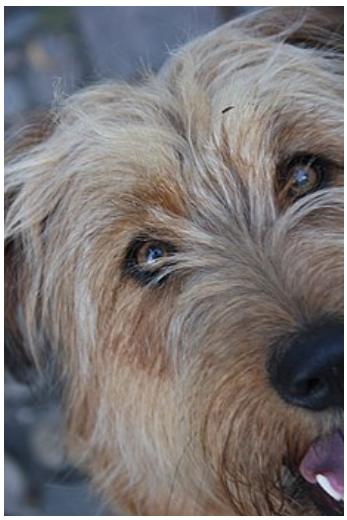
Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Mathematik für Anwender I

Vorlesung 4

Proof is the end product of a long interaction between creative imagination and critical reasoning. Without proof the program remains incomplete, but without the imaginative input it never gets started

Michael Atiyah



Vorli mag alle Menschen und achtet nicht auf Äußerlichkeiten. Ihr besonderes Talent ist aber, ...

Verknüpfungen

Die Rechenoperationen Addition und Multiplikation innerhalb der reellen Zahlen fassen wir als eine Abbildung

$$\mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

auf, d.h. es wird dem Paar

$$(x, y) \in \mathbb{R} \times \mathbb{R}$$

die reelle Zahl $x+y$ (bzw. $x \cdot y$) zugeordnet. Eine solche Abbildung heißt eine Verknüpfung.

DEFINITION 4.1. Eine *Verknüpfung* $\circ$ auf einer Menge M ist eine Abbildung

$$\circ\colon\ M \times M \longrightarrow M,\ (x,y) \longmapsto \circ(x,y) = x \circ y.$$

Der Definitionsbereich ist also die Produktmenge von M mit sich selbst und der Wertebereich ist ebenfalls M. Addition, Multiplikation und Subtraktion (auf $\mathbb{Z}$, auf $\mathbb{Q}$ oder auf $\mathbb{R}$) sind Verknüpfungen. Auf $\mathbb{Q}$ und $\mathbb{R}$ ist die Division keine Verknüpfung, da sie nicht definiert ist, wenn die zweite Komponente gleich 0 ist (und schon gar nicht auf $\mathbb{Z}$). Allerdings ist die Division eine Verknüpfung auf $\mathbb{R} \setminus \{0\}$. In dieser Vorlesung werden wir die algebraischen Eigenschaften der Addition und der Multiplikation auf den reellen Zahlen im Begriff des „Körpers“ zusammenfassen.

Axiomatik

Die Mathematik ist durchzogen von Strukturen, die immer wieder in ähnlicher Weise auftreten. Beispielsweise besitzen die rationalen Zahlen und die reellen Zahlen sehr viele gemeinsame Eigenschaften, bezüglich gewisser Eigenschaften weichen sie aber voneinander ab. Diese Beobachtung ist die Grundlage für den *axiomatischen Aufbau der Mathematik*. Dabei fasst man verschiedene strukturelle Eigenschaften, die in einem bestimmten Kontext immer wieder auftauchen, in einen neuen Begriff zusammen. Das Ziel ist dabei, weitere Eigenschaften aus einigen wenigen Grundeigenschaften logisch zu erschließen. Man argumentiert dann nicht auf der Ebene vertrauter Beispiele, wie der reellen Zahlen, sondern logisch-deduktiv auf der Ebene der Eigenschaften. Der Gewinn ist dabei, dass man mathematische Schlüsse nur einmal auf der abstrakten Ebene der Eigenschaften durchführen muss und diese dann für alle Modelle gelten, die die jeweiligen Grundeigenschaften erfüllen, also unter den Begriff fallen. Zugleich erkennt man logische Abhängigkeiten und Hierarchien zwischen den Eigenschaften. Grundlegende Eigenschaften von mathematischen Strukturen werden als *Axiome* bezeichnet.

Im axiomatischen Zugang werden die Gesetzmäßigkeiten in den Mittelpunkt gestellt. Mathematische Objekte, die diese Gesetzmäßigkeiten erfüllen, sind dann Beispiele oder Modelle für diese Gesetzmäßigkeiten. Als Eigenschaften wählt man dabei vor allem solche Eigenschaften, die einerseits einfach zu formulieren sind und andererseits starke Folgerungen erlauben. Die Vorteile dieses Aufbaus sind die folgenden Punkte.

- Die mathematischen Objekte werden auf eine mengentheoretisch-logische Grundlage gestellt, man muss sich nicht auf die Anschauung stützen.

- Man weiß jederzeit, welche Argumentation, um eine Eigenschaft nachzuweisen, erlaubt ist und welche nicht, erlaubt ist nämlich nur das logische Erschließen der Eigenschaft aus den Axiomen heraus.

• Es werden wenige grundlegende Eigenschaften herausgearbeitet. Es entsteht eine Hierarchie zwischen fundamentalen Gesetzmäßigkeiten und abgeleiteten Eigenschaften.

Es werden strukturelle Ähnlichkeiten sichtbar, die von einem intuitiven Standpunkt her übersehen werden könnten. Viele Aussagen, die man aus Axiomen ableiten kann, benötigen gar nicht das volle Axiomensystem, sondern nur Teile davon. Man kann daher die Axiome gruppieren, und wenn man aus einer bestimmten Axiomengruppe eine Aussage ableiten kann, so gilt diese auch für alle mathematischen Gebilde, die diese Axiomengruppe erfüllen. Durch „Gegenbeispiele“ kann man zeigen, dass gewisse Eigenschaften nicht aus anderen Eigenschaften folgen. Das Vorgehen ist sehr ökonomisch, da es Wiederholungen von Schlüssen vermeidet. Als Nachteile kann man die folgenden Punkte nennen.

• Großer begrifflicher Aufwand.

• Abstraktes, manchmal übertrieben formal oder unintuitiv scheinendes Vorgehen.

• Offensichtlich „triviale Eigenschaft“ brauchen eine Begründung, wenn sie nicht explizit im Axiomensystem vorkommen.

Körper

Wir werden nun die Eigenschaften der reellen Zahlen in einem axiomatischen Rahmen besprechen. Die Axiome für die reellen Zahlen gliedern sich in algebraische Axiome, Anordnungsaxiome und das Vollständigkeitsaxiom. Die algebraischen Axiome werden im Begriff des Körpers zusammengefasst. Unter algebraischen Eigenschaften versteht man solche Eigenschaften, die sich auf die Rechenoperationen, also die Addition, die Subtraktion, die Multiplikation und die Division, beziehen. Diese Operationen ordnen zwei Elementen der gegebenen Menge M, also beispielsweise zwei reellen Zahlen, ein weiteres Element der Menge zu, es handelt sich also um Verknüpfungen. Die folgende Definition nimmt nur auf zwei Verknüpfungen, Addition und Multiplikation, Bezug, Subtraktion und Division ergeben sich als abgeleitete Verknüpfungen.

Definition 4.2. Eine Menge K heißt ein *Körper*, wenn es zwei Verknüpfungen (genannt Addition und Multiplikation)

$$+ : K \times K \longrightarrow K \text{ und } \cdot : K \times K \longrightarrow K$$

und zwei verschiedene Elemente $0, 1 \in K$ gibt, die die folgenden Eigenschaften erfüllen.

(1) Axiome der Addition
   (a) Assoziativgesetz: Für alle $a, b, c \in K$ gilt: $(a+b)+c = a+(b+c)$.
   (b) Kommutativgesetz: Für alle $a, b \in K$ gilt $a + b = b + a$.

(c) 0 ist das neutrale Element der Addition, d.h. für alle $a \in K$ ist $a + 0 = a$.
(d) Existenz des Negativen: Zu jedem $a \in K$ gibt es ein Element $b \in K$ mit $a + b = 0$.

(2) Axiome der Multiplikation
(a) Assoziativgesetz: Für alle $a, b, c \in K$ gilt: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(b) Kommutativgesetz: Für alle $a, b \in K$ gilt $a \cdot b = b \cdot a$.
(c) 1 ist das neutrale Element der Multiplikation, d.h. für alle $a \in K$ ist $a \cdot 1 = a$.
(d) Existenz des Inversen: Zu jedem $a \in K$ mit $a \neq 0$ gibt es ein Element $c \in K$ mit $a \cdot c = 1$.

(3) Distributivgesetz: Für alle $a, b, c \in K$ gilt $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Dass all diese Axiome für die reellen Zahlen (und die rationalen Zahlen) mit den natürlichen Verknüpfungen gelten, ist aus der Schule bekannt.

In einem Körper gilt die *Klammerkonvention*, dass die Multiplikation stärker bindet als die Addition. Man kann daher $a \cdot b + c \cdot d$ statt $(a \cdot b) + (c \cdot d)$ schreiben. Zur weiteren Notationsvereinfachung wird das Produktzeichen häufig weggelassen. Die besonderen Elemente 0 und 1 in einem Körper werden als *Nullelement* und als *Einselement* bezeichnet. Nach der Definition müssen sie verschieden sein.

Die wichtigsten Beispiele für einen Körper sind für uns die rationalen Zahlen, die reellen Zahlen und die komplexen Zahlen, die wir in der nächsten Vorlesung kennenlernen werden.

LEMMA 4.3. *In einem Körper K ist zu einem Element $x \in K$ das Element y mit $x + y = 0$ eindeutig bestimmt. Bei $x \neq 0$ ist auch das Element z mit $xz = 1$ eindeutig bestimmt.*

Beweis. Sei x vorgegeben und seien y und y' Elemente mit $x+y = 0 = x+y'$. Dann gilt

$$y = y + 0 = y + (x + y') = (y + x) + y' = (x + y) + y' = 0 + y' = y'.$$

Insgesamt ist also $y = y'$. Für den zweiten Teil siehe Aufgabe 4.3. □

Zu einem Element $a \in K$ nennt man das nach diesem Lemma eindeutig bestimmte Element y mit $a + y = 0$ das *Negative* von a und bezeichnet es mit $-a$. Es ist $-(-a) = a$, da wegen $a + (-a) = 0$ das Element a gleich dem eindeutig bestimmten Negativen von $-a$ ist.

Statt $b + (-a)$ schreibt man abkürzend $b - a$ und spricht von der *Differenz*. Die Differenz ist also keine grundlegende Verknüpfung, sondern wird auf die Addition mit dem Negativen zurückgeführt.

Das zu $a \in K$, $a \neq 0$, nach diesem Lemma eindeutig bestimmte Element z mit $az = 1$ nennt man das *Inverse* von a und bezeichnet es mit a^{-1}.

Für $a, b \in K$, $b \neq 0$, schreibt man auch abkürzend

$$a/b := \frac{a}{b} = ab^{-1}.$$

Die beiden linken Ausdrücke sind also eine Abkürzung für den rechten Ausdruck.

Zu einem Körperelement $a \in K$ und $n \in \mathbb{N}$ wird a^n als das n-fache Produkt von a mit sich selbst definiert, und bei $a \neq 0$ wird a^{-n} als $(a^{-1})^n$ interpretiert.

Ein „kurioser“ Körper wird im folgenden Beispiel beschrieben. Dieser Körper mit zwei Elementen ist in der Informatik und der Kodierungstheorie wichtig, wird für uns aber keine große Rolle spielen. Er zeigt, dass es nicht für jeden Körper sinnvoll ist, seine Elemente auf der Zahlengeraden zu verorten.

Beispiel 4.4. Wir suchen nach einer Körperstruktur auf der Menge $\{0, 1\}$. Wenn 0 das neutrale Element einer Addition und 1 das neutrale Element einer Multiplikation sein soll, so ist dadurch schon alles festgelegt, da $1 + 1 = 0$ sein muss, da 1 ein inverses Element bezüglich der Addition besitzen muss, und da in jedem Körper nach Lemma 4.3 (1) $0 \cdot 0 = 0$ gelten muss. Die Operationstafeln sehen also wie folgt aus.

$+$	0	1
0	0	1
1	1	0

und

$\cdot$	0	1
0	0	0
1	0	1

Durch etwas aufwändiges Nachrechnen stellt man fest, dass es sich in der Tat um einen Körper handelt.

Die folgenden Eigenschaften sind für den Körper der reellen Zahlen vertraut, wir beweisen sie aber allein aus den Axiomen eines Körpers, sie gelten daher für einen beliebigen Körper.

Lemma 4.5. *Es sei K ein Körper und seien $a, b, c, a_1, \ldots, a_r, b_1, \ldots, b_s$ Elemente aus K. Dann gelten folgende Aussagen.*

(1) $a0 = 0$ *(*Annullationsregel*).*
(2)
$$(-a)b = -ab = a(-b)$$
*(*Vorzeichenregel*).*
(3)
$$(-a)(-b) = ab.$$
(4)
$$a(b - c) = ab - ac$$

(5) *Aus* $a \cdot b = 0$ *folgt* $a = 0$ *oder* $b = 0$ *(*Nichtnullteilereigenschaft*).*
(6) $(\sum_{i=1}^{r} a_i)(\sum_{k=1}^{s} b_k) = \sum_{1 \leq i \leq r,\, 1 \leq k \leq s} a_i b_k$ *(*allgemeines Distributivgesetz*).*

Beweis. (1) Es ist $a0 = a(0+0) = a0+a0$. Durch beidseitiges Abziehen (also Addition mit dem Negativen von $a0$) von $a0$ ergibt sich die Behauptung.
(2) Siehe Aufgabe 4.4.
(3) Siehe Aufgabe 4.4.
(4) Siehe Aufgabe 4.4.
(5) Nehmen wir an, dass a und b beide von 0 verschieden sind. Dann gibt es dazu inverse Elemente a^{-1} und b^{-1} und daher ist $(ab)(b^{-1}a^{-1}) = 1$. Andererseits ist aber nach Voraussetzung $ab = 0$ und daher ist nach der Annullationsregel

$$(ab)\big(b^{-1}a^{-1}\big) = 0\big(b^{-1}a^{-1}\big) = 0,$$

so dass sich der Widerspruch $0 = 1$ ergibt.
(6) Dies folgt aus einer Doppelinduktion, siehe Aufgabe 4.22.

□

Exkurs: Widerspruchsbeweise

Soeben haben wir einen Widerspruchsbeweis durchgeführt, dieses Argumentationsschema wollen wir kurz anhand von typischen Beispielen erläutern.

Bei einem *Widerspruchsbeweis* geht man folgendermaßen vor: Man möchte eine mathematische Aussage A beweisen. Man nimmt dann an, dass A nicht wahr ist, dass also die Negation von A wahr ist. Dann führt man eine mathematische Argumentation durch, die zu einem Widerspruch führt, typischerweise zu einer Aussage B, die sowohl gilt als auch nicht gilt. Da dies nicht sein kann, muss die Annahme falsch gewesen sein, und damit ist A bewiesen. Da die Argumentation mathematisch korrekt sein muss, bleibt als einzige Erklärung für den Widerspruch die Annahme übrig.

Wir geben zwei Hauptbeispiele für einen Widerspruchsbeweis.

Satz 4.6. *Es gibt keine rationale Zahl, deren Quadrat gleich* 2 *ist. D.h. die reelle Zahl* $\sqrt{2}$ *ist irrational.*

Beweis. Wir machen die Annahme, dass es eine rationale Zahl gibt, deren Quadrat gleich 2 ist, und führen das zu einem Widerspruch. Sei also angenommen, dass

$$x \in \mathbb{Q}$$

die Eigenschaft besitzt, dass

$$x^2 = 2$$

ist. Eine rationale Zahl hat die Beschreibung als ein Bruch, wobei Zähler und Nenner ganze Zahlen sind. Die rationale Zahl x können wir somit als

$$x = \frac{a}{b}$$

ansetzen. Ferner können wir annehmen (dieses Annehmen ist eine Vereinfachung der Situation und hat nichts mit der zum Widerspruch zu führenden Annahme zu tun), dass dieser Bruch gekürzt ist, dass also a und b keinen echten gemeinsamen Teiler haben. In der Tat brauchen wir lediglich, dass wir annehmen dürfen, dass zumindest eine Zahl, a oder b ungerade ist (wenn beide gerade sind, so können wir mit 2 kürzen, u.s.w.) Die Eigenschaft

$$x^2 = 2$$

bedeutet ausgeschrieben

$$x^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} = 2.$$

Multiplikation mit b^2 ergibt die Gleichung

$$2b^2 = a^2$$

(dies ist eine Gleichung in $\mathbb{Z}$ bzw. sogar in $\mathbb{N}$). Diese Gleichung besagt, dass a^2 gerade ist, da ja a^2 ein Vielfaches der 2 ist. Daraus ergibt sich aber auch, dass a selbst gerade ist, da ja das Quadrat einer ungeraden Zahl wieder ungerade ist. Deshalb können wir den Ansatz

$$a = 2c$$

mit einer ganzen Zahl c machen. Dies setzen wir in die obige Gleichung ein und erhalten

$$2b^2 = (2c)^2 = 2^2c^2.$$

Wir können mit 2 kürzen und erhalten

$$b^2 = 2c^2.$$

Also ist auch b^2 und damit b selbst gerade. Dies ist ein Widerspruch dazu, dass nicht sowohl a als auch b gerade sind. □

Der folgende Satz heißt *Satz von Euklid*.

Satz 4.7. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, die Menge aller Primzahlen sei endlich, sagen wir $\{p_1, p_2, \ldots, p_r\}$. Man betrachtet die Zahl

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_r + 1.$$

Diese Zahl ist durch keine der Primzahlen p_i teilbar, da bei Division von N durch p_i immer ein Rest 1 verbleibt. Damit sind die Primfaktoren von N, die es nach Satz 2.5 geben muss, nicht in der Ausgangsmenge enthalten - Widerspruch. □

Der Binomische Lehrsatz

DEFINITION 4.8. Zu einer natürlichen Zahl n nennt man die Zahl

$$n! := n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$$

die *Fakultät* von n (sprich n Fakultät).

Man setzt $0! = 1$.

DEFINITION 4.9. Es seien k und n natürliche Zahlen mit $k \leq n$. Dann nennt man

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

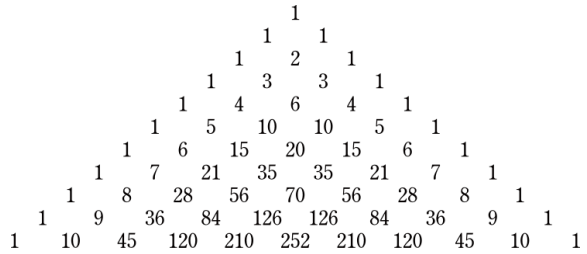
den *Binomialkoeffizienten* „n über k“.

Diesen Bruch kann man auch als

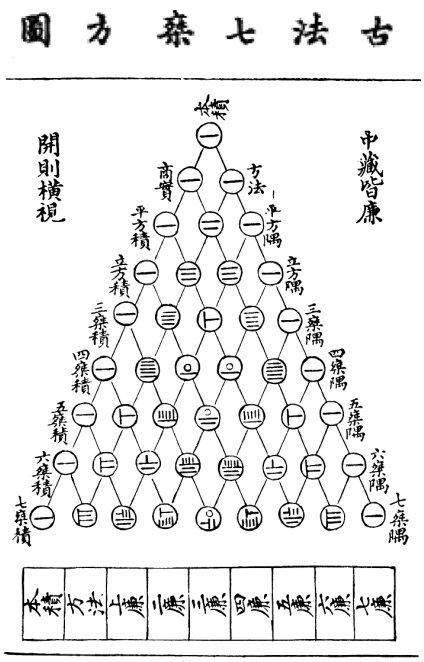
$$\frac{n(n-1)(n-2)\cdots(n-k+2)(n-k+1)}{k(k-1)(k-2)\cdots 2\cdot 1}$$

schreiben, da die Faktoren aus $(n-k)!$ auch in $n!$ vorkommen und daher kürzbar sind. In dieser Darstellung stehen im Zähler und im Nenner gleich viele Faktoren. Gelegentlich ist es sinnvoll, auch negative k oder $k > n$ zuzulassen und in diesen Fällen die Binomialkoeffizienten gleich 0 zu setzen.

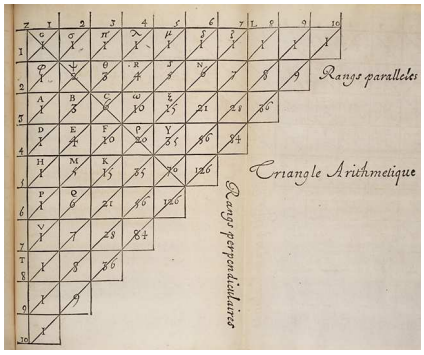
Von der Definition her ist es nicht sofort klar, dass es sich bei den Binomialkoeffizienten um natürliche Zahlen handelt. Dies folgt aus der folgenden Beziehung.



Das *Dreieck der Binomialkoeffizienten* war in Indien und in Persien schon um 1000 bekannt,



in China heißt es *Yanghui-Dreieck* (nach Yang Hui (um 1238-1298)),



in Europa heißt es das *Pascalsche Dreieck* (nach Blaise Pascal (1623-1662)).

LEMMA 4.10. *Die Binomialkoeffizienten erfüllen die rekursive Beziehung*[1]

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Beweis. Siehe Aufgabe 4.13. □

Die folgende Formel bringt die Addition und die Multiplikation miteinander in Beziehung.

[1]Bei $k = 0$ ist $\binom{n}{k-1}$ als 0 zu interpretieren.

SATZ 4.11. *Es seien a, b Elemente in einem Körper. Ferner sei n eine natürliche Zahl. Dann gilt*

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

Beweis. Wir führen Induktion nach n. Für $n = 0$ steht einerseits $(a+b)^0 = 1$ und andererseits $a^0 b^0 = 1$.[2] Sei die Aussage bereits für n bewiesen. Dann ist

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\
&= a\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) + b\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-k+1} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k}\right) a^k b^{n+1-k} + b^{n+1} \\
&= \sum_{k=1}^{n+1} \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.
\end{aligned}$$

□

BEMERKUNG 4.12. Für den Binomialkoeffizienten

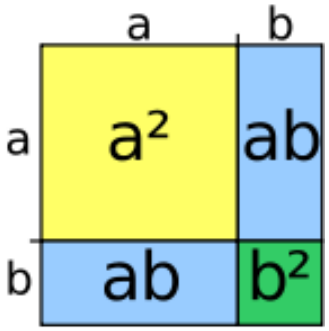
$$\binom{n}{k}$$

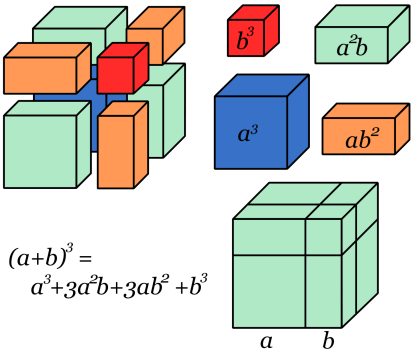
gibt es eine wichtige inhaltliche Interpretation. Er gibt die Anzahl der k-elementigen Teilmengen in einer n-elementigen Menge an. Z.B. gibt es in einer 49-elementigen Menge genau

$$\binom{49}{6} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 13983816$$

6-elementige Teilmengen. Der Kehrwert von dieser Zahl ist die Wahrscheinlichkeit, beim Lotto sechs Richtige zu haben.

[2] Wenn einem diese Aussage merkwürdig vorkommt, da sie von der Festlegung $x^0 = 1$ abhängt, so kann man auch bei $n = 1$ anfangen. Dann hat man einerseits $(a+b)^1 = a+b$ und andererseits $a^1 b^0 + a^0 b^1 = a + b$.





$(a+b)^3 =$
$a^3+3a^2b+3ab^2+b^3$

Abbildungsverzeichnis