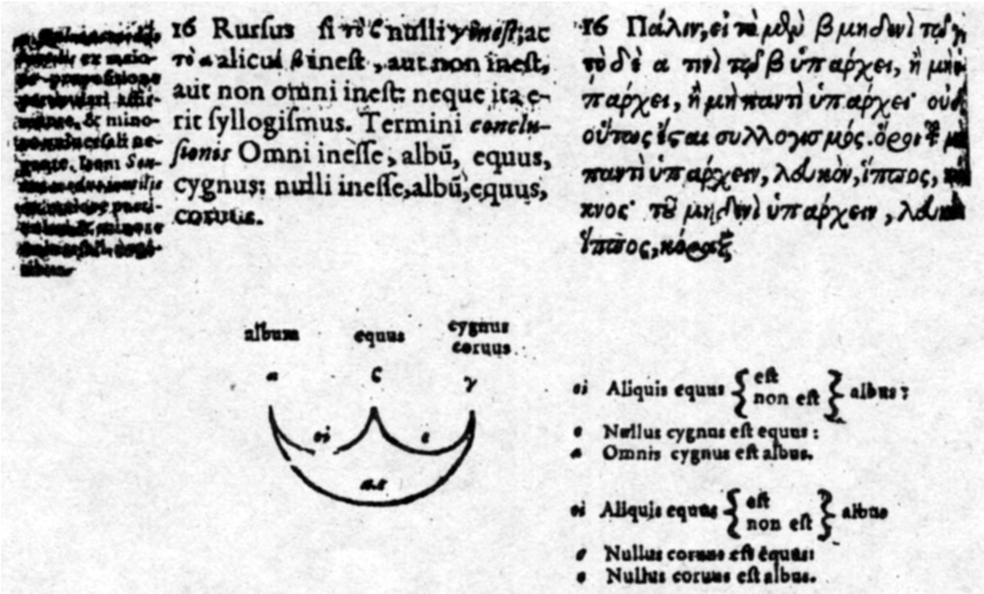
(iii) $\neg(\neg(A \vee B) \vee \neg(A \vee \neg B)) \leftrightarrow A$ (sog. **Robbins-Äquivalenz**).

bereits eine **Boolesche Algebra** ist, ein Beweis, den die Mathematiker seit 60 Jahren vergeblich zu führen suchten.[11]

Die moderne axiomatische Methode mit ihrem Verzicht auf Anschauung gab den MathematikerINNEn sehr viel Bewegungsfreiheit. Es geht nicht um

[11] Der EQP-Beweis, den die Maschine in 8 Tagen schaffte, ist für Menschen schwierig nachvollziehbar, da viele unintuitive, aber sehr komplexe Substitutionen durchgeführt werden. Informationen unter http://www.mcs.anl.gov/home/mccune/ar/robbins/.
Ein Preprint des Mc-Cune-Papiers ist unter ftp://info.mcs.anl.gov/pub/Otter/www-misc/robbins-jar-final.ps.gz erhältlich.

die Frage, ob die Axiome selbst wahr sind, sondern es geht um die Ableitung von Sätzen aus den Axiomen. So ist auch der Ausspruch von Bertrand Russell zu verstehen: „Die reine Mathematik ist jene Disziplin, bei der man weder weiß, worüber man spricht, noch ob das, was man sagt, wahr ist.“ Da unser Text hier für Menschen geschrieben ist, verzichten wir natürlich auf eine vollständig formalisierte Darstellung, eingedenk der Worte von A. Tarski: „Was eine (ergänze: voll formalisierte) Darstellung an Strenge und methodologischer Korrektheit gewinnt, verliert sie an Faßlichkeit und Durchsichtigkeit“. Es ist „nicht vernünftig zu fordern, daß die Beweise in einem gewöhnlichen Lehrbuch in vollständiger Gestalt angegeben werden“.


16 Rursus si τὸ C nulli τῷ B inest; ac τὸ A alicui B inest, aut non inest, aut non omni inest: neque ita erit syllogismus. Termini conclusionis Omni inesse, albũ, equus, cygnus: nulli inesse, albũ, equus, coruus.

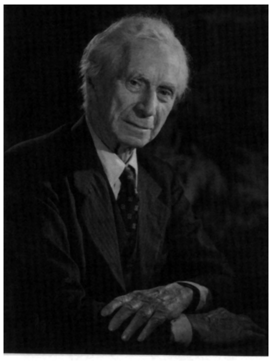
Der berühmte „weiße Rabe “(corvus albus) kommt in den antiken Logik-Lehrbüchern oft vor. Hier aus Aristoteles, Anal. Prior. IV, 16

1.3 Mengen, Relationen, Abbildungen

Die Objekte der Mengenlehre heißen **Klassen**. Es wird ferner mit einer **Elementbeziehung** $\in$ gearbeitet. Wenn a, A Klassen sind, so sagen wir im Falle der Schreibweise $a \in A$ „a ist Element von A“ oder „a ist in A“ oder „a gehört zu A“. Klasse und Elementbeziehung bleiben unerklärte Bausteine des Axiomensystems der Mengenlehre. In diesem Abschnitt bedeuten $A, B, C, \ldots, a, b, c, \ldots$ stets Bezeichnungen für Klassen. Wir treffen die Übereinkunft, daß kleine Buchstaben ausschließlich für Elemente reserviert seien.

Bei der Entwicklung der Mengenlehre stellte sich bald heraus, daß die Cantorsche Definition „Eine Menge ist die Zusammenfassung von wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen“ leider nicht brauchbar ist. Denn diese Definition führte in verschiedene Antinomien, zum Beispiel in die **Russellsche Antinomie**:

Sei M die „Menge“ (im Cantorschen Sinne) aller Mengen, die sich nicht selbst als Element enthalten. Kurzes Nachdenken über die Frage, ob dann M sich selbst als Element enthält, führt zu der Erkenntnis, daß sowohl $M \in M$ als auch $\neg(M \in M)$ gelten muß, was unmöglich sein kann.



B. Russell
(1872 - 1970)

Also mußte der Cantorsche Mengenbegriff aufgegeben werden. Heutzutage werden Mengen als spezielle Klassen definiert (vgl. Def. 1.6].

1.1 Definitionen :

$$A = B :\leftrightarrow \bigwedge_x (x \in A \leftrightarrow x \in B)$$

$$A \subset B :\leftrightarrow \bigwedge_x (x \in A \to x \in B)$$

A heißt im letzteren Fall eine **Teilklasse** von B.

1.2 Extensionalitätsaxiom : $x = y \wedge x \in A \to y \in A$

1.3 Bemerkungen : Es gelten

(i) $A = A$ (Reflexivität der Gleichheit)

(ii) $A = B \to B = A$ (Symmetrie der Gleichheit)

(iii) $A = B \wedge B = C \to A = C$ (Transitivität der Gleichheit)

(iv) $A \subset B \wedge B \subset A \to A = B$

(v) $A \subset B \wedge B \subset C \to A \subset C$

Beweis: Definitionen 1.1 und Extensionalitätsaxiom 1.2

1.4 Komprehensionsaxiom : Sei $P(x)$ eine Aussageform, die vollständig durch $\in$, $\vee$, $\neg$, $\bigvee$, $\bigwedge$, Klammern und Variable ausgedrückt werden kann. Dann existiert eine Klasse, die aus allen Elementen x besteht, für die $P(x)$ gilt, geschrieben: $\{x : P(x)\}$.

Warum werden in 1.4 nur Elemente zugelassen? Um nicht in Antinomien zu geraten; denn $\{A : \neg(A \in A)\}$ wäre genau die Bildung, die zur Russellschen Antinomie führt. Wohl aber ist die Bildung $\{x : \neg(x \in x)\}$ zulässig!

1.5 Satz : Die Klasse $U := \{x : \neg(x \in x)\}$ ist nicht Element einer Klasse.
Beweis: Indirekte Annahme: U ist Element einer Klasse. Es ist entweder $U \in U$ oder $\neg(U \in U)$. Wenn $U \in U$, so ist nach Definition von U aber $\neg(U \in U)$, und wenn $\neg(U \in U)$ gilt, so ist, da U als Element angenommen ist, nach Definition gerade $U \in U$. In jedem Fall ergibt sich also ein Widerspruch. (Wir haben uns also praktisch die Argumentation der Russellschen Antinomie für einen Widerspruchsbeweis von Satz 1.5 zunutze gemacht.)

1.6 Definitionen : Eine Klasse, die Element einer Klasse ist, heißt eine **Menge**. Eine Klasse, die nicht Menge ist, heißt eine **eigentliche Klasse**, **echte Klasse** oder **Unmenge**.

Nach Satz 1.5 ist $\{x : \neg(x \in x)\}$ keine Menge. Also gibt es echte Klassen. Aber gibt es Mengen? Das wird sichergestellt durch:

1.7 Axiom über die leere Menge :
Die **leere Klasse** $\emptyset := \{x : x \neq x\}$ ist eine Menge. Es gilt $\emptyset \subset A$ für alle Klassen A; denn die Aussage $x \in \emptyset \to x \in A$ ist wahr für jedes x.

1.8 Axiom der Paarung :
Wenn a, b Mengen sind, so ist $\{a, b\} := \{x : x = a \vee x = b\}$ eine Menge.

Wenn a eine Menge ist, so ist auch $\{a\} := \{x : x = a\}$ eine Menge; denn es ist offensichtlich $\{a\} = \{a, a\}$, und letzteres ist nach 1.8 eine Menge. Wegen $\{a\} = \{a, a\}$ kommen wir überein, gleiche Elemente zwischen geschweiften Klammern jeweils nur einmal aufzuführen.

1.9 Definitionen : Seien A, B Klassen.

1) $A \cup B := \{x : x \in A \vee x \in B\}$ heißt die **Vereinigung** von A und B.

2) $A \cap B := \{x : x \in A \wedge x \in B\}$ heißt der **Durchschnitt** von A und B.

3) $A \setminus B := \{x : x \in A \wedge \neg(x \in B)\}$ heißt die **Differenz** von A und B.

4) Ist $B \subset A$, so heißt $A \setminus B$ das **Komplement** von B in A, geschrieben $\mathcal{C}_A B$.

5) A, B heißen **disjunkt** oder **zueinander fremd**, wenn $A \cap B = \emptyset$ gilt.

Analog werden Vereinigung und Durchschnitt über eine Klasse $\mathcal{M}$ von Mengen definiert: $\bigcup\limits_{A\in\mathcal{M}} A := \{x : \bigvee\limits_{A\in\mathcal{M}} x \in A\}$; $\bigcap\limits_{A\in\mathcal{M}} A := \{x : \bigwedge\limits_{A\in\mathcal{M}} x \in A\}$.

Für die Begriffe von 1.9 können nun zahlreiche Regeln abgeleitet werden. Zwei oft verwendete sind die **Distributivgesetze**:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad ,$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad .$$

Letzteres folgt zum Beispiel nach Def 1.1 und 1.9 unter Verwendung der 1. Tautologie auf Seite 8....

1.10 Definitionen : $(a, b) := \{\{a\}, \{a, b\}\}$ heißt ein **geordnetes Paar**. $A \times B := \{(a, b) : a \in A \wedge b \in B\}$ heißt das **Cartesische Produkt** der Klassen A und B. Ist $A = \emptyset$ oder $B = \emptyset$, so definieren wir $A \times B = \emptyset$. Allgemein: $M_1 \times M_2 \times \ldots \times M_n =: X_{j=1}^n M_j$ ($=: M^n$, wenn $M_1 = \ldots = M_n = M$).

Beispiel: $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ kann als Menge der Punkte der euklidischen Ebene aufgefaßt werden.

Zusammen mit weiteren Axiomen läßt sich so die Mengenlehre axiomatisch aufbauen. Wer sich dafür interessiert, ziehe dazu Literatur zu Rate. Ein wichtiges Buch auf diesem Feld ist A.A. Fraenkel: Abstract set theory, Amsterdam 1953.

Wahrscheinlich reichen für den Tagesgebrauch in der Mathematik zusätzlich die folgenden Axiome aus:

1) **Axiom der Teilmenge:** Jede Teilklasse einer Menge ist eine Menge.

2) **Axiom der Vereinigung:** Ist $\mathcal{M}$ eine Menge von Mengen, so ist $\bigcup\limits_{A\in\mathcal{M}} A$ eine Menge.

3) **Axiom der Potenzmenge:** Zu jeder gegebenen Menge A existiert die Menge $\mathcal{P}(A)$ aller Teilmengen von A, die sogenannte **Potenzmenge**.

4) **Unendlichkeitsaxiom:** Es existiert eine **Nachfolger-Menge**, d.h. eine Menge, die mit jedem Element A auch ihren **Nachfolger** $A^+ := A \cup \{A\}$ enthält. Dieses Axiom sichert die Existenz der Menge $\mathbb{N}$ der natürlichen Zahlen.

5) **Auswahlaxiom:** Darüber jedoch später Näheres.

Wir arbeiten im Folgenden nur mit Mengen! Uns interessiert also der Unterschied zwischen Mengen und Klassen nicht weiter!

Wir wollen nun noch ausführen, wie die wichtigen Begriffe der Abbildung und der Relation mit Hilfe der Mengentheorie eingeführt werden können:

1.11 Definitionen : Eine **Abbildung** oder **Funktion** f von A nach B ist ein geordnetes Tripel (f, A, B), wobei A, B Klassen sind und $f \subset A \times B$ ist mit folgenden Eigenschaften

(i) $\bigwedge\limits_{x \in A} \bigvee\limits_{y \in B} (x, y) \in f$ (Existenz des Bildes)

(ii) $(x, y) \in f \wedge (x, z) \in f \to y = z$ (Eindeutigkeit des Bildes)

1) x heißt ein **Urbild** von y, y heißt das **Bild** von x. Es ist üblich, $f : A \to B$ statt (f, A, B) und $y = f(x)$ bzw. $f : x \mapsto y$ statt $(x, y) \in f$ zu schreiben. Wir sagen auch: f bildet x auf y ab.

2) A heißt der **Definitionsbereich** von f.

3) Bild $f := f(A) := \bigcup\limits_{x \in A} f(x)$ heißt der **Bildbereich** oder der **Wertevorrat** von f.

4) Sei $M \subset B$. $f^{-1}(M) := \{x : x \in A \wedge f(x) \in M\}$ heißt das (volle) **Urbild** von M. $f^{-1}(y)$ heißt **Faser**.

5) f heißt **injektiv**, wenn $\bigwedge\limits_{x,y \in A} (f(x) = f(y) \to x = y)$.

6) f heißt **surjektiv**, wenn $\bigwedge\limits_{y \in B} \bigvee\limits_{x \in A} f(x) = y$.

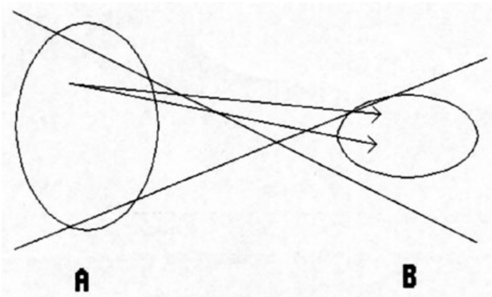
7) f heißt **bijektiv**, wenn f injektiv und surjektiv ist.

8) Die **Komposition** der Abbildungen $f : A \to B$ und $g : B \to C$ ist die durch $g \circ f(x) := g(f(x))$ definierte Abbildung $g \circ f : A \to C$.

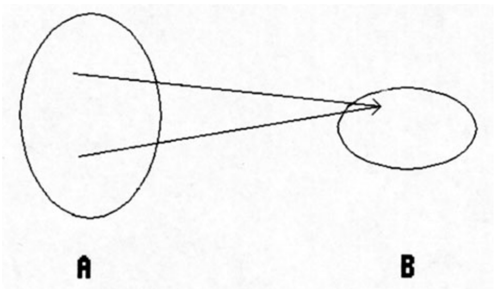
9) Die durch $\mathrm{id}_A(x) := x$ definierte Abbildung $\mathrm{id}_A : A \to A$ heißt die (auf A) **identische Abbildung**.

10) $f : A \to B$, $g : A \to B$ heißen **gleich**, wenn $f(x) = g(x)$ für alle x aus A gilt.

Slogans: Injektivität bedeutet Eindeutigkeit des Urbildes!
Surjektivität ist Abbildung „auf“, bedeutet also Existenz des Urbildes!



Keine Abbildung (Bild nicht eindeutig)



Keine inj. Abb. (Urbild nicht eindeutig)

1.12 Bemerkungen :

(i) Die Komposition von Abbildungen ähnelt der Multiplikation (reeller Zahlen) und wird daher entsprechend geschrieben: $g \circ f$ – nur wird hier von rechts nach links gelesen; denn zuerst wird f und dann g ausgeführt. Die Bezeichnung „Linksinverses“ rührt ebenfalls von der Multiplikation her. Es gilt doch: $\bigwedge\limits_{a \in \mathbb{R}\setminus\{0\}} \bigvee\limits_{b \in \mathbb{R}} ba = 1$, nämlich $b = \frac{1}{a} = a^{-1}$, also „b ist Linksinverses zu a“.

(ii) Eine Abbildung $f : A \to B$ schreiben wir auch als $A \underset{f}{\longrightarrow} B$. Seien nun f, g, h Abbildungen mit $A \underset{f}{\longrightarrow} B \underset{g}{\longrightarrow} C \underset{h}{\longrightarrow} D$. Dann gilt: $(f \circ g) \circ h = f \circ (g \circ h)$.
Beweis: Es gilt $h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x)))$ und ebenso $(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x)))$ für alle $x \in A$, also sind beide linke Seiten gleich.

(iii) Seien $f : A \to B$ und $g : B \to C$ surjektive (injektive bzw. bijektive) Abbildungen. Dann ist $g \circ f$ surjektiv (injektiv bzw. bijektiv).
Beweis als Übung.

1.13 Satz : Sei $f : A \to B$ eine Abbildung. Dann gelten:

(i) f ist genau dann injektiv, wenn ein $g : B \to A$ existiert mit $g \circ f = \mathrm{id}_A$. g heißt dann ein **Linksinverses** zu f.

(ii) f ist genau dann surjektiv, wenn ein $h : B \to A$ existiert mit $f \circ h = \mathrm{id}_B$. h heißt dann ein **Rechtsinverses** zu f.

(iii) f ist genau dann bijektiv, wenn es genau ein $g : B \to A$ gibt mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. Dieses eindeutig bestimmte g heißt dann die **Umkehrabbildung** oder die **inverse Abbildung** zu f, oft auch mit f^{-1} bezeichnet.

Achtung: Die inverse Abbildung f^{-1} nicht mit der Faser $f^{-1}(y)$ verwechseln!
Beweis:

I) Sei die rechte Seite der Behauptung (i) gültig. Wenn $f(x) = f(y)$ ist, so ist $g \circ f(x) = g \circ f(y)$, also $\mathrm{id}_A(x) = \mathrm{id}_A(y)$, also $x = y$, also f injektiv. Sei nun f injektiv. Dann gibt es zu jedem $b \in f(A)$ genau ein $a_b \in A$ mit $f(a_b) = b$. Wenn wir dann die Abbildung $g : B \to A$ mittels $g(b) = a_b$ für $b \in f(A)$ und $= a$ ($a \in A$, beliebig) für die übrigen b definieren, so ist g ein Linksinverses zu f. Also ist (i) bewiesen.

II) Führen Sie den Beweis von (ii) selber analog zu I.

III) Die „Wenn-Richtung“ von (iii) folgt direkt aus (i) und (ii). Sei nun f als bijektiv vorausgesetzt. Wir nehmen dann die nach (i) und (ii) zu f existierenden Abbildungen g und h. Es gilt $h = \mathrm{id}_A \circ h = (g \circ f) \circ h = g \circ (h \circ f) = g \circ \mathrm{id}_B = g$, also sind auch alle Linksinversen zu f gleich. Ebenso alle Rechtsinversen, und daher existiert **die** (eindeutig bestimmte) inverse Abbildung zu f.

1.14 Folgerung : Sei f eine Bijektion. Dann gilt $(f^{-1})^{-1} = f$.
Beweis: Es gilt sowohl $(f^{-1})^{-1} \circ f^{-1} = \mathrm{id}_B$ als auch $f \circ f^{-1} = \mathrm{id}_B$, also wegen der Eindeutigkeit der Inversen zu f nach Satz 1.13 $(f^{-1})^{-1} = f$.

AnfängerInnen müssen sich daran gewöhnen, nichts als selbstverständlich vorauszusetzen. Wir werden bald wichtige Strukturen kennenlernen, in denen die Existenz des Inversen keineswegs gesichert ist.

1.15 Definitionen : Sei M eine Menge. Eine Teilmenge R von $M \times M$ heißt eine **Relation** ρ auf M. Wir sagen: x **steht in Relation** zu y, geschrieben $x\ \rho\ y$, wenn $(x, y) \in R$ gilt.

(i) Ist $a\ \rho\ a$ für alle $a \in M$, so heißt ρ **reflexiv**.

(ii) Gilt $(a\ \rho\ b \to b\ \rho\ a)$, so heißt ρ **symmetrisch**.

(iii) Gilt $(a\ \rho\ b \wedge b\ \rho\ c \to a\ \rho\ c)$, so heißt ρ **transitiv**.

(iv) Eine Relation, die reflexiv, symmetrisch und transitiv ist, nennen wir eine **Äquivalenzrelation**, oft mit $\sim$ bezeichnet.

1.16 Beispiele :

(i) Die Gleichheit ist die bekannteste Äquivalenzrelation. Eine weitere Äquivalenzrelation ist die Ähnlichkeitsrelation auf der Menge aller Dreiecke.

(ii) Die Relation „ist ein Teiler von“ auf der Menge der natürlichen Zahlen ist reflexiv und transitiv, aber nicht symmetrisch.

(iii) Sei n eine natürliche Zahl. Die kleinsten nichtnegativen Reste, die bei Division von ganzrationalen Zahlen durch n auftreten können, sind $0, 1, 2, \ldots, n-1$. Seien a, b ganzrational. Wir sagen: $a \equiv b \bmod n$, wenn a und b bei Division durch n den gleichen kleinsten nichtnegativen Rest lassen, gesprochen: a **kongruent** zu b modulo n. Die Kongruenzrelation ist eine Äquivalenzrelation (Selbst überlegen!). Äquivalent mit $a \equiv b \bmod n$ ist die Aussage: n ist ein Teiler von $a - b$.[12]

1.17 Satz : Sei $\sim$ eine Äquivalenzrelation auf M. Dann ist M disjunkte Vereinigung (oder **Partition**) von (bzw. in) Teilmengen M_ν von M, geschrieben als $M = \dot{\bigcup\limits_{\nu}} M_\nu$, so daß gilt:

$$\bigwedge_{a,b \in M_\nu} a \sim b \wedge [(a \in M_\nu, b \in M_\mu, \mu \neq \nu) \to a \not\sim b] \quad .$$

Die Mengen M_ν heißen die **Äquivalenzklassen** von M bezüglich $\sim$. Also: M zerfällt in disjunkte Äquivalenzklassen.
Beweis: Aufgabe 1, 2. Übungsblatt.

[12]Die Bedeutung der Kongruenzrelation wird daraus ersichtlich, daß heutige Programmiersprachen wie Pascal, Modula, Lisp, Prolog einen Operator bzw. eine Funktion *mod* bereitstellen. In C/C++ wird das Zeichen % genommen: a%b ist der kleinste nichtnegative Rest von a modulo b.

1.18 Beispiele :

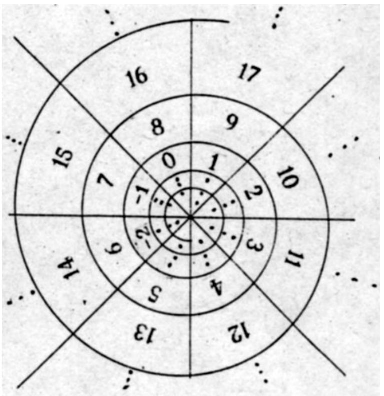
(i) Die Menge $\mathbb{Z}$ der ganzrationalen Zahlen zerfällt bezüglich der Kongruenz mod 8 in 8 Äquivalenzklassen, sog. **Restklassen**, nämlich

$$\hat{0} = \{0, \pm 8, \pm 16, \ldots\} \quad ,$$

$$\hat{1} = \{\ldots, -15, -7, 1, 9, 17, \ldots\} \quad ,$$

$$\ldots \quad ,$$

$$\hat{7} = \{\ldots, -9, -1, 7, 15, 23, \ldots\} \quad .$$



(ii) Zentralprojektion bedeutet eine Partition des gesamten Raumes (ohne Projektionspunkt) in die Projektionsstrahlen (Äquivalenzklassen) (siehe nachfolgendes Bild).

Dürer : Der Zeichner des liegenden Weibes

1.4 Elementare Kombinatorik

Eines der Axiome für die Menge $\mathbb{N} := \{1, 2, 3, \ldots\}$ der **natürlichen Zahlen** lautet:[13]

1.19 Induktionsaxiom : Sei $A(n)$ eine Aussage über die natürliche Zahl n mit den Eigenschaften

[13] Wir wollen die Axiomatik der Zahlensysteme auch später nur insoweit behandeln, als es die reellen und komplexen Zahlen betrifft (Kapitel 2, 3). Das bekannteste Axiomensystem für die Menge $\mathbb{N}$ der natürlichen Zahlen stammt von Guiseppe Peano. Aus $\mathbb{N}$ lassen sich leicht die Bereiche $\mathbb{Z}$ der ganzrationalen Zahlen und $\mathbb{Q}$ der rationalen Zahlen entwickeln (siehe z. B. E. Landau: Grundlagen der Analysis).

(i) $A(n)$ ist wahr für ein $n = n_0$ (**Induktionsanfang**) und

(ii) $\forall n \geq n_0 : A(n) \to A(n+1)$.

Dann gilt $A(n)$ für alle $n \geq n_0$.

Eine zweite, äquivalente Fassung des Induktionsaxioms lautet: Wenn $A(n_0)$ für ein $n_0 \in \mathbb{N}$ und $\bigwedge\limits_{\substack{n\in\mathbb{N} \\ n_0 \leq n < k}} A(n) \to A(k)$, dann gilt $A(n)$ für alle $n \geq n_0$.

Ein Beweis für die Aussage $\bigwedge\limits_{\substack{n\in\mathbb{N} \\ n \geq n_0}} A(n)$ mit Hilfe des Induktionsaxioms heißt ein **Beweis durch vollständige Induktion**. In einem solchen Beweis beweisen wir also (i) die Behauptung für ein festes n_0 und zeigen z.B. (ii): Sobald die Behauptung für ein n richtig ist, so ist sie es auch für den Nachfolger $n+1$ (sog. **Schluß von** n **auf** $n+1$). Es ist klar, daß dann die behauptete Aussage für jedes $n \geq n_0$ bewiesen ist, da wir uns ja von n_0 mit dem Induktionsschluß (ii) zu seinem Nachfolger $n_0 + 1$, von dem Nachfolger zu dessen Nachfolger etc. zu jedem $n \geq n_0$ „hochhangeln" können. Beispiele für solche Induktionsbeweise sind die Beweise der beiden folgenden Sätze.

1.20 Definition : Für $n \in \mathbb{N}$ heißt die Zahl $n! := 1 \cdot 2 \cdot 3 \cdots n$ n-**Fakultät**. Wir verabreden: $0! = 1$.

1.21 Satz : Es seien $A = \{a_1, a_2, \ldots, a_n\}$ und $B = \{b_1, b_2, \ldots, b_n\}$ zwei Mengen mit genau n Elementen (Mengen der **Mächtigkeit** n, Schreibweise: $|A| = |B| = n$). Dann gilt für die Anzahl $|S_n|$ der Bijektionen $f : A \to B$: $|S_n| = n!$.
Beweis: Durch vollständige Induktion.

(i) Induktionsanfang: Die Behauptung ist richtig für $n = 1$; denn zwischen $\{a_1\}$ und $\{b_1\}$ gibt es genau eine Bijektion. Also gilt $|S_1| = 1$.

(ii) Induktions-Annahme: Die Aussage sei richtig für n.

(iii) Induktions-Schluß: Wir zählen die Bijektionen zwischen $\{a_1, a_2, \ldots, a_{n+1}\}$ und $\{b_1, b_2, \ldots, b_{n+1}\}$. Da es für das Bild von a_1 genau n Möglichkeiten gibt (nämlich $j = 1, 2, \ldots, n$), gibt es also $(n+1) \cdot (n!)$ Möglichkeiten für eine bijektive Abbildung zwischen A und B.

1.22 Definitionen : Eine Bijektion $f : A \to A$ heißt **Permutation** oder **Transformation** von A. Die Menge aller Permutationen einer n-elementigen Menge wird mit S_n bezeichnet. Eine Anordnung mit Berücksichtigung der

Reihenfolge von n Elementen, unter denen n_1 gleiche seien, etwa alle gleich a_1; n_2 gleiche, etwa gleich a_2; $\ldots$ und n_r gleiche, die gleich a_r seien, heißt **Permutation mit Wiederholungen**.

1.23 Bemerkung : Die Anzahl dieser Permutationen mit Wiederholungen beträgt $\frac{n!}{n_1!n_2!\ldots n_r!}$. Überlege die Richtigkeit dieser Formel!

1.24 Binomischer Satz : Für a, $b \in \mathbb{R}$ und $n \in \mathbb{N}$ gilt

$$(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k}.$$

. Dabei gilt die Schreibweise $\sum_{k=0}^{n} c_k := c_0 + c_1 + \ldots + c_n$.

Beweis: Durch vollständige Induktion.

(i) Induktionsanfang: Offensichtlich gilt $a+b = \frac{1!}{0!1!}a^0b^1 + \frac{1!}{1!0!}a^1b^0$.

(ii) Induktionsschluß: Es gilt

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \frac{n!}{(k-1)!(n-k+1)!} a^k b^{n-k+1} + \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k+1} \quad .
\end{aligned}$$

Die Veränderung in der ersten Summe bei der letzten Umformung wird auch **Überschieben des Index** genannt.

> **Slogan:** Bei Erhöhung der Indexgrenzen um j ersetze den laufenden Index k durch $k-j$.

Ferner gilt doch die Beziehung (*)

$$\begin{aligned}
\frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} &= \frac{k \cdot n! + (n-k+1)\cdot n!}{k!(n-k+1)!} \\
&= \frac{(n+1)!}{k!(n-k+1)!} \quad , also
\end{aligned}$$

$$\begin{aligned}(a+b)^{n+1} &= \sum_{k=1}^{n} \frac{(n+1)!}{k!(n-k+1)!} a^k b^{n-k+1} + a^{n+1} + b^{n+1} \\ &= \sum_{k=0}^{n+1} \frac{(n+1)!}{k!(n-k+1)!} a^k b^{n-k+1} \quad .\end{aligned}$$

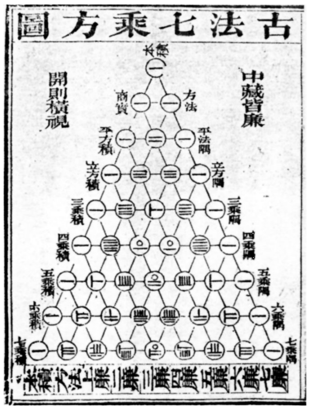
Übung: Überlege direkten Beweis mittels Permut. mit Wdhg.

1.25 Definitionen : Die Koeffizienten der Binomischen Formel werden **Binomialkoeffizienten** genannt und mit $\binom{n}{k} := \frac{n!}{k!(n-k)!}$ bezeichnet (definiert für $0 \leq k \leq n$).

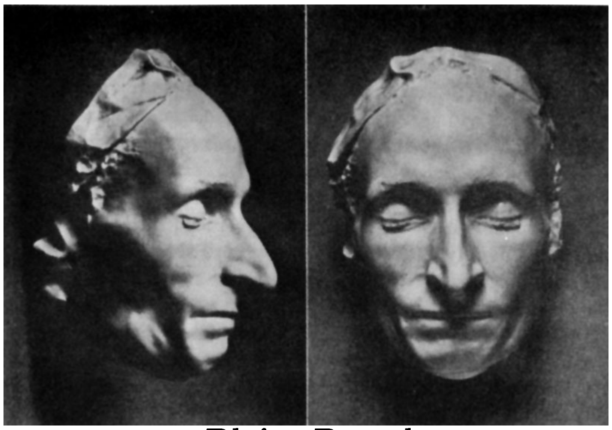
(*) aus 1.24 $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ ist Grundlage für das **Pascalsche Dreieck** der Binomialkoeffizienten:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{array}$$

Binom. Satz und Pascal-Dreieck waren in China lange vor Pascal bekannt.

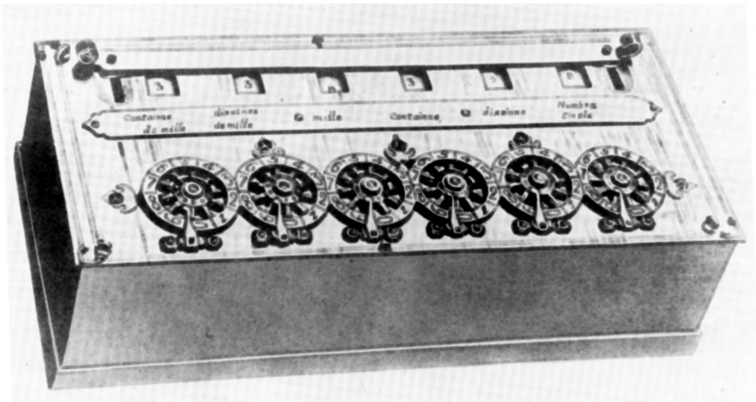


Aus Chu Shi-Chieh : Kostbarer Spiegel der 4 Elemente (13. Jh.)



Blaise Pascal (1623 - 1663)

Pascal war Mathematiker, Physiker, Philosoph, Theologe und Ingenieur. Er erfand die hydraulische Presse und baute eine Addiermaschine.



Pascals Rechenmaschine

1.26 Definitionen : Seien $k, n \in \mathbb{N}$ und $k \leq n$.

(i) Eine k-elementige Teilmenge einer n-elementigen Menge heißt eine **Kombination (ohne Wiederholung) von n Elementen zur k-ten Klasse**. Die Anzahl dieser Kombinationen sei mit $C(k, n)$ bezeichnet.

(ii) Entsprechend wird eine k Objekte umfassende Multimenge[14] , die mit Hilfe einer Teilmenge einer n-elementigen Menge gebildet wurde, **Kombination von n Elementen zur k-ten Klasse mit Wiederholung** genannt. Ihre Anzahl sei mit $C_W(k, n)$ bezeichnet.

(iii) Eine k-elementige Permutation, gebildet aus Elementen einer n-elementigen Menge, heißt **Variation (ohne Wiederholung) von n Elementen zur k-ten Klasse**. Ihre Anzahl: $V(k, n)$.

(iv) Analog können auch **Variationen mit Wiederholung** definiert werden. Ihre Anzahl: $V_W(k, n)$.

1.27 Bemerkungen : Es gelten

(i) $C(k, n) = \binom{n}{k}$,

(ii) $C_W(k, n) = \binom{n+k-1}{k}$,

[14]Als Multimenge bezeichnet man in der Kombinatorik bisweilen ein Aggregat vom Typ $\{\ldots, m, m, \ldots\}$, in dem also Elemente auch mehrfach auftreten.

(iii) $V(k,n) = \frac{n!}{(n-k)!}$,

(iv) $V_W(k,n) = n^k$.

Beweise: Für $C(k,n)$ ist stets $k \leq n$. Es gilt $C(n,n) = 1$. Zu zeigen bleibt also die Behauptung für $k < n$. Vollständige Induktion nach n: Die Formel ist richtig für $n = 1$, da $C(0,1) = 1$ ist. Die Formel sei für n als richtig angenommen. Gesucht ist $C(k, n+1)$ mit $k < n+1$. Sei M_1 (M_2) die Menge der Kombinationen der Ziffern $a_1, a_2, \ldots, a_{n+1}$ zur k-ten Klasse, die a_{n+1} (nicht) enthalten. Nach Induktionsannahme ist $|M_1| = C(k-1, n) = \binom{n}{k-1}$ und $|M_2| = C(k,n) = \binom{n}{k}$. Also gilt nach (*) von 1.24 $C(k, n+1) = |M_1| + |M_2| = \binom{n+1}{k}$.

Die Formel für $V(k,n)$ folgt aus der Tatsache, daß es sich bei Variationen von n Elementen zur k-ten Klasse um Permutationen mit Wiederholungen handelt: Die $n-k$ nichtauftretenden Ziffern werden als gleich angesehen!

Eine Variation von n Elementen zur k-ten Klasse zu bilden bedeutet, n Ziffern auf k Speicherzellen zu verteilen, also gibt es insgesamt $V_W(k,n) = n^k$ Möglichkeiten.[15]

Die Formel für $C_W(k,n)$ sei als Aufgabe (z.B. mittels vollständiger Induktion) gelassen.

1.28 Definitionen :

(i) Zwei Mengen M, N heißen **gleichmächtig**, geschrieben $|M| = |N|$ oder $M \cong N$, wenn es eine Bijektion von M auf N gibt.

(ii) M heißt **abzählbar**, wenn $M \cong \mathbb{N}$ oder $\exists n \in \mathbb{N} : M \cong \{1, 2, \ldots, n\}$.

(iii) Im letzteren Fall ist M eine **endliche** Menge der **Kardinalzahl** $|M| = n < \infty$.

(iv) Der Menge $\mathbb{N}$ der natürlichen Zahlen wird die Kardinalzahl $\aleph_0$ (**Aleph Null**) zugeordnet.

Slogans: Gleichmächtig bedeutet „gleichviele Elemente“.
Die Kardinalzahl einer Menge bedeutet die „Anzahl“ ihrer Elemente.

[15] So vermag also ein Byte $2^8 = 256$ Bitmuster zu speichern, daher erfaßt der ASCII-Code nur 256 Zeichen.

1.29 Bemerkungen :

(i) $\cong$ ist eine Äquivalenzrelation.

(ii) Für unendliche Mengen ist es möglich, daß $N \subsetneq M$ mit $M \cong N$ existiert. Z.B. ist $2\mathbb{Z} := \{0, \pm 2, \pm 4, \dots\} \subsetneq \mathbb{Z} := \{0, \pm 1, \pm 2, \dots\}$ und $f(x) := 2x$ vermittelt eine Bijektion von $\mathbb{Z}$ auf $2\mathbb{Z}$.

Ja, es gilt sogar das sog. **Dedekindsche Kriterium**:

(iii) M unendlich $\leftrightarrow$ M besitzt eine zu M gleichmächtige echte Teilmenge. (ohne Beweis)

1.30 Satz : Es seien A, B Mengen mit $\emptyset \neq A \subset B$, B abzählbar. Dann ist A abzählbar.
Beweis: Wenn B endlich ist, so ist natürlich auch A endlich. Wenn B abzählbar unendlich ist, so können wir $B = \{b_1, b_2, \dots\}$ schreiben. Jedes Element von B hat also einen natürlichen Index. Sei b_{n_1} das erste in der natürlichen Reihenfolge der Indizes auftauchende Element, das zu A gehört, b_{n_2} das zweite etc. Dann erhalten wir $A = \{b_{n_1}, b_{n_2}, \dots\}$, und mithin ist A abzählbar.

1.31 Satz : Wenn M, N abzählbare Mengen sind, so ist $M \times N$ abzählbar.
Beweis: Wegen 1.30 genügt es, die Aussage für abzählbar unendliche A, B zu beweisen. Seien also $A = \{a_1, a_2, \dots, a_i, \dots\}$ und $B = \{b_1, b_2, \dots, b_j, \dots\}$. Die Elemente von $A \times B$ erfassen wir nach dem sog. **Cantor'schen Diagonalverfahren**:

$(a_1, b_1), (a_1, b_2), (a_1, b_3), (a_1, b_4), \dots$
$(a_2, b_1), (a_2, b_2), (a_2, b_3), (a_2, b_4), \dots$
$(a_3, b_1), (a_3, b_2), (a_3, b_3), (a_3, b_4), \dots$
$(a_4, b_1), (a_4, b_2), \dots$
$\vdots$

$\frac{(i+j-1)(i+j-2)}{2} + j$ gibt den Index des Paares (a_i, b_j) an. Somit ist $A \times B$ abzählbar unendlich.

1.32 Folgerung : Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar.
Denn: Die Menge der positiven rationalen Zahlen ist eine Teilmenge von $\mathbb{N} \times \mathbb{N}$, also abzählbar (Jede positive rationale Zahl läßt sich als $\frac{a}{b}$ darstellen mit $a, b \in \mathbb{N}$). Der Rest der Aussage folgt aus dem nächsten Satz.

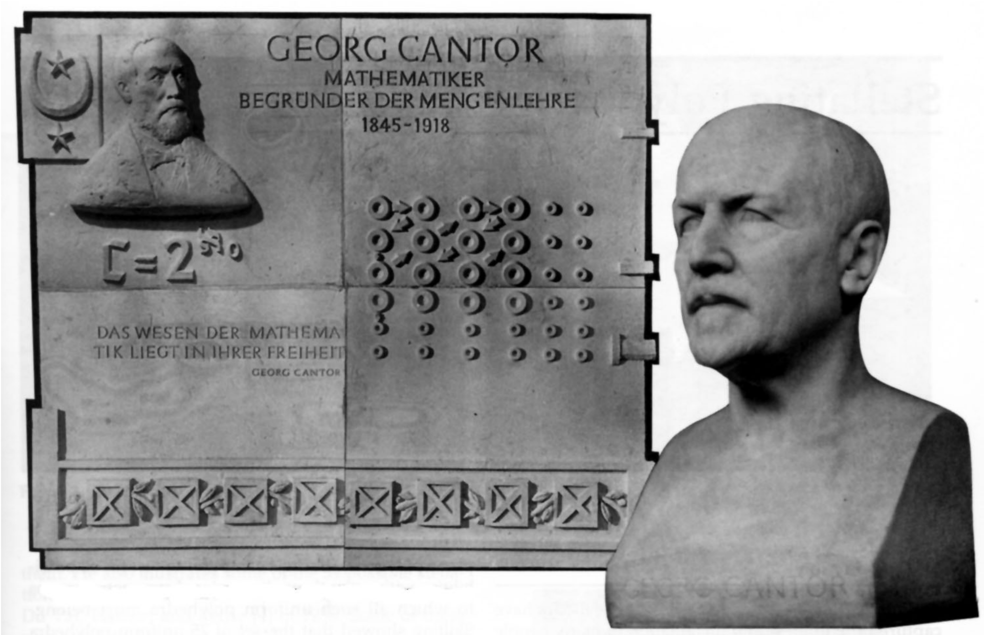
1.33 Satz : Wenn M_n abzählbar für alle $n \in \mathbb{N}$ ist, so ist $\bigcup\limits_{n\in\mathbb{N}} M_n$ abzählbar.
Beweis: Schreibe
$M_1 = \{m_{11}, m_{12}, m_{13}, \ldots\}$,
$M_2 = \{m_{21}, m_{22}, m_{23}, \ldots\}$,
$M_3 = \{m_{31}, m_{32}, m_{33}, \ldots\}$,
$\vdots$
und stelle die Menge $\bigcup M_n$ gemäß dem Cantor'schen Diagonalverfahren als abzählbare Folge $m_{11}, m_{12}, m_{21}, m_{13}, m_{22}, m_{31}, m_{14}, m_{23}, m_{32}, m_{41}, \ldots$ dar.

1.34 Satz : $M :=]0,1] := \{x \in \mathbb{R} : 0 < x \leq 1\}$ ist nicht abzählbar.
Beweis: Schreibe jedes $m \in M$ als nichtabbrechenden Dezimalbruch, also z.B. 0,5 als 0,499…9…. Diese Darstellung der Elemente von M ist eindeutig.
Annahme: M ist abzählbar. Dann können wir die Elemente von M als „durchnumeriert“ ansehen:
$m_1 = 0, a_{11}a_{12}a_{13}\ldots$
$m_2 = 0, a_{21}a_{22}a_{23}\ldots$
$\vdots$ mit $a_{ij} \in \mathbb{N}$ für alle i, j.
Betrachte die Zahl $r = 0, b_1b_2b_3\ldots$ mit $b_i \in \{1, 2, \ldots, 8\}$, $b_i \neq a_{ii} \quad \forall i = 1, 2, \ldots, n$. Es ist $r \in M$. Aber r unterscheidet sich von jedem m_i an der i-ten Nachkommastelle, und das ist ein Widerspruch zu der Annahme, daß r in der Abzählung auftauchen muß.

1.35 Folgerungen : Die Menge der irrationalen Zahlen in $]0,1]$ ist nicht abzählbar. Die Menge $\mathbb{R}$ der reellen Zahlen ist nicht abzählbar.

Übung: Überlegen Sie sich, daß gilt: Wenn M eine endliche Menge ist, so ist $|\mathcal{P}(M)| = 2^{|M|}$.

1.36 Bemerkung : Die Kardinalzahl der Potenzmenge einer Menge M ist stets größer als die Kardinalzahl von M, also erhalten wir auch eine ganze Hierarchie von sog. **transfiniten Zahlen** $2^{\aleph_0}$, $2^{2^{\aleph_0}}$, …. Natürlich gilt $\mathfrak{c} := |\mathbb{R}| = 2^{\aleph_0}$. Eine viel diskutierte These lautet: Es gibt keine Kardinalzahl $\mathfrak{a}$ mit $\aleph_0 < \mathfrak{a} < \mathfrak{c}$. (Die sogenannte **Kontinuumshypothese**). K. Gödel und P.J. Cohen bewiesen die Unabhängigkeit der Kontinuumshypothese von den anderen Axiomen der Mengenlehre.



Bronzetafel in Halle-Neustadt mit Cantorschem Diagonalverfahren

Marmorbüste Cantors in der Martin-Luther-Universität, Halle a. d. S.