Zahlentheoretische Funktionen

n sei eine natürliche Zahl ...
Eine zahlentheoretische Funktion ist eine auf der Menge der positiven ganzen Zahlen erklärte, reell- oder komplexwertige Funktion.
Eine zahlentheoretische Funktion f(n) heißt multiplikativ, wenn

$$f(m\,n) = f(m)\,f(n)$$

für teilerfremde m und n gilt. Für multiplikative, zahlentheoretische Funktionen f(n) gilt damit stets f(1) = 1.
Gilt f(m n) = f(m) f(n) ohne jede Einschränkung für m und n, so ist die Funktion f(n) total multiplikativ.

Eulersche Funktion $\phi(n)$

... Anzahl der zu n teilerfremden natürlichen Zahlen m, welche kleiner als n sind

$\phi(x)$ ist multiplikativ $\Rightarrow \phi(m*n) = \phi(m) * \phi(n)$ für ggT(mn,n)=1

Ist p Primzahl $\Rightarrow \phi(p) = p-1$
Ist $n=p^k$ und p Primzahl $\Rightarrow \phi(n) = p^{k-1}(p-1)$
Besitzt n die untereinander verschiedenen Primfaktoren $p_1, p_2, \ldots, p_r \Rightarrow \phi(n) = n\,(1-1/p_1)(1-1/p_2)\ldots(1-1/p_r)$

Weitere Funktionen

d(n) ... Anzahl aller positiven Teiler von n; multiplikative Funktion
$\sigma(n)$ ... Summe aller positiven Teiler von n
$\pi(n)$ ... Anzahl der Primzahlen kleiner gleich n
r(n) ... Anzahl der ganzzahligen Lösungspaare der Gleichung $x^2+y^2=n$

Satz von Euler-Fermat

Es seien a, n natürliche Zahlen und ggT(a, n) = 1 Dann gilt: $a^{\phi(n)} \equiv 1 \bmod n$
wobei $\phi(n)$ die Eulersche Phi-Funktion bezeichnet.
Da für prime Moduln p gilt: $\phi(p) = p-1$, geht für diese der Satz von Euler in den kleinen Satz von Fermat über.

Beweis: Sei $(Z/nZ)^\times = \{r_1, \ldots, r_{\phi(n)}\}$ die Menge der multiplikativ modulo n invertierbaren Elemente. Für jedes a mit ggT(a, n) = 1 ist dann $x \to ax$ eine Permutation von $(Z/nZ)^\times$, denn aus

$$ax \equiv ay \bmod n \quad \text{folgt } x \equiv y \bmod n$$

Da die Multiplikation kommutativ ist, folgt

$$r_1 \ldots r_{\phi(n)} \equiv (a\,r_1)\ldots(a\,r_{\phi(n)}) \equiv r_1 \ldots r_{\phi(n)}\, a^{\phi(n)} \bmod n$$

und da die r_i invertierbar sind für alle i, gilt

$$1 \equiv a^{\phi(n)} \bmod n.$$

Anwendung: Der Satz von Euler dient der Reduktion großer Exponenten modulo n. Praktische Anwendung findet er in dieser Eigenschaft in der computergestützten Kryptografie, beispielsweise im RSA-Verschlüsselungsverfahren.
Problem: Was ist die letzte Dezimalstelle von 7^{222}, d.h. welcher Zahl ist 7^{222} kongruent modulo 10?
Es ist ggT(7, 10) = 1 und $\phi(10) = 4$. Damit liefert der Satz von Euler

$$7^4 \equiv 1 \bmod 10 \quad \text{und} \quad 7^{222} \equiv 7^{4\cdot 55+2} \equiv (7^4)^{55}\cdot 7^2 \equiv 49 \equiv 9 \bmod 10$$

Allgemein gilt $a^b \equiv a^{b \bmod \phi(n)} \bmod n$, für teilerfremde natürliche a und b

Abschätzung der phi-Funktion

$$\Sigma_{n=1}^{N}\, \phi(n) = 1/(2\,\zeta(2))\, N^2 + O(N \log N)$$

wobei ζ die Riemannsche Zetafunktion und O das Landau-Symbol ist. D.h., im Mittel ist

$$\phi(n) / n \approx \pi^2 / 12$$

Eulersche Funktion (2)

Die Eulersche Funktion $\phi(n)$ gibt die Anzahl der zu n teilerfremden natürlichen Zahlen m an, welche kleiner als n sind.
Dabei zeigt sich, dass $\phi(n)$ nicht jede natürliche Zahl als Funktionswert annehmen kann. Schinzel bewies 1956, dass für jedes $k > 0$ die Werte $2\cdot z^k$ nicht auftreten.

1976 zeigte Mendelsohn, dass es unendlich viele Primzahlen p gibt, für die $2^k p$ ($k > 0$) nicht zum Wertebereich von $\phi(n)$ gehören.

Antikoindikator-Zahl

Unter einer Antikoindikator-Zahl (engl. noncototient, franz. anticoïndicateur) versteht man eine natürliche Zahl n, für die es keine natürliche Zahl m gibt, so dass $m - \phi(m) = n$ gilt, wobei $\phi(m)$ die Eulersche Funktion ist.
Die Differenz $m - \phi(m)$ wird Koindikator genannt. Mitunter wird die Funktion $\psi(m) = m - \phi(m)$ auch als Eulersche Psi-Funktion, oder kurz psi-Funktion, bezeichnet.

Die ersten Antikoindikator-Zahlen sind
10, 26, 34, 50, 52, 58, 86, 100, 116, 122, 130, 134, 146, 154, 170, 172, 186, 202, 206, 218, 222, 232, 244, 260, 266, 268, 274, 290, 292, 298, 310, 326, 340, 344, 346, 362, 366, 372, 386, 394, 404, 412, 436, 466, 470, 474, 482, 490, 518, 520, …
Durch Erdös und Sierpinski wurde die Vermutung aufgestellt, dass es unendlich viele derartige Zahlen gibt. 1995 wurde dies durch Browkin und Schinzel endgültig bewiesen. Eine sehr große Antikoindikator-Zahl ist $509203 \cdot 2^k$.

Noch nicht beantwortet ist die Vermutung, dass alle diese Zahlen gerade sind. Dies folgt aber aus der Goldbachschen Vermutung. Kann eine gerade Zahl n als Summe von zwei verschiedenen Primzahlen p und q dargestellt werden, dann ist

$$pq - \phi(pq) = pq - (p - 1)(q - 1) = p + q - 1 = n - 1$$

Damit kann keine ungerade Zahl größer 5 Antikoindikator-Zahl sein.

Carmichael-Funktion

Die Carmichael-Funktion λ ist eine zahlentheoretische Funktion, die eng mit der Euler-Funktion $\phi(n)$ zusammenhängt. Wie diese hat λ eine Beziehung zu Primzahlen und zu der Ordnung ganzer Zahlen. Der Name der Funktion geht auf den US-amerikanischen Mathematiker Robert D.Carmichael (1879-1967) zurück. Die Definition der Carmichael-Funktion $\lambda: N \rightarrow N$ ist anspruchsvoll:
Ist die Primfaktorzerlegung von n gegeben durch

$n = p_1^{a}1 \ldots p_k^{a}k$, so gilt $\lambda(n) = kgV[\lambda(p_1^{a}1), \ldots, \lambda(p_k^{a}k)]$, wo

$(p_i^{a}i) = 2^{a}i^{-2}$ wenn $p_i = 2$ und $a_i > 2$, sonst $p_i^{a}{}_{i-1}$ $(p_{i-1)}$

Beispiel: Es sei n = 12, mit der Primzahlzerlegung $12 = 2^2 \cdot 3$; dann ist $\lambda(12) = kgV[\lambda(2^2), \lambda(3)]$, mit $\lambda(2^2) = 1$ und $\lambda(3) = 2$, also $\lambda(12) = 2$. Mit etwas Aufwand ermittelt man die λ-Werte für die ersten natürlichen Zahlen n = 1, 2, …, 15 zu

$\lambda(n) = 1, 1, 2, 2, 4, 2, 6, 2, 6, 4, 10, 2, 12, 6, 4$

Eine der Eigenschaften der Carmichael-Funktion lässt sich für jede natürliche Zahl n beweisen: Der Wert der Carmichael-Funktion $\lambda(n)$ teilt stets den Wert der Euler-Funktion $\phi(n)$, d.h. $\lambda(n) | \phi(n)$. Der Wert der Carmichael-Funktion für eine Primzahl p ist einfach zu ermitteln:

$\lambda(p) = p-1$; p prim

Ist n das Produkt zweier Primzahlen p und q, n = p q, so gilt $\lambda(pq) = kgV(p-1, q-1)$. Beispiel: $\lambda(15) = kgV(3-1, 5-1) = 4$. Ferner gilt der folgende wichtige Satz.

Satz von Carmichael

Für zwei natürliche teilerfremde Zahlen m, n gilt $m^{\lambda(n)} = 1 \bmod n$.
Für festes n und variables m ist $\lambda(n)$ der kleinste Exponent mit dieser Eigenschaft.

Dirichletsches Produkt

Es seien f(n) und g(n) zwei zahlentheoretische Funktionen. Die zahlentheoretische Funktion

$$h(n) = \Sigma_{t/n}\, f(t)\, g(n/t)$$

heißt ihr Dirichletsches Produkt. Der Summationsindex bedeutet, dass die Summer über alle Teiler t von n zu bilden ist.
Das Dirichletsche Produkt ist kommutativ und assoziativ.

Sätze über zahlentheoretische Funktionen

1. Die Menge der zahlentheoretischen Funktionen f(n) mit $f(1) \neq 0$ bildet bezüglich der Dirichletschen Multiplikation eine kommutative Gruppe.
2. Sind f und g multiplikative Funktionen, so ist auch f*g multiplikativ.

3. Die zahlentheoretischen Funktionen g(n) und f(n)*g(n) seien mutiplikativ. Dann ist auch f(n) multiplikativ.

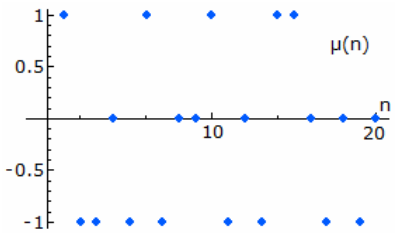
Möbiussche μ-Funktion

Die zu f(n) = 1 bezüglich der Dirichletschen Multiplikation inverse Funktion heißt Möbiussche μ-Funktion.

Es gilt μ(1) = 1 μ(p) = -1 , p ... Primzahl

Mit der eindeutigen Primfaktorzerlegung für $n = \Sigma_{i=1}^{r} p_i^{a}i$ gilt

$\mu(n) = (-1)^r$ für $a_1 = a_2 = ... = a_r = 1$ μ(n) = 0 für alle anderen Fälle



Die zahlentheoretisch wichtige Möbius-Funktion μ(n) kann auch wie folgt definiert werden:
μ(n) = 1 , wenn n quadratfrei ist und eine gerade Azahl verschiedener Primteiler besitzt
μ(n) = -1 , wenn n quadratfrei ist und eine ungerade Azahl verschiedener Primteiler besitzt
μ(n) = 0 , wenn n nicht quadratfrei ist
Weiterhin ist μ(1) = 1. μ(0) ist undefiniert.

Die Folge der Funktionswerte der Möbius-Funktion beginnt mit
1,-1,-1,0,-1,1,-1,0,0,1,-1,0,-1,1,1,0,-1,0,-1,0,1,1,-1,0,0, …

Zahlen mit μ = -1 und genau drei Primfaktoren werden sphenische Zahlen genannt. Die ersten sind
30, 42, 66, 70, 78, 102, 105, 110, 114, 130, 138, 154, 165, 170, 174, 182, 186, 190, 195, 222, …
Die kleinsten Zahlen mit μ = -1 und genau fünf Primfaktoren sind
2310, 2730, 3570, 3990, 4290, 4830, 5610, 6006, 6090, 6270, 6510, 6630, 7410, 7590, 7770, 7854, 8610, 8778, 8970, 9030, 9282, 9570, 9690, …

Die Möbius-Funktion ist mit anderen wichtigen Funktionen verbunden.
Mertens-Funktion $M(n) = \Sigma_{k=1}^{n} \mu(k)$
Riemannsche Zeta-Funktion $1/\zeta(s) = \Sigma_{n=1}^{\infty} \mu(n)/n^s$

Möbiussche Formeln

Ist g(n) eine multiplikative, zahlentheoretische Funktion, so gilt

$F(n) = f(n) * g(n) \Leftrightarrow f(n) = F(n) * [\mu(n)\, g(n)]$

$g(n) = \Sigma_{t/n}\, f(t) \Rightarrow f(n) = \Sigma_{t/n}\, \mu(t)\, g(n/t)$

$h(n) = \Sigma_{t/n}\, \mu(t)\, f(n/t) \Rightarrow f(n) = \Sigma_{t/n}\, h(n)$

Tschebyschowsche Funktionen

Als Tschebyschowsche Funktionen werden bezeichnet

$\vartheta(x) = \Sigma_{p\le x} \ln p$ $\psi(x) = \Sigma_{p\wedge m\le x}\, m \ln p$

Die zweite Summe ist wie folgt zu verstehen: ln p tritt als Summand genau n-mal auf, wenn p^m die höchste Potenz von p ist, welche x nicht überschreitet, zum Beispiel

$\psi(10) = 3 \ln 2 + 2 \ln 3 + \ln 5 + \ln 7$

Aus der Definition folgt $\vartheta(x) = \ln (\Pi_{p\le x}\, p)$

$\psi(x) = \ln$ (kgV aller positiven ganzen Zahlen $\le x$)

Mangoldt-Funktion

Die Mangoldt-Funktion (nach dem deutschen Mathematiker Hans von Mangoldt) ist eine zahlentheoretische Funktion, die mit Λ bezeichnet wird. Die Mangoldtsche Funktion ist definiert als

$\Lambda(n) = \ln p$, wenn n sich als $n = p^k$ darstellen lässt,

wobei p prim und k eine natürliche Zahl sind. Andernfalls ist $\Lambda(n) = 0$.
Die Funktion ist weder additiv noch multiplikativ.
Meist wird die Funktion $e^{\Lambda(n)}$ betrachtet. Für diese Funktion wird

$e^{\Lambda(n)} = kgV(1,2,…,n) / kgv(1,2,3,…,n-1)$

Die erste Werte sind

1, 2, 3, 2, 5, 1, 7, 2, 3, 1, 11, 1, 13, 1, 1, 2, 17, 1, 19, 1, 1, 1, 23, 1, 5, 1, 3, 1, 29, 1, 31, 2, 1, 1, 1, 1, 37, 1, 1, 1, 41, 1, 43, 1, 1, 1, 47, 1, 7, 1, 1, 1, 53, 1, 1, 1, 1, 1, 59, 1, 61, 1, 1, 2, 1, 1, 67, 1, 1, 1, 71, 1, 73, 1, 1, 1, 1, 1, 79, 1, 3, 1, 83, 1, 1, 1, 1, 1, 89, 1, 1, 1, 1, 1, 1, …
Die summierte Mangoldt-Funktion

$\psi(n) = \Sigma_{i=1}^{n} \Lambda(i)$

ist eine der Tschebyschowschen Funktionen. Diese ist beim Beweis des Primzahlsatzes von Bedeutung.
Zwischen der Mangoldt-Funktion μ(n) und der Möbius-Funktion bestehen die Beziehungen:

$\Sigma_{d|n} \mu(n/d) \ln d = \Lambda(n)$ $\quad\quad$ $\Sigma_{d|n} \Lambda(d) = \ln n$

$\Sigma_{d|n} \mu(d) \ln d = -\Lambda(n)$ $\quad\quad$ $\Sigma_{d|n} \mu(n/d) \Lambda(d) = -\mu(n) \ln n$

Liouville-Funktion

Die Liouville-Funktion (nach Joseph Liouville), ist eine multiplikative zahlentheoretische Funktion. Sie ist definiert durch $\lambda(n) = (-1)^{\Omega(n)}$
wobei $\Omega(n)$ die Anzahl der nicht notwendigerweise verschiedenen Primfaktoren bezeichnet.
Außerdem wird $\lambda(0) = 0$ und $\lambda(1) = 1$ festgelegt.
Die ersten Werte der Liouville-Funktion für n = 1, 2, … sind
1, -1, -1, 1, -1, 1, -1, -1, 1, 1, -1, -1, -1, 1, 1, 1, -1, -1, -1, -1, 1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, 1, 1, 1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1, 1, -1, -1, 1, -1, -1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1, …
Weiterhin gilt

$\Sigma_{d|n} \lambda(d) = 1$, wenn n eine Quadratzahl ist, sonst = 0

Für die Summe $L(n) = \Sigma_{k=1}^{n} \lambda(k)$ vermutete Polya, dass stets L(n) < 0 gilt.
Diese Vermutung wurde widerlegt; das kleinste Gegenbeispiel ist n = 906150257. Es ist noch nicht bekannt, ob L sein Vorzeichen unendlich oft wechselt.

Sigma-Funktion

Die Sigma-Funktion ist eine zahlentheoretische Funktion: $\sigma(n)$ … Summe aller positiven Teiler von n
Die Sigma-Funktion $\sigma(n)$ ist multiplikativ. Dabei ist für eine Primzahl p : $\sigma(p) = p+1$ und es gilt der Satz:
Ist p Primzahl und n natürliche Zahl, n > 0, so ist $\sigma(p^n) = (p^{n+1} - 1)/(p-1)$. d.h. z.B.
$\sigma(2000) = \sigma(2^4 5^3) = \sigma(2^4)\ \sigma(5^3) = (2^5 - 1)/(2-1)\ (5^4 - 1)/(5-1) = 31 \cdot 156 = 4836$.

Die verallgemeinerte Sigmafunktion $\sigma(n, k)$ in n.ter Potenz gibt für k = 0 die Anzahl der Teiler einer Zahl an und sonst die Summe der Teiler in n.ter Potenz. Allgemein gilt $\sigma_k(n) = \Sigma_{d|n} d^k$
$\sigma_0(n)$ hat die Werte 1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, … für $n \in N$.
$\sigma_1(n)$ hat die Werte 1, 3, 4, 7, 6, 12, 8, 15, 13, 18, … für $n \in N$
$\sigma_2(n)$ hat die Werte 1, 5, 10, 21, 26, 50, 50, 85, 91, 130, … für $n \in N$
$\sigma_3(n)$ hat die Werte 1, 9, 28, 73, 126, 252, 344, 585, 757, 1134, … für $n \in N$

Wallis-Problem

Gesucht sind alle Paare (x, y) natürlicher Zahlen, für welche $\sigma(x^2) = \sigma(y^2)$ gilt, wobei $\sigma(n)$ die zahlentheoretische Funktion der Summe aller positiven Teiler von n darstellt.
Aus der kleinsten bekannten Lösung (4 , 5) erhält man für m = 3, 7, 9, 11, 13, 17, 19, 23, ... mit (mx, my) weitere Lösungen des Wallis-Problems. Weitere n-Tupel (x_1 , x_2, ..., x_n), welche jeweils paarweise das Wallis-Problem erfüllen, sind
(326, 407), (406, 489), (627, 749), (740, 878), (880, 1451), (888, 1102), (1026, 1208), (1110, 1943), (1284, 1528, 1605), (1510, 1809), (1628, 1630, 2035), (1956, 2030, 2445), (2013, 2557), (2072, 3097), (2508, 2996, 3135, 3745), ...

Smarandache-Funktion

Die Smarandache-Funktion ist zahlentheoretische Funktion, die wie folgt definiert ist:
Die Smarandache-Funktion μ(n) ist die kleinste natürliche Zahl, für die n die Fakultät von μ(n) teilt. d.h. μ(n) ist die kleinste natürliche Zahl, für die gilt $n \mid \mu(n)!$
Für den Wert μ(8) testet man die kleinste der Zahlen 1!, 2!, 3!, …, die durch 8 teilbar ist. Hier wird 4! = 24 als Vielfaches von 8, d.h. μ(8) = 4.
Die ersten Werte der Funktion für n = 1, 2, 3, … sind

1, 2, 3, 4, 5, 3, 7, 4, 6, 5, 11, 4, 13, 7, 5, 6, 17, 6, 19, 5, 7, 11, 23, 4, 10, 13, 9, 7, 29, 5, 31, 8, 11, 17, 7, 6, 37, 19, 13, 5, 41, 7, 43, 11, 6, 23, 47, 6, 14, 10, 17, 13, 53, 9, 11, 7, 19, 29, 59, 5, 61, 31, 7, 8, 13, 11, 67, 17, 23, 7, 71, 6, 73, 37, 10, 19, 11, 13, 79, 6, 9, 41, 83, 7, …
Mitunter wird μ(1) auch gleich 0 gesetzt.
Zuerst wurde diese Funktion 1883 von Lucas, 1887 von Neuberg und 1918 von Kempner beschrieben. 1980 wurde sie von Florentin Smarandache wiederentdeckt.

Für alle n gilt $\mu(n) \leq n$, für Primzahlen p folglich $\mu(p) = p$. Außerdem ist $\mu(n!) = n$. Ist t der größte Primfaktor von n, dann wird auch $\mu(n) \geq t$.
Durch Tutescu wird vermutet, dass für zwei aufeinanderfolgende Zahlen die Werte der Smarandache-Funktion verschieden sind: $\mu(n) \neq \mu(n+1)$
Bisher konnte die Vermutung durch Computereinsatz bis 10^9 nachgewiesen werden.

Pseudosmarandache-Funktion

Unter dem Funktionswert der pseudosmarandache-Funktion Z(n) versteht man die kleinste ganze natürliche Zahl, für die $1 + 2 + 3 + \ldots + Z(n)$
Vielfaches von n ist, d.h. das kleinste natürliche n, für das gilt $n \mid Z(n)(Z(n)+1) / 2$
Die ersten Werte sind
1, 3, 2, 7, 4, 3, 6, 15, 8, 4, 10, 8, 12, 7, 5, 31, 16, 8, 18, 15, 6, 11, 22, 15, 24, 12, 26, 7, 28, 15, 30, 63, 11, 16, 14, 8, 36, 19, 12, 15, 40, 20, 42, 32, 9, 23, 46, 32, 48, 24, 17, 39, 52, 27, 10, 48, 18, 28, 58, 15, 60, 31, 27, 127, 25, 11, 66, 16, 23, 20, 70, 63, 72, 36, 24, …

Additive Funktion

Eine Funktion f(x) wird additiv genannt, wenn für alle relativ primen a, b des Definitionsbereiches die Beziehung
$f(a+b) = f(a) + f(b)$ gilt.
Gilt die Beziehung für alle a, b, auch für zueinander nicht prime, so heißt die Funktion vollständig additiv. Additive und vollständig additive Funktionen sind im Allgemeinen nicht umkehrbar.

Beispiele: Primteilersummenfunktion $f(n) = a_0(n)$, welche die Summe der Primteiler der natürlichen Zahl n darstellt, z.B. $a_0(20) = a_0(2^2 \cdot 5) = 2 + 2 + 5 = 9$.
$a_0(4) = 4$
$a_0(144) = a_0(2^4 \cdot 3^2) = a_0(2^4) + a_0(3^2) = 8 + 6 = 14$
echte Primteilersummenfunktion $g(n) = a_1(n)$, welche de Summe der verschiedenen Primteiler der natürlichen Zahl n darstellt, z.B. $a_1(1) = 0$, $a_1(20) = 2 + 5 = 7$.
$a_1(144) = a_1(2^4 \cdot 3^2) = a_1(2^4) + a_1(3^2) = 2 + 3 = 5$

Primteilerfunktion $\Omega(n)$, die Anzahl der Primteiler einer natürlichen Zahl n
echte Primteilerfunktion $\omega(n)$, die Anzahl der verschiedenen Primteiler einer natürlichen Zahl n
Das Radikal einer natürlichen Zahl n ist das Produkt ihrer verschiedenen Primteiler.

Primfakultät

Die Primfakultät von n ist das Produkt aller Primzahlen kleiner oder gleich n. Die Primfakultär ist eine natürliche Definition für das Produkt von Primzahlen. Als Notation verwendet man n#.
In der Zahlentheorie ist es üblich, bei der Betrachtung der Primfakultät nicht die multiplikative Schreibweise, sondern die additive zu verwenden, d.h statt n# wird ln(n#) untersucht.
Der Logarithmus der Primfakultät ist dabei die Tschebyschowsche Funktion $\vartheta(n) = \Sigma_{p \leq n} \ln p = \ln (n\#)$

Quadratfreier Kern

Der quadratfreie Kern sfk(n); squarefree kernel; von n ist das Produkt der verschiedenen Primfaktoren von n.
Damit wird die Primfakultät mit der gewöhnlichen Fakultät n! und dem kleinsten gemeinsamen Vielfachen der ersten n Zahlen in Zusammenhang gebracht: $n\# = sfk(n!)$
Die Primfakultät ist damit der quadratfreie Kern der gewöhnlichen Fakultät, und auch der quadratfreie Kern des kleinsten gemeinsamen Vielfachen des Anfangsabschnitts der natürlichen Zahlen.

Sphenische Zahlen

Als sphenische Zahl (griechisch $\sigma\phi\eta\nu$ = keilförmig) wird eine positive ganze Zahl bezeichnet, die das Produkt von genau drei verschiedenen Primzahlen ist.
Alle sphenischen Zahlen besitzten genau acht Teiler. Sind p, q, r deren Primfaktoren, so sind die Teiler

{1, p, q, r, pq, pr, qr, pqr}

Sphenische Zahlen sind quadratfrei und haben einen Möbius-Funktionswert von -1.
Die ersten sphenischen Zahlen sind

30, 42, 66, 70, 78, 102, 105, 110, 114, 130, 138, 154, …

Die größte gegenwärtig (2007) bekannte sphenische Zahl ist

$(2^{32582657} - 1)\cdot(2^{30402457} - 1)\cdot(2^{25964951} - 1)$

Deren Primfaktoren sind die größten bekannten Primzahlen (Mersennesche Primzahlen).

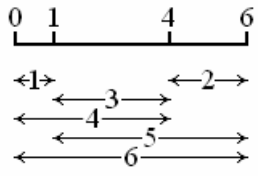
Die ersten zwei aufeinanderfolgenden sphenischen Zahlen sind

230 = 2·5·23 und 231 = 3·7·11,

die ersten drei aufeinanderfolgenden

1309 = 7·11·17, 1310 = 2·5·131 und 1311 = 3·19·23.

Vier und mehr unmittelbar aufeinanderfolgende sphenische Zahlen kann es nicht geben, da dann wenigstens eine durch 4 teilbar und somit nicht quadratfrei wäre.



Golomb-Lineal

Ein Golomb-Lineal ist ein Lineal, bei dem es keine zwei Markierungen mit dem gleichen Abstand zueinander gibt. Die Abbildung zeigt ein Golomb-Lineal der Ordnung 4 und Länge 6. Golomb-Lineale wurden nach Solomon W.Golomb benannt.
Golomb-Lineale werden nach Ordnung und Länge kategorisiert. Die Ordnung eines Golomb-Lineals ist definiert durch die Anzahl der Markierungen, die Länge durch den größten Abstand zweier Markierungen, wobei die kleinste Markierung üblicherweise auf 0 gesetzt wird.

Kann ein Golomb-Lineal alle Abstände bis zu seiner Länge messen, wird es ein perfektes Golomb-Lineal genannt. Ein Golomb-Lineal ist optimal, wenn es keine kürzeren Lineale derselben Ordnung gibt. Optimale Golomb-Lineale für eine gegebene Ordnung zu finden, ist eine rechenintensive Aufgabe. Mittels verteiltem Rechnen wurde der bisher bekannte Kandidat für optimale Golomb-Lineale der Ordnung 24 bestätigt.
Golomb-Lineale werden beim Entwurf von Gruppenantennen, wie beispielsweise Radioteleskopen, verwendet. Antennen in [0,1,4,6] Golomb-Anordnung findet man häufig bei Mobilfunkmasten.

Induktive Definition

Ähnlich wie bei reellen Zahlenfolgen kann man mittels Rekursionsgleichungen Funktionen in den natürlichen Zahlen definieren.
Zum Beispiel wäre $\phi(0) = 1$; $\phi(n+1) = \phi(n) + 2$
die Definition der ungeraden natürlichen Zahlen.
Für die Fakultät n! ergibt sich in den natürlichen Zahlen

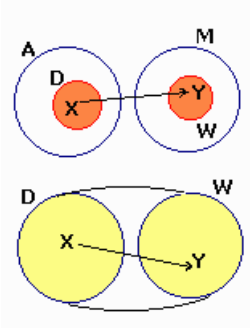
$0! = 1$; $(n+1)! = (n+1)\ n!$

Weitere Beispiele sind
Stirling-Zahlen $s(n,r) = s(n - 1,r - 1) + (n - 1) \cdot s(n - 1,r)$

mit den Anfangswerten $s(0,0) = 1$; $s(n,n) = 1$; $s(n,0) = 0$ für $n > 0$; $s(0,r) = 0$ für $r > 0$

Delannoy-Zahlen $D(a,b) = D(a-1,b) + D(a,b-1) + D(a-1,b-1)$ mit $D(0,0) = 1$
Schröder-Zahlen $S(n) = S(n-1) + \Sigma\ S(k) \cdot S(n-1-k)$; Summenbildung von k = 0 bis n-1
mit S(0) = 1 usw.
Insbesondere bei der Definition von Mengen und in der theoretischen Informatik werden induktive Definitionen gern verwendet.

Mengenabbildungen (Relationen)



Allgemein versteht man unter einer n-stelligen Relation R in einer Menge A eine Teilmenge von $A^n = A \times A \times \ldots \times A$, d.h. $R \subseteq A^n$

Jede Teilmenge $R \subseteq A \times B$ heißt zweistellige Relation oder binäre Relation zwischen A und B. Schreibweise: x R y mit x aus A und y aus B; Ist A = B = M, dann heißt R Relation auf M.
Für A = B ist eine binäre Relation eine Korrespondenz von A in A.
Mit jeder binären Relation R ist auch R^{-1}; die Umkehrrelation; eine Relation und mit zwei binären Relationen R und S auch die Verknüpfung R • S eine Relation.

Eigenschaften:

R ist reflexiv $\Leftrightarrow$ für alle x: x R x
R ist symmetrisch $\Leftrightarrow$ für alle x,y: Aus x R y folgt y R x
R ist transitiv $\Leftrightarrow$ für alle x,y,z: Aus x R y und y R z folgt x R z
R ist irreflexiv $\Leftrightarrow$ für kein x gilt x R x
R ist asymmetrisch $\Leftrightarrow$ für kein x,y folgt aus x R y auch y R x
R ist antisymmetrisch $\Leftrightarrow$ für alle x,y folgt aus x R y und y R x sofort x = y
R ist identitiv $\Leftrightarrow$ für alle x,y aus x R y und y R x folgt x = y
R ist linear $\Leftrightarrow$ für alle x,y gilt: es existiert mindestens eine der Beziehungen x R y, y R x oder x = y
Mit jeder Relation R ist auch die Umkehrung R^{-1} reflexiv, irreflexiv, symmetrisch, asymmetrisch oder antisymmetrisch. Außerdem folgt aus der Asymmetrie die Irreflexivität.

Spezielle Relationen

Für spezielle Relationen R auf einer Menge A wird definiert:

R heißt reflexive teilweise Ordnung auf A $\Leftrightarrow$ R ist reflexiv, transitiv und antisymmetrisch
R heißt lineare Ordnung (totale Ordnung) $\Leftrightarrow$ R ist transitiv, antisymmetrisch und linear
R heißt irreflexive teilweise Ordnung auf A $\Leftrightarrow$ R ist irreflexiv und transitiv
R heißt Äquivalenzrelation auf A $\Leftrightarrow$ R ist reflexiv, symmetrisch und transitiv.

Für die (gewöhnlichen) Ordnungsrelationen auf den reellen Zahlen ergibt sich:
Es seien a, b, c reelle Zahlen. Dann gilt für alle a, b und c

$a \leq a$; $\leq$ ist reflexiv
$a \ \ b \Rightarrow (\neg(b < a) \vee a = b)$; $\leq$ ist antisymmetrisch
$(a \leq b \wedge b \leq c) \Rightarrow a \leq c$; $\leq$ ist transitiv
$a < b \Rightarrow a \neq b$; $<$ ist irreflexiv
$(a < b \wedge b < c) \Rightarrow a < c$; $<$ ist transitiv
$a \leq b \vee b \leq a$; $\leq$ ist linear

Allgemein kann man Ordnungen in einer Menge A als Festlegungen einer Rangfolge von Elemente der Menge A auffassen, wobei Ordnungen nicht unbedingt linear sein müssen, d.h., nicht für jedes Paar von Elementen aus A muss festgelegt sein, welches vom größeren Rang ist.
Eine reflexive teilweise Ordnung kann mit einem Hasse-Diagramm veranschaulicht werden.

Ordnungsrelation

Eine binäre Relation R in einer Menge A heißt Ordnung oder Ordnungsrelation, wenn R reflexiv, antisymmetrisch und transitiv ist. Man spricht auch von einer teilweisen Ordnung.
Ist R zusätzlich linear, so heißt R vollständige Ordnung, vollständige Ordnungsrelation oder Kette. Die Menge A heißt dann durch R geordnet bzw. vollständig geordnet. In einer vollständig geordneten Menge sind also je zwei Elemente vergleichbar. Statt aRb verwendet man auch die Bezeichnung $a \leq_R b$ oder $a \leq b$, wenn die Ordnungsrelation R aus dem Zusammenhang bekannt ist.
Anstelle von Ordnung ist auch die Bezeichnung Halbordnung oder partielle Ordnung üblich.
R heißt reflexive Ordnungsrelation, wenn sie reflexiv, transitiv, identitiv und linear ist.
R heißt irreflexive Ordnungsrelation, wenn sie irreflexiv, transitiv und linear ist.

Eine teilweise Ordnung R in A heißt Wohlordnung genau dann, wenn jede Teilmenge ein kleinstes Element besitzt.
Jede Wohlordnung ist linear. Denn mit zwei Elementen x, y besitzt die Menge {x, y} ein kleinstes Element; oBdA sei dies x. Dann gilt x R y.
Andererseits ist aber nicht jede linear geordnete Menge wohlgeordnet. In Q mit der natürlichen Ordnung ≤ sei B = {q ∈ Q | 2 ≤ q²}. Das kleinste Element dieser Menge wäre √2, was keine rationale Zahl ist.

Beispiele: Die Zahlenbereiche N, Z, Q, R sind vollständig geordnet. Die Teilmengenbeziehung ist eine Ordnung, die nicht vollständig ist. Die lexikografische Ordnung auf den Wörtern der deutschen Sprache ist eine Kette.

Teilweise geordnete Mengen

Eine Menge M heißt teilweise geordnet, oder halbgeordnet wenn sie mit einer Relation ≤ versehen ist, die den folgenden Eigenschaften genügt:

- x ≤ x für alle x ∈ M (Reflexivität)
- für alle x, y ∈ M gilt: Aus x ≤ y und y ≤ x folgt x = y (Antisymmetrie)
- für alle x, y, z ∈ M gilt: Aus x ≤ y und y ≤ z folgt x ≤ z (Transitivität)

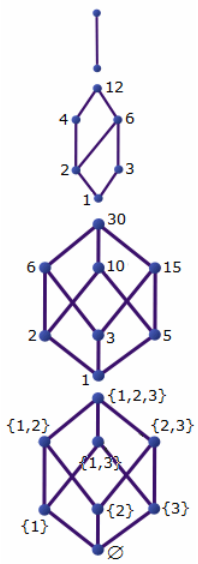
Im Englischen heißen teilweise geordnete Mengen auch posets von partially ordered set. Die Bezeichnung "teilweise" wird mitunter auch weggelassen.
Gilt für zwei Elemente x und y weder x ≤ y noch y ≤ x, so heißen die Elemente unvergleichbar. Im Allgemeinen müssen in einer teilweisen Ordnung zwei Elemente nicht vergleichbar sein. Sind je zwei Elemente vergleichbar, so heißt die Ordnung linear.

- ∈ ist linear genau dann, wenn für alle x, y: x ∈ y oder y ∈ x

Ist die Ordnung linear, so spricht man auch von einer totalen Ordnung oder einer kettengeordneten Menge. Eine total geordnete Teilmenge von M heißt auch Kette. Aus der Linearität folgt die Reflexivität.

Beispiele

1) Die Zahlenbereiche wie die natürlichen Zahlen N, ganzen Zahlen Z oder reellen Zahlen R bilden bzgl. der natürlichen Ordnungsrelation ∈ lineare Ordnungen.
2) Die natürlichen Zahlen N bilden bzgl. der Teilbarkeit eine teilweise Ordnung. Diese Ordnung ist nicht linear, da zwei teilerfremde Zahlen nicht vergleichbar sind.
3) Die Potenzmenge einer beliebigen Menge M bildet bzgl. der Inklusion eine teilweise geordnete Menge. Diese Ordnung ist nicht linear.

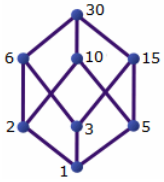


Hasse-Diagramm

Für endliche geordnete Mengen veranschaulicht man die Ordnungsstruktur in Form von speziellen Graphen. Diese werden Ordnungsdiagramme oder Hassediagramme genannt.
Die Elemente der geordneten Menge werden als Punkte dargestellt und zwei direkt vergleichbare Elemente werden durch Strecken verbunden, wobei kleinere Elemente weiter unten stehen. Die obere Grafik veranschaulicht eine aus zwei Elementen bestehende linear geordnete Menge.

2.Abbildung: Das Hasse-Diagramm zeigt die Teiler der Zahl 12, bezüglich der durch die Teilbarkeit gegebenen Ordnungsbeziehung.
3.Abbildung: Für die Zahl 30 können die Teiler durch dieses Ordnungsdiagramm veranschaulicht werden.
untere Abbildung: Zu einem gleich aussehenden Diagramm gelangt man, indem man von einer dreielementigen Menge ausgeht und die Inklusion als Ordnung in ihrer Potenzmenge definiert.

Majoranten und Minoranten



Sei M eine teilweise geordnete Menge mit der Ordnung ≤. Für eine nichtleere Teilmenge A ⊆ M heißt ein Element s ∈ M obere Schranke von A, wenn a ≤ s für alle a ∈ A gilt. Analog heißt s untere Schranke von A, wenn s ≤ a für alle a ∈ A gilt. Existieren die obere (untere) Schranke, so heißt die Menge nach oben (unten) beschränkt.

Die Menge aller oberen Schranken von A heißt Majorante von A (Bezeichnung: Ma(A)) und die Menge aller unteren Schranken heißt Minorante von A und wird mit Mi(A) bezeichnet.

$Ma(A) = \{x \in M \mid a \leq x \ \forall a \in A\}$ $Mi(A) = \{x \in M \mid x \leq a \ \forall a \in A\}$

Beispiel (Abbildung): Betrachtet man die Zahl 30 und ihre Teiler mit der Ordnung bezüglich der Teilbarkeit als Ordnung, und sei A = {2; 5}. Dann ist Mi(A) = {1} und Ma(A) = {10; 30}.

Eigenschaften von Minorante und Majorante

Sei M eine teilweise geordnete Menge mit der Ordnung ≤. Für nichtleere Teilmengen $A, B \subseteq M$ gilt dann

$A \subseteq Ma(Mi(A))$ und $A \subseteq Mi(Ma(A))$

$A \subseteq B \Rightarrow Ma(B) \subseteq Ma(A)$ und $Mi(B) \subseteq Mi(A)$

$Mi(Ma(Mi(A))) = Mi(A)$ und $Ma(Mi(Ma(A))) = Ma(A)$

für $a, b \in M$ gilt: $a \leq b \Leftrightarrow Mi(a) \subseteq Mi(b) \Leftrightarrow Ma(b) \subseteq Mi(a)$

Infimum und Supremum

Sei M eine teilweise geordnete Menge mit der Ordnung ≤ und A eine nichtleere Teilmenge $A \subseteq M$.

Minimum und Maximum

Unter dem Minimum min(A) von A versteht man alle unteren Schranken von A, die zu A gehören und dementsprechend ist das Maximum max(A) die Menge aller oberen Schranken von A, die zu A gehört. Mittels Minorante und Majorante kann man definieren

$min(A) = A \cap Mi(A)$ $max(A) = A \cap Ma(A)$ (*)

Existieren Minimum (Maximum) einer Menge A so sind sie eindeutig bestimmt.

Infimum und Supremum

Das Infimum inf(A) einer Menge A ist die größte untere Schranke von A und das Supremum sup(A) ist die kleinste obere Schranke von A. Mit (*) wird

$inf(A) = max(Mi(A)) = Mi(A) \cap Ma(Mi(A))$

$sup(A) = min(Ma(A)) = Ma(A) \cap Mi(Ma(A))$

Auch Infimum und Supremum sind eindeutig bestimmt, sofern sie existieren, da sie als Minimum bzw. Maximum von Minoranten- bzw. Majorantenmengen definiert sind.

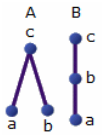
Sätze: Sei s = inf(A), dann gilt $s \leq a$ für alle $a \leq A$ und für alle $t \leq Mi(A)$ gilt: $s \geq t$. Das Infimum ist die größte untere Schranke. Insbesondere gilt: falls $x \leq a$ für alle $a \leq A$, dann ist auch $x \leq inf(A)$.

Sei s = sup(A), dann gilt $a \leq s$ für alle $a \leq A$ und für alle $t \leq Ma(A)$ gilt: $t \geq s$. Das Supremum ist die kleinste untere Schranke. Insbesondere gilt: falls $a \leq x$ für alle $a \leq A$, dann ist auch $x \geq sup(A)$.

Sei (M, ≤) eine teilweise geordnete Menge. $A \subseteq M$ eine Teilmenge. Dann gilt:

Existiert das Minimum (Maximum) von A so stimmt es mit dem Infimum (Supremum) überein.

Aus a = inf(A) bzw. a = sup(A) und $a \leq A$ folgt a = max(A) bzw. a = min(A)



Isotone Abbildung

Es seien M und N zwei teilweise geordnete Mengen und $f: M \to N$ eine Abbildung. Die Abbildung f heißt isoton oder ordnungserhaltend genau dann, wenn für alle $a, b \in M$ gilt

$a \leq b \Rightarrow f(a) \leq f(b)$

Die Abbildung heißt antiton, wenn gilt $a \leq b \Rightarrow f(a) \geq f(b)$

f ist ein Ordnungsisomorphismus zwischen M und N genau dann, wenn f bijektiv ist und sowohl f als auch die Umkehrabbildung f^{-1} isoton sind. Die beiden Mengen M und N heißen dann auch ordnungsisomorph.

Eine isotone Bijektion muss nicht notwendigerweise eine isotone Umkehrung haben, daher ist diese Forderung in der Definition des Ordnungsisomorphismus wesentlich.

Für die abgebildeten Hassediagramme ist die identische Abbildung $A \to B$ ($a \to a$, $b \to b$, $c \to c$) isoton. Die Umkehrung ist nicht isoton, da $a \leq b$ in B; jedoch a und b in A unvergleichbar sind.

Für linear geordnete Mengen gilt: Seien M und N linear geordnete Mengen und $f: M \to N$ eine isotone Bijektion. Dann ist die Umkehrabbildung von f isoton und damit ist f ein Ordnungsisomorphismus.

Umkehrrelation ... Zu jeder Relation existiert eine Umkehrrelation

Äquivalenzrelation

Ein Äquivalenzrelation ist eine Relation, welche reflexiv, symmetrisch und transitiv ist. Für a R b verwendet man a ~ b, wenn die Äquivalenzrelation bekannt ist, und sagt, a ist äquivalent zu b.

reflexiv a ~ a
symmetrisch aus a ~ b folgt b ~ a
transitiv aus a ~ b und b ~ c folgt a ~ c

Beispiel: A = Z und m natürliche Zahl > 0. Dann gilt a ~ b genau dann, wenn a und b bei Division durch m den gleichen Rest lassen (Kongruenzrechnung modulo m)

Äquivalenzklassen

Eine Menge M wird durch jede Äquivalenzrelation in Äquivalenzklassen zerlegt, welche paarweise elementfremd (disjunkt) sind.
Alle Elemente einer Klasse sind untereinander äquivalent, d.h. jedes a aus der Klasse kann als Repräsentant der Klasse gewählt werden. Die Menge aller Äquivalenzklassen A | R heißt das Restesystem von R nach A.
Auf die Reflexivität kann in der Definition der Äquivalenzrelation nicht verzichtet werden. Eine symmetrische und transitive Relation muss nicht notwendigerweise reflexiv sein. Es folgt zwar aus x R y wegen der Symmetrie sofort y R x und mit der Transitivität auch x R x. Dieser Schluss ist aber nur dann korrekt, wenn es ein y mit x R y gibt.

Zwei Äquivalenzklassen x | R und y | R sind genau dann gleich, wenn x R y, d.h. ihre Repräsentanten in Relation zueinander stehen.
Sei R eine Äquivalenzrelation in A. Dann gelten für das Restesystem A | R folgende Eigenschaften

- keine Äquivalenzklasse ist leer
- die Vereinigung aller Äquivalenzklassen ist die Menge A selbst
- je zwei verschiedene Äquivalenzklassen sind disjunkt

Ein Teilmengensystem mit diesen Eigenschaften nennt man auch eine Zerlegung oder Partition.

Relationsalgebra

Man kann die Eigenschaften von binären Relationen rein mengentheoretisch charakterisieren.
Sei $R \subseteq A \times A$ eine binäre Relation. Wir bezeichnen mit $R^T = R^{-1}$ die inverse Relation oder transponierte Relation. Die Bezeichnung transponierte Relation ergibt sich daher, dass bei einer Matrixdarstellung sie genau der transponierten Matrix entspricht.
Sind R und S binäre Relationen auf A, so ist auch$R \bullet S = \{(a, c): \exists\ b \in A: (a, b) \in R \text{ und } (b, c) \in S\}$
eine binäre Relation. Sie heißt die Komposition oder das Relationenprodukt von R und S. Zu beachten ist, dass diese Schreibweise entgegengesetzt zur Hintereinanderausführung von Abbildungen ist.
Bezeichnen man mit $I_A = \{(a, a) \mid a \in A\}$ die Identität, so ergibt sich für die algebraischen Eigenschaften von Relationen:

Sei $R \subseteq A \times A$ eine binäre Relation. Dann gilt:

R ist reflexiv $\Leftrightarrow I_A \subseteq R$	R ist irreflexiv $\Leftrightarrow I_A \cap R = \varnothing$
R ist symmetrisch $\Leftrightarrow R = R^T$	R ist asymmetrisch $\Leftrightarrow R \cap R^T = \varnothing$
R ist antisymmetrisch $\Leftrightarrow R \cap R^T \subseteq I_A$	R ist transitiv $\Leftrightarrow R \bullet R \subseteq R$

Auswahlaxiom

Das Auswahlaxiom sichert die Existenz einer Auswahlfunktion für eine beliebige Familie von nichtleeren Mengen. Diese wählt aus jeder Menge ein Element aus.
Sei I eine beliebige Indexmenge und A_i eine Familie von nichtleeren Mengen ($A_i \neq \varnothing$) dann existiert eine Abbildung

$f: I \rightarrow \cup_{i \in I} A_i$ mit $f(I) \in A_i$

Obwohl die Aussage dieses Axioms einleuchtend erscheint, ist sie für unendliche Mengen nicht trivial.

Zu beachten ist, dass es sich um eine reine Existenzaussage handelt. Es wird kein Verfahren angegeben, wie die Auswahlfunktion konstruiert werden kann.

Wohlordnungssatz

Der Wohlordnungssatz sagt aus, dass jede Menge wohlgeordnet werden kann.
In der axiomatischen Mengenlehre nach Zermelo-Fraenkel sind Auswahlaxiom, Wohlordnungssatz und Zornsches Lemma äquivalent.
Das Lemma von Kuratowski-Zorn oder Zornsches Lemma, ist ein Theorem der Zermelo-Fraenkel-Mengenlehre, die das Auswahlaxiom einbezieht. Es ist benannt nach dem Mathematiker Max Zorn, der es 1935 wieder entdeckte, obwohl es schon 1922 von dem polnischen Mathematiker Kazimierz Kuratowski gefunden wurde.

Lemma von Kuratowski-Zorn, Zornsches Lemma

Jede nichtleere halbgeordnete Menge, in der jede Kette, d.h. jede total geordnete Teilmenge, eine obere Schranke hat, enthält mindestens ein maximales Element.
Dieses Lemma wird in vielen wichtigen Beweisen benutzt, zum Beispiel für

- den Satz, dass jeder Vektorraum eine Basis hat
- das Hahn-Banach-Theorem in der Funktionalanalysis, nach dem man lineare Funktionale fortsetzen kann
- Tychonoffs Theorem, dass jedes Produkt kompakter Räume selbst kompakt ist
- den Satz, dass jeder Ring mit 1 ein maximales Ideal hat
- den Satz, dass jeder Körper einen algebraischen Abschluss hat

Multimenge

Die Multimenge ist ein Begriff aus der Mengenlehre der Mathematik. Die Besonderheit von Multimengen gegenüber dem gewöhnlichen Mengenbegriff besteht darin, dass die Elemente einer Multimenge mehrfach vorkommen können. Entsprechend haben auch die verwendeten Mengenoperationen eine modifizierte Bedeutung.

Als Multimenge über einer Menge M bezeichnet man eine Abbildung V von M in die Menge der natürlichen Zahlen. V(x) bezeichnet dann die Vielfachheit des Elementes x aus M.
Anschaulich ist eine Multimenge eine Menge, in der jedes Element beliebig oft vorkommen kann. Man notiert Multimengen dann auch wie Mengen explizit mit geschweiften Klammern und schreibt ein Element so oft hinein, wie es in der Multimenge vorkommt. Mengen sind in diesem Sinne ein Spezialfall von Multimengen, bei denen nur die Werte 0 (nicht enthalten) und 1 (enthalten) zugeordnet werden können.

Beispiel Sei V die Multimenge über {a, b, c}, mit V(a) = 1, V(b) = 3 und V(c) = 0. Dann schreibt man auch V = {a, b, b, b}.
Man nehme einen Würfel und würfle 20 mal hintereinander. Dann kann es sein, dass man

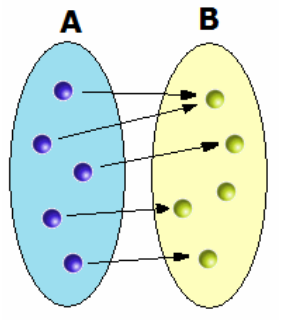
3 mal eine 1 2 mal eine 2 4 mal eine 3
5 mal eine 4 3 mal eine 5 3 mal eine 6

geworfen hat. Die Grundmenge ist dann {1, 2, 3, 4, 5, 6}; die Vielfachheit der 3 ist 4; also V(3) = 4.
Die Multimenge listet jeden Wurf auf, wobei die Reihenfolge außer Acht gelassen wird:

V = {1, 1, 1, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 5, 5, 5, 6, 6, 6}.

Anzahl der möglichen Multimengen

Gegeben sei eine Menge M mit n Elementen. Wie viele Multimengen über M gibt es dann, die k Elemente enthalten? Es gilt: $\binom{n+k-1}{k}$ Multimengen



Abbildung

Eine beliebige Teilmenge $F \subseteq X \times Y$ des kartesischen Produkts zweier Mengen X und Y heißt Korrespondenz oder Zuordnung.
Wenn einem Element $x \in X$ durch eine Korrespondenz F höchstens ein Element $y \in Y$ zugeordnet wird, spricht man von einer eindeutigen Korrespondenz. Diese Korrespondenzen werden als Abbildungen oder Funktionen bezeichnet.
Die Grafik verdeutlicht das Wesen der Abbildung. Die Zuordnungen sind

durch Pfeile symbolisiert. Von jedem Element der linken Menge geht höchstens ein Pfeil aus. Derartige Darstellungen werden Pfeildiagramm genannt.

Die Abbildung der Menge A auf die Menge B ordnet jedem Element x aus A Elemente y aus B zu. Man nennt x die unabhängige Variable und y die abhängige Variable.
Schreibweise: $f: A \to B$
A … Definitionsbereich, Definitionsmenge, Urbildmenge, Urbildbereich, Argumentbereich
B … Bildmenge, Bildbereich, Wertebereich, Zielmenge
x … Argument, Original, Urbild
y … Wert von x, Bild von x

Die Schreibweise $f: A \to B$ mit $x \in A$ und $y \in B$ kann auch in der Form $(x,y) \in f$ angegeben werden, d.h. eine Abbildung ist als eine Menge geordneter Paare (x,y) interpretierbar. Die Abbildung $f: A \to B$ ist damit eine Teilmenge des Kreuzproduktes A x B (Kartesisches Produkt). Zwei Abbildungen f und g sind gleich, wenn ihre Definitionsbereiche gleich sind und für jedes Argument x auch $f(x) = g(x)$ gilt. Während man zu jeder Korrespondenz F unmittelbar die Umkehrung F^{-1} bilden kann, muss die Umkehrung einer Abbildung f nicht unbedingt eindeutig sein und damit wieder eine Abbildung.
Hinweis: Mitunter wird die Zuordnung als Abbildung bezeichnet und deren Eindeutigkeit nicht gefordert. Eine eindeutige Abbildung ist dann Funktion.

Verkettung von Abbildungen

Wenn zwei Korrespondenzen $F \subseteq A \times B$ und $G \subseteq B \times C$ gegeben sind, kann die Verkettung oder Hintereinanderausführung oder Komposition von F und G definiert werden.
Man schreibt dafür $G \bullet F$. Dabei ist zu beachten, dass F zuerst ausgeführt wird.
Die Verkettung von Korrespondenzen ist assoziativ. Sind F, G und H Korrespondenzen, dann gilt

$$(F \bullet G) \bullet H = F \bullet (G \bullet H)$$

Nachweis:
Ist $(a, d) \in (F \bullet G) \bullet H$, dann existiert ein c mit $(a, c) \in F \bullet G$ und $(c, d) \in H$ und weiter existiert ein b mit $(a, b) \in F$ und $(b, c) \in G$.
Damit ist aber $(b, d) \in G \bullet H$ und $(a, d) \in F \bullet (G \bullet H)$, womit gezeigt ist, dass $(F \bullet G) \bullet H \subseteq F \bullet (G \bullet H)$. Die andere Inklusion zeigt man analog.

Für den Zusammenhang zwischen Umkehrung und Verkettung gilt $(F \bullet G)^{-1} = G^{-1} \bullet F^{-1}$
Nachweis: Sei $(c, a) \in (F \bullet G)^{-1}$ dann ist $(a, c) \in F \bullet G$ und es gibt ein b mit $(a, b) \in F$ und $(b, c) \in G$. Damit ist aber auch $(b, a) \in F^{-1}$ und $(c, b) \in G^{-1}$ und $(c, a) \in G^{-1} \bullet F^{-1}$. Entsprechend zeigt man die Umkehrung.

Funktion f (eindeutige Abbildung aus D in Z)

heißt injektiv $\Leftrightarrow$ aus $a \neq b$ folgt $f(a) \neq f(b)$ surjektiv $\Leftrightarrow$ Wertebereich = Zielmenge Z
bijektiv $\Leftrightarrow$ f ist injektiv und surjektiv

Eineindeutige Abbildung

Eine bijektive Abbildung ist eineindeutig, umkehrbar eindeutig, d.h. jedem Elemente aus D wird eindeutig ein Elemente aus B und diesem Element aus B eindeutig das Ausgangselement aus D zugewiesen.

Inverse Abbildung

Ist eine Abbildung injektiv und surjektiv, also eine eineindeutige Abbildung von A auf B, so gibt es eine inverse Abbildung, die jedem Element b aus B dasjenige Element von A zuordnet, dessen Bild b ist.

Gleichheit von Abbildungen

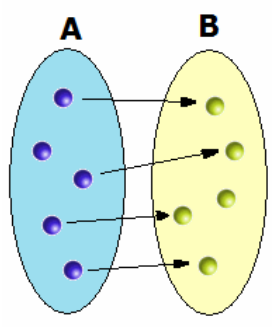
Zwei Abbildungen $f: A \to B$ und $g: C \to D$ heißen gleich $\Leftrightarrow$ A=C und B=D und für alle x aus A gilt $f(x) = g(x)$

Fixelement

Erfüllt eine Element $x \in X$ bei einer Abbildung $f: X \to Y$ die Gleichung $f(x) = x$, so heißt x Fixelement von X bei der Abbildung f.

Identische Abbildung

Die Abbildung f: X → X, welches jedes Element x auf sich selbst abbildet, heißt identische Abbildung.



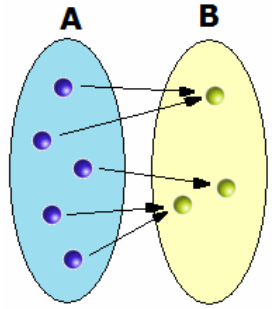
Injektive Funktion

Definition: Gegeben sei eine Funktion A → B. Eine injektive Funktion (Injektion) liegt vor, wenn jedes Element der Zielmenge B höchstens einmal als Bild (eines Elementes der Definitionsmenge) vorkommt.
Für eine solche Funktion f ist deren Umkehrung f^{-1} wieder eindeutig. f nennt man eineindeutig oder umkehrbar eindeutig oder injektiv.

Die Injektivität fordert nicht, dass alle Elemente aus B als Werte vorkommen müssen; dann wäre die Funktion surjektiv.
Die Grafik verdeutlicht das Wesen der Injektivität. Zu keinem Wert aus B gehen zwei Pfeile; bei jedem Element von B endet höchstens ein Pfeil.

Die Bezeichnung umkehrbar eindeutig drückt aus, dass die Umkehrung einer injektiven Funktion f wieder eine Funktion ist. Diese heißt Umkehrfunktion und wird mit f^{-1} bezeichnet. Wenn f nicht injektiv ist, muss die Umkehrung nicht eindeutig sein und damit keine Abbildung. In einer Koordinatendarstellung ist die Kurve entweder streng monoton steigend oder streng monoton fallend.

Beispiele: Die Funktion $f_1(x) = x$ ist injektiv auf R.
Die Funktion $f_2(x) = x^2$ ist nicht injektiv auf R, denn jedem x wird der gleiche Funktionswert wie -x zugeordnet. Schränkt man den Definitionsbereich von f_2 auf die nichtnegativen reellen Zahlen ein, so ist die Funktion auf diesem Intervall injektiv.
Die Injektivität hängt damit vom Definitionsbereich der Funktion ab.

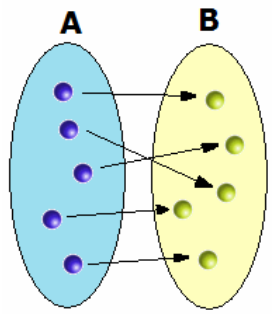


Surjektive Funktion

Definition: Gegeben sei eine Funktion A → B. Gehört jedes Element der Zielmenge B auch zur Wertemenge, so nennt man die Funktion surjektiv, d.h. wenn bei der Funktion die Bildmenge mit B zusammenfällt.
Man spricht mitunter auch von einer Aufabbildung.

Die Grafik verdeutlicht das Wesen der Surjektivität: Alle Werte aus B werden als Funktionswerte angenommen, was dadurch symbolisiert wird, dass sie von einem Pfeil erreicht werden; bei jedem Element von B endet mindestens ein Pfeil.
In einer Koordinatendarstellung kommt jedes Element von B als Bild vor.

Beispiele: Die Funktion $f_1(x) = x$ ist surjektiv auf R. Die Funktion $f_2(x) = x^2$ ist nicht surjektiv auf R, denn negative Zahlen werden nicht als Funktionswerte angenommen. Schränkt man den Wertebereich auf die nichtnegativen reellen Zahlen ein, so ist die Funktion auf diesem Intervall surjektiv.



Bijektive Funktion

Eine bijektive Funktion ist eine Funktion, die surjektiv und injektiv ist. Damit ist f eine eineindeutige Aufabbildung. Jedem Element aus A wird genau ein Element aus B zugeordnet und alle Elemente aus B kommen als Bilder vor.
andere Bezeichnungen: Umkehrbare Funktion bzw. eineindeutige Funktion

Unter den bijektiven Abbildungen einer Menge M auf sich gibt es eine ausgezeichnete Bijektion, die identische Abbildung f. f(a) = a.
Die Hintereinanderausführung zweier Bijektionen ist wieder eine Bijektion; ebsono ist die Umkehrung einer Bijektion eine Bijektion.

Ist f: A → B eine injektive Abbildung, dann ist die Einschränkung f: A → f(A) eine Bijektion, ebenso die Umkehrung f^{-1}: f(A) → A.

Im Fall der Abbildung einer endlichen Menge auf sich sind die Eigenschaften injektiv und bijektiv gleichwertig. Es gilt: Es sei f: A → A eine Abbildung einer endlichen Menge A auf sich. Dann sind die folgenden Aussagen paarweise äquivalent.

f ist injektiv f ist surjektiv f ist bijektiv

Konstante Abbildung

Ist y ein festes Element von Y, dann ist X x {y} eine eindeutige Abbildung von X in Y, die jedem x ∈X dasselbe Element y zuordnet, sie wird konstante Abbildung genannt.

Einschränkung einer Abbildung

Ist A eine Teilmenge von X und F eine Abbildung von X in Y, so ist die Menge **F ∩ (A x Y)** eine Abbildung, die Einschränkung von F auf die Menge A. Schreibweise: $F|_A$

Abbildungen von Mengen

Seien A, B Mengen und f: A → B eine Abbildung sowie $A_1, A_2 \subseteq A$ und $B_1, B_2 \subseteq B$, dann gilt:

$A_1 \subseteq A_2 \rightarrow f(A_1) \subseteq f(A_2)$ $B_1 \subseteq B_2 \rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$

$f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$ $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

$f(A_1 \cap A_2) = f(A_1) \cap f(A_2) \Leftrightarrow$ f ist injektiv

$f_1(f(A_1)) \supseteq A_1$ ist f injektiv so gilt $f^{-1}(f(A_1)) = A_1$

$f_1(f(B_1)) \subseteq B_1$ ist f surjektiv so gilt $f^{-1}(f(B_1)) = B_1$

$f^{-1}(B \setminus B_1) = A \setminus f^{-1}(B_1)$

Verkettung von Abbildungen

Das Hintereinanderausführen von mehreren Abbildungen ist eine Verkettung von Abbildungen. Gilt f: A → B und g: B → C, so existiert eine Abbildung (Verkettung g°f von f und g) mit

g°f: A → C mit (g°f)(x) = g[f(x)]

Es gilt: h°(g°f) = (h°g)°f ... assoziativ

Es seien f: X → Y, g: Y → Z, h: Z → W Abbildungen zwischen nichtleeren Mengen X, Y, Z, W. Dann gilt

h • (g • f) = (h • g) • f ; Assoziativität der Hintereinanderausführung

Sind f und g beide injektiv, so auch g • f. Sind beide surjektiv, so auch g • f.

Ist g • f injektiv, so ist f injektiv

Ist g • f surjektiv, so ist g surjektiv

Satz von Schröder-Bernstein

Bei Untersuchungen zur Gleichmächtigkeit von Mengen ist es oft einfacher injektive Abbildungen zwischen den Mengen zu finden als Bijektionen. Dabei hilft der Satz von Schröder-Bernstein weiter, der aus der Injektiviität zweier Mengen untereinander die Bijektivität folgert. Mit dem Hilfssatz

Sei f: A → B eine injektive Abbildung und B ⊆ A, dann lassen sich A und B bijektiv aufeinander abbilden.

kann bewiesen werden

Satz von Schröder-Bernstein

Seien A und B zwei Mengen und f: A → B sowie g: B → A zwei injektive Abbildungen. Dann existiert eine Bijektion h zwischen den Mengen A und B; insbesondere sind sie dann gleichmächtig.

Hüllen

Sei M eine Menge. Eine Abbildung H: P(M) → P(M) (P … Potenzmenge) heißt genau dann Hüllenoperator, wenn für alle A, B ⊆ M folgende Eigenschaften gelten:

$A \subseteq H(A)$; Extensivität $A \subseteq B \Rightarrow H(A) \subseteq H(B)$; Monotonie

$H(H(A)) = H(A)$; Idempotenz

Beispiele: In einem Vektorraum V ist die lineare Hülle ein Hüllenoperator. Die abgeschlossene Hülle in einem metrischen Raum ist ein Hüllenoperator.

Algebraische Verknüpfung, Operation

A, B, M seien nicht leere Mengen.
Jede Abbildung $(A \times B) \to M$, bei der jedem geordneten Paar $(a,b) \in (A \times B)$ ein Bild $(a \bullet b) \in M$ zugeordnet ist, heißt algebraische Verknüpfung oder Operation.
Innere Verknüpfung ... $(M \times M) \to M$ Äußere Verknüpfung 1.Art ... $(A \times M) \to M$
Äußere Verknüpfung 2.Art ... $(A \times A) \to M$

Abgeschlossenheit einer Verknüpfung

Die Tatsache, dass eine Verknüpfung auf einer Menge G abgeschlossen ist, entspricht einer innerer Verknüpfung in der Menge G: $G \times G \to G$

Algebraische Struktur

... ist eine nicht leere Menge mit mindestens einer inneren Verknüpfung $(M , \bullet)$: $(a,b) \to (a \bullet b)$, mit $a,b,a \bullet b \in M$
M ... Trägermenge, $(M , \bullet)$ mit genau einer Operation heißt Gruppoid

Abbildung algebraischer Strukturen

$(A , \bullet_1)$, $(B , \bullet_2)$ seien algebraische Strukturen mit den Operationen $\bullet_1$ und $\bullet_2$
Die Abbildung f: mit $a \in A$ und $f(a) = a' \in B$ heißt **Homomorphismus,**
wenn für alle $a,b \in A$ gilt: $f(a \bullet_1 b) = f(a) \bullet_2 f(b) = a' \bullet_2 b'$
Die Strukturen heißen zueinander homomorph, d.h. strukturverträglich.
Ist h: G_1 --> G_2 ein Gruppenhomomorphismus, so wird die Menge ker h aller Elemente von G_1, die auf das neutrale Element von G_2 abgebildet werden, Kern von h genannt. Der Kern von h erweist sich als Normalteiler von G_1.

Isomorphismus ... wenn f ein bijektiver Homomorphismus ist. Die Strukturen heißen zueinander isomorph (strukturgleichwertig). Es gilt ker f = E.
Automorphismus ... Ist ein Isomorphismus, von der Form $f: G \to G$.

Homomorphismus, Beispiele

Sei $R^* = R \setminus \{0\}$ und $(R^*, \cdot)$ die multiplikative Gruppe der reellen Zahlen.
Die Exponentialfunktion $f(x) = e^x$ ist ein Homomorphismus der additiven Gruppe der reellen Zahlen in die multiplikative Gruppe der positiven reellen Zahlen. Es gilt:

$$f(a + b) = e^{a+b} = e^a e^b = f(a) f(b)$$

Sei sgn: $R \to R$ die Signumfunktion wie folgt definiert:

sgn(x) = 1 für x > 0 ; = 0 für x = 0 ; = -1 für x < 0

Dann ist sgn ein Homomorphismus von der multiplikativen Gruppe R in die multiplikative Gruppe {+1, -1}. Dieser Homomorphismus spiegelt gerade die Regeln für die Multiplikation vorzeichenbehafteter Zahlen wider.
Der Kern dieses Homomorphismus ist die multiplikative Gruppe der positiven reellen Zahlen.
In der multiplikativen Gruppe der reellen Zahlen ist $f(x) = 1/x$ ein Homomorphismus. Es gilt:

$$f(a \cdot b) = 1 / (a \cdot b) = 1/a \cdot 1/b = f(a) \cdot f(b)$$

Da die Abbildung bijektiv ist, handelt es sich sogar um einen Isomorphismus.

Neutrales Element bei Homomorphismus

Es seien G und H zwei Gruppen, e_G und e_H die neutralen Elemente in G und H und $f: G \to H$ ein Homomorphismus. Dann gilt: $f(e_G) = e_H$ $f(a^{-1}) = f(a)^{-1}$ für alle $a \in G$
Homomorphismen überführen neutrale Elemente in neutrale Elemente und inverse Elemente in inverse.

Kern eines Homomorphismus

Ist h: $G_1 \to G_2$ ein Gruppenhomomorphismus, so wird die Menge ker h aller Elemente von G_1, die auf das neutrale Element von G_2 abgebildet werden, Kern von h genannt. Der Kern von h erweist sich als Normalteiler von G_1.
Das Bild von f im(f) ist die Menge aller in G_2 vorkommenden Bilder und wird Bild des Homomorphismus genannt. im(f) ist Untergruppe von G_2.

Kanonische Homomorphismen von Normalteilern

Sei G eine Gruppe und H Normalteiler in G. Dann existiert ein Homomorphismus

$f: G \to G/H$ mit ker(f) = H

Dieser Homomorphismus wird kanonischer Homomorphismus genannt und ist durch
$f(g) = gH$
gegeben.
Nachweis: f ordnet jedem Gruppenelement seine Linksnebenklasse zu. Außerdem ist G/H eine Gruppe. Die Homomorphie von f ergibt sich einfach auch der Definition.
Bleibt zu zeigen ker(f) = H. Dazu kann man folgende Äquivalenzkette aufbauen:
$h \in H \Rightarrow hH = H \Rightarrow f(H) = H \Rightarrow h \in \ker(f)$

Automorphismengruppe

Die Menge der Automorphismen einer Gruppe G wird mit aut(G) bezeichnet.
Die Automorphismen einer Gruppe aut(G) bilden bezüglich der Hintereinanderausführung von Abbildungen eine Gruppe, die so genannte Automorphismengruppe.

Isomorphie

Es seien (G, ·) und (G', ·) zwei Gruppen. Diese heißen isomorph genau dann, wenn es eine Abbildung $f: G \to G'$ mit folgenden Eigenschaften gibt:
f ist bijektiv, also eine eineindeutige Aufabbildung
f lässt das Produkt invariant: $\forall a, b \in G: f(a \cdot b) = f(a) \cdot f(b)$
Ein Isomorphismus ist ein bijektiver Homomorphismus.
Durch den Begriff der Isomorphie kann man Eigenschaften einer Gruppe auf eine andere übertragen, ohne sie im Einzelnen beweisen zu müssen. In isomorphen Gruppen gelten die gleichen Eigenschaften. Die Isomorphie legt damit Gestaltgleichheit fest.

Beispiele: Die Restklassengruppe Z_n ist isomorph zur zyklischen Gruppe C_n. Den Isomorphismus erhält man, wenn man logarithmiert, d.h. die Exponenten aus C_n als die Zahlen aus Z_n auffasst.
Einfach zu sehen ist, dass die zyklische Gruppe C_4 nicht isomorph zur Kleinschen Vierergruppe D_2 ist. Letzte enthält Elemente $a \neq 1$, für die gilt $a \cdot a = 1$, was für kein von 1 verschiedenes Element der zyklischen Gruppe gilt.
Wenn f ein Isomorphismus von G auf G', dann ist die Umkehrabbildung $f^{-1}: G' \to G$ ebenfalls ein Isomorphismus.

Algebra (Struktur)

... mathematische Struktur, die den Vektorraum- und den Ringeigenschaften genügt.
Beispiel: Die Menge der n x n-Matrizen mit der gewöhnlichen Matrizenaddition und -multiplikation ist eine Algebra.

Arten algebraischer Strukturen

Zusammenstellung verschiedener algebraischer Strukturen:

Magma (G,*)	eine Menge mit einer zweistelligen Verknüpfung *
Quasigruppe (G,*)	ein Gruppoid in dem die Division stets eindeutig möglich ist
Loop (G,*,1)	eine Quasigruppe mit einem neutralen Element
Halbgruppe (G,*)	ein assoziatives Gruppoid
Monoid (G,*,1)	eine Halbgruppe mit einem neutralen Element 1
Gruppe $(G,*,1,^{-1})$	ein Monoid mit einem inversen Element a-1 für jedes a, oder äquivalent dazu, eine assoziative Loop
Abelsche Gruppe (G,+,0,-)	eine kommutative Gruppe
Ring (R,+,0,-,·)	eine Menge R mit zwei Verknüpfungen + (Addition) und · (Multiplikation), so dass (R,+,0,-) eine Abelsche Gruppe, (R,·) eine Halbgruppe ist und die Distributivgesetze erfüllt sind
Unitärer Ring (R,+,0,-,·,1)	ein Ring mit neutralem Element 1 für die Multiplikation
Körper (R,+,0,-,·,1,-1)	ein Ring, so dass (R\{0},·,1,-1) eine Abelsche Gruppe ist
Modul (M,+,0,-,·,R)	über einem Ring R, Eine Menge M mit einer inneren Verknüpfung + und einer äußeren Verknüpfung $\cdot: R \times M \to M$ (Skalarmultiplikation), so dass (M,+,0,-) eine Abelsche Gruppe ist, die Skalarmultiplikation assoziativ ist und die Distributivgesetze erfüllt sind
Vektorraum (V,+,0,-,·,K)	ein Modul über einem Körper K

Algebra (V,+,0,-,·,*,K) Ein Vektorraum mit einer bilinearen Verknüpfung * ("Vektormultiplikation"), die die Distributivgesetze erfüllt und assoziativ mit der Skalarmultiplikation ist
Assoziative Algebra eine K-Algebra, deren Multiplikation assoziativ ist
Kommutative Algebra eine assoziative K-Algebra, deren Multiplikation kommutativ ist
algebraischer Verband (V,∩,∪) eine Menge mit zwei kommutativen, assoziativen, idempotenten Verknüpfungen (Durchschnitt und Vereinigung), die Absorptionsgesetze erfüllen
Boolescher Verband (V,∩,∪,0,1,¬) ein Verband mit neutralen Elementen 0 und 1 für ∩ und ∪, der zwei Distributivgesetze erfüllt und Komplemente ¬a hat Menge, eine algebraische Struktur ohne Verknüpfungen

Strukturen mit einer Verknüpfung

Die algebraischen Strukturen besitzen ein oder zwei zweistellige innere Verknüpfungen auf einer Menge M. Betrachtet werden folgende Axiom:

(E) Existenz und Eindeutigkeit:	$\forall\ a,b \in M: a \bullet b \in M$
(A) Assoziativgesetz:	$\forall\ a,b,c \in M: (a \bullet b) \bullet c = a \bullet (b \bullet c)$
(N) Existenz eines neutralen Elements	$\exists\ e \in M: \forall\ a \in M: a \bullet e = e \bullet a = a$
(I) Existenz des inversen Elements:	$\forall\ a \in M: \exists\ a^{-1} \in M: a \bullet a^{-1} = a^{-1} \bullet a = e$
(K) Kommutativgesetz:	$\forall\ a,b \in M: a \bullet b = b \bullet a$

Die folgenden Strukturen mit einer zweistelligen inneren Verknüpfung erfüllen folgende Axiome

Magma auch Gruppoid	Axiom E: Menge mit zweistelliger innerer Verknüpfung
Halbgruppe	Axiome EA: Gruppoid mit Assoziativgesetz
Monoid:	Axiome EAN: Halbgruppe mit einem neutralen Element e
Quasigruppe auch Semigruppe:	Axiome EI: Magma mit Inversen
Loop:	Axiome ENI: Quasigruppe mit neutralem Element
Gruppe:	Axiome EANI: Monoid und Quasigruppe
Abelsche Gruppe:	Axiome EANIK: Gruppe mit kommutativer Verknüpfung

Gruppoid

Unter einem Gruppoid oder einem Magma (G,*) versteht man eine nichtleere Menge G, auf der eine (zweistellige) (innere) Verknüpfung * definiert ist, d.h. je zwei Elementen a und b aus G ist ein drittes Element a*b aus G zugeordnet. Dabei nennt man * meistens eine Multiplikation auf G und a*b das Produkt des linken Faktors a und des rechten Faktors b.
In vielen Anwendungsfällen ist jedoch auch die additive Schreibweise üblich:
Man schreibt + für das Verknüpfungssymbol und nennt sie Addition auf G und a+b dann die Summe der Summanden a und b.

Eigenschaften

Eine innere Verknüpfung * auf G bzw. das Gruppoid (G,*) heißt kommutativ, wenn für alle a und b aus G gilt: (1) a*b = b*a
Hat man (2) a*a = a für ein a aus G, so nennt man dieses Element idempotent. Man bezeichnet mit E(G) die Menge aller idempotenten Elemente von (G,*) und nennt * bzw. (G,*) idempotent, falls E(G) = G gilt.

Ordnung eines Gruppoids

Unter der Ordnung eines Gruppoids (G,*) versteht man die Anzahl |G| der Elemente von G. Speziell für Gruppoide (G,*) kleiner Ordnungen beschreibt man die Verknüpfung * oft mit Hilfe einer Verknüpfungstafel.

Neutrales Element

Ein neutrales Element e eines Gruppoids (G,*) wird durch die Forderung
(3) e*a = a = a*e
für alle a aus G charakterisiert. Gilt wenigstens immer die linke Gleichung in (3), so nennt man e linksneutral, und entsprechend rechtsneutral, wenn wenigstens die rechte Gleichung in (3) für alle a aus G erfüllt ist. In jedem dieser Fälle ist e idempotent.
Außerdem ist ein neutrales Element immer eindeutig bestimmt, denn ist e_1 auch nur ein linksneutrales und e_2 ein rechtsneutrales Element desselben Gruppoids (G,*), so muss ihr Produkt e_1*e_2 sowohl mit e_2 als auch mit e_1 übereinstimmen.

Bei multiplikativer Schreibweise nennt man ein neutrales Element auch ein Einselement und schreibt dafür oft 1, bei additiver Bezeichnung spricht man dagegen von einer Null und benutzt das Symbol 0 oder o.

Komplexprodukt

Sind U und V beliebige Teilmengen eines Gruppoids (G,*), so heißt die Teilmenge

$$U*V = \{ u*v \mid u \text{ aus } U \text{ und } v \text{ aus } V \}$$

von G das Komplexprodukt von U und V. Natürlich ist U*V genau dann leer, wenn mindestens eine der Mengen U oder V leer ist.
Für einelementige Teilmenge U = { u } oder V = { v } schreibt man einfach u*V anstelle von { u }*V und U*v anstelle von U*{ v }. Damit wird die Potenzmenge P(G) zu einem Gruppoid (P(G),*), das die leere Menge als absorbierendes Element besitzt. Weiterhin ist (P(G),*) genau dann assoziativ bzw. kommutativ, wenn (G,*) die entsprechende Eigenschaft hat.

Halbgruppe

Eine algebraische Struktur (G, •) heißt Halbgruppe, wenn gilt:
1. Assoziativgesetz für alle a,b,c aus G: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
Eine idempotente Halbgruppe heißt auch ein Band, eine kommutative und idempotente Halbgruppe ein Halbverband.

Ein Element e einer Halbgruppe (G,•) ist genau dann linksneutral, wenn es idempotent und linkskürzbar ist. Ist nämlich $e = e \bullet e$ linkskürzbar, so folgt aus $e \bullet (e \bullet a) = (e \bullet e) \bullet a = e \bullet a$ bereits $e \bullet a = a$ für alle a aus G. Umgekehrt ist ein linksneutrales Element in jedem Gruppoid linkskürzbar und idempotent.
Ein Monoid ist eine Halbgruppe mit einem Einselement, dabei fallen links- und rechtsneutrales Element zusammen.
Sei M ein Monoid mit dem neutralen Element 1 und $a \in M$. Ein $b \in M$ heißt rechtsinvers zu a falls $ab = e$; analog heißt $c \in M$ linksinvers zu a falls $ca = 1$.
Ist $b \in M$ rechtsinvers und $c \in M$ linksinvers zu a, so ist $b = c$.
Ist a invertierbar, so schreibt man für das Inverse a^{-1}. Sind a, b $\in$ M invertierbar, so gilt

$$(a^{-1})^{-1} = a \qquad (ab)^{-1} = b^{-1} a^{-1}$$

Beispiele:

Sind N die natürlichen Zahlen einschließlich der Null, so ist (N, +) ein Monoid und (N\{0}, +) ist eine Halbgruppe. (N\{0}, •) ist ein Monoid.
Die Menge der ganzen Zahlen mit der Addition (Z, +, 0) ist ein Monoid. (Z, - 0) ist kein Monoid, da die Subtraktion nicht assoziativ ist.
Der dreidimensionale euklidische Raum mit dem Vektorprodukt (R^3, $\times$, $0^{\rightarrow}$) ist kein Monoid, da das Assoziativgesetz verletzt ist.
Die Menge der Vielfachen einer ganzen Zahl n (nZ, + 0) ist ein Monoid.
Die Menge der nichtnegativen rationalen Zahlen mit der Addition (Q^+, +, 0) ist ebenso wie die Menge der positiven rationalen Zahlen mit der Multiplikation ein Monoid.
Die Potenzmenge einer Menge X mit dem Durchschnitt ist ein kommutatives Monoid.

Es sei (H, •) eine Halbgruppe. Dann gilt:
(1) H besitzt höchstens ein Einselement und höchstens ein Nullelement.
(2) Hat H ein Einselement e und ist $h \in H$ invertierbar, so ist das zu h inverse Element h' eindeutig bestimmt.
Nachweis (1): Angenommen, e und e' sind Einselemente von H. Dann gilt

$$e \bullet e' = e' \bullet e = e'$$

wegen der Eigenschaft von e und

$$e \bullet e' = e' \bullet e = e$$

wegen der Eigenschaft von e'. Also e = e'. Analog folgt, dass es höchstens ein Nullelement gibt.
(2): Seien h' und h" inverse Elemente zu h. Dann gilt

$$h' = e \bullet h' = (h'' \bullet h) \bullet h' = h'' \bullet (h \bullet h') = h'' \bullet e = h''.$$

Unterhalbgruppe

Es sei (H, •) eine Halbgruppe und $H' \subseteq H$. Dann heißt H' Unterhalbgruppe von H, wenn (H', •) Halbgruppe ist.

Abschluss

Definition: Es sei (H, •) eine algebraische Struktur mit nur einer inneren Verknüpfung und H' $\subseteq$ H. Unter dem Abschluss <H'> von H' versteht man die Menge aller möglichen endlichen Produkte von Elementen aus H', d.h.

$$<H'> := \{a_1 \bullet a_2 \bullet \ldots a_r \mid r \in N \wedge \{a_1, a_2, \ldots, a_r\} \subseteq H'\}.$$

Falls (H, •) Halbgruppe, so ist <H'> die kleinste Unterhalbgruppe von H, die H' enthält.

Definitionen: Es sei (H, •) eine algebraische Struktur und H' $\subseteq$ H. Man sagt

H' erzeugt H :$\Leftrightarrow$ <H'> = H

H ist endlich erzeugt :$\Leftrightarrow \exists$H': <H'> = H $\wedge$ H' endlich.

Es sei (H, •) eine algebraische Struktur und <E> = H. Gilt für beliebige x und z aus H und beliebiges e aus E stets

$$x \bullet (e \bullet z) = (x \bullet e) \bullet z,$$

so ist (H, •) eine Halbgruppe.

Gruppe, algebraische Gruppe

Eine algebraische Struktur (G, •) heißt Gruppe, wenn G nicht leere Menge ist und es gilt:

1. Zusammensetzungsvorschrift jedem Elementepaar a, b aus G wird ein drittes Element a • b derselben Menge eindeutig zugeordnet, welches meist Produkt von a und b genannt wird
2. Assoziativgesetz für alle a, b, c aus G: (a • b) • c = a • (b • c)
3. Neutrales Elementin G existiert ein neutrales Element e, so dass für alle a aus G gilt: a • e = e • a = a
4. Inverses Element Zu jedem a aus G existiert ein a' in G, so dass a • a' = a' • a = e

3* linksseitiges Einselement es genügt statt 3. nur die Existenz eines linksseitigen Einselementes zu fordern, d.h. es existiert ein e in G mit e • a = a

4* linksseitiges Inverses ebenso genügt es nur die Existenz eines linksseitigen Inversen zu fordern, d.h. a' • a = e

Satz: Für alle a, b aus G existieren stets x, y in G mit a • x = b und y • a = b

Bei jeder Gruppe handelt es sich um ein Monoid, in dem jedes Element ein Inverses besitzt. Wie für jedes Monoid ist daher das Einselement einer Gruppe auch eindeutig bestimmt. Das zu jedem a aus G existierende inverse Element ist ebenfalls eindeutig bestimmt, denn sind a_1^{-1} und a_2^{-1} beide invers zu a, so folgt aus der Assoziativität ihre Gleichheit gemäß

$$a_1^{-1} = a_1^{-1} \bullet e = a_1^{-1} \bullet (a \bullet a_2^{-1}) = (a_1^{-1} \bullet a) \bullet a_2^{-1} = e \bullet a_2^{-1} = a_2^{-1}$$

Sind a und b beliebige Elemente einer Gruppe (G,•), so sind die beiden Gleichungen

$$x \bullet a = b \text{ und } a \bullet y = b$$

durch die Elemente $x = b \bullet a^{-1}$ und $y = a^{-1} \bullet b$ (eindeutig) lösbar.

Additive Gruppe

Bei dem Gruppenbegriff ist die Bezeichnung der Operation a • b ohne Bedeutung, d.h. die Operation kann auch eine Addition sein. Eine Gruppe, die eine Addition als Operation beinhaltet, wird additive Gruppe oder Modul genannt. Das Einselement wird nun Nullelement genannt.

Gruppe (2)

Man kann Gruppen als solche Halbgruppen charakterisieren, in denen jede Gleichung der Form x • a = b und a • y = b wenigstens eine Lösung besitzt:

Ist nämlich a ein beliebiges Element aus G, so gibt es ein e aus G, das e • a = a erfüllt. Weiterhin existiert zu jedem b aus G ein y aus G mit a • y = b. Hieraus folgt e • b = e • a • y = a • y = b, d.h., dass e ein Linkseinselement von (G,•) ist.

Weiterhin existiert wegen (5) zu jedem a aus G ein a' aus G mit a' • a = e für dieses Linkseinselement.

Aus dieser Eigenschaft lässt sich aber nun die Gruppeneigenschaft der Halbgruppe (G,•) zeigen. Zunächst folgt a' • a • a' = e • a' = a' und die Existenz von a'' aus G mit a'' • a' = e.

Dies impliziert a • a' = e • a • a' = a'' • a' • a • a' = a'' • a' = e und a = e • a = a • a' • a = a • e. Dies zeigt, dass e sogar zweiseitiges Einselement von (G,•) ist und a' zweiseitiges Inverses von a. Damit ist (G,•) Gruppe.
Die allgemeine Lösbarkeit von nur einer der beiden Gleichungen (5) führt dagegen jeweils auf eine größere Klasse von Halbgruppen.

Morphismus (Gruppenmorphismus)

Eine Abbildung f: G $\rightarrow$ F, a $\rightarrow$ f(a) heißt Morphismus, wenn f(ab) = f(a) f(b) für alle a,b $\in$ G gilt.

Kern des Morphismus

Es sei f: G $\rightarrow$ F ein Morphismus, r das Einselement von G und e' das Einselement von F. Alle Elemente von G, die auf das Einselement von F abbilden, gehören zum Kern des Morphismus f. D.h.

ker f := {x $\in$ G: f(x) = e'}

Abelsche Gruppe

Eine Gruppe heißt kommutativ oder Abelsche Gruppe, wenn

4. Kommutativgesetz: für alle a,b aus G: a o b = b o a gilt.

Beispiele: Die Menge der ganzen Zahlen mit der gewöhnlichen Addition ist eine Abelsche Gruppe. Die Menge der Drehungen im dreidimensionalen Raum mit der Nacheinanderausführung als Verknüpfung der Elemente ist eine nichtkommutative Gruppe.
Die Tabelle enthält die Anzahl der Abelschen Gruppen A und aller endlichen Gruppen N einer Ordnung h.

h	N	A	h	N	A	h	N	A	h	N	A
1	1	1	51	1	1	101	1	1	151	1	1
2	1	1	52	5	2	102	4	1	152	12	3
3	1	1	53	1	1	103	1	1	153	2	2
4	2	2	54	15	3	104	14	3	154	4	1
5	1	1	55	2	1	105	2	1	155	2	1
6	2	1	56	13	3	106	2	1	156	18	2
7	1	1	57	2	1	107	1	1	157	1	1
8	5	3	58	2	1	108	45	6	158	2	1
9	2	2	59	1	1	109	1	1	159	1	1
10	2	1	60	13	2	110	6	1	160	238	7
11	1	1	61	1	1	111	2	1	161	1	1
12	5	2	62	2	1	112	43	5	162	55	5
13	1	1	63	4	2	113	1	1	163	1	1
14	2	1	64	267	11	114	6	1	164	5	2
15	1	1	65	1	1	115	1	1	165	2	1
16	14	5	66	4	1	116	5	2	166	2	1
17	1	1	67	1	1	117	4	2	167	1	1
18	5	2	68	5	2	118	2	1	168	57	3
19	1	1	69	1	1	119	1	1	169	2	2
20	5	2	70	4	1	120	47	3	170	4	1
21	2	1	71	1	1	121	2	2	171	5	2
22	2	1	72	50	6	122	2	1	172	4	2
23	1	1	73	1	1	123	1	1	173	1	1
24	15	3	74	2	1	124	4	2	174	4	1
25	2	2	75	3	2	125	5	3	175	2	2
26	2	1	76	4	2	126	16	2	176	42	5
27	5	3	77	1	1	127	1	1	177	1	1
28	4	2	78	6	1	128	2328	15	178	2	1
29	1	1	79	1	1	129	2	1	179	1	1
30	4	1	80	52	5	130	4	1	180	37	4
31	1	1	81	15	5	131	1	1	181	1	1
32	51	7	82	2	1	132	10	2	182	4	1
33	1	1	83	1	1	133	1	1	183	2	1
34	2	1	84	15	2	134	2	1	184	12	3

35	1	1	85	1	1	135	5	3	185	1	1
36	14	4	86	2	1	136	15	3	186	6	1
37	1	1	87	1	1	137	1	1	187	1	1
38	2	1	88	12	3	138	4	1	188	4	2
39	2	1	89	1	1	139	1	1	189	13	3
40	14	3	90	10	2	140	11	2	190	4	1
41	1	1	91	1	1	141	1	1	191	1	1
42	6	1	92	4	2	142	2	1	192	1543	11
43	1	1	93	2	1	143	1	1	193	1	1
44	4	2	94	2	1	144	197	1	194	2	1
45	2	2	95	1	1	145	1	1	195	2	1
46	2	1	96	230	7	146	2	1	196	17	4
47	1	1	97	1	1	147	6	2	197	1	1
48	52	5	98	5	2	148	5	2	198	10	2
49	2	2	99	2	2	149	1	1	199	1	1
50	2	2	100	16	4	150	13	2	200	52	6

Die Anzahl A(n) der nicht isomorphen abelschen Gruppen der Ordnung n kann nach folgendem Verfahren berechnet werden. Wenn $n = \prod_i p_i^{\alpha}i$
die Primfaktorzerlegung mit paarweise verschiedenen Primfaktoren pi ist, so gilt für die Anzahl

$$A(n) = \prod_i P(\alpha_i)$$

wobei $P(\alpha_i)$ die Anzahl der Partitionen der $P(\alpha_i)$ ist.
Beispiel: Für die Anzahl A(n) der abelschen Gruppen der Ordnung 1008 wird
$n = 2^4\ 3^2\ 7$ $\alpha_i = 4, 2, 1$ $P(\alpha_i) = 5, 2, 1$ und somit
A(35280) = 5 * 2 * 1 = 10, d.h. 10 nichtisomorphe abelsche Gruppen der Ordnung 1008.

Die kleinsten Ordnungen n, für welche A(n) = 1, 2, 3, ... nichtisomorphe abelsche Gruppen existieren, sind damit 1, 4, 8, 36, 16, 72, 32, 900, 216, 144, 64, 1800, 0, 288, 128, ... Dabei bedeutet die 0 für A(n) = 13, dass für keine Ordnung n existiert, für die es genau 13 verschiedenen nichtisomorphe abelsche Gruppen existieren. Außer der 13 gibt es für A(n) = 13, 17, 19, 23, 26, 29, 31, 34, 37, 38, 39, 41, 43, 46, ... keine Ordnungen n.
Die Folge der wachsenden Werte A(n) ist 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101, ...
Diese Anzahl abelscher Gruppen tritt erstmals für die wachsenden Ordnungen n = 1, 4, 8, 16, 32, 64, 128, 256, 512, 1024, ..., also die Zweierpotenzen auf.

Zerlegungssatz von Kronecker: Jede endliche abelsche Gruppe kann als das direkte Produkt von zyklischen Gruppen mit Primzahlpotenzordnung erzeugt werden.

Ist die Ordnung der endlichen Gruppe eine Primzahl p, so existiert damit genau eine abelsche Gruppe der Ordnung p, konkret der Restklassengruppe Z_p. Eine nichtabelsche Gruppe der Ordnung p gibt es dann nicht.
Ist die Ordnung ein Primzahlquadrat p^2, so existieren zwei abelsche Gruppen Z_{p^2} und $Z_p \otimes Z_p$.
Ist die Ordnung ein Primzahlkubus p^3, so existieren drei abelsche Gruppen Z_{p^3}, $Z_p \otimes Z_{p^2}$ und $Z_p \otimes Z_p \otimes Z_p$. Zusätzlich gibt es hier noch 2 nichtabelsche Gruppen. Ist die Ordnung das Produkt pq zweier Primzahlen, so findet man genau eine abelsche Gruppe $Z_p \otimes Z_q$, aber keine nichtabelsche Gruppe.
Überraschend ist die von Srinivasan (1973) gefundene; und noch nicht verstandene; Beziehung der Anzahl A(n) der abelschen Gruppen der Ordnung n mit der Riemannschen Zetafunktion $\zeta(s)$:

$$\Sigma\ A(n)\ n^{-s} = \zeta(s)\ \zeta(2s)\ \zeta(3s)\ ...,\ \text{Summenbildung } n = 1, ..., \infty$$

Gruppentheorie - Begriffe

Innerhalb der Gruppentheorie werden spezielle Fachbegriffe genutzt. Eine unvollständige Auswahl ist:

abelsch

Abelsch heißt eine Gruppe $(G,\otimes)$, wenn die Verknüpfung $\otimes$ kommutativ ist, also $g\otimes h = h\otimes g$ für alle $g, h \in G$. Benannt nach Niels Henrik Abel.

allgemeine lineare Gruppe GL(n,F) vom Grad n über einem Körper F
Menge aller invertierbaren n×n-Matrizen mit Koeffizienten aus F und mit der Matrixmultiplikation als Gruppenverknüpfung.

alternierende Gruppe
Menge aller geraden Permutationen einer Menge von n Elementen; für n>2 eine nicht-triviale Untergruppe der symmetrischen Gruppe.

Darstellung einer Gruppe vom Grad n
Ein Homomorphismus von einer Gruppe auf eine allgemeine lineare Gruppe GL(n,..) mit der Absicht, eine abstrakte Gruppe durch invertierbare Matrizen darzustellen. Die Darstellungstheorie ist ein umfangreiches Unterkapitel der Gruppentheorie.

direktes Produkt (bei abelschen Gruppen auch direkte Summe) zweier Gruppen G und H
Eine Gruppe, deren Elemente Paare (g,h) mit $g \in G$ und $h \in H$ sind.

einfache Gruppe
Einfach heißt eine Gruppe, die nur {e} und sich selbst als Normalteiler enthält. Jede endliche Gruppe ist in gewisser Weise aus einfachen Gruppen zusammengesetzt. Die endlichen einfachen Gruppen sind abschließend klassifiziert.

Einselement … das neutrale Element in einer Gruppe mit multiplikativ aufgefasster Verknüpfung.
endlich … heißt eine Gruppe, wenn sie endlich viele Elemente enthält.
Epimorphismus … heißt ein surjektiver Homomorphismus.

Faktorgruppe, Quotientengruppe, Restklassengruppe
Für eine Gruppe G und einen Normalteiler N von G ist die Faktorgruppe G/N die Menge der Links-Nebengruppen {aN: $a \in G$} mit der Verknüpfung aN•bN = abN. Der Zusammenhang von Normalteilern, Homomorphismen und Faktorgruppen ist im Homomorphiesatz zusammengefasst.

Grad einer Darstellung … Grad der allgemeinen linearen Gruppe, in die eine Darstellung abbildet
Grad einer linearen Gruppe … die Zahl der Spalten oder Zeilen der quadratischen Matrizen, aus denen diese Gruppe besteht.

Homomorphiesatz
Verknüpft das Bild eines Gruppen-Homomorphismus mit der Faktorgruppe nach seinem Kern.

Homomorphismus von Gruppen
Eine Abbildung $f: (G,\cdot) \to (H,\times)$, die die Verknüpfungstafel erhält: $f(a \cdot b) = f(a) \times f(b)$ für alle a und b aus G.

Index einer Untergruppe … die Kardinalität der Menge der Rechts- oder Linksnebenklassen einer Untergruppe

isomorph … heißen Gruppen, die durch einen Isomorphismus aufeinander abgebildet werden können. Isomorphe Gruppen können als bis auf die Benennung ihrer Elemente identisch angesehen werden.
Isomorphismus von Gruppen … bijektiver, d.h. umkehrbarer Homomorphismus

Kern eines Gruppen-Homomorphismus
Die Teilmenge der Ausgangsgruppe, die auf das neutrale Element der Zielgruppe abgebildet wird. Jeder Normalteiler ist Kern eines Gruppen-Isomorphismus und umgekehrt.

Linksnebenklassen
Linksnebenklasse zu einem Gruppenelement $g \in G$ und einer Untergruppe U von G: die Menge $g \cdot U$, also die Menge aller $n \in G$, die sich als $n = g \cdot u$ mit $u \in I$ schreiben lassen. Eine Linksnebenklasse, die zugleich Rechtsnebenklasse ist, ist Normalteiler.
Monomorphismus heißt ein injektiver Homomorphismus.

Normalteiler
Normalteiler heißt eine Untergruppe N von G, wenn für alle $n \in N$ und alle $g \in G$ das konjugierte Element $g^{-1}ng$ in N liegt. Ein Normalteiler ist zugleich Rechts- und Links-Nebenklasse.

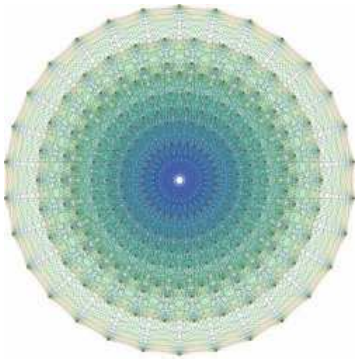
Nullelement … das neutrale Element in einer Gruppe mit additiv aufgefasster Verknüpfung
Ordnung einer endlichen Gruppe … die Anzahl ihrer Elemente

Ordnung eines Elements g einer Gruppe G
Wenn existent, die kleinste Zahl $m \in N^+$ für die $g^m = e$. Die Ordnung einer endlichen Gruppe ist durch die Ordnung jeden Elements teilbar

p-Gruppe … eine Gruppe mit der Eigenschaft: Die Ordnung eines jeden Elements ist eine Potenz der Primzahl p
Permutationsgruppe … symmetrische Gruppe - oder auch deren Untergruppe, d.h. alternierende Gruppe
Punktgruppe … Symmetriegruppe eines Körpers, insbesondere eines Moleküls
Raumgruppe … Symmetriegruppe eines Kristalls

spezielle lineare Gruppe SL(n,F) vom Grad n über einem Körper F
Menge aller invertierbaren n×n-Matrizen mit der Determinante 1; Untergruppe der allgemeinen linearen Gruppe

symmetrische Gruppe … besteht aus allen Permutationen einer Menge mit n Elementen, Gruppenverknüpfung ist die Verkettung der Permutationen
Quelle http://de.wikipedia.org/wiki/Gruppentheorie-Glossar



Lie-Gruppe
Eine Lie-Gruppe ist eine Gruppe, die auch analytische reelle oder komplexe Mannigfaltigkeit ist, und deren Verknüpfung eine analytische Funktion ist.

Typische Beispiele für Liesche Gruppen sind die allgemeine lineare Gruppe, die Gruppe der invertierbaren Matrizen mit der Matrizenmultiplikation als Verknüpfung und deren Untergruppen, zum Beispiel die Gruppe S(3) aller Drehungen im dreidimensionalen Raum.
Der Euklidische Raum R^n mit der Vektoraddition als Gruppenoperation ist eine reelle Lie-Gruppe.
Jede Lie-Gruppe ist eine topologische Gruppe. Man kann Lie-Gruppen auch nach ihren algebraischen, gruppentheoretischen Eigenschaften klassifizieren.
2007 gelang es nach fast fünf Jahren intensiver Forschung Mathematikern um Jeffrey Adams von der University of Maryland in College Park eine der komplexesten mathematischen Strukturen zu entschlüsseln, die Lie-Gruppe E8.
Deren Elemente beschreiben die isomorphen Drehungen eines 57-dimensionalen geometrischen Objekts. Die Abbildung zeigt eine Veranschaulichung dieser Gruppe.

Zyklische Gruppe
Eine Gruppe G, die von genau einem Element p erzeugt wird: alle Elemente von G sind Potenzen von p.

Endlicher Fall
Zuerst nehmen wir an, die Gruppe sei endlich und ord(G) = n. Wenn n = 1 muss das erzeugende Element a mit dem neutralen Element e der Gruppe identisch sein.

Nehmen wir jetzt n > 1 an. In G liegen dann die folgenden Elemente e = a^0, a^1, a^2, …, a^n, a^{n+1}, …
Da G endlich ist, muss $a^k = a^l$ für gewisse k, l ∈ N. ObdA. gelte k > l, dann ist auf Grund der Potenzgesetze $a^{k-l} = e$.
Sei m die kleinste Zahl, für die $a^m = e$. Wenn i, j < m und i ≠ j, dann gilt $a^i \neq a^j$. Damit bildet

$$<a> = (\{e, a, a^2, \ldots, a^{m-1}\}, \cdot)$$

eine Untergruppe von G. Andererseits ist G als von a erzeugte Gruppe die kleinste Untergruppe, die G und damit <a> enthält. Es gilt also und folglich $a^m = a^n = e$.

Unendlicher Fall

Im Unendlichen Fall besteht die zyklische Gruppe C_∞ aus den Elementen {… , a^{-n}, …, a^{-2}, a^{-1}, e, a, a^2, …, a^n, …}.
C_∞ ist isomorph zur additiven Gruppe der ganzen Zahlen.
Alle zyklischen Gruppen sind abelsche Gruppen. Weiter gilt: Sei G eine Gruppe mit ord(G) = p und p eine Primzahl, dann ist G zyklisch.

Auflösbare Gruppen

Eine Gruppe G heißt genau dann auflösbar, wenn es eine Folge

$$G_0 \subseteq G_1 \subseteq \ldots \subseteq G_{n-1} \subseteq G_n = G$$

von Untergruppen G_j in G gibt mit $G_0 = \{e\}$ und $G_n = G$, wobei für alle j gilt:

G_j ist Normalteiler von G_{j+1} und G_{j+1}/G_j ist kommutativ.

Beispiele: 1) Jede kommutative Gruppe ist auflösbar.
2) Permutationsgruppen: Die kommutative Gruppe S_2 ist auflösbar.
Die Gruppe S_3 ist auflösbar, z.B. $\{e\} \subseteq A_3 \subseteq S_3$.
Die Gruppe S_4 ist auflösbar, z.B. $\{e\} \subseteq K_4 \subseteq A_4 \subseteq S_4$.
Man beachte $ord(A_3) = 3$, $ord(S_j/A_j) = 2$ und $ord(A_4/K_4) = 3$. Da die Ordnungen Primzahlen sind, sind diese Gruppen zyklisch und kommutativ.
3) Die Gruppe S_n ist für n ≥ 5 nicht auflösbar. Der Grund liegt in der Einfachheit der Gruppe A_5. Nach der Galoistheorie sind damit Gleichungen vom Grad ≥ 5 nicht durch geschlossene Formeln darstellbar sind.

Quasigruppen, Loop

Fordert man die eindeutige Lösbarkeit sämtlicher Gleichungen der Form x*a = b und a*y = b dagegen unter Verzicht auf die Assoziativität, so gelangt man zu speziellen Gruppoiden, den Quasigruppen. Besitzt solch eine Quasigruppe ein Einselement, so spricht man von einer Loop.
Wie für jede algebraische Struktur bezeichnet man auch hier die Mächtigkeit | G | der Trägermenge G als Ordnung der Gruppe (Quasigruppe, Loop).

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Beispiele für Gruppen sind:
Die additive Gruppe (Z,+) der ganzen Zahlen mit dem neutralen Element 0. Sie ist abelsch und von unendlicher Ordnung.

*	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

Die additiven Gruppen (Q,+), (R,+) und (C,+) der Körper der rationalen, der reellen und der komplexen Zahlen sind ebenfalls abelsche Gruppen unendlicher Ordnung.
Die multiplikativen Gruppen (Q\{0},*), (R\{0},*) und (C\{0},*) der Körper der rationalen, der reellen und der komplexen Zahlen sind ebenfalls abelsche Gruppen unendlicher Ordnung.

*	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Die Menge V der Vektoren eines Vektorraumes bildet bezüglich der Addition von Vektoren eine abelsche Gruppe (V,+). Insbesondere gehören hierzu die arithmetischen Vektorräume (Rn,+), die unendliche Ordnung besitzen.
Die Menge T der Translationen, also der Parallelverschiebungen, eines Vektorraumes bildet bezüglich der Hintereinanderanwendung von Abbildungen eine abelsche Gruppe (T,o)

*	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

Quasigruppen der Ordnung 3

Auf einer dreielementigen Menge G = {a, b, c} lassen sich die fünf Verknüpfungen durch ihre jeweiligen Cayley-Tafeln definieren. Jede von ihnen liefert eine Quasigruppe, denn jedes Element kommt in jeder Zeile und jeder Spalte genau einmal vor.

*	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

Außerdem sind alle diese Quasigruppen nicht isomorph untereinander. Andererseits existieren genau 12 verschiedene Verknüpfungstafeln mit drei Elementen. Von diesen

12 Quasigruppen ist jede zu genau einer der angegebenen fünf isomorph.
von oben nach unten:
1. zyklische (kommutative) Gruppe der Ordnung 3. Sie enthält genau ein idempotentes Element, hier a
2. diese Quasigruppe ist nicht kommutativ und hat ein Linkseinselement a, das kein Rechtseinselement ist
3. die Quasigruppe ist nicht kommutativ und hat ein Rechtseinselement a, das kein Linkseinselement ist
4. die Quasigruppe ist idempotent und kommutativ
5. die Quasigruppe enthält kein idempotentes Element und ist kommutativ

Cayley-Tafeln

*	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	a	d	e
c	c	d	e	a	b
d	d	b	c	e	a

Zur Definition einer Verknüpfung * auf einer kleinen endlichen Menge G benutzt man oft die Form einer Tabelle, eine Methode die auf Arthur Cayley zurückgeht, der sie erstmals bei der Beschreibung von Gruppen einsetzte. Daher werden diese Verknüpfungstafeln auch oft Cayley-Tafeln genannt.
Dabei schreibt man die Elemente der Menge G in einer festen Reihenfolge als Kopfzeile und Kopfspalte einer quadratischen Tabelle und schreibt an den Schnittpunkt der mit dem Element a beschrifteten Zeile und der mit dem Element b beschrifteten Spalte dasjenige Element von G, das sich bei der Verknüpfung a*b ergeben soll.
So kann man auf der Menge G = {e, a, b, c, d} die Verknüpfung * wie folgt definieren:

Nun kann man beispielsweise aus dem Eintrag "b" in der mit "a" beschrifteten Zeile und der mit "c" beschrifteten Spalte ablesen, dass a*c = b gelten soll. Einige Eigenschaften der Verknüpfung * kann man leicht aus der Cayley-Tafel ablesen: Die Kommutativität zeigt sich an der Symmetrie der Tafel zur "Hauptdiagonalen", die von links oben nach rechts unten verläuft. Sie ist im obigen Beispiel nicht gegeben, da etwa a*c = b aber c*a = d gilt.
Die Idempotenz eines Elementes zeigt sich an seinem Auftreten auf der Hauptdiagonalen an der durch das Element selbst bestimmten Zeile und/oder Spalte. Damit ist auch die Idempotenz der Verknüpfung einfach zu erkennen. Im angegebenen Beispiel ist nur das Element e idempotent.
Ein neutrales Element macht sich dadurch bemerkbar, dass in "seiner" Zeile und "seiner" Spalte die Kopfzeile bzw. die Kopfspalte wiederholt wird. Dies ist im obigen Beispiel genau für das Element e der Fall.
Die Linkskürzbarkeit bzw. Rechtskürzbarkeit eines Elementes erkennt man daran, dass in seiner Zeile bzw. seiner Spalte jedes Element von G höchstens (und damit wegen der Endlichkeit von G genau) einmal auftritt. Sie ist im obigen Beispiel für alle Elemente gegeben und daher handelt es sich um eine Quasigruppe, wegen des neutralen Elementes also sogar um eine Loop.

Light's-Assoziativtest

a	a	e	d	b	c
	a	e	d	b	c
	e	a	c	d	b
	c	b	e	a	d
	d	c	b	e	a
	b	d	a	c	e

Am schwierigsten zu prüfen ist die Assoziativität. Dies geschieht durch den folgenden Assoziativitätstest nach F. W. Light.
Für jedes Element y von G ist zu prüfen, ob für alle x, z gilt : v(x,z) = x*(y*z) = (x*y)*z = v'(x,z), d.h., ob die beiden durch v und v' definierten Verknüpfungen auf G übereinstimmen. Man schreibt also im Prinzip für jedes y die Verknüpfungstafel für v(x,z)=x*(y*z) und für v'(x,z)=(x*y)*z nebeneinander und vergleicht sie anschließend.
Zur Aufstellung der Tafel für v(x,z) muss einfach nur in der Tafel für * die Spalte des Elemente "z" durch die Spalte des Elementes "y*z" ersetzt werden. Zur Aufstellung der Tafel für v'(x,z) muss entsprechend nur in der Tafel für * die Zeile des Elemente "x" durch die Zeile des Elementes "x*y" ersetzt werden. Dabei kann man sich das explizite Hinschreiben der Tafel für v'(x,z) sparen und nur nachschauen, ob die hinzuschreibende Zeile für v'(x,z)schon in der betreffenden Zeile für v(x,z) steht. Ist dies einmal nicht der Fall, hat man die Assoziativität von * bereits widerlegt und auch ein Gegenbeispiel gefunden.
In dem konkreten Beispiel von oben verläuft etwa der Test für y=a wie folgt:
Man stellt die Tafel für v(x,z)=x*(a*z) auf, indem man als Kopfzeile die Zeile von "a" aus der Tafel für * nimmt. Dies sind die Spaltenindizes a*z. Die Kopfspalte lässt man zunächst noch

a	a	e	d	b	c
a	a	e	d	b	c
e	e	a	c	d	b
c	c	b	e	a	d
d	d	c	b	e	a
b	b	d	a	c	e

leer! Nun schreibt man unter jedes Element der Kopfzeile die zugehörige Spalte aus der Tafel für *. Damit ist die Tafel bis auf die Kopfspalte ausgefüllt.
In diese Kopfspalte schreibt man nun die Spalte von "a" aus der Tafel von *. Dies sind die Zeilenindizes x*a. Jetzt muss man prüfen, ob die Zeile hinter jedem Element der Kopfspalte die Zeile dieses Elementes aus der Tafel von * ist. Dies entspricht dem Vergleich mit der Tafel von v'(x,z)=(x*a)*z.
In dem Beispiel stimmt dies erstmals nicht in der Zeile von e=(a*a) und der Spalte von d=(a*b). Dort steht ein c und es müsste ein b stehen. Man sieht also, dass (a*a)*b = e*b = b nicht gleich a*(a*b) = a*d = c ist und die Verknüpfung * daher nicht assoziativ. Es handelt sich also um eine echte Loop, die keine Gruppe ist. Natürlich leisten heutige Computerprogramme das Testen auf Assoziativität bedeutend schneller als dieser Test "per Hand".

Untergruppe

Gegeben sei eine Gruppe G und eine Menge G'. Das Gebilde (eine Menge und eine Verknüpfung) G' nennt man dann Untergruppe G' der Gruppe G, wenn das Gebilde G' folgende drei Bedingungen erfüllt:

1. G' liegt die gleiche Verknüpfung • zugrunde wie G
2. G' liegt eine nichtleere Teilmenge G' der Menge G zugrunde
3. Das Gebilde G' ist selbst wieder eine Gruppe

Aus 3. ergeben sich die Forderungen:

die Verknüpfung • muss auch in der Teilmenge G' abgeschlossen sein

zu jedem Element g' der Teilmenge G' muss ein inverses Element existieren, welches wieder in G' liegt

ist e das neutrale Element von G, dann ist e auch das neutrale Element von G'.

Untergruppenkriterium

Eine nichtleere Teilmenge $H \subseteq G$ ist genau dann Untergruppe von G, wenn für zwei Elemente a, $b \in H$ gilt

$a \bullet b_1 \in H$

Durchschnittssatz

Der Durchschnitt beliebiger Untergruppen ist eine Untergruppe.

Beispiele

$(Z, +)$ ist eine Untergruppe von $(Q, +)$, die ihrerseits eine Untergruppe von $(R, +)$ ist. $(Z_n, +_{\text{mod } n})$ ist für alle n eine Untergruppe von $(Z, +)$.
Betrachtet man alle durch 2 teilbaren Zahlen aus Z, so bilden diese bzgl. der Addition ein Gruppe, sind also Untergruppe von (Z, +). Analoges kann man für alle durch 3, 4, … teilbaren Zahlen feststellen.
Wenn S(F) die Symmetriegruppe einer ebenen Figur ist, so bilden die Drehungen Rot(F) eine Untergruppe zu dieser. Die Spiegelungen bilden im Allgemeinen keine Untergruppe, da man sich schon an der Symmetriegruppe des Rechtecks klarmachen kann, dass die Hintereinanderausführung der Spiegelungen eine Drehung ergibt.
Auch ist die Symmetriegruppe des Rechtecks eine Untergruppe der Symmetriegruppe des Quadrats.

Erzeugte Untergruppen

Sei (G, •) eine Gruppe und $M \subseteq G$ eine nichtleere Teilmenge von G. Dann heißt <M> als Durchschnitt aller Untergruppen, die M enthalten, die von M erzeugte Untergruppe oder das Erzeugnis von M.
Diese Definition ist möglich, da der Durchschnitt einer beliebigen Familie von Untergruppen wieder eine Untergruppe ist. <M> ist die kleinste Untergruppe von G ist, die die Menge M umfasst.

Wenn e das neutrale Element ist, ist <e> die triviale Untergruppe, die nur aus dem neutralen Element besteht. Weiterhin ist <G> = G, d.h. die ganze Gruppe erzeugt sich selbst.

Vereinigung von Untergruppen

Die Vereinigung zweier Untergruppen H_1 und H_2 muss nicht notwendigerweise wieder eine Untergruppe sein.
Benutzt man jedoch die von H_1 und H_2 erzeugte Untergruppe $<H_1 \cup H_2>$, so kann man auch für die Vereinigung von Untergruppen sinnvoll eine Untergruppe definieren.

Komplexprodukt

Seien A und B zwei nichtleere Teilmengen einer Gruppe G, dann definiert man das Komplexprodukt AB wie folgt:

$$AB = \{a \bullet b \mid a \in A, b \in B\}$$

Das Komplexprodukt enthält damit alle Elemente aus G, die sich als Produkt von Elementen aus A und B darstellen lassen.

Zyklische Untergruppen

Die Gruppe G selbst und {e} sind Untergruppen von G, die trivialen Untergruppen.
Außerdem bestimmt jedes Element $a \in G$ eine Untergruppe, die von a erzeugte zyklische Untergruppe

$$< a > = \{\ldots, a^{-2}, a^{-1}, e, a, a^1, a^2, \ldots\}$$

Ist die Gruppenoperation eine Addition, so schreibt man statt der Potenzen a^k als Abkürzung für die k-fache Verknüpfung von a mit sich selbst ganzzahlige Vielfache ka als Abkürzung für die k-fache Addition.

$< a >$ ist die kleinste Untergruppe von G die a enthält. Gilt $< a > = G$ für ein Element a aus G so heißt G eine zyklische Gruppe. Es gibt endliche und unendliche zyklische Gruppen.
Ist die Elementeanzahl einer endlichen Gruppe G eine Primzahl, so ist G stets zyklisch.
Man kann den Begriff der zyklischen Gruppe wie folgt verallgemeinern: Ist M eine nichtleere Teilmenge einer Gruppe G, so wird mit <M> die Untergruppe von G bezeichnet, deren Elemente sich sämtlich als Produkt von endlich vielen Elementen aus M und deren Inversen schreiben lassen. Die Teilmenge M heißt dann Erzeugendensystem von <M>. Besteht M nur aus einem Element, dann ist <M> zyklisch.

Zentrum einer Gruppe

Unter dem Zentrum Cent(G) einer Gruppe G versteht man alle kommutierenden Elemente.

$$Cent(G) = \{g \in G \mid \forall a \in G: ag = ga\}$$

Das Zentrum einer abelschen Gruppe ist die Gruppe insgesamt, da in ihr alle Elemente kommutieren. Das Zentrum einer Gruppe G ist Normalteiler. Cent(G) ist eine kommutative Gruppe.

Gruppenordnung, Links- und Rechtsnebenklassen

In der Gruppentheorie wird die Elementenzahl einer endlichen Gruppe mit ord G bezeichnet.
Ist die von einem Element a einer Gruppe erzeugte zyklische Untergruppe <a> endlich, so heißt deren Ordnung auch Ordnung des Elements a, d.h. $\text{ord } <a> = \text{ord } a$
Ist U eine Untergruppe einer Gruppe (G, •) und $a \in G$, so heißen die Teilmengen

$$aU = \{a \bullet u \mid u \in U\} \text{ bzw. } Ua = \{u \bullet a \mid u \in U\}$$

von G Linksnebenklassen bzw. Rechtsnebenklassen von U in G.
Sei H eine Untergruppe von G, $a, b \in G$ und e das neutrale Element. Dann gilt

$$aH = bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow a^{-1}b \in H \qquad eH = H \qquad a \in H \Leftrightarrow aH = Ha = H$$

Entsprechende Aussagen lassen sich auch für Rechtsnebenklassen formulieren.

Die Links- bzw. Rechtsnebenklassen bilden jeweils eine Zerlegung von G. Damit sind zwei Nebenklassen entweder disjunkt oder sie sind gleich und jedes Gruppenelement kommt in einer Nebenklasse vor. Je zwei Nebenklassen lassen sich bijektiv aufeinander abbilden und sind daher gleichmächtig.
Alle Links- oder Rechtsnebenklassen einer Untergruppe U in einer Gruppe G haben die gleiche Anzahl von Elementen, nämlich ord U. Daraus ergibt sich, dass die Anzahl der Linksnebenklassen gleich der Anzahl der Rechtsnebenklassen ist. Diese Zahl wird Index von U in G genannt. Aus den genannten Fakten ergibt sich der Satz von Lagrange.

Satz von Lagrange

Die Ordnung einer Untergruppe ist stets Teiler der Gruppenordnung.
Im allgemeinen ist es schwierig, alle Untergruppen einer Gruppe anzugeben. Im Falle endlicher Gruppen ist der Satz von Lagrange als notwendige Bedingung für die Existenz von Untergruppen hilfreich.

Darstellungssatz von Cayley

Zur Klassifikation von Gruppen gilt der Darstellungssatz von Cayley:
Jede Gruppe ist isomorph zu einer Gruppe von Permutationen. Für jede Gruppe $(G; \circ)$ gibt es einen injektiven Gruppenhomomorphismus $\pi: G \to S(G)$ in die symmetrische Gruppe auf G, und dessen Bild ist eine zu G isomorphe Untergruppe der S(G).
Für $a \in G$ leistet $\pi(a) := (g \in G \to ag \in G)$ das Gewünschte.

Normalteiler

Es seien $(G; \circ)$ eine Gruppe und $N \leq G$ eine Untergruppe. Man nennt N einen Normalteiler oder eine invariante Untergruppe von G, falls N unter Konjugationen mit Gruppenelementen invariant bleibt, $\forall\, g \in G: gNg^{-1} \subseteq N$.

In einer Abelschen Gruppe ist jede Untergruppe auch Normalteiler, in einer nicht-Abelschen Gruppe im Allgemeinen jedoch nicht. Eine Untergruppe vom Index 2 ist immer Normalteiler.
Für $n \in N$ bildet die Menge A_n aller geraden Permutationen einen Normalteiler von S_n.
Äquivalente Bedingung für eine Untergruppe N, Normalteiler in G zu sein: $\forall\, g \in G: gN = Ng$

d.h. Linksnebenklasse = Rechtsnebenklasse. Insbesondere ist die Menge aller Linksnebenklassen gleich der Menge aller Rechtsnebenklassen.
Diese Menge $G/N = \{ gN \mid g \in G\}$ ist für die Struktur von Gruppen und von Gruppenhomomorphismen besonders wichtig. Auf ihr lässt sich in natürlicher Weise eine Gruppenoperation definieren,

$$gN \circ hN = (gh)N$$

womit G/N die Struktur einer Gruppe mit dem neutralen Element N erhält. Die Abbildung

$$\pi: G \to G/N \text{ mit } \pi(g) = gN$$

die jedem Gruppenelement seine Nebenklasse zuordnet, ist surjektiv und wird als kanonische Projektion bezeichnet.

Einfache Gruppe

Eine Gruppe G der Ordnung n wird einfache Gruppe genannt, wenn alle ihrer Normalteiler die Ordnung 1 oder n haben. Einfache Gruppen werden in vier Typen eingeteilt:

- zyklische Gruppen von Primzahlordnung
- alternierende Gruppen von mindestens Ordnung 5
- endliche Liesche Gruppen vom Typ Chevalley
- endliche Liesche Drehgruppen der Ordnung 14, 52, 78, 133 und 248
- sporadische Gruppen (26 Möglichkeiten)

1980 wurde mit dem Nachweis, dass es nur 26 sporadische Gruppen gibt, die Klassifikation der einfachen Gruppen vervollständigt.

Sporadische Gruppe

Während die ersten vier Arten einfacher Gruppen in Serien eingeteilt werden können, sind die sporadischen Gruppen isoliert.
Bis 1965 waren nur fünf dieser Gruppen bekannt, die alle von dem französischen Mathematiker Mathieu zwischen 1861 und 1873 entdeckt wurden. Diese sehr speziellen Gebilde beschreiben Funktionen und kombinatorische Strukturen in 12- und 24-dimensionalen Räumen mit besonderen Symmetrieeigenschaften.
Interessant ist, dass die Mathieu-Gruppen die Grundlage zur Konstruktion hocheffizienter Korrekturcodes sind. Die Ordnungen dieser Gruppen sind 7920, 95040, 443520, 10200960 und 244823040.

1965 wurde durch Janko die sechste sporadische Gruppe mit der Ordnung 175560 entdeckt. Mittlerweile kennt man alle möglichen 26 sporadischen Gruppen. Die mit der größten Ordnung von

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

$= 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368 \cdot 10^9$
$= 8{,}08\ldots \cdot 10^{53}$

wird Monster-Gruppe genannt. Diese wurde 1982 von Robert Griess als Rotationsgruppe in einem 196883-dimensionalen Raum nachgewiesen.
Liste siehe

Liste der sporadischen Gruppen

Gruppe	Ordnung
Mathieugruppe M11	7 920
Mathieugruppe M12	95 040
Mathieugruppe M22	443 520
Mathieugruppe M23	10 200 960
Mathieugruppe M24	244 823 040
Jankogruppe J1	175 560
Jankogruppe J2	604 800
Jankogruppe J3	50 232 960
Jankogruppe J4	86 775 571 046 077 562 880
Higman-Sims-Gruppe HS	44 352 000
Conwaygruppe Co1	4 157 776 806 543 360 000
Conwaygruppe Co2	42 305 421 312 000
Conwaygruppe Co3	495 766 656 000
Heldgruppe He	4 030 387 200
McLaughlin-Gruppe Mc	898 128 000
SuzukigruppeSuz	448 345 497 600
Fischergruppe F22	64 561 751 654 400
Fischergruppe F23	4 089 470 473 293 004 800
Fischergruppe F24	1 255 205 709 190 661 721 292 800
Lyonsgruppe Ly	51 765 179 004 000 000
Rudvalisgruppe Ru	145 926 144 000
Baby-Monstergruppe F2	4 154 781 481 226 426 191 177 580 544 000 000
O'Nan-Gruppe ON	460 815 505 920
Thompsongruppe F3	90 745 943 887 872 000
Harada-Norton-Gruppe F5	273 030 912 000 000
Monstergruppe F1	808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

20 der 26 sporadischen Gruppen lassen sich als Untergruppen oder Quotientengruppen von Untergruppen der Monstergruppe auffassen. Die sechs Ausnahmegruppen sind die Jankogruppen J1, J3 und J4, die O'Nan-Gruppe, die Rudvalisgruppe und die Lyonsgruppe.

Freie Halbgruppen

Es sei A eine beliebige nichtleere Menge, die in diesem Zusammenhang auch Alphabet genannt wird und deren Elemente entsprechend Buchstaben heißen. Weiterhin bezeichne F_A die Menge aller Worte, d.h. aller endlichen Sequenzen $(a_1,\ldots,a_n)$ von Elementen a_i aus A.
Dabei ist auch das leere Wort als Sequenz der Länge 0 eingeschlossen. Für Worte $(a_1,\ldots,a_n)$ und $(b_1,\ldots,b_m)$ definiert man als innere Verknüpfung die Konkatenation gemäß

$(a_1,\ldots,a_n)*(b_1,\ldots,b_m) = (a_1,\ldots,a_n,b_1,\ldots,b_m)$.

Diese Verknüpfung ist assoziativ und das leere Wort ist neutrales Element. Also ist $(F_A,*)$ ein Monoid, das freie Monoid oder die freie Halbgruppe über A. Dieses Monoid ist genau dann kommutativ, wenn A aus einem Element besteht.
Man schreibt ein Wort $(a_1,\ldots,a_n)$ auch kurz als $a_1\ldots a_n$ und lässt das Verknüpfungssymbol bei der Konkatenation weg. Will man das leere Worte explizit ansprechen, so verwendet man meistens das Symbol l oder auch e, das natürlich nicht schon in A vorkommen darf. Eine große Bedeutung besitzen freie Monoide F_A in der Theorie der formalen Sprachen, wo sie meistens mit A* bezeichnet werden, denn eine formale Sprache L wird dort als beliebige Teilmenge von A* definiert.

Transformationshalbgruppen

Für eine beliebige nichtleere Menge X betrachte man die Menge T_X aller Abbildungen f: X -> X von X in sich, die Transformationen von X. Durch die Nacheinanderanwendung (f o g)(x) =

f(g(x)) für alle x aus X und alle f und g aus T_X ist eine assoziative Verknüpfung o auf T_X definiert.

S_3	123	132	213	231	312	321
123	123	132	213	231	312	321
132	132	123	312	321	213	231
213	213	231	123	132	321	312
231	231	213	321	312	123	132
312	312	321	132	123	231	213
321	321	312	231	213	132	123

Die identische Abbildung id_X auf X, die jedes x aus X auf sich selbst abbildet, ist neutrales Element bezüglich dieser Verknüpfung, so dass (T_X,o) ein Monoid ist.
In (T_X,o) sind genau die konstanten Abbildungen c_x : X -> X mit $c_x(y) = x$ für alle y aus X und ein jeweils festes x aus X linksabsorbierend und genau die injektiven Abbildungen linkskürzbar.
Sobald X zwei verschiedene Elemente enthält, existieren zwei verschiedene konstante Abbildungen, und (T_X,o) ist weder kommutativ noch eine Gruppe.

Symmetrische Gruppen

Wie in jedem Monoid, so kann man auch in (T_X,o) die Untergruppe der Einheiten bilden, d.h. in diesem Fall, der invertierbaren Abbildungen f: X -> X. Diese nennt man auch die Permutationen (der Elemente) von X und schreibt (S_X,o) für diese symmetrische Gruppe auf X. Im Fall X = {1,...,n} kürzt man dies zu (S_n,o) ab. Man sieht, dass S_n aus genau n! = 1*2*3*...*n verschiedenen Permutationen besteht und dass diese symmetrische Gruppe für n > 2 nicht kommutativ ist.
Die symmetrische Gruppe S_n enthält jede Gruppe der Ordnung n als Untergruppe.
Die Abbildung zeigt die Gruppentafel der symmetrischen Gruppe S_3.

Permutationsgruppe

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Unter einer Permutation einer Menge M versteht man die eineindeutige Abbildung der Menge M auf sich, d.h. eine Zuordnung s, bei der jedem Element a von M ein Bild s(a) entspricht und jedes Element von M das Bild genau eines a ist.
Ist M endlich und sind ihre Elemente mit den Nummern 1, 2, …, n versehen, so kann man jede Permutation vollständig durch ein Schema beschreiben, in dem man unter jeder Nummer k die Nummer s(k) des Bildelementes schreibt. (siehe Abbildung)
Unter dem Produkt st zweier Permutationen s und t wird diejenige Permutation verstanden, die entsteht, wenn man zuerst die Permutation t und dann auf die Bildmenge die Permutation s ausübt, d.h.

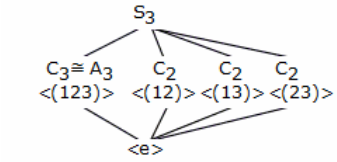
st(a) = s(t(a))

Für drei Permuationen r, s, t gilt das Assoziativgesetz (rs) t = r (st)
Die identische Permutation I bildet jedes Element auf sich selbst ab und es gilt

I(a) = a sowie Is = s

Das Inverse einer Permutation s ist diejenige Permutation, die s(a) auf a abbildet. Bezeichnet man sie mit s^{-1}, so gilt $s^{-1}s(a) = a$ und $s^{-1}s = I$
Damit bildet die Menge der Permuationen einer Menge M mit der Produktbildung eine Gruppe, die Permutationsgruppe.
Ist die Menge M endlich mit n Elementen, so spricht man von der symmetrischen Gruppe σ_n oder S_n. Der Name wurde gewählt, weil die Funktionen, die bei allen Permutationen der Gruppe invariant bleiben, die symmetrischen Funktionen sind.

(1)	(123)	(132)	(12)	(13)	(23)
(123)	(132)	(1)	(13)	(23)	(12)
(132)	(1)	(123)	(23)	(12)	(13)
(12)	(23)	(13)	(1)	(132)	(123)
(13)	(12)	(23)	(123)	(1)	(132)
(23)	(13)	(12)	(132)	(123)	(1)



Permutationsgruppe S_3

Die Permutationsgruppe S_3 bzw. symmetrische Gruppe S_3 besteht aus 6 Elementen, den Permutationen einer dreielementigen Menge.
In Zyklenschreibweise ergibt sich die oben abgebildete Gruppentafel.
Der Gruppentafel entnimmt man sofort, dass die S_3 isomorph zur Diedergruppe D_3 ist. Auch die Untergruppen der S_3 lassen sich relativ einfach aufklären.
Einerseits gibt es eine zur C_3 isomorphe Untergruppe, die von der Permutation (123) erzeugt wird. Diese Untergruppe ist auch genau die alternierende Gruppe A_3.
Andererseits erzeugen die Transpositionen (12), (13) und (23) zur C_2 isomorphe Untergruppen.

Der Zusammenhang zwischen den einzelnen Untergruppen wird durch den unten abgebildeten Untergruppengraphen veranschaulicht.

Permutationsgruppe S_4

S_4 sei die Menge aller möglichen 24 Permutationen von vier Elementen {1, 2, 3, 4}. Mit der Nacheinanderausführung zweier Permutationen bildet S_4 eine Gruppe, die Permutationsgruppe S_4. Die Permutationsgruppe S_4 besitzt 30 verschiedene Untergruppen. Zwei Untergruppen G_1 und G_2 gehören zur gleichen Klasse, wenn ein Element x mit $G_1 = x^{-1} G_2 x$ existiert. Für S_4 existieren 11 verschiedene Klassen.
In der Tabelle sind alle Untergruppen mit ihren Elementen nach Klassen sortiert aufgelistet. Als Kurzschreibweise wird [abcd] verwendet, d.h. zum Beispiel für die abgebildete Permutation [3421]. Desweiteren steht "e" für [1234], d.h. die identische Permutation.

Klasse	Elementzahl	Anzahl der Untergruppen	Klasse	Elementzahl	Anzahl der Untergruppen
1	1	1	2	6	2
3	3	2	4	4	3
5	3	4	6	3	4
7	1	4	8	4	6
9	3	8	10	1	12
11	1	24			

Klasse 1	e
Klasse 2	e [1243], e [1432], e [1324], e [4231], e [3214], e [2134]
Klasse 3	e [2143], e [3412], e [4321]
Klasse 4	e [1342] [1423], e [3241] [4213], e [2431] [4132], e [2314] [3124]
Klasse 5	e [2341] [3412] [4123], e [2413] [4321] [3142], e [3421] [2143] [4312]
Klasse 6	e [1243] [2134] [2143], e [1432] [3214] [3412], e [1324] [4231] [4321]
Klasse 7	e [2143] [3412] [4321]
Klasse 8	e [1243] [1324] [1423] [1342] [1432], e [1243] [3214] [4213] [3241] [4231] e [1432] [2134] [4132] [2431] [4231], e [1324] [2134] [3124] [2314] [3214]
Klasse 9	e [1243] [3412] [4312] [3421] [2134] [4321] [2143] e [1432] [2143] [4123] [2341] [3214] [4321] [3412] e [1324] [2143] [3142] [2413] [4231] [3412] [4321]
Klasse 10	e [1342] [1423] [2143] [3124] [4132] [2431] [2314] [4213] [3241] [3412] [4321]
Klasse 11	S4

Permutationsgruppe S_5

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

S_5 sei die Menge aller möglichen 120 Permutationen von fünf Elementen {1, 2, 3, 4, 5}. Mit der Nacheinanderausführung zweier Permutationen bildet S_5 eine Gruppe, die Permutationsgruppe S_5. Die Permutationsgruppe S_5 besitzt 156 verschiedene Untergruppen. Zwei Untergruppen G_1 und G_2 gehören zur gleichen Klasse, wenn ein Element x mit $G_1 = x^{-1} G_2 x$ existiert. Für S_5 existieren 19 verschiedene Klassen.
In der Tabelle ist jeweils eine Untergruppe mit ihren Elementen nach Klassen sortiert aufgelistet. Als Kurzschreibweise wird [abcde] verwendet, d.h. zum Beispiel für die abgebildete Permutation [35124]. Desweiteren steht "e" für [12345], d.h. die identische Permutation.

1.	e
2.	e [12354]
12.	e [13254]
27.	e [12453] [12534]
37.	e [13452] [14523] [15234]
52.	e [12354] [13245] [13254]
67.	e [13254] [14523] [15432]
72.	e [23451] [34512] [45123] [51234]
78.	e [21453] [12534] [21345] [12453] [21534]
88.	e [12354] [12435] [12534] [12453] [12543]
98.	e [12453] [12534] [21354] [21435] [21543]
108.	e [12354] [14523] [15423] [14532] [13245] [15432] [13254]

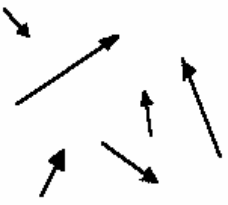
123. e [13254] [21435] [31524] [24153] [42513] [35142] [53412] [54321] [45231]
129. e [12354] [21435] [21534] [21453] [12543] [21543] [12453] [12435] [21345] [21354] [12534]
144. e [13254] [23415] [32514] [24351] [34125] [43521] [31452] [41235] [14532] [42153] [21543] [35241] [25134] [52431] [51324] [15423] [53142] [54213] [45312]
150. e [12354] [13425] [13524] [13452] [14235] [14532] [14253] [12543] [13542] [15234] [15432] [15243] [12453] [15423] [14352] [14325] [13245] [12534] [15324] [14523] [15342] [13254] [12435]
155. e [12453] [12534] [23145] [24153] [25134] [23451] [23514] [31245] [34251] [35214] [31452] [31524] [14352] [15324] [24531] [24315] [41253] [45231] [43215] [41532] [41325] [15432] [13425] [45312] [45123] [52431] [53412] [51423] [52314] [52143] [21543] [53124] [53241] [34512] [32541] [34125] [42351] [15243] [54132] [25341] [25413] [51234] [54213] [51342] [13542] [14523] [32415] [32154] [21354] [13254] [35142] [54321] [42513] [43521] [42135] [21435] [14235] [43152] [35421]
156. S5

Restklassengruppe Z/(n)

Für jede natürliche Zahl n bilden die ganzzahligen Vielfachen n*Z = { g*n | g aus Z} = {...,-2*n, -n, 0, n, 2*n,... }
eine Untergruppe der abelschen Gruppe (Z,+), denn die Differenz zweier Elemente aus n*Z liegt wieder in (der nichtleeren Menge) n*Z. Für n = 0 bzw. n = 1 sind dies gerade die trivialen Untergruppen { 0 } bzw. Z selbst.
Wegen der Kommutativität von (Z,+) ist jede dieser Untergruppen schon ein Normalteiler. Damit erhält man die jeweilige Faktorgruppe (Z/n*Z,+) = (Z/(n),+), die aus den Klassen der durch n*Z bestimmten Kongruenzrelation ~ besteht. Sie wird die Restklassengruppe Z modulo n genannt.
Dabei sind zwei Elemente a und b aus Z genau dann kongruent modulo n, wenn ihre Differenz durch n ohne Rest teilbar ist, d.h., wenn sie beide bei Division durch n denselben ganzzahligen Rest liefern. Für n > 0 wählt man als Repräsentanten der Klassen üblicherweise die Zahlen 0, 1, ..., n-1 und erhält so Z/(n) = { $[0]_n$, $[1]_n$, ..., $[n-1]_n$ }
(Z/(n),+) hat dann die Ordnung n und damit sind für verschiedene natürliche Zahlen n und m die Restklassengruppen (Z/(n),+) und (Z/(m),+) nicht isomorph. Außerdem ist jede dieser Gruppen zyklisch, denn sie wird von der Restklasse $[1]_n$ erzeugt. Es gibt also zu jeder natürlichen Zahl n > 0 eine (zyklische und damit abelsche) Gruppe der Ordnung n.

Restklassengruppe, Untergruppe

Ist (U,+) irgendeine von { 0 } verschiedene Untergruppe von der Restklassengruppe (Z,+), so gibt es wenigstens ein von 0 verschiedenes Element u in U. Damit liegt aber auch -u in U und daher wenigstens eine positive natürliche Zahl.
Es sei nun n die kleinste positive natürliche Zahl aus U. Dann ist n*Z schon in U enthalten. Ist nun u irgendein Element von U, so liefert die Division mit Rest eine Zerlegung u = g*n + r mit einer ganzen Zahl g und einem Rest 0 ≤ r < n.
Nun liegt aber r = u - g*n in U und wegen der Minimalität von n ist dies nur für r = 0 möglich, d.h. u = g*n liegt schon in n*Z und es gilt folglich U = n*Z. Daher sind die Untergruppen n*Z bereits sämtliche Untergruppen (und Normalteiler) von (Z,+).
Also ist nach dem Homomorphiesatz jedes homomorphe Bild von (Z,+) zu genau einer der zyklischen Restklassengruppen (Z/(n),+) isomorph.



Gruppe euklidischer Vektoren

Grundmenge: die Menge der (euklidischen) Vektoren der Ebene
Verknüpfung: Addition zweier euklidischer Vektoren der Ebene
Man addiert zwei Vektoren a und b, indem man den Anfang des Vektors b an das Ende des Vektors a verschiebt. Der Vektor a+b ist dann der Vektor, der vom Anfang vom a bis zum Ende von b reicht.
Abgeschlossenheit der Verknüpfung: Addiert man zwei Vektoren der Ebene, so ist das Ergebnis wieder ein Vektor der Ebene.
Assoziativität: Die Addition dreier Vektoren der Ebene ist assoziativ.
Neutrales Element: Das neutrale Element ist der Nullvektor.
Inverse Elemente: Die inversen Elemente sind Vektoren mit umgekehrter Richtung.

Kommutativität: Die Vektoraddition zweier Vektoren der Ebene ist kommutativ. (Kräfteparallelogramm)

Ideale von Gruppoiden

Unter einem Linksideal eines Gruppoids (G,*) versteht man eine nichtleere Teilmenge L von G, die

(l) g*a liegt in L für alle a aus L und alle g aus G

erfüllt. Analog heißt eine nichtleere Teilmenge R von G ein Rechtsideal von (G,*), wenn

(r) a*g liegt in R für alle a aus R und alle g aus G

gilt. Ein (zweiseitiges) Ideal I von (G,*) ist eine Teilmenge von G, die sowohl Links- als auch Rechtsideal ist.
Insbesondere ist jedes Linksideal, jedes Rechtsideal und jedes Ideal ein Untergruppoid von (G,*) und G selbst ist stets ein Ideal von (G,*). Eine einelementige Teilmenge L = { a } ist wegen (l) genau dann Linksideal, wenn a ein rechts-absorbierendes Element von (G,*) ist. Die analoge Aussage gilt für Rechtsideale und linksabsorbierende Elemente.
Daher besitzt ein Gruppoid genau dann ein (einziges) einelementiges Ideal, wenn es ein absorbierendes Element besitzt.
Dieses (nur eventuell vorhandene) Ideal und G selbst heißen die trivialen Ideale von (G,*). Ein Gruppoid, welches nur triviale Ideale besitzt, nennt man auch ideal-einfach.

Ideale

Aus rein mengentheoretischen Definitionen folgt, dass der Durchschnitt D von beliebig vielen Linksidealen (Rechtsidealen, zweiseitigen Idealen) von (G,*) entweder leer ist oder ein Linksideal (Rechtsideal, zweiseitiges Ideal) von (G,*).
Daher existiert zu jeder nichtleeren Teilmenge A von G der Durchschnitt aller Linksideale L_i von (G,*), die A enthalten, und ist ein Linksideal von (G,*), das von A erzeugte Linksideal.
Es ist somit das kleinste Linksideal von (G,*), das A enthält. Analog existieren das von A erzeugte Rechtsideal und das von A erzeugte Ideal.
Wird ein Linksideal von einer einelementigen Menge { a } erzeugt, so spricht man von einem Hauptlinksideal (oder Linkshauptideal) und entsprechend von einem Hauptrechtsideal (oder Rechtshauptideal) bzw. Hauptideal.
Ist das Gruppoid sogar eine Halbgruppe (S,*), so ist für jedes a aus S die Menge S*a = { s*a | s aus S } zwar ein Linksideal von (S,*), das aber nicht unbedingt a enthält.
Dagegen ist stets S^1*a = { a } ∪ S*a das von a erzeugte Hauptideal, das in vielen Fällen, z.B. für Monoide (S,*), mit S*a übereinstimmt. Entsprechendes gilt für Rechtsideale a*S und a*S^1 ={ a } ∪ a*S. Daher ist das von a erzeugte (zweiseitige) Ideal gegeben durch S^1*a*S^1 = { a } ∪ a*S ∪ S*a ∪ S*a*S.

Algebraischer Ring

Ringe und Körper sind algebraische Strukturen mit zwei Operationen, allgemein einer Addition und einer Multiplikation, wobei diese Namen nur der Anschaulichkeit halber gewählt sind.
Eine algebraische Struktur (G, +, •) mit zwei Operationen + und • heißt Ring, wenn gilt:
1. (G, +) ist Abelsche Gruppe
2. Assoziativgesetz für alle a,b,c aus G: (a • b) • c = a • (b • c)
3. Distributivgesetz für alle a,b,c aus G: (a + b) • c = a • b + a • c

Ein Ring heißt kommutativer Ring, falls zusätzlich das Kommutativgesetz bezüglich der zweiten Operation gilt.
Gibt es ein neutrales Element bzgl. der Multiplikation e mit e • a = a • e = a für alle a, so spricht man von einem Ring mit Einselement oder unitären Ring.

Beispiele:
Die Menge der ganzen Zahlen mit der gewöhnlichen Addition und Multiplikation ist ein kommutativer Ring. Die Menge der Polynome mit der gewöhnlichen Addition und Multiplikation ist ein kommutativer Ring.
Ist (G, +) eine abelsche Gruppe, so bilden die Endomorphismen von A einen Ring, den Endomorphismenring End(A). Die Multiplikation • ist dabei die Komposition von Abbildungen. Für f, g ∈ End(A) sind f + g und f • g komponentenweise durch (f + g)(x) = f(x) + g(x) und (f•g)(x) = f(g(x)) definiert.

Restklassenring

Ein Restklassenring ist ein kommutativer Ring $(Z_n,\oplus,\otimes)$ mit Einselement, wobei die Verknüpfungen $\oplus$ und $\otimes$ die gewöhnliche Addition und Multiplikation mod n darstellen

Ringeigenschaften

In einem Ring R gilt für alle $a, b \in R$:

$0a = a0 = a \quad (-a)b = a(-b) = -ab \quad (-a)(-b) = ab$

Nachweis:
(I) $0a = (a - a)a = aa - aa = 0$
(II) $(-a)b = (0 - a)b = 0b - ab = 0 - ab = -ab$
(III) $(-a)(-b) = - (-ab) = ab$

In einem unitären Ring folgt die Kommutativität der Addition aus den anderen Ringaxiomen und es gilt $1 \neq 0$, wenn der Ring vom Nullring verschieden ist und 1 das neutrale Element der Multiplikation und 0 das der Addition ist.
Nachweis: $a + a + b + b = 1a + 1a + 1b + 1b = (1+1) a + (1 + 1)b = (1 + 1)(a + b) = (a + b) + (a + b) = a + b + a + b$
Addiert man nun -a von links und -b von rechts ergibt sich mit $a + b = b + a$ die Behauptung.
Wenn R verschieden vom Nullring ist, gibt es ein $0 \neq a \in R$. Angenommen es ist $0 = 1$, dann gilt auch $0a = 1a$, also $a = 0$. Widerspruch!

Nullteiler

Ein Nullteiler eines kommutativen Ringes R ist ein vom Nullelement verschiedenes Element a, für das es ein Element b ungleich 0 gibt, so dass $ab = 0$, d.h.
wird $a b = 0$, ohne dass $a = 0$ oder $b = 0$, sind a und b Nullteiler von R
Ist R ein nichtkommutativer Ring und $a \neq 0$, dann unterscheidet man zwischen:

- Linksnullteiler: es gibt ein Element $b \neq 0$, so dass $ab = 0$
- Rechtsnullteiler: es gibt ein Element $b \neq 0$, so dass $ba = 0$
- beidseitiger Nullteiler: es gibt Elemente $b,c \neq 0$, so dass $ab = 0$, $ca = 0$.

Ein Ring ohne einseitige oder beidseitige Nullteiler heißt nullteilerfrei.
Ein nullteilerfreier kommutativer Ring mit multiplikativem Einselement heißt Integritätsring.

Integritätsbereich, Integritätsring

Ein Integritätsring oder Integritätsbereich ist ein nullteilerfreier kommutativer Ring mit Einselement. Integritätsringe sind Verallgemeinerungen der ganzen Zahlen und bilden den allgemeinsten Rahmen für die Untersuchung von Teilbarkeiten.
Alternativ kann man einen Integritätsring definieren als einen kommutativen Ring mit 1, in dem das Nullideal {0} ein Primideal ist, oder als einen Teilring eines Körpers.

Beispiele: Das bekannteste Beispiel ist der Ring Z der ganzen Zahlen.
Jeder Körper ist ein Integritätsring. Umgekehrt ist jeder artinsche Integritätsring ein Körper. Insbesondere ist jeder endliche Integritätsring ein endlicher Körper.

Ein Polynomring ist ein Integritätsring, wenn die Koeffizienten aus einem Integritätsring stammen. Zum Beispiel ist der Ring Z[X] der Polynome mit ganzzahligen Koeffizienten ein Integritätsring, ebenso wie der Ring R[X,Y] der reellen Polynome in zwei Variablen.
Der Ring aller reellen Zahlen der Form $a+b\sqrt{2}$ mit ganzen Zahlen a,b ist ein Integritätsring, da er Teilring von R ist.

Ist $U \subseteq C$ ein Gebiet; eine zusammenhängende offene Teilmenge; in den komplexen Zahlen, dann ist der Ring H(U) der homomorphen Funktionen $f: U \to C$ ein Integritätsring.
Ist R ein kommutativer Ring und P ein Primideal in R, dann ist der Faktorring R/P ein Integritätsring. Der Restklassenring Z/nZ ist genau dann ein Integritätsring, wenn n eine Primzahl ist.

Charakteristik eines Integritätsrings

Die Charakteristik eines Integritätsrings ist entweder 0 oder eine Primzahl.
Ist R ein Integritätsring mit der Primzahl-Charakteristik p, dann ist die Abbildung $f: R \to R$, $x \mapsto x^p$ ein injektiver Ringhomomorphismus und heißt Frobeniushomomorphismus.

Teilbarkeit, Primelemente, Irreduzibilität

Sind a und b Elemente des Integritätsrings R, dann sagt man a teilt b oder a ist ein Teiler von b oder b ist ein Vielfaches von a, wenn es ein Element x in R gibt, so dass ax = b. Man schreibt dann a | b.

Gilt a | b und b | c, dann folgt daraus a | c.
Gilt a | b, dann gilt auch a | bc für jedes c aus R, insbesondere auch a | - b.
Gilt a | b und a | c, dann gilt auch a | b + c und a | b - c.
Gilt a | b und b | a, dann heißen a und b zueinander assoziiert. a und b sind genau dann assoziiert, wenn es eine Einheit u gibt, so dass au = b.

Ist q keine Einheit, dann heißt q irreduzibel, falls q nicht als Produkt zweier Nicht-Einheiten darstellbar ist, falls also aus q = ab folgt a $\in$ R* oder b $\in$ R.
Ist p eine Nicht-Einheit ungleich 0, dann heißt p prim oder Primelement, falls gilt: Aus p | ab folgt p | a oder p | b.
Ist p ein Primelement von R, dann ist das Hauptideal (p) ein Primideal.
Jedes Primelement ist irreduzibel, aber nicht immer ist jedes irreduzible Element prim. In faktoriellen Ringen (engl. unique factorization domain, UFD) ist dagegen jedes irreduzible Element prim.
Der Begriff des Primelements verallgemeinert den Begriff der Primzahl. Primzahlen werden üblicherweise als irreduzible Elemente von Z definiert.

Quotientenkörper

Ist R ein Integritätsring, dann existiert ein kleinster Körper Quot(R), der R als Teilring enthält. Quot(R) ist bis auf Isomorphie eindeutig bestimmt und heißt Quotientenkörper von R. Seine Elemente haben die Form a/b mit a,b in R, b ungleich 0.
Der Quotientenkörper des Rings der ganzen Zahlen ist der Körper der rationalen Zahlen. Der Quotientenkörper eines Körpers ist der Körper selbst.
Abstrakt definiert man Quotientenkörper durch folgende Eigenschaft:
Ein Quotientenkörper ist ein Paar (K, ϕ), wobei ϕ ein Ringhomomorphismus von R nach K ist mit der Eigenschaft: Für jeden Körper L und Ringhomomorphismus ψ: R $\rightarrow$ L, gibt es genau einen Körperhomomorphismus α: K $\rightarrow$ L mit $\psi(x) = \alpha(\phi(x))$ für alle x aus R.

Einheiten in Ringen

Ein Element a $\in$ R eines unitären Ringes heißt invertierbar oder Einheit, falls es ein b $\in$ R gibt mit ab = ba = 1.
Die Menge aller invertierbaren Elemente eines unitären Rings werden mit U(R) oder R* bezeichnet. Sie bilden eine Gruppe, die Einheitengruppe.
Ein unitärer Ring R ist genau dann ein Körper, wenn die Einheitengruppe von R alle Elemente bis auf die 0 umfasst.

Nachweis: Es ist offensichtlich, dass in einem Körper die Einheitengruppe der multiplikativen Gruppe des Körpers entspricht. Alle von Null verschiedenen Elemente sind invertierbar.
Wenn die Einheitengruppe alle Ringelemente bis auf die 0 enthält, sind aber auch gerade die Körperaxiome erfüllt.

Beispiele: Im Ring der ganzen Zahlen Z besteht die Einheitengruppe aus {-1, 1}.
Im Falle des Matrizenrings Mat(n x n, K) umfasst die Einheitengruppe alle invertierbaren Matrizen (det A $\neq$ 0). Sie heißt generelle lineare Gruppe und wird mit GL(n, K) bezeichnet.

Teilring

Eine Teilmenge T eines Ringes R heißt Teilring, wenn T bezüglich der Ringoperationen einen Ring bildet. Analog wird ein Teilkörper definiert.
Beispiele: Z $\subseteq$ Q $\subseteq$ R $\subseteq$ C ist eine Folge von Teilringen.
nZ = {na | n, a $\in$ Z} sind alle Vielfachen von n. nZ ist ein Unterring von Z. Es ist 4Z ein Unterring von 2Z.
Jeder Ring R ist Teilring des Polynomrings R[X].

Primitivwurzel

Die additive Gruppe des Restklassenringes $(Z_n,\oplus,\otimes)$ mit den Verknüpfungen $\oplus$ und $\otimes$ ist nach Definition zyklisch, ein erzeugendes Element ist zum Beispiel die 1. Ist die multiplikative Gruppe $(Z_n,\otimes)$ auch zyklisch, so existiert ein Element ξ, dessen Potenzen ξ^k sämtliche Elemente von Z_n durchlaufen. Ein solches Element ξ heißt Primitivwurzel.
Es gilt: Ist n eine Primzahl p oder Potenz einer ungeraden Primzahl, so gibt es in $(Z_n,\otimes)$ mit Sicherheit Primitivwurzeln.
Dies folgt aus einem Satz von Gauß, dass eine multiplikative Restklassengruppe Z_p, bei der p Primzahl ist, zyklisch ist. Nach einem unbewiesenen Satz von Artin gibt es unendlich viele Primzahlen deren kleinste Primitivwurzel die 2 ist.
Die Tabelle enthält das Anwachsen der Rekordwerte für die kleinsten Primitivwurzeln kPW der Primzahlen p (gesucht bis 160 Millionen):

p	kPW	p	kPW	p	kPW	p	kPW
3	2	7	3	23	5	41	6
71	7	191	19	409	21	2161	23
5881	31	36721	37	55441	38	71761	44
110881	69	760321	73	5109721	94	17551561	97
29418841	101	33358081	107	45024841	111	90441961	113

Nilpotenz

Ein Element x eines Rings R wird als nilpotent bezeichnet, wenn eine positive natürliche Zahl n existiert, so dass $x^n = 0$
gilt. Ein Ideal I von R wird als nilpotent bezeichnet, wenn eine positive natürliche Zahl n existiert, so dass $I^n = 0$ ist.
Die Definition lässt sich insbesondere auf quadratische Matrizen anwenden. Beispielsweise ist die Matrix

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

nilpotent, da A^2 die Nullmatrix ergibt.
Im Restklassenring Z/8Z sind die Restklassen von 0, 2, 4 und 6 nilpotent, da jeweils ihre dritte Potenz kongruent zu 0 modulo 8 ist. In diesem Ring ist jedes Element entweder nilpotent oder Einheit.
Im Restklassenring Z/12Z sind die nilpotenten Elemente genau die Restklassen von 0 und 6.
Das Nullelement eines Ringes ist stets nilpotent, da $0^1 = 0$ ist.

Die Menge aller nilpotenten Elemente eines kommutativen Ringes bildet ein Ideal, das so genannte Nilradikal.
Der Durchschnitt aller Primideale in einem kommutativen Ring mit 1 ist genau das Nilradikal.
Sei im folgenden R ein Ring, a ein nilpotentes Element von R und n die kleinste natürliche Zahl mit $a^n = 0$. Ist $a \neq 0$, dann ist $n > 1$ und a ist Nullteiler, denn $aa^{n-1} = 0$ und $a^{n-1} = 0$.
Ist zusätzlich R ein Ring mit 1, dann gilt: a ist bezüglich der Multiplikation nicht invertierbar, denn aus $ab = 1$ für ein Ringelement b folgt der Widerspruch $0 = a^n b = a_{n-1}$.
1-a ist invertierbar, denn es gilt $(1 - a)(1 + a + a^2 + \ldots + a^{n-1}) = 1 - a^n = 1 = (1 + a + a^2 + \ldots + a^{n-1})(1 - a)$ ... Ist b eine Einheit von R, dann ist auch b + a invertierbar.

Sei R ein Restklassenring Z/mZ und p das Produkt aller Primteiler von m, d.h. aller Primzahlen die in der Primfaktorzerlegung von m auftreten. Dann sind die nilpotenten Elemente von R genau die Restklassen von ganzen Zahlen, die Vielfache von p sind.

Multiplikationstafel des Restklassenrings Z_6

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

Damit sind 2, 3 und 4 Nullteiler. Im Restklassenring Z_7 gibt es keine Nullteiler, da dieser Ring sogar Körper ist.

Algebraischer Körper

Eine algebraische Struktur (K, +, •) heißt Körper, wenn gilt:
1. (K,+) ist Abelsche Gruppe mit dem neutralen Element 0.
2. (K\{0},•) ist kommutative Gruppe mit dem neutralen Element 1.
3. Für alle a,b,c aus K gilt das Distributivgesetz $a \bullet (b + c) = (a \bullet b) + (a \bullet c)$

Beispiel: Körper der reellen bzw. komplexen Zahlen
Der Begriff "Körper" wurde zuerst von Richard Dedekind (1831-1916) benutzt. Ältere Bezeichnungen waren rationales Gebiet (ebenfalls Dedekind) und Rationalitätsbereich (Kronecker).
Schiefkörper: Eine algebraische Struktur, die alle Körperkriterien, bis auf die kommutative Multiplikation, erfüllt, heißt Schiefkörper.
Nullteilerfreiheit: Aus $a \bullet b = 0$ folgt stets $a = 0$ oder $b = 0$, d.h. die Struktur ist nullteilerfrei.
Zu beliebigen a und b aus K existiert genau ein x aus K mit $a \bullet x = b$, d.h. die Division kann für $a \neq 0$ eindeutig durchgeführt werden.

Vollständigkeit eines Körpers

Eine Körper ist vollständig, wenn jede Fundamentalfolge einen Grenzwert in diesem Körper besitzt.
Beispiel: Körper der reellen Zahlen

Unterkörper und Oberkörper

Ein Unterkörper oder Teilkörper eines Körpers L ist eine Teilmenge $K \subseteq L$, die 0 und 1 enthält und mit den auf K eingeschränkten Verknüpfungen selbst ein Körper ist. L wird dann Oberkörper von K genannt.
Eine Teilmenge $K \subseteq L$ ist genau dann ein Teilkörper von L, wenn sie 0 und 1 enthält und bezüglich der vier Verknüpfungen Addition, Multiplikation, Negation und Kehrwertbildung abgeschlossen ist, d.h. die Verknüpfung von Elementen von K liefert wieder ein Element von K.
Zum Beispiel ist der Körper C der komplexen Zahlen ein Oberkörper des Körpers R der reellen Zahlen.

Primkörper

Unter einem Primkörper versteht man einen Körper, der keine echten Teilkörper enthält.

Eigenschaften von Primkörpern

Jeder Primkörper ist bis auf Isomorphie entweder Q, der Körper der rationalen Zahlen, oder ein F_p-Körper mit p prim, d.h. ein Restklassenkörper modulo p.
Jeder Körper enthält einen Primkörper. Ist die Charakteristik des Körpers 0, so ist dessen Primkörper isomorph zu Q, ist sie hingegen eine Primzahl p, so ist der Primkörper isomorph zu F_p. Damit kann jeder Körper als Erweiterungskörper seines Primkörpers angesehen werden.

Galoisfelder

Genau die endlichen Schiefkörper heißen Galoisfelder. Jedes Galoisfeld ist ein Körper.
Zu jeder Primzahl p und zu n = 1, 2, … gibt es einen Körper mit p^n Elementen. Auf diese Weise erhält man alle Galoisfelder.
Zwei Galoisfelder sind genau dann isomorph, wenn sie die gleiche Anzahl von Elementen besitzen.

Geordneter Körper

Ein Körper heißt geordnet, wenn in K eine Relation "<" mit den Eigenschaften definiert ist:
(a, b, c aus K)
1. Trichotomiegesetz Es gilt entweder $a < b$, $a = b$ oder $a > b$
2. Transitivgesetz Aus $a < b$ und $b < c$ folgt $a < c$
3. Monotoniegesetz Aus $a < b$ folgt $a+c < b+c$ Aus $a < b$ und $0 < c$ folgt $a \cdot c < b \cdot c$

Die Richtung einer Ungleichung ändert sich nicht, wenn sie auf beiden Seiten gleich viel verkleinert oder vergrößert wird, oder wenn beide Seiten mit der gleichen positiven Zahl multipliziert oder dividiert werden. Multipliziert oder dividiert man hingegen mit einer negativen Zahl, dreht sich das Ungleichheitszeichen um.

Archimedisches Axiom
Zu jedem rationalen a und positivem rationalen b gibt es eine natürliche Zahl n, so dass $n \cdot b > a$ gilt

Archimedische geordnete Körper
Körper, die das archimedische Axiom erfüllen, heißen archimedisch geordneter Körper.
Diese Eigenschaft wird auch auf Nichtkörper erweitert. Die Menge der natürlichen Zahlen erfüllt ebenfalls das Archimedische Axiom und ist somit auch archimedisch geordnet.

Charakteristik eines Ringes
Die Charakteristik ist eine Kennzahl eines Ringes oder Körpers. Sie gibt an, wie oft man die im Ring bzw. Körper enthaltene Zahl 1 aufaddieren muss, um als Ergebnis 0 zu erhalten.
Die Charakteristik eines unitären Ringes R ist die kleinste natürliche Zahl $n \geq 1$, für die in der Arithmetik des Ringes die n-fache Summe des Einselementes 1 gleich dem Nullelement wird, also $\Sigma_{i=1}^{n} 1 = 0$
Ist jede endliche Summe von Einsen ungleich Null, wie zum Beispiel bei den reellen Zahlen, dann wird dem Ring definitionsgemäß die Charakteristik 0 zugeordnet.
Eine übliche Abkürzung der Charakteristik von R ist char(R).

Sie Charakteristik des unitären Rings R ist der eindeutig bestimmte nichtnegative Erzeuger des Kerns des kanonischen unitären Ringhomomorphismus $Z \to R$.
Die Charakteristik des unitären Rings R ist die eindeutig bestimmte nichtnegative ganze Zahl n, für die R einen unitären Teilring enthält, der isomorph zum Restklassenring Z/nZ ist.

Eigenschaften bei Ringen
Jeder unitäre Teilring S eines unitären Rings R hat dieselbe Charakteristik wie R.
Gibt es einen Ringhomomorphismus $R \to S$ zwischen zwei unitären Ringen R und S, so ist die Charakteristik von S ein Teiler der Charakteristik von R.
Für jeden Integritätsring, und insbesondere jeden Körper, ist die Charakteristik entweder 0 oder eine Primzahl. Im letzteren Fall spricht man auch von positiver Charakteristik.
Ist R ein unitärer Ring mit Primzahlcharakteristik p, dann gilt $(x + y)^p = x^p + y^p$
für alle $x, y \in R$. Die Abbildung $f: R \to R, x \to x^p$ ist dann ein Ringhomomorphismus und wird Frobenius-Homomorphismus genannt.

Beispiele: Der Restklassenring Z/nZ hat die Charakteristik n. Da die komplexen Zahlen die rationalen enthalten, ist auch ihre Charakteristik 0.
Für ein irreduzibles Polynom g vom Grad n über dem Restklassenkörper F_p ist der Faktorring $F_p[X]/(g)$ ein Körper, der isomorph ist zum endlichen Körper $F_p n$, der F_p enthält und die Charakteristik p hat.

Charakteristik eines Körpers
In jedem Körper K existieren natürliche Zahlen vermöge der Abbildung
$$i: N \to K: n \to i(n) = n \times 1 = \Sigma_{k=1}^{n} 1 = 1 + \ldots + 1 \text{ (k-mal)}$$
Allerdings besteht die Möglichkeit, dass ein $m \in N$ existiert mit $i(m) = 1 + \ldots + 1 = 0$, zum Beispiel ist im Z_2: $1 + 1 = i(2) = 0$.
Die Charakteristik eines Körpers ist
$$\chi(K) = \min \{m \in N \mid i(m) = \Sigma_{k=1}^{n} 1 = 0 \} \geq 2 \text{ , falls } \exists\, m \in N: i(m) = 0$$
andernfalls $\chi(k) = 0$
Beispiele: $\chi(Q) = \chi(R) = \chi(C) = 0$; $\chi(Z_2) = 2$

Eigenschaften der Charakteristik
$i(m + n) = i(m) + i(n)$ und für $m > n$: $i(m - n) = i(m) - i(n)$
$\chi(K) = 0 \Leftrightarrow i: N \to K$ ist injektiv
falls $\chi(K) \neq 0$, so ist die Charakteristik eine Primzahl

Charakteristik bei Körpern
Jeder geordnete Körper hat die Charakteristik 0; Beispiele sind die rationalen Zahlen oder die reellen Zahlen. Jeder Körper der Charakteristik 0 ist unendlich; er enthält einen Primkörper, der isomorph zum Körper der rationalen Zahlen ist.

Beispiele: Es gibt unendliche Körper mit Primzahlcharakteristik; Beispiele sind der Körper der rationalen Funktionen über F_p oder der algebraische Abschluss von F_p.
Die Mächtigkeit eines endlichen Körpers der Charakteristik p ist eine Potenz von p. Denn in diesem Fall enthält er den Teilkörper F_p und ist ein endlichdimensionaler Vektorraum über diesem Teilkörper. In der linearen Algebra wird gezeigt, dass die Ordnung des Vektorraums dann eine Potenz von p ist.
D.h., dass jeder endliche Vektorraum als Mächtigkeit eine Primzahlpotenz hat, da dieser dann ein endlichdimensionaler Vektorraum über einem endlichen Körper sein muss.

Euklidischer Ring

Ein Euklidischer Ring ist ein Ring, in dem eine verallgemeinerte Division mit Rest möglich ist, wie man sie von den ganzen Zahlen kennt.
Ein Integritätsring R, d.h. ein kommutativer, nullteilerfreier Ring mit 1; heißt euklidischer Ring, falls eine Bewertungsfunktion $g: R\backslash\{0\} \to N$
existiert, so dass es für Elemente $x, y \in R$ mit $y \neq 0$, Elemente $q, r \in R$ gibt, mit $x = qy + r$, wobei entweder $r = 0$ oder $g(r) < g(y)$ ist.
Die Abbildung g heißt dabei Euklidische Normfunktion oder Euklidischer Betrag.

D.h., ein euklidischer Ring ermöglicht eine Division mit Rest und dadurch einen euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers (ggT) zweier Ringelemente. Von dieser Eigenschaft ist der Name abgeleitet.
Ein Integritätsbereich R heißt euklidischer Ring, falls eine Bewertungsfunktion $g: R \to N$ existiert, so dass $g(0) = 0$ gilt und für alle $y \in R\backslash\{0\}$, $x \in R$ Elemente $q, r \in R$ existieren, so dass $x = qy + r$ gilt und $g(r) < g(y)$ ist.
Jeder euklidische Ring besitzt eine minimale euklidische Norm. Außerdem existiert ein Algorithmus zur iterativen Bestimmung des minimalen euklidischen Betrages in einem euklidischen Ring.
Jeder euklidische Ring ist ein Hauptidealring, denn wenn a ein minimal bewertetes Element eines Ideals I ist, so ist I = (a), also ein Hauptideal. Insbesondere ist jeder euklidische Ring faktoriell.

Beispiele: Der Ring Z der ganzen Zahlen ist ein euklidischer Ring. Die übliche Wahl für einen euklidischen Betrag ist $x \to |x|$. Der minimale euklidische Betrag einer ganzen Zahl ist gegeben durch die Länge der Binärdarstellung ihres Absolutbetrages.
Jeder Körper K ist ein euklidischer Ring mit dem euklidischen Betrag $a \to \delta_{0,a}$, wobei $\delta_{0,a}$ das Kronecker-Delta bezeichnet. Der Polynomring K[X] über einem Körper K in einer Variablen X ist ebenfalls euklidischer Ring.
Der Ring Z[i] der gaußschen Zahlen erklärt durch $(a+bi) \to a^2+b^2$ ist ein euklidischer Ring. Dagegen ist der Polynomring Z[X] kein euklidischer Ring. Auch der Ring $Z[\sqrt{-3}]$ ist nicht euklidisch, da $2+2\sqrt{-3}$ und 4 keinen ggT haben.

Monoidring

Seien R Ring und M Monoid. Ein Monoidring ist die folgende Menge von Abbildungen
$$R[M] = \{(a_m)_{m\in M} \in Abb(M, R) \mid a_m = 0 \text{ für fast alle } m\}$$
mit der Zuordnungsvorschrift $m \in M \to a_m \in R$.
Die a_m heißen Koeffizienten und nach Definition sind nur endlich viele verschieden von 0. R[M] ist Ring mit komponentenweiser Addition: $(a_m)_{m\in M} + (b_m)_{m\in M} = (a_m + b_m)_{m\in M}$
und der Faltung als Multiplikation: $(a_{m'})_{m'\in M} \cdot (b_{m''})_{m''\in M} = \Sigma_{\{(m', m'')\mid m = m'+m''\}} a_{m'} \cdot b_{m''}$
Dabei ist $0 = (0)_{m\in M}$ und $1 = (a_m)_{m\in M}$ mit $a_m = 1$ für $m = 0$, sonst $a_m = 0$.

Monoidringe sind eine Verallgemeinerung von Polynomringen.
R und M sind auf natürliche Weise in R[M] eingebettet.
$\phi: R \to R[M]$ mit $\lambda \in R$, $\phi(\lambda) = \lambda x^0$ ist ein injektiver Ringhomomorphismus.
Durch ϕ wird R[M] zu einer R-Algebra. Insbesondere ist im Falle eines Körpers R = K der Monoidring K[M] ein K-Vektorraum.

Ringideale

Es sei R ein Ring. Eine nichtleere Teilmenge $I \subseteq R$ heißt beidseitiges Ideal oder einfach nur Ideal, falls gilt
$$a, b \in I \Rightarrow a + b \in I \qquad r \in R, a \in I \Rightarrow r\,a \in I \text{ und } a\,r \in I$$

Ein Ideal ist eine Teilmenge I, die abgeschlossen bezüglich R-Linearkombinationen ist.

Beispiele: Für jeden Ring R sind R und {0} Ideale. Für jedes Ideal $I \subseteq R$ gilt $0 \in I$.
Die Menge der geraden ganzen Zahlen in Z ist ein Ideal, denn die Summe zweier gerader ganzer Zahlen ist gerade und die Multiplikation einer geraden mit einer beliebigen ganzen Zahl ist wieder gerade.
Wenn $\phi: R \to S$ ein Ringhomomorphismus ist, dann ist der Kern $\ker \phi$ ein Ideal.

Hauptideal, Hauptidealring

Es sei R ein Ring, $a \in R$ ein Element. Dann ist

$$(a) = \{r\, a \mid r \in R\}$$

ein Ideal, das von a erzeugte Ideal. Schreibweise: $(a) = aR = Ra$.
Solche Ideale heißen Hauptideale. Ringe, die nur Hauptideale besitzen, heißen Hauptidealringe.
Dies sind nach Körpern die einfachsten Ringe. Jeder Körper ist Hauptidealring.
Der Ring der ganzen Zahlen Z ist ebenfalls Hauptidealring.

Maximales Ideal

Es sei R ein kommutativer Ring und M ein Ideal. Man nennet M maximal oder ein maximales Ideal, wenn für alle Ideale $I \subseteq R$ gilt: aus $M \subset I$ folgt $I = R$
D.h., ein Ideal M ist maximal, wenn es nicht echte Teilmenge eines echten Ideals von R ist.

Primideal

Ein Primideal ist eine Teilmenge eines Ringes, die viele Eigenschaften einer Primzahl hat.

Primideal eines kommutativen Ringes

Sei R ein kommutativer Ring mit 1 und P ein Ideal in R. Man nennt P Primideal oder prim, wenn für alle $x, y \in R$ gilt: aus $xy \in P$ folgt $x \in p$ oder $y \in p$.
Ein Ideal P ist genau dann prim, wenn der Faktorring R/P Integritätsring ist.

für alle Ideale $a, b \subseteq R$ gilt: $a, b \subseteq P \Rightarrow a \subseteq P$ und $b \subseteq P$ und $P \neq R$

Beispiele: Die Menge 2Z der geraden ganzen Zahlen ist ein Primideal im Ring Z der ganzen Zahlen, da ein Produkt zweier ganzer Zahlen nur dann gerade ist, wenn wenigstens ein Faktor gerade ist.
Die Menge 6Z der durch 6 teilbaren ganzen Zahlen ist kein Primideal in Z, da $2 \cdot 3 = 6$ in der Teilmenge liegt, aber weder 2 noch 3. Jedes maximale Ideal ist prim.
Ein Element $p \in R$ ist genau dann ein Primelement, wenn das von p erzeugte Hauptideal (p) ein Primideal ist. Enthält ein Primideal einen Durchschnitt $\cap_{ai}$ von Idealen, so enthält es auch ein a_i.

Primideal eines nichtkommutativen Ringes

Sei R ein Ring mit 1 und $P \subseteq R$ ein beidseitiges Ideal in R. Man nennt P Primideal oder prim, wenn für alle $x, y \in R$ gilt: wenn für alle $r \in R$ gilt, dass $xry \in P$ liegt, dann ist $x \in P$ oder $y \in P$.
Für einen kommutativen Ring stimmt diese Definition mit der obigen überein, für einen nichtkommutativen unterscheiden sie sich im allgemeinen.

Algebra über einem kommutativen Ring, R-Algebra

Als Algebra über einem kommutativen Ring oder R-Algebra; wobei R ein kommutativer Ring ist; bezeichnet man eine algebraische Struktur, die aus einem Modul über einem kommutativen Ring und einer zusätzlichen, mit der Modulstruktur verträglichen Multiplikation besteht.

Es seien R ein kommutativer Ring und A ein R-Modul. Die Multiplikation ist eine bilineare, zweistellige Verknüpfung

$$A \times A \to A$$

d.h., für beliebige Elemente $x, y, z \in A$ und Skalare $\lambda \in R$ gilt

$$(x + y) \cdot z = x \cdot z + y \cdot z \qquad x \cdot (y + z) = x \cdot y + x \cdot z$$
$$\lambda\,(x \cdot y) = (\lambda\, x) \cdot y = x \cdot (\lambda\, y)$$

Dabei ist weder die Assoziativität noch Kommutativität noch die Existenz eines Einselements der Algebra-Multiplikation vorausgesetzt.

Beispiel: Jeder Ring ist eine Z-Algebra, also eine Algebra über dem kommutativen Ring Z der ganzen Zahlen.

Körpererweiterung

Sei L ein Körper, und sei K ein Unterkörper von L, dann heißt L Erweiterungskörper von K. Die verbreitetste Schreibweise für Körpererweiterungen ist L/K, mintunter auch L | K, selten L : K. Ein Körper M heißt Zwischenkörper der Körpererweiterung L/K, wenn M ein Unterkörper von L und ein Oberkörper von K ist, also $K \subseteq M \subseteq L$ gilt.

Körperadjunktion

Ist V eine Teilmenge von L, dann ist der Körper K(V) ("K adjungiert V") definiert als der kleinste Teilkörper von L, der K und V enthält. Er besteht aus allen Elementen von L, die mit endlich vielen Verknüpfungen +,-,·,/ aus den Elementen von K und V gebildet werden können. Ist L = K(V), dann sagt man, L wird von V erzeugt.

Beispiele für algebraische Strukturen

Die Zahlenbereiche Z, Q, R und C sind bezüglich der Addition und Multiplikation kommutative Ringe mit Einselement; Q, R und C sind sogar Körper. Die Menge der geraden ganzen Zahlen ist ein Beispiel für einen Ring ohne Einselement. Die Menge C ist der Erweiterungskörper von R.

Die Menge M_n aller n-reihigen Matrizen über den reellen Zahlen bildet einen nichtkommutativen Ring mit der Einheitsmatrix als Einselement.
Die Menge der reellen Polynome $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ bildet bezüglich der üblichen Addition und Multiplikation von Polynomen einen Ring, den Polynomring R[x]. Allgemeiner kann man anstelle des Polynomringes über R auch Polynomringe über beliebigen kommutativen Ringen mit Einselement betrachten.

Erweiterungsgrad, Grad einer Körpererweiterung

Sei L/K eine Körpererweiterung.
Man kann L als Vektorraum über K auffassen, wobei die Vektoraddition die Körper-Addition in L ist und die Skalarmultiplikation die Körper-Multiplikation von Elementen aus L mit Elementen aus K. Die Dimension dieses Vektorraums nennt man den Grad der Erweiterung, und schreibt [L : K].
Die Erweiterung heißt endlich oder unendlich, je nachdem ob der Grad endlich oder unendlich ist.

Zum Beispiel ist [C:R] = 2, d.h. die Erweiterung der reellen Zahlen zu den komplexen Zahlen ist endlich. Im Gegensatz dazu ist $[R:Q] = \infty$.
Sind M/L und L/K Körpererweiterungen, dann ist auch M/K eine Körpererweiterung, und es gilt der Gradsatz:

$$[M:K] = [M:L] \cdot [L:K].$$

Dies gilt für unendliche Erweiterungen. L/K heißt dabei eine Teilerweiterung von M/K.

Minimalpolynom

Sei L/K eine Körpererweiterung und x ein Element von L. Ein Minimalpolynom $m = \mathrm{minpol}_K(x)$ von x über K ist definiert als normiertes Polynom kleinsten Grades mit Koeffizienten in K, das x als Nullstelle hat.

Falls ein Minimalpolynom von x existiert, ist es eindeutig bestimmt, und das Element x heißt algebraisches Element der Erweiterung L/K oder algebraisch über K. Daher spricht man von dem Minimalpolynom.
Falls kein Minimalpolynom von x existiert, dann heißt x transzendent über K.
Minimalpolynome sind irreduzibel über dem Grundkörper. Jedes Polynom mit Koeffizienten im Grundkörper, das ein algebraisches Element x als Nullstelle hat, ist ein Polynomvielfaches des Minimalpolynoms von x. Der Grad des Minimalpolynoms von x ist gleich dem Grad der einfachen Erweiterung K(x)/K.

Beispiel: Gegeben sei die Körpererweiterung Q(i)/Q mit der imaginären Einheit i. Das Minimalpolynom von i ist x^2+1, denn es hat i als Nullstelle, ist normiert und jedes Polynom kleineren Grades wäre linear und hätte nur eine Nullstelle in Q.
Das Polynom $x^3 + x$ ist kein Minimalpolynom irgendeines Elementes irgendeiner Erweiterung, da es sich als $(x^2 + 1)\, x$ darstellen lässt, und für keine seiner Nullstellen ein Polynom kleinsten Grades ist.

Körper der reellen Zahlen

Das Axiomensystem der reellen Zahlen besteht aus drei Arten von Axiomen:

- Körperaxiome
- Anordnungsaxiome
- Vollständigkeitsaxiom

Die reellen Zahlen R werden dann als diejenige Menge charakterisiert, die obige Axiome erfüllen.

Körperaxiome

Die Körperaxiome fordern, dass es sich bei den reellen Zahlen um einen kommutativen Körper handeln soll.
Es existieren also binäre Operationen, die Addition + und die Multiplikation ·. Es gelten folgende Gesetze

Assoziativgesetze für alle $a, b, c \in R$ gilt
$a + (b + c) = (a + b) + c \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Existenz neutraler Elemente: es existieren zwei ausgezeichnete reelle Zahlen 0 und 1, so dass für alle $a \in R$ gilt
$a + 0 = a$ und $a \cdot 1 = a$
Existenz inverser Elemente: zu jedem $a \in R$ existiert ein $-a \in R$ mit $a + (-a) = 0$
Wenn a verschieden von 0 ist gibt es ein a^{-1}; für a^{-1} schreibt man auch 1/a; mit $a \cdot (a^{-1}) = 1$
Kommutativgesetze für alle $a, b \in R$ gilt: $a + b = b + a$ und $a \cdot b = b \cdot a$
Distributivgesetz $a \cdot (b + c) = a \cdot b + a \cdot c$

Mit den Axiomen gelten für die reellen Zahlen alle Eigenschaften, die für alle Körper gelten. Insbesondere sind die neutralen und inversen Elemente eindeutig bestimmt. Auf Grund dieses Axiomensystems kann man in den reellen Zahlen wie in jedem Körper rechnen und alle bekannten Rechenregeln herleiten. U.a. folgt sofort
Es seien $a, b, x, y \in R$, dann gilt: $x \cdot 0 = 0 \qquad (-x) \cdot y = -(x \cdot y) \qquad -(-a) = a$
Die Gleichung $a + x = b$ hat bei gegebenen a, b genau eine Lösung $x = b - a$.
Die Gleichung $a \cdot x = b$ hat für jedes a verschieden 0 genau eine Lösung $x = b \cdot a^{-1} = b/a$.
Es ist $x \cdot y = 0$ genau dann, wenn $x = 0$ oder $y = 0$ gilt.

Die Körperaxiome liefern Aussagen über das algebraische Verhalten der reellen Zahlen. Aus der Anschauung ist bekannt, dass die reellen Zahlen einer gewissen Anordnung unterliegen, so dass Begriffe wie kleiner und größer einen Sinn ergeben. Diese Anordnung wird durch die folgende Gruppe von Axiomen beschrieben.

Anordnungsaxiome

Es gibt eine Relation $\leq$ (kleiner gleich) in R mit folgenden Eigenschaften $\leq$ ist eine lineare Ordnung, d.h.

- $\forall\, x: x \leq x$ (Reflexivität)
- $\forall\, x,y: x \leq y$ und $y \leq x \Rightarrow x = y$ (Antisymmetrie)
- $\forall\, x,y,z: x \leq y$ und $y \leq z \Rightarrow x \leq z$ (Transitivität)

Für alle x,y gilt: $x \leq y$ oder $y \leq x$. Zwei Zahlen sind immer vergleichbar.
In Beziehung zur Addition und Multiplikation fordert man die Gültigkeit der Monotoniegesetze:
$\leq$ ist bzgl. der Addition monoton, d.h. $\forall\, a,b,c: a \leq b \Rightarrow a+c \leq b+c$
$\leq$ ist bzgl. der Multiplikation monoton; d.h. $\forall\, a,b,c: a \leq b$ und $0 \leq c \Rightarrow a \cdot c \leq b \cdot c$

Aus dieser Gruppe von Axiomen folgt:
1) $a \leq b \Rightarrow -b \leq -a$
2) $a \leq b$ und $c \leq d \Rightarrow a+c \leq b \leq d$
3) $a \neq 0 \Rightarrow a \cdot a > 0$

4) $a > 0 \Rightarrow 1/a > 0$
5) $0 < a < b \Rightarrow 1/b < 1/a$
6) $a < b$ und $b > 0$ und $0 < c < d \Rightarrow ac < bd$

Vollständigkeitsaxiom der reellen Zahlen

Die Körperaxiome und Anordnungsaxiome genügen nicht, um die reellen Zahlen zu charakterisieren. Auch die rationalen Zahlen sind ein Modell für dieses Axiomensystem.
Was die reellen Zahlen von den rationalen Zahlen unterscheidet ist, dass sie vollständig sind, es keine Lücken auf der Zahlengeraden mehr gibt. Mit den Begriffen Infimum und Supremum kann die Vollständigkeit erklärt werden.

Vollständigkeitsaxiom: Jede nichtleere nach unten beschränkte Menge reeller Zahlen besitzt ein Infimum.
oder äquivalent: Jede nichtleere nach oben beschränkte Menge besitzt ein Supremum.

Satz: Es seien $B \subset A \subset R$, $B \neq \emptyset$, dann gilt:
1) ist A beschränkt, so gilt $\inf A \leq \sup A$
2) ist A nach oben beschränkt, so ist auch B nach oben beschränkt und $\sup B \leq \sup A$
3) ist A nach unten beschränkt, so ist auch B nach unten beschränkt und $\inf A \leq \inf B$
4) ist A nach oben beschränkt und γ eine obere Schranke von A, so gilt
$\gamma = \sup A \Leftrightarrow \forall \varepsilon > 0\ \exists x \in A: x > \gamma - \varepsilon$
ist A nach unten beschränkt und γ eine untere Schranke von A, so gilt
$\gamma = \inf A \Leftrightarrow \forall \varepsilon > 0\ \exists x \in A: x < \gamma + \varepsilon$
Aus dem Vollständigkeitsaxiom ergibt sich die Existenz und Eindeutigkeit von Wurzeln nichtnegativer, reeller Zahlen.

Einzigkeit der reellen Zahlen

Die Axiome (Körperaxiome, Anordnungsaxiome und das Vollständigkeitsaxiom) verleihen dem Körper der reellen Zahlen eine Einzigartigkeit. Bis auf ordnungserhaltende Isomorphismen ist diese Körper eindeutig bestimmt.

Natürliche Zahlen als Teilmenge der reellen Zahlen

Neben dem in der Zahlentheorie üblichen Aufbau der natürlichen Zahlen mittels der Peanoschen Axiome, können die natürlichen Zahlen N auch als Teilmenge der reellen Zahlen charakterisiert werden.

Induktive Mengen

Eine Teilmenge $I \subseteq R$ heißt induktiv genau dann, wenn
$0 \in I \qquad \forall x: x \in I \Rightarrow (x+1) \in I$
Eine induktive Menge umfasst stets dass, was man anschaulich unter den natürlichen Zahlen versteht; sie kann jedoch auch größer sein. Es gibt z.B. eine induktive Menge I, so dass $\{1/2, 3/2, \ldots\} \subseteq I$ ist.
$J = \{I: I \subset R, I \text{ ist induktiv}\}$ entspricht der Menge aller induktiven Mengen aus R. Man definiert die natürlichen Zahlen N als Durchschnitt aller induktiven Teilmengen von R.
$N = \cap J = \{x \in R: \forall I \in J: x \in I\} \quad (1)$
Es gilt: Die Menge N in (1) ist die kleinste induktive Teilmenge von N.
Dies liefert die Rechtfertigung für das Prinzip der vollständigen Induktion. Gilt eine Aussage H für 0 und kann man aus der Gültigkeit von H auf die Gültigkeit für n+1 schließen, so gilt H für alle natürlichen Zahlen.

Körper der algebraischen Zahlen

Die Menge der algebraischen Zahlen ist abzählbar und bildet einen Körper.
Der Körper der algebraischen Zahlen ist algebraisch abgeschlossen, d.h. jedes Polynom mit algebraischen Koeffizienten besitzt nur algebraische Nullstellen.
Dieser Körper ist ein minimaler algebraisch abgeschlossener Oberkörper von Q und damit ein algebraischer Abschluss von Q.

Dieser Körper hat viele Automorphismen und jeder davon liefert eine Einbettung in die komplexen Zahlen C, d.h., es gibt keine kanonische Einbettung.

Zum Beispiel kann man die Nullstellen des Polynoms $x^2 + 1$ innerhalb des Körpers der algebraischen Zahlen nicht voneinander unterscheiden. Somit kann man wählen, welche der beiden als imaginäre Einheit i genutzt wird. Die andere Nullstelle dieses Polynoms ist dann eindeutig bestimmt und hat den Wert -i.

Oberhalb des Körpers der rationalen Zahlen und unterhalb des Körpers der algebraischen Zahlen befinden sich unendlich viele Zwischenkörper, zum Beispiel die Menge aller Zahlen der Form $a + b \cdot q$, wobei a und b rationale Zahlen sind und q die Quadratwurzel einer rationalen Zahl r ist.
Auch der Körper der mit Zirkel und Lineal aus {0, 1} konstruierbaren Punkte der komplexen Zahlenebene ist ein solcher algebraischer Zwischenkörper.

In der Galoistheorie werden diese Zwischenkörper untersucht, um Einblicke über die Lösbarkeit oder Nichtlösbarkeit von Gleichungen zu erhalten. Ein Resultat der Galoistheorie ist, dass zwar jede komplexe Zahl algebraisch durch "Radikale darstellbar" ist, die man aus rationalen Zahlen durch Verwendung der Grundrechenarten +,-,·,/ und Ziehen n-ter Wurzeln erhalten kann, umgekehrt aber algebraische Zahlen existieren, die man nicht in dieser Weise darstellen kann. Alle diese Zahlen sind Nullstellen von Polynomen des Grades > 4.

Algebraische Zahlen, die sogar Nullstellen eines normierten Polynoms mit ganzzahligen Koeffizienten sind, heißen algebraische Ganzzahlen oder ganzalgebraische Zahlen. Die ganzalgebraischen Zahlen, die rational sind, sind genau die ganzen Zahlen. Die ganzalgebraischen Zahlen bilden einen Unterring der algebraischen Zahlen.

Endliche Gruppen

Eine endliche Gruppe ist eine algebraische Gruppe endlicher Ordnung, d.h. mit endlich vielen Elementen. Typische Vertreter sind die Restklassengruppen, welche zu Restklassenkörpern oder -ringen erweitert werden können.
Anfang 2000 ist noch keine Gleichung bekannt, mit der die Anzahl nicht isomorpher endlicher Gruppen einer Ordnung n berechnet werden kann. Die Liste enthält eine Aufstellung der Anzahl endlicher Gruppen einer Ordnung n. Nach A steht die Anzahl Abelscher Gruppen, nach NA nichtabelscher Gruppen. Bis zur Ordnung 15 werden alle Gruppen genannt.
Z(n) ist die zyklische Gruppe, A(n) die alternierende Gruppe, D(n) die dihedrale Gruppe, T die kubische Gruppe, Q die Gruppe der Quaternionen. x symbolisiert das direkte Produkt zweier Gruppen.

Ordnung	A	NA	Vertreter
1	1	0	Gruppe des Einselements
2	1	0	Z 2
3	1	0	Z 3
4	2	0	Z2 ⊗ Z2, Z4
5	1	0	Z 5
6	1	1	Z 6 = Z2 ⊗ Z3, D 3
7	1	0	Z 7
8	3	2	Z2 ⊗ Z2 ⊗ Z2, Z2 ⊗ Z4, Z 8, Q 8, D 4
9	2	0	Z 9, Z3 ⊗ Z3
10	1	1	Z 10, D 5
11	1	1	Z 11
12	2	3	Z 12, A 4, D 6, T, Z2 ⊗ Z6
13	1	0	Z 13
14	1	1	Z 14, D 7
15	1	0	Z 15

Isomorphietypen

Ordnung 1

Es gibt nur eine Gruppe mit einem Element, die nur aus dem neutralen Element bestehende Gruppe $\langle e \rangle = (e, \cdot)$.
Eigenschaften: abelsche Gruppe, zyklische Gruppe C_1

Ordnung 2
Bis auf Isomorphie gibt es nur eine Gruppe mit 2 Elementen, bestehend aus e und a, wobei gilt $a^2 = e$.
Eigenschaften: abelsche Gruppe, zyklische Gruppe C_2, triviale Diedergruppe D_1

Ordnung 3
Bis auf Isomorphie gibt es nur eine Gruppe mit 3 Elementen.
Eigenschaften: abelsche Gruppe, zyklische Gruppe C_3

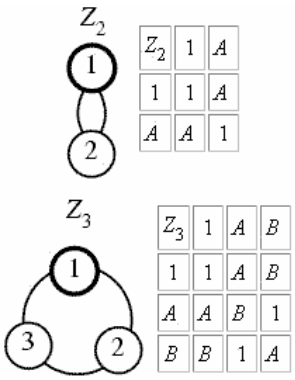
Ordnung 4
Bei den vierelementigen Gruppen gibt es zwei Isomorphietypen.
1.Zyklische Gruppe, Eigenschaften: abelsche Gruppe, zyklische Gruppe C_4
2. Kleinsche Vierergruppe
Gruppe, die von zwei Elementen mit den Beziehungen $a^2 = b^2 = (ab)^2 = e$ erzeugt wird.
Eigenschaften: abelsche Gruppe, Diedergruppe D_2, Symmetriegruppe des Rechtecks, direktes Produkt der zyklischen Gruppen $C_2 \times C_2$

Ordnung 5
Bis auf Isomorphie gibt es nur eine Gruppe mit 5 Elementen, diese ist isomorph zur zyklischen Gruppe mit 5 Elementen; zyklische Gruppe C_5

Zyklische Gruppen
Eine Gruppe G, die nur aus den Potenzen g, g^2, g^3, …, $g^n = e$ eines Elementes g besteht, heißt zyklische Gruppe Z_n der Ordnung n. Ein Element g, aus dessen Potenzen Z_n besteht, heißt erzeugendes Element von Z_n.
Zu jeder natürlichen Zahl n gibt es genau eine zyklische Gruppe der Ordnung n. Sie ist kommutativ und isomorph zur additiven Restklassengruppe modulo n.
Es sei G eine von g erzeugte zyklische Gruppe. Dann gelten die folgenden Aussagen:

a) Jede Untergruppe U von G ist zyklisch.

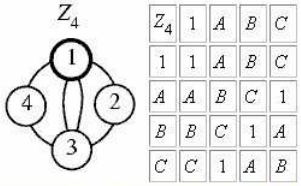
b) Hat $G = \{e, g, g^2, g3, \ldots g^{n-1}\}$ die Ordnung n, so gibt es zu jeder natürlichen Zahl d, die n teilt, genau eine zyklische Untergruppe U_d der Ordnung d von G, die von n/d erzeugt wird.



(in der Abbildung: links Struktur, rechts Multiplikationstafel)

zyklische Gruppe Z2
Z2 ist die einzige endliche Gruppe der Ordnung 2, abelsch und zyklisch.
Beispiele: Integeraddition modulo 2
Die Gruppe enthält das Einselement und ein Element A mit $A^2 = 1$

zyklische Gruppe Z3
Z3 ist die einzige Gruppe der Ordnung 3, abelsch und zyklisch.
Beispiel: Addition natürlicher Zahlen modulo 3



Zyklische Gruppe Z4
Z4 ist eine der zwei Gruppen der Ordnung 4 (vier Elemente).
Die Gruppe ist ähnlich zur Gruppe Z2 ⊗ Z2. Sie ist abelsch, allerdings auch zyklisch.
Beispiele: Modulo Multiplikationsgruppen M5 und M10

Die Gruppe kann durch die Zuordnung 1 = 1, A = i, B = -1 und C = -i, als Multiplikationsgruppe der komplexen Zahlen 1, -1, i und -i interpretiert werden.
Die untere Abbildung und das zugehörige Beispiel entstammen der sowjetischen mathematischen Schülerzeitschrift "Quant" 2/87:
Betrachtet man einen Wachposten, so kann und darf dieser eigentlich nur vier Bewegungen ausführen: 90° nach links, 90° nach rechts, 180° drehen (Kehrtwendung) und natürlich Stillstehen.

Führt der Wachtposten zwei Bewegungen nacheinander aus, so ergibt sich wieder eine der vier Bewegungen. Die zugehörige Gruppe ist gerade die zyklische Gruppe Z4, die Drehgruppe eines Quadrates.

Kleinsche Vierergruppe

Bei dieser 4 elementigen Gruppe handelt es sich um die Diedergruppe D_2, die in der Kristallografie auch als 222 notiert wird.
In der Mathematik wird sie Kleinsche Vierergruppe V_4 genannt. Diese Gruppe ist die Symmetriegruppe des Rechtecks. Sie ist isomorph zum direkten Produkt $Z_2 \times Z_2$. Die Kleinsche Vierergruppe ist die kleinste abelsche, nicht zyklische Gruppe.
Die Gruppe wurde nach Felix Klein benannt, der sie in seinen "Vorlesungen über das Ikosaeder" 1884 Vierergruppe nannte, und wird oft mit dem Buchstaben V bezeichnet.

*	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

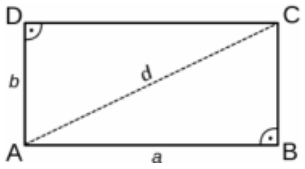
Die Vierergruppe tritt als Symmetriegruppe eines Rechtecks, dass kein Quadrat ist, auf.
Die vier Elemente sind dabei: die Identität, die Spiegelung an der waagerechten Mittelachse, die Spiegelung an der senkrechten Mittelachse und die 180°-Drehung um den Mittelpunkt des Rechtecks. Die drei Elemente ungleich der Identität haben die Ordnung 2.
Eine Permutationsdarstellung von V liefert die Nummerierung der Ecken eines Rechtecks:

V = e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3).

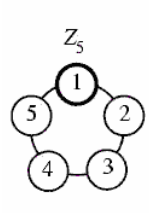
In dieser Darstellung ist V die Kommutatorgruppe und damit ein Normalteiler der alternierenden Gruppe A4 und auch Normalteiler der symmetrischen Gruppe S4.
In der Galoistheorie erklärt die Existenz der Kleinschen Vierergruppe die Existenz der Lösungsformel für Gleichungen vierten Grades.
Die Einheitengruppe des Ringes Z/8Z, das sind die Restklassen von 1, 3, 5 und 7 unter Multiplikation modulo 8, ist isomorph zu V.

Kleinsche Vierergruppe (2)

Die Kleinsche Vierergruppe tritt als die Symmetriegruppe eines nicht gleichseitigen Rechtecks, d.h. kein Quadrat, auf.
Die vier Elemente sind dabei: 1 als die Identität oder Drehung um 0°, a als die Spiegelung an der senkrechten Mittelachse, b als die Spiegelung an der waagerechten Mittelachse, und c = ab als die 180°-Drehung um den Mittelpunkt, die auch als Kombination der horizontalen und vertikalen Spiegelung aufgefasst werden kann.



(A,B,C,D) → (A,B,C,D), das Element 1 darstellend
(A,B,C,D) → (B,A,D,C), das Element a darstellend
(A,B,C,D) → (D,C,B,A), das Element b darstellend
(A,B,C,D) → (C,D,A,B), das Element ab darstellend
Die Vierergruppe ist Kommutatorgruppe und ein Normalteiler der alternierenden Gruppe A_4 und auch Normalteiler der symmetrischen Gruppe S_4. In der Galoistheorie erklärt die Existenz der Kleinschen Vierergruppe die Existenz der Lösungsformel für Gleichungen vierten Grades.

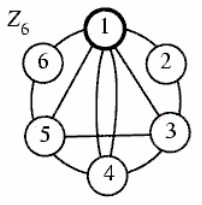


Z_5	1	A	B	C	D
1	1	A	B	C	D
A	A	B	C	D	1
B	B	C	D	1	A
C	C	D	1	A	B
D	D	1	A	B	C

Zyklische Gruppe Z5

Die Gruppe Z5 ist die einzige Gruppe der Ordnung 5, abelsch und zyklisch.
Da die Ordnung 5 Primzahl ist, existieren außer den trivialen Untergruppen keine anderen Untergruppen. Z5 ist eine einfache Gruppe.
In der Kristallographie tritt sie nicht auf, da in den dort betrachteten Symmetriegruppen keine Drehungen der Ordnung 5 vorkommen können

Beispiel: Addition natürlicher Zahlen modulo 5



Z_6	1	A	B	C	D	E
1	1	A	B	C	D	E
A	A	1	E	D	B	C
B	B	E	1	A	C	D
C	C	D	A	1	E	B
D	D	B	C	E	1	A
E	E	C	D	B	A	1

Zyklische Gruppe Z6

Z6 ist eine der zwei Gruppen der Ordnung 6.
Sie ist isomorph zur Gruppe Z2 ⊗ Z3, abelsch, zyklisch.

Beispiele: Modulo Multiplikationsgruppen M7, M9, M14; Addition natürlicher Zahlen modulo 6

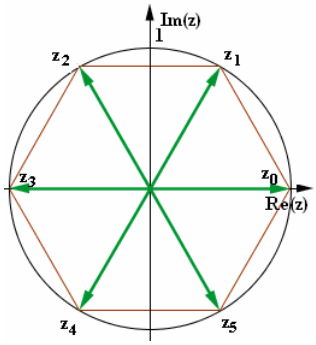
Restklassengruppe modulo 6 bezüglich der Addition als Verknüpfung

$Z_6 = \{e, g, g^2, g^3, g^4, g^5\} = \{0, 1, 2, 3, 4, 5\}$, erzeugendes Element 1 (I)
$= \{0, 5, 4, 3, 2, 1\}$, erzeugendes Element 5 (II)

Zyklische Untergruppen
$Z_3 = \{e, g, g^2\} = \{0, 2, 4\}$, erzeugendes Element 2 = {0, 4, 2}, erzeugendes Element 4
$Z_2 = \{e, g\} = \{0, 3\}$, erzeugendes Element 3

Restklassengruppe modulo 7 bezüglich der Multiplikation als Verknüpfung

$Z_6 = \{e, g, g^2, g^3, g^4, g^5\} = \{1, 3, 2, 6, 4, 5\}$, erzeugendes Element 3 (III)
$= \{1, 5, 4, 6, 2, 3\}$, erzeugendes Element 5 (IV)
Zyklische Untergruppen



$Z_3 = \{e, g, g^2\} = \{1, 2, 4\}$, erzeugendes Element 2 = {1, 4, 2} , erzeugendes Element 4
$Z_2 = \{e, g\} = \{1, 6\}$, erzeugendes Element 6

Zyklische Gruppe von Einheitswurzeln

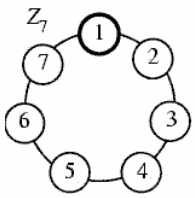
Die zyklische Gruppe der 6-ten Einheitswurzeln bezüglich der Multiplikation als Verknüpfung ist isomorph zur zyklischen Gruppe Z6.
Kreisteilungsgleichung $z^6 = 1$, z ist komplexe Zahl
Lösungen

$$z_k = \cos(k/6\ 2\pi) + i \sin(k/6\ 2\pi),\ k \in \{0, 1, 2, 3, 4, 5\}$$

Zyklische Gruppe der Ordnung 6
$Z6 = \{e, g, g^2, g^3, g^4, g^5\} = \{1, z_1, z_2, z_3, z_4, z_5\}$ Linksdrehung
$= \{1, z_5, z_4, z_3, z_2, z_1\}$ Rechtsdrehung

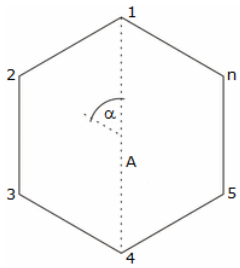
Zyklische Untergruppen $Z3 = \{e, g, g^2\} = \{1, z_2, z_4\}$ Linksdrehung $= \{1, z_4, z_2\}$ Rechtsdrehung
$Z2 = \{e, g\} = \{1, z_3\}$

Zyklische Gruppe Z7



Z7 ist die einzige Gruppe der Ordnung 7, abelsch und zyklisch.
In der Kristallographie tritt sie nicht auf, da in den dort betrachteten Symmetriegruppen keine Drehungen der Ordnung 7 vorkommen können
Beispiel: Addition natürlicher Zahlen modulo 7

Diedergruppe



Die n.te Diedergruppe (di-eder gesprochen) wird bezeichnet mit D_n oder D_{2n}.
Sie ist für n > 2 geometrisch erklärt als Symmetriegruppe der Drehungen und Spiegelungen eines regelmäßigen n-Ecks ("Dieder" = "Zweiflach").
Die Gruppe D_1 besteht neben der Identität nur aus einer einzigen Spiegelung und hat somit zwei Elemente. Die Gruppe D_2 beschreibt die Symmetriegruppe eines nichtquadratischen Rechtecks oder einer Strecke.
D_3 ist die Symmetriegruppe des gleichseitigen Dreiecks, D_4 die Symmetriegruppe des Quadrates.

Nach Durchnummerierung der Ecken kann man die Diedergruppe für n > 2 als Untergruppe der n.ten symmetrischen Gruppe S_n, also als Permutationsgruppe auffassen.
Die Diedergruppe wird erzeugt von zwei Abbildungen, der Drehung um den Winkel $\alpha = 2\pi / n$ und der Spiegelung A an der Symmetrieachse durch den Punkt 1. Die einzelnen Erzeuger erzeugen je eine Untergruppe der Diedergruppe, die isomorph zu den zyklischen Gruppen Z_n beziehungsweise Z_2 sind.
Die Ordnung der n.ten Diedergruppe ist 2n.
Die durch die Permutation definierte Zahlenverknüpfung wird bei Prüfsummenverfahren als Alternative zu diversen modulo-basierten Verfahren angewendet. Die deutschen Banknoten besaßen früher Dieder-Prüfsummen.

Geldschein-Prüfcode

Durch die Bundesbank der BRD wurde ein System zur Konstruktion von Prüfcodes auf Geldscheinen genutzt, dass die Diedergruppe D_5 verwendet.
Das Interessante an dieser Gruppe ist, dass sie nicht kommutativ ist. Zum Beispiel gilt $1 \cdot 6 = 7$ aber $6 \cdot 1 = 5$.
Diese Eigenschaft ist für die Erkennung von Zahlendrehern wichtig. Auf den DM-Scheinen wurde die Prüfziffer derart gewählt, dass die Dieder-Verknüpfung aller Stellen stets 0 ergibt.

Außer 8 Ziffern enthalten die Prüfcodes drei Buchstaben, an der 1., 2. und 10.Stelle. Die Buchstaben dienten ebenfalls der Absicherung gegen Fehler, besonders der letzte verhindert Dreher der letzten beiden Positionen. Dabei wurden die Buchstaben während der Kontrolle durch Ziffern ersetzt:

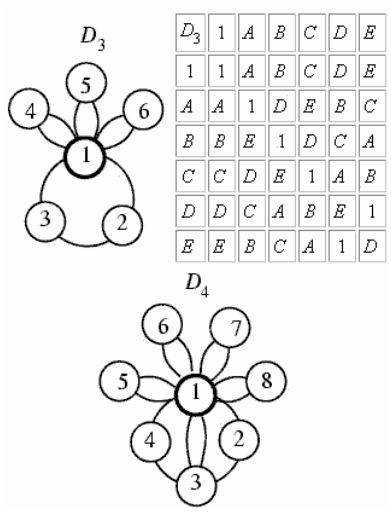
A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

Um weitere Zahlendreher zu unterbinden, werden die einzelnen Ziffern permutiert. Eine Permutation, die dies leistet, ist

p = {1, 5, 7, 6, 2, 8, 3, 0, 9, 4}.

Diese wird auf die erste Ziffer angewandt. Die Permutation für die 2. bis 10.Ziffer sind
5, 8, 0, 3, 7, 9, 6, 1, 4, 2, 8, 9, 1, 6, 0, 4, 3, 5, 2, 7, 9, 4, 5, 3, 1, 2, 6, 8, 7, 0, 4, 2, 8, 6, 5, 7, 3, 9, 0, 1, 2, 7, 9, 3, 8, 0, 6, 4, 1, 5, 7, 0, 4, 6, 9, 1, 3, 2, 5, 8, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 1, 5, 7, 6, 2, 8, 3, 0, 9, 4, 5, 8, 0, 3, 7, 9, 6, 1, 4, 2
Die 11.Ziffer wird nicht permutiert.

Abbildung: 10 DM-Schein mit Prüfcode



D_3	1	A	B	C	D	E
1	1	A	B	C	D	E
A	A	1	D	E	B	C
B	B	E	1	D	C	A
C	C	D	E	1	A	B
D	D	C	A	B	E	1
E	E	B	C	A	1	D

Dihedrale Gruppe D3

Die dihedrale Gruppe wird auch Diedergruppe genannt. Sie ist eine der beiden Gruppen der Ordnung 6.
Sie ist isomorph zur symmetrischen Gruppe S_3, nicht-abelsche und nicht-kommutative Gruppe.
Sie ist die kleinste nicht-Abelsche Gruppe.
Beispiele: Symmetriegruppe des gleichseitigen Dreiecks, Permutationsgruppe von drei Elementen

Dihedrale Gruppe D4

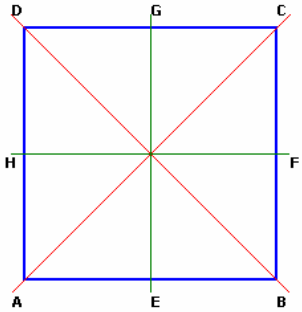
Eine der beiden nicht-Abelschen Gruppen der Ordnung 8, auch Okta-Gruppe genannt. Ist isomorph zur Symmetriegruppe des Quadrates

Untergruppen der Diedergruppe D3

Untergruppen von D_3 können nach dem Satz von Lagrange nur

die Mächtigkeiten 1, 2, 3 und 6 haben, da die Mächtigkeit von D_3 gleich 6 ist.
H_{ij} sei eine Untergruppe von D_3, wobei i die Mächtigkeit dieser Untergruppe bezeichnet und j der Nummerierung dient.
Als Untergruppe mit der Mächtigkeit 1 kommt nur $H_1 = \{e\}$ in Frage, da das Einselement in jeder Gruppe vorhanden sein muss.
Untergruppen mit der Mächtigkeit 2: $H_{21} = \{e,A\}$, $H_{22} = \{e,B\}$, $H_{23} = \{e,C\}$
Diese bestehen jeweils aus dem Einselement und einem anderem Element, das sein eigenes Inverses ist. Diese Forderung erfüllen die Spiegelungen am gleichseitigen Dreieck.

Untergruppen mit der Mächtigkeit 3:
Würde die Untergruppe eine Spiegelung enthalten, wäre eine weitere Spiegelung für die Mächtigkeit 3 nötig. Die Verknüpfung von zwei verschiedenen Spiegelungen ergibt aber eine Drehung. Die Untergruppe wäre nicht abgeschlossen. Diese Untergruppe muss daher zwei inverse Drehungen beinhalten, d.h. es ist nur H_3 {e,D,E} möglich, die Drehgruppe des regulären Dreiecks.
Von den Untergruppen von D_3 sind H_1, H_3 und D_3 selbst Normalteiler.



$$I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad D=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$$
$$A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \quad E=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$
$$B=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \quad F=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$
$$C=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \quad G=\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$$

Bewegungsgruppe des Quadrates D4

Die Bewegungsgruppe des Quadrates ist eine nicht-Abelsche Gruppe der Ordnung 8, auch Okta-Gruppe genannt.
Die Automorphismengruppe von D4 ist isomorph zu D4.
Die Gruppe lässt sich durch die acht Bewegungen (I, A bis G) beschreiben. Diese affinen Bewegungen überführen das Quadrat wieder in ein kongruentes Quadrat.

I	identische Abbildung
A	Drehung um Quadratmittelpunkt mit 90°
B	Drehung um Quadratmittelpunkt mit 180°
C	Drehung um Quadratmittelpunkt mit 270°
D	Spiegelung an Strecke EG
E	Spiegelung an Strecke AC
F	Spiegelung an Strecke FH
G	Spiegelung an Strecke BD

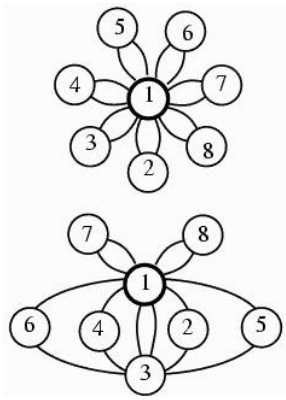
Die Gruppe besitzt 10 Untergruppen {I}, {I,B}, {I,D}, {I,E}, {I,F}, {I,G}, {I,A,B,C}, {I,B,D,F}, {I,B,E,G} und D4. Von diesen sind {I}, {I,B}, {I,A,B,C}, {I,B,D,F}, {I,B,E,G} und D4 Normalteiler.

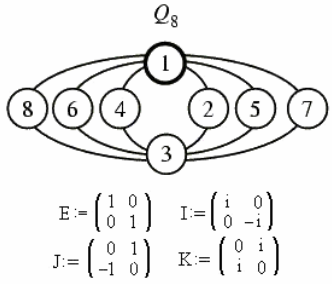
dung

Gruppen der Ordnung 8

Gruppe Z2 ⊗ Z2 ⊗ Z2

eine der drei Abelschen Gruppe, der fünf Gruppen der Ordnung 8; entspricht der Multplikationsgruppe modulo 24





$$E:=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad I:=\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}$$
$$J:=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \quad K:=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$

Gruppe Z2 ⊗ Z4

abelsche Gruppe der Ordnung 8
entspricht den Mulitplikationsgruppen modulo 15, 16, 20 und 30

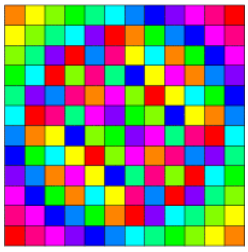
Endliche Gruppe Q8

Eine der zwei nicht-Abelschen Gruppen der insgesamt 5 endlichen Gruppen der Ordnung 8.
Diese Gruppe hat die Multiplikationstafel der Quaternionen ± 1, ± i, ± j, ± k und wird deshalb auch Quaternionengruppe genannt.
Quaternionen: {±E, ±I, ±J, ±K}. Jedes dieser 8 Elemente kann man mit einer 2 x 2-Matrix identifizieren

Mit der üblichen Multiplikation von Matrizen und der Relation $i^2 = -1$ erhält man die multiplikative Gruppe Q der Quaternionen. Für Anwendungen in der Dynamik, Astronomie und Wellentheorie suchte Hamilton fünfzehn Jahre lang nach einer geeigneten Multiplikation in der vierten Dimension.

Die Automorphismengruppe von Q8 ist isomorph zur symmetrischen Gruppe S_4.

Auf einem Spaziergang kam ihm dann die geniale Idee, einfach auf das Kommutativgesetz zu verzichten. Voller Begeisterung über seine Entdeckung ritzte er sofort die Formeln in den Pfeiler einer Brücke, auf der er gerade stand. (siehe Quaternionen)
Dies war allerdings auch der Beginn einer Tragödie, denn von diesem Zeitpunkt an arbeitete er Tag und Nacht daran, mit seinen Quaternionen den ganzen Kosmos erklären zu wollen. Er verfiel dem Alkohol, und nach seinem Tode entdeckte man in seinem Arbeitszimmer unter Bergen mathematischer Aufzeichnungen eine unglaubliche Menge von Tellern mit eingetrocknetem Essen.



Gruppe der Ordnung 12

Die endliche Gruppe Z2 ⊗ Z6 ist eine Gruppe der Ordnung 12 und das direkte Produkt der zyklischen Gruppen Z2 und Z6. Sie ist eine der beiden Abelschen Gruppen der Ordnung 12. Die andere Abelsche Gruppe dieser Ordnung ist die zyklische Gruppe Z12.
Die Abbildung zeigt die Multiplikationstafel von Z2 ⊗ Z6, wobei die Elemente durch unterschiedliche Farben charakterisiert werden.
Restklassengruppen modulo n mit n = 21, 28, 36 und 42 sind isomorph zu Z2 ⊗ Z6.
Die Gruppe besitzt 10 Untergruppen: die triviale Untergruppe, 3 Gruppen der Ordnung 2, 1 der Ordnung 3, 1 der Länge 4, 3 der Länge 6 und natürlich die ganze Gruppe.

Weitere Gruppen der Ordnung 12 sind die abelsche, zyklische Gruppe Z_{12}, und die nichtabelschen Gruppen: A_4 die alternierende Gruppe, D_6 die dihedrale Gruppe der Ordnung 6 und eine Gruppe T, die als semidirektes Produkt von Z_4 und Z_3 aufgefasst werden kann. Die dihedrale Gruppe D_6 ist isomorph zu S_3 x Z_2.

Gruppen der Ordnung 9

Es existieren 2 abelsche Gruppen: Z_9 und Z_3 x Z_3.

Gruppen der Ordnung 10

Es existieren 2 Gruppen, eine abelsche Z_{10} und eine nichtabelsche D_5.

	00	10	20	30	01	02	11	21	31	12	22	32
00	00	10	20	30	01	02	11	21	31	12	22	32
10	10	20	30	00	11	12	21	31	01	22	32	02
20	20	30	00	10	21	22	31	01	11	32	02	12
30	30	00	10	20	31	32	01	11	21	02	12	22
01	01	12	21	32	02	00	10	22	30	11	20	31
02	02	11	22	31	00	01	12	20	32	10	21	30
11	11	22	31	02	12	10	20	32	00	21	30	01
21	21	32	01	12	22	20	30	02	10	31	00	11
31	31	02	11	22	32	30	00	12	20	01	10	21
12	12	21	32	01	10	11	22	30	02	20	31	00
22	22	31	02	11	20	21	32	00	12	30	01	10
32	32	01	12	21	30	31	02	10	22	00	11	20

Gruppe T der Ordnung 12

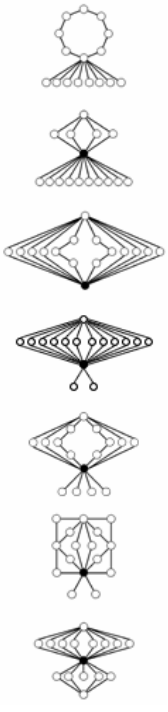
Die nichtabelsche Gruppe T der Ordnung 12 kann durch

$$\langle s, t; s^6 = 1, s^3 = t^2, sts = t \rangle$$

charakterisiert werden.
T ist damit das semidirekte Produkt der zyklischen Gruppen Z_3 und Z_4.
Äquivalent ist auch die Definition mit

$$\langle x, y; x^4 = y^3 = 1, yxy = x \rangle$$

Betrachtet man die Elemente der Gruppe
$1 = 00$; $x = 10$; $x^2 = 20$; $x^3 = 30$; $y = 01$; $y^2 = 02$; $xy = 11$; $x^2y = 21$; $x3y = 31$; $xy^2 = 12$; $x^2y^2 = 22$; $x^3y^2 = 32$
ergibt sich die links stehende Gruppentafel.
Eine Matrizendarstellung ergibt sich mit $x = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ und $y = \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}$
wobei w die nichtreelle kubische Einheitswurzel ist.



Endliche Gruppen der Ordnung 14 und 15

Gruppen der Ordnung 14 existieren 2, eine abelsche, die zyklische Gruppe Z_{14}, und eine nichtabelsche, die dihedrale Gruppe D_7. Mit der Ordnung 15 gibt es nur eine Gruppe, die zyklische Gruppe Z_{15}.

Gruppen der Ordnung 16

Folgende Gruppen der Ordnung 16 existieren:
Es gibt 14 Isomorphieklassen von Gruppen der Ordnung 16, d.h. 14 verschiedene endliche Gruppen der Ordnung 16, 5 abelsche und 9 nichtabelsche. Folgende Gruppen der Ordnung 16 existieren:

<16,1>: die zyklische Gruppe Z_{16}
<16,2>: das direkte Produkt zyklischer Gruppen $Z_4 \times Z_4$
<16,3>: das direkte Produkt zyklischer Gruppen $Z_4 \times Z_2 \times Z_2$
<16,4>: das direkte Produkt zyklischer Gruppen $Z_2 \times Z_2 \times Z_2 \times Z_2$
<16,5>: das direkte Produkt zyklischer Gruppen $Z_8 \times Z_2$
<16,6>: die dihedrale Gruppe: $D_8 = < a,b \mid a^2 = b^2 = 1, (ab)^8 = 1 >$, Abbildung 1
<16,7>: das direkte Produkt einer dihedralen Gruppe mit einer zyklischen Gruppe $D_4 \times Z_2$, Abbildung 2
<16,8>: das direkte Produkt der Quaternionengruppe mit einer zyklischen Gruppe $Q \times Z_2$, Abbildung 4
<16,9>: die semihedrale Gruppe der Ordnung 16 mit der Darstellung $<s,t: s^8 = t^2 = 1, st = ts^3>$, Abbildung 7
<16,10>: die Gruppe der Ordnung 16 mit der Darstellung $< s,t: s^4 = t^4 = 1, st = ts^3>$, Abbildung 5
<16,11>: die Gruppe der Ordnung 16 mit der Darstellung $<a,b,c: a^4 = b^2 = c^2 = 1, cbca^2b = 1, bab = a, cac = a>$, Abbildung 6
<16,12>: die Gruppe der Ordnung 16 mit der Darstellung $<s,t: s^4 = t^4 = 1, stst = 1, ts^3 = st^3>$
<16,13>: die verallgemeinerte Quaternionengruppe mit der Darstellung $<s,t: s^8 = 1, s^4 = t^2, sts = t>$, Abbildung 3
<16,14>: die modulare Gruppe der Ordnung 16 mit der Darstellung $<s,t: s^8 = t^2 = 1, st = ts^5>$, sie besitzt die Elemente $s^k t^m$ mit k = 0, 1, …, 7 und m = 0, 1

Gruppen der Ordnung 18

Gruppen der Ordnung 18 gibt es 5, die zwei abelschen Gruppen Z_{18} und $Z_6 \times Z_3$ und 3 nichtabelsche:
<18,3>: die dihedrale Gruppe D_9
<18,4>: das direkte Produkt $S_3 \times Z_3$
<18,4>: das semidirekte Produkt $Z_3 \times Z_3$ mit Z_2
mit der Darstellung $<x,y,z: x^2 = y^3 = z^3 = 1, yz = zy, yxy = x, zxz = x>$

Gruppen der Ordnung 20

Es gibt 5 Gruppen der Ordnung 20, zwei abelsche und 3 nichtabelsche.
<20,1>: die zyklische Gruppe Z_{20}
<20,2>: das direkte Produkt zyklischer Gruppen $Z_{10} \times Z_2$
<20,3>: die dihedrale Gruppe D_{10}
<20,4>: das semidirekte Produkt Z_5 mit Z_4 mit der Darstellung $<s,t: s^4 = t^5 = 1, tst = s>$
<20,5>: die Frobenius-Gruppe der Ordnung 20 mit der Darstellung $<s,t: s^4 = t^5 = 1, ts = st^2>$
diese Gruppe ist die Galois-Gruppe von $x^5 - 2$ über den rationalen Zahlen

Gruppen der Ordnung 21

Es gibt 2 Gruppen der Ordnung 21, die abelsche Z_{21} und eine nichtabelsche Gruppe mit der Darstellung
$<a,b: a^3 = b^7 = 1, ba = ab^2>$
diese Gruppe ist ebenfalls Frobenius-Gruppe und die Galois-Gruppe über den rationalen Zahlen von
$x^7 - 14x^5 + 56x^3 - 56x + 22$

Gruppen der Ordnung 22

Als Gruppen der Ordnung 22 gibt es die abelsche Gruppe Z_{22} und die nichtabelsche, dihedrale Gruppe D_{11}

Gruppen der Ordnung 25

zwei abelsche Gruppen Z_{25} und $Z_5 \times Z_5$

Gruppen der Ordnung 26

die abelsche zyklische Gruppe Z_{26} und die nichtabelsche dihedrale Gruppe D_{13}

Gruppen der Ordnung 24

U.a. existieren folgende Gruppen der Ordnung 24:

<24,1>: $< a,b \mid a^8 = 1, b^3 = 1, bab = a>$, Z_{12}, Z_6, Z_4, Z_3, Z_2 sind Untergruppen

<24,2>: die zyklische Gruppe Z_{24}: $Z_{24} = Z_8 \times Z_3$

<24,3>: die lineare Gruppe über GF(3), Untergruppen Q_4, Z_2
$SL(2,3) = < a,b \mid a^4 = 1, a^2 = b^2, c^3 = 1, aba = b , ac = cb , cab = bc >$

<24,4>: dizyklische Gruppe der Ordnung 24: $Q_{12} = < a,b \mid a^2 = b^6, b^{12} = 1, bab = a >$
Untergruppen Z_{12}, Q_6, Z_6, Z_4, $Z_3 3$, Z_2

<24,5>: direktes Produkt $D_6 \times Z_4 = S_3 \times Z_4$

<24,6>: dihedrale Gruppe D24, Untergruppen sind Z_{12}, D_{12}, Z_6, $Z_2 \times Z_2$, Z_3, Z_2

<24,7>: $< a,b \mid a^4 = 1, b^6 = 1, bab = a >$, Untergruppen D_{12}, $Z_2 \times Z_6$, Z_6, $Z_2 \times Z_2$, Z_3, Z_2

<24,8>: $< a,b,c \mid a^3 = 1, b^4 = 1, c^2 = 1, bcb = c, aba = b, ac = ca >$
Untergruppen D_{12}, Q_6, $Z_2 \times Z_6$, $Z_2 \times Z_2$, Z_3, Z_2

<24,9>: direktes Produkt $Z_{12} \times Z_2 = Z_6 \times Z_4 = Z_4 \times Z_3 \times Z_2$

<24,13>: direktes Produkt $A_4 \times Z_2$

<24,14>: direktes Produkt $D_{12} \times Z_2$

<24,15>: direktes Produkt $Z_6 \times Z_2 \times Z_2$

Insgesamt gibt es 3 abelsche und 12 nichtabelsche Gruppen der Ordnung 24.

Gruppen der Ordnung 27

5 Gruppen, davon 3 abelsche und 2 nichtabelsche

<27,1>: die zyklische Gruppe Z_{27}

<27,2>: das direkte Produkt $Z_9 \times Z_3$

<27,3>: das direkte Produkt $Z_3 \times Z_3 \times Z_3$

<27,4>: die nichtabelsche Gruppe mit der Darstellung $<s,t: s^9 = t^3 = 1, st = ts^4>$

<27,5>: die nichtabelsche Gruppe mit der Darstellung $<x,y,z: x^3 = y^3 = z^3 = 1, yz = zyx, xy = yx, xz = zx>$

Gruppen der Ordnung 28

<28,1>: die zyklische Gruppe Z_{28}

<28,2>: das direkte Produkt $Z_{14} \times Z_2$

<28,3>: die nichtabelsche dihedrale Gruppe D_{14}

<28,4>: das direkte Produkt dihedraler Gruppen $D_7 \times D_2$

Gruppen der Ordnung 30

<30,1>: die zyklische Gruppe Z_{30}

<30,2>: die nichtabelsche dihedrale Gruppe D_{15}

<30,3>: das direkte Produkt einer dihedralen mit einer zyklischen Gruppe $D_5 \times Z_3$

<30,4>: das direkte Produkt einer dihedralen mit einer zyklischen Gruppe $D_3 \times Z_5$

Homomorphiesatz für Gruppen

Die Menge der Nebenklassen eines Normalteilers N in einer Gruppe G wird bezüglich der Operation $aN \cdot bN = abN$ zu einer Gruppe, der Faktorgruppe von G nach N, die mit G/N bezeichnet wird.
Der folgende Satz beschreibt einen Zusammenhang zwischen homomorphen Bildern und Faktorgruppen einer Gruppe und wird deshalb Homomorphiesatz für Gruppen genannt:

Ein Gruppenhomomorphismus $h: G_1 \to G_2$ bestimmt einen Normalteiler von G_1 nämlich
$\ker h = \{a \in G_1 \mid h(a) = e\}$.
Die Faktorgruppe $G_1/\ker h$ ist isomorph zum homomorphen Bild
$h(G_1) = \{h(a) \mid a \in G_1\}$.
Umgekehrt bestimmt jeder Normalteiler N von G_1 eine homomorphe Abbildung
$nat_N: G_1 \to G_2/N$
mit $nat_N(a) = aN$. Diese Abbildung nat_N wird natürlicher Homomorphismus genannt.

Homomorphiesatz für Ringe

Ersetzt man im Homomorphiesatz für Gruppen den Begriff Normalteiler durch Ideal, so erhält man den Homomorphiesatz für Ringe:
Ein Ringhomomorphismus $h: R_1 \to R_2$ bestimmt ein Ideal von R_1 nämlich
$\ker h = \{a \in R_1 \mid h(a) = 0\}$.

Die Faktorgruppe $R_1/\ker h$ ist isomorph zum homomorphen Bild
$h(R_1) = \{h(a) \mid a \in R_1\}$.
Umgekehrt bestimmt jedes Ideal I von R_1 eine homomorphe Abbildung
$nat_I: R_1 \to R_2/I$
mit $nat_I(a) = a+I$. Diese Abbildung nat_I wird natürlicher Homomorphismus genannt.

Faktorring

Zum 150.Geburtstag Dedekinds wurde die abgebildete Briefmarke in der DDR herausgegeben. Neben dem Porträt enthält sie eine Formel. Diese beschreibt die von Dedekind gefundene Primfaktorzerlegung in Faktorringen.
Z ist ein faktorieller Ring, d.h. mit den Eigenschaften:
eine Menge mit kommutativer und assoziativer Addition mit Null und inversen Elementen,
kommutativer und assoziativer Multiplikation mit Eins
Distributivgesetz, Eins und Null sind verschieden.
Nullteilerfreiheit: Aus $n \cdot m = 0$ folgt $n = 0$ oder $m = 0$, d.h. "Integritätsring"
Faktorisierbarkeit: Jedes Element außer den Einheiten und der Null hat eine Zerlegung in irreduzible Elemente, die bis auf die Multiplikation der Faktoren mit Einheiten eindeutig bestimmt ist.
In faktoriellen Ringen stimmen die irreduziblen Elemente und die Primelemente überein.
Dedekind untersuchte andere Ringe von Zahlen darauf, ob sie faktoriell sind.
Das erste Beispiel ist die Menge der Gauß'schen Zahlen Z[i], bestehend aus den komplexen Zahlen $n + m \cdot i$ mit n, m ganzzahlig. Z[i] wird durch die Gitterpunkte mit ganzzahligen Koordinatenwerten in der komplexen Zahlenebene dargestellt. Z[i] ist ein faktorieller Ring mit den Einheiten 1, -1, i, -i . Während z.B. 3 eine Primzahl in Z[i] ist, gilt dies nicht für alle natürlichen Primzahlen: Es ist z.B. $2 = (1+i)\cdot(1-i)$ und $5 = (2+i)\cdot(2-i)$, also sind 2 und 5 nicht prim in Z[i]. Die Faktoren $1 \pm i$ und $2 \pm i$ sind Primzahlen, also wurden für 2 und 5 die eindeutige Primfaktorzerlegung angegeben. Diese gilt aber nur bis auf die Multiplikation der Faktoren mit Einheiten; es gilt auch $5 = (-1+2i)\cdot(-1-2i)$.
Das zweite Beispiel sein Z[d]; hier soll d für $i\cdot\sqrt{5}$ stehen. Z[d] besteht aus allen Zahlen $n + m\cdot i\cdot\sqrt{5}$ mit n, m ganzzahlig und wird ebenfalls durch ein Gitter in der komplexen Zahlenebene dargestellt; 1 und -1 sind die einzigen Einheiten. Auch in Z[d] lassen sich die Zahlen irreduzibel faktorisieren, aber hier gilt nicht mehr die Eindeutigkeit. So ist z.B. $6 = 2\cdot3 = (1+d)\cdot(1-d)$. Alle vier Faktoren sind irreduzibel, aber nicht prim. Z[d] ist also kein faktorieller Ring.
Dedekind fand einen Weg, eindeutige Primfaktorzerlegungen auch für Z[d] und andere Ringe ganzer Zahlen zu ermöglichen, allerdings nicht für Zahlen, sondern für Ideale. Echte Ideale sind von {0} und vom Ring verschieden. Ein Ideal p heißt Primideal, wenn aus $x_1\cdot x_2$ in *p* folgt, dass x_1 oder x_2 in *p* liegt. In Z und Z[i] sind die Primideale genau die durch jeweils eine Primzahl erzeugten Ideale. Darauf bezieht sich der auf Richard Dedekind zurückgehende Satz:

In Z[d] und anderen Ringen ganzer Zahlen in imaginär-quadratischen Zahlkörpern lässt sich jedes echte Ideal a eindeutig als endliches Produkt von Primidealen $\mathbf{p_i}$ darstellen: $a = p_1\text{^}e_1\ p_2\text{^}e_2 \ldots p_k\text{^}e_k$.

Da Z[d] nicht faktoriell ist, gibt es hier im allgemeinen keine eindeutige Zerlegung in Ideale, die nur von einer einzigen Zahl erzeugt werden.

Algebraischer Modul

Ist R ein Ring und (V,+) eine abelsche Gruppe, so heißt V R-Modul oder Modul über R, wenn gilt (R...Skalare , V...Vektoren):

$\forall\alpha, \beta \in R, \forall x \in V$: $(\alpha + \beta)\, x = \alpha\, x + \beta\, x$
$\forall\alpha \in R, \forall x, y \in V$: $\alpha\,(x + y) = \alpha\, x + \alpha\, y$
$\forall\alpha, \beta \in R, \forall x \in V$: $\alpha\,(\beta\, x) = (\alpha\, \beta)\, x$ $\qquad\qquad$ $\forall x \in V$: $1\, x = x$

Falls R ein Körper ist, so heißt V R-Vektorraum oder Vektorraum über R.

Untermodul Aus $x, y \in V'$ und $\alpha \in R$ folgt stets $x + y \in V'$ und $\alpha\, x \in V'$
Aus $x, y \in V'$ und $\alpha, \beta \in R$ folgt stets $\alpha\, x + \beta\, y \in V'$

Zahlbereiche (algebraische Strukturen)

Der Teilbereich der gebrochenen Zahlen der Form (k/1) ist dem Bereich der natürlichen Zahlen hinsichtlich Rechenoperationen und Ordnung isomorph.
Der Bereich der positiven rationalen Zahlen ist dem Bereich der absoluten rationalen Zahlen hinsichtlich Rechenoperationen und Ordnung isomorph.

Zahlkörper

Die rationalen Zahlen bilder einen archimedisch geordneten Körper.
Der Körper der reellen Zahlen enthält einen Teilkörper, welcher dem Körper der rationalen Zahlen hinsichtlich Operationen und Ordnung isomorph ist.

Restklassenkörper

ist n Primzahl, so ist der Restklassenring Z_n nullteilerfrei und Körper

Diskretes Logarithmusproblem

diskrete Exponentiation $y = a^x \pmod p$ ist innerhalb eines endlichen Körpers effizient ausführbar
... die Ermittlung des Index x von y zur Basis a heißt diskreter Logarithmus
... heute (1998) nicht in polynomialer Zeit ausführbar
... im Jahr 1801 veröffentlichte Gauß Tafeln bis p<100
... der Algorithmus von Gordan mit exponentiellen Aufwand benötigt für p mit 512 Bit ca. 108 Jahre

Index-Calculus-Algorithmus

Der Index-Calculus-Algorithmus ist ein Algorithmus zur Berechnung des diskreten Logarithmus

$$x = \log_\alpha \beta$$

Es sei G eine endliche zyklische Gruppe der Ordnung n, die durch α erzeugt wird.
Es sei $S = p_1, p_2, \ldots, p_t$, die Faktorbasis, eine Untermenge von G mit der Eigenschaft, dass ein bedeutender Teil der Gruppenelemente sich als Produkt der Elemente S schreiben lässt.

1. Schritt: Es wird eine Zufallszahl a gewählt und versucht α a als Produkt der Elemente aus der Faktorbasis S zu schreiben: $\alpha^a = \Pi_{i=1}^{t} p_i^{\lambda}i$
Wenn eine entsprechende Darstellung gefunden wurde kann eine lineare Kongruenz gebildet werden.

$$a \equiv \Sigma_{i=1}^{t} \lambda_i \log_\alpha p_i \bmod n$$

Wenn eine genügend große Anzahl, mehr als t, an Relationen gefunden wurde, kann erwartet werden, dass das zugehörige lineare Gleichungssystem eine eindeutige Lösung für die Unbekannten $\log_\alpha p_i$ mit $1 \le i \le t$ besitzt.
2. Schritt: In diesem Schritt werden die individuelle Logarithmen in G berechnet. $\beta \in G$ ist gegeben.
Es werden solange Zufallszahlen s gewählt, bis $\alpha^s \beta$ sich als Produkt von Elementen aus S schreiben lässt

$$\alpha^s \beta = \Pi_{i=1}^{t} p_i^{b}i$$

Es gilt: $\log_\alpha \beta = \Sigma_{i=1}^{t} b_i \log_\alpha p_i - s \bmod n$
Quelle http://de.wikipedia.org/wiki/Index-Calculus-Algorithmus

Babystep-Giantstep-Algorithmus

Der Babystep-Giantstep-Algorithmus berechnet den diskreten Logarithmus eines Elements einer zyklischen Gruppe. Der Algorithmus ist laufzeitmäßig dem Ausprobieren aller Möglichkeiten überlegen, aber dennoch für sehr große Gruppen praktisch nicht durchführbar.

Sei $G = \langle g \rangle$ eine endliche zyklische Gruppe der Ordnung n und $m = [\sqrt{n}]$. a sei ein Gruppenelement, $x = \log_g a$ der diskrete Logarithmus von a zur Basis g, d.h. die modulo n eindeutig bestimmte Zahl mit $a = g^x$.
Mit Division mit Rest gibt es dann eindeutige $0 \le i, j < m$ mit $x = im + j$. Es gilt $a = g^x = g^{im + j}$, und damit

$$g^j = ag^{-im}.$$

Der Algorithmus berechnet g^j für alle j und danach ag^{-im} für wachsendes i, bis der Wert einem g^j entspricht. Damit ergibt sich $x = im + j$.

Algorithmus

Eingabe: Endliche zyklische Gruppe G, Erzeuger g, Gruppenelement a
Ausgabe: $x = \log_g a$ mit $g^x = a$
Berechne $n = |G|$
Für alle $j \in \{0, \ldots, m-1\}$: Berechne g^j und speichere (j, g^j) in einer Tabelle.
Für alle $i \in \{0, \ldots, m-1\}$: Berechne $a(g^{-m})^i$ und suche danach in der zweiten Spalte der Tabelle. Wenn gefunden, gib $im + j$ aus.
Wegen $a(g^{-m})^i = a(g^{-m})^{i-1} g^{-m}$ lässt sich das Gruppenelement im letzten Schritt aus dem der vorhergehenden Iteration berechnen.
Für die Datenhaltung von (j, g^j) empfiehlt es sich, eine Hashtabelle zu verwenden, wobei der Hash-Wert von g^j berechnet wird. Sowohl Zeit- als auch Platzkomplexität liegen in $O(\sqrt{n})$.

Prinzip der kleinsten Zahlen

Für einen Zahlenbereich gilt das Prinzip der kleinsten Zahl, wenn jede nichtleere Teilmenge aus diesem Zahlenbereich eine kleinste Zahl besitzt

Permanenzprinzip bei Zahlbereichserweiterungen

Hermann Hankel formulierte 1867 das Prinzip von der Erhaltung der formalen Rechengesetze. Es besagt, dass bei Erweiterungen eines Zahlbereiches die Rechengesetze des Ausgangsbereiches nach Möglichkeit auch im erweiterten Bereich gelten sollen. Diese Forderung wird Permanenzprinzip genannt. Dabei handelt es sich weder um ein Axiom noch um einen Satz mit Beweiskraft, sondern um ein Prinzip. Es kann auch nicht erreicht werden, dass alle Gesetze des Ausgangsbereiches im erweiterten Zahlbereich unverändert gelten. Z.B. existieren im Bereich der komplexen Zahlen keine Monotoniegesetze mehr, da eine Größenrelation bei komplexen Zahlen nicht definiert werden kann.
Betrachtet man den Aufbau der Zahlenbereiche mengentheoretisch, so bedeutet dies, dass der neue Bereich den vorhergehenden Zahlenbereich als Teilmenge enthalten sollte.

Ganze Zahlen als Paare natürlicher Zahlen

Entsprechend dem Permanenzprinzip erweitert man zum Beispiel die natürlichen Zahlen zu den ganzen Zahlen, indem jede ganze Zahl einem Paar natürlicher Zahlen (a, b) mit den Eigenschaften

die natürliche Zahl $a = (a+b, b)$
die Null $0 = (b, b)$
die negative Zahl $-a = (b, a+b)$

entspricht. Die Grundoperationen werden dann

$(a,b) + (c,d) = (a+c, b+d)$
$(a,b) \cdot (c,d) = (ac + bd, ad + bc)$
$(a,b) < (c,d)$ falls $(a+d < b+c)$

Galoistheorie, Galois-Gruppe

Zusammenstellung einfacher Definitionen und Sätze des Galois-Theorie

Zur Untersuchung der Wurzeln eines Polynoms $f(x) = 0$ werden der Körper K, der durch die Koeffizienten des Polynoms f(x) erzeugt wird, und der Zerfällungskörper F von f(x) über K betrachet.

Ist F eine Körpererweiterung von K. Die Menge der Automorphismen ϕ: F -> F, so dass $\phi(a) = a$ für alle a von K ist, bildet mit der Nacheinanderausführung von Funktionen eine Gruppe.

Definition: Ist F eine erweiterung des Körper K, so heißt die Menge

$\{\theta \in \mathrm{Aut}(F) \mid \theta(a) = a \text{ für alle } a \in K\}$

die Galois-Gruppe von F über K und wird mit Gal(F/K) bezeichnet.

Definition: Ist K ein Körper, $f(x) \in K[x]$, und ist F Zerfällungskörper von f(x) über K, dann wird Gal(F/K) die Galois-Gruppe von f(x) über K genannt, oder auch Galois-Gruppe der Gleichung $f(x) = 0$ in K.

Satz: Ist F eine Körpererweiterung von K sowie $f(x) \in K[x]$. Dann definiert jedes Element von Gal(F/K) eine Permutation der Wurzeln von f(x), die in F liegen.

Lemma: Es sei $f(x) \in K[x]$ ein Polynom ohne doppelze Wurzlen und F der Zerfällungskörper von f(x) über K. Wenn ϕ: K -> L ein Körperisomorphismus ist, der f(x) auf $g(x) \in L[x]$ abbildet und E ist der Zerfällungskörper von g(x) über L, dann existiert genau ein [F:K] Isomorphismus θ: F -> E, so dass $\theta(a) = \phi(a)$ für alle a in K ist.

Satz: Es sei K Körper, $f(x) \in K[x]$, und F die Zerfällung von f(x) über K. Hat f(x) keine doppelten Wurzeln, dann ist |Gal(F/K)| = [F:K].
Folgerung: Ist K ein endlicher Körper, F eine Erweiterung von K mit [F:K] = m, dann ist Gal(F/K) eine zyklische Gruppe der Ordnung m.

Definition: Es sei f(x) ein Polynom in K[x] und F ein Zerfällungskörper für f(x) über K. Hat f(x) die Faktorisierung

$$f(x) = (x - r_1)^{m}1\ (x - r_2)^{m}2 \dots (x - r_t)^{m}t$$

über F, so hat die Wurzel r_i die Vielfachheit m_i.
Ist $m_i = 1$, so wird r_i einfache Lösung genannt.
Es sei $f(x) \in K[x]$ mit $f(x) = \Sigma_{k=0}^{t} a_k x^k$. Als formale Ableitung f'(x) von f(x) wird dann

$$f'(x) = \Sigma_{k=0}^{t} k\, a_k\, x^{k-1}$$

verstanden.

Satz: Das Polynom f(x) in K[x] hat nur einfache Nullstellen, genau dann, wenn ggT(f(x),f'(x)) = 1 ist.
Satz: Es sei f(x) ein irreduzibles Polynom über dem Körper K. Dann hat f(x) keine mehrfachen Lösungen, wenn chr(K) = $p \neq 0$ und f(x) von der Form ist $f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \dots + a_n x^{np}$.

Definition: Ein Polynom f(x) über dem Körper K heißt separabel, wenn sein irreduziblen Faktoren keine einfachen Lösungen haben.
Ein algebraische Körpererweiterung F von K ist separabel über K, wenn das Minimalpolynom jedes Elements von F separabel ist. Ein Körper K wird vollkommen genannt, wenn jedes Polynom über F separabel ist.

Satz: Jeder Körper der Charakteristik 0 ist vollkommen. Ein Körper mit einer Charakteristik p > 0 ist vollkommen, genau dann, wenn jedes Element ein p-te Wurzel besitzt.
Jeder endliche Körper ist vollkommen.
Satz: Es sei F eine endliche Erweiterung über dem Körper K. Ist F separable über K, dann ist F eine einfache Erweiterung über K.

Satz: Es sei F ein Körper und G eine Untergruppe von Aut(F). Dann ist

$$F^G = \{a \in F \mid \theta(a) = a \text{ für alle } \theta \in G\}$$

ein Unterkörper von F.
F^G wird dann G-invarianter Teilkörper von F genannt.

Satz: Ist F Zerfällungskörper über K eines separierbaren Polynoms und G = Gal(F/K), so ist $F^G = K$.

Artinsches Lemma: Es sei G eine endliche Gruppe von Automorphismen über einem Körper F und K = FG. Dann gilt

$$[F:K] \leq |G|$$

Definition: F sei algebraische Erweiterung des Körper K. F heißt dann normale Körpererweiterung von K, wenn jedes irreduzible Polynom in K[x], die eine Lösung in F enthält, ein Produkt von Linearfaktoren in F[x] ist.

Theorem: Folgende Bedingungen sind für einen Erweiterungskörper F von K äquivalent
(1) F ist Zerfällungskörper über K eines separablen Polynoms
(2) $K = F^G$ für eine endliche Gruppe G von Automorphismen von F
(3) F ist endliche, normale und separable Erweiterung von K

Folgerung: Wenn F Erweiterungskörper von K mit $K = F^G$ für eine endliche Gruppe G von Automorphismen von F ist, so gilt G = Gal(F/K).

Beispiel: Die Galois-Gruppe von $GF(p^n)$ über $GF(p)$ ist zyklisch von der Ordnung n und wird von dem Automorphismus θ: $\theta(x) = x^p$ für alle x in $GF(p^n)$ erzeugt.
Dieser Automorphismus wird Frobenius-Automorphismus von $GF(p^n)$ genannt.

Fundamentalsatz der Galois-Theorie: F sei der Zerfällungskörper eines separablen Polynoms über einem Körper K. Es sei weiter G = Gal(F/K).

(a) Dann existiert eine 1-1-ordnungserhaltende Beziehung zwischen den Untergruppen und G und Unterkörpern von F, die in K enthalten sind:
(i) Wenn H Untergruppe von G ist, dann ist der korrespondierende Teilkörper F^H mit H = $Gal(F/F^H)$.
(ii) Wenn E Teilkörper von F ist und in K enthalten, dann ist die korrespondierende Untergruppe von G die Untergruppe H = Gal(F/E) mit E = F^H.
(b) Für jede Untergruppe H von G gilt $[F:F^H] = |H|$ und $[F^H:K] = [G:H]$.
(c) Die Untergruppe H ist genau dann normal, wenn der Teilkörper $E = F^H$ eine normale Erweiterung von K ist. Dann gilt $Gal(E/K) \cong Gal(F/K) / Gal(F/E)$.
Als Folgerung kann vereinfacht gesagt werden, dass normale Untergruppen normalen Körpererweiterungen zugeordnet werden können.

Folgerungssatz:
F sei Zerfällungskörper eines separablen Polynoms über dem Körper K. E sei Teilkörper mit $K \subseteq E \subseteq F$, mit H = Gal(F/E). Wenn $\phi \in Gal(F/K)$ gilt, so ist $Gal(F/\phi(E)) = \phi H \phi^{-1}$.

Fundamentalsatz der Algebra: Jedes Polynom in C[x] hat eine Lösung in den komplexen Zahlen C.

Lösbarkeit in Radikalen

Definition: Ein Erweiterungskörper F über K wird radikale Erweiterung von K genannt, wenn Elemente $u_1, u_2, \ldots$ in F existieren, so dass
(i) $F = K(u_1, u_2, \ldots, u_m)$ und
(ii) $u_1^{n}1 \in K$ und $u_i^{n}i \in K(u_1, \ldots, u_{i-1})$ für i = 2, …, m und $n_1, n_2, \ldots, n_m \in Z$.
Für $f(x) \in K[x]$ heißt die Polynomgleichung f(x) = 0 lösbar in Radikalen, wenn eine radikale Erweiterung F von K existiert, die alle Lösungen von f(x) enthält.

Satz: Es sei F ein Zerfällungskörper von $x^n - 1$ über dem Körper K der Charakteristik Null. Dann ist Gal(F/K) eine abelsche Gruppe.

Theorem: Es sei K Körper der Charakteristik 0, der alle n-ten Wurzeln der Einheit enthält. Es sei $a \in K$ und F Zerfällungskörper von x^n-a über K. Dann ist Gal(F/K) zyklische Gruppe, deren Ordnung Teiler von n ist.

Theorem: p sei Primzahl. Der Körper K enthalte alle p-ten Wurzeln der Einheit und F sei Erweiterung von K. Wenn $[F:K] = |Gal(F/K)| = p$ ist, dann ist F = K(u) für einige $u \in F$, so dass $u^p \in K$.

Lemma: K ist Körper der Charakteristik 0 und E eine radikale Erweiterung von K. Dann existiert eine Erweiterung F von E, die normale radikale Erweiterung von K ist.

Theorem: f(x) sei Polynom über dem Körper K der Charakteristik 0. Die Gleichung f(x) = 0 ist lösbar durch Radikale genau dann, wenn die Galois-Gruppe von f(x) über K auflösbar ist.

Lemma: Jede Untergruppe von S_5, die eine Transposition und einen Zyklus der Länge 5 enthält, ist S_5 selbst.
Und da die symmetrische Gruppe S_n für n > 4 nicht auflösbar ist:
Theorem: Es existiert ein Polynom des Grades 5 mit rationalen Koeffizienten, das nicht in Radikalen lösbar ist.

Algebra (Struktur)

Eine Algebra (Plural: Algebren) ist eine Verallgemeinerung des Begriffes Ring. Es gibt zwei verschiedene Arten von Algebren:
1) Boolesche Algebren, insbesondere Mengenalgebren wie z.B. σ-Algebren
2) Algebren über Ringen, die eine Synthese aus den Begriffen Vektorraum und Ring darstellen, d.h. die den Vektorraum- und den Ringeigenschaften genügt.

Eine Algebra A über einem Körper k ist ein k-Vektorraum mit einer k-bilinearen Verknüpfung

$$A \times A \to A$$

Multiplikation genannt, die durch a·b oder ab symbolisiert wird. Das bedeutet für Elemente x, y, z von A und Skalare λ in k:

$$(x + y) \cdot z = xy + yz \qquad x \cdot (y + z) = xy + xz$$

$$\lambda \cdot (xy) = (\lambda\, x) \cdot y = x \cdot (\lambda\, y)$$

Beispiel: Die Menge der n x n-Matrizen mit der gewöhnlichen Matrizenaddition und -multiplikation ist eine Algebra.

Die Eigenschaften assoziativ, kommutativ oder unitär werden häufig vorausgesetzt. Eine assoziative Algebra ist eine Algebra, in der für die Multiplikation das Assoziativgesetz gilt. Eine assoziative Algebra ist ein Ring.
Eine kommutative Algebra ist eine, meist assoziative, Algebra, in der für die Multiplikation das Kommutativgesetz gilt.
Eine unitäre Algebra ist eine Algebra mit einem Einselement. Unitäre assoziative Algebren A über einem kommutativen Grundring R mit Einselement entsprechen unitären Ringhomomorphismen $R \to A$, deren Bild im Zentrum von A liegt.
Eine Divisionsalgebra ist eine Algebra, in der man dividieren kann, d.h. in der Gleichungen $ax = b$ oder $xa = b$ für $a \neq 0$ stets lösbar sind.
Eine Lie-Algebra ist eine Algebra, in der die beiden Bedingungen gelten; das Produkt wird in Lie-Algebren als [x, y] geschrieben: $[x, x] = 0$ $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$; Jacobi-Identität

Assoziative Algebra

Ein Vektorraum B über einem Körper A oder ein Modul B über einem Ring A zusammen mit einer bilinearen Abbildung $\bullet: B \times B \to B$; $(a, b) \to a \bullet b$
heißt assoziative Algebra, wenn das Assoziativgesetz gilt: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$
Es handelt sich um eine spezielle Algebra.

Beispiele: Die Menge aller Polynome mit reellen oder komplexen Koeffizienten bilden eine assoziative Algebra über den reellen bzw. den komplexen Zahlen.
Die linearen Abbildungen auf einem Vektorraum bilden mit der Verkettung eine assoziative Algebra
Der Vektorraum aller reell- oder komplexwertigen Funktionen auf einem beliebigen topologischem Raum bildet eine assoziative Algebra; dabei werden die Funktionen punktweise addiert und multipliziert.
Der Vektorraum aller stetigen reell- oder komplexwertigen Funktionen auf einem Banachraum bildet eine assoziative Algebra, bzw. sogar eine Banach-Algebra.
Die Menge aller $n \times n$ Matrizen zusammen mit der Matrizenmultiplikation bilden eine assoziative Algebra.
Die komplexen Zahlen bilden eine assoziative Algebra über dem Körper der reellen Zahlen.
Die Quaternionen sind eine assoziative Algebra über dem Körper der reellen Zahlen, aber nicht über den komplexen Zahlen.

Divisionsalgebra

Vereinfacht gesagt handelt es sich bei einer Divisionsalgebra um einen Vektorraum, in dem man Elemente multiplizieren und dividieren kann.

Eine Divisionsalgebra D ist eine nicht notwendigerweise assoziative Algebra, in der zu jedem $a \in D$ und zu jedem $b \in D$, $b \neq 0$ genau ein $x \in D$ mit der Eigenschaft $a = x \cdot b$
existiert. Dabei bezeichnet "·" die Vektormultiplikation in der Algebra. Zusätzlich fordert man, dass D mindestens zwei Elemente enthält.

Eine Divisionsalgebra über den reellen Zahlen hat stets die Dimension 1, 2, 4 oder 8. Dies wurde 1958 von Milnor und Kervaire bewiesen. Enthält die Divisionsalgebra die Zahl 1, so dass $a \cdot 1 = 1 \cdot a = a$ gilt, spricht man von einer Divisionsalgebra mit Eins.
Die 4 reellen Divisionsalgebren mit Eins sind bis auf Isomorphie

- die reellen Zahlen selbst
- die komplexen Zahlen
- die Quaternionen
- die Oktaven auch Oktonionen oder Cayley-Zahlen.

Dies ergibt sich aus dem Satz von Hurwitz, 1898.
Beispiel einer Divisionsalgebra ohne Einselement mit den beiden Einheiten e_1 und e_2, die mit beliebigen reellen Zahlen multipliziert werden können:

$e_1 \cdot e_1 = e_1 \quad e_1 \cdot e_2 = -e_2 \quad e_2 \cdot e_1 = -e_2 \quad e_2 \cdot e_2 = -e_1$

Banachalgebra

Banachalgebren (nach Stefan Banach) sind mathematische Objekte der Funktionalanalysis, die Funktionenräume anhand wesentlicher gemeinsamer Eigenschaften verallgemeinern. Eine Banachalgebra ist ein Vektorraum, in dem zusätzlich auch eine Multiplikation und eine Norm so definiert sind, die Zusatzbedingungen erfüllen.

Ein Vektorraum $(V,+)$ über dem Körper $K = R$ oder C mit einer Norm $|| \; ||$ und einem Produkt $\bullet: V \times V \to V$ ist eine Banachalgebra, wenn gilt:

- $(V, +, || \; ||)$ ist ein Banachraum, d.h. ein vollständiger normierter Vektorraum,
- $(V, +, \bullet)$ ist eine assoziative K-Algebra,
- $||A \bullet B|| \leq ||A|| \bullet ||B||$, d.h. die Norm ist submultiplikativ.

Beispiele: Jeder Banachraum wird mit der Null-Multiplikation, d.h. $xy = 0$ für alle Elemente x,y des Banachraums, zu einer Banachalgebra.
Ist V ein Banachraum, so ist die Algebra B(V) der stetigen, linearen Operatoren auf V eine Banachalgebra, die im Falle $\dim(v) > 1$ nicht kommutativ ist. Ist V ein Hilbertraum, so ist B(V) eine C*-Algebra.

Definition: Eine Banach-*-Algebra A über C oder involutive Banachalgebra ist eine Banachalgebra zusammen mit einer *-Involution $*: A \to A, a \to a^*$, so dass

- $\forall \; a \in A: (a^*)^* = a$ (involutiv)
- $\forall \; a,b \in A: (ab)^* = b^*a^*$ (anti-multiplikativ)
- $\forall \; a,b \in A, \forall \; z,w \in C: (za + wb)^* = \bar{z} a^* + \bar{w} b^*$ (semilinear, anti-linear oder konjugiert linear)
- $\forall \; a \in A: ||a|| = ||a^*||$ (isometrisch)

Für Banachalgebren B(H), wobei H ein Hilbertraum ist, definiert man:
Eine Banachalgebra V, auf der zusätzlich eine semilineare Involution $*: V \to V$ gegeben ist, heißt C*-Algebra, wenn gilt: $||x^* x|| = ||x||^2 \; ; \forall \; x \in V$

Boolesche Algebra - Algebraische Struktur

Eine algebraische Struktur $(B,\cap,\cup,\neg)$ heißt Boolesche Algebra, wenn
1. $\cap$ und $\cup$ zweistellige Verknüpfungen in B sind
2. $\neg$ eine einstellige Abbildung von B in B ist und wenn für alle a,b,c aus B gilt:
3.Kommutativgesetze $a \cap b = b \cap a$ $a \cup b = b \cup a$
4.Distributivgesetze $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$
5. es gibt mindestens ein Element 0 in B, so dass $a \cup 0 = a$ und $a \cap \neg a = 0$
6. es gibt mindestens ein Element 1 in B, so dass $a \cap 1 = a$ und $a \cup \neg a = 1$
Es gelten: Idempotenzgesetze, Assoziativgesetze, Morgansche Gesetze und Absorptionsgesetze

Omega-Algebra, Ω-Algebra

Es sei Ω eine Menge von Operationssymbolen, die in paarweise disjunkte Teilmengen Ω_n, $n \in N$, zerfällt. In Ω_0 liegen die Konstanten, in Ω_n, $n>0$, die n-stelligen Operationssymbole. Die Familie $(\Omega_n)_{n \in N}$ heißt Typ oder Signatur. Ist A eine Menge und ist jedem n-stelligen Operationssymbol $\omega \; \Omega_n$ eine n-stellige Operation ω^A in A zugeordnet, so heißt $A = (A, \{\omega^A \mid \omega \in \Omega\}$
eine Ω-Algebra oder Algebra vom Typ (oder der Signatur) Ω.

Ist Ω endlich, $\Omega = \{\omega_1, ..., \omega_k\}$, so schreibt man für A auch $A = (A, \omega_1^A, ..., \omega_k^A)$.
Fasst man einen Ring als Ω-Algebra auf, so zerfällt Ω in $\Omega_0 = \{\omega_1\}$, $\Omega_1 = \{\omega_2\}$, $\Omega_2 = \{\omega_3, \omega_4\}$, wobei den Operationssymbolen die Konstante 0, Inversenbildung bezüglich Addition, Addition und Multiplikation zugeordnet sind.
Es seien A und B Ω-Algebren. B heißt Ω-Unteralgebra von A, falls $B \subseteq A$ ist und die Operationen ω^B die Einschränkungen der Operationen ω^A ($\omega \in \Omega$) auf die Teilmenge B sind.

Direktes Produkt

Es seien A und B Gruppen, deren Gruppenoperation (z.B. Addition oder Multiplikation) mit * bezeichnet sein soll. Im kartesischen Produkt $A \times B$ kann man durch die folgende Vorschrift eine Operation $\bullet$ einführen: $(a_1, b_1) \bullet (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$
Damit wird $A \times B$ zu einer Gruppe, die das direkte Produkt von A und B genannt wird.
Mit (e,e) wird das Einselement von $A \times B$ bezeichnet, und (a^{-1}, b^{-1}) ist das inverse Element zu (a, b).
Für endliche Gruppen A, B gilt ord $A \times B$ = ord A * ord B. Die Gruppen $A' = \{(a,e) \mid a \in A\}$ bzw. $B' = \{(e,b) \mid b \in B\}$ sind zu A bzw. B isomorphe Normalteiler von $A \times B$. Das direkte Produkt Abelscher Gruppen ist wieder abelsch.
Für zyklische Gruppen gilt: Das direkte Produkt zweier zyklischer Gruppen A, B ist genau dann zyklisch, wenn der größte gemeinsame Teiler der Gruppenordnungen gleich 1 ist

Basissatz für Abelsche Gruppen

Jede endliche Abelsche Gruppe ist als direktes Produkt zyklischer Gruppen von der Primzahlpotenzordnung darstellbar.

Semidirektes Produkt

Das semidirekte Produkt beschreibt eine Methode, um aus zwei gegebenen Gruppen eine neue Gruppe zu konstruieren. Diese Konstruktion verallgemeinert das Konzept des direkten Produkts von Gruppen.
Definition: Gegeben seien zwei Gruppen N und H, sowie ein Homomorphismus θ: $H \rightarrow \mathrm{Aut}(N)$ der Gruppe H in die Gruppe der Automorphismen von N.
Das kartesische Produkt $G = N \times H$ der Mengen N und H wird dann zu einer Gruppe, indem man die Verknüpfung durch $(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \theta(h_1)(n_2), h_1 \cdot h_2)$
definiert. Man notiert das semidirekte Produkt als $N \times_\theta H$,
da der Homomorphismus θ die Struktur dieser Gruppe bestimmt.
Das semidirekte Produkt ist weder kommutativ noch assoziativ.

Äußeres und Inneres Produkt

Die durch die Definition konstruierte Produktgruppe ist das äußere semidirekte Produkt, da die Gruppe G bei dieser Definition aus vorgegebenen, disjunkten Gruppen konstruiert wird.
Innere Definitionen beziehen sich dagegen auf eine bereits gegebene Gruppe G mit einem Normalteiler N und einer Untergruppe H.

Beispiele:
Die Diedergruppe D_n, die Symmetriegruppe eines ebenen regelmäßigen n-Ecks, ist isomorph zum semidirekten Produkt der zyklischen Drehsymmetriegruppe Z_n mit einer zweielementigen zyklischen Gruppe Z4-2·
Für $n > 1$ ist die symmetrische Gruppe S_n isomorph zu einem semidirekten Produkt ihres Normalteilers $N = A_n$, der alternierenden Gruppe, und einer zweielementigen zyklischen Gruppe Z_2.

Strukturen der natürlichen Zahlen

Unter den natürlichen Zahlen wird die Menge $N = \{0, 1, 2, \ldots\}$ verstanden, die mit ihrer natürlichen Anordnung $0 < 1 < 2 < \ldots$ versehen sein soll.

Halbgruppen natürlicher Zahlen

Auf dieser Menge N ist als eine innere Verknüpfung die gewöhnliche Addition + definiert. Sie ist assoziativ und kommutativ und die Zahl 0 ist neutrales Element dieser Verknüpfung. Es handelt sich bei (N,+) um ein kommutatives Monoid.

Andererseits ist auf N auch die gewöhnliche Multiplikation · als innere Verknüpfung definiert, die ebenfalls assoziativ und kommutativ ist und für die die Zahl 1 neutrales Element ist. Damit ist (N,·) ein kommutatives Monoid.
Man kann auf N auch die durch a·b=min(a,b) für alle a und b aus N definierte Verknüpfung · betrachten.
Sie ist nicht nur assoziativ und kommutativ, sondern auch idempotent, besitzt aber kein neutrales Element. Es handelt sich bei (N,min) um eine (kommutative und idempotente) Halbgruppe, die kein Monoid ist.
Ändert man die Verknüpfung aus dem vorigen Beispiel zu a·b=max(a,b), so erhält man ein kommutatives und idempotentes Monoid (N,max), denn die Zahl 0 ist nun neutrales Element.

Halbringe natürlicher Zahlen

Da für die gewöhnliche Addition + und Multiplikation · natürlicher Zahlen die beiden Distributivgesetze gelten, handelt es sich bei (N,+,·) um einen kommutativen Halbring mit absorbierendem Nullelement 0 und Einselement 1. Da für alle a, b, c aus N die Gleichungen

$a \cdot \max(b,c) = \max(a \cdot b, a \cdot c)$ und $a + \max(b,c) = \max(a+b, a+c)$

$a \cdot \min(b,c) = \min(a \cdot b, a \cdot c)$ und $a + \min(b,c) = \min(a+b, a+c)$

gelten, sind auch (N,max,·), (N,max,+), (N,min,·) und (N,min,+) Halbringe.
Da es sich bei min und max um die beiden Verbandsoperationen in der linear geordneten Menge $N = \{0 < 1 < 2 < \ldots\}$ handelt, bilden sowohl (N, min, max) als auch (N, max, min) einen distributiven Verband, also ebenfalls je einen Halbring.

Multioperatorgruppe, Ω-Gruppe

Eine, nicht notwendig kommutative, Gruppe (G, +), auf der ein System Ω n-ärer algebraischer Operationen ω_n, n > 1, gegeben ist, heißt genau dann Multioperatorgruppe oder Ω-Gruppe, wenn gilt:
Für alle j: $a_j = 0$ und c = 0 wird für beliebige Operationen ω_n $\quad 0\ldots0\omega_n = 0$

Die Multioperatorgruppe vereint das Konzept von Gruppe, linearer Algebra und Ring.
Ein Ideal einer Ω-Gruppe ist eine normale Untergruppe N von G mit

$-(x_1 \ldots x_n \omega) + (x_1 \ldots x_{i-1}(a+x_i)x_{i+1} \ldots x_n \omega) \in N$

für alle a aus N, x_i aus G und jeder Operation ω.
Sind A, B und C Ω-Untergruppen der Ω-Gruppe G, wobei C von A und B erzeugt wird, so ist der Kommutator [A,b] der Untergruppen A und B in C das Ideal aller Elemente der Form

$-a-b+a+b$

$-(a_1 \ldots a_n\ \omega)\ -(b_1 \ldots b_n\ \omega)\ +((a_1 b_1)\ldots(a_n+b_n)\ \omega)$

Es sei G' = [G,G]. Dann ist die Ω-Gruppe abelsch, wenn G' = 0 ist.

Multioperatorring

Eine abelsche Gruppe (G, +), auf der ein System Ω n-ärer algebraischer Operationen ω_n, n > 1, gegeben ist, heißt genau dann Multioperatorring oder Ω-Ring, wenn für alle ω_n, alle Elemente a_i, b, c aus G, i = 1,...,n, und alle i gilt

$a_1 \ldots a_{i-1}(b+c)a_{i+1} \ldots a_n\omega_n = a_1 \ldots a_{i-1}ba_{i+1} \ldots a_n\omega_n + a_1 \ldots a_{i-1}ca_{i+1} \ldots a_n\omega_n$ (1)

Jeder Multioperatorring ist Multioperatorgruppe. Für alle j: $a_j = 0$ und c = 0 wird für beliebige Operationen ω_n:

$0 \ldots 0b0 \ldots 0\omega_n = 0\ldots0(b+0)0\ldots0\omega_n = 0\ldots0b0\ldots0\omega_n + 0\ldots0\omega_n = 0\ldots0b0\ldots0\omega_n + 0$

Für ein leeres Operationensystem wird G zum Modul. Enthält Ω nur eine algebraische binäre Multiplikation, bildet G eine ringartige Struktur, womit jeder assoziative oder nichtassoziative Ring Multioperatorring ist. Für diese Strukturen wird (1) zum bekannten Distributivgesetz.
Die vom Nullelement eines Moduls additiv erzeugte Untergruppe wird für ein beliebiges Operationensystem Ω n-ärer Operationen, n > 1, mit $0 \ldots 0\omega_n = 0$ zum Ω-Nullring. Einen Multioperatorring bildet der zweidimensionale reelle Punktraum R^2 mit der Vektoraddition und dem vektoriellen Tripelprodukt, welches ternär ist. Ein Multioperatorring heißt assoziativ, wenn für jedes Paar von Operationen ω_n, ω_k aus dem Operationensystem für jedes i = 1,...,k

$(x_1 \ldots x_n\omega_n)x_{n+1} \ldots x_{n+k-1}\omega_k = x_1 \ldots x_{i-1}(x_i \ldots x_{n+i-1}\omega_n)x_{n+i} \ldots x_{n+k-1}\omega_k$

für alle x_j aus G, j=1,...,n+k-1, gilt. Kommutativ nennt man einen Multioperatorring, wenn für jede Operation ω_n aus dem Operationensystem und jedes Paar (i, j), mit $i \neq j$, und i, j = 1,...,n, für alle x_l aus G, l = 1,...,n

$x_1 \ldots x_i \ldots x_j \ldots x_n\omega_n = x_1 \ldots x_j \ldots x_i \ldots x_n\omega_n$ gilt.

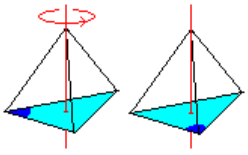
Ein Element 1 von G heißt Einselement von G, wenn für alle x aus G und jede Operation ω_n aus Ω: $1...1x1...1\omega_n = x$ ist.
Ein Element a eines Ω-Ringes nennt man genau dann Nullteiler bezüglich einer Operation ω_n aus dem Operationensystem, wenn ein (n-1)-Tupel von Elementen in G existiert, so dass

$$x_1...x_{i-1}ax_{j+1}...x_n\omega_n = 0$$

für ein beliebiges i gilt, wobei sowohl a als auch alle x_j des Tupels verschieden vom Nullelement sein müssen. In Multioperatorringen gilt $x_1...x_{i-1}0x_{j+1}...x_n\omega_n = 0$
für alle Operationen und alle x_i aus G. Dies folg unmittelbar aus dem Distributivgesetz und den Gruppeneigenschaften.

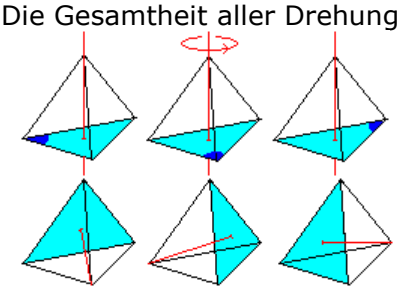
Geschichte der Gruppentheorie

In den Problemen, bei deren Untersuchung Gruppen auftraten, wie etwa der Symmetrie der Platonischen Körper, waren diese Axiome von selbst erfüllt.
Daher hatte man schon einige Erfahrungen über den Umgang mit diesen algebraischen Strukturen gesammelt, bevor die heute vier üblichen Axiome zu ihrer Definition aus diesen Erfahrungen extrahiert wurden.
Die Bezeichnung Gruppe für derartige Strukturen wurde erstmals 1868 durch Camille Jordan verwendet (Memoire sur les groupes des mouvements, Annali de matematica pura ed applicata, Ser. II, Vol. II, No. 3 (1868) 167 - 215, 322-345), obwohl er nur das Axiom der Abgeschlossenheit gegenüber der Verknüpfung von zwei Gruppenelementen explizit forderte. Da er Symmetriegruppen untersuchte, folgten die anderen Gruppeneigenschaften automatisch. Er entdeckte z. B. nicht die Existenz der eindeutig bestimmten inversen Symmetrieabbildung innerhalb der von ihm untersuchten Gruppen.
Im Jahre 1854 hatte Arthur Cayley die Notwendigkeit des Assoziativgesetzes und die Existenz eines Einselementes entdeckt. Er bezeichnete die Gruppenelemente durch abstrakte Symbole und definierte deren Verknüpfung mittels einer Tabelle, die heutzutage Cayley-Tafel genannt wird.
Im Jahre 1856 gab William Rowan Hamilton (Memorandum Respecting a New System of Roots of Unity) die erste Darstellung einer Gruppe, der Ikosaedergruppe, an, eine sehr platzsparende Methode eine konkrete Gruppe zu definieren, die in diesem Fall auf einer einzigen Zeile hingeschrieben werden kann, im Vergleich zu der Tabelle von 60 x 60 Einträgen der Cayley-Tafel.
Die erste Definition der Gruppe mit den heute üblichen Axiomen erfolgte 1882 unabhängig voneinander durch Walter van Dyck (Gruppentheoretische Studien) und Heinrich Weber.
Die erste große außermathematische Anwendung der Gruppentheorie bestand in der Bestimmung aller 230 Raumgruppen durch den russischen Kristallographen Fedorov im Jahre 1890.
Dies sind die Symmetriegruppen der dreidimensionalen Punktgitter. Solche periodischen diskreten Punktgitter wurden als Modelle für den Aufbau von Kristallen aus Atomen angesehen, obwohl dies erst 1912 experimentell bestätigt werden konnte. Jedes solche Gitter kann nämlich eindeutig durch seine Symmetriegruppe charakterisiert werden.



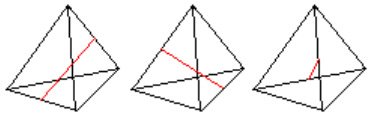
Tetraedergruppe

Bei der Tetraedergruppe geht es um Drehungen des Tetraeders um eine Achse, bei denen es in sich selbst übergeht.
Beispiel: Links sei eine Ausgangsstellung. Man legt durch eine Ecke und den Mittelpunkt des gegenüberliegenden Dreiecks eine Achse. Das Tetraeder wird um 120° nach links gedreht und kommt zur Deckung mit dem ersten Tetraeder. Der dunkelblau markierte Winkel wandert.
Die Gesamtheit aller Drehungen bildet eine Gruppe. Übersicht über alle Drehungen:



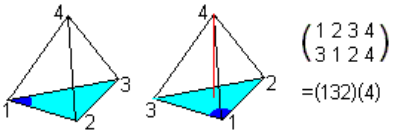
Man erhält eine weitere Drehung, wenn man das gedrehte Tetraeder um 120° weiterdreht.

Da das Tetraeder vier Seitenflächen bzw. Eckpunkte hat, gibt es drei weitere Drehachsen durch den Eckpunkt und den Mittelpunkt eines Dreiecks. Zu jeder Drehachse gibt es zwei Drehungen, die ein Tetraeder in sich selbst überführen. Insgesamt ergeben sich 8 Drehungen.

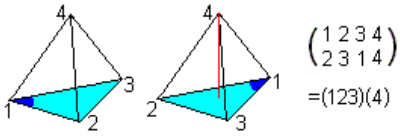


Verbindet man gegenüberliegende Kantenmitten, so ergeben sich drei weitere Drehachsen. Eine Drehung um 180° führt zu einer weiteren Deckung des Tetraeders. Diese Drehung könnte man auch Klappung nennen.
Insgesamt gibt es 3 Drehungen.

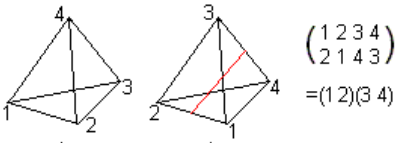
Es gibt insgesamt 11 Drehungen, die ein Tetraeder in sich selbst überführen.



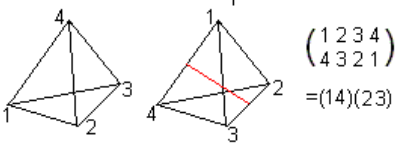
Drehung um eine Ecke/Mitte-Achse
Eine Drehung beschreibt man besser durch Zahlen. Man nummeriert die Ecken des Ausgangstetraeders mit 1, 2, 3 und 4. Nach einer 120°-Drehung nehmen die Eckpunkte die neue Position 3,1 und 2 an, 4 bleibt.
Das hält man in einer Schreibfigur fest: In der ersten Zeile 1 2 3 4, in der zweiten Zeile 3 1 2 4. Die Zuordnungen stehen untereinander.
Noch kürzer ist die Notation mit dem Zyklus (132)(4) oder kurz (132).
Das muss man so lesen: 1 geht über in 3, 3 geht über in 2 und 2 in 1. 123 wird zyklisch vertauscht. Die Ecke 4 bleibt stehen.



Für eine 240°-Drehung ergibt sich die nebenstehende Notation.
Man könnte diese Stellung des Tetraeders auch erreichen, wenn man das Ausgangstetraeder um 120° nach rechts dreht.
Alle Drehungen dieser Art sind (132), (123), (134), (143), (142), (124), (234), (243).

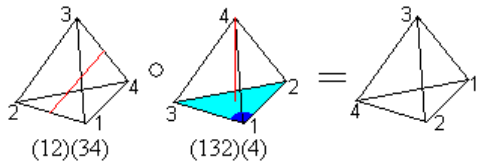


Drehung um eine Mitte/Mitte-Achse
Bei den Drehungen um eine Achse durch zwei Kantenmitten werden die Eckpunkte, die zu einer halbierten Kante gehören, paarweise ausgetauscht.



Die restlichen Möglichkeiten: Die drei Klappungen sind (12)(34), (14)(23), (13)(24).

Es liegt nahe den Fall zu untersuchen, ein Tetraeder zuerst um eine Achse und danach um eine zweite Achse zu drehen. Eine solche Verknüpfung zweier Drehungen, inklusive der identischen Drehung, ergibt wieder eine der genannten Drehungen.

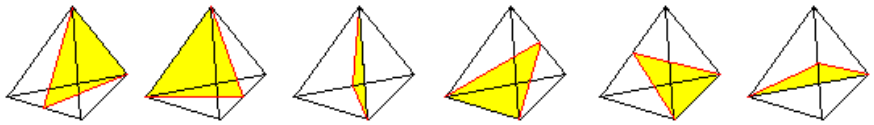


Beispiel: Es wird das um zwei Kantenmitten gedrehte Tetraeder um die vertikale Achse um 120° nach links weitergedreht. Es ergibt sich das rechte Tetraeder, das die Darstellung (143) hat.
Diesen Vorgang kann man als Verknüpfung von Zyklen beschreiben:
Aus (12)(34) und (132)(4) wird (143) oder (12)(34) • (132)(4) = (143)
Mit dem Symbol • wird ausgedrückt, dass man zwei Drehungen verknüpft hat.

Drehgruppe

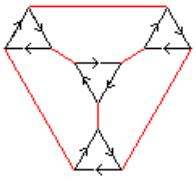
Es gibt 12 Drehungen. Die triviale Drehung (1) ist mitgezählt. Die Drehungen werden durch ein Hintereinanderschalten verknüpft.
Diese beschriebene Struktur ist eine abelsche Gruppe.
Setzt man r = (123) und f = (13)(24), so lassen sich die übrigen Elemente der Drehgruppe aus ihnen errechnen. Die Drehungen r und f beispielsweise "erzeugen" die Gruppe.
$f^2=(1)$, $r^2=(132)$, $rf=(243)$, $fr=(142)$, $(fr)^2=(124)$, $(rf)^2=(234)$, $frf=(134)$, $rfr=(143)$, $r^2fr=(14)(23)$, $rfr^2=(12)(34)$
Diese Drehgruppe ist isomorph zur Untergruppe der geraden Permutation der Permutationsgruppe S_4. Diese Untergruppe ist die alternierende Gruppe.
Auch die ungeraden Permutationen von S_4 kann man als Abbildungen des Tetraeders

interpretieren. Sie stellen eine Spiegelung an einer Mittelebene des Tetraeders dar. Es gibt sechs Spiegelungen dieser Art.



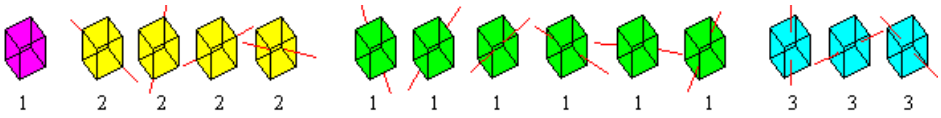
Die übrigen Permutationen (1234), (1243), (1342), (1324), (1432), (1423) sind Drehspiegelungen.

Damit sind alle Elemente der symmetrischen Gruppe als Abbildungen des Tetraeders gedeutet. Die Gesamtheit dieser Abbildungen bilden eine zur Symmetriegruppe S_4 isomorphe Gruppe.



Graph zur Tetraedergruppe

Die kleinen Dreiecke stehen für die Drehungen um die Ecke-Mitte-Achsen, die roten Linien für die Drehungen um die Mitte-Mitte-Achsen.



Oktaedergruppe

Man ersetzt das Tetraeder durch das Oktaeder bzw. den Würfel. Das führt zu einer Drehgruppe mit 24 Elementen. Sie ist isomorph der symmetrischen Gruppe S_4 zu vier Zahlen.

Die dritte Polyedergruppe ist die Ikosaedergruppe mit 60 Elementen. Man könnte wegen der Dualität statt des Ikosaeders das Pentagondodekaeder wählen. Die Ikosaedergruppe ist isomorph zu der alternierenden Gruppe zu fünf Zahlen.

Hauptsatz für endliche Drehgruppen: Eine endliche Drehgruppe ist notwendig von einem der folgenden Gruppentypen: Zyklische Gruppe, Diedergruppe, Tetraedergruppe, Oktaedergruppe, Ikosaedergruppe.

Endliche Transformationen in der Ebene

Viele Buchstaben des Alphabets genügen sehr einfachen Symmetrien. So sind zum Beispiel die Buchstaben

A E

spiegelsymmetrisch. Spiegelungen sind Transformationen der Ebene und werden immer durch die Angabe einer Spiegelungsachse gegeben. Andere Buchstaben weisen Drehsymmetrien auf

O Z

Diese Transformationen werden durch die Angabe von Drehzentrum und Drehwinkel gegeben, wobei das Zentrum als n-Polygon dargestellt wird. Damit soll angedeutet werden, dass an diesem Zentrum eine Drehung um $360^o/n$ stattfinden soll.

Drehsymmetrien werden durch die **zyklischen Gruppen n-ter Ordnung C_n** beschrieben

$$C_n = \{1, d, d^2, d^3, ..., d^{n-1}\} = < d >$$

Die Gruppe ist von endlicher Ordnung n, falls es eine positive ganze Zahl n gibt, so dass $d^n = 1$ gilt.

Kombiniert man Spiegelungen mit Drehungen, so erhält man die **Diedergruppen D_n**. Sie sind die Symmetriegruppen der regelmässigen n-Ecke. Im allgemeinen Fall gibt es eine Drehung d mit $d^n = 1$ und n Spiegelungen s_j mit $s_j^2 = 1$.

$$D_n = \{1, d, d^2, ..., d^{n-1}, s_1, d \circ s_1, ..., d^{n-1} \circ s_1\}$$

Bezeichne G die Gruppe aller diskreten Isometrien der euklidischen Ebene E. Ferner sei *P* ein in E liegendes Polygon: $P \subset E$.

S(P) sei die zum Polygon P gehörige Symmetriegruppe: $S(P) = \{\phi \in G \mid \phi(P) = P\}$

Es sei ferner Γ die Gruppe aller Isometrien der Ebene, die den Nullpunkt O festhalten. Schon Leonardo da Vinci suchte nach allen möglichen Untergruppen von Γ. Hermann Weyl fand die vollständige Antwort auf da Vincis Frage:

Satz von Weyl: Die endlichen Untergruppen von Γ werden, bis auf Konjugation, durch folgende vier Gruppen gegeben:

$$C_n , D_n , V_4 , W=\{1,s\},$$

wobei s die Spiegelung an einer Geraden durch den Nullpunkt ist.

Die Gruppe V_4 ist die Kleinsche Vierergruppe, gegeben durch eine Drehung um 180^o um den Nullpunkt O und zwei Spiegelungen an rechtwinklig aufeinanderstehenden Geraden durch O. So enthält z.B. die Symmetriegruppe eines Rhomboids mit Diagonalen unterschiedlicher Länge

V_4 als Untergruppe. Die Translationen bilden eine wichtige Untergruppe der Gruppe *G* der diskreten Bewegungen von E. Wir bezeichnen sie im folgenden mit T(G). T(G) ermöglicht eine Strukturierung von G:

(I) Gruppen H ⊂ G mit T(H) = ∅ heißen Rosettengruppen oder Punktgruppen

(II) Gruppen H ⊂ G, für die T(H) aus nur einer Translationsrichtung besteht, heissen Friesgruppen

(III) Gruppen H ⊂ G, für die T(H) aus zwei verschiedenen Translationsrichtungen besteht, heissen Ornamentgruppen

Friesgruppen

H^+ seien die eigentlichen und H^- die uneigentlichen Transformationen aus einer Friesgruppe H. Insbesondere ist dann $T(H) \subset H^+$. Im ersten Fall gilt $T(H) = H^+$. Da T(H) eindimensional ist, wird H^+ von einem einzigen Element t, erzeugt $H^+ = < t >$

Ist H^- leer, wird

Ist H^- nicht leer, so kann man eine Spiegelachse in Friesrichtung legen

oder senkrecht zur Friesrichtung

Schließlich gibt es die Möglichkeit, dass H^- eine Schubspiegelung, d.h. die Kombination aus einer Spiegelung und einer Translation um t/2 in Richtung der Spiegelachse enthält

Im zweiten Fall gilt $T(H) \subset H^+$ aber $T(H) \neq H^+$. Es gibt neben den Translationen noch andere eigentliche Abbildungen.

Dies kann die Kombination zweier Spiegelungen mit je einer Achse in Friesrichtung und einer senkrecht dazu sein

Es können auch Drehungen auftreten wie in den beiden letzten Fällen

Insgesamt finden sich auf diese Weise alle sieben möglichen Friesgruppen.

Fries-Symmetrien und Streifenornamente

Ein Fries ist ein theoretisch unendlich langes, periodisches Ornament, das zwischen zwei parallelen Geraden angeordnet ist. Damit es periodisch ist, muss zu seinen Symmetrie-Abbildungen, die es mit sich selbst zur Deckung bringen, eine kürzeste Parallelverschiebung in Richtung dieser Geraden gehören.
Außer diesen unendlich vielen Translationen kann es weitere Symmetrieabbildungen geben:

1) Spiegelungen an der waagerechten Mittellinie w des Streifens
2) Spiegelungen an einer zu den begrenzenden Geraden Senkrechten
3) Drehungen um 180 Grad um einen Punkt P der Mittelparallelen
4) Gleitspiegelungen, d.h. Translationen in Längsrichtung mit anschließender Spiegelung an der waagerechten Mittellinie

Für die sieben möglichen Kombinationen der Bewegungen gibt es eine Vielzahl von Beispielen aus verschiedenen Kulturkreisen bzw. Epochen.

1) nur Translationen
oberste zwei Abbildungen aus Babylon
2) Translationen und Drehungen um 180°
Die Drehpunkte befinden sich sowohl in der Mitte jedes Grundbildes als auch in der Mitte zwischen diesen.
3.Abbildung: antikes Olympia / 4.Abbildung: Italien 15.Jahrhundert

3) Translationen und Spiegelungen an waagerechter Mittalachse, d.h. auch Gleitspiegelungen
Bilder der 1.Reihe: Byzanz 5./6. Jahrhundert und Kloster Maulbronn 14. Jahrhundert

4) Translationen und Spiegelungen an senkrechten Achsen
Bilder der 2.Reihe: Theben, Altägypten und Chorsabad, antikes Assyrien

5) Translationen, Spiegelungen an waagerechten und senkrechten Achsen, d.h. auch Gleitspiegelungen
Bilder der 3.Reihe: Peruanisches Textilmuster und Palast in Nimrud

6) Gleitpiegelungen und Spiegelungen an senkrechten Achsen
Bild der 4.Reihe: Fußboden der Sanct Marien-Kirche in Rom

7) nur Gleitspiegelungen und die sich daraus ergebenden Translationen
Bild der 5.Reihe: Sanct Cunibert, Köln, romanisch

Geflochtene Friesornamente

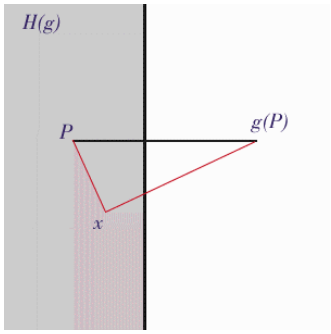
Außer den klassischen Friesgruppen kommen vor allem in der islamischen Ornamentik auch Flechtmuster, geflochtene Friesornamente, vor.
Die Abbildungen von links oben nach rechts unten zeigen: zwei Fußböden römischer Villen, Fußboden San Marco Venedig, Fußboden in Pisa, Darstellungen in Cordoba bzw. Sevilla

Lässt man Translationen entlang der x-Achse, Drehungen um die x-, y- und z-Achse, Spiegelungen an den zu den Raumachsen senkrechten Ebenen, Punktspiegelung am Schnittpunkt der Raumachsen, Gleitspiegelungen und die Schraubung um die x-Achse zu, so existieren 31 verschiedene Klassen von geflochtenen Friesornamenten.
Translationen, Gleitspiegelungen und Schraubungen sind nur in Richtung des Frieses möglich, da sie sonst aus dem Bereich des Frieses herausführen würden.

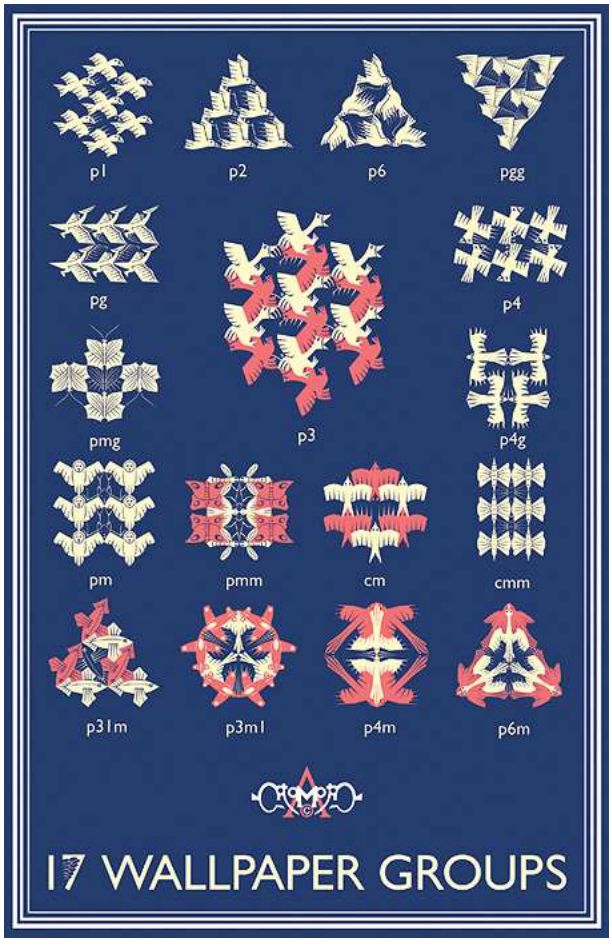
Ornamentgruppen und Parkettierungen

Schon schwieriger ist die komplette Aufzählung aller möglichen Ornamentgruppen.
Es gibt genau 17 Ornamentgruppen, die sogenannten 17 ebenen kristallographischen Gruppen.
Diese 17 Gruppen erlauben 93 verschiedene Parkettierungen der Ebene.
Wie die alternative Bezeichnung der Ornamentgruppen andeutet, waren es vor allem die Kristallographen, die erste Fortschritte bei der Untersuchung dieser Gruppen geliefert haben.
Die Aufzählung der 17 Gruppen ist ein Resultat von Fedorov (1890), dessen Beweis von Schoenflies 1891 vervollständigt wurde, und das 1924 von Polya wiederentdeckt wurde.
Das Parkettierungsproblem der Ebene besteht darin, dieselbe durch lauter deckungsgleiche Parkettsteine lückenlos und überlappungsfrei zu überdecken. Zur Klassifikation der angekündigten 93 Parkettierungen gibt es zwei Zugänge: einen algebraischen *und einen* topologischen *Ansatz.*
Der algebraische Zugang stellt auf die Symmetriegruppen der Parkette ab. Nach dem zitierten Satz von Fedorow gibt es 17 mögliche Symmetriegruppen für ebene Parkette.
Für später ist es nützlich, die Operation einer Ornamentgruppe H auf die Ebene E zu beschreiben. Dies geschieht am einfachsten durch Anwenden aller Gruppenelemente auf den Ursprung 0 in E. Man erhält als Bild ein Gitter, das wir mit G bezeichnen werden: $G = \{ g * 0 \mid g \in H \} \subset E$
Das Gitter liegt diskret in E. Nun gibt es für H in der Ebene E einen ausgezeichneten Bereich, den Fundamental- oder Dirichelet-Bereich.

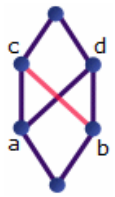
Sei dazu P irgendein Punkt der Ebene und g aus H so gewählt, dass $g * P \neq P$. Wir definieren den Bereich $H_{g;P} = \{x \in E \mid dist(x,p) < dist(x,g*p)\}$
Damit definieren wir den Fundamentalbereich von H auf E als
$F_H = \cap H_{g,P}$ wobei der Durchschnitt über alle $g \in H$ erfolgt.
Der Fundamentalbereich hat folgende charakteristische Eigenschaften:
$F(H) \cap g\,F(H) = \varnothing$ für alle $g \in H$
und die Vereinigung der topologischen Abschlüsse der g F(H) ist E, d.h. alle ihre Randpunkte seien inbegriffen.



Das zweite Unterscheidungsmerkmal für Parkette ist topologischer Natur. Man schaut sich an, in welcher Weise die Grenzlinien der Parkettsteine zu einem Netzwerk verknüpft sind. Dies führt auf die sogenannten Lavesnetze.
Sei P ein Parkett, $p \in P$ ein einzelner Punkt. Wir definieren die Zuordnung $p \rightarrow n(p)$, wo n(p) die Anzahl der Parkettsteine angibt, auf denen p liegt. Es gilt sicher immer $n(p) >= 1$. Ist $n(p) = 1$, so nennt man p einen inneren Punkt. Ein Randpunkt p, der in keiner Ecke des Parketts liegt, erfüllt $n(p) = 2$, während für alle Eckpunkte $n(p) >= 2$ gilt.
Damit definieren wir das Lavesnetz für P als $L = \{p \in P \mid n(p) >= 3\}$
Die Symmetriegruppe von P operiert auf L und führt es in sich über. Ein reguläres Parkett hat ja nur einen typischen Parkettstein. Somit können wir jedem Parkett P ein ausgezeichnetes Tupel von Zahlen zuordnen, welches das Lavesnetz L beschreibt: Es bezeichne $\varepsilon = \{e_1, ..., e_T\}$ die Menge der Ecken eines einzelnen Parkettsteins. Dann sei $e_j \rightarrow n_j = n(e_j)$ und $P = [n_1, ..., n_T]$ ist das dem Parkett mit seinem Lavesnetz zugeordnete ausgezeichnete r-Tupel. Mit diesem Instrument lässt sich folgendes Resultat beweisen:



Für reguläre Parkettierungen gibt es genau 11 nichtäquivalente Lavesnetze.



Verband
Sei M eine teilweise geordnete Menge mit der Ordnung ≤. M heißt verbandsgeordnete Menge oder Verband, wenn folgende Eigenschaften gelten
1) zu je zwei Elementen $a, b \in M$ existiert das Infimum inf(a, b)
2) zu je zwei Elementen $a, b \in N$ existiert das Supremum sup(a, b)
Damit besitzen dann auch endliche Teilmengen von M Infimum und Supremum. Der Beweis erfolgt durch vollständige Induktion.

Ist M selbst endlich, so besitzt M sowohl ein Minimum, das Ordnungsnull heißt, als auch ein Maximum, welches Ordnungseins genannt wird.
Jede kettengeordnete Menge ist ein Verband. Für jede zweielementige Teilmenge existieren dann Minimum und Maximum und sind mit dem Infimum und Supremum identische.

Beispiel: Das abgebildete Hassediagramm, ohne die hellrote Linie, veranschaulicht einen Verband. Es gilt d = sup(a, b) und a = inf(c, d).

Nimmt man die hellrote Linie hinzu, so ist die Verbandsstruktur zerstört, da sowohl c als auch d obere Schranken von a und b sind. Wegen ihrer Unvergleichbarkeit existiert jedoch d = sup(a, b) nicht.
Schreibweise: Um Gesetze mit Supremum und Infimum ohne Klammerung formulieren zu können, werden in Verbänden die Symbole $\vee$ für Supremum und $\wedge$ für Infimum verwendet.

$a \vee b = \sup(a, b)$ $\quad$ $a \wedge b = \inf(a, b)$

Mengenverband

Sei M eine beliebige Menge und P(M) ihre Potenzmenge. Unter einem Mengenverband $M \subseteq P(M)$ versteht man eine Teilmenge der Potenzmenge, die mit zwei Mengen A und B auch ihre Vereinigung $A \cup B$ und ihren Durchschnitt $A \cap B$ enthält.
Ein Mengenverband ist bezüglich der endlichern Durchschnitts- und Vereinigungsbildung abgeschlossen.
Jeder Mengenverband ist bezüglich der Inklusion $\subseteq$ ein Verband.

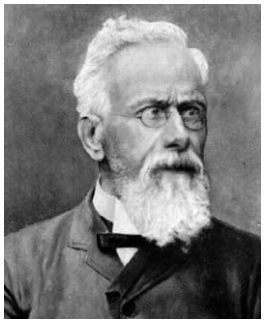
Geschichte der Algebra

Ursprünglich befasste sich die Algebra mit dem Lösen algebraischer Gleichungen, d.h. der Bestimmung der Nullstellen von Polynomen mit rationalen oder ganzzahligen Koeffizienten. In diesem Zusammenhang mussten immer neue Möglichkeiten entwickelt werden, was unter anderem auch zur Einführung der imaginären Zahlen führte. Wenn man z.B. die Nullstellen der Gleichung $x^2+1=0$ bestimmen will, reichen die reellen Zahlen nicht mehr aus, da das Quadrat einer reellen Zahl immer positiv oder Null ist und man nie auf Null kommt, wenn man zu einer nicht-negativen Zahl eins addiert.
Durch die Einführung der komplexen Zahlen, die sich aus reellen und imaginären Zahlen zusammensetzen, und der Hilfe der Analysis war es dann auch möglich den Fundamentalsatz der Algebra zu beweisen. Er besagt, dass in den komplexen Zahlen jede Gleichung in Linearfaktoren zerfällt, d.h. die Anzahl der Nullstellen mit dem Grad der Gleichung übereinstimmt. Auch versuchte man allgemeine Lösungen durch Radikale, was einfach verschachtelte Wurzelausdrücke sind, für Gleichungen zu finden.

Inzwischen befasst sich die Algebra jedoch nicht mehr nur damit Lösungen algebraischer Gleichungen zu finden, sondern mit der Theorie der Verknüpfungen auf einer Menge. Eine derartige Struktur einer Menge mit einer Verknüpfung nennt sich dann algebraische Struktur. Mit Hinzunahme besonderer Anforderungen an diese algebraischen Strukturen kommt man zu Begriffen wie Gruppe, Körper oder Vektorraum, deren Untersuchungen ein wichtiges Teilgebiet der Algebra bilden. Durch die Bildung unterschiedlicher Strukturen lässt sich auch die Algebra in verschiedene Teilgebiete unterteilen:
Die lineare Algebra behandelt vorwiegend die Theorie der Vektorräume über Körpern, die Körpertheorie, wie der Name schon sagt, die Theorie allgemeiner Körper und Körpererweiterungen, die Gruppentheorie und daneben gibt es noch weitere Bereiche (z.B. Ringtheorie, homologische Algebra, ...). Auch wird die Algebra in vielen anderen Gebieten eingebunden. In der Logik (Boolesche Algebra) oder der Zahlentheorie spielt sie eine wichtige Rolle.

Dass die Aufgabe der Algebra ursprünglich im Lösen von Gleichungen bestand, steckt schon in ihrem Namen, der aus dem Werk *al-kitab al-muhtasir fi hisab al-gabr wa-l-muqabala (Das kurzgefasste Buch über Rechnen mit Ergänzen und Zusammenfassen von Ausdrücken)* von dem arabischen Gelehrten al-Hwarizmi (rechte Abbildung oben) aus dem 9. Jahrhundert stammt. Aus dem Ausdruck al-gabr im Titel wurde später Algebra. Sich mit algebraischen Problemen zu befassen wurde jedoch schon im alten Ägypten und bei den Griechen begonnen. Die meisten algebraischen Methoden entstanden hierbei aus einem geometrischen Hintergrund. Weiterentwickelt wurde die Theorie dann zunächst hauptsächlich in China, Indien und der arabischen Welt, und erst im Mittelalter beschäftigte man sich in Europa wieder mit der Algebra.

Hier ist als wichtigster Vertreter Leonardo von Pisa, der auch unter dem Namen Leonardo Fibonacci (linke Abbildung, unten) bekannt ist, zu nennen. Im 16. Jahrhundert fand Niccolo Tartaglia (linke Abbildung, oben) dann die heute unter dem Namen Cardanosche Formel bekannte Lösung für Gleichungen dritten Grades und Ludovico Ferrari die für Gleichungen vierten Grades. Auch Isaac Newton und Leonard Euler leisteten wichtige Arbeiten.



Für den bis dato unbewiesenen Fundamentalsatz lieferte Carl-Friedrich Gauß gleich vier voneinander unabhängige Beweise, deren erster aus dem Jahre 1799 Gegenstand seiner Dissertation war.
Im Jahre 1824 war es Niels Henrik Abel, der beweisen konnte, dass Gleichungen fünften Grades nicht durch Radikale gelöst werden können. Den bedeutendsten Beitrag des 19. Jahrhundert zur Weiterentwicklung lieferte jedoch Evariste Galois durch die systematische Entwicklung einer Theorie, die heute unter dem Namen Galois-Theorie bekannt ist. Mit Hilfe dieser Theorie war es nun einfach zu beweisen, dass generell Gleichungen höheren als vierten Grades nicht durch Radikale lösbar sind. Dies ist auch Enrico Betti (1823-1892, rechte Abbildung unten) zu verdanken ist, der ab 1851 eine erste Präzisierung der Galois-Theorie mit einer Vervollständigung der Beweise präsentierte, da dies Galois aufgrund seiner kurzen Lebenszeit nicht möglich war.