ulm university universität ulm

Skript zur Vorlesung

Elemente der Algebra

Wintersemester 2011/ 12

Prof. Dr. Helmut Maier
Dipl.-Math. Hans- Peter Reck

Institut für Zahlentheorie und Wahrscheinlichkeitstheorie
Universität Ulm

Inhaltsverzeichnis

Kapitel 1

Gruppen

1.1 Definitionen und Beispiele

Definition 1.1.1. Es sei $X \neq \emptyset$ eine Menge. Eine Abbildung $\circ\colon X \times X \to X$ heißt eine Verknüpfung auf X.

Definition 1.1.2. Es sei $\circ$ eine Verknüpfung auf einer Menge $G \neq \emptyset$. Dann heißt $(G, \circ)$ eine Gruppe, wenn die folgenden Axiome gelten:

(G1) $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G$ (Assoziativgesetz).

(G2) Es gibt mindestens ein neutrales Element $e \in G$ mit $e \circ a = a \circ e = a$ für alle $a \in G$.

(G3) Ist ein neutrales Element $e \in G$ gegeben, so gibt es zu jedem $a \in G$ ein inverses Element $a' \in G$ mit $a \circ a' = a' \circ a = e$.

Gilt zusätzlich das Axiom

(G4) $a \circ b = b \circ a$ für alle $a, b \in G$ (Kommutativgesetz),

so heißt G eine abelsche (oder auch kommutative) Gruppe.

Die Definition lässt offen, ob es in der Gruppe G nicht mehr als ein Element oder, wenn das neutrale Element $e \in G$ gegeben ist, zu einem gegebenen $a \in G$ mehr als ein inverses Element gibt.
Der folgende Satz zeigt, dass die Situation immer sehr einfach ist:

Satz 1.1.1. *In einer beliebigen Gruppe gilt:*

i) Es gibt genau ein neutrales Element.

ii) Jedes $a \in G$ hat genau ein Inverses (das wir mit a^{-1} bezeichnen).

Beweis. Zu (i): Beweis durch Widerspruch:
Angenommen, es gibt verschiedene neutrale Elemente $e_1, e_2 \in G$. Da e_1 neutral ist gilt $e_1 \cdot a = a$ für alle $a \in G$, wir können also $a = e_2$ einsetzen und erhalten $e_1 \cdot e_2 = e_2$. Da auch e_2 neutral ist gilt $a \cdot e_2 = a$ für alle $a \in G$, einsetzen von $a = e_1$ ergibt $e_1 \cdot e_2 = e_1$. Zusammensetzen der beiden Gleichungen ergibt $e_1 = e_1 \cdot e_2 = e_2$, ein Widerspruch zur Annahme, daß $e_1 \neq e_2$ ist.

Zu (ii): Es sei $a \in G$ beliebig und $a_1, a_2 \in G$ zwei Inverse, also

$$a \cdot a_1 = a_1 \cdot a = e \quad \text{und} \quad a \cdot a_2 = a_2 \cdot a = e$$

mit dem nach (i) eindeutig bestimmten neutralen Element e von G. Wir multiplizieren die zweite Gleichung von links mit a_1 und erhalten

$$a_1 \cdot (a \cdot a_2) = a_1 \cdot e.$$

Anwendung des Axioms (G1) ergibt die Gleichungen

$$(a_1 \cdot a) \cdot a_2 = a_1 \cdot e.$$

Anwendung von (G3) auf der linken Seite ergibt

$$e \cdot a_2 = a_1 \cdot e$$

und nach (G2) folgt $a_2 = a_1$, also waren die Inversen gleich. □

Bemerkung 1.1.1. Üblicherweise schreibt man die Verknüpfung als Addition- man hat dann die Gruppe $(G, +)$- nur dann, wenn G abelsch ist. In diesem Fall schreibt man "0" für das neutrale Element, und nennt es das Nullelement von $(G, +)$. Es gilt dann $a + 0 = 0 + a = a$ für alle $a \in G$. Man schreibt $-a$ für das Inverse und benutzt $a - b$ als Abkürzung für den Ausdruck $a + (-b)$. Es gilt somit $a - a = -a + a = a + (-a) = 0$ für alle $a \in G$.
Für eine multiplikativ geschriebene Gruppe nennt man das neutrale Element auch Einselement und schreibt 1 statt e. Der Multiplikationspunkt wird oft weggelassen, man schreibt also ab statt $a \cdot b$.

Wir zeigen nun ein paar Rechenregeln für Gruppen:

Satz 1.1.2. *In jeder Gruppe $(G, \cdot)$ gilt:*

i) Zu beliebigen $a, b \in G$ gibt es eindeutig bestimmte $x, y \in G$ mit $ax = b$ und $ya = b$ (nämlich $x = a^{-1}b$ und $y = ba^{-1}$).

ii) Es gilt $(a^{-1})^{-1} = a$ für alle $a \in G$.

Beweis. Zu (i): Wir müssen zeigen, dass es eine Lösung der Gleichungen $ax = b$ bzw. $ya = b$ gibt und dass diese eindeutig bestimmt ist.

Existenz:
Einsetzen von $x = a^{-1}b$ und $y = ba^{-1}$ ergibt

$$ax = a(a^{-1}b) \underset{\text{(G1)}}{=} (aa^{-1})b \underset{\text{(G3)}}{=} eb \underset{\text{(G2)}}{=} b \quad \text{und} \quad ya = (ba^{-1})a \underset{\text{(G1)}}{=} b(a^{-1}a) \underset{\text{(G3)}}{=} be \underset{\text{(G2)}}{=} b.$$

Eindeutigkeit:
Sind $x_1, x_2 \in G$ zwei Lösungen von $ax = b$, so gilt $ax_1 = b = ax_2$. Nach Multiplikation von links mit a^{-1} erhalten wir $a^{-1}ax_1 = a^{-1}ax_2$, daraus folgt mit (G3) und (G2) $x_1 = x_2$, die Lösungen waren also gleich. Die Rechnung für die Lösungen von $ya = b$ verläuft analog.

Zu (ii): Nach (G3) ist $\tilde{a} = (a^{-1})^{-1}$ ein Element aus G mit der Eigenschaft $\tilde{a} \cdot a^{-1} = a^{-1} \cdot \tilde{a} = e$. Auch a erfüllt diese Eigenschaft wegen (G2). Nach Satz 1.1.1(ii) ist $a = \tilde{a} = (a^{-1})^{-1}$. □

Satz 1.1.3. *Für endlich viele Elemente $a_1, a_2, \ldots, a_n \in G$ gilt $(a_1 \cdot a_2 \cdots a_n)^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdots a_1^{-1}$.*

Beweis. Diese Aussage beweisen wir durch vollständige Induktion nach n:
Der Induktionsanfang ist $n = 1$: für nur ein einziges Element ist die Aussage $a_1^{-1} = a_1^{-1}$ richtig.
Die Induktionsannahme ist, dass für ein beliebiges $n \geq 1$ die Aussage $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ gilt.
Der Induktionsschritt besteht darin, dass wir die Aussage für $n+1$ zeigen, indem wir die Induktionsannahme für n verwenden. Die Aussage für n lautet, daß die rechte Seite des Satzes das Axiom (G3) erfüllt, also gilt

$$(a_1 \cdots a_n) \cdot (a_n^{-1} \cdots a_1^{-1}) = e.$$

Nach (G2) dürfen wir e in der Mitte einfügen ohne den Wert der linken Seite zu ändern:

$$(a_1 \cdots a_n) \cdot e \cdot (a_n^{-1} \cdots a_1^{-1}) = e.$$

Nach (G3) können wir e durch $a_{n+1}a_{n+1}^{-1}$ ersetzen, und erhalten

$$(a_1 \cdots a_n) \cdot (a_{n+1}a_{n+1}^{-1}) \cdot (a_n^{-1} \cdots a_1^{-1}) = e.$$

Wegen (G1) dürfen wir die Klammen umsetzen zu

$$(a_1 \cdots a_n \cdot a_{n+1}) \cdot (a_{n+1}^{-1} \cdot a_n^{-1} \cdots a_1^{-1}) = e.$$

Damit ist die rechte Klammer das Inverse der linken Klammer nach (G3). Das ist die gewünschte Aussage für $n+1$. Damit haben wir die Induktion abgeschlossen, und der Satz gilt für alle $n \in \mathbb{N}$. □

Definition 1.1.3. (Potenzen)
Es sei $(G, \circ)$ eine Gruppe und $a \in G$.

i) Für $n \in \mathbb{N} \cup \{0\}$ definieren wir rekursiv: $a^0 = e$ und $a^{n+1} = (a^n) \circ a$.

ii) Wir definieren $a^{-n} = (a^n)^{-1}$.

Satz 1.1.4. *(Potenzregeln)*
Es seien $(G, \circ)$ eine Gruppe und $a, b \in G$ mit $a \circ b = b \circ a$. Weiter seien $m, n \in \mathbb{Z}$. Dann haben wir

$$\begin{aligned} a^m \circ a^n &= a^{m+n} \\ (a \circ b)^m &= a^m \circ b^m \\ (a^m)^n &= a^{m \cdot n}. \end{aligned}$$

Beweis. ohne Beweis. □

1.2 Beispiele

Beispiele für Gruppen kommen in vielen Gebieten der Mathematik vor.

Beispiel 1.2.1. Es sei $\mathbb{Z}$ die Menge der ganzen Zahlen, $\mathbb{Q}$ die Menge der rationalen Zahlen und $\mathbb{R}$ die Menge der reellen Zahlen. Alle diese Mengen sind abelsche Gruppen bzgl. der Addition. Wir haben also die abelschen Gruppen $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$.

Beispiel 1.2.2. Die Menge $\mathbb{Z}$ der ganzen Zahlen bildet keine Gruppe bzgl. der Multiplikation. Es gibt zwar ein neutrales Element, nämlich die Zahl 1, aber es gibt für die Zahlen $a \neq \pm 1$ in $\mathbb{Z}$ keine Inversen.

Beispiel 1.2.3. Die Mengen $\mathbb{Q}\backslash\{0\}$ und $\mathbb{R}\backslash\{0\}$ bilden abelsche Gruppen bzgl. der Multiplikation.

Viele Beispiele von Gruppen werden durch Mengen von Abbildungen geliefert. Die Verknüpfung ist die Komposition (Hintereinanderausführung) von Abbildungen.

Definition 1.2.1. Es sei $\mathcal{M}$ eine beliebige nichtleere Menge.

i) Unter der Menge $S(\mathcal{M})$ verstehen wir die Menge aller bijektiver Abbildungen von $\mathcal{M}$ auf sich. Die Permutationsgruppe von $\mathcal{M}$ ist $(S(\mathcal{M}), \circ)$, wobei $\circ$ die Komposition von Abbildungen bedeutet.

ii) Es sei $n \in \mathbb{N}$. Unter der symmetrischen Gruppe S_n der Ordnung n versteht man die Permutationsgruppe.

Definition 1.2.2. (Darstellung von Permutationen)
Es sei $n \in \mathbb{N}$ und $\gamma \in S_n$. Dann schreiben wir

$$\gamma = \begin{pmatrix} 1 & 2 & \dots & n \\ \gamma(1) & \gamma(2) & \dots & \gamma(n) \end{pmatrix}.$$

Definition 1.2.3. (Zyklus)
Es sei $n \in \mathbb{N}$. Eine Permutation $\gamma \in S_n$ heißt Zyklus (der Länge m), wenn es paarweise verschiedene $a_1, a_2, \dots, a_m \in \{1, 2, \dots, n\}$ mit $\gamma(a_j) = a_{j+1}$ für $1 \leq j \leq m-1$, $\gamma(a_m) = a_1$ und $\gamma(l) = l$ für alle $l \notin \{a_1, a_2, \dots, a_m\}$ gibt. Wir schreiben $\gamma = (a_1\ a_2\ \dots\ a_m)$. Zwei Zyklen $\gamma = (a_1\ a_2\ \dots\ a_m)$ und $\delta = (b_1\ b_2\ \dots\ b_k)$ heißen elementefremd (disjunkt), wenn $\{a_1, a_2, \dots, a_m\} \cap \{b_1, b_2, \dots, b_k\} = \emptyset$ gilt.

Satz 1.2.1. *(Zyklendarstellung)*
Es sei $n \in \mathbb{N}$. Jede Permutation von S_n kann als Produkt elementefremder Zyklen dargestellt werden.

Beweis. Induktion nach n:
Der Fall $n = 1$ ist klar:

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = (1).$$

Es sei nun $n > 1$, und die Behauptung sei schon für alle $m < n$ bewiesen.
Es sei $\gamma \in S_n$. Wir definieren rekursiv $a_1 = 1$ und $a_{j+1} = \gamma(a_j)$.
Es sei $j_0 := \min\{j > 1 \colon a_j \in \{a_1, \dots, a_{j-1}\}\}$. Wäre jetzt $\gamma(a_{j_0-1}) = a_l$ für ein $l \neq 1$, so wäre $\gamma(a_{l-1}) = \gamma(a_{j_0}) = a_l$, im Widerspruch zur Bijektivität von γ.
Es sei weiter $\sigma_0 = (a_1\ \dots\ a_{j_0-1})$. Ist $j_0 - 1 = n$, so ist $\gamma = \sigma$. Andernfalls sei $A = \{a_1, \dots, a_{j_0-1}\}$ und $B = \{1, \dots, n\} - \{a_1, \dots, a_{j_0-1}\}$. Die Restriktion $\gamma\big|_B$ kann nach eventueller Umnummerierung der Elemente von B als Permutation in S_m mit $m = n - (j_0 - 1)$ angesehen werden.
Nach der Induktionshypothese ist aber $\gamma\big|_B$ ein Produkt von Zykeln: $\gamma\big|_B = \sigma_1 \circ \dots \circ \sigma_r$. Dann ist $\gamma = \sigma_0 \circ \gamma\big|_B = \sigma_0 \circ \sigma_1 \circ \dots \circ \sigma_r$. □

Beispiel 1.2.4. Es sei $n = 13$ und

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 4 & 7 & 10 & 1 & 2 & 5 & 8 & 11 & 13 & 12 & 9 & 6 & 3 \end{pmatrix}.$$

Dann ist

$$\gamma = \begin{pmatrix} 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 2 & 7 & 8 & 11 & 9 & 13 & 3 & 10 & 12 & 6 & 5 \end{pmatrix}.$$

Definition 1.2.4. Eine Gruppe $(G, \circ)$ heißt endlich, wenn sie endlich viele Elemente hat, andernfalls unendlich. Die Anzahl der Elemente heißt Ordnung von G, geschrieben: $|G|$. Ist G unendlich, so setzt man $|G| = \infty$.

Satz 1.2.2. *Es sei $n \in \mathbb{N}$.*

i) Es ist $|S_n| = n!$

ii) Für $n \geq 3$ ist $(S_n, \circ)$ nicht abelsch.

Beweis. i) Durch Induktion nach n.

ii) Es seien $\sigma, \gamma \in S_n$ mit $\sigma = (1\ 2)$ und $\gamma = (2\ 3)$ gegeben. Dann ist

$$\sigma \circ \gamma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 1 & \dots & n \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 3 & 1 & 2 & \dots & n \end{pmatrix} = \gamma \circ \sigma.$$

□

Wichtig sind auch Gruppen von Bijektionen auf einer Menge mit einer vorgegebenen Struktur. Von den Bijektionen wird verlangt, dass sie die "Struktur repektieren". In der Linearen Algebra begegnet man Mengen von linearen Abbildungen eines Vektorraumes.

Beispiel 1.2.5. Es sei V ein endlichdimensionaler Vektorraum und $GL(V)$ sei die Menge aller invertierbaren linearen Abbildungen von V auf sich selbst. Es sei $\circ$ die Komposition von Abbildungen. Dann ist $(GL(V), \circ)$ eine Gruppe.
Fordert man zusätzlich, dass die linearen Abbildungen eine vorgegebene Teilmenge $\mathcal{M} \subset V$ in sich überführen, so erhält man die Symmetriegruppe $\mathrm{Sym}(\mathcal{M})$ der Menge $\mathcal{M}$.

Beispiel 1.2.6. Es sei $Q = \{(1,1), (-1,1), (-1,-1), (1,-1)\}$ die Menge der Ecken eines Quadrats. Dann besteht $\mathrm{Sym}(\mathcal{M})$ aus acht Elementen: vier Drehungen um den Ursprung (die Identität eingeschlossen) und vier Spiegelungen (je zwei an den Verbindungsgeraden der Mittelpunkte gegenüberliegender Seiten und zwei an den Diagonalen).

1.3 Untergruppen, zyklische Gruppen

Definition 1.3.1. Es sei $(G, \circ)$ eine Gruppe und $U \subset G$. Dann heißt U Untergruppe von G, wenn auch $(U, \circ)$ eine Gruppe ist.

Beispiel 1.3.1. Die Gruppe $(\mathbb{R}, +)$ hat die Untergruppen $(\mathbb{Q}, +)$ und $(\mathbb{Z}, +)$.

Beispiel 1.3.2. Die Gruppe $(\mathbb{Z}, +)$ hat die Untergruppen

$$m\mathbb{Z} = \{k \cdot m \colon k \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, 2m, \dots\}$$

für alle $m \in \mathbb{N}_0$.

Um die Untergruppeneigenschaft einer Teilmenge $U \subset G$ nachzuweisen, genügt der Nachweis des folgenden Untergruppenkriteriums:

Satz 1.3.1. *(Untergruppenkriterium)*
Es sei $(G, \circ)$ eine Gruppe und $U \subset G$. Dann ist U genau dann eine Untergruppe von G, wenn gilt:

i) Die Menge U ist nichtleer: $U \neq \emptyset$

ii) Für alle $a, b \in U$ gilt $a \circ b^{-1} \in U$.

Beweis. Da das Assoziativgesetz auf ganz G gilt, gilt es auch auf der Teilmenge U. Es bleibt, die Abgeschlossenheit von U bzgl. $\circ$, die Existenz eines neutralen Elementes in U und die Abgeschlossenheit der Inversenbildung nachzuweisen.
Wegen $U \neq \emptyset$ gibt es ein $a \in U$. Nach (ii) gilt dann

$$e = a \circ a^{-1} \in U \tag{1}$$

und weiter

$$e \circ a^{-1} = a^{-1} \in U. \tag{2}$$

Damit folgt

$$a, b \in U \underset{(2)}{\Rightarrow} a, b^{-1} \in U \underset{(ii)}{\Rightarrow} a \circ (b^{-1})^{-1} = a \circ b \in U.$$

□

Untergruppen können auch durch Erzeugendensysteme definiert werden.

Definition 1.3.2. Es sei $(G, \circ)$ eine Gruppe und $\mathcal{M} \subset G$. Dann bedeutet $\langle \mathcal{M} \rangle$ die kleinste Untergruppe von G, die $\mathcal{M}$ enthält. So heißt $U = \langle \mathcal{M} \rangle$ die von $\mathcal{M}$ erzeugte Untergruppe von G, und $\mathcal{M}$ heißt ein Erzeugendensystem von U.
Ist $\mathcal{M} = \{a\}$ eine einelementige Menge, so schreiben wir $\langle a \rangle$ anstatt $\langle \{a\} \rangle$ und sagen: U wird von a erzeugt oder a ist ein erzeugendes Element. Eine Gruppe G heißt zyklisch, wenn es ein $g \in G$ mit $G = \langle g \rangle$ gibt.

Beispiel 1.3.3. Die Gruppe $(\mathbb{Z}, +)$ wird von 1 erzeugt. Es ist $\mathbb{Z} = \langle 1 \rangle$. Das einzige andere erzeugende Element ist -1, weswegen ebenfalls $\mathbb{Z} = \langle -1 \rangle$ gilt. Somit ist $(\mathbb{Z}, +)$ eine unendliche zyklische Gruppe.

Satz 1.3.2. *Es sei $(G, \circ)$ eine Gruppe und $a \in G$. Dann ist*

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

die Menge aller Potenzen von a.

Beweis. Es sei $H = \{a^n : n \in \mathbb{Z}\}$. Es seien weiter $c = a^m, d = a^n \in H$.
Dann ist auch $c \circ d^{-1} = a^{m-n} \in H$. Also erfüllt H das Untergruppenkriterium von Satz 1.3.1. □

Wir definieren nun die Ordnung eines Gruppenelements.

Definition 1.3.3. Es sei $(G, \circ)$ eine Gruppe und $a \in G$.

i) Sind alle Potenzen a^k mit $k \in \mathbb{Z}$ verschieden, so sagen wir: a hat die Ordnung ∞ oder ist von unendlicher Ordnung.

ii) Sind nicht alle Potenzen a^k mit $k \in \mathbb{Z}$ verschieden, so definieren wir die Ordnung von a als das kleinste $n \in \mathbb{N}$ mit $a^n = e$.

Die Ordnung einer endlichen zyklischen Gruppe ist gleich der Ordnung eines erzeugenden Elementes.

Satz 1.3.3. *Es sei $(G, \circ)$ eine Gruppe und $a \in G$.*

i) Ist a von unendlicher Ordnung, so ist $\langle a \rangle$ eine unendliche Gruppe.

ii) Hat a die Ordnung $n \in \mathbb{N}$, so ist $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$. Es ist dann $|\langle a \rangle| = n$.

Beweis. i) Annahme: $\langle a \rangle$ ist endlich. Dann können nicht alle Potenzen a^n mit $n \in \mathbb{N}$ verschieden sein. Es gibt also $k < l \in \mathbb{N}$ mit $a^k = a^l$. Dann ist $a^{l-k} = e$, also ist a nicht von unendlicher Ordnung., ein Widerspruch.

ii) Es ist $a^{n-1} \circ a = e$, also

$$a^{-1} = a^{n-1}. \tag{1}$$

Weiter sei $k = n \cdot q + r$ mit $0 \leq r \leq n-1$. Dann ist

$$a^k = (a^n)^q \cdot a^r = a^r. \tag{2}$$

Damit ist $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$. Wäre $a^k = a^l$ für $1 \leq k < l < n$, so wäre $a^{l-k} = e$, also die Ordnung von a kleiner als n.

□

Bemerkung 1.3.1. Nach Satz 1.3.3 kann die Ordnung eines Elements $a \in G$ kurz als $|\langle a \rangle|$ geschrieben werden.

Beispiel 1.3.4. Es sei $(G, \circ) = (S_8, \circ)$ sowie $\gamma = \sigma_1 \cup \sigma_2$ mit den beiden Zykeln $\sigma_1 = (1\ 2\ 3)$ und $\sigma_2 = (4\ 5\ 6\ 7\ 8)$. Dann ist $\sigma_1^2 = (1\ 3\ 2)$ und $\sigma_1^3 = \sigma_1^0 = id$. Also ist $|\langle \sigma_1 \rangle| = 3$. Analog ergibt sich dann $|\langle \sigma_2 \rangle| = 5$. Es ist $\gamma^m = \sigma_1^m \circ \sigma_2^m$, da offenbar elementfremde Zyklen vertauscht werden können. Es ist

$$\gamma^m = id \Leftrightarrow \sigma_1^m = id,\ \sigma_2^m = id,$$

also wenn m durch 3 und 5 teilbar ist. Damit ist $|\langle \gamma \rangle| = 15$.

1.4 Isomorphismen

Zur Beschreibung der Idee beginnen wir mit einem Beispiel:

Beispiel 1.4.1. Wir betrachten die beiden Gruppen $(G, \cdot)$ und $(S_2, \circ)$. Dabei sei $G = \{1, -1\}$ und $\cdot$ die Multiplikation. Es ist $S_2 = \{id, (1\ 2)\}$. Wir haben die Verknüpfungstafeln

für G:

$\cdot$	1	-1
1	1	-1
-1	-1	1

und für S_2:

$\circ$	id	$(1\ 2)$
id	id	$(1\ 2)$
$(1\ 2)$	$(1\ 2)$	id

.

Die beiden Gruppen $(G, \cdot)$ und $(S_2, \circ)$ sind "im wesentlichen gleich", sie unterscheiden sich nur durch die Namen ihrer Elemente. Die Namensänderung wird durch die Abbildung $\Phi\colon G \to S_2$ mit $\Phi(1) = id$ und $\Phi(-1) = (1\ 2)$ vermittelt.
Die Verknüpfungstafel von G geht durch die Namensänderung Φ in die Verknüpfungstafel von S_2 über. Damit ist Φ ein Isomorphismus, und $(G, \cdot)$ und $(S_2, \circ)$ sind isomorph.

Definition 1.4.1. Es seien $(G, \circ)$ und $(H, \star)$ Gruppen.
Eine Abbildung $\Phi\colon G \to H$ heißt Isomorphismus (von G nach H), wenn sie folgende Eigenschaften erfüllt:

i) Die Abbildung Φ ist bijektiv.

ii) Es gilt $\Phi(a \circ b) = \Phi(a) \star \Phi(b)$ für alle $a, b \in G$ (Relationstreue).

Beispiel 1.4.2. Es sei $\mathbb{R}^+ = (0, \infty)$. Die Gruppen $G = (\mathbb{R}, +)$ und $H = (\mathbb{R}^+, \cdot)$ sind isomorph. Der Isomorphismus von G nach H ist die Exponentialfunktion $\exp\colon \mathbb{R} \to \mathbb{R}^+$ mit $x \to e^x$ wegen der Funktionalgleichung $\exp(x_1 + x_2) = \exp(x_1) \cdot \exp(x_2)$. Die Umkehrabbildung $\log\colon \mathbb{R}^+ \to \mathbb{R}$ mit $y \to \log y$ ist ein Isomorphismus von H nach G.

Isomorphismen sind nützlich, wenn es darum geht, Gruppen zu klassifizieren. Darunter versteht man die Lösung des folgenden Problems:
Gegeben sei eine Kategorie von Gruppen einer festen Ordnung n. Es ist ein Katalog von Repräsentanten zu erstellen, so dass jede Gruppe der gegebenen Kategorie zu genau einem dieser Repräsentanten isomorph ist.
Wir lösen dieses Problem für den Fall der zyklischen Gruppen.

Satz 1.4.1. *i) Jede unendliche zyklische Gruppe ist isomorph zu $(\mathbb{Z}, +)$.*

ii) Eine endliche zyklische Gruppe der Ordnung n ist isomorph zur additiven Gruppe der Restklassen modulo n.

Beweis. Übungsaufgabe □

1.5 Homomorphismen

Schwächt man die Forderungen an die Eigenschaften eines Isomorphismus dadurch ab, dass man nur die Relationstreue, nicht jedoch die Bijektivität verlangt, so erhält man den allgemeinen Begriff des Homomorphismus.

Definition 1.5.1. Es seien $(G, \circ)$ und $(H, \star)$ Gruppen. Eine Abbildung $\varphi\colon G \to H$ heißt ein Homomorphismus (von G nach H), wenn $\varphi(a \circ b) = \varphi(a) \star \varphi(b)$ für alle $a, b \in G$ gilt (Relationstreue).

Ein Homomorphismus liefert ein im allgemeinen verkleinertes Bild der gegebenen Gruppe G (ein Miniaturmodell).

Beispiel 1.5.1. Es sei $(G, \circ) = (\mathbb{R}\backslash\{0\}, \cdot)$ und $(H, \star) = (\{-1, 1\}, \cdot)$. Ein Homomorphismus ist durch die Vorzeichenfunktion sgn mit

$$\operatorname{sgn}(x) = \begin{cases} 1, & \text{falls} \quad x > 0, \\ -1, & \text{falls} \quad x < 0. \end{cases}$$

gegeben. Die einzige Information, die erhalten bleibt, ist das Vorzeichen von x.
Die Verknüpfungstafel von $(H, \star)$

$\star$	1	-1
1	1	-1
-1	-1	1

illustriert dann die Vorzeichenregeln (z.B. "minus mal minus gibt plus").

Wir ergänzen die Definition des Homomorphismus wie folgt:

Definition 1.5.2. i) Ein surjektiver Homomorphismus heißt Epimorphismus.

ii) Ein injektiver Homomorphismus heißt Monomorphismus.

iii) Ein Isomorphismus einer Gruppe G auf sich selbst heißt Automorphismus.

1.6 Gruppenwirkungen

Definition 1.6.1. Man sagt: Eine Gruppe G wirkt (oder operiert) auf einer Menge M (von links), wenn eine Abbildung $G \times M \to M$, $(g, m) \to gm$ mit

i) $(fg)m = f(gm)$ für alle $f, g \in G$ und alle $m \in M$ und

ii) $1m = m$ für alle $m \in M$, wobei 1 das Einselement von G ist,

gegeben ist. Analog werden Gruppenwirkungen von rechts definiert.

Gruppenwirkungen kommen in vielen Gebieten der Mathematik vor. Sie sind jedoch auch in der Gruppentheorie von Bedeutung.

Beispiel 1.6.1. Es sei V ein Vektorraum über einem Körper K, und $G = K - \{0\}$ sei eine Gruppe bzgl. der Multiplikation. Dann wirkt G auf V durch Skalarmultiplikation:

$$(\lambda, \vec{v}) = \lambda\vec{v}$$

mit $\lambda \in G$ und $\vec{v} \in V$.

Beispiel 1.6.2. Es sei K ein Körper und $V = K^n$ der Vektorraum aller n- tupel über K (als Spaltenvektoren geschrieben). Weiter sei $GL(n, K)$ die Gruppe aller nicht- singulären Matrizen vom Typ (n, n). Dann wirkt $GL(n, K)$ auf V durch Matrixmultiplikation von links:

$$(A, \vec{v}) = A\vec{v}$$

mit $A \in GL(n, K)$ und $\vec{v} \in K^n$.

Beispiel 1.6.3. Es sei G eine Gruppe und $M = G$. Die Abbildung $G \times G \to G$ sei durch $(g, x) \to gx$ gegeben. Dann wirkt G auf sich selbst durch Linksmultiplikation.

Wir machen nun eine Exkursion in die Graphentheorie. Deren Objekte, die Graphen, sind nicht eigentlicher Gegenstand dieser Vorlesung. Sie liefern jedoch, wie die in Abschnitt 1.2 erwähnte Symmetriegruppe, viele Beispiele für Gruppenwirkungen und Gruppenisomorphismen.

Definition 1.6.2. Ein Graph ist ein Paar $\mathcal{G} = (E, K)$, wobei E eine beliebige Menge von Objekten, die Ecken genannt werden, während K eine Menge von zweielementigen Teilmengen $k = \{e_1, e_2\}$ mit $e_1, e_2 \in E$ ist. Für $k = \{e_1, e_2\}$ mit $e_1, e_2 \in E$ schreiben wir auch $k = \overline{e_1 e_2}$ und nennen k die Kante zwischen e_1 und e_2. Zwei Ecken e_1 und e_2 heißen verbunden (oder benachbart), falls $\overline{e_1 e_2} \in K$ ist. Für $e \in E$ heißt die Anzahl der zu e benachbarten Ecken der Grad von e ($\operatorname{grad} e$).

Definition 1.6.3. Es seien $\mathcal{G} = (E_1, K_1)$ und $\mathcal{U} = (E_2, K_2)$ Graphen. Eine bijektive Abbildung $\tau\colon E_1 \to E_2$ heißt genau dann (Graphen)- Isomorphismus, wenn

$$\overline{e_1 e_2} \in K_1 \Leftrightarrow \overline{\tau(e_1)\tau(e_2)} \in K_2$$

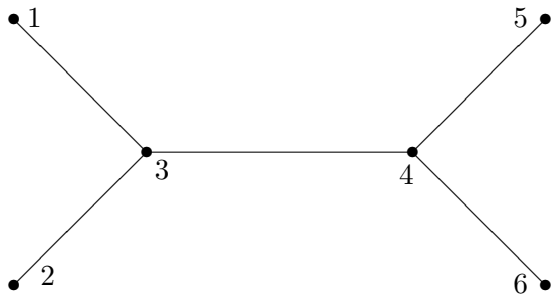
ist. Ist $\mathcal{G} = \mathcal{U}$, so heißt τ Automorphismus von $\mathcal{G}$. Die Menge aller Automorphismen von $\mathcal{G}$ heißt die Automorphismengruppe von $\mathcal{G}$ (Schreibweise: $\operatorname{Aut}(\mathcal{G})$).

Dieser Name erklärt sich aus folgendem leicht zu beweisendem Satz:

Satz 1.6.1. *Es sei $\mathcal{G}$ ein Graph. Dann ist $\operatorname{Aut}(\mathcal{G})$ eine Gruppe bezüglich der Hintereinanderausführung von Abbildungen.*

Beweis. Übungsaufgabe. □

Beispiel 1.6.4. Es sei $\mathcal{G} = (E, K)$ mit $E = \{1, 2, 3, 4, 5, 6\}$ und $K = \{\overline{13}, \overline{23}, \overline{34}, \overline{45}, \overline{46}\}$.



Bestimme $\mathrm{Aut}(\mathcal{G})$.

Lösung:
Ist $\tau \in \mathrm{Aut}(\mathcal{G})$, so gilt für alle $e \in E$, dass e und $\tau(e)$ mit derselben Anzahl von Ecken verbunden sind. Also ist $\operatorname{grad} e = \operatorname{grad} \tau(e)$. Da $e = 3$ und $e = 4$ die einzigen Ecken mit $\operatorname{grad} e = 3$ sind, muss für τ einer der folgenden Fälle gelten:
Fall 1: $\tau(3) = 3$, $\tau(4) = 4$
Fall 2: $\tau(3) = 4$, $\tau(4) = 3$.
In jedem der Fälle 1 und 2 gibt es vier Möglichkeiten für die Bilder der Ecken $\{1, 2, 5, 6\}$.
Wir erhalten

$$\begin{aligned}\mathrm{Aut}(\mathcal{G}) \;=\; &\left\{id, \begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&6&5\end{pmatrix}, \begin{pmatrix}1&2&3&4&5&6\\2&1&3&4&5&6\end{pmatrix}, \begin{pmatrix}1&2&3&4&5&6\\2&1&3&4&6&5\end{pmatrix},\right.\\ &\left.\begin{pmatrix}1&2&3&4&5&6\\5&6&4&3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4&5&6\\5&6&4&3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix}\right\}\end{aligned}$$

Die Automorphismengruppe $\mathrm{Aut}(\mathcal{G})$ eines Graphen $\mathcal{G}$ liefert Beispiele von Gruppenwirkungen.

Beispiel 1.6.5. Es sei $\mathcal{G} = (E, K)$ ein Graph. Dann wirkt die Automorphismengruppe sowohl auf E als auch auf K.

Definition 1.6.4. Die Gruppe G operiere von links auf der Menge M, und es sei $m \in M$.

i) $\mathrm{Stab}_G(m) := \{g \in G \colon gm = m\}$ heißt der Stabilisator von m in G.

ii) $Gm = \{gm \colon g \in G\}$ heißt die Bahn von m unter G.
Bei Operationen von rechts definiert man analog $\mathrm{Stab}_G(m) := \{g \in G \colon mg = m\}$ und eben $mG = \{mg \colon g \in G\}$.

iii) Die Menge der Bahnen wird mit $G\backslash M$ bezeichnet bzw. bei Operationen von rechts mit M/G.

Beispiel 1.6.6. Es sei K ein Körper und V ein Vektorraum über K. Die Gruppe $G = (K - \{0\}, \cdot)$ wirkt auf V durch Skalarmultiplikation.

i) Es sei $\vec{v} \neq \vec{0}$. Dann ist die Bahn von $\vec{v}$ gerade $G\vec{v} = \{\lambda\vec{v} \colon \lambda \in K - \{0\}\}$, der von $\vec{v}$ aufgespannte eindimensionale Unterraum (Gerade) ohne den Nullvektor.
Es ist $\mathrm{Stab}_G(\vec{v}) = \{1\}$.

ii) Es sei $\vec{v} = \vec{0}$. Dann ist die Bahn $G\vec{v} = \{\vec{0}\}$ und $\mathrm{Stab}_G(\vec{v}) = G$.

Satz 1.6.2. *Die Gruppe G wirke von links auf der Menge M.*

i) Der Stabilisator $\mathrm{Stab}_G(m)$ ist für alle $m \in M$ eine Untergruppe von G.

ii) Die Menge aller Bahnen auf M unter G bildet eine Partition auf M. Insbesondere sind zwei Bahnen entweder disjunkt oder gleich.

Beweis. i) Es ist $1 \in \mathrm{Stab}_G(m)$, insbesondere ist $\mathrm{Stab}_G(m) \neq \emptyset$.
Seien also $g, h \in \mathrm{Stab}_G(m)$, so ist $(gh^{-1})m = g(h^{-1}m) = gm = m$, denn aus $hm = m$ folgt $m = h^{-1}m$. Also ist $gh^{-1} \in \mathrm{Stab}_G(m)$, d.h. $\mathrm{Stab}_G(m)$ erfüllt das Untergruppenkriterium von Satz 1.3.1.

ii) Aus $m = 1m \in Gm$ für alle $m \in M$ folgt

$$M = \bigcup_{m \in M} Gm.$$

Wir zeigen, dass die Bahnen Gm entweder gleich oder disjunkt sind. Dazu seien $x, y \in M$ und $Gx \cap Gy \neq \emptyset$, womit ein $n \in Gx \cap Gy$ existiert. Da $n \in Gx$ liegt, gibt es ein $g \in G$ mit $n = gx$. Es gilt

$$Gn = \{hn \colon h \in G\} = \{h(gx) \colon h \in G\} = \{(hg)x \colon h \in G\} = \{ix \colon i \in G\} = Gx.$$

Analog erhält man $Gn = Gy$. Also ist $Gx = Gy$.

□

Definition 1.6.5. Eine Gruppe G wirke auf einer Menge M (von links oder rechts). Eine Menge $R \subset M$ heißt ein Repräsentantensystem der Gruppenwirkung, falls es zu jeder Bahn B genau ein $r \in R$ mit $r \in B$ gibt.

Beispiel 1.6.7. Wir kehren zu Beispiel 1.6.4 zurück.
Es sei $\mathcal{G} = (E, K)$ mit $E = \{1, 2, 3, 4, 5, 6\}$ und $K = \{\overline{13}, \overline{23}, \overline{34}, \overline{45}, \overline{46}\}$.

i) Bestimme die Bahnen sowie ein Repräsentantensystem der Gruppe $G = \mathrm{Aut}(\mathcal{G})$.

ii) Bestimme den Stabilisator $\mathrm{Stab}_G(3)$ sowie die Bahnen und ein Repräsentantensystem der Gruppenwirkung von $\mathrm{Stab}_G(3)$ auf E.

Lösung:

i) Aus der Liste der Elemente von $\mathrm{Aut}(\mathcal{G})$ in Beispiel 1.6.4 ist ersichtlich, dass es zu jedem Paar (e_1, e_2) mit $e_i \in B_1 = \{1, 2, 5, 6\}$ ein $g \in \mathrm{Aut}(\mathcal{G})$ mit $ge_1 = e_2$ gibt. Dasselbe gilt für (e_3, e_4) mit $e_i \in B_2 = \{3, 4\}$. Hingegen ist $g3 \notin B_1$ bzw $g4 \notin B_1$. Die Bahnen sind somit $B_1 = \{1, 2, 5, 6\}$ und $B_2 = \{3, 4\}$. Ein Repräsentantensystem ist daher $R = \{1, 3\}$.

ii) Es ist

$$\mathrm{Stab}_G(3) = \left\{ id, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 6 & 5 \end{pmatrix} \right\}.$$

Elemente, die bezüglich der Wirkung einer Gruppe G zur selben Bahn gehören, brauchen bezüglich der Wirkung einer Untergruppe U von G nicht zur selben Bahn gehören.
In diesem Fall zerfällt die Bahn $B_1 = \{1, 2, 5, 6\}$ bezüglich der Wirkung von $\mathrm{Aut}(\mathcal{G})$ in die Bahnen $B_{1,1} = \{1, 2\}$ und $B_{1,2} = \{5, 6\}$ unter der Wirkung von $\mathrm{Stab}_G(3)$ und die Bahn $B_2 = \{3, 4\}$ bezüglich der Wirkung von $\mathrm{Aut}(\mathcal{G})$ in die Bahnen $B_{2,1} = \{3\}$ und $B_{2,2} = \{4\}$ unter der Wirkung von $\mathrm{Stab}_G(3)$. Ein Repräsentantensystem ist $R' = \{1, 3, 4, 6\}$.

1.7 Nebenklassen, Normalteiler und Faktorgruppen

Um eine einfachere Schreibweise zur Verfügung zu haben, führen wir zunächst das Komplexprodukt ein.

Definition 1.7.1. (Komplexprodukt)
Es sei $(G, \cdot)$ eine Gruppe und $S, T \subset G$ Teilmengen von G (Komplexe). Unter dem Komplexprodukt ST versteht man

$$ST := \{st \colon s \in S, t \in T\}.$$

Ist S (bzw. T) eine einelementige Menge $S = \{s\}$ (bzw. $T = \{t\}$), so schreibt man auch sT statt $\{s\}T$ (bzw. St statt $S\{t\}$).

Eine entsprechende Definition kann auch für Gruppenwirkungen gegeben werden.

Definition 1.7.2. Die Gruppe G wirke auf der Menge M (von links). Es sei $S \subset G$ und $L \subset M$. Dann versteht man unter SL die Menge $SL = \{sl \colon s \in S, l \in L\}$. Sind $S = \{s\}$ (bzw. $L = \{l\}$) einelementige Mengen, so schreibt man sL (bzw. Sl).

Wir kommen nun zu einem wichtigen Spezialfall einer Gruppenwirkung. Es sei U eine Untergruppe der (multiplikativ geschriebenen) Gruppe G. Dann operiert U auf G durch Multiplikation von links (oder rechts). Ist G kommutativ, braucht zwischen links und rechts natürlich nicht unterschieden zu werden. In diesem Abschnitt werden wir die Bahnen dieser Gruppenwirkung betrachten, die sogenannten Nebenklassen von U. Eines der bekanntesten Beispiele entstammt der elementaren Zahlentheorie.

Definition 1.7.3. Es sei $m \in \mathbb{N}$ und $k, l \in \mathbb{Z}$.
Dann heißen k und l kongruent modulo m (Schreibweise: $k \equiv l \bmod m$), wenn $m|(k-l)$ gilt. Andernfalls heißen sie inkongruent modulo m, also $k \not\equiv l \bmod m$. Die Menge $\{l \in \mathbb{Z} \colon l \equiv k \bmod m\}$ heißt die Restklasse (Kongruenzklasse) $k \bmod m$.

Satz 1.7.1. *Es sei $m \in \mathbb{N}$.*

i) Für $k, l \in \mathbb{Z}$ gilt genau dann $k \equiv l \bmod m$, wenn k und l zu derselben Bahn der Wirkung von $(m\mathbb{Z}, +)$ auf $(\mathbb{Z}, +)$ durch Addition gehören.

ii) Es gibt m Bahnen dieser Gruppenwirkung, und zwar die Restklassen $0 \bmod m$, $1 \bmod m, \ldots,$ $(m-1) \bmod m$.

Beweis. i) Dies folgt sofort aus der Definition der Gruppenwirkung.

ii) Die Zahlen $0, 1, \ldots, m-1$ sind offenbar paarweise inkongruent modulo m. Also repräsentieren sie verschiedene Bahnen. Andererseits repräsentieren sie auch sämtliche Bahnen: Es sei $l = q \cdot m + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r \leq m-1$. Dann ist $l \equiv r \bmod m$.

□

Definition 1.7.4. Es sei $(G, \circ)$ eine Gruppe und $(U, \circ)$ eine Untergruppe von G. Die Bahnen der Wirkung von U auf G durch Multiplikation von rechts (bzw. von links) heißen Linksnebenklassen (bzw. Rechtsnebenklassen) modulo U.
Zwei Elemente $g, h \in G$ heißen linkskongruent (bzw. rechtskongruent) modulo U (Schreibweise: $g \equiv_l h \bmod U$ bzw. $g \equiv_r h \bmod U$), wenn sie derselben Links- (bzw. Rechts-) nebenklasse modulo U angehören.
Die Anzahl der Linksnebenklassen modulo U heißt der Index von U in G (Schreibweise: $(G \colon U)$). Dabei ist $(G \colon U) = \infty$ möglich.

Bemerkung 1.7.1. Aus Definition 1.7.3 ergibt sich für die Menge der Links- (bzw. Rechts-) nebenklassen die Bezeichnung G/U (bzw. $U\backslash G$).

Man sieht sofort die Gültigkeit von

Satz 1.7.2. *Es sei G eine Gruppe und $g \in G$. Die Links- (bzw. Rechts-) nebenklassen von g sind durch gU (bzw. Ug) im Sinne von Definition 1.7.1 gegeben. Es seien $g, h \in G$. Dann gilt*

$$\begin{aligned} g \equiv_l h \bmod U &\Leftrightarrow h^{-1}g \in U \\ g \equiv_r h \bmod U &\Leftrightarrow hg^{-1} \in U. \end{aligned}$$

Für endliche Gruppen G führt das Konzept der Nebenklassen zu einer wichtigen Beziehung zwischen der Ordnung der Gesamtgruppe G und der Ordnung einer Untergruppe U.

Satz 1.7.3. *(Lagrange)*
Es sei G eine endliche Gruppe und U eine Untergruppe von G. Dann gilt für alle $g \in G$

$$|gU| = |Ug| = |U|.$$

Dann teilt die Ordnung der Untergruppe U die Ordnung der Gruppe G. Die Anzahl der Linksnebenklassen von U in G ist gleich der Anzahl der Rechtsnebenklassen, und es gilt

$$|G/U| = |U\backslash G| = \frac{|G|}{|U|}.$$

Der Index von U in G (in Definition 1.7.4 als die Anzahl der Linksnebenklasen definiert) ist auch die Anzahl der Rechtsnebenklassen. Es ist $|G| = (G\colon U) \cdot |U|$.

Beweis. Nach Satz 1.6.2 bildet die Menge aller Links- (bzw. Rechts-) nebenklassen eine Partition von G, also $G = U \cup g_2U \cup \ldots \cup g_lU$. Die Abbildung $U \to gU$, $u \to gu$ ist eine Bijektion. Also gilt $|U| = |g_iU|$ für alle $i = 1, \ldots, l$ und damit $l \cdot |U| = |G|$.
Der Rest der Behauptung folgt aus Definition 1.7.4. □

Wir kehren noch einmal zum Thema der Gruppenwirkung zurück.

Satz 1.7.4. *(Bahnensatz)*
Die Gruppe G wirke (von links) auf der Menge M mit $m \in M$. Dann gibt es eine Bijektion τ zwischen den Elementen der Bahn von m und den Linksnebenklassen $G\backslash \operatorname{Stab}_G(m)$, welche durch

$$\tau\colon \begin{cases} Gm \to G\backslash \operatorname{Stab}_G(m) \\ gm \to g \operatorname{Stab}_G(m) \end{cases}$$

definiert ist. Insbesondere ist

$$|Gm| = \frac{|G|}{|\operatorname{Stab}_G(m)|}.$$

Beweis. Es sei $G = \operatorname{Stab}_G(m) \cup g_1 \operatorname{Stab}_G(m) \cup \ldots \cup g_l \operatorname{Stab}_G(m)$ die Partition von G in Linksnebenklassen von $\operatorname{Stab}_G(m)$ in G. Es ist zu zeigen, dass τ wohldefiniert ist, d.h. nicht von der Wahl des Repräsentanten g abhängt. Es seien $g, h \in G$. Dann gilt

$$gm = hm \Leftrightarrow h^{-1}gm = m \Leftrightarrow h^{-1}g \in \operatorname{Stab}_G(m) \Leftrightarrow g \operatorname{Stab}_G(m) = h \operatorname{Stab}_G(m).$$

Das zeigt auch die Injektivität von τ. Die Surjektivität ist klar. □

Unter gewissen Bedingungen ist es möglich, die Menge der Nebenklassen einer Untergruppe wieder zu einer Gruppe zu machen.

Beispiel 1.7.1. Es sei $m \in \mathbb{N}$. Die Menge $(\mathbb{Z}/m\mathbb{Z})$ der Restklassen modulo m ist bezüglich des Komplexproduktes (das in diesem Fall eine Addition von Komplexen ist), eine zyklische Gruppe der Ordnung m.

Entscheidend für das Gelingen dieser Konstruktion ist hier die Tatsache, dass das Produkt (hier die Summe) zweier Nebenklassen wieder eine Nebenklasse ist. Dies ist nicht immer der Fall, wie folgendes Beispiel zeigt:

Beispiel 1.7.2. Es sei $G = S_3 = \{id, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ mit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{und} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Es gilt $\tau\sigma = \sigma^2\tau$ und $\tau\sigma^2 = \sigma\tau$. Wir betrachten zunächste die "gute" Untergruppe $U_1 = \{id, \sigma, \sigma^2\}$. Obwohl die Verknüpfung nichtkommutativ ist, sind Links- und Rechtsnebenklassen identisch. Es gilt $id \cdot U_1 = U_1 \cdot id$ und $\tau \cdot U_1 = U_1 \cdot \tau$. In der Verknüpfungstafel gruppieren wir die Elemente aus den selben Nebenklassen zusammen:

	$id \cdot U_1$			$\tau \cdot U_1$		
$\circ$	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
id	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	id	$\tau\sigma$	$\tau\sigma^2$	τ
σ^2	σ^2	id	σ	$\tau\sigma^2$	τ	$\tau\sigma$
τ	τ	$\tau\sigma^2$	$\tau\sigma$	id	σ^2	σ
$\tau\sigma$	$\tau\sigma$	τ	$\tau\sigma^2$	σ	id	σ^2
$\tau\sigma^2$	$\tau\sigma^2$	$\tau\sigma$	τ	σ^2	σ	id

Wir haben die folgenden Eigenschaften:

i) Es gilt
$$g_1 \equiv_l g_2 \bmod U_1,\ h_1 \equiv_l h_2 \bmod U_1 \Rightarrow g_1h_1 \equiv_l g_2h_2 \bmod U_1.$$
Dasselbe gilt für die Rechtskongruenz.

ii) Die Linksnebenklassen U_1 und $\tau \cdot U_1 = \{\tau, \tau\sigma, \tau\sigma^2\}$ entsprechen den Rechtsnebenklassen U_1 und $U_1 \cdot \tau = \{\tau, \sigma\tau = \tau\sigma^2, \sigma^2\tau = \tau\sigma\}$.

iii) Das Komplexprodukt zweier Nebenklassen ist wieder eine Nebenklasse.

Auch die Menge der Nebenklasse bildet eine Gruppe bzgl. des Komplexproduktes

$\circ$	$id \cdot U_1$	$\tau \cdot U_1$
$id \cdot U_1$	$id \cdot U_1$	$\tau \cdot U_1$
$\tau \cdot U_1$	$\tau \cdot U_1$	$id \cdot U_1$.

Diese Gruppe werden wir später die Faktorgruppe S_3/U_1 nennen.
Die Abbildung $\Phi\colon S_3 \to S_3/U_1$, $\gamma \to \gamma U_1$ ist ein Epimorphismus.

Wir betrachten nun die "schlechte" Untergruppe $U_2 = \{id, \tau\}$:
Die Linksnebenklassen sind

$$U_2 = \{id, \tau\},\ \sigma U_2 = \{\sigma, \sigma\tau\},\ \sigma^2 U_2 = \{\sigma^2, \sigma^2\tau\}$$

und die Rechtsnebenklassen

$$U_2 = \{id, \tau\},\ U_2\sigma = \{\sigma, \sigma^2\tau\},\ U_2\sigma^2 = \{\sigma^2, \sigma\tau\}.$$

Weiter gilt

$\circ$	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
id	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	id	$\tau\sigma$	$\tau\sigma^2$	τ
σ^2	σ^2	id	σ	$\tau\sigma^2$	τ	$\tau\sigma$
τ	τ	$\tau\sigma^2$	$\tau\sigma$	id	σ^2	σ
$\tau\sigma$	$\tau\sigma$	τ	$\tau\sigma^2$	σ	id	σ^2
$\tau\sigma^2$	$\tau\sigma^2$	$\tau\sigma$	τ	σ^2	σ	id

Wir sehen, dass keine der Eigenschaften, die für U_1 die Konstruktion einer Faktorgruppe ermöglicht haben, für U_2 erfüllt ist.

Es stellt sich heraus, dass jede der drei Eigenschaften aus Beispiel 1.7.2 jeweils die beiden anderen impliziert. Wir legen eine dieser Eigenschaften der Definition des Normalteilers zugrunde.

Definition 1.7.5. Ein Normalteiler einer Gruppe G (geschrieben: $N \trianglelefteq G$) ist eine Untergruppe N von G, für die die Relation $\equiv_l \bmod N$ gleich der Relation $\equiv_r \bmod N$ ist. Man schreibt dann für beide Relationen einfach $\equiv \bmod N$.

Satz 1.7.5. *Es sei N eine Untergruppe der Gruppe G. Folgende Aussagen sind äquivalent:*

i) N *ist ein Normalteiler.*

ii) $gN = Ng$ *für alle* $g \in G$

iii) $gNg^{-1} = N$ *für alle* $g \in G$

iv) $gNg^{-1} \subset N$ *für alle* $g \in G$

v) $(gN)(hN) = (gh)N$ *für alle* $g, h \in G$

vi) $(Ng)(Nh) = N(gh)$ *für alle* $g, h \in G$

vii) Aus $g_1 \equiv_l g_2 \bmod N$ *und* $h_1 \equiv_l h_2 \bmod N$ *folgt* $g_1h_1 \equiv_l g_2h_2 \bmod N$.

viii) Aus $g_1 \equiv_r g_2 \bmod N$ *und* $h_1 \equiv_r h_2 \bmod N$ *folgt* $g_1h_1 \equiv_r g_2h_2 \bmod N$.

Beweis.

- (i) ist zu (ii) äquivalent, da die Links- (bzw. Rechts-) nebenklassen, die zu den Äquivalenzrelationen $\equiv_l$ (bzw. $\equiv_r$) gehören, Äquivalenzklassen sind. Äquivalenzklassen zweier Äquivalenzrelationen stimmen genau dann überein, wenn die Äquivalenzrelationen übereinstimmen.

- (ii) $\Rightarrow$ (iii):
  Mit $gN = Ng$ gilt auch $gNg^{-1} = (Ng)g^{-1} = N \cdot e = N$.

- (iii) $\Rightarrow$ (iv):
  Dies ist trivial.

- (iv) $\Rightarrow$ (i):
  Es gilt

$$g \equiv_l h \bmod N \Rightarrow h^{-1}g \in N \underset{(iv)}{\Rightarrow} gh^{-1} = g(h^{-1}g)g^{-1} \Rightarrow gNg^{-1} \subset N \Rightarrow g \equiv_r h \bmod N.$$

- (ii) $\Rightarrow$ (v):
  Wegen $NN = N$ gilt $(gN)(hN) = g(Nh)N = g(hN)N = (gh)N$.

- (v) $\Rightarrow$ (iv):
  Insbesondere ist $(gN)(g^{-1}N) = gg^{-1}N = N$.
  Annahme: $gNg^{-1} \not\subset N$. Dann ist $(gNg^{-1})N \not\subset N$, weswegen $(gN)(g^{-1}N) \not\subset N$ folgt, ein Widerspruch.
  Damit folgt die Äquivalenz von (i) bis (iv) mit (v) und analog mit (vi).

- (vii) $\Rightarrow$ (iv):
  Es seien $g \in G$ und $n \in N$. Aus $n \equiv_l 1 \bmod N$ und $g^{-1} \equiv_l g^{-1} \bmod N$ folgt

$$ng^{-1} \equiv_l g^{-1} \bmod N \Rightarrow gng^{-1} \in N \Rightarrow gNg^{-1} \subset N,$$

  also (iv).

- (ii) $\Rightarrow$ (vii):
  Aus $g_1 \equiv_l g_2 \bmod N$ und $h_1 \equiv_l h_2 \bmod N$ folgt $g_1 \in g_2N$ und $h_1 \in h_2N$. Also ist auch $g_1h_1 \in g_2(Nh_2)N = (g_2h_2)N$.
  Damit folgt die Äquivalenz (i) bis (vi) mit (vii). Ebenso folgt die Äquivalenz von (i) bis (vi) mit (viii).

□

Satz 1.7.6. *Es sei G eine Gruppe und N ein Normalteiler von G. Dann bildet die Gruppe G/N der Nebenklassen von N in G eine Gruppe mit dem Komplexprodukt als Verknüpfung. Die Abbildung $\Phi\colon G \to G/N$, $g \to gN$ ist ein Epimorphismus von der Gruppe G auf die Gruppe G/N. Also ist G/N ein homomorphes Bild von G.*

Beweis. Die Verknüpfung ist wegen der Eigenschaft (v) aus Satz 1.7.5 abgeschlossen. Das Assoziativgesetz von G überträgt sich auf G/N. Das neutrale Element ist $1_{G/N} = 1 \cdot N = N \in G/N$. Das Inverse von gN ist $g^{-1}N$. □

Definition 1.7.6. Die Abbildung Φ in Satz 1.7.6 heißt auch der kanonische Epimorphismus von G auf G/N.

1.8 Homomorphismen und Faktorgruppen

Nach Satz 1.7.6 ist mit jedem Normalteiler N einer Gruppe G ein Homomorphismus $\Phi\colon G \to G/N$ verbunden.
Wir werden hier die Umkehrung zeigen: Zu jedem Homomorphismus von G gehört ein Normalteiler von G, der sogenannte Kern des Homomorphismus.

Definition 1.8.1. Es sei $\Phi\colon G \to H$ ein Homomorphismus einer Gruppe G in eine Gruppe H mit Einselement 1_H. Unter dem Kern von Φ versteht man die Menge $\mathrm{Kern}(\Phi) = \{g \in G\colon \Phi(g) = 1_H\}$.

Beispiel 1.8.1. Der Begriff des Kerns ist schon aus der Linearen Algebra bekannt. Ist Φ eine lineare Abbildung vom Vektorraum V in den Vektorraum W, so ist $\mathrm{Kern}(\Phi) = \{\vec{v} \in V \colon \Phi(\vec{v}) = \vec{0}_W\}$. Dies steht in Einklang mit Definition 1.8.1, wenn Φ als Homomorphismus der Gruppe $(V, +)$ in die Gruppe $(W, +)$ betrachtet wird.

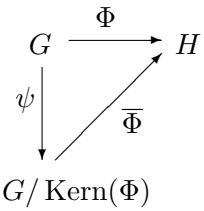
Satz 1.8.1. *(Homomorphiesatz)*
Es seien G und H Gruppen mit Einselementen 1_G und 1_H sowie $\Phi \colon G \to H$ ein Homomorphismus. Dann gilt

i) $\mathrm{Kern}(\Phi)$ *ist ein Normalteiler von G, $\Phi(G)$ ist eine Untergruppe von H, und es gilt $\Phi(1_G) = 1_H$.*

ii) Es gilt $G/\mathrm{Kern}(\Phi) \cong \Phi(G)$, und zwar wird ein solcher Isomorphismus $\overline{\Phi}$ durch

$$\overline{\Phi} = \begin{cases} G/\mathrm{Kern}(\Phi) \to \Phi(G) \\ g\,\mathrm{Kern}(\Phi) \to \Phi(g) \end{cases}$$

geliefert.
Ist ψ der kanonische Epimorphismus von G auf $G/\mathrm{Kern}(\Phi)$, so ist $\Phi = \overline{\Phi} \circ \psi$, d.h. das Diagramm



ist kommutativ.

iii) Der Homomorphismus Φ ist genau dann ein Monomorphismus, wenn $\mathrm{Kern}(\Phi) = \{1_G\}$ gilt.

Beweis. i) Für alle $g \in G$ gilt $\Phi(g) = \Phi(1_G \cdot g) = \Phi(1_G)\Phi(g)$. Daher ist $\Phi(1_G) = 1_H$.
Es seien $h_1, h_2 \in \Phi(G)$, etwa $h_1 = \Phi(g_1)$ und $h_2 = \Phi(g_2)$. Dann ist $h_1 h_2^{-1} = \Phi(g_1 g_2^{-1})$, also $h_1 h_2^{-1} \in \Phi(G)$, womit $\Phi(G)$ das Untergruppenkriterium (Satz 1.3.1) erfüllt.
Es sei $k \in \mathrm{Kern}(\Phi)$ und $g \in G$. Dann ist $\Phi(gkg^{-1}) = \Phi(g)\Phi(k)\Phi(g^{-1}) = \Phi(g) \cdot 1_H \cdot \Phi(g^{-1}) = 1_H$, also ist auch $gkg^{-1} \in \mathrm{Kern}(\Phi)$, d.h. $g\,\mathrm{Kern}(\Phi)g^{-1} \subseteq \mathrm{Kern}(\Phi)$. Nach Satz 1.7.5 (iv) ist dann $\mathrm{Kern}(\Phi)$ ein Normalteiler von G.

ii) Wir zeigen zunächst, dass die Abbildung $\overline{\Phi} \colon G/\mathrm{Kern}(\Phi) \to \Phi(G)$ wohldefiniert ist, d.h. nicht von dem Repräsentanten g der Nebenklasse $g\,\mathrm{Kern}(\Phi)$ abhängt:
Es impliziert $g_1\,\mathrm{Kern}(\Phi) = g_2\,\mathrm{Kern}(\Phi)$ für $g_1, g_2 \in G$ dann $g_1 = g_2 \cdot k$ für ein $k \in \mathrm{Kern}(\Phi)$, woraus $\Phi(g_1) = \Phi(g_2)\Phi(k) = \Phi(g_2)$ folgt.
Zur Relationstreue:

$$\begin{aligned} \overline{\Phi}(g_1\,\mathrm{Kern}(\Phi)g_2\,\mathrm{Kern}(\Phi)) &= \overline{\Phi}(g_1 g_2\,\mathrm{Kern}(\Phi)) = \Phi(g_1 g_2) = \Phi(g_1)\Phi(g_2) \\ &= \overline{\Phi}(g_1\,\mathrm{Kern}(\Phi))\overline{\Phi}(g_2\,\mathrm{Kern}(\Phi)). \end{aligned}$$

Zur Injektivität:

$$\begin{aligned} \overline{\Phi}(g_1\,\mathrm{Kern}(\Phi)) = \overline{\Phi}(g_2\,\mathrm{Kern}(\Phi)) &\Rightarrow \Phi(g_1) = \Phi(g_2) \Rightarrow 1_H = \Phi(g_1)\Phi(g_2)^{-1} = \Phi(g_1 g_2^{-1}) \\ &\Rightarrow g_1 g_2^{-1} \in \mathrm{Kern}(\Phi)) \Rightarrow g_1 \in g_2\,\mathrm{Kern}(\Phi) \\ &\Rightarrow g_1\,\mathrm{Kern}(\Phi) = g_2\,\mathrm{Kern}(\Phi) \end{aligned}$$

iii) Ist Φ injektiv, so folgt $\{1_G\} = \Phi^{-1}(\{1_H\}) = \operatorname{Kern}(\Phi)$.
Sei andererseits $\operatorname{Kern}(\Phi) = \{1_G\}$, dann gilt

$$\Phi(g_1) = \Phi(g_2) \Rightarrow g_1 \operatorname{Kern}(\Phi) = g_2 \operatorname{Kern}(\Phi) \Rightarrow g_1 = g_2$$

nach Teil (ii).

□

Beispiel 1.8.2. Es sei $G = (\mathbb{R}^3, +)$ und $\Phi\colon \mathbb{R}^3 \to \mathbb{R}^2$, $(x, y, z) \to (x, y)$.
Es ist dann Φ ein Epimorphismus mit $\operatorname{Kern}(\Phi) = \{(0, 0, z)\colon z \in \mathbb{R}\}$. Die Elemente der Faktorgruppe $G/\operatorname{Kern}(\Phi)$ sind die Nebenklassen $(x, y, 0) + \operatorname{Kern}(\Phi)$. Weiter ist $G/\operatorname{Kern}(\Phi)$ zum homomorphen Bild $\Phi(G) = \mathbb{R}^2$ isomorph.

Beispiel 1.8.3. Es sei $\eta = 2^{1/12}$ und $G = (\{\eta^n\colon n \in \mathbb{Z}\}, \cdot)$ sowie $H = (\mathbb{Z}/12\mathbb{Z}, +)$. Weiter sei $\Phi\colon G \to H$, $\eta^n \to n \bmod 12$. Dann ist

$$\operatorname{Kern}(\Phi) = \{\eta^n\colon \Phi(\eta^n) = 0 \bmod 12\} = \{\eta^n\colon n \equiv 0 \bmod 12\} =: \operatorname{Okt} = \{2^m\colon m \in \mathbb{Z}\}.$$

Nach dem Homomorphiesatz (Satz 1.8.1) ist $\Phi(G) = H \cong G/\operatorname{Okt}$.

Anwendungsbezug:
Es sei $C = 440$ und F die Abbildung $F\colon G \to \mathbb{R}$, $g \to Cg$. Dann enthält $F(G)$ die Frequenzen der Töne eines Klaviers (oder eines anderen Musikinstruments). Für die Bilder der Elemente der Faktorgruppe G/Okt unter der Abbildung F sind folgende Bezeichnungen üblich:

n	0	1	2	3	4	5	6	7	8	9	10	11
Bez. für $C(\eta^n \operatorname{Okt})$	a	ais	h	c	cis	d	dis	e	f	fis	g	gis

Kammerton a mit der Frequenz 440 Hz:

Homomorphismen der symmetrischen Gruppe S_n spielen in der Linearen Algebra in der Theorie der Determinanten eine wichtige Rolle. Wir erinnern an die folgenden Begriffe und Tatsachen der Linearen Algebra:

Definition 1.8.2. Es sei $\gamma \in S_n$.
Eine Inversion von γ ist eine zweielementige Teilmenge $\{a, b\} \subset \{1, \ldots, n\}$ mit $a < b$ und $\gamma(a) > \gamma(b)$. Bezeichnet $I(\gamma)$ die Anzahl der Inversionen von γ, so heißt γ gerade, falls $I(\gamma)$ gerade ist, ansonsten ungerade. Weiter heißt $\operatorname{sgn}(\gamma) = (-1)^{I(\gamma)}$ das Vorzeichen (oder Signum) von γ. Die Menge der geraden Permutationen von S_n heißt die alternierende Gruppe der Ordnung n und wird mit A_n bezeichnet.

Satz 1.8.2. *Jedes $\gamma \in S_n$ ist ein Produkt von Transpositionen. Ist γ gerade (bzw. ungerade), so ist in jeder Darstellung von γ als Produkt von Transpositionen die Anzahl der Faktoren gerade (bzw. ungerade). Sind $\sigma, \gamma \in S_n$ so ist* $\operatorname{sgn}(\sigma \circ \gamma) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\gamma)$.

Daraus ergibt sich

Satz 1.8.3. *Es sei $n \geq 2$. Die Abbildung*

$$\operatorname{sgn}\colon \begin{cases} S_n \to (\{-1,1\},\cdot) \\ \gamma \to \operatorname{sgn}(\gamma) \end{cases}$$

ist ein Epimorphismus mit $\operatorname{Kern}(\operatorname{sgn}) = A_n$.
Die Menge A_n bildet einen Normalteiler von S_n vom Index 2. Es ist $S_n/A_n \cong (\{-1,1\},\cdot) \cong (\mathbb{Z}/2\mathbb{Z},+)$ und $|A_n| = \frac{1}{2}n!$

Für $n \geq 5$ besitzen die Gruppen A_n die bemerkenswerte Eigenschaft der Einfachheit:

Definition 1.8.3. Eine Gruppe mit $|G| > 1$ heißt einfach, falls G nur die trivialen Normalteiler $\{1\}$ und G besitzt.

Satz 1.8.4. *Für $n \geq 5$ ist A_n einfach.*

Beweis. ohne Beweis. □

Satz 1.8.5. *Für $n \geq 5$ sind $\{id\}$, A_n und S_n die einzigen Normalteiler von A_n.*

Beweis. Es sei $N \trianglelefteq S_n$ und $N \notin \{A_n, S_n\}$. Es ist nun

$$N = \{id\} \tag{1}$$

zu zeigen. Es ist $N \cap A_n \trianglelefteq A_n$. Wegen der Einfachheit von A_n folgt

$$N \cap A_n = \{id\}. \tag{2}$$

Annahme: es existiert ein $\gamma \in N - \{id\}$.
Dann ist wegen (2) auch $\gamma \notin A_n$, also $\operatorname{sgn}(\gamma) = -1$ und $\operatorname{sgn}(\gamma^2) = 1$, also $\gamma^2 = id$. Damit muss in der Zyklendarstellung von γ jeder Zyklus die Länge 1 oder 2 haben. Alos gilt $\gamma = (a_1\ b_1) \circ \ldots \circ (a_s\ b_s)$ mit $a_j, b_j \in \{1,\ldots,n\}$ und einem ungeraden s. Wäre nun $\sigma \in N - \{id, \gamma\}$, so wäre $\sigma \circ \gamma \in A_n$, aber $\sigma \circ \gamma \neq id$, da $\gamma^{-1} = \gamma$ im Widerspruch zu (2) steht. Also gilt

$$N = \{id, \gamma\}. \tag{3}$$

Es sei weiter $\rho \in S_n$ mit $\rho(a_1) = a_1$ und $\rho(b_1) \notin \{a_1, b_1\}$. Dann ist

$$\rho\gamma\rho^{-1} = (\rho(a_1)\ \rho(b_1)) \circ \ldots \circ (\rho(a_j)\ \rho(b_j)) \neq \gamma$$

und $\rho\gamma\rho^{-1} \in N$ wegen $N \trianglelefteq S_n$ im Widerspruch zu (3).
Damit ist (1) gezeigt. □

Satz 1.8.6. *Es sei $n \geq 5$ und $\Phi\colon S_n \to H$ ein Epimorphismus von S_n auf H.*
Dann gilt einer der folgenden drei Fälle:

1. $H \cong S_n$
2. $H \cong (\{-1,1\},\cdot)$
3. $H \cong \{1\}$

Beweis. Nach dem Homomorphiesatz (Satz 1.8.1) ist $H \cong S_n/\operatorname{Kern}(\Phi)$.
Wegen $\operatorname{Kern}(\Phi) \trianglelefteq S_n$ ist nach Satz 1.8.5 nun also $H \cong S_n/\{id\} = S_n$ oder $H \cong S_n/A_n \cong (\{-1,1\},\cdot)$ oder $H \cong S_n/S_n = \{1\}$. □

Kapitel 2

Ringe

2.1 Ringe und Körper

Definition 2.1.1. Ein Ring ist ein Tripel $(R, +, \cdot)$, bestehend aus einer nichtleeren Menge R, einer als Addition bezeichneten Verknüpfung $+$ und einer als Multiplikation bezeichneten Verknüpfung $\cdot$, so dass folgende Ringaxiome erfüllt sind:
Es seien $a, b, c \in R$.

(R1) $(R, +)$ ist eine abelsche Gruppe.

(R2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativgesetz)

(R3) $a \cdot (b + c) = a \cdot b + a \cdot c$ (1. Distributivgesetz) und $(b + c) \cdot a = b \cdot a + c \cdot a$ (2. Distributivgesetz)

Dabei wird die Regel "Punkt vor Strich" angewandt.
Gilt zusätzlich das Kommutativgesetz der Multiplikation

(R4) $a \cdot b = b \cdot a$,

so spricht man von einem kommutativen Ring.

Das neutrale Element der Gruppe $(R, +)$ heißt Null des Rings R. Für $a \in R$ wird das Inverse bzgl. $+$ mit $-a$ bezeichnet und heißt auch das Negative von a. Der Ring R heißt Ring mit Eins, falls ein eindeutiges Element $1 \in R$ mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$ existiert.

Aus den Distributivgesetzen folgt sofort

Satz 2.1.1. *Es sei $(R, +, \cdot)$ ein Ring. Für alle $a, b, c \in R$ gilt*

i) $a \cdot 0 = 0 \cdot a = 0$

ii) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$

iii) $(-a) \cdot (-b) = a \cdot b$.

Beispiel 2.1.1. Es sei $R = \{0\}$. Setzt man $0 + 0 = 0$ und $0 \cdot 0 = 0$, so ist $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Es ist $1_R = 0_R$. Dieser Ring heißt Nullring. Aus Satz 2.1.1 folgt sofort, dass für jeden Ring $(R, +, \cdot)$ mit Eins, für den $1_R = 0_R$ gilt, auch $R = \{0\}$ folgt.

Definition 2.1.2. Es sei $(R, +, \cdot)$ ein Ring.

i) Ein Element $a \in R$ heißt linker bzw. rechter Nullteiler, wenn es $x \in R$ mit $x \neq 0$ und $a \cdot x = 0$ bzw. $x \cdot a = 0$ gibt.

ii) Der Ring R heißt nullteilerfrei, wenn R außer 0_R keine Nullteiler besitzt.

iii) Weiter heißt R Integritätsring, wenn R ein kommutativer Ring mit Eins und nullteilerfrei ist und zudem $1_R \neq 0_R$ gilt.

iv) Es sei R ein Ring mit Eins und $1_R \neq 0_R$. Dann heißt $a \in R$ eine Einheit, falls es ein $b \in R$ mit $a \cdot b = b \cdot a = 1_R$ gibt. Wie man leicht sieht, bildet die Menge aller Einheiten in R eine Gruppe, die Einheitengruppe von R, die mit R^* bezeichnet wird.

v) Schließlich heißt R Schiefkörper, wenn R ein Ring mit Eins ist, $1 \neq 0$ und $R^* = R \backslash \{0_R\}$ gilt. Ist R zusätzlich ein kommutativer Ring, so heißt R ein Körper.

Beispiel 2.1.2. $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsring. Die Einheitengruppe ist $\mathbb{Z}^* = \{-1, 1\}$.

Beispiel 2.1.3. Es sei R ein Ring, $n \in \mathbb{N}$ und $R^{(n,n)}$ die Menge der Matrizen vom Typ (n, n) mit Elementen in R. Dann ist auch $(R^{(n,n)}, +, \cdot)$ ein Ring. Ist R ein Ring mit Eins 1_R, so ist auch $(R^{(n,n)}, +, \cdot)$ ein Ring mit Eins. Die Eins ist dann die Einheitsmatrix

$$E_n = \begin{pmatrix} 1_R & 0_R & \dots & 0_R \\ 0_R & 1_R & \dots & 0_R \\ \vdots & \ddots & & \vdots \\ 0_R & \dots & & 1_R \end{pmatrix}.$$

Andere Eigenschaften von R wie beispielweise die Kommutativität oder die Nullteilerfreiheit übertragen sich im allgemeinen nicht auf $R^{(n,n)}$.

Im Rest dieses Kapitels betrachten wir nur noch Ringe mit Eins. Die Existenz des Einselements wird im folgenden stets vorausgesetzt, ohne dass es explizit verlangt wird.

2.2 Homomorphismen und Ideale

Definition 2.2.1. Es seien $(R, +, \cdot)$ und $(S, \boxplus, \boxdot)$ Ringe.

i) Eine Abbildung $\Phi \colon R \to S$ heißt (Ring-) homomorphismus, falls für alle $a, b \in R$

(a) $\Phi(a + b) = \Phi(a) \boxplus \Phi(b)$,

(b) $\Phi(a \cdot b) = \Phi(a) \boxdot \Phi(b)$,

(c) $\Phi(1_R) = 1_S$

gilt. Die Menge $\mathrm{Kern}(\Phi) = \{r \in R \colon \Phi(r) = 0_S\}$ wird der Kern von Φ genannt.
Ein bijektiver, injektiver bzw. surjektiver (Ring-)homomorphismus heißt (Ring-) isomorphismus, (Ring-) monomorphismus bzw. (Ring-) epimorphismus.

ii) Es sei $(R, +, \cdot)$ ein Ring. Eine nichtleere Teilmenge T von R heißt ein Teilring von R, falls $(T, +) \leq (R, +)$, $1_R \in T$ und $t_1 \cdot t_2 \in T$ für alle $t_1, t_2 \in T$ gilt. Dann heißt R Oberring von T (Bezeichnung: $T \leq R$).

iii) Eine Teilmenge $J \subseteq R$ heißt Ideal (bzw. zweiseitiges Ideal) von R, falls $(J,+) \leq (R,+)$ und $r \cdot a,\ a \cdot r \in J$ für alle $a \in J$ und $r \in R$ gilt. Schreibweise: $J \trianglelefteq R$.

iv) Es sei $M \subseteq R$. Das kleinste Ideal

$$\bigcap_{\substack{J \trianglelefteq R \\ M \subseteq J}} J$$

welches M enthält, heißt das von M erzeugte Ideal, und wird mit (M) bezeichnet.
Wir nennen J Hauptideal von R, falls $J = (\{m\})$ für ein $m \in R$ gilt. In diesem Fall schreiben wir auch $J = (m)$.

Bemerkung 2.2.1. Ist R kommutativ und $m \in R$, so hat das von m erzeugte Hauptideal offenbar die Form

$$(m) = \{mr \colon r \in R\} = mR = Rm.$$

Zwischen Ringhomomorphismen und den Idealen besteht ein Zusammenhang, der dem zwischen Gruppenhomomorphismen und den Normalteilern entspricht. Zunächst wird die Menge der Nebenklassen definiert, indem lediglich die Addition betrachtet wird.

Definition 2.2.2. Es sei $(R,+,\cdot)$ ein Ring und J ein Ideal von R. Unter einer Restklasse von J in R versteht man eine Nebenklasse der Untergruppe $(J,+)$ von $(R,+)$ im Sinne von Definition 1.7.4. Die Menge aller Restklassen wird mit R/J bezeichnet: $R/J = \{x + J \colon x \in R\}$.

Satz 2.2.1. *Es sei $(R,+,\cdot)$ ein Ring, $J \trianglelefteq R$ ein Ideal und $\Phi \colon (R,+) \to (R/J,+)$ der kanonische Epimorphismus (der Gruppen bzgl $+$). Dann gibt es genau eine Verknüpfung "$\cdot$" (für die wir dieselbe Bezeichnung verwenden, wie für die Multiplikation auf R) auf R/J, so dass $(R/J,+,\cdot)$ ein Ring und Φ ein Ringhomomorphismus ist, und zwar ist $\cdot$ durch*

$$(x + J) \cdot (y + J) = (x \cdot y) + J$$

für alle $x, y \in R$ definiert.

Beweis. Wir zeigen, dass das Produkt zweier Restklassen wohldefiniert ist. Es seien $x_1 + J = x_2 + J$ und $y_1 + J = y_2 + J$, und wir wollen zeigen, dass $(x_1 \cdot y_1) + J = (x_2 \cdot y_2) + J$ gilt. Es folgt dann $x_1 - x_2 \in J$ sowie $y_1 - y_2 \in J$, also $(x_1 - x_2) \cdot y_1 \in J$ und somit $(x_1 \cdot y_1) + J = (x_2 \cdot y_1) + J$. Aber ebenso folgt mittels $x_2 \cdot (y_1 - y_2) \in J$ dann $(x_2 \cdot y_1) + J = (x_2 \cdot y_2) + J$, also die Wohldefiniertheit.
Die Rechenregeln (Assoziativ- und Distributivgesetze) folgen aus den entsprechenden Regeln in R. Die Restklasse $1 + J$ ist neutrales Element der Multiplikation in R/J. Damit ist $(R/J,+,\cdot)$ ein Ring und Φ ein Ringhomomorphismus. Wegen $x \cdot y + J = \Phi(x \cdot y) = \Phi(x) \cdot \Phi(y) = (x + J) \cdot (y + J)$ ist $\cdot$ die einzige mögliche Multiplikation auf R/J mit den geforderten Eigenschaften. □

Definition 2.2.3. Der Ring $(R/J,+,\cdot)$ von Satz 2.2.1 heißt Restklassenring von R modulo J.

Wie im Homomorphiesatz der Gruppentheorie (Satz 1.8.1) betrachten wir nun die umgekehrte Situation. Es sei ein Ringhomomorphismus $\Phi \colon R \to S$ gegeben. Gesucht ist ein Restklassenring, der zu dem Bild $\Phi(R)$ isomorph ist.

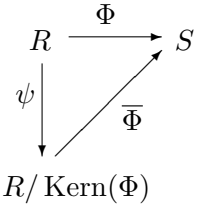
Satz 2.2.2. *(Homomorphiesatz für Ringe)*
Es seien R und S Ringe und $\Phi \colon R \to S$ ein Ringhomomorphismus.

i) Der Kern von Φ ist ein Ideal von R, und $\Phi(R)$ ist ein Teilring von S.

ii) Die Abbildung

$$\overline{\Phi} = \begin{cases} R/\operatorname{Kern}(\Phi) \to \Phi(R) \\ x + \operatorname{Kern}(\Phi) \to \Phi(x) \end{cases}$$

ist ein Ringisomorphismus, also $R/\operatorname{Kern}(\Phi) \cong \Phi(R)$*. Ist* ψ *der kanonische Epimorphismus von* R *auf* $R/\operatorname{Kern}(\Phi)$*, so ist* $\Phi = \overline{\Phi} \circ \psi$*, d.h. das Diagramm*



ist kommutativ.

iii) Die Abbildung Φ *ist genau dann ein Monomorphismus, wenn* $\operatorname{Kern}(\Phi) = \{0_R\}$ *ist.*

Beweis. Betrachtet man zunächst nur die Addition allein, so folgen die behaupteten Eigenschaften (beispielsweise $(\operatorname{Kern}(\Phi), +)$ Untergruppe von $(R, +)$) unmittelbar aus dem Homomorphiesatz für Gruppen. Man rechnet unmittelbar nach, dass auch die Eigenschaften, die die Multiplikation betreffen, erfüllt sind. □

Definition 2.2.4. Es sei R ein kommutativer Ring.

i) Ein Ideal $\mathfrak{p} \in R$ heißt Primideal, wenn $\mathfrak{p} \neq R$ ist und für alle $a, b \in R$ mit $a \cdot b \in \mathfrak{p}$ stets $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ gilt.

ii) Ein Ideal $\mathfrak{m} \lhd R$ heißt maximales Ideal, wenn $\mathfrak{m} \neq R$ ist und für jedes Ideal J von R mit $m \subseteq J \neq R$ stets $\mathfrak{m} = J$ gilt.

Satz 2.2.3. *Es sei* R *ein kommutativer Ring.*

i) Ein Ideal $\mathfrak{p}$ *von* R *ist genau dann ein Primideal, wenn* $R/\mathfrak{p}$ *ein Integritätsring ist.*

ii) Ein Ideal $\mathfrak{m}$ *von* R *ist genau dann ein maximales Ideal, wenn* $R/\mathfrak{m}$ *ein Körper ist.*

iii) Jedes maximale Ideal ist auch ein Primideal.

Beweis. i) "⇒":
Es sei $\mathfrak{p}$ ein Primideal. Nun ist zu zeigen, dass $R/\mathfrak{p}$ nullteilerfrei ist. Es seien $a, b \in R$ mit $(a + \mathfrak{p})(b + \mathfrak{p}) = 0_R + \mathfrak{p}$. Dann ist auch $(a \cdot b) + \mathfrak{p} = 0_R + \mathfrak{p}$, also $a \cdot b \in \mathfrak{p}$. Da $\mathfrak{p}$ prim ist folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, d.h. $a + \mathfrak{p} = 0_R + \mathfrak{p}$ oder $b + \mathfrak{p} = 0_R + \mathfrak{p}$.
"⇐":
Sei $R/\mathfrak{p}$ ein Integritätsring. Wegen $R/\mathfrak{p} \neq \{0 + \mathfrak{p}\}$ ist $\mathfrak{p} \neq R$. Sind nun $a, b \in R$ mit $a \cdot b \in \mathfrak{p}$ gegeben und gilt $0_R + \mathfrak{p} = (a \cdot b) + \mathfrak{p} = (a + \mathfrak{p}) \cdot (b + \mathfrak{p})$, dann ist $a + \mathfrak{p} = 0_R + \mathfrak{p}$ oder $b + \mathfrak{p} = 0_R + \mathfrak{p}$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

ii) "⇒":
Es sei $\mathfrak{m} \trianglelefteq R$ ein maximales Ideal. Dann ist

$$a + \mathfrak{m} \in R/\mathfrak{m} - \{0_R + \mathfrak{m}\} \Leftrightarrow a \notin \mathfrak{m}.$$

Zu zeigen ist also, dass $a + \mathfrak{m}$ in diesem Fall ein multiplikatives Inverses besitzt. Wir betrachten das Ideal $J = (\{a\}, \mathfrak{m}) = aR + \mathfrak{m}$. Es ist $J \neq \mathfrak{m}$, da $a = 1_R \cdot a \in J$ aber $a \notin \mathfrak{m}$ gilt. Wegen der

Maximalität von $\mathfrak{m}$ folgt $J = R$, insbesondere ist $1_R \in J$, d.h. es gibt $r \in R$ mit $a \cdot r + \mathfrak{m} = 1_R + \mathfrak{m}$, woraus $a \cdot r + \mathfrak{m} = 1_R + \mathfrak{m} = (a + \mathfrak{m}) \cdot (b + \mathfrak{m})$ folgt.
"$\Leftarrow$":
Es sei $R/\mathfrak{m}$ ein Körper und $J \trianglelefteq R$ mit $\mathfrak{m} \subseteq J \subseteq R$ und $J \neq \mathfrak{m}$. Zu zeigen ist dann $J = R$. Es gibt $a \in J - \mathfrak{m}$, also $a + \mathfrak{m} \neq 0 + \mathfrak{m}$. Das multiplikative Inverse von $a + \mathfrak{m}$ sei $r + \mathfrak{m}$ mit $r \in R$, d.h. $(a + \mathfrak{m}) \cdot (r + \mathfrak{m}) = (a \cdot r) + \mathfrak{m} = 1_R + \mathfrak{m}$. Wegen $a \cdot r \in J$ ist $1_R \in J$, woraus $J = R$ folgt.

iii) Dies folgt direkt aus der Tatsache, dass jeder Körper ein Integritätsring ist.

□

Satz 2.2.4. *Für $p \in \mathbb{Z}$ mit $p \geq 1$ sind folgende Aussagen äquivalent:*

i) Es ist p eine Primzahl.

ii) $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist ein Integritätsring.

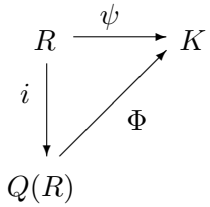
iii) $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist ein Körper.

Beweis. Die Kette $(iii) \Rightarrow (ii) \Rightarrow (i)$ ist klar.
Es bleibt noch $(i) \Rightarrow (iii)$ zu zeigen, d.h. nach Satz 2.2.3 (ii), dass $p\mathbb{Z}$ ein maximales Ideal von $\mathbb{Z}$ ist. Es sei $J \trianglelefteq \mathbb{Z}$ ein Ideal mit $p\mathbb{Z} \subseteq J \subseteq \mathbb{Z}$ und $J \neq \mathbb{Z}$. Da $(J, +)$ eine Untergruppe von $(\mathbb{Z}, +)$ ist, folgt nun $J = a\mathbb{Z}$ für ein $a \in \mathbb{Z}$, da jede Untergruppe einer zyklischen Gruppe zyklisch ist. Also gilt $p = ab$ mit $a, b \in \mathbb{Z}$. Da $a \neq \pm 1$ und p eine Primzahl ist, folgt $a = \pm p$, also $J = p\mathbb{Z}$. □

2.3 Quotientenkörper

In diesem Abschnitt sei R stets ein Integritätsring. So wie der Integritätsring $(\mathbb{Z}, +, \cdot)$ ein Teilring des Körpers $(\mathbb{Q}, +, \cdot)$ der rationalen Zahlen ist, der aus den Quotienten ganzer Zahlen besteht, so kann jeder Integritätsring in einen Quotientenkörper eingebettet werden.

Definition 2.3.1. Es sei R ein Integritätsring. Ein Paar $(Q(R), i)$, bestehend aus einem Körper $Q(R)$ und einem injektiven Ringhomomorphismus $i\colon R \to Q(R)$ heißt Quotientenkörper von R, wenn für jeden Körper K und jeden injektiven Ringhomomorphismus $\psi\colon R \to K$ genau ein Ringhomomorphismus $\Phi\colon Q(R) \to K$ mit $\psi = \Phi \circ i$ existiert, d.h. das Diagramm



ist kommutativ.

Da $Q(R)$ ein Körper ist, ist Φ injektiv. Aufgrund der Eindeutigkeitsaussage für Φ ist klar, dass das Paar $(Q(R), i)$ bis auf Isomorphie eindeutig bestimmt ist. Im Fall $R = \mathbb{Z}$ ist $Q(\mathbb{Z}) = \mathbb{Q}$ der Körper der rationalen Zahlen.

Satz 2.3.1. *Es sei R ein Integritätsring.*

i) Auf $M = \{(a, b)\colon a \in R, b \in R \backslash \{0_R\}\}$ erklärt man die Äquivalenzrelation

$$(a, b) \sim (a', b') \Leftrightarrow a \cdot b' = a' \cdot b.$$

ii) Bezeichnet man mit $\frac{a}{b}$ die Äquivalenzklasse von (a,b) unter $\sim$, so ist

$$Q(R) = \left\{ \frac{a}{b} \colon a \in R, b \in R \backslash \{0_R\} \right\}$$

eine Menge, wobei die Identität $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow a \cdot b' = a' \cdot b$ erklärt ist.
Auf $Q(R)$ erklärt man die Verknüpfungen

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} := \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \quad \textit{und} \quad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} := \frac{a_1 a_2}{b_1 b_2}.$$

Damit ist $(Q(R), +, \cdot)$ ein Körper.

iii) Die Abbildung $i \colon R \to Q(R)$, $r \to \frac{r}{1}$ ist ein injektiver Ringhomomorphismus.

iv) Es ist $(Q(R), +, \cdot)$ der Quotientenkörper von R.

Beweis. i) Symmetrie und Reflexivität der Relation $\sim$ sind klar.
Zur Transitivität: Es seien $(a_1, b_1) \sim (a_2, b_2)$ und $(a_2, b_2) \sim (a_3, b_3)$. Daraus folgt $a_1 \cdot b_2 = a_2 \cdot b_1$ und $a_2 \cdot b_3 = a_3 \cdot b_2$, also $a_1 b_2 b_3 = a_2 b_1 b_3 = b_1 a_3 b_2$ und damit $b_2(a_1 b_3) = b_2(a_3 b_1)$. Wegen der Nullteilerfreiheit von R kann der gemeinsame Faktor b_2 "gekürzt" werden, und wir erhalten $(a_1, b_1) \sim (a_3, b_3)$.

ii) Wir zeigen, dass die Addition wohldefiniert ist: Es seien

$$\frac{a_1}{b_1} = \frac{\alpha_1}{\beta_1} \quad \text{und} \quad \frac{a_2}{b_2} = \frac{\alpha_2}{\beta_2},$$

b1 also $a_1 \beta_1 = \alpha_1 b_1$ und $a_2 \beta_2 = \alpha_2 b_2$. Dann folgt

$$(a_1 b_2 + a_2 b_1)\beta_1 \beta_2 = a_1 \beta_1 b_2 \beta_2 + a_2 \beta_2 b_1 \beta_1 = \alpha_1 b_1 b_2 \beta_2 + a_2 b_2 b_1 \beta_1 = (\alpha_1 \beta_2 + \alpha_2 \beta_1) b_1 b_2.$$

Es ist unmittelbar einsichtig, dass die Multiplikation wohldefiniert ist. Man rechnet außerdem leicht nach, dass $(Q(R), +, \cdot)$ ein Körper mit dem Nullelement $\frac{0}{1}$, dem Negativen $\frac{-a}{b}$ zu $\frac{a}{b}$, dem Einselement $\frac{1}{1}$ und dem Inversen $\frac{b}{a}$ zu $\frac{a}{b}$ ist.

iii) Die Abbildung i ist injektiv, denn aus $i(r) = \frac{r}{1} = \frac{0}{1}$ folgt $r \cdot 1_R = 1_R \cdot 0_R = 0_R$, also $r = 0_R$. Damit ist $\text{Kern}(i) = \{0_R\}$.

iv) Ist $\psi \colon R \to K$ ein injektiver Ringhomomorphismus, so ist $\psi(R - \{0_R\}) \subseteq K$. Also ist

$$\Phi \colon Q(R) \to K \quad \text{mit} \quad \Phi\left(\frac{a}{b}\right) := \psi(a)\psi(b)^{-1}$$

wohldefiniert und offenbar ein Ringhomomorphismus.

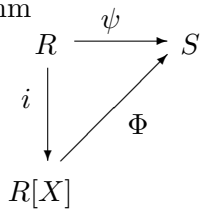
□

2.4 Polynomringe

Im folgenden sei R stets ein kommutativer Ring und $\psi \colon R \to S$ ein Ringhomomorphismus.

Definition 2.4.1. Ein Tripel $(R[X], X, i)$, bestehend aus einem kommutativen Ring $R[X]$, einem ausgezeichneten Element X und einem Ringhomomorphismus $i \colon R \to R[X]$, heißt ein Polynomring über R, wenn es für jeden Ringhomomorphismus $\psi \colon R \to S$ mit einem kommutativen Ring S und für jedes $x \in S$ genau einen Ringhomomorphismus $\Phi \colon R[X] \to S$ mit $\psi = \Phi \circ i$ und $\Phi(X) = x$ gibt.

Man hat ein kommutatives Diagramm



Satz 2.4.1. *Für jeden kommutativen Ring R gilt:*

i) Es gibt (bis auf Isomorphie) genau einen Polynomring $(R[X], X, i)$ in einer Unbestimmten X über R.

ii) Die Abbildung i ist injektiv. Man kann R mit $i(R)$ identifizieren und somit als Unterring von $R[X]$ auffassen. Für jedes $f \in R[X]$ mit $f \neq 0_{R[X]}$ gibt es eindeutig bestimmte $a_0, \ldots, a_n \in R$ mit $a_n \neq 0$, so dass

$$f = a_n \cdot X^n + a_{n-1} \cdot X^{n-1} + \ldots + a_1 \cdot X^1 + a_0$$

gilt. Die Zahl $n \in \mathbb{N}$ heißt Grad von f (Schreibweise: $\deg(f)$).
Für $f = 0_{R[X]}$ schreiben wir $\deg(f) = -\infty$.

Beweis. Setze

$$R[X] := \left\{ \sum_{i=0}^{\infty} a_i \cdot X^i \colon a_i \in R,\ \exists \text{ nur endlich viele } i \text{ mit } a_i \neq 0_R \right\},$$

wobei $\sum a_i X^i$ nur ein endlicher formaler Ausdruck mit Koeffizienten $a_i \in R$ ist. Formaler Ausdruck bedeutet, dass

$$\sum_{i=0}^{\infty} a_i X^i = \sum_{i=0}^{\infty} b_i X^i \Leftrightarrow \forall i \in \mathbb{N}_0 \colon a_i = b_i$$

gilt. In $R[X]$ erklärt man die Verknüpfungen

$$\begin{aligned} \left(\sum_{i=0}^{\infty} a_i X^i \right) + \left(\sum_{i=0}^{\infty} b_i X^i \right) &:= \sum_{i=0}^{\infty} (a_i + b_i) X^i \\ \left(\sum_{i=0}^{\infty} a_i X^i \right) \cdot \left(\sum_{i=0}^{\infty} b_i X^i \right) &:= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) X^k. \end{aligned}$$

Dadurch wird $1_{R[X]} = 1_R \cdot X^0$. Man definiert $i \colon R \to R[X]$, $r \to r \cdot X^0$. So ist i offenbar ein injektiver Ringhomomorphismus. Zum Nachweis der universellen Eigenschaft gebe man sich (ψ, x) vor, wobei $\psi \colon R \to S$ ein Ringhomomorphismus und $x \in S$ beliebig ist. Dann definiert man

$$\Phi \colon R[X] \to S \text{ mit } \Phi \left(\sum_{i=0}^{\infty} a_i X^i \right) := \sum_{i=0}^{\infty} \psi(a_i) x^i.$$

Durch Nachrechnen bestätigt man, dass Φ ein Ringhomomorphismus ist. Die Eindeutigkeit ist klar. □

Wir erweitern Definition 2.4.1 auf den Fall mehrerer Unbestimmter:

Definition 2.4.2. Es sei R ein kommutativer Ring und $n \in \mathbb{N}$. Unter einem Polynomring über R in n unabhängigen Unbestimmten $X_1, \ldots, X_n$ verstehen wir eine Folge der Länge n von Tripeln

$$\tau_k := (R[X_1, \ldots, X_{k-1}][X_k], X_k, i_k)$$

mit $1 \leq k \leq n$. Dabei soll τ_k ein Polynomring über $R[X_1, \ldots, X_{k-1}]$ in der Unbestimmten X_k im Sinne von Definition 2.4.1 sein.

Durch vollständige Induktion beweist man folgende Verallgemeinerung von Satz 2.4.1:

Satz 2.4.2. *Es gibt (bis auf Isomorphie) genau einen Polynomring über R in n unabhängigen Unbestimmten $X_1, \ldots, X_n$.*

Definition 2.4.3. Es sei R ein kommutativer Ring.

i) Es sei $R \leq S$ und $x_1, \ldots, x_n \in S$. Unter $R[x_1, \ldots, x_n]$ versteht man den kleinsten Teilring von S, der die Menge $R \cup \{x_1, \ldots, x_n\}$ enthält:

$$R[x_1, \ldots, x_n] = \bigcap_{\substack{T \leq S \\ R \cup \{x_1, \ldots, x_n\} \subseteq T}} T.$$

ii) Es sei $(R[X], X, i)$ der Polynomring über R in der Unbestimmten X. Das Element x heißt Unbestimmte über R, falls x Element eines kommutativen Oberrings S von R ist und der nach Satz 2.4.1 existierende Homomorphismus $\Phi\colon R[X] \to S$ mit $\Phi(X) = x$ ein Monomorphismus ist.

iii) Die $x_1, \ldots, x_n$ heißen unabhängige Unbestimmte über R, falls $x_1, \ldots, x_n$ Elemente eines kommutativen Oberrings S von R sind, x_1 Unbestimmte über R ist und für alle $2 \leq k \leq n$ gilt, dass x_k Unbestimmte über $R[x_1, \ldots, x_{k-1}]$ ist.

Aus Satz 2.4.1 ergibt sich die Gültigkeit von

Satz 2.4.3. *Es sei S ein kommutativer Oberring von R und $x, x_1, \ldots, x_n \in S$. Weiter sei $(R[X], X, i)$ der Polynomring über R in der Unbestimmten X und $((R[X_1, \ldots, X_{k-1}][X_k], X_k, i_k))_{1 \leq k \leq n}$ der Polynomring über R in n unabhängigen Unbestimmten $X_1, \ldots, X_n$.*

i) Folgende Aussagen sind äquivalent:

   (a) Es ist x eine Unbestimmte über R.
   (b) $R[X] \cong R[x]$.

ii) Aus $\sum a_i x^i = 0$ mit $a_0, \ldots, a_n \in R$ und $a_j = 0$ für $j > m$ für ein $m \in \mathbb{N}_0$ folgt $a_j = 0$ für alle $j \in \mathbb{N}_0$.

iii) Folgende Aussagen sind äquivalent:

   (a) Es sind $x_1, \ldots, x_n$ unabhängige Unbestimmte über R.
   (b) $R[X_1, \ldots, X_n] \cong R[x_1, \ldots, x_n]$
   (c) Aus

$$\sum_{(i_1, \ldots, i_n) \in I} a_{i_1, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} = 0$$

   mit $a_{i_1, \ldots, i_n} \in R$ und I eine endliche Menge von n- Tupeln folgt $a_{j_1, \ldots, j_n} = 0$ für alle $j_1, \ldots, j_n \in \mathbb{N}_0$.

Für einen gegebenen kommutativen Ring R bedeute künftig $R[X]$ bzw. $R[X_1, \ldots, X_n]$ stets den Polynomring über R in der Unbestimmten X bzw. in den n unabhängigen Unbestimmten $X_1, \ldots, X_n$.

Definition 2.4.4. Es sei R ein Teilring von S. Ein Element $\alpha \in S$ heißt Nullstelle des Polynoms

$$f = \sum_{j=0}^{n} r_i X^i \in R[X],$$

wenn

$$f(\alpha) = \sum_{j=0}^{n} t_i \alpha^i = 0_S$$

ist.

Satz 2.4.4. *Es sei R ein Integritätsring. Dann besitzt jedes Polynom $f \in R[X]$ mit $f \neq 0$ höchstens* $\deg(f)$ *Nullstellen in R.*

Beweis. Wir zeigen dies mittels vollständiger Induktion nach $n := \deg(f)$.
Ist $n = 0$, so ist $f \in R$ und wegen $f \neq 0$ ist f das konstante Polynom, welches keine Nullstelle besitzt.
Es sei nun $n \geq 1$. Hat f keine Nullstelle, so gilt die Behauptung. Ansonsten gibt es $\alpha \in R$ mit $f(\alpha) = 0$. Durch "lange Division" erhält man ein $q \in R[X]$ mit $\deg(q) = n-1$, so dass $f = q \cdot (X-\alpha)+r$ mit $r \in R$ ist. Aus $f(\alpha) = 0$ folgt aber $r = 0$. Weil R ein Integritätsring ist, ist $\beta \in R$ genau dann Nullstelle von f, wenn β Nullstelle von q oder $\beta = \alpha$ ist. Nach Induktionsvoraussetzung hat q aber höchstens $n-1$ Nullstellen, also hat f höchstens n Nullstellen. □

2.5 Teilbarkeitstheorie

In diesem Abschnitt sei R stets ein Integritätsring.

Definition 2.5.1. Es seien $a, b, a' \in R$. Es heißt a ein Teiler von b (oder a teilt b), wenn es ein $r \in R$ mit $b = r \cdot a$ gibt (Schreibweise: $a|b$). Ist a kein Teiler von b, so schreibt man $a \not| b$. Die Elemente a und a' heißen assoziiert, wenn es eine Einheit $u \in R^*$ mit $a' = ua$ gibt (Schreibweise: $a \sim a'$).

Folgende Teilbarkeitsregeln sind unmittelbar klar:

Satz 2.5.1. *Es sei R ein Integritätsring und $a, b, c, a', b_j \in R$. Dann gilt*

i) $a|b \Leftrightarrow (b) = bR \subseteq (a) = aR$

ii) $a \sim a' \Leftrightarrow (a) = (a')$

iii) $a|b$ *und* $b|c \Rightarrow a|c$

iv) $a|b_1, \ldots, a|b_n \Rightarrow a \big| \sum_{j=1}^{n} b_j r_j$ *für alle* $r_j \in R$

v) $a|1_R \Leftrightarrow a \in R^*$

vi) $a|a'$ *und* $a'|a \Leftrightarrow a \sim a'$.

Definition 2.5.2. Es sei R ein Integritätsring.

i) Ein Element $0 \neq a \in R - R^*$ heißt irreduzibel oder unzerlegbar, falls jede Faktorisierung von a in R trivial ist, d.h. falls $a = a_1 a_2$ für $a_1, a_2 \in R$ gilt, so ist $a_1 \in R^*$ oder $a_2 \in R^*$.

ii) Ein Element $a \in R - R^*$ heißt prim oder Primelement, falls $a|b_1 b_2$ impliziert, dass $a|b_1$ oder $a|b_2$ für alle $b_1, b_2 \in R$ gilt.

Bemerkung 2.5.1. Offenbar ist a genau dann prim, wenn $(a) = aR$ Primideal ist.

Satz 2.5.2. *Ist a prim, so ist a auch unzerlegbar.*

Beweis. Es sei a zerlegbar, d.h. $a = a_1 a_2$ mit $a_1, a_2 \in R - R^*$. Wir nehmen an, es gelte $a|a_1$. Dann ist $a_1 = f \cdot a = f \cdot a_1 \cdot a_2$ mit $f \in R$. Daraus folgt aber der Widerspruch $f \cdot a_2 = 1$ bzw. $a_2 \in R^*$. Also gilt $a \nmid a_1$. Ebenso folgt $a \nmid a_2$. Damit ist $a|a_1 a_2$ aber $a \nmid a_1$ und $a \nmid a_2$, also ist a nicht prim. □

Bemerkung 2.5.2. Die Umkehrung gilt im allgemeinen nicht.

Beispiel 2.5.1. Es sei $R = \mathbb{Z}[\sqrt{-5}]$ und $a, b, c, d \in \mathbb{Z}$. Es sei

$$3 = (a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) \Rightarrow 3 = (a - b\sqrt{-5}) \cdot (c - d\sqrt{-5}) \Rightarrow 9 = (a^2 + 5b^2) \cdot (c^2 + 5d^2),$$

also $b = 0$ oder $d = 0$ sowie $(a+b\sqrt{-5})|1$ oder $(c+d\sqrt{-5})|1$. Nun ist aber $3 \cdot 2 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$, weswegen $3|(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ aber $3 \nmid (1 + \sqrt{-5})$ und $3 \nmid (1 - \sqrt{-5})$ gilt.
Damit ist 3 in $\mathbb{Z}[\sqrt{-5}]$ unzerlegbar, aber nicht prim.

Definition 2.5.3. Ein Ring R heißt faktoriell oder ein Ring mit eindeutiger Faktorisierung (oder auch Gaußscher Bereich), falls jede Nichteinheit eine im wesentlichen eindeutige Faktorisierung in unzerlegbare Elemente besitzt.

Das bedeutet: Falls $a = a_1 \cdots a_n = b_1 \cdots b_m$ Faktorisierungen von a in unzerlegbare Elemente von R sind, so folgt $m = n$, und nach Umnummerierung der b_j ist $a_j \sim b_j$ für $j = 1, \ldots, n$.

Satz 2.5.3. *Ein Ring R ist faktoriell, falls*

i) es keine unendlichen Teilerketten $a_1, a_2, \ldots$ mit $a_{j+1}|a_j$ und $a_j \not\sim a_{j+1}$ für alle $j \in \mathbb{N}$ in R gibt,

ii) und jedes irreduzible Element in R prim ist.

Die Umkehrung gilt trivialerweise.

Beweis. Es gelte (i). Wir zeigen zunächst, dass für jedes $a \in R - R^*$ eine Zerlegung in irreduzible Elemente existiert. Dazu konstruieren wir eine endliche Folge $b_0, \ldots, b_k$ von Teilern von a, so dass b_k irreduzibel ist. Sei $b_0 := a$ gesetzt. Falls b_0 unzerlegbar ist setzen wir $k = 0$ und sind fertig. Ansonsten existiert ein $b_1 \in R - R^*$ mit $b_1|a$ und $b_1 \not\sim a$. Sind $b_0, \ldots, b_{i-1}$ schon konstruiert, und ist keines davon irreduzibel, so existiert $b_i \in R - R^*$ mit $b_i|b_{i-1}$ und $b_i \not\sim b_{i-1}$. Wegen (i) erhalten wir auf diese Weise in endlich vielen Schritten ein irreduzibles $b_k|a$. Wir konstruieren als nächstes die Folge (a_j). Dazu setzen wir $a_1 = b_k$, und es gilt $a = a_1 \tilde{a_1}$. Wir konstruieren in der selben Weise wie oben für $\tilde{a_1}$ ein irreduzibles a_2 mit $a_2|\tilde{a_1}$ und setzen $a = a_1 a_2 \tilde{a_2}$. Nach n Schritten ist $a = a_1 \cdots a_n \cdot \tilde{a_n}$, wobei alle a_i irreduzibel sind. Falls $\tilde{a_n}$ für alle n zerlegbar wäre, so wäre wieder die Folge $(\tilde{a_i})$ eine unendliche Teilerkette im Widerspruch zu (i). Damit ist die Existenz der Faktorisierung gezeigt.
Zur Eindeutigkeit: Es seien $a_1 \cdots a_n = b_1 \cdots b_m$ und alle $a_i, b_j \in R$ unzerlegbar. Wir führen den Beweis durch Induktion über das Minimum von m und n. Es teilt a_1 das Produkt $b_1 \cdots b_m$, und da a_1 nach (ii) prim ist, teilt a_1 eines der b_j. Ohne Einschränkung sei $j = 1$. Also gilt: a_1 teilt b_1 und b_1 ist unzerlegbar. Das heißt $a_1 \sim b_1$, und man kann ohne Einschränkung $a_1 = b_1$ annehmen. Es folgt $a_2 \cdots a_n = b_2 \cdots b_m$. Nach Induktionshypothese ist $m = n$ und (nach Umnummerierung) $a_i \sim b_i$. □

Definition 2.5.4. Es sei R ein Integritätsring und $a, b \in R$ mit $a \neq 0$ oder $b \neq 0$. Dann heißt $c \in R$ der größte gemeinsame Teiler von a und b (Schreibweise: $c = ggT(a, b)$), falls

i) $c|a$ und $c|b$,

ii) $d|a$ und $d|b$ impliziert $d|c$.

Weiter heißt $x \in R$ der kleinste gemeinsame Vielfache von a und b (Schreibweise: $x = kgV(a, b)$), falls

i) $a|x$ und $b|x$,

ii) $a|y$ und $b|y$ impliziert $x|y$.

Ist R faktoriell, so existieren ggT und kgV, und sind bis auf Einheiten eindeutig bestimmt.

Definition 2.5.5. Es sei R ein Integritätsring.

i) Dann heißt R Hauptidealring, falls jedes Ideal von R ein Hauptideal ist.

ii) Ein Euklidischer Ring ist ein Paar (R, δ), bestehend aus einem Integritätsring R und einer Abbildung $\delta\colon R - \{0_R\} \to \mathbb{N}_0$, so dass für alle $a, b \in R - \{0_R\}$ es $q, r \in R$ mit $a = qb + r$ und $\delta(r) < \delta(b)$ oder $r = 0$ gibt. Die Abbildung δ heißt Höhenfunktion von R.

Beispiel 2.5.2. Folgende Ringe sind Euklidisch:

i) $(\mathbb{Z}, \delta)$ mit $\delta(a) = |a|$.

ii) Der Polynomring $K[X]$ in einer Unbestimmten für einen Körper K mit $\delta(f) = \deg(f)$.
Die Polynome q und r in der vorhergehenden Definition können durch die wohlbekannte "lange Division" gefunden werden.

Satz 2.5.4. *Es gilt:*

i) Ein Euklidischer Ring ist immer ein Hauptidealring.

ii) Ein Hauptidealring ist immer faktoriell.

iii) In einem Hauptidealring ist jedes von $\{0\}$ verschiedene Primideal auch maximal.

Beweis. i) Es sei (R, δ) ein Euklidischer Ring und J ein Ideal von R. Wähle $a \in J - \{0_R\}$, so dass $\delta(a)$ minimal ist. Zu $b \in J$ gibt es $q \in R$, so dass $b = aq + r$ mit $\delta(r) < \delta(a)$ oder $r = 0_R$ ist. Da $r \in J$ ist und $\delta(a)$ minimal gewählt war, folgt $r = 0_R$. Also ist $b = aq \in aR$. Da $b \in J$ beliebig war, folgt $J = (a) = aR$.

ii) Nach Satz 2.5.3 genügt zu zeigen:

- Es existieren keine unendlichen Teilerketten.
- Jedes irreduzible Element ist prim.

Zum ersten Punkt: Angenommen es gäbe $a_1, a_2, \ldots$ mit $a_{i+1}|a_i$ und $a_i \not\sim a_{i+1}$ in R. Dann gilt $a_1R \subsetneqq a_2R \subsetneqq \ldots$. Wir setzen

$$J := \bigcup_{j=1}^{\infty} a_jR,$$

womit auch $J \trianglelefteq R$ ein Ideal ist. Da R ein Hauptidealring ist, gibt es $a \in R$ mit $J = aR$. Dann gibt es auch ein i mit $a \in a_iR$, woraus $a_iR = a_{i+1}R = \ldots$ im Widerspruch zur Annahme folgt.
Zum zweiten Punkt: Es sei $a \in R - R^*$ irreduzibel. Es genügt zu zeigen, dass $aR \trianglelefteq R$ prim ist. Wir zeigen aber die stärkere Eigenschaft, dass aR maximal ist, womit auch (iii) folgt. Es sei daher $aR \subseteq J \subsetneqq R$. Es folgt $J = dR$ für ein $d \in R - R^*$, und damit $a \in dR$, also $a = dd'$ mit $d' \in R$. Das bedeutet $d' \in R^*$, da a irreduzibel ist. Also gilt $a \sim d$ und damit $J = aR$.

iii) siehe (ii).

□

Satz 2.5.5. *(Euklidischer Algorithmus)*
Es sei (R, δ) ein Euklidischer Ring und $r_1, r_2 \in R$ mit $r_2 \neq 0_R$. Wir konstruiere $q_i, r_i \in R$, so dass

$$\begin{cases} r_1 = q_1r_2 + r_3 \quad mit \quad \delta(r_3) < \delta(r_2) \\ r_2 = q_2r_3 + r_4 \quad mit \quad \delta(r_4) < \delta(r_3) \\ \vdots \\ r_{n-1} = q_{n-1}r_n + r_{n+1} \quad mit \quad \delta(r_{n+1}) < \delta(r_n) \\ r_n = q_nr_{n+1} + r_{n+2} \quad mit \quad r_{n+2} = 0_R \end{cases} \tag{$*$}$$

gilt. Das so erhaltene Element r_{n+1} ist der größte gemeinsame Teiler von r_1 und r_2, und indem man $(*)$ rückwärts durchläuft, erhält man $a, b \in R$ mit $r_{n+1} = ar_1 + br_2$.

Beweis. Aus der letzten Gleichung von $(*)$ erhält man $r_{n+1}|r_n$, aus der vorletzten $r_{n+1}|r_{n-1}$, usw. Schließlich folgt aus der zweiten Gleichung $r_{n+1}|r_2$ und aus der ersten $r_{n+1}|r_1$. Das heißt, dass r_{n+1} ein gemeinsamer Teiler von r_1 und r_2 ist. Es sei nun t ein beliebiger Teiler von r_1 und r_2. Dann folgt aus der ersten Gleichung $t|r_3$, usw. bis aus der letzten Gleichung $t|r_{n+1}$ folgt. Also ist r_{n+1} der größte gemeinsame Teiler.
Zur Konstruktion von a und b:
Aus der vorletzten Gleichung ergibt sich r_{n+1} als Linearkombination von r_{n-1} und r_n mit Koeffizienten aus R, also $r_{n+1} = r_{n-1} - q_{n-1}r_n$. Ersetzt man mit Hilfe der vorigen Gleichung r_n, so erhält man r_{n+1} als Linearkombination von r_{n-2} und r_{n-1}. So fortfahrend erhält man schließlich r_{n+1} als Linearkombination von r_1 und r_2 mit Koeffizienten a und b aus R. □

Definition 2.5.6. Es sei R faktoriell. Das Polynom $f = a_0 + a_1X^1 + \ldots + a_{n-1}X^{n-1} + a_nX^n \in R[X]$ heißt primitiv, falls $ggT(a_0, \ldots, a_n) = 1_R$ gilt.

Satz 2.5.6. *(Gauß)*
Das Produkt zweier primitiver Polynome ist wieder primitiv (in $R[X]$, wobei R ein faktorieller Ring ist).

Beweis. Es seien $f = a_0 + a_1X^1 + \ldots + a_nX^n$ und $g = b_0 + b_1X^1 + \ldots + b_mX^m$ mit $ggT(a_0, \ldots, a_n) = 1$ und $ggT(b_0, \ldots, b_m) = 1$ sowie $fg = c_0 + c_1X^1 + \ldots + c_{n+m}X^{n+m}$ das Produkt. Wir nehmen an, fg sei nicht primitiv. Dann gibt es ein Primelement $p \in R$, das die c_i für $i = 0, \ldots, n+m$ teilt. Wir definieren a_l als letztes a_i mit $p \not| a_i$ und b_k als letztes b_j mit $p \not| b_j$. Dann gilt

$$c_{l+k} = \underbrace{a_0b_{l+k} + a_1b_{l+k-1} + \ldots}_{p|b_j} + a_lb_k + \underbrace{a_{l+1}b_{k-1} + \ldots + a_{l+k}b_0}_{p|a_i}.$$

Da p ein Teiler von c_{l+k} ist, muss p auch $a_l b_k$ teilen, also gilt $p|a_l$ oder $p|b_k$. Das ist aber ein Widerspruch zur Wahl von l und k. □

Satz 2.5.7. *Es sei R faktoriell und K der Quotientenkörper von R. Ist $f \in R[X]$ irreduzibel, so ist f auch irreduzibel in $K[X]$.*

Beweis. Da f in $R[X]$ irreduzibel ist, ist f auch primitiv. Wir nehmen an, f zerfiele in $f = f_1 f_2$ in $K[X]$ (also mit $f_1, f_2 \in K[X]$), so existiere ein $a \in R - \{0_R\}$ mit $af = \tilde{f}_1 \tilde{f}_2$ mit $\tilde{f}_1, \tilde{f}_2 \in R[X]$, womit $\tilde{f}_i$ ein R- Vielfaches von f_i ist. Ohne Einschränkung seien die $\tilde{f}_i$ primitiv. Mit dem Satz 2.5.6 folgt, dass auch $\tilde{f}_1 \tilde{f}_2 \in R[X]$ primitiv ist. Damit folgt, dass a eine Einheit in R ist, und so $f = (a^{-1}\tilde{f}_1)\tilde{f}_2$ in $R[X]$ reduzibel wäre, ein Widerspruch. □

Satz 2.5.8. *Ist R faktoriell, so ist auch $R[X]$ faktoriell.*

Beweis. Wir wenden Satz 2.5.3 an:

i) Es existieren keine unendlichen Teilerketten, da die Grade der Polynome beim Teilen bis auf Null verkleinert werden und auch in R keine unendlichen Teilerketten existieren, da R faktoriell ist.

ii) Sei $q \in R[X]$ unzerlegbar. Es sei K der Quotientenkörper von R. Dann ist q nach Satz 2.5.7 auch in $K[X]$ unzerlegbar und prim, da $K[X]$ ein Hauptidealring ist. Falls $q|ab$ mit $a, b \in R[X]$ gilt, folgt $q|a$ oder $q|b$ in $K[X]$. Da q primitiv ist, folgt $q|a$ in $R[X]$ oder $q|b$ in $R[X]$.

□

Satz 2.5.9. *(Eisensteinkriterium)*
Es sei R faktoriell mit Quotientenkörper K und $f = a_0 + a_1 X^1 + \ldots + a_n X^n \in R[X]$ mit $a_n \neq 0$ für $n > 1$. Es sei weiter $p \in R$ prim, so dass $p \nmid a_n$ und $p|a_i$ für $i = 0, \ldots, n-1$ und $p^2 \nmid a_0$. Dann ist f irreduzibel in $K[X]$.

Beweis. Ohne Einschränkung sei f primitiv. Wir nehmen an, f sei nicht irreduzibel, womit es sich als $f = gh$ mit $g = b_0 + \ldots + b_d X^d \in R[X]$ und $h = c_0 + \ldots + c_m X^m \in R[X]$ mit $b_d, c_m \neq 0$ darstellen ließe. Nun gilt $p|a_0 = b_0 c_0$, aber $p^2 \nmid b_0 c_0$. Daraus folgt ohne Einschränkung $p|c_0$ aber $p \nmid b_0$. Da p nicht $c_m b_d = a_n$ teilt, teilt p auch nicht c_m. Wähle nun r minimal, so dass p nicht c_r teilt. Dann ist $r > 0$ und $a_r = b_0 c_r + b_1 c_{r-1} + \ldots$. Da p weder b_0 noch c_r teilt, teilt es auch nicht das Produkt $b_0 c_r$. Andererseits gilt $p|c_{r-i}$ für $i = 1, \ldots, r$, da $p|c_i$ für $i < r$. Das ist aber ein Widerspruch zu $p|a_r$. □

Kapitel 3

Körpertheorie

3.1 Charakteristik und Primkörper

Definition 3.1.1. Es sei L ein Körper.

i) Unter einem Unterkörper K von L versteht man einen Teilring von L, der ein Körper ist.

ii) Es sei K ein Körper. Unter einer Körpererweiterung von K versteht man ein Paar (L, K), wobei L ein Körper ist, der K als Unterkörper hat (Schreibweise: L/K). Dann heißt L Oberkörper von K.

Beispiel 3.1.1. So sind etwa $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{R}$ Körpererweiterungen.

Definition 3.1.2. Es seien K_1 und K_2 Körper. Ein $\Phi\colon K_1 \to K_2$ heißt (Körper-)isomorphismus, falls es ein Ringisomorphismus ist. In diesem Fall heißen K_1 und K_2 isomorph (Schreibweise: $K_1 \cong K_2$).

Satz 3.1.1. *Es sei K ein Körper. Es gibt nun genau einen Ringhomomorphismus $\Phi\colon \mathbb{Z} \to K$ mit $\Phi(1) = 1_K$. Es gibt $p \in \mathbb{Z}$ mit $\operatorname{Kern}(\Phi) = p\mathbb{Z}$. Man unterscheidet zwei Fälle:*

i) Ist $p > 0$, so ist p eine Primzahl. Dann ist $\Phi(\mathbb{Z})$ der kleinste Unterkörper von K. Er ist isomorph zum Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

ii) Ist $p = 0$, so ist Φ injektiv. Dann gibt es genau einen Ringhomomorphismus $\psi\colon \mathbb{Q} \to K$ mit $\psi_{\mathbb{Z}} = \Phi$. Dann ist $\psi(\mathbb{Q})$ der kleinste Unterkörper von K. Dieser ist isomorph zu $\mathbb{F}_0 := \mathbb{Q}$.

Definition 3.1.3. Die Zahl p aus Satz 3.1.1 heißt Charakteristik von K (Schreibweise: $p = \operatorname{char}(K)$). Man nennt $\mathbb{F}_p$ den Primkörper der Charakteristik p. Der kleinste Unterkörper von K (d.h. der Durchschnitt aller Unterkörper von K) heißt Primkörper von K.

Beweis. (Beweis von Satz 3.1.1)
Offenbar ist $\Phi\colon \mathbb{Z} \to K$, $n \to n \cdot 1_K$ ein Ringhomomorphismus. Weil $\tilde{Phi}(1) = 1_K$ für jeden Ringhomomorphismus $\tilde{\Phi}\colon \mathbb{Z} \to K$ gilt, ist Φ eindeutig bestimmt. Da K Integritätsring ist, ist auch $\Phi(\mathbb{Z}) \subseteq K$ ein Integritätsring. Wegen $\Phi(\mathbb{Z}) \cong \mathbb{Z}/\operatorname{Kern}(\Phi)$ ist nach Satz 2.2.3 $\operatorname{Kern}(\Phi)$ ein Primideal von $\mathbb{Z}$. Nach Satz 2.2.4 folgt $\operatorname{Kern}(\Phi) = \{0\}$ oder $\operatorname{Kern}(\Phi) = p\mathbb{Z}$ mit einer Primzahl p. Da jeder Unterkörper von K das Einselement 1_K enthalten muss, muss er auch $\Phi(\mathbb{Z})$ enthalten, woraus die Behauptung im ersten Fall folgt.
Es sei $p = 0$. Dann ist Φ injektiv. Da $\mathbb{Q}$ ein Quotientenkörper von $\mathbb{Z}$ ist, gibt es nach Satz 2.3.1 genau einen Homomorphismus $\phi\colon \mathbb{Q} \to K$, der Φ fortsetzt. □

Definition 3.1.4. Es sei L/K eine Körpererweiterung und M eine Teilmenge von L. Dann setzt man

i) $[M]$ als den kleinsten Teilring von L, der M umfasst,

ii) (M) als den kleinsten Unterkörper von L, der M umfasst,

iii) $K[M] := [K \cup M]$,

iv) $K(M) := (K \cup M)$.

Ist $M = \{\alpha_1, \ldots, \alpha_n\}$, so schreibt man $K(\alpha_1, \ldots, \alpha_n)$ für $K(M)$. Eine Körpererweiterung L/K heißt einfach bzw. endlich erzeugt, falls $L = K(\alpha)$ bzw. $L = K(\alpha_1, \ldots, \alpha_n)$ für $\alpha, \alpha_1, \ldots, \alpha_n \in L$ ist. Sind K_1 und K_2 Unterkörper von L, so heißt $K_1(K_2) = K_2(K_1)$ das Kompositum von K_1 und K_2 (Schreibweise: K_1K_2).

3.2 Körpererweiterungen

Definition 3.2.1. Es sei L eine Erweiterung eines Körpers K. Unter dem Grad von L über K (Schreibweise $[L\colon K]$) versteht man die Dimension von L als Vektorraum über K. Es handelt sich bei L um eine unendliche Erweiterung von K, falls $[L\colon K] = \infty$ ist, bzw. heißt L eine endliche Erweiterung von K, falls $[L\colon K] = n < \infty$ ist.

Satz 3.2.1. *(Gradsatz)*
Es seien L, K und M Körper sowie L/K und M/L Körpererweiterungen (Schreibweise: $M/L/K$).

i) Es gilt genau dann $[M\colon K] < \infty$, wenn $[M\colon L] < \infty$ und $[L\colon K] < \infty$ gilt.

ii) In diesem Fall ist $[M\colon K] = [M\colon L] \cdot [L\colon K]$.

iii) Ist $\{x_1, \ldots, x_m\}$ eine Basis des Vektorraums L über K und $\{y_1, \ldots, y_n\}$ eine Basis von M über L, so ist $\{x_i \cdot y_j \colon 1 \le i \le m, 1 \le j \le n\}$ eine Basis von M über K.

Beweis. Wir beweisen (iii), woraus offenbar (i) und (ii) folgen.
Wir zeigen zunächst, dass $B = \{x_iy_j \colon 1 \le i \le m, 1 \le j \le m\}$ ein Erzeugendensystem des Vektorraums M über K ist. Es sei $\gamma \in M$. Da $\{y_1, \ldots, y_n\}$ eine Basis des Vektorraums M über dem Körper L ist, gibt es $\beta_1, \ldots, \beta_n \in L$ mit $\gamma = \beta_1 y_1 + \ldots + \beta_n y_n$. Da andererseits $\{x_1, \ldots, x_m\}$ eine Basis von L über K ist, gibt es α_{ij} für $1 \le i \le m$ und $1 \le j \le n$, so dass $\beta_j = \alpha_{1j}x_1 + \ldots \alpha_{mj}x_m$ für $1 \le j \le n$ ist. Es folgt

$$\gamma = \sum_{j=1}^{n} \sum_{i=1}^{m} \alpha_{ij} x_i y_j.$$

Somit bleibt noch die lineare Unabhängigkeit der x_iy_j über K zu zeigen. Angenommen, es gelte

$$\sum_{j=1}^{n} \sum_{i=1}^{m} \alpha_{ij} x_i y_j = 0$$

für Koeffizienten $\alpha_{ij} \in K$, dann folgt

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} \alpha_{ij} x_i \right) y_j = 0,$$

und damit für jedes j auch

$$\sum_{i=1}^{m} \alpha_{ij} x_i = 0,$$

da die y_i linear unabhängig über L sind. Aus der linearen Unabhängigkeit der x_i über K folgt damit dann $\alpha_{ij} = 0$ für alle $1 \leq i \leq m$ und $1 \leq j \leq n$. □

Wir untersuchen nun einfache Körpererweiterungen auf Endlichkeit.

Definition 3.2.2. Es sei L/K eine Körpererweiterung. Ein $\alpha \in L$ heißt algebraisch über K, falls es ein Polynom $f \in K[X] - \{0\}$ mit $f(\alpha) = 0$ gibt. Ein $\alpha \in L$ heißt transzendent über K, falls es nicht algebraisch über K ist. Die Erweiterung L/K heißt algebraisch über K, falls alle $\alpha \in L$ algebraisch über K sind. Nicht algebraische Erweiterungen heißen transzendent. Eine komplexe Zahl $z \in \mathbb{C}$ heißt algebraisch (bzw. transzendent), falls z algebraisch (bzw. transzendent) über $\mathbb{Q}$ ist.

Bemerkung 3.2.1. Es sei $\alpha \in L$.

i) Offenbar ist α genau dann transzendent über K, wenn α eine Unbestimmte über K ist.

ii) Man kann zeigen, dass wichtige Konstanten der Analysis (beispielsweise e und π) transzendent sind.

Definition 3.2.3. Unter einem normierten Polynom $f \in K[X]$ versteht man ein Polynom mit höchstem Koeffizienten 1_K, also

$$f = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0.$$

Satz 3.2.2. *Es sei X eine Unbestimmte über K und L/K eine Körpererweiterung von K mit $\alpha \in L$. Der Ringhomomorphismus Φ sei durch $\Phi\colon K[X] \to K[\alpha]$, $f \to f(\alpha)$ gegeben.*

i) Dann ist α genau dann transzendent über K, wenn $\mathrm{Kern}(\Phi) = \{0\}$ ist. In diesem Fall ist $K[\alpha] \cong K[X]$, und $K[\alpha]$ ist kein Körper. $K(\alpha)$ ist der Quotientenkörper von $K[\alpha]$.

ii) Es sei α algebraisch über K. Dann ist $\mathrm{Kern}(\Phi) = (g)$ für ein eindeutig bestimmtes, normiertes und irreduzibles Polynom $g \in K[X]$. Für $h \in K[x]$ gilt genau dann $h(\alpha) = 0$, wenn $g|h$, und g ist durch diese Eigenschaft eindeutig bestimmt: es ist das Polynom kleinsten Grades aus $K[X] - \{0\}$ mit der Nullstelle α. Es gilt $K(\alpha) = K[\alpha] \cong K[X]/(g)$ und

$$K(\alpha) = \{\beta\colon \beta = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1},\ a_i \in K,\ 0 \leq i \leq n-1\},$$

wobei jedes $\beta \in K(\alpha)$ genau eine Darstellung der Form $\beta = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ mit Koeffizienten aus K besitzt. Es ist $[K(\alpha)\colon K] = \deg(g) = n$.

iii) Folgende Aussagen sind äquivalent:

(a) α ist algebraisch über K.

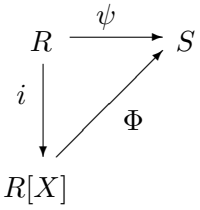
(b) $K(\alpha)/K$ ist eine endliche Erweiterung.

(c) $K(\alpha)/K$ ist eine algebraische Erweiterung.

Beweis. i) und ii):

Wir verwenden die Definition 2.4.1 des Polynomrings. Danach besteht ein Polynomring aus einem kommutativen Ring $R[X]$ und einem Ringhomomorphismus $i\colon R \to R[X]$, so dass es für jeden Ringhomomorphismus $\psi\colon R \to S$ mit einen kommutativen Ring S und $x \in S$ genau einen Ringhomomorphismus $\Phi\colon R[X] \to S$ mit $\psi = \Phi \circ i$ und $\Phi(X) = x$ gibt, d.h. wir haben

das kommutative Diagramm



von Ringen.Wir setzen nun $R = K$, $i = id_K$, $S = L$, $x = \alpha$ und $\psi = id_K$. Es gibt genau einen Ringhomomorphismus $\Phi\colon K[X] \to K[\alpha]$, für den wegen der Relationstreue $\Phi(f(X)) = f(\alpha)$ für alle $f \in K[X]$ gelten muss. Nach Satz 2.4.3 ist Φ genau dann ein Isomorphismus, wenn α eine Unbestimmte über K, d.h. transzendent über K ist. Da $K[X]$ kein Körper ist, ist auch $K[\alpha]$ keiner. Der kleinste Körper, der $K[\alpha]$ enthält, ist sein Quotientenkörper. Ist α algebraisch über K, so ist Kern(Φ) ein von $\{0\}$ verschiedenes Ideal. Da $K[X]$ ein Euklidischer Ring ist, ist Kern(Φ) $= (g)$ mit $g \in K[X] - \{0\}$. Nach dem Homomorphiesatz für Ringe (Satz 2.2.2) ist dann $K[X]/(g) \cong K[\alpha]$. Da $K[\alpha]$ ein Integritätsring ist, ist (g) nach Satz 2.2.3 (i) ein Primideal. Nach Satz 2.5.2 ist g irreduzibel. Nach Satz 2.5.4 (iii) ist dann (g) maximal. Damit ist nach Satz 2.2.3 (ii) der Faktorring $K[x]/(g)$ und somit auch $K[\alpha]$ ein Körper. Also gilt $K(\alpha) = K[\alpha]$. Es sei $h \in K[X]$, womit

$$h(\alpha) = 0 \Leftrightarrow h \in \text{Kern}(\Phi) = (g) \Leftrightarrow g|h$$

gilt. Es sei $f \in K[X]$ und $f(X) = g(X)q(X) + r(X)$ mit $\deg(r) < \deg(g) = n$. Dann ist $f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, und damit

$$K[\alpha] = \{r(\alpha)\colon r \in K[X],\ \deg(r) \leq n-1\} = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}\colon a_i \in K\}.$$

Es gilt genau dann $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = 0$, wenn $a_i = 0$ für alle i gilt. Damit ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Basis des Vektorraums $K(\alpha)$ über K, und die Darstellung jedes $\beta \in K(\alpha)$ in der angegebenen Form ist eindeutig. Es folgt $[K(\alpha)\colon K] = n$.

(iii) Die Aussage $(a) \Rightarrow (b)$ ist schon in (ii) enthalten.
$(b) \Rightarrow (c)$:
Es sei $\beta \in K(\alpha)$ mit $[K(\alpha)\colon K] = n$. Dann sind die $n+1$ Elemente $1, \beta, \ldots, \beta^n$ des Vektorraums $K(\alpha)$ über K linear abhängig, d.h. es gibt ein $g = b_0 + b_1X + \ldots + b_nX^n \in K[X]$ mit

$$g(\beta) = b_0 + b_1\beta + \ldots + b_n\beta^n = 0.$$

Das heißt, dass β algebraisch über K ist.
$(c) \Rightarrow (a)$:
Insbesondere ist α algebraisch über K, und nach Teil (ii) ist daher $K(\alpha)/K$ endlich.

□

Definition 3.2.4. Es sei α algebraisch über dem Körper K. Das Polynom g des Satzes 3.2.2 heißt Minimalpolynom von α über K (Schreibweise: $m_K(\alpha, X)$). Der Grad $\deg(m_K(\alpha, X))$ des Minimalpolynoms heißt auch Grad von α über K (Schreibweise: $\deg_K(\alpha)$). Nach Satz 3.2.2 ist $\deg_K(\alpha) = [K(\alpha)\colon K]$. Offenbar gilt

$$\deg_K(\alpha) = 1 \Leftrightarrow m_K(\alpha, X) = X - \alpha \Leftrightarrow \alpha \in K.$$

Beispiel 3.2.1. Es sei $K = \mathbb{Q}$ und $L = \mathbb{R}$. Nach dem Zwischenwertsatz der Analysis hat das Polynom $g(X) = X^3 - 2$ in $L = \mathbb{R}$ genau eine Nullstelle, nämlich $\alpha = \sqrt[3]{2}$. Somit ist nach dem Eisensteinkriterium (Satz 2.5.9) g irreduzibel. Daher ist $m_{\mathbb{Q}}(\sqrt[3]{2}, X) = X^3 - 2$. Nach Satz 3.2.2 ist

$$\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2\colon a_0, a_1, a_2 \in \mathbb{Q}\}$$

und $[\mathbb{Q}(\sqrt[3]{2}\colon \mathbb{Q}] = 3$. Es sei $\gamma = 4 - 2\sqrt[3]{2} + \sqrt[3]{2}^2 \in \mathbb{Q}(\sqrt[3]{2}$. Wir wollen γ^{-1} als Polynom höchstens zweiten Grades in $\sqrt[3]{2}$ schreiben.

Lösung:
Wir setzen $g(X) = m_{\mathbb{Q}}(\sqrt[3]{2}, X) = X^3 - 2$ und $f(X) = X^2 - 2X + 4$, also $\gamma = f(\sqrt[3]{2})$. Mittels des Euklidischen Algorithmus bestimen wir $s, t \in \mathbb{Q}[X]$ derart, dass $f \cdot s + g \cdot t = 1$ in $\mathbb{Q}[X]$ gilt:

$$\begin{aligned} X^3 - 2 &= (X+2)\cdot(X^2 - 2X + 4) - 10 \\ \Rightarrow 10 &= (X+2)\cdot(X^2 - 2X + 4) - (X^3 - 2) \\ \Rightarrow 1 &= \left(\frac{1}{10}X + \frac{1}{5}\right)\cdot(X^2 - 2X + 4) - \frac{1}{10}(X^3 - 2) \\ \Rightarrow 1 &= \left(\frac{1}{5} + \frac{1}{10}\sqrt[3]{2}\right)\cdot\left(4 - 2\sqrt[3]{2} + \sqrt[3]{2}^2\right), \end{aligned}$$

und damit $\gamma^{-1} = \frac{1}{5} + \frac{1}{10}\sqrt[3]{2}$.

Wir wenden uns nun Körpererweiterungen zu, die nicht notwendig einfach sind.

Satz 3.2.3. *Es sei L/K eine Körpererweiterung. Folgende Eigenschaften sind äquivalent:*

i) L/K ist endlich.

ii) L/K ist algebraisch und $L = K(\alpha_1, \ldots, \alpha_n)$.

iii) $L = K(\alpha_1, \ldots, \alpha_n)$ ist endlich erzeugt, wobei α_i jeweils algebraisch über $K(\alpha_1, \ldots, \alpha_{i-1})$ für $i = 1, \ldots, n$ ist.

Beweis. i) $\Rightarrow$ ii):
Es sei $\alpha \in L$. Wegen $K \subseteq K(\alpha) \subseteq L$ ist $K(\alpha)/K$ nach Satz 3.2.1 endlich. Nach Satz 3.2.2 (iii) ist α algebraisch über K. Also ist L/K algebraisch. Wir konstruieren nun eine beliebige (endliche oder unendliche) Folge (α_i) mit $\alpha_i \in L$, so dass $\alpha_1 \notin K$ und $\alpha_i \notin K(\alpha_1, \ldots, \alpha_{i-1})$ ist. Nach dem Gradsatz (Satz 3.2.1) ist dann

$$\begin{aligned} [K(\alpha_1, \ldots, \alpha_i)\colon K] = \quad & [K(\alpha_1, \ldots, \alpha_i)\colon K(\alpha_1, \ldots, \alpha_{i-1})] \\ & [K(\alpha_1, \ldots, \alpha_{i-1})\colon K(\alpha_1, \ldots, \alpha_{i-2})] \\ & \qquad\qquad \vdots \\ & \qquad\qquad [K(\alpha_1)\colon K] \geq 2^i. \end{aligned}$$

Da L/K endlich ist, muss nach endlich vielen Schritten $K(\alpha_1, \ldots, \alpha_n) = L$ gelten.

ii) $\Rightarrow$ iii):
Da L/K algebraisch ist, ist α_i algebraisch über K und damit auch über $K(\alpha_1, \ldots, \alpha_{i-1})$.

iii) $\Rightarrow$ i):
Nach dem Gradsatz und Satz 3.2.2 (iii)i st

$$[L\colon K] = [L\colon K(\alpha_1, \ldots, \alpha_{n-1})] \cdots [K(\alpha_1)\colon K] < \infty.$$

□

Satz 3.2.4. *Es seien $M/L/K$ Körpererweiterungen. Ist M algebraisch über L und L algebraisch über K, so ist auch M algebraisch über K.*

Beweis. Es sei $\beta \in M$. Dann ist β algebraisch über L, d.h. es gibt ein $\in L[X] - \{0\}$ mit

$$f(X) = \alpha_n X^n + \alpha_{n-1} X^{n-1} + \ldots + \alpha_0$$

mit $\alpha_i \in L$.und zudem $f(\beta) = 0$. Damit ist β auch algebraisch über $K(\alpha_0, \ldots, \alpha_n)$ und insbesondere ist $[K(\alpha_0, \ldots, \alpha_n, \beta)\colon K(\alpha 0, \ldots, \alpha_n)] < \infty$. Nach Satz 3.2.3 (iii) ist $[K(\alpha_0, \ldots, \alpha_n)\colon K] < \infty$, nach dem Gradsatz (Satz 3.2.1) ist also $[K(\alpha_0, \ldots, \alpha_n, \beta)\colon K] < \infty$, also auch $[K(\beta)\colon K] < \infty$, und β ist algebraisch über K. □

3.3 Endliche Körper

Endliche Körper sind isomorph zu endlichen Erweiterungen der Körper $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ mit einer Primzahl p.

Satz 3.3.1. *Es sei p eine Primzahl. Dann gibt es stets ein irreduzibles Polynom in $(\mathbb{Z}/p\mathbb{Z})[X]$ vom Grad m.*

Beweis. ohne Beweis. □

Satz 3.3.2. *Die Ordnung eines endlichen Körpers K ist stets eine Primzahlpotenz $|K| = p^m$ für eine Primzahl p und $m \in \mathbb{N}$. Der Primkörper P von K ist isomorph zu $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$.*

Beweis. Es sei P der Primkörper von K. Wäre $\mathrm{char}(P) = 0$, so wäre nach Satz 3.2.1 dann $P \cong \mathbb{Q}$, im Widerspruch zur Endlichkeit von K. Also folgt nach Satz 3.1.1 $\mathrm{char}(P) = p$ für eine Primzahl p und $P \cong (\mathbb{Z}/p\mathbb{Z})$. Es sei $[K\colon P] = m$ und $x_1, \ldots, x_m$ eine Basis des Vektorraums K über P. Dann ist

$$K = \{\alpha_1 x_1 + \ldots \alpha_m x_m\colon \alpha_i \in P,\ 1 \leq i \leq m\}.$$

Somit gilt $|K| = p^m$. □

Satz 3.3.3. *Es sei $q = p^m$ für eine Primzahl p und $m \in \mathbb{N}$. Dann gibt es einen Körper K mit $|K| = q$.*

Beweis. Nach Satz 3.3.1 gibt es ein irreduzibles Polynom g in $(\mathbb{Z}/p\mathbb{Z})[X]$ vom Grad m. Nach Bemerkung 2.5.1 ist (g) ein Primideal. Nach Satz 2.5.4 ist (g) maximal. Wir betrachten den Oberring $\mathbb{F}_q := (\mathbb{Z}/p\mathbb{Z})[X]/(g)$ von $\mathbb{Z}/p\mathbb{Z}$. Nach Satz 2.2.4 ist $\mathbb{F}_q$ ein Körper. Die Restklasse $\alpha := x + (g)$ ist Nullstelle von g, weswegen nach Satz 3.2.2 $\mathbb{F}_q = (\mathbb{Z}/p\mathbb{Z})(\alpha)$ und $[\mathbb{F}_q\colon (\mathbb{Z}/p\mathbb{Z})] = m$ ist. Also ist $|\mathbb{F}_q| = p^m$. □

Satz 3.3.4. *Es sei $q = p^m$ mit einer Primzahl p und $m \in \mathbb{N}$. Dann gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ mit $\mathbb{F}_q = q$.*

Beweis. ohne Beweis. □

3.4 Konstruktionen mit Zirkel und Lineal

Im Mittelpunkt der Geometrie der alten Griechen standen Konstruktionen geometrischer Figuren. Als Mittel zur Konstruktion waren dabei nur Zirkel und Linear zugelassen. Während viele Probleme auf diese Weise erfolgreich gelöst werden konnten, blieben andere ungeöst, vor allem drei berühmte Probleme:

i) Das Delische Problem der Würfelverdopplung:
Ein vorgegebener Würfel ist so zu vergrößern, dass ein Würfel doppelten Volumens entsteht.

ii) Die Winkeldreiteilung:
Ein Winkel ist mit Hilfe von Zirkel und Lineal in drei gleiche Teile zu zerlegen.

iii) Die Quadratur des Kreises:
Zu einem gegebenen Kreis ist ein Quadrat mit gleichem Flächeninhalt zu konstruieren.

Schon die alten Griechen vermuteten, dass die Lösung der genannten Probleme unmöglich sei. Dies konnte jedoch erst ca. 2000 Jahre später gezeigt werden. Eine erste wichtige Voraussetzung zur Lösung dieser Probleme wurde von Descartes geschaffen, indem er durch die Einführung von Kartesischen Koordinatensystemen und der damit verbundenen Identifizierung von Punkten mit Zahlenpaaren (bzw. n- tupeln) ermöglichte, geometrische Beziehungen in algebraische Beziehungen zu übersetzen. So liegt etwa der Punkt P mit den Koordinaten (x, y) genau dann auf dem Einheitskreis, wenn $x^2 + y^2 = 1$ erfüllt ist. In der weiteren Entwicklung wurde dann die Konstruierbarkeit von Punkten durch die Zugehörigkeit ihrer Koordinaten zu gewissen Zahlkörpern charakterisiert, und es wurde gezeigt, dass diese algebraischen Kriterien in den genannten Problemen nicht erfüllt sind.

Definition 3.4.1. Es sei $\mathfrak{F}$ eine Teilmenge der Euklidischen Ebene mit mindestens zwei Punkten.

i) (a) Eine $\mathfrak{F}$- Gerade ist jede Gerade g, die mindestens zwei Punkte aus $\mathfrak{F}$ enthält.
   (b) Ein $\mathfrak{F}$- Kreis ist jeder Kreis, dessen Mittelpunkt in $\mathfrak{F}$ liegt, und dessen Radius durch den Abstand von zwei Punkten aus $\mathfrak{F}$ gegeben ist.
   (c) Eine $\mathfrak{F}$- Figur ist eine $\mathfrak{F}$- Gerade oder ein $\mathfrak{F}$ -Kreis.

ii) Ein Schnittpunkt von zwei (verschiedenen) $\mathfrak{F}$- Figuren heißt aus $\mathfrak{F}$ elementar konstruierbar.

iii) Jeder Punkt der Euklidischen Ebene, für den endlich viele Punkte, etwa $P_1, \ldots, P_n$ existieren, so dass für alle $k = 0, \ldots, n-1$ der Punkt P_{k+1} aus $\mathfrak{F}_k = \mathfrak{F} \cup \{P_1, \ldots, P_k\}$ elementar konstruierbar ist, heißt aus $\mathfrak{F}$ konstruierbar.

Satz 3.4.1. *Es sei $\mathfrak{F} = \{P_1, \ldots, P_m\}$ mit $P_i = (x_i, y_i) \in \mathbb{R}^2$ gegeben. Für die Koordinaten jedes aus $\mathfrak{F}$ elementar konstruierbaren Punktes $P_{m+1} = (x_{m+1}, y_{m+1})$ gilt $x_{m+1}, y_{m+1} \in L(\sqrt{d_m})$ mit $L = \mathbb{Q}(x_1, \ldots, x_m, y_1, \ldots, y_m)$ und $d_m \in L \cap \mathbb{R}^+$ mit $\mathbb{R}^+ = [0, \infty)$.*

Beweis. Wir untersuchen zunächst, welchem Körper die Koeffizienten angehören, die in den Gleichungen für die $\mathfrak{F}$- Figuren auftreten:

$\mathfrak{F}$- Geraden:
Die Verbindungsgerade der Punkte $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ ist durch die Lösungen $P = (x, y)$ der Gleichung

$$(x_2 - x_1)(y - y_1) = (y_1 - y_1)(x - x_1),$$

also durch $ax + by = c$ für Koeffizienten $a, b, c \in L$ gegeben.

$\mathfrak{F}$- Kreise:
Der Radius r eines $\mathfrak{F}$- Kreises K ist durch den Abstand zweier Punkte $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ aus $\mathfrak{F}$ gegeben. Es ist $r^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2 \in L$. Ist $P_0 = (x_0, y_0)$ der Mittelpunkt von K aus $\mathfrak{F}$, so ist dessen Gleichung durch

$$(x - x_0)^2 + (y - y_0)^2 = r^2$$

bzw. $ax^2 + ay^2 + bx + cy + d = 0$ für Koeffizienten $a, b, c, d \in L$ und $a \neq 0$ gegeben.

$\mathfrak{F}$- Figur:
Diese beiden Gleichungen erlauben eine gemeinsame Darstellung von $\mathfrak{F}$- Geraden und $\mathfrak{F}$- Kreisen als Lösungen einer Gleichung

$$ax^2 + ay^2 + bx + cy + d = 0 \qquad (*)$$

mit $a, b, c, d \in L$, wobei es sich für $a \neq 0$ um einen $\mathfrak{F}$- Kreis und für $a = 0$ um eine $\mathfrak{F}$- Gerade handelt. Es seien nun zwei $\mathfrak{F}$- Figuren gegeben, etwa durch

$$a_1x^2 + a_1y^2 + b_1x + c_1y + d_1 = 0 \qquad (1)$$

und

$$a_2x^2 + a_2y^2 + b_2x + c_2y + d_2 = 0 \qquad (2)$$

mit $a_i, b_i, c_i, d_i \in L$.

Wir untersuchen die Koordinaten des Schnittpunkts:

Fall 1: $a_1 = a_2 = 0$:
Es liegen zwei $\mathfrak{F}$- Geraden vor. Die Koordinaten des Schnittpunkts S gehören dem Körper L an, da sie sich beispielsweise nach der Cramerschen Regel als rationale Funktionen der Koeffizienten b_i, c_i, d_i ausdrücken lassen.

Fall 2: $a_1 \neq 0$ oder $a_2 \neq 0$:
Es liegt mindestens ein $\mathfrak{F}$- Kreis vor, ohne Einschränkung sei dieser durch (1) gegeben, also $a_1 \neq 0$. Angenommen $a_2 = 0$, so lässt sich Gleichung (2) nach x oder y auflösen. Wir erhalten

$$y = kx + l \quad \text{bzw.} \quad x = ky + l \qquad (3)$$

mit $k, l \in L$. Dies in (1) eingesetzt, ergibt eine quadratische Gleichung für x bzw. y:

$$px^2 + qx + r = 0 \qquad (4)$$

mit $p, q, r \in L$.
Angenommen $a_2 \neq 0$. Durch Multiplikation mit $f \in L - \{0\}$ können wir $a_1 = a_2$ erreichen. Subtraktion der Gleichungen (1) und (2) ergibt eine lineare Gleichung für x und y, außer im Fall konzentrischer Kreise (in welchem die Koeffizienten von x und y beide verschwinden). Auflösung nach einer der Variablen ergibt wieder eine Gleichung der Form (3). Diese in (1) eingesetzt, ergibt wiederum eine quadratische Gleichung der Form (4). Die Lösungen von (4) seien für beliebiges a_2 nun durch

$$x_{1,2} = \frac{-q \pm \sqrt{q^2 - 4pr}}{2p}$$

für $d = q^2 - 4pr \geq 0$ gegeben. Für $d < 0$ gibt es keine Lösung, d.h. die Kreise schneiden sich nicht. Also ist $x_{1,2} \in L(\sqrt{d})$ mit $d \geq 0$ und insbesondere $d \in L$. Einsetzen in (3) ergibt nun dasselbe für die y- Koordinate $y_{1,2}$ der Schnittpunkte.
Damit ist der Satz bewiesen. □

Definition 3.4.2. Es sei nun im folgenden $\mathfrak{F}^* = \{(0, 0), (1, 0)\}$.

Satz 3.4.2. *Ist $P = (x, y)$ aus $\mathfrak{F}^*$ konstruierbar, so sind $x, y \in K$, wobei K ein Körper mit Grad $[K\colon \mathbb{Q}] = 2^k$ für ein $k \in \mathbb{N}_0$ ist.*

Beweis. Nach Definition 3.4.2 ist P_m genau dann konstruierbar, wenn es Punkte $P_1, \ldots, P_{m-1}$ gibt, so dass für alle $k = 0, \ldots, m-1$ der Punkt P_{k+1} aus $\mathfrak{F}_k = \mathfrak{F}^* \cup \{P_1, \ldots, P_k\}$ elementar konstruierbar ist. Es sei $P_i = (x_i, y_i)$ und $L_k = \mathbb{Q}(x_1, \ldots, x_k, y_1, \ldots, y_k)$ sowie $L_0 = \mathbb{Q}$. Es ist klar, dass die Koordinaten der Punkte aus $\mathfrak{F}_0 = \mathfrak{F}^*$ in $L_0 = \mathbb{Q}$ liegen. Nach Satz 3.4.1 ist $L_{k+1} = L_k(\sqrt{d_k})$ mit einem $d_k \in L_k \cap \mathbb{R}^+$. Dann ist

$$m_L(\sqrt{d_k}, X) = \begin{cases} X^2 - d_k, & \text{falls } \sqrt{d_k} \notin L_k, \\ X^2 - \sqrt{d_k}, & \text{falls } \sqrt{d_k} \in L_k. \end{cases}$$

Somit ist $[L_{k+1}\colon L_k] \in \{1, 2\}$. Nach dem Gradsatz ist dann

$$[L_m\colon L_0] = [L_m\colon L_{m-1}] \cdot [L_{m-1}\colon L_{m-2}] \cdots [L_1\colon L_0] = 2^n$$

für ein $n \in \mathbb{N}_0$. □

Satz 3.4.3. *Die Lösung des Delischen Problems der Würfelverdopplung ist mit Zirkel und Lineal nicht konstruierbar.*

Beweis. Die Lösung des Problems läuft auf die Konstruktion des Punktes $P = (\sqrt[3]{2}, 0)$ aus $\mathfrak{F}^*$ hinaus. Nach dem Satz von Gauß gilt für eine rationale Nullstelle $\alpha = \frac{a}{b}$ von $p(X) = X^3 - 2$ mit $ggT(a, b) = 1$ dann $a|2$ und $b|1$. Damit besitzt p keine Nullstelle in $\mathbb{Q}$ und ist damit über $\mathbb{Q}$ irreduzibel. Also gilt $m_{\mathbb{Q}}(\sqrt[3]{2}, X) = p(X) = X^3 - 2$. Damit ist $[\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}] = 3$, und mit Satz 3.4.2 ist $P = (\sqrt[3]{2}, 0)$ daher nicht aus $\mathfrak{F}^*$ konstruierbar. □

Satz 3.4.4. *Die Dreiteilung des Winkels mit Zirkel und Lineal ist unmöglich, denn es ist nicht möglich, aus $\mathfrak{F}^*$ den Punkt $(\cos\frac{\pi}{9}, 0)$ zu konstruieren.*

Beweis. Es sei $\gamma = \frac{\pi}{9}$ und

$$\cos\beta + i \cdot \sin\beta = (\cos\gamma + i \cdot \sin\gamma)^3 = \cos^3\gamma + 3i \cdot \cos^2\gamma \cdot \sin\gamma - 3 \cdot \cos\gamma \cdot \sin^2\gamma - i \cdot \sin^3\gamma,$$

also

$$\cos(3\gamma) = \cos^3\gamma - 3\cos\gamma \cdot (1 - \cos^2\gamma) = \cos^3\gamma + 3\cos^3\gamma - 3\cos\gamma = 4\cos^3\gamma - 3\cos\gamma.$$

Anders ausgedrückt: Es ist $\alpha = \cos\gamma$ eine Nullstelle des Polynoms $p(X) = 8X^3 - 6X - 1$. Nach dem Satz von Gauß gilt für eine rationale Nullstelle $\alpha = \frac{a}{b}$ mit $ggT(a, b) = 1$ aber $a|1$ und $b|8$. Man überprüft aber leicht, dass $p(x)$ keine Nullstelle dieser Art besitzt. Damit ist das Polynom $p(x)$ über $\mathbb{Q}$ irreduzibel, womit $[\mathbb{Q}(\cos\frac{\pi}{9})\colon \mathbb{Q}] = 3$ gilt. Nach Satz 3.4.2 ist der Punkt $(\cos\frac{\pi}{9}, 0)$ nicht aus $\mathfrak{F}^*$ konstruierbar. □

Satz 3.4.5. *Die Quadratur des Kreises ist mit Zirkel und Lineal unmöglich.*

Beweis. Es sei sei der Einheitskreis um den Nullpunkt, der durch die Gleichung $x^2 + y^2 = 1$ beschrieben wird, gegeben, welcher den Flächeninhalt π besitzt. Ein Quadrat mit Flächeninhalt π besitzt dann die Seitenlänge $\sqrt{\pi}$. Die Quadratur des Einheitskreises läuft also auf die Konstruktion des Punktes $(\sqrt{\pi}, 0)$ hinaus. Nach Satz 3.4.2 müsste dann die Zahl $\sqrt{\pi}$ in einem Körper K enthalten sein, dessen Grad über $\mathbb{Q}$ endlich ist. Dieser enthielte dann aber auch π, im Widerspruch zur Transzendenz von π, die wegen des dazu nötigen Aufwands in dieser Vorlesung nicht gezeigt wird, aber 1882 von Ferdinand von Lindemann gezeigt wurde. □