Joachim Gräter

Algebra

Potsdam, März 2005

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 oder Inverses 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. 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.

6. Für jedes $a \in G$ und $n \in \mathbb{N}_0$ definiert man die Potenz a^n rekursiv durch $a^0 = e$ und $a^n = a^{n-1}a$ falls $n \geq 1$. Für alle $n, m \in \mathbb{N}_0$ gilt dann

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

Potenzen mit negativen Exponenten definiert man durch

$$a^{-n} = (a^{-1})^n, n \in \mathbb{N}.$$

Für alle $n, m \in \mathbb{Z}$ gilt dann

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

Ist die Addition die Gruppenverknüpfung, so schreibt man na statt a^n für alle $n \in \mathbb{Z}$ und $a \in G$. Die Potenzrechengesetze übertragen sich entsprechend.

Beispiel.

1. Die Mengen $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind abelsche Gruppen bezüglich der Addition.
2. Bezüglich der gewöhnlichen Multiplikation sind die Mengen $\mathbb{Q}^\times, \mathbb{R}^\times$ und $\mathbb{C}^\times$ sowie $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$ und $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$ abelsche Gruppen.
3. Für jedes $n \in \mathbb{N}$ ist
$$\mathbf{S}_n = \{f : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\} \mid f \text{ ist bijektiv}\}$$
eine Gruppe bezüglich der Komposition (symmetrische Gruppe). Sie hat $n!$ Elemente und ist für $n \geq 3$ nicht abelsch.
4. Ist K ein Körper und $n \in \mathbb{N}$, dann sind $\mathrm{GL}(n; K)$ und $\mathrm{SL}(n; K)$ Gruppen bezüglich des üblichen Matrizenproduktes. Dabei ist $\mathrm{GL}(n; K)$ die Menge der regulären (n, n)-Matrizen über K und $\mathrm{SL}(n; K)$ die Menge der (n, n)-Matrizen über K mit Determinante 1.
5. Die Affinitäten eines affinen Raums und die Kongruenzen eines euklidischen Raums sind Gruppen bezüglich der Komposition.
6. Endliche Gruppen mit nicht zu vielen Elementen können durch ihre Verknüpfungstafeln (Gruppentafeln) dargestellt werden. Mit $G = \{g_1, \ldots, g_n\}$ schreibt man

	g_1	$\cdots$	g_j	$\cdots$	g_n
g_1			$\vdots$		
$\vdots$			$\vdots$		
g_i	$\cdots$	$\cdots$	$g_i g_j$		
$\vdots$					
g_n					

So ist zum Beispiel $G = \{e, a, b, c\}$ mit der Verknüpfungstafel

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

eine abelsche Gruppe.

Definition 1.2 *Ist G eine Gruppe, so hat $g \in G$ unendliche Ordnung , wenn $g^n \neq e$ für alle $n \in \mathbb{N}$ gilt (geschrieben* $\mathrm{ord} g = \infty$*). Gilt aber $g^n = e$ für $n \in \mathbb{N}$ und $g^k \neq e$ für alle $k \in \mathbb{N}, 1 \leq k < n$, so hat g die Ordnung n (geschrieben* $\mathrm{ord} g = n$*).*

Satz 1.3 *Sei G eine Gruppe und $g \in G$. Hat g unendliche Ordnung, so sind alle $g^n, n \in \mathbb{N}$ verschieden. Hat g die Ordnung $n \in \mathbb{N}$, so gibt es nur endlich viele verschiedene Potenzen von g, nämlich $g^0 = e, g, \ldots, g^{n-1}$, und jedes $k \in \mathbb{Z}$ mit $g^k = e$ ist Vielfaches von n.*

Beweis. Hat g unendliche Ordnung und gilt $g^n = g^m$ für $n, m \in \mathbb{N}$ mit $n \geq m$, so folgt $g^{n-m} = e$ und $n - m \in \mathbb{N}_0$, also $n = m$. Sei nun $n = \mathrm{ord} g \in \mathbb{N}$ und $g^k = e$ mit $k \in \mathbb{Z}$. Dann gibt es $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, n-1\}$ mit $k = qn + r$, also $e = g^k = g^{qn+r} = (g^n)^q g^r = g^r$, d.h. $r = 0$. Insbesondere gilt $g^{k_1} = g^{k_2}$ für $k_1, k_2 \in \mathbb{Z}$ genau dann, wenn $g^{k_1 - k_2} = e$, also $k_1 - k_2$ Vielfaches von n ist. Folglich sind $g^0 = e, g, \ldots, g^{n-1}$ paarweise verschieden und $g^k \in \{e, g, \ldots, g^{n-1}\}$ für alle $k \in \mathbb{Z}$.

□

Bemerkung. In jeder endlichen Gruppe hat somit jedes Element endliche Ordnung; die Umkehrung gilt jedoch nicht.

Das direkte Produkt von Gruppen.

Sind $G_1, \ldots, G_n$ Gruppen, so ist

$$G_1 \times \cdots \times G_n$$

bezüglich der komponentenweisen Verknüpfung eine Gruppe (direktes Produkt der Gruppen $G_1, \ldots, G_n$). Ist e_i das neutrale Element von G_i $(i = 1, \ldots, n)$, so ist $(e_1, \ldots, e_n)$ das neutrale Element von $G_1 \times \cdots \times G_n$, und für $g_i \in G_i, i = 1, \ldots, n$ gilt

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

Offenbar ist $G_1 \times \cdots \times G_n$ genau dann abelsch, wenn jedes G_i abelsch ist. Schreibt man die Gruppen G_i additiv, so spricht man von der direkten Summe und schreibt $G_1 \oplus \cdots \oplus G_n$.

Wählen wir zum Beispiel $G_1 = G_2 = \{1, -1\} \subseteq \mathbb{Q}^\times$, so sind G_1 und G_2 Gruppen bezüglich der Multiplikation.

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1, g_2 \in \{1, -1\}\}.$$

Mit $e = (1,1), a = (1,-1), b = (-1,1)$ und $c = (-1,-1)$ ergibt sich folgende Gruppentafel (vgl. Beispiel 6 nach Definition 1.1):

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

2. Untergruppen

Definition 2.1 *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. Für jeden Körper K und $n \in \mathbb{N}$ ist $\mathrm{SL}(n; K)$ eine Untergruppe von $\mathrm{GL}(n; K)$.

4. Für $n \in \mathbb{N}$ ist die Gruppe $\mathrm{SO}(n)$ der eigentlich orthogonalen Matrizen Untergruppe von $\mathrm{O}(n)$, der Gruppe der orthogonalen Matrizen, die Untergruppe von $\mathrm{GL}(n; \mathbb{R})$ ist.

Satz 2.2 *Eine nichtleere Teilmenge U einer Gruppe G ist genau dann eine Untergruppe von G, wenn $ab^{-1} \in U$ für alle $a, b \in U$ gilt.*

Beweis. $''\Longrightarrow''$: Die Gleichung $xb = a$ hat in U und G dieselbe eindeutige Lösung.
$''\Longleftarrow''$: Wegen $U \neq \emptyset$ gibt es ein $a \in U$, und es folgt $aa^{-1} = e \in U$. Für jedes $u \in U$ gilt somit $u^{-1} = eu^{-1} \in U$, und sind $x, y \in U$, so ergibt sich $y^{-1} \in U$, also $xy = x(y^{-1})^{-1} \in U$. Damit induziert die Verknüpfung von G eine assoziative Verknüpfung in U.

□

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

Anwendung von Satz 2.2.

1. Ist G eine Gruppe, so heißt $\mathrm{Z}(G) := \{z \in G \mid \forall g \in G : zg = gz\}$ Zentrum von G. Das Zentrum $\mathrm{Z}(G)$ ist eine Untergruppe von G: Wegen $e \in \mathrm{Z}(G)$ ist $\mathrm{Z}(G)$ nicht leer und sind $a, b \in \mathrm{Z}(G)$, so folgt für alle $g \in G$

$$ab^{-1}g = a(g^{-1}b)^{-1} = a(bg^{-1})^{-1} = agb^{-1} = gab^{-1},$$

   also $ab^{-1} \in \mathrm{Z}(G)$.

2. Ist $\{U_i | i \in I\}$ eine Menge von Untergruppen von G, so ist $U := \cap_{i \in I} U_i$ eine Untergruppe von G: Zunächst gilt $e \in U_i$ für alle $i \in I$, also $e \in \cap_{i \in I} U_i$, d.h., $\cap_{i \in I} U_i$ ist nicht leer. Sind $a, b \in \cap_{i \in I} U_i$, so folgt $a, b \in U_i$ für jedes $i \in I$, also $ab^{-1} \in U_i$ für jedes $i \in I$, d.h. $ab^{-1} \in \cap_{i \in I} U_i$.

3. 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. Insbesondere ist $\langle a \rangle$ für $a \in G$ die von a erzeugte Untergruppe von G. Wie man sich leicht mit Hilfe von Satz 2.2 überlegt, besteht $\langle a \rangle$ genau aus den Potenzen von a, d.h.

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \text{ und } |\langle a \rangle| = \text{ord} a.$$

Die Gruppe G heißt zyklisch, wenn es ein $a \in G$ mit $G = \langle a \rangle$ gibt. Zyklische Gruppen sind stets abelsch, denn für alle $n, m \in \mathbb{Z}$ gilt $a^n a^m = a^m a^n$.

Beispiel.

1. 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 $\text{ord}\sigma = n$, $\text{ord}\tau = 2$, und man überlegt sich weiterhin, daß auch folgendes gilt:

(a) $\sigma\tau = \tau\sigma^{n-1}$.

(b) $\mathrm{D}_n = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \ldots, \tau\sigma^{n-1}\}$.

(c) $| \mathrm{D}_n | = 2n$.

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.

2. Bezüglich der Addition ist $\mathbb{Z}$ eine unendliche zyklische Gruppe, die von 1 und auch von -1 erzeugt wird: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

3. Für jedes $n \in \mathbb{N}$ sei $\pi_n = (12 \ldots n) \in \mathbf{S}_n$. Dann hat π_n die Ordnung n, und $\langle \pi_n \rangle$ ist eine zyklische Gruppe mit n Elementen.

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 $a, b \in G$.
   Wie man sich leicht überlegt, ist $aU \longrightarrow bU, au \longmapsto ba^{-1}(au) = bu$ 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 $aU = bU$. Insbesondere folgt dann

   $$b \in aU \Longrightarrow aU = bU.$$

   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 2.3 *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 $U = \langle\tau\rangle = \{\mathrm{id}, \tau\}$.

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

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

Satz 2.4 (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).

□

Bemerkung.

1. Der Satz von Lagrange besagt auch folgendes: Sind zwei der Größen $|G|, |U|$ und $(G : U)$ endlich, so auch die dritte.
2. Ist G eine Gruppe, so bezeichnet man $|G|$ als Ordnung von G, geschrieben ord$G$. Insbesondere sagt also der Satz von Lagrange aus, daß die Ordnung einer Untergruppe die Gruppenordnung teilt. So hat zum Beispiel die Gruppe $\mathrm{GL}(2; \mathbb{Z}_3)$ keine Untergruppe der Ordnung 9, da $|\mathrm{GL}(2; \mathbb{Z}_3)| = 48$. Ob allerdings $\mathrm{GL}(2; \mathbb{Z}_3)$ eine Untergruppe der Ordnung 6 hat, kann mit Hilfe des Satzes von Lagrange nicht entschieden werden.

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. Sei G die multiplikative Gruppe $\mathbb{R}^\times$ und U die Untergruppe $\mathbb{R}^+$. Dann hat $\mathbb{R}^+$ die beiden Nebenklassen $\mathbb{R}^+$ (die positiven reellen Zahlen) und $(-1)\mathbb{R}^+$ (die negativen reellen Zahlen), d.h. $(\mathbb{R}^\times : \mathbb{R}^+) = 2$.

Folgerungen aus dem Satz von Lagrange.

1. Die Ordnung eines Gruppenelementes teilt die Gruppenordnung.
Beweis: Für jedes Gruppenelement a gilt ord$a = |\langle a \rangle|$. Mit Bemerkung 2 folgt die Behauptung.
2. 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. $\langle a \rangle = G$.
3. Ist G eine Gruppe und $|G| = n < \infty$, dann gilt $a^n = e$ für alle $a \in G$.
Beweis: Wegen Folgerung 1 gilt $n = k \cdot \mathrm{ord}a$ für ein $k \in \mathbb{N}$, also
$$a^n = (a^{\mathrm{ord}a})^k = e^k = e.$$
4. Sind U und V endliche Untergruppen einer Gruppe G und $|U|, |V|$ teilerfremd, so gilt $U \cap V = \{e\}$.
Beweis: Da $U \cap V$ Untergruppe sowohl von U als auch von V ist, ist $|U \cap V|$ ein gemeinsamer Teiler von $|U|$ und $|V|$, also $|U \cap V| = 1$.

3. Gruppenhomomorphismen

Definition 3.1 *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.
5. Die Menge Aut$G$ der Automorphismen von G ist bezüglich der Komposition eine Gruppe mit dem neutralen Element $\mathrm{id} : G \longrightarrow G, g \longmapsto g$; sie heißtAutomorphismengruppe von G.

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. Für jedes $g \in G$ ist $\mathrm{i}_g : G \longrightarrow G, x \longmapsto gxg^{-1}$ ein Automorphismus von G; er heißt der durch g induzierte innere Automorphismus .
3. 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.
4. 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.
5. Ist K ein Körper und V ein n-dimensionaler K-Vektorraum, so ist die Gruppe $\mathrm{Aut}_K(V)$ der Vektorraumautomorphismen von V isomorph zur Matrizengruppe $\mathrm{GL}(n; K)$, d.h. $\mathrm{Aut}_K(V) \cong \mathrm{GL}(n; K)$.
6. Für jedes $n \in \mathbb{N}$ ist $\mathrm{sgn} : \mathbf{S}_n \longrightarrow \{1, -1\}, \pi \longmapsto \mathrm{sgn}\pi$ ein Gruppenhomomorphismus.

Satz 3.2 *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. *$\text{Kern}\varphi := \{a \in G \mid \varphi(a) = e_H\}$ ist Untergruppe von G.*
4. *φ ist injektiv $\Longleftrightarrow \text{Kern}\varphi = \{e_G\}$.*

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:
$$\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(U).$$
Aufgrund von Satz 2.2 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: $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} \in V$, also $ab^{-1} \in \varphi^-(V)$. Aufgrund von Satz 2.2 ist damit $\varphi^-(V)$ Untergruppe von G.
3. Die Behauptung folgt sofort aus 2. mit $V = \{e_H\}$.
4. $''\Longrightarrow''$: Da φ injektiv ist, ist e_G das einzige Urbild von e_H, d.h. $\text{Kern}\varphi = \{e_G\}$.
$''\Longleftarrow''$: 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 $ab^{-1} \in \text{Kern}\varphi$, d.h. $ab^{-1} = e_G$, also $a = b$.

□

Definition 3.3 *Sind G, H Gruppen und ist $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus, so heißt* $\text{Kern}\varphi$ *der Kern von φ.*

Satz 3.4 *Sind G, H Gruppen und ist $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus sowie $N := \text{Kern}\varphi$, so gilt $aN = Na$ für alle $a \in G$.*

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

□

Definition 3.5 *Ist G eine Gruppe und U eine Untergruppe von G, so heißt U Normalteiler in G, wenn $aU = Ua$, also $aUa^{-1} = U$ für alle $a \in G$ gilt.*

Bemerkung. Eine Untergruppe U von G ist bereits dann Normalteiler in G, wenn $aU \subseteq Ua$ ($Ua \subseteq aU$) für alle $a \in G$ gilt, denn in diesem Falle ist auch $a^{-1}U \subseteq Ua^{-1}$ ($Ua^{-1} \subseteq a^{-1}U$) für alle $a \in G$, also $Ua \subseteq aU$ ($aU \subseteq Ua$).

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. Das Zentrum $\mathrm{Z}(G)$ einer Gruppe G ist Normalteiler in G.
4. Ist G abelsch, so ist jede Untergruppe Normalteiler; die Umkehrung gilt nicht.
5. Ist U eine Untergruppe von G mit $(G : U) = 2$, so ist U Normalteiler in G:
   Sei $g \in G$. Gilt $g \in U$, so folgt $gU = U = Ug$. Gilt aber $g \notin U$, so ist $G = U \cup gU$ und $U \cap gU = \emptyset$, da U den Index 2 hat, und es ergibt sich $gU = G \setminus U$. Entsprechend folgt $Ug = G \setminus U$, also $gU = Ug$.
6. 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 $\det : \mathrm{GL}(n; K) \longrightarrow K^\times$.
7. Für jedes $n \in \mathbb{N}$ ist $\mathrm{sgn} : \mathbf{S}_n \longrightarrow \{1, -1\}, \sigma \longmapsto \mathrm{sgn}\sigma$ ein Gruppenhomomorphismus. Der Kern heißt alternierende Gruppe und wird mit $\mathbf{A}_n$ bezeichnet; $\mathbf{A}_n$ ist Normalteiler in $\mathbf{S}_n$ und besteht aus den geraden Permutationen von $\mathbf{S}_n$.
8. Wie das Beispiel nach Definition 2.3 zeigt, ist in der Gruppe $G = \mathbf{S}_3 = \mathrm{D}_3$ die Untergruppe $U = \langle\tau\rangle$ kein Normalteiler.

Satz 3.6 *Ist G eine Gruppe und N ein Normalteiler in G, 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, $a^{-1}N$ ist das inverse Element von aN, und φ ein Homomorphismus, denn für alle $a, b \in G$ gilt

$$\varphi(ab) = abN = aN \cdot bN = \varphi(a)\varphi(b).$$

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 aus

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

□

Bemerkung.

1. In Satz 3.6 wird die Normalteilereigenschaft von N lediglich zum Nachweis der Wohldefiniertheit gebraucht.
2. Satz 3.6 besagt insbesondere, daß jeder Normalteiler der Kern eines Gruppenhomomorphismus ist.
3. In G/N schreibt man auch $\overline{a}$ statt aN für alle $a \in G$.
4. Ist G abelsch, so auch G/N.
5. Ist $G = \langle a \rangle$ zyklisch, so auch G/N, denn es gilt $G/N = \langle \overline{a} \rangle$.

Definition 3.7 *Ist G eine Gruppe und N ein Normalteiler, so heißt G/N bezüglich der in Satz 3.6 angegebenen Verknüpfung Faktorgruppe von G nach N, und φ heißt zugehöriger kanonischer Homomorphismus.*

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 3.8 (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 $\varphi(a) = \varphi(a'n) = \varphi(a')\varphi(n) = \varphi(a')e_H = \varphi(a')$. 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 3.2 ergibt sich die Injektivität von ψ aus

$$\begin{aligned} a\text{Kern}\varphi \in \text{Kern}\psi &\iff \psi(a\text{Kern}\varphi) = e_H \\ &\iff \varphi(a) = e_H \\ &\iff a \in \text{Kern}\varphi \\ &\iff a\text{Kern}\varphi = \text{Kern}\varphi. \end{aligned}$$

Somit besteht 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, denn zu jedem $x \in H$ existiert ein $a \in G$ mit $\varphi(a) = x$, also $\psi(a\text{Kern}\varphi) = x$.

□

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 $G/\{e\} \cong G$.
3. Bis auf Isomorphie ist $\{G/N \mid N \text{ ist Normalteiler in } G\}$ die Gesamtheit der homomorphen Bilder von 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. 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 $\text{Kern}\varphi = \{0\}$, also
$$\langle a\rangle \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}.$$
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 zu jedem $n \in \mathbb{N} \cup \{\infty\}$ genau eine zyklische Gruppe der Ordnung n, die für $n \in \mathbb{N}$ als multiplikative Gruppe mit $\mathcal{Z}_n$ bezeichnet wird. Insbesondere gibt es also für jede Primzahl p (bis auf Isomorphie) genau eine Gruppe der Ordnung p.

Satz 3.9 (1. Isomorphiesatz) *Ist G eine Gruppe, U eine Untergruppe von G und N ein Normalteiler in G, dann ist UN mit*

$$UN = \{un \mid u \in U \text{ und } n \in N\}$$

eine Untergruppe von G sowie $U \cap N$ ein Normalteiler in U und

$$\varphi : U/(U \cap N) \longrightarrow UN/N,\ u(U \cap N) \longmapsto uN$$

ein Gruppenisomorphismus.

Beweis. Wir zeigen zunächst, daß UN eine Untergruppe von G ist. Da U und N nicht leer sind, ist auch UN nicht leer. Sind weiterhin $g, h \in UN$, also $g = un$ und $h = vm$ mit $u, v \in U$ und $n, m \in N$, dann folgt

$$gh^{-1} = unm^{-1}v^{-1} = uv^{-1}vnm^{-1}v^{-1} \in UvNv^{-1} = UN,$$

da N ein Normalteiler ist. Als Normalteiler in G ist N auch ein Normalteiler in UN, und

$$\psi : U \longrightarrow UN/N,\ u \longmapsto uN$$

ist ein Gruppenhomomorphismus mit dem Kern $U \cap N$. Da

$$\psi(u) = uN = unN$$

für alle $u \in U, n \in N$ gilt, ist ψ surjektiv, und wegen des Homomorphiesatzes ist

$$\varphi : U/(U \cap N) \longrightarrow UN/N,\ u(U \cap N) \longmapsto uN$$

ein Gruppenisomorphismus.

□

Beispiel. Gegeben sind die beiden Gruppen G_1 und G_2 sowie ihr direktes Produkt $G = G_1 \times G_2$. Wir betrachten die surjektiven Gruppenhomomorphismen

$$\pi_1 :\ G = G_1 \times G_2 \longrightarrow G_1,\ (g_1, g_2) \longmapsto g_1,$$
$$\pi_2 :\ G = G_1 \times G_2 \longrightarrow G_2,\ (g_1, g_2) \longmapsto g_2.$$

Offenbar gilt

$$\text{Kern}\pi_1 = U_2 \cong G_2 \text{ und } \text{Kern}\pi_2 = U_1 \cong G_1$$

wobei

$$U_1 = \{(g_1, e_2) \mid g_1 \in G_1\} \text{ und } U_2 = \{(e_1, g_2) \mid g_2 \in G_2\}.$$

Damit sind U_1 und U_2 insbesondere Normalteiler in G. Wegen $G = U_1U_2$ und $U_1 \cap U_2 = \{e\}$ ergibt sich mit dem 1. Isomorphiesatz

$$G_1 \cong U_1 \cong U_1/\{e\} = U_1/(U_1 \cap U_2) \cong U_1U_2/U_2 = G/U_2,$$
$$G_2 \cong U_2 \cong U_2/\{e\} = U_2/(U_2 \cap U_1) \cong U_2U_1/U_1 = G/U_1.$$

Definition 3.10 *Ist G eine Gruppe und sind $U_1, \ldots, U_n$ Untergruppen von G, so heißt G (inneres) direktes Produkt der Untergruppen $U_1, \ldots, U_n$, wenn*

$$\varphi : U_1 \times \cdots \times U_n \longrightarrow G,\ (u_1, \ldots, u_n) \longmapsto u_1 \cdot \ \ldots \ \cdot u_n$$

ein Gruppenisomorphismus ist.

Bemerkung.

1. Ist die Gruppe G das (innere) direkte Produkt der Untergruppen U und V und ist U das (innere) direkte Produkt der Untergruppen $U_1, \ldots, U_n$ sowie V das (innere) direkte Produkt der Untergruppen $V_1, \ldots, V_m$, dann ist G das (innere) direkte Produkt der Untergruppen $U_1, \ldots, U_n, V_1, \ldots, V_m$. Um das einzusehen, müssen nur die beiden Isomorphismen

$$\begin{array}{ccccc} U_1 \times \cdots \times U_n \times V_1 \times \cdots \times V_m & \longrightarrow & U \times V & \longrightarrow & G \\ (u_1, \ldots, u_n, v_1, \ldots, v_m) & \longmapsto & (u_1 \ldots u_n, v_1 \ldots v_m) & \longmapsto & u_1 \ldots u_n \cdot v_1 \ldots v_m \end{array}$$

   betrachtet werden. Wir beschäftigen uns daher im folgenden nur mit dem (inneren) direkten Produkt von zwei Untergruppen; der allgemeine Fall läßt sich dann hieraus mit obiger Überlegung leicht durch Induktion ableiten.

2. Wie das Beispiel vor Definition 3.10 zeigt, ist jedes "äußere" direkte Produkt in natürlicher Weise auch ein inneres direktes Produkt, denn mit den Bezeichnungen aus dem Beispiel ist

$$U_1 \times U_2 \longrightarrow G,\ (u_1, u_2) \longmapsto u_1 u_2$$

   ein Gruppenisomorphismus. Da auch jedes innere direkte Produkt kanonisch isomorph zu einem "äußeren" direkten Produkt ist, wollen wir im folgenden nicht mehr zwischen inneren und "äußeren" direkten Produkten unterscheiden, sondern wir schreiben stets $G = U_1 \times \cdots \times U_n$ sowohl für das innere als auch das "äußere" direkte Produkt. Aus dem Zusammenhang geht dann hervor, was gemeint ist.

Satz 3.11 *Ist G eine Gruppe mit den Untergruppen U und V, dann sind die folgenden Aussagen äquivalent.*

1. *G ist das direkte Produkt von U und V, d.h. $G = U \times V$.*
2. *U und V sind Normalteiler in G, und es gilt $U \cap V = \{e\}$ sowie $UV = G$.*
3. *Es gilt $U \cap V = \{e\}$ sowie $UV = G$ und $uv = vu$ für alle $u \in U, v \in V$.*
4. *Jedes $g \in G$ läßt sich eindeutig in der Form $g = uv$ mit $u \in U, v \in V$ schreiben, und $uv = vu$ gilt für alle $u \in U, v \in V$.*

Beweis. 1) $\Longrightarrow$ 2): Sei $\varphi : U \times V \longrightarrow G,\ (u,v) \longmapsto uv$ ein Isomorphismus. Dann gilt $UV = G$, da φ surjektiv ist. Um $U \cap V = \{e\}$ zu zeigen, nehmen wir an, g liegt im Schnitt $U \cap V$, also $(g^{-1}, g) \in U \times V$ mit $\varphi((g^{-1}, g)) = g^{-1}g = e$. Da φ injektiv ist, folgt $(g^{-1}, g) = (e, e)$, also $g = e$ und $U \cap V = \{e\}$. Schließlich hat der Homomorphismus

$$G \xrightarrow{\varphi^{-1}} U \times V \xrightarrow{\pi_1} U,\ uv \longmapsto (u,v) \longmapsto u$$

den Kern V, d.h., V ist ein Normalteiler in G. Entsprechend folgt, daß auch U Normalteiler in G ist.

2) $\Longrightarrow$ 3): Zu zeigen ist nur $uv = vu$ für alle $u \in U, v \in V$. Da U Normalteiler in G ist, gilt $uvu^{-1}v^{-1} = u(vu^{-1}v^{-1}) \in UvUv^{-1} = U$, und $uvu^{-1}v^{-1} = (uvu^{-1})v^{-1} \in uVu^{-1}V = V$, da V Normalteiler ist, d.h. $uvu^{-1}v^{-1} \in U \cap V = \{e\}$. Also folgt $uv = vu$.

3) $\Longrightarrow$ 4): Wegen $G = UV$ läßt sich jedes $g \in G$ in der Form $g = uv$ mit $u \in U, v \in V$ schreiben, und gilt $uv = u'v'$ mit $u, u' \in U, v, v' \in V$, so folgt $u'^{-1}u = v'v^{-1} \in U \cap V = \{e\}$, also $u = u', v = v'$.

4) $\Longrightarrow$ 1): Da sich jedes $g \in G$ eindeutig als $g = uv$ mit $u \in U, v \in V$ schreiben läßt, ist

$$\varphi : U \times V \longrightarrow G,\ (u,v) \longmapsto uv$$

eine Bijektion. Für alle $u, u' \in U$ und $v, v' \in V$ folgt

$$\varphi((u,v)(u',v')) = \varphi((uu', vv')) = uu'vv' = uvu'v' = \varphi((u,v))\varphi((u',v')).$$

Damit ist φ ein Homomorphismus.

□

Bemerkung. Sind U, V Untergruppen der endlichen Gruppe G mit $U \cap V = \{e\}$ und $|U||V| = |G|$, so folgt $UV = G$, denn wegen $U \cap V = \{e\}$ gilt $|UV| = |U||V|$ (vergleiche Aufgabe 5.9).

Beispiel. Sind $n, m \in \mathbb{N}$ teilerfremd, so gilt

$$\mathcal{Z}_{nm} = \mathcal{Z}_n \times \mathcal{Z}_m.$$

Ist nämlich $\mathcal{Z}_{nm} = \langle a \rangle$, so hat a^n die Ordnung m und a^m die Ordnung n. Wählen wir $U = \langle a^n \rangle$ und $V = \langle a^m \rangle$, so sind $|U|$ und $|V|$ teilerfremd. Wegen Folgerung 4 aus dem Satz von Lagrange ist $U \cap V = \{e\}$. Aus obiger Bemerkung ergibt sich weiterhin $UV = G$, weil $|U||V| = |G|$. Die Elemente aus U und V vertauschen miteinander, da G abelsch ist, so daß schließlich mit Satz 3.11

$$\langle a \rangle = \langle a^n \rangle \times \langle a^m \rangle$$

folgt. Fassen wir das direkte Produkt als inneres direktes Produkt auf, so läßt sich jedes $g \in \langle a \rangle$ eindeutig in der Form $g = uv$ mit $u \in U$ und $v \in V$ schreiben. Fassen wir das direkte Produkt als "äußeres" direktes Produkt auf, so ist $\langle a^n \rangle \times \langle a^m \rangle$ zyklisch und hat zum Beispiel (a^n, a^m) als erzeugendes Element.

4. Die Sylowschen Sätze

Definition 4.1 *Es sei G eine Gruppe und X eine nichtleere Menge. Dann operiert G auf X, wenn es eine Abbildung*

$$G \times X \longrightarrow X,\ (g,x) \longmapsto g \circ x$$

mit folgenden Eigenschaften gibt:

i) $(gh) \circ x = g \circ (h \circ x)$ *für alle* $g, h \in G$ *und* $x \in X$.

ii) $e \circ x = x$ *für alle* $x \in X$.

Bemerkung.

1. Eine Gruppe G kann auf verschiedene Weise auf einer nichtleeren Menge X operieren.
2. Jede Operation von G auf einer nichtleeren Menge X entspricht einem Gruppenhomomorphismus $\varphi : G \longrightarrow \mathbf{S}_X$, wobei $\mathbf{S}_X$ die Gruppe der Bijektionen von X ist.
3. Operiert G auf X, so schreibt man auch einfach gx statt $g \circ x$.

Beispiel.

1. Ist G eine Gruppe und X eine nichtleere Menge, so heißt

   $$G \times X \longrightarrow X,\ (g,x) \longmapsto x$$

   triviale Operation. Im Sinne von Bemerkung 2 entspricht die triviale Operation dem trivialen Homomorphismus $\varphi : G \longrightarrow \mathbf{S}_X,\ g \longrightarrow \mathrm{id}_X$.

2. Ist K ein Körper und V ein K-Vektorraum, so operiert $K^\times$ auf V durch

   $$K^\times \times V \longrightarrow V,\ (k,v) \longmapsto kv.$$

3. Ist G eine Gruppe und X die Menge aller Untergruppen von G, so operiert G auf X durch Konjugation:

   $$G \times X \longrightarrow X,\ (g,U) \longmapsto gUg^{-1}.$$

   Man nennt die Untergruppen U und gUg^{-1} konjugiert.

4. Ist K ein Körper und V ein K-Vektorraum, dann operiert die Gruppe $\mathrm{Aut}_K(V)$ der Vektorraumautomorphismen auf V durch

   $$\mathrm{Aut}_K(V) \times V \longrightarrow V,\ (\varphi, v) \longrightarrow \varphi(v).$$

Definition 4.2 *Die Gruppe G operiere auf der nichtleeren Menge X. Für jedes $x \in X$ heißt*

$$G \circ x := \{g \circ x \mid g \in G\}$$

Bahn (oder Orbit) von x, und x heißt Fixpunkt, wenn $G \circ x = \{x\}$.

Bemerkung.

1. Man schreibt auch Gx statt $G \circ x$.

2. Die Menge aller Fixpunkte wird mit $\mathrm{Fix}_G(X)$ bezeichnet.

Beispiel.

1. K sei ein Körper und V ein K-Vektorraum. $K^\times$ operiere auf V durch $k \circ v := kv$. Wegen $K^\times \circ \mathcal{O} = \{\mathcal{O}\}$ ist $\mathcal{O}$ ein Fixpunkt. Für $v \neq \mathcal{O}$ folgt $K^\times \circ v = [v] \setminus \{\mathcal{O}\}$. Ist also $K = \mathbb{Z}_2$, so ist jeder Vektor aus V ein Fixpunkt. Ist aber $K \neq \mathbb{Z}_2$, so ist $\mathcal{O}$ der einzige Fixpunkt.

2. Die Gruppe G operiere auf der Menge aller Untergruppen von G durch Konjugation. Die Untergruppe U ist genau dann Fixpunkt, wenn $g \circ U = U$, also $gUg^{-1} = U$ für alle $g \in G$ gilt. Bei dieser Operation sind also genau die Normalteiler Fixpunkte.

Satz 4.3 *Die Gruppe G operiere auf der nichtleeren Menge X. Dann ist X die disjunkte Vereinigung ihrer Bahnen:*

$$X = \bigcup Gx \quad (\textit{disjunkt}).$$

Ist X endlich, so gilt

$$|X| = \sum |Gx|,$$

wobei über die verschiedenen Bahnen von X summiert wird.

Beweis. Wegen $x = ex \in Gx$ für alle $x \in X$ ist die Menge X Vereinigung ihrer Bahnen. Zu zeigen bleibt die Disjunktheit, d.h. $Gx = Gy$ falls $Gx \cap Gy \neq \emptyset$ für alle $x, y \in X$. Sei also $Gx \cap Gy \neq \emptyset$ und $gx = hy$ mit $g, h \in G$. Für jedes a in G folgt $ax = ag^{-1}hy \in Gy$, d.h. $Gx \subseteq Gy$. Entsprechend folgt $Gy \subseteq Gx$, also $Gx = Gy$.
Die zweite Behauptung des Satzes folgt unmittelbar aus der ersten.

□

Definition 4.4 *Die Gruppe G operiere auf der nichtleeren Menge X. Für jedes $x \in X$ heißt*

$$G_x := \{g \in G \mid gx = x\}$$

Stabilisator von x in G.

Satz 4.5 *Die Gruppe G operiere auf der nichtleeren Menge X. Für jedes $x \in X$ ist der Stabilisator G_x eine Untergruppe von G mit $|Gx| = (G : G_x)$.*

Beweis. Wir beweisen zunächst, daß G_x Untergruppe von G ist. Wegen $ex = x$ gilt $e \in G_x$, d.h., G_x ist nicht leer. Seien nun $a, b \in G_x$, also $ax = x$ und $bx = x$. Dann folgt $x = b^{-1}x$ und $ab^{-1}x = ax = x$, d.h. $ab^{-1} \in G_x$.
Für den Nachweis von $|Gx| = (G : G_x)$ zeigen wir, daß die folgende Zuordnung bijektiv ist:

$$\varphi : Gx \longrightarrow G/G_x,\ gx \longmapsto gG_x.$$

φ ist wohldefiniert: Sei $gx = hx$ mit $g, h \in G$. Dann ergibt sich $h^{-1}gx = x$, also $h^{-1}g \in G_x$. Somit ist $g \in hG_x$ und $gG_x = hG_x$.
φ ist injektiv: Sind $g, h \in G$ mit $gG_x = hG_x$, dann folgt $h^{-1}g \in G_x$, also $h^{-1}gx = x$ und somit $gx = hx$.
φ ist surjektiv: Für jedes gG_x mit $g \in G$ gilt $\varphi(gx) = gG_x$.

□

Korollar 4.6 *Operiert die endliche Gruppe G auf der nichtleeren Menge X, so ist $|Gx|$ ein Teiler der Gruppenordnung $|G|$ für jedes $x \in X$.*

Beweis. Wegen des Satzes von Lagrange ist $(G : G_x)$, also auch $|Gx|$ ein Teiler von $|G|$.

□

Satz 4.7 (Fixpunktsatz) *Es sei G eine endliche Gruppe mit $|G| = p^r$, p prim und X eine nichtleere endliche Menge. Operiert G auf X, so gilt*

$$|X| \equiv |\mathrm{Fix}_G(X)| \bmod p,$$

d.h., p teilt $|X| - |\mathrm{Fix}_G(X)|$.

Beweis. Wegen Satz 4.3 gilt

$$|X| = \sum |Gx| = \sum_{|Gx|>1} |Gx| + |\mathrm{Fix}_G(X)|.$$

Da $|Gx|$ ein Teiler von $|G| = p^r$ ist, wird $|Gx|$ für $|Gx| > 1$ von p geteilt. Daraus ergibt sich die Behauptung.

□

Korollar 4.8 *Ist G eine endliche Gruppe mit $|G| = p^r$, p prim und $r \geq 1$, so hat G ein nichttriviales Zentrum, d.h. $|\mathrm{Z}(G)| > 1$.*

Beweis. Die Gruppe G operiert auf $X := G \setminus \{e\}$ durch Konjugation, also

$$gx := gxg^{-1},\ g \in G.$$

Ein Element $x \in X$ ist genau dann Fixpunkt, wenn $gxg^{-1} = x$ für alle $g \in G$ gilt, wenn x also im Zentrum von G liegt. Das Korollar ist damit bewiesen, wenn $\mathrm{Fix}_G(X) \neq \emptyset$ gezeigt

ist. Wäre $\mathrm{Fix}_G(X)$ leer, so wäre $|\mathrm{Fix}_G(X)| = 0$ und p im Widerspruch zum Fixpunktsatz kein Teiler von $|X| - |\mathrm{Fix}_G(X)| = |X| = p^r - 1$.

□

Anwendung. Wir zeigen nun mit Hilfe von Korollar 4.8, daß es für jede Primzahl p bis auf Isomorphie genau zwei Gruppen der Ordnung p^2 gibt, nämlich $\mathcal{Z}_p \times \mathcal{Z}_p$ und $\mathcal{Z}_{p^2}$. Zunächst sind $\mathcal{Z}_p \times \mathcal{Z}_p$ und $\mathcal{Z}_{p^2}$ nicht isomorph, da $\mathcal{Z}_{p^2}$ ein Element der Ordnung p^2 hat, $\mathcal{Z}_p \times \mathcal{Z}_p$ aber nicht. Sei also G eine Gruppe der Ordnung p^2. Gibt es ein Element $g \in G$ der Ordnung p^2, so ist $G = \langle g \rangle \cong \mathcal{Z}_{p^2}$. Sei also wegen Folgerung 1 aus dem Satz von Lagrange $\mathrm{ord} g = p$ für alle $g \in G, g \neq e$. Mit Korollar 4.8 existiert $g \in \mathrm{Z}(G), g \neq e$, und wegen $|\langle g \rangle| = p$ ein $h \in G$ mit $h \notin \langle g \rangle$, also $\langle g \rangle \cap \langle h \rangle \subset \langle h \rangle$. Aufgrund des Satzes von Lagrange folgt $\langle g \rangle \cap \langle h \rangle = \{e\}$, da $|\langle h \rangle| = p$ prim. Nun liegt $\langle g \rangle$ im Zentrum von G, d.h. $uv = vu$ für alle $u \in \langle h \rangle$ und $v \in \langle g \rangle$. Schließlich zeigt die Bemerkung nach Satz 3.11, daß $\langle h \rangle \langle g \rangle = G$ gilt, da $|\langle h \rangle||\langle g \rangle| = p^2 = |G|$. Damit ist Bedingung 3 von Satz 3.11 nachgewiesen, d.h. $G = \langle h \rangle \times \langle g \rangle \cong \mathcal{Z}_p \times \mathcal{Z}_p$.

Ist $p = 2$, also $|G| = 4$, und ist G nicht zyklisch, also $G \cong \mathcal{Z}_2 \times \mathcal{Z}_2$, so heißt G Kleinsche Vierergruppe, und man schreibt $G \cong \mathfrak{V}_4$.

Satz 4.9 (1. Sylowscher Satz) *Ist G eine endliche Gruppe mit $|G| = p^r m$ und p eine Primzahl, die $m \in \mathbb{N}$ nicht teilt, dann gibt es für jedes $s \in \{1, 2, \ldots, r\}$ eine Untergruppe U von G mit $|U| = p^s$.*

Beweis. Sei $n = p^r m$ und $s \in \{1, 2, \ldots, r\}$. Wir zeigen zunächst

$(*)$ $\qquad p^{r+1-s}$ teilt $\binom{n}{p^s}$ nicht.

Wegen

$$\binom{n}{p^s} = \frac{n!}{p^s!(n-p^s)!} = \frac{n}{p^s}\binom{n-1}{p^s-1} = p^{r-s}m\binom{n-1}{p^s-1}$$

bleibt zu zeigen, daß p kein Teiler von $\binom{n-1}{p^s-1}$ ist. Dazu schreiben wir

$$\binom{n-1}{p^s-1} = \prod_{i=1}^{p^s-1} \frac{n-i}{i} = \prod_{i=1}^{p^s-1} \frac{a_i}{b_i},$$

wobei $\frac{n-i}{i} = \frac{a_i}{b_i}$ und $a_i, b_i \in \mathbb{N}$ teilerfremd sind. Wir überlegen uns nun, daß p weder a_i noch b_i teilt, womit dann schließlich $(*)$ gezeigt ist. Ist p^j die größte p-Potenz, die i teilt, dann gilt $p^j \leq i \leq p^s - 1 < p^s \leq p^r$, d.h. $j < r$. Somit ist p ein Teiler von $\frac{n}{p^j} = p^{r-j}m$, aber kein Teiler von $\frac{i}{p^j}$, also auch kein Teiler von $\frac{n-i}{p^j}$.

Wir beweisen jetzt Satz 4.9. Sei X die Menge der p^s-elementigen Teilmengen von G, d.h.

$$X = \{T \mid T \subseteq G \text{ und } |T| = p^s\}.$$

Dann gilt $|X| = \binom{n}{p^s}$, und G operiert auf X durch

$$g \circ T := \{gt \mid t \in T\},\ g \in G, T \in X.$$

Wegen Satz 4.3 gilt

$$\binom{n}{p^s} = |X| = \sum |G \circ T|,$$

wobei über alle Bahnen in X summiert wird. Aus $(*)$ folgt nun, daß es ein $T \subseteq G$ gibt mit $|T| = p^s$ und p^{r+1-s} teilt $|G \circ T|$ nicht. Wegen Satz 4.5 ist p^{r+1-s} für dieses T auch kein Teiler von $(G : G_T)$, wobei G_T der Stabilisator von T ist. Damit kommt p in $(G : G_T)$ höchstens $(r-s)$-mal als Primteiler vor und in $|G_T|$ mindestens s-mal, da

$$p^r m = |G| = (G : G_T) \cdot |G_T|.$$

Wir erhalten $|G_T| \geq p^s$ und zeigen $|G_T| \leq p^s$. Dann folgt $|G_T| = p^s$, und wir können $U = G_T$ setzen. Weil G_T der Stabilisator von T ist, gilt $G_T \circ T = T$, also $gt \in T$ für alle $g \in G_T$ und $t \in T$, d.h

$$G_T t = \{gt \mid g \in G_T\} \subseteq T,\ t \in T.$$

Es folgt $|G_T| = |G_T t| \leq |T| = p^s$.

□

Korollar 4.10 (Satz von Cauchy) *Ist G eine endliche Gruppe und p ein Primteiler von $|G|$, dann gibt es ein $g \in G$ mit* ord$g = p$.

Beweis. Wegen Satz 4.9 gibt es eine Untergruppe U von G mit $|U| = p$. Jedes $g \in U, g \neq e$ hat die Ordnung p.

□

Beispiel. Wir zeigen, daß es zu jeder Primzahl $p > 2$ bis auf Isomorphie genau zwei Gruppen der Ordnung $2p$ gibt, nämlich $\mathcal{Z}_{2p}$ und die Diedergruppe D_p. Zunächst sind $\mathcal{Z}_{2p}$ und D_p nicht isomorph, da $\mathcal{Z}_{2p}$ abelsch ist, D_p aber nicht. Sei nun G eine Gruppe mit $|G| = 2p$. Wegen des Satzes von Cauchy gibt es $a, b \in G$ mit ord$a = 2 < p =$ ord$b$, also $\langle a \rangle \cap \langle b \rangle = \{e\}$. Es folgt $|\langle a \rangle \langle b \rangle| = |\langle a \rangle||\langle b \rangle| = 2p = |G|$ und somit $G = \langle a \rangle \langle b \rangle$. Weil $\langle b \rangle$ den Index 2 hat, ist $\langle b \rangle$ Normalteiler in G, d.h.

$$a^{-1}ba = b^k \text{ für ein } k \in \{0, 1, \ldots, p-1\}.$$

Die Verknüpfung von G ist damit eindeutig durch k bestimmt. Aus

$$b = a^{-2}ba^2 = a^{-1}(a^{-1}ba)a = a^{-1}b^k a = b^{k^2}$$

ergibt sich $b^{k^2-1} = e$, d.h., die Ordnung p von b teilt $k^2 - 1 = (k-1)(k+1)$. Ist p Teiler von $k+1$, so ist $k = p-1$, also G nicht abelsch, und ist p Teiler von $k-1$, so ist $k = 1$, also G abelsch. Es gibt demnach bis auf Isomorphie höchstens zwei Gruppen der Ordnung $2p$, und damit ist die Behauptung gezeigt.

Definition 4.11 *G sei eine endliche Gruppe mit $|G| = p^r m$ und p eine Primzahl, die $m \in \mathbb{N}$ nicht teilt. Jede Untergruppe U von G mit $|U| = p^r$ heißt p-Sylowgruppe von G.*

Satz 4.12 (2. Sylowscher Satz) *G sei eine endliche Gruppe mit $|G| = p^r m$ und p eine Primzahl, die $m \in \mathbb{N}$ nicht teilt. Ist U eine Untergruppe von G mit $|U| = p^s, s \in \mathbb{N}$, dann ist U in einer p-Sylowgruppe von G enthalten, und zwei p-Sylowgruppen von G sind konjugiert.*

Beweis. Wegen Satz 4.9 gibt es eine p-Sylowgruppe P von G. Wir zeigen

$$(*) \qquad U \subseteq gPg^{-1} \text{ für ein } g \in G.$$

Da gPg^{-1} ebenfalls eine Untergruppe von G mit $|gPg^{-1}| = p^r$ ist, ist auch gPg^{-1}eine p-Sylowgruppe von G, und damit die erste Behauptung des Satzes bewiesen. Um die zweite Behauptung des Satzes zu erhalten, wählen wir U als eine p-Sylowgruppe von G, und wegen $|U| = |gPg^{-1}|$ folgt $U = gPg^{-1}$ aus $U \subseteq gPg^{-1}$.
Wir zeigen nun $(*)$. Sei $X = G/P = \{gP \mid g \in G\}$ die Menge der Linksnebenklassen von P. Dann operiert U auf X durch

$$u \circ gP := ugP, \ u \in U.$$

Wegen Satz 4.3 folgt

$$|G/P| = |X| = \sum |U \circ gP|,$$

wobei über die Menge aller Bahnen $U \circ gP$ summiert wird. p ist kein Teiler von $|X|$, da

$$|G/P| = (G : P) = \frac{|G|}{|P|} = \frac{p^r m}{p^r} = m,$$

d.h., es gibt mindestens eine Bahn $U \circ gP$, so daß $|U \circ gP|$ nicht von p geteilt wird. Aufgrund von Satz 4.5 gilt $|U \circ gP| = (U : U_{gP})$, wobei U_{gP} der Stabilisator von gP ist, und $|U \circ gP|$ teilt $|U| = p^s$. Also folgt $|U \circ gP| = 1$. Für alle $u \in U$ ergibt sich damit

$$ugP = u \circ gP = gP, \text{ d.h. } g^{-1}ugP = P.$$

Somit gilt $g^{-1}ug \in P$ für alle $u \in U$, also $g^{-1}Ug \subseteq P$ und $U \subseteq gPg^{-1}$.

□

Satz 4.13 (3. Sylowscher Satz) *G sei eine endliche Gruppe und p ein Primteiler von $|G|$. Dann gilt:*

1. *Die Anzahl der p-Sylowgruppen teilt $|G|$.*
2. *Die Anzahl der p-Sylowgruppen ist kongruent* 1 mod p.

Beweis. Sei X die Menge der p-Sylowgruppen von G. Um 1) zu zeigen, lassen wir G auf X durch Konjugation operieren, d.h.

$$g \circ P := gPg^{-1} \text{ für alle } g \in G \text{ und } P \in X.$$

Wegen Satz 4.12 sind die p-Sylowgruppen konjugiert, d.h. $G \circ P = X$ für alle $P \in X$. Ist $P \in X$, so folgt

$$|X| = |G \circ P| = (G : G_P),$$

wobei G_P der Stabilisator von P ist. Wegen des Satzes von Lagrange ist aber $(G : G_P)$ ein Teiler von $|G|$. Um 2) zu zeigen, wählen wir eine p-Sylowgruppe P und lassen sie ebenfalls auf X durch Konjugation operieren. Dann ist $P \in X$, und wegen $gPg^{-1} = P$ für alle $g \in P$ ist P ein Fixpunkt. Wir beweisen nun, daß P der einzige Fixpunkt ist, d.h., wir zeigen

$(*)$ Ist $U \neq P$ eine p-Sylowgruppe von G, so gilt $gUg^{-1} \neq U$ für mindestens ein $g \in P$.

Wäre $gUg^{-1} = U$ für alle $g \in P$, so wäre $PU = UP$ und PU eine Untergruppe von G, die P echt umfaßt (vgl. Aufgabe 5.9). Wegen

$$|P| < |PU| = \frac{|P||U|}{|P \cap U|}$$

ist aber $|PU|$ eine p-Potenz, die $|G|$ teilt, im Widerspruch dazu, daß $|P|$ die größte p-Potenz ist, die $|G|$ teilt. Damit ist $(*)$ gezeigt.
Für jede von P verschiedene p-Sylowgruppe U gilt also $|P \circ U| > 1$, und wegen $|P \circ U| = (P : P_U)$ ist $|P \circ U|$ als Teiler von $|P|$ eine p-Potenz (dabei ist P_U der Stabilisator von U). In der Darstellung

$$|X| = \sum |P \circ U|$$

aus Satz 4.3 ist genau ein Summand 1, nämlich $|P \circ P|$, und alle anderen sind durch p teilbar. □

Anwendung. Es seien p und q zwei Primzahlen mit $p < q$ und $q \not\equiv 1 \bmod p$. Dann ist $\mathcal{Z}_{pq}$ bis auf Isomorphie die einzige Gruppe der Ordnung pq. Zum Beispiel sind $\mathcal{Z}_{15}$ und $\mathcal{Z}_{35}$ die einzigen Gruppen der Ordnung 15 bzw. 35.
Sei G eine Gruppe mit $|G| = pq$ und U eine p-Sylowgruppe von G, also $|U| = p$, und V eine q-Sylowgruppe von G, also $|V| = q$. Weil p und q Primzahlen sind, folgt $U \cong \mathcal{Z}_p$ und $V \cong \mathcal{Z}_q$. Der einzige Teiler von pq, der bei Division durch p den Rest 1 läßt, ist 1. Wegen Satz 4.13 ist damit U die einzige p-Sylowgruppe von G und damit insbesondere Normalteiler in G. Entsprechend folgt, daß V die einzige q-Sylowgruppe von G ist, und auch V ist Normalteiler. Da $|U|$ und $|V|$ teilerfremd sind, gilt $U \cap V = \{e\}$, also $|UV| = pq = |G|$, d.h. $G = UV$. Wir können nun Satz 3.11 anwenden, und erhalten

$$G \cong U \times V \cong \mathcal{Z}_p \times \mathcal{Z}_q \cong \mathcal{Z}_{pq}.$$

5. Aufgaben

A 5.1 Untersuchen Sie, ob die folgenden Mengen G bezüglich $\circ$ Gruppen sind.

1. $G = \mathbb{Q} \setminus \{-1\}$ und $a \circ b := a + b + ab$ für alle $a, b \in G$.
2. $G = \mathbb{Q} \times \mathbb{Q} \setminus \{(0,0)\}$ und $(a,b) \circ (c,d) := (ac + 2bd, ad + bc)$ für alle $(a,b), (c,d) \in G$.
3. $G = \mathbb{R}$ und $a \circ b := a + b + 2$ für alle $a, b \in G$.

A 5.2 Es sei G eine nichtleere Menge mit einer assoziativen Verknüpfung $\circ$. Zeigen Sie, daß folgende Aussagen äquivalent sind:

1. G ist ein Gruppe bezüglich $\circ$.
2. Es gibt ein $e \in G$, so daß $e \circ g = g$ für alle $g \in G$ gilt und es zu jedem $g \in G$ ein $h \in G$ gibt mit $h \circ g = e$.
3. Es gibt ein $e \in G$, so daß $g \circ e = g$ für alle $g \in G$ gilt und es zu jedem $g \in G$ ein $h \in G$ gibt mit $g \circ h = e$.
4. Für alle $g, h \in G$ gibt es $x, y \in G$ mit $g \circ x = h$ und $y \circ g = h$.

A 5.3 Sei G eine Gruppe und $a, b \in G$ Gruppenelemente endlicher Ordnung. Zeigen Sie:

1. Gilt $ab = ba$ und sind $\mathrm{ord}a, \mathrm{ord}b$ teilerfremd, so folgt $\mathrm{ord}(ab) = \mathrm{ord}a \cdot \mathrm{ord}b$.
2. In 1. kann auf die Voraussetzung $ab = ba$ nicht verzichtet werden.
3. Für alle $k \in \mathbb{N}$ gilt $\mathrm{ord}a^k = \frac{\mathrm{ord}a}{\mathrm{ggT}(k, \mathrm{ord}a)}$.

A 5.4 Es 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 5.5 Sei G eine Gruppe und $a, b \in G$. Zeigen Sie: Gilt für drei aufeinanderfolgende natürliche Zahlen k die Gleichung $(ab)^k = a^k b^k$, so folgt $ab = ba$.

A 5.6 Zeigen Sie, daß eine Gruppe nicht die Vereinigung von zwei echten Untergruppen ist.

A 5.7 Zeigen Sie: Jede Untergruppe einer zyklischen Gruppe G ist zyklisch; ist G außerdem endlich, so gibt es zu jedem Teiler d von $|G|$ genau eine Untergruppe U der Ordnung d.

A 5.8 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 $\langle a, b\rangle = d\mathbb{Z}$ 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 5.9 Ist G eine Gruppe, so definiert man $AB := \{ab \mid a \in A, b \in B\}$ für alle Teilmengen A und B von G. Zeigen Sie:

1. Sind U und V Untergruppen der Gruppe G, so ist UV genau dann Untergruppe von G, wenn $UV = VU$.
2. Sind U und V endliche Untergruppen der Gruppe G, dann gilt $|UV| \cdot |U \cap V| = |U||V|$.

A 5.10 Sei K ein Körper und $n \in \mathbb{N}$. Berechnen Sie das Zentrum $\mathrm{Z}(\mathrm{GL}(n; K))$ von $\mathrm{GL}(n; K)$.

A 5.11 Sei p eine Primzahl und G die Menge der oberen Dreiecksmatrizen (a_{ij}) aus $\mathrm{GL}(p; \mathbb{Z}_p)$ mit $a_{11} = \cdots = a_{pp} = 1$. Zeigen Sie, daß G eine Untergruppe von $\mathrm{GL}(p; \mathbb{Z}_p)$ ist und daß $A^p = \mathrm{E}_p$ für alle $A \in G$ gilt. Für welche p ist G abelsch?

A 5.12 Es sei G die von (13) und (1234) erzeugte Untergruppe von $\mathbf{S}_4$. Berechnen Sie die Ordnung von G und geben Sie das Zentrum von G an.

A 5.13 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 5.14 H und K seien Gruppen sowie $\varphi : K \longrightarrow \mathrm{Aut}(H)$ ein Gruppenhomomorphismus. Zeigen Sie, daß $H \times K$ bezüglich $(x, y)(x', y') := (x\varphi(y)(x'), yy')$ eine Gruppe ist. Sie wird mit $H \rtimes_\varphi K$ bezeichnet und heißt das durch φ definierte semidirekte Produkt von H mit K.

A 5.15 Sei G eine Gruppe mit den Untergruppen H und K, so daß H Normalteiler in G ist und $HK = G$ sowie $H \cap K = \{e\}$ gilt. Zeigen Sie, daß dann G und $H \rtimes_\varphi K$ isomorph sind, wobei $\varphi : K \longrightarrow \mathrm{Aut}(H), y \longrightarrow \mathrm{i}_y$ gilt.

A 5.16 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 5.17 Sei Q die von den Matrizen $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ und $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ erzeugte Untergruppe der $\mathrm{GL}(2; \mathbb{C})$. Berechnen Sie die Ordnung von Q und geben Sie alle Elemente sowie den Untergruppenverband und das Zentrum von Q an. Gibt es Untergruppen von Q, die keine Normalteiler sind? Ist die Gruppe Q isomorph zur Gruppe G aus Aufgabe 5.16?

A 5.18 Sei G die von den Matrizen $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ und $\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^2 \end{pmatrix}$ erzeugte Untergruppe der $\mathrm{GL}(2; \mathbb{C})$, wobei $\epsilon^3 = 1$ und $\epsilon \neq 1$ gilt. Berechnen Sie die Ordnung sowie alle p-Sylowgruppen von G. Geben Sie der Gruppe einen Namen.

A 5.19 Berechnen Sie alle Untergruppen der Diedergruppe D_4. Welche davon sind Normalteiler?

A 5.20 Die Menge aller inneren Automorphismen einer Gruppe G wird mit $\mathrm{Inn}(G)$ bezeichnet. Zeigen Sie, daß $\mathrm{Inn}(G)$ ein Normalteiler in der Automorphismengruppe $\mathrm{Aut}(G)$ von G ist und daß $\mathrm{Inn}(G) \cong G/\mathrm{Z}(G)$ gilt.

A 5.21 Ist G eine Gruppe, so heißt das Produkt $a^{-1}b^{-1}ab$ mit $a, b \in G$ Kommutator von a und b. Die von allen Kommutatoren erzeugte Untergruppe von G heißt Kommutatorgruppe von G und wird mit $\mathrm{K}(G)$ bezeichnet. Zeigen Sie, daß die Kommutatorgruppe $\mathrm{K}(G)$ von G ein Normalteiler in G ist und daß für jeden Normalteiler N von G gilt: Genau dann ist die Faktorgruppe G/N abelsch, wenn $\mathrm{K}(G) \subseteq N$. (Die Kommutatorgruppe ist also der kleinste Normalteiler von G mit abelscher Faktorgruppe.)

A 5.22 Berechnen Sie $\mathrm{K}(\mathrm{D}_4), \mathrm{Inn}(\mathrm{D}_4)$ und $\mathrm{Aut}(\mathrm{D}_4)$.

A 5.23 Sei G eine Gruppe mit den Untergruppen A, B, C. Zeigen Sie:

1. Ist A in C enthalten, so gilt $(B \cap C)A = BA \cap C$.
2. Ist A Normalteiler in B und C Normalteiler in G, dann ist CA Normalteiler in CB.

A 5.24 Sei G eine Gruppe mit den Untergruppen H, H', K, K', wobei H' Normalteiler in H und K' Normalteiler in K ist. Zeigen Sie:

1. $K'(H' \cap K)$ ist Normalteiler in $K'(H \cap K)$.
2. $K'(H \cap K)/K'(H' \cap K) \cong (H \cap K)/(H \cap K')(H' \cap K)$.

A 5.25 Beweisen Sie den 2. Isomorphiesatz: Sind N und N' Normalteiler der Gruppe G mit $N \subseteq N'$, dann ist N'/N Normalteiler in G/N und $(G/N)/(N'/N) \cong G/N'$.

A 5.26 Sei H eine Untergruppe der abelschen Gruppe G und G/H eine zyklische Gruppe unendlicher Ordnung. Zeigen Sie: Es gibt eine Untergruppe U von G so, daß G direktes Produkt von H und U ist.

A 5.27 Formulieren und beweisen Sie Satz 3.11 für direkte Produkte mit mehr als zwei Faktoren.

A 5.28 Sei $G = \mathrm{GL}(3; \mathbb{Z}_2)$. Dann gilt $|G| = 2^3 \cdot 3 \cdot 7$. Geben Sie $A, B \in G$ mit $\mathrm{ord}A = 3$ und $\mathrm{ord}B = 7$ an. Deuten Sie A und B geometrisch. Gibt es ein $C \in G$ mit $\mathrm{ord}C = 4$ oder $\mathrm{ord}C = 8$? Geben Sie eine Untergruppe der Ordnung 8 an (Diese ist isomorph zur Diedergruppe D_4).

A 5.29 Seien p und q verschiedene Primzahlen und sei G eine Gruppe der Ordnung p^2q. Zeigen Sie, daß G einen Normalteiler hat, der p- oder q-Sylowgruppe von G ist.

A 5.30 Sei G eine endliche Gruppe und p der kleinste Primteiler von $|G|$. Zeigen Sie: Ist U eine Untergruppe von G mit $(G : U) = p$, dann ist U ein Normalteiler in G.

A 5.31 Zeigen Sie: Ist G eine Gruppe mit $|G| = 105$, dann hat G einen Normalteiler N mit $|N| = 35$.

A 5.32 Geben Sie bis auf Isomorphie alle Gruppen der Ordnung 8 an.

A 5.33 Geben Sie bis auf Isomorphie alle Gruppen der Ordnung 12 an.

A 5.34 Geben Sie bis auf Isomorphie alle Gruppen an, die das Geburtsjahr von Miguel de Cervantes als Ordnung haben.

A 5.35 Geben Sie bis auf Isomorphie alle Gruppen an, die das Geburtsjahr von Katharina der Großen als Ordnung haben.

A 5.36 Sei G eine endliche Gruppe und U eine Untergruppe mit $(G : U) = r$. Zeigen Sie, daß es $g_1, \ldots, g_r \in G$ gibt, die Repräsentanten sowohl für die Links- als auch für die Rechtsnebenklassen von U sind, d.h. $g_1U \cup \cdots \cup g_rU = G = Ug_1 \cup \cdots \cup Ug_r$.

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. Im folgenden sei R ein Ring mit den Verknüpfungen $+$ und $\cdot$.

1. R heißt kommutativ, wenn $a \cdot b = b \cdot a$ für alle $a, b \in R$ gilt.
2. Man nennt $+$ Addition und $\cdot$ Multiplikation.
3. *Punktrechnung geht vor Strichrechnung*, d.h., Ausdrücke der Form $a \cdot b + a \cdot c$ mit $a, b, c \in R$ sind als $(a \cdot b) + (a \cdot c)$ zu verstehen.
4. R heißt Ring mit Einselement (oder Ring mit Eins), wenn R bezüglich der Multiplikation ein neutrales Element hat. Existiert ein Einselement, so ist es eindeutig bestimmt und wird i.a. mit 1 bezeichnet; für alle $a \in R$ gilt dann $1 \cdot a = a \cdot 1 = a$.
5. Das neutrale Element der Addition wird mit 0 bezeichnet und das additive Inverse von $a \in R$ mit $-a$.
6. Man schreibt auch ab statt $a \cdot b$ und $a - b$ statt $a + (-b)$ für alle $a, b \in R$.
7. Für alle $a \in R$ und $n \in \mathbb{N}$ definiert man die Potenz a^n rekursiv durch $a^1 = a$ und $a^n = a^{n-1}a$ für alle $n > 1$; es gelten die üblichen Potenzrechengesetze. Hat R ein Einselement 1, setzt man $a^0 = 1$ für alle $a \in R$.

Beispiel.

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

2. $2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$ ist bezüglich der üblichen Addition und Multiplikation ein kommutativer Ring ohne Eins.

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

4. Sind $R_1, \ldots, R_n$ Ringe, so ist $R_1 \times \cdots \times R_n$ bezüglich der komponentenweisen Addition und Multiplikation ein Ring. Er heißt direktes Produkt der Ringe $R_1, \ldots, R_n$. Das direkte Produkt $R_1 \times \cdots \times R_n$ ist genau dann kommutativ, wenn jedes R_i kommutativ ist, und es hat genau dann ein Einselement, wenn jedes R_i ein Einselement hat.

5. Ist G eine additiv geschriebene abelsche Gruppe, dann ist

$$\mathrm{End}(G) = \{\varphi : G \longrightarrow G \mid \varphi \text{ ist ein Gruppenhomomorphismus}\}$$

bezüglich

$$\begin{aligned} \varphi + \psi : G &\longrightarrow G, \qquad g \longmapsto \varphi(g) + \psi(g), \\ \varphi \cdot \psi : G &\longrightarrow G, \qquad g \longmapsto \varphi(\psi(g)), \end{aligned}$$

ein Ring mit Einselement.

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) Ist R kommutativ, so heißt R Integritätsbereich, wenn $1 \neq 0$ und wenn für alle $a, b \in R$ gilt:
$$a, b \neq 0 \Longrightarrow ab \neq 0.$$

iii) Ist R kommutativ, so heißt R Körper, wenn $1 \neq 0$ und wenn jedes $a \in R, a \neq 0$ in R invertierbar ist.

Bemerkung.

1. Ist $a \in R$ invertierbar, so gibt ist genau ein $b \in R$ mit $ab = ba = 1$, das man mit a^{-1} bezeichnet. Man nennt a^{-1} das multiplikative Inverse von a.
2. Die Menge $\mathrm{E}(R)$ der Einheiten von R ist bezüglich der Multiplikation eine Gruppe; $\mathrm{E}(R)$ heißt Einheitengruppe von R.
3. Sind $a, b \in R$ mit $a, b \neq 0$ und $ab = 0$, so heißen a und b Nullteiler. Hat R keine Nullteiler, so nennt man R nullteilerfrei. Somit ist ein Integritätsbereich ein nullteilerfreier kommutativer Ring mit 1, wobei $1 \neq 0$.
4. Einheiten sind keine Nullteiler, denn ist $a \in R$ invertierbar und $b \in R$ mit $ab = 0$, so folgt $0 = a^{-1}ab = b$. Insbesondere ist somit jeder Körper ein Integritätsbereich.

Beispiel.

1. Bezüglich der üblichen Addition und Multiplikation sind $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ Körper.
2. $\mathbb{Z}$ ist bezüglich der üblichen Addition und Multiplikation ein Integritätsbereich, aber kein Körper; es gilt $\mathrm{E}(\mathbb{Z}) = \{1, -1\}$.

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:*

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

Ein bijektiver Ringhomomorphismus heißt Ringisomorphismus, und ein Ringisomorphismus $\varphi : R \longrightarrow R$ heißt Ringautomorphismus. Zwei Ringe R und S heißen isomorph (geschrieben $R \cong S$), wenn es einen Ringisomorphismus $\varphi : R \longrightarrow S$ gibt.

Bemerkung. Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus.

1. φ ist insbesondere ein Gruppenhomomorphismus zwischen den additiven Gruppen von R und S. Mit Kernφ bezeichnet man daher auch den Kern dieses Gruppenhomomorphismus: Kern$\varphi = \{r \in R \mid \varphi(r) = 0\}$. Insbesondere ist φ genau dann injektiv, wenn Kern$\varphi = \{0\}$.
2. Ist 1_R Einselement von R, so ist im allgemeinen $\varphi(1_R)$ kein Einselement von S.
3. Die Komposition von Ringhomomorphismen ist ein Ringhomomorphismus.
4. Ist φ ein Ringisomorphismus, so ist auch $\varphi^{-1} : S \longrightarrow R$ ein Ringisomorphismus.

Beispiel. K sei ein Körper und V ein n-dimensionaler K-Vektorraum. Dann ist der Ring $\mathrm{End}(V)$ der Endomorphismen von V isomorph zum Ring $K_{n,n}$ der (n, n)-Matrizen über K. Ordnet man bei fest gewählter Basis von V jedem $\varphi \in \mathrm{End}(V)$ die zugehörige Matrixdarstellung A_φ zu, so ist $\Theta : \mathrm{End}(V) \longrightarrow K_{n,n},\ \varphi \longmapsto A_\varphi$ ein Ringisomorphismus. Insbesondere vermittelt Θ einen Gruppenisomorphismus zwischen den Einheitengruppen $\mathrm{Aut}(V)$ und $\mathrm{GL}(n; K)$.

Satz 1.4 *Sind R, S Ringe und ist $\varphi : R \longrightarrow S$ ein Ringhomomorphismus sowie $I := \text{Kern}\varphi$, dann gilt:*

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

Beweis. Da φ bezüglich $+$ ein Gruppenhomomorphismus ist, ist I wegen Satz 3.2 aus Kapitel 1 bezüglich $+$ Untergruppe von R. Sind nun weiterhin $a \in R$ 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:*

i) I ist bezüglich $+$ Untergruppe von R.

ii) Für alle $a \in R$ und $i \in I$ gilt $ai, ia \in I$.

Bemerkung. Wegen Satz 2.2 aus Kapitel 1 ist eine nichtleere Teilmenge I eines Ringes R genau dann ein Ideal von R, wenn $i - j \in I$ und $ai, ia \in I$ für alle $i, j \in I$ und $a \in R$ gilt.

Beispiel.

1. Ist R ein Ring, dann sind $\{0\}$ und R Ideale von R; sie heißen triviale Ideale von R.
2. Der Kern eines Ringhomomorphismus $\varphi : R \longrightarrow S$ ist ein Ideal von R.
3. Ist K ein Körper und $n \in \mathbb{N}$, dann hat der Ring $K_{n,n}$ der (n, n)-Matrizen über K nur die trivialen Ideale.
4. Ist R ein kommutativer Ring mit 1 und $a \in R$, dann ist

$$aR := \{a \cdot r \mid r \in R\}$$

ein Ideal von R, das a enthält.
Beweis: Wegen $a = a \cdot 1 \in aR$, ist aR nicht leer, und es gilt $a \in aR$. Sind nun weiterhin $i, j \in aR$ und $r \in R$, also $i = as$ und $j = as'$ mit $s, s' \in R$, dann folgt $i - j = as - as' = a(s - s') \in aR$ und $ri = ir = (as)r = a(sr) \in aR$. Wegen obiger Bemerkung ist damit aR ein Ideal von R.
aR heißt das von a erzeugte Hauptideal. Ist ϵ eine Einheit in R, so gilt $aR = a\epsilon R$. Für $a = 0$ folgt $aR = \{0\}$ und $aR = R$ für $a = 1$.

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 $I = R$. Ein Körper hat somit nur die trivialen Ideale.

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. Für eine Teilmenge M von R bezeichnet $[M]$ den Durchschnitt aller Ideale von R, die M umfassen. Damit ist $[M]$ das kleinste Ideal von R, das M enthält; es heißt das von M erzeugte Ideal von R.

3. Sind $I_1, \ldots, I_n$ Ideale von R, so ist auch die Summe
$$I_1 + \cdots + I_n := \{i_1 + \cdots + i_n \mid i_j \in I_j, j = 1, \ldots, n\}$$
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. Wegen Satz 3.6 aus Kapitel 1 ist R/I insbesondere eine additive abelsche Gruppe bezüglich $(a + I) + (b + I) = (a + b) + I$.

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 $\text{Kern}\varphi = I$.

Beweis. Wegen Satz 3.6 aus Kapitel 1 ist R/I bezüglich $+$ eine abelsche Gruppe. Wir zeigen nun, daß die Multiplikation 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
$$ab + I = (a' + i)(b' + j) + I = (a'b' + a'j + ib' + ij) + I = a'b' + I,$$
weil $a'j, ib', ij \in I$. Das Assoziativgesetz der Multiplikation und die Distributivgesetze gelten offenbar. Damit ist R/I ein Ring. Wegen Satz 3.6 aus Kapitel 1 ist φ ein surjektiver Gruppenhomomorphismus mit $\text{Kern}\varphi = I$, 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. Satz 1.6 besagt insbesondere, daß jedes Ideal Kern eines Ringhomomorphismus ist.

3. Man schreibt auch $\overline{a}$ statt $a + I$ für alle $a \in R$. Mit dieser Bezeichnung gilt dann $\overline{a} + \overline{b} = \overline{a + b}$ und $\overline{a}\overline{b} = \overline{ab}$ für alle $a, b \in R$.

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

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

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 $\mathbb{Z}$ und für $n \in \mathbb{N}$ das von n erzeugte Hauptideal $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. Im Beispiel nach Definition 3.7 aus Kapitel 1 haben wir bereits die additive Gruppe

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

eingeführt. Bezüglich der in Satz 1.6 definierten Verknüpfungen ist $\mathbb{Z}_n$ ein kommutativer Ring mit dem Einselement $\overline{1}$; für alle $a, b \in \mathbb{Z}$ gilt

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

Ist $n > 1$ keine Primzahl, etwa $n = ab$ mit $a, b \in \mathbb{N}$ und $1 < a, b < n$, dann gilt $\overline{a}, \overline{b} \neq 0$, aber $\overline{a}\overline{b} = \overline{ab} = \overline{n} = \overline{0}$, d.h., $\mathbb{Z}_n$ hat Nullteiler und ist somit kein Körper. Wir werden später sehen, daß $\mathbb{Z}_p$ für primes p ein Körper ist und wie mit Hilfe des Euklidischen Algorithmus die multiplikativen Inversen berechnet werden können.

Definition 1.8 *Ist I ein Ideal eines Ringes R, dann heißt I Primideal, wenn $I \neq R$ und wenn für alle $a, b \in R$ gilt*

$$ab \in I \Longrightarrow a \in I \text{ oder } b \in I.$$

Beispiel. Wir betrachten den Ring $\mathbb{Z}$ und für $n \in \mathbb{N}$ das Hauptideal $n\mathbb{Z}$. Gilt $n = 1$, so ist $n\mathbb{Z} = \mathbb{Z}$ und damit $n\mathbb{Z}$ kein Primideal. Sei also $n > 1$. Ist n keine Primzahl, etwa $n = ab$ mit $a, b \in \mathbb{N}$ und $1 < a, b < n$, dann gilt $n = ab \in n\mathbb{Z}$, aber weder $a \in n\mathbb{Z}$ noch $b \in n\mathbb{Z}$, d.h., $n\mathbb{Z}$ ist kein Primideal. Ist aber $n = p$ prim und sind $a, b \in \mathbb{Z}$ mit $ab \in p\mathbb{Z}$, dann ist p Teiler von ab, also p Teiler von a oder Teiler von b, d.h., $a \in p\mathbb{Z}$ oder $b \in p\mathbb{Z}$. Da $p\mathbb{Z} \neq \mathbb{Z}$ auch erfüllt ist, ist $p\mathbb{Z}$ ein Primideal.

Satz 1.9 *Ist R ein kommutativer Ring mit 1 und I ein Ideal von R, dann gilt*

$$I \text{ ist ein Primideal von } R \Longleftrightarrow R/I \text{ ist ein Integritätsbereich.}$$

Beweis. $''\Longrightarrow''$: R/I ist ein kommutativer Ring mit dem Einselement $\overline{1}$. Wäre $1 + I = 0 + I$, also $\overline{1} = \overline{0}$, so wäre $1 \in I$, also $I = R$ - im Widerspruch zur Definition des Primideals. Seien nun $a, b \in R$ mit $\overline{a}\overline{b} = \overline{0}$. Dann folgt $\overline{ab} = \overline{0}$, also $ab \in I$. Weil I ein Primideal ist, ergibt sich $a \in I$ oder $b \in I$, also $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$.
$''\Longleftarrow''$: Wegen $\overline{1} \neq \overline{0}$ ist $1 + I \neq 0 + I$, d.h. $1 \notin I$ und $I \neq R$. Seien nun $a, b \in R$ mit $ab \in I$. Dann gilt $\overline{a}\overline{b} = \overline{ab} = \overline{0}$, also $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$, da R/I nullteilerfrei ist, also $a \in I$ oder $b \in I$. □

Beispiel. Wir betrachten den Ring $\mathbb{Z}$ und für $n \in \mathbb{N}$ das Hauptideal $n\mathbb{Z}$. Dann ist der Ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ genau dann ein Integritätsbereich, wenn $n = p$ eine Primzahl ist. Als endlicher Integritätsbereich ist $\mathbb{Z}_p$ dann sogar ein Körper.

Definition 1.10 *Ist I ein Ideal eines Ringes R, dann heißt I maximales Ideal, wenn $I \neq R$ und wenn es kein Ideal J von R mit $I \subset J \subset R$ gibt.*

Satz 1.11 *Ist R ein kommutativer Ring mit 1 und I ein Ideal von R, dann gilt*

$$I \text{ ist ein maximales Ideal von } R \Longleftrightarrow R/I \text{ ist ein Körper.}$$

Beweis. $''\Longrightarrow''$: R/I ist ein kommutativer Ring mit dem Einselement $\overline{1}$. Wäre $1+I = 0+I$, also $\overline{1} = \overline{0}$, so wäre $1 \in I$, also $I = R$ - im Widerspruch zur Definition des maximalen Ideals. Sei nun $\overline{a} \in R/I, \overline{a} \neq \overline{0}$. Wir zeigen, daß $\overline{a}$ in R/I invertierbar ist. Wegen $\overline{a} \neq \overline{0}$ gilt $a \notin I$, und $aR + I$ ist ein Ideal von R, das wegen $a = a \cdot 1 + 0 \in aR + I$ das Ideal I echt umfaßt. Aufgrund der Maximalität von I folgt $aR+I = R$, d.h., es gibt $r \in R$ und $i \in I$ mit $ar + i = 1$. Im Faktorring R/I bedeutet das $\overline{1} = \overline{a}\,\overline{r} + \overline{i} = \overline{a}\,\overline{r}$, d.h., $\overline{r}$ ist das multiplikative Inverse von $\overline{a}$.
$''\Longleftarrow''$: Wegen $\overline{1} \neq \overline{0}$ ist $1 + I \neq 0 + I$, d.h. $1 \notin I$ und $I \neq R$. Sei nun J ein Ideal von R mit $I \subset J$, d.h., es gibt ein $a \in J, a \notin I$. Dann ist $\overline{a} \neq \overline{0}$, und es existiert ein $b \in R$ mit $\overline{a}\,\overline{b} = \overline{1}$, weil R/I ein Körper ist. Es folgt $\overline{1 - ab} = \overline{0}$, also $1 - ab \in I \subset J$. Wegen $a \in J$ bedeutet das $1 \in J$ und $J = R$.

□

Korollar 1.12 *In einem kommutativen Ring mit 1 ist jedes maximale Ideal auch Primideal.*

Beispiel.

1. In einem Integritätsbereich ist $\{0\}$ ein Primideal, und in einem Körper ist $\{0\}$ ein maximales Ideal.

2. Im Ring $\mathbb{Z}$ sind die Ideale $p\mathbb{Z}$, p Primzahl, genau die maximalen Ideale; $\{0\}$ ist das einzige Primideal, das nicht maximal ist (vgl. Beispiel 2 nach Korollar 3.11).

Korollar 1.13 *Ist K ein Körper, R ein Ring und $\varphi : K \longrightarrow R$ ein Ringhomomorphismus, so ist φ injektiv oder φ ist die Nullabbildung, d.h. $\varphi(x) = 0$ für alle $x \in K$.*

Satz 1.14 (Homomorphiesatz) *Sind R, 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 3.8 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 weiterhin

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

wobei $\overline{a} = a + \text{Kern}\varphi$ und $\overline{b} = b + \text{Kern}\varphi$. Somit ist ψ ein Ringisomorphismus.

□

Bemerkung. Ist R ein kommutativer Ring mit 1 und $\varphi : R \longrightarrow S$ ein surjektiver Ringhomomorphismus, so ist S wegen Satz 1.9 genau dann ein Integritätsbereich, wenn Kernφ ein Primideal ist, und wegen Satz 1.11 ist S genau dann ein Körper, wenn Kernφ ein maximales Ideal ist.

Definition 1.15 *Ist R ein Ring und $S \subseteq R$ eine Teilmenge von R, so heißt S Teilring von R, wenn S bezüglich der Verknüpfungen von R selbst ein Ring ist. Ist S sogar ein Körper, so heißt S Teilkörper von R.*

Bemerkung. R sei ein Ring.

1. Eine nichtleere Teilmenge S von R ist genau dann ein Teilring von R, wenn $x-y, xy \in S$ für alle $x, y \in S$ gilt.

2. Der Durchschnitt von Teilringen eines Ringes R ist ein Teilring von R, der Durchschnitt von Teilkörpern eines Körpers K ist ein Teilkörper von K.

3. S sei ein Teilring von R. Hat R ein Einselement, so braucht S kein Einselement zu haben und umgekehrt. R und S können sogar verschiedene Einselemente haben. Ist F Teilkörper des Körpers K, so haben F und K dasselbe Einselement.

4. Ist $\varphi : S \longrightarrow R$ ein Ringhomomorphismus, so ist $\varphi(S)$ ein Teilring von R, und wegen des Homomorphiesatzes gilt $\varphi(S) \cong S/\text{Kern}\varphi$.

Beispiel.

1. $\mathbb{Z}$ ist ein Teilring von $\mathbb{Q}$ und $\mathbb{Q}$ ein Teilkörper von $\mathbb{R}$.

2. Jedes Ideal I eines Ringes R ist Teilring von R; so ist zum Beispiel $2\mathbb{Z}$ ein Teilring von $\mathbb{Z}$, der kein Einselement hat.

3. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ ist ein Teilring von $\mathbb{R}$ und $\{a + bi \mid a, b \in \mathbb{Z}\}$ mit $i^2 = -1$ ein Teilring $\mathbb{C}$.

Satz 1.16 (1. Isomorphiesatz) *Ist R ein Ring, S ein Teilring von R und I ein Ideal von R, dann ist $S + I$ mit*

$$S + I = \{s + i \mid s \in S \text{ und } i \in I\}$$

ein Teilring von R sowie $S \cap I$ ein Ideal von S und

$$\varphi : S/(S \cap I) \longrightarrow (S + I)/I,\ s + (S \cap I) \longmapsto s + I$$

ein Ringisomorphismus.

Beweis. Wir zeigen zunächst, daß $S+I$ ein Teilring von R ist. Wegen Satz 3.9 aus Kapitel 1 ist $S+I$ Untergruppe von R bezüglich $+$. Sind nun $s+i, s'+i' \in S+I$ mit $s, s' \in S, i, i' \in I$, dann gilt $(s+i)(s'+i') = ss' + si' + is' + ii' \in S+I$, weil $si', is', ii' \in I$.
Wie im Beweis von Satz 3.9 aus Kapitel 1 gezeigt wurde ist

$$\psi : S \longrightarrow (S+I)/I,\ s \longmapsto s+I$$

ein surjektiver Ringhomomorphismus mit dem Kern $S \cap I$. Für alle $s, s' \in S$ gilt

$$\psi(ss') = ss' + I = (s+I)(s'+I) = \psi(s)\psi(s'),$$

d.h., ψ ist ein Ringhomomorphismus. Wegen des Homomorphiesatzes für Ringe ist

$$\varphi : S/(S \cap I) \longrightarrow (S+I)/I,\ s+(S \cap I) \longmapsto s+I$$

ein Ringisomorphismus.

□

Definition 1.17 *Sei S ein Ring und R ein Teilring von S. Sind $a_0, \ldots, a_n \in R$ und $\alpha \in S$, dann heißt*

$$a_n\alpha^n + \cdots + a_1\alpha + a_0$$

Polynom in α mit den Koeffizienten $a_0, \ldots, a_n \in R$.

Bemerkung.

1. Die Menge aller Polynome in α mit Koeffizienten aus R wird mit $R[\alpha]$ bezeichnet.
2. Insbesondere ist jedes Element aus R ein Polynom in α mit Koeffizienten aus R, d.h. $R \subseteq R[\alpha]$.
3. Ist S kommutativ (oder allgemeiner: Gilt $\alpha r = r\alpha$ für alle $r \in R$), so zeigt man leicht mit Bemerkung 1 nach Definition 1.15, daß $R[\alpha]$ ein Teilring von S ist; R ist dann Teilring von $R[\alpha]$. Haben R und S dasselbe Einselement, so gilt $\alpha \in R[\alpha]$, und $R[\alpha]$ ist der kleinste Teilring von S, der R und α enthält. Es gilt zum Beispiel

   $$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \text{ und } \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\},$$

   wobei $\sqrt{2}, i \in \mathbb{C}$ und wir $\mathbb{Z}$ als Teilring von $\mathbb{C}$ auffassen.

Definition 1.18 *Sei S ein kommutativer Ring mit 1 und R ein Teilring von S mit $1 \in R$. Dann heißt $x \in S$ Unbestimmte über R, wenn für alle $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in R$ gilt:*

$$a_nx^n + \cdots + a_1x + a_0 = 0 \Longrightarrow a_n = \cdots = a_1 = a_0 = 0.$$

Ist $x \in S$ Unbestimmte über R, so heißt S Polynomring in x über R, wenn $S = R[x]$.

Bemerkung.

1. Ist S Polynomring in der Unbestimmten x über R, d.h. $S = R[x]$, so läßt sich jedes Element aus $S = R[x]$ eindeutig als Polynom in x schreiben, d.h., gilt

$$a_n x^n + \cdots + a_1 x + a_0 = b_m x^m + \cdots + b_1 x + b_0$$

mit $a_0, \ldots, a_n, b_0, \ldots, b_m \in R$ und $a_n, b_m \neq 0$, dann folgt $n = m$ sowie $a_i = b_i$ für $i = 0, \ldots, n$.

2. Ist $f(x) \in R[x]$ und x Unbestimmte über R, sowie

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

mit $a_n, \ldots, a_0 \in R$, dann heißt n der Grad von $f(x)$, falls $a_n \neq 0$, geschrieben $\operatorname{grad} f(x) = n$. Gilt $a_n = \cdots = a_0 = 0$, so heißt $f(x)$ Nullpolynom; das Nullpolynom hat den Grad $-\infty$. Gilt $a_n = 1$, so heißt $f(x)$ normiert.

Ist $g(x) \in R[x]$ ein weiteres Polynom mit $g(x) = b_m x^m + \cdots + b_1 x + b_0$, so folgt

$$f(x)g(x) = a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1) x + a_0 b_0.$$

Sind also $f(x), g(x) \neq 0$ und $a_n, b_m \neq 0$, dann hat $f(x)g(x)$ den Grad $n + m$, falls $a_n b_m \neq 0$. Ist also R ein Integritätsbereich, so gilt

$$\operatorname{grad} f(x)g(x) = \operatorname{grad} f(x) + \operatorname{grad} g(x),$$

und $R[x]$ ist ebenfalls ein Integritätsbereich.

3. S sei ein kommutativer Ring mit 1 und R ein Teilring von S mit $1 \in R$. Ist $x \in S$ Unbestimmte über R und $y \in S$ Unbestimmte über $R[x]$, dann ist y Unbestimmte über R sowie x Unbestimmte über $R[y]$, und es gilt $R[x][y] = R[y][x]$. Man schreibt dann $R[x][y] = R[x, y]$ und nennt x, y unabhängige Unbestimmte über R.

Beispiel. $\mathbb{Q}$ ist ein Teilring von $\mathbb{R}$. Dann ist $\alpha = 1 + \sqrt{5} \in \mathbb{R}$ keine Unbestimmte über $\mathbb{Q}$, da

$$\alpha^2 - 2\alpha - 4 = 0.$$

Allerdings ist $\pi \in \mathbb{R}$ Unbestimmte über $\mathbb{Q}$; man sagt in diesem Falle auch, daß π transzendent ist. e ist ebenfalls Unbestimmte über $\mathbb{Q}$, und zum Beispiel ist $e^{\sqrt{2}} \in \mathbb{R}$ Unbestimmte über $\mathbb{Q}[e]$. Ist π Unbestimmte über $\mathbb{Q}[e]$?

Satz 1.19 *Zu jedem kommutativen Ring R mit 1 gibt es einen Polynomring S in einer Unbestimmten x über R.*

Beweis. Sei S die Menge der endlichen Folgen von R, d.h., jedes Element aus S hat die Darstellung

$$(a_0, a_1, a_2, \ldots) \text{ mit } a_0, a_1, a_2, \ldots \in R,$$

so daß $a_i \neq 0$ nur für endlich viele Indizes $i \in \mathbb{N}_0$ gilt. Offenbar ist S bezüglich der gliedweisen Addition

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$

eine additive abelsche Gruppe mit dem Nullelement $(0, 0, 0, \dots)$. Durch

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$$

mit $c_n = a_0 b_n + a_1 b_{n-1} + \dots + a_{n-1} b_1 + a_n b_0$ wird auf S eine Multiplikation erklärt, denn ist $a_i = 0$ für alle $i \geq k$ und $b_i = 0$ für alle $i \geq l$, so ist $c_n = 0$ für alle $n \geq k + l$. Mit etwas Mühe rechnet man nach, daß S bezüglich obiger Addition und Multiplikation ein kommutativer Ring mit dem Einselement $(1, 0, 0, \dots)$ ist.

$$\varphi : R \longrightarrow S, \ a \longmapsto (a, 0, 0, \dots)$$

ist ein injektiver Ringhomomorphismus, und $\varphi(R)$ ist ein Teilring von S mit $1 \in \varphi(R)$. Identifiziert man die Elemente a und $\varphi(a)$ für alle $a \in R$, so ist R ein Teilring von S mit $1 \in R$. Wir definieren $x = (0, 1, 0, \dots)$ und erhalten mit vollständiger Induktion für alle $n \in \mathbb{N}$ und $a \in R$

$$a \cdot x^n = (a, 0, 0, \dots) \cdot (0, 1, 0, \dots)^n = (0, \dots, 0, \underset{\substack{\uparrow \\ (n+1)\text{-te Stelle}}}{a}, 0, \dots).$$

Für alle $a_0, a_1, a_2, \dots \in R$ gilt dann

$$\begin{aligned} a_n x^n + \dots + a_1 x + a_0 &= (a_0, a_1, \dots, a_n, 0, 0, \dots), \text{ also} \\ a_n x^n + \dots + a_1 x + a_0 = 0 &\iff a_0 = a_1 = \dots = a_n = 0. \end{aligned}$$

Damit ist x Unbestimmte über R und $S = R[x]$.

□

Bemerkung.

1. Ist R' ein kommutativer Ring mit 1 und R ein Teilring von R' mit $1 \in R$, dann ist $R[x]$ Teilring des Polynomringes $R'[x]$ über R' in der Unbestimmten x; dabei ist x auch Unbestimmte über R.

2. Verzichtet man im Beweis von Satz 1.19 bei der Definition von S auf die Bedingung " $a_i \neq 0$ *nur für endlich viele Indizes* $i \in \mathbb{N}_0$ ", definiert aber Addition und Multiplikation entsprechend, so ist S der sogenannte Ring der formalen Potenzreihen über R in der Unbestimmten x. Die Elemente von S lassen sich entsprechend schreiben als

$$a_0 + a_1 x + a_2 x^2 + \dots = \sum_{k=0}^{\infty} a_k x^k.$$

Für den Ring der formalen Potenzreihen führt man auch die Bezeichnung $R[[x]]$ ein. Die Elemente von $R[[x]]$ werden komponentenweise addiert und wie beim üblichen Ausmultiplizieren von Potenzreihen (Cauchy-Produkt) multipliziert.

Universelle Eigenschaft von $R[x]$

Der Polynomring $R[x]$ in einer Unbestimmten x über einem kommutativen Ring mit Eins hat folgende universelle Eigenschaft: *Ist S ein kommutativer Ring und $\varphi : R \longrightarrow S$ ein Ringhomomorphismus, so gibt es zu jedem $s \in S$ genau einen Ringhomomorphismus*

$$\psi : R[x] \longrightarrow S \text{ mit } \psi(x) = s \text{ und } \psi(r) = \varphi(r) \text{ für alle } r \in R.$$

Wegen

$$\begin{aligned} \psi(a_n x^n + \cdots + a_1 x + a_0) &= \psi(a_n)\psi(x)^n + \cdots + \psi(a_1)\psi(x) + \psi(a_0) \\ &= \varphi(a_n)s^n + \cdots + \varphi(a_1)s + \varphi(a_0) \end{aligned}$$

ist ψ eindeutig bestimmt, und durch

$$\psi(a_n x^n + \cdots + a_1 x + a_0) := \varphi(a_n)s^n + \cdots + \varphi(a_1)s + \varphi(a_0)$$

wird der gewünschte Ringhomomorphismus ψ definiert.

Anwendung.

1. Sind $R[x]$ und $R[x']$ zwei Polynomringe über R in den Unbestimmten x und x', so sind

   $$\psi : R[x] \longrightarrow R[x'],\ f(x) \longmapsto f(x') \text{ und } \psi' : R[x'] \longrightarrow R[x],\ f(x') \longmapsto f(x)$$

   Ringhomomorphismen. Da ψ die Umkehrabbildung von ψ' ist, sind ψ und ψ' Isomorphismen. Ist zum Beispiel x Unbestimmte über R, so sind auch x^2 und $x + 1$ Unbestimmte über R, also $R[x^2] \cong R[x + 1]$.

2. Ist R Teilring des kommutativen Ringes S und $s \in S$, so ist das *Einsetzen* ein Ringhomomorphismus, d.h.,

   $$\psi : R[x] \longrightarrow S,\ f(x) \longmapsto f(s)$$

   ist ein Ringhomomorphismus.

Definition 1.20 *Ist R ein kommutativer Ring mit Eins und $R[x]$ Polynomring über R in der Unbestimmten x, dann heißt $a \in R$ Nullstelle des Polynoms $f(x) \in R[x]$, wenn $f(a) = 0$.*

2. Quotientenkörper

Im folgenden sei R stets ein Integritätsbereich. Ziel dieses Paragraphen ist es zu zeigen, daß sich R dann in einen Körper einbetten läßt. Dabei werden wir wesentlich benutzen, daß in R folgende Kürzungsregel gilt:

$$\forall a, b \in R\ \forall x \in R \setminus \{0\} : (ax = bx \Longrightarrow a = b);$$

ist nämlich $ax = bx$, also $(a-b)x = 0$, und $x \neq 0$, so ergibt sich aus der Nullteilerfreiheit $a - b = 0$, d.h. $a = b$.
Zunächst definieren wir

$$\mathcal{F}(R) := \{(r,s) \mid r,s \in R \text{ und } s \neq 0\}$$

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

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

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. $((r,s) \sim (r',s') \ \wedge \ (r',s') \sim (r'',s'')) \implies (r,s) \sim (r'',s'')$ (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 $s' \neq 0$ ergibt sich aus der Kürzungsregel schließlich $rs'' = r''s$, d.h. $(r,s) \sim (r'',s'')$.

□

Damit ist $''\sim''$ eine Äquivalenzrelation, und für alle $r,s \in R, s \neq 0$ 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 $\cdot$ definiert:

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

Zunächst muß die Wohldefiniertheit von $+$ und $\cdot$ nachgewiesen werden:

Wohldefiniertheit von $+$: Aufgrund der Nullteilerfreiheit von R ergibt sich $s \cdot s' \neq 0$, also

$$\frac{r \cdot s' + s \cdot r'}{s \cdot s'} \in \mathrm{Q}(R).$$

Gilt nun $\frac{r}{s} = \frac{u}{v}$ und $\frac{r'}{s'} = \frac{u'}{v'}$, dann folgt $rv = su$ und $r'v' = s'u'$, also

$$rvs'v' + r'v'sv = sus'v' + s'u'sv, \text{ d.h. } (rs' + sr')vv' = ss'(uv' + u'v).$$

Somit ergibt sich $\frac{rs'+sr'}{ss'} = \frac{uv'+vu'}{vv'}$.

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

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

$\mathrm{Q}(R)$ ist sogar ein Körper: Ist $\frac{r}{s} \in \mathrm{Q}(R)$ und $\frac{r}{s} \neq \frac{0}{1}$, dann 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 betten wir R in $\mathrm{Q}(R)$ ein:

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

ist ein injektiver Ringhomomorphismus; zunächst gilt für alle $r, s \in R$:

$$\begin{aligned} f(r+s) &= \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = f(r) + f(s), \\ f(r \cdot s) &= \frac{r \cdot s}{1} = \frac{r}{1} \cdot \frac{s}{1} = f(r) \cdot f(s). \end{aligned}$$

f ist injektiv, denn $f(r) = \frac{0}{1}$ gilt genau dann, wenn $\frac{r}{1} = \frac{0}{1}$, d.h. $r = 0$.
Weiterhin ist $f(1)$ das Einselement von $\mathrm{Q}(R)$, und für alle $\frac{r}{s}$ aus $\mathrm{Q}(R)$ gilt:

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

Jedes Element aus $\mathrm{Q}(R)$ läßt sich also als Quotient von zwei Elementen aus $f(R)$ 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.

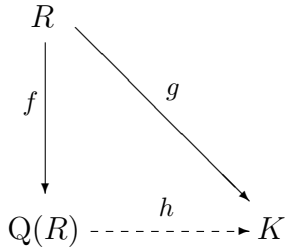
1. Schreibt man r statt $f(r)$ für alle $r \in R$, so ist R ein Teilring von $\mathrm{Q}(R)$ und
$$\mathrm{Q}(R) = \{rs^{-1} \mid r, s \in R, s \neq 0\}.$$
2. Wir werden später noch zeigen, daß es für jeden Integritätsbereich R im wesentlichen genau einen Quotientenkörper gibt. Man spricht daher auch von dem Quotientenkörper von R.
3. Ist K ein Körper und R ein Teilring von K mit $K = \{rs^{-1} \mid r, s \in R, s \neq 0\}$, so ist K ein Quotientenkörper von R.

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, dann ist der Polynomring $K[x]$ über K in der Unbestimmten x ein Integritätsbereich. Den Quotientenkörper von $K[x]$ bezeichnet man mit
$$K(x) = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ und } g(x) \neq 0\}$$
und nennt die Elemente von $K(x)$ gebrochen-rationale Funktionen über K in der Unbestimmten x.

Universelle Eigenschaft des Quotientenkörpers

Ist K ein Körper und $g : R \longrightarrow K$ ein injektiver Ringhomomorphismus, so existiert genau ein injektiver Ringhomomorphismus $h : \mathrm{Q}(R) \longrightarrow K$, so daß folgendes Diagramm kommutativ ist:



Die Kommutativität des Diagramms bedeutet dabei, daß $g = h \circ f$ gilt. Wegen

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

ist h eindeutig bestimmt, und durch

$$h(f(r)f(s)^{-1}) := g(r)g(s)^{-1}$$

wird der gewünschte Homomorphismus definiert. Die universelle Eigenschaft besagt, daß sich jede Einbettung eines Integritätsbereiches in einen Körper eindeutig auf den Quotientenkörper fortsetzen läßt. Wir wollen nun die universelle Eigenschaft nutzen, um die "Eindeutigkeit" des Quotientenkörpers zu zeigen. Dazu sei $\mathrm{Q}(R)'$ ein weiterer Quotientenkörper mit der Einbettung $f' : R \longrightarrow \mathrm{Q}(R)'$. Wir betrachten die beiden kommutativen Diagramme

Dann erhalten wir die kommutativen Diagramme

Wegen der Eindeutigkeit ist $g \circ h$ die Identität auf $\mathrm{Q}(R)$, d.h.

$$g \circ h : \mathrm{Q}(R) \longrightarrow \mathrm{Q}(R),\ x \longmapsto x.$$

Entsprechend ist $h \circ g$ die Identität auf $\mathrm{Q}(R)'$, d.h.

$$h \circ g : \mathrm{Q}(R)' \longrightarrow \mathrm{Q}(R)',\ x \longmapsto x.$$

Also sind h und g Isomorphismen, wobei $h^{-1} = g$ gilt.

3. Euklidische Ringe und Hauptidealringe

Definition 3.1 *Ein Integritätsbereich R heißt Euklidischer Ring, wenn es eine Funktion*

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

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. Ein Integritätsbereich kann bezüglich verschiedener Wertefunktionen ein Euklidischer Ring sein.
3. Ein Euklidischer Ring ist ein Integritätsbereich, in dem *Division mit Rest* möglich ist.

Beispiel.

1. Der Integritätsbereich $\mathbb{Z}$ ist bezüglich des Absolutbetrags $|\ |$ als Wertefunktion

   $$|\ | : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}_0, z \longmapsto |z|$$

   ein Euklidischer Ring. Zum Beispiel gilt mit $a = 17$ und $b = 6$ sowohl $17 = 2 \cdot 6 + 5$ als auch $17 = 3 \cdot 6 - 1$.

2. Der Integritätsbereich $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ mit $i^2 = -1$ ist bezüglich der Normfunktion

   $$\mathrm{N} : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{N}_0,\ a + bi \longmapsto a^2 + b^2$$

   als Wertefunktion ein Euklidischer Ring. Um das einzusehen, seien $a, b \in \mathbb{Z}[i], b \neq 0$. Dann gibt es $c, d \in \mathbb{Q}$ mit $\frac{a}{b} = c + di$ sowie $x, y \in \mathbb{Z}$ mit $|c - x| \leq \frac{1}{2}$ und $|d - y| \leq \frac{1}{2}$. Mit $q = x + yi$ und $r = ((c - x) + (d - y)i)b$ folgt $q, r \in \mathbb{Z}[i]$ sowie

   $$a = \frac{a}{b}b = (c + di)b = (x + yi)b + ((c - x) + (d - y)i)b = qb + r.$$

   Benutzen wir die Multiplikativität der Normfunktion (vgl. Aufgabe 5.27), so ergibt sich

   $$\mathrm{N}(r) = \mathrm{N}((c - x) + (d - y)i)\mathrm{N}(b) = ((c - x)^2 + (d - y)^2)\mathrm{N}(b) < \mathrm{N}(b).$$

3. Ist K ein Körper, so ist der Polynomring $K[x]$ über K in der Unbestimmten x bezüglich der Gradfunktion ein Euklidischer Ring, denn sind $g(x), h(x) \in K[x], h(x) \neq 0$, so gibt es $q(x), r(x) \in K[x]$ mit $g(x) = q(x)h(x) + r(x)$ und $\operatorname{grad} r(x) < \operatorname{grad} h(x)$ oder $r(x) = 0$. Um das einzusehen, sei $g(x) = g_n x^n + \cdots + g_0$ und $h(x) = h_m x^m + \cdots + h_0$, $h_m \neq 0$. Gilt $g(x) = 0$, so wählen wir $q(x) = r(x) = 0$. Sei also $g(x) \neq 0$ und $\operatorname{grad} g(x) = n$. Wir beweisen die Behauptung durch Induktion nach n.

$n = 0$: Im Falle $\operatorname{grad} h(x) > 0$ wählen wir $q(x) = 0$ sowie $r(x) = g(x) = g_0$, und es gilt $g_0 = 0 \cdot h(x) + g_0$ mit $0 = \operatorname{grad} g_0 < \operatorname{grad} h(x)$. Ist aber $\operatorname{grad} h(x) = 0$, 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 $\operatorname{grad} g(x) < \operatorname{grad} h(x)$. 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 $\operatorname{grad} k(x) < \operatorname{grad} g(x)$. 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 $\operatorname{grad} r(x) < \operatorname{grad} h(x)$. Es folgt

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

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.

$$\begin{array}{llll} x^4 & -4x^2 & +6x & +4 \;:x^2+2x-2 = x^2-2x+2 \\ \cline{1-3} x^4 & +2x^3 & -2x^2 & \\ \cline{1-3} & -2x^3 & -2x^2 & +6x+4 \\ & -2x^3 & -4x^2 & +4x \\ \cline{2-4} & & 2x^2 & +2x+4 \\ & & 2x^2 & +4x-4 \\ \cline{3-4} & & & -2x+8 \end{array}$$

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

Satz 3.2 *In einem Euklidischen Ring R ist jedes Ideal I ein Hauptideal.*

Beweis. Sei R ein Euklidischer Ring bezüglich der Wertefunktion g. Gilt $I = \{0\}$, so ist $I = 0R$. Sei also $I \neq \{0\}$ und $M = \{g(r) \mid r \in I, r \neq 0\} \subseteq \mathbb{N}_0$. Da M nicht leer ist, hat M ein kleinstes Element n. Sei $a \in I, a \neq 0$ mit $g(a) = n = \min\{g(r) \mid r \in I, r \neq 0\}$. Wir zeigen $I = aR$. Wegen $a \in I$ folgt $ar \in I$ für alle $r \in R$, also $aR \subseteq I$. Ist nun andererseits $i \in I$, dann gibt es $q, r \in R$ mit $i = qa + r$, wobei $r = 0$ oder $g(r) < g(a)$. Wäre $r \neq 0$, so wäre $r = i - qa \in I$ mit $g(r) < g(a)$, im Widerspruch dazu, daß $n = g(a)$ in M minimal ist. Also folgt $i = qa \in aR$, d.h. $I \subseteq aR$.

□

Definition 3.3 *Ein Integritätsbereich R heißt Hauptidealring, wenn jedes Ideal von R ein Hauptideal ist.*

Bemerkung.

1. Satz 3.2 besagt also, daß jeder Euklidische Ring ein Hauptidealring ist.

2. Der Integritätsbereich $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ ist ein Hauptidealring, der kein Euklidischer Ring ist.

Definition 3.4 *R sei ein Integritätsbereich sowie $a, b \in R$.*

i) a teilt b (geschrieben $a|b$), wenn es $c \in R$ mit $b = ac$ gibt. a heißt dann Teiler von b.

*ii) $d \in R$ heißt größter gemeinsamer Teiler von a und b (*ggT *von a und b), wenn d ein Teiler von a und b ist und wenn jeder Teiler d' von a und b auch Teiler von d ist.*

Bemerkung.

1. a teilt $b \iff bR \subseteq aR$.

2. a teilt b und b teilt $a \iff aR = bR \iff a = b\epsilon$ für eine Einheit $\epsilon \in R$.

3. Entsprechend definiert man den Begriff *kleinstes gemeinsames Vielfaches* (kgV).

4. Im allgemeinen gibt es zu $a, b \in R$ weder einen ggT noch ein kgV.

5. Ein $d \in R$ ist genau dann ein ggT von a und b, wenn $aR, bR \subseteq dR$ und wenn für jedes $d' \in R$ mit $aR, bR \subseteq d'R$ auch $dR \subseteq d'R$ gilt. Sind also d und d' zwei ggT's von a und b, so gilt $dR = d'R$ und umgekehrt, d.h., $\{d\epsilon \mid \epsilon$ Einheit in $R\}$ ist die Menge aller ggT's von a und b, wenn d ein ggT von a und b ist.

6. Bemerkung 5 gilt entsprechend für kgV's.

Satz 3.5 *Ist R ein Hauptidealring und sind $a, b \in R$, dann gilt für alle $d \in R$:*

1. d ist ein ggT *von a und $b \iff aR + bR = dR$.*

2. d ist ein kgV *von a und $b \iff aR \cap bR = dR$.*

Beweis. Wir beweisen nur 1). Die Behauptung 2) ergibt sich analog.
$''\Longrightarrow''$: Ist d ein ggT von a und b, so folgt $aR, bR \subseteq dR$, also $aR + bR \subseteq dR$. Weil R ein Hauptidealring ist, existiert $d' \in R$ mit $aR + bR = d'R$, also $aR, bR \subseteq d'R$. Da d größter gemeinsamer Teiler ist, ergibt sich $dR \subseteq d'R = aR + bR$, also $dR = d'R = aR + bR$.
$''\Longleftarrow''$: Wegen $aR + bR = dR$, also $aR, bR \subseteq dR$, ist d ein Teiler von a und b. Ist nun $d' \in R$ mit $aR, bR \subseteq d'R$, so folgt $dR = aR + bR \subseteq d'R$, d.h., d ist ein ggT von a und b.

□

Im folgenden soll gezeigt werden, wie in einem Euklidischen Ring R ein ggT von zwei Elementen $a, b \in R, a, b \neq 0$ mit Hilfe des sogenannten Euklidischen Algorithmus berechnet werden kann. Dazu ermittelt man $r_1, q_1, r_2, q_2, \ \ldots \ \in R$ nach folgendem Schema:

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

Wegen $g(b) > g(r_1) > \cdots > g(r_{n-1}) \geq 0$ bricht das Verfahren ab, etwa $r_n = 0$ und $r_{n-1} \neq 0$ für ein $n \in \mathbb{N}$.
Für alle $x, y, r \in R$ gilt $xR + yR = (x + yr)R + yR$, und wir erhalten aus obigem Schema

$$\begin{aligned} aR + bR &= (q_1 b + r_1)R + bR = bR + r_1 R, \\ bR + r_1 R &= (q_2 r_1 + r_2)R + r_1 R = r_1 R + r_2 R, \\ r_1 R + r_2 R &= (q_3 r_2 + r_3)R + r_2 R = r_2 R + r_3 R, \\ &\vdots \\ r_{n-2} R + r_{n-1} R &= (q_n r_{n-1} + r_n)R + r_{n-1} R = r_{n-1} R + r_n R. \end{aligned}$$

Wegen $r_n = 0$ ergibt sich schließlich $aR + bR = r_{n-1}R$, und aufgrund von Satz 3.5 ist r_{n-1} ein ggT von a und b.

Beispiel. Wir berechnen im Ring $\mathbb{Z}$ der ganzen Zahlen einen ggT von 356 und 103.

$$\begin{aligned} 356 &= 3 \cdot 103 + 47 \\ 103 &= 2 \cdot 47 + 9 \\ 47 &= 5 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1. \end{aligned}$$

Somit ist 1 ein ggT von 356 und 103, und man nennt 356 und 103 deshalb auch teilerfremd. Mit 1 ist auch -1 ein ggT von 356 und 103.
Wegen Satz 3.5 läßt sich in einem Hauptidealring R jeder ggT von a und b in der Form

$$d = xa + yb \text{ mit } x, y \in R$$

darstellen. Ist R sogar ein Euklidischer Ring, so können x und y mit Hilfe des Euklidischen Algorithmus und anschließendem *Rückwärtseinsetzen* berechnet werden. Für das obige Beispiel ergibt sich:

$$\begin{aligned} 1 &= 9 - 4 \cdot 2 \\ &= 9 - 4 \cdot (47 - 5 \cdot 9) = 21 \cdot 9 - 4 \cdot 47 \\ &= 21 \cdot (103 - 2 \cdot 47) - 4 \cdot 47 = 21 \cdot 103 - 46 \cdot 47 \\ &= 21 \cdot 103 - 46 \cdot (356 - 3 \cdot 103) \\ &= 159 \cdot 103 - 46 \cdot 356. \end{aligned}$$

Diese Methode zur Berechnung der Darstellung eines ggT's kann benutzt werden, um konkret in den Ringen $\mathbb{Z}_n$ zum Beispiel multiplikative Inverse zu berechnen. Da 356 keine Primzahl ist, ist $\mathbb{Z}_{356}$ kein Körper. Wegen der Teilerfremdheit von 356 und 103 ist aber $\overline{103}$ in $\mathbb{Z}_{356}$ eine Einheit. In $\mathbb{Z}_{356}$ gilt:

$$\begin{aligned}\overline{1} &= \overline{159 \cdot 103 - 46 \cdot 356} \\ &= \overline{159} \cdot \overline{103} - \overline{46} \cdot \overline{356} \\ &= \overline{159} \cdot \overline{103},\end{aligned}$$

d.h. $\overline{103}^{-1} = \overline{159}$ in $\mathbb{Z}_{356}$.

Definition 3.6 *R sei ein Integritätsbereich. Ist $p \in R$ keine Einheit und von 0 verschieden, so heißt p Primelement (oder prim), wenn für alle $a, b \in R$ gilt:*

$$p|ab \implies p|a \text{ oder } p|b.$$

Bemerkung. Ist p ein Primelement und teilt p das Produkt $a_1 \cdot \ldots \cdot a_n$ mit $a_1, \ldots, a_n \in R$, so teilt p mindesten ein $a_i, i = 1, \ldots, n$.

Satz 3.7 *R sei ein Integritätsbereich und $p \in R$.*

$$p \text{ ist ein Primelement} \iff pR \text{ ist ein Primideal } \neq \{0\}.$$

Beweis. $''\Longrightarrow''$: Da p Primelement ist, gilt $p \neq 0$, also $pR \neq \{0\}$. Wir zeigen nun, daß pR ein Primideal ist. Wäre $pR = R$, so gäbe es ein $r \in R$ mit $pr = 1$, d.h., p wäre eine Einheit - im Widerspruch zur Definition des Primelementes. Also gilt $pR \neq R$. Sind nun $a, b \in R$ mit $ab \in pR$, so ist p ein Teiler von ab. Da p prim ist, folgt $p|a$ oder $p|b$, d.h. $a \in pR$ oder $b \in pR$. $''\Longleftarrow''$: Wegen $pR \neq \{0\}$ ist $p \neq 0$, und p ist keine Einheit wegen $pR \neq R$. Sind nun $a, b \in R$ mit $p|ab$, dann gilt $ab \in pR$, also $a \in pR$ oder $b \in pR$, da pR Primideal ist. Es folgt $p|a$ oder $p|b$.

□

Definition 3.8 *R sei ein Integritätsbereich. Ist $u \in R$ keine Einheit und von 0 verschieden, so heißt u unzerlegbar (oder irreduzibel), wenn für alle $a, b \in R$ gilt:*

$$u = ab \implies a \text{ ist eine Einheit oder } b \text{ ist eine Einheit.}$$

Satz 3.9 *R sei ein Integritätsbereich und $p \in R$. Ist p prim, so ist p unzerlegbar.*

Beweis. Ist p prim, dann ist p keine Einheit und von 0 verschieden. Sei nun $p = ab$ mit $a, b \in R$, also $p \cdot 1 = ab$. Dann gilt $p|ab$, d.h., $p|a$ oder $p|b$, da p prim ist. O.B.d.A. gelte $p|a$, und es gibt $r \in R$ mit $a = pr$. Wegen $p = ab = prb$ und der Nullteilerfreiheit von R ergibt sich $1 = rb$, d.h., b ist eine Einheit.

□

Bemerkung. Im allgemeinen sind unzerlegbare Elemente nicht prim. Zum Beispiel ist 3 im Integritätsbereich $\mathbb{Z}[\sqrt{-5}]$ unzerlegbar, aber nicht prim.

Satz 3.10 *R sei ein Hauptidealring und $u \in R$.*

$$u \text{ ist unzerlegbar} \iff uR \text{ ist ein maximales Ideal} \neq \{0\}.$$

Beweis. $''\Longrightarrow''$: Da u unzerlegbar ist, gilt $u \neq 0$, also $uR \neq \{0\}$. Wir zeigen nun, daß uR maximales Ideal ist. Wäre $uR = R$, so gäbe es ein $r \in R$ mit $ur = 1$, d.h., u wäre eine Einheit - im Widerspruch zur Definition des unzerlegbaren Elementes. Also gilt $uR \neq R$. Ist nun I ein Ideal von R mit $uR \subseteq I \subseteq R$, dann gibt es ein $a \in R$ mit $I = aR$, da R ein Hauptidealring ist. Wegen $u \in I = aR$ existiert ein $b \in R$ mit $u = ab$, d.h., a ist Einheit oder b ist Einheit, weil u unzerlegbar ist. Ist a Einheit, so folgt $I = R$, ist b Einheit, so folgt $I = aR = abR = uR$.

$''\Longleftarrow''$: Ist $uR \neq \{0\}$ ein maximales Ideal, dann ist uR wegen Korollar 1.12 auch ein Primideal, d.h., u ist prim wegen Satz 3.7 und wegen Satz 3.9 unzerlegbar.

□

Korollar 3.11 *Ist R ein Hauptidealring, dann sind unzerlegbare Elemente und Primelemente dasselbe, und jedes Primideal $\neq \{0\}$ ist maximal.*

Beispiel.

1. Weil 3 in $\mathbb{Z}[\sqrt{-5}]$ unzerlegbar ist, aber nicht prim, ist $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring.

2. Im Ring $\mathbb{Z}$ sind die Ideale $p\mathbb{Z}$, p prim genau die maximalen Ideale, und $\{0\}$ ist das einzige Primideal, das nicht maximal ist.

3. K sei ein Körper. Die Einheiten des Polynomringes $K[x]$ über K in der Unbestimmten x sind genau die Elemente $k \in K, k \neq 0$. Ein Polynom $f(x) \in K[x]$ ist damit genau dann unzerlegbar oder prim, wenn $\operatorname{grad} f(x) \geq 1$ und wenn sich $f(x)$ nur trivial zerlegen läßt, d.h., wenn für alle $g(x), h(x) \in K[x]$ gilt:

   $$f(x) = g(x)h(x) \Longrightarrow g(x) = g_0 \in K \text{ oder } h(x) = h_0 \in K;$$

   $f(x)$ heißt dann irreduzibel über K. Jedes Polynom $f(x)$ vom Grad 1 ist irreduzibel; z.B. $f(x) = x - a, a \in K$. Sei nun $\operatorname{grad} f(x) \geq 2$. Hat $f(x)$ eine Nullstelle $a \in K$, so gilt

   $$f(x) = q(x)(x-a) + r(x) \text{ mit } q(x), r(x) \in K[x],$$

   wobei $r(x) = 0$ oder $\operatorname{grad} r(x) < \operatorname{grad}(x-a) = 1$. Es ergibt sich $r(x) = r \in K$, und wegen $0 = f(a) = q(a)(a-a) + r = r$ folgt $f(x) = q(x)(x-a)$, d.h., $f(x)$ ist reduzibel. Ist andererseits $f(x)$ reduzibel, so braucht $f(x)$ aber keine Nullstelle in K zu haben; zum Beispiel ist $(x^2+1)(x^2+2)$ reduzibel über $\mathbb{Q}$, hat aber in $\mathbb{Q}$ keine Nullstelle. Gilt jedoch $\operatorname{grad} f(x) = 2$ oder $\operatorname{grad} f(x) = 3$, so ist $f(x)$ genau dann irreduzibel über K, wenn $f(x)$ in K keine Nullstelle hat, denn bei jeder nichttrivialen Zerlegung von $f(x)$ hat mindestens ein Faktor den Grad 1. Zum Beispiel hat $x^3 - 3$ keine Nullstelle in $\mathbb{Q}$ und ist daher irreduzibel über $\mathbb{Q}$, aber reduzibel über $\mathbb{R}$, und x^2+1 ist irreduzibel über $\mathbb{R}$, aber reduzibel über $\mathbb{C}$.

4. Gaußsche Ringe

Definition 4.1 *Ist R ein Integritätsbereich, dann heißt R Gaußscher Ring, wenn sich jedes Element $a \in R$, $a \neq 0$, das keine Einheit ist, als Produkt von Primelementen schreiben läßt.*

Bemerkung. Ist $p \in R$ keine Einheit und von 0 verschieden sowie $\epsilon \in R$, $\epsilon \neq 1$ eine Einheit, dann ist p wegen Satz 3.7 genau dann prim, wenn $p\epsilon$ prim ist. Eine Darstellung von $a \in R$ als Produkt von Primelementen $a = p_1 \cdot \ \ldots \ \cdot p_n$ ist daher im allgemeinen nicht eindeutig, da $a = (\epsilon p_1) \cdot (\epsilon^{-1} p_2) \cdot \ \ldots \ \cdot p_n$ zum Beispiel eine weitere Darstellung von a als Produkt von Primelementen liefert, die sich allerdings von der ersten nicht wesentlich unterscheidet.

Definition 4.2 *Ist R ein Integritätsbereich, so heißen $a, b \in R$ assoziiert, wenn es eine Einheit $\epsilon \in R$ mit $a = b\epsilon$ gibt.*

Bemerkung. In einem Integritätsbereich R sind $a, b \in R$ genau dann assoziiert, wenn $aR = bR$ gilt.

Beispiel.

1. In $\mathbb{Z}$ sind a und b genau dann assoziiert, wenn $a = b$ oder $a = -b$ gilt.
2. In $\mathbb{Z}[i]$ sind $1 + 2i$ und $2 - i$ assoziiert.
3. Ist K ein Körper und x eine Unbestimmte über K, so sind $f(x), g(x) \in K[x]$ genau dann assoziiert, wenn es ein $k \in K, k \neq 0$ mit $f(x) = kg(x)$ gibt. Sind $f(x)$ und $g(x)$ normiert, so sind $f(x)$ und $g(x)$ genau dann assoziiert, wenn $f(x) = g(x)$.

Satz 4.3 *Ist R ein Gaußscher Ring sowie $a \in R$ keine Einheit und von 0 verschieden mit*

$$a = p_1 \cdot \ \ldots \ \cdot p_r = q_1 \cdot \ \ldots \ \cdot q_s,$$

wobei $p_1, \ldots, p_r, q_1, \ldots, q_s$ Primelemente aus R sind, dann gilt $r = s$, und bei geeigneter Indizierung sind p_i, q_i für $i = 1, \ldots, r$ assoziiert.

Beweis. Wir beweisen die Behauptung durch Induktion nach r.

$r = 1$: Wir nehmen $s > 1$ an. Da p_1 wegen Satz 3.9 als Primelement unzerlegbar ist, folgt aus $p_1 = q_1 \cdot (q_2 \cdot \ \ldots \ \cdot q_s)$, daß q_1 oder $q_2 \cdot \ \ldots \ \cdot q_s$ eine Einheit ist. Als Primelement ist q_1 keine Einheit, und es gibt ein $t \in R$ mit $(q_2 \cdot \ \ldots \ \cdot q_s)t = 1$, d.h., q_2 ist Einheit - Widerspruch. Damit ergibt sich $s = 1$ und $p_1 = q_1$.

$r > 1$: Da q_1 prim ist, folgt o.B.d.A., daß q_1 Teiler von p_1 ist, also $p_1 = q_1 t$ für ein $t \in R$. Als Primelement ist p_1 unzerlegbar und q_1 keine Einheit, d.h., t ist Einheit in R. Aus

$$\begin{aligned} p_1 \cdot p_2 \cdot \ \ldots \ \cdot p_r &= (q_1 \cdot t) \cdot p_2 \cdot \ \ldots \ \cdot p_r \\ &= q_1 \cdot (t \cdot p_2) \cdot \ \ldots \ \cdot p_r \\ &= q_1 \cdot q_2 \cdot \ \ldots \ \cdot q_s \end{aligned}$$

folgt $(t \cdot p_2) \cdot \ \ldots \ \cdot p_r = q_2 \cdot \ \ldots \ \cdot q_s$. Dabei ist $t \cdot p_2$ ein Primelement in R. Nach Induktionsvoraussetzung ergibt sich $r - 1 = s - 1$, also $r = s$, und bei geeigneter Indizierung sind $t \cdot p_2$ und q_2 sowie p_i und q_i für $i > 2$ assoziiert. Somit sind schließlich bei geeigneter Indizierung p_i und q_i für alle $i = 1, \ldots, r$ assoziiert.

□

Bemerkung.

1. In einem Gaußschen Ring sind Primelemente und unzerlegbare Elemente dasselbe, denn ist p prim, so ist p unzerlegbar wegen Satz 3.9, und ist p unzerlegbar sowie $p = p_1 \cdot \ \ldots \ \cdot p_n$ mit $n > 1$ eine Zerlegung von p in Primelemente, so ist $p_2 \cdot \ \ldots \ \cdot p_n$ eine Einheit, weil p_1 als Primelement keine Einheit ist.

2. In einem Gaußschen Ring R existieren zu $a, b \in R \setminus \{0\}$ stets ein ggT und ein kgV, denn gilt
$$a = p_1^{k_1} \cdot \ \ldots \ \cdot p_n^{k_n} \epsilon_a \quad \text{sowie} \quad b = p_1^{l_1} \cdot \ \ldots \ \cdot p_n^{l_n} \epsilon_b$$
mit paarweise nicht-assoziierten Primelementen $p_1, \ldots, p_n$ sowie $k_1, \ldots, k_n, l_1, \ldots, l_n$ aus $\mathbb{N} \cup \{0\}$ und Einheiten $\epsilon_a, \epsilon_b \in R$, dann ist
$$p_1^{\min\{k_1,l_1\}} \cdot \ \ldots \ \cdot p_n^{\min\{k_n,l_n\}} \quad \text{ein ggT von } a \text{ und } b$$
sowie
$$p_1^{\max\{k_1,l_1\}} \cdot \ \ldots \ \cdot p_n^{\max\{k_n,l_n\}} \quad \text{ein kgV von } a \text{ und } b.$$
Ist d ein ggT von a und b, so ist also $\frac{ab}{d}$ ein kgV von a und b. Gilt $d = 1$, so heißen a und b teilerfremd.

Satz 4.4 *Jeder Hauptidealring R ist ein Gaußscher Ring.*

Beweis. Wir definieren

$$M := \{a \in R \mid a \neq 0 \text{ und } a \notin \mathrm{E}(R) \text{ und } a \text{ ist nicht Produkt von Primelementen}\}$$

und nehmen an, daß M nicht leer ist. Zuerst zeigen wir

$(*)$ Zu jedem $a \in M$ gibt es ein $a' \in M$ mit $aR \subset a'R \subset R$.

Wegen $a \in M$ ist a nicht prim, und wegen Satz 3.7 ist aR kein Primideal, also auch nicht maximal wegen Korollar 1.12. Es existiert somit ein Ideal I von R mit $aR \subset I \subset R$, das aufgrund der Voraussetzung des Satzes sogar ein Hauptideal ist: $I = bR$. Sei $c \in R$ mit $a = bc$. Wegen $a \neq 0$ ist $b \neq 0$ und $c \neq 0$, wegen $aR \neq I$ ist c keine Einheit, und wegen $I \neq R$ ist b auch keine Einheit. Wären also b und c nicht aus M, so wäre a Produkt von Primelementen. Also folgt $b \in M$ oder $c \in M$. Ist $b \in M$, so setzen wir $a' = b$, anderenfalls $a' = c$, und es gilt $aR \subset a'R \subset R$, womit $(*)$ gezeigt ist.

Da M nicht leer ist, gibt es wegen $(*)$ eine aufsteigende Kette $a_1R \subset a_2R \subset \cdots \subset R$ von Idealen, wobei $a_1, a_2, \ldots \in M$. Offenbar ist die Vereinigung

$$I = \bigcup_{i \in \mathbb{N}} a_i R$$

ein Ideal von R. Da R ein Hauptidealring ist, gilt $I = aR$ für ein $a \in R$. Wegen $a \in I$ liegt a in einem a_iR; also folgt mit $aR \subseteq a_iR \subset a_{i+1}R \subseteq I = aR$ ein Widerspruch.

□

Beispiel.

1. Als Euklidischer Ring ist $\mathbb{Z}$ ein Hauptidealring, also ein Gaußscher Ring. Jede natürliche Zahl $n \in \mathbb{N}, n > 1$ läßt sich damit eindeutig (bis auf die Reihenfolge der Faktoren) als Produkt von Primzahlen schreiben.

2. Ist K ein Körper, so ist der Polynomring $K[x]$ über K in der Unbestimmten x ein Gaußscher Ring. Jedes normierte Polynom $f(x) \in K[x]$ mit $\operatorname{grad} f(x) \geq 1$ läßt sich eindeutig (bis auf die Reihenfolge der Faktoren) als Produkt normierter irreduzibler Polynome aus $K[x]$ schreiben. Sind z.B. $a_1, \ldots, a_r \in K$ paarweise verschieden, dann sind $x - a_1, \ldots, x - a_r$ paarweise verschiedene nicht-assoziierte irreduzible Polynome aus $K[x]$. Ist jedes a_i Nullstelle von $f(x) \in K[x]$, so ist jedes $x - a_i$ Teiler von $f(x)$ in $K[x]$ (vgl. Beispiel 3 nach Korollar 3.11), und wir erhalten

Korollar 4.5 *Ist K ein Körper und $f(x) \in K[x], f(x) \neq 0$ ein Polynom mit paarweise verschiedenen Nullstellen $a_1, \ldots, a_r \in K$, so ist $(x - a_1) \cdot \ \ldots \ \cdot (x - a_r)$ ein Teiler von $f(x)$ in $K[x]$. Hat $f(x)$ den Grad n, so hat $f(x)$ höchstens n verschiedene Nullstellen in K.*

Lemma 4.6 *Ist R ein Gaußscher Ring und $R[x]$ der Polynomring über R in der Unbestimmten x, dann ist jedes $p \in R$, das in R prim ist, auch in $R[x]$ Primelement.*

Beweis. Weil p Primelement in R ist, ist $p \neq 0$ und p keine Einheit in R, also auch keine Einheit in $R[x]$. Seien nun $f(x), g(x) \in R[x]$ und sei p ein Teiler von $f(x)g(x)$. Gilt $f(x) = 0$ oder $g(x) = 0$, so folgt $f(x) = 0 \cdot p$ oder $g(x) = 0 \cdot p$. Sei also

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \ g(x) = b_m x^m + \cdots + b_1 x + b_0$$

mit $a_0, \ldots, a_n, b_0, \ldots, b_m \in R$ und $a_n, b_m \neq 0$.

Annahme: p teilt in R nicht jedes a_i und nicht jedes b_i. Dann gibt es ein $r \in \{0, \ldots, n\}$ minimal mit der Eigenschaft, daß p kein Teiler von a_r ist, und ein $s \in \{0, \ldots, m\}$ minimal mit der Eigenschaft, daß p kein Teiler von b_s ist. Folglich wird jedes a_i mit $i < r$ und jedes b_i mit $i < s$ von p geteilt, d.h., p ist Teiler von $a_i \cdot b_{r+s-i}$ für alle $i \neq r$. Da p Primelement in R ist, wird $a_r b_s$ nicht von p geteilt und damit auch nicht

$$h_{r+s} := \sum_i a_i b_{r+s-i} = a_r b_s + \sum_{i \neq r} a_i b_{r+s-i}.$$

Somit ist p kein Teiler von $f(x)g(x)$, weil h_{r+s} der Koeffizient von x^{r+s} in $f(x)g(x)$ ist - Widerspruch.

Also teilt p jedes a_i, d.h. $p|f(x)$, oder jedes b_i, d.h. $p|g(x)$.

□

Definition 4.7 *Ist R ein Gaußscher Ring und $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x], a_n \neq 0$, dann heißt $f(x)$ primitiv, wenn es kein Primelement p in R gibt, das $a_0, a_1, \ldots, a_n$ teilt.*

Bemerkung. R sei ein Gaußscher Ring und K der Quotientenkörper von R.

1. Ein Polynom $f(x) \in R[x], f(x) \neq 0$ ist genau dann primitiv, wenn es von keinem $p \in R$, das in R prim ist, in $R[x]$ geteilt wird.
2. Ist $f(x) \in K[x], f(x) \neq 0$, so gibt es ein $a \in K$ und ein primitives $g(x) \in R[x]$ mit $f(x) = a \cdot g(x)$.

Korollar 4.8 (Gaußsches Lemma) *Ist R ein Gaußscher Ring, dann ist das Produkt primitiver Polynome aus $R[x]$ primitiv.*

Korollar 4.9 *Es sei R ein Gaußscher Ring mit dem Quotientenkörper K und $f(x) \in R[x]$, $f(x) \neq 0$ primitiv. Ist $a \in K$ mit $af(x) \in R[x]$, dann gilt $a \in R$.*

Beweis. Sei $a = uv^{-1} \neq 0$ mit $u, v \in R$ und u, v teilerfremd. Ist v Einheit in R, so folgt $a \in R$. Ist v keine Einheit in R, so hat v einen Primteiler p in R, der wegen Lemma 4.6 auch prim in $R[x]$ ist. Da $v(af(x)) = uf(x)$ gilt, ist p Teiler von u oder Teiler von $f(x)$. Das erste widerspricht der Teilerfremdheit von u, v, das zweite der Tatsache, daß $f(x)$ primitiv ist.

□

Hilfssatz 4.10 *Ist R ein Gaußscher Ring, K der Quotientenkörper von R und $f(x) \in R[x]$ primitiv, dann ist $f(x)$ Primelement in $R[x]$, wenn $f(x)$ Primelement in $K[x]$ ist.*

Beweis. Sei $f(x) \in R[x]$ primitiv und prim in $K[x]$. Dann ist $f(x) \neq 0$ und keine Einheit in $K[x]$, also auch keine Einheit in $R[x]$. Seien nun $g(x), h(x) \in R[x]$ und sei $f(x)$ Teiler von $g(x)h(x)$ in $R[x]$. Dann ist $f(x)$ Teiler von $g(x)h(x)$ in $K[x]$, d.h., $f(x)$ teilt $g(x)$ in $K[x]$ oder $f(x)$ teilt $h(x)$ in $K[x]$, da $f(x)$ prim in $K[x]$ ist. O.B.d.A. gelte $g(x) = f(x)q(x)$ mit $q(x) \in K[x]$. Es gibt ein $a \in K$ und ein primitives $s(x) \in R[x]$ mit $q(x) = as(x)$, also $g(x) = af(x)s(x)$. Wegen des Gaußschen Lemmas ist $f(x)s(x)$ primitiv, und wegen Korollar 4.9 ist $a \in R$, d.h., $f(x)$ teilt $g(x)$ in $R[x]$.

□

Satz 4.11 *Ist R ein Gaußscher Ring, dann ist der Polynomring $R[x]$ über R in der Unbestimmten x auch ein Gaußscher Ring.*

Beweis. Sei $f(x) \in R[x]$, $f(x) \neq 0$ und $f(x)$ keine Einheit in $R[x]$. Zu zeigen ist, daß $f(x)$ Produkt von Primelementen aus $R[x]$ ist. Gilt $\operatorname{grad} f(x) = 0$, so ist $f(x) \in R$ konstant, also das Produkt von Primelementen aus R, die wegen Lemma 4.6 auch prim in $R[x]$ sind. Sei also $\operatorname{grad} f(x) \geq 1$. Dann ist $f(x)$ keine Einheit in $K[x]$, wobei K der Quotientenkörper von R ist. $K[x]$ ist ein Gaußscher Ring, und es gibt irreduzible Polynome $g_1(x), \ldots, g_r(x) \in K[x]$ mit $f(x) = g_1(x) \cdot \ \ldots \ \cdot g_r(x)$. Zu jedem $i = 1, \ldots, r$ gibt es weiterhin $a_i \in K$ und ein primitives $h_i(x) \in R[x]$ mit $g_i(x) = a_i h_i(x)$. Weil $g_i(x)$ irreduzibel in $K[x]$ ist, ist $g_i(x)$ und damit $h_i(x)$ prim in $K[x]$, da a_i Einheit in $K[x]$. Mit Hilfssatz 4.10 ist $h_i(x)$ prim in $R[x]$.

Es folgt also $f(x) = ah_1(x) \cdot \ \ldots \ \cdot h_r(x)$, wobei $a \in K$ und $h_1(x) \cdot \ \ldots \ \cdot h_r(x)$ primitiv ist, d.h. $a \in R$ wegen Korollar 4.9. Ist a Einheit in R, dann ist $ah_1(x)$ prim in $R[x]$ und $f(x) = (ah_1(x))h_2(x) \cdot \ \ldots \ \cdot h_r(x)$ die gewünschte Darstellung von $f(x)$. Ist a keine Einheit in R, dann gilt $a = p_1 \cdot \ \ldots \ \cdot p_s$ mit $p_i \in R$ und p_i prim in R, $i = 1, \ldots, s$. Wegen Lemma 4.6 sind $p_1, \ldots, p_s$ prim in $R[x]$, und $f(x) = p_1 \cdot \ \ldots \ \cdot p_s \cdot h_1(x) \cdot \ \ldots \ \cdot h_r(x)$ ist die gewünschte Darstellung.

□

Beispiel.

1. Der Polynomring $\mathbb{Z}[x]$ über $\mathbb{Z}$ in der Unbestimmten x ist ein Gaußscher Ring, der kein Hauptidealring ist; z.B. ist $2\mathbb{Z}[x] + x\mathbb{Z}[x]$ in $\mathbb{Z}[x]$ kein Hauptideal.

2. Ist K ein Körper und sind $x_1, \ldots, x_n$ endlich viele unabhängige Unbestimmte über K, so ist $K[x_1, \ldots, x_n]$ ein Gaußscher Ring.

Irreduzibilitätskriterien.

1. R sei ein Integritätsbereich und $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in R[x]$. Für jedes $a \in R$ gilt $f(x) = q(x)(x - a) + f(a)$ mit $q(x) \in R[x]$, d.h., $f(x)$ ist irreduzibel in $R[x]$ genau dann, wenn $f(x)$ in R keine Nullstelle hat. Zum Beispiel ist $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ irreduzibel über $\mathbb{Z}_2$, da $f(x)$ in $\mathbb{Z}_2$ keine Nullstelle hat.

2. R sei ein Gaußscher Ring, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ und K der Quotientenkörper von R. Ist $a \in K$ Nullstelle von $f(x)$, so gilt $a \in R$ und a ist Teiler von a_0 in R, denn gilt $a = uv^{-1} \neq 0$ mit teilerfremden $u, v \in R$, so folgt

   $$(*) \qquad u^n + a_{n-1}u^{n-1}v + \cdots + a_1uv^{n-1} + a_0v^n = 0$$

   wegen $f(a) = 0$. Ist also v keine Einheit in R, so hat v einen Primteiler p, der wegen $(*)$ auch u teilt - Widerspruch. Somit ergibt sich $a \in R$, und a ist Teiler von a_0 in R wegen $a^n + a_{n-1}a^{n-1} + \cdots + a_1a = -a_0$.
   Zum Beispiel ist $x^3 + x^2 + 2x + 1 \in \mathbb{Q}[x]$ irreduzibel über $\mathbb{Q}$, denn hätte $x^3 + x^2 + 2x + 1$ eine Nullstelle $a \in \mathbb{Q}$, so wäre $a \in \mathbb{Z}$ und a ganzzahliger Teiler von 1, d.h. $a = 1$ oder $a = -1$; aber 1 und -1 sind keine Nullstellen von $x^3 + x^2 + 2x + 1$.

3. Ist R Gaußscher Ring, K Quotientenkörper von R und $f(x) \in R[x]$ mit $\operatorname{grad} f(x) \geq 1$, dann ist $f(x)$ irreduzibel über K, wenn $f(x)$ irreduzibel in $R[x]$ ist. Denn für jede nichttriviale Zerlegung $f(x) = g_1(x)g_2(x)$ von $f(x)$ in $K[x]$ gibt es $a_1, a_2 \in K$ und primitive Polynome $h_1(x), h_2(x) \in R[x]$ mit $g_1(x) = a_1h_1(x)$ und $g_2(x) = a_2h_2(x)$, also $f(x) = a_1a_2h_1(x)h_2(x)$. Aufgrund von Korollar 4.9 ist $a_1a_2 \in R$, d.h., wir erhalten die nichttriviale Zerlegung $f(x) = (a_1a_2h_1(x))h_2(x)$ von $f(x)$ in $R[x]$.

4. **Eisensteinkriterium:** R sei ein Gaußscher Ring und gegeben sei das primitive Polynom $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$. Gibt es ein Primelement $p \in R$ mit $p \not| a_n, p|a_{n-1}, \ldots, p|a_0$ und $p^2 \not| a_0$, dann ist $f(x)$ irreduzibel in $R[x]$.
   Beweis. Sei $f(x) = g(x)h(x)$ mit $g(x), h(x) \in R[x]$, wobei $g(x) = b_mx^m + \cdots + b_1x + b_0$ und $h(x) = c_lx^l + \cdots + c_1x + c_0$, $b_m, c_l \neq 0$. Da p kein Teiler von $a_n = b_mc_l$ ist, ist p kein Teiler von b_m und kein Teiler von c_l. Da p ein Teiler von $a_0 = b_0c_0$ ist, p^2 aber

nicht, wird entweder b_0 oder c_0 von p geteilt. O.B.d.A. sei p Teiler von b_0, aber kein Teiler von c_0. Sei weiterhin i minimal mit $p \not| b_i$. Wir betrachten

$$a_i = \sum_{j \geq 0} c_j b_{i-j} = c_0 b_i + \sum_{j>0} c_j b_{i-j}.$$

Zunächst wird $c_0 b_i$ nicht von p geteilt, aber p teilt jeden Summanden $c_j b_{i-j}$ für $j > 0$, d.h., p teilt a_i nicht. Der einzige Koeffizient von $f(x)$, den p nicht teilt, ist a_n, also $n = i \leq m \leq n$. Damit ist $n = m$ und $l = 0$, d.h. $h(x) = h \in R$. Wäre nun h keine Einheit in R, so hätte h einen Primteiler q in R, der dann Primteiler von $f(x)$ in $R[x]$ wäre - im Widerspruch dazu, daß $f(x)$ primitiv ist. □

Ist zum Beispiel $p \in \mathbb{N}$ eine Primzahl und $n \in \mathbb{N}$, dann ist $x^n - p \in \mathbb{Z}[x]$ primitiv und nach dem Eisensteinkriterium irreduzibel in $\mathbb{Z}[x]$, also wegen Kriterium 3 irreduzibel über $\mathbb{Q}$.

5. R und R' seien Integritätsbereiche sowie $\varphi : R \longrightarrow R'$ ein Ringhomomorphismus, der die Einselemente aufeinander abbildet. Wir betrachten nun den Ringhomomorphismus $\psi : R[x] \longrightarrow R'[x]$ mit $\psi(x) = x$ und $\psi(r) = \varphi(r)$ für alle $r \in R$. Ist $f(x) \in R[x]$ normiert und $f(x) = g(x)h(x)$ eine nichttriviale Zerlegung von $f(x)$ in $R[x]$, so ist $\psi(f(x)) = \psi(g(x))\psi(h(x))$ eine nichttriviale Zerlegung von $\psi(f(x))$ in $R'[x]$; insbesondere ist also $f(x)$ irreduzibel in $R[x]$, wenn $\psi(f(x))$ irreduzibel in $R'[x]$ ist.

   Dieses Kriterium wird insbesondere für $R = \mathbb{Z}$ und $R' = \mathbb{Z}_p$ mit p Primzahl angewendet, wobei

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_p,\ x \longmapsto \overline{x}$$

   der kanonische Restklassenhomomorphismus ist.

   Beispiel. Wir betrachten das Polynom $f(x) = x^4 + x^2 + x + 1 \in \mathbb{Z}[x]$ und versuchen zunächst, das oben erläuterte Kriterium mit $p = 2$ zu benutzen. Dann gilt

$$\psi(f(x)) = x^4 + x^2 + x + \overline{1} \in \mathbb{Z}_2[x].$$

   Man schreibt auch $\overline{f}(x)$ statt $\psi(f(x))$. Wegen $\overline{f}(\overline{1}) = \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{0}$ hat $\overline{f}(x)$ in $\mathbb{Z}_2$ eine Nullstelle und ist damit reduzibel über $\mathbb{Z}_2$. Über die Irreduzibilität von $f(x)$ in $\mathbb{Z}[x]$ kann keine Aussage gemacht werden

   Wir versuchen nun das Kriterium mit $p = 3$. Es gilt

$$\overline{f}(x) = \psi(f(x)) = x^4 + x^2 + x + \overline{1} \in \mathbb{Z}_3[x].$$

   Wäre $\overline{f}(x)$ in $\mathbb{Z}_3[x]$ reduzibel, so hätte $\overline{f}(x)$ in $\mathbb{Z}_3[x]$ einen irreduziblen (normierten) Teiler vom Grad 1 oder 2. Die einzigen irreduziblen normierten Polynome in $\mathbb{Z}_3[x]$ vom Grad 1 sind x, $x + \overline{1}$ sowie $x + \overline{2}$, und $x^2 + \overline{1}$, $x^2 + x + \overline{2}$ sowie $x^2 + \overline{2}x + \overline{2}$ sind die vom Grad 2. Alle diese teilen aber $\overline{f}(x)$ in $\mathbb{Z}_3[x]$ nicht. Damit ist $\overline{f}(x)$ irreduzibel in $\mathbb{Z}_3[x]$, also $f(x)$ irreduzibel in $\mathbb{Z}[x]$ und damit $f(x)$ irreduzibel über $\mathbb{Q}$.

   Es gibt Polynome $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, die irreduzibel in $\mathbb{Z}[x]$ sind, aber für jede Primzahl p ist $\overline{f}(x)$ reduzibel in $\mathbb{Z}_p[x]$ (siehe Aufgabe 5.19 aus Kapitel 3).

5. Aufgaben

A 5.1 Sei M eine Menge. Dann heißt $A\Delta B := (A \cap (M \setminus B)) \cup (B \cap (M \setminus A))$ für $A, B \subseteq M$ die symmetrische Differenz von A und B. Zeigen Sie, daß die Potenzmenge von M bezüglich Δ als Addition und $\cap$ als Multiplikation ein kommutativer Ring mit Eins ist. Berechnen Sie die Einheiten dieses Ringes.

A 5.2 Zeigen Sie: Ist G eine additiv geschriebene abelsche Gruppe, so ist

$$\mathrm{End}(G) := \{\varphi : G \longrightarrow G \mid \varphi \text{ ist ein Gruppenhomomorphismus}\}$$

ein Ring mit Eins, wobei die Komposition die Multiplikation ist und die Addition durch $\varphi + \psi : G \longrightarrow G,\ g \longmapsto \varphi(g) + \psi(g)$ definiert wird.

A 5.3 Beweisen Sie die Rechenregeln vor Definition 1.2.

A 5.4 Sei $\mathbb{H} = \{\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \mid a,b,c,d \in \mathbb{R}\} \subseteq \mathbb{C}_{2,2}$.

1) Zeigen Sie, daß $\mathbb{H}$ bezüglich der gewöhnlichen Addition und Multiplikation von Matrizen ein Schiefkörper ist, d.h., $\mathbb{H}$ ist ein Ring mit Eins, in dem jedes von 0 verschiedene Element invertierbar ist. $\mathbb{H}$ heißt Hamiltonsche Quaternionenalgebra.

2) Zeigen Sie, daß $R = \{\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}\}$ ein Teilring von $\mathbb{H}$ ist. Die Einheitengruppe von R heißt Quaternionengruppe; vergleichen Sie diese mit den Gruppen aus den Aufgaben 5.16 und 5.17 aus Kapitel 1.

A 5.5 Es sei G eine additiv geschriebene abelsche Gruppe der Ordnung $|G| = p^n$, p prim. Es gelte weiterhin $pg = g + \cdots + g = 0$ für alle $g \in G$. Zeigen Sie, daß man die Gruppe G als n-dimensionalen Vektorraum über $\mathbb{Z}_p$ auffassen kann und daß der Ring $\mathrm{End}(G)$ isomorph zum Ring aller $(n,n)-$Matrizen über $\mathbb{Z}_p$ ist.

A 5.6 Benutzen Sie Aufgabe 5.5 um die Automorphismengruppe (bis auf Isomorphie) der Kleinschen Vierergruppe zu berechnen.

A 5.7 Geben Sie einen Ring R und einen Teilring S so an, daß S ein Einselement hat, R aber nicht.

A 5.8 Geben Sie einen Ring R mit Einselement und einen Teilring S so an, daß S ebenfalls ein Einselement hat, das aber nicht das Einselement von R ist.

A 5.9 Sei K ein Körper und $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in K_{2,2}$ sowie R die Menge aller Matrizen $A \in K_{2,2}$ mit $AM = MA$. Zeigen Sie, daß R ein kommutativer Teilring von $K_{2,2}$ ist und daß R genau dann ein Körper ist, wenn -1 in K kein Quadrat ist.

A 5.10 Es sei p eine Primzahl und $V_p = \{\frac{a}{b} \in \mathbb{Q} \mid p \text{ teilt } b \text{ nicht}\}$. Zeigen Sie, daß jedes Ideal von V_p ein Hauptideal ist und daß die Ideale von V_p bezüglich der Inklusion linear geordnet sind.

A 5.11 Sei R ein Ring mit Eins. Zeigen Sie, daß für jedes Ideal I von R die Menge $I_{n,n}$ der (n,n)-Matrizen über I ein Ideal des Matrizenringes $R_{n,n}$ ist und daß sich jedes Ideal von $R_{n,n}$ auf diese Weise durch ein Ideal I von R darstellen läßt.

A 5.12 Sei R ein Ring mit Eins und I ein Ideal von R. Zeigen Sie $R_{n,n}/I_{n,n} \cong (R/I)_{n,n}$.

A 5.13 Zeigen Sie: Für jeden Körper K hat der Matrizenring $K_{n,n}$ nur die trivialen Ideale.

A 5.14 Es sei R ein Ring und I, J seien Ideale von R. Dann definiert man das Produkt IJ als das von $\{ij \mid i \in I \text{ und } j \in J\}$ erzeugte Ideal von R. Zeigen Sie $IJ \subseteq I \cap J$ und $IJ = I \cap J$, falls $I + J = R$ und R ein Einselement hat.

A 5.15 Es sei R ein kommutativer Ring mit Eins und $I, J \neq R$ zwei verschiedene Ideale von R mit $I + J = R$. Zeigen Sie $R/IJ \cong R/I \times R/J$.

A 5.16 Beweisen Sie den 2. Isomorphiesatz: Sind I und I' Ideale des Ringes R mit $I \subseteq I'$, dann ist I'/I Ideal in R/I und $(R/I)/(I'/I) \cong R/I'$.

A 5.17 Geben Sie einen kommutativen Ring R an, der ein maximales Ideal hat, das kein Primideal ist. Diskutieren Sie dieses Beispiel im Zusammenhang mit Korollar 1.12.

A 5.18 Zeigen Sie, daß in dem Polynomring $R = \mathbb{Z}[x]$ über $\mathbb{Z}$ in der Unbestimmten x das Ideal xR ein Primideal ist, aber nicht maximal, und daß $2R + xR$ kein Hauptideal ist.

A 5.19 K sei ein Körper und $R = K[[x]]$ der Ring der formalen Potenzreihen über K. Zeigen Sie, daß $a_0 + a_1x + a_2x^2 + \cdots \in K[[x]]$ genau dann in R invertierbar ist, wenn $a_0 \neq 0$ gilt. Geben Sie alle Ideale von R an.

A 5.20 Es sei K ein Körper und $K[x]$ der Polynomring über K in der Unbestimmten x. Zeigen Sie, daß $I := \{f(x) \in K[x] \mid f(a) = 0\}$ für jedes $a \in K$ ein maximales Ideal in $K[x]$ ist und daß $K[x]/I \cong K$ gilt.

A 5.21 R sei ein Euklidischer Ring, $a, b \in R\backslash\{0\}$ und $r_1, \ldots, r_n, q_1, \ldots, q_n \in R$ wie im Euklidischen Algorithmus nach Satz 3.5. Die Elemente $s_{-1}, s_0, \ldots, s_n \in R$ sowie $t_{-1}, t_0, \ldots, t_n \in R$ werden rekursiv durch $s_{-1} = 0, s_0 = 1$ und $s_k = q_k s_{k-1} + s_{k-2}$ für $k \geq 1$ sowie $t_{-1} = 1, t_0 = 0$ und $t_k = q_k t_{k-1} + t_{k-2}$ für $k \geq 1$ definiert. Zeigen Sie, daß für alle $k = 0, 1, \ldots, n$ gilt:

$$t_{k-1}r_k + t_k r_{k-1} = b, \quad s_{k-1}r_k + s_k r_{k-1} = a, \quad t_{k-1}s_k - t_k s_{k-1} = (-1)^k.$$

Schließen Sie hieraus $t_{n-1}a - s_{n-1}b = \pm r_{n-1}$. Dieses Verfahren zur Berechnung einer Darstellung des ggT als Linearkombination von a und b heißt Berlekamp-Algorithmus. Unter welchem Gesichtspunkt ist der Berlekamp-Algorithmus besser als das *Rückwärtseinsetzen*?

A 5.22 Zeigen Sie: Ist R ein Euklidischer Ring mit der Wertefunktion $g : R \setminus \{0\} \longrightarrow \mathbb{N}_0$, dann ist R auch bezüglich $h : R \setminus \{0\} \longrightarrow \mathbb{N}_0,\ x \longmapsto \min\{g(xy) \mid y \in R \setminus \{0\}\}$ ein Euklidischer Ring, und h ist sogar regulär, d.h., $h(a) \leq h(ab)$ gilt für alle $a, b \in R \setminus \{0\}$.

A 5.23 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 5.24 K sei ein Körper und $f_1(x), \ldots, f_m(x) \in K[x]$ nichtkonstante, paarweise teilerfremde Polynome sowie

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

Zeigen Sie, daß es zu jedem Polynom $h(x) \in K[x]$ mit $\operatorname{grad} h(x) < \operatorname{grad} f(x)$ eindeutig bestimmte Polynome $h_1(x), \ldots, h_m(x) \in K[x]$ mit $\operatorname{grad} h_i(x) < \operatorname{grad} f_i(x)$ für alle $i = 1, \ldots, m$ so gibt, daß $h(x) = h_1(x)g_1(x) + \cdots + h_m(x)g_m(x)$ gilt.

A 5.25 K sei ein Körper und $f(x) \in K[x]$ ein Polynom mit $\operatorname{grad} f(x) = n \geq 1$. 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 $\operatorname{grad} p_i(x) < \operatorname{grad} f(x)$ für $i = 0, \ldots, m$ so gibt, daß $g(x) = p_m(x)f^m(x) + \cdots + p_1(x)f(x) + p_0(x)$ gilt.

A 5.26 Erläutern Sie die Partialbruchzerlegung gebrochen-rationaler Funktionen mit Hilfe der Aufgaben 5.24 und 5.25.

A 5.27 Es sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Auf $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ sei die Funktion N definiert durch

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

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 $\mathrm{ggT}(\mathrm{N}(x), \mathrm{N}(y))$.

A 5.28 Zeigen Sie für $R = \mathbb{Z}[\sqrt{-3}]$:

a) $1 + \sqrt{-3}$ ist unzerlegbar in R, aber nicht prim.
b) 4 besitzt in R zwei verschiedene Darstellungen als Produkt unzerlegbarer Elemente.
c) 4 und $2(1 + \sqrt{-3})$ haben in R keinen ggT.
d) Berechnen Sie in R 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 5.29 Zeigen Sie, daß $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ mit $d \in \{-2, -1, 2, 3\}$ bezüglich der Funktion N aus Aufgabe 5.27 als Wertefunktion ein Euklidischer Ring ist.

A 5.30 Sei $p \in \mathbb{N}$ eine Primzahl. Ist $p = a^2 + b^2$ mit $a, b \in \mathbb{N}$, dann sind a, b eindeutig bestimmt.

A 5.31 Zeigen Sie, daß $\{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\}$ die Einheitengruppe des Ringes $\mathbb{Z}[\sqrt{2}]$ ist.

A 5.32 Geben Sie alle ganzzahligen Lösungen der Gleichung $x^2 - 2y^2 = 7$ an.

A 5.33 Geben Sie alle ganzzahligen Lösungen der Gleichung $x^2 - 3y^2 = -2$ an.

A 5.34 Berechnen Sie in $\mathbb{Z}[\sqrt{2}]$ einen ggT von 7 und $2 + 3 \cdot \sqrt{2}$ und stellen Sie ihn in der Form $7 \cdot u + (2 + 3 \cdot \sqrt{2}) \cdot v$ mit $u, v \in \mathbb{Z}[\sqrt{2}]$ dar.

A 5.35 Schreiben Sie 7 und $2 + 3 \cdot \sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$ als Produkt von Primelementen.

A 5.36 Zeigen Sie, daß 9 und $6 + 3 \cdot \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ weder einen ggT noch ein kgV haben.

A 5.37 Geben Sie ein Ideal in $\mathbb{Z}[\sqrt{-5}]$ an, das kein Hauptideal ist.

A 5.38 Zeigen Sie, daß 3 in $\mathbb{Z}[\sqrt{-5}]$ unzerlegbar, aber kein Primelement ist.

A 5.39 Es sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Zeigen Sie: Ist $a \in \mathbb{Z}[\sqrt{d}]$ weder 0 noch eine Einheit, so ist a das Produkt unzerlegbarer Elemente aus $\mathbb{Z}[\sqrt{d}]$.

A 5.40 Zeigen Sie, daß $4 - \sqrt{5}$ ein Primelement in $\mathbb{Z}[\sqrt{5}]$ ist. Sind $1 - \sqrt{5}$ und $3 + \sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$ assoziiert?

A 5.41 Sei p eine Primzahl. Zeigen Sie, daß das Polynom $x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ über $\mathbb{Q}$ irreduzibel ist.

A 5.42 Berechnen Sie alle irreduziblen Polynome über $\mathbb{Z}_2$ vom Grad ≤ 4.

A 5.43 Überprüfen Sie die folgenden Polynome auf Irreduzibilität über $\mathbb{Q}$:

a) $x^7 + 2x^5 + 3x^3 - 5x^2 + 9x + 1$,
b) $x^4 + 4x^3 + 6x^2 + 9x + 2$,
c) $x^4 - x^3 + 2x^2 - x + 2$.

A 5.44 Es sei K ein Körper, $n, m \in \mathbb{N}$ sowie d ein ggT von n und m. Zeigen Sie, daß $x^n - 1$ genau dann $x^m - 1$ in $K[x]$ teilt, wenn n Teiler von m ist, und daß $x^d - 1$ ein ggT von $x^n - 1$ und $x^m - 1$ in $K[x]$ ist.

A 5.45 Zeigen Sie, daß $x^3 + y^3 + xy^2 + 3xy + 2x - y$ in $\mathbb{Z}[x, y]$ irreduzibel ist, wobei x und y unabhängige Unbestimmte über $\mathbb{Z}$ sind.

A 5.46 Zeigen Sie, daß $x^4 + 28x^2 + (6 + 9\sqrt{2})x + 2 + 3\sqrt{2}$ über $\mathbb{Q}(\sqrt{2})$ irreduzibel ist.

A 5.47 Zeigen Sie, daß $4x^4 + (-10 - 5\sqrt{-2})x^3 - 15x^2 + 5$ über $\mathbb{Q}(\sqrt{-2})$ irreduzibel ist.

A 5.48 Das Polynom $f(x) \in \mathbb{Z}[x]$ habe den Grad $2k + 1$ und an $2k + 1$ verschiedenen (ganzzahligen) Stellen den Wert 1. Zeigen Sie, daß $f(x)$ irreduzibel über $\mathbb{Q}$ ist, und geben Sie ein sinnvolles Beispiel an.

KAPITEL 3

Körper

1. Körpererweiterungen

Definition 1.1 *Ist K ein Körper und F ein Teilkörper von K, so heißt K Erweiterungskörper von F.*

Bemerkung.

1. Ist K ein Erweiterungskörper des Körpers F, so sagt man auch, daß K/F eine Körpererweiterung ist.

2. Ist K ein Körper, so ist der Durchschnitt F aller Teilkörper von K ein Teilkörper von K (vgl. Bemerkung 2 nach Definition 1.15 aus Kapitel 2); er ist der kleinste Teilkörper von K und heißt Primkörper von K. Der Primkörper eines Körpers hat keine echten Teilkörper.

Satz 1.2 *Ist K ein Körper, so ist der Primkörper von K isomorph zu $\mathbb{Q}$ oder isomorph zu einem $\mathbb{Z}_p$, p prim.*

Beweis. Sei F der Primkörper von K und 1 das gemeinsame Einselement von F und K. Dann ist

$$\psi : \mathbb{Z} \longrightarrow F,\ z \longmapsto z \cdot 1$$

ein Ringhomomorphismus und damit $\psi(\mathbb{Z})$ ein Teilring von F mit $1 \in \psi(\mathbb{Z})$. Als Teilring eines Körpers ist $\psi(\mathbb{Z})$ nullteilerfrei, d.h., $\psi(\mathbb{Z})$ ist ein Integritätsbereich. Wegen des Homomorphiesatzes für Ringe folgt

$$\psi(\mathbb{Z}) \cong \mathbb{Z}/\mathrm{Kern}\psi.$$

Mit Satz 1.9 aus Kapitel 2 ergibt sich, daß $I := \mathrm{Kern}\psi$ ein Primideal in $\mathbb{Z}$ ist. Gilt $I = \{0\}$, so ist ψ injektiv, und aufgrund der universellen Eigenschaft des Quotientenkörpers läßt sich ψ zu einem injektiven Ringhomomorphismus $\psi : \mathbb{Q} \longrightarrow F$ fortsetzen. $\psi(\mathbb{Q})$ ist ein Teilkörper von F, also $\psi(\mathbb{Q}) = F$, da F als Primkörper keine echten Teilkörper hat. Es folgt $F \cong \mathbb{Q}$.

Ist $I \neq \{0\}$, so gilt $I = n\mathbb{Z}$ für ein $n \in \mathbb{N}$, da $\mathbb{Z}$ Hauptidealring ist, und $n = p$ ist prim, wegen Satz 3.7 aus Kapitel 2, also $\psi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$. Wie oben ergibt sich $F = \psi(\mathbb{Z})$, weil $\mathbb{Z}_p$ ein Körper ist, d.h. $F \cong \mathbb{Z}_p$.

□

Korollar 1.3 *Jeder Körper K hat einen eindeutig bestimmten Teilkörper, der entweder zu $\mathbb{Q}$ oder zu einem $\mathbb{Z}_p$, p prim, isomorph ist.*

Bemerkung. Ist K ein Körper, so werden wir im folgenden stets annehmen, daß entweder $\mathbb{Q}$ oder genau ein $\mathbb{Z}_p$, p prim, Teilkörper von K ist. Ist $\mathbb{Q}$ ein Teilkörper von K, so gilt $n \cdot 1 = 1 + \cdots + 1 \neq 0$ für alle $n \in \mathbb{N}$, d.h., K hat die Charakteristik 0, geschrieben $\chi(K) = 0$. Ist $\mathbb{Z}_p$ ein Teilkörper von K, so gilt $p \cdot 1 = 1 + \cdots + 1 = 0$, d.h., K hat die Charakteristik p, geschrieben $\chi(K) = p$. Gilt $\chi(K) = 0$, so ist K ein Erweiterungskörper von $\mathbb{Q}$, gilt $\chi(K) = p$, so ist K ein Erweiterungskörper von $\mathbb{Z}_p$.

Beispiel.

1. Die Körper $\mathbb{R}$ und $\mathbb{C}$ haben die Charakteristik 0 und sind Erweiterungskörper von $\mathbb{Q}$.

2. Der Körper $\mathbb{Z}_p(x)$ der gebrochen-rationalen Funktionen über $\mathbb{Z}_p$ in der Unbestimmten x ist ein Erweiterungskörper von $\mathbb{Z}_p$, d.h., $\mathbb{Z}_p(x)$ ist ein unendlicher Körper mit der Charakteristik p.

Ist K ein Körper und F ein Erweiterungskörper von K, dann ist F in natürlicher Weise ein K-Vektorraum, d.h., die Addition im K-Vektorraum ist die Addition von F und die Multiplikation von Elementen aus K mit Elementen aus F ist die Multiplikation in F. Mit $[F : K]$ bezeichnet man die Dimension von F über K, also $[F : K] = \dim_K F$. Man nennt $[F : K]$ den Erweiterungsgrad der Körpererweiterung F/K, und F/K heißt endliche Körpererweiterung, wenn $[F : K] = \dim_K F < \infty$.

Beispiel. Ist $K = \mathbb{R}$ und $F = \mathbb{C}$, so ist $\{1, i\}$ eine Basis von F über K, denn jedes $z \in \mathbb{C}$ läßt sich eindeutig in der Form $z = a + bi$ mit $a, b \in \mathbb{R}$ schreiben. Also gilt $[\mathbb{C} : \mathbb{R}] = 2$, d.h., $\mathbb{C}/\mathbb{R}$ ist eine endliche Körpererweiterung mit dem Erweiterungsgrad 2. Die Körpererweiterungen $\mathbb{R}/\mathbb{Q}$ und $\mathbb{Z}_p(x)/\mathbb{Z}_p$ sind unendliche Körpererweiterungen.

Satz 1.4 *Sind E/F und F/K Körpererweiterungen, so gilt $[E : K] = [E : F][F : K]$.*

Beweis. Sei $\{e_i \mid i \in I\}$ eine F-Basis von E und $\{f_j \mid j \in J\}$ eine K-Basis von F. Der Satz ist bewiesen, wenn wir gezeigt haben, daß $\{f_j e_i \mid i \in I, j \in J\}$ eine K-Basis von E ist.

$\{f_j e_i \mid i \in I, j \in J\}$ ist linear unabhängig über K: Seien $k_{ij} \in K$ und $k_{ij} \neq 0$ für nur endlich viele Indizes sowie

$$\sum_i (\sum_j k_{ij} f_j) e_i = 0.$$

Wegen $\sum_j k_{ij} f_j \in F$ und der linearen Unabhängigkeit von $\{e_i \mid i \in I\}$ über F folgt zunächst $\sum_j k_{ij} f_j = 0$ für alle $i \in I$. Wegen der linearen Unabhängigkeit von $\{f_j \mid j \in J\}$ über K ergibt sich schließlich $k_{ij} = 0$ für alle $i \in I, j \in J$.

$\{f_j e_i \mid i \in I, j \in J\}$ erzeugt E als K-Vektorraum: Sei $x \in E$. Dann existieren zunächst $y_i \in F$ mit $y_i \neq 0$ für nur endlich viele $i \in I$ und

$$x = \sum_i y_i e_i,$$

da $\{e_i \mid i \in I\}$ eine F-Basis von E ist. Weil $\{f_j \mid j \in J\}$ eine K-Basis von F ist, gibt es weiterhin zu jedem $i \in I$ mit $y_i \neq 0$ Elemente $k_{ij} \in K$ mit

$$y_i = \sum_j k_{ij} f_j,$$

wobei für nur endlich viele Indizes $k_{ij} \neq 0$ gilt. Insgesamt erhalten wir

$$x = \sum_i y_i e_i = \sum_i (\sum_j k_{ij} f_j) e_i.$$

Dabei sind die auftretenden Summen jeweils nur endlich.

□

Korollar 1.5 *Sind E/F und F/K Körpererweiterungen, so gilt:*

1. *Genau dann ist E/K endliche Körpererweiterung, wenn E/F und F/K endliche Körpererweiterungen sind.*

2. *$[E : F]$ und $[F : K]$ sind Teiler von $[E : K]$.*

Anwendung. Oft ist man an den Zwischenkörpern einer Körpererweiterung F/K interessiert; dabei ist ein Zwischenkörper L von F/K ein Teilkörper von F, der K als Teilkörper enthält. Ist etwa $[F : K] = p$ eine Primzahl, so hat F/K keine echten Zwischenkörper. Zum Beispiel gibt es keine echten Teilkörper von $\mathbb{C}$, die $\mathbb{R}$ echt umfassen, da $[\mathbb{C} : \mathbb{R}] = 2$.

Definition 1.6 *K sei ein Körper, F ein Erweiterungskörper sowie $a_1, \ldots, a_n \in F$. Dann ist $K(a_1, \ldots, a_n)$ der kleinste Teilkörper von F, der K und $a_1, \ldots, a_n$ umfaßt. $K(a_1, \ldots, a_n)$ heißt der von $a_1, \ldots, a_n$ erzeugte Erweiterungskörper von K, und F/K heißt einfache Körpererweiterung, wenn es ein $a \in F$ mit $F = K(a)$ gibt. Gilt $F = K(a)$, so heißt a primitives Element der einfachen Körpererweiterung F/K.*

Bemerkung.

1. $K(a_1, \ldots, a_n)$ ist der Durchschnitt aller Teilkörper von F, die K sowie $a_1, \ldots, a_n$ umfassen.

2. Ist $F = K(x)$ der Körper der gebrochen-rationalen Funktionen über K in der Unbestimmten x, dann ist $K(x)$ der kleinste Teilkörper von F, der K und x umfaßt.

Wir untersuchen zunächst einfache Körpererweiterungen $K(a)/K$ und betrachten dazu den Einsetzungshomomorphismus

$$\varphi_a : K[x] \longrightarrow K(a),\ f(x) \longmapsto f(a).$$

Mit $I := \text{Kern}\varphi_a$ unterscheiden wir die zwei Fälle $I = \{0\}$ und $I \neq \{0\}$.
$I = \{0\}$: Für alle vom Nullpolynom verschiedenen Polynome $f(x) \in K[x]$ gilt $f(a) \neq 0$, und *a heißt transzendet über K*. Der Homomorphismus φ_a ist injektiv und läßt sich wegen der universellen Eigenschaft des Quotientenkörpers eindeutig zu einem injektiven Ringhomomorphismus

$$\varphi_a : K(x) \longrightarrow K(a)$$

fortsetzen. $\varphi_a(K(x))$ ist ein Teilkörper von $K(a)$, der den Körper K und a enthält, d.h. $\varphi_a(K(x)) = K(a)$, und

$$\varphi_a : K(x) \longrightarrow K(a) \text{ mit } \varphi_a(x) = a \text{ und } \varphi_a(k) = k \text{ für alle } k \in K$$

ist ein Isomorphismus, also $K(a) \cong K(x)$.
$I \neq \{0\}$: Da $K[x]$ ein Hauptidealring ist, gibt es ein Polynom $f(x) \in K[x], f(x) \neq 0$ mit $I = f(x)K[x]$. Man kann sogar annehmen, daß $f(x)$ normiert ist. Wegen $f(x) \in I = \text{Kern}\varphi_a$ folgt $f(a) = \varphi_a(f(x)) = 0$, d.h., a ist Nullstelle eines vom Nullpolynom verschiedenen Polynoms über K; *a heißt dann algebraisch über K*. Als Teilring von $K(a)$ ist $\varphi_a(K[x])$ nullteilerfrei, und wegen $1 \in \varphi_a(K[x])$ ist $\varphi_a(K[x])$ ein Integritätsbereich. Aufgrund des Homomorphiesatzes für Ringe folgt

$$\varphi_a(K[x]) \cong K[x]/I,$$

d.h., I ist ein Primideal in $K[x]$ wegen Satz 1.9 aus Kapitel 2 und damit ein maximales Ideal von $K[x]$ wegen Korollar 3.11 aus Kapitel 2; also ist $f(x)$ irreduzibel. Mit Satz 1.11 aus Kapitel 2 ist $\varphi_a(K[x])$ ein Teilkörper von $K(a)$, der K und a enthält, d.h. $\varphi_a(K[x]) = K(a)$, also $K(a) \cong K[x]/I$.

Insgesamt haben wir somit folgenden Satz bewiesen:

Satz 1.7 *K sei ein Körper, F ein Erweiterungskörper von K und $a \in F$.*

1. *Ist a transzendent über K, dann ist*

$$\varphi : K(x) \longrightarrow K(a), f(x)g(x)^{-1} \longmapsto f(a)g(a)^{-1}$$

   ein Isomorphismus.

2. *Ist a algebraisch über K, dann gibt es genau ein normiertes irreduzibles Polynom $f(x) \in K[x]$ mit $f(a) = 0$;*

$$\varphi : K[x]/f(x)K[x] \longrightarrow K(a),\ g(x) + f(x)K[x] \longmapsto g(a)$$

   ist ein Isomorphismus. Für jedes $g(x) \in K[x]$ gilt $g(a) = 0$ genau dann, wenn $f(x)$ Teiler von $g(x)$ ist. Unter allen Polynomen $\neq 0$ über K mit a als Nullstelle hat $f(x)$ minimalen Grad.

Definition 1.8 *K sei ein Körper, F ein Erweiterungskörper von K und $a \in F$. Ist a algebraisch über K, so heißt das eindeutig bestimmte normierte irreduzible Polynom aus $K[x]$ mit a als Nullstelle das Minimalpolynom von a über K, geschrieben* $\mathrm{Irr}(a, K)$.

Bemerkung.

1. Unter allen (normierten) Polynomen $\neq 0$ aus $K[x]$ mit a als Nullstelle hat $\mathrm{Irr}(a, K)$ minimalen Grad.

2. Ist $f(x) \in K[x]$ normiert und irreduzibel, so gilt $\mathrm{Irr}(a, K) = f(x)$ genau dann, wenn $f(a) = 0$.

Satz 1.9 *Ist K ein Körper, F ein Erweiterungskörper von K und $a \in F$ algebraisch über K, dann gilt $[K(a) : K] = n$, und $\{1, a, \ldots, a^{n-1}\}$ ist eine K-Basis von $K(a)$, wobei n der Grad des Minimalpolynoms* $\mathrm{Irr}(a, K)$ *von a über K ist.*

Beweis. Die erste Behauptung folgt aus der zweiten. Sei also n der Grad des Minimalpolynoms $\mathrm{Irr}(a, K)$, und wir zeigen, daß $\{1, a, \ldots, a^{n-1}\}$ eine K-Basis von $K(a)$ ist.
$1, a, \ldots, a^{n-1}$ sind linear unabhängig über K: Sind $k_0, k_1, \ldots, k_{n-1} \in K$ mit

$$k_{n-1}a^{n-1} + \cdots + k_1 a + k_0 = 0,$$

so hat das Polynom $f(x) = k_{n-1}x^{n-1} + \cdots + k_1 x + k_0 \in K[x]$ die Nullstelle a in F. Wegen Satz 1.7 folgt $f(x) = 0$, d.h. $k_0 = k_1 = \cdots = k_{n-1} = 0$.
$1, a, \ldots, a^{n-1}$ erzeugen den K-Vektorraum $K(a)$: Wegen Satz 1.7 ist

$$\varphi : K[x]/f(x)K[x] \longrightarrow K(a),\ g(x) + f(x)K[x] \longmapsto g(a)$$

mit $f(x) = \mathrm{Irr}(a, K)$ ein Isomorphismus. Jedes Element aus $K(a)$ läßt sich also als $g(a)$ mit einem $g(x) \in K[x]$ darstellen. Es gibt $q(x), r(x) \in K[x]$ so, daß $g(x) = q(x)f(x) + r(x)$ gilt, wobei $\operatorname{grad} r(x) < \operatorname{grad} f(x) = n$. Ist $r(x) = k_{n-1}x^{n-1} + \cdots + k_1 x + k_0$ mit $k_{n-1}, \ldots, k_0 \in K$, dann folgt

$$g(a) = q(a)f(a) + r(a) = k_0 + k_1 a + \cdots + k_{n-1}a^{n-1},$$

da $f(a) = 0$.

□

Beispiel. Das Polynom $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$ ist irreduzibel über $\mathbb{Q}$, da $f(x)$ in $\mathbb{Z}$ keine Nullstelle hat. Es gibt ein $\alpha \in \mathbb{R}$ mit $f(\alpha) = 0$, d.h., $\alpha \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$ und $\mathrm{Irr}(\alpha, \mathbb{Q}) = x^3 + x + 1$. Wegen Satz 1.9 folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, und zu jedem $\beta \in \mathbb{Q}(\alpha)$ gibt es eindeutig bestimmte $a, b, c \in \mathbb{Q}$ mit

$$\beta = a + b\alpha + c\alpha^2 \in \mathbb{Q}(\alpha).$$

Ist $\beta' \in \mathbb{Q}(\alpha)$ mit $\beta' = a' + b'\alpha + c'\alpha^2$ und $a', b', c' \in \mathbb{Q}$, dann folgt

$$\beta\beta' = aa' + (ba' + b'a)\alpha + (ca' + bb' + ac')\alpha^2 + (bc' + cb')\alpha^3 + cc'\alpha^4.$$

Wegen $\alpha^3+\alpha+1=0$ folgt $\alpha^3=-\alpha-1$ und $\alpha^4=-\alpha^2-\alpha$, so daß man $\beta\beta'$ in der Form

$$\beta\beta'=A+B\alpha+C\alpha^2 \text{ mit } A,B,C\in\mathbb{Q}$$

schreiben kann. Gilt $\beta\neq 0$, so ist $(a,b,c)\neq(0,0,0)$, und die Gleichung $\beta\beta'=1$ führt auf $A=1,B=0,C=0$, also auf ein lineares Gleichungssystem in a',b',c' mit Koeffizienten aus $\mathbb{Q}$, das eindeutig lösbar ist. Für die so berechneten $a',b',c'\in\mathbb{Q}$ gilt dann

$$\beta^{-1}=a'+b'\alpha+c'\alpha^2.$$

Um β^{-1} zu berechnen, kann man auch mit Hilfe des Euklidischen Algorithmus und anschließendem *Rückwärtseinsetzen* zwei Polynome $g(x),h(x)\in\mathbb{Q}[x]$ so berechnen, daß

$$g(x)\cdot(x^3+x+1)+h(x)(a+bx+cx^2)=1$$

gilt, denn wegen $\operatorname{grad}(a+bx+cx^2)<\operatorname{grad} f(x)$ und der Irreduzibilität von $f(x)$ sind $f(x)$ und $a+bx+cx^2$ teilerfremd. Es folgt dann

$$g(\alpha)\cdot(\alpha^3+\alpha+1)+h(\alpha)\cdot(a+b\alpha+c\alpha^2)=1,$$

also $h(\alpha)=\beta^{-1}$, da $\alpha^3+\alpha+1=f(\alpha)=0$. Für $\beta=1+\alpha$ ergibt sich zum Beispiel

$$-(x^3+x+1)+(x^2-x+2)(1+x)=1,$$

also $(1+\alpha)^{-1}=2-\alpha+\alpha^2$.

Definition 1.10 *K sei ein Körper und F ein Erweiterungskörper von K. Dann heißt F algebraisch über K und F/K algebraisch, wenn jedes $a\in F$ algebraisch über K ist.*

Bemerkung. K ist algebraisch über K.

Satz 1.11 *Ist K ein Körper und F ein Erweiterungskörper von K, dann sind folgende Aussagen äquivalent:*

1. *$[F:K]<\infty$.*
2. *F ist algebraisch über K, und es gibt $a_1,\ldots,a_n\in F$ mit $F=K(a_1,\ldots,a_n)$.*
3. *Es gibt $a_1,\ldots,a_n\in F$ mit $F=K(a_1,\ldots,a_n)$, und $a_1,\ldots,a_n$ sind algebraisch über K.*

Beweis. " 1.) $\Longrightarrow$ 2.) " : Sei $\{a_1,\ldots,a_n\}$ eine K-Basis von F. Dann gilt

$$F=a_1K+\cdots+a_nK\subseteq K(a_1,\ldots,a_n)\subseteq F,$$

also $F=K(a_1,\ldots,a_n)$. Zu zeigen bleibt, daß jedes $a\in F$ algebraisch über K ist. Zunächst sind $\{1,a,\ldots,a^n\}$ wegen $n=[F:K]=\dim_K F$ über K linear abhängig, und es gibt $k_0,\ldots,k_n\in K$, nicht alle 0, mit $k_0+k_1a+\cdots+k_na^n=0$. Also ist $f(x)=k_nx^n+\cdots+k_1x+k_0$ ein vom Nullpolynom verschiedenes Polynom über K mit $f(a)=0$, d.h., a ist algebraisch über K.
" 2.) $\Longrightarrow$ 3.) " : Gilt offenbar.

" 3.) $\Longrightarrow$ 1.) " : Wir beweisen die Behauptung durch Induktion nach n, wobei der Induktionsanfang $n = 1$ aus Satz 1.9 folgt. Sei nun $n > 1$ und $F = K(a_1, \ldots, a_{n-1})(a_n)$ mit $a_1, \ldots, a_n$ algebraisch über K. Dann ist $[F : K(a_1, \ldots, a_{n-1})] < \infty$, da a_n algebraisch über $K(a_1, \ldots, a_{n-1})$ ist, und $[K(a_1, \ldots, a_{n-1}) : K] < \infty$ nach Induktionsvoraussetzung. Insgesamt ergibt sich

$$[F : K] = [F : K(a_1, \ldots, a_{n-1})] \cdot [K(a_1, \ldots, a_{n-1}) : K] < \infty.$$

□

Korollar 1.12 *Sind E/F und F/K Körpererweiterungen, so ist E genau dann algebraisch über K, wenn E algebraisch über F und F algebraisch über K ist.*

Beweis. Ist E algebraisch über K, so ist offenbar F algebraisch über K und E algebraisch über F. Sei nun umgekehrt E algebraisch über F und F algebraisch über K. Zu zeigen ist, daß jedes $a \in E$ algebraisch über K ist. Zunächst ist a algebraisch über F, also

$$a^n + b_{n-1}a^{n-1} + \cdots + b_1 a + b_0 = 0$$

mit $b_0, \ldots, b_{n-1} \in F$. Da F algebraisch über K ist, folgt $[K(b_0, \ldots, b_{n-1}) : K] < \infty$ aufgrund von Satz 1.11, und a ist algebraisch über $K(b_0, \ldots, b_{n-1})$, d.h.,

$$[K(b_0, \ldots, b_{n-1}, a) : K(b_0, \ldots, b_{n-1})] < \infty.$$

Insgesamt ergibt sich $[K(b_0, \ldots, b_{n-1}, a) : K] < \infty$, also $[K(a) : K] < \infty$, da $K(a)$ ein Zwischenkörper von $K(b_0, \ldots, b_{n-1}, a)/K$ ist.

□

Korollar 1.13 *K sei ein Körper, E ein Erweiterungskörper von K und F die Menge aller $a \in E$, die algebraisch über K sind. Dann ist F ein Teilkörper von E, der K umfaßt, und F ist in E algebraisch abgeschlossen, d.h., jedes $x \in E, x \notin F$ ist transzendent über F.*

Beweis. Offenbar gilt $K \subseteq F$, und F ist nicht leer. Zu zeigen ist $a - b, ab^{-1} \in F$ für alle $a, b \in F, b \neq 0$. Wegen Satz 1.11 ist $K(a, b)$ ein algebraischer Erweiterungskörper von K, d.h., $a - b, ab^{-1}$ sind als Elemente von $K(a, b)$ algebraisch über K, also $a - b, ab^{-1} \in F$.
Ist nun $x \in E$ algebraisch über F, so ist $F(x)$ ein algebraischer Erweiterungskörper von F wegen Satz 1.11 und wegen Korollar 1.12 algebraisch über K, d.h. $x \in F$ aufgrund der Definition von F.

□

Beispiel. Die reellen Zahlen, die algebraisch über $\mathbb{Q}$ sind, bilden einen Teilkörper von $\mathbb{R}$, den Körper der reellen algebraischen Zahlen. Die komplexen Zahlen, die algebraisch über $\mathbb{Q}$ sind, bilden einen Teilkörper von $\mathbb{C}$, den Körper der algebraischen Zahlen. Die Körper der algebraischen und der reellen algebraischen Zahlen bilden unendliche algebraische Körpererweiterungen von $\mathbb{Q}$.

2. Zerfällungskörper

Ist $f(x) \in \mathbb{Q}[x]$ ein nichtkonstantes Polynom über $\mathbb{Q}$, so hat $f(x)$ eine Nullstelle in $\mathbb{C}$ wegen des Fundamentalsatzes der Algebra, d.h., es gibt einen Erweiterungskörper von $\mathbb{Q}$, in dem $f(x)$ eine Nullstelle hat. Wir wollen nun zeigen, daß es zu jedem Körper K und jedem Polynom $f(x) \in K[x]$ mit $\operatorname{grad} f(x) \geq 1$ einen Erweiterungskörper F gibt, in dem $f(x)$ eine Nullstelle hat.

Satz 2.1 *Ist K ein Körper und $f(x) \in K[x]$ ein Polynom über K mit $n := \operatorname{grad} f(x) \geq 1$, dann gibt es einen Erweiterungskörper F von K mit $[F : K] \leq n$, in dem $f(x)$ eine Nullstelle hat.*

Beweis. O.B.d.A. sei $f(x)$ irreduzibel über K; anderenfalls betrachten wir einen irreduziblen Faktor von $f(x)$ in $K[x]$. Weiterhin können wir sogar annehmen, daß $f(x)$ normiert ist. Wegen der Irreduzibilität von $f(x)$ ist $f(x)K[x] =: I$ ein vom Nullideal verschiedenes Primideal in $K[x]$, d.h., I ist maximal, da $K[x]$ ein Hauptidealring ist, und $K[x]/I$ ist ein Körper. Wir definieren $F := K[x]/I$ sowie $a := x + I = \overline{x} \in F$. Durch

$$\varphi : K \longrightarrow K[x]/I = F,\ k \longmapsto k + I = \overline{k}$$

wird K in F eingebettet, da φ ein injektiver Ringhomomorphismus ist. Identifizieren wir k und $\overline{k}$ für alle $k \in K$, so ist K ein Teilkörper von F. Sei nun

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x].$$

Wir zeigen $f(a) = 0$; dann ist $f(x)$ das Minimalpolynom von a über K, und $f(x)$ hat eine Nullstelle in $K(a)$ mit $[K(a) : K] = n$. Da $f(a) = 0$ gleichbedeutend mit

$$\overline{x}^n + \overline{a_{n-1}}\ \overline{x}^{n-1} + \cdots + \overline{a_1}\ \overline{x} + \overline{a_0} = \overline{0}$$

ist, muß demnach $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in I$ gezeigt werden. Dieses gilt aber offensichtlich, weil $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = f(x) \in f(x)K[x] = I$.

□

Definition 2.2 *K sei ein Körper und $f(x) \in K[x]$ ein nichtkonstantes Polynom über K. Ein Erweiterungskörper F von K heißt Zerfällungskörper von $f(x)$ über K, wenn $f(x)$ über F in Linearfaktoren zerfällt, d.h., wenn es $b, a_1, \ldots, a_n \in F$ mit $f(x) = b(x-a_1)\cdot\ \ldots\ \cdot(x-a_n)$ gibt, $f(x)$ aber über keinem echten Zwischenkörper in Linearfaktoren zerfällt.*

Bemerkung. Ist b wie in Definition 2.2, so gilt $b \in K$.

Beispiel.

1. Ist $f(x) = x^2 + ax + b \in K[x]$ irreduzibel über K, und ist $\alpha \in F$ in einem Erweiterungskörper F von K Nullstelle von $f(x)$, so gilt in $K(\alpha)[x]$

$$f(x) = (x - \alpha)(x - b\alpha^{-1}),$$

d.h., $K(\alpha)$ ist ein Zerfällungskörper von $f(x)$ über K.

2. Das Polynom $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ ist irreduzibel über $\mathbb{Q}$ und hat genau eine reelle Nullstelle $\alpha \in \mathbb{R}$. Dann ist $\mathbb{Q}(\alpha)$ kein Zerfällungskörper von $f(x)$ über $\mathbb{Q}$. Ist nun weiterhin $\epsilon \in \mathbb{C}$ mit $\epsilon^2+\epsilon+1 = 0$, dann ist ϵ algebraisch über $\mathbb{Q}$ mit $\mathrm{Irr}(\epsilon, \mathbb{Q}) = x^2+x+1$, und wegen

$$x^3 - 2 = (x - \alpha)(x - \epsilon\alpha)(x - \epsilon^2\alpha)$$

zerfällt $f(x)$ über $\mathbb{Q}(\alpha, \epsilon)$ in Linearfaktoren; $\mathbb{Q}(\alpha, \epsilon)$ ist sogar ein Zerfällungskörper von $f(x)$ über $\mathbb{Q}$.

Satz 2.3 *K sei ein Körper und $f(x) \in K[x]$ mit* $\operatorname{grad} f(x) \geq 1$. *Ist F ein Erweiterungskörper von K und sind $b, a_1, \ldots, a_n \in F$ mit $f(x) = b(x-a_1)\cdot \ \ldots \ \cdot(x-a_n)$, dann ist $K(a_1, \ldots, a_n)$ ein Zerfällungskörper von $f(x)$ über K.*

Beweis. Zunächst zerfällt $f(x)$ über $K(a_1, \ldots, a_n)$ in Linearfaktoren. Sei nun weiterhin E mit $K \subseteq E \subseteq K(a_1, \ldots, a_n)$ ein Zwischenkörper, über dem $f(x)$ auch in Linearfaktoren zerfällt, d.h.

$$d(x - c_1)\cdot \ \ldots \ \cdot(x - c_n) = f(x) = b(x - a_1)\cdot \ \ldots \ \cdot(x - a_n)$$

mit $d, c_1, \ldots, c_n \in E$. Dann folgt $d = b$, also

$$(x - c_1)\cdot \ \ldots \ \cdot(x - c_n) = (x - a_1)\cdot \ \ldots \ \cdot(x - a_n).$$

Wie in Beispiel 2 nach Satz 4.4 aus Kapitel 2 erklärt, folgt bei geeigneter Indizierung

$$x - c_1 = x - a_1, \ldots, x - c_n = x - a_n,$$

d.h. $c_1 = a_1, \ldots, c_n = a_n$, wobei wir $f(x)$ als Polynom über F auffassen. Es ergibt sich $a_1, \ldots, a_n \in E$, also $K(a_1, \ldots, a_n) \subseteq E$.

□

Im folgenden sind K und K' Körper, und $\varphi : K \longrightarrow K'$ ist ein Isomorphismus, der sich aufgrund der universellen Eigenschaft des Polynomringes $K[x]$ eindeutig zu einem Isomorphismus (den wir auch mit φ bezeichnen)

$$\varphi : K[x] \longrightarrow K'[x]$$

so fortsetzen läßt, daß $\varphi(x) = x$ gilt, d.h.

$$\varphi(a_n x^n + \cdots + a_1 x + a_0) = \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0)$$

mit $a_0, \ldots, a_n \in K$. Ein Polynom $f(x) \in K[x]$ ist genau dann irreduzibel über K bzw. normiert, wenn $\varphi(f(x))$ irreduzibel über K' bzw. normiert ist.

Satz 2.4 *Mit den Bezeichnungen von oben gilt: Ist $f(x) \in K[x]$ irreduzibel über K und ist $a \in F$ Nullstelle von $f(x)$ in einem Erweiterungskörper F von K sowie $a' \in F'$ Nullstelle von $\varphi(f(x))$ in einem Erweiterungskörper F' von K', so läßt sich $\varphi : K \longrightarrow K'$ eindeutig zu einem Isomorphismus*

$$\psi : K(a) \longrightarrow K'(a') \text{ mit } \psi(a) = a'$$

fortsetzen.

Beweis. Sei $n = \operatorname{grad} f(x)$ und o.B.d.A. $f(x)$ normiert. Dann ist $f(x)$ das Minimalpolynom von a über K und $\varphi(f(x))$ das Minimalpolynom von a' über K'. Wegen Satz 1.9 ist $\{1, a, \ldots, a^{n-1}\}$ eine K-Basis von $K(a)$. Jeder Isomorphismus $K(a) \longrightarrow K'(a')$ ist damit eindeutig durch das Bild von a und die Bilder aller $k \in K$ bestimmt, d.h., es gibt höchstens einen Isomorphismus $\psi : K(a) \longrightarrow K'(a')$ mit $\psi(a) = a'$ und $\psi(k) = \varphi(k)$ für alle $k \in K$.

Wir zeigen nun die Existenz. Für den Ringisomorphismus $\varphi : K[x] \longrightarrow K'[x]$ gilt

$$\varphi(f(x)K[x]) = \varphi(f(x))K'[x],$$

und der Einsetzungshomomorphismus

$$\rho : K'[x] \longrightarrow K'(a'),\ g(x) \longrightarrow g(a')$$

hat den Kern $\varphi(f(x))K'[x]$, d.h., der surjektive Ringhomomorphismus

$$\rho \circ \varphi : K[x] \longrightarrow K'(a')$$

hat den Kern $f(x)K[x]$. Aufgrund des Homomorphiesatzes für Ringe ergibt sich schließlich ein Isomorphismus

$$\psi_1 : K[x]/(f(x)K[x]) \longrightarrow K'(a')$$

mit $\psi_1(\overline{x}) = a'$ und $\psi_1(\overline{k}) = \varphi(k)$ für alle $k \in K$. Mit Satz 1.7 haben wir auch einen Isomorphismus

$$\psi_2 : K[x]/(f(x)K[x]) \longrightarrow K(a)$$

mit $\psi_2(\overline{x}) = a$ und $\psi_2(\overline{k}) = k$ für alle $k \in K$. Offenbar ist

$$\psi := \psi_1 \circ \psi_2^{-1} : K(a) \longrightarrow K'(a')$$

der gesuchte Isomorphismus.

□

Korollar 2.5 *Ist K ein Körper, F ein Erweiterungskörper von K und sind $a, a' \in F$ algebraisch über K mit $\operatorname{Irr}(a, K) = \operatorname{Irr}(a', K)$, dann gibt es genau einen K-Isomorphismus $\psi : K(a) \longrightarrow K(a')$ mit $\psi(a) = a'$.*

Bemerkung. Ein Isomorphismus ψ heißt dabei K-Isomorphismus, wenn $\psi(k) = k$ für alle $k \in K$ gilt.

Beispiel. Sei $\epsilon \in \mathbb{C}$ mit $\epsilon^2 + \epsilon + 1 = 0$ und $\sqrt[3]{2} \in \mathbb{R}$ die einzige reelle Nullstelle von $x^3 - 2$ in $\mathbb{C}$. Dann hat $x^3 - 2$ in $\mathbb{C}$ die drei verschiedenen Nullstellen $\sqrt[3]{2}, \epsilon\sqrt[3]{2}, \epsilon^2\sqrt[3]{2}$, und es gibt zum Beispiel genau einen Isomorphismus

$$\psi : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\epsilon\sqrt[3]{2}).$$

Korollar 2.6 *K und K' seien Körper, $\varphi : K \longrightarrow K'$ sei ein Isomorphismus und $f(x) \in K[x]$ mit $n := \operatorname{grad} f(x) \geq 1$. Ist F ein Zerfällungskörper von $f(x)$ über K und F' ein Zerfällungskörper von $\varphi(f(x))$ über K', so gibt es einen Isomorphismus $\psi : F \longrightarrow F'$, der φ fortsetzt.*

Beweis. O.B.d.A. sei $f(x)$ normiert. Wir beweisen das Korollar durch Induktion nach n. Ist $n = 1$, so folgt $F = K$ und $F' = K'$, und wir wählen $\psi = \varphi$. Sei also $n > 1$ und

$$\begin{aligned} F = K(a_1, \ldots, a_n) \quad &\text{mit} \quad f(x) = (x - a_1) \cdot \ \ldots \ \cdot (x - a_n), \\ F' = K'(a'_1, \ldots, a'_n) \quad &\text{mit} \quad \varphi(f(x)) = (x - a'_1) \cdot \ \ldots \ \cdot (x - a'_n). \end{aligned}$$

Sei $g(x) = \operatorname{Irr}(a_1, K)$. Dann folgt

$$\begin{aligned} f(x) &= g(x)h(x) \text{ für ein } h(x) \in K[x], \text{ also} \\ \varphi(f(x)) &= \varphi(g(x))\varphi(h(x)) \text{ mit } \varphi(g(x)), \varphi(h(x)) \in K'[x]. \end{aligned}$$

Mindestens ein a'_i ist Nullstelle von $\varphi(g(x))$. Wir können annehmen, daß dies a'_1 ist, und erhalten $\operatorname{Irr}(a'_1, K') = \varphi(g(x))$. Wegen Satz 2.4 gibt es einen Isomorphismus

$$\psi_1 : K(a_1) \longrightarrow K'(a'_1) \text{ mit } \psi_1(a_1) = a'_1,$$

der φ fortsetzt. Es gilt dann

$$f(x) = (x - a_1)f_1(x) \text{ mit } f_1(x) \in K(a_1)[x],$$

also

$$\varphi(f(x)) = \psi_1(f(x)) = (x - a'_1)\psi_1(f_1(x))$$

mit $\psi_1(f_1(x)) \in K'(a'_1)[x]$. Somit erhalten wir

$$f_1(x) = (x - a_2) \cdot \ \ldots \ \cdot (x - a_n) \text{ und } \psi_1(f_1(x)) = (x - a'_2) \cdot \ \ldots \ \cdot (x - a'_n),$$

d.h., der Körper $F = (K(a_1))(a_2, \ldots, a_n)$ ist ein Zerfällungskörper von $f_1(x)$ über $K(a_1)$, und $F' = (K'(a'_1))(a'_2, \ldots, a'_n)$ ist ein Zerfällungskörper von $\psi_1(f_1(x))$ über $K'(a'_1)$. Wegen $\operatorname{grad} f_1(x) < \operatorname{grad} f(x)$ können wir die Induktionsvoraussetzung anwenden und erhalten einen Isomorphismus

$$\psi : F \longrightarrow F',$$

der ψ_1 und damit φ fortsetzt.

□

Satz 2.7 *K sei ein Körper und $f(x) \in K[x]$ mit $n := \operatorname{grad} f(x) \geq 1$. Dann gibt es einen Zerfällungskörper F von $f(x)$ über K mit $[F : K] \leq n!$, und ist F' auch ein Zerfällungskörper von $f(x)$ über K, so gibt es einen K-Isomorphismus $\psi : F \longrightarrow F'$.*

Beweis. Wir beweisen die Behauptung durch Induktion nach n. Gilt $n = 1$, so ist K einziger Zerfällungskörper von $f(x)$ über K. Sei also $n > 1$. Wegen Satz 2.1 gibt es einen Erweiterungskörper L von K mit $[L : K] \leq n$, in dem $f(x)$ eine Nullstelle a hat. Sei

$$f(x) = (x - a)g(x) \text{ mit } g(x) \in L[x].$$

Aufgrund von $\operatorname{grad} g(x) < \operatorname{grad} f(x)$ und der Induktionsvoraussetzung existiert ein Zerfällungskörper E von $g(x)$ über L mit $[E : L] \leq (n-1)!$, da $\operatorname{grad} g(x) = n - 1$. Somit zerfällt $f(x)$ über E in Linearfaktoren, und E enthält einen Zerfällungskörper F von $f(x)$ über K, wobei $[F : K] \leq [E : K] = [E : L] \cdot [L : K] \leq n!$.
Ist nun F' auch ein Zerfällungskörper von $f(x)$ über K, so gibt es wegen Korollar 2.6 mit $K = K'$ und $\varphi = \mathrm{id}$ einen K-Isomorphismus $\psi : F \longrightarrow F'$.

□

Beispiel.

1. Ist F Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$, so gilt $[F : \mathbb{Q}] = 6 = 3!$, wie in Beispiel 2 nach Definition 2.2 gezeigt wurde.

2. Wegen des Eisensteinkriteriums ist $f(x) = x^3 - 3x^2 + 3 \in \mathbb{Q}[x]$ irreduzibel über $\mathbb{Q}$. Sei $\alpha \in \mathbb{R}$ eine Nullstelle von $f(x)$. Dann ist $F = \mathbb{Q}(\alpha)$ Zerfällungskörper von $f(x)$ über $\mathbb{Q}$, da $f(x)$ in $\mathbb{Q}(\alpha)$ die Nullstellen $\alpha, -\alpha^2 + \alpha + 3, \alpha^2 - 2\alpha$ hat; es gilt $[F : \mathbb{Q}] = 3$.

3. Galoiserweiterungen

Im folgenden ist K ein Körper und $\mathrm{Aut}(K)$ die Menge aller Automorphismen von K; dabei ist ein Automorphismus von K ein bijektiver Ringhomomorphismus $\varphi : K \longrightarrow K$. Offenbar ist $\mathrm{Aut}(K)$ eine Gruppe bezüglich der Hintereinanderschaltung (Komposition) und heißt Automorphismengruppe von K. Ist F ein Erweiterungskörper von K, so definiert man

$$\mathrm{Gal}(F/K) := \{\varphi \in \mathrm{Aut}(F) \mid \varphi(k) = k \text{ für alle } k \in K\}.$$

Man zeigt leicht, daß $\mathrm{Gal}(F/K)$ eine Untergruppe von $\mathrm{Aut}(F)$ ist; $\mathrm{Gal}(F/K)$ heißt Galoisgruppe der Körpererweiterung F/K. Genau die Automorphismen φ von F gehören zu $\mathrm{Gal}(F/K)$, die K elementweise festlassen. Ist zum Beispiel P der Primkörper von K, so läßt jeder Automorphismus φ von K den Körper P elementweise fest, d.h. $\mathrm{Gal}(K/P) = \mathrm{Aut}(K)$.

Lemma 3.1 (Dedekind) *K und K' seien Körper und $\varphi_1, \ldots, \varphi_n$ paarweise verschiedene Einbettungen (injektive Ringhomomorphismen) $\varphi_i : K \longrightarrow K'$. Dann sind $\varphi_1, \ldots, \varphi_n$ linear unabhängig über K', d.h., sind $x_1, \ldots, x_n \in K'$ so, daß*

$$x_1\varphi_1(a) + \cdots + x_n\varphi_n(a) = 0$$

für alle $a \in K$ gilt, dann folgt $x_1 = \cdots = x_n = 0$.

Beweis. Wir beweisen das Lemma durch Induktion nach n. Ist $n = 1$, so folgt insbesondere $x_1\varphi_1(1) = 0$, also $x_1 = 0$, da $\varphi_1(1) \neq 0$. Sei nun $n > 1$. Wegen $\varphi_1 \neq \varphi_n$ existiert $a' \in K$ mit $\varphi_1(a') \neq \varphi_n(a')$. Für alle $a \in K$ folgt

$$x_1\varphi_1(a'a) + x_2\varphi_2(a'a) + \cdots + x_n\varphi_n(a'a) = 0,$$

also
$$x_1\varphi_1(a')\varphi_1(a) + x_2\varphi_2(a')\varphi_2(a) + \cdots + x_n\varphi_n(a')\varphi_n(a) = 0.$$

Es gilt weiterhin

$$x_1\varphi_1(a')\varphi_1(a) + x_2\varphi_1(a')\varphi_2(a) + \cdots + x_n\varphi_1(a')\varphi_n(a) = 0.$$

Subtrahiert man die linken Seiten der beiden letzten Gleichungen, so folgt für alle $a \in K$

$$x_2(\varphi_2(a') - \varphi_1(a'))\varphi_2(a) + \cdots + x_n(\varphi_n(a') - \varphi_1(a'))\varphi_n(a) = 0.$$

Nach Induktionsvoraussetzung ergibt sich hieraus

$$x_2(\varphi_2(a') - \varphi_1(a')) = \cdots = x_n(\varphi_n(a') - \varphi_1(a')) = 0.$$

Mit $\varphi_n(a') \neq \varphi_1(a')$ ist $x_n = 0$, d.h., für alle $a \in K$ gilt

$$x_1\varphi_1(a) + \cdots + x_{n-1}\varphi_{n-1}(a) = 0,$$

also $x_1 = \cdots = x_{n-1} = 0$ nach Induktionsvoraussetzung.

□

Satz 3.2 *K und K' seien Körper und $\varphi_1, \ldots, \varphi_n$ paarweise verschiedene Einbettungen $\varphi_i : K \longrightarrow K'$. Dann ist*

$$E := \{x \in K \mid \varphi_1(x) = \cdots = \varphi_n(x)\}$$

ein Teilkörper von K mit $[K : E] \geq n$.

Beweis. Wir zeigen zunächst, daß E ein Teilkörper von K ist. Mit $\varphi_1(0) = \cdots = \varphi_n(0) = 0$ ist 0 in E, d.h., E ist nicht leer. Seien nun $x, y \in E$. Dann gilt $\varphi_1(x) = \cdots = \varphi_n(x)$ sowie $\varphi_1(y) = \cdots = \varphi_n(y)$, und es folgt

$$\varphi_1(x) - \varphi_1(y) = \cdots = \varphi_n(x) - \varphi_n(y), \text{ also } \varphi_1(x - y) = \cdots = \varphi_n(x - y),$$

d.h., $x - y \in E$. Entsprechend ergibt sich $xy^{-1} \in E$ falls $y \neq 0$.

Um $[K : E] \geq n$ zu zeigen, nehmen wir an, daß $\{a_1, \ldots, a_r\}$ mit $r < n$ eine E-Basis von K ist, und führen das zum Widerspruch. Dazu betrachten wir das folgende homogene lineare Gleichungssystem über K':

$$\begin{array}{ccccccc} x_1\varphi_1(a_1) & + & \ldots & + & x_n\varphi_n(a_1) & = & 0 \\ & & \vdots & & & & \vdots \\ x_1\varphi_1(a_r) & + & \ldots & + & x_n\varphi_n(a_r) & = & 0 \end{array}$$

Da es mehr Unbekannte als Gleichungen hat, existiert eine nichttriviale Lösung $(x_1, \ldots, x_n)$ über K'. Wir zeigen, daß

$$x_1\varphi_1(a) + \cdots + x_n\varphi_n(a) = 0$$

für alle $a \in K$ gilt - im Widerspruch zu Lemma 3.1. Zunächst gibt es $e_1, \ldots, e_r \in E$ mit

$$a = e_1a_1 + \cdots + e_ra_r,$$

also

$$\begin{aligned} x_1\varphi_1(a) + \cdots + x_n\varphi_n(a) &= x_1 \sum_{i=1}^{r} \varphi_1(e_i)\varphi_1(a_i) + \cdots + x_n \sum_{i=1}^{r} \varphi_n(e_i)\varphi_n(a_i) \\ &= \sum_{j=1}^{n} \sum_{i=1}^{r} x_j\varphi_j(e_i)\varphi_j(a_i) \\ &\overset{(*)}{=} \sum_{i=1}^{r} \varphi_1(e_i)\big(\sum_{j=1}^{n} x_j\varphi_j(a_i)\big) \\ &= \sum_{i=1}^{r} \varphi_1(e_i) \cdot 0 \\ &= 0. \end{aligned}$$

Dabei ergibt sich Gleichung $(*)$ aus der Voraussetzung $\varphi_1(x) = \cdots = \varphi_n(x)$ für alle $x \in E$. □

Bemerkung. Im folgenden betrachten wir insbesondere den Spezialfall, in dem $K = K'$ gilt und $G = \{\varphi_1, \ldots, \varphi_n\}$ eine Untergruppe der Automorphismengruppe $\mathrm{Aut}(K)$ ist. Dann enthält G die identische Abbildung, und es folgt

$$E = \{x \in K \mid \varphi_1(x) = \cdots = \varphi_n(x)\} = \{x \in K \mid \varphi(x) = x \text{ für alle } \varphi \in G\},$$

d.h., G ist Untergruppe von $\mathrm{Gal}(K/E)$; es gilt $[K : E] \geq |G|$.

Definition 3.3 *Ist K ein Körper und G eine Untergruppe von $\mathrm{Aut}(K)$, so heißt*

$$\Phi(G) = \{x \in K \mid \varphi(x) = x \textit{ für alle } \varphi \in G\}$$

Fixkörper von G.

Bemerkung. Ist G eine unendliche Untergruppe von $\mathrm{Aut}(K)$, so ist $\Phi(G)$ auch ein Teilkörper von K, und es gilt $[K : \Phi(G)] = \infty$.

Beispiel. Sei K ein Körper und $G = \{\varphi_1, \ldots, \varphi_n\}$ eine endliche Untergruppe der Automorphismengruppe $\mathrm{Aut}(K)$. Für jedes $a \in K$ nennt man

$$S_G(a) = \varphi_1(a) + \cdots + \varphi_n(a)$$

die G-Spur von a. Offenbar gilt $S_G(a) \in \Phi(G)$ für alle $a \in K$, d.h., $S_G(a)$ ist invariant unter jedem $\varphi \in G$, denn für jedes $\varphi \in G$ gilt

$$\{\varphi \circ \varphi_1, \ldots, \varphi \circ \varphi_n\} = \{\varphi_1, \ldots, \varphi_n\},$$

also
$$\begin{aligned}\varphi(S_G(a)) &= \varphi\circ\varphi_1(a)+\cdots+\varphi\circ\varphi_n(a)\\ &= \varphi_1(a)+\cdots+\varphi_n(a)\\ &= S_G(a).\end{aligned}$$

Wegen Lemma 3.1 kann $\varphi_1(a)+\cdots+\varphi_n(a)=0$ nicht für alle $a\in K$ gelten, d.h., es gibt ein $a\in K$ mit $S_G(a)\neq 0$.

Satz 3.4 *K sei ein Körper und G eine endliche Untergruppe von* $\mathrm{Aut}(K)$*. Dann gilt*

$$[K:\Phi(G)]=|G|.$$

Beweis. Sei $G=\{\varphi_1,\ldots,\varphi_n\}$. Wegen Satz 3.2 gilt $[K:\Phi(G)]\geq n$, und wir zeigen nun $[K:\Phi(G)]\leq n$. Dazu seien $a_1,\ldots,a_m\in K$ mit $m>n$. Die Behauptung ist bewiesen, wenn nachgewiesen ist, daß dann $a_1,\ldots,a_m$ linear abhängig über $\Phi(G)$ sind. Wegen $m>n$ hat das lineare Gleichungssytem

$$\begin{array}{ccccccc} x_1\varphi_1^{-1}(a_1) & + & \ldots & + & x_m\varphi_1^{-1}(a_m) & = & 0\\ & & \vdots & & & & \vdots\\ x_1\varphi_n^{-1}(a_1) & + & \ldots & + & x_m\varphi_n^{-1}(a_m) & = & 0 \end{array}$$

eine nichttriviale Lösung $(x_1,\ldots,x_m)\in K^m$. O.B.d.A. sei $x_1\neq 0$. Wie im obigen Beispiel erläutert, existiert ein $a\in K$ mit $S_G(a)=\varphi_1(a)+\cdots+\varphi_n(a)\neq 0$, und $(a,ax_1^{-1}x_2,\ldots,ax_1^{-1}x_m)$ ist ebenfalls eine nichttriviale Lösung des obigen Systems. O.B.d.A. können wir also gleich annehmen, daß $x_1=a$ gilt. Dann folgt

$$\begin{array}{ccccccc} \varphi_1(x_1)a_1 & + & \ldots & + & \varphi_1(x_m)a_m & = & 0\\ & & \vdots & & & & \vdots\\ \varphi_n(x_1)a_1 & + & \ldots & + & \varphi_n(x_m)a_m & = & 0, \end{array}$$

d.h. $S_G(x_1)a_1+\cdots+S_G(x_m)a_m=0$ mit $S_G(x_1),\ldots,S_G(x_m)\in\Phi(G)$ und $S_G(x_1)\neq 0$. Somit sind $a_1,\ldots,a_m$ linear abhängig über $\Phi(G)$.

□

Definition 3.5 *Ist K ein Körper und F ein Erweiterungskörper von K, so heißt F/K Galoiserweiterung, wenn $K=\Phi(\mathrm{Gal}(F/K))$ gilt.*

Bemerkung.

1. Es gilt stets $K\subseteq\Phi(\mathrm{Gal}(F/K))$.
2. Ist F/K endliche Körpererweiterung, so gilt wegen Satz 3.4 und Bemerkung 1
$$|\mathrm{Gal}(F/K)|=[F:\Phi(\mathrm{Gal}(F/K))]\leq[F:K]<\infty.$$
Eine endliche Körpererweiterung F/K ist somit genau dann Galoiserweiterung, wenn $[F:K]=|\mathrm{Gal}(F/K)|$. Da $[F:K]\geq|\mathrm{Gal}(F/K)|$ stets gilt, ist F/K endliche Galoiserweiterung, wenn $[F:K]\leq|\mathrm{Gal}(F/K)|$.

Satz 3.6 (Hauptsatz der Galoistheorie) *K sei ein Körper und F ein Erweiterungskörper von K. Ist F/K eine endliche Galoiserweiterung und $G = \mathrm{Gal}(F/K)$, so induziert die Zuordnung*

$$U \longmapsto \Phi(U)$$

eine antitone Bijektion zwischen der Menge aller Untergruppen von G und der Menge aller Zwischenkörper von F/K.

Bemerkung. Daß Φ antiton ist bedeutet, $U_1 \subseteq U_2 \Longrightarrow \Phi(U_2) \subseteq \Phi(U_1)$ gilt für alle Untergruppen U_1 und U_2 von $G = \mathrm{Gal}(F/K)$.

Beweis von Satz 3.6. Wir zeigen zunächst, daß Φ antiton ist: Sind U_1 und U_2 Untergruppen von G mit $U_1 \subseteq U_2$, so gilt

$$\begin{aligned} \Phi(U_2) &= \{x \in F \mid \varphi(x) = x \text{ für alle } \varphi \in U_2\} \\ &\subseteq \{x \in F \mid \varphi(x) = x \text{ für alle } \varphi \in U_1\} \\ &= \Phi(U_1). \end{aligned}$$

Die Bijektivität von Φ beweisen wir nun dadurch, daß wir die Umkehrabbildung von Φ angeben. Dazu sei L ein Zwischenkörper von F/K.

$$\Gamma(L) := \{\varphi \in G \mid \varphi(l) = l \text{ für alle } l \in L\}.$$

Offenbar gilt $\Gamma(L) = \mathrm{Gal}(F/L)$, und $\Gamma(L)$ ist Untergruppe von $\mathrm{Gal}(F/K)$. Sind nun L_1 und L_2 Zwischenkörper von F/K mit $L_1 \subseteq L_2$, so folgt

$$\begin{aligned} \Gamma(L_2) &= \{\varphi \in G \mid \varphi(l) = l \text{ für alle } l \in L_2\} \\ &\subseteq \{\varphi \in G \mid \varphi(l) = l \text{ für alle } l \in L_1\} \\ &= \Gamma(L_1). \end{aligned}$$

Wir zeigen nun für alle Untergruppen U von G

(∗) $U \subseteq \Gamma(\Phi(U))$.
Ist $\varphi \in U$, so gilt $\varphi(x) = x$ für alle $x \in \Phi(U)$ aufgrund der Definition von $\Phi(U)$. Aufgrund der Definition von Γ ergibt sich $\varphi \in \Gamma(\Phi(U))$.

Entsprechend beweist man für Zwischenkörper L von F/K

(∗∗) $L \subseteq \Phi(\Gamma(L))$.

Γ ist die Umkehrabbildung von Φ, wenn wir

$$U = \Gamma(\Phi(U)) \text{ und } L = \Phi(\Gamma(L))$$

für alle Untergruppen U von G und alle Zwischenkörper L von F/K gezeigt haben.

Wegen $(*)$ ist $\Phi(\Gamma(\Phi(U))) \subseteq \Phi(U)$, da Φ antiton ist, und wegen $(**)$ ist $\Phi(U) \subseteq \Phi(\Gamma(\Phi(U)))$, also

$$\Phi(U) = \Phi(\Gamma(\Phi(U))).$$

Mit Satz 3.4 erhalten wir

$$|U| = [F : \Phi(U)] = [F : \Phi(\Gamma(\Phi(U)))] = |\Gamma(\Phi(U))|.$$

Da G endlich ist und $U \subseteq \Gamma(\Phi(U))$ wegen $(*)$ gilt, erhalten wir $U = \Gamma(\Phi(U))$.

Wir zeigen nun $L = \Phi(\Gamma(L))$. Für jeden Automorphismus $\varphi \in G = \mathrm{Gal}(F/K)$ ist die Einschränkung $\varphi_{_L} : L \longrightarrow F$ ein injektiver Ringhomomorphismus (eine Einbettung). Für alle $\varphi, \psi \in G$ gilt

$$\begin{aligned}
\varphi_{_L} = \psi_{_L} &\iff \varphi(l) = \psi(l) \text{ für alle } l \in L \\
&\iff \psi^{-1}\varphi(l) = l \text{ für alle } l \in L \\
&\iff \psi^{-1}\varphi \in \Gamma(L) \\
&\iff \varphi \cdot \Gamma(L) = \psi \cdot \Gamma(L).
\end{aligned}$$

Es gibt also genau $s := (G : \Gamma(L))$ verschiedene Einbettungen $\varphi_{1_{_L}}, \ldots, \varphi_{s_{_L}}$. Wegen

$$\{x \in L \mid \varphi_{1_{_L}}(x) = \cdots = \varphi_{s_{_L}}(x)\} = \{x \in L \mid \varphi(x) = x \text{ für alle } \varphi \in G\} = K$$

und Satz 3.2 erhalten wir

$$[L : K] \geq s = (G : \Gamma(L)).$$

Insgesamt ergibt sich

$$\begin{aligned}
|G| = [F : K] &= [F : \Phi(\Gamma(L))] \cdot [\Phi(\Gamma(L)) : L] \cdot [L : K] \\
&\geq |\Gamma(L)| \cdot [\Phi(\Gamma(L)) : L] \cdot (G : \Gamma(L)) \\
&\geq (G : \Gamma(L)) \cdot |\Gamma(L)| \\
&= |G|,
\end{aligned}$$

also $\Phi(\Gamma(L)) = L$.

□

Bemerkung.

1. Auf die Voraussetzung $[F : K] < \infty$ kann im Hauptsatz nicht verzichtet werden.

2. Ist F/K eine endliche Galoiserweiterung, U eine Untergruppe von $\mathrm{Gal}(F/K)$ und $L = \Phi(U)$ der zugehörige Fixkörper, so wurde im Beweis des Hauptsatzes insbesondere gezeigt, daß zwei Automorphismen $\varphi, \psi \in \mathrm{Gal}(F/K)$ genau dann auf L übereinstimmen, wenn φ und ψ in derselben Linksnebenklasse von U liegen, d.h. $\varphi \cdot U = \psi \cdot U$.

Beispiel. F sei der Zerfällungskörper von $f(x) = x^3 - 2$ über $\mathbb{Q}$, also $F = \mathbb{Q}(\sqrt[3]{2}, \epsilon)$; dabei ist $\sqrt[3]{2} \in \mathbb{R}$ die einzige reelle Nullstelle von $x^3 - 2$ in $\mathbb{C}$ und $\epsilon \in \mathbb{C}$ mit $\epsilon^2 + \epsilon + 1 = 0$, d.h., ϵ ist algebraisch über $\mathbb{Q}$ mit $\mathrm{Irr}(\epsilon, \mathbb{Q}) = x^2 + x + 1$. Wir berechnen $\mathrm{Gal}(F/K)$, wobei $K = \mathbb{Q}$ der Primkörper von F ist; es gilt also $\mathrm{Gal}(F/K) = \mathrm{Aut}(F)$. In F hat $f(x)$ die drei verschiedenen Nullstellen

$$\sqrt[3]{2},\ \epsilon\sqrt[3]{2} \text{ und } \epsilon^2\sqrt[3]{2}.$$

Da jeder Automorphismus $\varphi \in \mathrm{Gal}(F/K)$ durch $\varphi(\sqrt[3]{2})$ und $\varphi(\epsilon)$ eindeutig festgelegt ist, überlegen wir uns zunächst, welche Elemente aus F überhaupt als Bilder von $\sqrt[3]{2}$ und ϵ in Frage kommen. Folgende Überlegungen gelten ganz allgemein für jede Körpererweiterung F/K:

Ist $a \in F$ algebraisch über K und $f(x) \in K[x]$ mit $f(a) = 0$, dann ist auch $\varphi(a)$ Nullstelle von $f(x)$ für jedes $\varphi \in \mathrm{Gal}(F/K)$. Um das einzusehen, betrachten wir

$$f(x) = a_m x^m + \cdots + a_1 x + a_0 \in K[x].$$

Gilt $f(a) = 0$, so folgt für jedes $\varphi \in \mathrm{Gal}(F/K)$

$$\begin{aligned} 0 = \varphi(f(a)) &= \varphi(a_m a^m + \cdots + a_1 a + a_0) \\ &= \varphi(a_m)\varphi(a)^m + \cdots + \varphi(a_1)\varphi(a) + \varphi(a_0) \\ &= a_m \varphi(a)^m + \cdots + a_1 \varphi(a) + a_0 \\ &= f(\varphi(a)). \end{aligned}$$

Da das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ in F die Nullstellen $\sqrt[3]{2},\ \epsilon\sqrt[3]{2},\ \epsilon^2\sqrt[3]{2}$ und das Minimalpolynom von ϵ über $\mathbb{Q}$ in F die Nullstellen ϵ und ϵ^2 hat, gilt für jedes $\varphi \in \mathrm{Gal}(F/K)$

$$\varphi(\sqrt[3]{2}) \in \{\sqrt[3]{2},\ \epsilon\sqrt[3]{2},\ \epsilon^2\sqrt[3]{2}\}, \quad \varphi(\epsilon) \in \{\epsilon, \epsilon^2\}.$$

Damit hat $\mathrm{Gal}(F/K)$ höchstens 6 Elemente. Wir zeigen, daß $\mathrm{Gal}(F/K)$ genau 6 Elemente hat. Wegen

$$6 = [F : K] = [F : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[3]{2})] \cdot 3$$

folgt $[F : \mathbb{Q}(\sqrt[3]{2})] = 2$. Mit $F = \mathbb{Q}(\sqrt[3]{2})(\epsilon)$ und $\epsilon^2 + \epsilon + 1 = 0$ ist $x^2 + x + 1$ auch das Minimalpolynom von ϵ über $\mathbb{Q}(\sqrt[3]{2})$. Wegen Korollar 2.5 und $\mathbb{Q}(\sqrt[3]{2})(\epsilon) = \mathbb{Q}(\sqrt[3]{2})(\epsilon^2)$ gibt es einen Automorphismus τ von $F = \mathbb{Q}(\sqrt[3]{2})(\epsilon)$ mit

$$\tau(\epsilon) = \epsilon^2 \text{ und } \tau(\sqrt[3]{2}) = \sqrt[3]{2}.$$

Entsprechend überlegt man sich, daß $[F : \mathbb{Q}(\epsilon)] = 3$ gilt, d.h., $x^3 - 2$ ist auch das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}(\epsilon)$. Wegen Korollar 2.5 und $\mathbb{Q}(\epsilon)(\sqrt[3]{2}) = \mathbb{Q}(\epsilon)(\epsilon\sqrt[3]{2})$ gibt es einen Automorphismus σ von $F = \mathbb{Q}(\epsilon)(\sqrt[3]{2})$ mit

$$\sigma(\sqrt[3]{2}) = \epsilon\sqrt[3]{2} \text{ und } \sigma(\epsilon) = \epsilon.$$

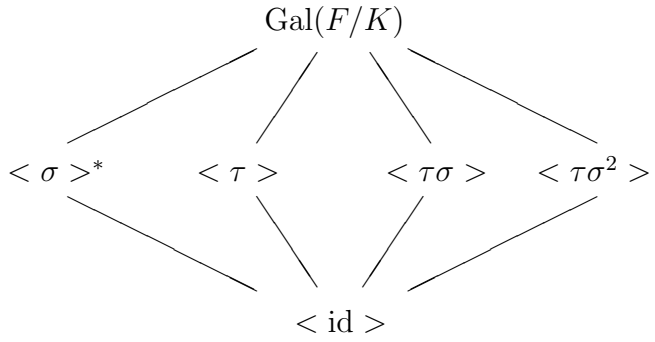
Wir zeigen nun, daß wir mit $\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$ tatsächlich 6 verschiedene Automorphismen aus $\mathrm{Gal}(F/K)$ erhalten haben. Dazu berechnen wir die Bilder von $\sqrt[3]{2}$ und ϵ unter $\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$:

- $\mathrm{id}(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \mathrm{id}(\epsilon) = \epsilon.$
- $\sigma(\sqrt[3]{2}) = \epsilon\sqrt[3]{2}, \quad \sigma(\epsilon) = \epsilon.$
- $\sigma^2(\sqrt[3]{2}) = \sigma(\epsilon\sqrt[3]{2}) = \sigma(\epsilon)\sigma(\sqrt[3]{2}) = \epsilon^2\sqrt[3]{2}, \quad \sigma^2(\epsilon) = \sigma(\epsilon) = \epsilon.$
- $\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\epsilon) = \epsilon^2.$
- $\tau\sigma(\sqrt[3]{2}) = \tau(\epsilon\sqrt[3]{2}) = \tau(\epsilon)\tau(\sqrt[3]{2}) = \epsilon^2\sqrt[3]{2}, \quad \tau\sigma(\epsilon) = \tau(\epsilon) = \epsilon^2.$
- $\tau\sigma^2(\sqrt[3]{2}) = \tau(\epsilon^2\sqrt[3]{2}) = \tau(\epsilon)^2\tau(\sqrt[3]{2}) = \epsilon\sqrt[3]{2}, \quad \tau\sigma^2(\epsilon) = \tau(\epsilon) = \epsilon^2.$

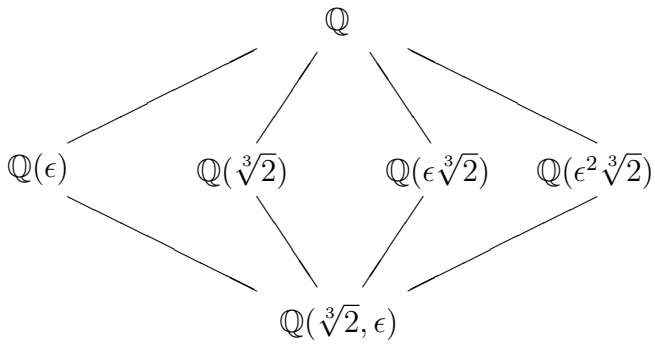
Wegen $\sigma\tau = \tau\sigma^2 \neq \tau\sigma$ ist $\mathrm{Gal}(F/K)$ eine nichtabelsche Gruppe mit 6 Elementen, d.h.

$$\mathrm{Gal}(F/K) \cong \mathbf{S}_3 \cong \mathrm{D}_3.$$

Mit $[F : \mathbb{Q}] = 6 = |\mathrm{Gal}(F/K)|$ ist F/K aufgrund von Bemerkung 2 nach Definition 3.5 eine Galoiserweiterung. Für $\mathrm{Gal}(F/K)$ ergibt sich folgender Untergruppenverband:



$< \sigma >$ ist der einzige nichttriviale Normalteiler in $\mathrm{Gal}(F/K)$. Die Fixkörper der Untergruppen sind wegen des Hauptsatzes genau die Zwischenkörper von F/K, also genau die Teilkörper von F, da $K = \mathbb{Q}$. Es ergibt sich folgender Teilkörperverband von F:



Wir rechnen nun nach, daß der obige Zwischenkörperverband tatsächlich aus dem Untergruppenverband von $\mathrm{Gal}(F/K)$ mit Hilfe der Funktion Φ hervorgeht.

- Da F/K eine Galoiserweiterung ist, ist $\mathbb{Q}$ der Fixkörper von $\mathrm{Gal}(F/K)$.
- Wegen $3 = |<\sigma>| = [F : \Phi(<\sigma>)]$ ergibt sich $[\Phi(<\sigma>) : \mathbb{Q}] = 2$.
  Mit $\sigma(\epsilon) = \epsilon$ folgt $\mathbb{Q}(\epsilon) \subseteq \Phi(<\sigma>)$, also $\mathbb{Q}(\epsilon) = \Phi(<\sigma>)$.
- Wegen $2 = |<\tau>| = [F : \Phi(<\tau>)]$ ergibt sich $[\Phi(<\tau>) : \mathbb{Q}] = 3$.
  Mit $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ folgt $\mathbb{Q}(\sqrt[3]{2}) \subseteq \Phi(<\tau>)$, also $\mathbb{Q}(\sqrt[3]{2}) = \Phi(<\tau>)$.
- Wegen $2 = |<\tau\sigma>| = [F : \Phi(<\tau\sigma>)]$ ergibt sich $[\Phi(<\tau\sigma>) : \mathbb{Q}] = 3$.
  Mit $\tau\sigma(\epsilon\sqrt[3]{2}) = \epsilon\sqrt[3]{2}$ folgt $\mathbb{Q}(\epsilon\sqrt[3]{2}) \subseteq \Phi(<\tau\sigma>)$, also $\mathbb{Q}(\epsilon\sqrt[3]{2}) = \Phi(<\tau\sigma>)$.
- Wegen $2 = |<\tau\sigma^2>| = [F : \Phi(<\tau\sigma^2>)]$ ergibt sich $[\Phi(<\tau\sigma^2>) : \mathbb{Q}] = 3$.
  Mit $\tau\sigma^2(\epsilon^2\sqrt[3]{2}) = \epsilon^2\sqrt[3]{2}$ folgt $\mathbb{Q}(\epsilon^2\sqrt[3]{2}) \subseteq \Phi(<\tau\sigma^2>)$, also $\mathbb{Q}(\epsilon^2\sqrt[3]{2}) = \Phi(<\tau\sigma^2>)$.
- Offenbar ist F der Fixkörper von $\{\mathrm{id}\}$.

Bemerkung. F/K sei eine Galoiserweiterung, U eine Untergruppe von $\mathrm{Gal}(F/K)$ und L ein Zwischenkörper von F/K. Ist $\varphi \in \mathrm{Gal}(F/K)$, dann ist $\varphi U \varphi^{-1}$ Untergruppe von $\mathrm{Gal}(F/K)$ und $\varphi(L)$ Zwischenkörper von F/K. Die Untergruppen U und $\varphi U \varphi^{-1}$ sowie die Zwischenkörper L und $\varphi(L)$ heißen konjugiert. Ist nun L der Fixkörper von U, also $L = \Phi(U)$, dann gilt für alle $x \in F$:

$$\begin{aligned} x \in \varphi(L) &\iff \varphi^{-1}(x) \in L = \Phi(U) \\ &\iff \forall \sigma \in U : \sigma(\varphi^{-1}(x)) = \varphi^{-1}(x) \\ &\iff \forall \sigma \in U : \varphi\sigma\varphi^{-1}(x) = x \\ &\iff x \in \Phi(\varphi U \varphi^{-1}). \end{aligned}$$

Es folgt also $\varphi(L) = \Phi(\varphi U \varphi^{-1})$, d.h., $\varphi(L)$ ist der Fixkörper von $\varphi U \varphi^{-1}$, und U ist genau dann Normalteiler in $\mathrm{Gal}(F/K)$, wenn $\varphi(L) = L$ für alle $\varphi \in \mathrm{Gal}(F/K)$ gilt. Im obigen Beispiel gilt

$$\sigma(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\epsilon\sqrt[3]{2}) \text{ und } \mathbb{Q}(\sqrt[3]{2}) = \Phi(<\tau>),$$

und wegen $\sigma <\tau> \sigma^{-1} =<\sigma\tau\sigma^{-1}> =<\tau\sigma>$ ergibt sich

$$\mathbb{Q}(\epsilon\sqrt[3]{2}) = \sigma(\mathbb{Q}(\sqrt[3]{2})) = \Phi(\sigma <\tau> \sigma^{-1}) = \Phi(<\tau\sigma>).$$

Wegen $\sigma^2 <\tau> \sigma^{-2} =<\sigma^2\tau\sigma^{-2}> =<\tau\sigma^2>$ erhalten wir schließlich

$$\mathbb{Q}(\epsilon^2\sqrt[3]{2}) = \sigma^2(\mathbb{Q}(\sqrt[3]{2})) = \Phi(\sigma^2 <\tau> \sigma^{-2}) = \Phi(<\tau\sigma^2>).$$

Satz 3.7 *Es sei F/K eine endliche Galoiserweiterung und L ein Zwischenkörper von F/K sowie $L = \Phi(U)$, wobei U eine Untergruppe von $\mathrm{Gal}(F/K)$ ist. Dann gilt:*

1. *Für jedes $\varphi \in \mathrm{Gal}(F/K)$ ist $\varphi(L) = \Phi(\varphi U \varphi^{-1})$.*
2. *F/L ist eine Galoiserweiterung mit $\mathrm{Gal}(F/L) = U$.*
3. *L/K ist genau dann eine Galoiserweiterung, wenn U Normalteiler in $\mathrm{Gal}(F/K)$ ist. In diesem Falle ist*

$$\mathrm{Gal}(F/K)/U \longrightarrow \mathrm{Gal}(L/K),\ \varphi U \longmapsto \varphi_{_L}$$

ein Gruppenisomorphismus, wobei $\varphi_{_L}$ die Einschränkung von φ auf L ist.

Beweis. Die erste Behauptung wurde in obiger Bemerkung gezeigt. Die zweite Behauptung ergibt sich aus dem Hauptsatz und dem zugehörigen Beweis, da $U = \Gamma(L) = \mathrm{Gal}(F/L)$. Wir zeigen nun die dritte Behauptung. Wie in Bemerkung 2 nach dem Hauptsatz erläutert wurde, gibt es $(\mathrm{Gal}(F/K) : U)$ verschiedene Einschränkungen $\varphi_{_L} : L \longrightarrow F, \varphi \in \mathrm{Gal}(F/K)$. Ist nun U ein Normalteiler in $\mathrm{Gal}(F/K)$, so folgt $\varphi_{_L}(L) = L$, und $\mathrm{Gal}(L/K)$ hat mindestens $(\mathrm{Gal}(F/K) : U)$ verschiedene Elemente. Mit

$$[L : K] = \frac{[F : K]}{[F : L]} = \frac{|\mathrm{Gal}(F/K)|}{|\mathrm{Gal}(F/L)|} = \frac{|\mathrm{Gal}(F/K)|}{|U|} = (\mathrm{Gal}(F/K) : U)$$

und Bemerkung 2 nach Definition 3.5 ist L/K eine Galoiserweiterung mit der Galoisgruppe $\mathrm{Gal}(L/K) = \{\varphi_{_L} \mid \varphi \in \mathrm{Gal}(F/K)\}$. Wir erhalten den surjektiven Gruppenhomomorphismus

$$f : \mathrm{Gal}(F/K) \longrightarrow \mathrm{Gal}(L/K),\ \varphi \longmapsto \varphi_{_L}.$$

Offenbar liegt $\varphi \in \mathrm{Gal}(F/K)$ genau dann im Kern von f, wenn $\varphi_{_L}$ die Identität auf L ist, wenn also $\varphi(x) = x$ für alle $x \in L$ gilt, d.h. $\varphi \in \mathrm{Gal}(F/L) = U$. Aufgrund des Homomorphiesatzes für Gruppen ist

$$\mathrm{Gal}(F/K)/U \longrightarrow \mathrm{Gal}(L/K),\ \varphi U \longmapsto \varphi_{_L}$$

ein Gruppenisomorphismus.

Sei nun U kein Normalteiler in $\mathrm{Gal}(F/K)$, also $\varphi(L) \neq L$ für ein $\varphi \in \mathrm{Gal}(F/K)$. Mit $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_s\}$ gibt es also $s+1$ paarweise verschiedene Einbettungen $\sigma_1, \ldots, \sigma_s, \varphi_{_L}$ von L nach F und

$$K \subseteq E := \{x \in L \mid \varphi(x) = \sigma_1(x) = \cdots = \sigma_s(x)\}.$$

Wegen Satz 3.2 gilt

$$[L : K] \geq [L : E] \geq s + 1 > s = |\mathrm{Gal}(L/K)|,$$

d.h., L/K ist keine Galoiserweiterung.

□

4. Separable Körpererweiterungen

Definition 4.1 *Es sei K ein Körper. Die Abbildung*

$$\mathrm{D} : K[x] \longrightarrow K[x],\ a_n x^n + \cdots + a_1 x + a_0 \longmapsto n a_n x^{n-1} + \cdots + 2a_2 x + a_1$$

heißt formale Ableitung (Differentiation) in $K[x]$.

Bemerkung.

1. Für alle $n \in \mathbb{N}$ und $a \in K$ gilt $na = a + \cdots + a$. Hat zum Beispiel K die Charakteristik $p > 0$ und ist p ein Teiler von n, so gilt $na = 0$.

2. Für alle $f(x), g(x) \in K[x]$ und $a, b \in K$ gilt

   - $\mathrm{D}(af(x) + bg(x)) = a\mathrm{D}(f(x)) + b\mathrm{D}(g(x))$.
   - $\mathrm{D}(f(x)g(x)) = \mathrm{D}(f(x))g(x) + f(x)\mathrm{D}(g(x))$.
   - $\mathrm{D}(f(x)^n) = nf(x)^{n-1}\mathrm{D}(f(x))$ für alle $n \in \mathbb{N}$.

Satz 4.2 *K sei ein Körper und $f(x), g(x) \in K[x]$. Ist $g^2(x)$ ein Teiler von $f(x)$ in $K[x]$, dann ist $g(x)$ Teiler von $\mathrm{D}(f(x))$ in $K[x]$.*

Beweis. Sei $f(x) = g^2(x)h(x)$ mit $h(x) \in K[x]$. Dann gilt

$$\begin{aligned} \mathrm{D}(f(x)) &= \mathrm{D}(g^2(x))h(x) + g^2(x)\mathrm{D}(h(x)) \\ &= 2g(x)\mathrm{D}(g(x))h(x) + g^2(x)\mathrm{D}(h(x)) \\ &= g(x)(2\mathrm{D}(g(x))h(x) + g(x)\mathrm{D}(h(x))) \end{aligned}$$

mit $2\mathrm{D}(g(x))h(x) + g(x)\mathrm{D}(h(x)) \in K[x]$.

□

Bemerkung. Ist $f(x) \in K[x]$ irreduzibel über K und $\mathrm{D}(f(x))$ nicht das Nullpolynom, so sind die Polynome $f(x)$ und $\mathrm{D}(f(x))$ wegen $\operatorname{grad}\mathrm{D}(f(x)) < \operatorname{grad} f(x)$ in $K[x]$ und auch in jedem $F[x]$ teilerfremd, wobei F ein beliebiger Erweiterungskörper von K ist. Für jeden nicht-konstanten Teiler $g(x) \in F[x]$ von $f(x)$ ist dann also $g^2(x)$ kein Teiler von $f(x)$ in $F[x]$. Hat zum Beispiel $f(x)$ in F die Nullstelle a, so ist $x - a$ Teiler von $f(x)$ in $F[x]$, aber $(x-a)^2$ ist kein Teiler von $f(x)$, d.h.

$$f(x) = (x-a)g(x), g(x) \in F[x] \text{ und } g(a) \neq 0.$$

Man nennt dann a einfache Nullstelle von $f(x)$.

Insgesamt haben wir also folgenden Satz bewiesen:

Satz 4.3 *Es sei K ein Körper und $f(x) \in K[x]$ irreduzibel über K. Gilt $\mathrm{D}(f(x)) \neq 0$, so hat $f(x)$ in einem Zerfällungskörper nur einfache Nullstellen.*

Beispiel. Sei $K = \mathbb{Z}_p(t)$ der rationale Funktionenkörper über $\mathbb{Z}_p$ in der Unbestimmten t und $f(x) = x^p - t \in K[x]$. Dann ist t in $\mathbb{Z}_p[t]$ irreduzibel und $f(x)$ nach dem Eisensteinkriterium irreduzibel über K. Es gilt $\mathrm{D}(f(x)) = px^{p-1} = 0$ wie in Bemerkung 1 nach Definition 4.1 erläutert. Ist nun $a \in F$ in einem Erweiterungskörper F von K Nullstelle von $f(x)$, so gilt $a^p = t$, also

$$f(x) = x^p - t = x^p - a^p = (x - a)^p.$$

Damit ist $K(a)$ Zerfällungskörper von $f(x)$ über K, und $f(x)$ hat in $K(a)$ die p-fache Nullstelle a.

Definition 4.4 *Es sei K ein Körper und $f(x) \in K[x]$ irreduzibel über K. Dann heißt $f(x)$ separabel über K, wenn $f(x)$ in einem Zerfällungskörper nur einfache Nullstellen hat.*

Satz 4.5 *Es sei K ein Körper und $f(x) \in K[x]$.*

1. *Für $\chi(K) = 0$ gilt: $\mathrm{D}(f(x)) = 0 \Longleftrightarrow f(x)$ ist konstant.*
2. *Für $\chi(K) = p > 0$ gilt: $\mathrm{D}(f(x)) = 0 \Longleftrightarrow$ Es gibt ein $g(x) \in K[x]$ mit $f(x) = g(x^p)$.*

Beweis. Für $f(x) = a_n x^n + \cdots + a_1 x + a_0$ gilt zunächst

$$\mathrm{D}(f(x)) = na_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

Hat nun K die Charakteristik 0, so gilt für alle $k = 1, \ldots, n$ genau dann $ka_k = 0$, wenn $a_k = 0$, d.h., $\mathrm{D}(f(x)) = 0$ gilt genau dann, wenn $a_1 = a_2 = \cdots = a_n = 0$.
Hat K die Charakteristik $p > 0$, so gilt gemäß Bemerkung 1 nach Definition 4.1 für alle $k = 1, \ldots, n$ genau dann $ka_k = 0$, wenn $a_k = 0$ oder wenn p ein Teiler von k ist. Somit folgt $\mathrm{D}(f(x)) = 0$ genau dann, wenn $a_k = 0$ für alle die $k = 1, \ldots, n$ gilt, die p nicht teilt, also $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots = g(x^p)$ mit $g(x) = a_0 + a_p x + a_{2p} x^2 + \ldots$.

□

Definition 4.6 *Es sei K ein Körper und F ein Erweiterungskörper von K. Dann heißt $a \in F$ separabel über K, wenn a algebraisch über K und $\mathrm{Irr}(a, K)$ separabel über K ist. Die Körpererweiterung F/K heißt separabel, wenn jedes $a \in F$ separabel über K ist.*

Bemerkung. Ist F/K eine separable Körpererweiterung, dann sind für jeden Zwischenkörper E von F/K auch F/E und E/K separabel.

Satz 4.7 *Der Körper K habe die Charakteristik 0. Dann ist jedes irreduzible $f(x) \in K[x]$ separabel über K und jede algebraische Körpererweiterung F/K ist separabel.*

Beweis. Die zweite Behauptung folgt aus der ersten. Sei also $f(x) \in K[x]$ irreduzibel über K. Wegen Satz 4.5 gilt $\mathrm{D}(f(x)) \neq 0$, und $f(x)$ ist separabel wegen Satz 4.3.

□

Satz 4.8 *Jede endliche separable Körpererweiterung F/K ist einfach, d.h., es gibt ein $a \in F$ mit $F = K(a)$.*

Beweis. Sei zunächst K endlich. Dann ist auch F endlich, da $|F| = |K|^{[F:K]}$. Also ist $F^\times$ eine endliche abelsche Gruppe, und mit m bezeichnen wir die größte in $F^\times$ auftretende Ordnung. Sei $a \in F^\times$ mit der Ordnung m. Wegen Aufgabe 5.4 aus Kapitel 1 gilt dann $b^m = 1$ für alle $b \in K^\times$. Da aber $x^m - 1$ in $F^\times$ höchstens m verschiedene Nullstellen hat, folgt $|F^\times| \leq m$. Andererseits ist $m = |\langle a \rangle| \leq |F^\times|$, d.h. $|F^\times| = m$ und $F^\times = \langle a \rangle$. Also ist jedes Element von $F^\times$ eine Potenz von a und somit insbesondere $F = K(a)$.

Sei nun K nicht endlich. Wir beweisen den Satz durch vollständige Induktion nach dem Erweiterungsgrad $n = [F : K]$, wobei der Induktionsanfang $n = 1$ offenbar gilt. Ist $n > 1$, so wählen wir ein $a \in F$ mit $a \notin K$, und es gilt $[K(a) : K] > 1$, d.h. $[F : K(a)] < n$. Da auch $F/K(a)$ eine separable Erweiterung ist, gibt es nach Induktionsvoraussetzung ein $b \in F$ mit $F = K(a)(b) = K(a, b)$. Sei $f(x) = \mathrm{Irr}(a, K)$ und $g(x) = \mathrm{Irr}(b, K)$. In einem Zerfällungskörper E von $f(x)g(x)$ über K habe $f(x)$ die verschiedenen Nullstellen $a = a_1, \ldots, a_r$ und $g(x)$ die Nullstellen $b = b_1, \ldots, b_s$. Weil K unendlich ist, existiert ein $k \in K$ mit

$$k \neq (b_j - b)(a - a_i)^{-1} \text{ für } i = 2, \ldots, r \text{ und } j = 1, \ldots, s, \text{ also}$$

$$a_i \neq a - \frac{b_j - b}{k} \text{ für } i = 2, \ldots, r \text{ und } j = 1, \ldots, s.$$

Wir zeigen nun $K(a, b) = K(c)$ mit $c = ak + b$, wobei $K(c) \subseteq K(a, b)$ offenbar erfüllt ist. In $E[x]$ gilt

$$f(x) = (x - a_1) \cdot \ \ldots \ \cdot (x - a_r) \text{ und } g(x) = (x - b_1) \cdot \ \ldots \ \cdot (x - b_s), \text{ also}$$

$$\begin{aligned} g(c - xk) &= (c - xk - b_1) \cdot \ \ldots \ \cdot (c - xk - b_s) \\ &= (-k)^s (x - a + \frac{b_1 - b}{k}) \cdot \ \ldots \ \cdot (x - a + \frac{b_s - b}{k}). \end{aligned}$$

Aufgrund der Wahl von k ist $x - a$ ein ggT von $f(x)$ und $g(c - xk)$ in $E[x]$, also auch in $K(c)[x]$, d.h. $x - a \in K(c)[x]$. Es folgt $a \in K(c)$ und somit $b \in K(c)$, d.h. $K(a, b) \subseteq K(c)$.

□

Satz 4.9 *Ist F/K eine endliche Galoiserweiterung, dann ist F/K separabel, und für jedes $a \in F$ zerfällt das Minimalpolynom $f(x) = \mathrm{Irr}(a, K)$ von a über K in $F[x]$ in paarweise verschiedene Linearfaktoren*

$$f(x) = (x - a_1) \cdot \ \ldots \ \cdot (x - a_r),$$

wobei $\{a_1, \ldots, a_r\} = \{\varphi(a) \mid \varphi \in \mathrm{Gal}(F/K)\}$.

Beweis. Seien $a_1, \ldots, a_r \in F$ paarweise verschieden mit

$$\{a_1, \ldots, a_r\} = \{\varphi(a) \mid \varphi \in \mathrm{Gal}(F/K)\}.$$

Für jedes $\varphi \in \mathrm{Gal}(F/K)$ bezeichne φ ebenfalls die eindeutige Fortsetzung von φ auf $F[x]$ mit $\varphi(x) = x$. Dann gilt für $g(x) = (x - a_1) \cdot \ \ldots \ \cdot (x - a_r) \in F[x]$

$$\begin{aligned} \varphi(g(x)) &= (x - \varphi(a_1)) \cdot \ \ldots \ \cdot (x - \varphi(a_r)) \\ &= (x - a_1) \cdot \ \ldots \ \cdot (x - a_r) \\ &= g(x), \end{aligned}$$

d.h., die Koeffizienten von $g(x)$ liegen in $\Phi(\mathrm{Gal}(F/K))$. Da F/K Galoiserweiterung ist, gilt $\Phi(\mathrm{Gal}(F/K)) = K$, also $g(x) \in K[x]$. Wegen $g(a) = 0$ ist $f(x)$ Teiler von $g(x)$ in $K[x]$, also $\operatorname{grad} f(x) \leq \operatorname{grad} g(x)$. Andererseits gibt es zu jedem a_i ein $\varphi \in \mathrm{Gal}(F/K)$ mit $\varphi(a) = a_i$, also $0 = \varphi(0) = \varphi(f(a)) = f(\varphi(a)) = f(a_i)$. Folglich sind $a_1, \ldots, a_r$ paarweise verschiedene Nullstellen von $f(x)$, d.h. $\operatorname{grad} f(x) \geq r = \operatorname{grad} g(x)$. Da $f(x)$ und $g(x)$ normiert sind, ergibt sich $f(x) = g(x)$. Insbesondere ist somit $f(x)$ separabel über K, also auch a, und F/K ist eine separable Erweiterung.

□

Bemerkung. Die Elemente $a_1, \ldots, a_r \in F$ mit $\mathrm{Irr}(a, K) = (x - a_1) \cdot \ \ldots \ \cdot (x - a_r)$ heißen die zu a konjugierten Elemente über K.

Beispiel. Wir betrachten die Galoiserweiterung F/K mit $K = \mathbb{Q}$ und $F = \mathbb{Q}(\sqrt[3]{2}, \epsilon)$ und benutzen die Bezeichnungen aus dem Beispiel nach Satz 3.6. Dann ist $\mathrm{Gal}(F/K) = \{\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ mit $\sigma(\sqrt[3]{2}) = \epsilon\sqrt[3]{2}$ und $\sigma(\epsilon) = \epsilon$ sowie $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ und $\tau(\epsilon) = \epsilon^2$. Wir berechnen die Konjugierten von $a = \epsilon + \sqrt[3]{2}$. Es gilt

$$\begin{aligned} \mathrm{id}(\epsilon + \sqrt[3]{2}) &= \epsilon + \sqrt[3]{2} =: a_1 \\ \sigma(\epsilon + \sqrt[3]{2}) &= \epsilon + \epsilon\sqrt[3]{2} =: a_2 \\ \sigma^2(\epsilon + \sqrt[3]{2}) &= \epsilon + \epsilon^2\sqrt[3]{2} = \epsilon - \sqrt[3]{2} - \epsilon\sqrt[3]{2} =: a_3 \\ \tau(\epsilon + \sqrt[3]{2}) &= \epsilon^2 + \sqrt[3]{2} = -1 - \epsilon + \sqrt[3]{2} =: a_4 \\ \tau\sigma(\epsilon + \sqrt[3]{2}) &= \epsilon^2 + \epsilon^2\sqrt[3]{2} = -1 - \epsilon - \sqrt[3]{2} - \epsilon\sqrt[3]{2} =: a_5 \\ \tau\sigma^2(\epsilon + \sqrt[3]{2}) &= \epsilon^2 + \epsilon\sqrt[3]{2} = -1 - \epsilon + \epsilon\sqrt[3]{2} =: a_6 \end{aligned}$$

Da $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \epsilon, \epsilon\sqrt[3]{2}, \epsilon\sqrt[3]{2}^2\}$ eine K-Basis von F ist, sind $a_1, \ldots, a_6$ paarweise verschieden, d.h., $\mathrm{Irr}(a, \mathbb{Q}) = (x - a_1) \cdot \ \ldots \ \cdot (x - a_6)$ und $[\mathbb{Q}(a) : \mathbb{Q}] = 6$. Es folgt $F = \mathbb{Q}(\sqrt[3]{2}, \epsilon) = \mathbb{Q}(a)$. Somit ist $\epsilon + \sqrt[3]{2}$ ein primitives Element der Körpererweiterung F/K. Es gilt

$$\mathrm{Irr}(a, \mathbb{Q}) = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9.$$

Definition 4.10 *Ist K ein Körper und $f(x) \in K[x]$, so heißt $f(x)$ separabel über K, wenn jeder irreduzible Teiler von $f(x)$ in $K[x]$ separabel über K ist.*

Bemerkung. Hat K die Charakteristik 0, so ist jedes über K irreduzible Polynom auch separabel über K; somit ist jedes Polynom $f(x) \in K[x]$ separabel über K, falls $\chi(K) = 0$.

Satz 4.11 *Eine endliche Körpererweiterung F/K ist genau dann Galoiserweiterung, wenn F Zerfällungskörper eines über K separablen Polynoms $f(x) \in K[x]$ über K ist.*

Beweis. Sei F/K endliche Galoiserweiterung. Wegen $[F : K] < \infty$ und Satz 1.11 gilt $F = K(a_1, \ldots, a_n)$, wobei $a_1, \ldots, a_n \in F$ algebraisch über K sind. Ist $f_i(x) \in K[x]$ das Minimalpolynom von a_i über K, so ist $f_i(x)$ wegen Satz 4.9 separabel über K und zerfällt über F in Linearfaktoren. Dann ist $f(x) = f_1(x) \cdot \ \ldots \ \cdot f_n(x)$ separabel über K und $F = K(a_1, \ldots, a_n)$ Zerfällungskörper von $f(x)$ über K.

Sei nun andererseits $f(x) \in K[x]$ separabel über K und F Zerfällungskörper von $f(x)$ über K. Wir zeigen durch Induktion nach $n = [F : K]$, daß F/K Galoiserweiterung ist, wobei der Induktionsanfang $n = 1$ offensichtlich gilt. Sei also $n > 1$ und $g(x) \in K[x]$ ein irreduzibler normierter Teiler von $f(x)$ in $K[x]$ mit $r := \operatorname{grad} g(x) > 1$. Dann gibt es paarweise verschiedene $a_1, \ldots, a_r \in F$ mit $g(x) = (x - a_1) \cdot \ \ldots \ \cdot (x - a_r)$, also $\operatorname{Irr}(a_i, K) = g(x)$ für $i = 1, \ldots, r$, und wegen Korollar 2.5 zu jedem a_i einen K-Isomorphismus

$$\varphi_i : K(a_1) \longrightarrow K(a_i) \text{ mit } \varphi_i(a_1) = a_i.$$

Da nun F auch ein Zerfällungskörper von $f(x)$ über $K(a_i)$ ist und $\varphi_i(f(x)) = f(x)$ wegen $f(x) \in K[x]$ gilt (hier betrachten wir φ_i als Fortsetzung von φ_i auf $K(a_i)[x]$ mit $\varphi_i(x) = x$), läßt sich aufgrund von Korollar 2.6 jedes φ_i zu einem Isomorphismus $\psi_i : F \longrightarrow F$ fortsetzen. Es folgt $\psi_i \in \operatorname{Gal}(F/K)$ mit $\psi_i(a_1) = a_i$ für $i = 1, \ldots, r$. Wegen $[K(a_1) : K] = r$, also $[F : K(a_1)] = \frac{n}{r} < n$, und der Induktionsvoraussetzung ist $F/K(a_1)$ eine Galoiserweiterung, da F Zerfällungskörper von $f(x)$ über $K(a_1)$ ist. Es folgt $|\operatorname{Gal}(F/K(a_1))| = \frac{n}{r}$, und wir bezeichnen die Elemente von $\operatorname{Gal}(F/K(a_1))$ mit $\sigma_1, \ldots, \sigma_{\frac{n}{r}}$. Gilt nun

$$\psi_i\sigma_j = \psi_\nu\sigma_\mu \ \text{ mit } \ 1 \le i, \nu \le r \text{ und } 1 \le j, \mu \le \frac{n}{r},$$

so ist

$$a_i = \psi_i\sigma_j(a_1) = \psi_\nu\sigma_\mu(a_1) = a_\nu,$$

also $i = \nu$ und $\sigma_j = \sigma_\mu$, d.h. $j = \mu$. Wir erhalten schließlich

$$\begin{aligned} |\operatorname{Gal}(F/K)| &\ge |\{\psi_i\sigma_j \mid 1 \le i \le r \text{ und } 1 \le j \le \frac{n}{r}\}| \\ &= r\frac{n}{r} = n = [F : K], \end{aligned}$$

d.h., F/K ist eine Galoiserweiterung wegen Bemerkung 2 nach Definition 3.5.

□

Korollar 4.12 *Jede endliche separable Körpererweiterung F/K liegt in einer endlichen Galoiserweiterung E/K.*

Beweis. Sei $F = K(a)$ wegen Satz 4.8 und $f(x) = \mathrm{Irr}(a, K)$. Ist E ein Zerfällungskörper von $f(x)$ über K, der F enthält, so ist E/K wegen Satz 4.11 die gesuchte endliche Galoiserweiterung.

□

Wir wollen nun die Ergebnisse dieses Abschnitts anwenden, um den *Fundamentalsatz der Algebra* zu beweisen.

Fundamentalsatz der Algebra. Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.

Dabei heißt ein Körper K algebraisch abgeschlossen, wenn jedes nichtkonstante Polynom $f(x) \in K[x]$ über K in Linearfaktoren zerfällt. Gleichwertig hiermit ist, daß jedes nichtkonstante Polynom $f(x) \in K[x]$ in K eine Nullstelle hat. Dieses ist schließlich äquivalent dazu, daß K keine echte algebraische Körpererweiterung besitzt.

Bevor wir den Fundamentalsatz beweisen, müssen wir erklären, was wir unter dem Körper $\mathbb{C}$ verstehen wollen. Zunächst können wir $\mathbb{R}$ als Vervollständigung von $\mathbb{Q}$ bezüglich des gewöhnlichen Absolutbetrages definieren. Dann ist $\mathbb{R}$ insbesondere ein angeordneter Körper, und für alle $a \in \mathbb{R}$ gilt $a^2 \geq 0$. (Einzelheiten hierzu findet man zum Beispiel im Skript *Algebra und Arithmetik*.) Somit hat $x^2 + 1 \in \mathbb{R}[x]$ in $\mathbb{R}$ keine Nullstelle, d.h., $x^2 + 1$ ist irreduzibel über $\mathbb{R}$. Sei nun $\mathbb{C} = \mathbb{R}(i)$ mit $i^2 + 1 = 0$.

Für den Beweis des Fundamentalsatzes benötigen wir die beiden folgenden Eigenschaften von $\mathbb{R}$:

A) Hat $f(x) \in \mathbb{R}[x]$ ungeraden Grad, so hat $f(x)$ in $\mathbb{R}$ eine Nullstelle.

B) Jedes $a \in \mathbb{R}, a \geq 0$ ist in $\mathbb{R}$ ein Quadrat, d.h., es gibt ein $b \in \mathbb{R}$ mit $b^2 = a$.

Aus Eigenschaft B folgt, daß jedes $x + iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$ ein Quadrat in $\mathbb{C}$ ist, denn wir erhalten $x + iy = z^2$ mit

$$z = \sqrt{\frac{x + \sqrt{x^2 + y^2}}{2}} \pm i\sqrt{\frac{-x + \sqrt{x^2 + y^2}}{2}}.$$

Dabei gilt das positive Vorzeichen, falls $y \geq 0$, und das negative anderenfalls. Insbesondere hat damit jedes quadratische Polynom über $\mathbb{C}$ eine Nullstelle in $\mathbb{C}$.

Wir beweisen nun den Fundamentalsatz und nehmen an, daß es ein Polynom $f(x) \in \mathbb{C}[x]$ gibt, das irreduzibel über $\mathbb{C}$ ist und einen Grad größer als 1 hat. Dann gibt es eine echte endliche Körpererweiterung $K/\mathbb{C}$, also

$$\mathbb{R} \subset \mathbb{C} \subset K.$$

Wegen Satz 4.7 und Korollar 4.12 können wir sogar annehmen, daß $K/\mathbb{R}$ eine endliche Galoiserweiterung ist. Wegen $[\mathbb{C} : \mathbb{R}] = 2$ ist 2 ein Teiler von $[K : \mathbb{R}]$, also ein Teiler

von $|\mathrm{Gal}(K/\mathbb{R})|$. Sei U eine 2-Sylowgruppe von $\mathrm{Gal}(K/\mathbb{R})$, d.h. $|U| = 2^l$ mit $l \in \mathbb{N}$ und $(\mathrm{Gal}(K/\mathbb{R}) : U)$ ungerade. Ist $L = \Phi(U)$ der Fixkörper von U, so ist also

$$[L : \mathbb{R}] = (\mathrm{Gal}(K/\mathbb{R}) : U) \text{ ungerade}$$

und damit $[\mathbb{R}(a) : \mathbb{R}]$ ungerade für jedes $a \in L$, d.h., das Minimalpolynom $\mathrm{Irr}(a, \mathbb{R})$ hat einen ungeraden Grad. Aufgrund von Eigenschaft A besitzt $\mathrm{Irr}(a, \mathbb{R})$ eine Nullstelle in $\mathbb{R}$, d.h. $\mathrm{grad}\,\mathrm{Irr}(a, \mathbb{R}) = 1$ und $a \in \mathbb{R}$. Somit ergibt sich $L = \mathbb{R}$ und $U = \mathrm{Gal}(K/\mathbb{R})$. Es folgt

$$|\mathrm{Gal}(K/\mathbb{R})| = 2^l,\ l \in \mathbb{N}.$$

Da $K/\mathbb{R}$ eine Galoiserweiterung ist, ist auch $K/\mathbb{C}$ eine Galoiserweiterung mit

$$|\mathrm{Gal}(K/\mathbb{C})| = 2^r,\ l - 1 = r \geq 1.$$

Wegen des 1. Sylowschen Satzes existiert eine Untergruppe V von $\mathrm{Gal}(K/\mathbb{C})$ mit $|V| = 2^{r-1}$. Für den Fixkörper F von V erhalten wir $[K : F] = 2^{r-1}$, also $[F : \mathbb{C}] = 2$. Folglich gilt $F = \mathbb{C}(a)$, wobei $\mathrm{Irr}(a, \mathbb{C})$ den Grad 2 hat. Wegen der Folgerung aus Eigenschaft B besitzt $\mathrm{Irr}(a, \mathbb{C})$ aber eine Nullstelle in $\mathbb{C}$ - Widerspruch.

Somit ist die ursprüngliche Annahme über $f(x)$ falsch, d.h., jedes irreduzible Polynom über $\mathbb{C}$ hat den Grad 1, und $\mathbb{C}$ ist damit algebraisch abgeschlossen.

5. Aufgaben

A 5.1 Es sei F/K eine endliche Körpererweiterung und $a \in F$. Zeigen Sie, daß der Grad des Minimalpolynoms $\mathrm{Irr}(a, K)$ von a über K den Erweiterungsgrad $[F : K]$ teilt.

A 5.2 Zeigen Sie, daß eine Körpererweiterung F/K genau dann algebraisch ist, wenn jeder Teilring R von F, der K enthält, ein Teilkörper von F ist.

A 5.3 Es sei K ein Körper und $K(x)$ der Körper der gebrochen-rationalen Funktionen über K in der Unbestimmten x sowie $F = K(x^3(x+1)^{-1})$. Zeigen Sie, daß $K(x)/F$ eine einfache algebraische Körpererweiterung ist, und berechnen Sie das Minimalpolynom von $x \in K(x)$ über F.

A 5.4 K sei ein endlicher Körper. Zeigen Sie, daß es eine Primzahl p und ein $n \in \mathbb{N}$ mit $|K| = p^n$ gibt.

A 5.5 F sei ein Erweiterungskörper von $\mathbb{Z}_2$ und $a \in F$ algebraisch über $\mathbb{Z}_2$ mit dem Minimalpolynom $\mathrm{Irr}(a, \mathbb{Z}_2) = x^5 + x^4 + x^3 + x^2 + 1$. Berechnen Sie die multiplikativen Inversen von $a^4 + a^2 + a + 1$ und $a^4 + a^3 + a + 1$ in $\mathbb{Z}_2(a)$.

A 5.6 Zeigen Sie, daß das Polynom $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$ über $\mathbb{Q}$ irreduzibel ist. In einem Erweiterungskörper F von $\mathbb{Q}$ habe $f(x)$ die Nullstelle $a \in F$. Zeigen Sie, daß dann $f(x)$ auch die Nullstellen $a^2 - 2$ und $-a^2 - a + 2$ hat. Zeigen Sie weiterhin, daß $g(x) = x^2 + 6x + 2 \in \mathbb{Q}[x]$ keine Nullstelle in $\mathbb{Q}(a)$ hat.

A 5.7 Zeigen Sie, daß $f(x) = x^4+4x^3+4x^2+8 \in \mathbb{Q}[x]$ irreduzibel über $\mathbb{Q}$ ist und berechnen Sie das Minimalpolynom von $a^2 + 2a + 2$ über $\mathbb{Q}$, wobei $a \in \mathbb{C}$ eine Nullstelle von $f(x)$ ist.

A 5.8 Es sei K ein Körper, F ein Erweiterungskörper von K und $a, b \in F$ algebraisch über K, so daß die Erweiterungsgrade $[K(a) : K]$ und $[K(b) : K]$ teilerfremd sind. Zeigen Sie, daß dann $[K(a, b) : K] = [K(a) : K] \cdot [K(b) : K]$ gilt. Benutzen Sie dieses Ergebnis, um $\mathrm{Irr}(\sqrt{3} + \sqrt[3]{3}, \mathbb{Q})$ zu ermitteln.

A 5.9 Zeigen Sie $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ und berechnen Sie den Erweiterungsgrad $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$. Zeigen Sie weiterhin $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

A 5.10 Berechnen Sie die folgenden Minimalpolynome und begründen Sie jeweils Ihre Antwort: $\mathrm{Irr}(\sqrt[4]{3} + 1, \mathbb{Q})$, $\mathrm{Irr}(\sqrt{2 + \sqrt[3]{2}}, \mathbb{Q})$ und $\mathrm{Irr}(\sqrt{5} + \sqrt{6}, \mathbb{Q})$.

A 5.11 Zeigen Sie, daß jede endliche Untergruppe der multiplikativen Gruppe $K^\times$ eines Körpers K zyklisch ist.

A 5.12 Sei F ein Erweiterungskörper von $\mathbb{Z}_2$ und $a \in F$ algebraisch über $\mathbb{Z}_2$ mit dem Minimalpolynom $\mathrm{Irr}(a, \mathbb{Z}_2) = x^4+x+1$. Zeigen Sie, daß a die multiplikative Gruppe von $\mathbb{Z}_2(a)$ erzeugt, d.h. $\mathbb{Z}_2(a) = \{0, 1, a, \ldots, a^{14}\}$. Berechnen Sie das Minimalpolynom von $a^2 + a + 1$ über $\mathbb{Z}_2$ und geben Sie ein $b \in \mathbb{Z}_2(a)$ mit $\mathrm{Irr}(b, \mathbb{Z}_2) = x^4 + x^3 + x^2 + x + 1$ an.

A 5.13 $\mathcal{A}$ sei der Körper der algebraischen Zahlen. Zeigen Sie, daß $\mathcal{A}/\mathbb{Q}$ keine endliche Körpererweiterung ist.

A 5.14 Es sei $f(x) = x^6 - 3 \in \mathbb{Q}[x]$ und $\sqrt[6]{3} \in \mathbb{R}$ die einzige positive Nullstelle von $f(x)$ in $\mathbb{R}$. Zeigen Sie, daß $\mathbb{Q}(\sqrt[6]{3}, \epsilon)$ mit $\mathrm{Irr}(\epsilon, \mathbb{Q}) = x^2 + x + 1$ ein Zerfällungskörper von $f(x)$ über $\mathbb{Q}$ ist. Geben Sie Nullstellen $a_1, a_2, a_3 \in \mathbb{C}$ von $f(x)$ so an, daß $\mathbb{Q}(a_1, a_2)$ und $\mathbb{Q}(a_1, a_3)$ nicht isomorph sind.

A 5.15 F sei der Zerfällungskörper von $x^p - 1$ über $\mathbb{Q}$, wobei p eine Primzahl ist. Berechnen Sie den Erweiterungsgrad $[F : \mathbb{Q}]$.

A 5.16 Es sei K ein Körper. Zeigen Sie, daß die folgenden Aussagen äquivalent sind:

1. Jedes $f(x) \in K[x], \operatorname{grad} f(x) \geq 1$ zerfällt über K in Linearfaktoren.
2. Jedes $f(x) \in K[x], \operatorname{grad} f(x) \geq 1$ hat in K eine Nullstelle.
3. Ist $f(x) \in K[x]$ irreduzibel, so gilt $\operatorname{grad} f(x) = 1$.
4. Ist F/K eine algebraische Körpererweiterung, so gilt $F = K$.

A 5.17 Zeigen Sie, daß es zu jeder Primzahl p und jedem $n \in \mathbb{N}$ bis auf Isomorphie genau einen Körper mit p^n Elementen gibt. Hinweis: Betrachten Sie den Zerfällungskörper von $x^{p^n} - x$ über $\mathbb{Z}_p$.

A 5.18 Es sei $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Zeigen Sie, daß $f(x)$ das Produkt aller irreduziblen normierten Polynome $g(x) \in \mathbb{Z}_p[x]$ ist, für die $\operatorname{grad} g(x)$ ein Teiler von n ist.

A 5.19 Zeigen Sie, daß $x^4 + 1$ über $\mathbb{Q}$ irreduzibel ist, aber reduzibel über jedem $\mathbb{Z}_p$.

A 5.20 Zerlegen Sie $x^8 - 1 \in \mathbb{Z}_3[x]$ in irreduzible Polynome.

A 5.21 Zeigen Sie, daß $\mathbb{R}$ eine triviale Automorphismengruppe hat, d.h. $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$.

A 5.22 Zeigen Sie, daß jeder Automorphismus eines Körpers den Primkörper elementweise festläßt.

A 5.23 Es sei K ein endlicher Körper mit dem Primkörper $\mathbb{Z}_p$. Zeigen Sie, daß $K/\mathbb{Z}_p$ eine Galoiserweiterung mit zyklischer Galoisgruppe ist, die von $\sigma : K \longrightarrow K, a \longmapsto a^p$ erzeugt wird, d.h., σ ist ein Automorphismus von K und $\mathrm{Gal}(K/\mathbb{Z}_p) =< \sigma >$.

A 5.24 Zeigen Sie, daß $\mathbb{Q}(\alpha)$ mit $\mathrm{Irr}(\alpha, \mathbb{Q}) = x^4 - 4x^2 + 2$ eine Galoiserweiterung von $\mathbb{Q}$ ist. Geben Sie für jedes $\varphi \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ das Element $\varphi(\alpha)$ in der Form $a\alpha^3 + b\alpha^2 + c\alpha + d$ mit $a, b, c, d \in \mathbb{Q}$ an. Wieviele Zwischenkörper hat die Körpererweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$?

A 5.25 F/K sei eine endliche Galoiserweiterung und $f(x) \in K[x]$ irreduzibel über K. Zeigen Sie: Sind $g_1(x), \ldots, g_n(x) \in F[x]$ irreduzibel über F mit $f(x) = g_1(x) \cdot \ \ldots \ \cdot g_n(x)$, dann haben $g_1(x), \ldots, g_n(x)$ denselben Grad. Geben Sie ein sinnvolles Beispiel an.

A 5.26 F/K sei eine endliche Körpererweiterung und L ein Zwischenkörper. Zeigen Sie: Sind F/L und L/K Galoiserweiterungen, so ist F/K genau dann eine Galoiserweiterung, wenn sich jedes $\varphi \in \mathrm{Gal}(L/K)$ zu einem $\hat{\varphi} \in \mathrm{Gal}(F/K)$ fortsetzen läßt.

A 5.27 Zeigen Sie, daß $f(x) \in \mathbb{Q}[x]$ mit $f(x) = x^8 - 24x^6 + 144x^4 - 288x^2 + 144$ irreduzibel über $\mathbb{Q}$ ist. Sei $a \in \mathbb{C}$ Nullstelle von $f(x)$. Zeigen Sie, daß dann auch $\frac{1}{12}(a^5 - 18a^3 + 36a)$, $\frac{1}{14}(-a^7 + 20a^5 - 60a^3 - 246a)$ und $\frac{1}{12}(a^7 - 22a^5 + 102a^3 - 120a)$ Nullstellen von $f(x)$ sind und daß $\mathbb{Q}(a)/\mathbb{Q}$ eine Galoiserweiterung ist, deren Galoisgruppe isomorph zur Quaternionengruppe ist.

A 5.28 x und y seien unabhängige Unbestimmte über $\mathbb{Z}_p$ sowie $F = \mathbb{Z}_p(x, y)$. Zeigen Sie, daß die Körpererweiterung F/K mit $K = \mathbb{Z}_p(x^p, y^p)$ unendlich viele Zwischenkörper hat.

A 5.29 Zeigen Sie, daß jede endliche separable Körpererweiterung nur endlich viele Zwischenkörper hat.

A 5.30 Ein Körper K heißt perfekt, wenn jedes Polynom $f(x) \in K[x]$ separabel über K ist. Zeigen Sie, daß ein Körper K mit der Charakteristik $\chi(K) = p > 0$ genau dann perfekt ist, wenn es zu jedem $a \in K$ ein $b \in K$ mit $b^p = a$ gibt.

A 5.31 Beweisen Sie die Rechenregeln für die formale Ableitung aus Bemerkung 2 nach Definition 4.1.

A 5.32 Zeigen Sie: Ist F/K eine separable Körpererweiterung und E ein Zwischenkörper, dann sind auch F/E und E/K separable Körpererweiterungen.

A 5.33 Zeigen Sie, daß das Polynom $x^5 + 2x^3 - 26x^2 + 26x - 2 \in \mathbb{Q}[x]$ drei reelle Nullstellen und zwei nicht-reelle Nullstellen in $\mathbb{C}$ hat.

Index