**Prof. Dr. H. Brenner** **Osnabrück SS 2015**

# Elemente der Algebra

## Vorlesung 2

## Ringe

Die wichtigsten mathematischen Strukturen wie $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ besitzen nicht nur eine, sondern zwei Verknüpfungen.

DEFINITION 2.1. Ein *Ring* $R$ ist eine Menge mit zwei Verknüpfungen $+$ und $\cdot$ und mit zwei ausgezeichneten Elementen 0 und 1 derart, dass folgende Bedingungen erfüllt sind:

(1) $(R, +, 0)$ ist eine abelsche Gruppe.
(2) $(R, \cdot, 1)$ ist ein Monoid.
(3) Es gelten die *Distributivgesetze*, also $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ für alle $a, b, c \in R$.

DEFINITION 2.2. Ein Ring $R$ heißt *kommutativ*, wenn die Multiplikation kommutativ ist.

In einem kommutativen Ring muss man nicht zwischen den beiden Formen des Distributivgesetzes unterscheiden. Das Basismodell für einen (kommutativen) Ring bildet die Menge der ganzen Zahlen $\mathbb{Z}$ mit der natürlichen Addition und Multiplikation. Die 0 ist das neutrale Element der Addition und die 1 ist das neutrale Element der Multiplikation. Der Nachweis, dass $\mathbb{Z}$ die Axiome eines Ringes, also die oben aufgelisteten Eigenschaften, erfüllt, beruht letztlich auf den Peano-Axiomen für die natürlichen Zahlen $\mathbb{N}$ und ist ziemlich formal. Darauf wollen wir verzichten und stattdessen diese seit langem vertrauten Gesetzmäßigkeiten akzeptieren.

Die natürlichen Zahlen bilden keinen Ring, da sie noch nicht einmal eine additive Gruppe bilden. Die Zahlbereiche $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind ebenfalls kommutative Ringe, wobei der Nachweis der Eigenschaften dadurch geschieht, dass man die Konstruktion dieser Zahlbereiche aus den „vorhergehenden“ betrachtet (etwa $\mathbb{R}$ aus $\mathbb{Q}$) und die Gültigkeit (in $\mathbb{R}$) auf die Gültigkeit im „Vorgänger“ ($\mathbb{Q}$) zurückführt.

Wir benutzen allgemein die *Klammerkonvention*, dass Punktrechnung stärker bindet als Strichrechnung, d.h. wir schreiben einfach $ab+cd$ statt $(ab)+(cd)$. Das Inverse zu $a \in R$ bezüglich der Addition, das es ja immer gibt, schreiben wir als $-a$ und nennen es das *Negative* von $a$. Statt $a + (-b)$ schreiben wir $a - b$. An weiteren Notationen verwenden wir für ein Ringelement $a \in R$ und eine natürliche Zahl $n \in \mathbb{N}$ die Schreibweisen $na = a + \cdots + a$ ($n$ Summanden) und $a^n = a \cdots a$ ($n$ Faktoren). Bei einem negativen $n \in \mathbb{Z}$ ist $na = (-n)(-a)$

zu interpretieren (dies beruht auf den „Potenzgesetzen“ in einer Gruppe aus der ersten Vorlesung, wobei hier die Gruppe additiv geschrieben wird und deshalb Vielfache genommmen werden) (dagegen macht $a^n$ mit negativen Exponenten im Allgemeinen keinen Sinn). Statt $n1 = n1_R$ schreiben wir einfach $n$ (bzw. manchmal $n_R$), d.h. jede ganze Zahl findet sich in jedem Ring wieder.

Beispiel 2.3. Die einelementige Menge $R = \{0\}$ kann man zu einem Ring machen, indem man sowohl die Addition als auch die Multiplikation auf die einzig mögliche Weise erklärt, nämlich durch $0 + 0 = 0$ und $0 \cdot 0 = 0$. In diesem Fall ist $1 = 0$, dies ist also ausdrücklich erlaubt. Diesen Ring nennt man den *Nullring*.

Nach dem Nullring ist der folgende Ring der zweitkleinste Ring.

Beispiel 2.4. Wir suchen nach einer Ringstruktur auf der Menge $\{0, 1\}$. Wenn 0 das neutrale Element einer Addition und 1 das neutrale Element der Multiplikation sein soll, so ist dadurch schon alles festgelegt, da $1 + 1 = 0$ sein 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 kommutativen Ring handelt (sogar um einen Körper).

Eine „natürliche“ Interpretation dieses Ringes gewinnt man, wenn man sich die geraden ganzen Zahlen durch 0 und die ungeraden ganzen Zahlen durch 1 repräsentiert denkt. Beispielsweise ist die Summe zweier ungerader Zahlen stets gerade, was der obigen Gleichung $1 + 1 = 0$ entspricht.

Zu jeder natürlichen Zahl $n \in \mathbb{N}$ kann man einen kommutativen Ring $\mathbb{Z}/(n)$ definieren, nämlich als die Menge $\{0, 1, 2, \ldots, n-2, n-1$, wobei die Addition und die Multiplikation zuerst in $\mathbb{N}$ ausgeführt wird und davon der Rest bei Division durch $n$ genommen wird. Die exakte Durchführung dieser Konstruktion und der Nachweis der Ringeigenschaften verschieben wir auf später, es ist aber sinnvoll, diese (verglichen mit $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$) untypischen Ringe schon jetzt zur Verfügung zu haben. Der obige Ring mit zwei Elementen ist beispielsweise gleich $\mathbb{Z}/(2)$.

Lemma 2.5. *Sei $R$ ein Ring und seien $a, b, c, a_1, \ldots, a_r, b_1, \ldots, b_s$ Elemente aus $R$. Dann gelten folgende Aussagen*

(1) $0a = a0 = 0$ *(*Annullationsregel*),*
(2) $a(-b) = -(ab) = (-a)b$
(3) $(-a)(-b) = ab$ *(*Vorzeichenregel*),*
(4) $a(b-c) = ab - ac$ *und* $(b-c)a = ba - ca$,
(5) $(\sum_{i=1}^{r} a_i)\,(\sum_{k=1}^{s} b_k) = \sum_{1\le i\le r,\,1\le k\le s} a_i b_k$ *(*allgemeines Distributivgesetz*).*

*Beweis.* Wir beweisen im nicht kommutativen Fall je nur eine Hälfte.

(1) Es ist $a0 = a(0+0) = a0 + a0$. Durch beidseitiges Abziehen von $a0$ ergibt sich die Behauptung.
(2)
$$(-a)b + ab = (-a+a)b = 0b = 0$$
nach Teil (1). Daher ist $(-a)b$ das (eindeutig bestimmte) Negative von $ab$.
(3) Nach (2) ist $(-a)(-b) = (-(-a))b$ und wegen $-(-a) = a$ (dies gilt in jeder Gruppe) folgt die Behauptung.
(4) Dies folgt auch aus dem bisher Bewiesenen.
(5) Dies folgt aus einer einfachen Doppelinduktion.

□

## Die Binomialkoeffizienten

Die *erste binomische Formel* besagt bekanntlich
$$(a+b)^2 = a^2 + 2ab + b^2.$$
Für die dritte Potenz einer Summe gilt
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$
und für die vierte Potenz
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$
In dieser Weise kann man jede Potenz einer Summe als Summe von Produkten ausdrücken, wobei die auftretenden Koeffizienten *Binomialkoeffizienten* heißen. Diese werden mit Hilfe der Fakultät definiert, wobei die Fakultät $n!$ einer natürlichen Zahl durch
$$n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$$
definiert ist.

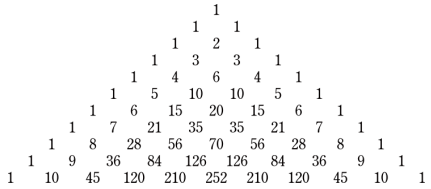
Definition 2.6. Es seien $k$ und $n$ natürliche Zahlen mit $k \le n$. Dann nennt man
$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$
den *Binomialkoeffizienten* „$n$ über $k$“.

Diesen Bruch kann man auch als

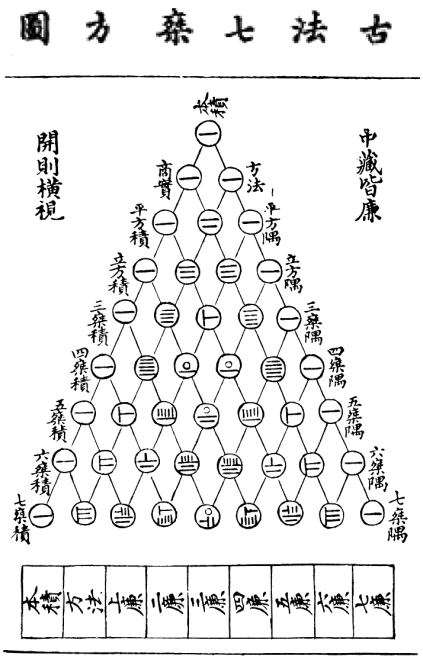
$$\frac{n(n-1)(n-2)\cdots(n-k+2)(n-k+1)}{k(k-1)(k-2)\cdots 2\cdot 1}$$

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.

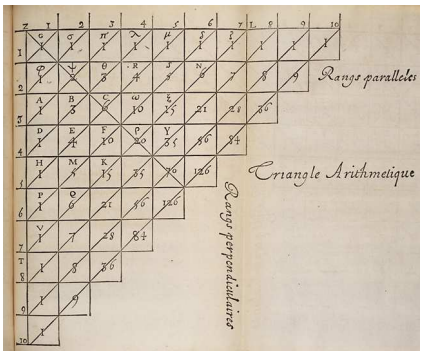
Von der Definition her ist es nicht sofort klar, dass es sich bei den Binomialkoeffizienten um natürliche Zahlen handelt. Dies folgt aus der folgenden Beziehung.




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)),



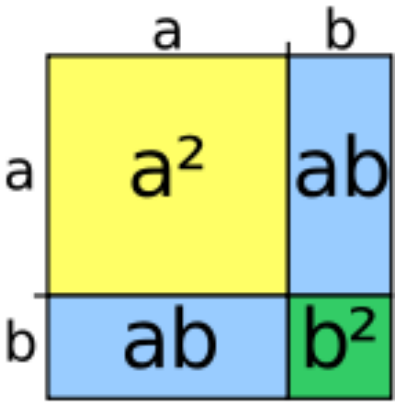

in Europa heißt es das *Pascalsche Dreieck* (nach Blaise Pascal (1623-1662)).

LEMMA 2.7. *Die Binomialkoeffizienten erfüllen die rekursive Beziehung*

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

*Beweis.* Siehe Aufgabe 2.7. □

Der Binomialkoeffizient $\binom{n}{k}$ hat die folgende inhaltliche Bedeutung: Er gibt für eine $n$-elementige Menge $M$ die Anzahl sämtlicher $k$-elementigen Teilmengen von $M$ an, siehe Aufgabe 2.8. Wenn $k > n$ ist oder wenn $k$ negativ ist so setzt man den Binomialkoeffizienten gleich null.




Die folgende *allgemeine binomische Formel* bringt die Addition und die Multiplikation in einem kommutativen Ring miteinander in Beziehung.

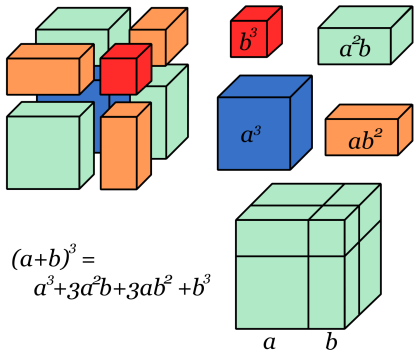
SATZ 2.8. *Es sei $R$ ein kommutativer Ring und $a, b \in R$. Ferner sei $n$ eine natürliche Zahl. Dann gilt*

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

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

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

□




## Nichtnullteiler und Integritätsbereiche

Definition 2.9. Ein Element $a$ in einem kommutativen Ring $R$ heißt *Nullteiler*, wenn es ein von 0 verschiedenes Element $b$ mit $ab = 0$ gibt. Andernfalls heißt es ein *Nichtnullteiler*.

Die Eins ist stets ein Nichtnullteiler, da aus $1b = 0$ sofort $b = 0$ folgt. Andererseits ist das Nullelement stets ein Nullteiler, es sei denn, der Nullring liegt vor. In $\mathbb{Z}/(6)$ gilt $2 \cdot 3 = 0$ und daher sind 2 und 3 Nullteiler in diesem Ring. Die folgende Aussage bedeutet, dass man in einer Gleichung Nichtnullteiler weg*kürzen* kann.

LEMMA 2.10. *Es sei $R$ ein kommutativer Ring und sei $f \in R$ ein Nichtnullteiler. Dann folgt aus einer Gleichung*

$$fx = fy\,,$$

*dass $x = y$ sein muss.*

*Beweis.* Man kann die Gleichung zu

$$0 = fx - fy = f(x - y).$$

umschreiben. Da $f$ ein Nichtnullteiler ist, ist $x - y = 0$, also $x = y$. □

Ein Ring, bei dem es außer der Null keine Nullteiler gibt, heißt *nullteilerfrei*.

DEFINITION 2.11. Ein kommutativer, nullteilerfreier, von null verschiedener Ring heißt *Integritätsbereich*.

Die Eigenschaft, dass jedes Element $\neq 0$ ein Nichtnullteiler ist, kann man auch so ausdrücken, dass aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt, bzw., dass mit $a \neq 0$ und $b \neq 0$ auch $ab \neq 0$ ist.

## Unterringe

Wir haben die Kette von Unterringen

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

im Sinne der folgenden Definition.

DEFINITION 2.12. Eine Teilmenge $S \subseteq R$ eines Ringes nennt man einen *Unterring*, wenn sowohl $(S, +, 0)$ eine Untergruppe von $(R, +, 0)$ als auch $(S, \cdot, 1)$ ein Untermonoid von $(R, \cdot, 1)$ ist.

Diese Bedingung besagt insbesondere, dass sich die Addition und die Multiplikation von $R$ auf $S$ einschränken lässt. Ein Unterring ist selbst ein Ring. Zum Nachweis, dass eine gegebene Teilmenge $S \subseteq R$ ein Unterring ist, hat man Folgendes zu zeigen.

(1) $0, 1 \in S$.
(2) $S$ ist abgeschlossen unter der Addition und der Multiplikation.
(3) Mit $f \in S$ ist auch $-f \in S$.

Die natürlichen Zahlen $\mathbb{N}$ erfüllen in $\mathbb{Z}$ die ersten beiden Bedingungen, aber nicht die dritte. Die Menge aller geraden Zahlen erfüllen alle Bedingungen außer der, dass 1 dazugehört. Ebenso ist $\{0\}$ kein Unterring, da darin die 1 fehlt (obwohl im Nullring für sich betrachtet $0 = 1$ ist, das ist aber nicht die 1 von $\mathbb{Z}$). Die Menge $\{-1, 0, 1\}$ erfüllt die erste und die dritte Bedingung und ist abgeschlossen unter der Multiplikation, aber nicht unter der Addition. Die ganzen Zahlen $\mathbb{Z}$ haben überhaupt nur sich selbst als Unterring.

Zu einer Teilmenge $M \subseteq R$ eines Ringes definiert man den durch $M$ *erzeugten Unterring* als den kleinsten Unterring von $R$, der $M$ umfasst. Wir bezeichnen ihn mit $\mathbb{Z}[M]$, da ja jeder Unterring automatisch alle Vielfachen der 1 enthalten muss. Dieser kleinste Unterring ist der Durchschnitt über alle Unterringe, die $M$ umfassen. Er besteht aus allen Termen, die man mit den Elementen aus $M$ und ihren Negativen mit Addition und Multiplikation erhalten kann.

# Abbildungsverzeichnis