Kapitel 3
Grundlegende algebraische Strukturen

Bisher sind wir so mit Zahlen und mit Gleichungen umgegangen, wie es bereits vor mehreren hundert oder sogar seit über zwei Tausend Jahren üblich war. Zu Beginn des zwanzigsten Jahrhunderts erhielt das Wort *Algebra* jedoch langsam eine andere Bedeutung: Im Mittelpunkt standen nicht mehr Gleichungen, sondern Strukturen.

Rechengesetze wie etwa das Kommutativgesetz der Addition oder Multiplikation waren natürlich schon lange bekannt; der neue Gesichtspunkt war, daß man völlig von der Art der Verknüpfung und den zu verknüpfenden Objekten abstrahierte und nur von den Rechenregeln ausging. Das führt zwar zu abstrakten und eher unanschaulichen Strukturen, hat aber den Vorteil, daß ein Satz, der nur unter Voraussetzung gewisser Regeln bewiesen wurde, in allen Zahl- und sonstigen Bereichen gilt, für die man diese Regeln nachweisen kann.

Wir beginnen mit dem Fall nur einer Verknüpfung, denn es gibt ja auch Gemeinsamkeiten zwischen beispielsweise Addition und Multiplikation, die auf diese Weise zusammen betrachtet werden können.

§ 1: Halbgruppen und Monoide

Fast alle Verknüpfungen, mit denen man in der Mathematik arbeitet, erfüllen das Assoziativgesetz; eine der wenigen Ausnahmen ist das Kreuzprodukt im $\mathbb{R}^3$: Hier ist beispielsweise

$$\begin{pmatrix}1\\0\\0\end{pmatrix} \times \left(\begin{pmatrix}1\\0\\0\end{pmatrix} \times \begin{pmatrix}0\\0\\1\end{pmatrix} \right) = \begin{pmatrix}1\\0\\0\end{pmatrix} \times \begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\end{pmatrix} ,$$

aber

$$\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\times\begin{pmatrix}1\\0\\0\end{pmatrix}\right)\times\begin{pmatrix}0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}\times\begin{pmatrix}0\\1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}\ .$$

Es bietet sich daher an, als einfachste Struktur eine zu definieren, bei der die Verknüpfung nur das Assoziativgesetz erfüllen muß:

Definition: Eine *Halbgruppe* ist eine Menge H zusammen mit einer Verknüpfung $*\colon H\times H\to H$, für die gilt:

$$a*(b*c)=(a*b)*c\quad\text{für alle } a,b,c\in H\ .$$

Beispiele von Halbgruppen sind die natürlichen Zahlen, sowohl bezüglich der Addition als auch bezüglich der Multiplikation, genauso natürlich die ganzen, rationalen und reellen Zahlen, $n\times m$-Matrizen bezüglich der Addition, $n\times n$-Matrizen bezüglich der Multiplikation und viele mehr. Vor allem in der Informatik populär sind sogenannte Worthalbgruppen; hier geht man aus von einem Alphabet A und betrachtet die Menge H aller nichtleerer Folgen von Elementen aus A; Verknüpfung ist das Hintereinanderschreiben:

$$\text{hintereinander}*\text{schreiben}=\text{hintereinanderschreiben}\ .$$

Wenn man in einer Halbgruppe ein Produkt von n Elementen $a_1,\dots,a_n$ berechnen will, muß man durch Klammerung die Reihenfolge der Rechenoperationen festlegen, bei vier Elementen etwa

$$a_1*\big(a_2*(a_3*a_4)\big),\quad \big((a_1*(a_2*a_3)\big)*a_4,\quad (a_1*a_2)*(a_3*a_4)$$

oder auf verschiedene andere Weisen. Wir definieren das Produkt

$$p_n=\prod_{i=1}^{n}a_i$$

von n Elementen $a_1,\dots,a_n$ für $n\geq 1$ rekursiv durch

$$\prod_{i=1}^{1}a_i=a_1\quad\text{und}\quad\prod_{i=1}^{n+1}a_i=\left(\prod_{i=1}^{n}a_i\right)*a_{n+1}\ .$$

Lemma: Das Produkt von n Elementen $a_1, a_2, \ldots, a_n$ (in dieser Reihenfolge) ist unabhängig von der Klammerung stets gleich $\prod_{i=1}^{n} a_i$.

Den *Beweis* führen wir durch vollständige Induktion: Für $n = 1$ und $n = 2$ sind alle Klammern überflüssig und können daher weggelassen werden; somit gibt es hier nichts zu beweisen. Sei also $n > 2$. Wir gehen aus von einem irgendwie geklammerten Produkt und betrachten die Operation, die als letzte ausgeführt wird. Diese verknüpft für ein $m < n$ ein irgendwie geklammertes Produkt der Elemente $a_1, \ldots, a_m$ mit einem irgendwie geklammerten Produkt der Elemente $a_{m+1}, \ldots, a_n$. Nach Induktionsannahme ist das erste Produkt gleich $p_m \underset{\text{def}}{=} \prod_{i=1}^{m} a_i$, das zweite ist $q_{nm} \underset{\text{def}}{=} \prod_{i=m+1}^{n} a_i$. Nach Definition ist $q_{nm} = q_{n-1,m} * a_n$, also ist $p_m * q_{nm} = p_m * (q_{n-1,m} * a_n) = (p_m * q_{n-1,m}) * a_n$. Da $p_m * q_{n-1,m}$ ein Produkt von $n - 1$ Faktoren ist, zeigt die Induktionsannahme, daß es den Wert p_{n-1} hat; somit ist $p_m * q_{nm} = p_{n-1} * a_n = p_n$. Damit ist das Lemma bewiesen. ∎

In einer Halbgruppe muß es kein Element geben, das sich bei Verknüpfung mit jedem anderen Element „neutral“ verhält wie etwa die Null bei der Addition. Wenn es so ein Element gibt, reden wir von einem *Monoid:*

Definition: Eine Halbgruppe H mit Verknüpfung $*$ heißt *Monoid,* wenn es ein Element $e \in H$ gibt, so daß $e * h = h * e = h$ ist für alle $h \in H$.

So sind beispielsweise die natürlichen Zahlen bezüglich der Addition *kein* Monoid, da $0 \notin \mathbb{N}$, sie sind aber ein Monoid bezüglich der Multiplikation, da $1 \in \mathbb{N}$. Die Menge $\mathbb{N}_0$ ist sowohl bezüglich der Addition als auch bezüglich der Multiplikation ein Monoid, da sie sowohl die Null als auch die Eins enthält. Eine Worthalbgruppe wird zum Monoid, wenn wir das leere Wort zulassen; es ist dadurch charakterisiert, daß es keinen einzigen Buchstaben enthält, also eine leere Zeichenkette ist.

In der Definition eines Monoids wurde nur gefordert, daß es *mindestens* ein Element e gibt, für das $h * e = e * h = h$ ist; tatsächlich ist e, wenn es existiert, durch die Verknüpfung eindeutig festgelegt:

Lemma: Erfüllt das Element $n \in H$ die Gleichung $n * h = h * n = h$ für alle $h \in H$, so ist $n = e$.

Beweis: Setzen wir speziell $h = e$, folgt, daß $n*e = e$ ist. Nach Definition eines Monoids ist aber $n * e = n$, so daß $n = e$ sein muß. ∎

§2: Gruppen

Außer neutralen Elementen haben wir oft auch noch inverse Elemente; ein Monoid, in dem es Inverse gibt, bezeichnen wir als *Gruppe.* Da Gruppen erheblich wichtiger sind als Halbgruppen und Monoide, seien sie, obwohl sie bereits aus der Linearen Algebra bekannt sein sollten, ausführlich definiert:

Definition: *a)* Eine *Gruppe* ist eine Menge G zusammen mit einer Verknüpfung $*$: $G * G \to G$, für die gilt

1.) $(x * y) * z = x * (y * z)$ für alle $x, y, z \in G$.
2.) Es gibt ein Element $e \in G$, das Neutralelement, so daß für alle $x \in G$ gilt $e * x = x * e = x$.
3.) Zu jedem $x \in G$ gibt es ein $x' \in G$, so daß $x * x' = x' * x = e$ ist.

Die Gruppe heißt *kommutativ* oder *abelsch*, wenn zusätzlich noch gilt

4.) $x * y = y * x$ für alle $x, y \in G$.

b) Eine Teilmenge $U \subseteq G$ heißt *Untergruppe* von G, in Zeichen $U \leq G$, wenn sie bezüglich der Operation $*$ selbst eine Gruppe ist.

Unter den bekannten Zahlbereichen sind $\mathbb{N}$ und $\mathbb{N}_0$ weder bezüglich der Addition noch bezüglich der Multiplikation Gruppen, $\mathbb{Z}$ ist eine Gruppe bezüglich der Addition, nicht aber der Multiplikation. Die Körper $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ (und auch alle anderen) sind ebenfalls additive Gruppen; wenn man die Null entfernt, werden sie zu multiplikativen Gruppen. Bezüglich der Addition ist $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, bezüglich der Multiplikation $\mathbb{Q} \setminus \{0\} \leq \mathbb{R} \setminus \{0\} \leq \mathbb{C} \setminus \{0\}$.

Als weiteres Beispiel für Untergruppen können wir die sämtlichen Untergruppen der (additiven) Gruppe $\mathbb{Z}$ bestimmen:

Lemma: Die Untergruppen von $\mathbb{Z}$ sind genau die Mengen

$$m\mathbb{Z} \underset{\text{def}}{=} \{mz \mid z \in \mathbb{Z}\} \quad \text{mit} \quad m \in \mathbb{N}_0 \,.$$

Beweis: Natürlich sind alle diese Mengen Untergruppen, denn

$$mz_1 + mz_2 = m(z_1 + z_2) \quad \text{und} \quad (-mz) + mz = 0 \,.$$

Umgekehrt sei $U \leq \mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$. Falls U nur aus der Null besteht, ist $U = \{0\} = 0\mathbb{Z}$. Andernfalls enthält U eine kleinste positive Zahl m, denn zu jedem negativen x muß U auch dessen Inverses $-x$ enthalten.

Nun sei x ein beliebiges Element von U. Nach dem erweiterten EUKLIDischen Algorithmus gibt es $\alpha, \beta \in \mathbb{Z}$, so daß ggT$(m, x) = \alpha m + \beta x$ ist. Wegen $m, x \in U$ liegt also auch der ggT von m und x in U. Er ist einerseits ein positiver Teiler von m, andererseits ist m die kleinste positive Zahl in U. Also muß er gleich m sein, d.h. x ist ein Vielfaches von m. ∎

Mit den Gruppen $\mathbb{Z}/m\mathbb{Z}$ werden wir es häufiger zu tun haben; daher vereinbaren wir die Abkürzung $\mathbb{Z}/m \underset{\text{def}}{=} \mathbb{Z}/m\mathbb{Z}$. In einigen Büchern wird auch einfach $\mathbb{Z}_m$ geschrieben; das möchte ich vermeiden, da es im Primzahlfall zu Verwechslungen mit den sogenannten p-adischen Zahlen führen kann.

Da eine Gruppe insbesondere auch ein Monoid ist, gibt es auch in einer Gruppe genau ein Neutralelement. Auch die inversen Elemente sind eindeutig bestimmt, denn ist $x' * x = x * x' = e$ und $x'' * x = x * x'' = e$, so ist

$$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x'' \,.$$

Im folgenden werden wir, wenn keine Verwechslung zu befürchten ist, die Gruppenoperation meist weglassen und statt $x * y$ einfach xy schreiben. Wenn die Gruppenoperation als Addition oder Multiplikation aufgefaßt werden kann, schreiben wir $x+y$ *bzw.* $x \cdot y$, wobei der Malpunkt ebenfalls meist weggelassen wird. Das eindeutig bestimmte Inverse bezeichnen wir meist mit x^{-1}; wenn die Gruppe additiv geschrieben wird,

schreiben wir $-x$. In additiven Gruppen wird das Neutralelement meist als 0 geschrieben, in multiplikativen als 1.

Damit eine Teilmenge $U \subseteq G$ eine Untergruppe ist, reicht es offensichtlich, daß das Produkt zweier Elemente $x, y \in U$ wieder in U liegt, außerdem auch das Neutralelement und zu jedem $x \in U$ das Inverse, denn das Assoziativgesetz gilt für alle Elemente von G, also erst recht für alle Elemente der Teilmenge U. Auf die Bedingung $e \in U$ können wir verzichten, falls U nicht leer ist, denn dann liegt zu $x \in U$ auch x^{-1} in U und damit auch $e = xx^{-1}$.

Die obigen Bedingungen können wir etwas kompakter formulieren mit Hilfe des sogenannten Komplexprodukts:

Definition: Sind $A, B \subseteq G$ zwei Teilmengen von G, so bezeichnen wir

$$AB = \{ab \mid a \in A \wedge b \in B\}$$

als das *Komplexprodukt* von A und B. Besteht $A = \{a\}$ nur aus einem Element a, schreiben wir statt AB auch kurz aB, entsprechend auch Ab, falls $B = \{b\}$. Außerdem definieren wir

$$A^{-1} = \{a^{-1} \mid a \in A\}$$

als die Menge aller inverser Elemente zu den Elementen von A.

Damit werden die beiden ersten Bedingungen für eine Untergruppe zu $UU \subseteq U$ und $U^{-1} \subseteq U$; als dritte Bedingung können wir entweder $e \in U$ oder $U \neq \emptyset$ fordern.

Wenn wir uns für die Lösung von Gleichungen interessieren, unterscheiden sich Gruppen von Halbgruppen und Monoiden durch die folgende

Kürzungsregel: Gilt für drei Elemente a, x, y einer Gruppe die Gleichung $ax = ay$ oder $xa = ya$, so ist $x = y$.

Beweis: Wenn wir die Gleichung $ax = ay$ von links mit a^{-1} multiplizieren, erhalten wir $a^{-1}ax = a^{-1}ay$, also $x = y$. Bei $xa = ya$ müssen wir entsprechend von rechts mit a^{-1} multiplizieren. ∎

Alternativ folgt diese Regel aus dem etwa allgemeineren

Lemma: Für jede Gruppe G und jedes Element $a \in G$ sind die Abbildung $x \mapsto ax$ und $x \mapsto xa$ bijektiv.

Beweis: Offensichtlich sind die Abbildungen $y \mapsto a^{-1}y$ und $y \mapsto ya^{-1}$ Umkehrabbildungen.

■

Korollar: In einer Gruppe G haben die Gleichungen $ax = b$ und $ya = b$ für jedes Paar von Elementen $a, b \in G$ genau eine Lösung.

■

Diese Lösungen lassen sich natürlich auch konkret angeben: $x = a^{-1}b$ und $y = ba^{-1}$.

Oft lösen wir in der Mathematik Probleme dadurch, daß wir sie auf ein oder mehrere einfachere Probleme in anderen Zahlbereichen zurückführen: Wenn wir beispielsweise eine Rechnung in ganzen Zahlen durchführen müssen, von der wir zeigen können, daß das Ergebnis einen Betrag von höchstens M hat, reicht es, wenn wir die entsprechende Rechnung modulo einer Primzahl p durchführen, die mindestens gleich $2M + 1$ ist, denn dann sind alle $2M + 1$ Zahlen zwischen $-M$ und M auch modulo p verschieden. Alternativ könnten wir auch modulo verschiedener kleinerer Primzahlen p_i rechnen und die Ergebnisse nach dem chinesischen Restesatz zusammensetzen; falls das Produkt der p_i größer ist als $2M + 1$, kennen wir auch dann das Ergebnis.

Um solche Methoden abstrakt anwenden zu können, brauchen wir nicht nur Strukturen wie Gruppen, Monoide und Halbgruppen, sondern auch Abbildungen zwischen solchen Strukturen, die mit den Verknüpfungen kompatibel sind. Diese werden als *Homomorphismen* bezeichnet. Die folgende Definition könnte wörtlich übernommen werden für Halbgruppen und Monoide; da wir es aber in dieser Vorlesung kaum je mit Halbgruppen zu tun haben werden, die keine Gruppen sind, beschränke ich mich auf diese:

Definition: *a)* Eine Abbildung $\varphi: G \to H$ zwischen zwei Gruppen G und H mit Verknüpfungen $*$ und $\times$ heißt (Gruppen-)*Homomorphismus,* falls für alle $x, y \in G$ gilt: $\varphi(x * y) = \varphi(x) \times \varphi(y)$.

b) Ein $\left\{\begin{array}{c}\textit{Monomorphismus}\\ \textit{Epimorphismus}\\ \textit{Isomorphismusa}\end{array}\right\}$ ist ein $\left\{\begin{array}{c}\textit{injektiver}\\ \textit{surjektiver}\\ \textit{bijektiver}\end{array}\right\}$ Homomorphismus.
Zwei Gruppen G und H heißen *isomorph,* in Zeichen $G \cong H$, wenn es einen Isomorphismus $\varphi\colon G \to H$ gibt.
c) Ist $G = H$, bezeichnen wir einen Homomorphismus von G nach G auch als *Endomorphismus* und einen Isomorphismus als *Automorphismus.*
d) Das *Bild* eines Homomorphismus $\varphi\colon G \to H$ ist

$$\operatorname{Bild}\varphi \underset{\text{def}}{=} \varphi(G) = \{\varphi(x) \mid x \in G\}\,;$$

sein *Kern* ist

$$\operatorname{Kern}\varphi \underset{\text{def}}{=} \{x \in G \mid \varphi(x) = e'\}\,,$$

wobei e' das Neutralelement von H bezeichnet.

Lemma: Für jeden Homomorphismus $\varphi\colon G \to H$ gilt:
a) Für die Neutralelemente $e \in G$ und $e' \in H$ ist $\varphi(e) = e'$.
b) Für alle $x \in G$ ist $\varphi(x)^{-1} = \varphi(x^{-1})$
c) $\operatorname{Kern}\varphi$ ist eine Untergruppe von G und $\operatorname{Bild}\varphi$ ist eine Untergruppe von H.

Beweis: Nach Definition eines Homomorphismus ist

$$\varphi(e)\varphi(e) = \varphi(ee) = \varphi(e)\,;$$

außerdem ist natürlich auch $e'\varphi(e) = \varphi(e)$. Da $x\varphi(e) = \varphi(e)$ in einer Gruppe genau eine Lösung hat, muß $\varphi(e) = e'$ sein. Genauso muß $\varphi(x^{-1}) = \varphi(x)^{-1}$ sein, denn $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e) = e'$ und auch $\varphi(x)^{-1}\varphi(x) = e'$.

Für zwei Elemente $x, y \in \operatorname{Kern}\varphi$ ist $\varphi(xy) = \varphi(x)\varphi(y) = e'e' = e'$ und $\varphi(x^{-1}) = \varphi(x)^{-1} = e'^{-1} = e'$, so daß auch Produkte und Inverse wieder im Kern liegen. Da $\varphi(e) = e'$, liegt auch e im Kern, also bildet dieser eine Untergruppe. Auch beim Bild liegen Produkte und Inverse wegen $\varphi(x)\varphi(y) = \varphi(xy)$ und $\varphi(x)^{-1} = \varphi(x^{-1})$ wieder im Bild, und da G als Gruppe nicht leer ist, ist auch $\operatorname{Bild}\varphi \neq \emptyset$.

■

Die Abbildungen $x \mapsto ax$ und $x \mapsto xa$ sind für $a \neq e$ natürlich keine Homomorphismen; ein Homomorphismus bildet schließlich das Neutralelement ab auf das Neutralelement. Um dies zu erreichen, können wir die Multiplikation von rechts mit a kombinieren mit der Multiplikation von links mit a^{-1}; wir betrachten also die Abbildung $x \mapsto a^{-1}xa$. Dann wird natürlich e auf e abgebildet, und wir haben auch einen Homomorphismus, denn für alle $x, y \in G$ ist

$$a^{-1}(xy)a = a^{-1}\big(x(aa^{-1})y\big)a = (a^{-1}xa)(a^{-1}ya)\,.$$

Die Abbildung ist auch bijektiv, also ein Automorphismus von G, denn sowohl die Linksmultiplikation mit a^{-1} als auch die Rechtsmultiplikation mit a sind bijektiv, also auch ihre Hintereinanderausführung.

Definition: Die Abbildung von G nach G, die jedem $x \in G$ das Element $x^g \underset{\text{def}}{=} g^{-1}xg$ zuordnet, heißt *Konjugation* mit $g \in G$. Ein Automorphismus $\varphi\colon G \to G$ heißt *innerer Automorphismus*, wenn es ein $g \in G$ gibt, so daß $\varphi(x) = x^g$ für alle $x \in G$.

Man beachte, daß die Konjugation genau die gleiche Gestalt hat, wie die aus der Linearen Algebra bekannte Konjugation von Matrizen: Auch dort betrachtet man zu einer Matrix M und einer invertierbaren Matrix B, der Matrix des Basiswechsels, die Matrix $B^{-1}MB$. Falls auch M invertierbar ist, stimmt dies mit der Konjugation in der Gruppe der invertierbaren $n \times n$-Matrizen überein.

Zu einem Vektorraum V betrachtet man in der Linearen Algebra auch seine Untervektorräume U und die Faktorräume V/U; wir wollen etwas analoges auch für Gruppen definieren:

Definition: Die Linksnebenklassen einer Untergruppe $U \leq G$ sind die Mengen $aU = \{au \mid u \in U\}$, die Rechtsnebenklassen entsprechend $Ua = \{ua \mid u \in U\}$.

Für $a \in U$ ist wegen der Bijektivität der Multiplikation mit a natürlich $aU = Ua = U$.

Wenn zwei Nebenklassen aU und bU nichtleeren Durchschnitt haben, gibt es Elemente $u, v \in U$, so daß $au = bv$ ist. Dann ist auch $a = bvu^{-1}$,

also $aU = bvu^{-1}U = bU$, da $vu^{-1} \in U$. Falls $aU \neq bU$ ist also $aU \cap bU = \emptyset$, genauso ist auch $Ua \cap Ub = \emptyset$ falls $Ua \neq Ub$.

Nun nehmen wir an, die Gruppe G sei endlich. Dann ist natürlich erst recht jede Untergruppe $U \leq G$ endlich, und es gibt nur endlich viele Nebenklassen.

Da die Multiplikation mit einem Gruppenelement eine injektive Abbildung ist, hat sowohl aU als auch Ua für jedes $a \in G$ dieselbe Elementanzahl, nämlich die von U. Insbesondere ist also die Anzahl der Linksnebenklassen gleich der der Rechtsnebenklassen.

Dies gilt auch, wenn G (und eventuell U) unendlich sind, denn da jedes Element einer Gruppe ein eindeutig bestimmtes Inverses hat, ist auch die Abbildung, die jedem Element von G dessen Inverses zuordnet, bijektiv, und sie ordnet der Linksnebenklasse aU die Rechtsnebenklasse Ua^{-1} zu und umgekehrt. Damit gibt es auch hier eine Bijektion zwischen der Menge der Linksnebenklassen und der der Rechtsnebenklassen: Sind a_iU mit i aus irgendeiner Indexmenge I die sämtlichen Linksnebenklassen, sind die Ua_i^{-1} die sämtlichen Rechtsnebenklassen. Wenn wir von der Anzahl der Nebenklassen sprechen, ist es also egal, ob wir Links- oder Rechtsnebenklassen meinen.

Definition: Falls die Untergruppe $U \leq G$ der Gruppe G nur eine endliche Anzahl n von Nebenklassen hat, sagen wir, U habe den Index n, in Zeichen $[G : U] = n$. Falls es unendlich viele Nebenklassen gibt, sagen wir, U habe unendlichen Index.

Im Falle einer endlichen Gruppe G ist auch die Anzahl $[G : U]$ der Nebenklassen endlich. Jede dieser Nebenklassen hat genau so viele Elemente wie U und jedes Element von G liegt in genau einer Nebenklasse; damit folgt der

Satz von Lagrange: Für eine endliche Gruppe G und eine Untergruppe $U \leq G$ ist $|G| = [G : U] \cdot |U|$. Insbesondere sind die Ordnung und der Index von U Teiler der Ordnung von G.

■

JOSEPH-LOUIS LAGRANGE (1736–1813) wurde als GIUSEPPE LODOVICO LAGRANGIA in Turin geboren und studierte dort zunächst Latein. Erst eine alte Arbeit von HALLEY über algebraische Methoden in der Optik weckte sein Interesse an der Mathematik, woraus ein ausgedehnter Briefwechsel mit EULER entstand. In einem Brief vom 12. August 1755 berichtete er diesem unter anderem über seine Methode zur Berechnung von Maxima und Minima; 1756 wurde er, auf EULERs Vorschlag, Mitglied der Berliner Akademie; zehn Jahre später zog er nach Berlin und wurde dort EULERs Nachfolger als mathematischer Direktor der Akademie. 1787 wechselte er an die Pariser Académie des Sciences, wo er bis zu seinem Tod blieb und unter anderem an der Einführung des metrischen Systems beteiligt war. Seine Arbeiten umspannen weite Teile der Analysis, Algebra und Geometrie.

Ist V ein Vektorraum und $U \leq V$ ein Untervektorraum, so können wir die Menge aller Nebenklassen (bei denen wir hier wegen der Kommutativität der Vektoraddition nicht zwischen links und rechts unterscheiden müssen) wieder zu einem Vektorraum machen mit der Addition $(v + U) + (w + U) = (v + w) + U$ Wir wollen uns überlegen, ob wir auch die Menge aller Links- oder Rechtsnebenklassen einer Untergruppe zu einer Gruppe machen können. Da beide Fälle völlig analog zueinander sind, beschränken wir uns auf Linksnebenklassen.

Falls diese eine Gruppe bilden bezüglich des Komplexprodukts, muß es zu $a, b \in G$ ein $c \in G$ geben, so daß $(aU)(bU) = cU$ ist. Da a in aU liegt und b in bU, liegt ab in cU, d.h. $cU = (ab)U$. Somit ist $(aU)(bU) = (ab)U$. Zu beliebigen Elementen $u, v \in U$ muß es also ein $w \in U$ geben, so daß $(au)(bv) = (ab)w$ ist. Speziell für $v = 1$ folgt, daß es zu jedem $u \in U$ ein $w \in U$ geben muß, so daß $aub = abw$ ist. Multiplizieren wir dies von links mit a^{-1}, folgt daß $ub = bw$ sein muß. Für jedes $u \in U$ muß es also ein $w \in U$ geben, so daß $ub = bw$ ist, d.h. die Linksnebenklasse von b muß gleich der Rechtsnebenklasse von b sein.

Wir können die Gleichung $ub = bw$ durch Linksmultiplikation mit b^{-1} auch umschreiben zu $b^{-1}ub = w$; damit haben wir die Bedingung, daß jedes Element von U durch Konjugation mit einem beliebigen $b \in G$ wieder auch ein Element von U abgebildet wird, daß U also unter der

Konjugation mit b auf sich selbst abgebildet wird.

Dies gilt aber nicht für jede Untergruppe: Nehmen wir etwa für G die Gruppe $\mathfrak{S}_4$ aller bijektiver Abbildungen der Menge $\{1,2,3,4\}$ auf sich selbst und für U die Untergruppe, die 4 festläßt, also im wesentlichen die Gruppe $\mathfrak{S}_3$ der Abbildungen von $\{1,2,3\}$ auf sich selbst, so liegt der Dreierzyklus (1 2 3) natürlich in der Untergruppe, aber sein Konjugiertes unter der Transposition (1 4), die Permutation

$$(1\ 4)^{-1}(1\ 2\ 3)(1\ 4) = (1\ 4)(1\ 2\ 3)(1\ 4) = (1\ 4\ 2\ 3)(1\ 4) = (2\ 3\ 4)$$

liegt nicht in U.

Die Menge der Links- oder Rechtsnebenklassen von $U \leq G$ kann also höchstens dann mit der offensichtlichen Verknüpfung zu einer Gruppe gemacht werden, wenn die Linksnebenklasse eines jeden Elements gleich seiner Rechtsnebenklasse ist oder, äquivalent, wenn jeder innere Automorphismus von G die Untergruppe U auf sich selbst abbildet.

In diesem Fall bilden die Nebenklassen auch tatsächlich eine Gruppe bezüglich des Komplexprodukts, denn

$$(aU)(bU) = (aU)(Ub) = a\big((UU)b\big) = a(Ub) = a(bU) = (ab)U\ .$$

Definition: *a)* Eine Untergruppe $N \leq G$ einer Gruppe G heißt *Normalteiler* von G, in Zeichen $N \trianglelefteq G$, wenn für jedes $n \in N$ und jedes $g \in G$ das konjugierte Element $n^g = g^{-1}ng$ in N liegt.
b) Die von den Nebenklassen $gN = Ng$ gebildete Gruppe heißt *Faktorgruppe* und wird mit G/N bezeichnet.

Nach dem folgenden Lemma sind die Normalteiler genau die Kerne der Homomorphismen:

Lemma: Der Kern eines jeden Homomorphismus $\varphi\colon G \to H$ ist ein Normalteiler von G, und umgekehrt gibt es auch zu jedem Normalteiler $N \trianglelefteq G$ einen Homomorphismus $\varphi\colon G \to H$ mit Kern N.

Beweis: Ist $n \in \operatorname{Kern}\varphi$ und $g \in G$, so ist

$$\begin{aligned}\varphi(n^g) = \varphi(g^{-1}ng) &= \varphi(g^{-1})\varphi(n)\varphi(g) = \varphi(g^{-1})e\varphi(g)\\ &= \varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e') = e\ ,\end{aligned}$$

wobei $e' \in G$ das Neutralelement von G bezeichnet. Somit liegt n^g in Kern φ, was die Normalität beweist.

Umgekehrt ist jeder Normalteiler $N \trianglelefteq G$ beispielsweise Kern der Restklassenabbildung $\varphi: G \to G/N$.

■

Homomorphiesatz: Für jedem Homomorphismus $\varphi: G \to H$ ist

$$G/\operatorname{Kern}\varphi \cong \operatorname{Bild}\varphi\,.$$

Beweis: Sei $N = \operatorname{Kern}\varphi$. Wir definieren eine Abbildung $\overline{\varphi}$ von G/N nach H, die die Nebenklasse Nx auf $\varphi(x)$ abbildet. Sie ist wohldefiniert, denn ist $Nx = Ny$, so liegt y in Nx, läßt sich also in der Form $y = nx$ schreiben mit $n \in N = \operatorname{Kern}\varphi$. Somit ist

$$\varphi(y) = \varphi(nx) = \varphi(n)\varphi(x) = e'\varphi(x) = \varphi(x)s\,.$$

Da φ ein Homomorphismus ist, ist auch $\overline{\varphi}$ einer, und $\overline{\varphi}$ ist injektiv, denn ist $\overline{\varphi}(Nx) = \overline{\varphi}(Ny)$, so ist $\varphi(x) = \varphi(y)$, also $\varphi(xy^{-1}) = e'$. Also ist $xy^{-1} \in N$ und damit $x \in Ny$, d.h. $Nx = Ny$. Das Bild von $\overline{\varphi}$ ist natürlich gleich dem von φ; schränken wir $\overline{\varphi}$ ein zu einer Abbildung von G/N nur nach $\operatorname{Bild}\varphi$ statt nach ganz H, haben wir daher einen bijektiven Homomorphismus, d.h. einen Isomorphismus.

■

Nach diesen vielen Begriffen, Lemmata und Sätzen wird es Zeit, endlich mehr Beispiele von Gruppen zu betrachten. Am einfachsten sind Gruppen, die von einem Element erzeugt werden:

Definition: Eine Gruppe G heißt *zyklisch*, wenn es ein $g \in G$ gibt, so daß sich jedes Element $x \in G$ als $x = g^n$ schreiben läßt mit einem $n \in \mathbb{Z}$. Dabei soll g^n für $n \in \mathbb{N}$ das Produkt von n Faktoren g bezeichnen und für $n < 0$ das von $-n$ Faktoren g^{-1}; g^0 ist natürlich das Neutralelement.

Lemma: Eine zyklische Gruppe G ist entweder isomorph zu $\mathbb{Z}$ oder es gibt ein $m \in \mathbb{N}$, so daß $G \cong \mathbb{Z}/m$.

Beweis: Wir betrachten die Abbildung

$$\varphi\colon \begin{cases} \mathbb{Z} \to G \\ n \mapsto g^n \end{cases}$$

Nach Definition einer zyklischen Gruppe ist sie surjektiv, und auf Grund des allgemeinen Assoziativgesetzes ist sie auch ein Homomorphismus. Falls sie auch injektiv ist, folgt $G \cong \mathbb{Z}$; andernfalls ist ihr Kern als Untergruppe von $\mathbb{Z}$ von der Form $\operatorname{Kern}\varphi = m\mathbb{Z}$ mit einem $m \in \mathbb{N}$. Nach dem Homomorphiesatz ist dann $G \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m$. ∎

Interessante Beispiele von Gruppen liefern auch die Symmetrien geometrischer Objekte. Betrachten wir etwa ein Rechteck mit Ecken (im Uhrzeigersinn) A, B, C, D, so gibt es (abgesehen von der identischen Abbildung id) drei Symmetrien: Die Spiegelung σ an der gemeinsamen Mittelsenkrechten der Strecken $\overline{AB}$ und $\overline{DC}$, die A mit B und C mit D vertauscht, die Spiegelung τ an der gemeinsamen Mittelsenkrechten von $\overline{AD}$ und $\overline{BC}$, die A mit D und B mit C vertauscht, und die Punktspiegelung ρ am Mittelpunkt des Rechtecks, die die gegenüberliegenden Ecken A, C sowie B, D miteinander vertauscht. Offensichtlich ist $\sigma^2 = \tau^2 = \rho^2 = \mathrm{id}$; die Gruppe ist also nicht zyklisch, da es kein Element mit vier verschiedenen Potenzen gibt. Indem man den Effekt auf die Ecken betrachtet, rechnet man auch leicht nach, daß $\sigma\tau = \tau\sigma = \rho$ ist, und daraus folgen die Gleichungen $\rho\sigma = \sigma\rho = \tau$ und $\rho\tau = \tau\rho = \sigma$. Die Verknüpfung in dieser Gruppe ist also durch die folgende Tafel gegeben:

	id	σ	τ	ρ
id	id	σ	τ	ρ
σ	σ	id	ρ	τ
τ	τ	ρ	id	σ
ρ	ρ	τ	σ	id

Die Gruppe heißt KLEINsche Vierergruppe V_4 nach dem deutschen Mathematiker FELIX KLEIN (1849–1925), der sich intensiv mit diskreten Symmetriegruppen beschäftigt hatte. Die Mengen $\{\sigma, \mathrm{id}\}$, $\{\tau, \mathrm{id}\}$ und

$\{\rho, \mathrm{id}\}$ sind Untergruppen und, da die Gruppe abelsch ist, auch Normalteiler von V_4. Weitere Untergruppen, abgesehen von den trivialen Untergruppen $\{\mathrm{id}\}$ und V_4 selbst, gibt es nicht, denn jede solche Untergruppe muß nach LAGRANGE die Ordnung zwei haben, besteht also aus der Identität und einem weiteren Element, dessen Quadrat die Identität ist.

Falls das Rechteck ein Quadrat ist, gibt es noch weitere Symmetrien, zum Beispiel die Drehung δ um 90° und ihre Potenzen. δ^2 ist die Punktspiegelung ρ, und $\delta^3 = \delta^{-1}$ ist die Drehung um -90°. Außerdem gibt es noch die Spiegelungen an den beiden Diagonalen, so daß die Gruppe acht Elemente enthält.

Allgemein wird die Symmetriegruppe des regelmäßigen n-Ecks als *Diedergruppe* D_n bezeichnet; die Symmetriegruppe des Quadrats ist also die Diedergruppe D_4. (Ein Polyeder ist es Körper, der von ebenen Polygonen begrenzt wird, der Würfel als Hexaeder etwa von sechs Quadraten und das Oktaeder von acht Dreiecken. Bei nur zwei Flächen entsteht etwas ebenes, ein *Dieder,* gesprochen Di-eder.)

Zur Untersuchung der allgemeinen Diedergruppen, identifizieren wir die reelle Ebene mit der komplexen Zahlenebene und betrachten das regelmäßige n-Eck mit Ecken

$$E_k = e^{2k\pi i/n}, \quad k = 0, \ldots, n-1\,.$$

Die Drehung δ um den Winkel $360^\circ/n$ können wir dann beschreiben durch die Multiplikation mit $\zeta = e^{2\pi i/n}$, seine Potenzen durch die mit $\zeta^k = e^{2k\pi i/n}$. Wenn n gerade ist, gehört dazu für $k = n/2$ auch die Multiplikation mit $e^{\pi i} = -1$, also die Punktspiegelung am Nullpunkt. Ansonsten haben für gerade $n = 2m$ noch die Spiegelungen an den Geraden durch zwei gegenüberliegende Ecken E_k und E_{k+m}, $k = 0, \ldots, m-1$, und die Spiegelungen an den Geraden durch die Mittelpunkte zweier gegenüberliegender Seiten. Die Steigungswinkel der Geraden durch zwei gegenüberliegende Ecken sind $k \cdot 360^\circ/n$, die durch zwei Kantenmittelpunkte liegen jeweils dazwischen und haben daher die Steigungen $(k + \frac{1}{2}) \cdot 360^\circ/n$. Insgesamt haben wir somit Spiegelungen σ_k an den n Geraden mit Steigungswinkeln $k \cdot 180^\circ/n$ für $k = 0, \ldots, n-1$. Für ungerade n haben wir keine Punktsymmetrie, aber auch Spiegelungen

an den Geraden der gerade aufgelisteten Steigungswinkel; der einzige Unterschied zum geraden Fall besteht darin, daß nun jede dieser Geraden durch eine Ecke und den gegenüberliegenden Kantenmittelpunkt geht. Insgesamt gibt es also in beiden Fällen $2n$ Symmetrieoperationen.

Die Potenzen der Drehung δ bilden eine zyklische Untergruppe der Ordnung n; diese ist ein Normalteiler. Dies kann man leicht direkt nachrechnen durch Konjugation mit einer der Drehungen, es geht aber auch einfacher ganz allgemein und abstrakt:

Lemma: Ist G eine (nicht notwendigerweise endliche) Gruppe und U eine Untergruppe vom Index zwei, so ist U ein Normalteiler.

Beweis: Da $[G : U] = 2$ ist, hat U genau zwei Nebenklassen. Eine davon ist natürlich U selbst, und die andere besteht aus den übrigen Elementen von G. Für jedes $a \notin U$ ist daher $Ua = aU = G \setminus U$, und damit ist U Normalteiler. ∎

Da jede Spiegelungen zu sich selbst invers ist, bildet jede von ihnen zusammen mit der Identität eine Untergruppe der Ordnung zwei. Diese Untergruppen sind keine Normalteiler: Konjugieren wir etwa σ_0 mit δ, so drehen wir zunächst um den Winkel $360^\circ/n$, ersetzen also einen Punkt $z \in \mathbb{C}$ durch ζz. Danach wird an der reellen Achse gespiegelt; dies entspricht der komplexen Konjugation, und dann wird für die Drehung δ^{-1} mit ζ^{-1} multipliziert. Insgesamt wird also z abgebildet auf $\zeta^{-1} \cdot \overline{\zeta z} = \zeta^{-1}\overline{\zeta}\overline{u}$. Wegen $\zeta\overline{\zeta} = |\zeta|^2 = 1$ ist $\overline{\zeta} = \zeta^{-1}$, also geht z insgesamt auf $\zeta^{-2}\overline{z}$. Wegen der komplexen Konjugation kann dies keine Drehung sein, also ist es eine der Spiegelungen σ_k. Da bei einer Spiegelung genau die Punkte auf der Achse fest bleiben, können wir die Achse leicht bestimmen: Für ein z vom Betrag eins ist $\overline{z} = z^{-1}$, also $\zeta^{-2}\overline{z} = z$ genau dann, wenn $\zeta^{-2} = z^2$ oder $z = \pm\zeta^{-1}$ ist. Die Fixgerade ist also die Gerade durch E_{n-1} und den gegenüberliegenden Punkt, d.h. $\delta^{-1}\sigma_0\delta = \sigma_{n-2} \neq \sigma_0$.

Da eine Symmetrieoperation auf einem n-Eck durch die Bilder der Ecken eindeutig bestimmt ist, gibt es eine natürlichen Monomorphismus φ von D_n in die symmetrische Gruppe $\mathfrak{S}_n$: Falls $\sigma \in D_n$ die Ecke

E_k abbildet auf $E_{\pi(k)}$, ist $\varphi(\sigma) = \pi$. Für $n = 3$ ist φ ein Isomorphismus: Die drei Spiegelungen σ_k vertauschen jeweils zwei Ecken und lassen eine fest, werden also auf die drei Transpositionen aus $\mathfrak{S}_n$ abgebildet, und die Drehungen um $\pm 120^\circ$ gehen auf die beiden Dreierzykel; die Identität geht natürlich auf die Identität.

Für $n = 4$ haben wir keinen Isomorphismus mehr, denn $\mathfrak{S}_4$ hat 24 Elemente, D_4 aber nur acht. In der Tat gibt es keine Symmetrie eines Quadrats, die zwei benachbarte Ecken eines Quadrats vertauscht, die beiden anderen aber festläßt; von den $\binom{4}{2} = 6$ Transpositionen liegen also nur die beiden im Bild, die zwei gegenüberliegende Ecken vertauschen und den Rest fest lassen: Das sind die Bilder der Spiegelungen an den beiden Diagonalen. Auch die acht Dreierzykel lassen sich nicht als Symmetrieoperationen eines Quadrats realisieren, denn sie lassen genau einen Punkt fest, während Spiegelungen entweder keinen oder zwei Punkte festlassen und Drehungen keinen. Die vier Produkte zweier elementfremder Transpositionen entsprechen den vier Spiegelungen, liegen also im Bild, genauso wie der Viererzyklus (1 2 3 4) und sein Inverses (1 4 3 2).

Es ist keine spezielle Eigenschaft der Gruppe D_n, daß sie in eine symmetrische Gruppe eingebettet werden kann:

Lemma: Für jede endliche Gruppe G gibt es einen Monomorphismus φ von G in eine symmetrische Gruppe $\mathfrak{S}_n$.

Beweis: Wir nummerieren die Elemente von G in irgendeiner Weise; für $|G| = n$ sei also $G = \{g_1, \ldots, g_n\}$. Für jedes Element $x \in G$ ist die Multiplikation mit x bijektiv, es gibt also eine Permutation $\pi \in \mathfrak{S}_n$, so daß $xg_i = g_{\pi(i)}$ ist. Die Abbildung $\varphi: G \to \mathfrak{S}_n$, die jedem x die entsprechende Permutation zuordnet, ist natürlich injektiv. Sie ist auch ein Homomorphismus, denn ist $\varphi(x) = \pi$ und $\varphi(y) = \pi'$, so ist

$$(xy)g_i = x(yg_i) = xg_{\pi'(i)} = g_{\pi\left(\pi'(i)\right)} = g_{\pi\circ\pi'(i)}\,,$$

d.h. $\varphi(xy) = \varphi(x) \circ \varphi(y) = \varphi(x)\varphi(y)$. ∎

Wie das Beispiel der Diedergruppen zeigt, kann man zumindest gelegentlich auch in eine $\mathfrak{S}_n$ einbetten, bei der n kleiner ist als die

Gruppenordnung; das Extrembeispiel ist natürlich die symmetrische Gruppe $\mathfrak{S}_n$ selbst, die wir nicht erst in $\mathfrak{S}_{n!}$ einbetten müssen.

Die Einbettbarkeit einer beliebigen endlichen Gruppe in eine symmetrische Gruppe ist nicht nur theoretisch interessant: In der symmetrischen Gruppe können wir explizit rechnen nach einfachen Regeln, die wir auch einem Computer beibringen können. Sobald wir eine Gruppe also in eine $\mathfrak{S}_n$ eingebettet haben, können wir dort beliebige Rechnungen per Computer ausführen. Die Einbettungen einer endlichen Gruppe G in symmetrische Gruppen bezeichnet man als ihre *Permutationsdarstellungen;* Computeralgebrasysteme wie Maple benutzen unter anderen diese, um konkret mit Gruppen zu rechnen.

Wenn wir bei den regelmäßigen n-Ecken n gegen unendlich gehen lassen, bekommen wir einen Kreis. Diesen können wir zunächst einmal selbst als Gruppe betrachten: Wenn wir ihn in die komplexe Zahlenebene einbetten als

$$\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\} ,$$

ist er offensichtlich eine Gruppe bezüglich der Multiplikation (und hat die Menge der Ecken E_k des regelmäßigen n-Ecks mit der obigen Einbettung als Untergruppe). Diese Gruppe operiert durch Multiplikation auf der *Menge* $\mathbb{S}^1$ dadurch, daß das Element z der Gruppe das Element w der Menge auf zw abbildet. Für $z = e^{i\varphi}$ und $w = e^{i\psi}$ bedeutet das geometrisch, daß der Kreispunkt mit Winkel ψ bezüglich der x-Achse um den Winkel φ gedreht wird. Diese Drehungen sind aber nicht die einzigen Symmetrieoperationen auf der Kreislinie; genau wie bei regelmäßigen n-Eck haben wir auch noch Spiegelungen, hier aber an Geraden zu jedem beliebigen Steigungswinkel. Wir haben also unendlich viele Untergruppen der Ordnung zwei, die genau wie im Fall der Diedergruppen keine Normalteiler sind. Die Gruppe aller Drehungen ist auch hier ein Normalteiler, da sie Index zwei hat: Eine orientierungserhaltende Bewegung, die den Kreis invariant läßt, muß eine Drehung sein, (Die Punktspiegelung am Mittelpunkt ist die Drehung um 180°.) Ist also σ eine beliebige Drehung und τ eine Symmetrieoperation des Kreises, die die Orientierung nicht erhält, so ist $\sigma\tau$ orientierungserhaltend, also eine Drehung. Damit hat auch hier die Gruppe $\mathbb{S}^1$ der Drehungen den

Index zwei, ist also Normalteiler. In Analogie zu den Gruppen D_n wird die Symmetriegruppe des Kreises mit D_∞ bezeichnet.

Die Lineare Algebra liefert eine ganze Reihe von Beispielen für Gruppen, vor allem als Teilmengen der Menge $k^{n\times n}$ der $n\times n$-Matrizen über einem Körper k. Am bekanntesten sind die allgemeine *(general)* lineare Gruppe

$$\mathrm{GL}_n(k) \underset{\text{def}}{=} \{A \in k^{n\times n} \mid \det A \neq 0\}$$

und die spezielle lineare Gruppe

$$\mathrm{SL}_n(k) \underset{\text{def}}{=} \{A \in k^{n\times n} \mid \det A = 1\}\,.$$

Natürlich ist $\mathrm{SL}_n(k)$ eine Untergruppe von $\mathrm{GL}_n(k)$; als Kern der Determinantenabbildung ist sie sogar ein Normalteiler, denn nach dem Multiplikationssatz für Determinanten ist diese Abbildung ein Homomorphismus.

Ist G eine endliche Gruppe, so gibt es auch einen Monomorphismus von G in eine Gruppe $\mathrm{GL}_n(k)$: Im einfachsten Fall können wir n gleich der Gruppenordnung von G nehmen, die Gruppenelemente wieder irgendwie als $g_1, \ldots, g_n$ durchnummerieren und g_i abbilden auf die Matrix der folgenden linearen Abbildung φ_i: Ist $g_i g_j = g_\ell$, so soll $\varphi_i(e_j) = e_\ell$ sein, wobei $e_1, \ldots, e_n$ die Standardbasis von k^n ist. Man beachte, daß diese Matrix eine Permutationsmatrix ist; wenn wir $\mathfrak{S}_n$ identifizieren mit der Untergruppe aller Permutationsmatrizen in $\mathrm{GL}_n(k)$ haben wir also wieder eine der oben betrachteten Permutationsdarstellungen. Allgemein bezeichnet man Homomorphismen $G \to \mathrm{GL}_n(k)$ als *lineare Darstellungen* der Gruppe G; die meisten dieser Darstellungen lassen sich nicht als Permutationsdarstellungen interpretieren.

Die sogenannte *Darstellungstheorie* beschäftigt sich mit der systematischen Untersuchung der linearen Darstellungen einer Gruppe. Sie ist ein wichtiges Teilgebiet der Gruppentheorie, mit der man auch Strukturaussagen über Gruppen beweisen kann, die sich mit anderen Methoden nur schwer oder gar nicht beweisen lassen. Oft reichen bereits die einfacher zu untersuchenden *Charaktere* der linearen Darstellungen, d.h. man betrachtet an Stelle der Darstellungsmatrizen nur deren Spuren.

Fast alle hier betrachteten Gruppen wurden so definiert, daß ihre Elemente als Operationen auf einer Menge aufgefaßt werden können: Bei der D_n sind das Drehungen und Spiegelungen in der Ebene, bei der $\mathrm{GL}_n(k)$ lineare Abbildungen von k^n nach k^n. Solche Operationen lassen sich auch allgemein definieren:

Definition: *a)* Eine *Operation* einer Gruppe G auf einer Menge M ist eine Abbildung

$$\begin{cases} G \times M \to M \\ (g,m) \mapsto g(m) \end{cases},$$

für die gilt: $g\big(h(m)\big) = (gh)(m)$ für alle $g, h \in G$ und $m \in M$ und $e(m) = m$ für das Neutralelement $e \in G$ und alle $m \in M$.
b) Die *Bahn* eines Element $m \in M$ ist die Menge

$$O(m) \underset{\text{def}}{=} \{g(m) \mid g \in G\} .$$

c) Der *Stabilisator* eines Elements $m \in M$ ist

$$\mathrm{Stab}(m) \underset{\text{def}}{=} \{g \in g \mid g(m) = m\} .$$

Für *Operation* sind auch die Synonyme *Aktion* oder *Wirkung* gebräuchlich; statt *Bahn* sagt man auch *Orbit.*

Der Stabilisator eines Element $m \in M$ ist eine Untergruppe von g, denn für zwei Elemente $g, h \in \mathrm{Stab}(m)$ ist $g\big(h(m)\big) = g(m) = m$ und

$$g^{-1}(m) = g^{-1}\big(g(m)\big) = (gg^{-1})(m) = e(m) = m .$$

Für zwei Elemente $g, h \in G$ ist $g(m) = h(m)$ genau dann, wenn $(h^{-1}g)(m) = m$ ist, wenn also $h^{-1}g$ im Stabilisator von m liegt. Dies ist genau dann der Fall, wenn g in der Nebenklasse $g\mathrm{Stab}(m)$ liegt, wenn also die beiden Nebenklassen $g\mathrm{Stab}(m)$ und $h\mathrm{Stab}(m)$ übereinstimmen. Somit gilt

Lemma: Für jedes $m \in M$ gibt es eine bijektive Abbildung

$$\begin{cases} G/\mathrm{Stab}(m) \to O(m) \\ g\mathrm{Stab}(m) \mapsto g(m) \end{cases} .$$

Im Falle einer endlichen Gruppe G gilt somit die *Bahnbilanzgleichung* $|O(m)| = |G| \,/\, |\mathrm{Stab}(m)|$.

■

§3: Ringe

Ein Ring ist eine algebraische Struktur mit zwei Rechenoperationen, von denen die eine als Addition und die andere als Multiplikation aufgefaßt wird. Wir fordern, daß wir bezüglich der Addition eine abelsche Gruppe haben und bezüglich der Multiplikation ein Monoid; außerdem sollen die üblichen Distributivgesetze gelten. Ausführlich aufgeschrieben:

Definition: Ein *Ring* ist eine Menge R zusammen mit zwei Verknüpfungen $+, \cdot : R \times R \to R$, so daß gilt

1.) Bezüglich + ist R eine abelsche Gruppe.

2.) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ für alle $x, y, z \in R$.

3.) Es gibt ein Element $1 \in R$, so daß $1 \cdot x = x \cdot 1 = x$ für alle $x \in R$.

4.) $x \cdot (y + z) = x \cdot y + x \cdot z$ und $(x + y) \cdot z = x \cdot z + y \cdot z$ für alle $x, y, z \in R$.

b) Der Ring heißt *kommutativ,* wenn zusätzlich noch gilt

5.) $x \cdot y = y \cdot x$ für alle $x, y \in R$.

c) Ein kommutativer Ring heißt *Körper,* wenn $R \setminus \{0\}$ bezüglich der Multiplikation eine Gruppe bildet, wenn also zusätzlich gilt

6.) Zu jedem $x \neq 0$ aus R gibt es ein $x' \in R$ gibt, so daß $x \cdot x' = 1$ ist.

d) Eine Abbildung $\varphi: R \to S$ zwischen zwei Ringen heißt (Ring-) *Homomorphismus,* wenn für alle $x, y \in R$ gilt

$$\varphi(x + y) = \varphi(x) + \varphi(y) \quad \text{und} \quad \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)\,,$$

wobei + und $\cdot$ auf der linken Seite jeweils die Operationen von R bezeichnen und rechts die von S.

e) Ein $\left\{ \begin{array}{c} \textit{Monomorphismus} \\ \textit{Epimorphismus} \\ \textit{Isomorphismusa} \end{array} \right\}$ ist ein $\left\{ \begin{array}{c} \textit{injektiver} \\ \textit{surjektiver} \\ \textit{bijektiver} \end{array} \right\}$ Homomorphismus.

Zwei Ringe R und S heißen *isomorph,* in Zeichen $R \cong S$, wenn es einen Isomorphismus $\varphi: R \to S$ gibt.

f) Ist $R = S$, bezeichnen wir einen Homomorphismus von R nach R auch als *Endomorphismus* und einen Isomorphismus als *Automorphismus*.

g) Das *Bild* eines Homomorphismus $\varphi: R \to S$ ist

$$\text{Bild}\,\varphi \underset{\text{def}}{=} \varphi(R) = \{\varphi(x) \mid x \in R\}\,;$$

sein *Kern* ist

$$\text{Kern}\,\varphi \underset{\text{def}}{=} \{x \in R \mid \varphi(x) = 0\}\,.$$

Das bekannteste Beispiel eines Rings ist der Ring $\mathbb{Z}$ der ganzen Zahlen; er ist kommutativ. Ein Beispiel eines nichtkommutativen Rings bilden die $n \times n$-Matrizen über einem Körper (oder Ring) k für $n \geq 2$.

In Ringen muß es keine multiplikativen Inverse geben, eine Gleichung $ax = b$ mit $a, b \in R$ muß also keine Lösung haben. In $\mathbb{Z}$ ist sie genau dann lösbar, wenn a ein Teiler von b ist; dieses Konzept wollen wir auch auf andere Ringe verallgemeinern. Wenn wir eindeutige Lösungen wollen, können wir allerdings keine beliebigen Ringe zulassen: Wenn wir modulo zehn rechnen, hat etwa die Gleichung $2x \equiv 4 \bmod 10$ sowohl $x = 2$ als auch $x = 7$ als Lösungen. Der Grund liegt darin, daß $2 \cdot (7 - 2) = 2 \cdot 5 \equiv 0 \bmod 10$ ist, daß es also Elemente $a, b \neq 0$ gibt, deren Produkt verschwindet. Solche Elemente a, b bezeichnet man als *Nullteiler;* für eine Teilbarkeitstheorie, die dem entspricht, was wir von $\mathbb{Z}$ gewohnt sind, müssen wir die ausschließen.

Definition: Ein Ring heißt *nullteilerfrei* wenn gilt: Ist $x \cdot y = 0$, so muß mindestens einer der beiden Faktoren x, y verschwinden. Ein nullteilerfreier kommutativer Ring heißt *Integritätsbereich* (englisch *domain*).

In diesem Sinne ist also $\mathbb{Z}$ ein Integritätsbereich, erst recht natürlich auch jeder Körper. In einem Integritätsbereich hat die Gleichung $ax = b$ für $a \neq 0$ höchstens eine Lösung, denn ist $ax = ay$, so ist $a(y - x) = 0$, also $y - x = 0$ und $y = x$.

Der Kern eines Ringhomomorphismus ist im Allgemeinen kein Ring: Ansonsten müßte er insbesondere die Eins enthalten, und für jedes Element $x \in R$ ist dann $\varphi(x) = \varphi(1 \cdot x) = \varphi(1) \cdot \varphi(x) = 0 \cdot \varphi(x) = 0$, so daß φ die Nullabbildung sein muß. (Vor allem in der älteren Literatur verzichtet man aus diesem Grund bei der Definition eines Rings häufig auf die Forderung, daß es ein Neutralelement für die Multiplikation geben muß; dann bilden beispielsweise auch die geraden Zahlen einen Unterring von $\mathbb{Z}$. Da praktisch alle interessanten Beispiele von Ringen eine Eins enthalten, betrachten wir nur Ringe mit Eins.)

Liegen zwei Elemente x, y im Kern eines Homomorphismus φ: $R \to S$, so ist

$$\varphi(x+y) = \varphi(x)+\varphi(y) = 0+0 = 0 \quad \text{und} \quad \varphi(x\cdot y) = \varphi(x)\cdot\varphi(y) = 0\cdot 0 = 0\,,$$

also liegen auch Summe und Produkt im Kern. Für das Produkt hätte es aber offensichtlich gereicht, wenn nur einer der beiden Faktoren im Kern liegt. Der Kern ist daher ein Ideal im Sinne der folgenden Definition:

Definition: Eine Teilmenge I eines Rings R heißt *Ideal* von R, in Zeichen $I \lhd R$, wenn I eine additive Untergruppe von R ist und wenn für alle $r \in R$ und $x \in I$ gilt: rx und xr liegen in I.

Für kommutative Ringe reicht natürlich eine der beiden Forderungen $rx \in I$ oder $xr \in I$. Bei nichtkommutativen Ringen betrachtet man auch Linksideale, bei denen nur rx in I liegen muß und Rechtsideale, bei denen díes nur für xr der Fall sein muß; wenn – wie in obiger Definition gefordert – beides gilt, spricht man von einem beidseitigen Ideal.

Der Name *Ideal* geht auf KUMMER zurück, der für einen Beweis der FERMAT-Vermutung eindeutige Primzerlegung in Einheitswurzelringen benötigte. Da dies im allgemeinen nicht gilt, aber mit Idealen erreichbar ist, bezeichnete er diese als *ideale Zahlen.*

Da jedes Ideal eine additive Untergruppe ist, kommen in $\mathbb{Z}$ als Ideale nur die Mengen $m\mathbb{Z}$ mit $m \in \mathbb{N}_0$ in Frage, und die sind offensichtlich auch alle Ideale. Wenn wir sie als Ideale betrachten, schreiben wir meist (m) an Stelle von $m\mathbb{Z}$ gemäß der folgenden Konvention:

Definition: *a)* Für eine Teilmenge M eines Rings R bezeichnet (M) das kleinste Ideal von R, das M enthält. Für eine endliche Menge $M = \{a_1, \ldots, a_r\}$ schreiben wir $(M) = (a_1, \ldots, a_r)$.
b) Ein Ideal $I \trianglelefteq R$ eines Rings R heißt *Hauptideal*, wenn es ein $a \in R$ gibt, so daß $I = (a)$ ist.
c) Ein Integritätsbereich R heißt *Hauptidealring*, wenn jedes Ideal von R ein Hauptideal ist.

In diesem Sinne ist also $\mathbb{Z}$ ein Hauptidealring. Sind $a_1, \ldots, a_r$ ganze Zahlen, so wird das Ideal $(a_1, \ldots, a_r)$ erzeugt vom größten gemeinsamen Teiler der a_i, der in diesem Ideal liegt, weil er sich nach dem erweiterten EUKLIDischen Algorithmus als Linearkombination der a_i schreiben läßt. Dies legt nahe, daß der erweiterte EUKLIDische Algorithmus etwas mit Hauptidealringen zu tun haben könnte.

Der EUKLIDische Algorithmus beruht auf der Division mit Rest; wir definieren daher

Definition: Ein EUKLIDischer Ring ist ein Integritätsbereich R zusammen mit einer Abbildung $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$, so daß gilt: Ist $x|y$, so ist $\nu(x) \leq \nu(y)$, und zu je zwei Elementen $x, y \in R$ gibt es Elemente $q, r \in R$ mit

$$x = qy + r \quad \text{und} \quad r = 0 \quad \text{oder} \quad \nu(r) < \nu(y)\,.$$

Wir schreiben auch $x : y = q$ Rest r und bezeichnen r als Divisionsrest bei der Division von x durch y.

Erwartungsgemäß gilt

Lemma: Jeder EUKLIDische Ring ist ein Hauptidealring.

Beweis: $I \neq (0)$ sei ein Ideal von R, und M sei die Menge aller $\nu(f)$ für $f \in I \setminus \{0\}$. Das ist eine Teilmenge von $\mathbb{N}_0$; sie hat also ein kleinstes Element. Dieses sei gleich $\nu(f)$. Wir wollen uns überlegen, daß $I = (f)$ ist: Für ein beliebiges Element $g \in R$ können wir g mit Rest durch f dividieren, es also als $g = qf + r$ schreiben, wobei entweder $r = 0$ ist oder $\nu(r) < \nu(f)$. Letzteres ist wegen der Minimalität von $\nu(f)$ nicht möglich; also liegt $g = qf$ in (f).

∎

Die Umkehrung dieses Lemmas gilt nicht, allerdings sind Gegenbeispiele nicht einfach zu konstruieren, da die Funktion ν aus der Definition eines EUKLIDischen Rings a priori völlig beliebig sein kann und außerdem der einfachste Beweis, daß ein Ring Hauptidealring ist, meist darin besteht, zu zeigen, daß er EUKLIDisch ist. THEODORE MOTZKIN (1908–1970) gab 1949 den Ring $\mathbb{Z} \oplus \mathbb{Z}\omega$ mit $\omega = \frac{1}{2}(1 + \sqrt{-19})$ als Gegenbeispiel an in

T. MOTZKIN: The Euclidian Algorithm, *Bulletin of the American Mathematical Society* **55** (1949), 1142–1146;

einen ausführlichen Beweis dafür, daß dies ein Hauptidealring ist, aber kein EUKLIDischer Ring, findet man in

JACK C. WILSON: A principal ideal ring that is not a Euclidean ring, *Mathematics Magazine* **46** (1973), 34–38

Das Standardbeispiel eines EUKLIDischen Rings ist natürlich der Ring $\mathbb{Z}$ der ganzen Zahlen mit $\nu(x) = |x|$. Aus der Schule bekannt ist aber auch die Division mit Rest bei Polynomen; hier definieren wir $\nu(g)$ für ein von Null verschiedenes Polynom als den Grad von g.

Polynome können wir wir nicht nur über den reellen Zahlen betrachten, sondern über beliebigen Ringen; hier wollen wir uns allerdings mit kommutativen Ringen begnügen:

Definition: R sei ein kommutativer Ring. Der *Polynomring* $R[X]$ ist die Menge aller (formaler) Summen

$$a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0$$

mit $d \in \mathbb{N}_0$ und $a_i \in R$ für alle i. Ist $a_d \neq 0$, bezeichnen wir $d = \deg f$ als den *Grad* von f. Addition und Multiplikation sind durch die üblichen Regeln definiert.

Offensichtlich ist auch $R[X]$ ein kommutativer Ring; wir können daher auch den Polynomring $R[X][Y]$ über $R[X]$ betrachten, den wir kurz als $R[X, Y]$ bezeichnen, und so weiter. Die Elemente des Polynomrings $R[X_1, \ldots, X_n]$ in n Variablen lassen sich offenbar alle schreiben als endliche Linearkombinationen sogenannter *Monome* $X_1^{e_1} \cdots X_n^{e_n}$ mit $e_1, \ldots, e_n \in \mathbb{N}_0$. Der Grad eines solchen Monoms ist die Summe $e_1 + \ldots + e_n$ der Exponenten; der Grad eines Polynoms ungleich dem Nullpolynom ist der größte Grad eines darin vorkommenden Monoms.

Wir können nicht erwarten, daß jeder Polynomring EUKLIDisch ist; im allgemeinen muß er schließlich nicht einmal nullteilerfrei sein. Immerhin gilt

Lemma: Ist R ein Integritätsbereich, so auch der Polynomring $R[X]$.

Beweis: Wir betrachten zwei Polynome

$$f = \sum_{i=0}^{d} a_i X^i \quad \text{und} \quad g = \sum_{j=0}^{e} b_j X^j \ ,$$

die beide von Null verschieden sind. Wir können annehmen, daß d und e so gewählt sind, daß a_d und b_e beide nicht verschwinden. Da R Integritätsbereich ist, kann dann auch das Produkt $a_d b_e$ nicht verschwinden, also ist der führende Term $a_d b_e X^{d+e}$ von fg von Null verschieden und damit auch fg selbst.

∎

Tatsächlich beweist dies sogar etwas mehr als die Nullteilerfreiheit, denn wir wissen nun, daß sich bei der Multiplikation zweier Polynome über einem Integritätsbereich die Grade addieren.

Auch der Polynomring über einem Integritätsbereich muß nicht EUKLIDisch sein; wie wir sehen werden, ist weder $\mathbb{Z}[X]$ noch ein Polynomring in mehr als einer Variablen EUKLIDisch. Es gilt aber

Lemma: Der Polynomring $k[X]$ über einem Körper k ist EUKLIDisch und damit auch ein Hauptidealring.

Beweis: Wir definieren $\nu(f)$ für ein Polynom $f \neq 0$ als den Grad von f; dann zeigt der Algorithmus zur Polynomdivision, daß es zu je zwei Polynomen $f, g \in k[X]$ mit $g \neq 0$ Polynome $q, r \in k[X]$ gibt mit $r = 0$ oder $\nu(r) < \nu(g)$ derart, daß $f = qg + r$ ist.

∎

Der EUKLIDische Algorithmus wird dazu verwendet, größte gemeinsame Teiler zu berechnen und als Linearkombination darzustellen; bevor wir das genauer untersuchen können, müssen wir erst definieren, was Teiler in einem beliebigen Ring sein sollen. Eine sinnvolle Theorie erhalten wir nur für Integritätsbereiche; daher wollen wir uns darauf beschränken.

Definition: R sei ein Integritätsbereich.
a) $u \in R$ heißt *Teiler* von $x \in R$, in Zeichen $u|x$, wenn es ein $q \in R$ gibt, so daß $x = q \cdot u$.

b) $u \in R$ heißt ***größter gemeinsamer Teiler*** von x und y, wenn u Teiler von x und von y ist und wenn für jeden anderen gemeinsamen Teiler v von x und y gilt: $v|u$.
c) Ein Element $e \in R$ heißt *Einheit*, falls es ein $e' \in R$ gibt mit dem $e \cdot e' = e'\dot{e} = 1$ ist. Die Menge aller Einheiten von R bezeichnen wir mit $R^\times$.
d) Zwei Elemente $x, y \in R$ heißen assoziiert, wenn es eine Einheit $e \in R$ gibt, so daß $y = e \cdot x$.

Mit Idealen ausgedrückt ist $u|x$ äquivalent zu $(x) \subseteq (u)$, und x, y sind genau dann assoziiert, wenn sie das gleiche Hauptideal erzeugen.

Für $R = \mathbb{Z}$ entspricht das nicht ganz den Begriffen, mit denen wir im vorigen Kapitel gearbeitet haben: Beispielsweise ist im Sinne obiger Definition auch -3 ein größter gemeinsamer Teiler von sechs und neun. Allgemein gilt:

Lemma: *a)* Die Menge $R^\times$ aller Einheiten eines Rings R bildet eine Gruppe bezüglich der Multiplikation.
b) Ein kommutativer Ring R ist genau dann ein Integritätsbereich, wenn die folgende *Kürzungsregel* erfüllt ist: Gilt für $x, y, z \in R$ und $z \neq 0$ die Gleichung $xz = yz$, so ist $x = y$.
c) Zwei Elemente x, y eines Integritätsbereich R sind genau dann assoziiert, wenn $x|y$ und $y|x$.
d) Ein größter gemeinsamer Teiler, so er existiert, ist bis auf Assoziiertheit eindeutig bestimmt.

Beweis: a) Sind $e, f \in R$ Einheiten, so gibt es Elemente e', f' mit $ee' = ff' = 1$. Damit ist $(ef)(f'e') = e(ff')e' = ee' = 1$, d.h. auch ef ist eine Einheit. Außerdem ist jede Einheit invertierbar, denn offensichtlich ist e' ein multiplikatives Inverses zu e.
b) Ist R ein Integritätsbereich und $xz = yz$, so ist $(x - y)z = 0$; da $z \neq 0$ vorausgesetzt war, folgt $x - y = 0$, also $x = y$. Folgt umgekehrt aus $xz = yz$ und $z \neq 0$ stets $x = y$, so ist R nullteilerfrei, denn ist $xy = 0$ und $y \neq 0$, so ist $xy = 0y$, also $x = 0$.
c) Ist $y = ex$, so ist x ein Teiler von y. Da Einheiten invertierbar sind, ist auch $x = e^{-1}y$, d.h. $y|x$.

Gilt umgekehrt $x|y$ und $y|x$, so gibt es Elemente q, r mit $x = qy$ und $y = rx$. Damit ist $1x = x = (qr)x$, also $qr = 1$. Somit ist q eine Einheit. *d)* Sind u, v zwei größte gemeinsame Teiler von x, y, so ist nach Definition u Teiler von v und v Teiler von u, also sind u und v assoziiert. ∎

Schauen wir uns an, was das für einen Polynomring bedeutet!

Lemma: Die Einheiten im Polynomring $R[X]$ über einem Integritätsbereich R sind genau die Einheiten von R.

Beweis: Ist $f \in R[X]$ eine Einheit, so gibt es ein $g \in R[X]$ mit $fg = 1$; da das konstante Polynom 1 den Grad Null hat, muß dasselbe auch für f und g gelten, d.h. $f, g \in R$ und damit in $R^\times$. ∎

Für Polynome über einem Körper bedeutet dies, daß zwei Polynome genau dann assoziiert sind, wenn sie sich durch eine multiplikative Konstante ungleich Null unterscheiden; wenn es einen größten gemeinsamen Teiler gibt, ist er also nur bis auf eine solche Konstante bestimmt. Das nächste Lemma zeigt, daß es ihn wirklich gibt:

Lemma: In einem EUKLIDischen Ring R gibt es zu je zwei Elementen $x, y \in R$ einen ggT. Dieser kann nach dem EUKLIDischen Algorithmus berechnet werden und läßt sich als Linearkombination mit Koeffizienten aus R von x und y darstellen

Beweis: In jedem Integritätsbereich folgt aus der Gleichung $x = qy + r$ mit $x, y, q, r \in R$, daß die gemeinsamen Teiler von x und y gleich denen von y und r sind. Speziell in einem EUKLIDischen Ring können wir dabei r als Divisionsrest wählen und, wie beim klassischen EUKLIDischen Algorithmus, danach y durch r dividieren *usw.*, wobei wir eine Folge (r_i) von Divisionsresten erhalten mit der Eigenschaft, daß in jedem Schritt die gemeinsamen Teiler von x und y gleich denen von r_{i-1} und r_i sind. Außerdem ist stets entweder $r_i = 0$ oder $\nu(r_i) < \nu(r_{i-1})$, so daß die Folge nach endlich vielen Schritten mit einem $r_n = 0$ abbrechen muß. Auch hier sind die gemeinsamen Teiler von r_{n-1} und $r_n = 0$ genau die gemeinsamen Teiler von x und y. Da jede Zahl Teiler der Null ist, sind die gemeinsamen Teiler von r_{n-1} und Null aber genau die Teiler

von r_{n-1}, und unter diesen gibt es natürlich einen größten, nämlich r_{n-1} selbst. Somit haben auch x und y einen größten gemeinsamen Teiler, nämlich den nach dem EUKLIDischen Algorithmus berechneten letzten von Null verschiedenen Divisionsrest r_{n-1}.

Auch die lineare Kombinierbarkeit folgt wie im klassischen Fall: Bei jeder Division mit Rest ist der Divisionsrest als Linearkombination von Dividend und Divisor darstellbar; beim EUKLIDischen Algorithmus beginnen wir mit Linearkombinationen von x und y darstellbar sind, und induktiv folgt, daß auch alle folgenden Dividenden und Divisoren sind als Reste einer vorangegangenen Division Linearkombinationen von x und y sind, also ist es auch ihr Divisionsrest. Insbesondere ist auch der ggT als letzter nichtverschwindender Divisionsrest Linearkombination von x und y, und die Koeffizienten können wie im vorigen Kapitel für $R = \mathbb{Z}$ mit dem erweiterten EUKLIDischen Algorithmus berechnet werden.

■

Im vorigen Kapitel hatten wir unter anderem mit Hilfe des erweiterten EUKLIDischen Algorithmus die eindeutige Primzerlegung gezeigt. Für ein ähnliches Resultat in allgemeineren Ringen definieren wir

Definition: *a)* Ein Element x eines Integritätsbereichs R heißt *irreduzibel*, falls gilt: x ist keine Einheit, und ist $x = yz$ das Produkt zweier Elemente aus R, so muß y oder z eine Einheit sein.
b) Ein Integritätsbereich R heißt *faktoriell* oder *ZPE*-Ring, wenn gilt: Jedes Element $x \in R$ läßt sich bis auf Reihenfolge und Assoziiertheit eindeutig schreiben als Produkt $x = u \prod_{i=1}^{r} p_i^{e_i}$ mit einer Einheit $u \in R^\times$, irreduziblen Elementen $p_i \in R$ und natürlichen Zahlen e_i.
(*ZPE* steht für **Z**erlegung in **P**rimfaktoren **E**indeutig.)

Lemma: In einem faktoriellen Ring gibt es zu je zwei Elementen x, y einen größten gemeinsamen Teiler.

Beweis: Wir wählen zunächst aus jeder Klasse assoziierter irreduzibler Elemente einen Vertreter; für die Zerlegung eines Elements in ein Produkt irreduzibler Elemente reicht es dann, wenn wir nur irreduzible Elemente betrachten, die Vertreter ihrer Klasse sind.

Sind $x = u\prod_{i=1}^{r} p_i^{e_i}$ und $y = v\prod_{j=1}^{s} q_j^{f_j}$ mit $u, v \in R^\times$ und p_i, q_j irreduzibel die entsprechenden Zerlegungen von x und y in Primfaktoren, so können wir, indem wir nötigenfalls Exponenten Null einführen, o.B.d.A. annehmen, daß $r = s$ ist und $p_i = q_i$ für alle i. Dann ist offenbar $\prod_{i=1}^{r} p_i^{\min(e_i,f_i)}$ ein ggT von x und y, denn $z = \prod_{i=1}^{r} p_i^{g_i}$ ist genau dann Teiler von x, wenn $g_i \leq e_i$ für alle i, und Teiler von y, wenn $g_i \leq f_i$. ∎

Satz: Jeder Hauptidealring ist faktoriell.

Beweis: Wir müssen zeigen, daß jedes Element $x \neq 0$ bis auf Reihenfolge und Assoziiertheit eindeutig als Produkt aus einer Einheit und geeigneten Potenzen irreduzibler Elemente geschrieben werden kann. Wir beginnen damit, daß sich x überhaupt in dieser Weise darstellen läßt. Wie beim Hauptsatz der elementaren Zahlentheorie beweisen wir dies durch Widerspruch.

Wir nehmen also an, es gäbe Elemente $x \neq 0$, die sich nicht als Produkte von irreduziblen Elementen und Einheiten darstellen lassen und betrachten in der Menge M aller dieser Elemente ein bezüglich der Teilbarkeit minimales, d.h. ein Element $x \in M$ derart, daß jedes $y \in M$, das y teilt, zu y assoziiert sein muß. Wir müssen uns zunächst überlegen, daß es so ein Element überhaupt gibt:

Wäre dies nicht der Fall, so hätten wir eine unendliche Folge von Elementen $x_1, x_2, \ldots$ aus M derart, daß stets x_{i+1} ein echter Teiler von x_i ist. Für die Hauptideale (x_i) bedeutet das, daß (x_i) stets echt enthalten ist in (x_{i+1}):

$$(x_1) \subset (x_2) \subset (x_3) \subset \cdots .$$

Die Vereinigung I der sämtlichen Hauptideale (x_i) ist wieder ein Ideal, und da wir in einem Hauptidealring sind, ist $I = (x)$ ein Hauptideal. Da I die Vereinigung alle (x_i) ist, muß x in einem dieser Ideale (x_i) liegen. Für $j > i$ ist dann

$$(x) \subseteq (x_i) \subset (x_j) \subset I = (x)\,,$$

im Widerspruch zur Annahme, daß (x_i) echt in (x_j) enthalten ist. Also gibt es ein bezüglich der Teilbarkeit minimales Element $x \in M$.

x kann nicht irreduzibel sein, denn sonst wäre $x = x$ eine Darstellung als Produkt irreduzibler Elemente. Daher läßt sich x als Produkt $x = yz$ zweier Elemente x, y schreiben, die beide keine Einheiten sind. Als echte Teiler von x können y und z nicht in M liegen, lassen sich also als Produkt einer Einheit mit einem Produkt irreduzibler Elemente darstellen. Multiplizieren wir die beiden Darstellungen miteinander und fassen die beiden Einheiten zusammen zu deren Produkt, erhalten wir eine entsprechende Darstellung für x, im Widerspruch zur Annahme $x \in M$. Also kann es keine Gegenbeispiele geben.

Als nächstes müssen wir uns überlegen, daß diese Darstellung bis auf Reihenfolge und Einheiten eindeutig ist. Das wesentliche Hilfsmittel hierzu ist wieder die folgende Zwischenbehauptung:

Falls ein irreduzibles Element p ein Produkt xy teilt, teilt es mindestens einen der beiden Faktoren.

Zum *Beweis* nehmen wir an, p sei kein Teiler von x. Dann liegt x nicht im Ideal (p), das Ideal (p, x) ist also echt größer als (p). Da wir den Ring als Hauptidealring vorausgesetzt haben, gibt es ein Element q, so daß $(p, x) = (q)$ ist, d.h. q ist ein Teiler von p. Da p irreduzibel ist, sind alle Teiler entweder assoziiert zu p oder Einheiten. Im Falle der Assoziiertheit wäre $(q) = (p)$, was hier nicht der Fall ist; somit muß q eine Einheit sein. Dann enthält (q) auch $q^{-1}q = 1$, ist also der ganze Ring. Da $(q) = (p, x)$ ist, gibt es also eine Darstellung

$$1 = \alpha p + \beta x$$

mit zwei Ringelementen α, β. Multiplikation dieser Gleichung mit y führt auf $y = \alpha p x + \beta x y$, und hier sind beide Summanden auf der rechten Seite durch p teilbar: Bei $\alpha p x$ ist das klar, und bei $\beta x y$ folgt es daraus, daß nach Voraussetzung p ein Teiler von xy ist. Also ist p Teiler von y, und die Zwischenbehauptung ist bewiesen.

Induktiv folgt sofort:

Falls ein irreduzibles Element p ein Produkt $\prod_{i=1}^{r} x_i$ teilt, teilt es mindestens einen der Faktoren x_i.

Um den Beweis des Satzes zu beenden, müssen wir noch zeigen, daß die Zerlegung bis auf Reihenfolge und Einheiten eindeutig ist. Wie-

der nehmen wir an, dies sei nicht der Fall, und wählen in der Menge aller Gegenbeispiele ein bezüglich der Teilbarkeit minimales Element x. Dieses hat somit mindestens zwei Zerlegungen

$$x = u \prod_{i=1}^{r} p_i^{e_i} = v \prod_{j=1}^{s} q_j^{f_j} \ ,$$

wobei wir annehmen können, daß alle $e_i, f_j \geq 1$ sind. Dann ist p_1 trivialerweise Teiler des ersten Produkts, also auch des zweiten. Wegen der Zwischenbehauptung teilt p_1 also mindestens eines der Elemente q_j, d.h. $p_1 = wq_j$ ist bis auf eine Einheit w gleich q_j. Da $x/p_i = x/(wq_j)$ ein echter Teiler von x ist, liegt dieses Element nicht in M, hat also eine bis auf Reihenfolge und Einheiten eindeutige Zerlegung in irreduzible Elemente. Damit hat auch x eine solche Zerlegung. ∎

Da der Polynomring in einer Veränderlichen über einem Körper Hauptidealring ist, läßt sich dort somit jedes Polynom in irreduzible Faktoren zerlegen. Wir wollen uns überlegen, daß die auch für Polynome in mehreren Veränderlichen gilt, sogar dann, wenn wir den Körper ersetzen durch beliebigen faktoriellen Ring. Der entsprechende Satz geht zurück auf GAUSS, der dazu einen beliebigen solchen Polynomring einbettet in einen Polynomring in einer Variablen über einem Körper.

Als ersten Schritt konstruieren wir zu einem Integritätsbereich R einen Körper, der R enthält; Vorbild ist die Konstruktion der rationalen Zahlen aus den ganzen.

Wir betrachten also auf der Menge aller Paare (f, g) mit $f, g \in R$ und $g \neq 0$ die Äquivalenzrelation

$$(f, g) \sim (r, s) \iff fs = gr \ ;$$

die Äquivalenzklasse von (f, g) bezeichnen wir als den *Bruch* $\dfrac{f}{g}$.

Verknüpfungen zwischen diesen Brüchen werden nach den üblichen Regeln der Bruchrechnung definiert:

$$\frac{f}{g} + \frac{r}{s} = \frac{fs + rg}{gs} \quad \text{und} \quad \frac{f}{g} \cdot \frac{r}{s} = \frac{fr}{gs} \ .$$

Dies ist wohldefiniert, denn sind $(f,g) \sim (\tilde{f},\tilde{g})$ und $(r,s) \sim (\tilde{r},\tilde{s})$, so ist

$$\frac{\tilde{f}}{\tilde{g}} + \frac{\tilde{r}}{\tilde{s}} = \frac{\tilde{f}\tilde{s} + \tilde{r}\tilde{g}}{\tilde{g}\tilde{s}} \quad \text{und} \quad \frac{\tilde{f}}{\tilde{g}} \cdot \frac{\tilde{r}}{\tilde{s}} = \frac{\tilde{f}\tilde{r}}{\tilde{g}\tilde{s}} \,.$$

Wegen $f\tilde{g} = \tilde{f}g$ und $r\tilde{s} = \tilde{r}s$ ist

$$\begin{aligned}(\tilde{f}\tilde{s} + \tilde{r}\tilde{g}) \cdot gs &= \tilde{f}\tilde{s}gs + \tilde{r}\tilde{g}gs = \tilde{f}gs\tilde{s} + \tilde{r}sg\tilde{g} \\ &= g\tilde{g}s\tilde{s} + r\tilde{s}g\tilde{g} = (gs + ry)\tilde{g}\tilde{s}\end{aligned}$$

und $(\tilde{f}\tilde{r})(gs) = \tilde{f}g\tilde{r}s = g\tilde{g}r\tilde{s} = (gr)(\tilde{g}\tilde{s})$, d.h. auch die Ergebnisse sind äquivalent.

Man rechnet leicht nach (wie bei $\mathbb{Q}$), daß diese Äquivalenzklassen einen Ring bilden mit $\frac{0}{1}$ als Null und $\frac{1}{1}$ als Eins; er ist sogar ein Körper, denn für $f, g \neq 0$ ist $\frac{g}{f}$ ein multiplikatives Inverses zu $\frac{f}{g}$, da $(fg, fg) \sim (1,1)$. Identifizieren wir schließlich ein Element $f \in R$ mit dem Bruch $\frac{f}{1}$, so können wir R in den Körper K einbetten.

Definition: Der so konstruierte Körper K heißt Quotientenkörper von R, in Zeichen $K = \text{Quot}\, R$.

Das Standardbeispiel ist natürlich $\mathbb{Q} = \text{Quot}\, \mathbb{Z}$, aber auch der Quotientenkörper $k(X) \underset{\text{def}}{=} \text{Quot}\, k[X]$ eines Polynomrings über einem Körper k ist wichtig: $k(X)$ heißt rationaler Funktionenkörper in einer Veränderlichen über k. Seine Elemente sind rationale Funktionen in X, d.h. Quotienten von Polynomen in X, wobei der Nenner natürlich nicht das Nullpolynom sein darf.

Für Polynome, die statt über einem Körper nur über einem faktoriellen Ring definiert sind, sind die beiden folgenden Begriffe sehr wesentlich:

Definition: *a)* Der *Inhalt* eines Polynoms $f = a_d X^d + \cdots + a_0 \in R[X]$ ist der größte gemeinsame Teiler $I(f)$ seiner Koeffizienten a_i.
b) f heißt *primitiv*, wenn die a_i zueinander teilerfremd sind.

Indem wir alle Koeffizienten eines Polynoms durch ihren gemeinsamen ggT dividieren sehen wir, daß sich jedes Polynom aus $R[X]$ als Produkt seines Inhalts mit einem primitiven Polynom schreiben läßt. Diese Zerlegung bleibt bei der Multiplikation zweier Polynome erhalten:

Lemma: R sei ein faktorieller Ring. Für zwei Polynome

$$f = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \quad \text{und}$$
$$g = b_e X^e + b_{e-1} X^{e-1} + \cdots + b_1 X + b_0$$

aus $R[X]$ ist $I(fg) = I(f) \cdot I(g)$. Insbesondere ist das Produkt zweier primitiver Polynome wieder primitiv.

Beweis: Wir schreiben $f = I(f) \cdot f^*$ und $g = I(g) \cdot g^*$ mit primitiven Polynomen f^* und g^*; dann ist $fg = I(f) \cdot I(g) \cdot (f^* g^*)$. Falls $f^* g^*$ wieder ein primitives Polynom ist, folgt, daß $I(fg) = I(f) \cdot I(g)$ sein muß.

Es genügt daher, zu zeigen, daß das Produkt zweier primitiver Polynome wieder primitiv ist. Sei $fg = c_{d+e} X^{d+e} + c_{d+e-1} X^{d+e-1} + \cdots + c_1 X + c_0$; dann ist $c_r = \sum_{i,j \text{ mit } i+j=r} a_i b_j$.

Angenommen, diese Koeffizienten c_r haben einen gemeinsamen Teiler, der keine Einheit ist. Wegen der Faktorialität von R gibt es dann auch ein irreduzibles Element p, das alle Koeffizienten c_r teilt.

Insbesondere ist p ein Teiler von $c_0 = a_0 b_0$; da p irreduzibel ist, muß mindestens einer der beiden Faktoren a_0, b_0 durch p teilbar sein. Da es im Lemma nicht auf die Reihenfolge von f und g ankommt, können wir o.B.d.A. annehmen, daß a_0 Vielfaches von p ist.

Da f ein primitives Polynom ist, kann nicht jeder Koeffizient a_i durch p teilbar sein; ν sei der kleinste Index, so daß a_ν kein Vielfaches von p ist. Genauso gibt es auch einen kleinsten Index $\mu \geq 0$, für den b_μ nicht durch p teilbar ist. In

$$c_{\mu+\nu} = \sum_{i,j \text{ mit } i+j=\mu+\nu} a_i b_j$$

ist dann der Summand $a_\nu b_\mu$ nicht durch p teilbar, aber für jeden anderen Summanden $a_i b_j$ ist entweder $i < \nu$ oder $j < \mu$, so daß mindestens einer der Faktoren und damit auch das Produkt durch p teilbar ist. Insgesamt ist daher $c_{\mu+\nu}$ nicht durch p teilbar, im Widerspruch zur Annahme. Somit muß fg ein primitives Polynom sein.

■

Satz von Gauß: R sei ein faktorieller Ring und $K = \operatorname{Quot} R$. Falls sich ein Polynom $f \in R[X]$ in $K[X]$ als Produkt zweier Polynome $g, h \in K[X]$ schreiben läßt, gibt es ein $\lambda \in K$, so daß $\widetilde{g} = \lambda g$ und $\widetilde{h} = \lambda^{-1} h$ in $R[X]$ liegen und $f = \widetilde{g} \cdot \widetilde{h}$.

Beweis: Durch Multiplikation mit einem gemeinsamen Vielfache aller Koeffizienten können wir aus einem Polynom mit Koeffizienten aus K eines mit Koeffizienten aus R machen. Dieses wiederum ist gleich seinem Inhalt mal einem primitiven Polynom. Somit läßt sich jedes Polynom aus $K[x]$ schreiben als Produkt eines Elements von K mit einem primitiven Polynom aus $R[x]$. Für g und h seien dies die Zerlegungen

$$g = cg^* \quad \text{und} \quad h = dh^* .$$

Dann ist $f = (cd)g^*h^*$, und nach dem Lemma ist g^*h^* ein primitives Polynom. Daher liegt $cd = I(f)$ in R, und wir können beispielsweise $\widetilde{g} = I(P)g^*$ und $\widetilde{h} = h^*$ setzen. ∎

CARL FRIEDRICH GAUSS (1777–1855) leistete wesentliche Beiträge zur Zahlentheorie, zur nichteuklidischen Geometrie, zur Differentialgeometrie und Kartographie, zur Fehlerrechnung und Statistik, zur Astronomie und Geophysik *usw.* Als Direktor der Göttinger Sternwarte baute er zusammen mit dem Physiker Weber den ersten Telegraphen. Er leitete die erste Vermessung und Kartierung des Königreichs Hannover, was sowohl seine Methode der kleinsten Quadrate als auch sein *Theorema egregium* motivierte, und zeitweise auch den Witwenfond der Universität Göttingen. Seine hierbei gewonnene Erfahrung nutzte er für erfolgreiche Spekulationen mit Aktien.

Korollar: Ein primitives Polynom $f \in R[X]$ ist genau dann irreduzibel in $R[X]$, wenn es in $K[X]$ irreduzibel ist. ∎

Für nichtprimitive Polynome gilt diese Aussage natürlich nicht: Das Polynom $2X + 2$ ist zwar irreduzibel in $\mathbb{Q}[X]$, hat aber in $\mathbb{Z}[X]$ die beiden irreduziblen Faktoren 2 und $X + 1$.

Aus dem Satz von GAUSS folgt induktiv sofort, daß seine Aussage auch für Produkte von mehr als zwei Polynomen gilt, und daraus folgt

Satz: Der Polynomring über einem faktoriellen Ring R ist faktoriell.

Beweis: Wir müssen zeigen, daß sich jedes $f \in R[X]$ bis auf Reihenfolge und Einheiten eindeutig als Produkt von Potenzen irreduzibler Elemente aus $R[X]$ und einer Einheit schreiben läßt. Dazu schreiben wir $f = I(f) \cdot f^*$ mit einem primitiven Polynom $f^* \in R[X]$ und zerlegen zunächst den Inhalt $I(f)$ in R. Da R nach Voraussetzung faktoriell ist, ist diese Zerlegung eindeutig bis auf Reihenfolge und Einheiten in R, und wie wir bereits wissen, sind die Einheiten von $R[X]$ gleich denen von R.

Als nächstes zerlegen wir das primitive Polynom f^* über dem Quotientenkörper K von R; dies ist möglich, da $K[X]$ als EUKLIDischer Ring faktoriell ist. Jedes der irreduziblen Polynome q_i, die in dieser Zerlegung vorkommen, läßt sich schreiben als $q_i = \lambda_i p_i$ mit einem $\lambda_i \in K^\times$ und einem primitiven Polynom $p_i \in R[X]$. Wir können daher annehmen, daß in der Zerlegung von f nur primitive Polynome aus $R[x]$ auftreten sowie eine Einheit aus K. Diese muß, da f^* Koeffizienten aus R hat und ein Produkt primitiver Polynome primitiv ist, in R liegen; da auch f^* primitiv ist, muß sie dort sogar eine Einheit sein.

Kombinieren wir diese Primzerlegung von f^* mit der Primzerlegung des Inhalts, haben wir eine Primzerlegung von f gefunden; sie ist (bis auf Reihenfolge und Einheiten) eindeutig, da entsprechendes für die Zerlegung des Inhalts, die Zerlegung von f^* sowie die Zerlegung eines Polynoms in Inhalt und primitiven Anteil gilt.

∎

Da wir einen Polynomring $R[X_1, \ldots, X_n]$ in n Veränderlichen als Polynomring $R[X_1, \ldots, X_{n-1}][X_n]$ in einer Veränderlichen über dem Polynomring $R[X_1, \ldots, X_{n-1}]$ in $n-1$ Veränderlichen auffassen können, folgt induktiv sofort:

Satz: Der Polynomring $R[X_1, \ldots, X_n]$ in n Veränderlichen über einem faktoriellen Ring R ist faktoriell. Insbesondere sind $\mathbb{Z}[X_1, \ldots, X_n]$ sowie $k[X_1, \ldots, X_n]$ für jeden Körper k faktoriell.

∎

Damit wissen wir also, daß auch Polynome in mehreren Veränderlichen über $\mathbb{Z}$ oder über einem Körper in Produkte irreduzibler Polynome zer-

legt werden können; insbesondere existieren daher auch in dieser Ringen größte gemeinsame Teiler.

Der Beweis des obigen Satzes ist allerdings nicht konstruktiv; die Computeralgebra kennt zwar Algorithmen, mit denen man die Faktorisierung für Polynome, auch in mehreren Veränderlichen, über den ganzen oder rationalen Zahlen (und einigen anderen) konstruktiv durchführen kann, sie benutzen aber ganz andere Methoden als der obige Beweis.

Nachdem wir nun wissen, daß auch beispielsweise die Ringe $\mathbb{Z}[X]$ und $\mathbb{R}[X,Y]$ faktoriell sind, wissen wir, daß auch dort größte gemeinsame Teiler existieren. Offensichtlich sind in $\mathbb{Z}[X]$ sowohl die Zwei als auch X irreduzible Elemente; ihr größter gemeinsamer Teiler ist also eins. Es gibt aber natürlich keine Darstellung $1 = 2\alpha + X\beta$ mit ganzzahligen Polynomen $\alpha, \beta \in \mathbb{Z}[X]$, denn der konstante Term eines Polynom der Form $2\alpha + X\beta$ ist immer gerade. Genauso ist in $\mathbb{R}[X,Y]$ der ggT von X und Y gleich eins, aber eine Darstellung in der Form $1 = X\alpha + Y\beta$ ist nicht möglich, da $X\alpha + Y\beta$ keinen konstanten Term hat. Beide Ringe sind daher zwar faktoriell, aber nicht EUKLIDisch. Sie sind auch keine Hauptidealringe, denn auch in einem Hauptidealring ist der ggT linear kombinierbar: Ist nämlich (x,y) das von zwei Elementen x, y erzeugte Ideal, so ist dieses ein Hauptideal (u). Da (u) sowohl x als auch y enthält und damit auch die Hauptideale (x) und (y), ist u sowohl Teiler von x als auch von y. Ist umgekehrt t ein gemeinsamer Teiler von x und y, so liegen x und y in s, also auch $(x,y) = (u)$. Also liegt (u) in (s), d.h. s ist ein Teiler von u. Somit ist u ein größter gemeinsamer Teiler von x und y; als Element von (x,y) hat er natürlich eine Darstellung der Form $u = \alpha x + \beta y$.

Zu Beginn dieses Paragraphen haben wir Ideale eingeführt als Teilmengen deren Eigenschaften gerade die der Kerne von Ringhomomorphismen sind. Von daher sollte es möglich sein, Faktorringe modulo einem Ideal zu bilden.

Wir beschränken uns auf kommutative Ringe R und betrachten ein Ideal $I \lhd R$. Da R insbesondere eine (additive) Gruppe ist und I eine Untergruppe, also wegen der Kommutativität der Addition automatisch

ein Normalteiler ist, können wir auf jeden Fall die additive Gruppe R/I bilden. Um sie zu einem Ring zu machen, brauchen wir noch eine Multiplikation. Es bietet sich an, diese durch die Vorschrift

$$(x + I)(y + I) = xy + I$$

zu definieren – falls dies wohldefiniert ist.

Ist $x + I = x' + I$ und $y + I = y' + I$, so ist

$$x'y' = \big(x + (x' - x)\big)\big(y + (y' - y)\big)$$
$$= xy + x(y' - y) + (x' - x)y + (x' - x)(y' - y)\,.$$

$x' - x$ und $y' - y$ liegen in I; nach Definition eines Ideals liegen daher auch alle Produkte einer dieser Differenzen mit einem beliebigen Ringelement in I. Somit unterscheiden sich xy und $x'y'$ nur durch ein Element von I, d.h. $xy + I = x'y' + I$. Dies zeigt die Wohldefiniertheit der Multiplikation; Assoziativ- und Distributivgesetz folgen daraus, daß sie in R gelten.

Definition: R/I mit den beiden Rechenoperationen

$$(x + I) + (y + I) = (x + y) + I \quad \text{und} \quad (x + I)(y + I) = xy + I$$

heißt *Faktorring* von R modulo dem Ideal I.

Wie bei Gruppen haben wir auch bei Ringen einen

Homomorphiesatz: Ist $\varphi\colon R \to S$ ein Homomorphismus von kommutativen Ringen, so ist

$$R/\operatorname{Kern}\varphi \cong \operatorname{Bild}\varphi\,.$$

Beweis: Zwei Elemente $x, y \in R$ haben genau dann das gleiche Bild $\varphi(x) = \varphi(y)$, wenn $y - x$ im Kern liegt. Daher werden alle Elemente einer Nebenklasse $x + \operatorname{Kern}\varphi$ auf dasselbe Element von S abgebildet, so daß

$$\widetilde{\varphi}\colon \begin{cases} R/\operatorname{Kern}\varphi \to S \\ x + \operatorname{Kern}\varphi \mapsto \varphi(x) \end{cases}$$

eine wohldefinierte Abbildung ist. Da verschiedene Nebenklassen verschiedene Bilder haben, ist sie injektiv, und sie ist ein Homomorphismus, denn

$$\widetilde{\varphi}\big((x + \operatorname{Kern}\varphi) + (y + \operatorname{Kern}\varphi)\big) = \widetilde{\varphi}\big((x + y) + I\big) = \varphi(x + y)$$
$$= \varphi(x) + \varphi(y) = \widetilde{\varphi}(x + \operatorname{Kern}\varphi) + \widetilde{\varphi}(y + \operatorname{Kern}\varphi)$$

und

$$\widetilde{\varphi}\big((x + \operatorname{Kern}\varphi)(y + \operatorname{Kern}\varphi)\big) = \widetilde{\varphi}(xy + I) = \varphi(xy) = \varphi(x)\varphi(y)$$
$$= \widetilde{\varphi}(x + \operatorname{Kern}\varphi)\widetilde{\varphi}(y + \operatorname{Kern}\varphi)\,.$$

Wenn wir sie einschränken zu einer Abbildung von $R/\operatorname{Kern}\varphi$ nach Bild φ, ist sie auch surjektiv, also ein Isomorphismus. ∎

Betrachten wir als Beispiel den Homomorphismus $\varphi\colon \mathbb{Q}[X] \to \mathbb{R}$, der jedes Polynom abbildet auf seinen Wert an der Stelle $x_0 = \sqrt{2}$. Ein Polynom $f \in \mathbb{Q}[X]$ liegt genau dann im Kern, wenn es bei $\sqrt{2}$ eine Nullstelle hat wie beispielsweise das Polynom $X^4 - 4$. In $\mathbb{R}[X]$ ist so ein Polynom durch $(X - \sqrt{2})$ teilbar, aber da $\sqrt{2} \notin \mathbb{Q}$, gibt es in $\mathbb{Q}[X]$ keine entsprechende Zerlegung. Trotzdem hilft uns diese Bemerkung bei der Bestimmung von Kern φ: Berechnen wir in $\mathbb{R}[X]$ den größten gemeinsamen Teiler eines Polynoms $f \in \operatorname{Kern}\varphi$ nach dem EUKLIDischen Algorithmus, erhalten wir als Ergebnis ein Polynom aus $Q[X]$, denn da beide Polynome rationale Koeffizienten haben, sind auch bei den Polynomdivisionen immer alle Quotienten und Reste Polynome aus $\mathbb{Q}[X]$. Daher erhalten wir genau das gleiche Ergebnis wie bei einer Berechnung in $\mathbb{Q}[X]$. Das Ergebnis muß in $\mathbb{R}[X]$ durch $(X - \sqrt{2})$ teilbar sein und ist ein Teiler von $X^2 - 2$; wegen der Irreduzibilität von $X^2 - 2$ in $\mathbb{Q}[X]$ ist der ggT also $X^2 - 2$. Somit ist jedes Polynom aus Kern φ ein Vielfaches von $X^2 - 2$, und umgekehrt liegt auch jedes Vielfache von $X^2 - 2$ im Kern, da bereits $X^2 - 2$ bei $x_0 = \sqrt{2}$ verschwindet.

Auch das Bild von φ läßt sich leicht bestimmen: Setzen wir $\sqrt{2}$ ein in ein Polynom mit rationalen Koeffizienten, erhalten wir als Ergebnis offenbar immer eine Zahl der Form $a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$. Umgekehrt erhalten wir, wenn wir f variieren, auch alle Zahlen dieser Art, denn $f = bX + a$ liefert den Wert $a + b\sqrt{2}$.

Nach dem Homomorphiesatz ist also $\mathbb{Q}[X]/\operatorname{Kern}\varphi \cong \mathbb{Q} \oplus \mathbb{Q}\sqrt{2}$. Das Urbild von $\sqrt{2}$ ist dabei die Nebenklasse von X, was wir auch so interpretieren können, daß wir die in $\mathbb{Q}$ unlösbare Gleichung $X^2 = 2$ im Ring $\mathbb{Q}[X]/(X^2-2)$ „gelöst“ haben: Die „Lösung“ ist die Nebenklasse von X modulo dem Ideal $I = (X^2-2)$, denn da $-(X^2-2)$ in I liegt, liegen X^2 und $X^2-(X^2-2) = 2$ in derseolben Nebenklasse modulo I, d.h. $(X+I)^2 = X^2 + I = 2 + I$.

Auf den ersten Blick mag dies wie ein überflüssiger Taschenspielertrick erscheinen; wenn wir uns aber daran erinnern, wie die komplexen Zahlen aus den reellen konstruiert wurden, dann entspricht das genau der *Definition* von $\mathbb{C}$ als $\mathbb{R}[X]/(X^2+1)$, wobei die Nebenklasse von X mit i bezeichnet wird.

Betrachten wir allgemein einen Körper k und ein irreduzibles Polynom $f \in k[X]$ vom Grad mindestens zwei. Dann hat f in k keine Nullstelle, denn wäre $z \in k$ eine Nullstelle, so wäre $(X-z)$ ein Teiler von f, was für ein irreduzibles Polynom vom Grad mindestens zwei nicht der Fall sein kann. Es ist aber natürlich möglich, daß k in einem größeren Körper K enthalten ist, in dem f eine Nullstelle z hat. Auch hier können wir den Homomorphismus

$$\varphi\colon \begin{cases} k[X] \to K \\ \quad f \mapsto f(z) \end{cases}$$

betrachten. Sein Kern enthält natürlich das Polynom f, denn $f(z) = 0$. Wie jedes Polynom aus $\operatorname{Kern}\varphi$ ist f in $K[X]$ durch $X-z$ teilbar; für ein ein beliebiges Polynom $g \in \operatorname{Kern}\varphi$ ist daher der in $K[X]$ berechnete ggT von f und g durch $X-z$ teilbar. Da keine der Rechenoperation bei der Anwendung des EUKLIDischen Algorithmus auf zwei Polynome aus $k[X]$ aus $k[X]$ hinaus führt, liegt dieser ggT in $k[X]$ und teilt natürlich das irreduzible Polynom f. Da er in $K[X]$ durch $X-z$ teilbar ist, hat er mindestens den Grad eins, kann also keine Einheit sein und ist somit gleich f. Damit ist g ein Vielfaches von f, d.h. $\operatorname{Kern}\varphi = (f)$.

Nach dem Homomorphiesatz ist $k[X]/(f)$ daher isomorph zu einem Teilring von K. Dieser Teilring ist tatsächlich sogar ein Körper: Schreiben wir wieder zur besseren Unterscheidung $I = (f)$, so ist $g + I$ genau

dann vom Nullelement des Rings $k[X]/I$ verschieden, wenn g nicht in I liegt. Wegen der Irreduzibilität von f sind f und g dann teilerfremd; da $k[X]$ ein EUKLIDischer Ring ist, gibt es also Polynome $g', g' \in k[X]$, so daß $g'g + f'f = 1$ ist. Also ist $g'g = 1 - f'f \in 1 + I$ und $(g' + I)(g + I) = g'g + I = 1 + I$. Somit hat jedes von Null verschiedene Element ein multiplikatives Inverses; $k[X]/I$ ist also ein Körper. In diesem Körper hat f das Element $X + I$ als Nullstelle, denn setzt man X in f ein, passiert gar nichts; setzt man also $X + I$ ein, erhält man $f + I = 0 + I$ und damit das Nullelement von $k[X]/I$.

Wir haben damit zu einem irreduziblen Polynom $f \in k[X]$ einen Erweiterungskörper gefunden, in dem das Polynom eine Nullstelle hat. Wenn wir eine numerische Lösung suchen, sind wir damit noch nicht viel weiter; wir brauchen dann zusätzlich eine Einbettung des Körpers $k[X]/I$ in einen Körper wie $\mathbb{R}$ oder $\mathbb{C}$. Im nächsten Kapitel werden wir aber sehen, daß uns der Körper $k[X]/I$ eine große Hilfe ist, bei der Untersuchung der Nullstellen des Polynoms f und der Möglichkeit, sie durch Grundrechenarten und Wurzeln auszudrücken.

Der Homomorphiesatz führt uns auch zu einer Verallgemeinerung des chinesischen Restesatzes auf Ringe und Ideale. Beginnen wir mit dem Fall von nur zwei Idealen:

Lemma: R sei ein kommutativer Ring, und I, J seien Ideale von R. Dann gibt es einen Monomorphismus von Ringen

$$\varphi\colon \begin{cases} R/(I \cap J) \to R/I \oplus R/J \\ \qquad\quad x \mapsto (x + I, x + J) \end{cases} .$$

Beweis: Es gibt natürlich einen (Ring-)Homomorphismus

$$\widetilde{\varphi}\colon \begin{cases} R \to R/I \oplus R/J \\ x \mapsto (x + I, x + J) \end{cases}$$

Ein Element $x \in R$ liegt genau dann im Kern von φ, wenn sowohl $x + I$ das Nullelement von R/I ist als auch $x + J$ das von R/J, das heißt x liegt sowohl in I als auch in J, und somit ist $\operatorname{Kern}\widetilde{\varphi} = I \cap J$. Nach dem Homomorphiesatz ist daher $R/(I + J) \cong \operatorname{Bild}\overline{\varphi}$, und da $\operatorname{Bild}\overline{\varphi}$

natürlich eine Teilmenge von $R/I \oplus R/J$ ist, haben wir die Behauptung bewiesen. ∎

Wir können allerdings nicht erwarten, daß dieser Monomorphismus stets ein Isomorphismus ist: Wenn wir $\mathbb{Z}$ nach $\mathbb{Z}/(4) \oplus \mathbb{Z}/(10)$ abbilden, kann etwa das Element $\big(1 + (4), 2 + (10)\big)$ unmöglich ein Urbild haben, denn dieses müßte ja sowohl gerade als auch ungerade sein. Da 4 und 10 beide gerade sind, kann $\big(y + (4), z + (10)\big)$ höchstens dann im Bild von $\overline{\varphi}$ liegen, wenn $y \equiv z \bmod 2$.

Bevor wir uns überlegen, was wir im allgemeinen Fall sagen können, zunächst eine

Vorbemerkung: Sind $I' \subset I \lhd R$ zwei Ideale eines Rings R, so ist die Projektion $\pi\colon R/I$ die Hintereinanderausführung der Projektion $\pi'\colon R \to I'$ und des Homomorphismus

$$\varphi\colon \begin{cases} R/I' \to R/I \\ x + I' \mapsto x + I \end{cases} .$$

Beweis: φ ist wohldefiniert, da I' ganz in I liegt, und für jedes $x \in R$ ist $(\varphi \circ \pi')(x) = \varphi(x + I') = x + I = \pi(x)$. ∎

Betrachten wir nun zu zwei Idealen eines kommutativen Rings R die drei natürlichen Projektionen

$$R \to R/I\,, \quad R \to R/J \quad \text{und} \quad R \to R/(I + J)\,,$$

wobei

$$I + J = \{x + y \mid x \in I \text{ und } y \in J\}$$

ist. Dies ist ein Ideal von R, denn für $x_1, x_2 \in I$ und $y_1, y_2 \in \mathbb{R}$ liegt wegen der Kommutativität und Assoziativität der Addition auch $(x_1 + y_1) + (x_2 + y_2) = (x_1 + x_2) + (y_1 + y_2)$ in $I + J$, und für $r \in R$ ist wegen des Distributivgesetzes auch $r(x_1 + y_1) = rx_1 + ry_1 \in I + J$.

Nach der Vorbemerkung haben wir dann auch Abbildungen

$$R/(I \cap J) \to R/I\,, \quad R/(I \cap J) \to R/J \quad \text{und} \quad R/(I \cap J) \to R/(I + J)\,.$$

Da I und J Teilmengen von $I + J$ sind (setze $y = 0$ *bzw.* $x = 0$), gibt uns die Vorbemerkung außerdem noch Abbildungen $\pi_1 \colon R/I \to R/(I + J)$ und $\pi_2 \colon R/J \to R/(I + J)$. Außerdem haben wir noch die natürliche Projektion

$$\pi \begin{cases} R \to R/(I + J) \\ x \mapsto x + (I + J) \end{cases} .$$

In der Abbildungsfolge

$$\begin{array}{ccccc} & & & & R/I & & \\ & & & \nearrow & & \searrow & \\ R & \to & R/(I \cap J) & & \longrightarrow & & R/(I + J) \\ & & & \searrow & & \nearrow & \\ & & & & R/J & & \end{array}$$

ist es offensichtlich gleichgültig, auf welchem Weg wir von R nach $R/(I + J)$ gehen; wenn es zu $(y + I, z + J) \in R/I \oplus R/J$ ein $x \in R$ gibt, so daß $(y + I, z + J) = (x + I, z + J)$ ist, muß also gelten

$$\pi_1(y + I) = \pi_2(z + J) = \pi(x) .$$

Ist umgekehrt $\pi_1(y + I) = \pi_2(z + J)$, so ist $y + (I + J) = z + (I + J)$, also $y - z \in I + J$. Es gibt daher Elemente $i \in I$ und $j \in J$, so daß $y - z = i + j$ ist und damit $y - i = z + j$. Da $y - i \in y + I$ und $z + j \in z + J$, wird $x = y - i = z + j$ daher von φ auf $(y + I, z + J)$ abgebildet, so daß dieses Element im Bild liegt. Somit haben wir gezeigt

Lemma: Die Abbildung

$$\varphi \colon \begin{cases} R/(I \cap J) \to R/I \oplus R/J \\ x \mapsto (x + I, x + J) \end{cases}$$

induziert einen Isomorphismus von $R/(I \cap J)$ auf

$$\big\{(x + I, y + J) \in R/I \oplus R/J \;\big|\; x + (I + J) = y + (I + J)\big\} .$$

∎

Im Falle $I + J = R$ besteht $R/(I + J)$ nur aus einem Element, so daß φ surjektiv ist. Durch vollständige Induktion folgt:

Chinesischer Restesatz für Ringe: R sei ein kommutativer Ring und $I_1, \ldots, I_r$ seien Ideale von R derart, daß $I_\mu + I_\nu = R$ für alle $\mu \neq \nu$. Dann gibt es einen Isomorphismus von Ringen

$$\varphi\colon R/(I_1 \cap \cdots \cap I_r) \to R/I_1 \oplus \cdots \oplus R/I_r\ .$$

Beweis: Für $r = 1$ gibt es nichts zu beweisen; für $r = 2$ haben wir den Satz gerade bewiesen.

Für $r > 2$ betrachten wir die Ideale $I = I_1 + \cdots + I_{r-1}$ und $J = I_r$. Nach dem gerade bewiesenen Lemma ist $R/(I \cap J) \cong R/I \oplus R/J$, also

$$R/(I_1 \cap \cdots \cap I_r) \cong R/(I_1 + \cdots + I_{r-1}) \oplus R/I_r\ .$$

Nach Induktionsvoraussetzung ist

$$R/(I_1 + \cdots I_{r-1}) \cong R/I_1 \oplus \cdots R/I_{r-1}\ ,$$

also ist

$$R/(I_1 \cap \cdots \cap I_r) \cong R/I_1 \oplus \cdots \oplus R/I_r\ .$$

Speziell für $R = \mathbb{Z}$ und Ideale $I_\nu = (m_\nu)$ erhalten wir den klassischen chinesischen Restesatz. Um Klammern zu sparen, schreiben wir künftig einfach, wie schon bisher bei der additiven Gruppe, $\mathbb{Z}/m$ auch für den *Ring* $\mathbb{Z}/(m)$; außerdem sagen wir meist einfach x, wenn wir die Nebenklasse $x + (m)$ meinen. Damit erhalten wir den folgenden Spezialfall:

Satz: Für paarweise teilerfremde natürliche Zahlen $m_1, \ldots, m_r$ ist die Abbildung

$$\varphi\colon \begin{cases} \mathbb{Z}/m_1 \cdots m_r \to \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r \\ \qquad\qquad x \mapsto (x \bmod m_1, \ldots, x \bmod m_r) \end{cases}$$

ein Isomorphismus von Ringen. ∎

Korollar: Sind $m_1, \ldots, m_r$ paarweise teilerfremd, so gibt es einen Isomorphismus multiplikativer Gruppen

$$\left(\mathbb{Z}/m_1 \cdots m_r\right)^\times \cong \left(\mathbb{Z}/m_1\right)^\times \oplus \cdots \oplus \left(\mathbb{Z}/m_r\right)^\times\ .$$

Beweis: Ein Isomorphismus $\varphi\colon R \to S$ von Ringen induziert einen Isomorphismus $R^\times \to S^\times$ zwischen den Einheitengruppen, denn ist $x \in R^\times$, so gibt es ein $y \in R$ mit $xy = 1$, also ist auch $\varphi(x)\varphi(y) = 1$. Ist umgekehrt $\varphi(x)$ eine Einheit von S, so gibt es in S ein multiplikatives Inverses, das sich wegen der Surjektivität von φ als $\varphi(y)$ mit einem $y \in R$ schreiben läßt. Da $\varphi(xy) = \varphi(x)\varphi(y) = 1 = \varphi(1)$ ist, muß $xy = 1$ sein wegen der Injektivität von φ.

Für das zu beweisende Korollar besagt dies, daß die Einheitengruppen der Ringe $\mathbb{Z}/(m_1 \cdots m_r)$ und $\mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_r$ isomorph sind. Da die Multiplikation sowohl in einer direkten Summe von Ringen als auch in einer direkten Summe von Gruppen komponentenweise definiert ist, ist letztere Gruppe isomorph zur direkten Summe der Einheitengruppen $\left(\mathbb{Z}/m_\mu\right)^\times$, womit das Korollar bewiesen ist.

∎

Definition: Für eine natürliche Zahl $m \geq 2$ bezeichnen wir $\left(\mathbb{Z}/m\right)^\times$ als die *prime Restklassengruppe modulo* m; ihre Gruppenordnung wird mit $\varphi(m)$ bezeichnet. Die Funktion $\varphi\colon \mathbb{N} \setminus \{1\} \to \mathbb{N}$ heißt EULERsche *φ-Funktion.*

LEONHARD EULER (1707–1783) wurde in Basel geboren und ging auch dort zur Schule und, im Alter von 14 Jahren, zur Universität. Dort legte er zwei Jahre später die Magisterprüfung in Philosophie ab und begann mit dem Studium der Theologie; daneben hatte er sich seit Beginn seines Studium unter Anleitung von JOHANN BERNOULLI mit Mathematik beschäftigt. 1726 beendete er sein Studium in Basel und bekam eine Stelle an der Petersburger Akademie der Wissenschaften, die er 1727 antrat. Auf Einladung FRIEDRICHS DES GROSSEN wechselte er 1741 an die preußische Akademie der Wissenschaften; nachdem sich das Verhältnis zwischen den beiden dramatisch verschlechtert hatte, kehrte er 1766 nach St. Petersburg zurück. Im gleichen Jahr erblindete er vollständig; trotzdem schrieb er rund die Hälfte seiner zahlreichen Arbeiten (Seine gesammelten Abhandlungen umfassen 73 Bände) danach. Sie enthalten bedeutende Beiträge zu zahlreichen Teilgebieten der Mathematik, Physik, Astronomie und Kartographie.

Das gerade bewiesene Korollar zeigt, daß die EULERsche φ-Funktion in manchen Fällen multiplikativ ist, genauer:

Definition: Eine Funktion φ von einer Teilmenge der natürlichen Zahlen nach $\mathbb{N}$ heißt *schwach multiplikativ,* wenn für zwei teilerfremde Zahlen m, n gilt: $\varphi(mn) = \varphi(m)\varphi(n)$.

Lemma: Die EULERsche φ-Funktion ist schwach multiplikativ.

Beweis: Sind m und n teilerfremd, so ist nach obigem Korollar $\left(\mathbb{Z}/mn\right)^\times \cong \left(\mathbb{Z}/m\right)^\times \oplus \left(\mathbb{Z}/n\right)^\times$. Die Gruppe links hat $\varphi(mn)$ Elemente; rechts steht, mengentheoretisch gesehen, das kartesische Produkt zweier Mengen mit $\varphi(m)$ und $\varphi(n)$ Elementen. Dies beweist die Behauptung. ∎

Die Voraussetzung, daß m und n teilerfremd sind, ist notwendig: Beispielsweise enthält $\left(\mathbb{Z}/4\right)^\times$ die Nebenklassen der Eins und der Drei, so daß $\varphi(4) = 2$ ist. Im Ring $\mathbb{Z}/2$ ist nur die Eins eine Einheit, d.h. $\varphi(2) = 1$ und $\varphi(2 \cdot 2) \neq \varphi(2) \cdot \varphi(2)$.

Wir können die Elemente der primen Restklassengruppe auch bestimmen, ohne daß wir zu jedem ein Inverses finden müssen:

Lemma: Die Nebenklasse $x+(m)$ in $\mathbb{Z}/m$ liegt genau dann in $\left(\mathbb{Z}/m\right)^\times$, wenn ggT$(x, m) = 1$ ist.

Beweis: Sind x und m teilerfremd, so liefert uns der erweiterte EUKLIDische Algorithmus ganze Zahlen y, n, so daß $xy + mn = 1$ ist, also $xy = 1 - mn \equiv 1 \bmod m$. Somit ist x eine Einheit.

Umgekehrt gibt es zu jeder Einheit x ein y, so daß $xy \equiv 1 \bmod m$ ist, es gibt also ein $n \in \mathbb{Z}$, so daß $xy = 1 + mn$ oder $xy - mn = 1$ ist. Daher muß jeder gemeinsame Teiler von m und n auch die Eins teilen; die beiden Zahlen sind also teilerfremd. ∎

Ist $m = p_1^{e_1} \cdots p_r^{e_r}$ die Primzerlegung einer natürlichen Zahl $m \geq 2$, so können wir $\varphi(m)$ wegen der schwachen Multiplikativität der EULERschen φ-Funktion berechnen, sobald wie die Werte $\varphi(p_i^{e_i})$ kennen. Eine ganze Zahl ist genau dann teilerfremd zu $p_i^{e_i}$, wenn sie nicht durch p teilbar ist. Unter den Zahlen von 0 bis $p_i^{e_i} - 1$ ist jede p_i-te durch p_i teilbar, also $p_i^{e_i-1}$ Stück, so daß $\varphi(p_i^{e_i}) = p_i^{e_i} - p_i^{e_i-1} = p_i^{e_i-1}(p_i - 1)$ dieser Zahlen nicht durch p_i teilbar sind. Damit folgt:

Satz: Für $m = p_1^{e_1} \cdots p_r^{e_r}$ ist $\varphi(m) = p_1^{e_1-1} \cdots p_r^{e_r-1}(p_1-1)\cdots(p_r-1)$. ∎

Für ein Produkt $m = pq$ zweier Primzahlen ist also $\varphi(m) = (p-1)(q-1)$; dies zeigt noch einmal, warum diese Zahl beim RSA-Verfahren eine so wichtige Rolle spielt.

Auch wenn die additive Gruppe $\mathbb{Z}/m$ stets zyklisch ist, gibt es natürlich keinen Grund, daß auch die prime Restklassengruppe $(\mathbb{Z}/m)^\times$ zyklisch sein müßte: $(\mathbb{Z}/12)^\times$ etwa besteht aus den vier Nebenklassen $1, 5, 7$ und 11, die allesamt das Quadrat eins haben, ist also isomorph zur KLEINschen Vierergruppe. Ist allerdings $m = p$ eine Primzahl, so ist $\mathbb{Z}/p$ ein Körper, und in diesem Fall ist $(\mathbb{Z}/p)^\times$ zyklisch nach dem folgenden

Satz: Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.

Beweis: Da die multiplikative Gruppe eines Körpers mit q Elementen aus allen Körperelementen außer der Null besteht, hat sie die Ordnung $q-1$, d.h. nach LAGRANGE ist die Ordnung eines jeden Elements ein Teiler von $q-1$. Wir müssen zeigen, daß es mindestens ein Element gibt, dessen Ordnung *genau* $q-1$ ist.

Für jeden Primteiler p_i von $q-1$ hat die Polynomgleichung

$$x^{(q-1)/p_i} = 1$$

höchstens $(q-1)/p_i$ Lösungen im Körper; es gibt also zu jedem p_i ein Körperelement a_i mit $a_i^{(q-1)/p_i} \neq 1$.

q_i sei die größte Potenz von p_i, die $q-1$ teilt, und $g_i = a_i^{(q-1)/q_i}$ die $(q-1)/q_i$-te Potenz von a_i. Dann ist

$$g_i^{q_i} = a_i^{q-1} = 1 \quad \text{und} \quad g_i^{\frac{q_i}{p_i}} = a_i^{\frac{q-1}{p_i}} \neq 1\,;$$

g_i hat also die Ordnung q_i. Da die verschiedenen q_i Potenzen verschiedener Primzahlen p_i sind, hat daher das Produkt g aller g_i das Produkt aller q_i als Ordnung, also $q-1$. Damit ist die multiplikative Gruppe des Körpers zyklisch.

∎

Definition: Ein Element g eines endlichen Körpers k heißt *primitive Wurzel,* wenn es die zyklische Gruppe $k^\times$ erzeugt.

Selbst im Fall der Körper $\mathbb{F}_p = \mathbb{Z}/p$ gibt es keine Formel, mit der man eine solche primitive Wurzel explizit in Abhängigkeit von p angeben kann. Üblicherweise wählt man zufällig ein Element aus und testet, ob es die Ordnung $p-1$ hat. Die Wahrscheinlichkeit dafür ist offenbar $\varphi(p-1) : (p-1)$, was für die meisten Werte von p recht gut ist. Der Test, ob die Ordnung gleich $p-1$ ist, läßt sich allerdings nur dann effizient durchführen, wenn die Primteiler p_i von $p-1$ bekannt sind, denn dann kann man einfach testen, ob alle Potenzen mit den Exponenten $(p-1)/p_i$ von eins verschieden sind. Für große Werte von p, wie sie in der Kryptographie benötigt werden, kann dies ein Problem sein, so daß man hier im allgemeinen von faktorisierten Zahlen r ausgeht und dann testet, ob $r+1$ prim ist.

Ist p eine Primzahl und a eine primitive Wurzel modulo p, so ist die Abbildung

$$\begin{cases} \mathbb{Z}/(p-1) \to (\mathbb{Z}/p)^\times \\ \qquad\quad x \mapsto a^x \end{cases}$$

ein Gruppenisomorphismus. Auch für große Primzahlen p ist es mit relativ geringem Aufwand möglich, das Bild eines Elements x zu berechnen; wir können dabei genauso vorgehen, wie bei der RSA-Verschlüsselung. Für die Berechnung der Umkehrfunktion, den sogenannten diskreten Logarithmus modulo p zur Basis a, sind allerdings keine effizienten Algorithmen bekannt, und daher lassen sich auch mit dieser Funktion Kryptoverfahren konzipieren.

Das älteste und einfache ist ein von DIFFIE und HELLMAN entwickeltes Verfahren, wie zwei Personen über eine unsichere Leitung einen Schlüssel für ein Kryptoverfahren vereinbaren können ohne daß sie vorher irgendwelche geheime Information vereinbar haben; auch kein öffentlicher Schlüssel ist notwendig.

Die beiden Teilnehmer einigen sich zunächst (über die unsichere Leitung) auf eine Primzahl p und eine natürliche Zahl a derart, daß die Potenzfunktion $x \mapsto a^x$ möglichst viele Werte annimmt. Als nächstes

wählt Teilnehmer A eine Zufallszahl $x < p$ und B entsprechend ein $y < p$. A schickt $u = a^x \bmod p$ an B und erhält dafür $y = a^y \bmod p$ von diesem. Sodann berechnet A die Zahl

$$v^x \bmod p = \left(a^y\right)^x \bmod p = a^{xy} \bmod p$$

und B entsprechend

$$u^y \bmod p = \left(a^x\right)^y \bmod p = a^{xy} \bmod p\,;$$

beide haben also auf verschiedene Weise dieselbe Zahl berechnet, die sie zum Beispiel verwenden können, um daraus einen Schlüssel für ein symmetrisches Kryptosystem zu bestimmen. Verfahren dazu gibt es mehr als genug: Sie könnten etwa die letzten oder sonst irgendwelche Bits dieser Zahl verwenden, aber auch einen irgendwie definierten Hashwert.

Ein Gegner, der den Datenaustausch abgehört hat, kennt die Zahlen p, a, u und v; er kann also problemlos alle möglichen Zahlen modulo p der Art $a^{\alpha x+\beta y} = u^\alpha \cdot v^\beta$ berechnen. Es fällt aber schwer, sich eine Art und Weise vorzustellen, wie er $a^{xy} \bmod p$ finden kann, ohne den diskreten Logarithmus von u oder v zu berechnen. (Bewiesen ist hier, wie üblich, natürlich nichts.)

In der Praxis wird dieses Verfahren nur selten verwendet wegen der folgenden Angriffsmöglichkeit:

Nehmen wir an, der Gegner habe eine gewisse Kontrolle über das Netz, in dem der Datenaustausch stattfindet – beispielsweise, weil er Systemverwalter eines für die betreffende Verbindung unbedingt notwendigen Knotenrechners ist. Dann kann er eine sogenannte *man in the middle attack* durchführen: Er fängt alle Datenpakete zwischen A und B ab und ersetzt sie durch selbstfabrizierte eigene Pakete.

Damit kann er sich gegenüber A als B auszugeben und umgekehrt: Alles, was A an B zu schicken glaubt, geht tatsächlich an den Gegner G, und alles was B von A zu erhalten glaubt, kommt tatsächlich von G. In Gegenrichtung ist es natürlich genauso.

Im einzelnen läuft der Angriff folgendermaßen ab:

Falls die Zahlen a und p nicht ohnehin Konstanten eines Verbunds sind, dem A und B angehören, läßt G die Kommunikation, die zu deren

Vereinbarung führt, ungehindert zu: In diesem Stadium beschränkt er sich auf reines Abhören.

Als nächstes wählen A und B ihre Zufallszahlen $x < p$ und $y < p$; gleichzeitig wählt G eine Zufallszahl $z < p$ oder vielleicht auch zwei verschiedene solche Zahlen z_A und z_B für die beiden Teilnehmer.

Wenn A die Zahl $u = a^x \bmod p$ an B schickt, fängt G diese Nachricht ab und ersetzt sie durch $w_B = a^{z_B} \bmod p$; entsprechend fängt er Bs Nachricht $y = a^y \bmod p$ ab und schickt stattdessen $w_A = a^{z_A}$ an A. Dies führt dazu, daß am Ende A und G einen gemeinsamen Schlüssel s_A haben und B und G einen gemeinsamen Schlüssel s_B. Sowohl A als auch B glauben, der ihnen bekannte Schlüssel s_A *bzw.* s_B sei aus $a^{xy} \bmod p$ abgeleitet und senden nun damit verschlüsselte Nachrichten an ihren Partner. Diese Nachrichten fängt G ab, entschlüsselt sie mit dem Schlüssel, den er mit dem Absender gemeinsam hat, und verschlüsselt sie anschließend, gegebenenfalls nach einer seinen Interessen entsprechenden Modifikation, mit dem Schlüssel, den er mit dem Empfänger gemeinsam hat. Auf diese Weise hat er die gesamte Konversation unter Kontrolle, ohne daß A und B etwas merken.

Die Möglichkeit für diese Attacke kommt natürlich daher, daß sich A und B nicht sicher sein können, den jeweils anderen am anderen Ende der Leitung zu haben. Die kryptographisch einwandfreie Modifikation, die das Verfahren gegen diese Art von Angriff sicher macht, bestünde beispielsweise darin, daß A und B ihre Nachrichten x und y vor dem Versenden unterschreiben – aber dann verschwindet auch wieder der Vorteil, daß sie ohne Kenntnis irgendeines Schlüssels miteinander kommunizieren können: Zur Verifikation einer Unterschrift braucht man schließlich den öffentlichen Schlüssel des Unterschreibenden.

Falls sich A und B hinreichend gut kennen, um die Stimme des jeweils anderen am Telephon einigermaßen sicher zu erkennen, können sie diese Art von Attacke auch dadurch erschweren, daß sie nach dem Austausch von u und v per Telephon über diese Zahlen (z.B. die 317. bis 320. Ziffer) und gegebenenfalls auch noch über Schwänke aus ihrer gemeinsamen Jugendzeit reden; dann müßte der Angreifer zusätzlich noch ein begabter, kundiger und reaktionsschneller Stimmenimitator sein, der

auch die Telephonverbindung als *man in the middle* so angreifen kann, daß weder A noch B etwas merkt. Bei Videokonferenzen könnte man auch die Zahlen langsam über den Bildschirm des jeweils anderen laufen lassen. Die volle Sicherheit einer Schlüsselvereinbarung via RSA wird aber nicht erreicht, und da oft zumindest einer der Teilnehmer ein Unternehmen ist, das sich einen zertifizierten RSA-Schlüssel leisten kann, werden Schlüssel für symmetrische Kryptoverfahren in der Praxis sehr viel häufiger via RSA vereinbart als via DIFFIE-HELLMAN.

Zwischen RSA und den Verfahren mit diskreten Logarithmen gibt es einen ganz wesentlichen Unterschied: Wer die Faktorisierung des RSA-Moduls N kennt, kann die sonst schwer zugängliche Umkehrfunktion von $x \mapsto x^e \bmod N$ leicht berechnen, so daß Potenzieren mit e direkt als Verschlüsselung benutzt werden kann.

Bei der modularen „Exponentialfunktion“ $x \mapsto a^x \bmod p$ sind keine speziellen Wahlen von a und p bekannt, die vermöge einer geheimen Information zu einer einfachen Umkehrfunktion führen – diskrete Logarithmen sind für alle gleich schwer zu berechnen.

Die geheime Information bei einem asymmetrischen Verfahren auf der Basis diskreter Logarithmen kann daher nur in der Kenntnis *einzelner* diskreter Logarithmen bestehen: Wer für einen speziellen Wert x die Potenz $u = a^x \bmod p$ berechnet hat, weiß anschließend, daß x der diskrete Logarithmus von u modulo p zur Basis a ist.

Bei diesen sehr viel spezielleren „Geheimnissen“ ist klar, daß Kryptoverfahren auf der Basis von diskreten Logarithmen anders aussehen müssen als RSA.

Im Prinzip könnte man die Schlüsselvereinbarung nach DIFFIE und HELLMAN direkt zu einem Verschlüsselungsverfahren erweitern: Nachdem das gemeinsame Geheimnis $\gamma = a^{xy} \bmod p$ vereinbart ist, können Nachrichtenblöcke m_i mit $0 \leq m_i < p - 1$ in beide Richtungen verschlüsselt werden als $c_i = \gamma m_i \bmod p$. Da beide Partner den Wert von γ kennen, können sie leicht nach dem erweiterten EUKLIDischen Algorithmus ein δ berechnen, so daß $\gamma\delta \equiv 1 \bmod p$, und die verschlüsselte Information kann einfach entschlüsselt werden als $m_i = \delta c_i \bmod p$.

Solange nur ein einzelner Block m übertragen werden soll, ist dagegen nichts einzuwenden. Sobald aber mehrere Blöcke zu übertragen sind, wird dieses Verfahren verwundbar gegen Angriffe mit bekanntem Klartext: Falls ein Gegner für einen einzigen Chiffreblock c_i den Klartextblock m_i kennt (oder errät), kann er $\delta = m_i/c_i \bmod p$ berechnen und damit den gesamten Klartext entschlüsseln. Um das Verfahren sicher zu machen, müßte man daher für jeden Block ein eigenes γ vereinbaren und dazu jedes Mal das gesamte DIFFIE-HELLMAN-Protokoll durchlaufen, was sehr aufwendig wäre.

Das Verfahren von ELGAMAL umgeht dieses Problem, indem es exakt dieselbe Mathematik mit einem leicht modifizierten Protokoll zu einem asymmetrischen Kryptoverfahren macht:

Die Parameter a und p sind entweder allgemein bekannte Systemparameter, oder jeder Teilnehmer A wählt sie selbst als Teil seines öffentlichen Schlüssels. Zusätzlich wählt er sich eine geheime Zufallszahl x und veröffentlicht $u = a^x \bmod p$.

Wer immer eine Nachricht $m_1, \ldots, m_r$ an A schicken möchte, erzeugt für jeden Block m_i eine Zufallszahl y_i berechnet daraus $v_i = a^{y_i} \bmod p$ und $c_i = u^{y_i} m_i$. Dann schickt er die Folge der Paare (v_i, c_i) an A. Der Chiffretext ist damit doppelt so lang wie der Klartext, was das Verfahren insbesondere für lange Texte nicht sonderlich attraktiv macht.

A muß zur Entschlüsselung den Multiplikator u^{y_i} kennen; dann kann er m_i als $c_i u^{-y_i}$ berechnen. Da $u^{y_i} \equiv a^{xy_i} \equiv \left(a^{y_i}\right)^x \equiv {v_i}^x \bmod p$ ist, hat er damit keine Probleme.

TAHER ELGAMAL wurde 1955 in Ägypten geboren. Er studierte zunächst Elektrotechnik an der Universität Kairo; nachdem er dort seinen BSc bekommen hatte, setzte er seine Studien fort an den Information Systems Laboratories der Stanford University. In seiner Masterarbeit ging es hauptsächlich um Systemtheorie, jedoch hörte er parallel auch freiwillig viele Mathematikvorlesungen und kam auf diesem Weg zur Kryptographie, die zum Thema seiner Doktorarbeit wurde. Nach dem Studium arbeitete er für eine ganze Reihe von Unternehmen, beispielsweise war er von 1995–1998 als Chefwissenschaftler von Netscape maßgeblich an der Entwicklung von SSL beteiligt. Zeitweise arbeitete er auch in selbst gegründeten Firmen. 2006 wurde er Chief Technology Officer der Tumbleweed Communications Corporation; seitdem diese 2008 von Axway übernommen wurde, ist er deren Chief Security Officer sowie Berater einer Reihe weiterer Unternehmen. Seit 2013 ist er Chief Technical Officer for Security des Cloud-Anbieters salesforce.com. Sein

Name wird in der Literatur oft auch EL GAMAL oder ELGAMAL geschrieben; die obige Schreibweise ist die, die er selbst im Englischen benutzt. Eine mögliche Transkription der arabischen Schreibweise seines Namens ins Deutsche wäre TAHIR AL-DSCHAMAL; „al“ ist der bestimmte Artikel im Arabischen.

Der offensichtliche Angriff eines Gegners besteht darin, aus u und a den diskreten Logarithmus x zu ermitteln, was nach derzeitigem Stand der Dinge schwierig erscheint. Ob andere Angriffe zum Erfolg führen könnten, ist (wie üblich) unbekannt – hoffentlich auch unseren Gegnern.

Der Nachteil des Verfahrens von ELGAMAL und anderer Verfahren auf der Basis diskreter Logarithmen ist, daß man für jeden Nachrichtenblock zwei Blöcke übertragen muß. Daher werden solche Verfahren nur selten zur Verschlüsselung eingesetzt; sie liefern aber nützliche und viel verwendete Ansätze für elektronische Unterschriften.

Eine RSA-Unterschrift sollte nach derzeitigem Sicherheitsstandard eine Länge von mindestens 2048 Bit haben. Was damit unterschrieben wird, ist meist ein Hashwert einer Länge von etwa 256 Bit.

Verglichen mit dieser Länge erscheint eine 2048 Bit lange Unterschrift weit übertrieben. Andererseits wäre eine Unterschrift, die auf diskreten Logarithmen in einem Körper mir nur etwa 2^{256} Elementen beruht, ohne großen Aufwand fälschbar.

Der *Digital Signature Algorithm* DSA bietet einen Ausweg aus diesem Dilemma, indem er zwar in einer großen Gruppe rechnet, dabei aber kurze Unterschriften aus einer deutlich kleineren Untergruppe liefert. Dieser Algorithmus wurde im *Digital Signature Standard* DSS der USA spezifiziert und zählt neben RSA auch zu den von der Bundesnetzagentur festgelegten „Geeigneten Algorithmen“.

Als Ordnung der Untergruppe wählt man eine Primzahl q, für die nach den derzeitigen Empfehlungen der Bundesnetzagentur seit Anfang 2010 eine Länge von mindestens 224 Bit notwendig ist; ab Anfang 2016 erhöht sich die Länge auf mindestens 256 Bit. Diese Längen hängen in erster Linie ab von den verwendeten (und zulässigen) Hashverfahren, nicht so sehr von Sicherheitsanforderungen.

Die Sicherheit wird gewährleistet (soweit dies möglich ist) durch eine

zweite Primzahl p, die so gewählt wird, daß $p \equiv 1 \bmod q$ ist; für ihre Größe sind mindestens 2048 Bit vorgeschrieben.

Primzahlen $p \equiv 1 \bmod q$ sind nicht schwerer zu finden als beliebige Primzahlen: Falls man bei der Primzahlsuche wirklich auf Nummer sicher geht und Zufallszahlen auf Primalität testet, nimmt man hier einfach Zufallszahlen k und testet $kq + 1$ auf Primalität. Falls man mit ERATOSTHENES arbeitet, kann man das Sieben leicht so modifizieren, daß nur Zahlen der Form $kq + 1$ gesiebt werden. An den Erfolgschancen ändert dies in beiden Fällen nichts: Nach einem Satz von DIRICHLET über Primzahlen in arithmetischen Folgen ist die Dichte der Primzahlen der Form $kq + i$ für jedes i mit $0 < i < q$ dieselbe; in der Größenordnung n ist also weiterhin im Mittel jede $\ln n$-te solche Zahl eine Primzahl. (Tatsächlich sind es sogar geringfügig mehr, denn außer q selbst gibt es natürlich keine Primzahl der Form $p = kq$. Bei den Größenordnungen von q mit denen wir arbeiten, geht aber der Unterschied zwischen q und $q - 1$ definitiv im „Rauschen“ der im Kleinen sehr unregelmäßigen Primzahlverteilung unter.)

Als nächstes muß ein Element g gefunden werden, dessen Potenzen im Körper $\mathbb{F}_p$ eine Gruppe der Ordnung q bilden. Auch das ist einfach: Man starte mit irgendeinem Element $g_0 \in \mathbb{F}_p \setminus \{0\}$ und berechne seine $(p-1)/q$-te Potenz. Falls diese ungleich eins ist, muß sie wegen $g_0^{p-1} = 1$ die Ordnung q haben; andernfalls muß ein neues g_0 betrachtet werden.

Die so bestimmten Zahlen q, p und g werden veröffentlicht und können auch in einem ganzen Netzwerk global eingesetzt werden. Geheimer Schlüssel jedes Teilnehmers ist eine Zahl x zwischen eins und $q - 1$; der zugehörige öffentliche Schlüssel ist $u = g^x \bmod p$.

Unterschreiben lassen sich mit diesem Verfahren Nachrichtenblöcke m mit $0 \leq m < q$; im allgemeinen wird es sich dabei um Hashwerte der eigentlich zu unterschreibenden Nachricht handeln. Dazu wählt man für jede Nachricht eine Zufallszahl k mit $0 < k < q$ und berechnet

$$r = (g^k \bmod p) \bmod q\,.$$

Man beachte, daß es in dieser Formel nicht um Restklassen geht, sondern um Zahlen aus $\mathbb{N}_0$: Aus $x \equiv y \bmod p$ folgt selbstverständlich nicht,

daß auch $x \equiv y \bmod q$ sein muß. Der Operator mod in dieser Gleichung bezeichnet den (nichtnegativen) Divisionsrest, also eine ganze Zahl zwischen 0 und $p-1$ *bzw.* $q-1$.

Da q eine Primzahl ist, hat k ein multiplikatives Inverses modulo q; man kann also modulo q durch k dividieren und somit eine Zahl s berechnen, für die gilt

$$sk \equiv m + xr \bmod q$$

Die Unterschrift unter die Nachricht m besteht dann aus den beiden Zahlen r und $s = k^{-1}(m + xr) \bmod q$, die beide zwischen 0 und $q-1$ liegen. Sie kann nur erzeugt werden von jemanden, der den geheimen Schlüssel x kennt.

Überprüfen kann die Unterschrift allerdings jeder: Ist t das multiplikative Inverse zu s modulo q, so ist $k \equiv tsk \equiv tm + xtr \bmod q$, also, da g die Ordnung q hat, $g^k \bmod p = g^{tm} g^{xtr} \bmod p = g^{tm} u^{tr} \bmod p$. Modulo q ist die linke Seite gleich r, und auf der rechten Seite können sowohl g^{tm} als auch u^{tr} aus öffentlicher Information und der Unterschrift berechnet werden. Modulo q kann diese Gleichung somit überprüft werden; die Unterschrift wird anerkannt, wenn

$$r \equiv (g^{tm} u^{tr} \bmod p) \bmod q$$

ist. (Die beiden Potenzen und ihr Produkt müssen natürlich auch hier zunächst modulo p berechnet werden: Zwei modulo p kongruente Zahlen sind praktisch nie auch kongruent modulo q.)

Ein Angreifer müßte sich nach allem was wir wissen x aus u verschaffen, müßte also ein diskretes Logarithmenproblem modulo der großen Primzahl p lösen, so daß der Sicherheitsstandard dem des diskreten Logarithmenproblems modulo p entsprechen sollte, obwohl die Unterschriften deutlich kürzer sind.

Diskrete Logarithmen lassen sich nicht nur für die prime Restklassengruppe definieren; wir können grundsätzlich für jede Gruppe G und jedes Element $a \in G$ der Ordnung r die „Exponentialfunktion“

$$\varphi\colon \begin{cases} \mathbb{Z}/r \to G \\ \quad x \mapsto a^x \end{cases}$$

betrachten und ihre Umkehrfunktion Bild $\varphi \to G$ als diskreten Logarithmus bezeichnen. Für manche Gruppen ist dieser recht einfach zu berechnen, etwa wenn G eine additive zyklische Gruppe ist; für andere kann die Berechnung sogar noch deutlich aufwendiger sein als im Fall der primen Restklassengruppe. Ein in der kryptographischen Praxis viel verwendetes Beispiel sind diskrete Logarithmen für elliptische Kurven. Dabei handelt es sich um ebene Kurven vom Grad drei (ohne Doppelpunkte), also Kurven mit Gleichungen wie $y^2 = x^3 + 2x + 5$. Man kann auf diesen Kurven eine Addition von Punkten erklären, mit einem „unendlich fernen“ zusätzlichen Punkt O als Nullelement. Mit diskreten Logarithmen auf solchen Kurven arbeitet beispielsweise die Unterschriftsfunktion der neuen Bundespersonalausweise.