Joachim Gräter

Algebra und Arithmetik

Potsdam, September 2004

Prof. Dr. J. Gräter
Universität Potsdam, Institut für Mathematik
Am Neuen Palais 10, 14469 Potsdam

Die neueste Version dieses Skriptes ist erhältlich unter
http://users.math.uni-potsdam.de/~graeter/

Inhaltsverzeichnis

KAPITEL 1

Gruppen

1. Gruppen

Definition 1.1 *Sei G eine Menge und $G \times G \longrightarrow G, (a,b) \longmapsto ab$ eine Verknüpfung. G heißt bezüglich dieser Verknüpfung Gruppe, wenn gilt:*

i) $a(bc) = (ab)c$ *für alle* $a, b, c \in G$ *(Assoziativgesetz).*

ii) Es gibt ein $e \in G$*, so daß* $ae = ea = a$ *für alle* $a \in G$ *gilt.*

iii) Zu jedem $a \in G$ *gibt es* $b \in G$ *mit* $ab = ba = e$*.*

Bemerkung.

1. Die Verknüpfung von n Elementen führt bei beliebiger Klammerung unter Einhaltung der Reihenfolge immer zum gleichen Ergebnis (allgemeines Assoziativgesetz).

2. G heißt abelsch, wenn $ab = ba$ für alle $a, b \in G$ gilt.

3. e heißt neutrales Element oder Einselement und ist eindeutig bestimmt.

4. Für jedes $a \in G$ gibt es genau ein $b \in G$ mit $ab = ba = e$. Man schreibt $b = a^{-1}$, und a^{-1} heißt inverses Element von a. Es gilt z.B. $(a^{-1})^{-1} = a$ und $(a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}$.

5. Erfüllt G nur i) und ii), so heißt G Monoid oder Halbgruppe mit Einselement. $a \in G$ heißt dann invertierbar oder Einheit, wenn es ein $b \in G$ mit $ab = ba = e$ gibt. Die Bemerkungen 1. bis 4. gelten entsprechend.

6. Die Verknüpfung in Definition 1.1 bezeichnet man auch als (Gruppen-) Multiplikation, und statt ab schreibt man auch $a \cdot b$ oder $a \circ b$. Insbesondere bei abelschen Gruppen benutzt man auch die Addition als Gruppenverknüpfung. So ist zum Beispiel $\mathbb{Z}$ eine Gruppe bezüglich $+$. Das Inverse von $a \in G$ wird dann nicht mit a^{-1} sondern mit $-a$ bezeichnet und das neutrale Element mit 0.

Satz 1.2 *Ist M ein Monoid, so ist* $\mathrm{E}(M) := \{a \in M \mid a \text{ ist invertierbar }\}$ *eine Gruppe bezüglich der Verknüpfung von M.*

Beweis. Zunächst muß gezeigt werden, daß die Verknüpfung von M auf $\mathrm{E}(M)$ eine Verknüpfung induziert, d.h., für alle $a, b \in \mathrm{E}(M)$ muß $ab \in \mathrm{E}(M)$ gelten. Wegen $a, b \in \mathrm{E}(M)$ ist $a^{-1}, b^{-1} \in M$. Damit folgt $(ab)(b^{-1}a^{-1}) = aa^{-1} = e$ und $(b^{-1}a^{-1})(ab) = b^{-1}b = e$, also $ab \in \mathrm{E}(M)$.

Das Assoziativgesetz gilt in M, also auch in $\mathrm{E}(M)$.

Ist e das neutrale Element von M, so folgt wegen $ee = e$ auch $e \in \mathrm{E}(M)$, und e ist das neutrale Element von $\mathrm{E}(M)$.

Für jedes invertierbare $a \in M$ ist auch a^{-1} invertierbar, also $a^{-1} \in \mathrm{E}(M)$.

□

Bemerkung. $\mathrm{E}(M)$ heißt Einheitengruppe von M.

Beispiel.

1. Die Mengen $\mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ sind abelsche Gruppen bezüglich der Addition. Bezüglich der Multiplikation sind $\mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ Monoide, die keine Gruppen sind. Es gilt $\mathrm{E}(\mathbb{Z}) = \{1, -1\}$, $\mathrm{E}(\mathbb{Q}) = \mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ und $\mathrm{E}(\mathbb{R}) = \mathbb{R}^\times := \mathbb{R} \setminus \{0\}$.

2. Ist M eine nichtleere Menge, so bezeichnet $\mathrm{Abb}(M) := \{f \mid f : M \longrightarrow M\}$ die Menge aller Abbildungen von M nach M, und $\mathrm{Abb}(M)$ ist ein Monoid bezüglich der Hintereinanderausführung $\circ$. Ein $f \in \mathrm{Abb}(M)$ ist genau dann bezüglich $\circ$ invertierbar, wenn f bijektiv ist, d.h. $\mathrm{E}(\mathrm{Abb}(M)) = \{f \mid f : M \longrightarrow M \text{ bijektiv }\}$.

3. Ist K ein Körper (z.B. $K = \mathbb{Q}$), so bezeichnet $K_{n,n}$ die Menge aller (n, n)-Matrizen über K, und $K_{n,n}$ ist ein Monoid bezüglich des Matrizenproduktes. Die Einheitengruppe von $K_{n,n}$ bezeichnet man mit $\mathrm{GL}(n; K)$. Sie besteht aus den regulären (n, n)- Matrizen über K, d.h. aus den Matrizen $A \in K_{n,n}$ mit $\det(A) \neq 0$.

Potenzen eines Elementes a in einem Monoid.

Die Potenzen a^n mit $n \in \mathbb{N}_0$ definiert man rekursiv durch $a^0 := e$ und $a^n := a^{n-1}a$ mit $n \geq 1$. Für alle $n, m \in \mathbb{N}_0$ gilt dann

$$a^{n+m} = a^n a^m, \quad (a^n)^m = a^{n \cdot m}.$$

Ist a eine Einheit, so definiert man für alle $n \in \mathbb{N}$:

$$a^{-n} := (a^{-1})^n.$$

Es gilt dann für alle $n, m \in \mathbb{Z}$:

$$a^{n+m} = a^n a^m, \quad (a^n)^m = a^{n \cdot m}.$$

$\langle a \rangle$ bezeichnet die Menge aller Potenzen von a. Ist a invertierbar, so gilt

$$\langle a \rangle = \{e, a, a^{-1}, a^2, a^{-2}, a^3, a^{-3}, \ldots\}.$$

Das kleinste $n \in \mathbb{N}$ mit $a^n = e$ heißt Ordnung von a, geschrieben $\mathrm{ord}a = n$, und die Elemente $e, a, a^2, \ldots, a^{\mathrm{ord}a-1}$ sind genau die verschiedenen Potenzen von a (vgl. Aufgabe 3.1). Gibt es kein $n \geq 1$ mit $a^n = e$, so hat a unendliche Ordnung, geschrieben $\mathrm{ord}a = \infty$. In diesem Falle sind $e, a, a^{-1}, a^2, a^{-2}, \ldots$ alle verschieden. Schreibt man die Verknüpfung nicht multiplikativ, sondern additiv, so spricht man nicht von den Potenzen eines Elementes, sondern von den Vielfachen. Statt a^n schreibt man $na = a + a + \ldots + a$, $0a = 0$ und $\langle a \rangle = \{0, \pm a, \pm 2a, \ldots\}$. Die Ordnung von a ist dann das kleinste $n \in \mathbb{N}$ mit $na = 0$.

Definition 1.3 *Sei G eine Gruppe.*

i) *$|G|$ heißt Ordnung von G, geschrieben* $\mathrm{ord}G = |G|$.

ii) *G heißt zyklisch, wenn es ein $a \in G$ mit $G = \langle a \rangle$ gibt. a heißt dann erzeugendes Element von G.*

Bemerkung.

1. $G = \langle a \rangle \Longrightarrow \mathrm{ord}G = \mathrm{ord}a$.

2. Jede zyklische Gruppe $G = \langle a \rangle$ ist abelsch, denn für alle $n, m \in \mathbb{Z}$ gilt $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$.

Beispiel.

1. $\mathbb{Z}$ ist bezüglich $+$ eine zyklische Gruppe, denn es gilt $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$. Also sind 1 und -1 jeweils erzeugende Elemente. Die additiven Gruppen $\mathbb{Q}$ und $\mathbb{R}$ sind nicht zyklisch.

2. Die komplexen Zahlen $1, -1, i, -i$ bilden bezüglich der Multiplikation eine zyklische Gruppe, denn es gilt $\{1, -1, i, -i\} = \{i^0, i^1, i^2, i^3\}$. Neben i ist auch $-i$ ein erzeugendes Element.

Die symmetrischen Gruppen $\mathbf{S}_n$.

Wegen Beispiel 2 nach Satz 1.2 ist für jedes $n \in \mathbb{N}$ die Menge der Bijektionen der Menge $\{1, 2, \ldots, n\}$ bezüglich der Komposition eine Gruppe. Sie heißt symmetrische Gruppe, geschrieben $\mathbf{S}_n$. Die Elemente von $\mathbf{S}_n$ heißen Permutationen, die sich auf unterschiedliche Weise darstellen lassen. So schreibt man z.B. für $\pi \in \mathbf{S}_n$, also $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ bijektiv,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}.$$

Ist zum Beispiel $n = 3$ und

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

so gilt $\pi(1) = 3, \pi(2) = 1, \pi(3) = 2$ sowie

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Da es genau $n!$ Möglichkeiten gibt, die Zahlen $1, 2, \ldots, n$ anzuordnen, folgt unter Benutzung obiger Darstellung, daß $|\mathbf{S}_n| = n!$ für alle $n \in \mathbb{N}$ gilt.

$\pi \in \mathbf{S}_n$ heißt Zykel der Länge r, wenn es paarweise verschiedene $k_1, \ldots, k_r$ aus $\{1, \ldots, n\}$ gibt, so daß gilt:

i) $\pi(k_1) = k_2, \pi(k_2) = k_3, \ldots, \pi(k_r) = k_1$.
ii) $\pi(k) = k$ für $k \neq k_i, i = 1, \ldots, r$.

Zykeln der Länge 2 heißen Transpositionen. Ist π ein Zykel wie oben angegeben, so schreibt man $\pi = (k_1 k_2 \ldots k_r)$, und es gilt dann $\pi = (k_2 k_3 \ldots k_r k_1) = (k_3 k_4 \ldots k_r k_1 k_2) = \ldots$.

Beispiel. Für $\pi \in \mathbf{S}_7$ mit $\pi(1) = 3, \pi(2) = 2, \pi(3) = 5, \pi(4) = 1, \pi(5) = 7, \pi(6) = 6, \pi(7) = 4$ gilt $\pi = (13574)$. Kein Zykel ist dagegen

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

Jede Permutation läßt sich als Produkt von (elementfremden) Zykeln schreiben. Zum Beispiel gilt

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 4 & 1 & 5 \end{pmatrix} = (165) \circ (23) \circ (4).$$

Für π aus $\mathbf{S}_n$ heißt

$$\mathrm{sgn}\pi := \prod_{j<i} \frac{\pi(i) - \pi(j)}{i - j}$$

Signum von π.

Es gilt stets $\mathrm{sgn}\pi \in \{1, -1\}$, da im Zähler und Nenner bis auf das Vorzeichen und die Reihenfolge dieselben Faktoren vorkommen. Für $a \neq b$ gilt zum Beispiel $\mathrm{sgn}(ab) = -1$. Um das einzusehen, sei o.B.d.A. $a = 1$ und $b = 2$, also $\pi = (12)$. Dann folgt

$$\mathrm{sgn}(12) = \prod_{j<i} \frac{\pi(i) - \pi(j)}{i - j} = \frac{\pi(2) - \pi(1)}{2 - 1} \cdot \prod_{3 \leq i} \frac{\pi(i) - \pi(1)}{i - 1} \frac{\pi(i) - \pi(2)}{i - 2} = \frac{1 - 2}{2 - 1} = -1.$$

Wichtig ist nun der folgende

Satz. *Für alle $\pi, \sigma \in \mathbf{S}_n$ gilt:*

$$\mathrm{sgn}(\pi \circ \sigma) = \mathrm{sgn}\pi \cdot \mathrm{sgn}\sigma.$$

Beweis.

$$\operatorname{sgn}(\pi\circ\sigma)=\prod_{j<i}\frac{\pi\circ\sigma(i)-\pi\circ\sigma(j)}{i-j}=\prod_{j<i}\frac{\pi(\sigma(i))-\pi(\sigma(j))}{\sigma(i)-\sigma(j)}\cdot\prod_{j<i}\frac{\sigma(i)-\sigma(j)}{i-j}=\operatorname{sgn}\pi\cdot\operatorname{sgn}\sigma.$$

□

Ist zum Beispiel $\pi\in\mathbf{S}_n$ ein Zykel, etwa $\pi=(a_1\ldots a_k)$, so folgt

$$\pi=(a_1a_k)\circ(a_1a_{k-1})\circ\ldots\circ(a_1a_3)\circ(a_1a_2),$$

und wegen des obigen Satzes gilt dann

$$\operatorname{sgn}(a_1\ldots a_k)=(-1)^{k-1}.$$

Da jede Permutation Produkt von Zykeln ist, ist damit jede Permutation π Produkt von Transpositionen:

$$\pi=\tau_1\circ\ldots\circ\tau_r,\ \tau_i\ \text{ Transposition.}$$

Obiger Satz liefert $\operatorname{sgn}\pi=(-1)^r$.

$$\pi\text{ heißt gerade }\ :\Longleftrightarrow\ \operatorname{sgn}\pi=1.$$

$$\pi\text{ heißt ungerade }\ :\Longleftrightarrow\ \operatorname{sgn}\pi=-1.$$

π ist also genau dann gerade, wenn bei jeder Darstellung von π als Produkt von Transpositionen die Anzahl der Transpositionen gerade ist.

Beispiel. Ist $\pi=(12387)\circ(6537)$, dann folgt $\operatorname{sgn}\pi=(-1)^{4+3}=-1$. Somit ist π ungerade. Zum Beispiel gilt $\pi=(17)\circ(18)\circ(13)\circ(12)\circ(67)\circ(63)\circ(65)$.

Das direkte Produkt von Gruppen.

Sind G und H zwei Gruppen, so ist die Menge $G\times H=\{(g,h)\mid g\in G,h\in H\}$ bezüglich der Verknüpfung

$$(g_1,h_1)(g_2,h_2):=(g_1g_2,h_1h_2)$$

eine Gruppe, wie man sich leicht überlegt. $G\times H$ heißt dann direktes Produkt von G und H. Entsprechend kann man ganz allgemein für Gruppen $G_1,\ldots,G_n$ das direkte Produkt $G_1\times\ldots\times G_n$ definieren. Dabei ist die zugehörige Verknüpfung komponentenweise definiert. Ist e_i das neutrale Element von $G_i(i=1,\ldots,n)$, dann ist $(e_1,\ldots,e_n)$ das neutrale Element von $G_1\times\ldots\times G_n$, und für $g_i\in G_i,i=1,\ldots,n$ gilt

$$(g_1,\ldots,g_n)^{-1}=(g_1^{-1},\ldots,g_n^{-1}).$$

Wählen wir zum Beispiel $G=H=\mathrm{E}(\mathbb{Z})=\{1,-1\}$, so ist

$$G\times H=\{(g,h)\mid g,h\in\{1,-1\}\}$$

eine Gruppe mit 4 Elementen. Wie man leicht nachrechnet, hat jedes Element aus $G\times H$ die Ordnung 1 oder 2, d.h., $G\times H$ ist nicht zyklisch.

Definition 1.4 *Ist G eine Gruppe und $U \subseteq G$ eine Teilmenge von G, so heißt U Untergruppe von G, wenn U bezüglich der Verknüpfung von G selbst eine Gruppe ist.*

Bemerkung. Ist U eine Untergruppe von G, so gilt insbesondere $ab \in U$ für alle $a, b \in U$.

Beispiel.

1. G und $\{e\}$ sind Untergruppen von G.

2. Bezüglich der Addition ist $\mathbb{Z}$ eine Untergruppe von $\mathbb{Q}$ und $\mathbb{Q}$ eine Untergruppe von $\mathbb{R}$. Bezüglich der Multiplikation ist $\mathbb{Q}^\times$ eine Untergruppe von $\mathbb{R}^\times$.

3. Ist K ein Körper und $\mathrm{SL}(n; K)$ die Menge der (n, n)-Matrizen über K mit Determinante 1, so ist $\mathrm{SL}(n; K)$ eine Untergruppe von $\mathrm{GL}(n; K)$.

Satz 1.5 *Eine nichtleere Teilmenge U einer Gruppe G ist genau dann eine Untergruppe von G, wenn für alle $a, b \in U$ gilt $ab^{-1} \in U$.*

Beweis. $''\Rightarrow''$: Die Gleichung $xb = a$ hat in U und G dieselbe eindeutige Lösung.
$''\Leftarrow''$: Wegen $U \neq \emptyset$ gibt es ein $a \in U$, und es folgt $aa^{-1} = e \in U$. Für jedes $u \in U$ folgt somit $u^{-1} = eu^{-1} \in U$, und sind $x, y \in U$, so ergibt sich $y^{-1} \in U$, also $xy = x(y^{-1})^{-1} \in U$.
□

Bemerkung. Aus obigem Beweis geht hervor, daß das neutrale Element einer Gruppe auch das neutrale Element jeder Untergruppe ist.

Korollar 1.6 *Ist G eine Gruppe und $a \in G$, so ist $\langle a \rangle$ eine Untergruppe von G.*

Beweis. Wegen $a \in \langle a \rangle$ ist $\langle a \rangle$ nicht leer, und sind $a^n, a^m \in \langle a \rangle$ mit $n, m \in \mathbb{Z}$, so folgt $a^n(a^m)^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle$. Wegen Satz 1.5 folgt die Behauptung.
□

Korollar 1.7 *Ist G eine Gruppe und $\{U_i | i \in I\}$ eine Menge von Untergruppen von G, so ist $U := \cap_{i \in I} U_i$ eine Untergruppe von G.*

Beweis. Für alle $i \in I$ gilt $e \in U_i$, also $e \in \cap_{i \in I} U_i$, d.h., $\cap_{i \in I} U_i$ ist nicht leer. Aus $a, b \in \cap_{i \in I} U_i$ folgt $a, b \in U_i$ für jedes $i \in I$, also $ab^{-1} \in U_i$ für jedes $i \in I$, d.h. $ab^{-1} \in \cap_{i \in I} U_i$. Wegen Satz 1.5 folgt die Behauptung.
□

Bemerkung.

1. Sind $U_1, \ldots, U_n$ Untergruppen von G, dann ist $U_1 \cap \ldots \cap U_n$ eine Untergruppe von G.

2. Gilt $I = \emptyset$, so folgt $\cap_{i \in I} U_i = G$.

Anwendung. Sind $a_1, \ldots, a_n \in G$, dann bezeichnet $\langle a_1, \ldots, a_n \rangle$ den Durchschnitt aller Untergruppen von G, die $a_1, \ldots, a_n$ enthalten. $\langle a_1, \ldots, a_n \rangle$ heißt die von $a_1, \ldots, a_n$ erzeugte Untergruppe und ist die kleinste Untergruppe von G, die $a_1, \ldots, a_n$ enthält. $\langle a \rangle$ bezeichnet nun einerseits die kleinste Untergruppe von G, die a enthält, und andererseits die Menge aller Potenzen von a. Wie man sich leicht überlegt, stimmen beide überein.

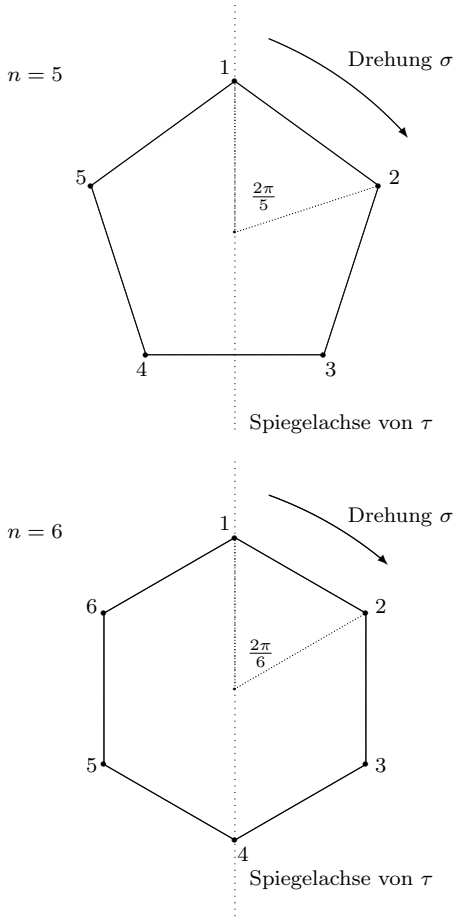
Beispiel. Für jedes $n \in \mathbb{N}, n > 2$ ist $\mathrm{D}_n = \langle \sigma, \tau \rangle$ die Untergruppe von $\mathbf{S}_n$, die von $\sigma, \tau \in \mathbf{S}_n$ mit

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ 2 & 3 & \ldots & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$$

erzeugt wird. D_n heißt Diedergruppe. Offenbar gilt $\mathrm{ord}\sigma = n,\ \mathrm{ord}\tau = 2$, und man überlegt sich weiterhin, daß auch folgendes gilt:

1. $\sigma\tau = \tau\sigma^{n-1}$.
2. $\mathrm{D}_n = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \ldots, \tau\sigma^{n-1}\}$.
3. $\mid \mathrm{D}_n \mid = 2n$.

Die Diedergruppe D_n läßt sich als Symmetriegruppe des regelmäßigen $n-$Ecks deuten. Dabei entspricht σ der positiven Drehung um den Mittelpunkt mit dem Winkel $\frac{2\pi}{n}$ und τ der Spiegelung an einer fest gewählten Geraden durch den Mittelpunkt und einen Eckpunkt.



Nebenklassen einer Untergruppe.

Ist G eine Gruppe und U eine Untergruppe von G, so definiert man für jedes $a \in G$:

$$aU = \{au \mid u \in U\} \quad \text{und} \quad Ua = \{ua \mid u \in U\}.$$

aU heißt Linksnebenklasse von U, und G/U bezeichnet die Menge aller Linksnebenklassen von U. Entsprechend heißt Ua Rechtsnebenklasse von U, und $U\backslash G$ ist die Menge alle Rechtsnebenklassen von U.

Einfache Eigenschaften.

1. $|aU| = |bU|$ für alle $a, b \in G$, denn $aU \longrightarrow bU, au \longmapsto bu$ ist eine Bijektion. Entsprechend gilt $|Ua| = |Ub|$ für alle $a, b \in G$.

2. Sind aU und bU verschieden, so gilt $aU \cap bU = \emptyset$.
   Wir zeigen: Ist $aU \cap bU$ nicht leer, so gilt $aU = bU$. Sei also $g \in aU \cap bU$, d.h. $g = av$ mit $v \in U$ und $g = bw$ mit $w \in U$. Für alle $u \in U$ gilt dann $au = bwv^{-1}u \in bU$, also $aU \subseteq bU$. Entsprechend folgt $bU \subseteq aU$ und damit die Behauptung.

3. $|G/U| = |U\backslash G|$.
   Die Abbildung $G/U \longrightarrow U\backslash G,\ aU \longmapsto Ua^{-1}$ ist wohldefiniert, denn für jedes $a \in G$ gilt $Ua^{-1} = \{ua^{-1} \mid u \in U\} = \{u^{-1}a^{-1} \mid u \in U\} = \{(au)^{-1} \mid u \in U\} = (aU)^{-1}$. Man überlegt sich nun leicht, daß sie sogar eine Bijektion ist.

4. $|aU| = |Ub|$ für alle $a, b \in G$.
   Mit Eigenschaft 1 genügt es, $|aU| = |Ua^{-1}|$ zu zeigen. Im Beweis zu Eigenschaft 3 wurde bewiesen, daß $Ua^{-1} = (aU)^{-1}$ gilt, also $|aU| = |(aU)^{-1}| = |Ua^{-1}|$.

5. G ist disjunkte Vereinigung der Linksnebenklassen (Rechtsnebenklassen).
   Da jedes $a \in G$ in der Linksnebenklasse aU (Rechtsnebenklasse Ua) liegt, ist G Vereinigung der Nebenklassen. Wegen Eigenschaft 2 ist die Vereinigung disjunkt.

Definition 1.8 *Ist G eine Gruppe und U eine Untergruppe von G, so heißt die Anzahl der Linksnebenklassen (Rechtsnebenklassen) von U Index von U (in G), geschrieben $(G : U)$.*

Beispiel. Wir betrachten die symmetrische Gruppe $G = \mathbf{S}_3$. Die Diedergruppe D_3 ist eine Untergruppe von $\mathbf{S}_3$, und wegen $|\mathrm{D}_3| = |\mathbf{S}_3| = 6$ folgt $\mathrm{D}_3 = \mathbf{S}_3$, also

$$G = \mathbf{S}_3 = \mathrm{D}_3 = \{\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\},$$

wobei $\sigma\tau = \tau\sigma^2$ gilt. Wir berechnen die Nebenklassen für $U = \langle\tau\rangle = \{\mathrm{id}, \tau\}$.

$$\underbrace{\begin{array}{ccccc} \mathrm{id}U & = & \{\mathrm{id}, \tau\} & = & \tau U \\ \sigma U & = & \{\sigma, \tau\sigma^2\} & = & \tau\sigma^2 U \\ \sigma^2 U & = & \{\sigma^2, \tau\sigma\} & = & \tau\sigma U \end{array}}_{\text{Linksnebenklassen}} \qquad \underbrace{\begin{array}{ccccc} U\mathrm{id} & = & \{\mathrm{id}, \tau\} & = & U\tau \\ U\sigma & = & \{\sigma, \tau\sigma\} & = & U\tau\sigma \\ U\sigma^2 & = & \{\sigma^2, \tau\sigma^2\} & = & U\tau\sigma^2 \end{array}}_{\text{Rechtsnebenklassen}}.$$

Offenbar gilt $(G : U) = 3$.

Satz 1.9 (Lagrange) *Ist G eine Gruppe und U eine Untergruppe von G, so gilt*

$$|G| = |U| \cdot (G : U).$$

Beweis. Wegen Eigenschaft 5 ist G die disjunkte Vereinigung von $(G : U)$ Mengen mit der Mächtigkeit $|U|$ (vgl. Eigenschaft 1).

□

Beispiel.

1. Für jede Gruppe G gilt $(G : G) = 1$ und $(G : \{e\}) = |G|$.
2. Sei $n \in \mathbb{N}, n > 2$ sowie $G = \mathbf{S}_n$ und $U = \mathrm{D}_n$. Dann gilt
$$(\mathbf{S}_n : \mathrm{D}_n) = \frac{|\mathbf{S}_n|}{|\mathrm{D}_n|} = \frac{n!}{2n} = \frac{(n-1)!}{2}.$$
3. Ist K ein Körper, dann gilt für alle $n \in \mathbb{N}$:
$$(\mathrm{GL}(n;K) : \mathrm{SL}(n;K)) = |K^\times|.$$
Um das einzusehen, betrachten wir $A, B \in \mathrm{GL}(n;K)$. Es gilt
$$\begin{aligned} A \cdot \mathrm{SL}(n;K) = B \cdot \mathrm{SL}(n;K) &\iff A \in B \cdot \mathrm{SL}(n;K) \\ &\iff B^{-1}A \in \mathrm{SL}(n;K) \\ &\iff \det(B^{-1}A) = 1 \\ &\iff \det A = \det B. \end{aligned}$$
Definieren wir nun für jedes $k \in K^\times$
$$A_k := \begin{pmatrix} k & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix},$$
dann gilt $\det A_k = k$. Offenbar liegt in jeder Nebenklasse von $\mathrm{SL}(n;K)$ genau ein A_k. Daraus folgt
$$\mathrm{GL}(n;K)/\mathrm{SL}(n;K) = \{A_k \cdot \mathrm{SL}(n;K) \mid k \in K^\times\} \text{ und}$$
$$(\mathrm{GL}(n;K) : \mathrm{SL}(n;K)) = |K^\times|.$$

□

Korollar 1.10 *Die Ordnung einer Untergruppe teilt die Gruppenordnung.*

Korollar 1.11 *Die Ordnung eines Gruppenelements teilt die Gruppenordnung.*

Beweis. Für jedes Gruppenelement a gilt $\mathrm{ord} a = |\langle a \rangle|$. Mit Korollar 1.10 folgt die Behauptung.

□

Korollar 1.12 *Gruppen von Primzahlordnung sind zyklisch.*

Beweis. Ist $|G| = p$ und p prim sowie $a \in G, a \neq e$, dann ist $\langle a \rangle$ Untergruppe von G und $|\langle a \rangle|$ ein Teiler von p. Damit gilt $|\langle a \rangle| = p = |G|$, d.h. $\langle a \rangle = G$.

□

Korollar 1.13 *Ist G eine Gruppe und $|G| = n < \infty$, dann gilt $a^n = e$ für alle $a \in G$.*

Beweis. Wegen Korollar 1.11 gilt $n = k \cdot \mathrm{ord}a$ für ein $k \in \mathbb{N}$, also

$$a^n = (a^{\mathrm{ord}a})^k = e^k = e.$$

□

Korollar 1.14 *Ist G eine endliche Gruppe mit den Untergruppen U und V, so daß $U \subseteq V$, dann gilt:*

$$(G : U) = (G : V)(V : U).$$

Beweis. Die Behauptung folgt sofort aus

$$|U| \cdot (G : U) = |G| = |V| \cdot (G : V) = |U| \cdot (V : U) \cdot (G : V).$$

□

2. Gruppenhomomorphismen

Definition 2.1 *Ist G eine Gruppe mit der Verknüpfung $\circ$ und H eine Gruppe mit der Verknüpfung $*$, dann heißt $\varphi : G \longrightarrow H$ Gruppenhomomorphismus, wenn $\varphi(a \circ b) = \varphi(a) * \varphi(b)$ für alle $a, b \in G$ gilt. Ein bijektiver Gruppenhomomorphismus heißt Gruppenisomorphismus, und ein Gruppenisomorphismus $\varphi : G \longrightarrow G$ heißt Gruppenautomorphismus. Zwei Gruppen G und H heißen isomorph (geschrieben $G \cong H$), wenn es einen Gruppenisomorphismus $\varphi : G \longrightarrow H$ gibt.*

Einfache Eigenschaften. Sei $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus.

1. Ist e das neutrale Element von G, dann ist $\varphi(e)$ das neutrale Element von H.
2. Ist a^{-1} das inverse Element von $a \in G$, so ist $\varphi(a^{-1})$ das inverse Element von $\varphi(a) \in H$, d.h. $\varphi(a)^{-1} = \varphi(a^{-1})$.
3. Die Komposition von Gruppenhomomorphismen ist ein Gruppenhomomorphismus.
4. Ist $\varphi : G \longrightarrow H$ ein Gruppenisomorphismus, so ist $\varphi^{-1} : H \longrightarrow G$ auch ein Gruppenisomorphismus.

Beispiel.

1. Ist G eine Gruppe, so ist $G \longrightarrow G, a \longmapsto e$ ein Gruppenhomomorphismus und die Identität $\mathrm{id} : G \longrightarrow G, a \longmapsto a$ ein Gruppenautomorphismus.

2. Betrachten wir $\mathbb{R}$ als Gruppe bezüglich der Addition und $\mathbb{R}^+ := \{x \in \mathbb{R} \mid x > 0\}$ als Gruppe bezüglich der Multiplikation, so ist $\exp : \mathbb{R} \longrightarrow \mathbb{R}^+, x \longmapsto e^x$ ein Gruppenisomorphismus.

3. Ist K ein Körper und $n \in \mathbb{N}$, so ist $\det : \mathrm{GL}(n; K) \longrightarrow K^\times, A \longmapsto \det A$ ein Gruppenhomomorphismus.

4. Für jedes $n \in \mathbb{N}$ ist $\mathrm{sgn} : \mathbf{S}_n \longrightarrow \{1, -1\}, \pi \longmapsto \mathrm{sgn}\pi$ ein Gruppenhomomorphismus.

Satz 2.2 *Sind G und H zwei Gruppen mit den neutralen Elementen e_G bzw. e_H und ist $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus, so gilt:*

1. *Ist U Untergruppe von G, so ist $\varphi(U) := \{\varphi(a) \mid a \in U\}$ Untergruppe von H.*

2. *Ist V Untergruppe von H, so ist $\varphi^-(V) := \{a \in G \mid \varphi(a) \in V\}$ Untergruppe von G.*

3. *$\mathrm{Kern}\varphi := \{a \in G \mid \varphi(a) = e_H\}$ ist Untergruppe von G.*

4. *φ ist injektiv $\Longleftrightarrow \mathrm{Kern}\varphi = \{e_G\}$.*

Beweis.

1. Wegen $e_G \in U$ ist $\varphi(e_G) \in \varphi(U)$, d.h. $\varphi(U) \neq \emptyset$, und für alle $a, b \in U$ gilt: $\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(U)$. Wegen Satz 1.5 ist damit $\varphi(U)$ Untergruppe von H.

2. Wegen $\varphi(e_G) = e_H \in V$ ist $e_G \in \varphi^-(V)$, d.h. $\varphi^-(V) \neq \emptyset$, und für alle $a, b \in \varphi^-(V)$ gilt: $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} \in V$, d.h. $ab^{-1} \in \varphi^-(V)$. Wegen Satz 1.5 ist damit $\varphi^-(V)$ Untergruppe von G.

3. Die Behauptung folgt sofort aus 2. mit $V = \{e_H\}$.

4. $''\Rightarrow''$: Da φ injektiv ist, ist e_G das einzige Urbild von e_H, d.h. $\mathrm{Kern}\varphi = \{e_G\}$.
   $''\Leftarrow''$: Sind $a, b \in G$ mit $\varphi(a) = \varphi(b)$, so folgt $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H$, also $ab^{-1} \in \mathrm{Kern}\varphi$, d.h. $ab^{-1} = e_G$, also $a = b$.

□

Definition 2.3 *Sind G, H Gruppen und ist $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus, so heißt* $\mathrm{Kern}\varphi$ *der Kern von φ.*

Satz 2.4 *Sind G, H Gruppen und ist $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus sowie $N := \mathrm{Kern}\varphi$, so gilt $aN = Na$ für alle $a \in G$.*

Beweis. Ist $n \in N$, so folgt $an = ana^{-1}a$. Wegen $\varphi(ana^{-1}) = \varphi(a)\varphi(n)\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = e_H$ gilt $ana^{-1} \in N$, also $aN \subseteq Na$, und $Na \subseteq aN$ ergibt sich entsprechend.

□

Definition 2.5 *Ist G eine Gruppe und U eine Untergruppe von G, so heißt U Normalteiler in G, wenn $aU = Ua$ für alle $a \in G$ gilt.*

Bemerkung. Offenbar ist eine Untergruppe U von G genau dann Normalteiler in G, wenn $aUa^{-1} = U$ für alle $a \in G$ gilt.

Beispiel.

1. Ist G eine Gruppe, so sind G und $\{e\}$ Normalteiler in G .
2. Der Kern eines Gruppenhomomorphismus $\varphi : G \longrightarrow H$ ist ein Normalteiler in G.
3. Ist G abelsch, so ist jede Untergruppe Normalteiler.
4. Ist K ein Körper und $n \in \mathbb{N}$, so ist $\mathrm{SL}(n; K)$ ein Normalteiler in $\mathrm{GL}(n; K)$, denn $\mathrm{SL}(n; K)$ ist Kern des Homomorphismus $\det : \mathrm{GL}(n; K) \longrightarrow K^\times$.

Satz 2.6 *Ist G eine Gruppe und N ein Normalteiler, dann ist G/N bezüglich*

$$aN \cdot bN := abN$$

eine Gruppe und

$$\varphi : G \longrightarrow G/N, a \longmapsto aN$$

ein surjektiver Gruppenhomomorphismus mit $\mathrm{Kern}\varphi = N$.

Beweis. Zunächst muß gezeigt werden, daß die Verknüpfung der Nebenklassen wohldefiniert ist, d.h., es muß $abN = a'b'N$ gelten für alle $a, a', b, b' \in G$ mit $aN = a'N$ und $bN = b'N$. Sei also $a' = an$ und $b' = bm$ mit $n, m \in N$. Da N ein Normalteiler in G ist, gibt es ein $n' \in N$ mit $nb = bn'$, also

$$a'b'N = anbmN = abn'mN = abN.$$

Die Verknüpfung ist offenbar assoziativ, $eN(= N)$ ist das neutrale Element und $a^{-1}N$ ist das inverse Element von aN. Ebenso leicht überprüft man, daß φ ein Homomorphismus ist, und wegen $\varphi(a) = aN$ tritt jede Nebenklasse als Bild unter φ auf, d.h., φ ist surjektiv. Zu zeigen bleibt $\mathrm{Kern}\varphi = N$. Dieses folgt aber sofort aus

$$a \in \mathrm{Kern}\varphi \Longleftrightarrow \varphi(a) = eN \Longleftrightarrow aN = eN \Longleftrightarrow a \in N.$$

□

Bemerkung. In Satz 2.6 wird die Normalteilereigenschaft von N lediglich für die Wohldefiniertheit der Verknüpfung gebraucht.

Definition 2.7 *Ist G eine Gruppe und N ein Normalteiler, so heißt G/N bezüglich der in Satz 2.6 angegebenen Verknüpfung Faktorgruppe von G nach N, und φ heißt zugehöriger kanonischer Homomorphismus.*

Bemerkung.

1. In G/N schreibt man auch $\overline{a}$ statt aN.
2. Ist G abelsch, so ist jede Untergruppe U Normalteiler und G/U abelsch.
3. Ist G zyklisch, so ist G/U zyklisch für jede Untergruppe U.

Beispiel. Wir betrachten $\mathbb{Z}$ als Gruppe bezüglich der Addition. Für jedes $n \in \mathbb{N}$ ist dann $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ eine Untergruppe von G, die sogar Normalteiler ist, da G abelsch. Jedes $z \in \mathbb{Z}$ läßt sich eindeutig in der Form $z = qn + r$ mit $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, n-1\}$ schreiben, d.h.,

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Man bezeichnet die Menge aller Nebenklassen auch mit $\mathbb{Z}_n$, und es folgt $|\mathbb{Z}_n| = (\mathbb{Z} : n\mathbb{Z}) = |\mathbb{Z}/n\mathbb{Z}| = n$. Es gilt für alle $a, b \in \{0, 1, \ldots, n-1\}$:

$$\overline{a} + \overline{b} = \overline{a+b} \text{ falls } a + b < n \text{ und } \overline{a} + \overline{b} = \overline{a+b-n} \text{ falls } a + b \geq n.$$

Bei dieser Darstellung der Addition liegen die Repräsentanten der Nebenklassen immer in $\{0, 1, \ldots, n-1\}$. Es gilt aber stets

$$\overline{a} + \overline{b} = \overline{a+b} \text{ für alle } a, b \in \mathbb{Z}.$$

$\mathbb{Z}_n$ ist bezüglich der Addition eine zyklische Gruppe der Ordnung n.
Zwei ganze Zahlen a, b liegen nun genau dann in derselben Nebenklasse, wenn sie bei Division durch n denselben Rest lassen. Die Nebenklassen werden daher auch als *Restklassen modulo* n bezeichnet, und statt $\overline{a} = \overline{b}$ schreibt man auch

$$a \equiv b \bmod n$$

und sagt: a und b sind kongruent modulo n.

Satz 2.8 (Homomorphiesatz) *Sind G und H Gruppen und ist $\varphi : G \longrightarrow H$ ein surjektiver Gruppenhomomorphismus, dann ist*

$$\psi : G/\mathrm{Kern}\varphi \longrightarrow H, \quad a\mathrm{Kern}\varphi \longmapsto \varphi(a)$$

ein Gruppenisomorphismus. Insbesondere gilt also

$$H \cong G/\mathrm{Kern}\varphi.$$

Beweis. Zunächst zeigen wir, daß ψ wohldefiniert ist. Gilt $a\text{Kern}\varphi = a'\text{Kern}\varphi$, so gibt es ein $n \in \text{Kern}\varphi$ mit $a = a'n$, also $\varphi(a) = \varphi(a'n) = \varphi(a')\varphi(n) = \varphi(a')$.
Wegen $\psi((a\text{Kern}\varphi)(b\text{Kern}\varphi)) = \psi(ab\text{Kern}\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(a\text{Kern}\varphi)\psi(b\text{Kern}\varphi)$ ist ψ ein Gruppenhomomorphismus, und mit Satz 2.2 ergibt sich die Injektivität von ψ aus $a\text{Kern}\varphi \in \text{Kern}\psi \iff \psi(a\text{Kern}\varphi) = e_H \iff \varphi(a) = e_H \iff a \in \text{Kern}\varphi \iff a\text{Kern}\varphi = \text{Kern}\varphi$. Somit besteht also der Kern von ψ nur aus dem neutralen Element von $G/\text{Kern}\varphi$, d.h., ψ ist injektiv. Die Surjektivität von ψ ergibt sich direkt aus der Surjektivität von φ.
□

Bemerkung.

1. Sind G und H Gruppen und ist $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus, dann gilt $G/\text{Kern}\varphi \cong \varphi(G)$.

2. Für jede Gruppe G gilt $G/\{e\} \cong G$.

Beispiel.

1. Ist K ein Körper und $n \in \mathbb{N}$, dann ist $\det : \text{GL}(n;K) \longrightarrow K^\times, A \longmapsto \det A$ ein surjektiver Gruppenhomomorphismus. Wegen $\text{Kern}\det = \text{SL}(n;K)$ folgt aus dem Homomorphiesatz
$$\text{GL}(n;K)/\text{SL}(n;K) \cong K^\times.$$

2. Für jedes $n \in \mathbb{N}, n > 1$ ist $\text{sgn} : \mathbf{S}_n \longrightarrow \{1,-1\}, \pi \longmapsto \text{sgn}\pi$ ein surjektiver Gruppenhomomorphismus. Der Kern heißt alternierende Gruppe und wird mit $\mathbf{A}_n$ bezeichnet. Die alternierende Gruppe besteht aus den geraden Permutationen und ist als Kern von sgn ein Normalteiler in $\mathbf{S}_n$. Wegen des Homomorphiesatzes gilt
$$\mathbf{S}_n/\mathbf{A}_n \cong \{1,-1\}.$$

3. Ist $\langle a\rangle$ eine zyklische (multiplikativ geschriebene) Gruppe, dann ist
$$\varphi : \mathbb{Z} \longrightarrow \langle a\rangle, \quad z \longmapsto a^z$$
ein surjektiver Gruppenhomomorphismus. Gilt $\text{ord}a = \infty$, so folgt $\text{Kern}\varphi = \{0\}$, d.h. $\langle a\rangle \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$ (vgl. Bemerkung 2). Gilt aber $\text{ord}a = n < \infty$, so ist $\text{Kern}\varphi = n\mathbb{Z}$, d.h. $\langle a\rangle \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Bis auf Isomorphie gibt es damit genau eine zyklische Gruppe der Ordnung $n, n \in \mathbb{N} \cup \{\infty\}$. Ist $n \in \mathbb{N}$, so bezeichnet man "die" additiv geschriebene zyklische Gruppe der Ordnung n mit $\mathbb{Z}_n$ und "die" multiplikativ geschriebene mit $\mathcal{Z}_n$.

Anwendung.

1. Ist p eine Primzahl, so gibt es "genau eine" Gruppe G mit $|G| = p$. Zunächst ist $\mathbb{Z}_p$ eine solche Gruppe, und ist G ebenfalls eine Gruppe mit $|G| = p$, so ist G wegen Korollar 1.12 zyklisch, also $G \cong \mathbb{Z}_p$.

2. Es gibt "genau zwei" Gruppen der Ordnung 4, und beide sind abelsch. Zunächst sind $\mathbb{Z}_4$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$ solche Gruppen, und wegen $a^2 = e$ für alle $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$ ist $\mathbb{Z}_2 \times \mathbb{Z}_2$ nicht zyklisch, d.h. $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$.
Sei nun andererseits G eine Gruppe mit $|G| = 4$.
1. Fall: Es gibt ein $g \in G$ mit $\mathrm{ord} g = 4$. Dann folgt $G = \langle g \rangle \cong \mathbb{Z}_4$.
2. Fall: $g^2 = e$ für alle $g \in G$. Dann folgt $G = \{e, a, b, c\}$ mit $a^2 = b^2 = c^2 = e$ und $ab = c$. Die Verknüpfung in G ergibt sich nun gemäß folgender Tabelle:

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

Definieren wir die Abbildung $\varphi : G \longrightarrow \langle a \rangle \times \langle b \rangle$ durch

$$e \longmapsto (e, e),\ a \longmapsto (a, e),\ b \longmapsto (e, b),\ c \longmapsto (a, b),$$

so zeigt man leicht, daß φ ein Gruppenisomorphismus ist, d.h. $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
Ist G eine nichtzyklische Gruppe der Ordnung 4, so heißt G *Kleinsche Vierergruppe*, geschrieben $G = \mathfrak{V}_4$.

3. Aufgaben

A 3.1 Es sei G eine Gruppe und a, b Elemente aus G mit endlicher Ordnung. Zeigen Sie:

1. Für jede natürliche Zahl $n \in \mathbb{N}$ gilt $a^n = e$ genau dann, wenn die Ordnung $\mathrm{ord} a$ von a ein Teiler von n ist.

2. $\mathrm{ord} a^{-1} = \mathrm{ord} a$.

3. $a^0, a^1, \ldots, a^{\mathrm{ord}a - 1}$ sind genau die verschiedenen Potenzen von a.

4. Gilt $ab = ba$ und sind die Ordnungen $\mathrm{ord} a, \mathrm{ord} b$ teilerfremd, so gilt $\mathrm{ord}(ab) = \mathrm{ord} a \cdot \mathrm{ord} b$.

A 3.2 1. Sei G eine Gruppe und $a \in G$ mit $\mathrm{ord} a < \infty$. Zeigen Sie für alle $k \in \mathbb{N}$:

$$\mathrm{ord} a^k = \frac{\mathrm{ord} a}{\mathrm{ggT}(k, \mathrm{ord} a)}.$$

2. Sei G eine endliche abelsche Gruppe und $m = \max\{\mathrm{ord} a \mid a \in G\}$. Zeigen Sie, daß $\mathrm{ord} a$ ein Teiler von m ist für alle $a \in G$.

A 3.3 Wir betrachten $\mathbb{Z}$ als Gruppe bezüglich der gewöhnlichen Addition. Zeigen Sie:

1. Ist U eine Untergruppe von $\mathbb{Z}$, dann gibt es ein $a \in \mathbb{Z}$ mit $U = a\mathbb{Z} = \{az \mid z \in \mathbb{Z}\}$.
2. Für $a, b \in \mathbb{Z} \setminus \{0\}$ gilt
$$\langle a, b\rangle = d\mathbb{Z} \text{ und } \langle a\rangle \cap \langle b\rangle = m\mathbb{Z}$$
wobei d ein ggT und m ein kgV von a und b ist.

A 3.4 Zeigen Sie, daß jede Untergruppe einer zyklischen Gruppe zyklisch ist.

A 3.5 Seien $\sigma, \tau \in \mathbf{S}_n$ disjunkt, d.h., für alle $x \in \{1, 2, \ldots, n\}$ gilt $\sigma(x) = x$ oder $\tau(x) = x$. Zeigen Sie, daß dann für alle $i, j \in \mathbb{N}$ auch σ^i und τ^j disjunkt sind und daß $\sigma \circ \tau = \tau \circ \sigma$ gilt. Weisen Sie weiterhin nach, daß gilt

$$\mathrm{ord}(\sigma \circ \tau) = \mathrm{kgV}(\mathrm{ord}\sigma, \mathrm{ord}\tau).$$

A 3.6 Gegeben sind die Permutationen:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 5 & 6 & 8 & 4 & 1 & 3 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 1 & 2 & 7 & 5 & 9 & 4 & 6 \end{pmatrix}.$$

Schreiben Sie σ und τ als Produkte disjunkter Zykeln. Berechnen Sie $\sigma \circ \tau$ und $\tau^{-1} \circ \sigma$ sowie $\mathrm{sgn}(\sigma \circ \tau)$ und $\mathrm{ord}(\tau^{-1} \circ \sigma)$.

A 3.7 Sei $n \in \mathbb{N}$, $n > 2$ und $\sigma, \tau \in \mathbf{S}_n$ mit

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}.$$

Die Untergruppe $\mathrm{D}_n :=< \sigma, \tau >$ von $\mathbf{S}_n$ heißt *Diedergruppe* (vgl. Beispiel nach Korollar 1.7).

1. Zeigen Sie $\mid \mathrm{D}_n \mid = 2n$.
2. Sei $n = 4$ und $U =< \tau >$. Berechnen Sie $(\mathrm{D}_4 : U)$ und geben Sie alle Links- und Rechtsnebenklassen von U in D_4 an. Ist U ein Normalteiler in D_4?

A 3.8 Berechnen Sie $(\mathbf{S}_4 : \mathrm{D}_4)$ und geben Sie alle Links- und alle Rechtsnebenklassen von D_4 in $\mathbf{S}_4$ an. Ist D_4 Normalteiler in $\mathbf{S}_4$?

A 3.9 Berechnen Sie alle Untergruppen der Diedergruppe D_4. Welche davon sind Normalteiler?

A 3.10 G sei eine Gruppe. Dann heißt $\mathrm{Z}(G) := \{a \in G \mid \forall b \in G : ab = ba\}$ Zentrum von G.

1. Zeigen Sie, daß $\mathrm{Z}(G)$ ein Normalteiler in G ist.
2. Zeigen Sie für die Diedergruppe $\mathrm{D}_n = \langle \sigma, \tau \rangle, n > 2$, daß $\mathrm{Z}(\mathrm{D}_n) = \{\mathrm{id}, \sigma^{\frac{n}{2}}\}$ für gerades n und $\mathrm{Z}(\mathrm{D}_n) = \{\mathrm{id}\}$ für ungerades n gilt.

A 3.11 G sei eine endliche abelsche Gruppe mit $\mid G \mid = m$. Zeigen Sie: Für alle $a, b \in G$ mit teilerfremden Ordnungen ist $\langle a\rangle \times \langle b\rangle$ zyklisch. Gilt außerdem $m = \mathrm{ord}a \cdot \mathrm{ord}b$, so ist G zyklisch und $G = \langle a, b\rangle$. Geben Sie ein sinnvolles Beispiel an.

A 3.12 Gegeben sind die reellen Matrizen

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

Zeigen Sie, daß $G = \{E, -E, I, -I, J, -J, K, -K\}$ eine Untergruppe der $\mathrm{GL}(4;\mathbb{R})$ ist. Geben Sie alle Untergruppen von G an. Welche sind Normalteiler?

A 3.13 Gegeben sind die Matrizen $A, B \in \mathrm{GL}(2;\mathbb{Q})$ mit

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Zeigen Sie $\mathrm{ord}A = 3$, $\mathrm{ord}B = 2$ und $AB = BA^2$ und daß $G = \{E, A, A^2, B, BA, BA^2\}$ eine Untergruppe von $\mathrm{GL}(2;\mathbb{Q})$ ist. Sind G und die Diedergruppe D_3 isomorph?

A 3.14 G sei eine Gruppe mit dem neutralen Element e. Zeigen Sie:

1. Gilt $g^2 = e$ für alle $g \in G$, so ist G abelsch.
2. Sind U,V endliche Untergruppen von G mit $U \cap V = \{e\}$, dann gilt $\mid UV \mid = \mid U \mid \cdot \mid V \mid$, wobei $UV = \{u \cdot v \mid u \in U, v \in V\}$.
3. Ist U eine Untergruppe von G mit $(G : U) = 2$, so ist U ein Normalteiler in G.
4. Ist U Untergruppe von G und N Normalteiler in G, so ist UN Untergruppe in G.

A 3.15 Es sei p eine Primzahl. Zeigen Sie, daß es bis auf Isomorphie genau zwei Gruppen der Ordnung $2p$ gibt.

A 3.16 Es seien G und H Gruppen und e das neutrale Element von G. Zeigen Sie: $\{e\} \times H$ ist Normalteiler in $G \times H$ und $(G \times H)/(\{e\} \times H) \cong G$. Hinweis: Betrachten Sie einen geeigneten Homomorphismus $\varphi : G \times H \longrightarrow G$ und wenden Sie den Homomorphiesatz an.

A 3.17 G sei eine Gruppe und $\mathrm{Aut}(G)$ die Menge aller Automorphismen von G. Zeigen Sie, daß $\mathrm{Aut}(G)$ eine Gruppe bezüglich der Hintereinanderschaltung ist. Geben Sie alle Automorphismen der $\mathbf{S}_3$ an und zeigen Sie $\mathrm{Aut}(\mathbf{S}_3) \cong \mathbf{S}_3$.

A 3.18 Geben Sie alle Automorphismen der Kleinschen Vierergruppe $\mathfrak{V}_4$ an. Zeigen Sie $\mathrm{Aut}(\mathfrak{V}_4) \cong \mathbf{S}_3$.

A 3.19 Ist G eine Gruppe und $a \in G$, so definiert man $i_a : G \longrightarrow G,\ g \longmapsto aga^{-1}$.

1. Zeigen Sie, daß i_a ein Automorphismus von G für jedes $a \in G$ ist. (Man nennt i_a einen inneren Automorphismus.)
2. Zeigen Sie, daß die inneren Automorphismen von G eine Untergruppe von $\mathrm{Aut}(G)$ bilden. (Die Gruppe der inneren Automorphismen bezeichnet man mit $\mathrm{Inn}(G)$.)
3. Zeigen Sie: $\mathrm{Inn}(G) \cong G/\mathrm{Z}(G)$.

KAPITEL 2

Ringe

1. Ringe und ihre Homomorphismen

Definition 1.1 *Eine Menge R mit den Verknüpfungen $+$ und $\cdot$ heißt Ring, wenn gilt:*

i) R ist eine abelsche Gruppe bezüglich der Verknüpfung $+$.

ii) Die Verknüpfung $\cdot$ ist assoziativ.

iii) Es gelten die Distributivgesetze, d.h., für alle $a, b, c \in R$ gilt

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Bemerkung.

1. Zur Vereinfachung der Darstellung werden in einem Ring R meistens die Klammern um Produkte weggelassen und die Regel *Punktrechnung geht vor Strichrechnung* eingeführt. Für $a, b, c \in R$ schreibt man also zum Beispiel $a \cdot (b + c) = a \cdot b + a \cdot c$ statt $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

2. Ein Ring R heißt kommutativ, wenn $a \cdot b = b \cdot a$ für alle $a, b \in R$ gilt.

3. Ein Ring R heißt Ring mit Eins, wenn R bezüglich der Multiplikation ein Einselement hat. Dieses wird im allgemeinen mit 1 bezeichnet.

4. Ist R ein Ring und S eine Teilmenge von R, so heißt S Teilring von R, wenn S bezüglich der in R definierten Addition und Multiplikation ein Ring ist.

Beispiel.

1. $\mathbb{Z}$ ist bezüglich der üblichen Addition und Multiplikation ein kommutativer Ring mit Eins.

2. Ist R ein Ring und $n \in \mathbb{N}$, so ist die Menge $R_{n,n}$ alle $(n,n)-$Matrizen über R bezüglich der üblichen Matrizenaddition und Matrizenmultiplikation ein Ring. Hat R ein Einselement, so auch $R_{n,n}$. Für $n > 1$ ist der Matrizenring $R_{n,n}$ im allgemeinen nicht kommutativ.

3. $R_1, \ldots, R_n$ seien Ringe und $R := R_1 \times \ldots \times R_n$. Definiert man die Addition $+$ und die Multiplikation $\cdot$ in R komponentenweise, so ist R ein Ring. Hat jedes R_i $(i = 1, \ldots, n)$ ein Einselement, so auch R, und R ist genau dann kommutativ, wenn jeder Ring R_i $(i = 1, \ldots, n)$ kommutativ ist. R heißt direktes Produkt der Ringe $R_1, \ldots, R_n$.

Bemerkung. Sei R ein Ring bezüglich der Verknüpfungen $+$ und $\cdot$.

1. $+$ heißt Addition und $\cdot$ Multiplikation.

2. Das neutrale Element der Addition wird mit 0 bezeichnet und das additive Inverse von $a \in R$ mit $-a$.

3. Man schreibt auch ab statt $a \cdot b$ und $a - b$ statt $a + (-b)$ für alle $a, b \in R$.

4. Da R bezüglich der Multiplikation eine Halbgruppe ist, gelten insbesondere die Ergebnisse aus Kapitel 1 über Halbgruppen und Halbgruppen mit Einselement. Zum Beispiel definiert man $a^1 = a$ und $a^{n+1} = a^n a$ für alle $n \in \mathbb{N}$, und es gelten die Potenzrechengesetze. Hat R ein Einselement 1, so ist es eindeutig bestimmt, und man definiert $a^0 = 1$ für alle $a \in R$.

Rechenregeln. Ist R ein Ring, so gilt für alle $a, b, c \in R$:

1. $a \cdot 0 = 0 \cdot a = 0$.

2. $a(-b) = -ab = (-a)b$.

3. $(-a)(-b) = ab$.

4. $a(b - c) = ab - ac$.

5. $(a - b)c = ac - bc$.

Definition 1.2 *R sei ein Ring mit 1.*

i) $a \in R$ heißt Einheit oder invertierbar, wenn es ein $b \in R$ mit $ab = ba = 1$ gibt.

ii) R sei kommutativ und es gelte $1 \neq 0$. Dann heißt R Integritätsbereich, wenn $ab \neq 0$ für alle $a, b \in R \setminus \{0\}$ gilt. R heißt Körper, wenn jedes $a \in R, a \neq 0$, Einheit in R ist.

Bemerkung.

1. $a \in R$ ist invertierbar, wenn a in der multiplikativen Halbgruppe von R invertierbar ist. a^{-1} bezeichnet dann das inverse Element (vgl. Kapitel 1).

2. Die Menge $\mathrm{E}(R)$ der Einheiten von R ist bezüglich $\cdot$ eine Gruppe (vgl. Satz 1.2 aus Kapitel 1).

3. Ist K ein Körper und F ein Teilring von K, der ebenfalls ein Körper ist, so heißt F Teilkörper von K.

Beispiel.

1. $\mathbb{Z}$ ist ein Integritätsbereich mit $\mathrm{E}(\mathbb{Z}) = \{1, -1\}$.

2. $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind Körper.

3. Sei $R = \mathbb{Z}_{2,2}$ der Ring der $(2,2)-$Matrizen über $\mathbb{Z}$. Dann ist $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$ das neutrale Element der Addition und $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$ das neutrale Element der Multiplikation. Wir betrachten

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} -2 & -2 \\ 1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}.$$

Es gilt $A, B \neq 0$ und $AB = 0$. Man nennt A und B daher auch Nullteiler. Wegen

$$\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} C = C \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = 1$$

ist C eine Einheit in R, und D ist weder Nullteiler noch Einheit in R.

Bemerkung.

1. Ein kommutativer Ring mit 1 ist genau dann ein Integritätsbereich, wenn $1 \neq 0$ und wenn R keine Nullteiler hat.

2. Da Einheiten keine Nullteiler sind, ist jeder Körper ein Integritätsbereich.

Polynome über einem Integritätsbereich.

R sei ein Integritätsbereich. Der formale Ausdruck

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots$$

mit $a_n \in R$ und $a_n \neq 0$ für nur endliche viele n heißt Polynom in der Unbestimmten x mit den Koeffizienten $a_0, a_1, a_2, \dots$.
Ist

$$g(x) = b_0 + b_1 x + b_2 x^2 + \dots$$

ebenfalls ein Polynom in x mit Koeffizienten aus R, so definiert man

$$f(x) = g(x) \quad :\Longleftrightarrow \quad (\forall n \in \mathbb{N}_0 : a_n = b_n).$$

$f(x)$ heißt Nullpolynom (geschrieben $f(x) = 0$), wenn $a_0 = a_1 = \ldots = 0$. Die Menge aller Polynome in x mit Koeffizienten aus R bezeichnet man mit $R[x]$, und auf $R[x]$ wird folgendermaßen eine Addition $+$ und eine Multiplikation $\cdot$ eingeführt:

$$\begin{aligned} f(x) + g(x) &:= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots \\ f(x) \cdot g(x) &:= c_0 + c_1 x + c_2 x^2 + \ldots \quad \text{mit} \quad c_n = \sum_{i=0}^{n} a_i b_{n-i}. \end{aligned}$$

Man zeigt leicht, daß $c_n \neq 0$ nur für endlich viele n gilt, d.h., die Multiplikation ist wohldefiniert. Bezüglich dieser Addition und Multiplikation ist $R[x]$ ein kommutativer Ring mit 1, und es gilt $1 \neq 0$. $R[x]$ heißt Polynomring in (der Unbestimmten) x über R. Man schreibt oft die Summanden $0x^n$ nicht mit. Dann hat jedes Polynom $f(x), f(x) \neq 0$, die Darstellung

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \quad \text{mit} \quad a_n \neq 0,$$

und n heißt Grad von $f(x)$, geschrieben $\mathrm{grad} f(x) = n$. Gilt $a_n = 1$, so heißt $f(x)$ normiert. a_n nennt man den führenden Koeffizienten von $f(x)$. Das Nullpolynom hat den Grad $-\infty$.

Es gilt $\mathrm{grad} f(x)g(x) = \mathrm{grad} f(x) + \mathrm{grad} g(x)$:
Ist $f(x) = 0$ oder $g(x) = 0$, so folgt die Behauptung unmittelbar. Sei also $f(x), g(x) \neq 0$ und $\mathrm{grad} f(x) = n, \mathrm{grad} g(x) = m$. Dann ergibt sich mit den Bezeichnungen von oben

$$(a_n x^n + \ldots)(b_m x^m + \ldots) = a_n b_m x^{n+m} + \ldots.$$

Da R ein Integritätsbereich ist, folgt $a_n b_m \neq 0$, d.h. $\mathrm{grad} f(x)g(x) = n + m$.

Folgerung. Ist R ein Integritätsbereich, so ist auch $R[x]$ ein Integritätsbereich.

Definition 1.3 *Sind R und S Ringe, so heißt eine Abbildung $\varphi : R \longrightarrow S$ Ringhomomorphismus, wenn für alle $a, b \in R$ gilt:*

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b).$$

Bemerkung.

1. Ein Ringhomomorphismus ist insbesondere ein Gruppenhomomorphismus zwischen den additiven Gruppen.

2. Ist $\varphi : R \longrightarrow S$ ein Ringhomomorphismus und 1_R Einselement von R, so ist im allgemeinen $\varphi(1_R)$ kein Einselement von S.

3. Ringisomorphismen und Ringautomorphismen werden entsprechend definiert.

4. Zwei Ringe R und S heißen isomorph (geschrieben $R \cong S$), wenn es einen Ringisomorphismus $\varphi : R \longrightarrow S$ gibt.

5. Ist $\varphi : R \longrightarrow S$ ein Ringhomomorphismus, so ist $\varphi(R)$ ein Teilring von S.

Satz 1.4 *Sind R und S Ringe und ist $\varphi : R \longrightarrow S$ ein Ringhomomorphismus, so gilt für*

$$I := \text{Kern}\varphi = \{a \in R | \varphi(a) = 0\} :$$

1. *I ist Untergruppe der additiven Gruppe von R.*
2. *Für alle $a \in R$ und $i \in I$ gilt $ai, ia \in I$.*
3. *φ ist injektiv $\Longleftrightarrow I = \{0\}$.*

Beweis. Die Behauptungen 1 und 3 gelten wegen Satz 2.2 aus Kapitel 1. Um Behauptung 2 zu beweisen, sei $a \in R$ und $i \in I$. Dann folgt $\varphi(ai) = \varphi(a)\varphi(i) = \varphi(a) \cdot 0 = 0$, also $ai \in I$. Entsprechend ergibt sich $ia \in I$.

□

Definition 1.5 *Eine Teilmenge I eines Ringes R heißt Ideal von R, wenn gilt:*

1. *I ist Untergruppe der additiven Gruppe von R.*
2. *Für alle $a \in R$ und $i \in I$ gilt $ai, ia \in I$.*

Beispiel.

1. Ist R ein Ring, dann sind $\{0\}$ und R Ideale von R.
2. Der Kern eines Ringhomomorphismus $\varphi : R \longrightarrow S$ ist ein Ideal von R.
3. Ist R ein kommutativer Ring mit 1 und $a \in R$, dann ist $(a) := \{a \cdot r \mid r \in R\}$ ein Ideal von R, das a enthält.

   Beweis: Wegen $a = a \cdot 1 \in (a)$ ist (a) nicht leer, und es gilt $a \in (a)$. Sind nun weiterhin $ar, as \in (a)$ mit $r, s \in R$, dann folgt $ar - as = a(r - s) \in (a)$. Wegen Satz 1.5 aus Kapitel 1 ist damit (a) Untergruppe der additiven Gruppe von R. Ist schließlich $ar \in (a)$ mit $r \in R$ und $s \in R$, so folgt $(ar)s = a(rs) \in (a)$, und damit ist insgesamt die Behauptung gezeigt.

   (a) heißt das von a erzeugte Hauptideal, und ist ϵ eine Einheit in R, so gilt $(a) = (a\epsilon)$. Für $a = 0$ folgt $(a) = (0) = \{0\}$.

Bemerkung. Sei R ein Ring.

1. Gilt $1 \in R$ und ist I ein Ideal von R mit $1 \in I$, so folgt $I = R$, denn für alle $r \in R$ gilt dann $r = r \cdot 1 \in I$. Ist ϵ eine Einheit in R und $\epsilon \in I$, so folgt $1 = \epsilon^{-1} \cdot \epsilon \in I$, also ebenfalls $I = R$.
2. Ist $\{I_j \mid j \in J\}$ eine Menge von Idealen von R, so ist auch $\cap_{j \in J} I_j$ ein Ideal von R. Insbesondere ist der Durchschnitt $I_1 \cap \ldots \cap I_n$ endlich vieler Ideale $I_1, \ldots, I_n$ ein Ideal von R.

3. Sind $I_1, \ldots, I_n$ Ideale von R, so ist auch

$$I_1 + \ldots + I_n := \{i_1 + \ldots + i_n \mid i_j \in I_j, j = 1, \ldots, n\}$$

ein Ideal von R.

Ist R ein Ring und I ein Ideal von R, dann ist I eine Untergruppe der additiven Gruppe von R, und mit $R/I = \{r + I \mid r \in R\}$ bezeichnet man die Menge aller Nebenklassen von I bezüglich $+$. Da die Addition in R kommutativ ist, ist I sogar ein Normalteiler.

Satz 1.6 *Ist R ein Ring und I ein Ideal von R, dann ist R/I bezüglich*

$$(a + I) + (b + I) := (a + b) + I, \ (a + I) \cdot (b + I) := ab + I$$

ein Ring und

$$\varphi : R \longrightarrow R/I, a \longmapsto a + I$$

ein surjektiver Ringhomomorphismus mit Kern$\varphi = I$.

Beweis. Wegen Satz 2.6 aus Kapitel 1 ist R/I bezüglich $+$ eine abelsche Gruppe. Wir zeigen nun, daß $\cdot$ wohldefiniert ist. Ist $a + I = a' + I$, also $a = a' + i$ für ein $i \in I$, und $b + I = b' + I$, also $b = b' + j$ für ein $j \in I$, dann folgt

$$\begin{aligned}(a + I)(b + I) &= ab + I = (a' + i)(b' + j) + I = a'b' + a'j + ib' + ij + I \\ &= a'b' + I \ (\text{da } a'j, ib', ij \in I) \\ &= (a' + I)(b' + I).\end{aligned}$$

Das Assoziativgesetz der Multiplikation und die Distributivgesetze gelten offenbar. Damit ist R/I ein Ring. Wegen Satz 2.6 aus Kapitel 1 ist φ ein surjektiver Gruppenhomomorphismus mit Kern$\varphi = I$, und wegen

$$\varphi(ab) = ab + I = (a + I)(b + I) = \varphi(a)\varphi(b)$$

für alle $a, b \in R$ ist φ ein Ringhomomorphismus.

□

Bemerkung.

1. Die Idealeigenschaft $''ai, ia \in I$ für alle $i \in I$ und $a \in R''$ wurde lediglich zum Nachweis der Wohldefiniertheit der Multiplikation benötigt.

2. Ist R kommutativ, so auch R/I.

3. Gilt $1 \in R$, so ist $1 + I$ das Einselement von R/I.

4. Man schreibt auch $\overline{a}$ statt $a + I$ für alle $a \in R$.

Definition 1.7 *Ist R ein Ring und I ein Ideal von R, so heißt R/I bezüglich der in Satz 1.6 angegebenen Verknüpfungen Faktorring von R nach I, und φ heißt zugehöriger kanonischer Homomorphismus.*

Beispiel. Wir betrachten den Ring $\mathbb{Z}$ sowie $I = n\mathbb{Z} = (n), n \in \mathbb{N}$. Dann ist I das von n erzeugte Hauptideal. Im Faktorring

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \mathbb{Z}_n$$

gilt

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{und} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

für alle $a, b \in \mathbb{Z}$.

Satz 1.8 (Homomorphiesatz) *Sind R und S Ringe und ist $\varphi : R \longrightarrow S$ ein surjektiver Ringhomomorphismus, dann ist*

$$\psi : R/\text{Kern}\varphi \longrightarrow S, \quad a + \text{Kern}\varphi \longmapsto \varphi(a)$$

ein Ringisomorphismus. Insbesondere gilt also

$$S \cong R/\text{Kern}\varphi.$$

Beweis. Wegen Satz 2.8 aus Kapitel 1 ist ψ ein Gruppenisomorphismus zwischen den additiven Gruppen von $R/\text{Kern}\varphi$ und S. Für alle $a, b \in R$ gilt schließlich

$$\psi(\overline{a} \cdot \overline{b}) = \psi(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(\overline{a})\psi(\overline{b}).$$

□

2. Teilbarkeit in Integritätsbereichen

Im folgenden ist R ein Integritätsbereich. Sind $a, b, c \in R$ mit $b \neq 0$, so gilt die Kürzungsregel:

$$ab = cb \Longrightarrow a = c,$$

denn aus $ab = cb$ folgt $(a - c)b = 0$, d.h. $a - c = 0$, da $b \neq 0$ und R nullteilerfrei ist. Sind $a, b \in R$, so heißt a Teiler von b (oder man sagt auch a teilt b), wenn es ein $c \in R$ mit $b = ac$ gibt, geschrieben $a|b$. Gilt $a|b$ und $b|a$ für $a, b \neq 0$, so gibt es $c, d \in R$ mit $b = ac$ und $a = bd$, also $b = bdc$. Wegen der Kürzungsregel folgt $dc = 1$, d.h. d und c sind Einheiten. Ist andererseits $c \in R$ eine Einheit und $b = ac$, dann gilt $a|b$ und wegen $a = bc^{-1}$ auch $b|a$. Die Elemente a und b heißen dann assoziiert, geschrieben $a \sim b$, d.h.

$$a \sim b \quad \Longleftrightarrow \quad \text{Es gibt eine Einheit } \epsilon \in R \text{ mit } a = b\epsilon.$$

Offenbar induziert $\sim$ auf R eine Äquivalenzrelation.

Beispiel.

1. Für den Ring $R = \mathbb{Z}$ der ganzen Zahlen gilt wegen $\mathrm{E}(\mathbb{Z}) = \{1, -1\}$ für alle $a, b \in \mathbb{Z}$

$$a \sim b \quad \Longleftrightarrow \quad |a| = |b|.$$

2. Ist K ein Körper und $R = K[x]$ der Polynomring von K über x, dann gilt $\mathrm{E}(R) = K^\times = K\backslash\{0\}$, denn ist $f(x) \in K[x]$ eine Einheit in $K[x]$, so gibt es ein $g(x) \in K[x]$ mit $f(x)g(x) = 1$, also $0 = \mathrm{grad}(f(x)g(x)) = \mathrm{grad}f(x) + \mathrm{grad}g(x)$, d.h. $\mathrm{grad}f(x) = 0$. Somit folgt für alle $f(x), g(x) \in K[x]$

$$f(x) \sim g(x) \quad \Longleftrightarrow \quad \text{Es gibt ein } k \in K^\times \text{ mit } f(x) = k \cdot g(x).$$

Definition 2.1 *Ist R ein Integritätsbereich und sind $a_1, \ldots, a_n \in R$, dann heißt $d \in R$ größter gemeinsamer Teiler (*ggT*) von $a_1, \ldots, a_n$, wenn folgendes gilt:*

i) d teilt $a_1, \ldots, a_n$.

ii) Für jedes $d' \in R$ gilt: Ist d' Teiler von $a_1, \ldots, a_n$, dann ist d' Teiler von d.

Bemerkung.

1. Entsprechend definiert man das kleinste gemeinsame Vielfache (kgV).
2. Im allgemeinen braucht kein ggT zu existieren (vgl. Aufgabe 4.2). Ist d ein ggT von $a_1, \ldots, a_n$ und d' auch, dann folgt $d \sim d'$. Andererseits ist mit d für jedes $\epsilon \in \mathrm{E}(R)$ auch ϵd ein ggT. Ein ggT ist also nur bis auf eine Einheit eindeutig bestimmt. Man schreibt $d \sim (a_1, \ldots, a_n)$, wenn d ein ggT von $a_1, \ldots, a_n$ ist.
3. Entsprechendes gilt für das kgV.

Beispiel. Im Ring $\mathbb{Z}$ der ganzen Zahlen sind wegen $\mathrm{E}(\mathbb{Z}) = \{1, -1\}$ sowohl ggT als auch kgV nur bis auf das Vorzeichen eindeutig bestimmt.

Satz 2.2 *Existiert in einem Integritätsbereich R der* ggT *von je zwei Elementen, so existiert er auch von n Elementen, $n \in \mathbb{N}, n \geq 2$.*

Beweis. Wir beweisen den Satz durch vollständige Induktion nach n, wobei sich der Induktionsanfang $n = 2$ direkt aus der Voraussetzung ergibt.
$n > 2$: Sind $a_1, \ldots, a_n$ gegeben, so existiert nach Induktionsvoraussetzung ein ggT von $a_1, \ldots, a_{n-1}$. Sei also $d' \sim (a_1, \ldots, a_{n-1})$ und d ein ggT von d' und a_n. Dann ist d als Teiler von d' auch Teiler von $a_1, \ldots, a_{n-1}$, d.h., d teilt $a_1, \ldots, a_n$. Ist nun $t \in R$ ebenfalls Teiler von $a_1, \ldots, a_n$, dann ist t auch Teiler von d', da $d' \sim (a_1, \ldots, a_{n-1})$. Also werden d' und a_n von t geteilt, d.h., t teilt d, da $d \sim (d', a_n)$.
Insgesamt haben wir damit gezeigt, daß d ein ggT von $a_1, \ldots, a_n$ ist.

□

Rechenregeln. Im folgenden ist R ein Integritätsbereich.

1. Haben in R je zwei Elemente einen ggT, so kann man in $(a_1, \ldots, a_n)$ für beliebige $a_1, \ldots, a_n \in R$ die Reihenfolge der a_i beliebig ändern, und man kann beliebig klammern. Zum Beispiel gilt:

$$(d \sim (a_1, a_2) \ \wedge \ d' \sim (a_3, a_4)) \Longrightarrow (a_1, a_2, a_3, a_4) \sim (d, d').$$

   Man schreibt auch $(a_1, a_2, a_3, a_4) \sim ((a_1, a_2), (a_3, a_4))$.

2. Für alle $a_1, \ldots, a_n, b_1, \ldots, b_n \in R$ gilt $(a_1, \ldots, a_n) \sim (a_1, \ldots, a_n, b_1a_1 + \ldots + b_na_n)$.

3. Für alle $a, b, r \in R$ gilt $(a, b) \sim (a, b + ra)$.

Definition 2.3 *R sei ein Integritätsbereich.*

i) $p \in R$ heißt prim oder Primelement, wenn $p \neq 0$, p keine Einheit und wenn für alle $a, b \in R$ gilt: Ist p Teiler von $a \cdot b$, dann ist p ein Teiler von a oder ein Teiler von b.

ii) $q \in R$ heißt unzerlegbar oder irreduzibel, wenn $q \neq 0$, q keine Einheit und wenn für alle $a, b \in R$ gilt: Ist $q = a \cdot b$, dann ist a eine Einheit in R oder b eine Einheit in R.

Satz 2.4 *Ist R ein Integritätsbereich und $p \in R$ prim, dann ist p unzerlegbar.*

Beweis. Zunächst ist $p \neq 0$ und p keine Einheit, da p prim ist. Sei $p = a \cdot b$ mit $a, b \in R$. Dann gilt insbesondere $p|ab$, also $p|a$ oder $p|b$. Gilt $p|a$, so folgt $a = pc$ für ein $c \in R$, also $p = pcb$, d.h. $1 = cb$. Damit ist b Einheit. Entsprechend ist a eine Einheit, wenn $p|b$.

□

Bemerkung. Im allgemeinen sind unzerlegbare Elemente nicht prim. Dazu betrachten wir den Integritätsbereich

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$$

(vgl. Aufgabe 4.2). Zunächst zeigen wir, daß 3 in $\mathbb{Z}[\sqrt{-5}]$ unzerlegbar ist. Sei also $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ mit $a, b, c, d \in \mathbb{Z}$. Wenden wir die Normfunktion aus Aufgabe 4.2 an, so erhalten wir $9 = \mathrm{N}(3) = (a^2 + 5b^2)(c^2 + 5d^2)$. Wegen $a^2 + 5b^2 \leq 9$ ist $|b| = 0$ oder $|b| = 1$. Ist $|b| = 1$, dann folgt $|a| = 2$, da $a^2 + 5b^2$ Teiler von 9 ist, und es ergibt sich $c^2 + 5d^2 = 1$, d.h. $c + d\sqrt{-5} = 1$ oder $c + d\sqrt{-5} = -1$. Damit ist $c + d\sqrt{-5}$ eine Einheit. Ist aber $|b| = 0$, so folgt $|a| = 1$ oder $|a| = 3$, da dann a^2 Teiler von 9 ist. Für $|a| = 1$ ist $a + b\sqrt{-5} = 1$ oder $a + b\sqrt{-5} = -1$, in jedem Falle eine Einheit. Ist schließlich $|a| = 3$, dann ergibt sich $c^2 + 5d^2 = 1$, also $c + d\sqrt{-5} = 1$ oder $c + d\sqrt{-5} = -1$. Damit ist $c + d\sqrt{-5}$ eine Einheit. Insgesamt haben wir also gezeigt, daß bei jeder Zerlegung von 3 ein Faktor eine Einheit ist.

Wegen $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$ ist 3 Teiler von $(2 + \sqrt{-5})(2 - \sqrt{-5})$. Offenbar teilt 3 aber weder $2 + \sqrt{-5}$ noch $2 - \sqrt{-5}$. Damit ist also 3 unzerlegbar und nicht prim.

3. Euklidische Ringe

Definition 3.1 *Ist R ein Integritätsbereich, dann heißt R euklidischer Ring, wenn es eine Funktion*

$$g : R\backslash\{0\} \longrightarrow \mathbb{N}_0$$

mit folgender Eigenschaft gibt: Zu $a, b \in R, b \neq 0$, existieren $q, r \in R$ mit $a = q \cdot b + r$, wobei $r = 0$ oder $g(r) < g(b)$.

Bemerkung.

1. g heißt Wertefunktion.
2. g heißt regulär, wenn $g(a) \leq g(ab)$ für alle $a, b \in R\backslash\{0\}$ gilt.

Beispiel.

1. Für den Ring $\mathbb{Z}$ der ganzen Zahlen ist der Absolutbetrag eine reguläre Wertefunktion, d.h., $\mathbb{Z}$ ist ein euklidischer Ring.
2. Ist $R := \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ mit $i^2 = -1$ wie in Aufgabe 4.2, dann ist R bezüglich der Normfunktion
$$\mathrm{N} : \mathbb{Z}[i] \longrightarrow \mathbb{N}_0,\ a + bi \longmapsto a^2 + b^2$$
ein euklidischer Ring. Die Normfunktion ist sogar eine reguläre Wertefunktion (vgl. Aufgabe 4.3).
3. Ist K ein Körper und $R := K[x]$ der Polynomring über K in der Unbestimmten x, dann ist $K[x]$ bezüglich der Gradfunktion ein euklidischer Ring, d.h., sind $g(x) = g_n x^n + \ldots + g_0$ und $h(x) = h_m x^m + \ldots + h_0, h_m \neq 0$ Polynome in x, so gibt es $q(x), r(x) \in K[x]$ mit
$$g(x) = q(x)h(x) + r(x),$$
wobei $r(x) = 0$ oder $\mathrm{grad} r(x) < \mathrm{grad} h(x)$.

   Beweis. Gilt $g(x) = 0$, so wählen wir $q(x) = r(x) = 0$. Sei also $g(x) \neq 0$ und $\mathrm{grad} g(x) = n$. Wir beweisen die Behauptung durch Induktion nach n.

$n = 0$: Im Falle $\mathrm{grad} h(x) > 0$ wählen wir $q(x) = 0$ sowie $r(x) = g(x) = g_0$, und es gilt $g_0 = 0 \cdot h(x) + g_0$ mit $0 = \mathrm{grad} g_0 < \mathrm{grad} h(x)$. Ist aber $\mathrm{grad} h(x) = 0$, also $h(x) = h_0 \neq 0$, dann gilt $g_0 = q(x)h(x) + r(x)$ mit $q(x) = g_0 h_0^{-1}$ und $r(x) = 0$.

$n > 0$: Ist $m > n$, so gilt $g(x) = 0 \cdot h(x) + g(x)$ mit $\mathrm{grad} g(x) < \mathrm{grad} h(x)$. Sei also $m \leq n$ und $k(x) := g(x) - g_n h_m^{-1} x^{n-m} h(x) = (g_n - g_n h_m^{-1} h_m) x^n + \ldots$, d.h. $k(x) = 0$ oder $\mathrm{grad} k(x) < \mathrm{grad} g(x)$. Nach Induktionsvoraussetzung existieren $\tilde{q}(x), r(x) \in K[x]$ mit $k(x) = \tilde{q}(x)h(x) + r(x)$, wobei $r(x) = 0$ oder $\mathrm{grad} r(x) < \mathrm{grad} h(x)$. Es folgt

$$\begin{aligned} g(x) &= k(x) + g_n h_m^{-1} x^{n-m} h(x) \\ &= \tilde{q}(x)h(x) + r(x) + g_n h_m^{-1} x^{n-m} h(x) \\ &= (\tilde{q}(x) + g_n h_m^{-1} x^{n-m}) h(x) + r(x). \end{aligned}$$

Damit ist $K[x]$ ein euklidischer Ring bezüglich der Gradfunktion, die sogar eine reguläre Wertefunktion ist.

Beispiel. (Polynomdivision)

Die Berechnung von $k(x) = g(x) - g_n h_m^{-1} x^{n-m} h(x)$ läßt sich am unten aufgeführten Schema veranschaulichen. Wir wählen $K = \mathbb{Q}, g(x) = x^4 - 4x^2 + 6x + 4$ und $h(x) = x^2 + 2x - 2$. Dann gilt $k(x) = -2x^3 - 2x^2 + 6x + 4$. Wie beim *schriftlichen Dividieren* reeller Zahlen wird $h(x)$ so mit einer geeigneten $x-$Potenz x^p und einer geeigneten Konstanten $a \in K$ multipliziert, daß $g(x) - ax^p h(x)$ einen kleineren Grad als $g(x)$ hat. Danach schreibt man $ax^p h(x)$ wie im Beispiel unter $g(x)$ in die zweite Zeile, und $k(x)$ erscheint in der dritten Zeile als Differenz $g(x) - ax^p h(x)$. Auf $k(x)$ wird nun gemäß Induktionsvoraussetzung dasselbe Verfahren angewandt. Wie obigem Beweis zu entnehmen ist, lassen $g(x)$ und $k(x)$ bei Division durch $h(x)$ denselben Rest.

$$
\begin{array}{llll}
x^4 & -4x^2 & +6x & +4 \;:x^2+2x-2 = x^2-2x+2 \\
x^4 & +2x^3 & -2x^2 & \\
\hline
 & -2x^3 & -2x^2 & +6x+4 \\
 & -2x^3 & -4x^2 & +4x \\
\hline
 & & 2x^2 & +2x+4 \\
 & & 2x^2 & +4x-4 \\
\hline
 & & & -2x+8
\end{array}
$$

Insgesamt erhalten wir also $x^4 - 4x^2 + 6x + 4 = (x^2 - 2x + 2)(x^2 + 2x - 2) - 2x + 8$.

Satz 3.2 *Ist R ein euklidischer Ring und sind $a, b \in R$, dann existiert ein* ggT *von a und b, und es gibt $x, y \in R$ mit $d = xa + yb$, wobei $d \sim (a, b)$.*

Beweis. Ist $a = 0$, dann ist b ein ggT von a und b, und ist $b = 0$, so ist a ein ggT von a und b. In beiden Fällen gilt die Behauptung. Seien also $a, b \neq 0$. Wir berechnen rekursiv $r_1, q_1, r_2, q_2, \ldots \in R$ durch

$$
\begin{aligned}
a &= q_1 b + r_1, \quad g(r_1) < g(b) \\
b &= q_2 r_1 + r_2, \quad g(r_2) < g(r_1) \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, \quad g(r_n) < g(r_{n-1}) \\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}
$$

Da die Werte von g in $\mathbb{N}_0$ liegen, bricht obiges Verfahren nach endlich vielen Schritten ab. Gemäß der Rechenregel 3 nach Satz 2.2 gilt

$$
\begin{aligned}
(a, b) &\sim (a - q_1 b, b) \sim (r_1, b) \sim (r_1, b - q_2 r_1) \sim (r_1, r_2) \sim \ldots \\
&\sim (r_{n-1}, r_n) \sim (q_{n+1} r_n, r_n) \\
&\sim r_n =: d.
\end{aligned}
$$

Die Darstellung von d in der Form $d = xa + yb$ erhält man durch "Rückwärtseinsetzen".

□

Bemerkung. Obiges Verfahren zur Berechnung eines ggT bezeichnet man als *euklidischen Algorithmus.*

Durch vollständige Induktion erhält man

Korollar 3.3 *Ist R ein euklidischer Ring und sind $a_1, \ldots, a_n \in R$, dann existiert $d \sim (a_1, \ldots, a_n)$, und es gibt $x_1, \ldots, x_n \in R$ mit $d = x_1 a_1 + \ldots + x_n a_n$.*

Beispiel. Wir berechnen im Ring $\mathbb{Z}$ der ganzen Zahlen einen ggT von $6, 10$ und 15.

Berechnung von $(6, 10)$			Rückwärtseinsetzen
10	$=$	$1 \cdot 6 + 4$	$6 - 1 \cdot 4 = 2$
6	$=$	$1 \cdot 4 + 2$	$6 - 1 \cdot (10 - 1 \cdot 6) = 2$
4	$=$	$2 \cdot 2$, also	$2 \cdot 6 - 1 \cdot 10 = 2.$
2	$\sim$	$(6, 10)$.	

Nun muß noch ein ggT von 2 und 15 berechnet werden. Wegen $(15, 2) \sim (15 - 2 \cdot 7, 2) \sim (1, 2) \sim 1$ ist 1 ein ggT von $6, 10$ und 15, und es folgt

$$1 = 15 - 7 \cdot 2 = 15 - 7 \cdot (2 \cdot 6 - 1 \cdot 10) = 15 - 14 \cdot 6 + 7 \cdot 10.$$

Satz 3.4 *Ist R ein euklidischer Ring und ist $q \in R$ unzerlegbar, so ist q prim.*

Beweis. Da q unzerlegbar ist, gilt $q \neq 0$, und q ist keine Einheit. Sei nun q Teiler von $a \cdot b$ mit $a, b \in R$, sowie $d \sim (q, a)$. Dann existieren $x, y, r, s \in R$ mit $d = ax + qy$ und $a = dr, q = ds$. Da q unzerlegbar ist, ist d eine Einheit oder s eine Einheit.
1. Fall: s ist eine Einheit. Dann folgt $a = q(s^{-1}r)$, d.h. $q|a$.
2. Fall: d ist eine Einheit. Dann folgt

$$b = baxd^{-1} + bqyd^{-1}.$$

Da q Teiler von ab ist, folgt $q|b$.

□

Satz 3.5 *Ist R ein euklidischer Ring, dann läßt sich jedes $a \in R, a \neq 0$, das keine Einheit ist, eindeutig als Produkt von Primelementen schreiben, d.h.*
i) Es gibt Primelemente $p_1, \ldots, p_n \in R$ mit $a = p_1 \cdot \ldots \cdot p_n$.
ii) Sind $q_1, \ldots, q_m \in R$ Primelemente mit $a = q_1 \cdot \ldots \cdot q_m$, so gilt $n = m$ und bei geeigneter Indizierung $p_i \sim q_i$ für $i = 1, \ldots, n$.

Beweis. Sei g eine Wertefunktion von R, die wegen Aufgabe 4.4 sogar als regulär angenommen werden kann. Wir beweisen zunächst i) und nehmen an, daß es ein Element $a \in R, a \neq 0, a \notin \mathrm{E}(R)$ gibt, das nicht Produkt von Primelementen ist. Wir können weiterhin annehmen, daß a mit dieser Eigenschaft einen minimalen Wert $g(a)$ hat, d.h., ist $b \in R, b \neq 0$ und b keine Einheit mit $g(b) < g(a)$, dann ist b Produkt von Primelementen. Zunächst ist a selbst kein Primelement und wegen Satz 3.4 damit nicht unzerlegbar, d.h., es gibt $b, c \in R \setminus \{0\}$ mit $b, c \notin \mathrm{E}(R)$ und $a = bc$.
Da R ein euklidischer Ring ist, existieren nun $q, r \in R$ mit $b = q \cdot a + r$, wobei $r = 0$

oder $g(r) < g(a)$. Gilt $r = 0$, so folgt $a = cqa$, d.h. $1 = cq$ und damit $c \in \mathrm{E}(R)$, also ein Widerspruch. Es folgt

$$0 \neq r = b - qa = b - qbc = b(1 - qc)$$

und $g(a) > g(r) = g(b(1 - qc)) \geq g(b)$ auf Grund der Regularität von g, also $g(a) > g(b)$. Entsprechend ergibt sich $g(a) > g(c)$. Wegen der Minimalität von $g(a)$ lassen sich nun b und c und mit $a = bc$ auch a als Produkt von Primelementen schreiben.
Wir zeigen nun die Eindeutigkeit der Zerlegung $a = p_1 \cdot \ldots \cdot p_n$ durch Induktion nach n.
$n = 1$: Es gilt $a = p_1 = q_1 \cdot \ldots \cdot q_m$, wobei $q_1, \ldots, q_m$ prim sind. Da p_1 als Primelement unzerlegbar ist, ist $q_2 \cdot \ldots \cdot q_m$ Einheit, also $q_2, \ldots, q_m \in \mathrm{E}(R)$, d.h. $m = 1$ und $p_1 = q_1$.
$n > 1$: Sei $p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$. Da p_1 prim ist, folgt $p_1 | q_i$ für ein $i = 1, \ldots, m$. O.B.d.A. sei p_1 Teiler von q_1, also $q_1 = p_1 \cdot e$ mit $e \in \mathrm{E}(R)$, da q_1 unzerlegbar ist. Somit gilt $p_1 \sim q_1$ und

$$p_2 \cdot \ldots \cdot p_n = (eq_2) \cdot q_3 \cdot \ldots q_m.$$

Wegen $e \in \mathrm{E}(R)$ ist eq_2 prim, und nach Induktionsvoraussetzung folgt $n - 1 = m - 1$, d.h. $n = m$, sowie $p_i \sim q_i$ für $i \geq 2$ bei geeigneter Indizierung.

□

Beispiel.

1. Jede ganze Zahl $z \in \mathbb{Z}, z \neq 0, 1, -1$ läßt sich "eindeutig" als Produkt von Primzahlen schreiben.

2. Ist K ein Körper und $f(x) \in K[x]$ mit grad $f(x) \geq 1$, so läßt sich $f(x)$ "eindeutig" als Produkt von irreduziblen Polynomen schreiben.

Anwendung: Nullstellen eines Polynoms.

Ist K ein Körper und $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ ein Polynom, so heißt $a \in K$ Nullstelle von $f(x)$, wenn $f(a) := a_n a^n + \ldots + a_1 a + a_0 = 0$.

Wir zeigen nun für alle $a \in K$:

$$f(a) = 0 \iff \text{ Es gibt } q(x) \in K[x] \text{ mit } f(x) = q(x)(x - a).$$

Beweis. Gilt $f(x) = q(x)(x - a)$, so folgt $f(a) = q(a)(a - a) = 0$. Ist nun andererseits a eine Nullstelle von $f(x)$, dann gibt es Polynome $q(x), r(x) \in K[x]$ mit $f(x) = q(x)(x - a) + r(x)$, wobei $r(x) = 0$ oder grad $r(x) = 0$, d.h. $r(x) = r \in K$. Wegen $0 = f(a) = q(a)(a - a) + r$ folgt $r(x) = 0$, also die Behauptung.

□

Sind $a_1, \ldots, a_l$ paarweise verschiedene Nullstellen von $f(x)$, so sind $x - a_1, \ldots, x - a_l$ paarweise nichtassoziierte Primteiler von $f(x)$, d.h.

$$f(x) = (x - a_1) \cdot \ldots \cdot (x - a_l) \cdot h(x)$$

für ein $h(x) \in K[x]$.

Folgerung. Ist K ein Körper und $f(x) \in K[x]$ ein Polynom über K mit $n = \text{grad } f(x) \geq 0$, so hat $f(x)$ in K höchstens n verschiedene Nullstellen.

Bemerkung. Ist R ein euklidischer Ring und sind $a, b \in R\backslash\{0\}$ keine Einheiten, so kann mit Hilfe des euklidischen Algorithmus ein ggT von a und b berechnet werden, ohne die Primfaktorzerlegung von a und b zu kennen. Dieses ist für die praktische Durchführung sehr wichtig, denn z.B. für sehr große natürliche Zahlen ist die Primfaktorzerlegung oft sehr schwierig und zum Teil praktisch nicht durchführbar. Ist d ein ggT von a und b, so ist $\frac{a \cdot b}{d}$ ein kgV von a und b, d.h., auch ein kgV kann berechnet werden, ohne die Primfaktorzerlegung von a und b zu kennen. Liegt aber die Zerlegung vor, d.h., sind $p_1, \ldots, p_n$ paarweise "verschiedene" Primelemente in R mit

$$a \sim p_1^{k_1} \cdot \ldots \cdot p_n^{k_n} \quad (k_1, \ldots, k_n \in \mathbb{N}_0) \text{ und } b \sim p_1^{l_1} \cdot \ldots \cdot p_n^{l_n} \quad (l_1, \ldots, l_n \in \mathbb{N}_0),$$

dann ist

$$p_1^{\min\{l_1,k_1\}} \cdot \ldots \cdot p_n^{\min\{l_n,k_n\}} \text{ ein ggT und } p_1^{\max\{l_1,k_1\}} \cdot \ldots \cdot p_n^{\max\{l_n,k_n\}} \text{ ein kgV von } a \text{ und } b.$$

Satz 3.6 *Ist R ein euklidischer Ring, dann ist jedes Ideal I von R ein Hauptideal.*

Beweis. Im folgenden ist g eine Wertefunktion von R, bezüglich der R ein euklidischer Ring ist. Gilt $I = \{0\}$, so ist $I = (0)$. Wir können also $I \neq \{0\}$ annehmen und definieren

$$M = \{g(r) \mid r \in I, r \neq 0\} \subseteq \mathbb{N}_0.$$

M ist nicht leer und hat somit ein kleinstes Element n. Es gibt ein $a \in I, a \neq 0$, mit $g(a) = n = \min\{g(r) \mid r \in I, r \neq 0\}$, und wir zeigen $I = (a)$.
Wegen $a \in I$ folgt $ar \in I$ für alle $r \in R$, da I ein Ideal von R ist, d.h. $(a) \subseteq I$. Ist nun andererseits $i \in I$, dann gibt es $q, r \in R$ mit $i = q \cdot a + r$, wobei $r = 0$ oder $g(r) < g(a)$. Wäre $r \neq 0$, so wäre $r = i - q \cdot a \in I$ mit $g(r) < g(a)$, im Widerspruch dazu, daß $n = g(a)$ in M minimal ist. Also folgt $i = q \cdot a \in (a)$, d.h. $I \subseteq (a)$.

□

Bemerkung. Ist R ein euklidischer Ring und sind $a, b \in R$, so gilt für $d \in R$:

$$d \text{ ist ein ggT von } a \text{ und } b \iff (d) = (a) + (b),$$

$$d \text{ ist ein kgV von } a \text{ und } b \iff (d) = (a) \cap (b).$$

Faktorringe von euklidischen Ringen.

Im folgenden ist R ein euklidischer Ring, der kein Körper ist, und I ein Ideal von R. Wir behandeln die Frage, unter welchen Voraussetzungen der Faktorring R/I ein Körper ist. Zunächst gibt es wegen Satz 3.6 ein $r \in R$ mit $I = (r)$. Ist $r = 0$, dann gilt $I = (0)$ und $R/I = R/(0) \cong R$, d.h., R/I ist kein Körper. Ist r eine Einheit, dann gilt $I = (r) = R$ wegen Bemerkung 1 nach Definition 1.5, da $r \in (r)$. Es folgt $\overline{0} = 0 + R = R = 1 + R = \overline{1}$, d.h., R/I ist kein Körper. Sei also im folgenden $r \neq 0$ und $r \notin \text{E}(R)$. Wir unterscheiden zwei Fälle.

1. Fall: r ist prim. Dann ist r keine Einheit, d.h. $1 \notin (r) = I$, und es gilt $\overline{0} \neq \overline{1}$. Wir zeigen nun, daß $\overline{a} \in R/I, \overline{a} \neq \overline{0}$ in R/I invertierbar ist. Wegen $\overline{a} \neq \overline{0}$ gilt $a \notin (r)$, d.h., r teilt a nicht. Da r prim ist, folgt $1 \sim (r, a)$, und es gibt $x, y \in R$ mit $1 = xr + ya$, d.h.

$$\overline{1} = \overline{x} \cdot \overline{r} + \overline{y} \cdot \overline{a} = \overline{y} \cdot \overline{a}.$$

Damit ist $\overline{y}$ das multiplikative Inverse von $\overline{a}$, d.h., R/I ist ein Körper.
2. Fall: r ist nicht prim. Dann ist r nicht unzerlegbar, d.h., es gibt $a, b \in R$ mit $r = a \cdot b$ und $a, b \neq \mathrm{E}(R)$. Wäre $a \in (r)$, so wäre $a = r \cdot s$ für ein $s \in R$, d.h. $a = a \cdot b \cdot s$, also $1 = b \cdot s$, im Widerspruch zu $b \notin \mathrm{E}(R)$. Somit gilt $\overline{a} \neq \overline{0}$, und entsprechend folgt $\overline{b} \neq \overline{0}$. Wegen $\overline{a} \cdot \overline{b} = \overline{r} = \overline{0}$ sind damit $\overline{a}, \overline{b}$ Nullteiler in R/I, d.h., R/I ist kein Körper.

Insgesamt haben wir also gezeigt:

Satz 3.7 *Ist R ein euklidischer Ring und $r \in R \setminus \{0\}$, dann gilt*

$$R/(r) \text{ ist ein Körper } \iff r \text{ ist prim.}$$

Obiger Beweis liefert sogar:

Satz 3.8 *Ist R ein euklidischer Ring und $r \in R \setminus \{0\}$, dann gilt*

$$R/(r) \text{ ist ein Integritätsbereich } \iff R/(r) \text{ ist ein Körper.}$$

Ziel ist es nun, folgenden Satz zu beweisen:

Satz 3.9 *Ist R ein euklidischer Ring und sind $r_1, \ldots, r_k \in R \setminus \{0\}$ keine Einheiten und paarweise teilerfremd, d.h., ist $(r_i, r_j) \sim 1$ für $i \neq j$, so gilt*

$$R/(r_1 \cdot \ldots \cdot r_k) \cong R/(r_1) \times \ldots \times R/(r_k).$$

Korollar 3.10 *Ist R ein euklidischer Ring sowie $r \in R \setminus \{0\}$ keine Einheit und ist $r \sim p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$ die Primfaktorzerlegung von r mit "verschiedenen" Primfaktoren $p_1, \ldots, p_k$, so gilt*

$$R/(r) \cong R/(p_1^{n_1}) \times \ldots \times R/(p_k^{n_k}).$$

Wir werden Satz 3.9 mit Hilfe des sogenannten *Chinesischen Restsatzes* beweisen. Dazu benötigen wir einige Vorbetrachtungen. Ist $r \in R, r \neq 0$ und sind $a, b \in R$, so definiert man

$$a \equiv b \bmod r \quad :\iff \quad r \text{ teilt } a - b.$$

Gilt $a \equiv b \bmod r$, so sagt man, daß a und b kongruent modulo r sind, und $a \equiv b \bmod r$ heißt Kongruenz. Offenbar ist folgendes erfüllt:

$$\begin{aligned} a \equiv b \bmod r &\iff \text{Es gibt ein } s \in R \text{ mit } a - b = rs \\ &\iff \text{Es gibt ein } s \in R \text{ mit } a = b + rs \\ &\iff a + (r) = b + (r) \\ &\iff \overline{a} = \overline{b} \text{ in } R/(r). \end{aligned}$$

Damit übertragen sich die Rechenregeln, die im Faktorring $R/(r)$ gelten, auf das Rechnen mit Kongruenzen. Für alle $c \in R$ folgt zum Beispiel aus $a \equiv b \bmod r$

$$a + c \equiv b + c \bmod r \quad \text{und } ac \equiv bc \bmod r.$$

Chinesischer Restsatz. Ist R ein euklidischer Ring und sind $r_1, \ldots, r_k \in R \setminus \{0\}$ paarweise teilerfremd, dann existiert zu beliebigen $a_1, \ldots, a_k \in R$ ein $x \in R$ mit

$$(*) \qquad x \equiv a_1 \bmod r_1, \ldots, x \equiv a_k \bmod r_k.$$

Ist x eine Lösung von $(*)$, so ist $x + r_1 \cdot \ldots \cdot r_k R$ die Gesamtlösungsmenge von $(*)$ in R.

Beweis. Wir definieren $u_i := \frac{r_1 \cdot \ldots \cdot r_k}{r_i}$. Dann ist r_i ein Teiler von u_j für $i \neq j$, und u_i, r_i sind teilerfremd. Es existieren $s_i, m_i \in R$ mit

$$1 = s_i \cdot r_i + m_i \cdot u_i, \text{ also } m_i u_i \equiv 1 \bmod r_i.$$

Mit $x := a_1 u_1 m_1 + \ldots + a_k u_k m_k$ folgt

$$x \equiv a_i u_i m_i \bmod r_i, \text{ also } x \equiv a_i \bmod r_i.$$

Jedes Element aus $x + r_1 \cdot \ldots \cdot r_k R$ ist offenbar ebenfalls eine Lösung von $(*)$, und ist $x' \in R$ eine weitere Lösung von $(*)$, so ist jedes r_i Teiler von $x' - x$, d.h. $r_1 \cdot \ldots \cdot r_k$ ist Teiler von $x' - x$, da $r_1, \ldots, r_k$ paarweise teilerfremd sind. Es folgt $x' - x = r_1 \cdot \ldots \cdot r_k \cdot s$ für ein $s \in R$, also $x' \in x + r_1 \cdot \ldots \cdot r_k R$.

□

Beispiel.

1. Folgendes Kongruenzensystem ist in $\mathbb{Z}$ zu lösen:

   $$(*) \qquad x \equiv 3 \bmod 5, \; x \equiv 4 \bmod 8, \; x \equiv 2 \bmod 11.$$

   Zunächst erhalten wir $u_1 = 88, u_2 = 55, u_3 = 40$. Gesucht sind nun $m_1, m_2, m_3 \in \mathbb{Z}$ mit

   $$\begin{aligned} m_1 \cdot 88 &\equiv 1 \bmod 5, \text{ also } m_1 \cdot 3 \equiv 1 \bmod 5, \\ m_2 \cdot 55 &\equiv 1 \bmod 8, \text{ also } m_2 \cdot 7 \equiv 1 \bmod 8, \\ m_3 \cdot 40 &\equiv 1 \bmod 11, \text{ also } m_3 \cdot 7 \equiv 1 \bmod 11. \end{aligned}$$

   Nach Anwenden des euklidischen Algorithmus mit anschließendem Rückwärtseinsetzen erhält man zum Beispiel $m_1 = 2, m_2 = 7, m_3 = 8$. Es ergibt sich

   $$x = 3 \cdot 88 \cdot 2 + 4 \cdot 55 \cdot 7 + 2 \cdot 40 \cdot 8 = 2708,$$

   und $2708 + 440 \cdot \mathbb{Z}$ ist die Gesamtlösungsmenge von $(*)$. Als betragskleinste Lösung erhält man 68.

2. (Zerlegung von Kongruenzen) Sind $r_1, \ldots, r_k$ nicht teilerfremd, so ist zunächst nicht klar, ob das gegebene Kongruenzensystem lösbar ist. Wie in diesem Falle zu verfahren ist, zeigt folgendes Beispiel. Wir betrachten über $\mathbb{Z}$ das System

$$x \equiv 13 \bmod 55,\ x \equiv 68 \bmod 88,\ x \equiv 28 \bmod 40.$$

Wegen des Chinesischen Restsatzes können die einzelnen Kongruenzen wie folgt äquivalent umgeformt werden:

$$\begin{aligned} x \equiv 13 \bmod 55 &\iff (x \equiv 3 \bmod 5 \text{ und } x \equiv 2 \bmod 11),\\ x \equiv 68 \bmod 88 &\iff (x \equiv 4 \bmod 8 \text{ und } x \equiv 2 \bmod 11),\\ x \equiv 28 \bmod 40 &\iff (x \equiv 3 \bmod 5 \text{ und } x \equiv 4 \bmod 8). \end{aligned}$$

Aus den einzelnen neuen Kongruenzen ergibt sich ein neues System:

$$x \equiv 3 \bmod 5,\ x \equiv 4 \bmod 8,\ x \equiv 2 \bmod 11,$$

das wegen des Chinesischen Restsatzes lösbar ist. Die Gesamtlösungsmenge des neuen Systems ist $68 + 440 \cdot \mathbb{Z}$ und damit die Gesamtlösungsmenge des ursprünglichen Systems. Ändert man nun zum Beispiel die Kongruenz $x \equiv 13 \bmod 55$ im ursprünglichen System um in $x \equiv 23 \bmod 55$, so erhält man $x \equiv 3 \bmod 5$ und $x \equiv 1 \bmod 11$ als neue Kongruenzen. Die zweite Kongruenz widerspricht nun der zweiten Kongruenz, die sich aus $x \equiv 68 \bmod 88$ ergibt, d.h., das System

$$x \equiv 23 \bmod 55,\ x \equiv 68 \bmod 88,\ x \equiv 28 \bmod 40$$

hat keine Lösung.

Es folgt nun der

Beweis von Satz 3.9.
Wir betrachten die Abbildung

$$\varphi :\ R \longrightarrow R/(r_1) \times \ldots \times R/(r_k), \quad x \longmapsto (x + (r_1), \ldots, x + (r_k)).$$

Offenbar ist φ ein Ringhomomorphismus, und wir zeigen, daß φ sogar surjektiv ist. Zu $(a_1 + (r_1), \ldots, a_k + (r_k))$ aus $R/(r_1) \times \ldots \times R/(r_k)$ gibt es wegen des Chinesischen Restsatzes ein $x \in R$ mit

$$\begin{gathered} x \equiv a_1 \bmod r_1, \ldots, x \equiv a_k \bmod r_k, \text{ also}\\ x + (r_1) = a_1 + (r_1), \ldots, x + (r_k) = a_k + (r_k), \text{ d.h.}\\ \varphi(x) = (x + (r_1), \ldots, x + (r_k)) = (a_1 + (r_1), \ldots, a_k + (r_k)). \end{gathered}$$

Der Kern von φ besteht schließlich genau aus den $x \in R$ mit

$$\begin{gathered} (x + (r_1), \ldots, x + (r_k)) = (0 + (r_1), \ldots, 0 + (r_k)), \text{ also}\\ x \equiv 0 \bmod r_1, \ldots, x \equiv 0 \bmod r_k. \end{gathered}$$

Wegen des Chinesischen Restsatzes folgt Kern$\varphi = r_1 \cdot \ldots \cdot r_k \cdot R = (r_1 \cdot \ldots \cdot r_k)$, und der Homomorphiesatz (Satz 1.8) liefert

$$R/(r_1 \cdot \ldots \cdot r_k) \cong R/(r_1) \times \ldots \times R/(r_k).$$

□

Wir wollen nun die obigen Ergebnisse speziell auf den euklidischen Ring $\mathbb{Z}$ anwenden. Wegen der Sätze 3.7 und 3.8 gilt für alle $n \in \mathbb{N}$:

$$\mathbb{Z}_n \text{ ist ein Integritätsbereich} \iff \mathbb{Z}_n \text{ ist ein Körper} \iff n \text{ ist eine Primzahl.}$$

Ist p eine Primzahl, so kann das multiplikative Inverse von $\overline{a} \in \mathbb{Z}_p, \overline{a} \neq \overline{0}$ mit Hilfe des euklidischen Algorithmus berechnet werden. Wegen $\overline{a} \neq \overline{0}$ gilt $a \notin (p)$, d.h., p ist kein Teiler von a. Da p prim ist, sind a und p teilerfremd. Es gibt also $x, y \in \mathbb{Z}$ mit

$$xp + ya = 1, \text{ also } \overline{1} = \overline{y} \cdot \overline{a} \text{ und } \overline{a}^{-1} = \overline{y}.$$

Als Beispiel wählen wir $p = 19$ und $\overline{a} = \overline{7}$.

Berechnung von $(7, 19)$			Rückwärtseinsetzen
19	$=$	$2 \cdot 7 + 5$	$(19 - 2 \cdot 7) \cdot 3 - 2 \cdot 7 = 19 \cdot 3 - 8 \cdot 7 = 1.$
7	$=$	$1 \cdot 5 + 2$	$5 - 2 \cdot (7 - 1 \cdot 5) = 5 \cdot 3 - 2 \cdot 7 = 1$
5	$=$	$2 \cdot 2 + 1,$ also	$5 - 2 \cdot 2 = 1.$

Damit gilt $\overline{7}^{-1} = \overline{11}$ in $\mathbb{Z}_{19}$.

Ist $n \in \mathbb{N}, n > 1$ keine Primzahl, so ist nicht jedes $\overline{a} \in \mathbb{Z}_n, \overline{a} \neq \overline{0}$ in $\mathbb{Z}_n$ invertierbar. Es gilt aber

$$\begin{aligned} \overline{a} \text{ ist in } \mathbb{Z}_n \text{ invertierbar} &\iff \text{Es gibt ein } \overline{b} \in \mathbb{Z}_n \text{ mit } \overline{a} \cdot \overline{b} = \overline{1} \\ &\iff \text{Es gibt } b, x \in \mathbb{Z} \text{ mit } a \cdot b = 1 + n \cdot x \\ &\iff a \text{ und } n \text{ sind teilerfremd.} \end{aligned}$$

Für die Einheitengruppe $\mathrm{E}(\mathbb{Z}_n)$ von $\mathbb{Z}_n$ ergibt sich damit

$$\mathrm{E}(\mathbb{Z}_n) = \{\overline{a} \in \mathbb{Z}_n \mid (a, n) \sim 1\} \text{ sowie}$$
$$|\mathrm{E}(\mathbb{Z}_n)| = |\{a \in \mathbb{N} \mid 1 \leq a \leq n \text{ und } (a, n) \sim 1\}|.$$

Definition 3.11 *Die Funktion*

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}, n \longmapsto |\mathrm{E}(\mathbb{Z}_n)|$$

heißt Eulersche φ-Funktion.

Satz 3.12 *1. Ist p eine Primzahl und $k \in \mathbb{N}$, so gilt $\varphi(p^k) = p^k - p^{k-1}$.*

2. Sind $n, m \in \mathbb{N}$ teilerfremd, so gilt $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

3. Ist $n \in \mathbb{N}$ und $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$ die Primfaktorzerlegung von n, so gilt

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_l}).$$

Beweis.

1. Für alle $a \in \mathbb{N}$ gilt $(a, p^k) \not\sim 1$ genau dann, wenn p ein Teiler von a ist, also

$$\begin{aligned} |\{a \in \mathbb{N} \mid 1 \leq a \leq p^k \text{ und } (a, p^k) \not\sim 1\}| &= |\{p \cdot l \mid 1 \leq p \cdot l \leq p^k\}| \\ &= |\{l \mid 1 \leq l \leq p^{k-1}\}| \\ &= p^{k-1}. \end{aligned}$$

   Es folgt

$$\begin{aligned} |\{a \in \mathbb{N} \mid 1 \leq a \leq p^k \text{ und } (a, p^k) \sim 1\}| &= p^k - |\{a \in \mathbb{N} \mid 1 \leq a \leq p^k \text{ und } (a, p^k) \not\sim 1\}| \\ &= p^k - p^{k-1}. \end{aligned}$$

2. Mit Satz 3.9 gilt $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$, also $|\mathrm{E}(\mathbb{Z}_{nm})| = |\mathrm{E}(\mathbb{Z}_n)| \cdot |\mathrm{E}(\mathbb{Z}_m)|$, d.h.

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m).$$

3. Wegen 1. und 2. gilt $\varphi(n) = \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_l^{k_l}) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdot \ldots \cdot (p_l^{k_l} - p_l^{k_l - 1})$, also

$$\varphi(n) = p_1^{k_1} \cdot (1 - \frac{1}{p_1}) \cdot \ldots \cdot p_l^{k_l}(1 - \frac{1}{p_l}) = n \cdot (1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_l}).$$

□

Satz 3.13 (Euler) *Sind $a, n \in \mathbb{N}$ teilerfremd, so gilt $a^{\varphi(n)} \equiv 1 \bmod n$.*

Beweis. Sind $a, n \in \mathbb{N}$ teilerfremd, so ist $\overline{a}$ Einheit in $\mathbb{Z}_n$, d.h. $\overline{a} \in \mathrm{E}(\mathbb{Z}_n)$. Wegen $|\mathrm{E}(\mathbb{Z}_n)| = \varphi(n)$ und Korollar 1.13 aus Kapitel 1 gilt $\overline{1} = \overline{a}^{|\mathrm{E}(\mathbb{Z}_n)|} = \overline{a}^{\varphi(n)}$, also $a^{\varphi(n)} \equiv 1 \bmod n$.

□

Korollar 3.14 (Fermat) *Ist $p \in \mathbb{N}$ eine Primzahl, so gilt $a^p \equiv a \bmod p$ für alle $a \in \mathbb{N}$.*

Beweis. Ist p ein Teiler von a, so gilt $a \equiv a^p \equiv 0 \bmod p$. Ist aber p kein Teiler von a, so sind a und p teilerfremd, und wegen $\varphi(p) = p - 1$ folgt $a^{p-1} \equiv 1 \bmod p$ mit Satz 3.13.

□

4. Aufgaben

A 4.1 Zeigen Sie: Ist R ein Ring und sind $I_1, \ldots, I_k$ Ideale von R, dann ist auch $I_1 + \ldots + I_k$ ein Ideal von R.

A 4.2 Es sei $d \in \mathbb{Z}$ quadratfrei und $d \neq 0, 1$. Auf dem Integritätsbereich

$$\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

sei die Normfunktion N definiert durch

$$\mathrm{N} : \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{N}_0,\ a + b\sqrt{d} \longmapsto \mid a^2 - db^2 \mid .$$

Berechnen Sie die Einheiten von $\mathbb{Z}[\sqrt{d}]$ für den Fall $d < 0$ und zeigen Sie für alle $x, y \in \mathbb{Z}[\sqrt{d}]$:
a) $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$.
b) Ist x Teiler von y, so ist $\mathrm{N}(x)$ Teiler von $\mathrm{N}(y)$.
c) x ist genau dann eine Einheit, wenn $\mathrm{N}(x) = 1$.
d) x und y sind genau dann assoziiert, wenn $\mathrm{N}(x) = \mathrm{N}(y)$ und x Teiler von y ist.
e) Ist $\mathrm{N}(x)$ eine Primzahl, so ist x unzerlegbar.
f) Ist z ein Teiler von x und y, dann ist $\mathrm{N}(z)$ ein Teiler von $\mathrm{ggT}(\mathrm{N}(x), \mathrm{N}(y))$.

Zeigen Sie speziell für $\mathbb{Z}[\sqrt{-3}]$:
a) $1 + \sqrt{-3}$ ist unzerlegbar, aber nicht prim.
b) 4 besitzt zwei verschiedene Darstellungen als Produkt unzerlegbarer Elemente.
c) 4 und $2(1 + \sqrt{-3})$ haben keinen ggT.
d) Berechnen Sie die folgenden ggT, falls sie existieren:

$$\mathrm{ggT}(2 + \sqrt{-3}, 1 + 2\sqrt{-3}),\ \mathrm{ggT}(1 + \sqrt{-3}, -1 + 3\sqrt{-3}),\ \mathrm{ggT}(7 + \sqrt{-3}, 3 - \sqrt{-3}).$$

A 4.3 a) Zeigen Sie, daß $\mathbb{Z}[i]$ ein euklidischer Ring bezüglich der Normfunktion ist und daß die Normfunktion eine reguläre Wertefunktion ist.

b) Zeigen Sie, daß eine Primzahl $p \in \mathbb{N}$ genau dann in $\mathbb{Z}[i]$ zerlegbar ist, wenn p in $\mathbb{N}$ Summe von zwei Quadraten ist.

c) Zeigen Sie: Ist $x \in \mathbb{Z}[i]$ prim, so gilt $x \mid p$ für eine Primzahl $p \in \mathbb{N}$.

d) Berechnen Sie die Primfaktorzerlegung von $7 + 4i$ und $16 - 13i$ in $\mathbb{Z}[i]$.

e) Berechnen Sie einen ggT von $7 + 4i$ und $8 - i$ in $\mathbb{Z}[i]$.

f) Stellen Sie in $\mathbb{Z}[i]$ einen ggT von $3 - 11i$ und $3 + 4i$ in der Form $x(3 - 11i) + y(3 + 4i)$ mit $x, y \in \mathbb{Z}[i]$ dar.

A 4.4 Zeigen Sie: Ist R ein euklidischer Ring bezüglich der Wertefunktion $g : R\backslash\{0\} \longrightarrow \mathbb{N}_0$, dann ist R auch bezüglich $h : R\backslash\{0\} \longrightarrow \mathbb{N}_0,\ x \longmapsto \min\{g(xy) \mid y \in R\backslash\{0\}\}$ ein euklidischer Ring, und h ist sogar regulär.

A 4.5 Berechnen Sie in $\mathbb{Q}[x]$ einen ggT von $f_1(x), f_2(x), f_3(x)$, wobei $f_1(x) = x^5+x^3-x^2-1$, $f_2(x) = x^6 + x^5 - 4x^4 + 5x^3 - 6x^2 + 4x - 1$, $f_3(x) = x^7 + 3x^6 + x^5 + 3x^4 - 2x^3 + x^2 - 2x + 1$.

A 4.6 Sei R ein euklidischer Ring mit $a, b, d, m \in R \setminus \{0\}$. Zeigen Sie:

$$d \sim \mathrm{ggT}(a,b) \Longleftrightarrow (d) = (a) + (b) \quad \text{und} \quad m \sim \mathrm{kgV}(a,b) \Longleftrightarrow (m) = (a) \cap (b).$$

A 4.7 a) Zeigen Sie: Ist $p \in \mathbb{N}$ eine Primzahl, dann ist die multiplikative Gruppe $\mathbb{Z}_p^\times$ des Körpers $\mathbb{Z}_p$ eine zyklische Gruppe der Ordnung $p-1$.

b) Ein $a \in \mathbb{Z}$ heißt *Primitivwurzel modulo p*, wenn $a \bmod p$ ein erzeugendes Element von $\mathbb{Z}_p^\times$ ist. Geben Sie alle Primitivwurzeln modulo 11 und 13 an.

A 4.8 Welche der folgenden Kongruenzensysteme sind in $\mathbb{Z}$ lösbar? Geben Sie im Falle der Lösbarkeit alle Lösungen an.

$$\text{a) } x \equiv 1 \bmod 6, \quad 5x \equiv 1 \bmod 14, \quad 8x \equiv 17 \bmod 21,$$
$$\text{b) } x \equiv 2 \bmod 6, \quad 5x \equiv 1 \bmod 14, \quad 8x \equiv 17 \bmod 21.$$

A 4.9 Sind 33 und 34 modulo 1615 invertierbar? Berechnen Sie ggf. die Inversen in $\mathbb{Z}_{1615}$.

A 4.10 Gegeben ist im euklidischen Ring $\mathbb{Z}[i]$ das System von Kongruenzen:

$$(*) \quad x \equiv a \bmod 1-2i \ , x \equiv b \bmod 1+i \ , x \equiv c \bmod 2+3i.$$

1. Zeigen Sie, daß $(*)$ für alle $a, b, c \in \mathbb{Z}[i]$ lösbar ist.

2. Geben Sie für $a = 1, b = i, c = 2$ alle Lösungen $x \in \mathbb{Z}[i]$ an.

3. Zeigen Sie, daß $(*)$ nicht mehr für alle $a, b, c \in \mathbb{Z}[i]$ lösbar ist, wenn man $1-2i$ durch $1-3i$ ersetzt. Geben Sie ein Beispiel dazu an.

A 4.11 Erläutern Sie die Neuner- und Elferprobe für die Dezimaldarstellung natürlicher Zahlen.

A 4.12 a) Die Gleichung $n^{13} = 54609997061205831773 27$ ist in $\mathbb{N}$ lösbar. Berechnen Sie die Lösung. Hinweis: Berechnen Sie die Lösung zunächst modulo 10 und 11.

b) Zeigen Sie, daß es kein $n \in \mathbb{N}$ mit $n^{13} = 1049726476761324302959 71$ gibt.

A 4.13 K sei ein Körper und $f_1(x), \ldots, f_m(x) \in K[x]$ nichtkonstante, paarweise teilerfremde Polynome sowie

$$f(x) = f_1(x) \cdot \ldots \cdot f_m(x) \quad \text{und} \quad g_i(x) = \tfrac{f(x)}{f_i(x)}, \ i = 1, \ldots, m.$$

Zeigen Sie, daß es zu jedem Polynom $h(x) \in K[x]$ mit $\mathrm{grad} h(x) < \mathrm{grad} f(x)$ eindeutig bestimmte Polynome $h_1(x), \ldots, h_m(x) \in K[x]$ mit $\mathrm{grad} h_i(x) < \mathrm{grad} f_i(x)$ so gibt, daß gilt:

$$h(x) = h_1(x)g_1(x) + \ldots + h_m(x)g_m(x).$$

A 4.14 K sei ein Körper und $f(x) \in K[x]$ ein Polynom mit $\mathrm{grad} f(x) = n \geq 1$. Zeigen Sie, daß es zu jedem Polynom $g(x) \in K[x]$, $g(x) \neq 0$ ein eindeutig bestimmtes $m \in \mathbb{N}_0$ und eindeutig bestimmte Polynome $p_0(x), \ldots, p_m(x) \in K[x]$ mit $p_m(x) \neq 0$ und $\mathrm{grad} p_i(x) < \mathrm{grad} f(x)$ für $i = 0, \ldots, m$ gibt, so daß gilt

$$g(x) = p_m(x)f^m(x) + \ldots + p_1(x)f(x) + p_0(x).$$

KAPITEL 3

Der Körper der reellen Zahlen

1. Die natürlichen und die ganzen Zahlen

Die folgenden Axiome (Peano-Axiome) bilden ein Axiomensystem für die Menge $\mathbb{N}$ der natürlichen Zahlen.

Axiom 1. $1 \in \mathbb{N}$.

Axiom 2. Zu jedem $n \in \mathbb{N}$ gibt es ein $n' \in \mathbb{N}$.

Axiom 3. Es gibt kein $n \in \mathbb{N}$ mit $n' = 1$.

Axiom 4. Für alle $n, m \in \mathbb{N}$ mit $n' = m'$ gilt $n = m$.

Axiom 5. (Induktionsaxiom) Ist M eine Teilmenge von $\mathbb{N}$, so ist $M = \mathbb{N}$, wenn folgendes gilt:
$1 \in M$ und für alle $n \in M$ gilt $n' \in M$.

Bemerkung.

1. Für $n \in \mathbb{N}$ heißt n' Nachfolger von n.
2. Das Induktionsaxiom ermöglicht es, Sätze über die natürlichen Zahlen mit Hilfe der vollständigen Induktion zu beweisen.

Einfache Eigenschaften.

1. Für alle $n, m \in \mathbb{N}$ gilt: $n \neq m \Longrightarrow n' \neq m'$.
2. Für alle $n \in \mathbb{N}$ gilt $n \neq n'$.
3. Für alle $n \in \mathbb{N}, n \neq 1$ gibt es genau ein $m \in \mathbb{N}$ mit $m' = n$.

Die folgenden Sätze und Eigenschaften sind zwar elementar beweisbar, zum Teil sind die Beweise aber recht mühsam und langatmig, so daß wir im folgenden meistens auf sie verzichten werden (vgl. E. Landau, Grundlagen der Analysis. Leipzig 1930, repr. Chelsea 1960).

Satz 1.1 *Es gibt genau eine Abbildung*

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},\ (n, m) \longmapsto n + m,$$

so daß für alle $n \in \mathbb{N}$ gilt:

1.) $n + 1 = n'$.

2.) Für alle $m \in \mathbb{N}$ gilt $n + m' = (n + m)'$.

Definition 1.2 *Die in Satz 1.1 angegebene, eindeutig bestimmte Funktion*

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},\ (n, m) \longmapsto n + m$$

heißt Addition.

Bemerkung. Üblicherweise werden folgende Symbole eingeführt:

$$2 := 1',\ 3 := 2',\ 4 := 3',\ 5 := 4',\ 6 := 5',\ 7 := 6',\ 8 := 7',\ 9 := 8'.$$

Beispiel. Die Addition zweier natürlicher Zahlen soll an folgendem Beispiel erläutert werden.

$$\begin{aligned} 3 + 2 &= 3 + 1' \ \text{(Definition von 2)} \\ &= (3 + 1)' \ \text{(Eigenschaft 2 der Addition)} \\ &= (3')' \ \text{(Eigenschaft 1 der Addition)} \\ &= 4' \ \text{(Definition von 4)} \\ &= 5 \ \text{(Definition von 5).} \end{aligned}$$

Satz 1.3 *Die Addition auf $\mathbb{N}$ ist assoziativ und kommutativ.*

Einfache Eigenschaften. Für alle $n \in \mathbb{N}$ gilt:

4. Für alle $m \in \mathbb{N}$ gilt $n + m \neq n$.
5. Für alle $l, m \in \mathbb{N}$ gilt: $n \neq m \Longrightarrow n + l \neq m + l$.

Lemma 1.4 *Für alle $n, m \in \mathbb{N}$ gilt genau eine der folgenden Aussagen:*

1. *n=m.*
2. *Es gibt (genau) ein $l \in \mathbb{N}$ mit $m = n + l$.*
3. *Es gibt (genau) ein $l \in \mathbb{N}$ mit $n = m + l$.*

Definition 1.5 *Seien $n, m \in \mathbb{N}$.*

$$\begin{aligned} n < m \quad &:\Longleftrightarrow \quad \textit{Es gibt ein } l \in \mathbb{N} \textit{ mit } m = n + l. \\ n \leq m \quad &:\Longleftrightarrow \quad (n < m \textit{ oder } n = m). \end{aligned}$$

Bemerkung.

1. Gilt $n < m$, so heißt n kleiner als m und m größer als n.
2. Durch $\leq$ wird auf $\mathbb{N}$ eine lineare Ordnung definiert, d.h., für alle $l, m, n \in \mathbb{N}$ gilt:

$$\begin{aligned} &n \leq n \quad \text{(Reflexivität)}. \\ &(n \leq m \ \wedge \ m \leq n) \implies n = m \quad \text{(Antisymmetrie)}. \\ &(n \leq m \ \wedge \ m \leq l) \implies n \leq l \quad \text{(Transitivität)}. \\ &n \leq m \ \vee m \leq n \quad \text{(Linearität)}. \end{aligned}$$

3. Die Ordnung ist mit der Addition verträglich, d.h., für alle $l, m, n \in \mathbb{N}$ gilt:

$$n \leq m \implies n + l \leq m + l.$$

Einfache Eigenschaften. Für alle $n, m \in \mathbb{N}$ gilt:

6. $n < n + m$.
7. $1 \leq n$.
8. $n < m \implies n + 1 \leq m$.

Satz 1.6 (Wohlordnung von $\mathbb{N}$) *Jede nichtleere Teilmenge M von $\mathbb{N}$ besitzt ein kleinstes Element.*

Beweis. Wir definieren $S := \{s \in \mathbb{N} \mid s \leq m \text{ für alle } m \in M\}$. Gäbe es ein $m \in M$ mit $m + 1 \in S$, so wäre insbesondere $m + 1 \leq m$, also $m < m + 1 \leq m$ wegen Eigenschaft 6. Auf Grund der Antisymmetrie erhielten wir $m = m + 1 = m'$ im Widerspruch zu Eigenschaft 2. Also gilt $m + 1 \notin S$ für alle $m \in M$, und da M nicht leer ist, folgt $S \neq \mathbb{N}$. Wegen $1 \in S$ (Eigenschaft 7) kann auf Grund des Induktionsaxioms nicht $k' \in S$ für alle $k \in S$ gelten. Sei also $k \in S$ mit $k' \notin S$. Wäre $k < m$ für alle $m \in M$, so wäre $k' = k + 1 \leq m$ für alle $m \in M$ (Eigenschaft 8), d.h. $k' \in S$ ein Widerspruch. Also gilt $k = m$ für ein $m \in M$, und k ist das kleinste Element von M.

□

Satz 1.7 *Es gibt genau eine Abbildung*

$$\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \ (n, m) \longmapsto n \cdot m,$$

so daß für alle $n \in \mathbb{N}$ gilt:

1.) $n \cdot 1 = n$.

2.) Für alle $m \in \mathbb{N}$ gilt $n \cdot m' = n \cdot m + n$.

Definition 1.8 *Die in Satz 1.7 angegebene, eindeutig bestimmte Funktion*

$$\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},\ (n, m) \longmapsto n \cdot m$$

heißt Multiplikation.

Satz 1.9 *Die Multiplikation auf* $\mathbb{N}$ *ist assoziativ und kommutativ; es gelten die Distributivgesetze. Die Ordnung ist mit der Multiplikation verträglich, d.h., für alle* $l, n, m \in \mathbb{N}$ *gilt:* $n < m \Longrightarrow n \cdot l < m \cdot l$.

Wegen Lemma 1.4 hat nicht jede Gleichung

$$n = m + x$$

mit $n, m \in \mathbb{N}$ eine Lösung in $\mathbb{N}$, d.h., $\mathbb{N}$ ist keine Gruppe bezüglich der Addition. Ziel ist es nun, $\mathbb{N}$ zu einem Zahlbereich zu erweitern, in dem alle Gleichungen der Art $a = b + x$ lösbar sind. Dazu führen wir zunächst die neuen Symbole 0 sowie $-n$ für alle $n \in \mathbb{N}$ ein und definieren

$$\mathbb{N}_0 := \{0\} \cup \mathbb{N}, \quad \mathbb{Z} := \{-n \mid n \in \mathbb{N}\} \cup \{0\} \cup \mathbb{N}.$$

Dabei soll $-n \neq 0$ für alle $n \in \mathbb{N}$ und $-n \neq -m$ für alle $n, m \in \mathbb{N}$ mit $n \neq m$ gelten. Die Elemente von $\mathbb{Z}$ heißen ganze Zahlen.

Die Addition und Multiplikation lassen sich nun folgendermaßen von $\mathbb{N}$ auf $\mathbb{Z}$ fortsetzen. Seien $n, m \in \mathbb{N}$.

$$0 + m := m,\ n + 0 := n,\ 0 + (-m) := -m,\ (-n) + 0 := -n,\ 0 + 0 := 0.$$

$$(-n) + (-m) := -(n + m),\ (-n) + n := 0,\ n + (-n) := 0.$$

$$(-n) + m := \begin{cases} l & \text{falls } n < m \text{ und } n + l = m \\ -l & \text{falls } m < n \text{ und } m + l = n \end{cases} \quad l \in \mathbb{N}.$$

$$n + (-m) := \begin{cases} l & \text{falls } m < n \text{ und } m + l = n \\ -l & \text{falls } n < m \text{ und } n + l = m \end{cases} \quad l \in \mathbb{N}.$$

$$0 \cdot m := 0 \cdot (-m) := n \cdot 0 := (-n) \cdot 0 := 0 \cdot 0 := 0.$$

$$n \cdot (-m) := (-n) \cdot m := -n \cdot m.$$

$$(-n) \cdot (-m) := n \cdot m.$$

Satz 1.10 *Bezüglich obiger Addition und Multiplikation ist $\mathbb{Z}$ ein Integritätsbereich. Dabei ist 0 das neutrale Element der Addition, 1 das Einselement und $-n$ das additive Inverse von n für jedes $n \in \mathbb{N}$.*

Definition 1.11 *Seien $x, y \in \mathbb{Z}$.*

$$\begin{aligned} x < y \quad &:\Longleftrightarrow \quad \text{Es gibt ein } n \in \mathbb{N} \text{ mit } y = x + n. \\ x \leq y \quad &:\Longleftrightarrow \quad (x < y \text{ oder } x = y). \end{aligned}$$

Bemerkung. Durch $\leq$ wird auf $\mathbb{Z}$ eine lineare Ordnung definiert.

Definition 1.12 *Ist R ein Integritätsbereich (Körper), dann heißt R geordneter Integritätsbereich (Körper), wenn es auf R eine lineare Ordnung gibt, so daß für alle $x, y, z \in R$ gilt:*

i) $x < y \implies x + z < y + z.$

ii) $(x < y \ \wedge \ 0 < z) \implies x \cdot z < y \cdot z.$

Satz 1.13 *$\mathbb{Z}$ ist bezüglich der angegebenen Addition, Multiplikation und Ordnung ein geordneter Integritätsbereich.*

Bemerkung. Die hier vorgestellte Methode, den Ring $\mathbb{Z}$ aus $\mathbb{N}$ zu konstruieren, ist mathematisch nicht besonders elegant. Durch die explizite Vorgabe der neuen Elemente $0, -1, -2, \ldots$ entspricht die gewählte Darstellung eher der natürlichen Vorstellung, den Ring $\mathbb{Z}$ der ganzen Zahlen einzuführen. Wie aus der Definition der Addition und Multiplikation zu erkennen ist, hat man zum Beispiel beim Nachweis der Assoziativgesetze eine Vielzahl von Fallunterscheidungen vorzunehmen, so daß die Beweise langatmig und mühsam werden. Eine Methode zur systematischen Zahlbereichserweiterung ohne Fallunterscheidungen wird im folgenden Paragraphen vorgestellt.

2. $\mathbb{Q}$ als Quotientenkörper von $\mathbb{Z}$

Ziel dieses Paragraphen ist es, $\mathbb{Q}$ als sogenannten Quotientenkörper von $\mathbb{Z}$ einzuführen. Die hierbei benutzte Methode kann aber nicht nur auf $\mathbb{Z}$, sondern auf jeden Integritätsbereich R angewendet werden. Wir werden also nicht nur $\mathbb{Q}$ als Quotientenkörper von $\mathbb{Z}$ erhalten, sondern zum Beispiel für jeden Körper K den Körper $K(x)$ der gebrochen rationalen Funktionen als Quotientenkörper des Polynomringes $K[x]$.

Im folgenden ist R ein Integritätsbereich sowie

$$\begin{aligned} R \times R &= \{(r,s) \mid r,s \in R\} \quad \text{und} \\ \mathcal{F}(R) &= \{(r,s) \mid r,s \in R \text{ und } s \neq 0\}. \end{aligned}$$

Die Elemente von $\mathcal{F}(R)$ werden später nicht die gewünschten Brüche sein, also nicht die Elemente des Quotientenkörpers, sondern nur "mögliche Bezeichnungen". Unter welcher Voraussetzung zwei Elemente aus $\mathcal{F}(R)$ denselben Bruch bezeichnen, wird durch folgende Relation festgelegt.

Für alle $(r,s),(r',s') \in \mathcal{F}(R)$ definieren wir:

$$(r,s) \sim (r',s') \iff rs' = sr'.$$

Dann gilt für alle $(r,s),(r',s'),(r'',s'') \in \mathcal{F}(R)$:

1. $(r,s) \sim (r,s)$ (Reflexivität)
2. $(r,s) \sim (r',s') \implies (r',s') \sim (r,s)$ (Symmetrie)
3. $((r,s) \sim (r',s') \ \wedge \ (r',s') \sim (r'',s'')) \Longrightarrow (r,s) \sim (r'',s'')$ (Transitivität)

Beweis. 1.) Wegen $rs = sr$ gilt $(r,s) \sim (r,s)$.

2.) Ist $(r,s) \sim (r',s')$, so folgt $rs' = sr'$, also $r's = s'r$, d.h. $(r',s') \sim (r,s)$.

3.) Gelten $(r,s) \sim (r',s')$ und $(r',s') \sim (r'',s'')$, dann ist $rs' = sr'$ und $r's'' = s'r''$. Aus $rs's'' = sr's''$ und $r's''s = s'r''s$ folgt nun $rs's'' = s'r''s$. Wegen der Nullteilerfreiheit von R und $s' \neq 0$ ergibt sich schließlich $rs'' = r''s$, d.h. $(r,s) \sim (r'',s'')$.

□

Damit ist $''\sim''$ eine Äquivalenzrelation, und für $r,s \in R, s \neq 0$ ist dann

$$\frac{r}{s} := \{(x,y) \in \mathcal{F}(R) \mid (r,s) \sim (x,y)\}$$

die Äquivalenzklasse, in der (r,s) liegt. Es gilt somit

$$\frac{r}{s} = \frac{r'}{s'} \iff (r,s) \sim (r',s') \iff rs' = sr'.$$

Zum Beispiel gilt $\frac{r}{r} = \frac{1}{1}$ für alle $r \in R, r \neq 0$. Die Menge aller Äquivalenzklassen bezeichnen wir mit

$$\mathrm{Q}(R) := \{\frac{r}{s} \mid r, s \in R \text{ und } s \neq 0\},$$

und auf $\mathrm{Q}(R)$ wird folgendermaßen eine Addition und eine Multiplikation definiert:

$$\frac{r}{s} + \frac{r'}{s'} = \frac{r \cdot s' + s \cdot r'}{s \cdot s'}, \qquad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{r \cdot r'}{s \cdot s'}.$$

Da beide Verknüpfungen mit Hilfe von Repräsentanten definiert sind, muß zunächst die Wohldefiniertheit überprüft werden.

Wohldefiniertheit von +: Gilt $\frac{r}{s} = \frac{u}{v}$ und $\frac{r'}{s'} = \frac{u'}{v'}$, dann folgt $rv = su$ und $r'v' = s'u'$, also $rvs'v' + r'v'sv = sus'v' + s'u'sv$, d.h. $(rs' + sr')vv' = ss'(uv' + u'v)$. Somit ergibt sich $\frac{rs'+sr'}{ss'} = \frac{uv'+vu'}{vv'}$.

Die Wohldefiniertheit der Multiplikation beweist man entsprechend. Mit etwas Ausdauer rechnet man nun nach, daß $\mathrm{Q}(R)$ bezüglich der oben definierten Addition und Multiplikation ein kommutativer Ring ist. Dabei gilt:

- $\frac{0}{1}$ ist das neutrale Element der Addition.
- $\frac{-r}{s}$ ist das inverse Element von $\frac{r}{s}$ bezüglich der Addition.
- $\frac{1}{1}$ ist das Einselement.

Schließlich zeigen wir noch, daß $\mathrm{Q}(R)$ ein Körper ist:

Für $\frac{r}{s} \in \mathrm{Q}(R)$ mit $\frac{r}{s} \neq \frac{0}{1}$ gilt $(r, s) \not\sim (0, 1)$, d.h. $r1 \neq s0$, also $r \neq 0$. Es folgt $\frac{s}{r} \in \mathrm{Q}(R)$ und $\frac{s}{r} \cdot \frac{r}{s} = \frac{sr}{sr} = \frac{1}{1}$.

Damit ist zunächst $\mathrm{Q}(R)$ formal der "Körper aller Brüche" von R, aber R selbst ist keine Teilmenge von $\mathrm{Q}(R)$. Das Ziel ist es nun, die Elemente von R mit geeigneten Elementen aus $\mathrm{Q}(R)$ zu identifizieren. Dazu definieren wir

$$[\ \ ] : R \longrightarrow \mathrm{Q}(R),\ r \longmapsto \frac{r}{1}.$$

$[\ \ ]$ ist ein injektiver Ringhomomorphismus (eine Einbettung), so daß das Einselement von R auf das Einselement von $\mathrm{Q}(R)$ abgebildet wird, denn es gilt:

- Für alle $r, s \in R$ ist $[r + s] = [r] + [s]$, da $\frac{r+s}{1} = \frac{r}{1} + \frac{s}{1}$.
- Für alle $r, s \in R$ ist $[r \cdot s] = [r] \cdot [s]$, da $\frac{r \cdot s}{1} = \frac{r}{1} \cdot \frac{s}{1}$.
- $[1]$ ist das Einselement von $\mathrm{Q}(R)$.
- $[\ \ ]$ ist injektiv, denn $[r] = \frac{0}{1}$ gilt genau dann, wenn $\frac{r}{1} = \frac{0}{1}$, d.h. $r = 0$. Damit besteht der Kern von $[\ \ ]$ nur aus 0, und, da $[\ \ ]$ ein Ringhomomorphismus ist, folgt mit Satz 1.4 aus Kapitel 2 die Behauptung.

Für jedes $\frac{r}{s}$ aus $\mathrm{Q}(R)$ ist nun weiterhin:

$$\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s} = \frac{r}{1} \cdot (\frac{s}{1})^{-1} = [r][s]^{-1}.$$

Jedes Element aus $\mathrm{Q}(R)$ läßt sich also als Quotient von zwei Elementen der Form $[r], [s]$ schreiben.

Definition 2.1 *Ist R ein Integritätsbereich, K ein Körper und $f : R \longrightarrow K$ ein injektiver Ringhomomorphismus, dann heißt K Quotientenkörper von R, wenn es zu jedem $k \in K$ Elemente $r, s \in R, s \neq 0$ mit*

$$k = f(r)f(s)^{-1}$$

gibt.

Somit wurde oben bewiesen:

Satz 2.2 *Jeder Integritätsbereich hat einen Quotientenkörper.*

Bemerkung.

1. Identifiziert man die Elemente r und $f(r)$ mit $r \in R$, dann gilt $R \subseteq \mathrm{Q}(R)$, und R ist ein Teilring von $\mathrm{Q}(R)$. Mit dieser Bezeichnung ist dann $\mathrm{Q}(R) = \{rs^{-1} \mid r, s \in R, s \neq 0\}$.

2. Wir werden später sehen, daß es für jeden Integritätsbereich R im wesentlichen genau einen Quotientenkörper gibt.

Beispiel.

1. Den Quotientenkörper von $\mathbb{Z}$ bezeichnet man mit $\mathbb{Q}$, und es gilt

$$\mathbb{Q} = \{\frac{n}{m} \mid n, m \in \mathbb{Z} \text{ und } m \neq 0\}.$$

   Die Elemente von $\mathbb{Q}$ heißen rationale Zahlen.

2. Ist K ein Körper, so bezeichnet man den Quotientenkörper von $K[x]$ mit $K(x)$. Es gilt

$$K(x) = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ und } g(x) \neq 0\}.$$

   Man nennt $K(x)$ den Körper der gebrochen rationalen Funktionen über K in der Unbestimmten x.

Satz 2.3 *R sei ein Integritätsbereich und $\mathrm{Q}(R)$ ein Quotientenkörper von R mit der Einbettung*

$$f : R \longrightarrow \mathrm{Q}(R).$$

Ist K ein Körper und

$$g : R \longrightarrow K$$

ebenfalls ein injektiver Ringhomomorphismus, so gibt es genau einen injektiven Ringhomomorphismus

$$h : \mathrm{Q}(R) \longrightarrow K$$

mit

$$h(f(r)) = g(r) \text{ für alle } r \in R.$$

Beweis. Wir zeigen zunächst die Eindeutigkeit. Sei also die Abbildung $h : \mathrm{Q}(R) \longrightarrow K$ wie im Satz angegeben und $x \in \mathrm{Q}(R)$. Dann gibt es $r, s \in R, s \neq 0$ mit $x = f(r)f(s)^{-1}$, also $h(x) = h(f(r))h(f(s))^{-1} = g(r)g(s)^{-1}$. Damit ist h, falls h existiert, eindeutig bestimmt. Wir zeigen nun, daß es tatsächlich einen solchen Ringhomomorphismus h gibt. Dazu definieren wir

$$h : \mathrm{Q}(R) \longrightarrow K,\ f(r)f(s)^{-1} \longmapsto g(r)g(s)^{-1},$$

und weisen zunächst nach, daß h wohldefiniert ist. Sind $r, r', s, s' \in R$ mit $s, s' \neq 0$ und $f(r)f(s)^{-1} = f(r')f(s')^{-1}$, so folgt $f(rs') = f(r)f(s') = f(r')f(s) = f(r's)$, also $rs' = r's$, da f injektiv ist. Somit gilt $g(r)g(s') = g(r')g(s)$, d.h. $g(r)g(s)^{-1} = g(r')g(s')^{-1}$. Daß h tatsächlich ein Ringhomomorphismus ist, rechnet man nun leicht nach. Wegen $h(f(r)) = g(r)$ für alle $r \in R$ bleibt nur noch die Injektivität von h zu zeigen. Dazu betrachten wir den Kern von h, der ein echtes Ideal von $\mathrm{Q}(R)$ ist, denn es gilt $1 \notin \mathrm{Kern}h$. Somit enthält $\mathrm{Kern}h$ keine Einheit. Da $\mathrm{Q}(R)$ ein Körper ist, folgt $\mathrm{Kern}h = \{0\}$, d.h., h ist injektiv.

□

Bemerkung. Satz 2.3 besagt, daß sich jede Einbettung von R nach K eindeutig zu einer Einbettung von $\mathrm{Q}(R)$ nach K fortsetzen läßt.

Anwendung.

1. Ist R ein Integritätsbereich, so ist der Quotientenkörper $\mathrm{Q}(R)$ bis auf Isomorphie eindeutig bestimmt. Um das zu beweisen, betrachten wir zwei Quotientenkörper $\mathrm{Q}(R)$, $\mathrm{Q}(R)'$ mit den entsprechenden Einbettungen $f : R \longrightarrow \mathrm{Q}(R)$ und $f' : R \longrightarrow \mathrm{Q}(R)'$. Wegen Satz 2.3 gibt es einen injektiven Ringhomomorphismus $h : \mathrm{Q}(R) \longrightarrow \mathrm{Q}(R)'$ mit $f' = h \circ f$ und einen injektiven Ringhomomorphismus $h' : \mathrm{Q}(R)' \longrightarrow \mathrm{Q}(R)$ mit $f = h' \circ f'$. Damit ist $h' \circ h : \mathrm{Q}(R) \longrightarrow \mathrm{Q}(R)$ ein injektiver Ringhomomorphismus mit $h' \circ h \circ f = f$. Da $\mathrm{id} \circ f = f$ für die Identität $\mathrm{id} : \mathrm{Q}(R) \longrightarrow \mathrm{Q}(R)$ gilt, läßt sich die Einbettung $f : R \longrightarrow \mathrm{Q}(R)$ einerseits zu $h' \circ h : \mathrm{Q}(R) \longrightarrow \mathrm{Q}(R)$ und andererseits zu $\mathrm{id} : \mathrm{Q}(R) \longrightarrow \mathrm{Q}(R)$ fortsetzen. Auf Grund der Eindeutigkeit der Fortsetzung (vergleiche Satz 2.3) folgt $h' \circ h = \mathrm{id}$, d.h., h' ist surjektiv und damit ein Isomorphismus.

   Im folgenden werden wir also von dem Quotientenkörper eines Integritätsbereiches R sprechen, der dann mit $\mathrm{Q}(R)$ bezeichnet wird. Dabei wird R wie oben beschrieben als Teilring von $\mathrm{Q}(R)$ aufgefaßt, und es gilt

$$\mathrm{Q}(R) = \{rs^{-1} \mid r, s \in R \text{ und } s \neq 0\}.$$

2. Ist K ein Körper mit dem Einselement 1_K, dann definieren wir $n \cdot 1_K = 0$ für $n = 0$,

$$n \cdot 1_K = \underbrace{1_K + \ldots + 1_K}_{\text{n-mal}} \text{ sowie } (-n) \cdot 1_K = \underbrace{-1_K - \ldots - 1_K}_{\text{n-mal}} \text{ für } n \in \mathbb{N}.$$

Mit dieser Bezeichnung ist die Abbildung

$$f : \mathbb{Z} \longrightarrow K,\ z \longmapsto z \cdot 1_K$$

der einzige nichttriviale Ringhomomorphismus $f : \mathbb{Z} \longrightarrow K$. Insbesondere ist $f(\mathbb{Z})$ ein Teilring von K, und der Kern $I := \text{Kern} f$ von f ist ein Ideal von $\mathbb{Z}$. Wegen Satz 3.6 aus Kapitel 2 ist I sogar ein Hauptideal, also $I = (n)$ mit $n \in \mathbb{N}_0$. Da 1 nicht in I liegt, ist $I \neq \mathbb{Z}$, d.h. $n \neq 1$. Es sind nun zwei Fälle zu unterscheiden.

1. Fall: $n \neq 0$. Wegen des Homomorphiesatzes für Ringe (Satz 1.8 aus Kapitel 2) gilt $f(\mathbb{Z}) \cong \mathbb{Z}/(n)$. Als Teilring mit Eins eines Körpers ist $f(\mathbb{Z})$ ein Integritätsbereich, d.h., n ist eine Primzahl wegen der Sätze 3.7 und 3.8 aus Kapitel 2. Es folgt $f(\mathbb{Z}) \cong \mathbb{Z}_p$ mit p prim.

2. Fall: $n = 0$. Dann ist $f : \mathbb{Z} \longrightarrow K$ eine Einbettung, die sich wegen Satz 2.3 zu einer Einbettung von $\mathbb{Q}$ nach K fortsetzen läßt.

Ergebnis: Ist K ein Körper, so treten folgende Fälle alternativ auf:

1. Es gibt genau eine Primzahl p, so daß K einen Teilkörper enthält, der isomorph zu $\mathbb{Z}_p$ ist (man nimmt dann $\mathbb{Z}_p$ als Teilkörper von K an). Es gilt für jedes $n \in \mathbb{N}$ genau dann $n \cdot 1_K = 0$, wenn p ein Teiler von n ist, und nennt p die Charakteristik von K, geschrieben $\chi(K) := p$.
2. K enthält einen Teilkörper, der isomorph zu $\mathbb{Q}$ ist (man nimmt dann $\mathbb{Q}$ als Teilkörper von K an). Es gilt dann $n \cdot 1_K \neq 0$ für alle $n \in \mathbb{N}$. In diesem Falle definiert man $\chi(K) := 0$.

3. $\mathbb{R}$ als vollständiger archimedisch geordneter Körper

Im folgenden ist R ein Integritätsbereich. Ist R ein geordneter Integritätsbereich (vergleiche Definition 1.12), dann heißt $a \in R$ positiv (negativ), wenn $0 < a$ ($a < 0$) gilt. Für jedes $a \in R, a \neq 0$ ist zum Beispiel $a^2 > 0$, denn gilt $a > 0$, so folgt $a^2 > 0 \cdot a = 0$, und ist $a < 0$, so folgt $-a > 0$, also $a^2 = (-a)^2 > 0$. Insbesondere gilt also $1 > 0$, da $1 = 1^2$. Sind nun $a_1, \ldots, a_n \in R$ von 0 verschieden, so gilt $a_i^2 > 0$ und somit $a_1^2 + \ldots + a_n^2 > 0$. Insbesondere ist also $1 + \ldots + 1 > 0$. Damit folgt einerseits, daß es genau eine lineare Ordnung von $\mathbb{Z}$ gibt, bezüglich der $\mathbb{Z}$ ein geordneter Integritätsbereich ist, und andererseits, daß jeder geordnete Körper K die Charakteristik 0 hat. Man kann also $\mathbb{Q}$ als Teilkörper von K auffassen.

Definition 3.1 *Ist R bezüglich $\leq$ ein geordneter Integritätsbereich, so heißt*

$$\mathrm{P}_{\leq} = \{a \in R \mid 0 < a\}$$

Positivbereich von R bezüglich $\leq$.

Bemerkung.

1. Ist R ein geordneter Integritätsbereich mit dem Positivbereich P und R' ein Teilring von R, so induziert die Ordnung $\leq$ von R eine Ordnung $\leq'$ von R' mit dem Positivbereich $P \cap R'$. Man sagt auch, daß $\leq$ die Ordnung $\leq'$ fortsetzt.

2. Ist $\mathrm{P}_\leq$ ein Positivbereich von R, so nennt man

$$-\mathrm{P}_\leq = \{-a \in R \mid 0 < a\} = \{a \in R \mid a < 0\}$$

   Negativbereich von R bezüglich $\leq$.

3. Wegen $$a < b \Longleftrightarrow 0 < b - a \Longleftrightarrow b - a \in \mathrm{P}_\leq$$

   ist $\leq$ eindeutig durch $\mathrm{P}_\leq$ bestimmt.

4. Ist $\mathrm{P}_\leq$ ein Positivbereich von R, so gilt

   (a) $\{0\} \cup \mathrm{P}_\leq \cup -\mathrm{P}_\leq = R$ und $\mathrm{P}_\leq \cap -\mathrm{P}_\leq = \emptyset$.

   (b) $\mathrm{P}_\leq + \mathrm{P}_\leq \subseteq \mathrm{P}_\leq$, d.h. $a + b \in \mathrm{P}_\leq$ für alle $a, b \in \mathrm{P}_\leq$.

   (c) $\mathrm{P}_\leq \cdot \mathrm{P}_\leq \subseteq \mathrm{P}_\leq$, d.h. $a \cdot b \in \mathrm{P}_\leq$ für alle $a, b \in \mathrm{P}_\leq$.

Satz 3.2 *Ist R ein Integritätsbereich und P eine Teilmenge von R mit*

1. *$\{0\} \cup P \cup -P = R$ und $P \cap -P = \emptyset$,*

2. *$P + P \subseteq P$,*

3. *$P \cdot P \subseteq P$,*

dann gibt es genau eine lineare Ordnung $\leq$ auf R, so daß R ein geordneter Integritätsbereich mit $P = \mathrm{P}_\leq$ ist.

Beweis. Die Eindeutigkeit der Ordnung ergibt sich aus Bemerkung 3. Wir definieren nun für alle $a, b \in R$

$$a < b \Longleftrightarrow b - a \in P, \quad \text{also} \quad a \leq b \Longleftrightarrow b - a \in P \cup \{0\}$$

und zeigen zunächst, daß $\leq$ auf R eine lineare Ordnung definiert. Dazu seien $a, b, c \in R$.

i) Wegen $a - a \in P \cup \{0\}$ gilt $a \leq a$.
ii) Für $a \leq b, b \leq a$ und $a \neq b$ folgt $b-a, a-b \in P$, d.h. $b-a \in P \cap -P$, also ein Widerspruch. Damit ist $a = b$, falls $a \leq b$ und $b \leq a$.
iii) Ist $a \leq b$ sowie $b \leq c$ und $a = b$ oder $b = c$, so folgt $a \leq c$ unmittelbar. Gilt aber $a < b$ und $b < c$, also $b - a, c - b \in P$, so folgt $c - a = b - a + c - b \in P$, d.h. $a < c$.
iv) Gilt $a \leq b$ nicht, so folgt $b - a \neq 0$ und $b - a \notin P$, also $b - a \in -P$, d.h. $a - b \in P$ und $b < a$.

Zu zeigen bleibt, daß $\leq$ mit der Addition und der Multiplikation verträglich ist.

v) Ist $a < b$, also $b - a \in P$, so folgt $b + c - (a + c) \in P$, d.h. $a + c < b + c$.
vi) Gilt $0 < c$ und $a < b$, so folgt $c, b - a \in P$, also $bc - ac \in P \cdot P \subseteq P$, d.h. $ac < bc$.

□

Satz 3.3 *Ist R ein geordneter Integritätsbereich mit dem Quotientenkörper K, so gibt es genau eine lineare Ordnung auf K, bezüglich der K ein geordneter Körper ist und die die Ordnung von R fortsetzt.*

Beweis. Sei R bezüglich $\leq$ ein geordneter Integritätsbereich. Wir zeigen zunächst die im Satz behauptete Eindeutigkeit. Dazu sei P ein Positivbereich von K mit $P \cap R = \mathrm{P}_{\leq}$. Für jedes $ab^{-1} \in K$ mit $a, b \in R, b \neq 0$, gilt $0 < ab^{-1}$ genau dann, wenn $0 < ab^{-1}b^2 = ab$. Damit ist P also eindeutig durch die Ordnung von R bestimmt. Zum Nachweis der Existenz definieren wir

$$P := \{ab^{-1} \mid 0 < ab\},$$

und weisen zunächst die Wohldefiniertheit nach. Sind $a, b, c, d \in R \setminus \{0\}$ mit $ab^{-1} = cd^{-1}$, so folgt $abd^2 = cdb^2$, d.h. $0 < ab$ gilt genau dann, wenn $0 < cd$. Daß nun P tatsächlich ein Positivbereich ist, weisen wir mit Hilfe von Satz 3.2 nach.

i) Sei $ab^{-1} \in K$. Ist $ab = 0$, so folgt $a = 0$ und $ab^{-1} = 0$. Gilt $ab < 0$, so folgt $-ab^{-1} \in P$, also $ab^{-1} \in -P$, und ist schließlich $0 < ab$, so gilt $ab^{-1} \in P$. Damit ist $\{0\} \cup P \cup -P = K$ gezeigt. Wäre schließlich $ab^{-1} \in P \cap -P$, so wäre $0 < ab$ und $ab < 0$. Also gilt $P \cap -P = \emptyset$.
ii) und iii) Sind ab^{-1} und cd^{-1} aus P, also $0 < ab, cd$, dann gilt $0 < abd^2, cdb^2$, also $0 < abd^2 + cdb^2$, d.h. $ab^{-1} + cd^{-1} = (ad + cb)(bd)^{-1} \in P$. Weiterhin ist $0 < abcd$, also $(ac)(bd)^{-1} = ab^{-1}cd^{-1} \in P$.

Zu zeigen bleibt schließlich, daß die durch P auf K definierte Ordnung die Ordnung $\leq$ von R fortsetzt, d.h. $P \cap R = \mathrm{P}_{\leq}$. Ist a aus $\mathrm{P}_{\leq}$, so gilt $a \in P$ wegen $a = a \cdot 1^{-1}$ und $0 < a \cdot 1$, und ist $a = a \cdot 1^{-1}$ aus $P \cap R$, so folgt $0 < a \cdot 1 = a$, also $a \in \mathrm{P}_{\leq}$.

□

Bemerkung. Da $\mathbb{Z}$ als geordneter Integritätsbereich eindeutig geordnet ist, gibt es wegen Satz 3.3 genau eine lineare Ordnung von $\mathbb{Q}$, bezüglich der $\mathbb{Q}$ ein geordneter Körper ist. Ist K ein beliebiger geordneter Körper, so können wir $\mathbb{Q}$ als Teilkörper von K auffassen, und die Ordnung von K induziert auf $\mathbb{Q}$ genau diese eindeutig bestimmte Ordnung.

Satz 3.4 *Ist K ein geordneter Körper, so sind folgende Aussagen äquivalent:*

1. *Zu jedem $a \in K$ gibt es ein $n \in \mathbb{N}$ mit $a < n$.*
2. *Zu beliebigen $a, b \in K, 0 < a$ gibt es ein $n \in \mathbb{N}$ mit $b < na$.*
3. *Zu jedem $a \in K, 0 < a$, gibt es ein $n \in \mathbb{N}$ mit $0 < \frac{1}{n} < a$.*

Bemerkung. Da K ein geordneter Körper ist, können wir $\mathbb{Q}$ als Teilkörper von K auffassen. Ist 1_K das Einselement von K, so identifizieren wir insbesondere $n \cdot 1_K$ und n für alle $n \in \mathbb{N}$, und $a < n$ bedeutet zum Beispiel $a < n \cdot 1_K$.

Beweis von Satz 3.4
″1) ⇒ 2)″: Wegen 1) gibt es ein $n \in \mathbb{N}$ mit $ba^{-1} < n$, also $b < na$.
″2) ⇒ 3)″: Wegen 2) gibt es ein $n \in \mathbb{N}$ mit $1 < na$, also $0 < \frac{1}{n} < a$.
″3) ⇒ 1)″: Ist $a \leq 0$, so gilt $a < 1$. Sei also $0 < a$. Dann gibt es wegen 3) ein $n \in \mathbb{N}$ mit $0 < \frac{1}{n} < a^{-1}$, also $a < n$.

□

Definition 3.5 *Ein geordneter Körper K heißt archimedisch geordnet, wenn eine der Aussagen aus Satz 3.4 gilt.*

Beispiel. Für jedes $q \in \mathbb{Q}, 0 < q$ mit $q = \frac{n}{m}$ und $m, n \in \mathbb{N}$ gilt $q \leq n < n + 1$, d.h., der Körper $\mathbb{Q}$ ist archimedisch geordnet. Ein Beispiel für einen geordneten Körper, der nicht archimedisch geordnet ist, findet man in Aufgabe 6.4.

Satz 3.6 *Ein geordneter Körper K ist genau dann archimedisch geordnet, wenn es zu beliebigen $a, b \in K$ mit $1 < a$ ein $n \in \mathbb{N}$ mit $b < a^n$ gibt.*

Beweis. Ist K archimedisch geordnet und sind $a, b \in K$ mit $1 < a$, so gibt es ein $n \in \mathbb{N}$ mit $b - 1 < n(a - 1)$, da $0 < a - 1$. Es folgt $b < 1 + n(a - 1) \leq (1 + (a - 1))^n = a^n$. Ist andererseits $a \in K$ gegeben, so gibt es ein $m \in \mathbb{N}$ mit $a < 2^m$. Für $n = 2^m$ folgt $a < n$, also die Behauptung.

□

Definition 3.7 *Ist K ein geordneter Körper und $a \in K$, so heißt*

$$|a| := \max\{a, -a\}$$

Betrag von a.

Einfache Eigenschaften. Für alle $a, b \in K$ gilt:

1. $|a| = |-a| \geq 0$, und $|a| = 0$ gilt genau dann, wenn $a = 0$.
2. $|a \cdot b| = |a| \cdot |b|$.
3. $|a + b| \leq |a| + |b|$ (Dreiecksungleichung).

   Beweis. O.B.d.A. sei $a \leq b$. Da die Fälle $a \leq b \leq 0$ und $0 \leq a \leq b$ trivial sind, nehmen wir weiterhin $a < 0 < b$ an. Gilt $|a| \leq |b|$, also $-a \leq b$, so folgt $|a + b| = a + b \leq -a + b = |a| + |b|$. Gilt $|b| \leq |a|$, also $b \leq -a$, so folgt $|a+b| = -b-a \leq b-a = |b|+|a|$.
4. $||a| - |b|| \leq |a - b|$.
   Beweis. Wegen der Dreiecksungleichung gilt $|a| = |(a-b)+b| \leq |a-b|+|b|$, also $|a|-|b| \leq |a-b|$. Analog folgt $|b|-|a| \leq |a-b|$, also $||a|-|b|| = \max\{|a|-|b|, |b|-|a|\} \leq |a-b|$.

Im folgenden ist K ein geordneter Körper und $''\epsilon > 0''$ soll stets $''\epsilon \in K$ und $\epsilon > 0''$ bedeuten.

Eine Folge (a_n) aus K heißt ...

1. ... beschränkt, wenn es ein $s \in K$ gibt, so daß $|a_n| < s$ für alle $n \in \mathbb{N}$ gilt.
2. ... konvergent in K, wenn es ein $a \in K$ gibt, so daß für alle $\epsilon > 0$ ein $n_0 \in \mathbb{N}$ existiert mit

   $$|a - a_n| < \epsilon$$

   für alle $n \geq n_0$. Man nennt a dann Grenzwert der Folge (a_n).

3. ... Cauchy-Folge, wenn es für alle $\epsilon > 0$ ein $n_0 \in \mathbb{N}$ gibt, so daß

$$|a_n - a_m| < \epsilon$$

für alle $n, m \geq n_0$ gilt.

Bemerkung. Ist K archimedisch geordnet, so kann "Für alle $\epsilon > 0$" stets ersetzt werden durch "Für alle $\epsilon \in \mathbb{Q}, \epsilon > 0$".

Einfache Eigenschaften.

A) Eine konvergente Folge (a_n) hat genau einen Grenzwert a; man schreibt $\lim a_n = a$. Gilt $\lim a_n = 0$, so heißt (a_n) Nullfolge.

B) Sind (a_n) und (b_n) konvergent in K, so auch $(a_n \pm b_n), (a_n \cdot b_n)$ und $(|a_n|)$. Dabei gilt

$$\begin{aligned} \lim(a_n \pm b_n) &= \lim a_n \pm \lim b_n. \\ \lim(a_n \cdot b_n) &= \lim a_n \cdot \lim b_n. \\ \lim |a_n| &= |\lim a_n|. \end{aligned}$$

Die letzte Behauptung folgt wegen $||a| - |a_n|| \leq |a - a_n|$ mit $a = \lim a_n$.

C) Jede konvergente Folge ist eine Cauchy-Folge, die Umkehrung gilt i.a. nicht.

D) Jede Cauchy-Folge ist beschränkt.
Beweis. Sei (a_n) eine Cauchy-Folge. Dann gibt es ein $n_0 \in \mathbb{N}$ mit $|a_n - a_m| < 1$ für alle $n, m \geq n_0$. Definieren wir $s := \max\{|a_1|, \ldots, |a_{n_0}|\} + 1$, so gilt offenbar $|a_n| < s$ für alle $n \leq n_0$, und für $n_0 < n$ ist wegen $|a_n - a_{n_0}| < 1$

$$|a_n| = |a_{n_0} + (a_n - a_{n_0})| \leq |a_{n_0}| + |a_n - a_{n_0}| < |a_{n_0}| + 1 \leq s.$$

E) Sind (a_n) und (b_n) Cauchy-Folgen in K, so auch $(a_n \pm b_n), (a_n \cdot b_n)$ und $(|a_n|)$.

Definition 3.8 *Ein geordneter Körper heißt vollständig, wenn jede Cauchy-Folge in ihm konvergiert.*

Im folgenden ist K ein archimedisch geordneter Körper und $\mathcal{C}$ die Menge aller Cauchy-Folgen aus K. Für alle $(a_n), (b_n) \in \mathcal{C}$ definieren wir

$$(a_n) + (b_n) := (a_n + b_n) \text{ sowie } (a_n) \cdot (b_n) := (a_n \cdot b_n),$$

und es gilt $(a_n) + (b_n), (a_n) \cdot (b_n) \in \mathcal{C}$. Man zeigt leicht, daß $\mathcal{C}$ bzgl. dieser Addition und Multiplikation ein kommutativer Ring mit dem Einselement $(1, 1, 1, \ldots)$ ist. Sei nun weiterhin $\mathcal{N}$ die Menge aller Nullfolgen aus K.

I. $\mathcal{N}$ ist ein Ideal in $\mathcal{C}$.
Beweis. Da jede konvergente Folge eine Cauchy-Folge ist, gilt $\mathcal{N} \subseteq \mathcal{C}$, und wegen $(0, 0, 0, \ldots) \in \mathcal{N}$ ist $\mathcal{N}$ nicht leer. Seien nun $(a_n), (b_n) \in \mathcal{N}$ und $(c_n) \in \mathcal{C}$. Wegen $\lim(a_n - b_n) = \lim a_n - \lim b_n = 0$ folgt $(a_n) - (b_n) \in \mathcal{N}$. Zu zeigen bleibt noch $(a_n) \cdot (c_n) \in \mathcal{N}$. Dazu sei $\epsilon > 0$. Da (c_n) als Cauchy-Folge beschränkt ist, gibt es ein

$s \in K$ mit $|c_n| < s$ für alle $n \in \mathbb{N}$, und da (a_n) eine Nullfolge ist, gibt es ein $n_0 \in \mathbb{N}$ mit

$$|a_n| < \frac{\epsilon}{s} \text{ für alle } n \geq n_0.$$

Somit folgt $|a_n \cdot c_n| = |a_n| \cdot |c_n| < \frac{\epsilon}{s} \cdot s = \epsilon$ für alle $n \geq n_0$.

□

Der Faktorring $\mathcal{K} := \mathcal{C}/\mathcal{N}$ ist ein kommutativer Ring mit 1.

II. $\mathcal{K}$ ist ein Körper.
Beweis. Ist $\overline{(a_n)}$ aus $\mathcal{K}$ und $\overline{(a_n)} \neq 0$, dann ist (a_n) keine Nullfolge, und wegen Aufgabe 6.1 gibt es ein $n_0 \in \mathbb{N}$ und ein $\mu > 0$ mit $|a_n| > \mu$ für alle $n \geq n_0$. Definieren wir die Folge (b_n) durch

$$b_1 = \ldots = b_{n_0} = \mu \text{ und } b_n = a_n \text{ für } n > n_0,$$

so ist (b_n) eine Cauchy-Folge, d.h. $(b_n) \in \mathcal{C}$, mit $\overline{(a_n)} = \overline{(b_n)}$ und

$$|b_n| \geq \mu > 0 \text{ für alle } n \in \mathbb{N}.$$

Wir zeigen nun, daß (b_n^{-1}) ein Cauchy-Folge ist. Dazu sei $\epsilon > 0$ gegeben. Weil (b_n) eine Cauchy-Folge ist, gibt es ein $k \in \mathbb{N}$ mit

$$|b_n - b_m| < \epsilon \cdot \mu^2 \text{ für alle } n, m \geq k,$$

also

$$|b_n^{-1} - b_m^{-1}| = |b_n - b_m||b_n b_m|^{-1} < \epsilon \cdot \mu^2 \mu^{-2} = \epsilon.$$

Da $\overline{(a_n)} \cdot \overline{(b_n^{-1})} = \overline{(b_n)} \cdot \overline{(b_n^{-1})} = \overline{(1, 1, 1, \ldots)} = 1$, ist $\overline{(a_n)}$ in $\mathcal{K}$ bzgl. der Multiplikation invertierbar.

□

Wegen $1 = \overline{(1, 1, 1 \ldots)}$ setzen wir

$$n := \overline{(n, n, n, \ldots)}$$

für jedes $n \in \mathbb{N}$ und für jedes $q \in \mathbb{Q}$ damit

$$q := \overline{(q, q, q, \ldots)}.$$

Auf diese Weise können wir $\mathbb{Q}$ als Teilkörper von $\mathcal{K}$ auffassen.

III. Die Menge $P := \{\overline{(a_n)} \mid$ Es gibt ein $\epsilon > 0$ und ein $n_0 \in \mathbb{N}$ mit $a_n \geq \epsilon$ für alle $n \geq n_0\}$ ist ein Positivbereich von $\mathcal{K}$.
Beweis. Zunächst zeigen wir, daß P wohldefiniert ist. Dazu sei $\overline{(a_n)} = \overline{(b_n)}$ und $a_n \geq \epsilon > 0$ für alle $n \geq n_0$. Da $(b_n - a_n)$ eine Nullfolge ist, kann man sogar

$$|b_n - a_n| < \frac{\epsilon}{2} \text{ für alle } n \geq n_0$$

annehmen. Es folgt $-\frac{\epsilon}{2} < b_n - a_n$, also

$$\frac{\epsilon}{2} = \epsilon - \frac{\epsilon}{2} \leq a_n - \frac{\epsilon}{2} < a_n + b_n - a_n = b_n$$

für alle $n \geq n_0$. Daß P tatsächlich ein Positivbereich von $\mathcal{K}$ ist, zeigen wir mit Hilfe von Satz 3.2. Wegen Aufgabe 6.1 gilt $\overline{(a_n)} \in P$ oder $-\overline{(a_n)} \in P$ für alle $\overline{(a_n)} \in \mathcal{K}$, $\overline{(a_n)} \neq 0$, d.h. $\{0\} \cup P \cup -P = \mathcal{K}$. Die übrigen Eigenschaften $P \cap -P = \emptyset, P + P \subseteq P$ und $P \cdot P \subseteq P$ folgen unmittelbar.

□

Somit ist $\mathcal{K}$ bzgl.

$$\overline{(a_n)} < \overline{(b_n)} \iff \overline{(b_n)} - \overline{(a_n)} \in P$$

ein geordneter Körper. Insbesondere gilt $\overline{(a_n)} \leq \overline{(b_n)}$ für $\overline{(a_n)}, \overline{(b_n)} \in \mathcal{K}$ falls $a_n \leq b_n$ für alle $n \geq n_0, n_0 \in \mathbb{N}$.

IV. $\mathcal{K}$ ist archimedisch geordnet.
Beweis. Sei $\overline{(a_n)} \in \mathcal{K}$, also (a_n) eine Cauchy-Folge. Dann gibt es ein $s \in K$ mit $a_n < s$ für alle $n \in \mathbb{N}$. Da K archimedisch geordnet ist, gibt es ein $k \in \mathbb{N}$ mit $s < k$, also $a_n < k$ für alle $n \in \mathbb{N}$. Es folgt $\overline{(a_n)} \leq \overline{(k, k, k, \ldots)} = k < k + 1$.

□

V. $\mathcal{K}$ ist vollständig.
Beweis. Sei $(x_1, x_2, \ldots)$ eine Cauchy-Folge aus $\mathcal{K}$. Wegen Aufgabe 6.2 gibt es zu jedem $n \in \mathbb{N}$ ein $q_n \in \mathbb{Q}$ mit

$$|x_n - q_n| < \frac{1}{n}.$$

Wir zeigen zunächst, daß (q_n) eine Cauchy-Folge in K ist. Sei $\epsilon > 0, \epsilon \in \mathbb{Q}$. Dann gibt es ein $n_0 \in \mathbb{N}$ mit $\frac{1}{n_0} < \frac{\epsilon}{3}$ und $|x_n - x_m| < \frac{\epsilon}{3}$ für alle $n, m \geq n_0$. Es folgt

$$|q_n - q_m| \leq |q_n - x_n| + |x_n - x_m| + |x_m - q_m| < \frac{1}{n} + \frac{\epsilon}{3} + \frac{1}{m} < \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon$$

für alle $n, m \geq n_0$.

Damit gilt $(q_k) \in \mathcal{C}$, also $\overline{(q_k)} \in \mathcal{K}$, und wir beweisen $\lim x_k = \overline{(q_k)}$. Sei $\epsilon \in \mathbb{Q}, \epsilon > 0$. Dann gibt es ein $n_0 \in \mathbb{N}$ mit $\frac{1}{n_0} < \frac{\epsilon}{2}$ und $|q_m - q_n| < \frac{\epsilon}{2}$ für alle $n, m \geq n_0$, also

$$\begin{gathered} -\frac{\epsilon}{2} < q_m - q_n < \frac{\epsilon}{2}, \quad \text{d.h.} \\ -\frac{\epsilon}{2} \leq \overline{(q_k)} - q_n \leq \frac{\epsilon}{2} \text{ und damit} \\ |x_n - \overline{(q_k)}| \leq |x_n - q_n| + |q_n - \overline{(q_k)}| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \end{gathered}$$

für alle $n \geq n_0$.

□

Satz 3.9 *Bis auf Isomorphie gibt es genau einen vollständigen archimedisch geordneten Körper.*

Beweis. Wir betrachten den archimedisch geordneten Körper $K = \mathbb{Q}$ und wählen die Bezeichnungen wie in den vorangegangenen Überlegungen, d.h., $\mathcal{C}$ ist der Ring aller Cauchy-Folgen und $\mathcal{N}$ das Ideal aller Nullfolgen aus K. Dann ist $\mathcal{K} := \mathcal{C}/\mathcal{N}$ ein vollständiger archimedisch geordneter Körper. Ist nun F ebenfalls ein vollständiger archimedisch geordneter Körper, dann ist $\mathbb{Q}$ ein Teilkörper von F, und jedes $x \in F$ ist Grenzwert einer Folge aus $\mathbb{Q}$, denn wegen Aufgabe 6.2 gibt es zu jedem $n \in \mathbb{N}$ ein $q_n \in \mathbb{Q}$ mit $|x - q_n| < \frac{1}{n}$, also $\lim q_n = x$. Wir zeigen nun, daß F und $\mathcal{K}$ isomorph sind. Ist (q_n) eine Cauchy-Folge aus $\mathbb{Q}$, d.h. $(q_n) \in \mathcal{C}$, dann ist (q_n) wegen der Eindeutigkeit der Ordnung von $\mathbb{Q}$ auch eine Cauchy-Folge in F und konvergiert damit in F. Die Abbildung

$$\varphi : \mathcal{C} \longrightarrow F, (q_n) \longmapsto \lim q_n$$

ist offenbar ein Ringhomomorphismus mit $\text{Kern}\varphi = \{(q_n) \mid \lim q_n = 0\} = \mathcal{N}$. Da jedes x aus F Grenzwert einer Folge aus $\mathbb{Q}$ ist (s.o.), ist φ sogar surjektiv. Wegen des Homomorphiesatzes für Ringe folgt

$$\mathcal{K} = \mathcal{C}/\mathcal{N} \cong F.$$

□

Definition 3.10 *Den bis auf Isomorphie eindeutig bestimmten vollständigen archimedisch geordneten Körper bezeichnet man mit $\mathbb{R}$. Die Elemente von $\mathbb{R}$ heißen reelle Zahlen.*

Bemerkung. Der Körper $\mathbb{R}$ der reellen Zahlen hat folgende Eigenschaften:

R1) $\mathbb{Q}$ ist Teilkörper von $\mathbb{R}$.

R2) $\mathbb{R}$ ist vollständig.

R3) Jedes Element von $\mathbb{R}$ ist Grenzwert einer Folge aus $\mathbb{Q}$.

Aus diesem Grund heißt $\mathbb{R}$ auch Komplettierung (Vervollständigung, vollständige Hülle) des Körpers $\mathbb{Q}$.

Weitere Eigenschaften von $\mathbb{R}$.

R4) Für alle $x \in \mathbb{R}$ gilt: $x \geq 0 \iff x$ ist in $\mathbb{R}$ ein Quadrat.
Ist x ein Quadrat, so wurde $x \geq 0$ bereits für beliebige geordnete Körper gezeigt. Sei nun andererseits $x \geq 0$. Dann definieren wir eine Folge (a_n) rekursiv durch

$$a_1 := 1 \text{ und } a_{n+1} := \frac{1}{2}(a_n + \frac{x}{a_n}) \text{ für } n \geq 1.$$

Wegen $x \geq 0$ gilt $a_n > 0$ für alle $n \in \mathbb{N}$. Wir zeigen, daß (a_n) ab dem zweiten Folgeglied monoton fallend ist:

$$\begin{aligned} a_n - a_{n+1} &= a_n - \frac{1}{2}(a_n + \frac{x}{a_n}) = \frac{1}{2a_n}(a_n^2 - x) \\ &\overset{n\geq 1}{=} \frac{1}{2a_n}(\frac{1}{4}(a_{n-1} + \frac{x}{a_{n-1}})^2 - x) = \frac{1}{8a_n}(a_{n-1} - \frac{x}{a_{n-1}})^2 \geq 0. \end{aligned}$$

Wegen Aufgabe 6.5 existiert $a := \lim a_n$ mit $a^2 = \frac{1}{2}(a^2 + x)$, also $a^2 = x$.

Definition 3.11 *Sind K_1 und K_2 zwei geordnete Körper mit den Ordnungen $<_1$ und $<_2$, so heißt $\varphi : K_1 \longrightarrow K_2$ ordnungstreu, wenn für alle $x, y \in K_1$ gilt:*

$$x <_1 y \iff \varphi(x) <_2 \varphi(y).$$

Wegen R4) folgt nun:

R5) Sind K_1 und K_2 zwei vollständige archimedisch geordnete Körper, so ist jeder Isomorphismus $\varphi : K_1 \longrightarrow K_2$ ordnungstreu.

Anwendungen.

1. Ist K ein Körper und $\varphi : K \longrightarrow \mathbb{R}$ ein (injektiver) Ringhomomorphismus, dann ist K bezüglich

   $$x < y \ :\iff \ \varphi(x) < \varphi(y)$$

   ein archimedisch geordneter Körper, wie man sich leicht überlegt. Es gilt nun auch, daß man auf diese Weise alle archimedischen Ordnungen von K erhält, so daß K ein geordneter Körper ist. Um das einzusehen sei also K ein archimedisch geordneter Körper und

   $$\psi : K \longrightarrow \mathcal{K} := \mathcal{C}/\mathcal{N}, \ k \longmapsto \overline{(k, k, k, \ldots)},$$

   wobei wir die Bezeichnungen von oben benutzen. $\mathcal{K}$ ist ein vollständiger archimedisch geordneter Körper und ψ ein ordnungstreuer (injektiver) Ringhomomorphismus. Wegen Satz 3.9 gibt es einen Isomorphismus $\rho : \mathcal{K} \longrightarrow \mathbb{R}$, der wegen R5) ordnungstreu ist. Dann ist $\varphi = \rho \circ \psi : K \longrightarrow \mathbb{R}$ ein (injektiver) Ringhomomorphismus mit

   $$x < y \quad \iff \quad \varphi(x) < \varphi(y).$$

2. Ist $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ ein Automorphismus, so gilt $\varphi = \mathrm{id}$, d.h., $\mathbb{R}$ hat nur den trivialen Automorphismus. Um das zu beweisen sei $x \in \mathbb{R}$ und $\varphi(x) \neq x$, z. B. $x < \varphi(x) =: y$. Dann gibt es ein $q \in \mathbb{Q}$ mit $x < q < y$, denn es gibt ein $n \in \mathbb{N}$ mit $1 < n(y-x) = ny - nx$, also ein $m \in \mathbb{Z}$ mit $nx < m < ny$, d.h. $x < \frac{m}{n} < y$. Wegen $\varphi(q) = q$ folgt der Widerspruch $\varphi(q) < \varphi(x)$.

   Dieses Resultat kann zum Beispiel folgendermaßen in der analytischen Geometrie benutzt werden. Der Hauptsatz der affinen Geometrie besagt: *Ist K ein Körper mit mindestens drei Elementen und $\mathfrak{A}$ ein mindestens 2-dimensionaler affiner Raum über K, so ist jede Kollineation $\varphi : \mathfrak{A} \longrightarrow \mathfrak{A}$ eine Semiaffinität.* Da jede Semiaffinität von $\mathfrak{A}$ eine Affinität ist, wenn K nur den trivialen Automorphismus hat, liefert obiger Hauptsatz:

   Jede Kollineation eines reellen affinen Raums der Dimension ≥ 2 ist eine Affinität.

4. Darstellungen reeller Zahlen

Im folgenden ist g eine natürliche Zahl mit $g \geq 2$ und $S_g := \{0, 1, \ldots, g-1\}$. Ist (c_n) eine Folge von Zahlen aus S_g, dann konvergiert die Reihe

$$\sum_{i=1}^{\infty} c_i g^{-i} = c_1 g^{-1} + c_2 g^{-2} + c_3 g^{-3} + \ldots$$

wegen

$$\sum_{i=1}^{\infty} c_i g^{-i} \leq (g-1) \sum_{i=1}^{\infty} g^{-i} = (g-1) g^{-1} \frac{1}{1 - \frac{1}{g}} = 1.$$

Gilt weiterhin $c_i \neq g-1$ für mindestens ein i, so folgt

$$\sum_{i=1}^{\infty} c_i g^{-i} \in [0,1) := \{x \in \mathbb{R} \mid 0 \leq x < 1\}.$$

Satz 4.1 *Jedes $x \in [0,1)$ hat genau eine Darstellung*

$$x = \sum_{i=1}^{\infty} c_i g^{-i}$$

mit $c_i \in S_g$ für alle $i \in \mathbb{N}$ und $c_i \neq g-1$ für unendlich viele $i \in \mathbb{N}$. Definiert man rekursiv

$$x_1 := x \quad \textit{und} \quad x_{i+1} := \{x_i g\} \quad \textit{für} \quad i \in \mathbb{N},$$

so folgt $c_i = [x_i g]$.

Bemerkung.

1. Für $x \in \mathbb{R}$ ist $[x]$ die größte ganze Zahl z mit $z \leq x$ und $\{x\} := x - [x] \in [0,1)$. Dabei heißt $[x]$ ganzer Teil von x und $\{x\}$ gebrochener Teil von x. Da $\mathbb{R}$ archimedisch geordnet ist, existiert $[x]$ für alle $x \in \mathbb{R}$.

2. Betrachtet man das aus der Schule bekannte Verfahren zur Umwandlung eines Bruches in eine Dezimalzahl, so stellt man schnell fest, daß der dort verwendete Algorithmus zur Berechnung der einzelnen Ziffern eine praktische Umsetzung der in Satz 4.1 angegebenen Methode zur Berechnung der einzelnen c_i ist.

Beweis von Satz 4.1. Wegen $x_i \in [0,1)$ gilt $x_i g \in [0, g)$, also

$$d_i := [x_i g] \in S_g \quad \text{für alle } i \in \mathbb{N}.$$

Für alle $j \in \mathbb{N}$ folgt $x_{j+1} = x_j g - d_j$, also

$$x_j = d_j g^{-1} + x_{j+1} g^{-1}.$$

Mit Hilfe der vollständigen Induktion beweist man leicht, daß

$$x_j = \sum_{i=j}^{j+k-1} d_i g^{j-1-i} + x_{j+k} g^{-k}$$

für alle $k \in \mathbb{N}$ gilt. Wegen $\lim_{k\to\infty} x_{j+k} g^{-k} = 0$ folgt speziell für $j = 1$

$$x = x_1 = \sum_{i=1}^{\infty} d_i g^{-i}.$$

Wir zeigen nun durch einen Widerspruchsbeweis, daß es unendlich viele $j \in \mathbb{N}$ mit $d_j \neq g-1$ gibt, und nehmen also an, daß $d_j \neq g-1$ nur für endlich viele $j \in \mathbb{N}$ gilt. Dann existiert ein $j \in \mathbb{N}$ mit

$$d_j = d_{j+1} = \ldots = g-1,$$

d.h., es gilt

$$x_j = \sum_{i=j}^{j+k-1} (g-1) g^{j-1-i} + x_{j+k} g^{-k}$$

für alle $k \geq 1$. Für $k \to \infty$ konvergiert die rechte Seite der Gleichung gegen

$$(g-1) \cdot g^{-1} \cdot \frac{1}{1-g^{-1}} = 1$$

im Widerspruch zu $x_j \in [0,1)$, d.h., es gibt tatsächlich unendlich viele $j \in \mathbb{N}$ mit $d_j \neq g-1$. Zu zeigen bleibt der Nachweis der Eindeutigkeit. Sei $x = \sum_{i=1}^{\infty} c_i g^{-i}$ mit $c_i \in S_g$ und $c_i \neq g-1$ für unendlich viele Indizes i. Wir nehmen an, daß es einen Index j mit $c_j \neq d_j$ gibt, und o.B.d.A. sei j mit dieser Eigenschaft minimal. Dann folgt

$$\begin{aligned} 1 &\leq |d_j - c_j| = |\sum_{i>j} (c_i - d_i) g^{j-i}| \\ &\leq \sum_{i>j} |c_i - d_i| g^{j-i} \\ &\leq (g-1) \sum_{t\geq 1} g^{-t} = 1. \end{aligned}$$

Also gilt $|c_i - d_i| = g-1$ für alle $i > j$, und entweder sind alle $c_i - d_i$ positiv oder alle negativ für $i > j$. Im 1. Fall folgt $c_i = g-1$ für alle $i > j$ und im 2. Fall $d_i = g-1$ für alle $i > j$, also ein Widerspruch.

□

Satz 4.1 läßt sich nun leicht zu folgendem Satz verallgemeinern.

Satz 4.2 *Jedes $x \in \mathbb{R}, x \geq 0$ hat eine Darstellung*

$$x = \sum_{i=-k}^{\infty} c_i g^{-i}$$

mit $k \in \mathbb{Z}, c_i \in S_g$ und $c_j \neq g-1$ für unendlich viele Indizes j. Ist $x \neq 0$ und $c_{-k} \neq 0$, so ist die Darstellung eindeutig.

Bemerkung. Die eindeutige Darstellung von $x \in \mathbb{R}, x > 0$ aus Satz 4.2 heißt g-adische Entwicklung oder g-adische Darstellung (bzw. Dezimalbruchentwicklung oder Dezimaldarstellung falls $g = 10$) von x. Die c_i heißen ($g-$) Ziffern von x. Für $k \geq 0$ schreibt man

$$x = c_{-k} \dots c_{-1} c_0, c_1 c_2 c_3 \dots .$$

Für $k < 0$, also $l := -k > 0$, schreibt man

$$x = 0, 0 \dots 0 c_l c_{l+1} \dots .$$

Die g-adische Darstellung heißt ...

... abbrechend, falls höchstens endlich viele Ziffern ungleich 0 sind.

... periodisch, falls es ein $l \in \mathbb{N}_0$ und ein $p \in \mathbb{N}$ gibt, so daß $c_{i+p} = c_i$ für alle $i > l$ gilt. Sind l und p minimal, so heißt l Vorperiodenlänge und p Periodenlänge der Darstellung. Die Darstellung heißt reinperiodisch, falls $l = 0$, sonst gemischtperiodisch. Man schreibt

$$x = \dots, \underbrace{c_1 c_2 \dots c_l}_{\text{Vorperiode}} \underbrace{\overline{c_{l+1} \dots c_{l+p}}}_{\text{Periode}}.$$

Ist die g-adische Darstellung von x periodisch, dann folgt mit obiger Bezeichnung:

$$\begin{aligned}
\{x\} &= c_1 g^{-1} + \dots + c_l g^{-l} + c_{l+1} g^{-(l+1)} + \dots + c_{l+p} g^{-(l+p)} \\
&\qquad + c_{l+1} g^{-(l+1+p)} + \dots + c_{l+p} g^{-(l+2p)} + \dots \\
&= \sum_{i=1}^{l} c_i g^{-i} + g^{-l} \Big(\sum_{k=1}^{p} c_{l+k} g^{-k}\Big) \underbrace{(1 + g^{-p} + g^{-2p} + \dots)}_{\frac{1}{1-g^{-p}}} \\
&= \frac{1}{g^l (g^p - 1)} [(g^p - 1) \sum_{i=1}^{l} c_i g^{l-i} + \sum_{k=1}^{p} c_{l+k} g^{p-k}].
\end{aligned}$$

Damit haben wir folgenden Satz bewiesen.

Satz 4.3 *Ist die g-adische Entwicklung von $x \in \mathbb{R}, x \geq 0$ periodisch, so ist x rational.*

Beispiel. Wir wählen $g = 10$ und betrachten $x = 0,12456\ \overline{2314}$. Dann gilt $l = 5$ und $p = 4$. Obige Formel liefert

$$x = \frac{(10^4 - 1)12456 \ + \ 2314}{10^5 (10^4 - 1)} = \frac{124549858}{999900000}.$$

Wie bereits aus dem Beweis von Satz 4.3 zu entnehmen ist, entspricht dabei die Ziffernfolge von 12456 gerade der Ziffernfolge der Vorperiode und die Ziffernfolge von 2314 der Ziffernfolge der Periode.

Als nächstes soll gezeigt werden, daß umgekehrt die g-adische Darstellung einer positiven rationalen Zahl x periodisch ist. Wir wollen weiterhin untersuchen, wie sich die Vorperioden- und die Periodenlänge von x berechnen lassen, auch wenn die g-adische Darstellung explizit nicht bekannt ist. Sei also $x = \frac{a}{b}$ mit $a, b \in \mathbb{N}$, wobei wir a und b als teilerfremd annehmen können. Dann existieren $q \in \mathbb{N}_0$ und $r \in \{0, \ldots, b-1\}$ mit $a = q \cdot b + r$, also

$$\frac{a}{b} = q + \frac{r}{b}, \quad \text{d.h} \quad \{\frac{a}{b}\} = \frac{r}{b}.$$

Wir benutzen die Bezeichnungen aus Satz 4.1, d.h.

$$x_1 := \{\frac{a}{b}\},\ x_{i+1} := \{gx_i\},\ c_i := [gx_i]$$

für $i \in \mathbb{N}$, und setzen $b_i := x_i \cdot b$. Dann gilt $b_i \in \{0, \ldots, b-1\}$, und damit existieren $s, t \in \mathbb{N}, 1 \leq s < t$ mit $b_s = b_t$, also $x_s = x_t$ und $x_{s+i} = x_{t+i}$ sowie $c_{s+i} = c_{t+i}$ für alle $i \geq 0$. Damit ist die g-adische Entwicklung von $\frac{a}{b}$ periodisch. Sei nun l die zugehörige Vorperiodenlänge und p die Periodenlänge. Dann gilt

$$\frac{a}{b} = \frac{B}{g^l(g^p - 1)} \quad \text{für ein } B \in \mathbb{N},$$

wie man dem Beweis von Satz 4.3 entnehmen kann. Da a und b teilerfremd sind, ist b ein Teiler von $g^l(g^p - 1)$. Wir setzen

$$b^* := \max\{m \in \mathbb{N} \mid m \text{ teilt } b \text{ und } g, m \text{ sind teilerfremd}\} \ \text{ sowie } \ b^{**} := \frac{b}{b^*}.$$

Dann ist b^* ein Teiler von $g^p - 1$, d.h. $g^p \equiv 1 \bmod b^*$, und b^{**} ein Teiler von g^l. Wir definieren nun

$$q := \min\{s \in \mathbb{N} \mid g^s \equiv 1 \bmod b^*\} \quad \text{und} \quad m := \min\{s \in \mathbb{N}_0 \mid b^{**} \text{ teilt } g^s\}$$

und zeigen $p = q$ sowie $l = m$, wobei $q \leq p$ und $m \leq l$ offenbar gelten. Zu beweisen bleibt $q \geq p$ und $m \geq l$. Da b^* ein Teiler von $g^q - 1$ und b^{**} ein Teiler von g^m ist, ist b ein Teiler von $g^m(g^q - 1)$, also

$$\{\frac{a}{b}\} g^m (g^q - 1) \in \mathbb{N}_0.$$

Es existieren nun $u, v \in \mathbb{N}_0$ mit

$$\{\frac{a}{b}\} g^m (g^q - 1) = u \cdot (g^q - 1) + v \quad \text{und} \quad 0 \leq v < g^q - 1,$$

also $0 \leq u < g^m$. Wegen Satz 4.2 lassen sich u und v eindeutig in der Form

$$u = u_1 g^{m-1} + \ldots + u_{m-1} g + u_m,$$
$$v = v_1 g^{q-1} + \ldots + v_{q-1} g + v_q$$

mit $u_i, v_i \in S_g$ und $v_k \neq g-1$ für mindestens ein k schreiben, wobei sich die letzte Behauptung wegen $v < g^q - 1$ ergibt. Es folgt

$$\begin{aligned}\{\frac{a}{b}\} &= ug^{-m} + v\,\frac{g^{-(m+q)}}{1-g^{-q}} \\ &= \sum_{i=1}^{m} u_i g^{-i} + g^{-m}(\sum_{j=1}^{q} v_j g^{-j})(\sum_{k=0}^{\infty} g^{-kq}) \\ &= \sum_{i=1}^{\infty} d_i g^{-i}.\end{aligned}$$

Dabei gilt

$$\begin{aligned} d_1 &= u_1, \ \ldots\ , d_m = u_m, \\ d_{m+1} &= v_1, \ \ldots\ , d_{m+q} = v_q \\ &\vdots \\ d_{m+kq+1} &= v_1, \ \ldots\ , d_{m+kq+q} = v_q \quad \text{für } k \in \mathbb{N}. \end{aligned}$$

Wegen $d_i \in S_g$ für alle i und $d_i \neq g-1$ für unendlich viele i ist damit

$$\{\frac{a}{b}\} = \sum_{i=1}^{\infty} d_i g^{-i}$$

die g-adische Entwicklung von $\{\frac{a}{b}\}$. Für die Vorperiodenlänge l gilt somit $l \leq m$, und für die Periodenlänge p gilt $p \leq q$. Insgesamt ist also $l = m$ und $p = q$.

Offenbar ist die g-adische Entwicklung von $\{\frac{a}{b}\}$ genau dann abbrechend, wenn $v = 0$, d.h. wenn $\{\frac{a}{b}\}g^m \in \mathbb{N}_0$. Damit ist die g-adische Entwicklung genau dann abbrechend, wenn b ein Teiler von g^m ist, d.h. wenn $b^* = 1$.

Insgesamt haben wir also folgenden Satz bewiesen.

Satz 4.4 *Sei $g \in \mathbb{N}, g \geq 2$ und seien $a, b \in \mathbb{N}$ teilerfremd. Ist $b^* \in \mathbb{N}$ der größte Teiler von b, der zu g teilerfremd ist, sowie $b^{**} = \frac{b}{b^*}$, dann gilt: Die g-adische Entwicklung von $\frac{a}{b}$ ist periodisch. Die Periodenlänge ist die Ordnung von g modulo b^*, und $\min\{s \in \mathbb{N}_0 \mid b^{**}$ teilt $g^s\}$ ist die Vorperiodenlänge. Die Entwicklung ist abbrechend genau dann, wenn $b^* = 1$, d.h., wenn jeder Primteiler von b auch g teilt.*

Bemerkung.

1. Sind $a, b \in \mathbb{N}$ teilerfremd, so hängt die Periodenlänge der g-adischen Entwicklung nur von b und g ab.

2. Wegen der Sätze 4.3 und 4.4 ist die g-adische Entwicklung einer positiven reellen Zahl x genau dann periodisch, wenn $x \in \mathbb{Q}$.

Beispiel. Wir wählen $g = 7$ und untersuchen die 7-adische Entwicklung von $\frac{1}{5}$, also $a = 1$ und $b = 5$. Da 5 und 7 teilerfremd sind, gilt $b^* = 5$ und $b^{**} = 1$. Damit hat die

7-adische Darstellung von $\frac{1}{5}$ die Vorperiodenlänge 0, d.h., die Darstellung ist reinperiodisch. Zur Berechnung der Periodenlänge ermitteln wir die Ordnung von $\overline{7}$ in $\mathbb{Z}_5$. Es gilt

$$\overline{7} = \overline{2},\ \overline{7}^2 = \overline{4},\ \overline{7}^3 = \overline{3},\ \overline{7}^4 = \overline{1}.$$

Damit ist 4 die Ordnung von 7 modulo 5. Die 7-adische Entwicklung von $\frac{1}{5}$ ergibt sich gemäß Satz 4.1:

$$\frac{1}{5} = 0,\overline{1254}.$$

Bemerkung. Die Periodenlänge ist stets ein Teiler von $\varphi(b^*)$. Sie ist gleich $\varphi(b^*)$ genau dann, wenn $\varphi(b^*)$ die Ordnung von g mod b^* ist, d.h., wenn $\mathrm{E}(\mathbb{Z}_{b^*})$ zyklisch ist und $\mathrm{E}(\mathbb{Z}_{b^*}) = \langle\overline{g}\rangle$. Man nennt g dann Primitivwurzel modulo b^*.

Sind speziell b und g teilerfremd, dann gilt $b^* = b$ und $b^{**} = 1$. Die g-adische Entwicklung von $\frac{a}{b}$ ($a \in \mathbb{N}$) ist dann reinperiodisch. Genau dann ist $\varphi(b)$ die Periodenlänge, wenn $\mathrm{E}(\mathbb{Z}_b)$ zyklisch und g eine Primitivwurzel modulo b ist.

Beispiel. Wir wählen $g = 10$ und $b = 7$. Dann sind b und g teilerfremd. In $\mathbb{Z}_7$ gilt:

$$\overline{10} = \overline{3},\ \overline{10}^2 = \overline{2},\ \overline{10}^3 = \overline{6},\ \overline{10}^4 = \overline{4},\ \overline{10}^5 = \overline{5},\ \overline{10}^6 = \overline{1}.$$

$\mathrm{E}(\mathbb{Z}_7)$ ist also zyklisch (vergleiche Aufgabe 4.7 aus Kapitel 2) und 10 eine Primitivwurzel modulo 7. Es gilt

$$\frac{1}{7} = 0,\overline{142857} \quad \text{(Dezimalbruchentwicklung)},$$
$$\frac{1}{7} = 0,\overline{010212} \quad \text{(3-adische Entwicklung)}.$$

Wir untersuchen nun speziell den Fall $g = 10$, also die Dezimalbruchentwicklung von $\frac{a}{b}$ mit $a, b \in \mathbb{N}$, wobei a und b wieder teilerfremd sind. Wegen Satz 4.4 ist die Dezimalbruchentwicklung genau dann ...

... abbrechend, wenn $b = 2^n 5^m$ mit $n, m \in \mathbb{N}_0$.

... reinperiodisch, wenn b weder von 2 noch von 5 geteilt wird.

Ist die Dezimalbruchentwicklung reinperiodisch, so ist die Periodenlänge ein Teiler von $\varphi(b)$ und gleich $\varphi(b)$ genau dann, wenn 10 eine Primitivwurzel modulo b ist. Die Periodenlänge von $\frac{a}{b}$ ist also höchstens $b-1$. Ist b keine Primzahl, so gilt $\varphi(b) < b-1$, und damit ist die Länge der Periode kleiner als $b-1$. Die Periodenlänge ist also genau dann gleich $b-1$, wenn b eine Primzahl und 10 eine Primitivwurzel modulo b ist.

Die folgende Tabelle gibt eine Übersicht für den reinperiodischen Fall bis $b = 21$, wobei $\mathrm{ord}_b 10$ die Ordnung von 10 modulo b bezeichnet.

b	3	7	9	11	13	17	19	21
$\varphi(b)$	2	6	6	10	12	16	18	12
$\mathrm{ord}_b 10$	1	6	1	2	6	16	18	6

Sei nun $g \in \mathbb{N}, g \geq 2$ und $b \in \mathbb{N}$ eine Primzahl, die g nicht teilt, sowie g eine Primitivwurzel modulo b. Ist $0, \overline{c_1 c_2 \dots c_p}$ die reinperiodische g-adische Entwicklung von $\frac{1}{b}$, so gilt

$$\frac{1}{b} = c_1 g^{-1} + c_2 g^{-2} + \dots .$$

Für jedes $s \in \mathbb{N}$ folgt

$$\frac{g^s}{b} = \underbrace{c_1 g^{s-1} + \dots + c_{s-1} g^1 + c_s}_{[\frac{g^s}{b}]} + \underbrace{c_{s+1} g^{-1} + c_{s+2} g^{-2} + \dots}_{0, \overline{c_{s+1} \dots c_p c_1 \dots c_s}}.$$

Wir wollen nun die g-adische Entwicklung von $\frac{a}{b}$ berechnen, wobei $a \in \mathbb{N}$ mit $0 < a < b$. Da g eine Primitivwurzel modulo b ist, gibt es ein $s \in \mathbb{N}$ mit $a \equiv g^s \bmod b$, d.h. $a = g^s + mb$ für ein $m \in \mathbb{Z}$. Mit den Bezeichnungen von oben ergibt sich

$$\frac{a}{b} = m + \frac{g^s}{b} = \underbrace{[\frac{a}{b}]}_{=0} + c_{s+1} g^{-1} + c_{s+2} g^{-2} + \dots ,$$

d.h., $0, \overline{c_{s+1} \dots c_p c_1 \dots c_s}$ ist die g-adische Entwicklung von $\frac{a}{b}$, die sich aus der g-adischen Entwicklung von $\frac{1}{b}$ durch zyklisches Vertauschen der Ziffern ergibt. Gilt $a \equiv g^s \bmod b$ mit $s \in \mathbb{N}$, so erhält man die Darstellung von $\frac{a}{b}$, nachdem man in der Darstellung von $\frac{1}{b}$ die Ziffern genau um s Positionen nach links zyklisch vertauscht hat.

Beispiel. Wegen

$$10^1 \equiv 3 \bmod 7,\ 10^2 \equiv 2 \bmod 7,\ 10^3 \equiv 6 \bmod 7,$$

$$10^4 \equiv 4 \bmod 7,\ 10^5 \equiv 5 \bmod 7,\ 10^6 \equiv 1 \bmod 7$$

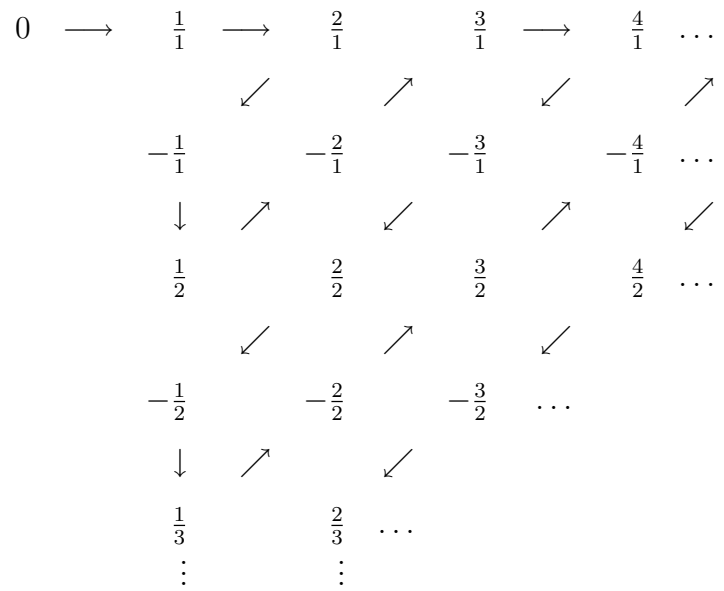
folgt für die Dezimaldarstellung

$$\frac{1}{7} = 0, \overline{142857}, \quad \frac{3}{7} = 0, \overline{428571}, \quad \frac{2}{7} = 0, \overline{285714},$$
$$\frac{6}{7} = 0, \overline{857142}, \quad \frac{4}{7} = 0, \overline{571428}, \quad \frac{5}{7} = 0, \overline{714285}.$$

Exkurs. Eine Menge M heißt abzählbar, wenn es eine surjektive Abbildung

$$f : \mathbb{N} \longrightarrow M$$

gibt. Ist M nicht abzählbar, so heißt M überabzählbar. Jede endliche Menge ist abzählbar, und offensichtlich sind auch $\mathbb{N}$ und $\mathbb{Z}$ abzählbar. Weniger offensichtlich ist, daß auch $\mathbb{Q}$ abzählbar ist. Die Abzählbarkeit von $\mathbb{Q}$ ergibt sich gemäß des ersten Cantorschen Diagonalverfahrens aus folgendem Schema:



Man überlegt sich nun leicht, daß die Produktmenge $M_1 \times \ldots \times M_n$ der Mengen $M_1, \ldots, M_n$ abzählbar ist, wenn jede Menge $M_i, i \in \{1, \ldots, n\}$ abzählbar ist, und daß die abzählbare Vereinigung

$$\bigcup_{i \in \mathbb{N}} M_i = M_1 \cup M_2 \cup \ldots$$

der abzählbaren Mengen $M_i,\ i \in \mathbb{N}$ abzählbar ist. Hieraus ergibt sich sofort, daß die Menge $\mathbb{Q}[x]$ der Polynome über $\mathbb{Q}$ abzählbar ist. Da jedes vom Nullpolynom verschiedene Polynom aus $\mathbb{Q}[x]$ nur endlich viele Nullstellen in $\mathbb{R}$ hat, ist die Menge der reellen algebraischen Zahlen abzählbar. Dabei heißt eine reelle Zahl algebraisch, wenn sie Nullstelle eines $f(x) \in \mathbb{Q}[x]$ mit $f(x) \neq 0$ ist. Die reellen Zahlen, die nicht algebraisch sind, heißen transzendent. Zum Beispiel ist $\sqrt[5]{\sqrt{5} - \sqrt[7]{41}}$ algebraisch, während π, e und $\sqrt{2}^{\sqrt{2}}$ transzendent sind.

Wir zeigen nun mit Hilfe des zweiten Cantorschen Diagonalverfahrens, daß $\mathbb{R}$ überabzählbar ist. Dazu nehmen wir zunächst an, daß $\mathbb{R}$ abzählbar ist. Dann ist auch $[0, 1)$ abzählbar, etwa

$$[0, 1) = \{r_1, r_2, r_3, \ldots\}.$$

Wegen Satz 4.1 hat jedes r_i eine eindeutige Dezimaldarstellung:

$$\begin{aligned} r_1 &= 0, a_{11}a_{12}a_{13}\ldots \\ r_2 &= 0, a_{21}a_{22}a_{23}\ldots \\ r_3 &= 0, a_{31}a_{32}a_{33}\ldots \\ &\vdots \end{aligned}$$

Es gibt nun ein $r \in [0, 1)$ mit der Dezimaldarstellung $r = 0, a_1a_2a_3\ldots$ wobei

$$a_i = \begin{cases} 2 & \text{für } a_{ii} = 1 \\ 1 & \text{für } a_{ii} \neq 1 \end{cases}.$$

Wegen $a_i \neq a_{ii}$ für alle $i \in \mathbb{N}$ gilt $r \notin \{r_1, r_2, r_3, \ldots\}$, im Widerspruch zu $r \in [0, 1)$.

Insbesondere ist damit die Menge der transzendenten reellen Zahlen überabzählbar. Im allgemeinen ist es sehr schwierig, von einer gegebenen Zahl (zum Beispiel π oder $\sqrt{2}^{\sqrt{2}}$) die Transzendenz nachzuweisen. Einfacher ist dagegen, überhaupt transzendente Zahlen zu konstruieren. So gilt zum Beispiel folgender

Satz 4.5 *Für $g \in \mathbb{N}, g \geq 2$ und $d_i \in S_g$ $(i \in \mathbb{N})$ mit $d_i \neq 0$ für unendlich viele Indizes i ist*

$$\sum_{i=1}^{\infty} d_i g^{-i!}$$

transzendent.

Mit Hilfe dieses Satzes können zum Beispiel überabzählbar viele transzendente reelle Zahlen in ihrer Dezimaldarstellung angegeben werden.

5. Zählen reeller Nullstellen

In diesem Abschnitt wird die Frage behandelt, wie die Anzahl reeller Nullstellen eines Polynoms $f(x) \in \mathbb{R}[x], f(x) \neq 0$ berechnet werden kann, ohne die Nullstellen selbst explizit ermitteln zu müssen. Dabei ist zunächst nicht klar, daß dieses überhaupt möglich ist. Als wichtiges Hilfsmittel in diesem Zusammenhang erweist sich dabei der Weierstraßsche Nullstellensatz für Polynome.

Weierstraßscher Nullstellensatz für Polynome.
Ist $f(x)$ ein reelles Polynom und sind $a, b \in \mathbb{R}, a < b$ mit $f(a) < 0$ und $0 < f(b)$, so gibt es ein $c \in (a, b)$ mit $f(c) = 0$.

Beweis. Siehe Aufgabe 6.8.

Eine unmittelbare Anwendung des Weierstraßschen Nullstellensatzes ist

Satz 5.1 *Ein reelles Polynom $f(x)$ ungeraden Grades hat mindestens eine reelle Nullstelle.*

Satz 5.1 folgt aus dem Weierstraßschen Nullstellensatz sobald gezeigt ist, daß es $a, b \in \mathbb{R}$, $a < b$ mit $f(a) < 0$ und $0 < f(b)$ gibt. Dieses liefert nun

Satz 5.2 *Ist $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$ und*

$$M := \max\{1, |a_{n-1}| + \ldots + |a_1| + |a_0|\},$$

so gilt $f(s) > 0$ für alle $s > M$ und $(-1)^n f(s) > 0$ für alle $s < -M$.

Beweis. Sei $|s| > M \geq 1$. Dann gilt

$$|\frac{a_{n-1}}{s} + \ldots + \frac{a_0}{s^n}| \leq |\frac{a_{n-1}}{s}| + \ldots + |\frac{a_0}{s^n}| \leq \frac{|a_{n-1}| + \ldots + |a_0|}{|s|} < 1.$$

Also folgt

$$f(s) = s^n(1 + \frac{a_{n-1}}{s} + \ldots + \frac{a_0}{s^n}) \text{ mit } 1 + \frac{a_{n-1}}{s} + \ldots + \frac{a_0}{s^n} > 0.$$

Ist $s > M$, dann gilt $f(s) > 0$, und ist $s < -M$, dann gilt $(-1)^n f(s) > 0$.

□

Korollar 5.3 *Mit den Bezeichnungen des obigen Satzes gilt: Jede reelle Nullstelle von $f(x)$ liegt im Intervall $[-M, M]$.*

Mehrfache Nullstellen.
Ist K ein Körper mit der Charakteristik 0 und $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x]$ ein Polynom über K sowie $a \in K$ eine Nullstelle von $f(x)$, dann gibt es ein $h(x) \in K[x]$ mit $f(x) = (x-a)h(x)$. Ist a auch Nullstelle von $h(x)$, so heißt a mehrfache Nullstelle von $f(x)$. Genauer heißt a nun l-fache Nullstelle von $f(x)$, wenn

$$f(x) = (x-a)^l \cdot h(x) \quad \text{mit} \quad h(x) \in K[x] \quad \text{und} \quad h(a) \neq 0$$

gilt. Zur Untersuchung mehrfacher Nullstellen führt man die formale Ableitung

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1$$

des Polynoms $f(x)$ ein, und man rechnet leicht nach, daß die aus der Analysis bekannten Rechenregeln wie zum Beispiel die Summen-, Produkt- und Kettenregel auch hier gelten. Somit ist dann

$$\begin{aligned} f'(x) &= l(x-a)^{l-1}h(x) + (x-a)^l h'(x) \\ &= (x-a)^{l-1}(lh(x) + (x-a)h'(x)) \\ &= (x-a)^{l-1}\tilde{h}(x), \end{aligned}$$

wobei $\tilde{h}(a) \neq 0$, d.h., $a \in K$ ist genau dann eine l-fache Nullstelle von $f(x)$, wenn a eine Nullstelle von $f(x)$ und eine $(l-1)$-fache Nullstelle von $(f(x), f'(x))$ ist, wobei $(f(x), f'(x))$ ein ggT von $f(x)$ und $f'(x)$ ist. Damit erhalten wir folgendes Ergebnis:

Jede Nullstelle von $\frac{f(x)}{(f(x),f'(x))}$ ist einfach, und bis auf Vielfachheit stimmen die Nullstellen von $f(x)$ und $\frac{f(x)}{(f(x),f'(x))}$ überein.

Mit ähnlichen Argumenten ergibt sich sogar allgemeiner: Jeder irreduzible Faktor des Polynoms $f(x) \in K[x], f(x) \neq 0$ tritt in der Zerlegung von $\frac{f(x)}{(f(x),f'(x))}$ nur einfach auf, und die beiden Polynome $f(x)$, $\frac{f(x)}{(f(x),f'(x))}$ haben bis auf Vielfachheit dieselben irreduziblen Faktoren.

Beispiel. Wir betrachten das Polynom $f(x) = x^6 + x^4 - x^2 - 1 \in \mathbb{R}[x]$. Dann gilt für die Ableitung $f'(x) = 6x^5 + 4x^3 - 2x$, und

$$f(x) = (x-1)(x+1)(x^2+1)^2, \quad f'(x) = x(x^2+1)(\sqrt{6}x + \sqrt{2})(\sqrt{6}x - \sqrt{2})$$

sind die Zerlegungen von $f(x)$ und $f'(x)$ in Primelemente (irreduzible Polynome) in $\mathbb{R}[x]$. Offenbar gilt $(f(x), f'(x)) \sim x^2 + 1$. In $\mathbb{R}$ hat $f(x)$ nur einfache Nullstellen, in $\mathbb{C}$ treten die doppelten Nullstellen $\pm i$, also $\pm\sqrt{-1}$ auf.

Wir untersuchen nun das Verhalten des Vorzeichens eines Polynoms beim "Passieren" einer Nullstelle. Dazu seien $a, b, c \in \mathbb{R}$ mit $a < b < c$, und es gelte

$$f(b) = 0 \ \text{ sowie } \ f(t), f'(t) \neq 0 \ \text{ für alle } \ t \in [a,c], t \neq b.$$

Dann gilt $f(x) = (x-b)^l r(x)$, wobei das Polynom $r(x)$ in $[a,c]$ keine Nullstelle hat, und $f'(x) = l(x-b)^{l-1} r(x) + (x-b)^l r'(x)$ sowie $(f(x), f'(x)) = (x-b)^{l-1} s(x)$, wobei auch $s(x)$ in $[a,c]$ keine Nullstelle hat. Definieren wir

$$\begin{aligned} g_0(x) &:= \frac{f(x)}{(f(x), f'(x))} = (x-b)\frac{r(x)}{s(x)} \in \mathbb{R}[x], \\ g_1(x) &:= \frac{f'(x)}{(f(x), f'(x))} = \frac{lr(x) + (x-b)r'(x)}{s(x)} \in \mathbb{R}[x], \end{aligned}$$

so gilt

(V) $g_0(a)$ und $g_1(a)$ haben verschiedene Vorzeichen, d.h. $g_0(a)g_1(a) < 0$.
$g_0(c)$ und $g_1(c)$ haben gleiches Vorzeichen, d.h. $g_0(c)g_1(c) > 0$.

Beweis von (V). Zunächst gilt $g_0(a) = (a-b)\frac{r(a)}{s(a)}$. Da $g_1(x), s(x)$ und $r(x)$ in $[a,c]$ keine Nullstelle besitzen, haben $g_1(a)$ und $g_1(b)$, $s(a)$ und $s(b)$ sowie $r(a)$ und $r(b)$ jeweils dasselbe Vorzeichen. Wegen $g_1(b) = l\frac{r(b)}{s(b)}$ und $a - b < 0$ folgt die erste Behauptung. Die zweite Behauptung ergibt sich entsprechend.

□

Bemerkung. Wegen $f(x) = g_0(x)(f(x), f'(x))$ und $f'(x) = g_1(x)(f(x), f'(x))$ gilt

$$f(a)f'(a) < 0 \ \text{ und } \ f(c)f'(c) > 0.$$

Wir wenden uns nun der Frage zu, wie man die Anzahl der reellen Nullstellen eines reellen Polynoms $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ berechnen kann. Dazu führen wir den Begriff der Sturmschen Kette ein. Dabei heißt die Folge $f(x), f'(x), f_2(x), f_3(x), \ldots, f_r(x)$ von Polynomen Sturmsche Kette von $f(x)$, wenn sie sich folgendermaßen aus dem euklidischen Algorithmus mit "negativem Rest" ergibt:

$$\begin{aligned} f(x) &=: f_0(x) \\ f'(x) &=: f_1(x) \\ f_0(x) &= q_1(x)f_1(x) - f_2(x) \\ &\vdots \\ f_i(x) &= q_{i+1}(x)f_{i+1}(x) - f_{i+2}(x) \\ &\vdots \\ f_{r-1}(x) &= q_r(x)f_r(x). \end{aligned}$$

Es gilt also grad $f_i <$ grad f_{i-1} für $i = 1, \ldots, r$. Für jedes $a \in \mathbb{R}$ sei weiterhin $w(a)$ die Anzahl der Vorzeichenwechsel in der Zahlenfolge

$$f(a), f'(a), f_2(a), \ldots, f_r(a),$$

in der man die Nullen weggelassen hat. Mit diesen Bezeichnungen gilt nun der folgende

Satz 5.4 (Theorem von Sturm) *Sind $a, b \in \mathbb{R}, a < b$, mit $f(a), f(b) \neq 0$, so hat $f(x)$ im Intervall $[a, b]$ genau $w(a) - w(b)$ verschiedene Nullstellen, wobei mehrfache Nullstellen nur einfach gezählt werden.*

Beweis. Der Einfachheit halber beweisen wir den Satz nur für den Fall, daß kein $f_i(x)$ bei a oder b eine Nullstelle hat. Der allgemeine Fall läßt sich aus den folgenden Argumenten leicht ableiten.
Zunächst ist klar, daß $f_r(x)$ ein ggT von $f(x)$ und $f'(x)$ ist (vgl. Kapitel 2.3). Definieren wir $g_i(x) := \frac{f_i(x)}{f_r(x)}$, so folgt $g_i(x) \in \mathbb{R}[x]$ und

$$\left.\begin{aligned} g_0(x) &= q_1(x)g_1(x) - g_2(x) \\ &\vdots \\ g_i(x) &= q_{i+1}(x)g_{i+1}(x) - g_{i+2}(x) \\ &\vdots \\ g_{r-2}(x) &= q_{r-1}(x)g_{r-1}(x) - 1. \end{aligned}\right\} (*)$$

Damit ist für jedes $c \in \mathbb{R}$ mit $f(c) \neq 0$ die Anzahl der Vorzeichenwechsel (nach dem Weglassen der Nullen) in

$$f_0(c), f_1(c), \ldots, f_r(c) \quad \text{und} \quad g_0(c), g_1(c), \ldots, g_r(c)$$

gleich. Weiterhin folgt wegen $(*)$ für jedes $c \in \mathbb{R}$ und jedes $k \in \{0, \ldots, r-2\}$: Gilt $g_k(c) = g_{k+1}(c) = 0$, so auch $g_{k+2}(c) = \ldots = g_{r-1}(c) = g_r(c) = 0$, im Widerspruch zu $g_r(x) = 1$. Damit gilt für jedes $c \in \mathbb{R}$ und jedes $k \in \{1, \ldots, r-1\}$:

$$(**) \quad g_k(c) = 0 \Longrightarrow g_{k+1}(c), g_{k-1}(c) \neq 0.$$

Sei nun

$$a = b_0 < a_1 < b_1 < a_2 < \ldots < a_m < b_m = b,$$

so daß für alle $i = 0, \ldots, r$ gilt:

$$\text{Ist } c \in [a, b] \text{ Nullstelle von } g_i(x), \text{ so folgt } c \in \{a_1, a_2, \ldots, a_m\}.$$

Mit V_i bezeichnen wir die Anzahl der Vorzeichenwechsel in

$$g_0(b_i), \ldots, g_r(b_i)$$

und untersuchen den Zusammenhang zwischen V_{i-1} und V_i für $i = 1, \ldots, m$:

1. Fall: $g_k(a_i) \neq 0$. Dann haben $g_k(b_{i-1}), g_k(a_i)$ und $g_k(b_i)$ dasselbe Vorzeichen.
2. Fall: $g_k(a_i) = 0$ und $k > 0$. Wegen $g_r(x) = 1$ ist dann $k < r$, und wir betrachten

$$\begin{array}{ccc} \vdots & \vdots & \vdots \\ g_{k-1}(b_{i-1}) & g_{k-1}(a_i) & g_{k-1}(b_i) \\ g_k(b_{i-1}) & g_k(a_i) & g_k(b_i) \\ g_{k+1}(b_{i-1}) & g_{k+1}(a_i) & g_{k+1}(b_i) \\ \vdots & \vdots & \vdots \end{array}$$

Wegen $(**)$ gilt dann $g_{k+1}(a_i), g_{k-1}(a_i) \neq 0$, d.h., $g_{k-1}(b_{i-1}), g_{k-1}(a_i), g_{k-1}(b_i)$ haben dasselbe Vorzeichen und $g_{k+1}(b_{i-1}), g_{k+1}(a_i), g_{k+1}(b_i)$ haben dasselbe Vorzeichen. Wegen $(*)$ haben aber $g_{k-1}(a_i)$ und $g_{k+1}(a_i)$ verschiedene Vorzeichen. Somit liegt in beiden Folgen

$$g_{k-1}(b_{i-1}), g_k(b_{i-1}), g_{k+1}(b_{i-1}) \quad \text{und} \quad g_{k-1}(b_i), g_k(b_i), g_{k+1}(b_i)$$

jeweils ein Vorzeichenwechsel vor.
3. Fall: $g_0(a_i) = 0$, d.h. $f(a_i) = 0$. Dann haben wegen (V) die Zahlen $g_0(b_{i-1})$ und $g_1(b_{i-1})$ verschiedene Vorzeichen sowie $g_0(b_i)$ und $g_1(b_i)$ gleiche Vorzeichen.

Somit erhalten wir folgendes Ergebnis:

$V_{i-1} = V_i$ falls a_i keine Nullstelle von $f(x)$ ist.

$V_{i-1} = V_i + 1$ falls a_i eine Nullstelle von $f(x)$ ist.

Hieraus folgt nun unmittelbar die Behauptung des Satzes.

□

Beispiel. Wir untersuchen das Polynom $f(x) = x^3 + 2x^2 - x - 2$ auf reelle Nullstellen. Wie man leicht nachrechnet gilt

$$f'(x) = 3x^2 + 4x - 1, \;\; f_1(x) = \frac{1}{9}(14x + 16) \;\; \text{und} \;\; f_2(x) = \frac{81}{49}.$$

Wieviele reelle Nullstellen hat $f(x)$? Dazu berechnen wir wegen Satz 5.2 und Korollar 5.3

$$M := \max\{1, 2 + 1 + 2\} = 5,$$

und erhalten:

$$\begin{array}{lll} f(-5) = -72 & f(0) = -2 & f(5) = 168 \\ f'(-5) = 54 & f'(0) = -1 & f'(5) = 94 \\ f_1(-5) = -\frac{54}{9} & f_1(0) = \frac{16}{9} & f_1(5) = \frac{86}{9} \\ f_2(-5) = \frac{81}{49} & f_2(0) = \frac{81}{49} & f_2(5) = \frac{81}{49}. \\ \text{3 Wechsel} & \text{1 Wechsel} & \text{0 Wechsel} \end{array}$$

Somit hat $f(x)$ drei reelle Nullstellen, und zwar zwei negative und eine positive. In diesem Falle kann das Ergebnis leicht überprüft werden, da -2,-1 und 1 die Nullstellen von $f(x)$ sind.

6. Aufgaben

A 6.1 Sei K ein geordneter Körper und (a_n) eine Cauchy-Folge in K, die keine Nullfolge ist. Zeigen Sie, daß es dann ein $\epsilon > 0$ und ein $n_0 \in \mathbb{N}$ gibt, so daß entweder $a_n \geq \epsilon$ für alle $n \geq n_0$ oder $-a_n \geq \epsilon$ für alle $n \geq n_0$ gilt.

A 6.2 Sei K ein geordneter Körper. Zeigen Sie, daß K genau dann archimedisch geordnet ist, wenn es zu jedem $x \in K$ und $\epsilon > 0$ ein $q \in \mathbb{Q}$ mit $\mid x - q \mid < \epsilon$ gibt.

A 6.3 Sei K ein geordneter Körper und seien $(a_n), (b_n)$ zwei Cauchy-Folgen in K. Zeigen Sie, daß dann auch $(a_n \pm b_n)$ und $(a_n \cdot b_n)$ Cauchy-Folgen in K sind.

A 6.4 Sei $P = \{a_n x^n + \ldots + a_1 x + a_0 \mid n \in \mathbb{N}_0 \text{ und } a_0, \ldots, a_n \in \mathbb{Q}, a_n > 0\} \subseteq \mathbb{Q}[x]$.

1. Zeigen Sie, daß es auf $\mathbb{Q}[x]$ eine lineare Ordnung gibt, bezüglich der $\mathbb{Q}[x]$ ein geordneter Integritätsbereich mit dem zugehörigen Positivbereich P ist.

2. $\mathbb{Q}(x)$ ist der gemäß Satz 3.3 geordnete Quotientenkörper von $\mathbb{Q}[x]$. Zeigen Sie, daß $\mathbb{Q}(x)$ nicht archimedisch geordnet ist. Hinweis: Betrachten Sie $x - n, n \in \mathbb{N}$.

A 6.5 Zeigen Sie, daß in $\mathbb{R}$ jede nach unten beschränkte, monoton fallende Folge konvergiert.

A 6.6 Zeigen Sie für $\mathbb{R}$ das Intervallschachtelungsaxiom: Ist $[a_1, b_1] \supseteq [a_2, b_2] \supseteq [a_3, b_3] \supseteq \ldots$ eine Folge von ineinander enthaltenen abgeschlossenen Intervallen mit $\lim(a_n - b_n) = 0$, so gibt es genau eine reelle Zahl x mit $x \in [a_i, b_i]$ für alle $i \in \mathbb{N}$.

A 6.7 Zeigen Sie: Ist K ein archimedisch geordneter Körper, in dem das Intervallschachtelungsaxiom gilt, so ist K vollständig, d.h, jede Cauchy-Folge aus K konvergiert in K. Dabei gilt in K das Intervallschachtelungsaxiom, wenn es zu jeder Folge $[a_1, b_1] \supseteq [a_2, b_2] \supseteq [a_3, b_3] \supseteq \ldots$ von ineinander enthaltenen abgeschlossenen Intervallen mit $\lim(a_n - b_n) = 0$ genau ein $x \in K$ mit $x \in [a_i, b_i]$ für alle $i \in \mathbb{N}$ gibt.

A 6.8 Zeigen Sie: Ist $f(x) \in \mathbb{R}[x]$ ein reelles Polynom und gibt es $a, b \in \mathbb{R}, a < b$ mit $f(a) < 0$ und $f(b) > 0$, so hat $f(x)$ eine Nullstelle in (a, b).

A 6.9 Zeigen Sie, daß in $\mathbb{R}$ der Satz vom Supremum gilt: Ist $M \subseteq \mathbb{R}$ eine nichtleere Teilmenge von $\mathbb{R}$, die in $\mathbb{R}$ eine obere Schranke hat, dann existiert in $\mathbb{R}$ das Supremum von M, d.h., M hat in $\mathbb{R}$ eine kleinste obere Schranke.

A 6.10 Berechnen Sie die g-adische Darstellung von $\frac{1}{45}$ für verschiedene $g \in \mathbb{N}$, $g \geq 2$ und diskutieren Sie die Längen der Vorperiode und Periode. Geben Sie $g \in \mathbb{N}$, $g \geq 2$ so an, daß die Periodenlänge der g-adischen Darstellung von $\frac{1}{45}$ maximal ist. Welche Periodenlängen können grundsätzlich auftreten? Geben Sie jeweils Beispiele an.

A 6.11 Geben Sie ein $g \in \mathbb{N}$, $g \geq 2$ so an, daß die Periodenlänge der g-adischen Darstellung von $\frac{1}{33}, \frac{1}{35}, \frac{1}{37}$ jeweils 10, 12 bzw. 9 ist (jeweils für dasselbe g).

A 6.12 Geben Sie alle Primzahlen p an, so daß 5 die Periodenlänge der 3-adischen Darstellung von $\frac{1}{p}$ ist. Berechnen Sie jeweils die 3-adische Entwicklung.

A 6.13 i) Zeigen Sie, daß 5 eine Primitivwurzel modulo 23 ist.
ii) Geben Sie die 5-adische Darstellung von $\frac{1}{23}$ an.
iii) Berechnen Sie möglichst effizient die 5-adische Darstellung von $\frac{2}{23}$, $\frac{10}{23}$, $\frac{4}{23}$, $\frac{20}{23}$ und $\frac{11}{23}$.

A 6.14 Berechnen Sie $b \in \mathbb{N}$ so, daß $0,\overline{0165}$ die 8-adische Darstellung von $\frac{1}{b}$ ist. Geben Sie die 3-adische Darstellung von $\frac{1}{b}$ an. Welche Periodenlängen können bei einer g-adischen Darstellung von $\frac{1}{b}$ genau auftreten? Geben Sie jeweils ein zugehöriges g an.

A 6.15 Zeigen Sie, daß es zu jedem $g \in \mathbb{N},\ g \geq 2$ stets zwei verschiedene $b \in \mathbb{N}$ gibt, so daß die g-adische Darstellung von $\frac{1}{b}$ reinperiodisch mit der Periodenlänge 4 ist. Geben Sie speziell für $g = 6$ alle $b \in \mathbb{N}$ mit dieser Eigenschaft an und berechnen Sie hierfür die 6-adische Entwicklung.

A 6.16 Sei $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, $n \geq 1$ ein reelles Polynom mit n reellen Nullstellen. Zeigen Sie:
i) Genau dann sind alle Nullstellen von $f(x)$ positiv, wenn die Zahlenfolge $1, a_{n-1}, \ldots, a_1, a_0$ insgesamt n Vorzeichenwechsel hat.
ii) Genau dann sind alle Nullstellen von $f(x)$ negativ, wenn $a_{n-1}, \ldots, a_1, a_0$ alle positiv sind.

A 6.17 Wieviele reelle Nullstellen hat das Polynom $f(x) = x^5 - 5x^4 + 5x - 1$?

A 6.18 Berechnen Sie die Anzahl der lokalen Maxima der Funktion

$$f : \mathbb{R} \longrightarrow \mathbb{R}, x \longmapsto x^6 + 6x^5 - 15x^2 - 6x + 1.$$

A 6.19 i) Berechnen Sie die Anzahl der reellen Nullstellen des reellen Polynoms $f(x)$, wobei gilt $f(x) = x^5 - 5x^2 + 15x - 3$.
ii) Zeigen Sie für das reelle Polynom

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + 1,$$

$n \geq 2, a_1, \ldots, a_{n-1} \geq 0$: Gilt $a_i = 0$ für mindestens ein $i \in \{1, \ldots, n-1\}$, so zerfällt $f(x)$ über $\mathbb{R}$ nicht vollständig in Linearfaktoren.

KAPITEL 4

Der Körper der komplexen Zahlen

1. Die komplexen Zahlen

Da $\mathbb{R}$ ein geordneter Körper ist, gilt $x^2 \geq 0$ für alle $x \in \mathbb{R}$, d.h., die Gleichung $x^2+1 = 0$ hat in $\mathbb{R}$ keine Lösung. Ziel dieses Paragraphen ist es zunächst, $\mathbb{R}$ so zu erweitern, daß in dem neuen Zahlbereich jedes Element ein Quadrat ist. Dazu definieren wir $\mathbb{C} := \mathbb{R} \times \mathbb{R}$. Die Elemente von $\mathbb{C}$ heißen komplexe Zahlen und für sie sind folgende Addition und Multiplikation erklärt:

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \quad (x_1, y_1) \cdot (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

Wie man nun leicht nachrechnen kann, ist $\mathbb{C}$ bezüglich dieser Verknüpfungen ein kommutativer Ring mit dem Nullelement $(0, 0)$ und dem Einselement $(1, 0)$. Wir zeigen, daß $\mathbb{C}$ sogar ein Körper ist. Dazu sei $(x, y) \neq (0, 0)$, also $x^2 + y^2 \neq 0$, weil $\mathbb{R}$ angeordnet ist. Dann gilt

$$(x, y) \cdot (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}) = (1, 0),$$

d.h., in $\mathbb{C}$ hat jedes von $(0, 0)$ verschiedene Element ein multiplikatives Inverses, und $\mathbb{C}$ ist damit ein Körper. Zunächst ist $\mathbb{C}$ keine Zahlbereichserweiterung von $\mathbb{R}$, da $\mathbb{R}$ in $\mathbb{C}$ nicht enthalten ist. $\mathbb{R}$ kann aber auf natürliche Weise in $\mathbb{C}$ eingebettet werden, denn offenbar ist

$$\varphi : \mathbb{R} \longrightarrow \mathbb{C}, \ x \longmapsto (x, 0)$$

ein injektiver Ringhomomorphismus. Schreibt man nun x statt $(x, 0)$ für alle $x \in \mathbb{R}$, so ist $\mathbb{R}$ ein Teilkörper von $\mathbb{C}$, und mit der üblichen Bezeichnung $i := (0, 1)$ erhält man

$$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\} \ \text{ wobei } \ i^2 = -1.$$

Für alle $x_1, x_2, y_1, y_2 \in \mathbb{R}$ ergeben sich folgende Rechenregeln:

1. $x_1 + iy_1 = x_2 + iy_2$ gilt genau dann, wenn $x_1 = x_2$ und $y_1 = y_2$.
2. $(x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i(y_1 + y_2)$.
3. $(x_1 + iy_1) \cdot (x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2)$.

Da -1 in $\mathbb{C}$ ein Quadrat ist, ist $\mathbb{C}$ bezüglich keiner Anordnung ein geordneter Körper.

Für jedes $z = x + iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$ heißt ...

... x Realteil von z (geschrieben $\mathrm{Re}z = x$).

... y Imaginärteil von z (geschrieben $\mathrm{Im}z = y$).

... $\overline{z} := x - iy \in \mathbb{C}$ die zu z konjugiert komplexe Zahl.

... $|z| :=_{+}\sqrt{z \cdot \overline{z}} =_{+}\sqrt{x^2 + y^2}$ der Betrag von z.

Die Konjugation

$$^{-} : \mathbb{C} \longrightarrow \mathbb{C},\ z \longmapsto \overline{z}$$

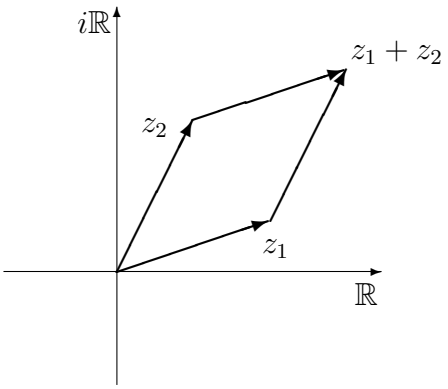
ist ein Automorphismus des Körpers $\mathbb{C}$, d.h., eine bijektive Abbildung, so daß für alle komplexen Zahlen z_1, z_2 gilt

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \ \text{ und } \ \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}.$$

Offenbar gilt $\overline{\overline{z}} = z$ für alle $z \in \mathbb{C}$, und damit ist die Konjugation ein Automorphismus der Ordnung 2. Genau dann gilt $\overline{z} = z$, wenn z reell ist.

Geometrische Darstellung der komplexen Zahlen

Da die komplexen Zahlen als Paare reeller Zahlen definiert sind, können sie in der reellen Ebene dargestellt werden. Man spricht dann von der Darstellung der komplexen Zahlen in der Gaußschen Zahlenebene:



Dabei entspricht die Addition von komplexen Zahlen der gewöhnlichen Vektoraddition im $\mathbb{R}^2$. Um die Multiplikation von komplexen Zahlen geometrisch zu veranschaulichen, führen wir die trigonometrische Darstellung (Polarkoordinaten) ein. Für jedes $z \in \mathbb{C}, z \neq 0$ mit $z = x + iy$ gilt

$$z = \sqrt{x^2 + y^2}\Big(\underbrace{\frac{x}{\sqrt{x^2 + y^2}}}_{a} + i\,\underbrace{\frac{y}{\sqrt{x^2 + y^2}}}_{b}\Big).$$

Wegen $a^2 + b^2 = 1$ gibt es ein eindeutig bestimmtes $\varphi \in [0, 2\pi)$ mit $a = \cos\varphi$ und $b = \sin\varphi$, d.h.

$$z = r(\cos\varphi + i\sin\varphi),$$

wobei $r = |z|$ der Betrag von z ist. Man nennt φ auch das Argument von z. Auf Grund der Additionstheoreme der Trigonometrischen Funktionen ergibt sich für die Multiplikation von komplexen Zahlen

$$\begin{aligned} r_1(\cos\varphi_1 + i\sin\varphi_1) \cdot r_2(\cos\varphi_2 + i\sin\varphi_2) = \\ &= r_1 r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)) \\ &= r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)). \end{aligned}$$

Bei der Multiplikation komplexer Zahlen werden also die Beträge multipliziert und die Argumente modulo 2π addiert. Hieraus ergibt sich unmittelbar die

Moivresche Formel: $(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi,\ n \in \mathbb{N}.$

Mit Hilfe der Moivreschen Formel lassen sich zum Beispiel schnell die Darstellungen von $\cos n\varphi$ und $\sin n\varphi$ als Polynome in $\cos\varphi$ und $\sin\varphi$ ermitteln. So erhält man für $n = 3$

$$\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\sin^2\varphi \quad \text{und} \quad \sin 3\varphi = 3\cos^2\varphi\sin\varphi - \sin^3\varphi.$$

Als weitere Anwendung ergeben sich die Lösungen der Gleichung $x^n - 1 = 0$ in $\mathbb{C}$ in der Form

$$\epsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n},\ k = 0, 1, \ldots, n-1.$$

Für diese Ergebnisse benötigt man die Cosinus- und Sinusfunktion, die wir allerdings nicht eingeführt haben. Ohne zusätzliche Hilfsmittel können wir zunächst nur den folgenden Satz beweisen.

Satz 1.1 *In $\mathbb{C}$ ist jedes Element ein Quadrat.*

Beweis. Zunächst ist in $\mathbb{R}$ jedes $x \geq 0$ ein Quadrat (vergleiche Eigenschaft R4 nach Definition 3.10 in Kapitel 3). Ist also $z \in \mathbb{C}$ mit $z = x + iy$, so gilt

$$\left(\sqrt{\frac{x + \sqrt{x^2+y^2}}{2}} + i\sqrt{\frac{-x + \sqrt{x^2+y^2}}{2}}\right)^2 = z \quad \text{falls} \quad y \geq 0$$

und

$$\left(\sqrt{\frac{x + \sqrt{x^2+y^2}}{2}} - i\sqrt{\frac{-x + \sqrt{x^2+y^2}}{2}}\right)^2 = z \quad \text{falls} \quad y < 0.$$

□

Im nächsten Paragraphen beweisen wir den Fundamentalsatz der Algebra, der besagt, daß jedes nichtkonstante Polynom über $\mathbb{C}$ eine komplexe Nullstelle hat. Dabei werden wir lediglich benutzen, daß in $\mathbb{C}$ jedes Element ein Quadrat ist, also Satz 1.1, und jedes reelle Polynom ungeraden Grades eine reelle Nullstelle hat, also Satz 5.1 aus Kapitel 3. Zur Vorbereitung

des Beweises erweitern wir den Begriff der Konjugation auf Polynome mit komplexen Koeffizienten.

Ist $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$ ein Polynom mit komplexen Koeffizienten, so heißt

$$\overline{f(x)} := \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \ldots + \overline{a_1}x + \overline{a_0} \in \mathbb{C}[x]$$

das zu $f(x)$ konjugierte Polynom, und die Konjugation

$$^- : \mathbb{C}[x] \longrightarrow \mathbb{C}[x],\ f(x) \longmapsto \overline{f(x)}$$

ist ein Automorphismus des Polynomrings $\mathbb{C}[x]$, d.h., eine bijektive Abbildung, so daß für alle komplexen Polynome $f(x), g(x)$ gilt

$$\overline{f(x) + g(x)} = \overline{f(x)} + \overline{g(x)} \quad \text{und} \quad \overline{f(x) \cdot g(x)} = \overline{f(x)} \cdot \overline{g(x)}.$$

Hieraus folgt nun unmittelbar für alle $f(x), g(x) \in \mathbb{C}[x]$ und $z \in \mathbb{C}$:

1. Ist $g(x)$ ein Teiler von $f(x)$, so ist $\overline{g(x)}$ ein Teiler von $\overline{f(x)}$.
2. Genau dann ist z Nullstelle von $f(x)$, wenn $\overline{z}$ Nullstelle von $\overline{f(x)}$ ist.
3. Ist $f(x)$ ein reelles Polynom, so ist mit z auch $\overline{z}$ eine Nullstelle von $f(x)$.
4. Genau dann ist $f(x)$ ein reelles Polynom, wenn $f(x) = \overline{f(x)}$.
5. $\overline{\overline{f(x)}} = f(x)$ und $f(x)\overline{f(x)}$ ist ein reelles Polynom.

2. Der Fundamentalsatz der Algebra

In diesem Paragraphen geben wir einen elementaren Beweis für den

Fundamentalsatz der Algebra. Jedes nichtkonstante komplexe Polynom hat in $\mathbb{C}$ eine Nullstelle.

Ist also $f(x)$ ein komplexes Polynom mit grad $f(x) > 1$, so gibt es wegen des Fundamentalsatzes ein $z \in \mathbb{C}$ und ein nichtkonstantes $g(x) \in \mathbb{C}[x]$ mit $f(x) = (x - z)g(x)$. Wendet man auf $g(x)$ den Fundamentalsatz an, so erhält man mit Hilfe der vollständigen Induktion folgende äquivalente Version für den

Fundamentalsatz der Algebra. Ist $f(x)$ ein nichtkonstantes komplexes Polynom, so gibt es $a \in \mathbb{C} \setminus \{0\}$ sowie $z_1, \ldots, z_n \in \mathbb{C}$ mit

$$f(x) = a(x - z_1) \cdot \ldots \cdot (x - z_n).$$

Ist nun $f(x)$ reell, so ist mit jeder Nullstelle $z = a + ib$ auch $\overline{z} = a - ib$ Nullstelle von $f(x)$. Ist also z nicht reell, d.h. $b \neq 0$, so ist

$$(x - z)(x - \overline{z}) = x^2 - 2ax + a^2 + b^2 \quad \text{und} \quad (-2a)^2 - 4(a^2 + b^2) = -4b^2 < 0.$$

Damit erhalten wir wegen Satz 1.1 folgende äquivalente reelle Version für den

Fundamentalsatz der Algebra. Ist $f(x)$ ein nichtkonstantes reelles Polynom, so gibt es ein $a \in \mathbb{R} \setminus \{0\}$ sowie $z_1, \ldots, z_k \in \mathbb{R}$ und $a_1, \ldots, a_m, b_1, \ldots, b_m \in \mathbb{R}$ mit

$$f(x) = a(x - z_1) \cdot \ldots \cdot (x - z_k) \cdot (x^2 + a_1 x + b_1) \cdot \ldots \cdot (x^2 + a_m x + b_m),$$

wobei $a_1^2 - 4b_1 < 0, \ldots, a_m^2 - 4b_m < 0$.

Bevor wir den Fundamentalsatz beweisen, diskutieren wir die Frage, auf welche Weise entschieden werden kann, ob zwei vom Nullpolynom verschiedene Polynome $f(x), g(x) \in K[x]$ einen nichtkonstanten gemeinsamen Teiler haben, wobei K ein belieber Körper ist. Besitzen $f(x)$ und $g(x)$ einen solchen gemeinsamen Teiler, so ist $(f(x), g(x))$ nicht konstant und damit

$$\text{grad } \frac{f(x)}{(f(x), g(x))} < \text{grad } f(x), \quad \text{grad } \frac{g(x)}{(f(x), g(x))} < \text{grad } g(x) \quad \text{sowie}$$

$$f(x)\frac{g(x)}{(f(x), g(x))} = g(x)\frac{f(x)}{(f(x), g(x))}.$$

Gibt es nun andererseits Polynome $a(x), b(x) \in K[x]$ mit $0 \leq \text{grad } a(x) < \text{grad } f(x)$ und $0 \leq \text{grad } b(x) < \text{grad } g(x)$ sowie $f(x)b(x) = g(x)a(x)$, so sind $f(x)$ und $g(x)$ nicht teilerfremd, denn anderenfalls wäre dann zum Beispiel $f(x)$ ein Teiler von $a(x)$, im Widerspruch zur Gradbedingung. Somit erhalten wir folgendes Kriterium:

> Ist K ein Körper und sind $f(x)$ und $g(x)$ vom Nullpolynom verschiedene Polynome über K, so haben $f(x)$ und $g(x)$ genau dann einen nichtkonstanten gemeinsamen Teiler, wenn es vom Nullpolynom verschiedene Polynome $a(x), b(x) \in K[x]$ mit grad $a(x) <$ grad $f(x)$ und grad $b(x) <$ grad $g(x)$ sowie $f(x)b(x) = g(x)a(x)$ gibt.

Um herauszufinden, ob es $a(x), b(x) \in K[x]$ mit obigen Eigenschaften tatsächlich gibt, schreiben wir $f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_1 x + f_0$ sowie $g(x) = g_m x^m + g_{m-1}x^{m-1} + \ldots + g_1 x + g_0$ mit $f_i, g_j \in K$ und machen den Ansatz $a(x) = a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ und $b(x) = b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$. Die Identität $f(x)b(x) = g(x)a(x)$ führt dann auf ein homogenes lineares Gleichungssystem für die a_i und b_j mit folgender Koeffizientenmatrix

$$\overbrace{\begin{pmatrix} g_m & 0 & \dots & 0 \\ g_{m-1} & g_m & & \vdots \\ \vdots & g_{m-1} & & \vdots \\ \vdots & \vdots & & \vdots \\ g_0 & \vdots & & g_m \\ 0 & g_0 & & g_{m-1} \\ \vdots & 0 & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & g_0 \end{pmatrix}}^{n \text{ Spalten}} \overbrace{\begin{pmatrix} -f_n & 0 & \dots & 0 \\ -f_{n-1} & -f_n & & \vdots \\ \vdots & -f_{n-1} & & \vdots \\ \vdots & \vdots & & \vdots \\ -f_0 & \vdots & & -f_n \\ 0 & -f_0 & & -f_{n-1} \\ \vdots & 0 & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & -f_0 \end{pmatrix}}^{m \text{ Spalten}}$$

Dieses System hat genau dann eine nichttriviale Lösung, wenn die Determinante der obigen Koeffizientenmatrix 0 ist. Definiert man nun im Falle $f_n, g_m \neq 0$

$$\mathrm{R}(f,g) := \begin{vmatrix} f_n & f_{n-1} & \dots & \dots & f_0 & 0 & \dots & \dots & 0 \\ 0 & f_n & f_{n-1} & \dots & \dots & f_0 & 0 & \dots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \dots & \dots & \dots & f_n & f_{n-1} & \dots & \dots & f_0 \\ g_m & g_{m-1} & \dots & \dots & g_0 & 0 & \dots & \dots & 0 \\ 0 & g_m & g_{m-1} & \dots & \dots & g_0 & 0 & \dots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \dots & \dots & \dots & g_m & g_{m-1} & \dots & \dots & g_0 \end{vmatrix}$$

so ist $\mathrm{R}(f,g)$ ein ganzzahliges Polynom in den Koeffizienten von $f(x)$ und $g(x)$. Offenbar unterscheiden sich $\mathrm{R}(f,g)$ und die Determinante der Koeffizientenmatrix höchstens um das Vorzeichen. Damit erhalten wir folgendes Kriterium:

> Ist K ein Körper und sind $f(x)$ und $g(x)$ vom Nullpolynom verschiedene Polynome über K, so haben $f(x)$ und $g(x)$ genau dann einen nichtkonstanten gemeinsamen Teiler, d.h. $(f(x), g(x)) \neq 1$, wenn $\mathrm{R}(f,g) = 0$.

$\mathrm{R}(f,g)$ heißt Resultante der Polynome $f(x)$ und $g(x)$. Es gilt stets $\mathrm{R}(f,g) \in K$. Ist $f_n = 1$, so kann man auf die Bedingung $g_m \neq 0$ verzichten.

Wir beweisen nun den Fundamentalsatz der Algebra und benutzen dabei

1. Jedes reelle Polynom ungeraden Grades hat eine reelle Nullstelle (Kapitel 3, Satz 5.1).
2. In $\mathbb{C}$ ist jedes Element ein Quadrat (Satz 1.1).

Es reicht aus zu zeigen, daß jedes nichtkonstante reelle Polynom $f(x) \in \mathbb{R}[x]$ eine Nullstelle in $\mathbb{C}$ hat, denn ist $f(x)$ nicht reell, so ist $f(x)\overline{f(x)}$ reell, und $f(x)\overline{f(x)}$ hat eine Nullstelle z. Ist z nicht Nullstelle von $f(x)$, dann ist z Nullstelle von $\overline{f(x)}$, also $\overline{z}$ Nullstelle von $f(x)$. Wir nehmen nun an, daß es ein nichtkonstantes reelles Polynom $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ gibt, das in $\mathbb{C}$ keine Nullstelle hat. Sei grad $f(x) = 2^l m$ mit $l \geq 0$ und m ungerade. Wir

wählen $f(x)$ so, daß l minimal und mit diesem l dann m minimal ist. Wegen Satz 5.1 aus Kapitel 3 gilt $l \geq 1$. Wir zeigen nun, daß unter diesen Voraussetzungen $f(x)$ doch eine komplexe Nullstelle besitzt. Dieses ist zum Beispiel der Fall, wenn $f(x)$ in $\mathbb{R}[x]$ reduzibel ist. Dann gilt nämlich $f(x) = g_1(x)g_2(x)$ mit $g_i(x) \in \mathbb{R}[x]$. Ist grad $g_i(x) = 2^{l_i}m_i$ mit $l_i \geq 0$ und m_i ungerade, so folgt $l_i < l$ oder $l_i = l$ und $m_i < m$ für ein i, da $2^l m = 2^{l_1}m_1 + 2^{l_2}m_2$. Für dieses i hat dann $g_i(x)$ eine komplexe Nullstelle, also auch $f(x)$.

Für jedes $t \in \mathbb{C}$ sei nun

$$F_t(x) = f(x+t) = F_0(t) + F_1(t)x + \ldots + F_n(t)x^n$$

mit reellen Polynomen $F_k(x)$. Es gilt $F_k(x) = \frac{f^{(k)}(x)}{k!}$ wobei $f^{(k)}(x)$ die (formale) k-te Ableitung von $f(x)$ ist (vgl. Aufgabe 3.4). Insbesondere ist $F_k(x)$ ein reelles Polynom vom Grad $n-k$ und dem führenden Koeffizienten $\binom{n}{k}$. Zum Beispiel gilt $F_{n-1}(x) = nx + a_{n-1}$ und $F_n(x) = 1$. Wir betrachten nun die Polynome

$$\begin{aligned} F_t^+(x) &= F_0(t) + F_2(t)x + F_4(t)x^2 + \ldots + F_n(t)x^{\frac{n}{2}}, \\ F_t^-(x) &= F_1(t) + F_3(t)x + F_5(t)x^2 + \ldots + F_{n-1}(t)x^{\frac{n}{2}-1}. \end{aligned}$$

Es gilt $F_t(x) = F_t^+(x^2) + xF_t^-(x^2)$. Gibt es ein $t \in \mathbb{C}$ mit $F_t^-(x) = 0$, so ist insbesondere $F_{n-1}(t) = nt + a_{n-1} = 0$, also t reell und damit $F_t^+(x)$ ein reelles Polynom vom Grad $\frac{n}{2}$. Somit hat $F_t^+(x)$ eine komplexe Nullstelle und auch $F_t^+(x^2)$, da in $\mathbb{C}$ jedes Element ein Quadrat ist. Wegen $F_t^+(x^2) = F_t(x) = f(x+t)$ hat auch $f(x)$ eine reelle Nullstelle. Sei also im folgenden $F_t^-(x) \neq 0$ für alle $t \in \mathbb{C}$. Wir untersuchen die Resultante

$$R(t) := \mathrm{R}(F_t^+(x), F_t^-(x)).$$

Offenbar ist $R(t)$ ein reelles Polynom in t, und - wie wir gleich zeigen werden - hat $R(t)$ den Grad $\frac{n(n-1)}{2} = 2^{l-1}m'$ mit ungeradem m'. Somit gibt es ein $t \in \mathbb{C}$ mit $R(t) = 0$. Für dieses t sind $F_t^+(x)$ und $F_t^-(x)$ vom Nullpolynom verschiedene komplexe Polynome, die einen nichtkonstanten gemeinsamen Teiler $g(x) \in \mathbb{C}[x]$ haben. Dann ist $g(x^2)$ ein Teiler von $F_t^+(x^2)$ und $F_t^-(x^2)$, also auch von $F_t(x)$, und $g((x-t)^2)$ ist ein Teiler von $f(x)$, d.h. $f(x) = g((x-t)^2)h(x)$ für ein komplexes Polynom $h(x) \in \mathbb{C}[x]$. Zunächst ist grad $g(x) \leq$ grad $F_t^-(x) < \frac{n}{2}$, also grad $g((x-t)^2) < n =$ grad $f(x)$. Damit ist $h(x)$ nicht konstant, und die reellen Polynome $f(x)$ und $h(x)\overline{h(x)}$ sind nicht teilerfremd. Im Falle grad $h(x) < \frac{n}{2}$ ergibt sich daraus, daß $f(x)$ über $\mathbb{R}$ reduzibel ist. Im Falle grad $h(x) > \frac{n}{2}$ betrachten wir $g((x-t)^2)$ statt $h(x)$. Zu diskutieren bleibt der Fall grad $g((x-t)^2) =$ grad $h(x) = \frac{n}{2}$. Dann hat aber das reelle Polynom $g(x-t)\overline{g(x-t)}$ eine komplexe Nullstelle wegen grad $g(x-t)\overline{g(x-t)} = 2^{l-1}m$. Folglich besitzt auch $g(x-t)$ eine komplexe Nullstelle und damit auch $g((x-t)^2)$, da in $\mathbb{C}$ jedes Element ein Quadrat ist. Somit ergibt sich schließlich, daß auch $f(x)$ eine komplexe Nullstelle hat.

Zu zeigen bleibt nur noch, daß die Resultante $\mathrm{R}(F_t^+(x), F_t^-(x))$ von $F_t^+(x)$ und $F_t^-(x)$ ein

Polynom in t vom Grad $\frac{n(n-1)}{2}$ ist. Zunächst gilt

$$\mathrm{R}(F_t^+(x), F_t^-(x)) = \begin{vmatrix} F_n & F_{n-2} & \dots & \dots & \dots & F_0 & 0 & \dots & \dots & 0 \\ 0 & F_n & F_{n-2} & \dots & \dots & \dots & F_0 & 0 & \dots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & \dots & 0 & F_n & F_{n-2} & F_{n-4} & \dots & \dots & \dots & F_0 \\ F_{n-1} & F_{n-3} & \dots & \dots & F_1 & 0 & \dots & \dots & \dots & 0 \\ 0 & F_{n-1} & F_{n-3} & \dots & F_3 & F_1 & 0 & \dots & \dots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & \dots & \dots & 0 & F_{n-1} & F_{n-3} & \dots & \dots & \dots & F_1 \end{vmatrix}.$$

Nach Vertauschen von geeigneten Zeilen ist dieses bis auf das Vorzeichen

$$|(r_{ij}(t))| := \begin{vmatrix} F_{n-1} & F_{n-3} & \dots & \dots & F_1 & 0 & \dots & \dots & \dots & 0 \\ F_n & F_{n-2} & \dots & \dots & \dots & F_0 & 0 & \dots & \dots & 0 \\ 0 & F_{n-1} & F_{n-3} & \dots & F_3 & F_1 & 0 & \dots & \dots & 0 \\ 0 & F_n & F_{n-2} & \dots & \dots & F_2 & F_0 & 0 & \dots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & \dots & 0 & F_n & F_{n-2} & F_{n-4} & \dots & \dots & \dots & F_0 \\ 0 & \dots & \dots & 0 & F_{n-1} & F_{n-3} & \dots & \dots & \dots & F_1 \end{vmatrix}.$$

Bezeichnet $r_{ij}(t)$ das Polynom in der rechten Determinante, das in der i-ten Zeile an der j-ten Stelle steht, so gilt $r_{ij}(t) = 0$ oder grad $r_{ij}(t) = 2j - i$, da grad $F_{n-k} = k$. Berechnen wir nun $|(r_{ij}(t))|$ mit Hilfe der Leibnizformel, so ergibt sich

$$|(r_{ij}(t))| = \sum_{\sigma \in \mathbf{S_{n-1}}} \mathrm{sgn}\sigma \cdot r_{1\sigma(1)} \cdot \ldots \cdot r_{n-1\sigma(n-1)}.$$

Wegen grad $r_{1\sigma(1)} \cdot \ldots \cdot r_{n-1\sigma(n-1)} = \frac{n(n-1)}{2}$, falls $r_{1\sigma(1)} \cdot \ldots \cdot r_{n-1\sigma(n-1)} \neq 0$, ist gemäß der Leibnizformel $|(r_{ij}(t))|$ eine Summe von Polynomen vom Grad $\frac{n(n-1)}{2}$. Den Koeffizienten von $t^{\frac{n(n-1)}{2}}$ in $R(t)$ erhalten wir also (bis auf das Vorzeichen) dadurch, daß wir in den obigen Determinanten die Funktionen $r_{ij}(t)$ bzw. F_k durch ihre führenden Koeffizienten ersetzen. Da $\binom{n}{k}$ der führende Koeffizient von F_k ist, ist der führende Koeffizient von $t^{\frac{n(n-1)}{2}}$ in $R(t)$ durch

$$\begin{vmatrix} \binom{n}{n} & \binom{n}{n-2} & \dots & \dots & \dots & \binom{n}{0} & 0 & \dots & \dots & 0 \\ 0 & \binom{n}{n} & \binom{n}{n-2} & \dots & \dots & \dots & \binom{n}{0} & 0 & \dots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & \dots & 0 & \binom{n}{n} & \binom{n}{n-2} & \binom{n}{n-4} & \dots & \dots & \dots & \binom{n}{0} \\ \binom{n}{n-1} & \binom{n}{n-3} & \dots & \dots & \binom{n}{1} & 0 & \dots & \dots & \dots & 0 \\ 0 & \binom{n}{n-1} & \binom{n}{n-3} & \dots & \binom{n}{3} & \binom{n}{1} & 0 & \dots & \dots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & \dots & \dots & 0 & \binom{n}{n-1} & \binom{n}{n-3} & \dots & \dots & \dots & \binom{n}{1} \end{vmatrix}$$

gegeben. Dieses ist offenbar die Resultante der Polynome

$$a(x) = \binom{n}{n} x^{\frac{n}{2}} + \binom{n}{n-2} x^{\frac{n}{2}-1} + \ldots + \binom{n}{0},$$
$$b(x) = \binom{n}{n-1} x^{\frac{n}{2}-1} + \binom{n}{n-3} x^{\frac{n}{2}-2} + \ldots + \binom{n}{1}.$$

Zu zeigen bleibt damit $\mathrm{R}(a(x), b(x)) \neq 0$. Wäre $\mathrm{R}(a(x), b(x)) = 0$, so hätten $a(x)$ und $b(x)$, also auch $a(x^2)$ und $xb(x^2)$ einen nichtkonstanten gemeinsamen Teiler. Dann wären aber auch $a(x^2) - xb(x^2)$ und $a(x^2) + xb(x^2)$ nicht teilerfremd. Dieses ist nun ein Widerspruch, da $a(x^2) - xb(x^2) = (x-1)^n$ und $a(x^2) + xb(x^2) = (x+1)^n$.

3. Aufgaben

A 3.1 Lösen Sie die Gleichung $z^2 + 6iz - 6 + 4i = 0$ in $\mathbb{C}$.

A 3.2 Geben Sie für das Polynom $f(x) = x^3 + ax + b \in \mathbb{C}[x]$ mit Hilfe von a und b ein Kriterium dafür an, daß $f(x)$ in $\mathbb{C}$ nur einfache Nullstellen hat. Hinweis: Untersuchen Sie die Resultante von $f(x)$ und $f'(x)$. Geben Sie sinnvolle Beispiele an.

A 3.3 Zeigen Sie: Hat $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ die rationale Nullstelle $q \in \mathbb{Q}$, so gilt $q \in \mathbb{Z}$, und q ist in $\mathbb{Z}$ ein Teiler von a_0.

A 3.4 K sei ein Körper mit der Charakteristik 0 und $f(x) \in K[x]$ ein Polynom vom Grad n. Zeigen Sie, daß für alle $t \in K$ gilt

$$f(x+t) = F_0(t) + F_1(t)x + \ldots + F_n(t)x^n,$$

wobei $F_k(x) = \frac{f^{(k)}(x)}{k!}$. Dabei ist $f^{(k)}(x)$ die formale k-te Ableitung von $f(x)$. Zeigen Sie weiterhin, daß $F_k(x)$ den Grad $n-k$ und - falls $f(x)$ normiert ist - den führenden Koeffizienten $\binom{n}{k}$ hat.

A 3.5 Das Polynom $f(x) = x^6 - 2x^5 + 5x^4 - 5x^3 + 10x^2 - 7x + 6 \in \mathbb{Z}[x]$ besitzt eine Darstellung

$$f(x) = (x^2 + a_1 x + b_1)(x^2 + a_2 x + b_2)(x^2 + a_3 x + b_3),$$

wobei $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Z}$. Berechnen Sie $a_1, a_2, a_3, b_1, b_2, b_3$. Hinweis: Finden Sie eine Zerlegung von $f(x)$ wie im Beweis des Fundamentalsatzes. Zur Berechnung einer Nullstelle der Resultante verwenden Sie Aufgabe 3.3. Die Resultante ist ein ganzzahliges Polynom vom Grad 15 mit großen Koeffizienten, das sich als ganzzahliges Polynom in $2t$ schreiben läßt.

Index