Einführung in die Algebra

Vorlesung Sommersemester 2005

Prof. Dr. Heinz Spindler

Fachbereich Mathematik/Informatik der Universität Osnabrück

Dies ist das Vorlesungsskript zur Vorlesung. Es gibt in knapper Form die Definitionen, Sätze, Beweise und Beispiele wieder. Ausführlicheres findet man in der Literatur. Insbesondere sei das Buch von M. Artin [1] als zusätzliche Lektüre empfohlen.

Literatur

Lehrbücher

[1] Artin, M.: Algebra, Birkhäuser Advanced Texts, Birkhäuser Verlag Basel 1993

[2] Van der Waerden, B. L.: Algebra, Erster Teil, Springer-Verlag Berlin Heidelberg New York 1966

[3] Reiffen/Scheja/Vetter: Algebra, BI Mannheim 1969

[4] Lang, S.: Undergraduate Algebra, (Undergraduate Texts in Mathematics), 3rd edition, Springer 2005

[5] Schafmeister/Wiebe: Grundzüge der Algebra, B.G.Teubner Stuttgart 1978

[6] Kostrikin, A.I.: Introduction to Algebra, universitext, Springer 1982

[7] Hungerford, Thomas W.: Algebra, GTM 73, Springer 1974

[8] Hornfeck, B.: Algebra, de Gruyter 1976

[9] Scheja/Storch: Lehrbuch der Algebra, Teil1 und Teil 2, Teubner Stuttgart 1988

[10] Wüstholz, G.: Algebra, vieweg 2004

[11] Bosch, S.: Algebra, Springer Verlag

Vorlesungsskripten

[12] Bruns, W.: Einführung in die Algebra, Osnabrück SS 2001

[13] Römer, T.: Einführung in die Algebra, Osnabrück SS 2003

[14] Vogt, R.: Einführung in die Algebra, Osnabrück SS 2000

- **Weiterführende und spezielle Literatur**

[15] Shafarevich, I. R.: Basic Notions in Algebra, Springer-Verlag Heidelberg 1997

[16] Ledermann, W.: Einführung in die Gruppentheorie, vieweg 1977

[17] Lidl/Niederreiter: Finite Fields, Encyclopedia of Mathematics 20, Addison-Wesley 1983

[18] Artin, E.: Galoissche Theorie, Verlag Harri Deutsch, Thun 1988

Gruppen

1 Grundbegriffe und Beispiele

Inhalt: Definition der Begriffe *Monoid*, *Gruppe*, erste Beispiele von Gruppen: die allgemeine lineare Gruppe $GL_n(K)$, die volle symmetrische Gruppe einer Menge. Der Begriff der *Untergruppe*, Untergruppen von $\mathbb{Z}$, *zyklische Gruppen*, *Erzeugendensystem* einer Gruppe, Beispiel: Zwei Erzeugende von $SL_2(\mathbb{Z})$. Definition der Begriffe *Isomorphismus*, *Homomorphismus*, *Automorphismus*, *Kern* und *Bild* eines Homomorphismus, *Ordnung* eines Gruppenelements, Beispiel: Unterguppen von S^1, Einheitswurzeln, Permutationen und ihre *Zykeldarstellung*, Permutationsmatrizen, die alternierende Gruppe.

- **Definition 1.1**

Es sei M eine Menge und

$$\cdot : M \times M \longrightarrow M,\ (x, y) \mapsto x \cdot y$$

eine zweistellige Verknüpfung auf M. Wir schreiben wie üblich auch kurz xy an Stelle von $x \cdot y$.

(1.1.1) Die Verknüpfung heißt *assoziativ*, wenn

$$x(yz) = (xy)z$$

für alle $x, y, z \in M$ gilt.

(1.1.2) Die Verknüpfung heißt *kommutativ*, wenn

$$xy = yx$$

für alle $x, y \in M$ gilt.

(1.1.3) Ein Element $e \in M$ heißt *neutrales Element* der Verknüpfung, wenn

$$ex = xe = x$$

für alle $x \in M$ gilt.
Es gibt höchstens ein neutrales Element, denn ist e' ein weiteres neutrales Element, so gilt $e = ee' = e'$.

■ **Definition 1.2**

(1.2.1) Ein *Monoid* ist eine Menge M mit einer assoziativen Verknüpfung, die ein neutrales Element besitzt. Man schreibt auch ausführlich $(M, \cdot, e)$ für ein Monoid M.

Es sei $(M, \cdot, e)$ ein Monoid.

(1.2.2) Sind $x, y \in M$ und gilt $xy = e = yx$, so heißt y ein *Inverses* von x.

Jedes Element x besitzt höchstens ein Inverses, denn sind y, y' Inverse von x, so gilt $y = ye = y(xy') = (yx)y' = ey' = y'$.

(1.2.3) $x \in M$ heißt *invertierbar*, wenn es ein Inverses $y \in M$ von x gibt. Dieses wird mit x^{-1} bezeichnet. Die Menge der invertierbaren Elemente in M wird mit $M^\times$ bezeichnet.

(1.2.4) Es gelten die Kürzungsregeln: Sind $x, y, z \in M$ und ist z invertierbar, so gilt:

(1.2.4.1) Aus $xz = yz$ folgt $x = y$,

(1.2.4.2) Aus $zx = zy$ folgt $x = y$.

Der Beweis von (1.2.4.1) ergibt sich durch Multiplikation mit z^{-1} von rechts: $xz = yz \Longrightarrow x = x \cdot 1 = x(zz^{-1}) = (xz)z^{-1} = (yz)z^{-1} = y(zz^{-1}) = y \cdot 1 = y$. Analog folgt (1.2.4.2) durch Multiplikation mit z^{-1} von links.

(1.2.5) Ist $x \in M$, so kann man die Potenzen x^n für $n \in \mathbb{N}$ induktiv definieren:

$$x^0 = e,\ x^n = xx^{n-1}$$

für $n > 0$. Ist x invertierbar, so kann man auch die negativen Potenzen x^n definieren durch

$$x^n := (x^{-1})^{-n}$$

für $n < 0$. Es gelten die bekannten Potenzregeln

$$x^{n+m} = x^n x^m,\ x^{nm} = (x^n)^m$$

für alle $x \in M$, $n, m \in \mathbb{N}$. Ist $x \in M^\times$, so gelten die Regeln sogar für alle $n, m \in \mathbb{Z}$.

■ **Definition 1.3**

(1.3.1) Eine *Gruppe* ist ein Monoid $(G, \cdot, e)$, in dem jedes Element invertierbar ist.

(1.3.2) Eine Gruppe heißt *abelsch*, wenn ihre Verknüpfung kommutativ ist.
Oft wird eine abelsche Gruppe A additiv geschrieben:
$+ : A \times A \longrightarrow A,\ (x, y) \mapsto x + y$ ist die Verknüpfung. Das neutrale Element wird dann

mit 0 bezeichnet und heißt auch das *Nullelement* von A. Das Inverse von $x \in A$ wird mit $-x$ bezeichnet und heißt auch das *Negative* von x.

- **Lemma 1.4**

Es sei $(G, \cdot, e)$ eine Gruppe.
(1.4.1) Für alle $x, y \in G$ gilt: $(xy)^{-1} = y^{-1}x^{-1}$.
(1.4.2) Für alle $a, b \in G$ besitzt die Gleichung $ax = b$ genau eine Lösung $x \in G$, nämlich $x = a^{-1}b$.

Beweis. Zu (1.4.1):
$(xy)(y^{-1}x^{-1}) = ((xy)y^{-1})x^{-1} = (x(yy^{-1}))x^{-1} = (xe)x^{-1} = xx^{-1} = e$.
Genauso folgt $(y^{-1}x^{-1})(xy) = e$.
Zu (1.4.2): $ax = b \Longleftrightarrow x = a^{-1}b$. □

In einem Monoid, also auch in einer Gruppe, kann man endliche Produkte bilden ohne auf die Klammerung zu achten. Man darf im allgemeinen jedoch nicht die Reihenfolge der Faktoren ändern.

- **Beispiele 1.5**

(1.5.1) Aus der linearen Algebra sind uns schon eine Reihe von Gruppen bekannt: Die *allgemeine lineare Gruppe* $\mathrm{GL}_n(K)$ der $n \times n$-Matrizen mit Einträgen in einem Körper K, die *orthogonale Gruppe* $O(n)$ der reellen orthogonalen $n \times n$-Matrizen.

(1.5.2) $(\mathbb{N}, +, 0)$ ist ein kommutatives Monoid, aber keine Gruppe.

(1.5.3) $(\mathbb{Z}, +, 0)$ ist eine abelsche Gruppe.

(1.5.4) Ist X irgendeine nicht-leere Menge, so ist die Menge M der Selbstabbildungen $f : X \longrightarrow X$ mit der Komposition als Verknüpfung ein Monoid. Das neutrale Element ist die identische Abbildung id_X.

(1.5.5) Ist X irgendeine nicht-leere Menge, so ist die Menge $S(X)$ der bijektiven Selbstabbildungen $f : X \longrightarrow X$ mit der Komposition als Verknüpfung eine Gruppe. Das neutrale Element ist die identische Abbildung id_X. Diese Gruppe heißt die *volle symmetrische Gruppe* der Menge X. Eine besondere Rolle spielt die Gruppe $S_n = S(X)$, wobei $X = \{1, 2, \ldots, n\}$. S_n heißt die *symmetrische Gruppe n-ten Grades*. Ihre Element heißen auch *Permutationen*. Ein Element $\pi \in S_n$ wird durch seine Wertetabelle

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}$$

vollständig beschrieben. Für $n \geq 3$ ist S_n nicht abelsch. Das sieht man so: Es sei $\pi \in S_n$ die Permutation

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

und $\sigma \in S_n$ die Permutation

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

Dann ist $\pi \circ \sigma(1) = \pi(2) = 1$ und $\sigma \circ \pi(1) = \sigma(3) = 3$. Also ist $\pi \circ \sigma \neq \sigma \circ \pi$.

- **Definition 1.6**

Es sei $(G, \cdot, e)$ eine Gruppe. Eine Teilmenge H von G heißt *Untergruppe* von G, wenn gilt:
(1.6.1) Für alle $x, y \in H$ ist $xy \in H$,
(1.6.2) $e \in H$,
(1.6.3) Ist $x \in H$, so ist auch $x^{-1} \in H$.

Ist G endlich, so folgt (1.6.3) aus (1.6.1) und (1.6.2), denn für $x \in H$ die Abbildung $H \longrightarrow H, y \mapsto xy$ injektiv und da H endlich ist, auch automatisch bijektiv und somit ist insbesondere e im Bild dieser Abbildung, d.h. es gibt ein $y \in H$ mit $xy = e$. Damit ist $x^{-1} \in H$.

- **Lemma 1.7**

Eine nicht-leere Teilmenge H einer Gruppe G ist genau dann eine Untergruppe, wenn gilt:
(1.7.1) Für alle $x, y \in H$ ist $xy^{-1} \in H$.

Beweis. Übung! □

- **Beispiele 1.8**

(1.8.1) $\mathrm{SO}(n) \subset \mathrm{O}(n) \subset \mathrm{GL}_n(\mathbb{R})$ sind Untergruppen (→Lineare Algebra).

(1.8.2) $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right\}$ ist eine Untergruppe von S_3. Allgemeiner: Ist X eine nicht-leere Menge und $a \in X$ ein festes Element, so ist $H = \{f \in S(X) \mid f(a) = a\}$ eine Untergruppe der symmetrischen Gruppe $S(X)$. Dies folgt sofort mit Lemma 1.7.

(1.8.3) Für $m \in \mathbb{Z}$ ist $H = \mathbb{Z}m := \{nm \mid n \in \mathbb{Z}\}$, also die Menge der ganzzahligen Vielfachen von m, eine Untergruppe von $\mathbb{Z}$. Dies sind die einzigen Untergruppen von $(\mathbb{Z}, +)$. Die letzte Aussage beweist man so: Ist $H \subset \mathbb{Z}$ irgendeine Untergruppe und ist $H \neq \{0\}$, so gibt es eine von Null verschiedene Zahl $k \in H$. Da H eine Untergruppe von $\mathbb{Z}$ ist, ist auch $-k \in H$. Damit gibt es auf jeden Fall eine positive Zahl in H. Es sei nun m die kleinste positive Zahl in H. Dann gilt natürlich $\mathbb{Z}m \subset H$.

Wir zeigen, dass auch $H \subset \mathbb{Z}\, m$ gilt. Zum Beweis wählen wir eine beliebige Zahl $k \in H$. Dividieren wir k durch m so erhalten wir $k = q\, m + r$ mit $q \in \mathbb{Z}$ und einem Rest $r \in \mathbb{Z}$ mit $0 \le r < m$. Da $k, m \in H$, ist auch $r = k - q\, m \in H$. Da $r < m$ und da nach Definition m die kleinste positive Zahl in H ist, muss $r \le 0$, also (wegen $r \ge 0$) sogar $r = 0$ gelten. Damit ist $k = q\, m \in \mathbb{Z}\, m$. Damit ist $H \subset \mathbb{Z}\, m$ bewiesen. Es gilt wie behauptet $H = \mathbb{Z}\, m$.

(1.8.4) Es sei K ein Körper und V ein K-Vektorraum. Dann ist
$H = \{f \in S(V) \mid \exists\, A \in \mathrm{GL}(V), b \in V\, \forall\, v \in V : f(v) = A(v) + b\}$
eine Untergruppe von $S(V)$, die sogenannte *affine Gruppe* von V, die man auch mit $\mathrm{Aff}(V)$ bezeichnet. (Beweis: Übung)

(1.8.5) Es sei $(M, \cdot, e)$ ein Monoid. Dann ist $M^\times$ mit der Multiplikation eine Gruppe. Dazu muss man sich nur überlegen, dass mit $x, y \in M^\times$ auch $x\, y \in M^\times$, vgl (1.4.1).

- **Proposition 1.9**

Es sei G eine Gruppe und M eine Teilmenge von G. Es sei $M^{-1} := \{x^{-1} \mid x \in M\}$.
(1.9.1) Die Menge aller endlichen Produkte $x_1 \cdot \ldots \cdot x_n$ von Elementen $x_j \in M \bigcup M^{-1} \bigcup \{e\}$ ist eine Untergruppe $\langle M \rangle$ von G.
(1.9.2) Ist H eine Untergruppe von G mit $M \subset H$, so gilt $\langle M \rangle \subset H$.

Beweis. zu (1.9.1): Offensichtlich sind die Bedingungen (1.6.1) - (1.6.3) erfüllt.
zu (1.9.2): Ist $M \subset H$, so ist auch $M \bigcup M^{-1} \bigcup \{e\} \subset H$ und somit gilt auch $\langle M \rangle \subset H$. □

- **Definition 1.10**

Es sei G eine Gruppe und M eine Teilmenge von G.
(1.10.1) $\langle M \rangle$ heißt die von M *erzeugte Untergruppe*.

(1.10.2) M heißt ein *Erzeugendensystem* von G, wenn $\langle M \rangle = G$.

(1.10.3) G heißt *endlich erzeugt*, wenn G ein endliches Erzeugendensystem besitzt.

(1.10.4) G heißt *zyklisch*, wenn G von einem Element erzeugt wird, wenn also ein Element $x \in G$ existiert, so dass

$$G = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}.$$

x heißt dann ein *Erzeuger* von G.

- **Beispiele 1.11**

(1.11.1) $(\mathbb{Z}, +)$ ist zyklische Gruppe mit 1 als Erzeuger. -1 ist ebenfalls ein Erzeuger.

(1.11.2) Jedes Element x einer Gruppe G erzeugt eine zyklische Untergruppe $\langle x\rangle$ von G.

(1.11.3) (*Die Hilbertsche Modulgruppe*) Zum Beispiel erzeugt die Matrix

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

die unendliche zyklische Untergruppe $\langle S\rangle = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \, n \in \mathbb{Z} \right\}$ von $\mathrm{SL}_2(\mathbb{Z})$. Dagegen erzeugt die Matrix

$$D = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

eine zyklische Untergruppe mit vier Elementen, denn

$D^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $D^1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $D^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $D^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $D^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

und somit ist $D^n = D^r$ für $n \in \mathbb{Z}$ mit $n = 4q + r,\ 0 \le r < 4$, also

$\langle D\rangle = \{E, D, D^2, D^3\}$.

Wir bemerken: Ist $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ eine beliebige Matrix in $\mathrm{SL}_2(\mathbb{Z})$, so kann man A durch wiederholte elementare Spaltenumformungen vom Typ

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b + an \\ c & d + cn \end{pmatrix}$$

und vom Typ

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$$

auf die Form $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ bringen. Den Beweis lassen wir dem Leser als Übung.

Hinweis: Wegen $ad - bc = 1$ sind c, d teilerfremd. Durch wiederholtes Anwenden der Operation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a & b - qa \\ c & d - qc \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} qa - b & a \\ qc - d & c \end{pmatrix}$$

kommt man daher (Euklidischer Algorithmus) in der zweiten Zeile schließlich auf $(0, \pm 1)$, also auf eine Matrix der Form

$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = S^n$ oder $\begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix} = S^{-n} D^2$.

Damit ist gezeigt, dass die Gruppe $\mathrm{SL}_2(\mathbb{Z})$ von den beiden Matrizen S und D erzeugt wird. Man erkennt sofort, dass die folgende Relation zwischen den Erzeugern besteht:

$$D^2 S = S D^2.$$

Es ist aber

$$D S - S D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

denn $D S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $S D = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. $\mathrm{SL}_2(\mathbb{Z})$ ist also nicht abelsch. Diese Gruppe heißt die *Hilbertsche Modulgruppe* oder *elliptische Modulgruppe*. Sie spielt eine wichtige Rolle in der Theorie der elliptischen Kurven und der Modulformen. Literatur: Freitag / Busam: Funktionentheorie 1, Kapitel 5, 3. Auflage, Springer 2000

- **Definition 1.12**

Es seien $M = (M, \cdot, e), M' = (M', \cdot, e')$ Monoide. Ein *Monoidhomomorphismus* (kurz: *Homomorphismus*) von M nach M' ist eine Abbildung $\varphi : M \longrightarrow M'$, so dass gilt:
(1.12.1) $\varphi(x y) = \varphi(x)\varphi(y)$ für alle $x, y \in M$,
(1.12.2) $\varphi(e) = e'$.

(1.12.3) Ein *Isomorphismus* ist ein bijektiver Homomorphismus.

(1.12.4) Sind M, M' Gruppen, so nennt man einen Monoidhomomorphismus bzw. Monoidisomorphismus auch *Gruppenhomomorphismus*
bzw. *Gruppenisomorphismus.*
Die Eigenschaft (1.12.2) ist in diesem Fall eine Folgerung aus (1.12.1) und der Kürzungsregel (1.2.4.2), denn
$\varphi(e)\varphi(x) = \varphi(e x) = \varphi(x) = e'\varphi(x) \Longrightarrow \varphi(e) = e'$.

- **Lemma 1.13**

Es sei $\varphi : M \longrightarrow M'$ ein Monoidhomomorphismus. Dann gilt
(1.13.1) Ist $x \in M$ invertierbar, so ist $\varphi(x)$ invertierbar in M' und es gilt

$$\varphi(x)^{-1} = \varphi(x^{-1}).$$

(1.13.2) Ist H eine Untergruppe von $M^\times$, so ist $\varphi(H)$ eine Untergruppe von $M'^\times$.

Beweis. zu (1.13.1): Aus $e = x x^{-1} = x^{-1} x$ folgt wegen (1.12.1) und (1.12.2) sofort $e' = \varphi(e) = \varphi(x)\varphi(x^{-1}) = \varphi(x^{-1})\varphi(x)$ und damit die Behauptung.
zu (1.13.2): $\varphi(H)$ ist nicht-leer und die Bedingung (1.7.1) ist für $\varphi(H)$ erfüllt, denn nach (1.13.1) gilt für $x, y \in H$: $\varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(x y^{-1}) \in \varphi(H)$, weil $x y^{-1} \in H$. □

■ **Lemma 1.14**

(1.14.1) Ist $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus, $H' \subset G'$ eine Untergruppe, so ist $\varphi^{-1}(H')$ eine Untergruppe von G.
Insbesondere ist der *Kern* von φ, das ist die Menge $\ker\varphi := \{x \in G \mid \varphi(x) = e'\}$ eine Untergruppe von G.

(1.14.2) Ist $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus, $H \subset G$ eine Untergruppe, so ist $\varphi(H)$ eine Untergruppe von G'.
Insbesondere ist das *Bild* von φ, das ist die Menge $\operatorname{im}\varphi := \{\varphi(x) \mid x \in G\}$ eine Untergruppe von G'.

(1.14.3) Ein Gruppenhomomorphismus $\varphi : G \longrightarrow G'$ ist genau dann injektiv, wenn $\ker\varphi = \{e\}$.

Beweis. zu (1.14.1): Da $e \in \varphi^{-1}(H')$, ist $\varphi^{-1}(H') \neq \emptyset$ und es ist nur (1.7.1) zu verifizieren:
$x, y \in \varphi^{-1}(H') \Longrightarrow \varphi(x), \varphi(y) \in H' \Longrightarrow \varphi(xy^{-1}) = \varphi(x)\,\varphi(y)^{-1} \in H' \Longrightarrow xy^{-1} \in \varphi^{-1}(H')$.
zu (1.14.2): Für $u, v \in \operatorname{im}\varphi$ gibt es $x, y \in G$, so dass $u = \varphi(x)$, $v = \varphi(y)$ und somit gilt $uv^{-1} = \varphi(x)\,\varphi(y)^{-1} = \varphi(x)\,\varphi(y^{-1}) = \varphi(xy^{-1}) \in \operatorname{im}\varphi$.
zu (1.14.3): Das Argument ist aus der linearen Algebra bekannt: Sei $\ker\varphi = \{e\}$. Ist nun $\varphi(x) = \varphi(y)$, so gilt $e' = \varphi(x)\,\varphi(y^{-1}) = \varphi(xy^{-1})$, also $xy^{-1} \in \ker\varphi$, d. h. $x = y$. φ ist somit injektiv. □

■ **Lemma 1.15**

(1.15.1) Ist G eine Gruppe, so ist $\mathrm{id}_G : G \longrightarrow G$ ein Homomorphismus.

(1.15.2) Sind $\varphi : G \longrightarrow G'$, $\psi : G' \longrightarrow G''$ Gruppenhomomorphismus, so ist auch $\psi \circ \varphi : G \longrightarrow G''$ ein Gruppenhomomorphismus.

(1.15.3) Ein Gruppenhomomorphismus $\varphi : G \longrightarrow G'$ ist genau dann ein Isomorphismus, wenn es einen Gruppenhomomorphismus $\psi : G' \longrightarrow G$ gibt, so dass $\varphi \circ \psi = \mathrm{id}_{G'}$ und $\psi \circ \varphi = \mathrm{id}_G$.

(1.15.4) Die Menge $\operatorname{Aut} G := \{\varphi : G \longrightarrow G \mid \varphi \text{ Isomorphismus}\}$ ist eine Untergruppe von $S(G)$, die sogenannte *Automorphismengruppe* von G.

Beweis. leichte Übung. □

■ **Lemma 1.16**

Es sei $G = \langle x \rangle$ eine zyklische Gruppe mit Erzeuger x. Es sei $\varphi : \mathbb{Z} \longrightarrow G$ die Abbildung $\varphi(n) := x^n$. Dann gilt:
(1.16.1) Die Abbildung φ ist ein surjektiver Gruppenhomomorphismus.
(1.16.2) φ ist Isomorphismus oder $|G| = m < \infty$. Im letzteren Fall ist $\ker \varphi = \mathbb{Z}\, m$ und $G = \{e, x, x^2, \ldots, x^{m-1}\}$. Es gilt also: $x^k = e \Longleftrightarrow m$ ist Teiler von k.
(1.16.3) Zwei zyklische Gruppen mit gleicher Anzahl von Elementen sind isomorph.

Beweis. Zu (1.16.1): Offensichtlich gilt $\varphi(n+m) = x^{n+m} = x^n x^m = \varphi(n)\,\varphi(m)$. Damit ist φ ein Homomorphismus. Da x Erzeuger von G ist, ist φ surjektiv.
zu (1.16.2): φ sei nicht isomorph. Dann gibt es Zahlen $k, n \in \mathbb{Z}, k < n$, so dass $\varphi(k) = \varphi(n)$, also $\varphi(n-k) = \varphi(n)\,\varphi(k)^{-1} = \varphi(k)\,\varphi(k)^{-1} = e$. Für $m = n - k$ gilt somit $\varphi(m) = e$. Es sei nun $m > 0$ die kleinste positive natürliche Zahl mit $\varphi(m) = e$. Ist nun $n \in \mathbb{Z}$, so schreiben wir $n = m\,q + r$ mit $q \in \mathbb{Z}$, $0 \le r < m$ und erhalten
$\varphi(n) = x^n = x^{m\,q}\, x^r = (x^m)^q\, x^r = e\, x^r = x^r$.
Damit besteht also G aus den Potenzen x^k mit Exponenten $k = 0, 1, \ldots, m-1$. Wir zeigen jetzt, dass die Potenzen x^k für $k = 0, 1, \ldots, m-1$ paarweise verschieden sind: Sind $k, l \in \{0, 1, \ldots, m-1\}$, $k < l$, so ist $0 < l - k < m$ und nach Definition von m also $\varphi(l-k) \neq e$, und somit $\varphi(k) \neq \varphi(l)$, d. h. $x^k \neq x^l$. Weiter ist offensichtlich $\mathbb{Z}\, m \subset \ker \varphi$. Sei umgekehrt $n \in \ker \varphi$. Wir schreiben $n = m\,q + r$ mit $q \in \mathbb{Z}$, $0 \le r < m$ und erhalten
$e = \varphi(n) = x^n = x^{m\,q}\, x^r = (x^m)^q\, x^r = e\, x^r = x^r$. Wegen $0 \le r < m$ folgt $r = 0$, also $n = m\,q \in \mathbb{Z}\, m$.
zu (1.16.3): Es seien $G = \langle x \rangle$, $H = \langle y \rangle$ zyklische Gruppen mit m Elementen. Dann ist $\psi : G \longrightarrow H$ mit $\psi(x^k) = y^k (k = 0, 1, \ldots, m-1)$ eine Bijektion und weiter gilt für $k, l \in \{0, 1, \ldots, m-1\}$, $k + l = q\,m + r$ mit $0 \le r < m$ die Relation $x^k\, x^l = x^r$ und somit $\psi(x^k\, x^l) = \psi(x^r) = y^r = y^k\, y^l = \psi(x^k)\,\psi(x^l)$. ψ ist also ein Isomorphismus. □

■ **Definition 1.17**

Es sei G eine Gruppe und $x \in G$. Dann heißt $\operatorname{ord}(x) := |\langle x \rangle| = \inf\{k > 0 \mid x^k = 0\}$ die *Ordnung* von x. Es gilt $1 \le \operatorname{ord}(x) \le \infty$. x heißt Element endlicher Ordnung, wenn $\operatorname{ord}(x) < \infty$. Die Anzahl $|G|$ der Elemente der Gruppe G heißt die *Ordnung* von G.

■ **Beispiele 1.18**

(1.18.1) Es sei S^1 die multiplikative Gruppe der komplexen Zahlen vom Absolutbetrag 1.

$$\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$$

ist eine zyklische Untergruppe der Ordnung n von S^1. Beweis: Da ein komplexes Polynom vom Grad n höchstens n komplexe Nullstellen hat, gilt $|\mu_n| \le n$. Offensichtlich ist μ_n eine Untergruppe von S^1. Wir zeigen, dass

$$\zeta = e^{\frac{2\pi i}{n}}$$

ein Element der Ordnung n in μ_n ist. Dann ist klar, dass $|\mu_n| = n$ ist und dass μ_n von ζ erzeugt wird und somit zyklisch ist. Es gilt

$$\zeta^n = e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1.$$

Ist $0 \le k \le n-1$, so ist $\zeta^k \ne 1$, denn bekanntlich gilt $e^{ix} = 1$ genau dann, wenn $x \in 2\pi\mathbb{Z}$. Die Erzeuger von μ_n heißen *primitive n-te Einheitswurzeln.*

(1.18.2) Ist $x \in \mathbb{R}\setminus\mathbb{Q}$, so ist $u = e^{2\pi i x}$ ein Element der Ordnung ∞ in S^1, denn nach Voraussetzung ist $nx \notin \mathbb{Z}$ für alle $n \in \mathbb{Z}$. Die von u erzeugte zyklische Gruppe $\langle u\rangle \subset S^1$ ist also unendlich, $n \mapsto u^n$ ist ein Isomorphismus $\mathbb{Z} \longrightarrow \langle u\rangle$.

(1.18.3) Weiter gilt für $u = e^{2\pi i x}$, $x \in \mathbb{R}\setminus\mathbb{Q}$ sogar: Die Gruppe $\langle u\rangle$ liegt dicht in S^1. Jede Zahl $z \in S^1$ ist also Grenzwert einer Folge von Potenzen von u. Wie kann man das beweisen? (→Arnold: Gewöhnliche Differentialgleichungen, 2. Auflage Springer 2001, Seite 222) So: Es sei $\varepsilon > 0$. Wir wählen $n \in \mathbb{N}$, $n > 0$, so dass $\frac{2\pi}{n} < \varepsilon$ und unterteilen S^1 in n Kreissegmente

$$X_k = \{e^{2\pi i t} \mid \tfrac{k-1}{n} \le t < \tfrac{k}{n}\},\ k = 1,\ \ldots,\ n,$$

der Bogenlänge $\frac{2\pi}{n}$. Nach dem Dirichletschen Schubfächerprinzip müssen zwei der $n+1$ Elemente $1, u, u^2, \ldots, u^n$, sagen wir u^p, u^q, $p \ne q$, im selben Segment X_k liegen, die Bogenlänge von u^p bis u^q ist also kleiner als $\frac{2\pi}{n}$ und somit gilt für u^s, wobei $s = q - p$ ist, dass die Bogenlänge von 1 bis u^s kleiner als $\frac{2\pi}{n}$ ist. Dann ist natürlich in der Folge u^{sm}, $m = 0, 1, 2, \ldots$ die Bogenlänge zwischen zwei benachbarten Gliedern ebenfalls kleiner als $\frac{2\pi}{n}$, also kleiner als ε . Ist nun $z \in S^1$, so wähle man ein $m \in \mathbb{Z}$, so dass z auf dem Kreissegment zwischen den Gliedern u^{sm} und $u^{s(m+1)}$ liegt. Dann ist die Bogenlänge zwischen z und u^{sm} kleiner als ε. Damit ist die Behauptung bewiesen.

(1.18.4) Die Permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix} \in S_n$ hat die Ordnung n, erzeugt also eine zyklische Untergruppe der Ordnung n.

(1.18.5) Die Abbildung $\varphi : S_n \longrightarrow \mathrm{GL}_n(\mathbb{C})$ mit

$$\varphi(\pi) := (e^{\pi(1)},\ \ldots,\ e^{\pi(n)}) = (\delta_{i\,\pi(j)}),$$

wobei $e^j = [\delta_{1j},\ \ldots,\ \delta_{nj}]$ den j-ten Spalteneinheitsvektor bezeichnet, ist ein Gruppenhomomorphismus. *Beweis*:
$\varphi(\pi)\,\varphi(\sigma) = (\delta_{i\,\pi(j)})\,(\delta_{j\,\sigma(k)}) = (\sum_{j=1}^{n} \delta_{i\,\pi(j)}\,\delta_{j\,\sigma(k)}) = (\delta_{i\,i}\,\delta_{\pi^{-1}(i)\,\sigma(k)}) = (\delta_{i,(\pi\circ\sigma)(k)}) = \varphi(\pi\circ\sigma)$,
denn in der Summe wird nur über j mit $i = \pi(j)$, also $j = \pi^{-1}(i)$ summiert und es gilt

natürlich $\delta_{\nu\mu} = \delta_{\pi(\nu)\pi(\mu)}$. φ ist injektiv, denn ist $\varphi(\pi) = (\delta_{i\pi(j)}) = E = (\delta_{ij})$ die Einheitsmatrix, so muss $\pi(j) = j$, also π die identische Permutation sein. Dieser Homomorphismus ist die Darstellung der Permutationen in S_n durch *Permutationsmatrizen*. Die Permutationsmatrizen bilden eine zu S_n isomorphe Untergruppe von $GL_n(\mathbb{Z})$,

Beispiel: $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, hat die Darstellung $\varphi(\pi) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

(1.18.6) Nach dem Determinatenmultiplikationssatz ist die Abbildung

$$\text{sign} : S_n \longrightarrow \{\pm 1\},\ \text{sign}(\pi) := \det(e^{\pi(1)},\ ...,\ e^{\pi(n)})$$

ein Homomorphismus. Der Kern $A_n = \ker(\text{sign})$ heißt die *alternierende Gruppe n-ten Grades.* Die Elemente aus A_n heißen gerade Permutationen. Nach der Regel $\det(\ldots, v, \ldots, w, \ldots) = -\det(\ldots, w, \ldots, v, \ldots)$ der Determinantenrechnung folgt

$$\text{sign}\,\pi = (-1)^k,$$

wobei k eine Anzahl von Vertauschungen in der Liste $(\pi(1), \ldots, \pi(n))$ ist, die diese Liste in die natürliche Reihenfolge $(1, 2, \ldots, n)$ bringt.

- **Beispiel 1.19**

Wir wollen die Darstellung von Permutationen als Produkt elementfremder Zyklen erklären.

Wir beginnen mit einigen expliziten Beispielen: Es sei

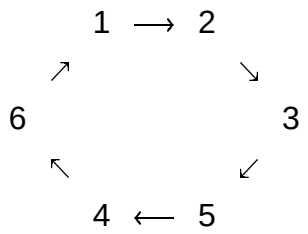
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 2 & 5 & 4 \end{pmatrix} \in S_6$$

Diese Permutation ist ein sogenannter *4-Zyklus*, denn beschreibt man σ durch ein Pfeildiagramm, so ergibt sich ein geschlossener Weg mit den vier Ecken 2, 3, 6, 4 und die nicht vorkommenden Elemente 1 und 5 bleiben unter σ fest.

$$\begin{array}{ccc} 2 & \longrightarrow & 3 \\ \uparrow & & \downarrow \\ 4 & \longleftarrow & 6 \end{array}$$

Wir schreiben kurz: $\sigma = (2\ \ 3\ \ 6\ \ 4)$ für diesen 4-Zyklus. Das ist die sogenannte Zykelschreibweise.

Das folgende Diagramm beschreibt den *6-Zyklus* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 4 & 1 \end{pmatrix} \in S_6$.



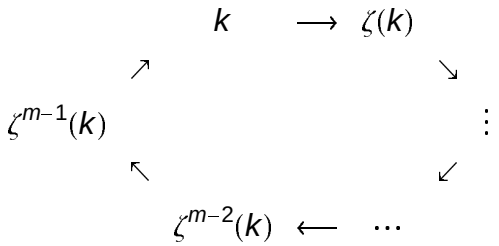
Hier schreiben wir

$$\pi = (1\ \ 2\ \ 3\ \ 5\ \ 4\ \ 6).$$

Diese Schreibweise ist natürlich nicht eindeutig. Mit $(2\ \ 3\ \ 5\ \ 4\ \ 6\ \ 1)$ wird offensichtlich derselbe Zyklus beschrieben. In der Standardform steht das kleinste Element des Zyklus an der ersten Stelle. So ist zum Beispiel $(2\ \ 3\ \ 6\ \ 4)$ die Standardform von $(6\ \ 4\ \ 2\ \ 3)$.

Die allgemeine Definition eines *m*-Zyklus ist nun wohl klar: Es sei $\zeta \in S_n$. Es sei $M = \{1, 2, \ldots, n\}$. Dann ist also $\zeta : M \longrightarrow M$ eine bijektive Abbildung von *M* in sich. ζ heißt *m*-Zyklus, wenn es eine Teilmenge *A* von *M* mit genau *m* Elementen gibt, so dass $\zeta(i) = i$ für alle $i \in M \setminus A$ und für ein $k \in A$ gilt:

$A = \{k, \zeta(k), \zeta^2(k), \ldots, \zeta^{m-1}(k)\}$



A heißt der *Wirkungsbereich* von ζ. Es gilt dann natürlich

$$\zeta^m(k) = k,\ \zeta^{m+1}(k) = \zeta(k),\ \ldots.$$

Die Ordnung eines *m*-Zyklus ist also *m*. ζ erzeugt eine zyklische Untergruppe *H* der Ordnung *m* von S_n. Sind alle Elemente von *H* Zyklen? Offensichtlich nicht! Zum Beispiel ist

$$(2\ \ 3\ \ 6\ \ 4)^2 = (2\ \ 6) \circ (3\ \ 4)$$

das Produkt zweier elementfremder 2-Zyklen.

Es sei jetzt $\sigma \in S_n$. Wir wollen σ als Produkt (=Komposition) elementfremder Zyklen schreiben. Wir beginnen mit $k = 1$. Durch sukzessives Anwenden von σ auf *k* erhalten wir den *m*-Zyklus

$$\zeta = (k, \sigma(k), \sigma^2(k), \ldots, \sigma^{m-1}(k)),$$

wobei m die erste positive Zahl mit $\sigma^m(k) = k$ ist. Bleiben noch Elemente in $M \setminus \{k, \sigma(k), \sigma^2(k), \ ..., \ \sigma^{m-1}(k)\}$ übrig, so findet man weitere Zyklen. Man wählt etwa das minimale l in $M \setminus \{k, \sigma(k), \sigma^2(k), \ ..., \ \sigma^{m-1}(k)\}$ und erhält einen weiteren Zyklus

$$\eta = (l, \sigma(l), \sigma^2(l), \ ..., \ \sigma^{s-1}(l)),$$

wobei s die erste positive Zahl mit $\sigma^s(l) = l$ ist. Die Zyklen ζ und η sind elementfremd, das soll heißen

$$\{k, \sigma(k), \sigma^2(k), \ ..., \ \sigma^{m-1}(k)\} \cap \{l, \sigma(l), \sigma^2(l), \ ..., \ \sigma^{s-1}(l)\} = \emptyset.$$

Wäre nämlich $\sigma^j(k) = \sigma^j(l)$ für gewisse i, j, so wäre
$l = \sigma^{i-j}(k) \in \{k, \sigma(k), \sigma^2(k), \ ..., \ \sigma^{m-1}(k)\}$ im Widerspruch zur Wahl von l.

Man iteriert dies Verfahren solange, bis keine Elemente in M mehr übrig sind. Die so erhaltenen elementfremdem Zyklen ergeben die *Zykeldarstellung* von σ.

Die vollständige Zykeldarstellung einer Permutation kann man folgendermaßen bestimmen.

- Input: $\sigma \in S_n$
- Initialisierung: $M = \{1, 2, \ ..., n\}$, $Z = \emptyset$.
- Solange $M \neq \emptyset$, wählt man $k = \text{Min}(M)$ und bildet
  $\zeta = (k, \sigma(k), \sigma^2(k), \ ..., \sigma^{m-1}(k))$, wobei m der erste positive Exponent mit
  $\sigma^m(k) = k$. Dann setzt man $M := M \setminus \{\sigma^j(k) \mid j = 0, \ ..., m-1\}$ und $Z := Z \bigcup \{\zeta\}$.
- Output: Z, die Liste der Zyklen. Man kann die Einerzyklen weglassen, da sie die Identität beschreiben.

Wir illustrieren dies an einem konkretem Beispiel:

$$n = 12, \ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 1 & 6 & 8 & 5 & 7 & 9 & 2 & 10 & 12 & 11 \end{pmatrix}.$$

Die Zykleldarstellung von σ ist

$$\sigma = (1 \ \ 3) \circ (2 \ \ 4 \ \ 6 \ \ 5 \ \ 8 \ \ 9) \circ (7) \circ (10) \circ (11 \ \ 12).$$

Die 1-Zyklen kann man weglassen, weil diese die Identität beschreiben:

$$\sigma = (1 \ \ 3) \circ (2 \ \ 4 \ \ 6 \ \ 5 \ \ 8 \ \ 9) \circ (11 \ \ 12).$$

Jede Permutation $\sigma \in S_n$ lässt sich bis auf Reihenfolge der Faktoren eindeutig als Produkt elementfremder Zyklen schreiben: $\sigma = \zeta_1 \circ \zeta_2 \circ ... \circ \zeta_s$ mit $\zeta_i \circ \zeta_j = \zeta_j \circ \zeta_i$ und $X_i \cap X_j = \emptyset$ für $i \neq j$, wobei X_i der Wirkungsbereich von ζ_i ist. Wir nennen diese Darstellung die *Zykeldarstellung* von σ. Es ist klar, dass elementfremde Zyklen vertauschbar sind, weil die Identität mit allem vertauschbar ist. Ist d die Ordnung von σ und d_i die Länge von ζ_i, so ist wegen
$e = \sigma^d = \zeta_1{}^d \circ ... \circ \zeta_s{}^d$ und weil $X_i \cap X_j = \emptyset$ für $i \neq j$ auch $\zeta_i{}^d = e$, also d Vielfaches

von d_i. Die Ordnung von σ ist also das kleinste gemeinsame Vielfache der in der Zykeldarstellung von σ auftretenden Zykellängen.

■ Übungen 1

(1.1) Zeigen Sie, dass man den Gruppenbegriff auch folgendermaßen einführen kann:
Eine nicht-leere Menge G zusammen mit einer Verknüpfung $\cdot : G \times G \longrightarrow G$ und einem ausgezeichneten Element $e \in G$ ist eine Gruppe, wenn gilt:
(a) Es gilt das Assoziativgesetz.
(b) e ist linksneutral, d. h.: $e\,x = x$ für alle $x \in G$.
(c) Zu jedem $x \in G$ gibt es mindestens ein linksseitiges Inverses, d. h. ein $y \in G$ mit $y\,x = e$.

(1.2) Es sei $K = \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ der Körper mit fünf Elementen. Welche der folgenden Teilmengen von $G = \mathrm{GL}_2(K)$ ist eine Untergruppe? Bestimme gegebenenfalls die Ordnung der Untergruppe.
(a) $H_1 = \{A \in G \mid \det(A) \in \{1, 4\}\}$, (b) $H_2 = \{A \in G \mid \det(A) = 1\}$,
(c) $H_3 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a\,c \neq 0 \right\}$, (d) $H_4 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \right\}$,
(e) $H_5 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix} \right\}$, (f) $H_6 = \{A \in G \mid \mathrm{Spur}(A) = 1\}$.

(1.3) Es seien $x = (1, 2, 3), y = (1, 2) \in S_3$. Zeigen Sie, dass x, y die Gruppe S_3 erzeugen, genauer, dass $S_3 = \{e, x, x^2, y, y\,x, y\,x^2\}$ gilt und dass die "Relationen" $x^3 = e$, $y^2 = e$, $x^2\,y = y\,x$ gelten. Stellen Sie allein mit Hilfe dieser Relationen und der Gruppenaxiome die "Gruppentafel" (Cayley-Tafel) von S_3 auf. Beispiel: $x \cdot y\,x^2 = x\,(y\,x)\,x = x(x^2\,y)\,x = x^3\,y\,x = y\,x$ usw.

(1.4) Es sei G eine Gruppe und $x, y \in G$ seien vertauschbare Elemente endlicher Ordnung und es gelte $\langle x \rangle \bigcap \langle y \rangle = \{e\}$. Zeigen Sie: Dann gilt $\mathrm{ord}(x\,y) = \mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y))$. Gilt das auch, wenn die Elemente nicht vertauschbar sind? (Betrachte etwa geeignete Elemente der Gruppe $\mathrm{SL}_2(\mathbb{F}_5)$ oder S_3.)

(1.5) Es sei K ein Körper. Es sei $X := \mathbb{P}^1(K)$ die Menge der eindimensionalen Untervektorräume von K^2. X heißt die *projektive Gerade* über K. G sei die Menge der bijektiven Abbildungen $f : X \longrightarrow X$, die von Matrizen $A \in \mathrm{GL}_2(K)$ induziert werden, für die also gilt: $f(K\,u) = K(A\,u)$ für alle Spaltenvektoren $u \in K^2$, $u \neq 0$. Zeige: (a) G ist eine Untergruppe von $S(X)$, (b) Die Abbildung $A \mapsto f$ ist ein surjektiver Gruppenhomomorphismus $\mathrm{GL}_2(K) \longrightarrow G$. Welche Ordnung hat G im Fall $K = \mathbb{F}_p$, wobei p eine Primzahl ist?

(1.6) Es sei K ein Körper. Zeigen Sie: Es gibt einen injektiven Homomorphismus $\varphi : S_3 \longrightarrow \mathrm{GL}_2(K)$, der $x = (1, 2, 3)$ auf $A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ und $y = (1, 2)$ auf $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ abbildet. (Hinweis: Benutzen Sie Aufgabe (1.3).)

(1.7) Es sei G eine Gruppe und x, y seien zwei Elemente in G mit der Eigenschaft $x^7 = e$, $x^4 y = y x^4$. Dann sind x und y vertauschbar.

(1.8) Zeigen Sie: (a) Die symmetrische Gruppe S_n wird von den *Transpositionen* $(1, 2), (2, 3), \ ..., (n-1, n)$ erzeugt.
(b) Die symmetrische Gruppe wird von $(1, 2)$ und $(1, 2, 3, \ ..., n)$ erzeugt.

(1.9) Zeigen Sie: Für $n \geq 3$ wird die alternierende Gruppe A_n von den Dreierzyklen $(1, 2, k)$, $k = 3, \ ..., n$ erzeugt.

(1.10) Zerlegen Sie die folgenden Permutationen in elementfremde Zyklen und bestimmen Sie die Ordnung:

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 4 & 7 & 10 & 5 & 8 & 9 & 2 & 6 \end{pmatrix}$,

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 2 & 7 & 8 & 9 & 10 & 6 \end{pmatrix}$,

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 9 & 8 & 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$.

Welches ist die maximale Ordnung von Elementen in S_{10}?

(1.11) Mit C_n werde 'die' zyklische Gruppe n-ter Ordnung bezeichnet. Bestimmen Sie die Automorphismengruppe von C_n für $n = 2, 3, 4, 5$. Kann man eine allgemeine Aussage über $\mathrm{Aut}(C_n)$ machen?

(1.12) Es sei G eine Gruppe. $\varphi : G \longrightarrow G$ sei ein Automorphismus. Zeigen Sie:
(a) Für $x \in G$ gilt $\mathrm{ord}(x) = \mathrm{ord}(\varphi(x))$
(b) Für $x, y \in G$ gilt $\mathrm{ord}(xy) = \mathrm{ord}(yx)$

(1.13) Zeigen Sie: $H = \{(1), (12)(34), (13)(24), (14)(23)\}$ ist eine abelsche Untergruppe von S_4 und es gilt $\mathrm{Aut}(H) \cong S_3$.

(1.15) Zeigen Sie: Untergruppen zyklischer Gruppen sind wieder zyklisch.

(1.16) Finden Sie eine Gruppe, in der es Elemente der Ordnung 2 gibt, deren Produkt von unendlicher Ordnung ist.

(1.17) Schreiben Sie $A = \begin{pmatrix} 23 & 32 \\ 5 & 7 \end{pmatrix}$ als Produkt der in (1.11.3) definierten Erzeuger $S, D \in \mathrm{SL}_2(\mathbb{Z})$.

2 Gruppenoperationen

Inhalt: Die grundlegenden Begriffe über Gruppenoperationen: *G-Menge*, *Linksoperation*, *Rechtsoperation*, *treue* Operation, Beispiele: Operation von $S(X)$ auf X, die *Diedergruppe*, Linksoperationen auf X als Homomorphismen $\Phi : G \longrightarrow \mathrm{Aut}(S(X))$, *äquivariante* und *invariante* Abbildungen, der Begriff der *Kategorie*, die Kategorie der *G*-Mengen, der Begriff des *Isomorphismus*. *Bahnen*, der *Bahnenraum*, *Standgruppen*, Beispiele: Die Operation einer zyklischen Untergruppe $\langle\sigma\rangle$ von S_n auf $X = \{1, 2, 3, \ldots, n\}$.
Die Bahnen von $\mathrm{SO}(2)$ in $\mathbb{R}^2$. Die Bahnen der 1-Parametergruppe eines Vektorfelds.
Der Begriff des *G-Moduls*, d. h. der *linearen Darstellung*.
Linksnebenklassen einer Untergruppe H einer Gruppe G. Die Menge G/H der Linksnebenklassen als *G*-Menge. *konjugierte Untergruppen* als Standgruppen verschiedener Bahnelemente, die Indexformel und die Bahnformel, *homogene G*-Mengen, *freie G*-Mengen, Beispiele: das Hopfbündel $S^3 \longrightarrow S^2$, S^n als homogener $\mathrm{SO}(n+1)$-Raum, die orthogonale Darstellung $\mathrm{SU}(2) \longrightarrow \mathrm{SO}(3)$ von $\mathrm{SU}(2)$.

■ Definition 2.1

Es sei G eine Gruppe und X eine Menge. Eine *(Links-)Operation* von G auf X ist eine Abbildung $\cdot : G \times X \longrightarrow X$, $(g, x) \mapsto g\,x$ mit den Eigenschaften
(2.1.1) $e\,x = x$ für alle $x \in X$,
(2.2.2) $(g\,h)\,x = g(h\,x)$ für alle $x \in X$, $g, h \in G$.

Eine Menge mit der Operation einer Gruppe G nennt man auch eine *G-Menge.*

Analog führt man den Begriff der *Rechtsoperation* $\cdot : X \times G \longrightarrow X$, $(g, x) \mapsto x\,g$. Sie hat folgende Eigenschaften
(2.1.3) $x\,e = x$ für alle $x \in X$,
(2.2.4) $x(g\,h) = (x\,g)\,h$ für alle $x \in X$, $g, h \in G$.

(2.1.5) Die Operation $\cdot : G \times X \longrightarrow X$, $(g, x) \mapsto g\,x$ heißt *treu*, wenn ausschließlich das neutrale Element von G identisch auf X operiert, wenn also gilt: Ist $g\,x = x$ für alle $x \in X$, so ist $g = e$.

- **Beipiele 2.2**

(2.2.1) Es sei X eine Menge und G sei die volle Symmetriegruppe $S(X)$ von X. Dann operiert G in natürlicher Weise auf X durch $\varphi x := \varphi(x)$ für $\varphi \in G, x \in X$. Dieses ist sozusagen der Prototyp einer Operation. Untergruppen von G operieren dann ebenfalls auf X.
Untergruppen von G erhält man zum Beispiel, wenn X Struktur besitzt und man die Elemente von G betrachtet, die diese Struktur respektieren oder wenn man nur die Tranformationen aus G betrachtet, die eine gegebene Teilmenge von X invariant lassen. Die folgenden Beispiele sind von dieser Natur.

(2.2.2) Es sei V ein n-dimensionaler euklidischer Vektorraum, $G = O(V)$ die orthogonale Gruppe von V (→Lineare Algebra). Dann operiert G auf V und zwar wie in (2.2.1) durch $g\,x := g(x)$.

(2.2.3) Es sei $X \subset \mathbb{R}^2$ die Menge der Ecken

$$P_k = (\cos \tfrac{2\pi k}{n}, \sin \tfrac{2\pi k}{n}),\ k = 0, 1, \ ..., n-1$$

eines regelmäßigen n-Ecks mit Mittelpunkt Null. Es sei G die von der Drehung

$$D = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}$$

und der Spiegelung

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

erzeugte Untergruppe von $O(2)$. Jedes Element A von G permutiert die Ecken P_k. Man erhält somit eine Operation $G \times X \longrightarrow X$.
Die Ecke P_k werde einfach mit ihrer Nummer $k+1$ notiert. Dann entspricht D die Permutation

$$\delta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix} = (\,1\ \ 2\ \ 3\ \ \cdots\ \ n\,)$$

und S entspricht die Permutation

(2.2.3.1) $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & k & k+1 & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & k+2 & k+1 & \cdots & 3 & 2 \end{pmatrix},$$

falls $n = 2k$ gerade ist und die Permutation

(2.2.3.2) $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & k & k+1 & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & k+1 & k & \cdots & 3 & 2 \end{pmatrix},$$

falls $n = 2k - 1$ ungerade ist.
Die Zykeldarstellung von σ enthält die elementfremden Transpositionen $(2, n), (3, n-1), (4, n-2), \ldots$.

Die Gruppe G ist die Symmetriegruppe des regelmäßigen n-Ecks. Sie heißt *Diedergruppe* n-ter Ordnung und wird auch mit $\mathcal{D}_n$ bezeichnet. Wir fassen $\mathcal{D}_n = \langle \sigma, \delta \rangle$ als Untergruppe von S_n auf. Sie enthält stets die zyklische Gruppe $C_n = \langle \delta \rangle$ als Untergruppe.

- **Lemma 2.3**

Es sei G eine Gruppe, X eine Menge und $\cdot : G \times X \longrightarrow X$, $(g, x) \mapsto g\,x$ eine Operation von G auf X. Für $g \in G$ ist dann $\Phi_g : X \to X$ mit $\Phi_g(x) := g\,x$ eine Bijektion und es gilt: $g \mapsto \Phi_g$ ist ein Homomorphismus $\Phi : G \longrightarrow S(X)$, also

(2.3.1) $\Phi_e = \mathrm{id}_X$,

(2.3.2) $\Phi_{g\,h} = \Phi_g \circ \Phi_h$,

(2.3.3) $\Phi_{g^{-1}} = (\Phi_g)^{-1}$.

Linksoperationen $\cdot : G \times X \longrightarrow X$ von G auf X und Gruppenhomomorphismen $\Phi : G \longrightarrow S(X)$ von G in die volle symmetrische Gruppe von X entsprechen sich auf diese Weise eineindeutig. Die treuen Operationen entsprechen den injektiven Gruppenhomomorphismen $\Phi : G \longrightarrow S(X)$.

(2.3.4) Die *triviale Operation* von G auf einer Menge X ist durch $g\,x = x$ gegeben. Sie entspricht dem trivialen Homomorphismus $g \mapsto \Phi_g = \mathrm{id}_X$ von G in $S(X)$.

Beweis. (2.3.1) ist klar.
zu (2.3.2): $\Phi_{g\,h}(x) = (g\,h)\,x = g(h\,x) = \Phi_g(h\,x) = \Phi_g(\Phi_h(x)) = (\Phi_g \circ \Phi_h)(x)$.
Die weiteren Aussagen folgen hieraus. □

- **Definition 2.4**

Es sei G eine Gruppe. X, Y seien G-Mengen.

(2.4.1) Eine Abbildung $f : X \longrightarrow Y$ heißt *G-Abbildung* oder *G-äquivariant*, wenn f die Operationen von G respektiert, d. h. wenn $f(g\,x) = g\,f(x)$ für alle $x \in X$, $g \in G$ gilt.

(2.4.2) Es sei Z eine Menge. Eine Abbildung $f : X \longrightarrow Z$ heißt *G-invariant*, wenn f eine G-Abbildung ist bezüglich der trivialen Operation von G auf Z, wenn also $f(g\,x) = f(x)$ für alle $x \in X$, $g \in G$ gilt.

(2.4.3) Eine Teilmenge $A \subset X$ heißt *G-invariant*, wenn $g\,x \in A$ für alle $x \in A$, $g \in G$.

- **Lemma 2.5**

Es sei G eine Gruppe. Die identische Abbildung einer G-Menge ist eine G-Abbildung. Die Komposition von G-Abbildungen ist eine G-Abbildung. Die Umkehrabbildung einer bijektiven G-Abbildung ist eine G-Abbildung.

Beweis. Wir zeigen nur die letzte Aussage. Sei also $f: X \longrightarrow Y$ eine bijektive G-Abbildung. Ist $y = f(x)$, so ist $g\,y = f(g\,x)$ und somit $g\,f^{-1}(y) = g\,x = f^{-1}(g\,y)$. □

- **Bemerkung 2.6**

Wir erläutern hier kurz ein sehr abstraktes Konzept, den Begriff der *Kategorie*. Zunächst ein Beispiel: Es sei G eine Gruppe. Die G-Mengen zusammen mit den G-Abbildungen bilden eine Kategorie.
Der Begriff der Kategorie beschreibt eine Struktur, die allen mathematischen Theorien zugrunde liegt, in denen es um eine bestimmte Klasse mathematischer Objekte und die Frage nach ihrer strukturellen Gleichheit (Isomorphie) geht. Wir geben die Definition und einige Beispiele. (Wir kümmern uns hier nicht um die Problematik der präzisen Begründung der Mengenlehre.)

(2.6.1) Eine *Kategorie* $\mathcal{C}$ besteht aus

(2.6.1.1) einer Menge $\mathrm{Ob}(\mathcal{C})$ von Objekten,

(2.6.1.2) einer Menge von Morphismen: für jedes Paar (X, Y) von Objekten ist eine Menge $\hom_{\mathcal{C}}(X, Y)$ von Morphismen mit *Start* X und *Ziel* Y gegeben.

(2.6.1.3) einer Komposition von Morphismen: für jedes Tripel (X, Y, Z) von Objekten ist eine zweistellige Verknüpfung
$\hom_{\mathcal{C}}(Y, Z) \times \hom_{\mathcal{C}}(X, Y) \longrightarrow \hom_{\mathcal{C}}(X, Z),\ (f, g) \mapsto f \circ g,$
gegeben, so dass folgende Axiome erfüllt sind:

(2.6.1.4) $(f \circ g) \circ h = f \circ (g \circ h)$
für alle $h \in \hom_{\mathcal{C}}(X, Y)$, $g \in \hom_{\mathcal{C}}(Y, Z)$, $f \in \hom_{\mathcal{C}}(Z, W)$.

(2.6.1.5) für jedes Objekt X gibt es einem Morphismus $\mathrm{id}_X \in \hom_{\mathcal{C}}(X, X)$,
so dass $h \circ \mathrm{id}_X = \mathrm{id}_Y \circ h = h$ für alle $h \in \hom_{\mathcal{C}}(X, Y)$.

Hierdurch ist id_X eindeutig bestimmt, denn hat man $\tilde{\mathrm{id}}_X$ mit $h \circ \tilde{\mathrm{id}}_X = \tilde{\mathrm{id}}_Y \circ h = h$ für alle $h \in \hom_{\mathcal{C}}(X, Y)$, so gilt für $h = \mathrm{id}_X$: $\mathrm{id}_X = \mathrm{id}_X \circ \tilde{\mathrm{id}}_X = \tilde{\mathrm{id}}_X$.

Wir bemerken, dass für jedes Objekt X die Menge $\mathrm{end}_{\mathcal{C}}(X) = \hom_{\mathcal{C}}(X, X)$ der Endomorphismen von X ein Monoid ist.

(2.6.2) Die Kategorie $\mathcal{S}ets$ der Mengen. Objekte sind die Mengen. Morphismen sind die Abbildungen. Die Komposition ist die übliche Komposition von Abbildungen.

(2.6.3) Die Kategorie $\mathcal{V}ect_K$ der K-Vektorräume.
Objekte sind die K-Vektorräume.
Morphismen sind die K-linearen Abbildungen.
Die Komposition ist die übliche Komposition von Abbildungen.

(2.6.4) Die Kategorie $\mathcal{G}roups$ der Gruppen.
Objekte sind die Gruppen.
Morphismen sind die Gruppenhomorphismen.
Die Komposition ist die übliche Komposition von Abbildungen.

(2.6.5) Die Kategorie $G - \mathcal{S}ets$ der G-Mengen.
Objekte sind die G-Mengen.
Morphismen sind die G-Abbildungen.
Die Komposition ist die übliche Komposition von Abbildungen.

(2.6.6) Ein Beispiel einer 'kleinen' Kategorie: Es sei $(M, \cdot, e)$ ein Monoid: Man kann dann eine Kategorie $\mathcal{M}$ definieren, deren einziges Objekt e ist und deren Morphismen $f : e \longrightarrow e$ die Elemente aus M sind. Hier sind die Morphismen keine Abbildungen, sondern einfach abstrakte Elemente, die man multiplizieren kann. Die Komposition von Morphismen ist hier die Multiplikation. Die Axiome sind dann erfüllt, wobei $\mathrm{id}_e = e$ ist. Ein Monoid M ist also im wesentlichen nichts anderes als eine Kategorie $\mathcal{M}$ mit nur einem einzigen Objekt X. Die Menge $\hom_{\mathcal{M}}(X, X)$ ist dann mit der Komposition das Monoid M.

Der Begriff des *Isomorphismus* in einer Kategorie $\mathcal{C}$ ist folgendermaßen erklärt: Ein Morphismus $f \in \hom_{\mathcal{C}}(X, Y)$ heißt *Isomorphismus*, wenn es ein $g \in \hom_{\mathcal{C}}(Y, X)$ gibt, so dass $f \circ g = \mathrm{id}_Y$, $g \circ f = \mathrm{id}_X$ gilt.
Eine Kategorie, in der alle Morphismen Isomorphismen sind, heißt ein *Gruppoid.* Das ist eine Verallgemeinerung des Gruppenbegriffs, denn eine Gruppe ist nichts anderes als ein Gruppoid mit genau einem Objekt.

- **Definition und Lemma 2.7**

Es sei G eine Gruppe und X eine G-Menge.

(2.7.1) Für $x, y \in X$ definiert man: $x \underset{G}{\sim} y \Longleftrightarrow \exists\, g \in G : y = g\,x$. Dadurch wird eine Äquivalenzrelation auf X definiert. Ist $x \underset{G}{\sim} y$, so sagen wir auch, dass y mittels G von x aus erreichbar ist. Die Äquivalenzklasse von x heißt die *Bahn* (oder *Orbit*) von x (genauer *G-Bahn* von x) und wird mit $G\,x$ oder auch oft mit $\mathrm{Bahn}_G(x)$

bezeichnet. Es gilt $G\,x = \{g\,x \mid g \in G\} = \{\Phi_g(x) \mid g \in G\}$. Es gilt also genau dann $x \underset{G}{\sim} y$, wenn y in der Bahn von x liegt.

(2.7.2) Die Menge aller G-Bahnen in X heißt der *Bahnenraum* (auch *Orbitraum*) von X und wird mit X/G bezeichnet. Dazu gehört die *kanonische Projektion* $\pi : X \to X/G$, die jedem Element $x \in X$ seine Bahn $G\,x \in X/G$ zuordnet. Die Abbildung π ist offensichtlich G-invariant und erfüllt die folgende universelle Eigenschaft: Zu jeder G-invarianten Abbildung $f : X \longrightarrow Z$ von X in eine Menge Z gibt es genau eine Abbildung $\bar{f} : X/G \longrightarrow Z$ mit $\bar{f} \circ \pi = f$.

(2.7.3) Für $x \in X$ ist $G_x := \{g \in G \mid g\,x = x\}$ eine Untergruppe von G. G_x heißt die *Standgruppe* (oder *Isotropiegruppe*) von x. Sie besteht aus allen Gruppenelementen g, die das Element x festlassen, für die also x ein Fixpunkt der Bijektion Φ_g ist.

Beweis. zu (2.7.1): Es gilt $x \underset{G}{\sim} x$, weil $x = e\,x$. Also ist die Relation $\underset{G}{\sim}$ reflexiv.
Ist $x \underset{G}{\sim} y$, etwa $y = g\,x$, so ist $x = (g^{-1}\,g)\,x = g^{-1}(g\,x) = g^{-1}\,y$, also $y \underset{G}{\sim} x$. Die Relation $\underset{G}{\sim}$ ist also symmetrisch. Ist $x \underset{G}{\sim} y$ und $y \underset{G}{\sim} z$, etwa $y = g\,x$, $z = h\,y$, so folgt $z = h(g\,x) = (h\,g)\,x$ und somit ist $x \underset{G}{\sim} z$. Die Relation $\underset{G}{\sim}$ ist also transitiv.
zu (2.7.2): Wegen der Invarianz von f haben alle Elemente einer Bahn dasselbe Bild. Man kann also $\bar{f}(G\,x) \in Z$ als $f(x)$ definieren. Es gilt dann
$\bar{f}(\pi(x)) = \bar{f}(G\,x) = f(x)$, also $\bar{f} \circ \pi = f$.
zu (2.7.3):
$g, h \in G_x \Longrightarrow g\,x = x,\ h\,x = x \Longrightarrow h^{-1}\,x = x,\ (g\,h^{-1})\,x = g(h^{-1}\,x) = g\,x = x$.
Also ist $g\,h^{-1} \in G_x$. □

- **Beispiele 2.8**

(2.8.1) Die symmetrische Gruppe S_n operiert auf $X = \{1, 2, 3, \ldots, n\}$. Ist $\sigma \in S_n$ und $G = \langle\sigma\rangle$ die von σ erzeugte zyklische Untergruppe, so operiert auch G auf X. Die G-Bahnen bilden eine Zerlegung der Menge X. Die Elemente $k \in X$ mit $\sigma(k) = k$, also die Fixpunkte von σ bestimmen einelementige Bahnen: $G\,k = \{k\}$. Die Standgruppe eines Fixpunktes ist die volle Gruppe $G_k = G$.
Ist $k \in X$ kein Fixpunkt von σ, so erhält man die Bahn von k durch sukzessives Anwenden von σ auf k. Es gilt:

$$G\,k = \{k,\ \sigma(k),\ \sigma^2(k),\ \ldots,\ \sigma^{m-1}(k)\},$$

wobei m die kleinste positive Zahl mit $\sigma^m(k) = k$ ist. Die Bahn $G\,k$ ist also nichts anderes der Wirkungsbereich des Zyklus

$$\zeta = (k,\ \sigma(k),\ \sigma^2(k),\ \ldots,\ \sigma^{m-1}(k))$$

von σ (vgl. Beispiel 1.19). Die kleinste positive Potenz von σ in der Standgruppe G_k von k ist gerade σ^m. Ist $a \in \mathbb{Z}$, $a = q\,m + r$, $0 \le r < m$, und $\sigma^a \in G_k$, also $\sigma^a(k) = k$, so ist auch $\sigma^r(k) = \sigma^r(\sigma^{q\,m}(k)) = \sigma^{r+q\,m}(k) = \sigma^a(k) = k$ und nach Wahl von m ist somit $r = 0$. Damit ist gezeigt, dass $G_k = \langle\sigma^m\rangle$ die von σ^m erzeugte zyklische Gruppe ist. Die Ordnung d von σ ist ein Vielfaches von m, denn wegen $\sigma^d = \mathrm{id}$ ist natürlich auch $\sigma^d(k) = k$. Demzufolge ist die Länge der Bahn, das ist ja m, ein Teiler der Ordnung von σ:

$$d = m\,\ell,\ d = |G|,\ m = |\mathrm{Bahn}_G(k)|.$$

Da G_k aus den Elementen σ^m, $\sigma^{2\,m}$, ..., σ^d besteht, ist $\ell = |G_k|$. Die Formel

$$|G| = |G_k|\ |\mathrm{Bahn}_G(k)|$$

gilt ganz allgemein für Operationen, wie wir zeigen werden. Zu jeder Bahn $G\,k$ gehört ein Zyklus ζ, dessen Wirkungsbereich $G\,k$ ist. σ ist das Produkt der so gewonnenen Zykeln.
Dies ergibt die in Beispiel 1.19 eingeführte Zykeldarstellung von σ.

(2.8.2) Die Drehgruppe $\mathrm{SO}(2)$ operiert auf $\mathbb{R}^2$. Der Nullpunkt ist Fixpunkt der Operation und die Bahnen der anderen Punkte sind Kreise. Die Abbildung $f : \mathbb{R}^2 \longrightarrow [0, \infty)$, $f(x, y) := \sqrt{x^2 + y^2}$ ist $\mathrm{SO}(2)$-invariant und induziert sogar eine Bijektion des Bahnenraums $\mathbb{R}^2 / \mathrm{SO}(2)$ auf das Intervall $[0, \infty)$.

(2.8.3) Dynamische Systeme
(das sind Systeme gewöhnlicher Differentialgleichungen)
erzeugen sogenannte *1-Parametergruppen*. Das wollen wir kurz erläutern: Es sei etwa X eine kompakte glatte Fläche (um nicht zu allgemein zu werden, etwa eine Sphäre oder ein Torus). Auf der Fläche sei ein differenzierbares *Vektorfeld* v gegeben. In jedem Punkt x der Fläche ist also ein Tangentialvektor $v(x)$ an die Fläche gegeben, der differnzierbar von x abhängt. Man kann nun zu jedem Punkt x genau eine differenzierbare Kurve $c : \mathbb{R} \longrightarrow X$ finden, deren Geschwindigkeitsvektor $\frac{d\,c}{d\,t}(t)$ mit dem vorgegebenem Vektor $v(c(t))$ übereinstimmt und die zur Zeit Null durch x geht, für die also $c(0) = x$ gilt. Wir schreiben genauer $c(t) = \varphi(t, x)$. Man kann nun zeigen, dass $\varphi : \mathbb{R} \times X \longrightarrow X$ eine Linksoperation der additiven Gruppe $(\mathbb{R}, +)$ auf X ist. Zum Beweis braucht man den Existenz- und Eindeutigkeitssatz für Differentialgleichungssysteme. Man nennt φ eine 1-Parametergruppe auf X. Die Kurven $\{\varphi(t, x) \mid t \in \mathbb{R}\}$ auf der Fläche sind die Bahnen. Man nennt sie auch die *Integralkurven* des Vektorfeldes v. Die Abbildungen $\Phi_t : X \longrightarrow X$, $\Phi_t(x) = \varphi(t, x)$ bilden den *globalen Fluss* des Vektorfeldes. Die Punkte von X 'fließen': $\Phi_t(x)$ ist der Ort von x zur Zeit t.

Ein konkretes Beispiel wird durch folgene Abbildung $\varphi : \mathbb{R} \times S^2 \longrightarrow S^2$gegeben,
wobei $S^2 = \{x \in \mathbb{R}^3 \mid \|x\| = 1\}$ die Einheitssphäre ist

$$\varphi(t, x) = \begin{pmatrix} \cos t & -\sin t & 0 \\ \sin t & \cos t & 0 \\ 0 & 0 & 1 \end{pmatrix} x.$$

Das zugehörige Vektorfeld ist offensichtlich

$$v\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -x_2 \\ x_1 \\ 0 \end{pmatrix}.$$

(2.8.4) Ein wichtiges Beispiel von G-Mengen sind die G-Moduln. Es sei ein Körper K fest gegeben. Ein *G-Modul* (über K) ist ein K-Vektorraum V zusammen mit einer *linearen* Linksoperation $G \times V \longrightarrow V$ von G auf V, das soll heißen, einer Linksoperation, bei der alle Abbildungen $\Phi_g : V \longrightarrow V$ linear sind. Dazu äquivalent ist, dass das Bild des Homomorphismus $\Phi : G \longrightarrow S(V)$ eine Untergruppe von $\mathrm{GL}(V)$ ist. Man nennt $G \times V \longrightarrow V$ oder $\Phi : G \longrightarrow \mathrm{GL}(V)$ dann auch eine *lineare Darstellung* von G. Zwei G-Moduln V, W heißen *isomorph* (als G-Moduln), wenn es einen G-äquivarianten Vektorraumisomorphismus $\varphi : V \longrightarrow W$ gibt. Eine zentrale Aufgabe der Darstellungstheorie ist es, für eine gegebene Gruppe G die möglichen linearen Darstellungen von G bis auf Isomorphie zu klassifizieren. Wir betrachten den Fall $G = S_3$ ausführlich im Übungsprogramm (Aufgabe (2.6)-(2.8)).

- **Definition und Satz 2.9**

Es sei H eine Untergruppe der Gruppe G. Die Einschränkung der Multiplikation $G \times G \longrightarrow G$ auf $G \times H$ definiert eine Rechtsoperation von H auf G. Die Bahnen in G sind die sogenannten *Linkssnebenklassen*

$$gH = \{gh \mid h \in H\}$$

von H (g wird von links an H multipliziert). Der Bahnenraum G/H der *Rechtsoperation* $G \times H \longrightarrow G$ ist die Menge aller Linksnebenklassen $K = gH$, $g \in G$. Die Anzahl der Linksnebenklassen von H in G heißt der *Index* von H in G und wird mit $[G : H]$ bezeichnet.

(2.9.1) Man erhält eine Linksoperation von G auf G/H durch $(g, K) \mapsto gK$. Die Standgruppe von $K = sH (s \in G)$ ist die Untergruppe $sHs^{-1} = \{shs^{-1} \mid h \in H\}$ von G. sHs^{-1} heißt zu H *konjugierte Untergruppe*.

(2.9.2) Für $s \in G$ ist $h \mapsto sh$ eine Bijektion von H auf sH.

(2.9.3) (*Indexformel*) Es gilt $|G| = |H|[G : H]$.

(2.9.4) Ist G endlich, so teilt die Ordnung von H die Ordnung von G (*Satz von Lagrange*).

(2.9.5) Für $s, g \in G$ gilt $sH = gH$ genau dann, wenn $s \in gH$.

Beweis. zu (2.9.1): Ist $K = sH$ eine Linksnebenklasse von H, $g \in G$, so ist auch $gK = (gs)H$ eine Linksnebenklasse von H. Die Eigenschaften (2.1.1), (2.1.2) einer Operation sind offensichtlich erfüllt. Es gilt weiter
$g \in G_K \Longleftrightarrow gK = K \Longleftrightarrow gsH = sH \Longleftrightarrow s^{-1}gsH = H \Longleftrightarrow s^{-1}gs \in H \Longleftrightarrow g \in sHs^{-1}$.
zu (2.9.2): $H \longrightarrow sH$, $h \mapsto sh$ besitzt offensichtlich die Abbildung $sH \longrightarrow H$, $g \mapsto s^{-1}g$ als Umkehrabbildung, denn $s(s^{-1}g) = (ss^{-1})g = eg = g$ und $s^{-1}(sg) = (s^{-1}s)g = eg = g$.
zu (2.9.3): Die surjektive Abbildung $\pi : G \longrightarrow G/H$ hat nach Definition als Fasern die Linksnebenklassen. Nach (2.9.2) sind diese alle gleichmächtig. Damit gilt
$|G| = |H|\,|G/H|$.
zu (2.9.4): Das folgt unmittelbar aus (2.9.3).
zu (2.9.5): Das ist klar, weil die Linksnebenklassen von H die Äquivalenzklassen der Äquivalenzrelation $s \underset{H}{\sim} g \Longleftrightarrow \exists\, h \in H : s = gh$ sind. (vgl. (2.7.1)) □

- **Lemma 2.10**

Es sei G eine Gruppe und X eine G-Menge. Es sei $x \in X$ ein Punkt in X und $Y := \mathrm{Bahn}_G(x)$ sei die Bahn von x. Schließlich sei $H = G_x$ die Standgruppe von x.

(2.10.1) Die Abbildung $\pi : G \longrightarrow Y$, $\pi(g) = gx$ von G auf die Bahn Y ist surjektiv und H-invariant (bezüglich der Rechtsmultiplikation von H auf G) und induziert eine bijektive Abbildung $\overline{\pi} : G/H \longrightarrow Y$ von der Menge aller Linksnebenklassen von H auf die Bahn Y.

(2.10.2) Versieht man die Menge G/H der Linksnebenklassen mit der kanonischen G-Linksoperation, so ist $\overline{\pi} : G/H \longrightarrow Y$ G-äquivariant, also ein Isomorphismus von G-Mengen.

(2.10.3) (*Bahnformel*) $|G| = |G_x|\,|\mathrm{Bahn}_G(x)|$

Beweis. zu (2.10.1): Es sei $g \in G, h \in H$. Dann gilt also $hx = x$ und somit $\pi(gh) = (gh)x = g(hx) = gx$. Damit ist π H-invariant. $\overline{\pi} : G/H \longrightarrow Y$ mit $\overline{\pi}(gH) := gx$ ist offensichtlich surjektiv. Wir zeigen die Injektivität von $\overline{\pi}$. Seien $s, g \in G$ und sei $\overline{\pi}(sH) = \overline{\pi}(gH)$. Dann gilt $sx = gx$ und somit $g^{-1}sx = x$, also $g^{-1}s \in H$ und folglich $s \in gH$. Nach (2.9.5) gilt somit $sH = gH$.
zu (2.10.2): Es sei $K = sH \in G/H$, $g \in G$. Dann gilt
$\overline{\pi}(gK) = \overline{\pi}(gsH) = gsx = g\overline{\pi}(sH) = g\overline{\pi}(K)$.
zu (2.10.3): Die Bahnformel folgt aus (2.10.1) und der Indexformel (2.9.3). □

- **Definition 2.11**

Es sei G eine Gruppe und X eine G-Menge.

(2.11.1) X heißt *freie* G-Menge, wenn alle Standgruppen G_x trivial sind, wenn also alle Elemente $g \in G \setminus e$ *fixpunktfrei* auf X wirken ($g\,x \neq x$ für alle $x \in X$). Man kann diese Eigenschaft auch so ausdrücken: Es gilt die Kürzungsregel:

$$\forall\, g, h \in G, x \in X\colon g\,x = h\,x \Longrightarrow g = h.$$

(2.11.2) G operiert *transitiv* auf X, wenn für alle $x, y \in X$ ein $g \in G$ existiert, so dass $y = g\,x$, wenn also $|X/G| = 1$ gilt. X heißt dann eine *homogene* G-Menge.

(2.11.3) $x \in X$ heißt *Fixpunkt* der G-Menge X, wenn $g\,x = x$ für alle $g \in G$ gilt. Mit $\mathrm{Fix}_G(X)$wird die Menge aller G-Fixpunkte von X bezeichnet.

Die Bahnen $G\,x$ einer G-Menge sind homogene G-Mengen und die Fasern der surjektiven Abbildung $\pi\colon G \longrightarrow G\,x$, $g \mapsto g\,x$ sind die sämtlichen zu $H := G_x = \pi^{-1}(x)$ konjugierten Untergruppen $G_{g\,x} = g\,H\,g^{-1} = \pi^{-1}(g\,x)$ (Übung!). Die Standgruppen ändern sich also längs einer Bahn nicht wesentlich (nur durch Konjugation). Wechselt man jedoch in eine andere Bahn, so kann sich der Isomorphietyp der Standgruppe sehr wohl ändern.
Wenn der extreme Fall einer *freien* Operation vorliegt, sind alle Standgruppen trivial und alle Bahnen sind gleichmächtig: $G \longrightarrow G\,x$, $g \mapsto g\,x$ ist für alle $x \in X$ bijektiv. Damit hat man die folgende Bahnformel für freie Operationen.

- **Lemma 2.12**

Es sei G eine Gruppe und X eine freie G-Menge. Dann gilt

$$|X| = |G|\,|X/G|.$$

Beweis. □

Eine Bemerkung am Rande: Freie G-Mengen sind wichtig in der *Topologie* und der *Differentialgeometrie*. Die Mengen und auch die Gruppe haben dann natürlich noch zusätzlich eine *topologische* bzw. eine *differenzierbare* Struktur. Die Quotientenabbildung $\pi\colon X \to B = X/G$ einer freien G-Menge X ist ein sogenanntes *G-Prinzipalbündel* (Es müssen noch einige weitere Eigenschaften erfüllt sein.). Ein konkretes Beispiel werden wir in (2.13.1) kennenlernen.

Weiter bemerken wir: Die Aussage (2.10.2) besagt, dass jede homogene G-Menge X zur Menge G/H der Linksnebenklassen einer Untergruppe $H \subset G$ mit der natürlichen Linksoperation von G auf G/H isomorph ist. Für H kann man die Standgruppe irgendeines Elementes von X wählen.

■ **Beispiele 2.13**

(2.13.1) Es sei S^3 die dreidimensionale Einheitssphäre in $\mathbb{C}^2$,
$S^3 = \{(z, w) \in \mathbb{C}^2 \mid z\overline{z} + w\overline{w} = 1\}$. Man kann sich S^3 als die sogenannte *Einpunktkompaktifizierung* des Zahlenraums $\mathbb{R}^3$ vorstellen: $S^3 \cong \mathbb{R}^3 \bigcup \{\infty\}$ (Stichwort: Stereografische Projektion $S^3 \setminus \{(0, 1)\} \longrightarrow \mathbb{R}^3$).
Die skalare Multiplikation $\mathbb{C} \times \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ lässt sich zu einer Abbildung

$$S^1 \times S^3 \longrightarrow S^3, (u, (z, w)) \mapsto u(z, w) = (uz, uw).$$

einschränken . Offensichtlich ist dies eine freie Linksoperation von S^1 auf S^3. Damit ist S^3 eine freie S^1-Menge. Wir bestimmen den Bahnenraum S^3/S^1. Dazu betrachten wir die Riemannsche Zahlenkugel $S^2 = \mathbb{C} \bigcup \{\infty\}$ und definieren

$$\varphi : S^3 \longrightarrow S^2$$

durch $\varphi((z, w)) = \frac{z}{w}$, wobei $\frac{z}{0} := \infty$, falls $z \neq 0$. Offensichtlich ist diese Abbildung S^1-invariant und induziert daher eine Abbildung

$$\overline{\varphi} : S^3/S^1 \longrightarrow S^2$$

Man kann leicht zeigen, dass $\overline{\varphi}$ bijektiv ist. Der Bahnenraum S^3/S^1 ist also isomorph zur Riemannschen Zahlenkugel. Die kanonische Projektion $\pi : S^3 \longrightarrow S^3/S^1$ ist das berühmte *Hopfbündel* der Topologen, das wichtigste S^1-Prinzipalbündel über S^2.

(2.13.2) Die n-Sphäre $S^n = \{x \in \mathbb{R}^{n+1} \mid \|x\| = 1\}$ ist ein homogener $\mathrm{SO}(n+1)$-Raum, nämlich die Bahn des Einheitsspaltenvektors $e^1 = [1, 0, \ldots, 0] \in \mathbb{R}^{n+1}$ unter der Standardoperation von $\mathrm{SO}(n+1)$ auf $\mathbb{R}^{n+1}$. Die Standgruppe von e^1 ist die Untergruppe $\{1\} \times \mathrm{SO}(n)$ von $\mathrm{SO}(n+1)$, die aus allen Blockmatrizen $\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$ mit $A \in \mathrm{SO}(n)$ besteht. Man kann daher S^n auch als Menge der Linksnebenklassen der Untergruppe $\{1\} \times \mathrm{SO}(n) \subset \mathrm{SO}(n+1)$ auffassen:

$$S^n = \mathrm{SO}(n+1)/\{1\} \times \mathrm{SO}(n).$$

(2.13.3) Die spezielle unitäre Gruppe $\mathrm{SU}(2) = \left\{U \in \mathrm{GL}_2(\mathbb{C}) \,\middle|\, U\overline{U}^t = E, \det U = 1\right\}$ operiert in natürlicher Weise auf $\mathbb{C}^2$. $\mathrm{SU}(2)$ hat die Gestalt einer dreidimensionalen Sphäre S^3, denn wie aus der linearen Algebra bekannt ist, gilt

$$\mathrm{SU}(2) = \left\{\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \,\middle|\, a\overline{a} + b\overline{b} = 1\right\}.$$

Die Abbildung $(a, b) \mapsto \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ ist eine Bijektion von S^3 auf $\mathrm{SU}(2)$. Man zeige, dass die Operation $\mathrm{SU}(2) \times \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ den Nullpunkt in $\mathbb{C}^2$ als Fixpunkt hat und auf

dem Komplement $\mathbb{C}^2\setminus\{0\}$ frei operiert. Die Norm eines Punktes in $\mathbb{C}^2\setminus\{0\}$ ist invariant unter der Operation von SU(2).

(2.13.4) Wir wollen hier aber eine andere interessante Operation untersuchen, durch die ein tiefer Zusammenhang zwischen SU(2) und der Drehgruppe SO(3) erhellt wird. Dazu betrachten wir den folgenden dreidimensionalen reellen Vektorraum Y.
Y bestehe aus allen Matrizen $A \in M_2(\mathbb{C})$, die reelle Linearkombination der schiefhermiteschen Matrizen

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

mit Spur Null sind.
Bemerkung: Durch Multiplikation mit i erhält man einen Isomorphismus des vierdimensionalen $\mathbb{R}$-Vektorraums $\mathcal{H}erm_2$ der hermitischen 2×2-Matrizen auf den $\mathbb{R}$-Vektorraums der schiefhermiteschen 2×2-Matrizen.

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

sind die sogenannten Pauli-Matrizen. Sie erzeugen den dreidimensionalen Untervektorraum $\mathcal{E}$ der hermiteschen Matrizen mit Spur Null von $\mathcal{H}erm_2$. $i\cdot : \mathcal{E} \longrightarrow Y$ ist ein Isomorphismus. $I = i\,\sigma_1$, $J = i\,\sigma_2$, $K = i\,\sigma_3$.

$$Y := \left\{A \in M_2(\mathbb{C}) \;\middle|\; A + \overline{A}^t = 0,\ \text{Spur}(A) = 0\right\} = \left\{\begin{pmatrix} a\,i & -b + i\,c \\ b + i\,c & -a\,i \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R}\right\}.$$

Die Operation von SU(2) auf Y wird wie folgt erklärt: für $U \in \text{SU}(2)$, $A \in Y$ sei

$$\Phi_U(A) := U\,A\,U^{-1}.$$

Wir zeigen, dass $U\,A\,U^{-1} \in Y$. Beweis: Da $U^{-1} = \overline{U}^t$ und $A + \overline{A}^t = 0$, gilt
$(U\,A\,U^{-1}) + (\overline{U\,A\,U^{-1}})^t = U\,A\,U^{-1} + U\,\overline{A}^t\,\overline{U}^t = U\left(A + \overline{A}^t\right)U^{-1} = 0.$
Da die Spur eine Invariante bezüglich Konjugation mit $\text{GL}_2(\mathbb{C})$ ist, gilt $\text{Spur}(U\,A\,U^{-1}) = \text{Spur}(A) = 0$. Also gilt $U\,A\,U^{-1} \in Y$.
Offensichtlich (Übung!) ist somit

$$\Phi : \text{SU}(2) \longrightarrow \text{GL}(Y)$$

ein Gruppenhomomorphismus. Y ist also ein reeller SU(2)-Modul (unter der Konjugation von SU(2) auf Y).
Wir definieren für $A, B \in Y$

$$\langle A, B\rangle := -\tfrac{1}{2}\,\text{Spur}(A\,B) \qquad \textbf{(1)}$$

Dies ist offensichtlich eine symmetrische reelle Bilinearform auf Y.
Außerdem ist sie positiv-definit, denn für $A = \begin{pmatrix} a\,i & -b + i\,c \\ b + i\,c & -a\,i \end{pmatrix} \neq 0$ ergibt sich

$\langle A, A\rangle = -\frac{1}{2}\,\mathrm{Spur}(A^2) = a^2 + b^2 + c^2 > 0.$
Damit ist Y mit dem Skalarprodukt (1) ein euklidischer Raum. Wir notieren noch die Formel

$$\langle A, A\rangle = \det A. \tag{2}$$

Wir zeigen nun, dass die Operation von $\mathrm{SU}(2)$ auf Y orthogonal ist, dass also für alle $U \in \mathrm{SU}(2)$, $A, B \in Y$ gilt

$$\langle \Phi_U(A), \Phi_U(B)\rangle = \langle A, B\rangle. \tag{3}$$

Beweis. Das ist ganz einfach:

$$\langle \Phi_U(A), \Phi_U(B)\rangle =$$
$$\langle U A U^{-1}, U B U^{-1}\rangle = -\tfrac{1}{2}\,\mathrm{Spur}(U A U^{-1} U B U^{-1}) = -\tfrac{1}{2}\,\mathrm{Spur}(A B) = \langle A, B\rangle.$$

Damit ist Φ_U Element von $O(Y)$, der orthogonalen Gruppe des euklidischen Raumes $(Y, \langle , \rangle)$.
Wir wollen weiter sehen, dass die orthogonale Abbildung Φ_U für alle $U \in \mathrm{SU}(2)$ die Determinante 1 hat. Dazu benutzen wir ein Stetigkeitsargument: Da $\mathrm{SU}(2) = S^3$ zusammenhängend ist, die Determinante einer orthogonalen Abbildung nur die Werte ±1 annehmen kann und $\det(\Phi_E) = \det(\mathrm{id}_Y) = 1$, gilt aus Stetigkeitsgründen $\det(\Phi_U) = 1$ für alle $U \in \mathrm{SU}(2)$. Damit liegt das Bild von $\mathrm{SU}(2)$ in der speziellen orthogonalen Gruppe $\mathrm{SO}(Y)$.
Schließlich wollen wir zeigen, dass die Abbildung $\Phi : \mathrm{SU}(2) \longrightarrow \mathrm{SO}(Y)$ surjektiv ist, was nicht offensichtlich ist.

Behauptung. $\Phi : \mathrm{SU}(2) \longrightarrow \mathrm{SO}(Y)$ ist surjektiv.

Beweis. Man sieht leicht, dass die Matrizen

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

eine Orthonormalbasis von Y bilden. Damit erhält man einen Isomorphismus $\mathcal{M} : \mathrm{SO}(Y) \xrightarrow{\cong} \mathrm{SO}(3)$, indem man $F \in \mathrm{SO}(Y)$ die Matrix $A = \mathcal{M}(F)$ bezüglich der Basis (I, J, K) zuordnet. Es sei $D = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \in \mathrm{SU}(2)$. Die Matrix von $\Phi_D : Y \longrightarrow Y$ bezüglich der Basis (I, J, K) ist dann die Drehmatrix

$$\begin{pmatrix} \cos 2\theta & -\sin 2\theta & 0 \\ \sin 2\theta & \cos 2\theta & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

wie man direkt nachrechnet:

$$D I D^{-1} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \begin{pmatrix} 0 & i e^{2i\theta} \\ i e^{-2i\theta} & 0 \end{pmatrix} = \cos(2\theta)\, I + \sin(2\theta)\, J,$$

$$D\,J\,D^{-1} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \begin{pmatrix} 0 & -e^{2i\theta} \\ e^{-2i\theta} & 0 \end{pmatrix} = -\sin(2\theta)\,I + \cos(2\theta)\,J,$$

$$D\,K\,D^{-1} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = K.$$

$\mathcal{M}(\Phi(T)) = H \cong \mathrm{SO}(2)\times\{1\} \subset \mathrm{SO}(3)$ entspricht also der Untergruppe der Drehungen um die Achse $\mathbb{R}K \subset Y$, wobei $T \subset \mathrm{SU}(2)$ die Untergruppe aller Diagonalmatrizen der Form

$$\begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

bezeichnet. Die Einschränkung von $\mathcal{M}\circ\Phi$ auf T ist die 2:1 Überlagerung $T \longrightarrow H$, die von $e^{i\theta} \mapsto e^{2i\theta}$ induziert wird. Es sei nun $F \in \mathrm{SO}(Y)$, $F \neq \mathrm{id}_Y$. Dann ist $\ker(F - \mathrm{id}_Y) \subset Y$ die Drehachse von F. Man wähle nun einen normierten Eigenvektor $v \in Y$ von F zum Eigenwert 1. Dann hat v die Form

$$v = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$$

mit $a + \overline{a} = 0$ und $\langle v, v\rangle = -\frac{1}{2}\,\mathrm{Spur}(v\,v) = a\,\overline{a} + b\,\overline{b} = 1$. Wir können also v als Element in SU(2) mit Spur Null auffassen. Es gilt $\Phi_v(v) = v\,v\,v^{-1} = v = F(v)$. Damit sind Φ_v und F Drehungen in Y um dieselbe Achse $\mathbb{R}v$. Das charakteristische Polynom von v als Element in SU(2) ist

$$p(t) = \det\begin{pmatrix} t-a & -b \\ \overline{b} & t-\overline{a} \end{pmatrix} = t^2 + 1.$$

v hat also die Eigenwerte $\pm i$. Daher (→Lineare Algebra: Die unitäre Gruppe) gibt es eine Matrix $U \in \mathrm{SU}(2)$, so dass $v = U\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}U^{-1} = U\,K\,U^{-1}$. Es folgt:

$\Phi(U\,T\,U^{-1}) = \Phi_U\,\Phi(T)\,{\Phi_U}^{-1}$ ist die Menge aller Drehungen mit Drehachse $\mathbb{R}v$, denn $\Phi(T)$ ist die Menge der Drehungen um die Achse $\mathbb{R}K$. Insbesondere gibt es ein λ, so dass $F = \Phi_U\begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}{\Phi_U}^{-1}$. Damit ist die Surjektivität von $\Phi : \mathrm{SU}(2) \longrightarrow \mathrm{SO}(Y)$ bewiesen.

Wir zeigen noch:

Behauptung. $\ker\Phi = \pm E$.

Beweis. Es sei $U = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \ker\Phi$. Dann gilt: $U\,I = I\,U$, $U\,J = J\,U$. Das sind zwei Gleichungen für a, b, die sofort $b = \overline{b} = -b$ und $a = \overline{a}$ implizieren, was aber wegen $\det U = 1$ die Behauptung $b = 0$, $a = \pm 1$ zur Folge hat.

Man kann zeigen (Übung): Drei Matrizen $A, B, C \in Y$ bilden genau dann eine Orthonormalbasis von Y, wenn gilt

$A\,B = -B\,A,\ A\,C = -C\,A,\ B\,C = -C\,B,\ A^2 = -E,\ B^2 = -E,\ C^2 = -E.$

Die Matrizen I, J, K sind ein Beispiel dafür.

Das Kreuzprodukt auf Y kann man mithilfe der Matrizenmulziplikation einführen. Für $A, B \in Y$ setze

$$A \times B := -\tfrac{1}{2}\,(A\,B - B\,A) \qquad \textbf{(4)}$$

In der Tat ist $A \times B \in Y$, denn $\mathrm{Spur}(A\,B - B\,A) = \mathrm{Spur}(A\,B) - \mathrm{Spur}(B\,A) = 0$ und $(A\,B - B\,A) + (\overline{(A\,B - B\,A)})^t =$

$A\,B - B\,A + \overline{B}^t\,\overline{A}^t - \overline{A}^t\,\overline{B}^t = A\,B - B\,A + (-B)\,(-A) - (-A)\,(-B) = 0.$

Weiter gilt

$$\langle A,\, A \times B\rangle = 0 \qquad \textbf{(5)}$$

Beweis.

$\langle A, A \times B\rangle =$

$-\tfrac{1}{2}\,\mathrm{Spur}(A(A \times B)) = \tfrac{1}{4}\,\mathrm{Spur}(A(A\,B - B\,A)) = \tfrac{1}{4}\,(\mathrm{Spur}(A\,A\,B) - \mathrm{Spur}(A\,B\,A)) = 0.$

Schließlich untersuchen wir die Norm von $A \times B$. Es gilt die bekannte Formel

$$\|A \times B\| = \sqrt{\|A\|^2\,\|B\|^2 - \langle A,\, B\rangle^2} = \|A\|\,\|B\| \sin\alpha \qquad \textbf{(6)}$$

Beweis.

$\langle A \times B, A \times B\rangle = -\tfrac{1}{8}\,\mathrm{Spur}((A\,B - B\,A)\,(A\,B - B\,A)) =$

$-\tfrac{1}{8}\,(\mathrm{Spur}(A\,B\,A\,B) + \mathrm{Spur}(B\,A\,B\,A) - (\mathrm{Spur}(B\,A\,A\,B) + \mathrm{Spur}(A\,B\,B\,A))) =$

$-\tfrac{1}{4}\left(\mathrm{Spur}\left((A\,B)^2\right) - \mathrm{Spur}(A^2\,B^2)\right) \overset{(*)}{=}$

$-\tfrac{1}{4}\left((\mathrm{Spur}(A\,B))^2 - \mathrm{Spur}(A^2)\,\mathrm{Spur}(B^2)\right) = \det\begin{pmatrix} \langle A, A\rangle & \langle A, B\rangle \\ \langle B, A\rangle & \langle B, B\rangle \end{pmatrix}.$

Die Verifikation der Gleichung (*) lassen wir als Übung.

■ Übungen 2

(2.1) (a) Ist G eine additiv geschriebene abelsche Gruppe und H eine Untergruppe von G, so kann man die Menge G/H der Nebenklassen $g + H$, $g \in G$, in genau einer Weise mit einer Gruppenstruktur versehen, so dass die kanonische Quotientenabbildung

$$\pi : G \longrightarrow G/H$$

ein Gruppenhomomorphismus ist.

(b) Untersuche den Fall $G = (\mathbb{C}, +)$, $H = \langle 1, a + b\,i\rangle$, wobei $a, b \in \mathbb{R}$, $b > 0$.

(c) Zeige, dass die Gruppe $\mathbb{Z}/m\,\mathbb{Z}$ zyklisch ist.

(d) Ist K ein Körper, V ein K-Vektorraum und U ein Untervektorraum von V. Dann trägt die abelsche Gruppe $V/U = \{x + U \mid x \in V\}$ auch die Strukur eines K-Vektorraums und zwar in der Weise, dass die Quotientenabbildung $\pi : V \longrightarrow V/U$ linear ist. V/U heißt der Quotientenvektorraum. Es gilt $\ker \pi = U$.

(2.2) Es sei p eine Primzahl. Dann gibt es bis auf Isomorphie genau eine Gruppe der Ordnung p.

(2.3) Zeigen Sie: Die Menge der Matrizen $A = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$ mit $a, b \in \mathbb{C}$, $(a, b) \neq 0$, d.h. $A \neq 0$ ist mit der Matrizenmultiplikation eine Gruppe, die wir mit $\mathbb{H}^\times$ bezeichnen. Bestimmen Sie Bild und Kern der Determinante $\det : \mathbb{H}^\times \longrightarrow \mathbb{C}^\times$. Stellen Sie die Multiplikationstafel für die Menge $Q_8 = \{\pm E, \pm I, \pm J, \pm K\}$ auf (siehe: (2.13.4)). Q_8 heißt die *Quaternionengruppe*.

(2.4) Es sei G eine Untergruppe von S_n, $X = \{1, 2, ..., n\}$. Die Operation $G \times X \longrightarrow X$, $(g, k) \mapsto g(k)$, heißt *zweifach transitiv*, wenn es zu je zwei Paaren $(i, j), (k, l) \in X \times X$ mit $i \neq j$, $k \neq l$ eine Permutation $g \in G$ gibt mit $(k, l) = (g(i), g(j))$. Wie wird man den Begriff *k-fach transitiv* für $2 \leq k < n$ einführen?
(a) Zeigen Sie: S_n operiert $(n - 1)$-fach transitiv auf X. $(n \geq 2)$
(b) Zeigen Sie: G operiert genau dann zweifach transitiv auf X, wenn G transitiv auf X operiert und wenn für jedes $k \in X$ die Standgruppe G_k transitiv auf der Menge $X \setminus \{k\}$ operiert.
(c) Zeigen Sie: A_n operiert $(n - 2)$-fach transitiv auf X. $(n \geq 3)$

(2.5) X, Y seien G-Mengen. Zeigen Sie: Es gibt eine G-Menge Z zusammen mit G-Abbildungen $p_1 : Z \longrightarrow X$, $p_2 : Z \longrightarrow Y$, so dass für alle G-Mengen W und G-Abbildungen $q_1 : W \longrightarrow X$, $q_2 : W \longrightarrow Y$ genau eine G-Abbildung $f : W \longrightarrow Z$ existiert mit $p_i \circ f = q_i$ $(i = 1, 2)$.

(2.6) Es sei V ein n-dimensionaler K-Vektorraum und $\mathcal{B} = (v_1, ..., v_n)$ sei eine Basis von V.
a) Zeigen Sie: Die natürliche Operation von S_n auf $\{1, ..., n\}$ induziert eine Linksoperation von S_n auf V. Für $v = x_1 v_1 + ... + x_n v_n$ und $\pi \in S_n$ ist $\pi v := x_{\pi^{-1}(1)} v_1 + ... + x_{\pi^{-1}(n)} v_n$. Die Abbildung $\Phi_\pi : V \longrightarrow V$, $v \mapsto \pi v$ ist linear. Bestimmen Sie die Matrix von Φ_π bezüglich der Basis $\mathcal{B}$. Finden Sie einen $(n - 1)$-dimensionalen S_n-invarianten Untervektorraum von V.
b) Beschreiben Sie die natürliche Operation von S_3 auf $\mathbb{C}^3$. Geben Sie $\pi(z_1, z_2, z_3)$ an. Zeigen Sie , dass der Untervektorraum V von $\mathbb{C}^3$ mit der Basis $\mathcal{B} = (v_1, v_2)$ mit $v_1 = (\omega, 1, \omega^2)$, $v_2 = (1, \omega, \omega^2)$ S_3-invariant ist. Dabei ist $\omega = e^{\frac{2\pi i}{3}} = \frac{1}{2}\left(-1 + \sqrt{3}\,i\right)$

primitive dritte Einheitswurzel, es gilt also $1 + \omega + \omega^2 = 0$. Geben Sie die Matrix von $\Phi_\pi \mid V$ bezüglich der Basis $\mathcal{B}$ an für $\pi = (123)$ und für $\pi = (12)$.

(2.7) Es seien $x = (123), y = (12) \in S_3$ wie in Übung (1.3). Nun sei eine Linksoperation $S_3 \times W \longrightarrow W$ auf einem endlich-dimensionalen $\mathbb{C}$-Vektorraum gegeben und zwar in der Weise, dass die Abildungen $\Phi_\pi : W \longrightarrow W, v \mapsto \pi v$ linear sind. Kurz: Es sei ein endlich-dimensionaler S_3-Modul W über $\mathbb{C}$ gegeben. Die folgenden Aufgaben sollen klären, wie solch eine komplexe lineare Darstellung von S_3 aufgebaut ist ($\longrightarrow$Fulton/Harris: Representation Theory, A First Course, GTM RIM 129, Springer 1996). Zeigen Sie:

a) Die Eigenwerte von Φ_x sind dritte Einheitswurzeln, also Potenzen von $\omega = e^{\frac{2\pi i}{3}} = \frac{1}{2}\left(-1 + \sqrt{3}\, i\right)$.

b) Ist $V \subset W$ ein minimaler Φ_x-invarianter nichttrivialer Untervektorraum, so ist $\dim V = 1$. (Hinweis: Betrachte $\Phi_x - \lambda \mathrm{id}_V : V \longrightarrow V$ für einen Eigenwert λ von $\Phi_x \mid V$ und zeige, dass $\ker(\Phi_x - \lambda \mathrm{id}_V) = V$ gelten muss. Folgere dann $\dim V = 1$.)

c) Ist $V \subset W$ ein Φ_x-invarianter Untervektorraum, so gibt es einen zu V komplementären Φ_x-invarianten Untervektorraum $U \subset W$, d. h. $W = V \oplus U$. (Hinweis: Es sei h ein unitäres Skalarprodukt auf W. Bilde das neue Skalarprodukt h' mit $h'(v, w) = h(v, w) + h(\Phi_x v, \Phi_x w) + h(\Phi_{x^2} v, \Phi_{x^2} w)$. Man kann dann U als orthogonales Komplement von V bezüglich h' wählen. Beachte, dass jetzt Φ_x orthogonale Abbildung bezüglich h' ist.)

d) Φ_{x^i} ist diagonalisierbar für alle $i \in \mathbb{N}$. Man kann also eine Basis $(v_1, \ldots, v_m)$ von W wählen, so dass $\Phi_x(v_i) = \omega^{\alpha_i} v_i$ mit gewissen $\alpha_i \in \{0, 1, 2\}$. Damit ist dann klar wie $A_3 = \langle x \rangle$ operiert.

e) Es gilt die Relation $xy = yx^2$. Ist $v \in W$ ein Eigenvektor von Φ_x mit Eigenwert ω^i, so ist $\Phi_y(v)$ Eigenvektor von Φ_x mit Eigenwert ω^{2i} und $\mathrm{Span}(v, \Phi_y(v))$ ist ein S_3-invarianter Untervektorraum.

f) W ist eine direkte Summe von höchstens zweidimensionalen S_3-invarianten Untervektorräumen.

(2.8) Man nennt einen G-Modul *irreduzibel*, wenn er keine echten G-invarianten Untervektorräume besitzt. Die einzigen irreduziblen S_3-Moduln über $\mathbb{C}$ sind die folgenden drei Beispiele:

a) $V_1 = (\mathbb{C}^1, \pi z = z)$.

b) $V_2 = (\mathbb{C}^1, \pi z = \mathrm{sign}(\pi)\, z)$.

c) $V_3 = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \mid z_1 + z_2 + z_3 = 0\}$ mit der natürlichen Operation von S_3.

(2.9) a) Betrachte die Operation $\mathrm{GL}_2(\mathbb{C}) \times M_2(\mathbb{C}) \longrightarrow M_2(\mathbb{C}), (A, B) \mapsto AB$. Wie sehen die Bahnen dieser Operation aus? Liegen $\begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix}$ und $\begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}$ in derselben Bahn?

b) Betrachte die Operation $\mathrm{GL}_2(\mathbb{C}) \times M_2(\mathbb{C}) \longrightarrow M_2(\mathbb{C}), (A, B) \mapsto ABA^{-1}$. Wie sehen die Bahnen dieser Operation aus? Liegen $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ und $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ in derselben Bahn?

(2.10) a) Es sei K ein Körper und L ein Erweiterungskörper von K. Dann bilden die Körperautomorphismen $\varphi : L \longrightarrow L$, die auf $K \subset L$ die Identität induzieren eine Gruppe, die mit $\mathrm{Aut}(L/K)$ bezeichnet wird. Genauer: $\mathrm{Aut}(L/K)$ ist eine Untergruppe von $\mathrm{GL}(L)$, wobei L in natürlicher Weise als K-Vektorraum aufgefasst wird.
b) Bestimmen Sie $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$.
c) Bestimmen Sie $\mathrm{Aut}(K/\mathbb{Q})$, wobei $K = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$.

(2.11) Zeigen Sie:
a) Die Standarddarstellung von $\mathrm{SO}(n)$ auf $\mathbb{R}^n$ ist irreduzibel (siehe Übung (2.8))
b) Der $\mathrm{SU}(2)$-Modul Y aus Beispiel 2.13.4 ist irreduzibel.

(2.12) Eine Gruppe G operiere treu auf einer Menge X mit fünf Elementen und besitze eine Bahn A mit drei und eine weitere Bahn B mit zwei Elementen. Beweisen Sie, dass G zu einer Untergruppe von $\{\pi \in S(X) \mid \pi(A) = A\}$ isomorph ist. Welche Möglichkeiten gibt es für G?

(2.13) Es seien X, Y G-Mengen. a) Erklären Sie eine natürliche Operation von G auf $X \times Y$. Beschreiben Sie die Standgruppen. b) Erklären Sie eine natürliche Operation von G auf der Potenzmenge $\mathcal{P}(X)$. Welche Elemente von $\mathcal{P}(X)$ sind G-Fixpunkte?

3 Normalteiler, Faktorgruppen und Produkte von Gruppen

Inhalt: *Normalteiler*, *Faktorgruppe*, universelle Eigenschaft der Faktorgruppe, Homomorphiesatz, Beispiele: $A_n \lhd S_n$, $\mathrm{SL}_n(K) \lhd \mathrm{GL}_n(K)$, $S^1 \cong \mathbb{R}/2\pi\mathbb{Z}$, die *Kleinsche Vierergruppe* als Normalteiler in S_4. *Konjugationsklassen*, *innere Automorphismen*, Beispiel: Konjugation in S_n. konkrete Beschreibung der Konjugationsklassen in S_5 und A_5.
direkte Produkte, Produktsatz, *semidirekte Produkte*, Beispiel: $\mathrm{Aff}(V) = V \times_\Phi \mathrm{GL}(V)$.

- **Definition 3.1**

Es sei G eine Gruppe. Eine Untergruppe N von G heißt *Normalteiler* in G, in Zeichen: $N \lhd G$, wenn jede Linksnebenklasse gN mit der entsprechenden Rechtsnebenklasse Ng übereinstimmt, wenn also gilt:
(3.1.1) Für alle $g \in G$ gilt $gN = Ng$.

- **Bemerkung 3.2**

⚠ Achtung: Die Gleichung $gN = Ng$ soll natürlich nicht bedeuten, dass $gn = ng$ für alle $n \in N$ gilt, sonderen vielmehr folgendes:
Zu jedem $n \in N$ gibt es ein $m \in N$, so dass $gn = mg$ gilt, und umgekehrt: Zu jedem $n \in N$ gibt es ein $m \in N$, so dass $ng = gm$ gilt.

- **Einführung 3.3**

Wir kommen zum wichtigen Begriff der *Faktorgruppe*. Das Ziel ist es, die Menge der Linksnebenklassen eines Normalteilers zu einer Gruppe zu machen und zwar in der Weise, dass die kanonische Quotientenabbildung ein Gruppenhomorphismus ist. Es sei also G eine Gruppe und N ein Normalteiler in G, $N \lhd G$. Die Linksoperation von G auf der Menge der Linksnebenklassen G/N, $(x, gN) \mapsto \Phi_x(gN) = xgN$, die ja für jede Untergruppe, also auch für N erklärt ist, hat in diesem Fall eine besondere Eigenschaft. Liegen nämlich $x, y \in G$ in derselben Linksnebenklasse von N, gilt also $y = xn$ für ein $n \in N$, so gibt es zu $g \in G$, weil N ein Normalteiler ist, auch ein $m \in N$, so dass $ng = gm$. Es folgt daher
$\Phi_y(gN) = ygN = xngN = xgmN = xgN = \Phi_x(gN)$.
x und y operieren also identisch auf G/N, d.h. $\Phi_x = \Phi_y$. Die Linksoperation $G \times G/N \longrightarrow G/N$ induziert somit eine Multiplikation
$* : G/N \times G/N \longrightarrow G/N,\ (xN, gN) \mapsto xgN$.
Bezeichnet man mit $\pi : G \longrightarrow G/N$ die Quotientenabbildung, so gilt also für alle $x, g \in G$: $\pi(xg) = xgN = \Phi_x(gN) = \Phi_x(\pi(g)) = \pi(x) * \pi(g)$. Hieraus kann man sofort ableiten, dass die Multplikation $*$ assoziativ ist, dass $\pi(e)$ das neutrale Element von G/N ist und dass jedes Element in G/N invertierbar ist, G/N somit eine Gruppe ist! Dies ist die *Faktorgruppe* von G nach dem Normalteiler N. Wir wollen diese Konstruktion nocheinmal mithilfe des *Komplexproduktes* ausführlich erklären.

- **Definition 3.4**

Es sei G eine Gruppe. Für beliebige Teilmengen A, B von G wird das Produkt (auch *Komplexprodukt* genannt) AB in naheliegender Weise definiert als die Menge aller Produkte xy mit $x \in A$, $y \in B$, also

$$AB := \{xy \mid x \in A, y \in B\}.$$

Ist $A = \{x\}$ einelementig, so gilt offensichtlich $xB = AB$.

■ **Lemma 3.5**

Es sei G eine Gruppe. Es gilt:
(3.5.1) Das Komplexprodukt ist assoziativ: Für alle Teilmengen A, B, $C \subset G$ gilt

$$(A\,B)\,C = A(B\,C).$$

(3.5.2) Ist H eine Untergruppe von G, so gilt $H\,H = H$.
(3.5.3) Ist N ein Normalteiler von G, so gilt für alle $x, y \in G$: $(x\,N)\,(y\,N) = x\,y\,N$. Das Produkt zweier Nebenklassen von N ist also wieder eine Nebenklasse von N.

Beweis. (3.5.1) folgt aus dem Assoziativgesetz für die Multiplikation in G.
zu (3.5.2): Da $e \in H$, ist $H = H\,e \subset H\,H$. Da mit $a, b \in H$ auch $a\,b \in H$, gilt auch $H\,H \subset H$.
zu (3.5.3): $(x\,N)\,(y\,N) = x\,N\,N\,y = x\,N\,y = x\,y\,N$. □

■ **Satz und Definition 3.6**

Es sei G eine Gruppe und N ein Normalteiler von G. Dann ist durch das Komplexprodukt $(x\,N)\,(y\,N) = x\,y\,N$ eine Gruppenstruktur auf der Menge G/N der Linksnebenklassen von N in G definiert. Die Quotientenabbildung $\pi : G \longrightarrow G/N$ ist ein surjektiver Gruppenhomomorpismus mit N als Kern.
G/N heißt die *Faktorgruppe* von G nach N. $\pi : G \longrightarrow G/N$ heißt auch der kanonische Homomorphismus. Er besitzt die folgende universelle Eigenschaft:

(3.6.1) Zu jedem Gruppenhomomorphismus $\varphi : G \longrightarrow G'$ mit $N \subset \ker\varphi$ gibt es genau einen Homomorphismus $\overline{\varphi} : G/N \longrightarrow G'$ mit $\varphi = \overline{\varphi} \circ \pi$. Man nennt $\overline{\varphi}$ den von φ induzierten Homomorphismus.

Beweis. Nach (3.5.3) gilt $(x\,N)\,(y\,N) = x\,y\,N$. Wir haben also durch das Komplexprodukt eine Multiplikation auf G/N. Nach (3.5.1) ist diese Multiplikation assoziativ. Weiter gilt $g\,N\,e\,N = g\,N\,N = N\,g\,N = e\,N\,g\,N$. Damit ist $N = e\,N$ das neutrale Element in G/N. Da $g\,N\,g^{-1}\,N = g\,g^{-1}\,N = e\,N = g^{-1}\,g\,N$, ist $g^{-1}\,N$ das Inverse von $g\,N$. Damit ist G/N eine Gruppe. $\ker\pi = \{g \in G \mid g\,N = N\} = N$, denn es gilt ja bekanntlich für zwei Restklassen $g\,N = h\,N$ genau dann, wenn $g \in h\,N$.
Zu (3.6.1): Wir setzen $\overline{\varphi}(g\,N) := \varphi(g)$. Dies ist wohldefiniert, denn ist $g\,N = h\,N$, so ist $h^{-1}\,g\,N = N$, also $h^{-1}\,g \in N \subset \ker\varphi$ und somit $\varphi(h^{-1}\,g) = e$, woraus $\varphi(g) = \varphi(h)$ folgt. $\overline{\varphi}$ hat die gewünschten Eigenschaften und ist offensichtlich durch die Eigenschaft $\varphi = \overline{\varphi} \circ \pi$ eindeutig bestimmt. □

- **Korollar 3.7 (Homomorphiesatz)**

Es sei $\varphi : G \longrightarrow G'$ ein surjektiver Gruppenhomorphismus. Dann ist der induzierte Homomorphismus $\overline{\varphi} : G/\ker\varphi \longrightarrow G'$ ein Isomorphismus.

Beweis. Wir müssen nur noch zeigen, dass $\overline{\varphi}$ injektiv ist, also der Kern von $\overline{\varphi}$ nur das neutrale Element von $G/\ker\varphi$ enthält. Es gilt aber nach Konstruktion $\overline{\varphi}(g\ker\varphi) = e \Longleftrightarrow g \in \ker\varphi$. □

- **Bemerkung 3.8**

Man kann die Normalteiler einer Gruppe G auch folgendermaßen charakterisieren: Es sei $N \subset G$ eine Untergruppe. Dann sind folgene Aussagen äquivalent.
(3.8.1) N ist Normalteiler in G.
(3.8.2) Für alle $g \in G$, $x \in N$ gilt $g\,x\,g^{-1} \in N$. Also: Mit x enthält N auch alle zu x konjugierten Elemente $g\,x\,g^{-1}$.
(3.8.3) Es gibt einen Gruppenhomorphismus $\varphi : G \longrightarrow G'$ mit $N = \ker\varphi$.
(3.8.4) Alle zu N konjugierten Untergruppen stimmen mit N überein: $N = g\,N\,g^{-1}$ für alle $g \in N$.

Beweis. Wir zeigen nur (3.8.3)$\Longrightarrow$(3.8.2): Es sei $\varphi : G \longrightarrow G'$ Homomorphismus und $N = \ker\varphi$. Ist nun $g \in G$, $x \in N$, so gilt
$\varphi(g\,x\,g^{-1}) = \varphi(g)\,\varphi(x)\,\varphi(g^{-1}) = \varphi(g)\,e\,\varphi(g^{-1}) = \varphi(g)\,\varphi(g^{-1}) = \varphi(g\,g^{-1}) = \varphi(e) = e$, also $g\,x\,g^{-1} \in N$. Damit ist N ein Normalteiler. □

Es ist nicht einfach, die Normalteiler in einer Gruppe G aufzuspüren. Es läuft darauf hinaus, Homomorphismen von G in eine andere Gruppe zu beschreiben. Gruppen, die überhaupt keine nicht-trivialen Normalteiler enthalten, für die also jede nichtkonstante Gruppenhomomorphismus in eine andere Gruppe automatisch injektiv ist, heißen *einfache Gruppen*. Das Suchen nach den einfachen endlichen Gruppen war eine abenteuerliche Geschichte! ($\longrightarrow$G. Hiss: Die Sporadischen Gruppen, in: Jahresbericht der DMV 4-2003) Das geht weit über diese Vorlesung hinaus. Es folgen einige Besipiele:

- **Beispiele 3.9**

(3.9.1) Die alternierende Gruppe A_n ist der Kern des Homomorphismus $\mathrm{sign} : S_n \longrightarrow \{\pm 1\}$, A_n ist also ein Normalteiler in S_n und nach dem Homomorphiesatz gilt $S_n/A_n \cong \{\pm 1\}$.

(3.9.2) $\mathrm{SL}_n(K)$ ist der Kern der Determinante $\det : \mathrm{GL}_n(K) \to K^\times$, und es gilt $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K^\times$.

(3.9.3) $\mathrm{SO}(n)$ ist eine Untergruppe aber kein Normalteiler in $\mathrm{SL}_n(\mathbb{R})$, falls $n \geq 1$, denn es gilt zum Beispiel $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix} \notin \mathrm{SO}(2)$.

(3.9.3) $S^1 \cong \mathbb{R}/2\pi\mathbb{Z}$, denn $t \mapsto e^{it}$ ist ein surjektiver Gruppenhomomorphismus der additiven Gruppe $(\mathbb{R}, +)$ auf die multiplikative Gruppe $S^1 \subset \mathbb{C}^\times$ mit Kern $2\pi\mathbb{Z}$.
(3.9.4) $\mathbb{C}^\times / S^1 \cong \mathbb{R}_{>0}$, induziert von $z \mapsto |z|$.

(3.9.5) Es sei $H = \{(1), (12)(34), (13)(24), (14)(23)\}$(siehe Übung (1.13)). H ist ein Normalteiler in S_4, denn wir können zeigen, dass die Teilmenge $M = \{(12)(34), (13)(24), (14)(23)\}$ eine volle Klasse konjugierter Elemente in S_4 ist. Nach (3.8.2) ist somit H ein Normalteiler. Die Menge M besteht offensichtlich aus allen Permutationen deren Zykeldarstellung das Produkt zweier elementfremder Transpositionen ist. Nach dem folgenden Lemma 3.11 ist daher M -wie behauptet- eine volle Konjugationsklasse. H heißt die *Kleinsche Vierergruppe*.

(3.9.6) Die zyklische Gruppe C_n mit Erzeuger x ist isomorph zu der (additiven) Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$, denn $\varphi : \mathbb{Z} \longrightarrow C_n$, $k \mapsto x^k$ ist surjektiv und hat den Kern $n\mathbb{Z}$. Wir schreiben üblicherweise, wenn der 'Modul' n festgelegt ist, die Elemente von $\mathbb{Z}/n\mathbb{Z}$ als Reste 0, 1, 2, 3, ..., $n-1$ und rechnen modulo n. Legen wir zum Beispiel $n = 13$ fest, so gilt in $\mathbb{Z}/n\mathbb{Z}$: $4 + 10 = 1$, $9 + 9 = 5$. Klassischerweise schreibt man dafür nach Gauss auch

$$4 + 10 \equiv 1 \bmod 13, \quad 9 + 9 \equiv 5 \bmod 13.$$

$$a \equiv b \bmod n$$

ist die von Gauss eingeführte Kongruenzschreibweise für die Tatsache 'n teilt $b - a$'. Wir gehen einen Schritt weiter und erlauben uns einfach $a = b$ (eventuell mit dem Zusatz 'in $\mathbb{Z}/n\mathbb{Z}$') zu schreiben. Wichtig dabei ist, dass man sich klar macht in welchem Kontext man sich befindet, dass also hier zum Beispiel 9 als Symbol für ein Element in der Faktorgruppe $\mathbb{Z}/13\mathbb{Z}$ zu verstehen ist, nämlich als die Restklasse $9 + 13\mathbb{Z}$. In diesem Kontext ist also $9 + 9 = 5$ vollkommen ok.

(3.9.7) Es gilt $\mathrm{SU}(2)/\{\pm E\} \cong \mathrm{SO}(3)$.

- **Lemma und Definition 3.10**

Es sei G eine Gruppe. Dann operiert G durch *Konjugation* auf sich selbst: $G \times G \longrightarrow G$, $(g, x) \mapsto I_g(x) := g x g^{-1}$. Die Bahn von x unter dieser Operation heißt die *(volle) Konjugationsklasse* von x und wird mit $C_G(x)$ oder kürzer mit $C(x)$ bezeichnet: $C(x) = \{y \in G \mid \exists\, g \in G : y = g x g^{-1}\} = \{g x g^{-1} \mid g \in G\}$. $x, y \in G$ heißen *konjugiert*, wenn es ein $g \in G$ gibt, so dass $y = g x g^{-1}$. $I_g : G \longrightarrow G$ ist ein Automorphismus und heißt der von g definierte *innere Automorphismus* die Menge aller inneren Automorphismen ist eine Untergruppe von $\mathrm{Aut}(G)$.

Beweis. Die Eigenschaften einer Linksoperation sind erfüllt: $I_e(g) = e\,g\,e^{-1} = g$, $I_{g\,h}(x) = (g\,h)\,x\,(g\,h)^{-1} = g\,h\,x\,h^{-1}\,g^{-1} = I_g(I_h(x))$.
I_g ist ein Automorphismus, denn: $I_g(x\,y) = g\,x\,y\,g^{-1} = g\,x\,g^{-1}\,g\,y\,g^{-1} = I_g(x)\,I_g(y)$.
□

■ **Lemma 3.11**

Es sei $\pi = \zeta_1 \circ ... \circ \zeta_s$ die Zykeldarstellung der Permutation $\pi \in S_n$ (einschließlich der Einerzyklen). Es sei d_i die Ordnung von ζ_i. Es gelte $d_1 \geq d_2 \geq ... \geq d_s$. Dann ist $(d_1,\ ...,\ d_s)$ eine Partition von n, d.h. $\sum_{j=1}^{s} d_j = n$. Diese Partition heißt der Zykeltyp von π. Es gilt nun:

(3.11.1) Ist $\sigma \in S_n$, $\zeta = (a_1,\ ...,\ a_d) \in S_n$ Zykel der Länge d, so ist $\sigma \circ \zeta \circ \sigma^{-1}$ Zykel der Länge d: $\sigma \circ \zeta \circ \sigma^{-1} = (\sigma(a_1),\ ...,\ \sigma(a_d))$.

(3.11.2) $\sigma \circ \pi \circ \sigma^{-1} = (\sigma \circ \zeta_1 \circ \sigma^{-1}) \circ (\sigma \circ \zeta_2 \circ \sigma^{-1}) \circ ... \circ (\sigma \circ \zeta_d \circ \sigma^{-1})$
ist die Zykeldarstellung von $\sigma \circ \pi \circ \sigma^{-1}$.

(3.11.3) Zwei Permutationen in S_n sind genau dann zueinander konjugiert in S_n, wenn sie denselben Zykeltyp besitzen.

Beweis. Zu (3.11.1):
$\sigma \circ \zeta \circ \sigma^{-1}(\sigma(a_j)) = \sigma(\zeta(a_j)) = \sigma(a_{j+1})$, $\sigma \circ \zeta \circ \sigma^{-1}(\sigma(k)) = \sigma(\zeta(k)) = \sigma(k)$,
falls $k \notin \{a_1,\ ...,\ a_d\}$.
Zu (3.11.2): Das ist klar wegen (3.11.1).
Zu (3.11.3): Sind $\pi = (a_1,\ ...,\ a_{k_1})(a_{k_1},\ ...,\ a_{k_2}) ... (a_{k_{s-1}},\ ...,\ a_{k_s})$ und
$\gamma = (b_1,\ ...,\ b_{k_1})(b_{k_1},\ ...,\ b_{k_2}) ... (b_{k_{s-1}},\ ...,\ b_{k_s})$ gegeben, so ist $\sigma(a_j) = b_j$ eine Permutation in S_n, so dass $\gamma = \sigma\,\pi\,\sigma^{-1}$. Das ist klar wegen (3.11.1). □

- **Beispiel 3.12**

Die Anzahl der Klassen konjugierter Elemente in S_5 ist die Anzahl der Partitionen von 5. Man erhält durch Probieren die Partitionen
$(1, 1, 1, 1, 1), (2, 1, 1, 1), (3, 1, 1), (4, 1), (5), (2, 2, 1), (3, 2)$.
Die zugehörigen Konjugationsklassen sind
$C((1)), C((12)), C((123)), C((1234)), C((12345)), C((12)(34)), C((123)(45))$.
Da die Konjugationsklassen Bahnen einer S_5-Operation sind, sind ihre Ordnungen Teiler von 120. Nach der Bahnformel (2.10.3) gilt $|C(\sigma)| = 120/|H|$, wobei H die Standgruppe von σ ist, also $H = \{\pi \in S_5 \mid \pi\sigma = \sigma\pi\}$. Für $\sigma = (12)$ gilt $\pi\sigma = \sigma\pi$ genau dann, wenn in der Zykeldarstellung von π entweder die Einerzyklen $(1), (2)$ vorkommen oder aber die Transposition σ selbst (Beweis als Übung). Dafür gibt es $2 \cdot (3!) = 12$ Möglichkeiten. Also ist $|C((12))| = 10$. Das ist -wie es nach (3.11.3) sein muss- die Anzahl der möglichen Transpositionen $(i\ j), 1 \le i < j \le 5$, nämlich $\binom{5}{2} = 10$. Analog bekommt man durch Abzählen der Dreierzyklen
$|C((123))| = \frac{3!}{3}\binom{5}{3} = 20$, und durch Abzählen der Viererzyklen
$|C((1234))| = \frac{4!}{4}\binom{5}{4} = 3!\,5 = 30$, weiter $|C((12345))| = \frac{5!}{5} = 4! = 24$,
$|C((12)(34))| = \binom{5}{3}\binom{3}{2}\frac{1}{2} = 15, |C((123)(45))| = 20$. Man erhält die Zerlegung

$$120 = |C((1))| + |C((12))| + |C((123))| + |C((1234))| + |C((12345))| + |C((12)(34))| + |C((123)(45))| = 1 + 10 + 20 + 30 + 24 + 15 + 20$$

Ein Normalteiler $N \lhd S_5$ der Ordnung 60 muss somit (!) je eine Klasse konjugierter Elemente mit 1, 24, 15, 20 Elementen enthalten. Also ist $C((12)(34)) \subset N$. Für die Klasse mit 20 Elementen gibt es zwei Möglichkeiten. Wäre $C((123)(45)) \subset N$, so wäre auch
$(123)(45)(45)(12) = (123)(12) = (13) \in N$, also wären alle Transpositionen in N. Da die Transpositionen S_5 erzeugen, wäre dann $N = S_5$. Also ergibt sich $N = A_5$. Man kann sich leicht überlegen, dass es keine weiteren Normalteiler in S_5 gibt. Wie steht es aber mit Normalteilern in A_5? Die Klasse $K = C((12345))$ mit 24 Elementen ist in A_5 enthalten. K besteht aus den Elementen der Ordnung 5. Da nun 24 kein Teiler von 60 ist, kann K keine Konjugationsklasse von A_5 sein. Ist $\zeta \in K$, so ist die Standgruppe H von ζ in S_5 von der Ordung 5, also zyklisch mit einem erzeugenden Element der Ordnung 5. Da Fünferzyklen gerade Permutationen sind, gilt also $H \subset A_5$ und somit zerfällt K in zwei A_5-Konjugationsklassen der Ordnung $\frac{60}{5} = 12$. Repräsentanten dieser zwei Klassen sind zum Beispiel
$(12345), (12354) = (45)(12345)(45)$. (Begründung! Wird in (4.5.2) ausgeführt.)
Die anderen Klassen, nämlich $C((1)), C((123)), C((12)(34))$ sind auch A_5-Konjugationsklassen (Begründung mit Hilfe von Standgruppen! Wird in (4.5.2)

ausgeführt.)

- **Definition und Satz 3.13**

Es seien G_1, G_2 Gruppen. Auf dem cartesischen Produkt $G = G_1 \times G_2$ werde die folgende Verknüpfung eingeführt: $(x_1, x_2)(y_1, y_2) := (x_1 y_1, x_2 y_2)$. Dann gilt:

(3.13.1) G ist eine Gruppe. Die Projektionen $\pi_j : G \longrightarrow G_j,\ (x_1, x_2) \mapsto x_j$
sind Gruppenhomomorphismen.

(3.13.2) (universelle Eigenschaft)
Für jedes Paar (φ_1, φ_2) von Gruppenhomomorphismen $\varphi_j : H \longrightarrow G_j$ gibt es genau einen Gruppenhomomorphismus $\varphi : H \longrightarrow G$, so dass $\varphi_j = \pi_j \circ \varphi$ gilt.

(3.13.3) $\iota_1 : G_1 \longrightarrow G,\ \iota_2 : G_2 \longrightarrow G$ mit $\iota_1(x) = (x, e), \iota_2(x) = (e, x)$
sind injektive Gruppenhomomorphismen und es gilt
$H_1 := \operatorname{im} \iota_1 = \ker \pi_2, H_2 := \operatorname{im} \iota_2 = \ker \pi_1$.
Insbesondere sind H_1 und H_2 Normalteiler in G.

(3.13.4) $G = H_1 H_2$ (als Komplexprodukt)

(3.13.5) Für alle $x_1 \in H_1, x_2 \in H_2$ gilt $x_1 x_2 = x_2 x_1$.
Die Gruppe G (zusammen mit den Projektionen π_j) heißt das (direkte) Produkt von G_1 und G_2.

Beweis. Zu (3.13.1): Solche Beweise sind aus der linearen Algebra bekannt. Es steckt kein Tiefsinn dahinter. Man muss sich nur vergewissern, dass die gewünschten Regeln gelten. Zum Beispiel ist (e, e) das neutrale Element in G und $(x, y)^{-1} = (x^{-1}, y^{-1})$ das Inverse zu (x, y).
Zu (3.13.2): Man setzt $\varphi(h) := (\varphi_1(h), \varphi_2(h))$. Es gilt $\varphi : H \longrightarrow G$ ist Homomorphismus und $\varphi_j = \pi_j \circ \varphi$. Offensichtlich ist φ auch eindeutig durch $\varphi_j = \pi_j \circ \varphi$ bestimmt.
Zu (3.13.3): Es gilt $(x, e)(y, e) = (xy, e)$ also ist ι_1 ein Homomorphismus. Dasselbe gilt für ι_2. Weiter ist $(x, y) \in \operatorname{im} \iota_1 \Longleftrightarrow y = e \Longleftrightarrow (x, y) \in \ker \pi_2$. Genauso klar ist $\operatorname{im} \iota_2 = \ker \pi_1$.
Zu (3.13.4): $(x, y) = (x, e)(e, y)$.
Zu (3.13.5): $(x, e)(e, y) = (e, y)(x, e)$. □

- **Beispiele 3.14**

(3.14.1) Die Kleinsche Vierergruppe (3.9.5) ist isomorph zu $C_2 \times C_2$.

(3.14.2) Die zyklische Gruppe C_{nm} der Ordnung nm mit teilerfremden Zahlen m, n ist isomorph zu dem direkten Produkt $C_n \times C_m$. Diese Aussage ist äquivalent zu dem bekannten 'Chinesischen Restsatz' der elementaren Zahlentheorie. Der

Beweis ist ganz einfach: Es seien x, y Erzeuger von C_n beziehungsweise C_m und z sei ein Erzeuger von C_{nm}. Man erhält wohldefinierte Homomorphismen $\varphi_1 : C_{nm} \longrightarrow C_n$, $\varphi_2 : C_{nm} \longrightarrow C_m$ mit $\varphi_1(z^k) = x^k$, $\varphi_2(z^k) = y^k$ und somit einen Homomorphismus $\varphi : C_{nm} \longrightarrow C_n \times C_m$ mit $\varphi(z^k) = (x^k, y^k)$. Dieser Homomorphismus ist injektiv, denn $\varphi(z^k) = e \Longleftrightarrow (x^k = e \text{ und } y^k = e) \Longleftrightarrow k$ ist gemeinsames Vielfaches von n und $m \Longleftrightarrow k$ ist Vielfaches von $nm \Longleftrightarrow z^k = e$. Da C_{nm} und $C_n \times C_m$ die gleiche Anzahl von Elementen haben, ist φ ein Isomorphismus.

Ein konkretes Beispiel: Der Isomorphismus $\varphi : \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ hat die Wertetabelle

0	(0, 0)
1	(1, 1)
2	(2, 2)
3	(3, 0)
4	(0, 1)
5	(1, 2)
6	(2, 0)
7	(3, 1)
8	(0, 2)
9	(1, 0)
10	(2, 1)
11	(3, 2)

Bemerkung: Es gibt einen Algorithmus zur Berechnung der Umkehrabbildung $\varphi^{-1} : C_n \times C_m \longrightarrow C_{nm}$. Man bestimmt mit Hilfe des *erweiterten euklidischen Algorithmus* zwei ganze Zahlen a, b mit

$$a\,m \equiv 1 \bmod n,\ b\,n \equiv 1 \bmod m$$

und setzt

$$e = a\,m,\ f = b\,n.$$

Für $x, y \in \mathbb{Z}$ gilt dann

$$e\,x + f\,y = a\,m\,x + b\,n\,y \equiv x \bmod n$$
$$e\,x + f\,y = a\,m\,x + b\,n\,y \equiv y \bmod m.$$

Damit wird durch

$$\psi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z},\ \psi(x, y) := e\,x + f\,y$$

die Umkehrabbildung von φ induziert. Für $n = 4, m = 3$ kann man $a = -1, b = 1$ wählen, also $e = -3$, $f = 4$.

Es gilt also $\varphi^{-1}(x, y) = -3x + 4y \bmod 12$, zum Beispiel:
$\varphi^{-1}(3, 2) = -3 \cdot 3 + 4 \cdot 2 = 11$ in $\mathbb{Z}/12\mathbb{Z}$.

(3.14.3) Die Gruppe S_3 ist nicht isomorph zu einem direkten Produkt nichttrivialer Gruppen, denn dies müssten ja die Gruppen C_2 und C_3 sein und S_3 wäre dann abelsch. Man kann auch zeigen (→Übung (4.7)), dass S_n nicht zu einem direkten Produkt nichttrivialer Gruppen isomorph ist.

- **Satz 3.15**

Es sei G eine Gruppe und H, K seien Untergruppen. Die surjektive Abbildung

$$\varphi : H \times K \longrightarrow HK, (h, k) \mapsto hk$$

hat die folgenden Eigenschaften:

(3.15.1) φ ist genau dann injektiv, wenn $H \cap K = \{e\}$.

(3.15.2) Ist K ein Normalteiler von G, so gilt $HK = KH$ und HK ist eine Untergruppe von G der Ordnung $|H|\,|K| / |H \cap K|$.

(3.15.3) Gilt $H \cap K = \{e\}$ und gilt $hk = kh$ für alle $h \in H, k \in K$, so ist HK eine Untergruppe und φ ein Isomorphismus, wobei $H \times K$ die direkte Produktgruppenstruktur trägt.

(3.15.4) Sind H, K beide Normalteiler in G und gilt $H \cap K = \{e\}$, so ist φ ein Isomorphismus, wobei $H \times K$ die direkte Produktgruppenstruktur trägt.

Beweis. Zu (3.15.1):
'$\Longrightarrow$': Ist $x \in H \cap K$, so ist auch $x^{-1} \in H \cap K$, also $(x, x^{-1}) \in H \times K$ und $\varphi(x, x^{-1}) = e = \varphi(e, e)$. Wegen der Injektivität von φ folgt somit $x = e$.
'$\Longleftarrow$':
$\varphi(h, k) = \varphi(x, y) \Longrightarrow hk = xy \Longrightarrow x^{-1}h = yk^{-1} \in H \cap K = \{e\} \Longrightarrow h = x, k = y$.

Zu (3.15.2): Es sei $k \in K$, $h \in H$. Da K Normalteiler ist, ist somit $m := hkh^{-1} \in K$ und somit $hk = mh$, also $HK \subset KH$. Natürlich ist auch $n := h^{-1}kh \in K$, also $kh = hn$ und somit $KH \subset HK$. Wir zeigen, dass $L = HK$ eine Untergruppe von G ist: Dazu müssen wir nur zeigen, dass mit $x, y \in L$ auch $xy^{-1} \in L$. Sei dazu $x = hk$, $y = ab$ mit $h, a \in H, k, b \in K$. Dann gilt $kb^{-1} \in K$, also $kb^{-1}a^{-1} \in KH$ und wegen $KH = HK$ gibt es somit $c \in H, d \in K$, so dass $kb^{-1}a^{-1} = cd$. Es folgt $xy^{-1} = hkb^{-1}a^{-1} = hcd \in HK$.
Die Formel für die Ordnung von HK ergibt sich durch Untersuchung der Fasern der Abbildung $\varphi : H \times K \longrightarrow HK$. Für $x = h'k' \in HK$ ist
$\varphi^{-1}(x) = \{(h, k) \in H \times K \mid hk = h'k'\} = \{(h'k'k^{-1}, k) \mid k \in (K \cap H)k'\}$
von derselben Mächtigkeit wie $H \cap K$.

Zu (3.15.3): Es gilt offensichtlich
$\varphi((h, k)(x, y)) = \varphi(hx, ky) = hxky = hkxy = \varphi(h, k)\varphi(x, y)$. Damit ist
$\varphi : H \times K \longrightarrow HK$ ein Isomorphismus.
Zu (3.15.4): Wegen (3.15.3) genügt es zu zeigen, dass $hk = kh$ für alle $h \in H$, $k \in K$ gilt. Es gilt $hk(kh)^{-1} = (hkh^{-1})k^{-1} \in K$, weil K Normalteiler ist. Da auch H Normalteiler ist, gilt auch $hk(kh)^{-1} = h(kh^{-1}k^{-1}) \in H$. Damit ist $hk(kh)^{-1} \in H \cap K = \{e\}$, also $hk = kh$.

- **Beispiel 3.16**

(3.16.1) Ist G eine endliche Gruppe, so kann man versuchen die Struktur von G zu ergründen, indem man einen nichttrivialen Normalteiler $N \lhd G$ aufspürt und eventuell eine Untergruppe $H \subset G$, so dass $N \cap H = \{e\}$ und $|G| = |N|\,|H|$. Dann ist $G = NH$ (nach (3.15.2)). Aber NH ist im allgemeinen kein direktes Produkt. Jedes Element $g \in G$ hat zwar eine eindeutig bestimmte Zerlegung $g = nh$ mit $n \in N$, $h \in H$. Die bijektive Abbildung $(n, h) \mapsto nh$ ist kein Homomorphismus $\varphi : N \times H \longrightarrow G$. Es ist vielmehr so: H operiert auf N durch Konjugation: $I_h(n) = hnh^{-1}$. Es gilt dann für $n, m \in N$, $h, k \in H$:

$$(nh)(mk) = nhmk = n(hmh^{-1})hk = nI_h(m)hk.$$

Definiert man nun auf dem cartesischen Produkt $N \times H$ eine Multiplikation $*_I$ durch $(n, h) *_I (m, k) := (nI_h(m), hk)$, so wird $\varphi : N \times H \longrightarrow G$ ein Isomorphismus. Durch N, H und die Operation von H auf N ist damit G vollständig beschrieben. Für $G = S_3$ kann man $N = A_3 = \langle x \rangle$, $x = (123)$ und $H = \langle y \rangle$, $y = (12)$ wählen. Die Konjugation $I_y : N \longrightarrow N$ ist dann der Automorphismus mit $x = (123) \mapsto (213) = x^2$. Es gilt $S_3 = NH \cong N \times H$, wobei auf $N \times H$ die Multiplikation wie folgt zu definieren ist:

$$(x^k, y^i) * (x^m, y^j) = (x^k I_{y^i}(x^m), y^{i+j}) = \left(x^{k+2^i m}, y^{i+j}\right) = \begin{cases} (x^{k+m}, y^{i+j}), & \text{falls } i = 0 \\ (x^{k+2m}, y^{i+j}), & \text{falls } i = 1 \end{cases}$$

(3.16.2) Es sei V ein endlich-dimensionaler K-Vektorraum und $G = \mathrm{Aff}(V)$ die affine Gruppe von V. $N = \mathrm{Trans}(V) \subset G$ sei die zur additiven Gruppe $(V, +)$ isomorphe Untergruppe der Translationen. Weiter sei $H = \mathrm{GL}(V) \subset G$ die allgemeine lineare Gruppe. Offensichtlich ist $N \cap H = \{\mathrm{id}_V\}$ und N ist ein Normalteiler in G. Abstrakt sieht man das so ein: Die Abbildung $D : G \longrightarrow H$, die einer Affinität $f : V \longrightarrow V$ ihre Ableitung Df im Punkt $0 \in V$ zuordnet, ist nach der Kettenregel ein Gruppenhomomorphismus, der auf der Untergruppe H die Identität ist und als Kern die Gruppe N der Translationen (das sind die Affinitäten, deren Ableitung die Identität auf V ist) hat. Es gilt $G = NH$. Aber wieder ist dieses keine direkte Produktzerlegung von G, sondern H operiert durch Konjugation auf N. Ist $A \in H$, $a \in V$, $T_a \in N$ die zugehörige Translation $T_a(x) = x + a$, so ist
$A \circ T_a \circ A^{-1}(x) = A(A^{-1}(x) + a) = x + A(a) = T_{A(a)}(x)$.
Erklärt man auf $V \times \mathrm{GL}(V)$ die Multiplikation $*$ durch

$(a, A) * (b, B) := (a + A(b), A\,B)$, so erhält man eine zu Aff(V) isomorphe Gruppe $(V \times \mathrm{GL}(V), *)$. Dies ist (wie auch schon (3.16.1)) ein Beispiel eines sogenannten *semidirekten* Produktes. Das wollen wir jetzt erklären:

■ Definition und Satz 3.17

Es seien N, H Gruppen und $\Phi : H \longrightarrow \mathrm{Aut}(N)$, $h \mapsto \Phi_h$, sei ein Homomorphismus. Auf dem kartesischen Produkt $N \times H$ definiere man die Multiplikation $*_\Phi$ durch
$(n, h) *_\Phi (m, k) := (n\,\Phi_h(m), h\,k)$.
(3.17.1) Dann ist $G := (N \times H, *_\Phi)$ eine Gruppe. Sie heißt das *semidirekte Produkt* von N und H bezüglich der Operation Φ und wird auch mit $N \times_\Phi H$ bezeichnet.
(3.17.2) Die Projektion auf den zweiten Faktor $\pi_2 : N \times H \longrightarrow H$, $(n, h) \mapsto h$ ist ein Gruppenhomomorphismus mit Kern $N' = N \times \{e\} \cong N$. Die Einschränkung von π_2 auf die Untergruppe $H' = \{e\} \times H$ ist ein Isomorphismus von H' auf H.
(3.17.3) Es gilt $G = N'\,H'$, N' ist Normalteiler in G, $N' \cap H' = \{(e, e)\}$ und die Konjugation $I_{(e,h)} : N' \longrightarrow N'$ stimmt mit Φ_h überein in folgendem Sinne: $I_{(e,h)}(n, e) = (\Phi_h(n), e)$.

Beweis. Zu (3.17.1): Man verifiziert leicht die Gruppenaxiome. a) Der Nachweis des Assoziativgesetzes sei als Übung empfohlen:
b) Das neutrale Element ist $e = (e, e)$.
c) Das Inverse von (n, h) ist $(\Phi_{h^{-1}}(n^{-1}), h^{-1})$.
Zu (3.17.3):
$I_{(e,h)}(n, e) = (e, h) * (n, e) * (e, h^{-1}) = (\Phi_h(n), h) * (e, h^{-1}) =$
$(\Phi_h(n)\,\Phi_h(e), h\,h^{-1}) = (\Phi_h(n), e)$. □

Wir bemerken, dass das semidirekte Produkt direkt ist, wenn der Homomorphismus Φ trivial ist, d. h. wenn $\Phi_h = \mathrm{id}_N$ für alle $h \in H$.
Das direkte Produkt abelscher Gruppen ist wieder abelsch. Dagegen ist das semidirekte Produkt abelscher Gruppe im allgemeinen nicht abelsch, wie das Beispiel S_3 zeigt (3.16.1).

■ Übungen 3

(3.1) Es sei
$N = \{(1), (12)(34), (13)(24), (14)(23)\}$, $H = \{(1), (12), (13), (23), (123), (132)\}$.
a) Zeigen Sie, dass N Normalteiler und H eine Untergruppe von S_4 ist.
b) Zeigen Sie, dass $S_4 = N\,H$ gilt und beschreiben Sie die Konjugationsoperation von H auf N.
c) Versuchen Sie S_4 irgendwie als 'semidirektes' Produkt von drei Exemplaren C_2 und C_3 zu beschreiben. Dabei bezeichnet C_n eine zyklische Gruppe der Ordnung n.

(3.2) Es sei G eine endliche abelsche Gruppe der Ordnung n und p sei ein Primteiler von n. Durch Induktion nach $m = \frac{n}{p}$ zeige man, dass G ein Element der Ordnung p besitzt.

(3.3) Es sei G eine endliche abelsche Gruppe der Ordnung n. Durch Induktion nach n zeige man, dass es zu jedem Teiler m von n eine Untergruppe der Ordnung m von G gibt. Hinweis: Benutze Aufgabe (3.2).

(3.4) Es seien H, K Untergruppen einer Gruppe G. Zeigen Sie: Das Komplexprodukt HK ist genau dann eine Untergruppe von G, wenn $GH = HG$ gilt.

(3.5) Zeigen Sie: Konjugierte Elemente haben dieselbe Ordnung.

(3.6) Es sei G die Menge der oberen Dreiecksmatrizen $A = (a_{ij})$, $a_{ii} \neq 0$, $a_{ij} = 0$, falls $i > j$ in $\mathrm{GL}_n(K)$. Zeigen Sie , dass $N = \{A = (a_{ij}) \in G \mid a_{ii} = 1 \text{ für } I = 1, \ldots, n\}$ ein Normalteiler in G ist. Finden Sie eine Untergruppe H von G, so dass $G \cap N = \{E\}$ und $HN = G$. Zeigen Sie weiter, dass $G/N \cong H$ gilt.

(3.7) Finden Sie Untergruppen H, K der Diedergruppe D_4, so dass $H \lhd K \lhd D_4$ aber H kein Normalteiler von D_4 ist. (Die Folge $H \lhd K \lhd D_4$ nennt man dann übrigens eine Kompositionsreihe von D_4.)

(3.8) Es sei N ein abelscher Normalteiler einer Gruppe G. Ist dann jede Untergruppe von N auch ein Normalteiler von G? Gegenbeispiel: $G = S_4$. Behandeln Sie dieselbe Frage für zyklische Normalteiler.

(3.9) Es sei G eine Gruppe. Beweisen Sie: Bis auf Isomorphie gibt es genau eine abelsche Gruppe $\tilde{G}$ zusammen mit einem surjektiven Homomorphismus $\pi : G \longrightarrow \tilde{G}$ derart, dass die folgende universelle Eigenschaft erfüllt ist: Zu jedem Homomorphismus $\varphi : G \longrightarrow A$ von G in eine abelsche Gruppe A gibt es genau einen Homomorphismus $\tilde{\varphi} : \tilde{G} \longrightarrow A$ mit $\varphi = \tilde{\varphi}\pi$. (Hinweis: $\ker\varphi$ enthält notwendig alle Elemente der Form $k = xyx^{-1}y^{-1} (x, y \in G)$, das sind die sogenannten *Kommutatoren*. Konjugierte Elemente gkg^{-1}von Kommutatoren k sind wieder Kommutatoren. Das Inverse eines Kommutators ist wieder ein Kommutator. Damit folgt, dass die Menge aller endlichen Produkte von Kommutatoren ein Normalteiler in G ist. Dieser Normalteiler heißt die *Kommutatoruntergruppe* von G. Die Faktorgruppe dieses Normalteilers ist die gesuchte Gruppe $\tilde{G}$.)

(3.10) Jede Untergruppe vom Index 2 ist ein Normalteiler.

(3.11) Bestimmen Sie alle Normalteiler in D_n.

(3.12) Kann man aus $G_1 \times H \cong G_2 \times H$ auf $G_1 \cong G_2$ schließen?

(3.13) Es sei $N \lhd G$. Kann man schließen, dass G isomorph zu einem semidirektem Produkt $N \times_\Phi (G/N)$ ist? Falls nicht, welche Hindernisse treten auf?

(3.14) Es sei G eine Gruppe mit einem abelschen Normalteiler A. Die Konjugation von G auf A induziert dann eine Linksoperation der Faktorgruppe G/A auf A und somit einen Homomorphismus $\Phi: G/A \longrightarrow \mathrm{Aut}(A)$. Führen sie dies explizit aus für
a) $G = S_3$, $A = A_3$.
b) $G = S_4$, $A = \{(1), (12)(34), (13)(24), (14)(23)\}$.

(3.15) Die Quaternionengruppe Q_8 ist nicht das Produkt einer Untergruppe der Ordnung 2 und einer Untergruppe der Ordnung 4.

(3.16) Beweisen Sie den 'Zweiten Isomorphiesatz': Es sei H eine Untergruppe von G. Es seien M, $N \lhd G$ Normalteiler in G und $M \subset N$ Dann gilt $(G/M)/(M/N) \cong G/N$.

(3.17) Beweisen Sie den 'Dritten Isomorphiesatz': Es sei H eine Untergruppe von G. Weiter sei $N \lhd G$. Dann gilt $HN/N \cong N/N \bigcap H$.

(3.18) Es sei $M = \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ die Menge der Homomorphismen zwischen $\varphi: \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$. Zeigen Sie, dass man M in natürlicher Weise zu einer additiven abelschen Gruppe machen kann. Bestimmen Sie M.

4 Operationen von Gruppen auf sich, die Sylow-Sätze

Inhalt: Satz von Cayley, Konjugation, Zentrum, Klassengleichung, Beispiel: A_5. p-Gruppen, die drei Sylow-Sätze, welche sich mit den den p-Untergruppen einer endlichen Gruppe befassen. Anwendungen: Gruppen der Ordnung pq. Gruppen der Ordnung 12

- **Satz 4.1 (Cayley)**

Jede Gruppe ist isomorph zu einer *Transformationsgruppe*, d.h. zu einer Untergruppe einer symmetrischen Gruppe $S(X)$. Insbesondere ist jede endliche Gruppe isomorph zu einer Untergruppe von S_n für geeignetes n.

Beweis. Es sei G eine Gruppe. Die Multiplikation $G \times G \longrightarrow G$ kann man als eine treue Linksoperation von G auf sich auffassen. Man erhält einen injektiven Gruppenhomorphismus $\Phi: G \longrightarrow S(G)$, $g \mapsto \Phi_g = (a \mapsto ga)$. □

Wichtig für das Studium nicht-abelscher Gruppen ist die Konjugation (vgl (3.10),(3.11),(3.12)). Wir wiederholen einige Definitionen und untersuchen die Konjugation hier etwas genauer.

■ **Definition 4.2**

Es sei G eine Gruppe. Die *Konjugation* definiert eine Linksoperation von G auf sich:

$$G \times G \longrightarrow G,\ (g, a) \mapsto I_g(a) = g\,a\,g^{-1}.$$

(4.2.1) Die Bahnen dieser Operation heißen *Konjugationsklassen* oder Klassen konjugierter Elemente. Mit $C(a)$ (oder genauer $C_G(a)$) wird die Konjugationsklasse von $a \in G$ bezeichnet.

(4.2.2) Die Standgruppen der Konjugationsoperation heißen *Zentralisatoren*. Der Zentralisator von a in G ist die Untergruppe

$$Z(a) = Z_G(a) := \{g \in G \mid a\,g = g\,a\}.$$

(4.2.3) Im allgemeinen ist die Konjugation I keine treue Operation. Der Kern von $I : G \to \mathrm{Aut}(G)$ heißt das *Zentrum* von G und wird mit $Z(G)$ bezeichnet. Es gilt

$$Z(G) = \{g \in G \mid \forall\, a \in G : a\,g = g\,a\} = \bigcap_{a \in G} Z(a)\,.$$

■ **Lemma 4.3**

Es sei G eine Gruppe. Die Elemente des Zentrums von G sind folgendermaßen charakterisiert: $g \in Z(G) \Longleftrightarrow Z(g) = G \Longleftrightarrow C(g) = \{g\}$. □

■ **Lemma 4.4**

Es sei G eine endliche Gruppe.
(4.4.1) Es gilt $|G| = |Z(a)|\,|C(a)|$ für alle $a \in G$.
(4.4.2) Es seien $K_1, \ldots, K_m$ die verschiedenen Klassen konjugierter Elemente in G. Dann gilt die sogenannte *Klassengleichung*

$$|G| = |K_1| + \ldots + |K_m|.$$

Die Anzahl der Einsen in der Klassengleichung ist die Ordnung des Zentrums von G.

Beweis. (4.4.1) folgt aus der Bahnformel.
(4.4.2) gilt, weil $K_1, \ldots, K_m$ die Bahnen der Konjugationsoperation auf G sind. □

■ **Beispiele 4.5**

(4.5.1) Die Klassengleichung von S_4 ist $24 = 1 + 6 + 3 + 8 + 6$, denn (siehe Lemma 3.11): $Z(S_4) = C((1)) = \{e\}$ hat ein Element, $K_1 = C((12))$ hat 6 Elemente, weil es 6 zweielementige Teilmengen von {1, 2, 3, 4} gibt. $K_2 = C((12)(34))$ hat 3 Elemente, $K_3 = C((123))$ hat 8 Elemente, denn es gibt genau 8 Dreierzyklen. $K_4 = C((1234))$ hat 6 Elemente, nämlich

$$(1234),(1243),(1324),(1343),(1423),(1432).$$

Daraus entnimmt man (siehe (3.8.2), dass die einzig möglichen Ordnungen von Normalteileren in S_4 die Zahlen 1,4,12,24 sind, denn nur diese Teiler von 24 lassen sich aus den Konjugationsklassenordnungen 1,6,3,8,6 kombinieren, wobei 1 dazugehören muss. In der Tat sind die Mengen $\{e\} \bigcup K_2$ (siehe Übung (3.1)) und $A_4 = \{e\} \bigcup K_2 \bigcup K_3$ die einzigen echten Normalteiler in S_4.

(4.5.2) Die Klassengleichung von A_5 ist

$$60 = 1 + 15 + 20 + 12 + 12.$$

Die Klassen sind:
$K_1 = \{(1)\}$, $K_2 = C((12)(34))$, $K_3 = C((123))$, $K_4 = C((12345))$, $K_5 = C((21345))$. Man beachte, dass $(12345), (21345)$ zwar in S_5 konjugiert sind, denn es gilt ja (siehe (3.11.2) und Beispiel 3.12) $(21345) = (12)(12345)(12)$. Aber in A_5 sind sie nicht konjugiert! Wie zeigt man das? So! Annahme: $(21345) = \sigma(12345)\sigma^{-1}$ für eine gerade Permutation σ. Dann ist also $(12)(12345)(12) = \sigma(12345)\sigma^{-1}$, und folglich ist $\sigma^{-1}(12)$ ein Element der Standgruppe von (12345) in S_5, d.h. $\sigma^{-1}(12)$ liegt im Zentralisator $Z(\pi)$ von $\pi = (12345)$ in S_5. Diesen Zentralisator kann man aber berechnen. Es ergibt sich $Z(\pi) = \langle\pi\rangle \subset A_5$, wie wir gleich zeigen werden. Insbesondere ist somit $\sigma^{-1}(12)$ gerade und folglich ist auch (12) gerade, ein Widerspruch! Die Annahme ist also falsch.
Wir berechnen $Z(\pi)$: Nach der Formel (4.3.1) ist $Z(\pi)$ von der Ordnung $5 = \frac{120}{24}$, also ist, da natürlich $\pi \in Z(\pi)$ und π die Ordnung 5 hat, $Z(\pi)$ die von π erzeugte zyklische Gruppe. Da $\pi \in A_5$, ist $Z(\pi) \subset A_5$, $Z(\pi)$ also auch die Standgruppe von π unter der Konjugation auf A_5. Damit ist K_4 von der Ordnung $12 = \frac{60}{5}$. Dasselbe gilt für K_5.
Die anderen Zentralisatoren kann man auch berechnen. Für $\pi = (123)$ ist $Z(\pi)$ eine Untergruppe der Ordnung $\frac{120}{20} = 6$. Da $(45), (123) \in Z(\pi)$ ist $Z(\pi) \bigcap A_5 = \langle(123)\rangle$, also von der Ordnung 3 und folglich hat K_3 die Ordnung $\frac{60}{3} = 20$, stimmt also mit der Konjugationsklasse von (123) in S_5 überein. Schließlich kann man auch den Zentralisator $Z(\pi)$ für $\pi = (12)(34)$ berechnen. Er hat die Ordnung $\frac{120}{15} = 8$ und enthält offensichtlich die Elemente $(12), (34), (13)(24)$, welche eine Gruppe der Ordnung 8, also $Z(\pi)$, erzeugen. Damit ist $Z(\pi) \bigcap A_5 = \{(1), (12)(34), (13)(24), (14)(23)\}$ von der Ordnung 4 und folglich hat

K_2die Ordnung $\frac{60}{4} = 15$. Damit ist die Klassengleichung von A_5 vollständig bewiesen.

Aus der Klassengleichung sieht man nun sofort, dass A_5 keine echten Normalteiler besitzt, also eine *einfache* Gruppe ist.
Bemerkung: Diese Gruppe ist isomorph zu der zum Beispiel von Felix Klein ausführlich untersuchten *Ikosaedergruppe*, das ist die Untergruppe von SO(3), die aus allen Drehungen besteht, die ein fest gegebenes Ikosaeder (mit Mittelpunkt 0) invariant lassen. Man schaue in das Algebra-Buch von Artin.

(4.5.3) Die Diedergruppe $\mathcal{D}_8$ hat die Ordnung 16 und wird von zwei Elementen d, s erzeugt mit

$$d^8 = s^2 = e,\ d\,s = s\,d^{-1}.$$

Dass $\mathcal{D}_8$ genau 16 Elemente hat kann man daran sehen, dass die Teilmenge

$$\{e,\ d,\ d^2,\ \ldots,\ d^7,\ s,\ s\,d,\ s\,d^2,\ \ldots,\ s\,d^7\}$$

abgeschlossen gegenüber der Multiplikation ist, denn es gilt ja $d^k(s\,d^m) = s\,d^{m-k}$ und $(s\,d^k)(s\,d^m) = d^{m-k}$.

Konjugieren wir d^k mit $s\,d^m$:
$s\,d^m\,d^k(s\,d^m)^{-1} = s\,d^m\,d^k\,d^{-m}\,s^{-1} = s\,d^k\,s = d^{-k} = d^{8-k}$.
Das liefert die Klassen
$K_1 = \{e\},\ K_2 = \{d^4\},\ K_3 = \{d,\ d^{-1}\},\ K_4 = \{d^2,\ d^{-2}\},\ K_5 = \{d^3,\ d^{-3}\},$

Die Klasse von s ist $K_6 = \{s,\ s\,d^2,\ s\,d^4,\ s\,d^6\}$, denn $d^k\,s\,d^{-k} = s\,d^{-2k}$. Das Element $s\,d$ kommt noch nicht vor. Es hat die Klasse $K_7 = \{s\,d,\ s\,d^3,\ s\,d^5,\ s\,d^7\}$, denn $d^k(s\,d)\,d^{-k} = s\,d^{1-2k}$.
Somit hat $\mathcal{D}_8$ die Klassengleichung

$$16 = 1 + 1 + 2 + 2 + 2 + 4 + 4.$$

Insbesondere ist das Zentrum von $\mathcal{D}_8$ nicht trivial: $Z(\mathcal{D}_8) = \{e,\ d^4\}$. Man sieht unmittelbar, dass $\mathcal{D}_8 / Z(\mathcal{D}_8)$ eine Gruppe der Ordnung 8 ist, die von zwei Elementen $\overline{d}$, $\overline{s}$ erzeugt wird mit den Relationen

$$\overline{d}^4 = \overline{s}^2 = e,\ \overline{d}\,\overline{s} = \overline{s}\,\overline{d}^{-1}.$$

Damit gilt $\mathcal{D}_8 / Z(\mathcal{D}_8) \cong \mathcal{D}_4$.

- **Definition 4.6**

Es sei p eine Primzahl. Eine endliche Gruppe G heißt eine *p-Gruppe*, wenn die Ordnung von G eine Potenz von p ist, $|G| = p^n$ mit $n \geq 1$.

Die Diedergruppe $\mathcal{D}_8$ ist eine 2-Gruppe und wir haben gesehen, dass ihr Zentrum nicht-trivial ist. Das ist ein allgemeines Phänomen bei p-Gruppen: Aus Lemma 4.4

folgt sofort, dass das Zentrums $Z(G)$ einer p-Gruppe G nicht-trivial ist, also ebenfalls eine p-Gruppe ist, denn: Sind $K_1, ..., K_m$ die verschiedenen Konjugationsklassen mit mindestens zwei Elementen, so gilt nach (4.4.1) $|K_j| = p^{n_j}$, $n_j > 0$ und nach (4.4.2) gilt somit $p^n = |G| = |Z(G)| + p^{n_1} + ... + p^{n_m}$ und daher ist p ein Teiler von $|Z(G)|$. Wir haben also

- **Satz 4.7**

Es sei G eine *p-Gruppe.* Dann ist das Zentrum von G nicht-trivial. □

Es sei G eine endliche Gruppe. Dann operiert G in natürlicher Weise von links auf der Potenzmenge $\mathcal{P}(G)$ durch Linksmultiplikation. Ist $A \in \mathcal{P}(G)$, so operiert die Standgruppe $H = G_A = \{g \in G \mid gA = A\}$ selbst durch Linksmultiplikation auf der Menge A. Diese Operation $H \times A \longrightarrow A$ ist frei. Folglich ist $|H|$ ein Teiler von $|A|$. Damit haben wir gezeigt

- **Lemma 4.8**

Es sei G eine endliche Gruppe. Ist $A \in \mathcal{P}(G)$, $H = G_A = \{g \in G \mid gA = A\}$ die Standgruppe von A, so ist $|H|$ ein gemeinsamer Teiler von $|A|$ und $|G|$. Sind $|A|$ und $|G|$ teilerfremd, so ist $H = \{e\}$. □

Neben der Linksmultiplikation spielt auch die Konjugation von G auf Teilmengen von G eine sehr wichtige Rolle. Ist $A \in \mathcal{P}(G)$, $g \in G$, so heißt gAg^{-1} zu A konjugierte Teilmenge von G. G operiert insbesondere durch Konjugation auf der Menge $\mathcal{U}(G)$ aller Untergruppen von G.

- **Lemma und Definition 4.9.**

Es sei G eine Gruppe und H sei eine Untergruppe von G.

(4.9.1) Die Bahn von H unter der Konjugation von G ist die Klasse $\mathcal{C}(H) = \{gHg^{-1} \mid g \in G\}$ der zu H konjugierten Untergruppen. H ist genau dann ein 'Fixpunkt' (d. h. $\mathcal{C}(H) = \{H\}$), wenn H ein Normalteiler in G ist.

(4.9.2) Die Standgruppe von H in G ist der sogenannte *Normalisator* $N_G(H) = \{g \in G \mid gH = Hg\}$ von H in G. H ist Normalteiler in $N_G(H)$.

(4.9.3) Nach der Bahnformel gilt: Der Index $[G : N_G(H)]$ ist die Anzahl $|\mathcal{C}(H)|$ der zu H konjugierten Untergruppen. □

- **Satz 4.10 (Erster Satz von Sylow)**

Es sei G eine endliche Gruppe der Ordnung $n = p^e m$, wobei p eine Primzahl ist, $e \geq 0$ und p kein Teiler von m. Dann gibt es eine Untergruppe der Ordnung p^e.

Beweis. Es sei $\mathcal{X}$ die Menge aller Teilmengen $A \subset G$ mit p^e Elementen. Dann ist $|\mathcal{X}| = \binom{n}{p^e}$. Wir zeigen im nachfolgenden Lemma, dass $\binom{n}{p^e}$ nicht durch p teilbar ist. Damit gibt es auch mindestens eine Bahn $GA = \{gA \mid g \in G\} \subset \mathcal{X}$, deren Ordnung $|GA|$ nicht durch p teilbar ist. Da nun aber nach der Bahnformel $p^e m = |G| = |G_A|\,|GA|$, ist p^e ein Teiler der Ordnung $|G_A|$ der Standgruppe von A. Andererseits ist nach Lemma 4.8 $|G_A|$ ein Teiler von $|A| = p^e$. G_A ist also eine Untergruppe der Ordnung p^e. □

Im Beweis haben wir die folgende einfache Tatsache der elementaren Zahlentheorie benutzt.

- **Lemma 4.11**

Es sei n eine positive natürliche Zahl, p eine Primzahl und e die größte natürliche Zahl, so dass p^e ein Teiler von n ist. Dann gilt: $\binom{n}{p^e}$ ist nicht durch p teilbar.

Beweis. Nach Definition gilt
$\binom{n}{p^e} = \prod_{k=0}^{p^e-1} \frac{n-k}{p^e-k} = \prod_{k=0}^{p^e-1} \frac{mp^e-k}{p^e-k} = m \prod_{k=1}^{p^e-1} \frac{mp^e-k}{p^e-k}$.
Es sei nun $v_p : \mathbb{Q}^\times \longrightarrow \mathbb{Z}$ die p-adische Bewertung, die einer von Null verschiedenen rationalen Zahl $r = \frac{a}{b}$ die Vielfachheit $v_p(r) = v_p(a) - v_p(b)$ zuordnet, wobei $v_p(n) := \max\{e \geq 0 \mid p^e \text{ teilt } n\}$ für $n \in \mathbb{Z}$, $n \neq 0$. Dann gilt $v_p\left(\frac{mp^e-k}{p^e-k}\right) = v_p(k) - v_p(k) = 0$ für $1 \leq k \leq p^e - 1$
(Zeige dies! Hinweis: $v_p(a+b) = v_p(a)$, falls $v_p(a) < v_p(b)$).
Folglich gilt $v_p\binom{n}{p^e} = v_p(m) + \sum_{k=1}^{p^e-1} v_p\left(\frac{mp^e-k}{p^e-k}\right) = v_p(m) = 0$ nach Wahl von e. □

- **Korollar 4.12 (Satz von Cauchy)**

Es sei G eine endliche Gruppe und p ein Primteiler der Ordnung von G. Dann gibt es ein Element der Ordnung p in G.

Beweis. Nach dem ersten Satz von Sylow findet man ein Element x mit $\text{ord}(x) = p^m$ mit $m > 0$. Dann ist $y = x^{p^{m-1}}$ ein Element der Ordnung p. □

- **Definition 4.13**

Eine Untergruppe H einer endlichen Gruppe G heißt *p-Sylowuntergruppe* von G, wenn p ein Primteiler der Ordnung von G ist und wenn $|H| = p^e$, wobei $e = v_p(|G|)$. Folgende Erweiterung ist nützlich, um Fallunterscheidungen zu vermeiden: Ist p eine Primzahl, aber kein Teiler der Ordnung von G, so soll $\{e\}$ als die p-Sylowuntergruppe von G gelten.

- **Satz 4.14 (Zweiter Satz von Sylow)**

Es sei G eine endliche Gruppe, K sei eine Untergruppe der Ordnung k und p ein Primteiler von k. Weiter sei H eine p-Sylowuntergruppe von G. Dann gibt es eine zu H konjugierte Untergruppe H' in G, so dass $H' \cap K$ eine p-Sylowuntergruppe von K ist.

Beweis. Wir betrachten die homogene G-Menge

$$X := G/H$$

der Linksnebenklassen von H. Die Standgruppe von $gH \in X$ ist die zu H konjugierte Untergruppe gHg^{-1}(siehe (2.9.1)). Nach der Indexformel ist $|G| = |H|\,|X|$ und somit ist p kein Teiler von $|X|$. Wir schränken die Operation von G auf X zu einer Operation der Untergruppe K auf X ein. Da X in die K-Bahnen zerlegt wird, und $|X|$ nicht durch p teilbar ist, ist die Länge mindestens einer K-Bahn $Y \subset X$ nicht durch p teilbar. Es sei $y = gH \in Y$. Die Standgruppe von y in K ist offensichtlich $K_y = gHg^{-1} \cap K$ und somit als Untergruppe der p-Gruppe gHg^{-1} selbst eine p-Gruppe. Nach der Bahnformel ist $k = |K| = |K_y|\,|Y|$ und da $|Y|$ nicht durch p teilbar ist, ist K_y nicht nur eine p-Gruppe, sondern sogar eine p-Sylowuntergruppe von K. Der Satz ist bewiesen.
Eine Zusammemfassung der Beweisidee: Zunächst sei erinnert: Die Linksmultiplikation von G auf der Menge X der Linksnebenklassen von H in G ist transitiv und hat als Standgruppen gerade die zu H konjugierten p-Sylowuntergruppen (das sind alle, wie gleich folgt). Die Linksmultiplikation von K auf der Menge X der Linksnebenklassen von H in G besitzt die Standgruppen $gHg^{-1} \cap K$, welche somit als Untergruppen einer p-Gruppe selbst p-Gruppen sind. Nun gibt es einen 'zu p teilerfremdem' K-Orbit. Die Standgruppe eines solchen Orbits ist folglich nach der Bahnformel eine p-Sylowuntergruppe von K. □

- **Korollar 4.15**

Es sei G eine endliche Gruppe der Ordnung n und p sei ein Primteiler von n. Dann gilt:
(4.15.1) Ist K Untergruppe von G und eine p-Gruppe (man sagt eine p-Untergruppe von G), so ist K Untergruppe einer p-Sylowuntergruppe von G.
(4.15.2) Alle p-Sylowuntergruppen von G sind zueinander konjugiert.
(4.15.3) Ist H eine p-Sylowuntergruppe von G, so ist H die einzige p-Sylowuntergruppe des Normalisators $N_G(H)$.

Beweis. Zu (4.15.1): K ist die einzige p-Sylowuntergruppe von K. Für die nach 4.14 existierende p-Sylowgruppe H' gilt dann also $H' \cap K = K$, d.h. $K \subset H'$.
Zu (4.15.2): Sind K, H zwei p-Sylowuntergruppen von G, so gibt es eine zu H konjugierte Gruppe H', so dass $H' \cap K$ eine p-Sylowuntergruppe von K ist, also $H' \cap K = K$ gilt. Da K und H' dieselbe Ordnung haben, folgt $H' = K$.
zu (4.15.3): H ist natürlich auch p-Sylowuntergruppe von $N_G(H)$. Da H auch Normalteiler in $N_G(H)$ ist, ist nach (4.15.2) H die einzige p-Sylowuntergruppe von $N_G(H)$. □

- **Satz 4.16 (Dritter Satz von Sylow)**

Es sei G eine endliche Gruppe der Ordnung $n = p^e m$, $m \not\equiv 0 \bmod p$, $e > 0$, p Primzahl. s sei die Anzahl der p-Sylowuntergruppen von G. Dann gilt:

(4.16.1) $m \equiv 0 \bmod s$.

(4.16.2) $s \equiv 1 \bmod p$.

Beweis. Es sei H eine p-Sylowuntergruppe von G.
Zu (4.16.1): s ist nach (4.15.2) die Anzahl der zu H konjugierten Untergruppen und somit nach (4.9.3) gleich dem Index $[G : N_G(H)]$. Wegen $H \subset N_G(H) \subset G$ gilt $m = [G : H] = [G : N_G(H)][N_G(H) : H] = s\,[N_G(H) : H]$, also ist s ein Teiler von m.
Zu (4.16.2): Es sei $C(H) = \{H_1, ..., H_s\}$ die Klasse der zu H konjugierten Untergruppen, $H_1 = H$. Die Konjugationsoperation von G auf $C(H)$ schränken wir nun zu einer Operation von H auf $C(H)$ ein. Es sei t die Anzahl der 'Fixpunkte' dieser Operation. Da nach der Bahnformel die Länge der H-Bahnen stets Teiler von $|H| = p^e$ sind, sind die Bahnlängen, die nicht zu Fixpunkten gehören, durch p teilbar und somit gilt $s = t$ +Vielfaches von p, also $s \equiv t \bmod p$. Wir müssen nur noch zeigen, dass $t = 1$ gilt, dass also $H_1 = H$ der einzige Fixpunkt von $C(H)$ unter der Konjugation von H ist. Es sei $K \in C(H)$ ein Fixpunkt, d. h. $\forall\, h \in H : h K h^{-1} = K$ und dies besagt, dass H eine Untergruppe des Normalisators $N_G(K)$ ist. Damit sind K, H zwei p-Sylowuntergruppen des Normalisators $N_G(K)$. Nach Korollar (4.15.3) gilt somit $H = K$. □

Es folgen nun einige Anwendungen der Sylowschen Sätze. Zunächst untersuchen wir Gruppen der Ordnung $p\,q$, wobei p, q verschiedene Primzahlen sind. Man erhält in diesem Fall eine vollständige Klassifikation! Danach behandeln wir exemplarisch den Fall der Ordnung $p^2\,q$.

- **Lemma 4.17**

Es seien p, q Primzahlen mit $p < q$. G sei eine Gruppe der Ordnung $p\,q$.

(4.17.1) Dann gibt es genau eine q-Sylowuntergruppe N in G. N ist Normalteiler von G. Es sei H eine p-Sylowuntergruppe von G. Dann ist $G = N\,H$. Wir bezeichnen mit $\Phi : H \longrightarrow \mathrm{Aut}(N)$ die Einschränkung der Konjugation, also $\Phi_h(n) = h\,n\,h^{-1}$ für $h \in H$, $n \in N$. Dann ist $G \cong N \times_\Phi H$.
Weiter gilt:

(4.17.2) N, H sind zyklische Gruppen der Ordnung q bzw. p.

(4.17.3) Ist $\Phi : H \longrightarrow \mathrm{Aut}(N)$ trivial, also $h\,n = n\,h$ für alle $h \in H$, $n \in N$, so ist $G = N\,H \cong N \times H$ und G ist zyklisch.

Ist $q - 1 \not\equiv 0 \bmod p$, so ist Φ trivial. In diesem Fall gibt es also bis auf Isomorphie nur eine Gruppe der Ordnung $p\,q$.

(4.17.4) Es sei jetzt $q - 1 \equiv 0 \bmod p$ und Φ sei nicht-trivial. Dann ist G nicht abelsch und der Isomorphietyp von G kann wie folgt beschrieben werden. Es sei $N = \langle y \rangle$, $y^q = e$, $H = \langle x \rangle$, $x^p = e$. Es gibt ein $k \in \{2,\ ...,\ q-1\}$ mit

$$k^p \equiv 1 \bmod q,$$

so dass

$$\Phi_x(y) = x\,y\,x^{-1} = y^k.$$

(4.17.5) Es gelte weiter $q - 1 \equiv 0 \bmod p$. Dann ist $U = \{k \in \mathbb{F}_q{}^\times \mid k^p = 1\}$ eine zyklische Gruppe der Ordnung p. Verschiedene Zahlen $k_1, k_2 \in \{2,\ ...,\ q-1\}$ mit ${k_1}^p = {k_2}^p \equiv 1 \bmod q$ liefern zueinander isomorphe Gruppen.

Zusammenfassend kann man sagen: Ist $q \not\equiv 1 \bmod p$, so gibt es bis auf Isomorphie nur eine Gruppe der Ordnung $p\,q$, nämlich die zyklische Gruppe $C_{p\,q}$ der Ordnung $p\,q$.
Ist $q \equiv 1 \bmod p$, so gibt es bis auf Isomorphie genau zwei Gruppen der Ordnung $p\,q$, nämlich die zyklische Gruppe $C_{p\,q}$ der Ordnung $p\,q$ und das semidirekte Produkt $C_q \times_\Phi C_p$ mit den Erzeugern x, y und den Relationen $y^q = e$, $x^p = e$, $\Phi_x(y) = x\,y\,x^{-1} = y^k$, wobei $k^p \equiv 1 \bmod q$, $k \not\equiv 1 \bmod q$.

Beweis. Zu (4.17.1): Nach dem dritten Sylowschen Satz gilt für die Anzahl t der q-Sylowuntergruppen

$$p \equiv 0 \bmod t,\ \ t \equiv 1 \bmod q.$$

Da $p < q$ können diese beiden Kongruenzen nur für $t = 1$ gelten. Damit ist (4.17.1) bewiesen.
Zu (4.17.2): Das ist klar, weil p, q Primzahlen sind.
Zu (4.17.3): Ist $q - 1$ nicht durch p teilbar, so muss Φ der triviale Homomorphismus sein, also $\Phi_x(y) = x\,y\,x^{-1} = y$ und somit

$$x\,y = y\,x$$

für alle $x \in H$, $y \in N$ gelten. Nach dem Satz über Produkte (3.15.3) ist G das direkte Produkt von N und H. Ist x Erzeuger von H, y Erzeuger von N, so ist $x\,y$ ein Element der Ordnung $p\,q$, also ein Erzeuger von G.
Zu (4.17.4): Es sei $N = \langle y\rangle$, $y^q = e$, $H = \langle x\rangle$, $x^p = e$, es gibt dann ein $k \in \{1, \ldots, q-1\}$, so dass $\Phi_x(y) = x\,y\,x^{-1} = y^k$. k unterliegt weiteren Begingungen: Da Φ nicht trivial sein soll, ist $k > 1$. Da $x^p = e$, ist $(\Phi_x)^p = \mathrm{id}$, d. h. $y = \Phi_{x^p}(y) = y^{k^p}$ und somit $k^p \equiv 1 \bmod q$.

Zu (4.17.5): $U = \{k \in \mathbb{F}_q{}^\times \mid k^p = 1\}$ ist eine Untergruppe von $\mathbb{F}_q{}^\times$. Da $\mathbb{F}_q$ ein Körper ist und die Polynomgleichung $x^p - 1 = 0$ höchstens p Elemente aus $\mathbb{F}_q$ als Lösungen hat, ist die Ordnung von U kleiner oder gleich p. Nach dem Satz von Cauchy besitzt $\mathbb{F}_q{}^\times$ ein Element k der Ordnung p dieses erzeugt eine Untergruppe der Ordnung p von U. Damit ist $U = \langle k\rangle$ zyklisch von der Ordnung p. Seien nun verschiedene Zahlen $k_1, k_2 \in \{2, \ldots, q-1\}$ mit $k_1{}^p = k_2{}^p \equiv 1 \bmod q$ gegeben. Sie definieren Gruppen G_i mit Erzeugern x_i, y_i mit den Relationen $y_i{}^q = e$, $x_i{}^p = e$, $x_i\,y_i\,x_i{}^{-1} = y_i{}^{k_i}$ ($i = 1, 2$). Wir wollen einen Isomorphismus $\varphi : G_1 \longrightarrow G_2$ konstruieren. φ muss die Sylowgruppen respektieren, also $\langle y_1\rangle$ in $\langle y_2\rangle$ abbilden. Ohne Einschränkung kann man daher $\varphi(y_1) = y_2$ annehmen. Wir versuchen es mit dem Ansatz $\varphi(x_1) = x_2{}^b$. Wendet man φ auf die Gleichung $x_1\,y_1 = y_1{}^{k_1}\,x_1$ an, so erhält man die Beziehung $x_2{}^b\,y_2 = y_2{}^{k_1}\,x_2{}^b$, also $x_2{}^b\,y_2\,x_2{}^{-b} = y_2{}^{k_1}$ und dies ist äquivalent zu $y_2{}^{k_2{}^b} = y_2{}^{k_1}$. Somit muss $k_2{}^b \equiv k_1 \bmod q$ gelten. Nun ist aber $U = \{k \in \mathbb{F}_q{}^\times \mid k^p = 1\}$ eine zyklische Untergruppe der Ordnung p und somit kann man in der Tat einen Exponenten b finden, so dass $k_2{}^b \equiv k_1 \bmod q$. Nach Wahl von k_1, k_2 muss $b \not\equiv 0 \bmod p$ gelten. Wählt man $c \in \mathbb{N}$ mit $b\,c \equiv 1 \bmod p$, so erhält man die Umkehrabbildung von φ durch $x_2 \mapsto x_1{}^c$, $y_2 \mapsto y_1$. □

- **Beispiele 4.18**

(4.18.1) Die Gruppen der Ordnung p, p^2 sind abelsch (→Übung 4.2)). Es sind dies: C_p, C_{p^2}, $C_p \times C_p$.
(4.18.2) Die Gruppen der Ordnung $n = p\,q$, $n < 40$ führen wir in einer Tabelle auf:

6	10	14	15	21	22	26	33	34	35	38
C_6	C_{10}	C_{14}	C_{15}	C_{21}	C_{22}	C_{26}	C_{33}	C_{34}	C_{35}	C_{38}
S_3	D_5	D_7		$C_{7,3}$	D_{11}	D_{13}		D_{17}		D_{19}

(4.18.3) Die nicht-abelsche Gruppe $G = C_{7,3}$ der Ordnung 21 hat die Erzeuger x, y mit den Relationen

$$x^3 = e = y^7,\ x\,y\,x^{-1} = y^2.$$

Beachte, dass $2^3 \equiv 1 \bmod 7$. G hat eine 7-Sylowuntergruppe, nämlich $\langle y\rangle$ und nach dem dritten Sylowschen Satz hat sie sieben 3-Sylowuntergruppen, nämlich die zu $H = \langle x\rangle$ konjugierten Untergruppen von G. Das sind die Gruppen $y^i H y^{-i},\ i = 0, 1, \ldots, 6$.

(4.18.4) Da $11 - 1$ durch 5 teilbar ist, gibt es eine nicht-abelsche Gruppe G der Ordnung 55. Sie hat Erzeuger x, y mit den Relationen $y^{11} = e = x^5$, $x\,y\,x^{-1} = y^k$ mit einer fest gewählten Zahl k, die die Kongruenz $k^5 \equiv 1 \bmod 11$erfüllt. Man kann zum Beispiel $k = 4$ wählen, denn $4^5 = 4 \cdot 16 \cdot 16 \equiv 4 \cdot 5 \cdot 5 = 100 \equiv 1 \bmod 11$.

- **Lemma 4.19**

Es seien p, q Primzahlen, $p < q$. G sei eine Gruppe der Ordnung $n = p^2 q$.

(4.19.1) Ist $q \not\equiv 1 \bmod p$, so ist G abelsch und zwar entweder zyklisch oder isomorph zu $C_p \times C_{pq}$.

(4.19.2) Es sei $p = 2$ und $q = 3$, G also eine Gruppe der Ordnung 12. Es gilt dann:

(4.19.2.1) $G \cong C_{12}$ oder $G \cong C_2 \times C_6$ oder

(4.19.2.2) $G \cong A_4$ oder

(4.19.2.3) $G \cong D_6 \cong S_3 \times C_2 = \langle x, y, z\rangle$
mit $x^2 = y^2 = e$, $x\,y = y\,x$, $z^3 = e$, $x\,z\,x^{-1} = z^2$, $y\,z = z\,y$ oder

(4.19.2.4) $G \cong \langle x, y\rangle$ mit $x^4 = y^3 = e,\ x\,y\,x^{-1} = y^2$.

Beweis. Nach dem dritten Sylowschen Satz gilt für die Anzahl t der q-Sylowuntergruppen $p^2 \equiv 0 \bmod t$, $t \equiv 1 \bmod q$ und für die Anzahl s der p-Sylowuntergruppen gilt $q \equiv 0 \bmod s$, $s \equiv 1 \bmod p$. Da $p < q$ ist $t \neq p$, also $t = 1$ oder $t = p^2$. Für s kommen nur die Werte 1 und q in Betracht. $s = q$ kann allerdings nur gelten, wenn p ein Teiler von $q - 1$ ist.
Zu (4.19.1): $q \not\equiv 1 \bmod p$. Dann ist $s = 1$. Es sei N die Untergruppe der Ordnung p^2. Da $s = 1$, ist N ein Normalteiler und die Konjugation auf G induziert die Operation $\Phi : H \to \mathrm{Aut}(N)$, $h \mapsto (n \mapsto h\,n\,h^{-1})$, einer q-Sylowuntergruppe H von G auf N. Es folgt $G = N \times_\Phi H$. Ist N zyklisch, so hat die Automorphismengruppe von N die Ordnung $\varphi(p^2) = |\{k \mid 1 \le k \le p^2, k \not\equiv 0 \bmod p\}| = p(p-1)$. Da $p < q$ ist q sicher kein Teiler von

$p(p-1)$ und folglich muss der Homomorphismus Φ trivial sein. Es folgt somit, dass G das direkte Produkt von N und H, also zyklisch ist. Ist N nicht zyklisch, so ist $N \cong C_p \times C_p$ und die Automorphismengruppe von N ist isomorph zur Gruppe $GL_2(\mathbb{F}_p)$ und somit von der Ordnung $(p^2-1)p(p-1) = (p+1)p(p-1)^2$. In diesem Fall muss Φ nicht notwendig trivial sein. Ist jedoch q kein Teiler von $p+1$, so muss Φ trivial sein. Da $q > p$, tritt der Fall, dass q ein Teiler von $p+1$ ist nur für $p = 2$, $q = 3$ ein. Damit gilt im Fall $q \neq 3$: $G \cong C_p \times C_p \times C_q \cong C_p \times C_{pq}$.
Wir behandeln jetzt den Fall $p = 2$, $q = 3$:
Zu (4.19.2): Im Fall $s = 1$ ergibt sich dieselbe Schlusskette wie in (4.19.1). Der jedoch hier mögliche Ausnahmefall, dass $\Phi: H \longrightarrow N$ nichttrivial ist, ergibt die Gruppe $G \cong A_4$ mit Erzeugern x, y, z von der Ordnung 2, 2 bzw. 3 und den weiteren Relationen: $xy = yx$, $\Phi_z = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, *d.h.* : $zxz^{-1} = xy$, $zyz^{-1} = x$.
Die alternierende Gruppe A_4 mit den Erzeugern
$x = (12)(34)$, $y = (13)(24)$, $z = (123)$ hat diesen Isomorphietyp, wie man leicht durch Prüfen der Relationen sieht.
Es bleibt der Fall $s = 3$ zu untersuchen:
1. Fall: $t = 1$. Wir erhalten einen Normalteiler N, der zyklisch von der Ordnung 3 ist, nämlich die (wegen $t = 1$) eindeutig bestimmte 3-Sylowuntergruppe von G. Wir wählen eine 2-Sylowuntergruppe H von G. Diese hat die Ordnung 4 und operiert nicht-trivial durch Konjugation auf N. $\Phi: H \longrightarrow \mathrm{Aut}(N)$ ist somit surjektiv.
Fall 1a: H ist zyklisch, $H = \langle x \rangle$, $x^4 = e$. $N = \langle y \rangle$ mit $y^3 = e$. Dann ist $\Phi_x(y) = xy\,x^{-1} = y^2$. G ist die Gruppe mit Erzeugern x, y und den Relationen

$$x^4 = e,\ y^3 = e,\ xy\,x^{-1} = y^2.$$

Fall 1b: $H = \langle x, z \rangle$ mit $x^2 = e = z^2$, $xz = zx$. $N = \langle y \rangle$ mit $y^3 = e$. $\Phi_x(y) = xy\,x^{-1} = y^2$, $\Phi_z(y) = zy\,z^{-1} = y$. Dies ergibt die Isomorphie $G \cong S_3 \times C_2 \cong D_6$. Der Isomorphismus $\varphi: G \longrightarrow S_3 \times C_2$ wird durch $x \mapsto ((12), e)$, $y \mapsto ((123), e)$, $z \mapsto (e, z)$ definiert und der Isomorphismus $\varphi: G \longrightarrow D_6$ durch $x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} y \mapsto \begin{pmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix}$, $z \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.
2. Fall: $t = 4$. In diesem Fall wären die Sylowgruppen keine Normalteiler. Wir wollen zeigen, dass dieser Fall nicht auftritt: Es sei H eine Untergruppe der Ordnung 3 und N eine Untergruppe der Ordnung 4. Da $t = 4$ ist, gibt es 4 zu H konjugierte Untergruppen $H = H_1, H_2, H_3, H_4$. Wie man leicht überlegt, besteht ihre Vereinigung aus $1 + 4 \cdot 2 = 9$ Elementen. Gäbe es nun 3 Sylowgruppen der Ordnung 4, so würde jede dieser Untergruppen die Vereinigung $H_1 \cup H_2 \cup H_3 \cup H_4$ nur in e schneiden. Im Komplement dieser Vereingung liegen aber nur 3 Elemente. Also kann es nur eine Sylowgruppe der Ordnung 4 geben: Wir sind damit im Fall $s = 1$. Der Fall $t = 4$, $s = 3$ ist damit ausgeschlossen. Die Klassifikation der Gruppen der Odnung 12 ist vollständig. Wir haben zwei abelsche Gruppen der Ordnung 12 und drei nicht-abelsche, nämlich A_4, D_6 und schließlich das semidirekte Produkt $C_3 \times_\Phi C_4$

mit $C_3 = \langle y \rangle$, $C_4 = \langle x \rangle$, $\Phi_x(y) = y^2$, also
$(y^i, x^j)\,(y^k, x^m) = (y^i\,\Phi_{x^j}(y^k),\, x^{j+m}) = \left(y^{i+2^j k},\, x^{j+m}\right)$.

■ Übungen 4

(4.1) Zeigen Sie: Eine p-Gruppe, die auf einer endlichen Menge X operiert, deren Ordnung $|X|$ nicht durch p teilbar ist, hat mindestens einen Fixpunkt in X.

(4.2) Es sei p eine Primzahl und sei G eine Gruppe der Ordnung p^2. Zeigen Sie:
a) G ist abelsch und
b) G ist entweder zyklisch oder isomorph zu dem direkten Produkt zweier zyklischer Gruppen der Ordnung p.
Hinweis zu a): Für das Zentrum $Z(G)$ kommen nach Satz 4.7 die Ordnungen p und p^2 in Betracht. Wir müssen nur p als Ordnung von $Z(G)$ ausschließen: Wie sähe denn $Z(x) \supset Z(G)$ für ein $x \in G \setminus Z(G)$aus? Hinweis zu b): Ist G nicht zyklisch, so haben alle Elemente $x \neq e$ die Ordnung p. Wähle $y \in G \setminus \langle x \rangle$ und beweise $G = \langle x \rangle\,\langle y \rangle$.

(4.3) Den ersten Sylowschen Satz kann man auch anderes beweisen. Man benutze die Übung (3.2) und (3.3) und führe den Beweis durch Induktion nach der Ordnung von G (→[4] Reiffen/Scheja/Vetter: Algebra, Seiten 58-60).

(4.4) Bestimmen Sie die Klassen konjugierter Elemente in der nicht abelschen Gruppe der Ordnung 21.

(4.5) Klassifizieren Sie alle Gruppen der Ordnung 8 (Es gibt drei abelsche und zwei nicht-abelsche Gruppen der Ordnung 8: die Diedergruppe D_4 und die Quaternionengruppe Q_8 aus Übung (2.3))

(4.6) Ist G eine nicht-abelsche Gruppe der Ordnung p^3(p Primzahl). Dann ist das Zentrum $Z(G)$ die Kommutatoruntergruppe (→Übung (3.9)) von G.

(4.7) Die alternierende Gruppe A_n ist für $n > 4$ einfach (→[7] Theorem 6.10, [2] § 55, [4] Seiten 65-68). Dazu zeige man folgendes:
a) A_n wird (→Übung (1.9)) von den Dreierzyklen $(123), (124), \ldots, (12n)$ erzeugt ($n \geq 3$).
b) Ist N ein Normalteiler von A_n, der mindestens einen Dreierzyklus enthält, so ist $N = A_n (n \geq 3)$.
c) Ist N ein Normalteiler von A_n, der eine Permutation σ enthält, deren Zykeldarstellung einen Zyklus $\zeta = (i_1\, i_2\, i_3 \ldots i_r)$ der Länge $r > 3$ enthält, so betrachte $\delta = (i_1\, i_2\, i_3)$ und zeige, dass $\pi := \sigma^{-1}\,\delta\,\sigma\,\delta^{-1}$ ein Dreierzyklus ist, der in N liegt.
d) Ist N ein Normalteiler von A_n, der eine Permutation σ enthält, deren Zykeldarstellung zwei Dreierzyklen $(i\,j\,k), (l\,m\,p)$enthält, so betrachte $\delta = (i\,j\,l)$ und zeige dass $\pi := \sigma^{-1}\,\delta\,\sigma\,\delta^{-1}$ein Zyklus der Länge 5 ist.
e) Ist N ein Normalteiler von A_n, der eine Permutation $\sigma = (i\,j\,k)(l\,m)$ enthält, so

enthält N auch einen Dreierzyklus.
f) Ist N ein Normalteiler von A_n, der eine Permutation σ enthält, deren Zykeldarstellung ausschließlich aus Transpositionen besteht, so ist enthält N auch einen Dreierzyklus.

(4.8) Was bedeuten bedeuten die Sylow-Sätze für die endlichen abelschen Gruppen?

(4.9) Es sei G eine Gruppe der Ordnung n und m sei ein Teiler von n. Gibt es stets eine Untergruppe der Ordnung m von G? Hinweis: Untersuche S_4.
Untersuchen Sie dieselbe Frage für endliche abelsche Gruppen.

(4.10) Es seien p, q Primzahlen, $p > q$ und q sei kein Teiler von $p^2 - 1$. Zeigen sie: Jede Gruppe der Ordnung $p^2 q$ ist abelsch. Welche Isomorphietypen kommen vor?

(4.11) Es gibt keine einfachen nicht-abelschen Gruppen der Ordnung $n < 60$.

(4.12) Bestimmen sie alle Sylowuntergruppen von S_4.

(4.13) Es sei H eine Sylowuntergruppe von G. Weiter sei $N \lhd G$. Zeigen Sie:
a) $N \cap H$ ist Sylowuntergruppe von N.
b) HN/N ist eine Sylowuntergruppe von G/N.

(4.14) Welche Ordnungen kommen bei Untergruppen von A_5 vor?

(4.15) Es sei p eine Primzahl. Bestimmen Sie die Ordnung und das Zentrum von $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{F}_p \right\}$.

(4.16) Es sei $G = \mathrm{SL}_2(\mathbb{F}_3)$. Zeigen Sie: a) $N = \left\langle \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \right\} \right\rangle$ ist die einzige 2-Sylowuntergruppe von G. b) Die 2-Sylowuntergruppe von G ist isomorph zur Quaternionengruppe Q_8. c) $G \ncong S_4$. d) Ist $G/Z(G) \cong A_4$?

5 Endlich erzeugte abelsche Gruppen, Elementarteiler

Inhalt: In diesem Abschnitt behandeln wir endlich erzeugte abelsche Gruppen. Es gibt Verbindungen zur linearen Algebra. Das Gaußsche Eliminationsverfahren in Kombination mit dem euklidischen Algorithmus tritt hier als wichtiges Hilfsmittel auf. Es werden allgemein die freien abelschen Gruppen eingeführt, Torsionsgruppen, endlich erzeugte abelsche Gruppen als Faktorgruppen von $\mathbb{Z}^n$, als Kokerne von Matrizen $A \in \mathbb{Z}^{n,m}$. Normalformen dieser Matrizen, Determinantenteiler und Elementarteiler. Der Hauptsatz.

Einleitung

In diesem Abschnitt werden nur abelsche Gruppen behandelt und wie üblich werden abelsche Gruppen additiv geschrieben. Das neutrale Element wird mit 0 bezeichnet, das Inverse von x mit $-x$. Ist M eine solche additiv geschriebene abelsche Gruppe, so gibt es eine Multiplikation mit ganzzahligen Skalaren $\mathbb{Z} \times M \longrightarrow M$, die (n, x) das Element $n\,x$ zuordnet. Es gilt:

$$0\,x = 0,\ (n+1)\,x = n\,x + x \text{ für } n \geq 0,\ \ n\,x = -((-n)\,x) \text{ für } n < 0.$$

Es gelten dieselben Regeln wie bei einem K-Vektorraum, nur, dass die Skalare nur einen kommutativen Ring und keinen Körper bilden, was strukturelle Konsequenzen hat: Man kann nicht mehr aus $n\,x = 0$, $n \neq 0$ auf $x = 0$ schließen, wie ja schon die zyklische Gruppe $M = \mathbb{Z}/m\mathbb{Z}$ ($m \neq 0$) zeigt, in der zum Beispiel $m\,x = 0$ für alle $x \in M$ gilt. Wir nennen additiv geschriebene abelsche Gruppen auch *$\mathbb{Z}$-Moduln*. Untergruppen eines $\mathbb{Z}$-Moduls nennt man auch *Untermoduln*.

Definition 5.1

Es sei M ein $\mathbb{Z}$-Modul.
(5.1.1) Ein Element $x \in M$ heißt *Torsionselement* von M, wenn es ein $n \in \mathbb{Z}$, $n \neq 0$ mit $n\,x = 0$ gibt. Mit M_{tor} wird die Menge aller Torsionselemente von M bezeichnet. Dies ist also die Menge aller Gruppenelemente endlicher Ordnung. M_{tor} ist offensichtlich eine Untergruppe von M.
M heißt *torsionsfrei*, wenn $M_{\text{tor}} = 0$ gilt.
(5.1.2) Ein Tupel $(x_1, \ldots, x_n)$ von Elementen $x_i \in M$ heißt *$\mathbb{Z}$-linear unabhängig*, wenn für $k_1, \ldots, k_n \in \mathbb{Z}$ gilt: Ist $\sum_{i=1}^{n} k_i\,x_i = 0$, so ist $k_1 = 0, \ldots, k_n = 0$.
Eine Familie $(x_i)_{i \in I}$ von Elementen $x_i \in M$ heißt $\mathbb{Z}$-linear unabhängig, wenn jede endliche Teilfamilie $(x_i)_{i \in J}$, $J \subset I$ endlich, es ist.
(5.1.3) Eine Familie $(x_i)_{i \in I}$ von Elementen $x_i \in M$ heißt $\mathbb{Z}$-Basis von M, wenn $(x_i)_{i \in I}$ ein $\mathbb{Z}$-linear unabhängiges Erzeugendensystem von M ist. Wie aus der linearen Algebra bekannt, lässt sich dann jedes Element $x \in M$eindeutig als endliche ganzzahlige Linearkombination von Basiselementen schreiben.
(5.1.4) Gibt es eine (endliche) $\mathbb{Z}$-Basis von M, so heißt M ein (*endlich erzeugter) freier $\mathbb{Z}$-Modul,* auch (endliche erzeugte) *freie abelsche Gruppe*.

■ **Satz 5.2**

(5.2.1) Es sei X eine beliebige Menge. Es sei $F(X)$ die Menge aller Funktionen $f: X \longrightarrow \mathbb{Z}$ mit der Eigenschaft: $\mathrm{supp}(f) := \{x \in X \mid f(x) \neq 0\}$ ist endlich. Die Addition auf $F(X)$ sei die gewöhnliche Addition von Funktionen. Dann gilt: $F(X)$ ist eine freie abelsche Gruppe und die charakteristischen Funktionen χ_x ($\chi_x(x) = 1$, $\chi_x(y) = 0$ für $y \neq x$) der Elemente $x \in X$ bilden eine $\mathbb{Z}$-Basis von $F(X)$. $F(X)$ heißt die *freie abelsche Gruppe über der Menge* X.
(5.2.2) Eine abelsche Gruppe M ist genau dann eine freie abelsche Gruppe, wenn es eine Menge X gibt, so dass $M \cong F(X)$.

Beweis. Zu (5.2.1): Offensichtlich ist $F(X)$ eine abelsche Gruppe (Untergruppe von $(\mathrm{Abb}(X, \mathbb{Z}), +)$). Wir müssen nur zeigen, dass die Famile $(\chi_x)_{x \in X}$ eine $\mathbb{Z}$-Basis von $F(X)$ ist.
a) Ist $f \in F(X)$ und $\mathrm{supp}(f) = \{x_1, \ldots, x_n\}$, so ist $f(x) = \sum_{k=1}^{n} f(x_k)\, \chi_{x_k}(x)$ für alle $x \in X$, also $f = \sum_{k=1}^{n} f(x_k)\, \chi_{x_k}$. Damit ist $(\chi_x)_{x \in X}$ ein Erzeugendensystem von $F(X)$.
b) Sei nun $\sum_{k=1}^{n} a_k\, \chi_{x_k} = 0$. Dann ist $a_i = \sum_{k=1}^{n} a_k\, \chi_{x_k}(a_i) = 0$. Damit ist $(\chi_x)_{x \in X}$ eine $\mathbb{Z}$-linear unabhängige Familie.
Zu (5.2.2) Ist M frei und X eine $\mathbb{Z}$-Basis von M, so ist $\Phi: F(X) \longrightarrow M$ mit $\Phi(\sum_{k=1}^{n} a_k\, \chi_{x_k}) = \sum_{k=1}^{n} a_k\, x_k$ ($a_k \in \mathbb{Z}$, $x_k \in X$) offensichtlich ein Isomorphismus. □

Aus den freien abelschen Gruppen werden durch Bilden von Faktorgruppen alle abelschen Gruppen gewonnen. Jede abelsche Gruppe M ist isomorph zu der Faktorgruppe einer freien abelschen Gruppe. Man kann ja einfach den von der Inklusion $i: X \longrightarrow M$ eines Erzeugendensystems X von M induzierten surjektiven Homomophismus

$$F(X) \longrightarrow M,\ \sum_{k=1}^{n} a_k\, \chi_{x_k} \mapsto \sum_{k=1}^{n} a_k\, x_k\ (a_k \in \mathbb{Z},\ x_k \in X)$$

betrachten. Natürlich gibt es viele Möglichkeiten eine gegebene abelsche Gruppe als Faktorgruppe einer freien abelschen Gruppe zu realisieren. Dies soll jetzt genauer ausgeführt werden. Im folgenden wollen wir nur endlich erzeugte abelsche Gruppen betrachten, also Faktorgruppen von $\mathbb{Z}^n$. Wir werden eine vollständige Klassifikation dieser Gruppen erreichen. Das ist der sogenannte *Hauptsatz über endlich erzeugte abelsche Gruppen.*
Wir beginnen mit endlich erzeugten freien abelschen Gruppen.

■ **Satz 5.3**

Es sei M ein endlich erzeugter freier $\mathbb{Z}$-Modul. Dann gilt:

(5.3.1) $M \cong \mathbb{Z}^n = \mathbb{Z} \times \ldots \times \mathbb{Z}$ (n – mal) für ein $n \geq 0$. Diese Zahl n ist eindeutig durch M bestimmt und heißt der *Rang* $\mathrm{rg}\, M$ von M.

(5.3.2) Alle $\mathbb{Z}$-Basen von M haben dieselbe Länge $n = \operatorname{rg} M$.

Beweis. Zu (5.3.1): Es sei $\mathcal{B} = (x_1, \ldots, x_n)$ ein $\mathbb{Z}$-Basis von M. Wie in der linearen Algebra zeigt man, dass

$$\Phi_{\mathcal{B}} : \mathbb{Z}^n \longrightarrow M,\ (k_1, \ldots, k_n) \mapsto \sum_{i=1}^{n} k_i x_i$$

ein Isomorphismus ist. Ist nun $\varphi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ ein Isomorphismus, so muss $n = m$ gelten, denn φ induziert eine $\mathbb{Q}$-lineare Abildung $\Phi : \mathbb{Q}^n \longrightarrow \mathbb{Q}^m$ mit $\Phi(\frac{1}{a} v) = \frac{1}{a} \varphi(v)$ für $v \in \mathbb{Z}^n$, $a \in \mathbb{Z}$, $a \neq 0$. Da φ injektiv ist, ist auch Φ injektiv und da φ surjektiv ist, ist auch Φ surjektiv. Aus der linearen Algebra folgt daher $n = m$.
Zu (5.3.2): Das folgt sofort aus (5.3.1). □

- **Satz 5.4**

Jeder Untermodul N von $\mathbb{Z}^n$ ist endlich erzeugt und die minimale Anzahl von Erzeugern von N ist $\leq n$.

Beweis durch Induktion nach n. Für $n = 1$ ist das klar, weil alle Untergruppen von $\mathbb{Z}$ von der Form $m\mathbb{Z}$ sind.
Induktionsschluss $n - 1 \to n$: Wir betrachten $N \subset \mathbb{Z}^n$ und eine Projektion $\pi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^{n-1}$, $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{n-1})$. Es gilt $\ker \pi \cong \mathbb{Z}$. Das Bild $\pi(N)$ wird nach Induktionsvoraussetzung von $r \leq n - 1$ Elementen erzeugt. Wir wählen r Urbilder $z_1, \ldots, z_r$ dieser Erzeuger in N. Diese erzeugen einen Untermodul $U \subset N$. Wir wählen weiter einen Erzeuger z_{r+1} von $N \bigcap \ker \pi$. Wir zeigen nun, dass $(z_1, \ldots, z_{r+1})$ ein Erzeugendensystem von N ist. Sei dazu $z \in N$, $\pi(z) = \sum_{i=1}^{r} a_i \pi(z_i)$. Setze $w := \sum_{i=1}^{r} a_i z_i$. Dann gilt $\pi(z - w) = 0$, also $z - w \in N \bigcap \ker \pi$ und somit $z - w = a_{r+1} z_{r+1}$, also $z = \sum_{i=1}^{r+1} a_i z_i$. □

- **Satz 5.5**

(5.5.1) Zu jedem endlich erzeugten $\mathbb{Z}$-Modul M gibt es eine ganzzahlige $n \times m$-Matrix $A = (a_{i,j}) \in \mathbb{Z}^{n,m}$und einen surjektiven Homomorphismus $\pi : \mathbb{Z}^n \longrightarrow M$, so dass

$$\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \xrightarrow{\pi} M \longrightarrow 0$$

exakt ist. Dabei bedeutet A die $\mathbb{Z}$-lineare Abbildung $w \mapsto z = Aw$, d. h. $z_i = \sum_{j=1}^{m} a_{ij} w_j$. wobei z, w Spalten mit den Einträgen z_i bzw. w_j sind. Die Exaktheit bedeutet, dass $\operatorname{im} A = \ker \pi$, $\operatorname{im} \pi = M$ und π surjektiv ist. Nach dem Homomorphiesatz gilt dann $M \cong \mathbb{Z}^n / \operatorname{im} A$. Die Faktorgruppe $\mathbb{Z}^n / \operatorname{im} A$ heißt auch der *Kokern* von A und wird mit $\operatorname{coker} A$ bezeichnet.

Man sagt dann, dass M durch die Matrix A *präsentiert* sei. Die exakte Sequenz $\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \xrightarrow{\pi} M \longrightarrow 0$ heißt *Präsentation* von M. A heißt eine M präsentierende Matrix.

(5.5.2) Ist $\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \xrightarrow{\pi} M \longrightarrow 0$ eine Präsentation von M und ist $B = S A T$ mit $T \in \mathrm{GL}_m(\mathbb{Z})$, $S \in \mathrm{GL}_n(\mathbb{Z})$, so ist auch $\mathbb{Z}^m \xrightarrow{B} \mathbb{Z}^n \xrightarrow{\pi S^{-1}} M \longrightarrow 0$ eine Präsentation von M.

Beweis. Zu (5.5.1): Es sei $(x_1, \ldots, x_n)$ ein Erzeugendensystem von M. Dann ist $\pi : \mathbb{Z}^n \longrightarrow M$ mit $\pi \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = z_1 x_1 + \ldots + z_n x_n$ ein surjektiver Homomorphismus. $N = \ker \pi$ ist eine Untergruppe von $\mathbb{Z}^n$ und somit nach 5.4 endlich erzeugt. Seien die Spaltenvektoren $a^1, \ldots, a^m \in \mathbb{Z}^n$ Erzeuger von $\ker \pi$. Dann ist $A := (a^1, \ldots, a^m) \in \mathbb{Z}^{n,m}$ mit $\mathrm{im}\, A = \ker \pi$. □

Zu (5.5.2): Es gelte $B = S A T$ mit $T \in \mathrm{GL}_m(\mathbb{Z})$, $S \in \mathrm{GL}_n(\mathbb{Z})$. Wir zeigen, dass auch $\mathbb{Z}^m \xrightarrow{B} \mathbb{Z}^n \xrightarrow{\pi S^{-1}} M \longrightarrow 0$ eine Präsentation von M ist.
Beweis. Aus $\pi S^{-1} B = \pi S^{-1} S A T = \pi A T = 0\, T = 0$ folgt $\mathrm{im}\, B \subset \ker \pi S^{-1}$. Ist umgekehrt $z' \in \ker \pi S^{-1}$, also $\pi S^{-1} z' = 0$, so setze $z = S^{-1} z'$, Dann ist also $\pi z = 0$ und somit $z = A w$ mit $w \in \mathbb{Z}^m$. Es sei $w = T w'$. Dann folgt $B w' = S A T w' = S A w = S z = z'$, also $z' \in \mathrm{im}\, B$ und somit ist $\ker \pi S^{-1} \subset \mathrm{im}\, B$. □

Das Ziel ist es nun, eine Normalform für M zu finden. Dies soll durch einen Rechenalgorithmus geschehen, der es praktisch erlaubt, die Normalform, die sogenannte *Elementarteilermatrix,* einer ganzzahligen Matrix zu bestimmen. Dazu startet man mit irgendeiner Präsentation $\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \xrightarrow{\pi} M \longrightarrow 0$ von M und führt elementare Spalten- und Zeilenumformungen an der Matrix A durch, die Rechts- bzw Linksmultiplikation mit einer Elementarmatrix in $\mathrm{GL}(\mathbb{Z})$ bedeuten, bis man eine Normalform $B = S A T$ mit $T \in \mathrm{GL}_m(\mathbb{Z})$, $S \in \mathrm{GL}_n(\mathbb{Z})$ erhält. B wird aus einer quadratischen Diagonalmatrix und Nullmatrizen bestehen. Nach (5.5.2) repräsentiert B ebenfalls den Modul M. Dieses Ergebnis, natürlich noch genauer zu formulieren, ist der sogenannte *Elementarteilersatz*.

Bevor wir den Elementarteilersatz beweisen können, müssen wir zunächst an den *euklidischen Algorithmus* zur Bestimmung des größten gemeinsamen Teilers zweier ganzer Zahlen erinnern. Sind a, b zwei ganze Zahlen, die nicht beide Null sind, so gibt es eine eindeutig bestimmte positive ganze Zahl d, so dass $\langle a, b\rangle = \langle d\rangle$. d heißt der *größte gemeinsame Teiler* (ggT) von a und b.

Zur Bestimmung des größten gemeinsamen Teilers verwendet man den euklidischen Algorithmus, der auf den folgenden offensichtlichen Regeln beruht:
$\langle a, b\rangle = \langle a, b - q\, a\rangle$, $\langle a, b\rangle = \langle b, a\rangle$, $\langle a, 0\rangle = \langle a\rangle$.

Ein Beispiel:
$\langle 12, 15\rangle = \langle 12, 15 - 12\rangle = \langle 12, 3\rangle = \langle 3, 12\rangle = \langle 3, 12 - 4 \cdot 3\rangle = \langle 3, 0\rangle = \langle 3\rangle$.

Wir bezeichnen mit Mod[a, b] den Rest r mit $0 \le r = a - q\,b < b$. Damit haben wir dann folgendes Programm zur Bestimmung des größten gemeinsamem Teiler zweier Zahlen:
Input: (a, b) mit $a > 0$.
Initialisierung: $(x, y) = (a, b)$
Programm(While-Schleife): Solange $x > 0$ setze $(x, y) = (\text{Mod}[y, x], x)$.
Output: $d = y$.
Da bei jedem Schritt der erste Eintrag des Paares (x, y) kleiner wird, kommt das Programm nach endlich vielen Schritten zum Stillstand, d.h. zum Wert $x = 0$.
Man kann natürlich induktiv den ggT von n Zahlen a_1, ..., a_n berechnen, denn, ist d der ggT von a_1 und a_2, so ist $\langle a_1, a_2, \ldots, a_n\rangle = \langle d, a_3, \ldots, a_n\rangle$.

Wir kommen nun zum Elementarteilersatz. Wir beginnen mit einigen Beispielen:

- **Beispiele 5.6**

(5.6.1) Mit der aus der linearen Algebra bekannten Methode wird die Matrix $A = \begin{pmatrix} 6 & 9 \\ 10 & 13 \end{pmatrix}$ umgeformt. Allerdings dürfen nur Transformationen in $GL_2(\mathbb{Z})$ benutzt werden.
Das macht das Verfahren komplizierter als das gewöhnliche Gausssche Eliminationsverfahren. Ziel ist es, eine Diagonalmatrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ zu erreichen, so dass a ein Teiler von b ist. Es soll also nicht nur eine Diagonalmatrix hergestellt werden! Es wird sich ergeben, dass
$a = \text{ggT}(6, 9, 10, 13) = 1$, $b = |\det(A)| = 12$.

Zeilenoperationen	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}6&9\\10&13\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	Spaltenoperationen
		$\begin{pmatrix}6&3\\10&3\end{pmatrix}$	$\begin{pmatrix}1&-1\\0&1\end{pmatrix}$	$S_{2,1}(-1)$
		$\begin{pmatrix}3&6\\3&10\end{pmatrix}$	$\begin{pmatrix}-1&1\\1&0\end{pmatrix}$	$ST_{1,2}$
		$\begin{pmatrix}3&0\\3&4\end{pmatrix}$	$\begin{pmatrix}-1&3\\1&-2\end{pmatrix}$	$S_{2,1}(-2)$
$Z_{2,1}(-1)$	$\begin{pmatrix}1&0\\-1&1\end{pmatrix}$	$\begin{pmatrix}3&0\\0&4\end{pmatrix}$		
$Z_{1,2}(1)$	$\begin{pmatrix}0&1\\-1&1\end{pmatrix}$	$\begin{pmatrix}3&4\\0&4\end{pmatrix}$		
		$\begin{pmatrix}3&1\\0&4\end{pmatrix}$	$\begin{pmatrix}-1&4\\1&-3\end{pmatrix}$	$S_{2,1}(-1)$
		$\begin{pmatrix}1&3\\4&0\end{pmatrix}$	$\begin{pmatrix}4&-1\\-3&1\end{pmatrix}$	$ST_{1,2}$
		$\begin{pmatrix}1&0\\4&-12\end{pmatrix}$	$\begin{pmatrix}4&-13\\-3&10\end{pmatrix}$	$S_{2,1}(-3)$
$Z_{2,1}(-4)$	$\begin{pmatrix}0&1\\-1&-3\end{pmatrix}$	$\begin{pmatrix}1&0\\0&-12\end{pmatrix}$		
		$\begin{pmatrix}1&0\\0&12\end{pmatrix}$	$\begin{pmatrix}4&13\\-3&-10\end{pmatrix}$	$S_2(-1)$

Für $A=\begin{pmatrix}6&9\\10&13\end{pmatrix}$ haben wir $SAT=\begin{pmatrix}1&0\\0&12\end{pmatrix}$ erhalten, wobei
$S=\begin{pmatrix}0&1\\-1&-3\end{pmatrix}$, $T=\begin{pmatrix}4&13\\-3&-10\end{pmatrix}\in \mathrm{GL}_2(\mathbb{Z})$.
Damit ist die Faktorgruppe $\mathbb{Z}^2\Big/\left\langle\begin{pmatrix}6\\10\end{pmatrix},\begin{pmatrix}9\\13\end{pmatrix}\right\rangle$ von $\mathbb{Z}^2$ nach der von den Spalten $\begin{pmatrix}6\\10\end{pmatrix},\begin{pmatrix}9\\13\end{pmatrix}\in\mathbb{Z}^2$ erzeugten Untergruppe isomorph zu $\mathbb{Z}^2\Big/\left\langle\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\12\end{pmatrix}\right\rangle$ und diese Gruppe ist isomorph zur zyklischen Gruppe $\mathbb{Z}/12\mathbb{Z}$.

(5.6.2) Die Matrix $A=\begin{pmatrix}3&9\\6&18\\30&90\end{pmatrix}$ kann mit demselben Verfahren auf die Matrix $\begin{pmatrix}3&0\\0&0\\0&0\end{pmatrix}$ transformiert werden und somit ist $\operatorname{coker} A\cong\mathbb{Z}^2\times(\mathbb{Z}/3\mathbb{Z})$.

$$\begin{array}{l|l|l|l} \text{Zeilenoperationen} & \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} & \begin{pmatrix}3&9\\6&18\\30&90\end{pmatrix} & \begin{pmatrix}1&0\\0&1\end{pmatrix} \text{ Spaltenoperationen} \\ Z_{2,1}(-2),\, Z_{3,1}(-10) & \begin{pmatrix}1&0&0\\-2&1&0\\-10&0&1\end{pmatrix} & \begin{pmatrix}3&9\\0&0\\0&0\end{pmatrix} & \\ & & \begin{pmatrix}3&0\\0&0\\0&0\end{pmatrix} & \begin{pmatrix}1&-3\\0&1\end{pmatrix} \qquad S_{2,1}(-3) \end{array}$$

(5.6.3) $A = \begin{pmatrix}2&4&5\\1&0&3\\3&30&1\end{pmatrix}$ hat die Normalform $\begin{pmatrix}1&0&0\\0&1&0\\0&0&2\end{pmatrix}$, also als Kokern die zyklische Gruppe $\mathbb{Z}/2\mathbb{Z}$. Wir geben die Unformungen an:

$$\begin{pmatrix}2&4&5\\1&0&3\\3&30&1\end{pmatrix} \to \begin{pmatrix}1&0&3\\2&4&5\\3&30&1\end{pmatrix} \to \begin{pmatrix}1&0&3\\0&4&-1\\0&30&-8\end{pmatrix} \to \begin{pmatrix}1&0&0\\0&4&-1\\0&30&-8\end{pmatrix},$$

$$\begin{pmatrix}4&-1\\30&-8\end{pmatrix} \to \begin{pmatrix}1&4\\8&30\end{pmatrix} \to \begin{pmatrix}1&4\\0&-2\end{pmatrix} \to \begin{pmatrix}1&0\\0&2\end{pmatrix}$$

(5.6.4) Etwas komplizierter ist das folgende Beispiel

$$A = \begin{pmatrix}2&4&6\\2&3&5\\8&7&6\end{pmatrix} \to \begin{pmatrix}2&4&6\\0&-1&-1\\0&-9&-18\end{pmatrix} \to \begin{pmatrix}2&0&0\\0&-1&-1\\0&-9&-18\end{pmatrix} \to$$

$$\begin{pmatrix}2&0&0\\0&1&1\\0&9&18\end{pmatrix} \to \begin{pmatrix}0&1&1\\2&0&0\\0&9&18\end{pmatrix} \to \begin{pmatrix}1&0&1\\0&2&0\\9&0&18\end{pmatrix} \to \begin{pmatrix}1&0&0\\0&2&0\\9&0&9\end{pmatrix} \to \begin{pmatrix}1&0&0\\0&2&0\\0&0&9\end{pmatrix}$$

weiter $\begin{pmatrix}2&0\\0&9\end{pmatrix} \to \begin{pmatrix}2&2\\0&9\end{pmatrix} \to \begin{pmatrix}2&2\\-8&1\end{pmatrix} \to \begin{pmatrix}-8&1\\2&2\end{pmatrix} \to \begin{pmatrix}1&-8\\2&2\end{pmatrix} \to \begin{pmatrix}1&0\\2&18\end{pmatrix} \to \begin{pmatrix}1&0\\0&18\end{pmatrix}.$

Die Normalform ist also $\begin{pmatrix}1&0&0\\0&1&0\\0&0&18\end{pmatrix}$. Es folgt $\operatorname{coker} A \cong \mathbb{Z}/18\mathbb{Z}$.

(5.6.5) Wie geht man bei der folgenden Matrix vor? $A = \begin{pmatrix} 2022 & 644 & -3954 \\ 2790 & 1090 & -4860 \\ -24338 & -6466 & 51396 \end{pmatrix}$.

Die Normalform von A ist $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 60 \end{pmatrix}$. Man sollte einen allgemeinen Algorithmus entwickeln! Das führt zum Elemenarteilersatz für Matrizen.

- **Satz 5.7 (Elementarteilersatz für Matrizen)**

Es sei $A = (a_{i,j}) \in \mathbb{Z}^{n,m}$ eine Matrix vom Rang r. Dann gibt es eindeutig bestimmte positive ganze Zahlen $\gamma_1, \gamma_2, \ldots, \gamma_r$ mit der Teilbarkeitsrelation γ_i teilt γ_{i+1} für alle $i = 1, \ldots, r-1$, so dass für geeignete unimodulare Matrizen $T \in \mathrm{GL}_m(\mathbb{Z})$, $S \in \mathrm{GL}_n(\mathbb{Z})$ gilt:

$$SAT = \begin{pmatrix} \boxed{\begin{matrix} \gamma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \gamma_r \end{matrix}} & & 0 \\ & 0 & \\ 0 & & 0 \end{pmatrix} \qquad \textbf{(7)}$$

Es gilt: $\delta_k := \gamma_1 \ldots \gamma_k$ ist der sogenannte k-te *Determinantenteiler* von A, d.h. der größte gemeinsame Teiler aller k-reihigen Unterdeterminanten von A.
Die Zahlen $\gamma_1, \ldots, \gamma_r$ heißen die *Elementarteiler* von A.

Beweis. I. **Existenz**: Der Beweis wird durch Beschreibung eines Algorithmus erbracht. Dieser Algorithmus ist eine Kombination des euklidischen Algorithmus und des Gaußschen Eliminationsverfahrens: Wir geben ihn als ein Programm in 'Pseudocode' an:
Input: Eine Matrix $A \in \mathbb{Z}^{n,m}$.
Initialisierung: Man startet mit $M := A$ und der leeren Liste $L = \emptyset$. Die Einträge in M seien mit x_{ij} bezeichnet.
Output: Die Liste $L = \{\gamma_1, \ldots, \gamma_r\}$ der Elementarteiler.
Programm: While-Schleife: Solange $M \neq 0$ tue man folgendes:

1. Man wähle ein Paar (i, j), so dass $x_{ij} \neq 0$ (etwa mit $|x_{ij}| = \min\{|x_{kl}| \mid x_{kl} \neq 0\}$). Jetzt vertausche man die erste und die i-te Zeile und dann die erste und die j-te Spalte und multipliziere die neue erste Zeile mit dem Vorzeichen von x_{11}. Das Ergebnis setze man als neues M. Dann hat M an die Stelle $(1, 1)$ den positiven Wert x_{11}.

2. Auf die erste Zeile der Matrix M wende man nun den euklidischen Algorithmus an. Das geht so: Man teile x_{12} mit Rest durch x_{11}: $x_{12} = q\,x_{11} + r$. Jetzt subtrahiere man das q-fache der ersten Spalte von der zweiten Spalte. An der Stelle $(1, 2)$ steht jetzt $x_{12} = r$. Ist $x_{12} > 0$ so vertausche man erste und zweite Spalte. Das Ergebnis nenne man wieder M. An der Stelle $(1, 1)$ steht jetzt $x_{11} = r$, welches

kleiner ist als das alte x_{11} ist. Daher hat die Matrix M nach endlich vielen Schritten an der Stelle $(1, 1)$ den ggT von den ursprünglichen Werten x_{11} und x_{12} und an der Stelle $(1, 2)$ den Wert 0. Genauso verfahre man mit jetzt mit x_{11} und x_{13} usw. Man erhält schließlich eine Matrix der Form

$M = \begin{pmatrix} d & 0 \\ * & M' \end{pmatrix}$. Bei diesen Spaltenoperationen hat sich der ggT der Elemente in der ersten Zeile nicht geändert. d ist also dieser ggT. Auch der ggT aller Matrixelemente hat sich nicht geändert.

3. Ist d Teiler aller Einträge der ersten Spalte, so kann man durch Zeilenoperationen M auf die Form $\begin{pmatrix} d & 0 \\ 0 & M' \end{pmatrix}$ bringen. Ist das nicht der Fall, so kann man mit entsprechenden Zeilenoperationen die Matrix auf die Form $M = \begin{pmatrix} d & * \\ 0 & M' \end{pmatrix}$ bringen, wobei jetzt d der ggT aller Einträge in der ersten Zeile ist und außerdem kleiner als das alte d ist. Da man eventuell wieder Einträge in der ersten Zeile produziert hat, gehe man zurück zum 2. Schritt. Jedes Mal wenn man den 2. und 3. Schritt durchlaufen ist, hat sich d verkleinert. Da $d > 0$ ist, hat man nach endlich vielen Durchläufen dieser beiden Schritte M in die Form $M = \begin{pmatrix} d & 0 \\ 0 & M' \end{pmatrix}$ transformiert.

4. Falls d alle Einträge der Matrix M' teilt, d also der ggT aller Koeffizienten von M ist, so ist d ein Elementarteiler und man füge d zur Liste L hinzu, d. h. man setze $L := L \bigcup \{d\}$ und mache nun weiter mit der Untermatrix $M := M'$. (Zurück zum Anfang der While-Schleife! Ist M' leer, so soll auch $M = 0$ gesetzt werden, so dass die While-Schleife also in diesem Fall stoppt.)
Ist noch ein Eintrag in M' vorhanden, der nicht von d geteilt wird, so kann man ein Paar (i, j) wählen, so dass $x_{ij} = q\,d + r$ mit $0 < r < d$. Dann addiere man die i-te Zeile zur ersten Zeile und subtrahiere dann das q-fache der ersten von der j-ten Spalte. Das ist die Operation $\begin{pmatrix} d & 0 \\ 0 & x_{ij} \end{pmatrix} \to \begin{pmatrix} d & x_{ij} \\ 0 & x_{ij} \end{pmatrix} \to \begin{pmatrix} d & r \\ 0 & x_{ij} \end{pmatrix}$. Durch Spaltenvertauschung bringe man r von der Position $(1, j)$ an die Stelle $(1, 1)$. M hat jetzt r an der Stelle $(1, 1)$, welches kleiner als d ist. Es sind nun eventuell wieder weitere von Null verschiedene Elemente in der ersten Zeile und Spalte! (Zurück zum Anfang der While-Schleife!)

Nach endlich vielen Durchläufen der While-Schleife hat die Matrix M den Wert Null (M = Nullmatrix $\in \mathbb{Z}^{n-r,m-r}$) und die Liste L ist aufgefüllt zu $L = \{\gamma_1, \ldots, \gamma_r\}$. Man hat A in eine Matrix

$$SAT = \begin{pmatrix} \boxed{\begin{matrix} \gamma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \gamma_s \end{matrix}} & & 0 \\ & & \\ 0 & & 0 \end{pmatrix}$$

transformiert. Der Algorithmus zeigt auch, dass gilt: γ_i teilt γ_{i+1} für alle $i = 1, \ldots, r-1$. Die unimodularen Matrizen S, T haben wir hier außer Acht gelassen. Man könnte sie natürlich mit berechnen.

II. **Eindeutigkeit**: Offensichtlich ist $\delta_k = \gamma_1 \ldots \gamma_k$ der ggT aller k-reihigen Unterdeterminanten von $SAT = \begin{pmatrix} \boxed{\begin{matrix} \gamma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \gamma_r \end{matrix}} & & 0 \\ & & \\ 0 & & 0 \end{pmatrix}$ und somit auch von A, wie das nachfolgende Lemma (5.9.4) zeigt. Die δ_k sind also durch A festgelegt und damit auch $\gamma_k = \frac{\delta_k}{\delta_{k-1}}$. □

- **Lemma 5.9 (Determinantenteiler)**

Es sei $A = (a_{ij}) \in \mathbb{Z}^{n,m}$. Für $k = 1, \ldots, \min(n, m)$ sei $\delta_k(A)$ der ggT aller k-reihigen Unterdeterminanten von A. Weiter sei (man denke sich die Matrix A nach links und unten durch Nullen fortgesetzt) $\delta_k(A) = 0$ für $k > \min(n, m)$ und $\delta_k(A) := 1$ für $k \le 0$. Dann gilt:

(5.9.1) $\delta_k(A)$ ist ein Teiler von $\delta_{k+1}(A)$ für alle $k \in \mathbb{Z}$.

(5.9.2) Ist $B \in \mathbb{Z}^{p,n}$, so gilt $\delta_k(BA)$ ist ein Vielfaches von $\delta_k(B)\,\delta_k(A)$ für alle k.

(5.9.3) Ist $A \in \mathrm{GL}_n(\mathbb{Z})$, so ist $\delta_k(A) = 1$ für alle $k \le n$.

(5.9.4) Ist $B = SAT$ mit unimodularen Matrizen S, T, so gilt $\delta_k(A) = \delta_k(B)$ für alle k.

Beweis. Zu (5.9.1): Dies gilt nach dem Laplaceschen Entwicklungssatz, nach dem jede $(k+1)$-reihige Unterdeterminante eine Linearkombination von k-reihigen Unterdeterminanten ist ($1 \le k < \min(n, m)$).
Zu (5.9.2): Ohne Einschränkung sei $p = m = k$. Wir berechnen $\det(BA)$. Es sei A_i die k-reihige Untermatrix von A aus den Zeilen $i_1, \ldots, i_k$ für $i = (i_1, \ldots, i_k)$, $1 \le i_1 < \ldots < i_k \le n$. Analog sei B^i die k-reihige Untermatrix von B aus den Spalten $i_1, \ldots, i_k$. Dann kann man (mit einer kleinen Indexschlacht, Übung!) direkt verifizieren, dass $\det(BA) = \sum_i \det(B^i)\det(A_i)$ gilt und folglich $\det(BA)$ ein Vielfaches von $\delta_k(B)\,\delta_k(A)$ ist.
Zu (5.9.3): Es sei E die Einheitsmatrix. Dann ist nach (5.9.2) $1 = \delta_k(E)$ ein Vielfaches von $\delta_k(A^{-1})\,\delta_k(A)$, also ist $\delta_k(A) = 1$, weil ja beide $\delta_k(A^{-1})$ und $\delta_k(A)$ in $\mathbb{N}$

liegen.
Zu (5.9.4): Das folgt jetzt aus (5.9.3). □

- **Satz 5.10 (Hauptsatz über endlich erzeugte abelsche Gruppen)**

Es sei M ein endlich erzeugter $\mathbb{Z}$-Modul. Dann gibt es eindeutig bestimmte Zahlen $r, s \geq 0$ und ein s-Tupel ganzer Zahlen $(\gamma_1, \ldots, \gamma_s)$, so dass $\gamma_i \geq 2$ und γ_i Teiler von γ_{i+1} ist für alle $i = 1, \ldots, s-1$ und so dass

$$M \cong \mathbb{Z}^r \times (\mathbb{Z}/\gamma_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/\gamma_s\mathbb{Z}).$$

Die Zahl r heißt der *Rang* von M und wird mit $\operatorname{rg}(M)$ bezeichnet. Die Zahlen $\gamma_1, \ldots, \gamma_s$ heißen die *Elementarteiler* von M.

Beweis. 1. **Existenz**: Die Existenz folgt leicht aus dem Elementarteilersatz: Es sei A eine Präsentationsmatrix von M, $\operatorname{rg} A = t$. Nach dem Elementarteilersatz kann man A transformieren zu $\begin{pmatrix} \boxed{\begin{matrix} \gamma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \gamma_t \end{matrix}} & 0 \\ 0 & 0 \end{pmatrix}$. Zur Kokernberechnung kann man sowohl die vollständigen Nullspalten weglassen als auch die Zeilen mit $\gamma_i = 1$, denn $\mathbb{Z}/1\mathbb{Z} = 0$. Somit erhält man M als Kokern einer Matrix $\begin{pmatrix} \boxed{\begin{matrix} \gamma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \gamma_s \end{matrix}} \\ 0 \\ \vdots \\ 0 \end{pmatrix} : \mathbb{Z}^s \longrightarrow \mathbb{Z}^{s+r}$ mit $\gamma_1 \geq 2$, $\gamma_i \mid \gamma_{i+1}$ für $i = 1, \ldots, s-1$. Dies ist die gesuchte Darstellung.
2. **Eindeutigkeit**: Offensichtlich reicht es nach 5.7 aus, zu beweisen, dass für zwei Präsentationen $\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \xrightarrow{\pi} M \longrightarrow 0$, $\mathbb{Z}^p \xrightarrow{B} \mathbb{Z}^q \xrightarrow{\sigma} M \longrightarrow 0$ von M die von 1 verschiedenen Determinantenteiler übereinstimmen, genauer

$$\delta_{n-k}(A) = \delta_{q-k}(B) \text{ für alle } k \in \mathbb{Z}.$$

Beweis. Die Schwierigkeit besteht darin, dass $n \neq q$ gelten kann. Wir gehen in mehreren Schritten vor:
1. Schritt: Es sei zunächst $q = n$ und $\pi = \sigma$. Es gilt dann $\operatorname{im} A = \operatorname{im} B$.
Man findet dann eine Matrix $C \in \mathbb{Z}^{p,m}$, so dass $A = BC$. Dazu wähle man $c_j \in \mathbb{Z}^p$ mit $Bc_j = Ae_j$. Dabei ist e_j der j-te Einheitsspaltenvektor in $\mathbb{Z}^m$. Nach (5.9.2) ist dann (beachte $n = q$) $\delta_{n-k}(A)$ ein Vielfaches von $\delta_{q-k}(B)$ für alle $k \in \mathbb{Z}$. Man findet natürlich genauso eine Matrix $D \in \mathbb{Z}^{m,p}$, so dass $B = AD$ und somit gilt auch $\delta_{n-k}(B)$ ein Vielfaches von $\delta_{q-k}(A)$ für alle $k \in \mathbb{Z}$. In diesem Fall ist also die Behauptung bewiesen.

2. Schritt: Es sei $\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \xrightarrow{\pi} M \longrightarrow 0$ gegeben und $x \in M$ beliebig aber fest. Dann ist $\sigma : \mathbb{Z}^{n+1} \longrightarrow M$ mit $\sigma\begin{pmatrix} k \\ t \end{pmatrix} = \pi(k) + t\,x$, $(k \in \mathbb{Z}^n, t \in \mathbb{Z})$ ebenfalls surjektiv. Wähle $r \in \mathbb{Z}^n$ mit $\pi(r) = x$. Dann ist $\ker \sigma = \left\{ \begin{pmatrix} k \\ t \end{pmatrix} \in \mathbb{Z}^n \times \mathbb{Z} \;\middle|\; \pi(k) + t\,\pi(r) = 0 \right\} =$ $\left\{ \begin{pmatrix} k \\ t \end{pmatrix} \in \mathbb{Z}^n \times \mathbb{Z} \;\middle|\; \pi(k + t\,r) = 0 \right\} = \left\langle \begin{pmatrix} A\,e_1 \\ 0 \end{pmatrix}, \ldots \begin{pmatrix} A\,e_m \\ 0 \end{pmatrix}, \begin{pmatrix} -r \\ 1 \end{pmatrix} \right\rangle \subset \mathbb{Z}^{n+1}$. Damit gilt für $B = \begin{pmatrix} A & -r \\ 0 & 1 \end{pmatrix} : \mathbb{Z}^{m+1} \longrightarrow \mathbb{Z}^{n+1}$: $\operatorname{coker} B = M$. Entwickeln nach der letzten Zeile von B zeigt sofort: $\det(B) = \pm\det(A)$, also $\delta_{n+1}(B) = \delta_n(A)$. Man sieht auch: Die k-reihigen Unterdeterminanten von A sind $(k+1)$-reihige Unterdeterminanten von B, also ist $\delta_k(A)$ ein Vielfaches von $\delta_{k+1}(B)$. Die $(k+1)$-reihige Unterdeterminanten von B sind entweder $(k+1)$-reihige Unterdeterminanten von A oder k-reihige Unterdeterminanten von A oder ganzzahlige Linearkombinationen von k-reihigen Unterdeterminanten von A, also in jedem Fall ganzzahlige Linearkombinationen von k-reihigen Unterdeterminanten von A, also ist $\delta_{k+1}(B)$ ein Vielfaches von $\delta_k(A)$. Damit folgt $\delta_{k+1}(B) = \delta_k(A)$ für alle k, d.h. $\delta_{n+1-k}(B) = \delta_{n-k}(A)$ für alle k. Nach dem 1. Schritt darf man an Stelle von B irgendeine Matrix $C : \mathbb{Z}^p \longrightarrow \mathbb{Z}^{n+1}$ mit $\operatorname{im} C = \ker \sigma$ wählen.

3. Schritt: Iteriert man den zweiten Schritt, so kann man $\pi : \mathbb{Z}^n \longrightarrow M$ zu einer Surjektion $\tau : \mathbb{Z}^n \times \mathbb{Z}^q \longrightarrow M$, $\tau(k, 0) = \pi(k)$ fortsetzen und erhält für eine beliebige Präsentation $\mathbb{Z}^s \xrightarrow{C} \mathbb{Z}^n \times \mathbb{Z}^q \xrightarrow{\tau} M \longrightarrow 0$: $\delta_{n+q-k}(C) = \delta_{n-k}(A)$ für alle k. Sind nun zwei Präsentationen $\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \xrightarrow{\pi} M \longrightarrow 0$, $\mathbb{Z}^p \xrightarrow{B} \mathbb{Z}^q \xrightarrow{\sigma} M \longrightarrow 0$ von M gegeben, so erhält man eine Präsentation $\mathbb{Z}^s \xrightarrow{C} \mathbb{Z}^n \times \mathbb{Z}^q \xrightarrow{\tau} M \longrightarrow 0$ mit $\tau(k, l) := \pi(k) + \sigma(l)$ und somit nach dem schon bewiesenem $\delta_{q-k}(B) = \delta_{n+q-k}(C) = \delta_{n-k}(A)$ für alle k. □

Wir erhalten dieses Ergebnis als Satz fest.

- **Satz 5.11 (Determinantenteiler)**

Es sei M ein endlich erzeugter $\mathbb{Z}$-Modul. Es seien zwei Präsentationen $\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \xrightarrow{\pi} M \longrightarrow 0$, $\mathbb{Z}^p \xrightarrow{B} \mathbb{Z}^q \xrightarrow{\sigma} M \longrightarrow 0$ von M gegeben Dann gilt $\delta_{q-k}(B) = \delta_{n-k}(A)$ für alle k. □

- **Korollar 5.12**

Es sei M ein endlich erzeugter $\mathbb{Z}$-Modul. Dann gilt:

(5.12.1) $M / M_{\text{tor}} \cong \mathbb{Z}^r$ ist freie abelsche Gruppe vom Rang $r = \operatorname{rg} M$.

(5.12.2) M_{tor} ist eine endliche Untergruppe von M und isomoph zu $\prod_{i=1}^{s} \mathbb{Z} / \gamma_i \mathbb{Z}$, wobei $\gamma_1, \ldots, \gamma_s$ die Elementarteiler von M sind.

(5.12.3) Ist M torsionfrei vom Rang r, so ist M frei vom Rang r:

$$M \cong \mathbb{Z}^r \ . \ \square$$

- **Bemerkung 5.13**

In der Literatur ist die Terminologie nicht ganz einheitlich. Manchmal werden die Elementarteiler einer endlichen abelschen Gruppe auch *invariante Faktoren* genannt, während der Begriff Elementarteiler den Primzahlpotenzen in der Primfaktorzerlegung der invarianten Faktoren vorbehalten bleibt [6]. Diese Terminologie ist die ursprünglich von Weierstraß vorgeschlagene. Wir wollen aber hier bei unserer Definition bleiben.

- **Beispiel 5.14**

(5.14.1) Wieviele endliche abelsche Gruppen der Ordnung p^n (p Primzahl) gibt es? Nach dem Hauptsatz gibt es soviele, wie es monotone Folgen $(n_1, n_2, ..., n_s)$ gibt mit $n_1 + n_2 + ... + n_s = n$, und $1 \le n_1 \le ... \le n_s$. Damit ist die Anzahl $\pi(n)$ der Partitionen von n auch die Anzahl der verschiedenen abelschen Gruppen der Ordnung p^n. Es gibt also 3 abelsche Gruppen der Ordnung $2^3 = 8$, entsprechend den Partitionen 111,12,3 der Zahl 3. Weiter gibt es 7 Gruppen der Ordnung $2^5 = 32$, entsprechend den Partitionen

$$11111,\ 1112,\ 113,\ 14,\ 5,\ 122,\ 23$$

der Zahl 5. (Fakt: Es gibt insgesamt 51 Gruppen der Ordnung 32)

(5.14.2) Die endliche Gruppe $G = C_5 \times C_{15} \times C_{25} \times C_{36} \times C_{54}$
hat die Präsentationsdiagonalmatrix mit den Diagonaleinträgen
$(5, 15, 25, 36, 54) = (5, 3 \cdot 5, 5^2, 2^2 3^2, 2 \cdot 3^3)$.
Die Determinantenteiler dieser Matrix sind $(1, 1, 3 \cdot 5, 2 \cdot 3^3 5^2, 2^3 \cdot 3^6 5^4)$.
Die Elementarteiler sind somit
$(1, 1, 3 \cdot 5, 2 \cdot 3^2 \cdot 5, 2^2 \cdot 3^3 \cdot 5^2) = (1, 1, 15, 90, 2700)$.
Die Normalform von G ist also $G \cong C_{15} \times C_{90} \times C_{2700}$.
Eine andere Möglichkeit die Normalform aufzuspüren benutzt den Chinesischen Restsatz und die Primfaktorzerlegung:
$G = C_5 \times (C_3 \times C_5) \times C_{5^2} \times (C_{2^2} \times C_{3^2}) \times (C_2 \times C_{3^3})$.
Wir sammeln verschiedene Potenzen (immer von 2,3,5) zusammen, mit den größten Exponenten beginnend: $\gamma_3 = 2^2 \cdot 3^3 \cdot 5^2$, $\gamma_2 = 2 \cdot 3^2 \cdot 5$, $\gamma_1 = 3 \cdot 5$ und erhalten die Elementarteiler in absteigender Reihenfolge! Für praktische Berechnungen ist diese Methode nicht geeignet, weil sie auf der Primfaktorzerlegung beruht. Besser ist es den Elementarteileralgorithmus (5.7) auf eine Präsentationsmatrix anzuwenden. Alternativ kann man auch zunächst die Determinantenteiler bestimmen, da man Determinanten mit dem Gaußschen Eliminationsverfahren und ggT's mit dem euklidischen Algorithmus effektiv berechnen kann.

■ Übungen 5

(5.1) Es sei M eine freie abelsche Gruppe vom Rang r und N sei eine Untergruppe von M. Beweisen Sie: Es gibt eine $\mathbb{Z}$-Basis $(x_1, ..., x_r)$ von M und ein $s \le r$ und Zahlen $\gamma_1, ..., \gamma_s$mit γ_i teilt γ_{i+1} für alle $i = 1, ..., s-1$, so dass $(\gamma_1 x_1, ..., \gamma_s x_s)$ eine $\mathbb{Z}$-Basis von N ist.

(5.2) Zeigen Sie:
a) Eine endlich erzeugte, torsionsfreie abelsche Gruppe ist eine freie abelsche Gruppe.
b) $(\mathbb{Q}, +)$ ist eine torsionsfreie abelsche Gruppe. Aber $\mathbb{Q}$ besitzt keine $\mathbb{Z}$-Basis und ist demzufolge nicht endlich erzeugte abelsche Gruppe. Hinweis: Zwei rationale Zahlen sind stets $\mathbb{Z}$-linear abhängig.

(5.3) Ist G eine endliche abelsche Gruppe der Ordnung n und ist m ein Teiler von n, so gibt es eine Untergruppe der Ordnung m von G. Zeige durch ein Gegenbeispiel, dass diese Aussage für endliche nicht-abelsche Gruppen im allgemeinen nicht gilt.

(5.4) Zeigen Sie: Die Menge $\mathcal{M}$ der Isomorphieklassen endlicher abelscher Gruppen bildet mit der Verknüpfung $[A] + [B] := [A \times B]$, wobei A, B endliche abelsche Gruppen sind und $[A]$ die Isomorphieklasse von A bezeichnet ($[A] = [B] \Longleftrightarrow A \cong B$), ein kommutatives Monoid mit der Kürzungsregel '$x + y = x + z \Longrightarrow y = z$'. Mit $[n] \in \mathcal{M}$ bezeichne man die Isomorphieklasse von $\mathbb{Z}/n\mathbb{Z}$. Gilt a) $[2] + [3] = [6]$, b) $[12] + [72] = [18] + [48]$ c) $[4] = [2] + [2]$ in $\mathcal{M}$?

(5.5) Zeigen Sie: Das direkte Produkt zweier freier abelscher Gruppen ist eine freie abelsche Gruppe.

(5.6) Ist die multiplikative Gruppe $(\mathbb{Q}\setminus 0, \cdot)$ eine freie abelsche Gruppe?

(5.7) Die additive Gruppe $(\mathbb{Z}[x], +)$ ist isomorph zur Untergruppe $(\mathbb{Q}_+, \cdot)$ von $(\mathbb{Q}\setminus 0, \cdot)$. Dabei bezeichnet $\mathbb{Z}[x]$ die Menge der Polynome in der Unbestimmten x mit ganzzahligen Koeffizienten und $\mathbb{Q}_+$ die Menge der positiven rationalen Zahlen.

(5.8) Es sei G die von $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ und $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ erzeugte Untegruppe von $\mathrm{GL}_2(\mathbb{Q})$. Berechnen Sie $A^n B A^{-n}$ für $n \in \mathbb{Z}$. Es sei $H = G \cap \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{Q} \right\}$. Zeigen Sie: H ist eine *nicht* endlich erzeugte abelsche Gruppe.

(5.9) Es seien $x_1, ..., x_n$ $\mathbb{Z}$-linear unabhängig in $\mathbb{Z}^n$. Ist dann $(x_1, ..., x_n)$ eine $\mathbb{Z}$-Basis von $\mathbb{Z}^n$?

(5.10) Zeigen Sie: Eine endliche abelsche Gruppe, die nicht zyklisch ist, enthält eine Untergruppe, die isomorph zu $C_p \times C_p$ ist, wobei p eine geeignete Primzahl ist.

(5.11) Berechnen Sie die Elementarteiler von

a) $\begin{pmatrix} 28 & 50 & 78 \\ 0 & -2 & 2 \end{pmatrix}$, b) $\begin{pmatrix} 90 & 141 & 231 \\ -21 & -33 & -54 \end{pmatrix}$, c) $\begin{pmatrix} 2 & 3 & 5 \\ 1 & 2 & 3 \\ 5 & -4 & 2 \end{pmatrix}$, d) $\begin{pmatrix} 128 & 190 & 100 \\ 76 & 116 & 62 \\ 62 & 16 & -14 \end{pmatrix}$.

(5.12) Ist H Untergruppe einer endlichen abelschen Gruppe G, so gibt es eine Untergruppe von G, die zu G/H isomorph ist.

Ringe und Körper

6 Grundlegende Konstruktionen und Beispiele

Inhalt: Ringe, Unterringe, ganze Gaußsche Zahlen, der Ring $\mathbb{Z}/m\mathbb{Z}$, der Polynomenring, Ideale, Restklassenringe, Beispiele von Restklassenringen, Integritätsbereiche, der Quotientenkörper eines Integritäsbereichs

- **Vorbemerkung**

Der Begriff des Körpers wurde schon in der Vorlesung 'Lineare Algebra' eingeführt, ebenso der Begriff des Ringes. Wir wollen jetzt Ringe und Körper etwas ausführlicher behandeln. Grundlegende Aussagen über Restklassenringe und Erweiterungen von Ringen und Körpern sollen behandelt werden. Zunächst wiederholen wir die Definition des Rings.

■ **Definition 6.1**

Es sei R eine Menge und $+, \cdot : R \times R \longrightarrow R$ seien zweistellige Verknüpfungen auf R (Addition und Multiplikation). Dann heißt $(R, +, \cdot)$ oder kurz R ein *Ring* genau dann, wenn gilt

(6.1.1) $(R, +)$ ist eine abelsche Gruppe.

(6.1.2) $(R, \cdot)$ ist ein Monoid.

(6.1.3) Es gelten die Distributivgesetze:
$\forall\, a, b, c \in R : (a+b)\,c = a\,c + b\,c,\ a(b+c) = a\,b + a\,c.$

Das neutrale Element bezüglich der Addition heißt Nullelement und wird mit 0 oder 0_R bezeichnet. Das neutrale Element bezüglich der Multiplikation heißt Einselement und wird mit 1 oder 1_R bezeichnet. Wir betrachten nur Ringe mit Einselement.

(6.1.4) Die invertierbaren Elemente des Monoids $(R, \cdot)$ werden *Einheiten* von R genannt. Sie bilden eine Gruppe bezüglich der Multiplikation, die wir mit $R^\times$ bezeichnen wollen. $R^\times$ heißt die *Einheitengruppe* von R.

(6.1.5) Ein Ring heißt *kommutativ*, wenn die Multiplikation kommutativ ist.

■ **Beispiel 6.2**

(6.2.1) Das trivialste Beispiel ist der *Nullring*, der nur aus einem Element $0 = 1$ besteht.

(6.2.2) Der einfachste wichtige kommutative Ring ist der Ring $\mathbb{Z}$ der ganzen Zahlen. Es gilt $\mathbb{Z}^\times = \{\pm 1\}$.

(6.2.3) Ist R ein kommutativer Ring, X eine Unbestimmte, so kann man den Polynomenring $R[X]$ definieren (vgl. Vorlesung: 'Lineare Algebra' Abschnitt 14). Dieser Ring wird noch ausführlich untersucht.

(6.2.4) Ist R ein kommutativer Ring, $n \geq 2$, so ist die Menge $M_n(R)$ der $n \times n$-Matrizen mit Koeffizienten in R ein Ring. Dieser Ring ist nicht kommutativ (vgl. Vorlesung: 'Lineare Algebra' Abschnitt 14). $M_n(R)^\times$ ist die Gruppe $\mathrm{GL}_n(R)$.

(6.2.5) Ist R ein Ring, X eine Menge, so ist die Menge $\mathrm{Abb}(X, R)$ der Funktionen $f : X \longrightarrow R$ mit den bekannten Verknüpfungen

$$(f+g)(x) = f(x) + g(x),\ (f\,g)(x) = f(x)\,g(x)$$

ein Ring. Das Nullelement ist die konstante Funktion $x \mapsto 0$. Das Einselement ist die konstante Funktion $x \mapsto 1$.

■ **Definition 6.3**

Es sei R ein Ring. Eine Teilmenge $S \subset R$ heißt *Unterring* von R, wenn gilt:

(6.3.1) $1 \in S$,
(6.3.2) $a, b \in S \Longrightarrow a - b \in S$,
(6.3.3) $a, b \in S \Longrightarrow a\,b \in S$.

S ist dann selbst ein Ring.

■ **Beispiel 6.4**

Offensichtlich ist der Durchschnitt von Unterringen von R wieder ein Unterring von R. Ist $M \subset R$ eine beliebige Teilmenge, so ist

$$\bigcap_{S \subset R \text{ Unterring mit } M \subset S} S$$

der kleinste Unterring von R, der die Menge M enthält.
Eine Teilmenge $R \subset \mathbb{C}$ ist ein Unterring von $\mathbb{C}$, wenn sie 1 enthält und abgeschlossen gegenüber der Addition und Multiplikation und der Bildung des Negativen ist. So ist etwa $\mathbb{Z}$ ein Unterring von $\mathbb{C}$. Dagegen sind zum Beispiel $2\mathbb{Z}$, $\mathbb{N}$ und S^1 keine Unterringe. Jeder Unterring von $\mathbb{C}$ enthält offensichtlich den Ring $\mathbb{Z}$ der ganzen Zahlen. Ist $M \subset \mathbb{C}$, so können wir den kleinsten Unterring von $\mathbb{C}$ betrachten, der M enthält. Er wird üblicherweise mit $\mathbb{Z}[M]$ bezeichnet. Alle Ausdrücke der Form

$$\sum_{i_1=0,\ldots,i_k=0}^{n} a_{i_1 \ldots i_k}\, x_1^{i_1} \ldots x_k^{i_k},$$

wobei $n, k \in \mathbb{N}$, $a_{i_1 \ldots i_k} \in \mathbb{Z}$, $x_1, \ldots, x_k \in M$ liegen offensichtlich in $\mathbb{Z}[M]$. Man nennt sie *polynomiale Ausdrücke* in den Elementen von M mit Koeffizienten in $\mathbb{Z}$. Das Produkt und die Differenz zweier polynomialer Ausdrücke in den Elementen von M sind wieder polynomiale Ausdrücke in den Elementen von M. Damit ist $\mathbb{Z}[M]$ genau die Menge aller dieser Ausdrücke. Man nennt $\mathbb{Z}[M]$ auch den von M erzeugten Unterring von $\mathbb{C}$. Besteht M nur aus einer komplexen Zahl α, so ist

$$\mathbb{Z}[M] = \mathbb{Z}[\alpha] = \{\textstyle\sum_{k=0}^{n} a_k\, \alpha^k \mid n \in \mathbb{N},\ a_k \in \mathbb{Z}\}.$$

Ein bekanntes Beispiel ist der *Ring der ganzen Gaußschen Zahlen* $\mathbb{Z}[i]$. Da $i^2 = -1$, besteht $\mathbb{Z}[i]$ aus den ganzzahligen Linearkombinationen $a + b\,i$ von 1 und i. Es gilt ja $i^{2k} = \pm 1$, $i^{2k+1} = \pm i$ und somit ist

$$\sum_{k=0}^{n} a_k\, i^k = \sum (\pm a_{2k}) + \sum (\pm a_{2k+1})\, i.$$

Die Elemente aus $\mathbb{Z}[i]$ bilden ein quadratisches Gitter in der komplexen Ebene. Man sieht leicht, dass die Zahlen ± 1, $\pm i$ Einheiten in $\mathbb{Z}[i]$ sind. Da

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2},$$

ist $\frac{1}{a+bi} \in \mathbb{Z}[i]$ genau dann, wenn $a^2 + b^2 = 1$, also sind $\pm 1, \pm i$ die einzigen Einheiten in $\mathbb{Z}[i]$.

- **Beispiel 6.5**

Es sei $I = \{x \in \mathbb{R} \mid 0 \le x \le 1\} = [0, 1]$ das abgeschlossene Einheitsintervall in $\mathbb{R}$. Dann enthält der Ring $\mathcal{F} = \text{Abb}(I, \mathbb{R})$ der reellwertigen Funktionen auf I eine ganze Reihe interessanter Unterringe:

$$\{\text{konstante Funktionen}\} \subset \{\text{Polynomfunktionen}\} \subset$$
$$C^\infty(I) = \{\text{beliebig oft differenzierbare Funktionen}\} \subset$$
$$C(I) = \{\text{stetige Funkionen}\} \subset \mathcal{F}.$$

- **Beispiel 6.6**

Es sei $m \in \mathbb{Z}$. Die Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$ ist eine abelsche Gruppe mit der Addition
$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}$, wie wir schon wissen. Die Addition kann als Komplexsumme gelesen werden. Es gilt:
$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = \{a + mk + b + ml \mid k, l \in \mathbb{Z}\} = \{a + b + mk \mid k \in \mathbb{Z}\}$.
Man definiert nun die Multiplikation von Restklassen wie folgt:
$(a + m\mathbb{Z})(b + m\mathbb{Z}) := (ab) + m\mathbb{Z}$.
Wir müssen zeigen, dass dies wohldefiniert ist. Dazu sei

$$a' = a + mk,\ b' = b + ml \text{ mit } k, l \in \mathbb{Z}.$$

Dann gilt

$$a'b' = ab + m(al + bk + mkl) \in ab + m\mathbb{Z}$$

und somit gilt

$$a'b' + m\mathbb{Z} = ab + m\mathbb{Z}.$$

Die Multiplikation ist somit wohldefiniert, d. h. unabhängig von der Wahl der Repräsentanten der Restklassen.
Man zeigt nun sehr leicht, dass $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Einselement $1 + m\mathbb{Z}$ ist.

Bemerkung. Man beachte, dass das Produkt der Klassen $a + m\mathbb{Z}$ und $b + m\mathbb{Z}$ *nicht* das Komplexprodukt $\{(a + mk)(b + ml) \mid k, l \in \mathbb{Z}\}$ ist!
Beispiel: $(2 + 8k)(2 + 8l) = 4 + 16k + 16l + 64kl \in 4 + 16\mathbb{Z}$.
Also ist das Komplexprodukt der Restklassen $2 + 8\mathbb{Z}$ und $2 + 8\mathbb{Z}$ in der Menge $4 + 16\mathbb{Z}$ enthalten, während das Produkt als $4 + 8\mathbb{Z}$ definiert ist.

Notation: Wenn m fixiert ist, schreiben wir kurz $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, ..., m-1\}$. Gerechnet wird 'modulo m'.
Ein Beispiel: Sei $m = 12$. In $\mathbb{Z}/12\mathbb{Z}$ gilt $5 \cdot 3 = 3$, $6 \cdot 2 = 0$, $4 \cdot 4 = 4$, $5 \cdot 5 = 1$.
Die Konstruktion der Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ soll nun verallgemeinert werden auf Faktorgruppen R/I der additiven Gruppen $(R, +)$ eines Ringes R nach gewissen additiven Untergruppen I. Damit man die Multiplkation auf R/I definieren kann, muss I weitere Eigenschaften erfüllen.

- **Definition 6.7**

Es seien R, S Ringe. Ein *Ringhomomorphismus* φ von R nach S ist eine Abbildung $\varphi : R \longrightarrow S$ mit den Eigenschaften:
(6.7.1) $\varphi(1) = 1$,
(6.7.2) $\forall\, a, b \in R:\ \varphi(a + b) = \varphi(a) + \varphi(b)$,
(6.7.3) $\forall\, a, b \in R:\ \varphi(a\,b) = \varphi(a)\,\varphi(b)$.

Ein *Ringisomorphismus* ist ein bijektiver Ringhomomorphismus.

- **Definition 6.8**

(6.8.1) Es sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Dann heißt
$\ker \varphi = \{a \in R \mid \varphi(a) = 0\}$ der Kern von φ.
(6.8.2) Eine Teilmenge $I \subset R$ heißt *(zweiseitiges) Ideal* in R, wenn gilt:
(6.8.2.1) I ist additive Untergruppe und
(6.8.2.2) $\forall\, a \in R, b \in I:\ \ a\,b \in I,\ b\,a \in I$.

(6.8.3) R sei ein kommutativer Ring. Für jede Teilmenge $M \subset R$ erhält man dann das kleinste Ideal $I \subset R$ mit $M \subset I$ als Menge aller R-Linearkombinationen von Elementen in M. Dieses Ideal wird mit $\langle M \rangle$ bezeichnet und heißt das von M erzeugte Ideal in R.

$$\langle M \rangle = \{\textstyle\sum_{k=0}^{n} a_k\, x_k \mid a_k \in R,\ x_k \in M\}.$$

- **Lemma 6.9**

Es sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Dann ist $\ker \varphi$ ein Ideal in R.

Beweis. Es sei $a \in R$ und $b \in \ker \varphi$. Dann gilt $\varphi(a\,b) = \varphi(a)\,\varphi(b) = \varphi(a)\,0 = 0$ und genauso folgt $\varphi(\,b\,a) = \varphi(b)\,\varphi(a) = 0\,\varphi(a) = 0$. □

- **Satz und Definition 6.10**

Es sei R ein Ring und I ein Ideal in R. Dann ist auf der additiven Faktorgruppe R/I aller Restklassen $a + I,\ a \in R,$ durch die Definition

$$(a+I)(b+I) := ab+I$$

eine Multiplikation definiert. Es gilt dann:
R/I ist eine Ring. Die Restklassenabbildung $\pi: R \longrightarrow R/I$ ist ein surjektiver Ringhomomorphismus und besitzt die folgende *universelle Eigenschaft*:

(6.10.1) Ist $\varphi: R \longrightarrow S$ ein Ringhomomorphismus mit $I \subset \ker\varphi$, so gibt es genau einen Ringhomomorphismus $\overline{\varphi}: R/I \longrightarrow S$ mit $\overline{\varphi} \circ \pi = \varphi$.
R/I heißt der *Restklassenring* von R nach I.

Beweis. Die Multiplikation ist wohldefiniert: Ist $a' = a+k$, $b' = b+l$ mit $k, l \in I$, so gilt $a'b' = ab + (kb + al)$ und da I ein zweiseitiges Ideal ist, ist $kb + al \in I$ und somit $a'b' + I = ab + I$. Die Rechenregeln übertragen sich mühelos von R auf R/I. Wir demonstrieren dies am Distributivgesetz:
$(a+I)((b+I)+(c+I)) = (a+I)(b+c+I) = a(b+c)+I \underset{[\text{Regel in } R]}{=} ab+ac+I$
$= (ab+I)+(ac+I) = (a+I)(b+I)+(a+I)(c+I)$.
Klar ist: $0+I$ ist das Nullelement, $1+I$ ist das Einelement.
Ebenso ist nach Definition klar, dass die Restklassenabbildung $\pi(a) = a+I$ ein surjektiver Ringhomomorphismus ist.
Zur universellen Eigenschaft. Für die additive Gruppe von R/I ist uns die universelle Eigenschaft schon bekannt. Wir haben also zu $\varphi: R \longrightarrow S$ schon die Abbildung $\overline{\varphi}: R/I \longrightarrow S$ mit $\overline{\varphi} \circ \pi = \varphi$.
Diese Abbildung ist auch ein Ringhomomorphismus, denn
$\overline{\varphi}((a+I)(b+I)) = \overline{\varphi}(ab+I) = \overline{\varphi}(\pi(ab)) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(a+I)\overline{\varphi}(b+I)$
und $\overline{\varphi}(1+I) = \varphi(1) = 1$. □

- **Satz 6.11 (Homomorphiesatz)**

Jeder surjektive Ringhomomorphismus

$$\varphi: R \longrightarrow S$$

induziert einen Isomorphismus

$$\overline{\varphi}: R/\ker\varphi \longrightarrow S.$$

Beweis. Nach der universellen Eigenschaft wird ein Homomorphismus
$\overline{\varphi}: R/\ker\varphi \longrightarrow S$ induziert, der hier offensichtlich ein Isomorphismus ist. □

- **Satz 6.12 (Entsprechungssatz)**

Es sei $\varphi: R \longrightarrow S$ ein surjektiver Ringhomomorphismus. $I_0 = \ker\varphi$. Dann gilt:

(6.12.1) Ist $I \subset R$ ein Ideal, so ist auch $\varphi(I)$ ein Ideal in S.

(6.12.2) Ist $J \subset S$ ein Ideal, so ist auch $\varphi^{-1}(J)$ ein Ideal in R.

(6.12.3) Die Zuordnung $J \mapsto \varphi^{-1}(J)$ ist eine Bijektion von der Menge aller Ideale in S auf die Menge aller Ideale in R, die das Ideal I_0 enthalten. Die Umkehrabbildung ist durch $I \mapsto \varphi(I)$ gegeben.

(6.12.4) Ist J ein Ideal in S, so induziert φ einen Isomorphismus $R/\varphi^{-1}(J) \longrightarrow S/J$.

Beweis. Zu (6.12.1): $\varphi(I)$ ist eine additive Untergruppe. Ist nun
$y \in S,\ a \in I,\ b = \varphi(a)$, so gibt es ein $x \in R$ mit $\varphi(x) = y$, und es gilt
$a\,x, x\,a \in I, y\,b = y\ \varphi(a) = \varphi(x\,a) \in \varphi(I),\ b\,y = \varphi(a)\,y = \varphi(a\,x) \in \varphi(I)$.
Damit ist $\varphi(I)$ ein Ideal in S.
Zu (6.12.2): Das ist noch einfacher als (6.12.1): Wir beweisen die Eigenschaft: $a \in \varphi^{-1}(J),\ x \in R \Longrightarrow a\,x \in \varphi^{-1}(J)$. Das geht so:
$a \in \varphi^{-1}(J),\ x \in R \Longrightarrow \varphi(a) \in J, \varphi(x) \in S \Longrightarrow \varphi(a\,x) = \varphi(a)\,\varphi(x) \in J \Longrightarrow a\,x \in \varphi^{-1}(J)$.
Zu (6.12.3): Da φ surjektiv ist, gilt $\varphi\,\varphi^{-1}(J) = J$. Weiter gilt trivialerweise $I \subset \varphi^{-1}\,\varphi(I)$. Es bleibt nur die umgekehrte Inklusion zu zeigen: Sei also $a \in \varphi^{-1}\,\varphi(I)$. Dann ist $\varphi(a) \in \varphi(I)$, also gilt $\varphi(a) = \varphi(b)$ für ein $b \in I$. Es folgt $\varphi(a-b) = 0$, also $a - b \in \ker\varphi \subset I$ und somit $a = (a-b) + b \in I$. Damit ist $I = \varphi^{-1}\,\varphi(I)$.
Zu (6.12.4): Die Komposition $\pi \circ \varphi : R \longrightarrow S/J$ von φ mit der Restklassenabbildung $\pi : S \longrightarrow S/J$ induziert nach dem Homomorphiesatz einen Isomorphimus $R/\ker(\pi\circ\varphi) \longrightarrow S/J$. Da aber $\ker(\pi\circ\varphi) = \varphi^{-1}(\ker\pi) = \varphi^{-1}(J)$, ist die Behauptung bewiesen. □

- **Beispiele 6.13**

(6.13.1) Alle Ideale in $\mathbb{Z}$ sind von der Form $m\,\mathbb{Z}$. Ist nun $n\,\mathbb{Z} \subset m\,\mathbb{Z}$, so heißt das: m ist ein Teiler von n. Nach (6.12.4) gilt für das Ideal
$J := m\,(\mathbb{Z}/n\,\mathbb{Z}) = \{m\,k + n\,\mathbb{Z} \mid k \in \mathbb{Z}\} = m\,\mathbb{Z}/n\,\mathbb{Z}$ in $\mathbb{Z}/n\,\mathbb{Z}$ die Isomorphie
$\mathbb{Z}/m\,\mathbb{Z} \cong (\mathbb{Z}/n\,\mathbb{Z})/J = (\mathbb{Z}/n\,\mathbb{Z})/(m\,\mathbb{Z}/n\,\mathbb{Z})$.

(6.13.2) Wir betrachten den Restklassenring $R = \mathbb{Z}[i]/I$, wobei $I = (1+3\,i)\,R$. Die Elemente von R schreiben wir in der Form $[a+b\,i] := (a+b\,i) + I$. Wir untersuchen den Ringhomomorphismus $\varphi : \mathbb{Z} \longrightarrow R$. (Es gibt nur einen!). Behauptung: φ ist surjektiv. Sei dazu $[a+b\,i] \in R$. Da $i - 3 = i\,(1+3\,i) \in I$, ist $[i-3] = [0]$, also gilt im Ring R

$$[i] = [3]$$

und somit erhalten wir

$$[a+b\,i] = [a] + [b][i] = [a] + [b][3] = [a+3\,b] = \varphi(a+3\,b).$$

Damit ist $[a+b\,i]$ das Bild der ganzen Zahl $a+3\,b$ unter dem Homomorphismus φ. φ ist also surjektiv. Nach dem Homomorphiesatz ist $R \cong \mathbb{Z}/\ker\varphi$. Wir berechnen $\ker\varphi$. Es gilt: $n \in \ker\varphi \Longleftrightarrow [n] = [0] \Longleftrightarrow \exists\, a, b \in \mathbb{Z}$:
$n = (a+b\,i)\,(1+3\,i)$, d.h. $n = a - 3\,b,\ 0 = b + 3\,a$.

Also: $n \in \ker\varphi \iff n = a + 9a$ für ein $a \in \mathbb{Z} \Longleftrightarrow n \in 10\,\mathbb{Z}$. Damit ist R isomorph zu $\mathbb{Z}/10\,\mathbb{Z}$.

(6.13.3) Ist R ein beliebiger kommutativer Ring und $a \in R$, so ist

$$\langle a\rangle := a\,R = \{a\,x \mid x \in R\}$$

das von a erzeugte Ideal in R. Im Restklassenring $R/a\,R$ ist die Restklasse von a das Nullelement: $a + a\,R = a\,R$. Restklassenringe dieser Art können schon recht kompliziert sein, selbst wenn R ein 'einfacher' Ring ist, wie die nachfolgenden Beispiele zeigen.

(6.13.4) Wir definieren zunächst den Polynomenring $\mathbb{C}[x, y]$ in zwei Unbestimmten x, y durch $\mathbb{C}[x, y] = \mathbb{C}[x][y]$. Elemente in $\mathbb{C}[x, y]$ sind von der Form

$$F = \sum_{k=0}^{n} P_k\,y^k,$$

wobei

$$P_k = \sum_{j=0}^{n} a_{j\,k}\,x^j \in \mathbb{C}[x]$$

ist. Nach dem Distributivgesetz ergibt sich dann

$$F = \sum_{j,k=0}^{n} a_{j\,k}\,x^j\,y^k.$$

Dies ist ein Polynom in den Unbestimmten x, y. Es sei nun

$$R = \mathbb{C}[x, y]/\langle y - p\rangle,$$

wobei $p \in \mathbb{C}[x]$ und mit $\langle y - p\rangle$ das Ideal $(y - p)\,\mathbb{C}[x, y]$ bezeichnet wird.

Behauptung. Die Abbildung $\varphi : \mathbb{C}[x] \longrightarrow R$, die von der Inklusion $\mathbb{C}[x] \subset \mathbb{C}[x, y]$ induziert wird, ist ein Isomorphismus.

Beweis. φ ist injektiv, denn $\langle y - p\rangle$ enthält keine von Null verschiedenen Polynome, die nur von x abhängen, d. h. $\ker\varphi = \mathbb{C}[x] \bigcap \langle y - p\rangle = 0$: Ist

$$f = a_0(x) + a_1(x)\,y + \ldots + a_n(x)\,y^n$$

mit $b = (y - p)\,f \in \mathbb{C}[x]$, so folgt nämlich

$$b(x) = (y - p(x))\,f = -p\,a_0 + y(a_0 - p\,a_1) + y^2(a_1 - p\,a_2) + \ldots + y^n(a_{n-1} - p\,a_n) + a_n\,y^{n+1}.$$

Koeffizientenvergleich liefert
$b = -p\,a_0$, $0 = a_0 - p\,a_1$, ..., $0 = a_{n-1} - p\,a_n$, $0 = a_n$, also $a_i = 0$ für alle i und somit $b = 0$. φ ist auch surjektiv, weil für $F = \sum_{k=0}^{n} P_k\,y^k \in \mathbb{C}[x, y]$ gilt:

$$F - \sum_{k=0}^{n} P_k\,p^k = \sum_{k=0}^{n} P_k(y^k - p^k) \in \langle y - p\rangle,$$

denn $y^k - p^k = (y - p)\sum_{j=0}^{k-1} y^{k-1-j}\,p^j$. Also ist $F + \langle y - p\rangle = \varphi(\sum_{k=0}^{n} P_k\,p^k)$.
Dieses Beispiel ist ein Spezialfall der Isomorphie $R \cong R[x]/\langle x - a\rangle$ für alle $a \in R$.

(6.13.5) Es sei $R = \mathbb{C}[x, y] / \langle x y \rangle$. Wir betrachten die Auswertungshomomorphismen

$$\varphi_1 : \mathbb{C}[x, y] \longrightarrow \mathbb{C}[x],\ f \mapsto f(x, 0),\ \varphi_2 : \mathbb{C}[x, y] \longrightarrow \mathbb{C}[y],\ f \mapsto f(0, y).$$

Diese induzieren einen Homomorphismus in den Produktring

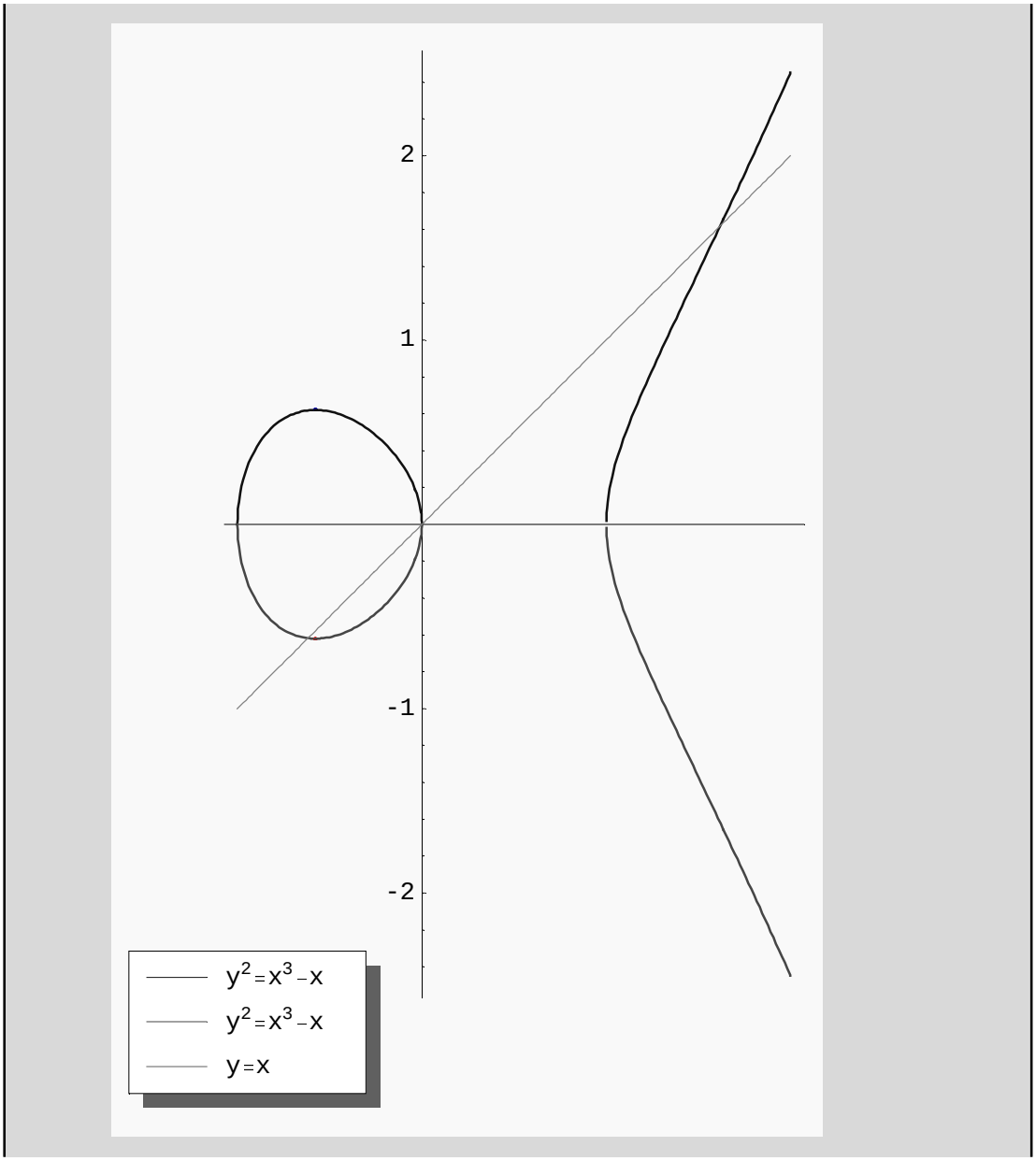
$$\varphi = (\varphi_1, \varphi_2) : \mathbb{C}[x, y] \longrightarrow \mathbb{C}[x] \times \mathbb{C}[y]$$

Es sollte klar sein, wie die Ringstruktur auf dem kartesischen Produkt zweier Ringe einzuführen ist. Siehe (6.15.1). $S = \{(p, q) \mid p(0) = q(0)\}$ ist ein Unterring von $\mathbb{C}[x] \times \mathbb{C}[y]$ (Übung) und S ist das Bild von φ, denn:
$\varphi(f) = (f(x, 0), f(0, y)) \in S$ und zu gegebenen $(p, q) \in S$ mit $p(0) = q(0) = c$ ist
$\varphi(p + q - c) = (p + q(0) - c, p(0) + q - c) = (p, q)$.
Weiter ist f genau dann im Kern von φ, wenn $f(x, 0) = 0 = f(0, y)$, d.h. in $f = \sum_{i,j} a_{ij} x^j y^j$ treten nur Koeffizienten a_{ij} mit positiven Indizes auf, also nur Monome, die durch $x y$ teilbar sind. Damit ist $\ker \varphi = \langle x y \rangle$.
Nach dem Homomorphiesatz ist daher $R \cong S$.

(6.13.6) $R = \mathbb{C}[x, y] / \langle y^2 - x^3 + x \rangle$ ist ein algebraisch nicht so leicht zu beschreibender Ring. Man sieht, dass man $\mathbb{C}[x]$ als Unterring von R auffassen kann (vgl. (6.13.4)). Die Restklasse von x werde mit ξ bezeichnet. ($\mathbb{C}[x] \longrightarrow R$ mit $x \mapsto \xi$ ist injektiv). Dann ist $R = \{a + b\,\eta \mid a, b \in \mathbb{C}[\xi]\}$, wobei η die Restklasse von y sei. Wir wollen dies beweisen: Es sei $f = y^2 - x^3 + x$ und $\pi : \mathbb{C}[x, y] \longrightarrow R$ sei die Restklassenabbildung, also $\pi(x) = \xi$, $\pi(y) = \eta$. Es gilt dann, da π ein Ringhomomorphismus ist
$\pi(f) = \pi(y^2 - x^3 + x) = \pi(y)^2 - \pi(x)^3 + \pi(x) = \eta^2 - \xi^3 + \xi$. Natürlich ist $\pi(f) = 0$, weil $f \in \ker \pi = \langle f \rangle$. Man kann also schließen, dass $\eta^2 = \xi^3 - \xi$ im Ring R gilt. Damit kann man jedes Element $\sum_{k=0}^{n} a_k(\xi)\, \eta^k$
umformen zu einem Ausdruck $a + b\,\eta$ mit $a, b \in \mathbb{C}[\xi]$.
Es gilt $(a + b\,\eta)(c + d\,\eta) = (a\,c + b\,d(\xi^3 - \xi)) + (a\,d + b\,c)\,\eta$. Mehr kriegen wir zunächst nicht heraus.

$$y^2 - x^3 + x = 0$$

ist die Gleichung einer sogenannten elliptischen Kurve. Die Lösungsmenge dieser Gleichung in $\mathbb{C}^2$ hat auch eine interessante topologische Gestalt, nämlich die eines gelochten Torus. Sie ist reell zweidimensional, aber komplex eindimensional, Die vollständige Kurve (Torus ohne Loch) findet man in der komplex-projektiven Ebene, parametrisiert durch eine geeignete Weierstraßsche $\wp$-Funktion und ihre Ableitung $\wp'$. Das führt in das sehr interessante Gebiet der elliptischen Funktionen und elliptischen Kurven.



Literatur dazu:
M. Reid: Undergraduate Algebraic Geometry, Cambridge University Press 1988,
Freitag/Busam: Funktionentheorie, Springer 1993
interessant ist auch:
Silverman/ Tate: Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics, Springer 1992

(6.13.7) Eine einfache aber wichtige Bemerkung: Die einzigen Ideale in einem Körper K sind $I = \{0\}$ und $I = K$. Ist nämlich $I \neq 0$, so gibt es ein $a \in I$ mit $a \neq 0$. Dann ist $1 = a^{-1} a \in I$ und somit $b = b\,1 \in I$ für alle $b \in I$.

■ **Definition 6.14**

(6.14.1) Es sei R ein Ring. Ein Element $a \in R$ heißt *Linksnullteiler* (*Rechtsnullteiler*), wenn es ein $b \in R$ gibt mit $b \neq 0$ und $a\,b = 0\,(b\,a = 0)$. In einem kommutativen Ring fallen beide Begriffe zusammen. Man spricht dann einfach von Nullteilern. a ist *Nicht-Nullteiler*, wenn gilt: Aus $a\,b = 0$ folgt stets $b = 0$ mit anderen Worten: $a \in R$ ist genau dann Nichtnullteiler, wenn die Abbildung $R \longrightarrow R$, $b \mapsto a\,b$ injektiv ist.

(6.14.2) Ein kommutativer Ring R heißt *Integritätsbereich*, wenn $0 \neq 1$ gilt und wenn 0 der einzige *Nullteiler* in R ist, wenn also aus $a\,b = 0$ folgt, dass $a = 0$ oder $b = 0$ gilt.
In einem Integritätsbereich gilt die Kürzungsregel: $a\,b = a\,c,\ a \neq 0 \Longrightarrow b = c$.

■ **Beispiel 6.15**

(6.15.1) Sind R, S Ringe, so wird das kartesische Produkt $R \times S$ durch $(a, b) + (c, d) = (a + c, b + d), (a, b)\,(c, d) = (a\,c, b\,d)$ ein Ring, der *Produktring* von R und S. $1 = (1, 1)$ ist das Einselement. $0 = (0, 0)$ ist das Nullelement. Für $a = (1, 0), b = (0, 1)$ gilt: $a\,b = b\,a = 0,\ a^2 = a, b^2 = b$. Insbesondere sind a, b Nullteiler in $R \times S$ (vorausgesetzt $R \neq 0$, $S \neq 0$).

(6.15.2) In $R = \mathbb{Z}/12\,\mathbb{Z}$ gilt $3 \cdot 4 = 0$. Die Restklassen 3 und 4 sind also Nullteiler in R. Die Abbildung $\varphi : R \longrightarrow \mathbb{Z}/3\,\mathbb{Z} \times \mathbb{Z}/4\,\mathbb{Z}$, $\varphi(n) = (n \bmod 3,\ n \bmod 4)$ ist ein Ringisomorphismus.

(6.15.3) Der Ring $C([0, 1])$ der stetigen Funktionen auf dem Intervall $[0, 1]$ enthält viele Nullteiler! Jede stetige Funktion, die auf einem Teilintervall $[a, b] \subset [0, 1]$ verschwindet ist ein Nullteiler in $C([0, 1])$.

(6.15.4) Ist K ein Körper, x eine Unbestimmte, so ist der Polynomenring $K[x]$ ein Integritätsbereich.

(6.15.5) Alle Unterringe von $\mathbb{C}$ sind Integritätsbereiche, zum Beispiel $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\sqrt{2}\right]$. (Damit befasst sich die *algebraische Zahlentheorie*.) Der kleinste Unterkörper von $\mathbb{C}$ ist $\mathbb{Q}$. Der kleinste Unterkörper von $\mathbb{C}$, der den Ring $\mathbb{Z}[i]$ enthält ist $\mathbb{Q}[i] = \{a + b\,i \mid a, b \in \mathbb{Q}\} = \left\{ \frac{x}{y} \;\middle|\; x, y \in \mathbb{Z}[i], y \neq 0 \right\}$. Man nennt $\mathbb{Q}[i]$ den Quotientenkörper von $\mathbb{Z}[i]$, da er aus Brüchen besteht, deren Zähler und Nenner in $\mathbb{Z}[i]$ liegen.

(6.15.6) Der Ring $R = \mathbb{C}[x, y]/\langle y^2 - x^3 + x \rangle$, den wir schon in (6.13.6) betrachtet haben, ist ebenfalls ein Integritätsbereich. Dazu muss man folgendes zeigen: Sind $p, q \in \mathbb{C}[x, y]$Polynome, deren Produkt ein Vielfaches von $y^2 - x^3 + x$ ist, so gilt dies schon für p oder q selbst. Man sagt: das Polynom $y^2 - x^3 + x$ ist ein *Primpolynom*. Zum Beweis benötigen wir den Satz von der eindeutigen Primfaktorzerlegung von

Polynomen in $\mathbb{C}[x, y]$. Wir können uns jetzt schon überlegen, dass $y^2 - x^3 + x$ nicht das Produkt zweier Polynome $a, b \in \mathbb{C}[x, y]$ ist, die beide nicht konstant sind, mit anderen Worten, dass $y^2 - x^3 + x$ *irreduzibel* ist. Schreiben wir $a = \sum_{k=0}^{n} a_k(x)\, y^k$, $b = \sum_{k=0}^{m} b_k(x)\, y^k$ mit $a_n \neq 0$, $b_m \neq 0$, und nehmen an, dass $a\, b = y^2 - x^3 + x$, so folgt durch Koeffizientenvergleich der Koeffizienten vor den Potenzen von y: $a_n\, b_m \neq 0$ ist der Koeffizient vor y^{n+m}. es muss also $n + m = 2$ gelten und $a_n\, b_m = 1$. Annahme: $n = m = 1$. Dann ist $a = a_1\, y + a_0$, $b = b_1\, y + b_0$ und $a_1\, b_1 = 1$ woraus folgt, dass a_1, b_1 konstante Polynome in x sind, also ohne Einschränkung $a_1 = b_1 = 1$. Es folgt nun $a\, b = y^2 + (a_0 + b_0)\, y + a_0\, b_0$ und somit $a_0 + b_0 = 0$, $a_0\, b_0 = -x^3 + x$. Damit müsste der Grad von $-x^3 + x$ gerade sein, ein Widerspruch! Es muss also $n = 2$ oder $n = 0$ gelten. Es folgt jetzt leicht, dass a oder b konstant (unabhängig von x und y) sein muss. Der Satz über die eindeutige Primfaktorzerlegung im Polynomenring $\mathbb{C}[x, y]$, den wir noch beweisen werden, liefert nun, dass $y^2 - x^3 + x$ ein *Primpolynom* und der Restklassenring R folglich ein Integritätsring ist.

Wir führen jetzt die allgemeine Konstruktion durch, die einen Integritätsbereich R zu einem Körper K erweitert, in dem alle Elemente 'Brüche' $\frac{x}{y}$ von Elementen $x, y \in R$, $y \neq 0$ sind.

- **Satz 6.16**

Es sei R ein Integritätsbereich. Dann gibt es einen Körper K, der R als Unterring enthält und für den gilt: Zu jedem $r \in K$ gibt es Elemente $x, y \in R$, $y \neq 0$, so dass $r = x y^{-1}$ gilt.
Es gilt die universelle Eigenschaft:
(6.16.1) Ist $\varphi : R \longrightarrow L$ ein injektiver Ringhomomorphismus und L ein Körper, so gibt es genau eine Fortsetzung von φ zu einem Körperhomomorphismus $\varphi : K \longrightarrow L$.

Durch die universelle Eigenschaft ist K bis auf kanonische Isomorphie festgelegt. K heißt der *Quotientenkörper* von R.

Beweis. Auf der Menge $X = R \times (R \setminus \{0\})$ führen wir eine Äquivalenzrelation ein: $(a, b) \sim (c, d) \Longleftrightarrow a\, d = b\, c$. In der Tat ist dies eine Äquivalenzrelation:
a) $(a, b) \sim (a, b)$, weil $a\, b = b\, a$.
b) $(a, b) \sim (c, d)$ und $(c, d) \sim (e, f)$
$\Longrightarrow a\, d = b\, c$, $c\, f = d\, e \Longrightarrow d(a\, f) = a\, d\, f = b\, c\, f =$
$b\, d\, e = d\, (b\, e) \Longrightarrow a\, f = b\, e \Longrightarrow (a, b) \sim (e, f)$.
c) $(a, b) \sim (c, d) \Longrightarrow a\, d = b\, c \Longrightarrow c\, b = d\, a \Longrightarrow (c, d) = (a, d)$.
Nun betrachten wir die Menge der Äquivalenzklassen: $K := X / \sim$. Die Äquivalenzklasse von (a, b) bezeichnen wir mit $\frac{a}{b}$. Es gilt dann also $\frac{a}{b} = \frac{c}{d} \Longleftrightarrow a\, d = b\, c$. Jetzt führen wir die Addition und Multiplikation auf K ein.

Addition: $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$,

Multiplikation: $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$.

Wir müssen zeigen, dass dies wohldefiniert ist: Zur Addition: Es sei $\frac{a}{b} = \frac{x}{y}$, $\frac{c}{d} = \frac{u}{v}$, also $ay = bx$, $cv = du$. Es folgt
$yv(ad + bc) = ayvd + cvyb = bxvd + duyb = bd(xv + yu)$ und somit ist $\frac{ad+bc}{bd} = \frac{xv+yu}{yv}$. Die Addition ist also wohldefiniert.
Zur Multiplikation: Es sei $\frac{a}{b} = \frac{x}{y}$, $\frac{c}{d} = \frac{u}{v}$, also $ay = bx, cv = du$. Dann gilt $yvac = aycv = bxdu = bdxu$, also $\frac{ac}{bd} = \frac{xu}{yv}$. Auch die Multiplikation ist wohldefiniert.
Behauptung: K ist ein Körper. Es gilt die Körperaxiome zu verifzieren (siehe Lineare Algebra, Abschnitt 6):

(K1)
$(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{(ad+bc)f+bde}{bdf} = \frac{adf+b(cf+de)}{bdf} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f})$

(K2) $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} = \frac{cb+da}{db}$ $\frac{c}{d} + \frac{a}{b}$.

(K3) $\frac{0}{1} + \frac{a}{b} = \frac{0b+1a}{1b} = \frac{a}{b}$.

(K4) $\frac{a}{b} + \frac{-a}{b} = \frac{ab+b(-a)}{b^2} = \frac{0}{b^2} = \frac{0}{1}$, weil $1 \cdot 0 = b^2 \cdot 0$.

(K5) $(\frac{a}{b}\ \frac{c}{d})\ \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b}\ (\frac{c}{d}\ \frac{e}{f})$.

(K6) $\frac{a}{b}\ \frac{c}{d} = \frac{ac}{bd} = \frac{c}{d}\ \frac{a}{b}$.

(K7) $\frac{1}{1}\ \frac{a}{b} = \frac{1a}{1b} = \frac{a}{b}$.

(K8) $\frac{a}{b} \neq \frac{0}{1} \Longrightarrow a1 \neq b0 \Longrightarrow a \neq 0 \Longrightarrow \frac{b}{a} \in K$, $\frac{b}{a}\ \frac{a}{b} = \frac{ba}{ab} = \frac{1}{1}$.

(K9) $\frac{a}{b}\ (\frac{c}{d} + \frac{e}{f}) = \frac{a(cf+de)}{bdf} = \frac{ba(cf+de)}{bbdf} = \frac{acbf+bdae}{bdbf}$ $\frac{ac}{bd} + \frac{ae}{bf}$.

Die Behauptung ist bewiesen.
Die Abbildung $\iota : R \longrightarrow K$, $\iota(a) := \frac{a}{1}$ ist ein injektiver Ringhomomorphismus, wie man sehr leicht nachprüft. Wir identifizieren das Element $a \in R$ mit dem Element $\frac{a}{1}$ in K. Auf diese Weise ist R ein Unterring von K.
Wir kommen zur universellen Eigenschaft: Sei $\varphi : R \longrightarrow L$ ein injektiver Ringhomomorphismus und L ein Körper. Wir setzen $\varphi(\frac{a}{b}) := \varphi(a)\varphi(b)^{-1}$. Das ist wohldefiniert, denn zunächst ist $\varphi(b) \neq 0$, wenn $b \neq 0$, weil φ nach Voraussetzung injektiv ist. Da L ein Körper ist, kann man also $\varphi(a)\varphi(b)^{-1}$ bilden. Ist nun $\frac{a}{b} = \frac{c}{d}$, so ist $ad = bc$ und somit auch $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$, also $\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$. Damit ist die Wohldefiniertheit gezeigt. Man sieht leicht, dass $\varphi : K \longrightarrow L$ ein Homomorphismus ist und zwar der einzige, der $\varphi : R \longrightarrow L$ von R nach K fortsetzt. □

■ Beispiel 6.17

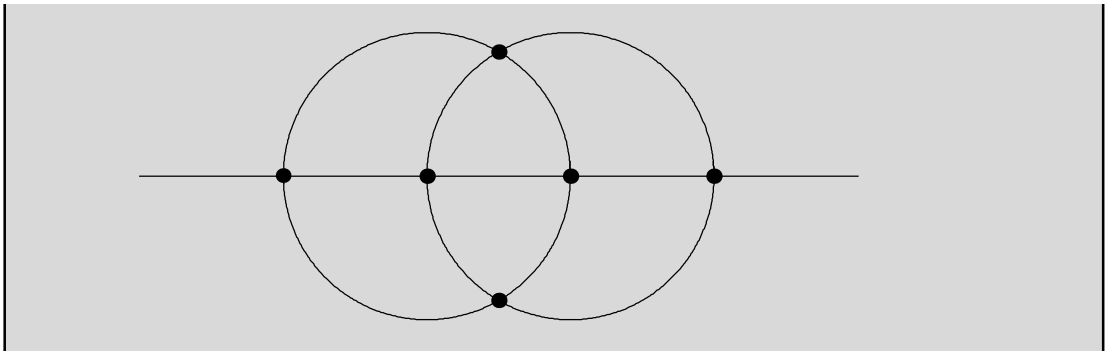
(6.17.1) Der Quotientenkörper von $\mathbb{Z}$ ist $\mathbb{Q}$.

(6.17.2) Es sei K ein Körper und x eine Unbestimmte. Der Quotientenkörper von $K[x]$ heißt Körper der *rationalen Funktionen* in der Unbestimmten x über dem Körper K und soll mit $K(x)$ bezeichnet werden. $K(x) = \left\{ \frac{p}{q} \mid p, q \in K[x], q \neq 0 \right\}$. Ist $K = \mathbb{C}$, so kann man die rationalen Funktionen als Abbildungen der Riemannschen Zahlenkugel $S = \mathbb{C} \bigcup \infty$ in sich beschreiben. Wir stellen $r \in \mathbb{C}(x)$ in der Form $r = \frac{p}{q}$ mit Polynomen p, q die keine gemeinsamen Nullstellen besitzen dar. Dann ist $r(z) \in \mathbb{C}$ für $z \in \mathbb{C}$ mit $q(z) \neq 0$. Ist $q(z) = 0$, so setzen wir $p(z) = \infty$. Schließlich definieren wir auch den Wert $r(\infty)$ und zwar als 0, wenn der Grad von p kleiner als der Grad von q ist, ∞, wenn der Grad von p größer als der Grad von q ist und als $\frac{a_n}{b_n}$, wenn p und q beide den Grad n haben mit Leitkoeffizienten a_n bzw. b_n.

(6.17.3) Ist R ein Unterring von $\mathbb{C}$, so ist der Quotientenkörper K von R nach der universellen Eigenschaft ein Unterkörper von $\mathbb{C}$ und zwar der kleinste Unterkörper von $\mathbb{C}$, der R enthält. Ist $M \subset \mathbb{C}$ eine beliebige Teilmenge, so ist der kleinste Unterkörper von $\mathbb{C}$, der die Menge M enthält, der Quotientenkörper von $\mathbb{Z}[M]$, besteht also aus den *rationalen Audrücken* in M mit Koeffizienten in $\mathbb{Z}$, das sind Brüche $\frac{p}{q}$ von Elementen $p, q \in \mathbb{Z}[M]$, welche ja polynomiale Ausdrück in Elementen von M sind. Wir bezeichnen diesen Körper auch mit $\mathbb{Q}(M)$. Zum Beispiel ist für $d \in \mathbb{Z}$, d quadratfrei, $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left[\sqrt{d}\right] = \left\{ a + b\sqrt{d} \mid a, b \in \mathbb{Q} \right\}$ eine sogenannte *quadratische Erweiterung* von $\mathbb{Q}$. $\mathbb{Q}\left[\sqrt{d}\right]$ ist der Quotientenkörper von $\mathbb{Z}\left[\sqrt{d}\right] = \left\{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \right\}$. Man muss sich hier überlegen, dass die Terme $a + b\sqrt{d} \mid a, b \in \mathbb{Q}$ wirklich einen Unterkörper von $\mathbb{C}$ bilden (Übung!)

■ **Beispiel 6.18**

Ein weiteres für die Frage der Konstruierbarkeit mit Zirkel und Lineal wichtiges Beispiel ist die Menge $\mathfrak{K}$ der aus 0 un 1 konstruierbaren komplexen Zahlen. Es stellt sich heraus, dass $\mathfrak{K}$ ein Unterkörper von $\mathbb{C}$ ist. Um $\mathfrak{K}$ zu definieren, denken wir uns $\mathbb{C}$ als die komplexe Zahlenebene. Eine Teilmenge M von $\mathbb{C}$ denken wir uns demzufolge als Punktmenge in der Ebene. Es sei nun $M \subset \mathbb{C}$ mit $0, 1 \in M$. Mit $\mathcal{G}_M$ bezeichnen wir die Menge aller Geraden in der Ebene, die durch mindestens zwei Punkte von M gehen. Dies ist die Menge der allein mit einem Lineal aus M 'konstruierbaren' Geraden. Ist $M = \{0, 1\}$, so besteht $\mathcal{G}_M$ nur aus einem Element, der Verbindungsgeraden von 0 und 1 (das ist die reelle Achse in $\mathbb{C}$). Weiter bezeichne $\mathcal{K}_M$ die Menge aller Kreise C in der Ebene, deren Mittelpunkt ein Punkt von M ist und deren Radius der Abstand zweier Punkt aus M ist. Dies ist die Menge der allein mit dem Zirkel aus M konstruierbaren Kreise. Man nimmt den Abstand zweier Punkte aus M in den Zirkel und zieht den Kreis mit diesem Radius um einen weiteren Punkt aus M. Ist $M = \{0, 1\}$, so sind nur zwei Kreise in $\mathcal{K}_M$, nämlich die Kreise um 0 und 1 mit dem Radius 1. Wir definieren nun: $z \in \mathbb{C}$ ist *elementar aus M konstruierbar*, wenn gilt:
i) z ist der Schnittpunkt zweier Geraden $L_1, L_2 \in \mathcal{G}_M$oder
ii) z ein Schnittpunkt einer Geraden $L \in \mathcal{G}_M$ und eines Kreises $C \in \mathcal{K}_M$ oder
iii) z ist ein Schnittpunkt zweier Kreise $C_1, C_2 \in \mathcal{K}_M$.
Offensichtlich sind genau die sechs Zahlen $0, 1, -1, 2, \frac{1}{2}\left(1 + \sqrt{3}\, i\right), \frac{1}{2}\left(1 - \sqrt{3}\, i\right)$ elementar aus $\{0, 1\}$ konstruierbar. Wie man sieht ist die Menge dieser sechs Punkte invariant unter der Konjugation, d.h. der Spiegelung an der reellen Achse.



Aus dieser Menge $M = \left\{0, 1, -1, 2, \frac{1}{2}\left(1 + \sqrt{3}\, i\right), \frac{1}{2}\left(1 - \sqrt{3}\, i\right)\right\}$ sind zum Beispiel folgende Punkte elementar konstruierbar: $\frac{1}{2}$ als Schnittpunkt der Gerade durch 0 und 1 mit der Geraden durch $\frac{1}{2}\left(1 + \sqrt{3}\right), \frac{1}{2}\left(1 - \sqrt{3}\right)$.
Wir definieren nun:
Eine Zahl $z \in \mathbb{C}$ ist *(mit Hilfe von Zirkel und Lineal) aus 0 und 1 konstruierbar,* wenn es eine endliche Kette M_k von Teilmengen von $\mathbb{C}$ gibt, so dass $\{0, 1\} = M_0 \subset M_1 \subset \ldots M_n$ gilt mit $z \in M_n$ und so dass für $i = 1, \ldots, n$ gilt: Alle Zahlen aus M_i sind elementar aus M_{i-1} konstruierbar. Mit $\mathfrak{K}$ wollen wir die Menge aller aus

0 und 1 konstruierbaren Zahlen bezeichnen.
Es gilt nun:
$\mathfrak{K}$ ist ein Unterkörper von $\mathbb{C}$. $\mathfrak{K}$ ist invariant unter der komplexen Konjugation $z \mapsto \overline{z}$.
Beweis. 1) $0, 1 \in \mathfrak{K}$,
2) Sind $z, w \in \mathfrak{K}$, so ist auch $z+w \in \mathfrak{K}$. Dazu sei $r = |z|, s = |w|$. Dies sind die Abstände von z und w zu 0. Der Kreis vom Radius r um w schneidet den Kreis vom Radius s um z im Punkt $z+w$ wie man analytisch verifizieren kann: $x = z+w$ erfüllt offensichtlich die Gleichungen $|x-z| = s, |x-w| = r$.
3) mit z ist auch $-z$ konstruierbar, den $-z$ ist ein Schnittpunkt des Kreises vom Radius $r = |z|$ um 0 mit der Verbindungsgeraden von 0 und z.
4) Ist $z \in \mathfrak{K}$, so ist auch $|z| \in \mathfrak{K}$, denn dies ist ja ein Schnittpunkt der Verbindungsgerade von 0 und 1 mit dem Kreis vom Radius $|z|$ um den Nullpunkt.
5) Ist $z \in \mathfrak{K}$, $z \neq 0$, so ist auch $\frac{z}{|z|} \in \mathfrak{K}$, denn dies ist ein Schnittpunkt des Einheitskreises um 0 mit der Verbindungsgeraden von 0 und z.
6) Sind $z, w \in \mathfrak{K}$, so ist auch $zw \in \mathfrak{K}$. *Beweis*. a) Sind z, w reell, so ist zw konstruierbar: i und iz sind konstruierbar. Die Parallele zur Verbindungsgeraden von i und w durch den Punkt iz (ist konstruierbar!) schneidet die reelle Achse in zw.
b) Sind nun $z, w \in \mathfrak{K}$ beliebig, so sind $\frac{z}{|z|}$, $\frac{w}{|w|}$ konstruierbar und offensichtlich auch $\frac{z}{|z|}\ \frac{w}{|w|}$(wie?) und somit auch $zw = (|z|\ |w|)\left(\frac{z}{|z|}\ \frac{w}{|w|}\right)$ (wie?).
7) Ist $z \in \mathfrak{K}$, so ist auch $\overline{z} \in \mathfrak{K}$. (warum?)
8) Ist $z \in \mathfrak{K} \setminus 0$, so ist $\frac{1}{|z|} \in \mathfrak{K}$ (Begründe!), also gilt auch $z^{-1} = \frac{1}{|z|^2}\,\overline{z} \in \mathfrak{K}$.
Wir werden im folgenden die Struktur von $\mathfrak{K}$ noch genauer untersuchen und auf diese Weise Antworten auf klassische Konstruierbarkeitsfragen erhalten (siehe Übungen zu Abschnitt 9).

■ Übungen 6

(6.1) Führen Sie die Beweisschritte 6)-8) in Beispiel 6.18 genau aus.

(6.2) Es seien m, n teilerfremde natürliche Zahlen. Zeigen Sie, dass die Ringe $\mathbb{Z}/mn\mathbb{Z}$ und $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ zueinander isomorph sind.

(6.3) Es sei p eine Primzahl und R ein kommutativer Ring, so dass $px = 0$ für alle $x \in R$. Zeigen Sie: Für alle $x, y \in R$, $n \in \mathbb{N}: x^{p^n} + y^{p^n} = (x+y)^{p^n}$

(6.4) Ist der Ring $\mathbb{C}[x, y]/\langle xy \rangle$ nullteilerfrei?

(6.5) Zeigen Sie: $S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in \mathbb{Z} \right\}$ ist ein Unterring von $M_2(\mathbb{Z})$. $I = \left\{ \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \middle| d \in \mathbb{Z} \right\}$ ist ein zweiseitiges Ideal in S und der Restklassenring S/I ist isomorph zum Produktring $\mathbb{Z} \times \mathbb{Z}$.

(6.6) Ein Element x eines Rings R heißt *nilpotent*, wenn es einen Exponenten $n > 0$ gibt, so dass $x^n = 0$. Zeigen Sie: Ist $x \in R$ nilpotent, so ist $1 - x$ eine Einheit in R.

(6.7) Schreibe $r = \frac{x^3}{x^2+1} \in \mathbb{C}(x)$ in der Form $p + \frac{a}{x+i} + \frac{b}{x-i}$ mit einem Polynom $p \in \mathbb{C}[x]$. Untersuche die zugehörige Abbildung auf der Riemannschen Zahlenkugel $S = \mathbb{C} \bigcup \infty$. Wieviele Urbildpunkte hat $w \in S$?

(6.8) a) Es seien R, S Ringe. Beweisen Sie: Die Einheitengruppe von $R \times S$ ist das direkte Produkt der Einheitengruppen $R^\times$ und $S^\times$.
b) Bestimmen Sie die Elementarteiler der Gruppen
$(\mathbb{Z}/12\,\mathbb{Z})^\times$, $(\mathbb{Z}/8\,\mathbb{Z})^\times$, $(\mathbb{Z}/7\,\mathbb{Z})^\times$.

(6.8) Beweisen Sie: $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$, $\mathbb{R}[x]/\langle x+1\rangle \cong \mathbb{R}$.

(6.9) Es sei R ein kommutativer Ring. x sei eine Unbestimmte. Eine unendliche Folge $(a_k)_{k\in\mathbb{N}}$ von Elementen $a_k \in R$ definiert eine sogenannte *formale Potenzreihe* $p = a_0 + a_1 x + a_2 x^2 + ... = \sum_{k=0}^{\infty} a_k x^k$. Mit $R[[x]]$ werde die Menge aller formalen Potenzreihen in x mit Koeffizienten in R bezeichnet.
a) Man führe Summe und Produkt formaler Potenzreihen ein (analog zu Polynomen) und zeige, dass $R[[x]]$ ein Ring ist, der den Polynomenring als echten Unterring enthält.
b) Zeigen Sie: $p = a_0 + a_1 x + a_2 x^2 + ...$ ist Einheit in $R[[x]]$, wenn a_0 Einheit in R ist.

(6.10) Es sei R ein kommutativer Ring und $e \in R\setminus\{0, 1\}$ mit $e^2 = e$. Es sei $e' = 1 - e$. Dann gilt auch $e'^2 = e'$, $e\,e' = e'\,e$, $R_1 = e\,R$, $R_2 = e'\,R$ sind echte Unterringe von R und es gilt R ist isomorph zum Produktring $R_1 \times R_2$.

7 Polynome und Ringerweiterungen

Inhalt: Erweiterungen von Ringen, Algebren, der Polynomenring $R[x]$, der kovarinte Funktor $S \mapsto V_S(M)$, der einer R-Algebra die Nullstellen in S eines fest gegebenen Systems M von Polynomen in $R[x]$ zuordnet. Einfache Erweiterungen $R[\alpha]$ mit Relationen, Beispiel $R[x]/\langle p\rangle$, p normiertes Polynom in $R[x]$, Divisionsalgorithmus, $K[x]$ ist Hauptidealring, das Minimalpolynom einer einfachen Ringerweiterung $K[\alpha]$. Polynome in n Unbestimmtem. Homogene Polynome, symmetrische Polynome.

■ Definition 7.1

(7.1.1) Es seien R, S kommutative Ringe. Ist R Unterring von S, so heißt S ein *Erweiterungsring* von R. Ist ein Ringhomorphismus

$$\gamma : R \longrightarrow S$$

gegeben, so heißt (S, γ) eine *R-Algebra*. γ heißt der *Strukturhomomorphismus* von *S*.
Ist $R \subset S$ eine Ringerweiterung, so ist *S* zusammen mit der Inklusionsabbildung $i : R \longrightarrow S$ als Strukturhomomorphismus eine *R*-Algebra. Im allgemeinen braucht aber der Strukturhomomorphismus $\gamma : R \longrightarrow S$ einer *R*-Algebra *S* nicht injektiv zu sein. In jedem Fall ist aber *S* ein Erweiterungsring von $\overline{R} = \gamma(R) \subset S$.

(7.1.2) Es seien S, T zwei Erweiterungsringe von *R*. Dann heißt ein Ringhomomorphismus $\varphi : S \longrightarrow T$ ein *R-Homomorphismus*, wenn φ den Unterring *R* festlässt, was gleichbedeutend ist zu $\varphi(a\,x) = a\,\varphi(x)$ für $a \in R,\ x \in S$.
Sind $(S, \gamma), (T, \delta)$ zwei *R*-Algebren, so heißt ein Ringhomomorphismus $\varphi : S \longrightarrow T$ ein *R-Homomorphismus*, wenn gilt $\delta \circ \varphi = \gamma$.
Mit $\mathrm{Hom}_R(S, T)$ wird die Menge der *R*-Homomorphismen von *S* nach *T* bezeichnet. Die *R*-Algebren bilden zusammen mit den *R*-Homomorphismen eine Kategorie, die wir mit $\mathcal{Alg}_R$ bezeichnen wollen.

(7.1.3) Eine Ringerweiterung $R \subset S$ heißt *einfach*, wenn es ein Element $\alpha \in S$ gibt, so dass $S = R[\alpha] = \{\sum_{k=0}^{n} a_k\,\alpha^k \mid a_k \in R\}$. α heißt dann *primitives Element* von *S* über *R*.
Entsprechend heißt eine *R*-Algebra (S, γ) einfach, wenn es ein Element $\alpha \in S$ gibt, so dass $S = R[\alpha] = \{\sum_{k=0}^{n} \gamma(a_k)\,\alpha^k \mid a_k \in R\}$. Auch hier heißt α *primitives Element* von *S* über *R*.

▪ Beispiel 7.2

(7.2.1) Der Polynomenring $R[x]$ in einer Unbestimmten *x* ist ein einfacher Erweiterungsring von *R*. Die Elemente aus *R* werden als Polynome vom Grad Null aufgefasst. Der Strukturhomomorphismus ist die Abbildung $a \mapsto a\,x^0$.

(7.2.2) Es sei (S, γ) eine *R*-Algebra und sei $\alpha \in S$. Dann kann man die einfache *R*-Algebra $R[\alpha] = \{\sum_{k=0}^{n} \gamma(a_k)\,\alpha^k \mid a_k \in R\}$ mit Strukturhomomorphismus $\gamma : R \longrightarrow R[\alpha]$ bilden. Die Inklusion $R[\alpha] \subset S$ ist ein *R*-Homomorphismus. Nach der universellen Eigenschaft des Polynomenrings gilt: Es gibt genau einen Ringhomomorphismus $\varphi : R[x] \longrightarrow R[\alpha]$ mit $\varphi(a) = \gamma(a)$ für $a \in R$ und $\varphi(x) = \alpha$. Für ein Polynom $p = \sum_{k=0}^{n} a_k\,x^k \in R[x]$ ist $\varphi(p) = \sum_{k=0}^{n} \varphi(a_k)\,\varphi(x)^k = \sum_{k=0}^{n} \gamma(a_k)\,\alpha^k$, wofür wir auch $p(\alpha)$ schreiben.

$$\varphi(p) = \sum_{k=0}^{n} \varphi(a_k)\,\varphi(x)^k = \sum_{k=0}^{n} \gamma(a_k)\,\alpha^k = p(\alpha).$$

φ heißt auch Einsetzungsabbildung. Die Unbekannte *x* wird durch das Ringelement α ersetzt und auf die Koeffizienten aus *R* wird der Strukturhomomorphismus angewendet. (siehe: Lineare Algebra, Abschnitt 14, Satz 14.15). Der Kern der Einsetzungsabbildung $I = \ker\varphi$ besteht somit aus allen Polynomen $p \in R[x]$, für die $p(\alpha) = 0$ gilt, die also α als *Nullstelle* besitzen. Man nennt die Elemente $p \in I$ auch

algebraische Relationen für α. Nach Konstruktion ist $I_0 := \ker\gamma = I \bigcap R$. Nach dem Homomorphiesatz ist $R/I_0 \cong \overline{R} = \gamma(R)$ und $\overline{R} \subset R[x]/I \cong R[\alpha]$. Der Isomorphismus identifiziert α mit der Restklasse $x + I$ von x.

Diese Überlegungen führen zu folgender Konstruktion:

- **Definition 7.3**

Es sei R ein kommutativer Ring mit Eins. Weiter sei $M \subset R[x]$ eine Menge von Polynomen.

(7.3.1) Für eine R-Algebra (S, γ) definiert man

$$V_S(M) := \{\alpha \in S \mid \forall\, p \in M : p(\alpha) = 0\}.$$

(7.3.2) Ist weiter $\varphi : S \longrightarrow T$ ein R-Homomorphismus (also $\varphi \circ \gamma = \delta$), so erhält man eine Abbildung

$$\varphi_* : V_S(M) \longrightarrow V_T(M)$$

mit $\varphi_*(\alpha) = \varphi(\alpha)$, denn für $p = \sum_{k=0}^{n} a_k x^k \in R[x]$ gilt: $p(\alpha) = 0 \Longrightarrow$
$\sum_{k=0}^{n} \gamma(a_k)\,\alpha^k = 0 \Longrightarrow \sum_{k=0}^{n} \delta(a_k)\,\varphi(\alpha)^k = \varphi(\sum_{k=0}^{n} \gamma(a_k)\,\alpha^k) = 0 \Longrightarrow p(\varphi(\alpha)) = 0.$

- **Lemma 7.4**

Die in Definition 7.3 definierte Zuordnung $S \mapsto V_S(M)$, $\varphi \mapsto \varphi_*$ ist ein *kovarianter Funktor* von der Kategorie $\mathcal{Alg}_R$ der R-Algebren in die Kategorie $\mathcal{Sets}$ der Mengen, d. h. es gelten die sogenannten *funktoriellen Eigenschaften*

(i) Für R-Homomorphismen $\varphi : S \longrightarrow T$, $\psi : T \longrightarrow U$ gilt: $(\psi \circ \varphi)_* = \psi_* \circ \varphi_*$.
(ii) Für alle R-Algebren S gilt: $(\mathrm{id}_S)_* = \mathrm{id}_{V_S(M)}$.

Beweis. Der Beweis ist evident. □

- **Satz 7.5**

Es sei R ein kommutativer Ring mit Eins. $M \subset R[x]$ sei eine Menge von Polynomen und $I = \langle M \rangle$ das von M erzeugte Ideal in $R[x]$. Es sei weiter

$$S = R[x]/I$$

und $\gamma : R \longrightarrow S$ sei die Komposition der natürlichen Inklusion $R \longrightarrow R[x]$ mit der Restklassenabbildung $\pi : R[x] \longrightarrow S$. Weiter sei

$$\alpha = \pi(x).$$

Dann ist $\alpha \in V_S(M)$ und für (S, α) gilt die folgende universelle Eigenschaft:
(7.5.1) Für jede R-Algebra T und jedes $\beta \in V_T(M)$ gibt es genau einen R-Homomorphismus $\varphi : S \longrightarrow T$ mit $\varphi(\alpha) = \beta$, mit anderen Worten: die Abbildung

$$\Phi_T : \mathrm{Hom}_R(S, T) \to V_T(M),\ \varphi \mapsto \varphi_*(\alpha)$$

ist bijektiv.

(S, α) heißt die von α erzeugte R-Algebra mit Relationen in M. Es gilt $S = R[\alpha]$, S besteht aus den polynomialen Ausdrücken $\sum_{k=0}^{n} \gamma(a_k)\, \alpha^k$ mit $a_k \in R$ und es gilt $p(\alpha) = 0$ für alle $p \in I$.
Man sagt auch: S ist durch *Adjunktion* eines Elementes α mit den Relationen $p(\alpha) = 0$, $p \in M$ entstanden.

(7.5.2) Man kann S genau dann als einfache Ringerweiterung von R auffassen, wenn $\gamma : R \longrightarrow S$ injektiv ist, wenn also das von den 'Relationen' $p \in M$ erzeugte Ideal I keine von Null verschiedenen 'Konstanten' enthält, d.h. wenn $I \bigcap R = 0$ gilt.
Ist R ein Körper, so ist die Strukturabbildung $\gamma : R \longrightarrow S$ stets injektiv.

Beweis. Wir zeigen zunächst, dass $\alpha \in V_S(M)$. Es sei dazu $p = \sum_{k=0}^{n} a_k\, x^k \in M$. Dann ist $p \in I$ und nach Definition von π gilt folglich $\pi(p) = 0$. Nun gilt aber $p(\alpha) = \sum_{k=0}^{n} \gamma(a_k)\, \alpha^k = \sum_{k=0}^{n} \pi(a_k)\, \pi(x)^k = \pi(\sum_{k=0}^{n} a_k\, x^k) = \pi(p)$ und somit $p(\alpha) = 0$, also $\alpha \in V_S(M)$.

Zu (7.5.1): Sei (T, δ) irgendeine R-Algebra. Wir betrachten die Abbildung
$\Phi_T : \mathrm{Hom}_R(S, T) \longrightarrow V_T(M),\ \varphi \mapsto \varphi_*(\alpha)$, von der Menge aller R-Abbildungen $\varphi : S \longrightarrow T$ in die Menge derjenigen Elemente $\beta \in T$, die Nullstellen von M sind. Da zwei R-Homomorphismen $S \longrightarrow T$ durch ihre Werte von α bestimmt sind, ist die Abbildung Φ_T injektiv. Zur Surjektivität von Φ_T: Sei $\beta \in V_T(M)$. Dann gibt es zunächst nach der universellen Eigenschaft des Polynomenrings genau einen R-Homomorphismus $\hat{\varphi} : R[x] \longrightarrow T$ mit $\hat{\varphi}(x) = \beta$. Dann ist $\hat{\varphi}(p) = p(\beta) = 0$ für $p \in M$. Da I das von M erzeugte Ideal ist, ist auch $\hat{\varphi}(p) = p(\beta) = 0$ für $p \in I$, denn: $p = \sum_{k=1}^{n} f_i\, p_i,\ p_i \in M \Longrightarrow \hat{\varphi}(p) = \sum_{k=1}^{n} \hat{\varphi}(f_i)\, \hat{\varphi}(p_i) = 0$. Also folgt $I \subset \ker \hat{\varphi}$. Nach der universellen Eigenschaft des Restklassenrings induziert $\hat{\varphi}$ somit einen R-Homomorphismus $\varphi : S = R[x]/I \longrightarrow T$ mit $\varphi \circ \pi = \hat{\varphi}$, also
$\varphi(\alpha) = \varphi(\pi(x)) = \hat{\varphi}(x) = \beta$. Damit ist die universelle Eigenschaft für (S, α) bewiesen.
Der Beweis von (7.5.2) ist evident. □

Wir wollen sehen, dass (S, α) durch die universelle Eigenschaft (7.5.1) bis auf kanonische Isomorphie eindeutig bestimmt ist (Dies ist ein abstraktes Argument, das generell bei universellen Konstruktionen anwendbar ist).
Es sei (S', α') eine weitere R-Algebra mit ausgezeichnetem Element $\alpha' \in V_{S'}(M)$, so dass die universelle Eigenschaft für (S', α') gilt:
Für jede R-Algebra T ist die Abbildung $\mathrm{Hom}_R(S', T) \longrightarrow V_T(M),\ \psi \mapsto \psi_*(\alpha')$ eine

Bijektion.
Wir finden insbesondere nach der universellen Eigenschaft für S bzw. S' Homomorphismen $\varphi : S \longrightarrow S'$ mit $\varphi_*(\alpha) = \alpha'$ und $\psi : S' \longrightarrow S$ mit $\psi_*(\alpha') = \alpha$. Da
$(\varphi \circ \psi)_*(\alpha') = \varphi_*(\psi_*(\alpha')) = \alpha' = \mathrm{id}_*(\alpha')$, $(\psi \circ \varphi)_*(\alpha) = \alpha = \mathrm{id}_*(\alpha)$
folgt nach der Eindeutigkeitsaussage in den universellen Eigenschaften $\varphi \circ \psi = \mathrm{id}$, $\psi \circ \varphi = \mathrm{id}$. φ ist also Isomorphismus mit $\varphi^{-1} = \psi$. □

- **Beispiel 7.6**

(7.6.1) Ist $R \subset S$ eine Ringerweiterung, $\alpha \in S$, so ist die in (7.2.2) betrachtete Erweiterung $R[\alpha] \subset S$ zusammen mit dem Element α die von α erzeugte Erweiterung von R mit Relationen in $I := \{p \in R[x] \mid p(\alpha) = 0\}$. Nach dem Homomorphisatz ist ja $R[\alpha] = R[x]/I$.
(7.6.2) Es sei $M = \{x^2 + 1\} \subset \mathbb{Z}[x]$. Das von M erzeugte Ideal $I = (x^2 + 1)\,\mathbb{Z}[x]$ schneidet $\mathbb{Z}$ nur in 0. Die einfache Erweiterung von $\mathbb{Z}$ mit der Relation $x^2 + 1$ ist nach dem Satz 7.5 der Restklassenring $\mathbb{Z}[x]/(x^2 + 1)\,\mathbb{Z}[x]$ mit dem ausgezeichneten Element $\alpha = x \bmod (x^2 + 1) = x + (x^2 + 1)\,\mathbb{Z}[x]$. Aber auch der Unterring $\mathbb{Z}[i] \subset \mathbb{C}$ mit dem ausgezeichneten Element i erfüllt die universelle Eigenschaft (7.5.1). Dazu muss man zeigen, dass der Kern des Einsetzungshomomorphismus $\mathbb{Z}[x] \longrightarrow \mathbb{Z}[i]$, $x \mapsto i$ aus den Vielfachen von $x^2 + 1$ besteht. Es gilt daher nach dem Homomorphiesatz
$\mathbb{Z}[x]/(x^2 + 1)\,\mathbb{Z}[x] \cong \mathbb{Z}[i]$, $\alpha \leftrightarrow i$.

(7.6.3) Die einfache Erweiterung von R mit Relationen in der Menge $M = \{0\}$ (also sozusagen ohne Relationen) ist der Polynomenring $R[x]$ in einer Unbestimmten x, denn $R[x]/\langle 0\rangle = R[x]$.

Wir behandeln einen wichtigen Spezialfall von 7.5.

- **Satz 7.7**

Es sei R ein kommutativer Ring mit Eins. Ist $p = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ ein *normiertes* Polynom in $R[x]$ vom Grad $n > 0$, so ist $R \cap \langle p\rangle = 0$ und es gibt eine einfache Erweiterung von R mit Relation p, nämlich $R[\alpha] = R[x]/p\,R[x]$, wobei $\alpha := x \bmod p$. Es gilt weiter:

(7.7.1) Jedes Element in $R[\alpha]$ besitzt eine eindeutig bestimmte Darstellung als Linearkombination von 1, α, $\ldots \alpha^{n-1}$ mit Koeffizienten in R. Wir schreiben dafür

$$R[\alpha] = R \oplus R\,\alpha \oplus R\,\alpha^2 \oplus \ldots \oplus R\,\alpha^{n-1}.$$

(7.7.2) Für jede R-Algebra S ist die Menge $\mathrm{Hom}_R(R[\alpha], S)$ der R-Homomorphismen von $R[\alpha]$ nach S in natürlicher eineindeutiger Beziehung zur Menge $V_S(P)$ der S-wertigen Nullstellen des Polynoms p.

Beweis. Zu (7.7.1): Da p normiert ist und $\text{grad}(p) = n > 0$, gilt für $a \in R[x]$: $a\,p \in R \Longrightarrow a = 0$. Also ist $R \cap \langle p\rangle = 0$. Damit haben wir $R \subset R[\alpha] = R[x]/\langle p\rangle$, wobei $\alpha = x \bmod p$ und $a \in R$ mit der Restklasse $a\,\alpha^0 \in R[\alpha]$ identifiziert wird. Es sei $V = R + R\,\alpha + ... + R\,\alpha^{n-1}$ die Menge aller polynomialen Ausdrücke $b_0 + b_1\,\alpha + ... + b_{n-1}\,\alpha^{n-1} \in R[\alpha]$, wobei $b_k \in R$. Da $p(\alpha) = 0$, ist
$\alpha^n = -(a_{n-1}\,\alpha^{n-1}. + ... + a_0) \in V$. Durch Induktion folgt, dass $\alpha^k \in V$ für alle $k \geq n$. Ist nämlich schon $\alpha^k = b_0 + b_1\,\alpha + ... + b_{n-1}\,\alpha^{n-1} \in V$ gezeigt, so gilt

$$\alpha^{k+1} = \alpha(b_0 + b_1\,\alpha + ... + b_{n-1}\,\alpha^{n-1}) = b_0\,\alpha + b_1\,\alpha^2 + ... + b_{n-1}\,\alpha^n =$$
$$b_0\,\alpha + b_1\,\alpha^2 + ...\, b_{n-2}\,\alpha^{n-1} - b_{n-1}(a_{n-1}\,\alpha^{n-1}. + ... + a_0) \in V.$$

Daraus folgt nun leicht: $R[\alpha] = V$. Jedes Element aus $R[\alpha]$ ist also eine R-Linearkombination von 1, α, ..., α^{n-1}. Wir zeigen, dass 1, α, ..., α^{n-1} R-linear unabhängig sind: Ist $b_{n-1}\,\alpha^{n-1} + ... + b_0 = 0$, so ist
$q := b_{n-1}\,x^{n-1} + ... + b_0 \in \langle p\rangle = \ker(\pi : R[x] \longrightarrow R[\alpha])$
im Kern der Restklassenabbildung, denn $\pi(q) = q(\alpha) = 0$. Damit folgt aus Gradgründen $q = 0$, denn ein Polynom vom Grad $< n$ kann nur Vielfaches von p sein, wenn es Null ist (beachte $\text{grad}(0) = -\infty$). Die Elemente 1, α, ... α^{n-1}sind also R-linear unabhängig. Folglich kann man jedes Element in $R[\alpha]$ eindeutig als R-Linearkombination von 1, α, ... α^{n-1} darstellen.
Zu (7.7.2): Das ist wegen (7.5.1) klar. □

■ Korollar 7.8

Es sei K ein Körper, $p \in K[x]$ ein normiertes Polynom vom Grad $n > 0$. Dann ist $K[\alpha] = K[x]/\langle p\rangle$, wobei $\alpha = x \bmod p$, ein n-dimensionaler K-Vektorraum und die Abbildung

$$K^n \longrightarrow K[\alpha],\ (b_0, b_1,\ ..., b_{n-1}) \mapsto b_0 + b_1\,\alpha\ ... + b_{n-1}\,\alpha^{n-1}$$

ist ein K-Vektorraumisomorphismus. Die Vektorraumstruktur von $K[\alpha]$ hängt nur von n ab. Die Ringstruktur auf $K[\alpha]$ ist dagegen komplizierter!

■ Beispiele 7.9

(7.9.1) $S = \mathbb{Z}[\alpha] = \mathbb{Z}[x]/\langle x^3 + 3x + 1\rangle$, $\alpha = x \bmod (x^3 + 3x + 1)$. Ist $\beta \in S$, so gibt es eindeutig bestimmte Zahlen $a, b, c \in \mathbb{Z}$ mit $\beta = a + b\,\alpha + c\,\alpha^2$. Es gilt die Relation $\alpha^3 = -3\,\alpha - 1$. Also ist zum Beispiel:
$(2 + \alpha - \alpha^2)(1 + \alpha) = 2 + 3\,\alpha - \alpha^3 = 3 + 6\,\alpha$.
Wenn man so will, hat man auf $\mathbb{Z}^3$ eine Ringstruktur:
$(a, b, c) \cdot (d, e, f) = (x, y, z)$, wenn
$(a + b\,\alpha + c\,\alpha^2)(d + e\,\alpha + f\,\alpha^2) = x + y\,\alpha + z\,\alpha^2$.

(7.9.2) $S = \mathbb{F}_5[\alpha] = \mathbb{F}_5[x]/\langle x^2 - 3\rangle$. Man adjungiert hier also eine formale Quadratwurzel von $3 \in \mathbb{F}_5$ zu $\mathbb{F}_5$. In $\mathbb{F}_5$ gilt

x	0	1	2	3	4
x^2	0	1	4	4	1

Also hat die Zahl 3 keine Quadratwurzel in $\mathbb{F}_5$.
Daher kann man das Polynom $x^2 - 3$ über dem Körper $\mathbb{F}_5$ *nicht* in Linearfaktoren zerlegen. Als Konsequenz ergibt sich, dass der Ring S ein Erweiterungskörper von $\mathbb{F}_5$ ist. Dazu ist zu beweisen, dass jedes von Null verschiedene Element in S eine Einheit ist. Wir werden später ein allgemeines Argument kennenlernen. Versuchen wir jedoch hier dies ad hoc zu beweisen. Es sei $(a, b) \in \mathbb{F}_5{}^2 \setminus \{(0, 0)\}$ gegeben. Wir suchen $x, y \in \mathbb{F}_5$, so dass $(a + b\alpha)(x + y\alpha) = 1$, d.h. wegen $\alpha^2 = 3$

$$a x + 3 b y = 1$$
$$b x + a y = 0.$$

$A = \begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$ ist die Matrix dieses inhomogenen linearen Gleichungssystems. Es gilt $\det A = a^2 - 3b^2 \neq 0$ in $\mathbb{F}_5$., denn es gibt ja keine Quadratwurzel von 3 in $\mathbb{F}_5$. Damit gibt es eine Lösung (x, y), d.h. $a + b\alpha$ ist eine Einheit S. Man erhält auch sofort eine Formel für das Inverse:

$$(a + b\alpha)^{-1} = \tfrac{a - b\alpha}{a^2 - 3b^2}.$$

Wir haben damit insbesondere einen Körper mit 25 Elementen gefunden.

(7.9.3) Wir wiederholen die Betrachtung mit der Primzahl 11 an Stelle von 5.
(Bemerkung: Nach Gauß ist es ganz einfach zu prüfen, ob 3 Quadratzahl modulo einer Primzahl p ist: Die Gleichung $x^2 = 3$ ist im Körper $\mathbb{F}_p$ genau dann lösbar, wenn $p \equiv \pm 1 \bmod 12$ gilt. Das ist ein einfacher Spezialfall des sogenannten *Quadratischen Reziprozitätsgesetzes,* welches Gauß im Alter von 19 Jahren bewiesen hat.)
3 ist eine Quadratzahl in $\mathbb{F}_{11}$ und zwar ist $(\pm 5)^2 = 3$ in $\mathbb{F}_{11}$. Jetzt ist $x^2 - 3 = (x - 5)(x + 5)$ in $\mathbb{F}_{11}[x]$ und somit folgt
$S := \mathbb{F}_{11}[\alpha] = \mathbb{F}_{11}[x]/\langle x^2 - 3\rangle = \mathbb{F}_{11}[x]/\langle (x - 5)(x + 5)\rangle$ und somit sind $\alpha - 5$ und $\alpha + 5$ Nullteiler, denn $(\alpha + 5)(\alpha - 5) = 0$, S ist insbesondere kein Körper. S besteht sozusagen aus zwei Kopien von $\mathbb{F}_{11}$. Gemeint ist folgendes:
Die Diagonalabbildung
$S \longrightarrow S/\langle \alpha - 5\rangle \times S/\langle \alpha + 5\rangle,\ \beta \mapsto (\beta \bmod (\alpha - 5),\ \beta \bmod (\alpha + 5))$
definiert einen Isomorphismus von S in den Produktring, denn erstens ist diese Abbildung injektiv und zweitens ist jeder
Faktor $S/\langle \alpha \pm 5\rangle \cong \mathbb{F}_{11}[x]/\langle x \pm 5\rangle \cong \mathbb{F}_{11}$
isomorph zu $\mathbb{F}_{11}$. Da $b\alpha + a = b(\alpha \pm 5) + (\mp 5b + a)$, ist der Isomorphismus $\varphi : S \longrightarrow \mathbb{F}_{11} \times \mathbb{F}_{11}$ durch $\varphi(a + b\alpha) = (a + 5b,\ a - 5b)$ gegeben.

(7.9.4) Für die Primzahl $p = 2$ tritt ein neues Phänomen auf.
$S = \mathbb{F}_2[x] / \langle x^2 + 1 \rangle = \mathbb{F}_2[x] / \langle (x+1)^2 \rangle$ ist weder ein Körper noch das Produkt zweier Körper, sondern von der Form $S = \{a + b\ \alpha \mid a, b \in \mathbb{F}_2\}$, $\alpha^2 = 0$. α ist ein nilpotentes Element von S.

Wir beweisen jetzt die folgende allgemeine Variante der 'Polynomdivision mit Rest'.

- **Satz 7.10 (Divisionsalgorithmus)**

Es sei R ein kommutativer Ring. Es sei $g = a_n x^n + a_{n-1} x^{n-1} + ... + a_0 \in R[x]$ und a_n sei Einheit in R. Dann gilt: Zu jedem $f \in R[x]$ gibt es eindeutig bestimmte Polynome $q, r \in R[x]$, so dass $f = q g + r$ und $\text{grad}(r) < n$.

Beweis. Der Beweis geht genauso wie im Fall, dass R ein Körper ist, weil wir a_n als Einheit vorausgesetzt haben (siehe: Vorlesung 'Lineare Algebra'). Wir führen den Beweis durch:
Es sei $f = b_m x^m + ... b_0,\ b_m \neq 0$. Wir beweisen die Aussage durch Induktion nach m.
1) $m = 0$: Ist $n > 0$, so kann man $q = 0$ und $r = f$ wählen. Ist $n = 0$ so wähle man $q = b_0 a_0^{-1}$, $r = 0$.
2) $m - 1 \to m$: Ohne Einschränkung sei $m \geq n$. Es folgt: $\hat{f} := f - a_n b_m^{-1} x^{m-n} g$ ist vom Grad kleiner als m. Nach Induktionsvoraussetzung gibt es also $\hat{q}, \hat{r}$ mit $\hat{f} = \hat{q} g + \hat{r}$ und $\text{grad}(\hat{r}) < n$. Mit $q = \hat{q} + a_n b_m^{-1} x^{m-n}$, $r = \hat{r}$ haben wir dann $f = q g + r$ und $\text{grad}(r) < n$.
Zur Eindeutigkeit der Darstellung führen wir wieder Gradgründe wie im Beweis von 7.7 ins Feld. □

Wir können den Divisionsalgorithmus verwenden, um den Restklassenring $R[\alpha] = R[x] / \langle g \rangle$ zu untersuchen. g soll dabei normiert sein. Es ergibt sich ein neuer Beweis für Satz 7.7. Aufgrund des Divisionsalgorithmus ist nämlich die Einschränkung der Restklassenabbildung $\pi : R[x] \longrightarrow R[x] / \langle g \rangle$ auf die additive Untergruppe aller Polynome $r \in R[x]$ vom Grad kleiner als n eine Bijektion, was bedeutet, dass das Element $\pi(f) \in R[x] / \langle g \rangle$ eindeutig durch den Rest r beim Teilen von f durch g beschrieben ist. Der Rest r kann durch den Divisionsalgorithmus ermittelt werden.

- **Beispiel 7.11**

Es sei $R = \mathbb{Z}[\alpha] = \mathbb{Z}[x] / \langle x^3 - x + 1 \rangle$. Jedes Element $\beta \in R$ lässt sich als ganzzahlige Linearkombination von $1, \alpha, \alpha^2$ schreiben. Beispiel $\beta = 7\alpha^4 - 3$. Um β als ganzzahlige Linearkombination von $1, \alpha, \alpha^2$ zu bekommen, teilt man das Polynom $f = 7x^4 - 3$ (mit $f(\alpha) = \beta$) mit Rest durch $g = x^3 - x + 1$:

$$7x^4 - 3 \quad : \; x^3 - x + 1 \; = \; 7x \;\; \text{Rest} = 7x^2 - 7x - 3$$
$$7x^4 - 7x^2 + 7x$$
$$7x^2 - 7x - 3$$

Damit gilt $\beta = 7\alpha^2 - 7\alpha - 3$ ist die gesuchte Darstellung von β als Linearkombination von 1, α, α^2

- **Definition 7.12**

Es sei R ein kommutativer Ring. Ein Ideal I in R heißt *Hauptideal*, wenn $I = \langle a \rangle$ für ein $a \in R$. Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*.

Aus dem Divisionsalgorithmus folgt

- **Lemma 7.13**

Es sei K ein Körper und x eine Unbestimmte. Dann ist $K[x]$ ein Hauptidealring. Für jedes Ideal $I \subset K[x]$ gibt es ein eindeutig bestimmtes normiertes Polynom $g \in K[x]$ mit $I = \langle g \rangle$.

Beweis. Es sei $I \subset K[x]$ ein von Null verschiedenes Ideal. Es sei $g \in I \backslash 0$ ein Polynom minimalen Grades. Da K ein Körper ist, können wir g als normiert annehmen. Dann gilt $I = \langle g \rangle$. Ist nämlich $f \in I$, so schreiben wir $f = qg + r$ mit $\text{grad}(r) < \text{grad}(g)$. Es folgt $r = f - qg \in I$ und nach Wahl von g ist somit $r = 0$ und damit $f \in \langle g \rangle$. □

- **Korollar und Definition 7.14**

Es sei K ein Körper und A eine K-Algebra (A darf hier auch nicht-kommutativ sein). Es sei $\alpha \in A$ und $S = K[\alpha]$. Dann ist entweder $K[\alpha] \cong K[x]$ oder es gibt genau ein normiertes Polynom kleinsten Grades $g \in K[x]$, so dass $g(\alpha) = 0$. Es gilt dann $K[x]/\langle g \rangle \cong S$. g heißt das *Minimalpolynom* von α. Das Element α heißt in diesem Fall *algebraisch* über K.

Beweis. Die Einsetzungsabbildung $\pi : K[x] \longrightarrow S$, $x \mapsto \alpha$, die auf K die Identität ist, ist surjektiv und hat nach 7.9 ein Hauptideal, sagen wir $\langle g \rangle$, als Kern. Nach dem Homomorphiesatz wird also die Isomorphie $K[x]/\langle g \rangle \cong S$ induziert. Ist $g = 0$, so ist $K[\alpha]$ isomorph zum Polynomenring $K[x]$. Ist $g \neq 0$, so können wir g normiert wählen, g ist dann eindeutig bestimmt und hat natürlich den kleinsten Grad unter allen Polynomen mit Nullstelle α. □

■ **Satz und Definition 7.15**

Es sei R ein Integritätsbereich. Es sei $f \in R[x] \backslash 0$, $a \in R$. Dann gilt:

(7.15.1) Ist $f(a) = 0$, so ist $x - a$ ein Teiler von f in $R[x]$.

(7.15.2) a heißt *k-fache Nullstelle* von f, wenn $(x-a)^k$ ein Teiler von f ist, aber $(x-a)^{k+1}$ nicht, d.h. wenn $f = (x-a)^k\, q$ mit $q \in R[x]$ und $q(a) \neq 0$ gilt. Man schreibt auch $v_a(f) = k$, wenn a eine k-fache Nullstelle von f ist.

(7.15.3) Es seien $a_1, \ldots, a_r$ Nullstellen von f mit den Vielfachheiten $v_{a_i}(f) = k_i$. Dann gibt es ein $q \in R[x]$ mit $f = (x-a_1)^{k_1} \ldots (x-a_r)^{k_r}\, q$ und $q(a_i) \neq 0$ für i = 1, ..., r.
Insbesondere ist $k_1 + \ldots + k_r \leq \operatorname{grad}(f)$.

(7.15.4) Ein Polynom f vom Grad n mit Koeffizienten in einem Integritätsbereich R besitzt mit Vielfachheiten gezählt höchstens n Nullstellen in R.

Beweis. Zu (7.15.1): Nach dem Divisionsalgorithmus kann man schreiben: $f = q \cdot (x-a) + r$, $\operatorname{grad}(r) < 1$. Es folgt: $0 = f(a) = q(a)\,(a-a) + r$, also $r = 0$.
Zu (7.15.2): Nach Voraussetzung können wir schreiben:
$(x-a)^k\, q = f = (x-a)^{k+1}\, q_1 + r$, $\operatorname{grad}(r) \leq k$, $q, q_1, r \in R[x]$, $r \neq 0$.
Da $r = (x-a)^k\,(q - (x-a)\, q_1)$, ist also $s := q - (x-a)\, q_1$ ein von Null verschiedenes konstantes Polynom. Damit folgt $q(a) = s \neq 0$.
Zu (7.15.3): Induktion nach r: Für $r = 1$ ist die Aussage in (7.13.2) gezeigt worden. Wir führen den Induktionsschluss $r - 1 \to r$ durch: Nach Induktionsvoraussetzung ist $f = (x-a_1)^{k_1} \ldots (x-a_{r-1})^{k_{r-1}}\, g$ und $g(a_i) \neq 0$ für i = 1, ..., $r - 1$.
Behauptung: g hat a_r als k_r-fache Nullstelle.
Beweis: Da $f(a_r) = 0$ und $a_i \neq a_r$ für $i = 1, \ldots, r-1$, gilt $g(a_r) = 0$. Es gilt dann $f = (x-a_r)\,\tilde{f}$ und auch $g = (x-a_r)\,\tilde{g}$. Da der Polynomenring $R[x]$ nullteilerfrei ist, folgt durch Kürzen aus der Gleichung $f = (x-a_1)^{k_1} \ldots (x-a_{r-1})^{k_{r-1}}\, g$ die Gleichung $\tilde{f} = (x-a_1)^{k_1} \ldots (x-a_{r-1})^{k_{r-1}}\, \tilde{g}$.
Induktiv ergibt sich die Behauptung. Also ist $g = (x-a_r)^{k_r}\, q$ und $q(a_r) \neq 0$. (7.15.3) ist bewiesen. □

■ **Bemerkung 7.16**

(7.16.1) Im Beweis der Aussage (7.15.3) wurde wesentlich benutzt, dass R nullteilerfrei ist, wie Beispiel (7.16.2) zeigt. Es wurde aber nicht der Satz von der eindeutigen Primfaktorzerlegung in $R[x]$ benutzt, der ja auch gar nicht gilt, wenn er nicht in R gilt, der aber stets in $K[x]$ gilt, wobei K Quotientenkörper von R. Dies wird im nächsten Abschnitt untersucht.
(7.16.2) Es sei $R = \mathbb{Z}/8\mathbb{Z}$. R ist nicht nullteilerfrei, denn $2 \cdot 4 \equiv 0 \bmod 8$. Das Polynom $x^3 \in R[x]$ hat *mehr* als drei Nullstellen in R, nämlich 0, 2, 4, 6.

a	0	1	2	3	4	5	6	7
$a^3 \bmod 8$	0	1	0	3	0	5	0	7

In $R[x]$ gilt $(x-2)(x-4) = x^2 - 6x + 8 = x(x-6)$,
$x^3 = x(x-4)^2 = (x-6)^2(x-2)$. Die Aussage (7.15.3) ist hier falsch! (7.15.1) gilt aber, wie die Gleichungen zeigen.

Die Gleichheit von Polynomen über einem Integritätsbereich kann man, wenn der Ring genügend viele Elemente enthält auch folgendermaßen testen.

- **Korollar 7.17**

Es sei R ein Integritätsbereich. Es sei $f, g \in R[x]$ seien Polynome vom Grad $\leq n$. Es gebe $n+1$ verschiedene Elemente $a_1, \ldots, a_{n+1}$ in R, so dass $f(a_i) = g(a_i)$ für $i = 1, \ldots, n+1$. Dann gilt $f = g$. □

Dieser Satz bedeutet folgendes: Ist $|R| = n$, so kann man Polynome $p \in R[x]$ vom Grad kleiner als n mit den von ihnen definierten Polynomfunktionen $R \longrightarrow R, a \mapsto p(a)$ identifizieren. Insbesondere sind im Falle unendlicher Integritätsbereiche Polynome und Polynomfunktionen im wesentlichen dasselbe.

Wir kommen nun zu Polynomenringen in mehreren Unbestimmten.

- **Definition 7.18**

Es sei R ein kommutativer Ring, $x_1, \ldots, x_n$ seien Unbestimmte. Dann definieren wir den *Polynomenring* $R[x_1, \ldots, x_n]$ in n Unbestimmtem rekursiv durch $R[x_1, x_2] := R[x_1][x_2]$, $R[x_1, x_2, x_3] = R[x_1, x_2][x_3]$, ...,
$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$.
(7.18.1) Man kann ein Polynom

$$f = \sum_{k=0}^{d} f_k {x_n}^k$$

mit $f_k \in R[x_1, \ldots, x_{n-1}]$ auch als R-Linearkombination von *Monomen* $x^i := {x_1}^{i_1} \ldots {x_n}^{i_n}$ schreiben. Ist etwa

$$f_k = \sum_{i_1,\ldots,i_{n-1}=0}^{m} a_{i_1,\ldots,i_{n-1},k} {x_1}^{i_1} \ldots {x_{n-1}}^{i_{n-1}},$$

so folgt

$$f = \sum_{k=0}^{d} \sum_{i_1,\ldots,i_{n-1}=0}^{m} a_{i_1,\ldots,i_{n-1},k} {x_1}^{i_1} \ldots {x_{n-1}}^{i_{n-1}} {x_n}^k = \sum_i a_i x^i,$$

wobei in der letzten Summe über die Multiindizes $i = (i_1, \ldots, i_n)$ summiert wird und $x^i = {x_1}^{i_1} \ldots {x_n}^{i_n}$ gesetzt wird.

(7.18.2) Ein Polynom $f \in R[x_1, \ldots, x_n]$ ist eindeutig durch seine sogenannte *Koeffizientenfolge* $(a_i)_{i \in \mathbb{N}^n}$ beschrieben. Dabei sind nur solche Koeffizientenfolgen

zulässig, für die $a_i \neq 0$ nur für endlich viele Multiindizes i gilt.
Es ergibt sich mit den obigen Bezeichnungen durch Induktion nach n:
$f = 0 \Longleftrightarrow (\forall\, k : f_k = 0) \Longleftrightarrow (\forall\, k\ \forall\, i \in \mathbb{N}^{n-1} : a_{i,k} = 0) \Longleftrightarrow (\forall\, i \in \mathbb{N}^n : a_i = 0)$.

(7.18.3) Der *Totalgrad* eines Monoms $x^i = {x_1}^{i_1} \ldots {x_n}^{i_n}$ wird definiert als $|i| := i_1 + \ldots + i_n$. Man kann damit die Terme eines Polynoms auch nach dem Totalgrad ordnen: $f = f_0 + f_1 + \ldots + f_d$, wobei $f_k := \sum_{|i|=k} a_i x^i$. Ist $f_d \neq 0$, so heißt d der Grad $\mathrm{grad}(f)$ von f. Man setzt $\mathrm{grad}(0) := -\infty$. Die Terme f_k heißen die *homogenen Bestandteile von f.* Ein Polynom heißt *homogen* vom Grad k, wenn alle seine Monome denselben Totalgrad k haben. Die homogenen Polynome vom Grad 0 sind die Elemente in R. $R[x_1, \ldots, x_n]$ ist ein Erweiterungring von R. Homogene Polynome vom Grad 1 nennt man auch *Linearformen*. Homogene Polynome vom Grad 2 heißen *quadratische Formen* (vgl Vorlesung 'Lineare Algebra'). Homogene Polynome vom Grad 3 nennt man auch *kubische Formen.*

- **Lemma 7.19**

Ist R ein Integritätsbereich, so ist auch $R[x_1, \ldots, x_n]$ ein Integritätsbereich.
Für $f, g \in R[x_1, \ldots, x_n]$ gilt: $\mathrm{grad}(f\,g) = \mathrm{grad}(f) + \mathrm{grad}(g)$.

Beweis. Induktion nach n. Für $n = 1$ haben wir das schon in der Vorlesung 'Lineare Algebra' Abschnitt 14 bewiesen. Der Induktionsschluss ist damit wegen der rekursiven Definition $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ klar. Die Formel für den Grad erhält man folgendermaßen: Wir zerlegen f und g in ihre homogenen Bestandteile: $f = f_0 + f_1 + \ldots + f_d$, $g = g_0 + \ldots + g_e$, $f_d \neq 0$, $g_e \neq 0$. Dann ist offensichtlich $h_k = \sum_{i+j=k} f_i\, g_j$ der homogene Bestandteil vom Grad k von $g\,f$. Der höchste auftretende Bestandteil ist $h_{d+e} = f_d\, g_e$. Da $R[x_1, \ldots, x_n]$ nullteilerfrei ist, ist $h_{d+e} \neq 0$, also $\mathrm{grad}(f\,g) = d + e = \mathrm{grad}(f) + \mathrm{grad}(g)$. □

- **Lemma 7.20 (universelle Eigenschaft von $R[x_1, \ldots, x_n]$)**

Es seien R, S kommutative Ringe. $x_1, \ldots, x_n$ seien Unbestimmte. Weiter seien $s_1, \ldots, s_n$ irgendwelche Elemente aus S. $\varphi : R \longrightarrow S$ sei ein Ringhomomorphismus. Dann gibt es genau einen Ringhomomorphismus $\varphi : R[x_1, \ldots, x_n] \longrightarrow S$, der $\varphi : R \longrightarrow S$ fortsetzt und der x_i auf s_i abbildet.

Beweis. Für $n = 1$ ist der Satz bekannt (Einsetzungshomomorphismus). Duch Induktion folgt leicht die allgemeine Aussage.
Man kann die Aussage des Lemmas auch so formulieren: Ist S eine R-Algebra, so gibt es eine kanonische Bijektion

$$\mathrm{Hom}_R(R[x_1, \ldots, x_n], S) \longrightarrow S^n,\ \varphi \mapsto (\varphi(x_1), \ldots, \varphi(x_n)).$$

□

■ **Korollar 7.21**

Es sei R ein kommutativer Ring. $x_1, \ldots, x_n$ seien Unbestimmte. Die R-Homomorphismen (also Ringhomomorphismen, die auf R die Identität sind) von $R[x_1, \ldots, x_n]$ in sich entsprechen eineindeutig den n-Tupeln $(f_1, \ldots, f_n)$ von Polynomen $f_i \in R[x_1, \ldots, x_n]$. $(f_1, \ldots, f_n)$ definiert den Homomorphismus $\varphi(f) = f(f_1, \ldots, f_n)$ (Einsetzungshomomorphismus: für x_i wird f_i eingesetzt). □

■ **Definition 7.22**

Die symmetrische Gruppe S_n operiert von links auf $R[x_1, \ldots, x_n]$ durch

$$(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).$$

Es gilt nämlich

$$((\sigma \circ \tau) f)(x_1, \ldots, x_n) = f(x_{\tau^{-1}(\sigma^{-1}(1))}, \ldots, x_{\tau^{-1}(\sigma^{-1}(n))}) =$$
$$(\tau f)(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}) = (\sigma(\tau f))(x_1, \ldots, x_n).$$

Dabei ist $\Phi_\sigma : f \mapsto \sigma f$ ein Ringisomorphismus, der auf R die Identität ist. Nach der universellen Eigenschaft ist Φ_σ durch die Bedingung

$$x_i \mapsto x_{\sigma^{-1}(i)}$$

vollständig bestimmt. Die *Invarianten* (d. h. die 'Fixpunkte') unter dieser Operation heißen *symmetrische Polynome* in $x_1, \ldots, x_n$.

Die *elementarsymmetrischen* Polynome $\sigma_i(x_1, \ldots, x_n)$ sind durch die Identität

$$t^n + \sigma_1 t^{n-1} + \sigma_2 t^{n-2} + \ldots + \sigma_{n-1} t + \sigma_n = (t + x_1)(t + x_2) \ldots (t + x_n)$$

definiert. Es gilt also

$$\sigma_1 = \sum_{k=1}^{n} x_k$$
$$\sigma_2 = \sum_{k<m} x_k x_m$$
$$\vdots$$
$$\sigma_n = x_1 x_2 \ldots x_n$$

Wir zitieren ohne Beweis den schönen und wichtigen Satz (für einen Beweis siehe van der Waerden [2])

- **Satz 7.23 (Hauptsatz über symmetrische Polynome)**

  Die Menge S der symmetrischen Polynome ist ein Unterring von $R[x_1, ..., x_n]$ mit $R \subset S$. Dieser Unterring wird von R und den elementarsymmetrischen Polynomen $\sigma_1, ..., \sigma_n$ erzeugt: $S = R[\sigma_1, ..., \sigma_n]$.

Übungen 7

(7.1) Es sei $R = \mathbb{Z}[x] / \langle x^3 + 5x^2 - 7 \rangle$, $\alpha := x \bmod (x^3 + 5x^2 - 7) \in R$ die Restklasse von x. Stellen sie die folgenden Elemente als $\mathbb{Z}$-Linearkombination von 1, α, α^2 dar.
a) $\alpha^5 - \alpha^4 - \alpha + 2$, b) α^6, c) $(\alpha^4 - 1)^2$.

(7.2) Es sei $R = \mathbb{Z}[x] / \langle 2, x^2 + x + 1 \rangle$. Zeigen Sie, dass R ein Körper mit vier Elementen ist. Hinweis: Benutzen Sie den Entsprechungssatz 6.12 mit $I_0 = \langle 2 \rangle \subset I = \langle 2, x^2 + x + 1 \rangle$ und dann Satz 7.5.

(7.3) Untersuche, ob der Ring $\mathbb{F}_3[x] / \langle x^3 + x^2 + 1 \rangle$ Nullteiler besitzt.

(7.4) Zeigen Sie $\mathbb{C}[x, y] / \langle x^2 + y^2, y - 1 \rangle \cong \mathbb{C} \times \mathbb{C}$. Wie steht es mit $\mathbb{R}[x, y] / \langle x^2 + y^2, y - 1 \rangle$?

(7.5) Bestimmen sie den Restklassenring $R[x_1, ..., x_n] / \langle x_1, ..., x_k \rangle$.

(7.6) Konstruieren sie einen Erweiterungsring von $\mathbb{R}$, in dem ein Element α liegt mit der Relation $\alpha^3 + 2 = 0$. Gibt es mehrere? Hinweis: Studieren Sie die universelle Eigenschaft in Satz 5.5.

(7.7) Zeigen Sie: $\langle x, y \rangle$ ist kein Hauptideal in $\mathbb{C}[x, y]$.
b) $\langle 3, 1 - \sqrt{-5} \rangle$ ist kein Hauptideal in $\mathbb{Z}[\sqrt{-5}]$.

(7.8) Bestimmen Sie die Nullstellen von $x^5 - x^3$in $R = \mathbb{Z} / 8\mathbb{Z}$. Teilen Sie $x^5 - x^3$ durch $x - a$, wobei a eine Nullstelle von $x^5 - x^3$ sei.

(7.9) Erarbeiten Sie einen Beweis (siehe [2]) des Hauptsatzes über symmetrische Polynome.

(7.10) Es sei a_n die Anzahl der möglichen Klammerungen eines Produktes aus n Faktoren in jeweils zwei Faktoren: $a_1 = 1$, $a_2 = 1$, $a_3 = 2$, $a_4 = 5$,...

a				
$x = a\,a$				
$y = a(a\,a)$	$z = (a\,a)\,a$			
$a\,y = a(a(a\,a))$	$a\,z = a((a\,a)\,a)$	$x\,x = (a\,a)\,(a\,a)$	$y\,a = (a(a\,a))\,a$	$z\,a = ((a\,a)\,a)\,a$

a) Beweisen Sie die Rekursionsformel $a_n = a_1 a_{n-1} + a_2 a_{n-2} + ... + a_{n-1} a_1$.
b) Folgern Sie für die formale Potenzreihe $p := \sum_{k=1}^{\infty} a_k t^k \in \mathbb{Z}[[t]]$ die Relation $p^2 = p - t$. p heißt die erzeugende Funktion der Folge (a_n).
c) Zeigen Sie, dass p die Taylorreihe von $f(t) = \frac{1}{2}\left(1 - \sqrt{1-4t}\right)$ um den Nullpunkt ist.
d) Mit der Binomialentwicklung von $(1-4t)^{\frac{1}{2}}$ (siehe etwa: Forster, Analysis 1) schließe man $a_n = \frac{1}{n}\binom{2n-2}{n-1}$.

(7.11) a) Bestimmen sie das Minimalpolynom von $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{R}$ über $\mathbb{Q}$.
b) Es sei $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \in M_3(\mathbb{Q})$. Bestimmen sie das Minimalpolynom von A über $\mathbb{Q}$.

8 Faktorielle Ringe

Inhalt: Teilbarkeit, irreduzibele Elemente in Integritätsbereichen, Primelemente, faktorielle Ringe. Gauß-Lemma, Satz: Hauptidealringe sind faktoriell, Satz: Ist R faktoriell, so ist auch $R[X]$ faktoriell, Irreduzibilitätskriterium von Eisenstein. Beispiele für faktorielle und nicht faktorielle Ringe.

In diesem Abschnitt sei R stets ein Integritätsbereich, es sei denn, es wird ausdrücklich etwas anderes gesagt.

- **Definition 8.1**

Es seien $a, b \in R$.

(8.1.1) *a teilt b* (kurz: $a \mid b$), wenn ein $c \in R$ existiert, so dass $b = a\,c$. kurz: wenn $b \in \langle a \rangle$, d.h. wenn $\langle b \rangle \subset \langle a \rangle$.

(8.1.2) a ist *assoziiert* zu b, wenn $\langle b \rangle = \langle a \rangle$, wenn also eine Einheit $u \in R$ existiert mit $b = u\,a$.

(8.1.3) a ist *echter Teiler* von b, wenn $\langle b \rangle \subset_{\neq} \langle a \rangle \neq \langle 1 \rangle$, wenn also a Nichteinheit ist und eine Nichteinheit c existiert, so dass $b = a\,c$.

(8.1.4) a heißt *irreduzibel in R*, wenn $a \neq 0$, $\langle a \rangle \neq R$ und wenn a keine echten Teiler besitzt, wenn also a eine von Null verschiedene Nichteinheit ist und nicht als Produkt zweier Nichteinheiten $b, c \in R$ geschreiben werden kann.

Es sei $a \neq 0$ eine Nichteinheit in R. a sei nicht irreduzibel, also *reduzibel*. Ist nun b_1 ein echter Teiler von a, so gibt es eine Nichteinheit a_1, so dass $a = b_1 a_1$. Ist a_1 oder

b_1 nicht irreduzibel, so kann man a weiter zerlegen. Sei etwa a_1 reduzibel. Man findet dann Nichteinheiten a_2, b_2 so dass $a_1 = b_2 a_2$. Es gilt dann $a = b_1 b_2 a_2$. Ein Tupel $(a_1, ..., a_k)$ von Nichteinheiten a_i in R heißt eine *Zerlegung* von a, wenn $a = a_1 ... a_k$ gilt. Diese Zerlegung ist zum Beispiel eine Verfeinerung von $(a_1, ..., a_{k-2}, a_{k-1} \cdot a_k)$. Zwei Zerlegungen $(a_1, ..., a_k)$, $(b_1, ..., b_k)$ von a heißen äquivalent, wenn es ein Permutation $\pi \in S_k$ und Einheiten $e_i \in R$ gibt, so dass $b_{\pi(i)} = e_i a_i$ für $i = 1, ..., k$ gilt. Äquivalente Zerlegungen unterschieden sich nur in der Reihenfolge der Faktoren und sich entsprechende Faktoren unterscheiden sich nur um eine Einheit. Wir betrachten die Menge $\mathcal{Z}(a)$ der (Äquivalenzklassen von) Zerlegungen von a. Diese Menge ist geordnet. Die Ordnung wird von der folgenden Relation erzeugt: Die Zerlegung $(a_1, ..., a_k)$ ist einfache Verfeinerung der Zerlegung $(b_1, ..., b_{k-1})$, wenn $(a_1, ..., a_k)$ aus $(b_1, ..., b_{k-1})$ dadurch entsteht, dass ein Faktor b_i in zwei Nichteinheiten zerlegt wird. Die Zerlegung $z_2 = (a_1, ..., a_k)$ ist *feiner* als Zerlegung $z_1 = (b_1, ..., b_m)$, (in Zeichen: $z_1 \succ z_2$) wenn $(a_1, ..., a_k)$ durch eine Kette von $k - m$ einfachen Verfeinerungen aus $(b_1, ..., b_m)$ entsteht. Ziel ist es nun durch sukzessives Zerlegen von a zu einer Zerlegung $a = a_1 ... a_k$ in irreduzible Faktoren a_i zu gelangen. Die Klasse von $(a_1, ..., a_k)$ ist dann minimal in der Menge $\mathcal{Z}(a)$. Wir sagen: Eine absteigende Folge $(z_1 \succ z_2 \succ ...)$ von Zerlegungen $z_i = (a_{i,1}, ..., a_{i,i})$ von a wird stationär, wenn sie bei einer Zerlegung z_k abbricht. Ist z_k minimal in $\mathcal{Z}(a)$, so ist z_k eine Zerlegung von a in irreduzible Faktoren. Ist die Folge nicht stationär, so kann man die Zerlegung von a ad infinitum fortsetzen. Man muss beachten, dass es eventuell viele verschiedene minimale Elemente in $\mathcal{Z}(a)$ gibt oder vielleicht überhaupt keine. Denkbar ist auch, dass eine absteigende Kette von Zerlegungen von a stationär ist, eine andere aber nicht!
Bekanntlich kann das im Ring $\mathbb{Z}$ der ganzen Zahlen nicht passieren. Es gilt der Satz von der eindeutigen Primfaktorzerlegung, den wir im folgenden allgemein für Hauptidealringe beweisen werden.

Beispiel: a) Man kann auf verschiedene Weise zur Primfaktorzerlegung von 120 kommen: $120 \succ (24, 5) \succ (12, 2, 5) \succ (6, 2, 2, 5) \succ (3, 2, 2, 2, 5)$ oder
$120 \succ (10, 12) \succ (2, 5, 12) \succ (2, 5, 4, 3) \succ (2, 5, 2, 2, 3)$.
b) Die Menge $M = 1 + 4\mathbb{N} = \{1, 5, 9, 13, ...\}$ ist ein Untermonoid von $(\mathbb{Z}, \cdot)$. Die Zahlen 5, 9, 13, 17, 21, 29, 33, 37, 41, 49, 53, ... sind irreduzibel in M. (Die Zerlegung $21 = 3 \cdot 7$ ist keine Zerlegung in M, weil $3, 7 \notin M$.) $25 = 5 \cdot 5, 45 = 5 \cdot 9$ sind reduzibel in M. Auch 441 ist reduzibel in M. Es gibt hier zwei wesentlich verschiedene Zerlegungen in irreduzible Faktoren:

$$441 = 21 \cdot 21 = 9 \cdot 49.$$

Dies zeigt, dass die Eindeutigkeit von Primfaktorzerlegungen keine Selbstverständlichkeit ist (Dieses einfache Beispiel stammt von Hilbert).

- **Satz 8.2**

Die folgenden Bedingungen sind äquivalent:
(8.2.1) Für jede von Null verschiedene Nichteinheit $a \in R$ gilt: Jede absteigende Zerlegungsfolge von a wird stationär, führt also zu einer Zerlegung

$$a = q_1 \ldots q_k$$

in ein endliches Produkt von irreduziblen Elementen $q_j \in R$.
(8.2.2) Jede aufsteigende Folge von Hauptidealen in R wird stationär, d.h. Sind $a_1, a_2, \ldots$ Elemente in R mit $\langle a_1\rangle \subset \langle a_2\rangle \subset \langle a_3\rangle \subset \ldots$, so gibt es ein n_0, so dass $\langle a_n\rangle = \langle a_{n_0}\rangle$ für alle $n > n_0$.

Beweis. (8.2.1)$\Longrightarrow$(8.2.2): Angenommen, es gibt eine *nicht* stationäre Haupidealkette $\langle a_1\rangle \subset \langle a_2\rangle \subset \langle a_3\rangle \subset \ldots$ in R. Dann gibt es für jedes $n > 1$ eine Nichteinheit b_n mit $a_{n-1} = a_n b_n$. Also ist
$a_1 = b_2 a_2 = b_2 b_3 a_3 = \ldots = b_2 b_3 \ldots b_n a_n$ usw.. Die absteigende Zerlegungsfolge $z_k = (b_2, \ldots, b_k, a_k)$, $k > 1$ von a_1 ist also nicht stationär.
(8.2.2)$\Longrightarrow$(8.2.1): Ist $(z_1 \succ z_2 \succ \ldots)$ eine Folge von Zerlegungen $z_i = (a_{i,1}, \ldots, a_{i,i})$ von a mit jeweils elementaren Verfeinerungen, so ergibt sich nach Umnummerieren und Multiplikation mit Einheiten:
$z_1 = (a_1)$, $z_2 = (b_2, a_2)$, ..., $z_k = (b_2, \ldots, b_k, a_k)$, ..., mit $a_{n-1} = a_n b_n$ und man erhält die aufsteigende Hauptidealkette $\langle a_1\rangle \subset \langle a_2\rangle \subset \langle a_3\rangle \subset \ldots$ Da diese stationär wird, gilt das auch für die Zerlegungsfolge .□

- **Definition 8.3 (Faktorieller Ring)**

Ein Integritäsbereich R heißt *faktoriell* :$\Longleftrightarrow$
(8.3.1) $\forall\, a \in R \setminus R^\times,\ a \neq 0\ \exists\ q_1, \ldots, q_k \in R$ irreduzibel (nicht notwendig verschieden), $u \in R^\times$, so dass

$$a = u\ q_1 \cdot \ldots \cdot q_k.$$

und

(8.3.2) Sind $q_1, \ldots, q_k, \hat{q}_1, \ldots, \hat{q}_m \in R$ irreduzibel u, $\hat{u}$ Einheiten in R und gilt

$$u\, q_1 \cdot \ldots \cdot q_k = \hat{u}\ \hat{q}_1 \cdot \ldots \cdot \hat{q}_m,$$

so ist $k = m$ und es gibt eine Permutation $\pi \in \mathcal{S}_k$, so dass $\langle \hat{q}_j\rangle = \langle q_{\pi(j)}\rangle$ für alle j, also $\hat{q}_j, q_{\pi(j)}$ zueinander assoziiert sind , d.h. bis auf Multiplikation mit einer Einheit übereinstimmen.
Man nennt dann $a = u\ q_1 \cdot \ldots \cdot q_k$ die eindeutige Zerlegung in irreduzible Faktoren. (Man darf die Reihenfolge der Faktoren vertauschen und die Faktoren mit Einheiten multiplizieren.) Die Hauptideale $\langle q_i\rangle$sind eindeutig durch a bestimmt.

- **Beispiel 8.5**

$R = \mathbb{Z}\left[\sqrt{-5}\right]$ ist nicht faktoriell, denn $6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$ sind zwei wesentlich verschiedene Zerlegungen in irreduzible Elemente (Beweis als Übung). In der algebraischen Zahlentheorie wird das Problem der eindeutigen Primfaktorzerlegung durch weiteres Verfeineren der Zerlegungen mithilfe 'idealer' Faktoren gelöst. Man erhält tatsächlich eine eindeutige Zerlegung in '*ideale Primzahlen' .* Dabei werden die Ideale in R als 'ideale' Zahlen aufgefasst. Die Elemente von R selbst entsprechen den Hauptidealen. Die Multiplikation von R kann auf die Menge der Ideale forgesetzt werden: Sind $I, J \subset R$ Ideale, so definiert man

$$I \cdot J = \langle a\, b \mid a \in I, b \in J \rangle.$$

Wir illustrieren dies an unserem Beispiel:
Das Ideal $I = \left\langle 2, 1 + \sqrt{-5} \right\rangle$ ist ein *'idealer* Faktor' sowohl von 2 als auch von $1 + \sqrt{-5}$, d.h. $\langle 2 \rangle, \left\langle 1 + \sqrt{-5} \right\rangle \subset I$. Es gilt
$I^2 = \left\langle 4, 2 + 2\sqrt{-5}, \left(1 + \sqrt{-5}\right)^2 \right\rangle = \left\langle 4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5} \right\rangle =$
$\left\langle 4, 2 + 2\sqrt{-5}, 2\sqrt{-5} \right\rangle = \left\langle 4, 2, 2\sqrt{-5} \right\rangle = \langle 2 \rangle$. Betrachtet man also neben den gewöhnlichen Zahlen (d. h. Hauptidealen) auch noch Ideale (ideale Zahlen), so ist 2 nicht mehr irreduzibel, sondern das Quadrat von I. Wir sehen auch, dass I zu sich selbst konjugiert ist:
$\bar{I} = \left\langle 2, 1 - \sqrt{-5} \right\rangle = \left\langle 2, -1 - \sqrt{-5} \right\rangle = \left\langle 2, 1 + \sqrt{-5} \right\rangle = I$.
Das ist nicht so für $J = \left\langle 3, 1 + \sqrt{-5} \right\rangle$. Es gilt wieder (das Produkt von Idealen wird erzeugt von den Produkten der Erzeuger):
$J \cdot \bar{J} = \left\langle 9, 3 - 3\sqrt{-5}, 3 + 3\sqrt{-5}, 6 \right\rangle = \langle 3 \rangle$ und außerdem:
$I \cdot J = \left\langle 6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, \left(1 + \sqrt{-5}\right)^2 \right\rangle = \left\langle 1 + \sqrt{-5} \right\rangle,$
$I \cdot \bar{J} = \left\langle 6, 2\left(1 - \sqrt{-5}\right), 3 + 3\sqrt{-5}, 6 \right\rangle = \left\langle 6, 2\left(1 - \sqrt{-5}\right), -3 + 3\sqrt{-5} \right\rangle =$
$\left\langle 1 - \sqrt{-5} \right\rangle$.
Damit haben wir die 'eindeutige Primfaktorzerlegung' $\langle 6 \rangle = I^2 \cdot J \cdot \bar{J}$, die eine gemeinsame Verfeinerung der Zerlegungen $2 \cdot 3, \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$ darstellt. Dies muss natürlich noch näher begründet werden!

- **Definition 8.6**

Es sei R ein beliebiger kommutativer Ring.

(8.6.1) Eine von Null verschiedene Nichteinheit $p \in R$ heißt *Primelement* $\Longleftrightarrow$ $\forall\, a, b \in R : p \mid a\, b \Longrightarrow p \mid a$ oder $p \mid b$.

Offensichtlich ist $p \in R \setminus \{0\}$ genau dann ein Primelement, wenn der Restklassenring $R/\langle p\rangle$ nullteilerfrei ist, denn $(p \mid a\,b \Longrightarrow p \mid a \text{ oder } p \mid b)$ bedeutet ja dasselbe wie $((a \bmod p)(b \bmod p) = 0 \Longrightarrow a \bmod p = 0 \text{ oder } b \bmod p = 0)$.

(8.6.2) Ein Ideal $P \subset R$ heißt *Primideal*, wenn R/P ein Integritätsbereich ist.
Offensichtlich erzeugen Primelemente von Null verschiedene Primideale. Man beachte, dass in einem Integritätsbereich das Nullideal ein Primideal ist. Jedoch wird das Nullelement nicht als Primelement betrachtet.

Es sei nun wieder R ein Integritätsbereich. Man sieht leicht, dass jedes Primelement irreduzibel ist. Denn ist $p \in R$ Primelement und gilt $p = a\,b$, so teilt ja p insbesondere $a\,b$ und damit auch ohne Einschränkung a. Es gilt also $a = p\,c$ für ein $c \in R$. Einsetzen in die Gleichung $p = a\,b$ ergibt $p = p\,c\,b$ und da wir in einem Integritätsbereich sind folgt $1 = c\,b$. Damit ist b eine Einheit in R und p irreduzibel. Die Umkehrung ist dagegen im allgemeinen falsch. Zum Beispiel ist 2 kein Primelement in $\mathbb{Z}\left[\sqrt{-5}\,\right]$, denn 2 teilt 6 aber weder $1 + \sqrt{-5}$ noch $1 - \sqrt{-5}$.

- **Satz 8.7**

Folgende Aussagen sind äquivalent:
(8.7.1) R ist faktoriell.
(8.7.2) Es gilt:
(i) Jedes irreduzible Element in R ist ein Primelement und
(ii) Jede aufsteigende Hauptidealkette in R wird stationär,

Beweis: (8.7.1)$\Longrightarrow$(8.7.2): Zu (i): Es sei q irreduzibel. Sind nun $a, b \in R$ mit $q \mid a\,b$, so gibt es ein $c \in R$, so dass $a\,b = c\,q$. Da q irreduzibel ist, folgt jetzt aus der Eindeutigkeit der Primfaktorzerlegung ohne Mühe, dass q einer der Primfaktoren von a oder b ist, also a oder b teilt.
Zu (ii): Es sei $\langle a_1\rangle \subset \langle a_2\rangle \subset \langle a_3\rangle \subset \ldots$ eine aufsteigende Hauptidealkette. Es sei $a_1 = q_1 \ldots q_{s_1}$ die Primfaktorzerlegung von a_1. Wegen der Eindeutigkeit der Primfaktorzerlegung sind dann etwa $q_1, \ldots, q_{s_2}$, $s_2 \le s_1$ die Primfaktoren von a_2, $q_1, \ldots, q_{s_3}$, $s_3 \le s_2$ die Primfaktoren von a_3 usw. Es kann nur endlich oft $s_i < s_{i-1}$ auftreten, d. h. die Kette $\langle a_i\rangle$ wird stationär.
(8.7.2)$\Longrightarrow$(8.7.1): Wir müssen die Eindeutigkeit der Zerlegung in irreduzible Faktoren beweisen. Seien dazu $q_1, \ldots, q_k, \hat{q}_1, \ldots, \hat{q}_m \in R$ irreduzibel und es gelte $q_1 \cdot \ldots \cdot q_k = \hat{q}_1 \cdot \ldots \cdot \hat{q}_m$. Da $\hat{q}_1$ ein Primelement ist, teilt $\hat{q}_1$ einen der Faktoren q_j. Ohne Einschränkung sei dies q_1.Da q_1 irreduzibel ist, sind somit $\hat{q}_1$ und q_1 zueinander assoziiert. Ohne Einschränkung gilt $\hat{q}_1 = q_1$ und folglich $q_2 \cdot \ldots \cdot q_k = \hat{q}_2 \cdot \ldots \cdot \hat{q}_m$. Was haben wir damit erreicht? Klar! Man kann die Eindeutigkeit durch Induktion nach m beweisen. Den Induktionsschluss haben wir gerade durchgeführt. Der Induktionsanfang ist einfach (überlege dies!). □

- **Korollar 8.8**

In einem faktoriellen Ring besitzen zwei Elemente a, b, die nicht beide Null sind, einen größten gemeinsamen Teiler (ggT) d, der bis auf Multiplikation mit Einheiten durch folgende Bedingungen charakterisiert ist:
(1) $d \mid a$ und $d \mid b$.
(2) Ist $x \in R$ mit $x \mid a$ und $x \mid b$, so gilt $x \mid d$. □

Man beachte aber, dass man d im allgemeinen nicht als Linearkombination von a und b darstellen kann, wie man das für den ggT ganzer Zahlen kennt. Wir werden zeigen, dass der Polynomenring $K[x, y]$ faktoriell ist. Der ggT von x und y ist 1 und 1 ist keine Linearkombination von x und y. Anders verhält es sich in einem *Hauptidealring.* Hier kann man den ggT d zweier Elemente a, b einfach durch die Gleichung

$$\langle d \rangle = \langle a, b \rangle$$

definieren. In diesem Fall ist d Linearkombination von a und b. In den Ring $\mathbb{Z}$ der ganzen Zahlen und im Polynomenring $K[x]$ über einem Körper K kann man den ggT durch den *euklidischen Algorithmus*, der aus einer Iteration der Schritte $\langle a, b \rangle \to \langle r, a \rangle$, $r = b - q\,a =$ Rest beim Teilen von b durch a, besteht, gewinnen.

- **Satz 8.9**

In einem Hauptidealring ist jedes irreduzible Element ein Primelement.

Beweis. Wir beweisen zunächst den folgenden nützlichen Trick:
In einem Hauptidealring gilt:
(*) Sind $a, b, d \in R$ und sind a, d teilerfremd (d. h. $\langle a, d \rangle = R$) und ist d Teiler von $a\,b$, so ist d Teiler von b.
Beweis: a, d teilerfremd $\Longrightarrow \langle a, d \rangle = \langle 1 \rangle \Longrightarrow \exists\, x, y \in R$:

$$1 = a\,x + d\,y.$$

Multipliziert man diese Gleichung mit b, so erhält man

$$b = a\,b\,x + b\,d\,y.$$

Nun ist nach Voraussetzung $a\,b = c\,d$ für ein $c \in R$. Setzt man dies ein, so ergibt sich $b = c\,d\,x + b\,d\,y = (c\,x + b\,y)\,d$, also $d \mid b$. □
Sei jetzt q irreduzibel. Um zu sehen, dass q ein Primelement ist, nehmen wir an, dass q das Produkt $a\,b$ teilt, nicht aber a. Da q irreduzibel ist, also keine echten Teiler besitzt, sind somit a und q teilerfremd. Nach obigem Trick (*) teilt daher q den Faktor b. □

■ **Satz 8.10**

Ein Hauptidealring ist faktoriell.

Beweis. Das ist nun nicht mehr schwierig! Nach Satz 8.9 und Satz 8.7 ist nur noch zu zeigen, dass jede aufsteigende Kette $\langle a_1\rangle \subset \langle a_2\rangle \subset \langle a_3\rangle \subset ...$ von Hauptidealen in einem Hauptidealring stationär wird, was ganz einfach ist: $I := \bigcup_j \langle a_j\rangle$ ist ein Ideal, wie man leicht sieht, also ein Hauptideal $\langle a\rangle$. Für alle j gilt $\langle a_j\rangle \subset \langle a\rangle$ und nach Definition von I gilt $a \in \langle a_{j_0}\rangle$ für ein j_0, also $\langle a\rangle \subset \langle a_{j_0}\rangle$. Damit folgt: $\langle a_j\rangle = \langle a_{j_0}\rangle$ für alle $j > j_0$. □

■ **Korollar 8.11**

(8.11.1) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist faktoriell.
(8.11.2) Der Polynomenring $K[x]$ in einer Unbestimmten x über einem Körper K ist faktoriell. □

■ **Definition 8.12**

Es sei R ein faktorieller Ring. Ein Polynom $f = a_n x^n + a_{n-1} x^{n-1} + ... + a_0 \in R[x]$ heißt *primitiv* über R, wenn die Koeffizienten in R teilerfremd sind.

■ **Lemma 8.13**

Es sei R ein faktorieller Ring und K sein Quotientenkörper. Jedes Polynom $f \in K[x]$ lässt sich eindeutig bis auf Multiplikation mit Einheiten in R als Produkt $f = c\, f_0$ schreiben mit einer Konstante $c \in K$ und einem primitiven Polynom $f_0 \in R[x]$. Wir nennen f_0 den *primitiven Faktor* und c den *Inhalt* von f.

Beweis. Sei $f = \frac{a_n}{b_n} x^n + \frac{a_{n-1}}{b_{n-1}} x^{n-1} + ... + \frac{a_0}{b_0} \in K[x]$ mit $a_j, b_j \in R,\ b_j \neq 0$. Es sei dann b ein kleinstes gemeinsames Vielfaches von $b_0,\ ...,\ b_n$. Dann ist $b\, f \in R[x]$. Weiter sei a ein größter gemeinsamer Teiler von $b\,\frac{a_0}{b_0},\ ...,\ b\,\frac{a_n}{b_n}$. Dann ist $f_0 = \frac{b}{a} f$ primitiv in $R[x]$ und mit $c = \frac{a}{b}$ erhalten wir die gewünschte Darstellung $f = c\, f_0$. Wir müssen noch die Eindeutigleit beweisen: Sei $c\, f_0 = d\, g_0$ mit primitiven Polynomen f_0, g_0 und Konstanten $c, d \in K$. Es folgt $n\, f_0 = m\, g_0$, wobei $c = \frac{n}{h},\ d = \frac{m}{h},\ m, n, h \in R$. Da f_0, g_0 primitiv sind, folgt durch Koeffizientenvergleich, dass n und m in R assoziiert sind. □

■ **Lemma 8.14 (Gaußsches Lemma)**

Es sei R faktoriell. Ein Produkt primitiver Polynome in $R[x]$ ist wieder primitiv.

Beweis. Es seien $f, g \in R[x]$ primitiv und $h = f\,g$. Um zu sehen, dass h primitiv ist müssen wir nur zeigen, dass kein Primelement $p \in R$ ein Teiler von h ist. d.h. Die Reduktion $\pi_p(h) \in R/\langle p\rangle[x]$ von h, die man erhält, indem man die Koeffizienten von h durch ihre Restklassen modulo p ersetzt, ist von Null verschieden. Nun ist aber offensichtlich $\pi_p : R[x] \longrightarrow R/\langle p\rangle[x]$ ein Ringhomomorphismus. Der Restklassenring $R/\langle p\rangle$ ist ein Integritätsbereich, weil p Primelement ist und damit ist auch $R/\langle p\rangle[x]$ ein Integritätsbereich. Aus $\pi_p(f) \neq 0$, $\pi_p(g) \neq 0$ folgt dann $\pi_p(h) = \pi_p(f)\,\pi_p(g) \neq 0$. □

- **Satz 8.15**

Die Voraussetzungen seien wie in Lemma 8.13. Dann gilt:
(8.15.1) Es seien $f, g \in K[x]$, $f_0, g_0 \in R[x]$ ihre primitiven Faktoren. Gilt $f \mid g$ in $K[x]$, so gilt auch $f_0 \mid g_0$ in $R[x]$.
(8.15.2) Es seien $f, g \in R[x]$ und f sei primitiv. Gilt $f \mid g$ in $K[x]$, so gilt auch $f \mid g$ in $R[x]$.
(8.15.3) Es seien $f, g \in R[x]$ und $d \in K[x]$ sei ein gemeinsamer Teiler von f und g in $K[x]$. Dann ist der primitive Faktor von d ein gemeinsamer Teiler von f und g in $R[x]$.
(8.15.4) Es sei $f \in R[x]$. Dann gilt: Ist f in $R[x]$ irreduzibel, so auch in $K[x]$.

Beweis. Zu (8.15.1): Sei $g = q\,f$. (Primitive Faktoren werden durch den Index Null gekennzeichnet.) Nach dem Gaußschen Lemma ist $q_0\,f_0$ primitiv. Nach 8.13 ist $g_0 = q_0\,f_0$ (bis auf Multiplikation von Einheiten in R).
Zu (8.15.2): Sei $g = q\,f$ mit $q \in K[x]$. Dann ist $g_0 = q_0\,f$, also $g = (c\,q_0)\,f$, wobei $c \in R$ der Inhalt von g sei. Da $c\,q_0 \in R[x]$, teilt also f das Polynom g in $R[x]$.
Zu (8.15.3): Wenn d die Polynome $f, g \in R[x]$ in $K[x]$ teilt, so gilt dies natürlich auch für jedes konstante Vielfache von d, also insbesondere für den primitiven Faktor d_0. Jetzt können wir (8.15.2) anwenden.
Zu (8.15.4): $f \in R[x]$, $f = p\,q$, $p, q \in K[x] \Longrightarrow f = f_0 = p_0\,q_0 \Longrightarrow p_0$ oder q_0 ist Einheit in $R[x] \Longrightarrow f$ oder g ist Einheit in $K[x]$. □

- **Satz 8.16**

Es sei R faktoriell mit Quotientenkörper K. Es sei $f \in R[x]$, $f \neq 0$, $f \notin R^\times$ Dann sind folgende Aussagen äquivalent:
(8.16.1) f ist irreduzibel in $R[x]$.
(8.16.2) $\operatorname{grad}(f) = 0$ und f ist Primelement in R oder
$\operatorname{grad}(f) > 0$ und f ist primitiv über R und irreduzibel in $K[x]$.
(8.16.3) f ist Primelement in $R[x]$.

Beweis. (8.16.1)$\Longrightarrow$(8.16.2): Dies folgt aus (8.15.4).
(8.16.2)$\Longrightarrow$(8.16.1): Es sei $\operatorname{grad}(f) > 0$ und f ist primitiv über R und irreduzibel in $K[x]$. Ist nun $f = g\,h$ mit $g, h \in R[x]$, so ist g oder h eine Einheit in $K[x]$, also

konstant. Da f primitiv ist, muß g oder h eine Einheit in R sein.
(8.16.2)$\Longrightarrow$(8.16.3): Es seien $g, h \in R[x]$ und f sei ein Teiler von gh in $R[x]$, also $gh = qf$ mit $q \in R[x]$. Ist $\text{grad}(f) = 0$ und f ist Primelement in R folgt: f teilt das Produkt cd, wobei c der Inhalt von g und d der Inhalt von h ist. Da f ein Primelement in R ist, teilt f wenigstens einen der beiden Faktoren c, d und damit auch g oder h. Im Fall $\text{grad}(f) > 0$ und f ist primitiv über R und irreduzibel in $K[x]$ folgt: f teilt g oder h in $K[x]$ und nach (8.15.2) auch in $R[x]$. □

■ **Satz 8.17**

Ist R faktoriell, so ist auch $R[x]$ faktoriell.

Beweis. Wir müssen nur noch die aufsteigende Kettenbedingung für Hauptidealketten in $R[x]$ beweisen. Es sei $0 \neq \langle f_1 \rangle \subset \langle f_2 \rangle \subset \langle f_3 \rangle \subset \ldots$ eine Kette, $f_j \in R[x]$. Dann ist $\text{grad}(f_j) \leq \text{grad}(f_{j-1})$, also wird der Grad stationär. Es folgt $f_j = a_j f_{j_0}$ mit $a_j \in R \setminus 0$ für alle $j > j_0$ (j_0 geeignet). Da R faktoriell ist, wird die Kette $\langle a_{j_0} \rangle \subset \langle a_{j_0+1} \rangle \subset \langle a_{j_0+3} \rangle \subset \ldots$ stationär und somit auch $\langle f_1 \rangle \subset \langle f_2 \rangle \subset \langle f_3 \rangle \subset \ldots$ □

■ **Korollar 8.18**

(8.18.1) Ist K ein Körper, so ist $K[x_1, \ldots, x_n]$ faktoriell.
(8.18.2) $\mathbb{Z}[x_1, \ldots, x_n]$ ist faktoriell. □

■ **Beispiel 8.19 (Primfaktorzerlegung in $\mathbb{Z}[x]$ nach Kronecker)**

Es ist bisher nur die Existenz von Primfaktorzerlegungen in $\mathbb{Z}[x]$ bewiesen worden. Wie aber kann man die Primfaktorzerlegung eines vorgelegten Polynoms bestimmen? (siehe [2] van der Waerden: Algebra I, § 32).
Es sei $f = a_n x^n + a_{n-1} x^{n-1} + \ldots a_0 \in \mathbb{Z}[x]$, $a_n \neq 0$. Wir können f als primitiv anehmen. Ist nun f nicht irreduzibel, so muß es einen Faktor vom Grad $m \leq k := [\frac{n}{2}]$ geben. Solch einen Faktor setzen wir an als $g = b_k x^k + \ldots + b_0$. Weiter wählen wir $k+1$ verschiedene ganze Zahlen $x_0, \ldots, x_k$. Ist g Faktor von f so ist auch $g(x_j)$ Faktor von $f(x_j)$. Für $g(x_j)$ gibt es also nur endlich viele Möglichkeiten, da $f(x_j)$ nur endlich viele Teiler besitzt. Damit hat man nur endlich viele Wertelisten $(g(x_0), \ldots, g(x_k))$ in Betracht zu ziehen. Da g den Grad $\leq k$ hat, liegt g durch die Werteliste fest und man kann jeweils die Teilbarkeit von f durch g mit dem Divisionsalgorithmus prüfen. Finden wir auf diese Weise keinen Teiler, so ist f irreduzibel. Ansonsten wiederhole man das Verfahren mit den Faktoren, bis man bei einer Primfaktorzerlegung angekommen ist. Dies ist natürlich nicht das schnellste Verfahren! Aber es ist ein konstruktives Verfahren!

■ **Satz 8.20**

Es sei $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ und $p \in \mathbb{Z}$ eine Primzahl, die a_n nicht teilt. Dann ist die Reduktion $\bar{f} = \sum_{k=0}^{n} (a_k \bmod p) x^k \in \mathbb{F}_p[x]$ ein Polynom vom Grad n und es gilt: Ist $\bar{f}$ irreduzibel in $\mathbb{F}_p[x]$, so ist f irreduzibel in $\mathbb{Q}[x]$.

Beweis. Die koeffizientenweise Reduktion modulo p definiert einen Ringhomomorphismus $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$ liefert. Ein einfache Gradbetrachtung gibt uns den Beweis. Dabei ist natürlich die Voraussetzung $a_n \not\equiv 0 \bmod p$ wichtig! □

■ **Beispiel 8.21**

(8.21.1) Die irreduziblen Polynome in $\mathbb{F}_p[x]$, deren Grad kleiner als eine vorgegebene Schranke n ist, kann man mit dem Sieb des Eratosthenes finden: Man listet zunächst alle nichtkonstanten normierten Polynome vom Grad $\leq n$ nach dem Grad geordnet auf (es sind ja nur endlich viele!). Die linearen Polynome sind x, $x+1$, ..., $x+p-1$. Man wählt x aus. Man streicht aus dem Rest alle Polynome, die Vielfache von x sind. Aus dieser Menge wählt man $x+1$ aus und streicht aus dem Rest alle Polynome, die Vielfache von $x+1$ sind. Nachdem die linearen Polynome aufgebraucht sind, sind quadratischen Polynome in der Restliste irreduzibel. Man fährt jetzt mit den quadratischen Polynomen fort!

Wir illustrieren das Verfahren an $\mathbb{F}_2[x]$: Die normierten nichtkonstanten Polynome vom Grad $\leq n$ entsprechen den $2^{n+1} - 2$ von Null und $(1, 0, ..., 0)$ verschiedenen $(n+1)$-Tupeln $(a_0, ..., a_n)$ von Koeffizienten $a_i \in \{0, 1\}$. Für $n = 4$ erhalten wir die folgende Tabelle. Die irreduziblen Elemente sind eingerahmt.

1
$\boxed{x}$, $\boxed{x+1}$
x^2, x^2+x, x^2+1, $\boxed{x^2+x+1}$
x^3, x^3+1, x^3+x, $\boxed{x^3+x+1}$, x^3+x^2, x^3+x^2+x, $\boxed{x^3+x^2+1}$, x^3+x^2+x+1
x^4, x^4+1, x^4+x, $\boxed{x^4+x+1}$, x^4+x^2, x^4+x^2+x, x^4+x^2+1, x^4+x^2+x+1, x^4+x^3, $\boxed{x^4+x^3+1}$, x^4+x^3+x, x^4+x^3+x+1, $x^4+x^3+x^2$, $x^4+x^3+x^2+x$, $x^4+x^3+x^2+1$, $\boxed{x^4+x^3+x^2+x+1}$

Wir können nun Satz 8.20 etwa auf das irreduzible Polynom $x^4+x^3+1 \in \mathbb{F}_2[x]$ anwenden, um eine ganze Reihe irreduzibler Polynome in $\mathbb{Q}[x]$ anzugeben: Das

Polynom $3x^4 - 5x^3 + 4x^2 + 12x + 13$ ist zum Beispiel irreduzibel in $\mathbb{Q}[x]$, da seine Reduktion modulo 2 es ist.

(8.21.2) Das Polynom $x^4 - 10x^2 + 1$ ist ebenfalls irreduzibel in $\mathbb{Q}[x]$, obwohl die Reduktion bezüglich jeder beliebigen Primzahl reduzibel ist, was wir hier nicht beweisen wollen. Man kann also die Methode der Reduktion modulo p nicht immer anwenden. Wir führen den Nachweis der Irreduzibilität von $q = x^4 - 10x^2 + 1$ indirekt:
Annahme: $q = (x^2 + ax + b)(x^2 + cx + d)$. Koeffizientenvergleich liefert:

$$c = -a,\ d = \tfrac{1}{b},\ a(1 - b^2) = 0,\ b + \tfrac{1}{b} - a^2 = -10,$$

also gilt
1. Fall: $a = 0$, $b^2 + 10b + 1 = 0$. b kann dann nicht rational sein.
2. Fall: $b = \pm 1$. $a^2 = 10 \pm 2$, a kann dann nicht rational sein.
Also gibt es keine Zerlegung von q in Polynome vom Grad 2 mit Koeffizienten in $\mathbb{Q}$. Da q auch keine rationalen Nullstellen besitzt, ist q irreduzibel.

- **Satz 8.22 (Eisensteinsches Irreduzibilitätskriterium)**

Es sei R ein faktorieller Ring, K sein Quotientenkörper. Es sei $p \in R$ ein Primelement und $f = a_n x^n + ... + a_1 x + a_0 \in R[x]$ ein Polynom vom Grad n. Es gelte:
(i) $a_n \not\equiv 0 \bmod p$,
(ii) $a_i \equiv 0 \bmod p$ für $i = 0, ..., n-1$,
(iii) $a_0 \not\equiv 0 \bmod p^2$.
Dann ist f irreduzibel in $K[x]$. Ist f primitiv, so ist f auch irreduzibel in $R[x]$.

Beweis. Da p Primelement ist, ist der Restklassenring $S = R/\langle p \rangle$ ein Integritätsbereich. Mit L bezeichnen wir den Quotientenkörper von S. Es sei nun eine Zerlegung von f in $K[x]$ gegeben. Das führt zu einer Gleichung

$$bf = gh \qquad \textbf{(8)}$$

mit $b \in R \setminus \{0\}$, $g, h \in R[x]$. Wir müssen zeigen, dass g oder h konstant ist.
Auf (8) wenden wir den Reduktionshomomorphismus $\mathrm{red}_p : R[x] \longrightarrow S[x]$ an und erhalten wegen unserer Voraussetzungen

$$(b\, a_n \bmod p)\, x^n = \mathrm{red}_p(bf) = \mathrm{red}_p(g)\,\mathrm{red}_p(h). \qquad \textbf{(9)}$$

Ist nun etwa $b \equiv 0 \bmod p$, so gilt $\mathrm{red}_p(g) = 0$ oder $\mathrm{red}_p(h) = 0$, es gilt also $\frac{1}{p} g \in R[x]$ oder $\frac{1}{p} h \in R[x]$. Man kann somit in der Gleichung (8) durch p teilen. Dies kann man solange wiederholen, bis $b \not\equiv 0 \bmod p$. Aus der Gleichung (9) folgt dann (weil $L[x]$ ein faktorieller Ring ist)
$\mathrm{red}_p(g) = \frac{\alpha}{\beta} x^m$, $\mathrm{red}_p(h) = \frac{\gamma}{\delta} x^l$ wobei $\alpha, \beta, \gamma, \delta \in S \setminus \{0\}$, $m + l = n$.
Wir müssen nur noch zeigen, dass $m = 0$ oder $l = 0$.

Annahme: $m, l > 0$. Dann haben $\mathrm{red}_p(g)$ und $\mathrm{red}_p(h)$ keinen konstanten Term, d.h. der konstante Term von g und von h ist durch p teilbar. Nach (8) ist somit $b\,a_0 = b\,f(0) = g(0)\,h(0)$ durch p^2 teilbar. Da b nicht durch p teilbar ist, ist also a_0 durch p^2 teilbar entgegen der Voraussetzung (iii). Damit ist der Satz bewiesen. □

- **Beispiele 8.23**

(8.23.1) In $\mathbb{Z}[x]$ ist $x^n + p$ für jede Primzahl p und jeden Grad $n > 0$ irreduzibel.

(8.23.2) Das Polynom $10x^5 + 6x^4 - 9x^2 - 3x + 15$ ist irreduzibel in $\mathbb{Z}[x]$ nach dem Eisensteinschen Kriterium für $p = 3$.

(8.23.3) Interessant ist auch der Ring $\mathbb{C}[x, y]$. Ein irreduzibles Polynom $f \in \mathbb{C}[x, y]$ besitzt als Nullstellengebilde eine irreduzible ebene algebraische Kurve

$$C = V(f) = \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\}.$$

Es sei bemerkt, dass man die 'Gleichung' f von C aus der Punktmenge C zurückgewinnen kann. Es gilt nämlich:

$$\langle f \rangle = I(C), \text{ wobei } I(C) := \{g \in \mathbb{C}[x, y] \mid g \mid C = 0\}$$

das Ideal aller Polynome, die auf C verschwinden, bezeichnet. Der schwierige Punkt ist dabei, zu zeigen, dass ein Polynom g, das auf C verschwindet, ein Vielfaches von f ist. Das ist ein Spezialfall des Hilbertschen Nullstellensatzes. Eine elementare Begründung findet man in dem schönen Buch von Fulton (Fulton: Algebraic Curves, Chap. 1.7.).
Mit dem Eisensteinschen Kriterium kann man bisweilen auch die Irreduzibilität von $f \in \mathbb{C}[x, y]$ nachweisen: Zum Beispiel ist $y^n - p(x)$ irreduzibel in $\mathbb{C}[x, y]$, wenn das Polynom $p \in \mathbb{C}[x]$ eine einfache Nullstelle besitzt. Die kubische Kurve $y^2 - (x - a)(x - b)(x - c)$, wobei a, b, c komplexe Zahlen sind, von denen mindestens zwei verschieden sind, ist also irreduzibel.
Etwas allgemeiner sei $f = a_n(x)\,y^n + \ldots + a_1(x)\,y + a_0(x)$ mit $a_i \in \mathbb{C}[x]$. Es gelte $a_i(0) = 0$, für $i = 0, 1, \ldots n - 1$, $a_n(0) \neq 0$. Aber $x = 0$ sei nur eine einfache Nullstelle von a_0. Weiter mögen $a_0, \ldots, a_n$ keine gemeinsame Nullstelle besitzen. Nach dem Eisensteinschen Kriterium ist dann f irreduzibel in $\mathbb{C}[x, y]$.

(8.23.4) Ist p Primzahl, so ist $x^{p-1} + .. + x^2 + x + 1$ irreduzibel in $\mathbb{Q}[x]$. Das Eisensteinkriterium ist nicht direkt anwenbar, aber nachdem wir die Substitution $x \to t + 1$ durchgeführt haben:

$$\sum_{k=0}^{p-1} (t+1)^k = \tfrac{(t+1)^p - 1}{t} = \sum_{k=1}^{p} \binom{p}{k} t^{k-1} = p + \binom{p}{2} t + \ldots + t^{p-1}.$$

■ Übungen 8

(8.1) Prüfen Sie, ob die folgenden Elemente irreduzibel in $\mathbb{Q}[x, y]$ sind.
a) $y^4 + 3x^2y^2 + 4x^7y + 2x$, b) $y^6 + 3xy^4 + 3x^2y^2 + x^3$.

(8.2) a) Zeigen Sie, dass $\mathbb{Z}[i]$ ein Hauptidealring ist. Hinweis: Zeigen Sie zunächst: Sind $a, b \in \mathbb{Z}[i]$, $b \neq 0$, so gibt es eindeutig bestimmte $q, r \in \mathbb{Z}[i]$, so dass $a = qb + r$ und $|r| < |b|$.
b) Zeigen Sie, dass $x^3 - 6x^2 + 4ix + 1 + 3i$ irreduzibel in $\mathbb{Z}[i][x]$ ist.
c) Finden Sie die Primfaktorzerlegungen von 2,3,5,7 in $\mathbb{Z}[i]$.

(8.3) Geben Sie alle irreduziblen normierten Polynome vom Grad 2 in $\mathbb{F}_7[x]$an.

(8.4) Geben Sie die Primfaktorzerlegung von $x^3 + 2$ in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ und in $\mathbb{C}[x]$ an.

(8.5) Zeigen Sie: Den ggT zweier normierter Polynome $p, q \in \mathbb{Z}[x]$ kann man als Linearkombination $ap + bq$ mit Polynomen $a, b \in \mathbb{Z}[x]$ schreiben, so dass $\text{grad}(a) < \text{grad}(q)$, $\text{grad}(b) < \text{grad}(p)$.

(8.6) Welcher der folgenden Ringe ist faktoriell?
a) $\mathbb{Z}\left[\sqrt{-3}\right]$, b) $\mathbb{Z}[x] / \langle 8 \rangle$, c) $\mathbb{C}[x, y] / \langle y^2 - x^3 + x \rangle$.

(8.7) Es sei K ein Körper, x eine Unbestimmte. Zeigen Sie, dass $K[[x]]$ faktoriell ist. Hinweis: Bis auf Multiplikation mit Einheiten ist x das einzige Primelement in $K[[x]]$.

(8.8) Es sei $R = \mathbb{Z}[x_{ij}, i, j = 1, ..., n]$ der Polynomenring über $\mathbb{Z}$ in den n^2 Unbestimmten. Zeigen Sie: $\det(x_{ij})$ ist irreduzibles homogenes Polynom vom Grad n in R.

(8.9) Zeige, dass $x^5 - x^2 + 1$, $x^5 - x - 1$ irreduzibel in $\mathbb{Q}[x]$ sind. Hinweis: Reduktion modulo p.

(8.10) Es sei K ein Körper und $f \in K[x]$ ein normiertes Polynom vom Grad $n \geq 1$. Es sei $L = K[x] / \langle f \rangle$. Zeigen sie, dass folgende Aussagen äquivalent sind:
(i) f ist irreduzibel,
(ii) L ist ein Integritätsbereich,
(iii) L ist ein Körper.

9 Algebraische Körpererweiterungen

Inhalt: algebraische Elemente, algebraische Erweiterungen, endliche Erweiterungen, Minimalpolynom, Körpergrad, Gradformel, Beispiele: $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, $\mathbb{Q}[\sqrt[3]{2}]$, Zerfällungskörper, Existenz und Eindeutigkeit des Zerfällungskörpers, Galois-Gruppe

- **Definition 9.1**

Es sei K ein Körper und L sei ein Erweiterungskörper von K.

(9.1.1) Ein Element $\alpha \in L$ heißt *algebraisch über K*, wenn es ein Polynom $p \in K[x]$ vom Grad $n \geq 1$ gibt, so dass $p(\alpha) = 0$.

(9.1.2) $\alpha \in L$ heißt *algebraisch über K vom Grad n*, wenn das *Minimalpolynom* von α, d.h. das normierte Polynom $p \in K[x]$ kleinsten Grades mit $p(\alpha) = 0$ den Grad n hat.

(9.1.3) L heißt *algebraische Erweiterung* von K, wenn alle Elemente von L algebraisch über K sind.

- **Satz 9.2**

Es sei K ein Körper und L sei ein Erweiterungskörper von K. $\alpha \in L$ sei algebraisch über K. Dann gilt

(9.2.1) Der Einsetzungshomomorphismus $\varphi : K[x] \longrightarrow K[\alpha]$ ist surjektiv aber nicht injektiv und das *Minimalpolynom* von α über K ist irreduzibel.

(9.2.2) Ist α vom Grad n über K, so ist $(1, \alpha, \alpha^2, ..., \alpha^{n-1})$ eine K-Vektorraumbasis von $K[\alpha]$. Insbesondere ist $K[\alpha]$ ein n-dimensionaler K-Vektorraum.

(9.2.3) $K(\alpha) = K[\alpha]$, d.h. $K[\alpha]$ ist der kleinste Unterkörper von L, der K und α enthält.

Beweis. Zu (9.2.1): Wir müssen nur noch zeigen, dass das Minimalpolynom $q \in K[x]$ von α irreduzibel ist. Da $K[x] / \langle q \rangle \cong K[\alpha]$ und $K[\alpha]$ als Unterring eines Körpers nullteilerfrei ist, ist q ein Primelement, also irreduzibel.

Zu (9.2.2): Das haben wir schon in Abschnitt 7 bewiesen.

Zu (9.2.3): Wir müssen zeigen, dass $K[\alpha]$ ein Körper ist, dass also jedes Element $\beta \in K[\alpha] \backslash 0$ invertierbar ist. Es sei $\beta = \sum_{k=0}^{n-1} a_k \alpha^k$ mit $a_k \in K$, also $\beta = p(\alpha)$ mit $p \in K[x]$, $\operatorname{grad} p < n = \operatorname{grad} q$. Da q irreduzibel ist, folgt, dass p und q teilerfremd

sind und somit Polynome $r, s \in K[x]$ existieren, so dass
$1 = r\,p + s\,q$ gilt. Dann ist

$$1 = r(\alpha)\,\beta + s(\alpha)\,q(\alpha) = r(\alpha)\,\beta.$$

Damit ist $\beta^{-1} = r(\alpha) \in K[\alpha]$. □

- **Definition 9.3**

Es sei K ein Körper und L sei ein Erweiterungskörper von K. L heißt *endliche Erweiterung* von K, wenn folgende äquivalente Bedingungen erfüllt sind:
(9.3.1) L ist endlich-dimensional als K-Vektorraum.
(9.3.2) Es gibt endlich viele über K algebraische Elemente $\alpha_1, \ldots, \alpha_m \in L$, so dass $L = K(\alpha_1, \ldots, \alpha_m)$.
Die Dimension von L als K-Vektorraum heißt der *Körpergrad* von L über K und wird mit $[L : K]$ bezeichnet.

Die Äquivalenz von (9.3.1) und (9.3.2) ist einfach zu sehen mit der folgenden Gradformel:

- **Satz 9.4 (Gradformel)**

Es sei K ein Körper, L sei ein Erweiterungskörper von K und M sei ein Erweiterungskörper von L. Dann ist M Erweiterung von K vom Grad $[M : K] = [M : L][L : K]$.

Beweis. Ohne Einschränkung seien $[M : L], [L : K] < \infty$. Es sei $(x_1, \ldots, x_n)$ Basis von L über K und $(y_1, \ldots, y_m)$ Basis von M über L. Dann ist offensichtlich $\{x_i\, y_j \mid i = 1, \ldots, n;\ j = 1, \ldots, m\}$ eine Basis von M über K (Beweisdetails als Übung). □

Jetzt sieht man leicht, dass für algebraische Elemente $\alpha_1, \ldots, \alpha_m$ der Körper $L = K(\alpha_1, \ldots, \alpha_m)$ als Kette endlicher Erweiterungen
$K \subset K[\alpha_1] \subset K[\alpha_1][\alpha_2] =$
$K[\alpha_1, \alpha_2] \subset K[\alpha_1, \alpha_2][\alpha_3] \subset \ldots \subset K[\alpha_1, \ldots, \alpha_m] = K(\alpha_1, \ldots, \alpha_m) = L$
endlich über K ist. Das beweist (9.3.2)$\Longrightarrow$(9.3.1). Ungekehrt ist natürlich auch jede endliche Erweiterung L von K von endlich vielen über K algebraischen Elementen erzeugt: Ist nämlich $[L : K] = n < \infty$, so ist jedes Element $\alpha \in L$ algebraisch vom Grad $\leq n$, denn $1, \alpha, \alpha^2, \ldots, \alpha^n$ sind ja K-linear abhängig. Man kann also einfach irgendeine K-Vektorraumbasis von L nehmen. Das beweist (9.3.1)$\Longrightarrow$(9.3.2). □

■ **Beispiel 9.5**

(9.5.1) $L = \mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right] \subset \mathbb{R}$ ist endlicher Erweiterungskörper von $\mathbb{Q}$ vom Grad 4, denn $K = \mathbb{Q}\left[\sqrt{2}\right]$ ist vom Grad 2 über $\mathbb{Q}$ und $L = K\left[\sqrt{3}\right]$ ist vom Grad 2 über K denn $x^2 - 3$ ist irreduzibel in $K[x]$, also das Minimalpolynom von $\sqrt{3}$ über K. (Es gilt $\sqrt{3} \notin K$. Wäre $\sqrt{3} = a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$, so wäre (quadriere!), weil 1, $\sqrt{2}$ linear unabhängig über $\mathbb{Q}$ sind, $3 = a^2 + 2b^2$, $0 = ab$, also $3 = a^2$ oder $3 = 2b^2$, Widerspruch!). Es sei $\alpha := \sqrt{2} + \sqrt{3}$. Wir wollen zeigen, dass $L = \mathbb{Q}[\alpha]$. Offensichtlich ist $\mathbb{Q}[\alpha] \subset L$. Wir müssen nur noch zeigen, dass das Minimalpolynom von α über $\mathbb{Q}$ vom Grad 4 ist. Dazu suchen wir nach einer Relation von α: Das Verfahren kennen wir aus der Schule: $\alpha^2 = \left(\sqrt{2} + \sqrt{3}\right)^2 = 5 + 2\sqrt{6} \Longrightarrow \alpha^2 - 5 = 2\sqrt{6} \Longrightarrow (\alpha^2 - 5)^2 = 24$. Damit ist α Nullstelle von $x^4 - 10x^2 + 1$ und dieses Polynom ist irreduzibel in $\mathbb{Q}[x]$, wie wir schon in Abschnitt 8 gezeigt haben.

Damit haben wir gezeigt, dass $x^4 - 10x^2 + 1$ das Minimalpolynom von $\sqrt{2} + \sqrt{3}$ ist. Damit ist $\left[\mathbb{Q}\left[\sqrt{2} + \sqrt{3}\right] : \mathbb{Q}\right] = 4$ und folglich ist $\alpha = \sqrt{2} + \sqrt{3}$ ein Erzeuger des von $\sqrt{2}$ und $\sqrt{3}$ erzeugten Erweiterungskörpers L von $\mathbb{Q}$. Wir folgern weiter, dass $\{1, \alpha, \alpha^2, \alpha^3\}$ eine Basis von L über $\mathbb{Q}$ ist. Genauso ist aber auch nach der Gradformel $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$ eine Basis von L über $\mathbb{Q}$. Der Basiswechsel lässt sich leicht angeben. Es gilt nämlich: $1 = 1$, $\alpha = \sqrt{2} + \sqrt{3}$, $\alpha^2 = 5 + 2\sqrt{6}$,
$\alpha^3 = \alpha\left(5 + 2\sqrt{6}\right) = \left(\sqrt{2} + \sqrt{3}\right)\left(5 + 2\sqrt{2}\sqrt{3}\right) = 11\sqrt{2} + 9\sqrt{3}$.
Damit ist der Basiswechsel durch die Matrix

$$A = \begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 2 & 0 \end{pmatrix}$$

gegeben. Es gilt $\det(A) = 4 \neq 0$. Das ergibt einen weiteren Beweis, dass 1, α, α^2, α^3 linear unabhängig über $\mathbb{Q}$ sind und als Konsequenz, dass $q = x^4 - 10x^2 + 1$ in $\mathbb{Q}[x]$ irreduzibel ist.

(9.5.2) $\mathbb{Q}[\omega] \subset \mathbb{C}$,wobei $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{3}\,i$ eine primitive dritte Einheitswurzel ist, ist Erweiterung vom Grad 2, denn bekanntlich ist $x^2 + x + 1$ das Minimalpolynom. Etwas allgemeiner: Nach (8.23.4) ist $x^{p-1} + \ldots + x + 1$ irreduzibel in $\mathbb{Q}[x]$, wenn p eine Primzahl ist. Damit ist $K := \mathbb{Q}[\zeta_p]$ eine Erweiterung vom Grad $p - 1$ von $\mathbb{Q}$, wo bei ζ_p eine primitive p-te Einheitswurzel in $\mathbb{C}$ ist. $x^p - 1 = (x - 1)(x^{p-1} + \ldots + x + 1)$. In $K[x]$ zerfällt das Minimalpolynom $x^{p-1} + \ldots + x + 1$ von $\zeta_p$über $\mathbb{Q}$ in Linearfaktoren: $x^{p-1} + \ldots + x + 1 = \prod_{j=1}^{p-1}(x - \zeta_p{}^j)$.

Bisher sind wir von einer Körpererweiterung $K \subset L$ ausgegangen und haben gesehen, welche Struktur der von einem über K algebraischen Element $\alpha \in L$

erzeugte Erweiterung $K[\alpha]$ hat. Es gilt $K[\alpha] \cong K[x]/\langle q\rangle$, wobei q ein normiertes irreduzibles Polynom vom Grad $n = [K[\alpha] : K]$ ist.
Jetzt starten wir mit einem Körper K und einem beliebigen normierten irreduziblen Polynom $q \in K[X]$ vom Grad $n \geq 1$. Der Restklassenring $K[x]/\langle q\rangle$ ist dann ein Integritätsbereich und wie wir schon in 7.7 gezeigt haben, ein n-dimensionaler K-Vektorraum mit der Basis $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$, wobei α die Restklasse der Unbestimmtem x ist. Mit derselben Argumentation wie in (9.2.3) folgt, dass $K[x]/\langle q\rangle$ ein Körper ist (Übung) $K[x]/\langle q\rangle = K[\alpha]$ ist somit ein endlicher Erweiterungskörper und q ist das Minimalpolynom von α über K. Es gilt $q(\alpha) = 0$. Damit haben wir insbesondere bewiesen:

- **Satz 9.6**

Es sei K Körper und $q \in K[X]$ ein *irreduzibles* normiertes Polynom vom Grad $n \geq 1$. Dann gibt es eine endlichen Erweiterungskörper L von K, in dem q eine Nullstelle α besitzt.

Man kann $L = K[x]/\langle q\rangle$ wählen. $\alpha = x \bmod q$ ist dann Nullstelle von q.

- **Beispiel 9.7**

(9.7.1) Ein Körper mit 16 Elementen ist nun leicht zu konstruieren. Wie wir in Abschnitt 8 mit dem Sieb des Eratosthenes gesehen haben, ist $x^4 + x + 1$ irreduzibel in $\mathbb{F}_2[x]$. Folglich ist $K = \mathbb{F}_2[x]/\langle x^4 + x + 1\rangle = \mathbb{F}_2[\alpha]$ mit $\alpha^4 = \alpha + 1$ ein Körper mit $[K : \mathbb{F}_2] = 4$. K hat somit die 16 Elemente. Die von Null verschiedenen Elemente bilden die multiplikative Gruppe der Ordnung 15. Es gilt somit $b^{15} = 1$ für alle $b \in K^\times$. Somit ist $b^{16} - b = 0$ für alle $b \in K$. Mit anderen Worten: Das Polynom $f = x^{16} - x \in \mathbb{F}_2[x]$ hat im Erweiterungskörper K von $\mathbb{F}_2$ genau 16 verschiedene Nullstellen, zerfällt also über K in Linearfaktoren $f = \prod_{b\in K}(x - b)$. Das ist kein Zufall: Ist K ein Erweiterungskörper vom Grad n von $\mathbb{F}_p$, so zerfällt das Polynom $x^{p^n} - x$ über K in Linearfaktoren. Wir kommen darauf in Abschnitt 10 zurück.

(9.7.2) Nach dem Eisensteinschen Irreduzibilitätskriterium ist $x^3 - 2$ irreduzibel in $\mathbb{Q}[x]$. Man erhält eine Erweiterung $K = \mathbb{Q}[x]/\langle x^3 - 2\rangle \cong \mathbb{Q}\left[\sqrt[3]{2}\right] \subset \mathbb{R}$. Sei $\alpha := \sqrt[3]{2}$. In K spaltet $x^3 - 2 = x^3 - \alpha^3$ einen linearen Faktor ab:

$$x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2).$$

Das quadratische Polynom $x^2 + \alpha x + \alpha^2$ ist aber irreduzibel in $K[x] \subset \mathbb{R}[x]$, denn die Nullstellen von $x^2 + \alpha x + \alpha^2$ sind nicht reell. Damit kann man den Erweiterungskörper $L = K[x]/\langle x^2 + \alpha x + \alpha^2\rangle$ betrachten. Es gilt $[L : K] = 2$ und somit nach der Gradformel $[L : \mathbb{Q}] = 6$. Es sei β die Restklasse von x in L. Es gilt also

$$\beta^2 + \alpha\beta + \alpha^2 = 0.$$

Nach dem Gradsatz ist $\{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ ein Basis von L über $\mathbb{Q}$. Es gilt $L = \mathbb{Q}[\alpha, \beta]$ und über L zerfällt das Polynom $x^3 - 2$ in Linearfaktoren:

$$x^3 - 2 = (x - \alpha)(x - \beta)(x - \gamma),$$

wobei sich $\gamma = \frac{\alpha^2}{\beta} = \frac{\alpha^2\beta^2\alpha}{\beta\beta^2\alpha} = \frac{\beta^2}{\alpha}$ ergibt. Man nennt daher L einen *Zerfällungskörper* des Polynoms $x^3 - 2$. Was ist sonst noch interessant an L? Zum Beispiel die sogenannte Galois-Gruppe $G = \mathrm{Aut}(L/\mathbb{Q})$ aller $\mathbb{Q}$-Isomorphismen $\varphi : L \longrightarrow L$. Offensichtlich ist G eine Untergruppe von S_3, der symmetrischen Gruppe der drei Nullstellen α, β, γ von $x^3 - 2$, denn jeder Automorphismus hat keine andere Wahl als diese drei Lösungen der Gleichung $x^3 = 2$ untereinander zu permutieren und durch die Werte von α und β liegt ein Automorphismus fest, da α und β den Körper L erzeugen. Tatsächlich führen hier alle sechs Permutationen zu Automorphismen von L. Beispielsweise definiert die Transposition $(\alpha\beta) \in S_3$ den Automorphismus $\varphi(\alpha) = \beta$, $\varphi(\beta) = \alpha$, $\varphi(\gamma) = \varphi\left(\frac{\alpha^2}{\beta}\right) = \frac{\beta^2}{\alpha} = \gamma$. Es ist jedoch nicht ganz klar, dass dadurch wirklich ein Automorphismen von L definiert wird. Wir wollen die Gruppe G auf andere Weise bestimmen: Wir können β konkret als komplexe Zahl angeben: $\omega := \frac{\beta}{\alpha}$. Dies ist eine primitive dritte Einheitswurzel. Mit $\theta := \alpha - \beta = \alpha - \alpha\omega = \alpha(1 - \omega)$ erhält man ein Element von L, das L über $\mathbb{Q}$ erzeugt. Es gilt nämlich

$$\theta^6 = \alpha^6 (1 - \omega)^6 = 4 (1 - \omega)^6 =$$
$$4 (1 - 6\omega + 15\omega^2 - 20 + 15\omega - 6\omega^2 + 1) = 4 (-18 + 9 (\omega + \omega^2)) = -4 \cdot 27.$$

Wir behaupten: $q = x^6 + 108$ ist das Minimalpolynom von θ. Dazu Schreiben wir die Potenzen $1, \theta, \theta^2, \ldots, \theta^5$ als rationale Linearkombinationen der Basiselemente $1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta$ und berechnen die Determinante der Koeffizientenmatrix A:

$$\begin{aligned}
\theta &= \alpha - \beta \\
\theta^2 &= \alpha^2 - 2\alpha\beta + \beta^2 = \alpha^2 - 2\alpha\beta - \alpha^2 - \alpha\beta = -3\alpha\beta \\
\theta^3 &= -3\alpha\beta(\alpha - \beta) = -3a^2\beta + 3\alpha(-\alpha^2 - \alpha\beta) = -6 - 6\alpha^2\beta \\
\theta^4 &= 9\alpha^2\beta^2 = -9\alpha^4 - 9\alpha^3\beta = -18\alpha - 18\beta \\
\theta^5 &= -18\alpha^2 + 18\beta^2 = -32\alpha^2 - 18\alpha\beta
\end{aligned}$$

Damit ist die Übergangsmatrix A von der Form

$$A = \begin{pmatrix}
1 & 0 & 0 & -6 & 0 & 0 \\
0 & 1 & 0 & 0 & -18 & 0 \\
0 & 0 & 0 & 0 & 0 & -32 \\
0 & -1 & 0 & 0 & -18 & 0 \\
0 & 0 & -3 & 0 & 0 & -18 \\
0 & 0 & 0 & -6 & 0 & 0
\end{pmatrix}.$$

Es gilt $\det(A) = -2^8 3^4 \neq 0$. Damit sind die Potenzen θ^k, $k = 0, ..., 5$ linear unabhängig über $\mathbb{Q}$, also ist q das Minimalpolynom von θ. q zerfällt in $L[x]$ in Linearfaktoren. Es seien $\theta_1, ..., \theta_6 \in L$ die Nullstellen von $x^6 + 4 \cdot 27$, $\theta_{k+1} = \theta(1+\omega)^k$ für $k = 0, ..., 5$. Dabei ist $1 + \omega$ eine primitive sechste Einheitswurzel. Nach Satz 7.5 gibt es zu jedem $i = 1, ..., 6$ genau einen $\mathbb{Q}$-Homomorphismus $\varphi_i : L \longrightarrow L$ mit $\varphi_i(\theta) = \theta_i$. Diese Homomorphismen sind Isomorphismen, weil auch (L, θ_i) die universelle Eigenschaft aus (7.5.1) erfüllt. Damit haben wir die Galois-Gruppe G von $L/\mathbb{Q}$ bestimmt. Es gilt $G \cong S_3$.
Die Transposition $(\alpha\beta)$ bestimmt den Automorphismus $\theta \mapsto -\theta = \theta(1+\omega)^3 = \theta_4$. Der Dreierzyklus $(\alpha\beta\gamma)$ bestimmt den Automorphismus
$\theta = \alpha - \beta \mapsto \beta - \gamma = \beta - \frac{\beta^2}{\alpha} = \theta \frac{\beta}{\alpha} = \theta\,\omega = \theta(1+\omega)^2 = \theta_3$.
Der Isomorphismus $S_3 \longrightarrow G$ ist durch die folgende Tabelle dargestellt.

1	$\theta \mapsto \theta_1$
$(\alpha\beta)$	$\theta \mapsto \theta_4$
$(\alpha\beta\gamma)$	$\theta \mapsto \theta_3$
$(\alpha\gamma)$	$\theta \mapsto \theta_6$
$(\alpha\gamma\beta)$	$\theta \mapsto \theta_5$
$(\beta\gamma)$	$\theta \mapsto \theta_2$

- **Definition 9.8**

Es sei K ein Körper und $f \in K[x]$ sei ein normiertes (aber nicht notwendig irreduzibles) Polynom vom Grad $n \geq 1$. Ein Erweiterungskörper L von K heißt ein *Zerfällungskörper* von f, wenn gilt: Es gibt Elemente $c_1, ..., c_n \in L$, so dass
(9.8.1) $f = (x - c_1) ... (x - c_n)$,
(9.8.2) $L = K(c_1, ..., c_n)$.

Offensichtlich ist K selbst schon ein Zerfällungskörper von f, wenn f über K in Linearfaktoren zerfällt. Interessant ist natürlich der Fall, wenn f in $K[x]$ irreduzible Komponenten vom Grad größer als 1 besitzt.

- **Satz 9.9 (Existenz eines Zerfällungskörper)**

Es sei K ein Körper und $f \in K[x]$ sei ein normiertes (aber nicht notwendig irreduzibles) Polynom vom Grad $n \geq 1$. Dann gibt es einen Zerfällungskörper L von f. Es gilt $[L : K] \leq n!$

Beweis. Wir zerlegen f in $K[x]$ in seine normierten irreduziblen Faktoren.

$$f = f_1 \cdot ... \cdot f_m,$$

$f_k \in K[x]$ irreduzibel. Nach Satz 9.6 gibt es einen Erweiterungskörper K_1 von K, in dem f_1 eine Nullstelle c_1 besitzt. Hat man nun schon einen Erweiterungskörper K_k von K und Elemente $c_1, \ldots, c_k \in K_k$ konstruiert, so dass

$$f = (x - c_1) \ldots (x - c_k)\, g_1 \ldots g_r$$

mit irreduziblen Polynomen $g_j \in K_k[x]$, so kann man, falls $r \geq 1$ ist, einen Erweiterungskörper K_{k+1} von K_k finden, in dem g_1 eine Nullstelle $c_{k+1} \in K_{k+1}$ besitzt. In $K_{k+1}[x]$ ist

$$f = (x - c_1) \ldots (x - c_k)\,(x - c_{k+1})\, \tilde{g}_1\, g_2 \ldots g_r,$$

wobei $\tilde{g}_1 \in K_{k+1}[x]$. Nach n Schritten hat man einen Erweiterungskörper K_n von K erhalten, über dem f in Linearfaktoren zerfällt:

$$f = (x - c_1) \ldots (x - c_n).$$

$L = K(c_1, \ldots, c_n)$ ist ein Zerfällungskörper von K. Die Gradabschätzung ist offensichtlich. □

- **Satz 9.10 (Eindeutigkeit des Zerfällungskörpers)**

Es seien $K, \tilde{K}$ Körper und $\varphi : K \longrightarrow \tilde{K}$ sei ein Isomorphismus. x sei eine Unbestimmte. Mit φ werde auch die eindeutig bestimmte Fortsetzung $\varphi : K[x] \longrightarrow \tilde{K}[x]$ von $\varphi : K \longrightarrow \tilde{K}$ mit $\varphi(x) = x$ bezeichnet. $f \in K[x]$ sei ein normiertes (aber nicht notwendig irreduzibles) Polynom vom Grad $n \geq 1$. Es sei $\tilde{f} := \varphi(f)$. Es sei nun L ein Zerfällungskörper von f und $\tilde{L}$ sei ein Zerfällungskörper von $\tilde{f}$. Dann gibt es $k \leq \left[\tilde{L} : K\right]$ verschiedene Fortsetzungen von φ zu einem Isomorphismus $\psi : L \longrightarrow \tilde{L}$. Sind die Nullstellen von $\tilde{f}$ in $\tilde{L}$ paarweise verschieden, so ist $k = \left[\tilde{L} : K\right]$.

Beweis. Induktion nach $[L : K]$.
1. $[L : K] = 1$. Dann ist $L = K$ und offensichtlich auch $\tilde{L} = \tilde{K}$.
2. Induktionsschluss: Es sei $[L : K] = d > 0$ und für Zerfällungskörper vom Grad kleiner als d sei die Behauptung bewiesen.
Schritt I:
Es sei $L = K(c_1, \ldots, c_n)$, $f = (x - c_1) \ldots (x - c_n)$ und
$\tilde{L} = \tilde{K}(\tilde{c}_1, \ldots, \tilde{c}_n)$, $\tilde{f} = (x - \tilde{c}_1) \ldots (x - \tilde{c}_n)$. Da $d > 1$, ist ohne Einschränkung c_1 vom Grad $d_1 \geq 2$ über K. Dann ist $K[c_1]$ Erweiterung von K mit Minimalpolynom $q_1 \in K[x]$ vom Grad d_1, $f = q_1 f_1$. Es folgt $\tilde{f} = \tilde{q}_1 \tilde{f}_1$. q_1, $\tilde{q}_1 = \varphi(q_1)$ sind irreduzibel und $\gamma_1 : K[x]/\langle q_1 \rangle \xrightarrow{\cong} K[c_1]$, $x \mapsto c_1$ ist ein K-Isomorphismus. Weiter induziert φ einen Isomorphismus $\delta_1 : K[x]\big/\langle q_1 \rangle \longrightarrow \tilde{K}[x]\big/\langle \tilde{q}_1 \rangle$, der $\varphi : K \longrightarrow \tilde{K}$ fortsetzt und die Restklasse von x auf die Restklasse von x abbildet. Es seien nun genau k_1 verschiedene Elemente aus $\{\tilde{c}_1, \ldots, \tilde{c}_n\}$ Nullstellen des Faktors $\tilde{q}_1$. Seien dies ohne Einschränkung $\tilde{c}_1, \ldots, \tilde{c}_{k_1}$. Für jedes $j = 1, \ldots, k_1$ erhalten wir nach (7.5.1) einen Isomorphismus $\tilde{\psi}_j : \tilde{K}[x]\big/\langle \tilde{q}_1 \rangle \longrightarrow \tilde{K}[\tilde{c}_j]$, der $\tilde{K}$ festlässt und die Restklasse von x auf

$\tilde{c}_j$ abbildet. Man erhält so für jedes $j = 1, \ldots, k_1$ einen Isomorphismus
$\varphi_{1j} = \tilde{\psi}_j \circ \delta_1 \circ \gamma_1^{-1} : K[c_1] \longrightarrow \tilde{K}[\tilde{c}_j]$,
der $\varphi : K \longrightarrow \tilde{K}$ fortsetzt und c_1 in $\tilde{c}_j$ abbildet. Sind die Nullstellen von $\tilde{q}_1$ paarweise verschieden, so ist $k_1 = d_1$.
Schritt II:
Wir können nun L auch als Zerfällungskörper von f über $K[c_1]$ auffassen und $\tilde{L}$ als Zerfällungskörper von $\tilde{f}$ über $\tilde{K}[\tilde{c}_j]$. Es gilt $[L : K[c_1]] < d$. Nach Induktionsvoraussetzung gibt es dann $\ell \le [L : K[c_1]]$ verschiedene Fortsetzungen des Isomorphismus $\varphi_{1j} : K[c_1] \longrightarrow \tilde{K}[\tilde{c}_j]$ zu einem Isomorphismus $L \longrightarrow \tilde{L}$. Damit erhält man insgesamt $k_1 \ell \le d_1 [L : K[c_1]] = [L : K]$ mögliche Fortsetzungen von φ zu einem Isomorphismus $L \longrightarrow \tilde{L}$. Sind die Nullstellen $\tilde{c}_1, \ldots, \tilde{c}_n$ paarweise verschieden, so gibt es genau $[L : K]$ verschiedene Fortsetzungen von φ zu einem Isomorphismus $L \longrightarrow \tilde{L}$.
Schritt III:
Ist $\psi : L \longrightarrow \tilde{L}$ irgendeine Fortsetzung von φ, so ist $\psi \mid K[c_1]$ einer der Isomorphismen $\varphi_{1,j}$ und somit ist ψ eine der beschriebenen Fortsetzungen. □

- **Korollar 9.11**

Bis auf Isomorphie besitzt ein Polynom $f \in K[x]$ genau einen Zerfällungskörper.

- **Korollar 9.12**

Ist L der Zerfällungskörper eines Polynoms $f \in K[x]$, so ist die *Galois-Gruppe* $\mathrm{Aut}(L/K)$ eine endliche Gruppe der Ordnung $d \le [L : K]$. Ist $f = \prod_{k=1}^{n} (x - c_k)$ mit $c_k \in L$, $c_k \neq c_j$ für $k \neq j$, so ist $|\mathrm{Aut}(L/K)| = [L : K]$.

- **Beispiel 9.13**

Der Kreisteilungskörper $L = \mathbb{Q}[\zeta_p] = \mathbb{Q}[x] / \langle x^{p-1} + \ldots + x + 1 \rangle$, p Primzahl, ist der Zerfällungskörper von $f = x^p - 1 \in \mathbb{Q}[x]$. Die Galois-Gruppe ist eine Gruppe der Ordnung $p - 1 = [L : \mathbb{Q}]$. Wegen $\zeta_p \mapsto \zeta_p{}^m \mapsto (\zeta_p{}^k)^m = \zeta_p{}^{mk}$ ist $\mathrm{Aut}(L/\mathbb{Q}) \cong \mathbb{F}_p{}^\times$. Wir werden sehen, dass diese Gruppe zyklisch von der Ordnung $p - 1$ ist.

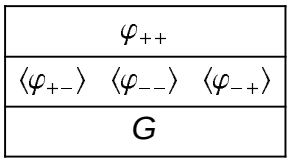
- **Beispiel 9.14**

Wir betrachten noch einmal das Beispiel

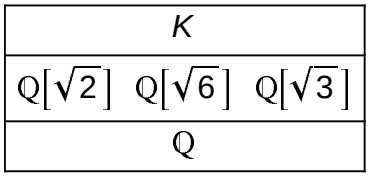
$$K = \mathbb{Q}\left[\sqrt{2} + \sqrt{3}\right] = \mathbb{Q}[x] / \langle x^4 - 10x^2 + 1 \rangle.$$

Hier ist schon K der Zerfällungskörper von $x^4 - 10x^2 + 1$, denn die vier Nullstellen $\pm\sqrt{2} \pm \sqrt{3}$ liegen in K. Die Galois-Gruppe $G = \mathrm{Aut}(K/\mathbb{Q})$ ist hier offensichtlich die

Kleinsche Vierergruppe! Die Untergruppen von G entsprechen eineindeutig den Unterkörpern von K. G hat die folgenden Untergruppen:



Dabei ist $\varphi_{++}: \sqrt{2}+\sqrt{3} \mapsto \sqrt{2}+\sqrt{3}$, $\varphi_{+-}: \sqrt{2}+\sqrt{3} \mapsto \sqrt{2}-\sqrt{3}$ usw.
Eine Untergruppe $H \subset G$ bestimmt den Zwischenkörper F, $\mathbb{Q} \subset F \subset K$ mit $F = K^H = \{\beta \in K \mid \forall\, \varphi \in H: \varphi(\beta) = \beta\}$. Man erhält:
$K^{\langle\varphi_{+-}\rangle} = \{\beta \in K \mid \varphi_{+-}(\beta) = \beta\} = \mathbb{Q}[\sqrt{2}]$,
$K^{\langle\varphi_{--}\rangle} = \{\beta \in K \mid \varphi_{--}(\beta) = \beta\} = \mathbb{Q}[\sqrt{6}]$,
$K^{\langle\varphi_{-+}\rangle} = \{\beta \in K \mid \varphi_{+-}(\beta) = \beta\} = \mathbb{Q}[\sqrt{3}]$
und damit das Diagramm der Unterkörper



■ Übungen 9

(9.1) Bestimmen Sie das Minimalpolynom q von $\sqrt{2}+\sqrt{5}$ über $\mathbb{Q}$ und konstruieren Sie den Zerfällungskörper von q über $\mathbb{Q}$.

(9.2) Es sei $K = \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$.
a) Welchen Grad hat der Körper K über $\mathbb{Q}$? Geben Sie eine Basis von K über $\mathbb{Q}$ an.
b) Zeigen Sie: Für $\theta := \sqrt{2}+\sqrt[3]{2}$ gilt $K = \mathbb{Q}[\theta]$. Hinweis: Prüfen Sie die lineare Unabhängigkeit der Potenzen 1, θ, θ^2, ..., θ^5.
c) Bestimmen Sie das Minimalpolynom q von θ über $\mathbb{Q}$. (Antwort: $q = -4 - 24x + 12x^2 - 4x^3 - 6x^4 + x^6$).
d) Bestimmen Sie den Grad des Zerfällungskörpers L von q über $\mathbb{Q}$. (Antwort: $[L:\mathbb{Q}] = 12$)

(9.3) Gibt es einen $\mathbb{Q}$-Homomorphismus $\varphi: K \longrightarrow L$?
a) $K = \mathbb{Q}[i]$, $L = \mathbb{Q}[\sqrt{2}\, i]$,
b) $K = \mathbb{Q}[i]$, $L = \mathbb{Q}[\alpha]$, wobei $\alpha^3 + \alpha + 1 = 0$,
c) $K = \mathbb{Q}[\sqrt{2}]$, $L = \mathbb{Q}[\sqrt{3}]$.

(9.4) Zeigen Sie: $\mathbb{Q}[\sqrt[m]{2}, \sqrt[n]{3}] = \mathbb{Q}[\sqrt[m]{2}\ \sqrt[n]{3}]$, falls ggT$(n, m) = 1$. Bestimmen Sie das Minimalpolynom von $\sqrt[m]{2}\ \sqrt[n]{3}$ über $\mathbb{Q}$.

(9.5) Es sei $\alpha \in \mathbb{C}$ mit $\alpha^3 + 2\alpha - 1 = 0$. Bestimmen Sie die Minimalpolynome von α und von $\alpha^2 + \alpha$ über $\mathbb{Q}$.

(9.6) Gibt es einen Isomorphismus $\mathbb{F}_2[x] / \langle x^3 + x^2 + 1 \rangle \longrightarrow \mathbb{F}_2[x] / \langle x^3 + x + 1 \rangle$?

(9.7) Bestimmen Sie das Minimalpolynom von $\sqrt{3} + \sqrt{5}$ über dem Körper K.
a) $K = \mathbb{Q}$, b) $K = \mathbb{Q}\left[\sqrt{5}\right]$, c), $K = \mathbb{Q}\left[\sqrt{10}\right]$ d) $K = \mathbb{Q}\left[\sqrt{15}\right]$.

(9.8) Es sei $[K[\alpha] : K] = 5$. Zeigen Sie dass $K[\alpha^2] = K[\alpha]$ gilt.

(9.9) a) Zeigen Sie: Ist $\alpha \in \mathfrak{K}$, also aus 0 und 1 konstruierbar (Beispiel (6.18)), so ist α algebraisch über $\mathbb{Q}$ und ihr Grad ist eine Zweierpotenz.
b) Zeigen Sie: 'Die Würfelverdopplung ist unmöglich'. Gemeint ist damit: Die Seitenlänge eines Würfels mit dem Volumen 2 ist nicht konstruierbar.

(9.10) a) Zeigen Sie: Ist p eine Primzahl, derart, dass $p - 1$ keine Zweierpotenz ist, so ist die primitive p-te Einheitswurzel $\zeta_p = e^{\frac{2\pi i}{p}}$ nicht konstruierbar, der Winkel $\frac{360}{p}$ Grad ist also nicht konstruierbar.
b) Zeigen Sie: Primzahlen der Form $2^n + 1$ haben sogar die Form $2^{2^m} + 1$. Sie heißen Fermat-Primzahlen.
c)* Zeigen Sie: Ist p eine Fermat-Primzahl, so ist $\zeta_p = e^{\frac{2\pi i}{p}}$ konstruierbar. Gauss hat diese Aufgabe im Alter von 19 Jahren gelöst!

10 Anwendungen: Der Fundamentalsatz der Algebra, endliche Körper

Inhalt: Es werden drei elementare Beweise des Fundamentalsatzes der Algebra gegeben. Einer dieser Beweise ist eine Anwendung von Zerfällungskörpern. Als weitere Anwendung von Zerfällungskörpern werden die endlichen Körper klassifiziert. Eine Formel für die Anzahl der normierten irreduziblen Polynome vom Grad m in $\mathbb{F}_q[x]$ wird hergeleitet.

■ **Definition 10.1**

Es sei K ein Körper. K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom $f \in K[x]$ eine Nullstelle in K besitzt und somit über K in Linearfaktoren zerfällt.

- **Bemerkung 10.2**

Jeder Körper besitzt einen algebraisch abgeschlossenen Erweiterungskörper. Das wollen wir hier nicht beweisen (siehe [1]). Vielmehr wollen wir uns mit dem *Hauptsatz der Algebra* beschäftigen und drei verschiedene Beweise vorstellen. Weitere Beweise werden in der *Funktionentheorie* behandelt (siehe: Freitag/Busam: Funktionentheorie 1 oder Fischer/Lieb: Funktionentheorie). Natürlich kommt man, bedingt durch die Konstruktion der reellen Zahlen, nicht ganz ohne Analysis, beziehungsweise Topologie (Stetigkeitsüberlegungen) aus.

- **Satz 10.3 (Fundamentalsatz der Algebra)**

Der Körper der komplexen Zahlen ist algebraisch abgeschlossen.

- **Bemerkung 10.4**

Wir wollen den drei Beweisen einige Bemerkungen vorausschicken. Für das Verständnis ist es wichtig, die richtge geometrische Vorstellung in der komplexen Zahlenebene zu entwickeln: Ein komplexes nicht-konstantes Polynom definiert eine stetige Abbildung F der komplexen Ebene in sich. Die geometrischen Eigenschaften dieser Abbildung sollen untersucht werden. Wie werden Kreise

$$K_r = \{z \in \mathbb{C} \mid |z| = r\}$$

abgebildet, welche Gestalt hat also die Bildkurve

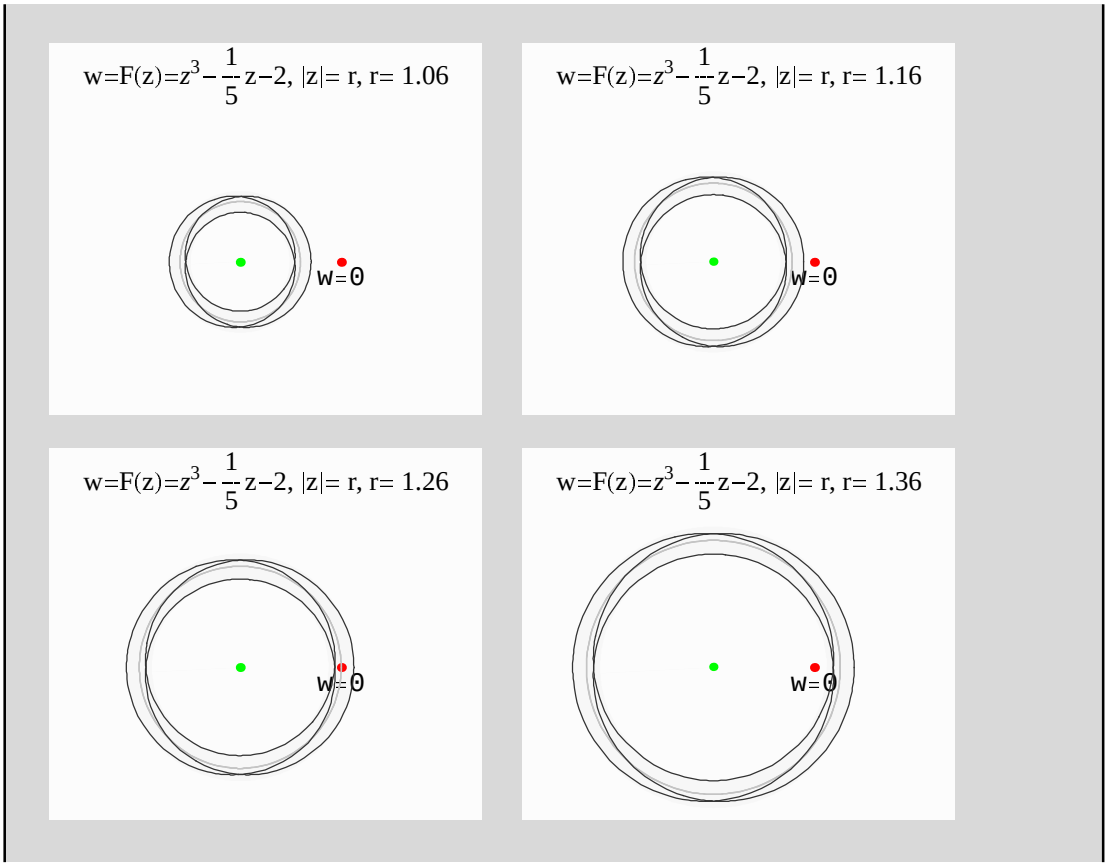
$$F(K_r),\ t \mapsto F(r\, e^{2\pi i t})$$

der einmal durchlaufenen Kreislinie

$$K_r,\ t \mapsto r\, e^{2\pi i t},\ 0 \le t \le 1?$$

Ist zum Beispiel $G(z) = z^3 - 2$, so wird $G(K_r)$ ein dreimal durchlaufener Kreis vom Radius r^3 mit Mittelpunkt -2 sein. Ist r klein ($r < \sqrt[3]{2}$), so wird der Nullpunkt außerhalb dieses Bildkreises sein. Ist r jedoch groß ($r > \sqrt[3]{2}$), so wird der Nullpunkt im Inneren des Kreises liegen. Nach dem Zwischenwertsatz für stetige Funktionen muss es somit einen Radius r geben, so dass der Nullpunkt *auf* dem Bildkreis liegt. In diesem Beispiel kennen wir das Ergebnis: $r = \sqrt[3]{2}$. Der Bildkreis des Kreises vom Radius $r = \sqrt[3]{2}$ durchläuft dreimal den Nullpunkt. G hat drei komplexe Nullstellen. Betrachtet man nun eine 'kleine' Störung $F(z) = G(z) + a\,z = z^3 + a\,z - 2$, $a \in \mathbb{C}$, von G, etwa mit $|a| < \frac{1}{4}$, so sieht man, dass der 'Störterm' $a\,z$ die alte Bildkurve in jedem Punkt $G(r\, e^{2\pi i t}) = r\, e^{6\pi i t} - 2$ um den Punkt $a\,r\, e^{2\pi i t}$ verschiebt. Es gilt $|F(z) - G(z)| = |a|\,r$ für alle $|z| = r$. Damit verläuft die Bildkurve $F(K_r)$ ganz in dem Kreisring mit Mittelpunkt -2 zwischen den Randkreisen mit den Radien $r^3 + |a|\,r$ und

$r^3 - |a|\,r$, wobei $r^2 > |a|$ gelten muss. $F(K_r)$ ist jedoch kein Kreis, sondern eine geschlossene Kurve, die den Punkt -2 dreimal umläuft. Natürlich werden auch alle Punkte, die einen Abstand kleiner als $r^3 - |a|\,r$ von -2 haben von $F(K_r)$ dreimal umlaufen. Ist nun $r^2 > |a|$, $r^3 + |a|\,r < 2$, so liegt der Nullpunkt 'außerhalb' der Bildkurve $F(K_r)$. Ist jedoch $r^3 - |a|\,r > 2$, so liegt der Nullpunkt 'innerhalb' der Bildkurve. Lässt man den Radius zwischen diesen beiden Extremen laufen, so muss aus Stetigkeitsgründen irgendwann der Nullpunkt auf der Bildkurve liegen, d.h. F muss eine Nullstelle besitzen.



Diese Idee kann man verallgemeinern: Man startet mit einem beliebigen normierten Polynom

$$F(z) = z^n + a_{n-1}\,z^{n-1} + \ldots + a_0.$$

Ist $a_0 = 0$, so ist $z = 0$ eine Nullstelle. Wir setzen also voraus, dass $F(0) = a_0 \neq 0$ gilt. Wir denken uns $F(z)$ als Störung des einfachen Polynoms

$$G(z) = z^n + a_0,$$

dessen n verschiedene Nullstellen wir ja schon kennen: Es sind $c_k = a\,e^{\frac{2\pi i k}{n}}$, $k = 0, \ldots, n-1$, wobei a eine n-te Wurzel von $-a_0$ ist. Die Bildkurve $G(K_r)$ ist ein n-mal durchlaufener Kreis vom Radius r^n mit Mittelpunkt a_0. Da $a_0 \neq 0$, wird für sehr kleine Radien r der Nullpunkt außerhalb des Bildkreises $G(K_r)$ liegen. Man muss sich überlegen, dass dies auch für die Bildkurve $F(K_r)$ gilt, wenn r sehr klein ist. Ist hingegen r sehr groß, so liegt sicher der Nullpunkt im Inneren des

Kreises $G(K_r)$. Der Nullpunkt wird dann also n-mal von dem Bildkreis $G(K_r)$ 'umlaufen' Wieder muss man sich überlegen, dass dies dann auch für die Bildkurve $F(K_r)$ gilt, sofern man r nur groß genug gewählt hat. Aus Stetigkeitsgründen muss dann für ein gewisses r die Bildkurve durch den Nullpunkt laufen, also F eine Nullstelle besitzen. Wir werden dies unten etwas genauer ausführen (*dritter Beweis*, siehe auch: Artin [1], Seite 606 und Fulton: Algebraic Topology, A First Course, Seiten 41 und 48). Insbesondere muss man präzisieren, was es bedeuten soll, dass eine geschlossene Kurve einen Punkt n-mal umläuft. Das führt zum Begriff der *Umlaufzahl* (winding number).

Man kann den Fundamentalsatz der Algebra auch so formulieren. Ist $F : \mathbb{C} \longrightarrow \mathbb{C}$ die durch ein nicht-konstantes Polynom definierte Abbildung der komplexen Zahlenebene in sich, so ist F surjektiv.

Wir beginnen mit Vorbereitungen aus der Analysis.

- **Satz 10.5**

Es sei $f = a_n x^n + a_{n-1} x^{n-1} ... + a_0 \in \mathbb{C}[x]$ ein Polynom vom Grad $n > 0$. Zu jeder Zahl $C > 0$ gibt es ein $r > 0$, so dass für alle $z \in \mathbb{C}$ mit $|z| > r$ gilt:

$$|a_n z^n| > C\,|a_{n-1} z^{n-1} + ... + a_0|.$$

Beweis. Es sei $A := C \max_{i<n} |a_i|$. $r := \frac{A}{|a_n|} + 1$, also $A = |a_n|\,(r - 1)$. Es sei nun $|z| > r$, also insbesondere $|z| > 1$ und $|a_n|\,(|z| - 1) > |a_n|\,(r - 1) = A$, also

$$|a_n| > \frac{A}{|z|-1}$$

und somit

$$C\,|a_{n-1} z^{n-1} + ... + a_0| \le C(|a_0| + |a_1|\,|z| + ... + |a_{n-1}|\,|z|^{n-1}) \le A(1 + |z| + ... + |z|^{n-1}) =$$
$$A\,\frac{|z|^n - 1}{|z|-1} < A\,\frac{|z|^n}{|z|-1} < |a_n z^n|. \quad \square$$

- **Korollar 10.6**

(10.6.1) Es sei $f = a_n x^n + a_{n-1} x^{n-1} ... + a_0 \in \mathbb{R}[x]$ ein reelles Polynom vom Grad $n > 0$. Dann gibt es ein $r > 0$, so dass für alle $x \in \mathbb{R}$ mit $|x| > r$ der Leitterm $a_n x^n$ und $f(x)$ dasselbe Vorzeichen besitzen.

(10.6.2) Es sei $f = a_n x^n + a_{n-1} x^{n-1} ... + a_0 \in \mathbb{C}[x]$ ein Polynom vom Grad $n > 0$. Zu jedem $s > 0$ gibt es ein $r > 0$ so dass $|f(z)| > s$ für alle $z \in \mathbb{C}$ mit $|z| > r$ gilt.
(Bemerkung: Setzt man $f(\infty) = \infty$, so wird f eine *stetige* Abbildung der Riemannschen Zahlenkugel $\mathbb{C} \bigcup \{\infty\}$ in sich, wobei die Mengen $U_r = \{\infty\} \bigcup \{z \in \mathbb{C} \mid |z| > r\}$, $r > 0$, offene Umgebungen von ∞ sind.)

Beweis. Zu (10.6.1): Nach Satz 10.5 gibt es ein $r > 0$, so dass
$|f(x) - a_n x^n| = |a_{n-1} x^{n-1} + ... + a_0| < |a_n x^n|$ für alle $x \in \mathbb{R}$ mit $|x| > r$. Es gilt also

$$a_n x^n - |a_n x^n| < f(x) < a_n x^n + |a_n x^n|,$$

falls $|x| > r$. Daraus folgt die Behauptung: Ist $a_n x^n$ negativ, so ist $f(x) < a_n x^n + |a_n x^n| = 0$, also $f(x)$ negativ. Ist $a_n x^n$ positiv, so ist $0 = a_n x^n - |a_n x^n| < f(x)$, also $f(x)$ positiv.

Zu (10.6.2): Nach Satz 10.5 gibt es ein $r > 0$, so dass
$\frac{1}{2} |a_n z^n| > |f(z) - a_n z^n|$ für $|z| > r$.
Es folgt $|f(z)| \geq |a_n z^n| - |f(z) - a_n z^n| > |a_n z^n| - \frac{1}{2} |a_n z^n| > \frac{1}{2} |a_n| r^n$ für $|z| > r$. Daraus folgt leicht die Behauptung. □

Aus (10.6.1) folgt nun sehr leicht mit dem *Nullstellensatz* für stetige Funktionen, dass ein reelles Polynom ungeraden Grades eine reelle Nullstelle besitzt.
Der *Nullstellensatz* für stetige Funktionen besagt: Eine reellwertige stetige Funktion auf einem Intervall $[a, b]$, die in a und b Werte mit verschiedenen Vorzeichen hat, besitzt zwischen a und b eine Nullstelle.

- **Satz 10.7**

Jedes reelle Polynom ungeraden Grades besitzt eine reelle Nullstelle. □

Mit diesem Satz wird es uns gelingen den Fundamentalsatz mit Hilfe von Zerfällungskörpern zu beweisen. Das wird unser *zweiter Beweis* sein.

Für einen ersten Beweis des Fundamentalsatzes brauchen wir die folgende Folgerung aus (10.6.2).

- **Satz 10.8**

Es sei $f = a_n x^n + a_{n-1} x^{n-1} ... + a_0 \in \mathbb{C}[x]$ ein Polynom vom Grad $n > 0$. Dann gibt es eine komplexe Zahl z_0, so dass $|f(z_0)| \leq |f(z)|$ für alle $z \in \mathbb{C}$. Man sagt: Die Funktion $|f|$ nimmt ihr Minimum an.

Beweis. Es sei s irgendein Wert der Funktion $|f|$. Dann gibt es nach (10.6.2) ein $r > 0$, so dass $|f(z)| > s$ für alle $|z| > r$. Wir brauchen nach dem Minimum von $|f|$ nur in dem abgeschlossenen Kreis $K = \{z \in \mathbb{C} \mid |z| \leq r\}$ zu suchen. Aus der Analysis ist bekannt, dass jede stetige Funktion $h : K \longrightarrow \mathbb{R}$ ihr Minimum in K annimmt (siehe etwa Forster: Analysis 1, Seite 67, §11 Satz 2 bzw. Analysis 2, Seite 22, §3, Satz 7). □

Aus diesem Satz und dem folgenden Satz ergibt sich nun verblüffend schnell unser *erster Beweis* des Fundamentalsatzes.

- **Satz 10.9**

Es sei $f = a_n x^n + a_{n-1} x^{n-1} ... + a_0 \in \mathbb{C}[x]$ ein Polynom vom Grad $n > 0$. Zu jeder komplexen Zahl z_0 mit $f(z_0) \neq 0$ gibt es eine komplexe Zahl z_1 mit $|f(z_1)| < |f(z_0)|$.

Beweis. Ohne Einschränkung sei $z_0 = 0$, also $f(0) = a_0 \neq 0$. Ansonsten ersetze man f durch $h(x) = f(x + z_0)$. Wir können f in folgender Form darstellen
$f = a_n x^n + a_{n-1} x^{n-1} ... + a_k x^k + a_0 = x^{k+1} g(x) + a_k x^k + a_0$
mit $1 \leq k \leq n$, $a_k \neq 0$ und $g \in \mathbb{C}[x]$. Wähle jetzt $b \in \mathbb{C}$ mit $|b| = 1$ so, dass a_0 und $a_k b^k$ reell linear abhängig sind und entgegengesetzte Richtung haben (durch Multiplikation mit b^k muss also a_k in die engegengesetzte Richtung von a_0 'gedreht' werden, was natürlich möglich ist).
Dann gilt für alle $t \in \mathbb{R}$ mit $0 < t \leq \left(\frac{|a_0|}{|a_k|}\right)^{\frac{1}{k}}$:

$$|a_k b^k t^k + a_0| = -|a_k| t^k + |a_0|$$

und somit

$$|f(t\,b)| \leq t^{k+1} |g(t\,b)| + |a_k b^k t^k + a_0| = t^{k+1} |g(t\,b)| - |a_k| t^k + |a_0| = |a_0| - t^k(|a_k| - t\,|g(t\,b)|).$$

Wenn man nun $t > 0$ klein genug wählt, so ist $|a_k| - t\,|g(t\,b)| > 0$, also gilt dann für $z_1 = t\,b$ die gewünschte Ungleichung $|f(z_1)| < |a_0|$.

- **Erster Beweis des Fundamentalssatzes**

Aus 10.8 folgt, dass der minimale Wert von $|f|$ angenommen wird, und nach 10.9 muss dieser Wert dann Null sein, f besitzt also eine Nullstelle. □

Im zweiten Beweis kommen wir mit dem Satz 10.7 aus, der einfacher ist als Satz 10.8. Dieser Beweis ist mehr algebraisch. Wesentlich wird der Zerfällungskörper eines Polynoms benutzt.

▪ Zweiter Beweis des Fundamentalssatzes

Wir gehen in mehreren Schritten vor.
Schritt I:
Es sei f ein reelles normiertes Polynom vom Grad $n > 0$.
Behauptung: f hat eine Nullstelle $z \in \mathbb{C}$.
Wir führen den Beweis dieser Behauptung durch Induktion nach der Vielfachheit $m = v_2(n)$ der Primzahl 2 in n.
Induktionsanfang: $m = 0$. Das bedeutet $n = 2^0 k$, k ungerade. Nach Satz 10.7 besitzt f sogar eine reelle Nullstelle. Damit ist der Induktionsanfang bewiesen.
Induktionsschluss: Es sei $m > 0$ und f sei Polynom vom Grad $n = 2^m k$, k ungerade. Für Polynome vom Grad $2^{m'} k'$, $m' < m$, k' ungerade, sei die Behauptung schon bewiesen. Es sei L ein Zerfällungskörper von f über $\mathbb{C}$. Insbesondere zerfällt f über L in Linearfaktoren und es gilt $\mathbb{C} \subset L$. Es seien $c_1, \ldots, c_n \in L$, so dass

$$f = \prod_{j=1}^{n} (x - c_j).$$

Wir wählen nun einen reellen Parameter a, über den wir später noch weiteres fordern. a wird als konstant angesehen. Es sei nun

$$y_{ij} = c_i c_j + a(c_i + c_j)$$

für $1 \le i < j \le n$. Die Anzahl dieser Elemente $y_{ij} \in L$ ist $d := \binom{n}{2} = \frac{n(n-1)}{2} = 2^{m-1} k'$, wobei $k' = k(n-1)$ ungerade ist, weil k und $n - 1$ es sind.
Nach Induktionsvoraussetzung haben alle reellen Polynome vom Grad d eine komplexe Nullstelle. Das Polynom

$$h = h_a := \prod_{i<j} (x - y_{ij}) = x^d - s_1 x^{d-1} + \ldots + (-1)^d s_d$$

hat den Grad d, ist allerdings nach Definition ein Polynom mit Koeffizienten in dem Erweiterungskörper L von $\mathbb{R}$. Wir werden jedoch zeigen, dass die Koeffizienten s_ν in $\mathbb{R}$ liegen! Die Koeffizienten s_ν sind nach Definition die elementarsymmetrischen Polynome in den Nullstellen y_{ij} von h. Bei festem a hängen die s_ν nur von den Nullstellen $c_1, \ldots, c_n$ ab. Wir schreiben

$$h_\nu(c_1, \ldots, c_n) = s_\nu(y_{ij}, 1 \le i < j \le n).$$

Es gilt $s_\nu \in \mathbb{Z}[y_{ij}]$ und da $a \in \mathbb{R}$ folgt

$$h_\nu \in \mathbb{R}[c_1, \ldots, c_n].$$

Man sieht nun sehr leicht ein, dass h_ν symmetrisch in den Nullstellen $c_1, \ldots, c_n$ von f ist, denn vertauscht man die Nullstellen $c_1, \ldots, c_n$ mit einer Permutation $\pi \in S_n$, so werden die 'Variablen' y_{ij} von s_ν ebenfalls nur vertauscht mit der Permutation $(i\ j) \mapsto (\pi i, \pi j)$. Da s_ν symmetrisch in den y_{ij} ist, ist auch h_ν symmetrisch in den c_i.

Nach dem Hauptsatz über symmetrische Polynome (7.20) gibt es Polynome $g_\nu \in \mathbb{R}[x_1, \ldots, x_n]$, so dass

$$h_\nu(c_1, \ldots, c_n) = g_\nu(\sigma_1, \ldots, \sigma_n),$$

wobei σ_j das j -te elementarsymmetrische Polynom von $c_1, \ldots, c_n$ ist. Das heißt, es gilt

$$f = \prod_{j=1}^{n}(x - c_j) = x^n - \sigma_1 x^{n-1} + \ldots + (-1)^n \sigma_n.$$

Da nach Voraussetzung f ein reelles Polynom ist, gilt $\sigma_j \in \mathbb{R}$ für alle $j = 1, \ldots, n$. Es folgt $s_\nu = h_\nu(c_1, \ldots, c_n) = g_\nu(\sigma_1, \ldots, \sigma_n) \in \mathbb{R}$. Damit ist h ein reelles Polynom und hat somit nach Induktionsvoraussetzung eine komplexe Nullstelle, mit anderen Worten: eine der Nullstellen $y_{ij} = c_i c_j + a(c_i + c_j)$ von h muss komplex sein. Das Indexpaar (i, j) hängt dabei von a ab. Da aber nur endlich viele Indexpaare (i, j) jedoch unendlich viele Parameter a vorkommen, können wir zwei verschiedene reelle Zahlen a, a' und ein Indexpaar (i, j) finden, so dass $c_i c_j + a(c_i + c_j)$ und $c_i c_j + a'(c_i + c_j)$ beide komplex sind! Ohne Einschränkung sei $i = 1$, $j = 2$. Es folgt, dass dann (beachte $a \neq a'$) auch $c_1 + c_2$ und $c_1 c_2$ komplex sind. Die Nullstellen c_1, c_2 von $x^2 - (c_1 + c_2)x + c_1 c_2 \in \mathbb{C}[x]$ sind dann ebenfalls komplex. f besitzt also -wie behauptet- eine komplexe Nullstelle.

Schritt II:
Es sei f ein komplexes normiertes Polynom vom Grad $n > 0$.
Behauptung: f hat eine Nullstelle $z \in \mathbb{C}$.
Zum Beweis betrachte man das Polynom $\bar{f}$, welches das Bild unter dem Isomorphismus $\mathbb{C}[x] \longrightarrow \mathbb{C}[x]$, $\sum_{j=0}^{n} a_j x^j \mapsto \sum_{j=0}^{n} \bar{a}_j x^j$ ist. Dann ist $f\bar{f} \in \mathbb{R}[x]$, wie man leicht nachprüft. $f\bar{f}$ hat also nach Schritt I eine komplexe Nullstelle c. Es folgt $f(c)\bar{f}(c) = 0$. Da $f(\overline{c}) = \overline{\bar{f}(c)}$, ist somit c oder $\overline{c}$ Nullstelle von f. Der Fundamentalsatz ist bewiesen. □

Wie versprochen, soll ein dritter Beweis, der etwas Topologie verwendet, folgen:

- **Dritter Beweis des Fundamentalssatzes**

Hier benutzen wir den etwas scherzhaft *'Hund an einer Leine' Theorem* (*'Dog-on-a-Leash'* Theorem) genannten Satz des berühmten französischen Mathematikers Henri Poincaré (1854-1912):

Läuft ein Mann mit seinem Hund sagen wir n-mal um einen Hydranten und ist sein Abstand zum Hydranten stets größer als die Länge der Hundeleine, so läuft auch der Hund n-mal herum.

Die mathematisch präzise Formulierung benutzt den Begriff der Umlaufzahl.
Es sei $\gamma : [0, 1] \longrightarrow \mathbb{C}\setminus\{0\}$ ein geschlossener Weg, d. h. eine stetige Abbildung mit $\gamma(0) = \gamma(1)$. Man kann genau eine stetige Abbildung $\varphi : [0, 1] \longrightarrow \mathbb{R}$ finden, so dass

$\gamma(t) = |\gamma(t)|\, e^{2\pi i \varphi(t)}$ und $\varphi(0) = 0$. (Da dies anschaulich klar ist, wollen wir das hier nicht beweisen, siehe Fulton loc. cit.) Dann heißt $w(\gamma, 0) := \varphi(1)$ die *Umlaufzahl* von γ bezüglich 0. Wichtig ist nun die sogenannte *Homotopieinvarianz* dieser Definition. Sind $\gamma_0, \gamma_1 : [0, 1] \longrightarrow \mathbb{C}\setminus\{0\}$ zwei *homotope* geschlossene Wege, d. h. gibt es eine stetige Abbildung $H : [0, 1] \times [0, 1] \longrightarrow \mathbb{C}\setminus\{0\}$ mit

$H(t, 0) = \gamma_0(t)$, $H(t, 1) = \gamma_1(t)$, $H(0, s) = H(1, s)$ für alle $t, s \in [0, 1]$, so ist $w(\gamma_0, 0) = w(\gamma_1, 0)$. H nennt man eine *Homotopie* zwischen γ_0 und γ_1. (Zum Beweis siehe Fulton loc. cit.)

Das 'Hund an einer Leine' Theorem lautet nun folgendermaßen:

Satz: Es seien $\gamma_0, \gamma_1 : [0, 1] \longrightarrow \mathbb{C}\setminus\{0\}$ zwei geschlossene Wege und für kein $t \in [0, 1]$ liege 0 auf der Verbindungstrecke von $\gamma_0(t)$ und $\gamma_1(t)$. Dann ist $w(\gamma_0, 0) = w(\gamma_1, 0)$.

Beweis. $H(s, t) = (1 - s)\,\gamma_0(t) + s\,\gamma_1(t)$ definiert eine Homotopie $H : [0, 1] \times [0, 1] \longrightarrow \mathbb{C}\setminus\{0\}$ zwischen γ_0 und γ_1 und somit folgt $w(\gamma_0, 0) = w(\gamma_1, 0)$. □

Die Voraussetzungen dieses Satzes sind offenbar erfüllt, wenn die "Leine kürzer ist als der Abstand des Mannes zum Hypranten". $\gamma_0(t)$ sei der Ort des Mannes, $\gamma_1(t)$ sei der Ort des Hundes und 0 die Position des Hydranten. Dann ist also die Bedingung des Satzes erfüllt, wenn
$|\gamma_0(t) - \gamma_1(t)| < |\gamma_0(t)|$ für alle $t \in [0, 1]$.

Jetzt können wir den dritten Beweis des Fundamentalsatzes führen: Es sei $f = a_n x^n + a_{n-1} x^{n-1} \ldots + a_0 \in \mathbb{C}[x]$ ein Polynom vom Grad $n > 0$. Es sei $r > 0$. Die Umlaufzahl des Weges $\gamma_0(t) = a_n r^n e^{2\pi i n t} = a_n z^n$, $0 \le t \le 1$, bezüglich 0 ist offensichtlich n, denn $\varphi(t) = n\,t$ und $\varphi(1) = n$.

Der Weg $\gamma_1(t) = f(r\, e^{2\pi i\, t}) = f(z)$, $0 \le t \le 1$ hat nach Satz 10.5 die folgende Eigenschaft, wenn man nur r hinreichend groß wählt:
$|\gamma_0(t) - \gamma_1(t)| = |f(z) - a_n z^n| = |a_{n-1} z^{n-1} + \ldots + a_0| < |a_n z^n| = |\gamma_0(t)|$
für alle $t \in [0, 1]$, wobei $z = r\, e^{2\pi i\, t}$.

Nach dem 'Hund an einer Leine' Theorem gilt nun auch $w(\gamma_1, 0) = n$.

Nehmen wir nun an, dass f keine Nullstellen hat. Dann definiert f also eine Abbildung $f : \mathbb{C} \longrightarrow \mathbb{C}\setminus\{0\}$ und somit ist $H : [0, 1] \times [0, 1] \longrightarrow \mathbb{C}\setminus\{0\}$ mit $H(t, s) = f(r\, s\, e^{2\pi i\, t})$ eine Homotopie zwischen dem konstanten Weg $\delta : t \mapsto f(0)$, welcher natürlich die Umlaufzahl 0 hat, und dem Weg γ_1. Es folgt wegen der Homotopieinvarianz der Umlaufzahl $w(\gamma_1, 0) = w(\delta, 0) = 0$, womit wir einen Widerspruch zu $w(\gamma_1, 0) = n > 0$ erhalten haben. Die Annahme war also falsch. f hat also eine komplexe Nullstelle. Damit ist der dritte Beweis beendet. □

Der zweite Beweis des Fundamentalsatzes ist eine schöne Anwendung der Zerfällungskörper und des Hauptsatzes über symmetrische Funktionen.

Eine weitere Anwendung der Zerfällungskörper ist die Klassifikation der endlichen Körper, also der Körper mit nur endlich vielen Elementen. Das wollen wir jetzt untersuchen. Die endlichen Körper spielen eine sehr wichtige Rolle in der Kodierungstheorie (Stichwort: Fehlerkorrigierende Codes, error-correcting codes)

- **Satz 10.10**

Es sei K ein endlicher Körper und $n \geq 1$. Dann gibt es bis auf K-Isomorphie genau eine endliche Erweiterung L von K vom Grad n über K.
Ist q die Anzahl der Elemente von K, so ist L isomorph zum Zerfällungskörper von $f = x^{q^n} - x$ über K.

Beweis. Zur Eindeutigkeit: Es sei $|K| = q$. Ist L Erweiterung von K vom Grad n über K, so ist $|L| = q^n$. Damit ist die multiplikative Gruppe von L von der Ordnung $q^n - 1$ und folglich gilt für alle Elemente $a \in L \setminus 0 : a^{q^n-1} = 1$ und folglich für alle Elemente $a \in L$: $a^{q^n} - a = 0$. Damit zerfällt das Polynom $x^{q^n} - x \in K[x]$ über L in Linearfaktoren. L ist also ein Zerfällungskörper von $x^{q^n} - x$ über K und nach dem Satz über die Eindeutigkeit des Zerfällungskörpers ist L also eindeutig durch den Grad n über K bestimmt.
Zur Existenz: Wir müssen nur noch zeigen, dass der Zerfällungskörper L von $x^{q^n} - x$ über K den Grad n hat. Es ist also zu zeigen, dass L q^n Elemente hat. Zunächst sieht man leicht, dass

$$f = x^{q^n} - x$$

nur einfache Nullstellen in L besitzt. Da die Ableitung f' von f den konstanten Wert -1 hat, denn in L gilt ja $q^n = 0$, sind nach dem folgenden Lemma 10.11 alle Nullstellen von f einfach. Damit folgt, dass L mindestens q^n Elemente hat. Es können aber auch nicht mehr sein: Dazu zeigt man, dass die q^n Nullstellen von f einen Unterkörper F von L bilden. Da L der kleinste Körper ist über dem f in Linearfaktoren zerfällt, ist $L = F$ und wir sind fertig. Zu zeigen ist also nur noch die folgende
Behauptung: Die Menge F der q^n Nullstellen von f ist ein Unterkörper von L.
Beweis. 1) 0, 1 sind Nullstellen von f.
2) Sind a, b Nullstellen von f, so gilt $a^{q^n} = a, b^{q^n} = b$ und da $q = p^m$ mit einer Primzahl p folgt $(a+b)^{q^n} = a^{q^n} + b^{q^n} = a + b$, also ist auch $a + b$ Nullstelle von f.
3) Aus $a^{q^n} = a, b^{q^n} = b$ folgt $(a\,b)^{q^n} = a^{q^n}\, b^{q^n} = a\,b$ und
$(a^{-1})^{q^n} = \left(a^{q^n}\right)^{-1} = a^{-1}$.
Damit ist die Behauptung bewiesen. □

■ **Lemma 10.11**

Es sei K ein Körper und L ein Erweiterungskörper. Ist $f \in K[x]$ und $a \in L$, so gilt: a ist mehrfache Nullstelle von f genau dann, wenn $f(a) = f'(a) = 0$.

Beweis. Die Ableitung f' eines Polynoms $f = \sum_{j=0}^{n} a_j x^j$ wird algebraisch erklärt durch $f' = \sum_{j=1}^{n} j\, a_j x^{j-1}$. Es gelten die bekannten Rechenregeln, z. B. die Produktregel $(f\,g)' = f'\,g + f\,g'$.
Ist nun a eine mehrfache Nullstelle von f, so ist $f = (x-a)^2\, g$, also $f' = 2\,(x-a)\,g + (x-a)^2\, g'$, und somit $f(a) = 0$, $f'(a) = 0$.
Ist umgekehrt $f(a) = 0$ und $f'(a) = 0$, so ist $f = (x-a)\,h$, $f' = h + (x-a)\,h'$ und somit $0 = f'(a) = h(a)$, woraus folgt, dass f ein mehrfache Nullstelle in a besitzt. □

■ **Definition 10.12**

Es sei p eine Primzahl und $q = p^n$. Den Zerfällungskörper von $x^q - x$ über $\mathbb{F}_p$ bezeichnen wir mit $\mathbb{F}_q$.

Nach Satz 10.10 ist $[\mathbb{F}_q : \mathbb{F}_p] = n$. Es ist noch unklar, wie der Körper $\mathbb{F}_q$ im Detail aussieht. Wir wollen die wichtigsten Eigenschaften des Körpers $\mathbb{F}_q$ vorstellen, natürlich mit Beweis! Die erste wichtige Aussage ist die auf den ersten Blick verblüffende Eigenschaft, dass die multiplikative Gruppe von $\mathbb{F}_q$, also $\mathbb{F}_q \backslash 0$, eine zyklische Gruppe ist. Da wir den Hauptsatz über endliche abelsche Gruppen zur Verfügung haben, sollte der Beweis nicht schwierig sein.

■ **Satz 10.13**

(10.13.1) Ist K ein Körper und G eine endliche Untergruppe der multiplikativen Gruppe $K^\times$, so ist G zyklisch.

(10.13.2) Die multiplikative Gruppe $\mathbb{F}_q{}^\times$ von $\mathbb{F}_q$ ist zyklisch von der Ordnung $q - 1$.

Beweis. Wir brauchen nur (10.13.1) zu beweisen. Es sei $d \geq 1$ ein Teiler der Ordnung von G. Da das Polynom $f = x^d - 1$ höchstens d Nullstellen in K hat, besitzt die Gruppe G höchstens d Elemente g mit $g^d = e$ und folglich ist G nach dem folgenden Satz 10.14 zyklisch. □

■ **Satz 10.14**

Es sei G eine endliche abelsche Gruppe der Ordnung m. Für jeden Teiler d von m gebe es höchstens d Elemente $g \in G$ mit $g^d = e$. Dann ist G zyklisch.

Beweis. Wir können den Hauptsatz über endliche abelsche Gruppen heranziehen. G ist ein direktes Produkt zyklischer Gruppen G_j der Ordnung γ_j mit $\gamma_1 \mid \gamma_2 \mid \ldots \mid \gamma_s$.

Ist G nicht zyklisch, also $s > 1$, so gibt es mehr als nur γ_1 Elemente $x \in G$ mit $x^{\gamma_1} = e$. Alle Elemente im direkten Faktor G_1 haben diese Eigenschaft. Da γ_1 Teiler von γ_2 kommen im direkten Faktor G_2 weitere solche Elemente vor. Da γ_1 die Gruppenordnung teilt, haben wir im Fall, dass G nicht zyklisch ist, einen Teiler d der Gruppenordnung gefunden, so dass die Anzahl der Elemente $g \in G$ mit der Eigenschaft $g^d = e$ größer als d ist. □

- **Satz 10.15**

Es sei p eine Primzahl und $q = p^n$.
(10.15.1) Es sei $\theta \in \mathbb{F}_q^\times$ ein Erzeuger der zyklischen Gruppe $\mathbb{F}_q^\times$. Dann gilt $\mathbb{F}_q = \mathbb{F}_p[\theta]$ und das Minimalpolynom $f \in \mathbb{F}_p[x]$ von θ über $\mathbb{F}_p$ ist ein irreduzibles Polynom vom Grad n. Es gilt

$$f = \prod_{k=1}^{n} \left(x - \theta^{p^k}\right).$$

Insbesondere gibt es für jedes $n \geq 1$ mindestens ein irreduzibles Polynom vom Grad n in $\mathbb{F}_p[x]$. Man nennt θ ein *primitives Element* von $\mathbb{F}_q$.

(10.15.2) Die Galoisgruppe $\mathrm{Aut}(\mathbb{F}_q / \mathbb{F}_p)$ hat die Ordnung n.

(10.15.3) Der sogenannte *Frobenius*-Homomorphismus $\Phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ mit $\Phi(a) := a^p$ ist ein Erzeuger der Galoisgruppe $\mathrm{Aut}(\mathbb{F}_q / \mathbb{F}_p)$. Insbesondere ist die Galoisgruppe $\mathrm{Aut}(\mathbb{F}_q / \mathbb{F}_p)$ zyklisch.

(10.15.4) Es gibt eine bijektive Beziehung zwischen den Untergruppen von $\mathrm{Aut}(\mathbb{F}_q / \mathbb{F}_p)$ und den Unterkörpern von $\mathbb{F}_q$. Zur Untergruppe $\langle \Phi^d \rangle$, $d \mid n$, gehört der Unterkörper $\{a \in \mathbb{F}_q \mid \Phi^d(a) = a\} \cong \mathbb{F}_{p^d}$.

Beweis. Zu (10.15.1): Aus $\mathbb{F}_q^\times = \left\{1, \theta, \theta^2, \ldots, \theta^{q-2}\right\}$ folgt natürlich insbesondere $\mathbb{F}_q = \mathbb{F}_p[\theta]$. Da $q = p^n$, hat das Minimalpolynom $f \in \mathbb{F}_p[x]$ von θ über $\mathbb{F}_p$ den Grad n. Es sei

$$f = \textstyle\sum_{k=0}^{n} a_k x^k.$$

Aus $f(\theta) = 0$ folgt $f(\theta^p) = \sum_{k=0}^{n} a_k \theta^{pk} = \sum_{k=0}^{n} (a_k \theta^k)^p = f(\theta)^p = 0$. Damit sind

$$\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$$

die verschiedenen Nullstellen von f.

Zu (10.15.2): Da $\mathbb{F}_q$ der Zerfällungskörper von $x^q - x$ über $\mathbb{F}_p$ ist, und da die Nullstellen von $x^q - x$ einfach sind, hat die Galoisgruppe $\mathrm{Aut}(\mathbb{F}_q / \mathbb{F}_p)$ nach Korollar 9.12 die Ordnung n.

Zu (10.15.3): Da die Charakteristik von $\mathbb{F}_q$ gleich p ist, ist Φ ein Körperisomorphismus. Da θ ein Element der Ordnung $q - 1 = p^n - 1$ ist, ist

$\Phi^k(\theta) = \theta^{p^k} \neq \theta$ für $1 \leq k < n$ und somit ist Φ von der Ordnung $\geq n$, also von der Ordnung n und ein Erzeuger von $\mathrm{Aut}(\mathbb{F}_q / \mathbb{F}_p)$.

Zu (10.15.4): Es sei $\mathcal{A}$ die Menge der Untergruppen von $\mathrm{Aut}(\mathbb{F}_q / \mathbb{F}_p)$ und $\mathcal{B}$ die Menge der Unterkörper von $\mathbb{F}_q$. Ist $H \in \mathcal{A}$, so ist $H = \langle \Phi^d \rangle$ für ein $d > 0$ mit $d \mid n$. $K^H := \{a \in \mathbb{F}_q \mid \Phi^d(a) = a\}$ ist dann ein Unterkörper von $K = \mathbb{F}_q$, wie man sofort sieht. Um die Ordnung von K^H zu bestimmen, schreiben wir $n = d\,r$ mit $r \in \mathbb{N}$. Dann ist $q - 1 = (p^d)^r - 1 = (p^d - 1)\,s$ mit $s \in \mathbb{N}$. Folglich ist
$x^{q-1} - 1 = x^{(p^d-1)\,s} - 1 = \left(x^{(p^d-1)} - 1\right) g$ mit $g \in \mathbb{F}_p[x]$ und somit
$x^q - x = \left(x^{p^d} - x\right) g$. Da die Elemente von $\mathbb{F}_q$ genau die Nullstellen von $x^q - x$ sind, müssen genau p^d Elemente von $\mathbb{F}_q$ Nullstellen von $x^{p^d} - x$ sein. Das sind nach Definition die Elemente in K^H. Also ist $K^H \cong \mathbb{F}_{p^d}$. Die Abbildung $H \mapsto K^H$ ist somit injektiv. Sie ist aber auch surjektiv. Sei dazu $F \subset K$ ein Unterkörper vom Grad d über $\mathbb{F}_p$. Nach der Gradformel ist dann d ein Teiler von n. Weiter ist $F \cong \mathbb{F}_{p^d}$ und somit gilt $a^{p^d} = a$ für alle $a \in F$. Das heißt: $F = K^H$ mit $H = \langle \Phi^d \rangle$. □
Bemerkung: (10.15.4) ist ein Beispiel für den Hauptsatz der Galoistheorie, der für sogenannte Galoiserweiterungen L / K die Untergruppen der Galoisgruppe $\mathrm{Aut}(L / K)$ mit den Zwischenkörpern $K \subset F \subset L$ in eineindeutige Beziehung setzt.

■ Beispiel 10.16

(10.16.1) $\mathbb{F}_8 = \{0, 1, \alpha_2, \ldots, \alpha_7\}$ ist nach Definition der Zerfällungskörper von $x^8 - x$ über $\mathbb{F}_2$. Es gilt $x^8 - x = x(x-1)(x-\alpha_2)\ldots(x-\alpha_7)$. Da $\mathbb{F}_8{}^\times$ zyklisch von der Ordnung 7 ist und 7 eine Primzahl ist, ist jedes Element α_j, $j = 2, \ldots, 7$ ein primitives Element von $\mathbb{F}_8$. Es sei $\alpha = \alpha_2$. Dann ist $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$. Das Minimalpolynom f von $\alpha = \alpha_2$ hat den Grad 3 und, wie wir gesehen haben, die Faktorisierung

$$f = (x - \alpha)(x - \alpha^2)(x - \alpha^4). \tag{10}$$

Da f ein irreduzibles Polynom in $\mathbb{F}_2[x]$ ist, folgt

$$f = x^3 + x^2 + 1 \tag{11}$$

oder

$$f = x^3 + x + 1 \tag{12}$$

(dies sind die einzigen irreduziblen Polynome vom Grad 3 in $\mathbb{F}_2[x]$) und durch Koeffizientenvergleich erhält man aus (10) und (11)
(i) $1 = \alpha + \alpha^2 + \alpha^4$, $0 = \sigma_2(\alpha, \alpha^2, \alpha^4) = \alpha^3 + \alpha^5 + \alpha^6$, $1 = \alpha^7$
und aus (10) und (12)
(ii)= $0 = \alpha + \alpha^2 + \alpha^4$, $1 = \sigma_2(\alpha, \alpha^2, \alpha^4) = \alpha^3 + \alpha^5 + \alpha^6$, $1 = \alpha^7$.
Man kann dies aber jeweils auch direkt aus der Relation $f(\alpha) = 0$ ableiten. Wir demonstrieren dies im Fall (i): Aus der Isomorphie
$\mathbb{F}_2[x] / \langle x^3 + x^2 + 1 \rangle \cong \mathbb{F}_8$, $x \mapsto \alpha$, folgt

$\alpha^3 = 1 + \alpha^2$ und somit folgt weiter
$\alpha^4 = \alpha\,\alpha^3 = \alpha(1+\alpha^2) = \alpha + \alpha^3 = 1 + \alpha + \alpha^2$, Hat α
$\alpha^5 = \alpha(1+\alpha+\alpha^2) = \alpha + \alpha^2 + \alpha^3 = 1 + \alpha$, $\alpha^6 = \alpha^3 + \alpha^5 = 1 + \alpha^2 + 1 + \alpha = \alpha + \alpha^2$,
$\alpha^7 = 1$.
das Minimalpolynom $x^3 + x^2 + 1$, so folgt für $\beta = \alpha^3$ die Gleichung $\beta^3 + \beta + 1 = \alpha^9 + \alpha^3 + 1 = \alpha^2 + \alpha^3 + 1 = 0$. β hat also das Minimalpolynom $x^3 + x + 1$.
Es ist klar: alle irreduziblen Polynome desselben Grades n in $\mathbb{F}_q[x]$ definieren (bis auf Isomorphie) denselben Erweiterungskörper vom Grad n von $\mathbb{F}_q$. Das ist vollständig verschieden von der Situation in Charakteristik Null. Es gibt sehr viele verschiedene (nicht isomorphe) Körpererweiterungen von festem Grad von $\mathbb{Q}$ oder etwa von $\mathbb{C}(x)$, dem Körper der komplexen rationalen Funktionen in einer Unbekannten. Der Fall der endlichen Erweiterungen $K/\mathbb{Q}$ 'ist' die *algebraische Zahlentheorie* und der Fall der endlichen Erweiterungen $K/\mathbb{C}(x)$ ist die *Theorie der algebraischen Kurven*. Das sind zwei klassische, wundervolle Gebiete der Reinen Mathematik mit einer Fülle tiefliegender Theoreme.

Wir wollen zum Abschluss die Frage untersuchen, wieviele irreduzible Polynome vom Grad d es in $\mathbb{F}_q[x]$ gibt. Etwas elementare Zahlentheorie kommt hier ins Spiel.

- **Satz 10.17**

Es sei p eine Primzahl, $n \geq 1$, $q = p^n$. Mit F_d werde das Produkt aller normierten irreduziblen Polynome vom Grad d in $\mathbb{F}_q[x]$ bezeichnet. Dann gilt:

(10.17.1) $x^{q^m} - x = \prod_{d|m} F_d$ für alle $m \in \mathbb{N}$.

Bezeichnet man mit $N_d(q)$ die Anzahl aller normierten irreduziblen Polynome vom Grad d in $\mathbb{F}_q[x]$, so gilt

(10.17.2) $q^m = \sum_{d|m} d\,N_d(q)$ für alle $m \in \mathbb{N}$.

Beweis. Der Beweis erfolgt in mehreren Schritten.
1. Behauptung. Wir überlegen uns zunächst, dass jeder irreduzible Faktor von $x^{q^m} - x$ nur einfach vorkommt.
Beweis. Für $f, g \in \mathbb{F}_q[x]$ gilt nämlich:
$x^{q^m} - x = f^2 g \Longrightarrow -1 = q^m x^{q^m-1} - 1 = 2 f f' g + f^2 g' \Longrightarrow f$ ist Einheit in $\mathbb{F}_q[x]$.
2. Behauptung. Ist $f \in \mathbb{F}_q[x]$ normiertes irreduzibles Polynome vom Grad d, und ist d Teiler von m, so ist f Teiler von $x^{q^m} - x$.
Beweis. Sei $K = \mathbb{F}_q[x]/\langle f\rangle$ und $\alpha = x + \langle f\rangle$ sei die Restklasse von x. Dann ist $f(\alpha) = 0$ und f ist das Minimalpolynom von α. Der Fall $\alpha = 0$, d.h. $f = x$, ist trivial. Es sei also $\alpha \neq 0$. Da K q^d Elemente hat, gilt dann $\alpha^{q^d-1} = 1$ und da $d \mid m$, gilt auch $q^d - 1 \mid q^m - 1$, also folgt $\alpha^{q^m-1} = 1$. Damit ist α eine Nullstelle von $x^{q^m} - x$. Da f das Minimalpolynom von α ist, ist f ein Teiler von $x^{q^m} - x$ in $\mathbb{F}_q[x]$.

3. Behauptung. Ist $f \in \mathbb{F}_q[x]$ normiertes irreduzibles Polynome vom Grad d, und ist f Teiler von $x^{q^m} - x$, so ist d Teiler von m.
Beweis. Es sei $x^{q^m} - x = f\,g$ und wie oben sei $K = \mathbb{F}_q[x]/\langle f\rangle$ und $\alpha = x + \langle f\rangle$ die Restklasse von x. Aus $f(\alpha) = 0$ folgt dann $\alpha^{q^m} = \alpha$. Für beliebige $\beta = \sum_{j=0}^{d} a_j\,\alpha^j$, $a_j \in \mathbb{F}_q$, folgt

$$\beta^{q^m} = \sum_{j=0}^{d} (a_j\,\alpha^j)^{q^m} = \sum_{j=0}^{d} a_j\big(\alpha^{q^m}\big)^j = \sum_{j=0}^{d} a_j\,\alpha^j = \beta.$$

Damit ist $x - \beta$ und folglich auch $x^{q^d} - x = \prod_{\beta\in K} (x - \beta)$ ein Teiler von $x^{q^m} - x$. Das geht nur, wenn d ein Teiler von m ist, wie das nachfolgende Lemma zeigt. Damit ist (10.17.1) beweisen. (10.17.2) folgt durch Gradbilden aus (10.17.1). □

- **Lemma 10.18**

Es sei K irgendein Körper. Für $a, b \in \mathbb{N}$, $a, b > 0$ gilt: Ist $x^a - 1$ Teiler von $x^b - 1$ in $K[x]$, so gilt $a \mid b$. Ist $q \in \mathbb{N}$, $q > 1$ und $a = q^d - 1$, $b = q^m - 1$, so folgt weiter $d \mid m$.

Beweis. Es sei $b = s\,a + r$, $0 \le r < a$. Es folgt:
$x^b - 1 = x^{s\,a+r} - 1 = x^r(x^{s\,a} - 1) + x^r - 1$. Da $x^a - 1$ Teiler von $x^b - 1$ und von $x^{s\,a} - 1$, folgt, dass $x^a - 1$ auch Teiler von $x^r - 1$ ist. Aus Gradgründen muss $r = 0$ gelten. Also ist a Teiler von b. Aus $q^d - 1 \mid q^m - 1$ folgt mit demselben (etwas modifizierten) Argument $d \mid m$. □

Mit der Möbiusschen Umkehrformel erhalten wir aus (10.17.2) ein explizite Formel für die Anzahl $N_d(q)$. Das wollen wir jetzt erklären.

- **Definition 10.19**

Die *Möbiusfunktion* $\mu : \mathbb{N}_+ \longrightarrow \mathbb{N}$ ist definiert durch $\mu(n) := 0$, wenn n eine Quadratzahl größer als 1 als Faktor besitzt. Ist dagegen n quadratfrei und ist k die Anzahl der Primfaktoren, so ist $\mu(n) := (-1)^k$.
Offensichtlich gilt $\mu(1) = 1$, $\mu(n\,m) = \mu(n)\,\mu(m)$, wenn n, m teilerfremd sind.

Weiter gilt für $n = {p_1}^{\alpha_1} \ldots {p_k}^{\alpha_k}$, wobei $p_1, \ldots, p_k$ paarweise verschiedene Primzahlen, $\alpha_i > 0$ $(k > 0)$ und $n_0 := p_1 \ldots p_k$, die Gleichung:

(*) $$\sum_{d\mid n} \mu(d) = \sum_{d\mid n_0} \mu(d) = \sum_{j=0}^{k} \binom{k}{j} (-1)^j = (1-1)^k = 0.$$

- **Lemma 10.20 (Möbiussche Umkehrformel)**

Es seien $f, g : \mathbb{N}_+ \longrightarrow \mathbb{N}$ Funktionen und es gelte $f(m) = \sum_{d\mid m} g(d)$. Dann gilt:

$$g(m) = \sum_{d|m} \mu(\tfrac{m}{d})\, f(d).$$

Beweis.

$$\sum_{m|k} \mu(\tfrac{k}{m})\, f(m) = \sum_{m|k} \mu(\tfrac{k}{m}) \sum_{d|m} g(d) = \sum_{d|k} g(d) \sum_{d|m|k} \mu(\tfrac{k}{m})$$

Nach (*) gilt für alle Teiler d von k:

$$\sum_{d|m|k} \mu(\tfrac{k}{m}) = \sum_{s|\frac{k}{d}} \mu(s) = \begin{cases} 1, & \text{falls } d = k \\ 0, & \text{falls } d < k. \end{cases}$$

Setzt man dies oben ein, so ergibt sich die Umkehrformel. □

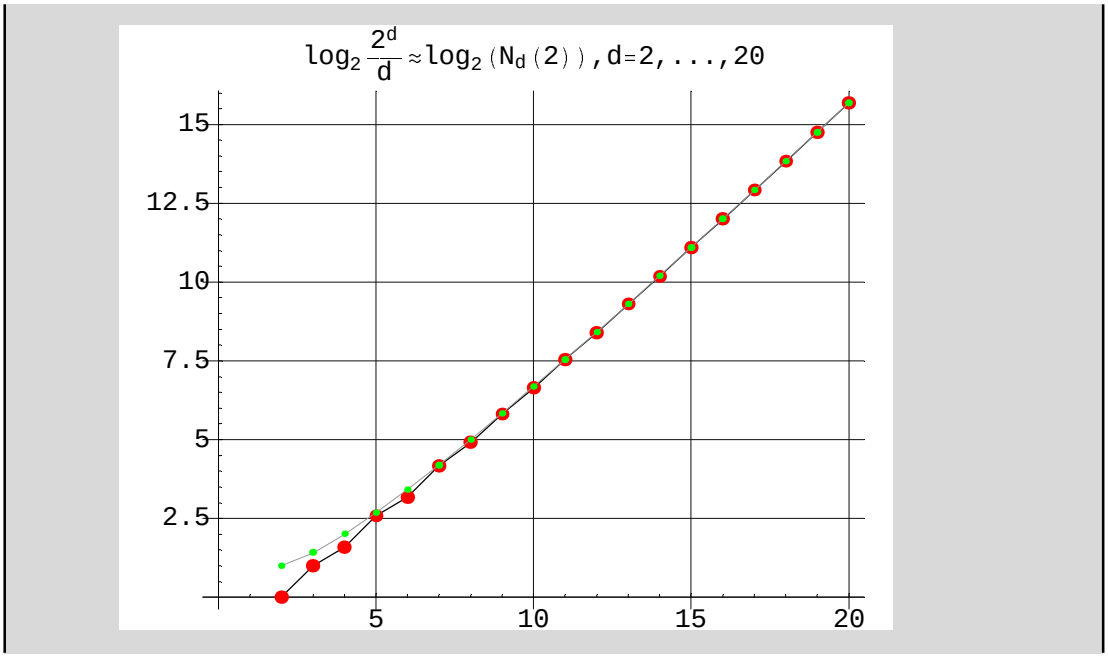
Aus (10.17.2) folgt jetzt mithilfe der Umkehrformel

- **Korollar 10.21**

$$N_m(q) = \tfrac{1}{m} \sum_{d|m} q^d\, \mu(\tfrac{m}{d}).$$ □

Man sieht, dass $\log_q N_m(q)$ ungefähr mit $\log_q \frac{q^m}{m} = m - \log_q m$ übereinstimmt.

Beispiel: $\log_2 N_d(2)$ für $d = 2, 3, \ldots, 20$. (rote Punkte)



Die Zahlenwerte $\left[\frac{2^d}{d}\right]$, $N_d(2)$ für $d = 2, \ldots, 20$.

d	$[\frac{2^d}{d}]$	$N_d(2)$
2	2	1
3	2	2
4	4	3
5	6	6
6	10	9
7	18	18
8	32	30
9	56	56
10	102	99
11	186	186
12	341	335
13	630	630
14	1170	1161
15	2184	2182
16	4096	4080
17	7710	7710
18	14563	14532
19	27594	27594
20	52428	52377

Obwohl es viele irreduzible Polynome von gegebenem Grad gibt, ist es in der Regel sehr schwierig für ein vorgelegtes Polynom in $\mathbb{F}_q[x]$ zu entscheiden, ob es irreduzibel ist.

■ Übungen 10

(10.1) Zeigen Sie: Ist $f = x^n + a_{n-1}x^{n-1} ... + a_0 \in \mathbb{C}[x]$ ein normiertes Polynom vom Grad $n > 0$ und $\alpha \in \mathbb{C}$ eine Nullstelle von f, so ist $|\alpha| \leq 1 + 2\max_{0 \leq i < n} |a_i|$.

(10.2) Welche Gestalt haben die irreduziblen Polynome in $\mathbb{R}[x]$ in $\mathbb{C}[x]$. Welche endlichen Körpererweiterungen besitzt $\mathbb{R}$?

(10.3)* Zeigen Sie: Ist $x^n + x + 1$ irreduzibel in $\mathbb{F}_2[x]$, so ist auch $x^n + x^{n-1} + 1$ irreduzibel in $\mathbb{F}_2[x]$.

(10.4) Wieviele Unterkörper hat $\mathbb{F}_q$ a) für $q = p^{13}$, b) allgemein für $q = p^n$?

(10.5) Es sei K ein Körper und $F_1, F_2 \subset K$ seien endliche Unterkörper mit gleich vielen Elementen. Zeigen Sie: $F_1 = F_1$ (d. h. F_1, F_2 sind als Teilmengen gleich, nicht nur isomorph).

(10.6) Es sei t eine Unbestimmte, p Primzahl. Dann ist $R = \mathbb{F}_p[t^p]$ ein Unterring von $S = \mathbb{F}_p[t]$. Es sei K der Quotientenkörper von R und L der Quotientenkörper von S.

L ist dann ein Erweiterungskörper von K. Zeigen Sie:
a) t ist algebraisch über K und es gilt $L = K[t]$.
b) Bestimmen Sie das Minimalpolynom f von t über K. Ist L der Zerfällungskörper von f?
c) Bestimmen Sie $\mathrm{Aut}(L/K)$.

(10.7) Zeigen Sie $\cos\frac{\pi}{9}$ ist nicht mit Zirkel und Lineal aus 0, 1 konstruierbar.

(10.8) Seien F, K endliche Körper. Wann kann gibt es einen Homomorphismus $F \longrightarrow K$?

(10.9) Es sei $K = \mathbb{F}_{16}$ und $\theta \in K$ mit $K = \mathbb{F}_2[\theta]$. Ist dann θ ein Erzeuger der multiplikativen Gruppe $K^\times$?

(10.10) Es seien K, L endliche Körper, L Erweiterung von K. Bestimmen Sie die Galoisgruppe $\mathrm{Aut}(L/K)$.