Algebra I

WS 2002/03

Tim Römer

Fachbereich Mathematik/Informatik
Universität Osnabrück

Inhaltsverzeichnis

KAPITEL 1

Gruppentheorie

1. Grundbegriffe der Gruppentheorie

Definition 1.1. Eine Menge G zusammen mit einer Verknüpfung

$$\cdot : G \times G \longrightarrow G, (a, b) \mapsto a \cdot b = ab$$

heißt *Gruppe*, wenn Folgendes gilt:

(i) $\cdot$ ist assoziativ, d.h. für alle $a, b, c \in G$ gilt $(ab)c = a(bc)$.

(ii) Es gibt ein Element $e \in G$ mit folgenden Eigenschaften:
   (a) Für alle $a \in G$ gilt $ea = a$.
   (b) Zu jedem $a \in G$ existiert ein $b \in G$ mit $ba = e$.

   Die Gruppe heißt *abelsch (kommutativ)*, wenn zusätzlich gilt:

(iii) Für alle $a, b \in G$ gilt $ab = ba$.

Man schreibt $(G, \cdot)$ oder G für die Gruppe. Das Element e heißt *das neutrale Element* der Gruppe. Das Element b aus (ii)(b) heißt *das inverse Element* zu a und man schreibt a^{-1}.

Bemerkung 1.2. Es gilt:

(i) Das neutrale Element ist eindeutig.

(ii) Zu jedem Element ist das inverse Element eindeutig.

(iii) ...

In 1.1 wurde die Gruppe multiplikativ geschrieben. In diesem Fall wird das neutrale Element auch mit 1 bezeichnet. Alternativ lässt sich eine Gruppe additiv (mit einer Verknüpfung $+$) schreiben. Dann wird das neutrale Element auch mit 0 und das inverse Element zu a mit $-a$ bezeichnet.

Beispiel 1.3. Nun ein paar Beispiele:

(i) Die Menge der ganzen Zahlen $\mathbb{Z}$ mit der Addition als Verknüpfung ist eine abelsche Gruppe.

(ii) Die Menge der natürlichen Zahlen $\mathbb{N}$ mit der Addition als Verknüpfung ist keine Gruppe.

(iii) $G = \{e, a\}, e =$ neutrales Element, $a^2 = aa = e$ ist eine abelsche Gruppe mit zwei Elementen.

(iv) Eine Gruppe kann man durch eine Gruppentafel beschreiben:

$\cdot$	...	b	...
...			
a		$a \cdot b$	
...			

Sei $G = \{e, a, b, c\}$. Die Menge G mit

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

ist eine abelsche Gruppe. G mit

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

ist auch eine abelsche Gruppe.

(v) Sei $X \neq \emptyset$ ein Menge. Mit $S(X)$ bezeichnen wir die Menge aller bijektiven Abbildungen von X nach X. Die Menge $S(X)$ zusammen mit der Verknüpfung als Abbildung ist eine Gruppe. $S(X)$ heißt die *symmetrische Gruppe auf X*. Speziell:

$$S_n = S(\{1, \ldots, n\}).$$

Die Elemente von $S(X)$ heißen *Permutationen*. Falls $|X| \geq 3$, dann ist $S(X)$ nicht abelsch. Denn seien:

(a) $x_1, x_2, x_3 \in X$,

(b) $\varphi_1 \in S(X)$ mit $\varphi_1(x_1) = x_2,\ \varphi_1(x_2) = x_1,\ \varphi_1(x_3) = x_3,\ \varphi_1(x) = x$ sonst,

(c) $\varphi_2 \in S(X)$ mit $\varphi_2(x_1) = x_2,\ \varphi_2(x_2) = x_3,\ \varphi_2(x_3) = x_1,\ \varphi_2(x) = x$ sonst.

Dann gilt:

$$\varphi_1 \circ \varphi_2 \neq \varphi_2 \circ \varphi_1, \text{ etwa } \varphi_1 \circ \varphi_2(x_1) = x_1 \neq x_3 = \varphi_2 \circ \varphi_1(x_1).$$

Sei X endlich und $\varphi \in S(X)$, dann kann φ wie folgt beschrieben werden:

(a) $\begin{pmatrix} x_1 & x_2 & \ldots \\ \varphi(x_1) & \varphi(x_2) & \ldots \end{pmatrix}$

(b) (Zyklenschreibweise) Z.B.:

$$\varphi\colon (x_1, x_2)(x_4, x_5, x_6) \text{ für}$$

$$\varphi(x_1) = x_2,\ \varphi(x_2) = x_1,$$

$$\varphi(x_4) = x_5,\ \varphi(x_5) = x_6,\ \varphi(x_6) = x_4,$$

$$\varphi(x) = x \text{ sonst.}$$

Definition 1.4. Seien G, H Gruppen. Eine Abbildung $\varphi\colon G \longrightarrow H$ heißt *Gruppenhomomorphismus*, wenn für alle $a, b \in G$ gilt: $\varphi(ab) = \varphi(a) \circ \varphi(b)$. Ein Gruppenhomomorphismus φ heißt

(i) *Monomorphismus*, wenn φ injektiv ist,
(ii) *Epimorphismus*, wenn φ surjektiv ist,
(iii) *Isomorphismus*, wenn φ bijektiv ist.

Bemerkung 1.5. Man überlegt sich, dass

(i) $\varphi(e_G) = e_H$,
(ii) $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Beispiel 1.6. Betrachte:

(i) Jede beliebige Gruppe G lässt sich in eine symmetrische Gruppe einbetten. Genauer gilt, dass

$$\varphi\colon G \longrightarrow S(G),\ a \mapsto \varphi(a)$$

mit

$$\varphi(a)\colon G \longrightarrow G,\ b \mapsto ab$$

ein Monomorphismus ist.

(ii) Sei $G = \{e, a\}$ die Gruppe von 1.3 (iii), also $a^2 = e$. Definiere

$$\varphi\colon \mathbb{Z} \longrightarrow G = \{e, a\},$$

$$z \mapsto \begin{cases} e & \text{falls z gerade,} \\ a & \text{falls z ungerade.} \end{cases}$$

φ ist ein Epimorphismus.

(iii) Die beiden Gruppen aus 1.3(iv) sind nicht isomorph, obwohl beide vier Elemente besitzen.

Definition 1.7. Sei G eine Gruppe. Eine nicht leere Teilmenge H von G ($H \subseteq G$) heißt *Untergruppe* von G, wenn:

(i) Für alle $a, b \in H$ gilt $ab \in H$,
(ii) H zusammen mit der induzierten Abbildung $H \times H \longrightarrow H, (a, b) \mapsto ab$ ist eine Gruppe.

Lemma 1.8. Sei G eine Gruppe. Eine nicht leere Teilmenge $H \subseteq G$ ist genau dann eine Untergruppe von G, wenn für alle $a, b \in H$ gilt:

$$ab^{-1} \in H.$$

Dies ist das sogenannte *Untergruppenkriterium*.

Beweis. Ist H eine Untergruppe von G, so folgt direkt aus der Definition, dass $ab^{-1} \in H$ für alle $a, b \in H$ gilt.

Gelte nun das Untergruppenkriterium für eine Menge $H \subseteq G$. Dann gilt:

(i) Sei $a \in H \neq \emptyset$ beliebig. Dann ist $e = aa^{-1} \in H$.
(ii) Sei $a \in H$ beliebig. Dann ist nach (i) $e \in H$ und es gilt $a^{-1} = ea^{-1} \in H$.
(iii) Sei $a, b \in H$. Dann folgt nach (ii), dass $b^{-1} \in H$ und somit $ab = a(b^{-1})^{-1} \in H$.

Mit Hilfe dieser Aussagen folgt, dass H eine Gruppe, speziell eine Untergruppe von G, ist. □

Beispiel 1.9. Betrachte:

(i) Die Teilmenge $n\mathbb{Z}$, der durch n teilbaren ganzen Zahlen, ist eine Untergruppe von $\mathbb{Z}$.
(ii) In jeder der Gruppen aus 1.3 ist die Untergruppe mit zwei Elementen enthalten.

Lemma 1.10. Seien G, H Gruppen und $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus. Dann gilt:

(i) $\mathrm{Im}(\varphi) = \{b \in H\colon \text{ es gibt ein } a \in G \text{ mit } \varphi(a) = b\}$ ist eine Untergruppe von H.
(ii) Sei e_H das neutrale Element von H. $\mathrm{Ker}(\varphi) = \{a \in G\colon \varphi(a) = e_H\}$ ist eine Untergruppe von G.

$\mathrm{Im}(\varphi)$ heißt das *Bild* und $\mathrm{Ker}(\varphi)$ der *Kern* von φ.

Beweis. (i) Seien $b_1, b_2 \in \mathrm{Im}(\varphi)$ und $a_1, a_2 \in G$ mit $\varphi(a_1) = b_1$, $\varphi(a_2) = b_2$. Wir zeigen, dass $b_1 b_2^{-1} \in \mathrm{Im}(\varphi)$. Dann folgt aus 1.8 die Behauptung. Es gilt:

$$b_1 b_2^{-1} = \varphi(a_1)\varphi(a_2)^{-1} = \varphi(a_1)\varphi(a_2^{-1}) = \varphi(a_1 a_2^{-1}) \in \mathrm{Im}(\varphi).$$

(ii) Seien $a_1, a_2 \in \mathrm{Ker}(\varphi)$ und somit $\varphi(a_1) = \varphi(a_2) = e_H$. Wir zeigen, dass $a_1 a_2^{-1} \in \mathrm{Ker}(\varphi)$. Es gilt:

$$\varphi(a_1 a_2^{-1}) = \varphi(a_1)\varphi(a_2^{-1}) = \varphi(a_1)\varphi(a_2)^{-1} = e_H e_H^{-1} = e_H.$$

Es folgt, dass $a_1 a_2^{-1} \in \mathrm{Ker}(\varphi)$ und somit mit 1.8 die Behauptung. □

Korollar 1.11. Jede Gruppe G ist als Untergruppe in einer symmetrischen Gruppe enthalten.

Beweis. In 1.6 wurde gezeigt, dass ein Monomorphismus existiert, der G in $S(G)$ einbettet. Nach einer Identifikation von G mit dem Bild in $S(G)$ folgt die Aussage. □

Definition 1.12. Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und $a \in G$ beliebig.

(i) Die Menge $aH = \{ab\colon b \in H\}$ heißt eine *Linksnebenklasse von H*.
(ii) Die Menge $Ha = \{ba\colon b \in H\}$ heißt eine *Rechtsnebenklasse von H*.
(iii) Mit G/H bezeichnen wir die Menge der Linksnebenklassen von H.

Bemerkung 1.13. Im Folgenden betrachten wir nur Linksnebenklassen. Alle Aussagen gelten jedoch analog für Rechtsnebenklassen.

Lemma 1.14. Seien aH und bH Linksnebenklassen von H in G. Dann sind folgende Aussagen äquivalent:

(i) $aH = bH$,
(ii) $aH \cap bH \neq \emptyset$,
(iii) $a \in bH$,
(iv) $b^{-1}a \in H$.

Beweis. Gilt (i), so folgt direkt (ii), da $H \neq \emptyset$.

Sei nun (ii) gegeben. Dann existiert ein $c \in aH \cap bH$ und $c = ah_1 = bh_2$ für $h_1, h_2 \in H$. Dann ist $a = bh_2 h_1^{-1} \in bH$ und daher gilt (iii).

Aus (iii) folgt ähnlich (iv). Gelte (iv), etwa $b^{-1}a = h \in H$. Dann ist $a = bh \in bH$ und es folgt $aH \subseteq bH$. Mit $b^{-1}a \in H$ ist auch das inverse Element $(b^{-1}a)^{-1} = a^{-1}b \in H$. Es folgt analog $bH \subseteq aH$ und somit $aH = bH$. □

Definition 1.15. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe von G.

(i) Die *Ordnung* $\mathrm{ord}(G)$ von G ist die Anzahl der Elemente von G.
(ii) Der *Index* $[G : H]$ von H in G ist definiert als die Anzahl der Linksnebenklassen von H.

Satz 1.16. *(Lagrange)* Sei G eine endliche Gruppe und H eine Untergruppe von G. Dann gilt:

$$\mathrm{ord}(G) = [G : H]\mathrm{ord}(H).$$

Beweis. Seien $a_1, \ldots, a_r$ so gewählt, dass $G/H = \{a_1H, \ldots, a_rH\}$ und $a_iH \neq a_jH$. Es folgt, dass

$$G = \bigcup_{i=1}^{r} a_iH.$$

Wegen 1.14 ist diese Vereinigung disjunkt und somit $\mathrm{ord}(G) = \sum_{i=1}^{r} |a_iH|$. Die Abbildung

$$H \longrightarrow a_iH, \quad b \mapsto a_ib$$

ist bijektiv, also gilt $|H| = |a_iH|$. Daher

$$\mathrm{ord}(G) = \sum_{i=1}^{r} |a_iH| = r|H| = [G : H]\mathrm{ord}(H).$$

□

Korollar 1.17. Sei G eine Gruppe mit $\mathrm{ord}(G)$ ist eine Primzahl. Dann besitzt G keine echten Untergruppen, d.h. $\{e\}$ und G sind die einzigen Untergruppen von G.

Definition 1.18. Sei G ein Gruppe und $a \in G$.

(i) Wir bezeichnen mit

$$\mathrm{ord}(a) = \begin{cases} \infty, \text{ falls } a^n \neq e \text{ für alle } n > 0, \\ \inf\{n \in \mathbb{N} \colon a^n = e\}. \end{cases}$$

die *Ordnung* von dem Element a.
(ii) Für $z \in \mathbb{Z}$ ist

$$a^z = \begin{cases} a^z & \text{für } z > 0, \\ e & \text{für } z = 0, \\ (a^{-1})^{-z} & \text{für } z < 0. \end{cases}$$

Lemma 1.19. Sei G eine endliche Gruppe und $a \in G$. Dann gilt:

(i) $\mathrm{ord}(a) < \infty$,
(ii) $\mathrm{ord}(a) | \mathrm{ord}(G)$,
(iii) (kleiner Fermatsche Satz) $a^{\mathrm{ord}(G)} = e$.

Beweis. Zu (i): Die Menge $H = \{a^z : z \in \mathbb{Z}\}$ ist eine Untergruppe von G. Da G endlich ist folgt, dass auch H endlich ist. Somit ist $\mathrm{ord}(a)$ eine endliche Zahl.

Zu (ii): Die Menge $H = \{a, a^2, \ldots, a^{\mathrm{ord}(a)} = e\}$ bildet eine Untergruppe von G. Es gilt $\mathrm{ord}(H) = \mathrm{ord}(a)$. Die Behauptung folgt aus 1.16.

Zu (iii): Es gilt

$$a^{\mathrm{ord}(G)} = (a^{\mathrm{ord}(a)})^{\mathrm{ord}(G)/\mathrm{ord}(a)} = e.$$

□

2. Normalteiler, Faktorgruppen, Isomorphiesätze

Problem: Sei G eine Gruppe. Welche Untergruppen sind Kern eines Gruppenhomomorphismus $\varphi\colon G \to G'$ für eine Gruppe G'.

Sei $H = \mathrm{Ker}(\varphi)$, dann gilt $\mathrm{Ker}(\varphi) = a\mathrm{Ker}(\varphi)a^{-1}$ für alle $a \in G$.

Definition 2.1. Sei G eine Gruppe. Eine Untergruppe $H \subseteq G$ heißt *Normalteiler*, wenn $aHa^{-1} = H$ für alle $a \in G$ gilt. Wir schreiben hierfür $H \triangleleft G$.

Bemerkung 2.2. Die Bedingung lässt sich umschreiben zu $aH = Ha$, d.h. die zugehörigen Links- und Rechtsnebenklassen von H in G stimmen überein.

Konstruktion 2.3. Sei G eine Gruppe und $H \triangleleft G$. Wir erklären auf G/H eine Gruppenstruktur. Sei $aH, bH \in G/H$, dann definieren wir $aH \cdot bH = abH$. Dieses Produkt ist wohldefiniert. Sei $a_1H = a_2H$ und $b_1H = b_2H$. Dann gilt $a_1^{-1}a_2, b_1^{-1}b_2 \in H$ und somit

$$(a_1b_1)^{-1}a_2b_2 = b_1^{-1}a_1^{-1}a_2b_2 = (b_1^{-1}(a_1^{-1}a_2)b_1)(b_1^{-1}b_2) \in H.$$

Also $a_1b_1H = a_2b_2H$. G/H ist zusammen mit dieser Abbildung eine Gruppe (H ist das neutrale Element; $a^{-1}H$ ist das inverse Element zu aH).

Satz 2.4. Sei G eine Gruppe und $H \triangleleft G$. Dann gilt:

(i) G/H ist zusammen mit der Verknüpfung

$$G/H \times G/H \to G/H, \quad aH \times bH \mapsto abH$$

eine Gruppe. Sie heißt die *Faktorgruppe* von G modulo H.

(ii) Die Abbildung

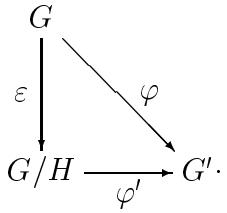
$$\varepsilon\colon G \to G/H, \quad a \mapsto aH$$

ist ein Epimorphismus und heißt der *kanonische Epimorphismus*. Es gilt $\mathrm{Ker}(\varepsilon) = H$.

Korollar 2.5. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Genau dann ist $H \triangleleft G$, wenn $H = \mathrm{Ker}(\varphi)$ für einen geeigneten Gruppenhomomorphismus.

Beweis. Ist $H = \mathrm{Ker}(\varphi)$, so habe wir schon gesehen, dass $H \triangleleft G$. Wenn umgekehrt $H \triangleleft G$ gilt, so ist $H = \mathrm{Ker}(\varepsilon)$, wobei ε der kanonische Epimorphismus von $G \to G/H$ ist. □

Satz 2.6. *(Die universelle Eigenschaft der Faktorgruppe)* Seien G, G' Gruppen, $H \triangleleft G$ und $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus mit $H \subseteq \mathrm{Ker}(\varphi)$. Dann gibt es genau einen Gruppenhomomorphismus $\varphi'\colon G/H \longrightarrow G'$ mit $\varphi = \varphi' \circ \varepsilon$, d.h. folgendes Diagramm ist kommutativ:



Es gilt $\mathrm{Ker}(\varphi') = \mathrm{Ker}(\varphi)/H = \varepsilon(\mathrm{Ker}(\varphi))$ und $\mathrm{Im}(\varphi') = \mathrm{Im}(\varphi)$.

Beweis. Eindeutigkeit von φ': Sei $aH \in G/H$ für ein $a \in G$. Dann ist

$$\varphi'(aH) = \varphi' \circ \varepsilon(a) = \varphi(a).$$

und somit folgt die Behauptung

Existenz von φ': Sei $aH \in G/H$ für ein $a \in G$. Wir definieren $\varphi'(aH) = \varphi(a)$. Als erstes ist zu zeigen, dass φ' wohldefiniert ist. Sei $aH = bH$ für $a, b \in G$, d.h. $a^{-1}b \in H$. Da $H \subseteq \mathrm{Ker}(\varphi)$, folgt $e_{G'} = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b)$. Daher $\varphi(a) = \varphi(b)$.

φ' ist ein Gruppenhomomorphismus: Seien $aH, bH \in G/H$ für $a, b \in G$. Dann gilt

$$\varphi'(aHbH) = \varphi'(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \varphi'(aH)\varphi'(bH).$$

Sei $aH \in \mathrm{Ker}(\varphi')$. Dann gilt $e = \varphi'(aH) = \varphi(a)$ und es folgt $a \in \mathrm{Ker}(\varphi)$. Daher $\mathrm{Ker}(\varphi') \subseteq \mathrm{Ker}(\varphi)/H$. Sei umgekehrt $a \in \mathrm{Ker}(\varphi)$. Es folgt, dass $\varphi'(aH) = \varphi(a) = e$ und somit $\mathrm{Ker}(\varphi') \supseteq \mathrm{Ker}(\varphi)/H$. Insgesamt folgt die Behauptung. □

Korollar 2.7. *(Homomorphiesatz)* Seien G, G' Gruppen und $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus. Dann ist die induzierte Abbildung $\varphi'\colon G/\mathrm{Ker}(\varphi) \longrightarrow \mathrm{Im}(\varphi)$ ein Isomorphismus.

Satz 2.8. Seien G, G' Gruppen und $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus. Dann gilt:

(i) Ist $U' \subseteq G'$ eine Untergruppe von G', so ist $\varphi^{-1}(U')$ eine Untergruppe von G.
(ii) Ist $U' \subseteq G'$ ein Normalteiler von G', so ist $\varphi^{-1}(U')$ ein Normalteiler von G.
(iii) Ist $U \subseteq G$ eine Untergruppe, so ist $\varphi(U)$ eine Untergruppe von G'.
(iv) Ist $U \subseteq G$ ein Normalteiler und φ surjektiv, so ist $\varphi(U)$ ein Normalteiler von G'.
(v) Ist φ surjektiv, so induziert φ eine Bijektion der Menge aller Untergruppen (Normalteiler) von G, die $\mathrm{Ker}(\varphi)$ umfassen, auf die Menge aller Untergruppen (Normalteiler) von G'.

Beweis. Wir zeigen:

(i) Seien $a, b \in \varphi^{-1}(U')$. Dann ist $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} \in U'$. Daher ist $ab^{-1} \in \varphi^{-1}(U')$ und nach dem Untergruppenkriterium 1.8 ist $\varphi^{-1}(U')$ eine Untergruppe.

(ii) Sei $a \in G$ und $b \in \varphi^{-1}(U')$ beliebig. Es ist $\varphi(aba^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1} \in U'$, da U' ein Normalteiler ist. Es folgt, dass $a\varphi^{-1}(U')a^{-1} \subseteq \varphi^{-1}(U')$ und daher $a\varphi^{-1}(U')a^{-1} = \varphi^{-1}(U')$. Also ist $\varphi^{-1}(U')$ ein Normalteiler von G.

(iii) Seien $a', b' \in \varphi(U)$ mit $\varphi(a) = a'$ und $\varphi(b) = b'$. Dann ist $a'(b')^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \in \varphi(U)$, da $ab^{-1} \in U$ gilt. Wieder nach dem Untergruppenkriterium folgt, dass $\varphi(U)$ eine Untergruppe ist.

(iv) Seien $a' \in G'$ und $b' \in \varphi(U)$ mit $b' = \varphi(b)$. Die Abbildung φ ist surjektiv und es folgt, dass ein $a \in G$ existiert mit $\varphi(a) = a'$. Dann ist $a'b'(a')^{-1} = \varphi(a)\varphi(b)\varphi(a)^{-1} = \varphi(aba^{-1}) \in \varphi(U)$, da U ein Normalteiler ist und daher $aba^{-1} \in U$ gilt. Es folgt, dass $a'\varphi(U)(a')^{-1} \subseteq \varphi(U)$ und somit $a'\varphi(U)(a')^{-1} = \varphi(U)$. Daraus folgt die Behauptung.

(v) Behauptung: Für eine Untergruppe $\mathrm{Ker}(\varphi) \subseteq U \subseteq G$ ist $U = \varphi^{-1}(\varphi(U))$. Es gilt immer $U \subseteq \varphi^{-1}(\varphi(U))$. Sei $a \in \varphi^{-1}(\varphi(U))$. Da $\varphi(a) \in \varphi(U)$, existiert ein $b \in U$ mit $\varphi(a) = \varphi(b)$. Daher

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(a)^{-1} = e_{G'}$$

und somit $ab^{-1} = c \in \mathrm{Ker}(\varphi) \subseteq U$. Es folgt $a = cb \in U$ und dies zeigt die Behauptung.

Da φ surjektiv ist, gilt analog für jede Untergruppe $V \subseteq G'$, dass $V = \varphi(\varphi^{-1}(V))$. Dies zeigt (v).

□

Satz 2.9. *(1. Isomorphiesatz)* Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe, $N \triangleleft G$. Dann gilt:

(i) $HN = \{ab\colon a \in H, b \in N\}$ ist eine Untergruppe von G.

(ii) $N \triangleleft HN$.

(iii) Der kanonische Homomorphismus $\varepsilon\colon H \longrightarrow HN/N, a \mapsto aN$ ist ein Epimorphismus mit $\mathrm{Ker}(\varepsilon) = H \cap N$. Insbesondere ist $H \cap N \triangleleft H$ und

$$H/(H \cap N) \cong HN/N.$$

Beweis. Zu (i): Sei $a_1b_1, a_2b_2 \in HN$ mit $a_1, a_2 \in H$ und $b_1, b_2 \in N$. Dann ist

$$a_1b_1(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} = (a_1a_2^{-1})(a_2(b_1b_2^{-1})a_2^{-1}) \in HN.$$

Aus dem Untergruppenkriterium 1.8 folgt die Behauptung.

Zu (ii): Es gilt $N \triangleleft HN$, da $N \triangleleft G$ vorausgesetzt wurde.

Zu (iii): Nach (ii) gilt $N \triangleleft HN$ und somit ist HN/N eine Gruppe. Es ist leicht zu überprüfen, dass ε ein Gruppenhomomorphismus ist. Sei nun $aN \in HN/N$ beliebig mit $a = bc \in HN$ für ein $b \in H$ und $c \in N$. Dann gilt

$$aN = bcN = (bN)(cN) = bN = \varepsilon(b).$$

Somit ist ε ein Epimorphismus. Als nächstes zeigen wir $\mathrm{Ker}(\varepsilon) = H \cap N$. Es gilt $H \cap N \subseteq N \subseteq \mathrm{Ker}(\varepsilon)$. Sei nun $a \in \mathrm{Ker}(\varepsilon) \subseteq H$. Dann ist $N = \varepsilon(a) = aN$ und

daher $a \in N$. Es folgt, dass $a \in H \cap N$ und insgesamt $H \cap N = \mathrm{Ker}(\varepsilon)$. Nach dem Homomorphiesatz 2.7 gilt nun $H/(H \cap N) \cong HN/N$. □

Beispiel 2.10. Sei $G = S_3$, $H = \{id, (1,2)\}$, $N = \{id, (1,2,3), (1,3,2)\}$. Dann ist H kein Normalteiler und N ist ein Normalteiler von G. Es gilt $HN = G$ und $H \cap N = \{id\}$. Nach dem 1. Isomorphiesatz folgt

$$S_3/N = HN/N \cong H/H \cap N = H.$$

Satz 2.11. *(2. Isomorphiesatz)* Sei G eine Gruppe, $H \triangleleft G$, $N \triangleleft G$ und $N \subseteq H$. Dann gibt es einen kanonischen Epimorphismus $\varepsilon\colon G/N \to G/H$ mit $\mathrm{Ker}(\varepsilon) = H/N$. Insbesondere gilt

$$(G/N)/(H/N) \cong G/H.$$

Beweis. Definiere ε wie folgt:

$$\varepsilon\colon G/N \to G/H, aN \mapsto aH.$$

Da $N \subseteq H$ gilt, ist diese Abbildung wohldefiniert und man sieht leicht, dass ε ein Epimorphismus ist. Es bleibt zu zeigen, dass $\mathrm{Ker}(\varepsilon) = H/N$ gilt. Sei $aN \in H/N$ mit $a \in H$. Dann gilt $\varepsilon(aN) = aH = H$ und somit $aN \in \mathrm{Ker}(\varepsilon)$. Sei nun $aN \in \mathrm{Ker}(\varepsilon)$, dann ist $H = \varepsilon(aN) = aH$ und daher $a \in H$. Es folgt, dass $\mathrm{Ker}(\varepsilon) = H/N$. Nach dem Homomorphiesatz 2.7 gilt nun $(G/N)/(H/N) \cong G/H$. □

3. Zyklische Gruppen

Konstruktion und Definition 3.1. Sei G eine Gruppe und $\emptyset \neq S \subset G$ ein Teilmenge. Wir bezeichnen mit $\langle S \rangle$ die kleinste Untergruppe von G, die S enthält. Man überlegt sich, dass

$$\langle S \rangle = \bigcap_{S \subseteq U \subseteq G,\ U \text{ Untergruppe}} U$$

$$= \{a \in G\colon \text{ Es gibt } a_1, \ldots, a_r \in G \text{ und } \varepsilon_1, \ldots, \varepsilon_r \in \{1, -1\} \text{ mit } a = a_1^{\varepsilon_1} \cdots a_r^{\varepsilon_r}\}.$$

$\langle S \rangle$ heißt die von S erzeugte Untergruppe. Ist $S = \{a\}$, so schreiben wir kurz $\langle a \rangle (= \{a^z\colon z \in \mathbb{Z}\})$. Die Gruppe $\langle a \rangle$ heißt die von a erzeugte *zyklische Untergruppe* von G. Ist $G = \langle a \rangle$, so heißt G eine *zyklische Gruppe*.

Korollar 3.2. Jede zyklische Gruppe ist abelsch.

Beispiele 3.3. Es gilt:

(i) Die ganzen Zahlen $\mathbb{Z}$ zusammen mit der Addition sind eine zyklische Gruppe.

(ii) Sei G eine endliche Gruppe und $a \in G$. Die Untergruppe

$$\{a, a^2, \ldots, a^{\mathrm{ord}(a)} = e\}$$

ist zyklisch.

(iii) Sei $n \in \mathbb{N}$ und Z_n die von $(1, \ldots, n)$ erzeugte Untergruppe von S_n. Dann ist Z_n zyklisch von der Ordnung n. Insbesondere ist für jede Primzahl p die zyklische Gruppe Z_p von der Ordnung p. Der folgende Satz zeigt, dass es keine weiteren Gruppen von Primzahlordnung existieren.

Satz 3.4. Sei p eine Primzahl und G eine Gruppe der Ordnung p. Dann ist G isomorph zu Z_p.

Beweis. Sei $e \neq a \in G$. Dann ist $\mathrm{ord}(a) = p$, da $\mathrm{ord}(a)|p$ gilt. Insbesondere ist $G = \langle a \rangle$ zyklisch. Betrachte den Homomorphismus

$$Z_n \longrightarrow G, \quad (1, \ldots, p)^i \mapsto a^i.$$

Dies ist ein Isomorphismus und beweist den Satz. □

Lemma 3.5. Sei $H \subseteq \mathbb{Z}$ eine Untergruppe. Dann existiert ein $m \in \mathbb{Z}$ mit $H = m\mathbb{Z}$. Insbesondere ist H eine zyklische Gruppe.

Beweis. Ist $H = \{0\}$, so können wir $m = 0$ wählen. Sei also $H \neq \{0\}$. Mit $z \in H$ ist auch $-z \in H$, also existieren positive Zahlen in H. Sei m die kleinste positive Zahl in H. Wir behaupten, dass $m\mathbb{Z} = H$. Es gilt immer $m\mathbb{Z} \subseteq H$. Sei nun $a \in H$. Dividiere a durch m mit Rest, d.h. es existieren zwei Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < m$ und $a = qm + r$. Wegen $r = a - qm \in H$ und der Wahl von m folgt $r = 0$, also $a = qm$. Somit gilt $m\mathbb{Z} = H$. □

Satz 3.6. Sei G eine zyklische Gruppe. Dann gilt:

$$G \cong \begin{cases} \mathbb{Z}, & \text{falls } \mathrm{ord}(G) = \infty, \\ \mathbb{Z}/m\mathbb{Z}, & \text{falls } \mathrm{ord}(G) < \infty. \end{cases}$$

Insbesondere existiert zu jedem $n \in \mathbb{N}$ eine zyklische Gruppe der Ordnung n.

Beweis. Mit Hilfe von 2.7 und 3.5 lässt sich die Behauptung leicht beweisen. □

Satz 3.7. Sei G eine zyklische Gruppe. Dann gilt:

(i) Ist $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus für eine Gruppe G', so sind $\mathrm{Ker}(\varphi)$ und $\mathrm{Im}(\varphi)$ zyklische Gruppen.
(ii) Jede Untergruppe $H \subseteq G$ ist zyklisch.

Beweis. Zu (i): Sei $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus. Es folgt aus der Definition einer zyklischen Gruppe, dass $\mathrm{Im}(\varphi)$ zyklisch ist. $\mathrm{Ker}(\varphi) \subseteq G$ ist eine Untergruppe von G und somit bleibt (ii) zu zeigen.

Zu (ii): Sei G eine zyklische Gruppe und $H \subseteq G$ eine Untergruppe. Sei ferner $\varepsilon\colon \mathbb{Z} \longrightarrow G$ ein Epimorphismus. $\varepsilon^{-1}(H)$ ist eine Untergruppe von $\mathbb{Z}$ und somit zyklisch nach 3.5. Dann ist $H = \varepsilon(\varepsilon^{-1}(H))$ wieder zyklisch. □

KAPITEL 2

Ringtheorie

1. Grundbegriffe der Ringtheorie

Definition 1.1. Ein *Ring* ist eine Menge R zusammen mit zwei Verknüpfungen $+\colon R \longrightarrow R$ (Addition) und $\cdot\colon R \longrightarrow R$ (Multiplikation), so dass folgende Bedingungen erfüllt sind:

(i) $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0.
(ii) $\cdot$ ist assoziativ, d.h. für alle $a, b, c \in R$ gilt $(ab)c = a(bc)$.
(iii) Es gelten die Distributivgesetze, d.h. für alle $a, b, c \in R$ gilt $a(b+c) = ab+ac$ und $(b + c)a = ba + ca$.

Der Ring heißt *Ring mit 1*, wenn ein Element $1 \in R$ existiert, so dass für alle $a \in R$ gilt $1a = a = a1$. Der Ring heißt *kommutativ*, wenn für alle $a, b \in R$ gilt $ab = ba$.

Bemerkung 1.2. In einem Ring kann auch $1 = 0$ gelten, z.B. wenn $R = \{0\}$. Es gelten die Rechenregeln:

(i) 0a=a0=0,
(ii) a(-b)=-ab=(-a)b,
(iii) (-a)(-b)=ab,
(iv) ...

Vorsicht, es gilt nicht in jedem Ring die Kürzungsregel. Wir betrachten im Folgenden nur kommutative Ringe $R \neq \emptyset$ mit 1.

Definition 1.3. Sei R ein Ring.

(i) Ein Element $a \in R$ heißt *Nullteiler*, wenn ein $0 \neq b \in R$ existiert mit $ab = 0$.
(ii) R heißt ein *Integritätsbereich (oder nullteilerfrei)*, wenn R keine Nullteiler außer 0 besitzt.
(iii) Ein Element $a \in R$ heißt *Einheit*, wenn ein $b \in R$ existiert mit $ab = 1$.
(iv) Die Menge der Einheiten E_R von R bildet hinsichtlich der Multiplikation eine Gruppe. Sie heißt die *Einheitengruppe* von R.
(v) $S \subseteq R$ heißt ein *Unterring* von R, wenn S mit der induzierten Verknüpfung von R ein Ring ist. Das Paar $S \subseteq R$ heißt dann eine *Ringerweiterung*.

Beispiele 1.4. Betrachte:

(i) $\mathbb{Z}$ ist ein Integritätsring mit $E_{\mathbb{Z}} = \{-1, 1\}$.
(ii) R ist ein Körper genau dann, wenn $E_R = R \setminus \{0\}$.
(iii) Seien $R_1, \ldots, R_n$ Ringe. Dann ist $R = R_1 \times \ldots \times R_n$ mit komponentenweiser Addition und Multiplikation ein Ring. Es gilt $1_R = (1_{R_1}, \ldots, 1_{R_n})$, $0_R = (0_{R_1}, \ldots, 0_{R_n})$ und $E_R = E_{R_1} \times \cdots \times E_{R_n}$. Für $n \geq 2$ ist R kein

Integritätsbereich, da

$$(0,1,0,\dots)(1,0,0,\dots) = (0,0,0,\dots).$$

Definition 1.5. Seien R und S Ringe. Eine Abbildung $\varphi\colon R \longrightarrow S$ heißt ein *Ringhomomorphismus*, wenn für alle $a, b \in R$ gilt

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b) \text{ und } \varphi(1) = 1.$$

Ein Ringhomomorphismus φ heißt

(i) *Monomorphismus*, wenn φ injektiv ist.
(ii) *Epimorphismus*, wenn φ surjektiv ist.
(iii) *Isomorphismus*, wenn φ bijektiv ist.

Die Ringe R, S sind *isomorph*, wenn φ ein Isomorphismus ist. Man schreibt dann $R \cong S$.

Definition 1.6. Seien R, S Ringe und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus.

(i) Die Menge $\mathrm{Ker}(\varphi) = \{a \in R\colon \varphi(a) = 0\}$ heißt der *Kern* von φ.
(ii) Die Menge $\mathrm{Im}(\varphi) = \{\varphi(a) \in S\colon a \in R\}$ heißt das *Bild* von φ.

Bemerkung 1.7. Es gilt:

(i) $\mathrm{Im}(\varphi)$ ist ein Unterring von S.
(ii) $\mathrm{Ker}(\varphi)$ ist i.A. kein Unterring von R, da i.A. $1 \notin \mathrm{Ker}(\varphi)$.
(iii) φ induziert einen Gruppenhomomorphismus $E_R \longrightarrow E_S$ zwischen den Einheitengruppen von R und S.

Definition 1.8. Sei R ein Ring. Eine Teilmenge $I \subseteq R$ heißt ein *Ideal*, wenn:

(i) $(I, +)$ ist eine Untergruppe von $(R, +)$.
(ii) Für alle $a \in R$ und $b \in I$ gilt $ab \in I$.

Beispiele 1.9. Sei R ein Ring.

(i) $\{0\}$ und R sind die trivialen Ideale von R.
(ii) R ist ein Körper genau dann, wenn $\{0\}$ und R die einzigen Ideale von R sind.
(iii) Sei S ein weiterer Ring und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus. Dann ist $\mathrm{Ker}(\varphi)$ ein Ideal von R. Ist insbesondere R ein Körper, so ist φ entweder die Nullabbildung oder injektiv.
(iv) Genau die Mengen $n\mathbb{Z}$ sind die Ideale von $\mathbb{Z}$.
(v) Ein Ideal von der Form $(a) = \{ra\colon r \in R\}$ heißt *Hauptideal* von R.

Lemma und Definition 1.10. Sei R ein Ring und $(J_i)_{i\in I}$ eine Familie von Idealen von R. Dann gilt:

(i) Der *Durchschnitt* $\bigcap_{i\in I} J_i$ ist ein Ideal von R.
(ii) Die *Summe* $\sum_{i\in I} J_i = \{\sum_{i\in I} a_i\colon a_i \in J_i, \text{ fast alle } a_i = 0\}$ ist ein Ideal von R.

Beispiel 1.11. Sei R ein Ring und I, J Ideale in R. Dann ist $I + J = \{a + b\colon a \in I, b \in J\}$. Z.B. $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.

Definition 1.12. Sei R ein Ring und $\{a_i\}_{i\in I}$ eine Familie von Elementen von R. Das von dieser Familie erzeugte Ideal ist das kleinste Ideal, das alle a_i enthält. Es

wird mit $(a_i)_{i\in I}$ bezeichnet. Wird J von $a_1, \dots, a_n \in R$ erzeugt, so schreibt man $J = (a_1, \dots, a_n) = \{\sum_{i=1}^n r_i a_i : r_i \in R\}$.

Definition 1.13. Sei R ein Ring und $J_1, \dots, J_n$ Ideale von R. Dann ist

$$J_1 \cdots J_n = (a_1 \cdots a_n : a_i \in J_i)$$

das *Produkt* der Ideale $J_1, \dots, J_n$.

Lemma 1.14. Sei R ein Ring und I, J, J' Ideale von R. Dann gilt:

(i) $I(JJ') = (IJ)J'$.
(ii) $IJ \subseteq I \cap J$.

Bemerkung 1.15. In 1.14 (ii) gilt im Allgemeinen keine Gleichheit. Zum Beispiel: $(4)(6) = (24)$ und $(4) \cap (6) = (12)$.

Definition 1.16. Ein Ring R heißt *Hauptidealring*, wenn jedes Ideal I von R ein Hauptideal ist, d.h. $I = (a)$ für ein $a \in R$.

Satz 1.17. Der Ring $\mathbb{Z}$ ist ein Hauptidealring.

Beweis. Sei $I \subseteq \mathbb{Z}$ ein Ideal. Dann ist $(I, +)$ eine Untergruppe von $(\mathbb{Z}, +)$, also hat I nach Kapitel 1, 3.5 die Gestalt $n\mathbb{Z} = (n)$ für ein $n \in \mathbb{Z}$. Die zeigt die Behauptung. □

2. Restklassen- und Quotientenringe

Konstruktion 2.1. Sei R ein Ring und $I \subseteq R$ ein Ideal. Sei $R/I = \{a + I : a \in R\}$. Da I ein Normalteiler von R ist, ist dies eine (additive) Gruppe. Wir erklären nun auch ein Produkt auf R/I. Seien $a_1 + I, a_2 + I \in R/I$. Setze $(a_1 + I)(a_2 + I) = a_1a_2 + I$. Diese Definition ist unabhängig von der Wahl der Repräsentanten. Seien etwa $a_1 + I = b_1 + I$ und $a_2 + I = b_2 + I$, d.h. $a_1 - b_1 = c_1 \in I$ und $a_2 - b_2 = c_2 \in I$. Dann gilt

$$b_1b_2 = (a_1 - c_1)(a_2 - c_2) = a_1a_2 + (c_1c_2 - a_1c_2 - a_2c_1) \in a_1a_2 + I.$$

Daraus folgt, dass $a_1a_2 + I = b_1b_2 + I$. Man sieht nun leicht, dass R/I ein Ring ist. Dieser Ring heißt der *Restklassenring (Faktorring) von R modulo I*.

Bemerkung 2.2. Für $a + I = b + I$ schreibt man auch $a \equiv b \mod I$.

Satz 2.3. Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann gilt:

(i) Die Abbildung $\varepsilon : R \to R/I$ ist ein surjektiver Ringhomomorphismus und $\mathrm{Ker}(\varepsilon) = I$. ε heißt der kanonische Epimorphismus.
(ii) (Die universelle Eigenschaft des Restklassenrings) Sei S ein weiterer Ring und $\varphi : R \to S$ ein Ringhomomorphismus mit $I \subseteq \mathrm{Ker}(\varphi)$. Dann existiert genau ein Ringhomomorphismus $\varphi' : R/I \to S$ mit $\varphi = \varphi' \circ \varepsilon$. Es gilt $\mathrm{Im}(\varphi') = \mathrm{Im}(\varphi)$ und $\mathrm{Ker}(\varphi') = \mathrm{Ker}(\varphi)/I \subseteq R/I$.

Beweis. Der Beweis verläuft analog zu dem entsprechenden Beweis in der Gruppentheorie (Die universelle Eigenschaft der Faktorgruppe). □

Korollar 2.4. Es gilt:

(i) (Homomorphiesatz) Seien R, S Ringe und $\varphi : R \to S$ ein (Ring-) Epimorphismus. Dann gilt $R/\mathrm{Ker}(\varphi) \simeq S$.

(ii) (Isomorphiesatz) Sei R ein Ring und $I, J \subseteq R$ Ideale mit $J \subseteq I$. Dann gilt $R/I \simeq (R/J)/(I/J)$.

Beweis. Die Beweise verlaufen analog zu den entsprechenden Beweisen in der Gruppentheorie. □

Definition 2.5. Sei R ein Ring und $I, J \subseteq R$ Ideale. I und J heißen *teilerfremd (koprim)*, wenn $I + J = R$ gilt.

Bemerkung 2.6. In der Zahlentheorie wird meist folgender Satz bewiesen. Für zwei Zahlen $m, n \in \mathbb{Z}$ gilt $(m) + (n) = \mathbb{Z}$ genau dann, wenn n und m teilerfremd sind.

Satz 2.7. *(Chinesischer Restsatz)* Sei R ein Ring und $I_1, \ldots, I_n$ paarweise teilerfremde Ideale von R. Dann ist die Abbildung

$$\varphi\colon R \longrightarrow R/I_1 \times \cdots \times R/I_n, \quad a \mapsto (a + I_1, \ldots, a + I_n)$$

ein Epimorphismus mit $\mathrm{Ker}(\varphi) = \bigcap_{i=1}^{n} I_i$. Insbesondere gilt

$$R/(\bigcap_{i=1}^{n} I_i) \simeq R/I_1 \times \cdots \times R/I_n.$$

Beweis. Man sieht leicht, dass φ ein Ringhomomorphismus ist und das $\mathrm{Ker}(\varphi) = \bigcap_{i=1}^{n} I_i$ gilt. Es bleibt zu zeigen, dass φ surjektiv ist.

Behauptung: Für $i = 1, \ldots, n$ existieren Elemente x_i mit $x_i \equiv 1 \mod I_i$ und $x_i \equiv 0 \mod I_j$ für $j \neq i$. Ist dann $(a_1 + I_1, \ldots, a_n + I_n) \in R/I_1 \times \cdots \times R/I_n$ beliebig gewählt, dann gilt

$$\varphi(a_1 x_1 + \cdots + a_n x_n) = (a_1 x_1 + I_1, \ldots, a_n x_n + I_n) = (a_1 + I_1, \ldots, a_n + I_n)$$

und somit ist φ surjektiv. Es bleibt die Behauptung zu zeigen. Sei im Folgenden $i \in \{1, \ldots, n\}$ fest gewählt. Für $j \neq i$ gilt nach Voraussetzung $I_i + I_j = R$, also existiert ein $a_j \in I_i$ und $b_j \in I_j$ mit $a_j + b_j = 1$. Dann gilt

$$1 = \prod_{j \neq i} (a_j + b_j) = c_i + x_i \text{ mit } c_i \in I_i \text{ und } x_i \in \prod_{j \neq i} I_j.$$

Es gilt $x_i - 1 = c_i \in I_i$, $x_i \in I_j$ für $j \neq i$. Also $x_i \equiv 1 \mod I_i$ und $x_i \equiv 0 \mod I_j$ für $j \neq i$. □

Korollar 2.8. Seien $b_1, \ldots, b_n \in \mathbb{Z}$ paarweise teilerfremde Zahlen. Dann ist das simultane Kongruenzsystem $x \equiv a_i \mod (b_i)$ für $i = 1, \ldots, n$ und beliebige Zahlen $a_1, \ldots, a_n \in \mathbb{Z}$ lösbar. Die Lösung ist eindeutig modulo $b_1 \cdots b_n$.

Beweis. Für beliebige i, j gilt $(b_i) + (b_j) = \mathbb{Z}$ und $(b_i b_j) = b_i \cap b_j$. Nun folgt die Behauptung aus 2.7. □

Bemerkung 2.9. Der Beweis von 2.7 zeigt auch, wie eine Lösung in 2.8 gewonnen werden kann.

Definition 2.10. Sei R ein Ring. Ein Ideal $P \subseteq R$ heißt *Primideal*, wenn $P \neq R$ und wenn für alle $a, b \in R$ mit $ab \in P$ folgt, dass $a \in P$ oder $b \in P$ gilt.

Lemma 2.11. Sei $n \in \mathbb{Z}, n > 1$. Dann ist (n) genau dann ein Primideal, wenn n eine Primzahl ist.

Beweis. Sei (n) ein Primideal, $n = dm$ für $d, m \in \mathbb{Z}$ und o.E. $d > 1, m \geq 1$. Dann ist $dm \in (n)$. Es folgt, dass $d \in (n)$ oder $m \in (n)$. Da $1 \leq m = n/d < n$, gilt $m \notin (n)$. Somit $d = cn \in (n)$. Nun folgt $d = cn = cdm$, also $1 = cm$ und daher $1 = c$. Insgesamt gilt $d = n$. Es folgt, dass n eine Primzahl ist.

Sei nun n eine Primzahl. Ist $ab \in (n)$ für $a, b \in \mathbb{Z}$, dann gilt $n|ab$. Da n eine Primzahl ist, folgt $n|a$ oder $n|b$. Also $a \in (n)$ oder $b \in (n)$. □

Satz 2.12. Sei R ein Ring und $P \subseteq R$ ein Ideal. Folgende Aussagen sind äquivalent:

(i) P ist ein Primideal,
(ii) R/P ist ein Integritätsbereich.

Beweis. (i) ⇒ (ii): Sei $P \neq a + P, b + P \in R/P$. Also gilt $a \notin P$ und $b \notin P$. Da P ein Primideal ist, folgt $ab \notin P$, also $ab + P \neq P$.

(ii) ⇒ (i): Seien $a, b \in R$ mit $ab \in P$. Es folgt, dass $P = ab + P = (a + P)(b + P)$. Da R/P ein Integritätsbereich ist, gilt $a + P = P$ oder $b + P = P$. Dies ist äquivalent zu $a \in P$ oder $b \in P$. □

Definition 2.13. Sei R ein Ring. Ein Ideal $M \subseteq R$ heißt ein *maximales Ideal*, wenn $M \neq R$ und für alle Ideale $I \subseteq R$ mit $M \subseteq I$ folgt, dass $I = M$ oder $I = R$ gilt.

Lemma 2.14. *(Zorn)* Sei $\mathcal{M} \neq \emptyset$ eine partiell geordnete Menge. Besitzt jede total geordnete Teilmenge von $\mathcal{M}$ eine obere Schranke in $\mathcal{M}$, dann besitzt $\mathcal{M}$ ein maximales Element.

Satz 2.15. Sei R ein Ring und $I \neq R$ ein Ideal. Dann existiert ein maximales Ideal $M \subseteq R$ mit $I \subseteq M$.

Beweis. Sei $\mathcal{M}$ die Menge der Ideale $J \neq R$ mit $I \subseteq J$. Dann ist $\mathcal{M} \neq \emptyset$, da $I \in \mathcal{M}$. Mit der Inklusion ist $\mathcal{M}$ partiell geordnet. Sei $(J_k)_{k \in K}$ eine vollständig geordnete Teilmenge von $\mathcal{M}$. Man sieht leicht, dass $I \subseteq \bigcup_{i \in K} J_i = J$ ein Ideal ist. Angenommen $J = R$. Dann wäre $1 \in J$ und somit $1 \in J_k$ für ein $k \in K$. Dann ist $J_k = R$ ein Widerspruch. Also gilt $J \neq R$ und es ist $J \in \mathcal{M}$ eine obere Schranke für $(J_k)_{k \in K}$.

Nach 2.14 besitzt $\mathcal{M}$ ein maximales Element M. Dieses Element ist dann das gesuchte maximale Ideal. □

Satz 2.16. Sei R ein Ring und $M \subseteq R$ ein Ideal. Folgende Aussagen sind äquivalent:

(i) M ist ein maximales Ideal,
(ii) R/M ist ein Körper.

Beweis. (i) ⇒ (ii): Sei M ein maximales Ideal. Sei $0 \neq a + M \in R/M$ beliebig mit $a \notin M$. Betrachte das Ideal $M \subseteq J = M + (a)$. Es gilt $J \neq M$ und daher $J = R$. Dann ist $1 \in J$, d. h. es existiert ein $b \in R$ und ein $c \in M$ mit $1 = ba + c$. Somit ist $(b + M)(a + M) = ba + M = 1 + M$. Also ist $b + M$ das inverse Element zu $a + M$ und R/M ist ein Körper.

(ii) ⇒ (i): Sei $M \subseteq J \subseteq R$ ein Ideal mit $M \neq J$. Sei $a \in J \setminus M$. Dann ist $a + M \neq M$ in R/M. Da R/M ein Körper ist, existiert ein $b \in R$ mit $(b + M)(a + M) =$

$ba + M = 1 + M$. Es folgt, dass $1 - ba \in M$, also $1 \in (a) + M \subseteq J$. Somit $J = R$ und M ist ein maximales Ideal. □

Korollar 2.17. Maximale Ideale sind Primideale.

Beweis. Sei M ein maximales Ideal in einem Ring R. Nach 2.16 ist R/M ein Körper, also insbesondere ein Integritätsbereich. Aus 2.12 folgt, dass M ein Primideal ist. □

Beispiel 2.18. Maximale in $\mathbb{Z}$ sind die Ideale (p) für eine Primzahl p. Das Ideal (0) ist das einzige Primideal in $\mathbb{Z}$, das nicht maximal ist.

Satz 2.19. Sei R ein Ring. Folgende Aussagen sind äquivalent:

(i) (0) ist ein Primideal,
(ii) R ist ein Integritätsbereich.

Beweis. Betrachte die Abbildung $id\colon R \to R$. Es ist $\mathrm{Ker}(id) = (0)$ und nach dem Homomorphiesatz gilt $R \cong R/(0)$. Die Behauptung folgt aus 2.12. □

Satz 2.20. Sei R ein Integritätsbereich mit endlich vielen Elementen. Dann ist R ein Körper.

Beweis. Sei $0 \neq a \in R$ beliebig. Die Abbildung $\varphi_a : R \to R, b \mapsto ab$ ist injektiv, da R ein Integritätsbereich ist. Da $|R| < \infty$ folgt, dass φ_a bijektiv ist. Somit $1 \in \mathrm{Im}(\varphi_a)$, d.h. es existiert ein $b \in R$ mit $1 = ba$. Dies zeigt die Behauptung. □

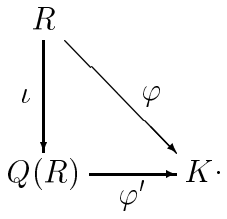
Konstruktion 2.21. *(Quotientenringe)* Sei R ein Integritätsbereich, $T = R \setminus \{0\}$. Wir definieren auf der Menge der Paare $\{(a,b)\colon a \in R, b \in T\}$ eine Äquivalenzrelation: $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = a_2 b_1$. Die Äquivalenzklasse (a,b) wird mit $\frac{a}{b}$ bezeichnet. Die Menge der Äquivalenzklassen bezeichnen wir mit $Q(R)$. Definiere Addition und Multiplikation auf $Q(R)$ wie folgt:

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2} \text{ und } \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}.$$

Die Definitionen sind unabhängig von der Wahl der Repräsentanten und $(Q(R), +, \cdot)$ ist ein Körper mit $\frac{1}{1}$ als Einselement, ...

Satz 2.22. Sei R ein Integritätsbereich. Dann gilt:

(i) $(Q(R), +, \cdot)$ ist ein Körper.
(ii) Die Abbildung $\iota\colon R \to Q(R), a \mapsto \frac{a}{1}$ ist ein Monomorphismus und wird die kanonische Einbettung genannt.
(iii) (Universelle Eigenschaft des Quotientenkörpers) Sei $\varphi\colon R \to K$ ein Ringhomomorphismus in einen Körper K. Dann gibt es genau einen Körperhomomorphismus $\varphi'\colon Q(R) \to K$ mit $\varphi = \varphi' \circ \iota$, d.h. folgendes Diagramm ist kommutativ:



Beweis. Eindeutigkeit: Sei $\frac{a}{b} \in Q(R)$ beliebig. Dann gilt

$$\varphi'(\frac{a}{b}) = \varphi'(\frac{a}{1} \cdot \frac{1}{b}) = \varphi'(\frac{a}{1} \cdot (\frac{b}{1})^{-1}) = \varphi'(\frac{a}{1}) \cdot \varphi'(\frac{b}{1})^{-1}$$
$$= \varphi'(\iota(a)) \cdot \varphi'(\iota(b))^{-1} = \varphi(a) \cdot \varphi(b)^{-1}.$$

Existenz: Zeige, dass die Abbildung φ' mit $\varphi'(\frac{a}{b}) = \varphi(a) \cdot \varphi(b)^{-1}$ die gewünschten Eigenschaften hat. □

3. Teilbarkeitstheorie in Integritätsbereichen

Definition 3.1. Sei R ein Integritätsbereich und $a, b \in R$. Das Element a heißt ein *Teiler* von b, wenn ein $c \in R$ existiert mit $b = ac$. Man schreibt hierfür $a|b$. Das Element a heißt *assoziiert* zu b, wenn $a|b$ und $b|a$ gilt. Dies wird mit $a \sim b$ bezeichnet (Bemerkung: $\sim$ ist eine Äquivalenzrelation).

Lemma 3.2. Sei R ein Integritätsbereich und $a, b, c, d \in R$. Dann gelten folgende Rechenregeln:

(i) $a|b$ und $b|c \Rightarrow a|c$.
(ii) $a|b$ und $a|c \Rightarrow a|b \pm c$.
(iii) $a|b$ und $a|b + c \Rightarrow a|c$.
(iv) $a|b$ und $c|d \Rightarrow ac|bd$.
(v) $a|b \Leftrightarrow (a) \supseteq (b)$.
(vi) $a \sim b \Leftrightarrow (a) = (b) \Leftrightarrow a = cb$ mit $c \in E_R$.

Beweis. Diese Regeln rechnet man leicht nach. □

Definition 3.3. Sei R ein Integritätsbereich. Ein Element $0 \neq a \in R \setminus E_R$ heißt *irreduzibel*, wenn für $b, c \in R$ mit $a = bc$ stets $b \in E_R$ oder $c \in E_R$ gilt.

Satz 3.4. Sei R ein Integritätsbereich und Hauptidealring. Für ein $0 \neq a \in R$ sind folgende Aussagen äquivalent:

(i) a ist irreduzibel,
(ii) (a) ist ein maximales Ideal.

Beweis. (i) $\Rightarrow$ (ii): Sei $(a) \subseteq (b) \subseteq R$ ein Ideal mit $b \in R$. Da $a \in (b)$ existiert ein $c \in R$ mit $a = bc$. Nun folgt wegen der Irreduzibilität von a, dass $b \in E_R$ oder $c \in E_R$. Dies ist äquivalent zu $(b) = R$ oder $(a) = (b)$. Daher ist (a) ein maximales Ideal.

(ii) $\Rightarrow$ (i): Sei $a = bc$ mit $b, c \in R$. Nun gilt $(a) \subseteq (b) \subseteq R$. Da (a) ein maximales Ideal ist, folgt $(a) = (b)$ oder $(b) = R$. Gilt $(b) = R$, dann ist $b \in E_R$, da dann $1 \in (b)$. Sonst ist $(a) = (b)$, also existiert ein $d \in R$ mit $ad = b$. Es folgt, dass $a = bc = adc$ und somit $1 = dc$. Daher gilt $c \in E_R$. Insgesamt folgt die Behauptung. □

Definition 3.5. Sei R ein Integritätsbereich. Eine Folge von Elementen $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in R \setminus \{0\}$ heißt *Teilerkette*, wenn für alle $n \in \mathbb{N}$ $a_{n+1}|a_n$ gilt. In R gilt der *Teilerkettensatz*, wenn jede Teilerkette $(a_n)_{n\in\mathbb{N}}$ stationär wird, d.h. es gibt ein $n_0 \in \mathbb{N}$ mit $a_n \sim a_{n+1}$ für $n \geq n_0$.

Beispiel 3.6. In $\mathbb{Z}$ gilt der Teilerkettensatz. Sei $(a_n)_{n\in\mathbb{N}}$ ein Teilerkette in $\mathbb{Z}$. Die Menge $\{|a_n| : n \in \mathbb{N}\}$ besitzt ein kleinstes Element $|a_{n_0}|$. Da $|a_{n+1}| \leq |a_n|$ für alle $n \in \mathbb{N}$ gilt, folgt $a_n \sim a_{n+1}$ für $n \geq n_0$.

Satz 3.7. In R gelte der Teilerkettensatz. Dann lässt sich jedes Element $0 \neq a \in R \setminus E_R$ als Produkt $a = b_1 \cdots b_n$ mit endlich vielen irreduziblen Elementen $b_1, \ldots, b_n$ darstellen (das Produkt ist nicht notwendigerweise eindeutig).

Beweis. Sei $a \in R$ ein beliebiges Element. Angenommen a lässt sich nicht als Produkt von endlich vielen irreduziblen Elementen schreiben. Wir definieren induktiv ein Kette von Elementen $(a_n)_{n\in\mathbb{N}}$ mit $a_{n+1}|a_n$, $a_n \not\sim a_{n+1}$ und a_n lässt sich für alle $n \in \mathbb{N}$ nicht als Produkt von endlich vielen irreduziblen Elementen schreiben. Dies ist ein Widerspruch zur Voraussetzung, dass in R der Teilerkettensatz gilt.

Für $n = 0$ setze $a_0 = a$. Sei $n > 0$ und die Kette $a_0, \ldots, a_n$ bereits konstruiert. a_n kann nicht irreduzibel sein, also existieren $0 \neq b, c \in R \setminus E_R$ mit $a_n = bc$. Wegen der Wahl von a_n können b und c sich nicht beide als Produkt von endlich vielen irreduziblen Elementen schreiben lassen. Lässt sich etwa b nicht so schreiben, dann setze $a_{n+1} = b$. Dies zeigt die Behauptung. □

Lemma 3.8. Sei R ein Integritätsbereich und ein Hauptidealring. Dann gilt in R der Teilerkettensatz.

Beweis. Sei $(a_n)_{n\in\mathbb{N}}$ ein Teilerkette in R. Da $a_{n+1}|a_n$ für alle $n \in \mathbb{N}$ gilt, folgt

$$(a_0) \subseteq (a_1) \subseteq \ldots \subseteq (a_n) \subseteq \ldots$$

Sei $I = \bigcup_{n\in\mathbb{N}}(a_n)$. Dann ist I ein Ideal, insbesondere ein Hauptideal. Also existiert ein $b \in R$ mit $I = (b)$. Sei n_0 so gewählt, dass $b \in a_{n_0}$ gilt. Dann ist $(a_n) = (a_{n+1})$ für $n \geq n_0$ und somit $a_n \sim a_{n+1}$ für $n \geq n_0$. □

Definition 3.9. Sei R ein Integritätsbereich und $0 \neq p \in R \setminus E_R$. Das Element p heißt ein *Primelement*, wenn für alle $a, b \in R$ mit $p|ab$ folgt, dass $p|a$ oder $p|b$ gilt.

Bemerkung 3.10. Sei R ein Integritätsbereich. Dann gelten folgende Regeln:

(i) Seien $p, q \in R$, p ein Primelement und $p \sim q \Rightarrow q$ ist ein Primelement.
(ii) Sind $p, q \in R$ Primelemente mit $p|q \Rightarrow p \sim q$.
(iii) Ist $p \in R$ ein Primelement mit $p|a_1 \cdots a_n \Rightarrow p|a_i$ für ein $i \in \{1, \ldots, n\}$.

Lemma 3.11. Sei R ein Integritätsbereich und $0 \neq p \in R \setminus E_R$. Dann gilt:

(i) p ist ein Primelement $\Leftrightarrow$ (p) ist ein Primideal.
(ii) p ist ein Primelement $\Rightarrow$ p ist irreduzibel.

Beweis. Zu (i): Dies folgt direkt aus den Definitionen von Primelement und Primideal.

Zu (ii): Sei p ein Primelement und $p = ab$ für $a, b \in R$. Da $p|ab$ gilt, folgt $p|a$ oder $p|b$. Gelte etwa $p|a$, dann existiert ein $c \in R$ mit $pc = a$. Somit folgt aus $p = ab = pcb$, dass $1 = cb$ gilt. Also ist $b \in E_R$. Damit ist p irreduzibel. □

Satz 3.12. Sei R ein Integritätsbereich und Hauptidealring, $0 \neq p \in R \setminus E_R$. Dann sind folgende Aussagen äquivalent:

(i) p ist ein Primelement,

(ii) p ist irreduzibel,
(iii) (p) ist ein maximales Ideal.

Beweis. In 3.4 und 3.11 wurde bereits (i) $\Rightarrow$ (ii) und (ii) $\Leftrightarrow$ (iii) bewiesen. Es bleibt zu zeigen, dass (iii) $\Rightarrow$ (i) gilt. Ist (p) ein maximales Ideal, so ist (p) ein Primideal nach 2.17. Aus 3.11 (i) folgt die Behauptung. □

Lemma 3.13. Sei R ein Integritätsbereich und $0 \neq a \in R$. Seien $a = p_1 \cdots p_m = q_1 \cdots q_n$ zwei Darstellungen von a als Produkt von Primelementen. Dann gilt:

(i) $m = n$.
(ii) Nach einer geeigneten Umnummerierung gilt $p_i \sim q_i$.

Die Darstellung von Primelementen ist also im Wesentlichen eindeutig.

Beweis. Wir beweisen den Satz durch eine Induktion nach $l = \min\{m, n\}$. O.E. ist $l = m$.

Für $l = 1$ folgt wegen $p_1 | q_1 \cdots q_n$, dass $p_1 | q_i$ für ein $i \in \{1, \dots, n\}$ und somit nach 3.10 $p_1 \sim q_i$, etwa $q_i = \varepsilon p_1$ für ein $\varepsilon \in E_R$. Außerdem gilt nach Kürzen durch p_1, dass $1 = \varepsilon q_1 \cdots q_{i-1} q_{i+1} \cdots q_n$. Also gilt $n = 1$ und damit die Behauptung.

Sei nun $l > 1$. Es gilt $p_m | q_1 \cdots q_n$ und daher wieder $p_1 | q_i$ für ein $i \in \{1, \dots, n\}$. O.E. $i = n$ und daher $p_m \sim q_n$, etwa $q_m = \varepsilon p_n$ für ein $\varepsilon \in E_R$. Nach Kürzen gilt $p_1 \cdots p_{m-1} = \varepsilon q_1 \cdots q_{n-1}$ mit $\min\{m-1, n-1\} < l$. Nach der Induktionsvoraussetzung gilt $m - 1 = n - 1 \Leftrightarrow m = n$ und nach einer geeigneten Nummerierung gilt $p_i \sim q_i$ für $i = 1, \dots, n-1$. □

Definition 3.14. Sei R ein Integritätsbereich. R heißt *faktoriell*, wenn sich jedes Element $0 \neq a \in R \setminus E_R$ eindeutig als Produkt von Primelementen schreiben lässt.

Bemerkung 3.15. Sei R ein faktorieller Ring, $0 \neq a \in R$ und $\mathcal{P}$ ein Vertretersystem der Primelemente von R. Dann besitzt a die Darstellung

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

mit $\varepsilon \in E_R$, $v_p(a) \in \mathbb{N}$ und fast alle $v_p(a) = 0$.

Korollar 3.16. Sei R ein Integritätsbereich und Hauptidealring, dann ist R faktoriell.

Beweis. Dies folgt aus 3.7, 3.8, 3.12 und 3.13. □

Definition 3.17. Ein Integritätsbereich R zusammen mit einer Abbildung $\delta\colon R \setminus \{0\} \to \mathbb{N}$ heißt ein *euklidischer Ring*, wenn für alle Elemente $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit

(i) $a = qb + r$,
(ii) $r = 0$ oder $\delta(r) < \delta(b)$.

Die Abbildung δ wird mit *Grad- oder Normabbildung* von R bezeichnet.

Beispiel 3.18. $\mathbb{Z}$ bildet zusammen mit der Betragsfunktion $|\cdot|$ einen euklidischen Ring. Jeder Körper ist aus trivialen Gründen ein euklidischer Ring.

Satz 3.19. Sei R ein euklidischer Ring. Dann ist R ein Integritätsbereich und Hauptidealring. Insbesondere gilt:

$$R \text{ ist ein euklidischer Ring}$$

$$\Rightarrow R \text{ ist ein Integritätsbereich und Hauptidealring}$$

$$\Rightarrow R \text{ ist ein faktorieller Ring.}$$

Beweis. Sei $I \subseteq R$ ein beliebiges Ideal. Ist $I = (0)$, so ist I ein Hauptideal. Sei also $I \neq (0)$. Definiere $m = \min\{\delta(a) \colon a \in I, a \neq 0\}$ und $0 \neq a \in I$ mit $\delta(a) = m$. Behauptung: $I = (a)$. Es gilt immer $(a) \subseteq I$. Sei nun $0 \neq b \in I$. Dann existieren $q, r \in R$ mit $b = qa + r$ und $r = 0$ oder $0 \leq \delta(r) < \delta(a)$. Da $r = b - qa \in I$ folgt wegen der Wahl von a, dass $r = 0$ und $b = qa \in (a)$ gilt. □

Definition 3.20. Sei R ein Integritätsbereich. Seien $a_1, \ldots, a_n \in R$.

(i) $d \in R$ heißt *grösster gemeinsamer Teiler* von $a_1, \ldots, a_n$, wenn gilt:
   (a) $d | a_i$ für $i = 1, \ldots, n$.
   (b) Ist $e \in R$ mit $e | a_i$ für $i = 1, \ldots, n$, so gilt $e | d$.
   Wir schreiben dann $\mathrm{ggT}(a_1, \ldots, a_n)$ für d.

(ii) $v \in R$ heißt *kleinstes gemeinsames Vielfaches* von $a_1, \ldots, a_n$, wenn gilt:
   (a) $a_i | v$ für $i = 1, \ldots, n$.
   (b) Ist $u \in R$ mit $a_i | u$ für $i = 1, \ldots, n$, so gilt $v | u$.
   Wir schreiben dann $\mathrm{kgV}(a_1, \ldots, a_n)$ für v.

Bemerkung 3.21. $\mathrm{ggT}(a_1, \ldots, a_n)$ und $\mathrm{kgV}(a_1, \ldots, a_n)$ sind bis auf Assoziiertheit eindeutig.

Satz 3.22. Sei R ein faktorieller Ring, $a_1, \ldots, a_n \in R \setminus \{0\}$, $\mathcal{P}$ ein Vertretersystem der Primelemente von R und

$$a_i = e_i \prod_{p \in \mathcal{P}} p^{v_p(a_i)} \text{ für } i = 1, \ldots, n$$

die Primfaktorzerlegungen von $a_1, \ldots, a_n$. Dann existieren ggT und kgV und es gilt

$$\mathrm{ggT}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\min(v_p(a_1), \ldots, v_p(a_n))},$$

$$\mathrm{kgV}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a_1), \ldots, v_p(a_n))}.$$

Beweis. Man beachte, dass für

$$\prod_{p \in \mathcal{P}} p^{v_p(a)} \Big| \prod_{p \in \mathcal{P}} p^{v_p(b)}$$

$v_p(a) \leq v_p(b)$ für alle $p \in \mathcal{P}$ gelten muss. Nun folgt die Behauptung. □

Satz 3.23. *(Euklidischer Algorithmus)* Sei R ein euklidischer Ring mit Gradabbildung δ. Für Elemente $a, b \in R \setminus \{0\}$ betrachte man die Folge $z_0, z_1, \ldots \in R$, die induktiv gegeben ist durch:

$$\begin{aligned} z_0 &= a \\ z_1 &= b \\ z_{i+1} &= \begin{cases} \text{der Rest der Division von } z_{i-1} \text{ durch } z_i, \text{ falls } z_i \neq 0, \\ 0 \text{ sonst.} \end{cases} \end{aligned}$$

Dann gibt es einen kleinsten Index $n \in \mathbb{N}$ mit $z_{n+1} = 0$. Für dieses n gilt $z_n = \mathrm{ggT}(a, b)$.

Beweis. Nach der Definition der Folge $(z_i)_{i \in \mathbb{N}}$ hat man für $i > 0$ und unter der Voraussetzung $z_i \neq 0$ eine Gleichung der Form

$$z_{i-1} = q_i z_i + z_{i+1} \text{ mit } \delta(z_{i+1}) < \delta(z_i) \text{ oder } z_{i+1} = 0.$$

Die Folge $\delta(z_i)$ ist für $i > 0$ und $z_i \neq 0$ streng monoton fallend. Daher hat die Menge $\mathcal{N} = \{\delta(z_i) \colon z_i \neq 0\}$ ein Minimum und es kann nur endlich viele $z_i \neq 0$ geben. Sei n minimal mit $z_{n+1} = 0$.

Behauptung: z_n teilt z_i für $0 \leq i < n$. Wir beweisen die Behauptung durch eine Induktion nach $n - i$. Für $n - 1$ folgt dies aus der Gleichung $z_{n-1} = q_n z_n$. Sei die Aussage für $n - i$ gezeigt. Aus der Gleichung

$$z_{n-i-1} = q_{n-i} z_{n-i} + z_{n-i+1}$$

folgt aus der Induktionsvoraussetzung $z_n | z_{n-i+1}$ und $z_n | z_{n-i}$, dass $z_n | z_{n-i-1}$. Insbesondere gilt $z_n | z_0 = a$ und $z_n | z_1 = b$.

Sei $c \in R$ mit $c | a$ und $c | b$. Wir zeigen durch eine Induktion nach i, dass $c | z_i$ gilt. Insbesondere $c | z_n$ und es folgt $z_n = \mathrm{ggT}(a, b)$. Für $i = 0$ und $i = 1$ gilt $c | z_i$ nach Voraussetzung. Sei nun $i > 1$. Wegen der Gleichung

$$z_{i-1} = q_i z_i + z_{i+1}$$

und der Induktionsvoraussetzung gilt $c | z_{i+1}$. □

Bemerkung 3.24. Durch den Beweis des Satzes 3.23 lässt sich eine explizite Darstellung des ggT's durch a und b gewinnen. Man muss lediglich die Gleichungen rückwärts auflösen.

Bemerkung 3.25. Mit dem $\mathrm{ggT}(a, b)$ hat man in der Situation von 3.23 auch den $\mathrm{kgV}(a, b)$ bestimmt, da

$$ab = \mathrm{ggT}(a, b)\mathrm{kgV}(a, b)$$

gilt.

4. Polynomringe

Konstruktion 4.1. Sei $R \subseteq S$ eine Ringerweiterung und $\{a_i\}_{i \in I}$ eine Teilmenge von S. Der Ring $R[\{a_i\}_{i \in I}]$ ist der kleinste Unterring $P \subseteq S$ mit den Eigenschaften

(i) $R \subseteq P$,
(ii) Für $i \in I$ gilt $a_i \in P$.

Ist $I = \{1, \dots, n\}$ endlich, dann schreiben wir $R[a_1, \dots, a_n]$. Man sagt auch, dass $R[\{a_i\}_{i\in I}]$ aus R durch Adjunktion der Elemente $\{a_i\}_{i\in I}$ von S entsteht.

Beispiel 4.2. Betrachte:

(i) $S = \mathbb{C}[X, Y]$, $R = \mathbb{C}$, $I = \{1\}$ und $a_1 = X$. Dann ist $R[X] \subseteq S$ ein Polynomring

(ii) $S = \mathbb{C}$, $R = \mathbb{R}$, $I = \{1\}$ und $a_1 = i$. Dann ist $R[i] = S$ kein Polynomring, da $i^2 + 1 = 0$ gilt.

Lemma 4.3. Sei $R \subseteq S$ eine Ringerweiterung und $a_1, \dots, a_n \in S$. Dann gilt

$$R[a_1, \dots, a_n] = \{a \in S \colon a = \sum_{(m_1,\dots,m_n)\in\mathbb{N}^n} c_{(m_1,\dots,m_n)} a_1^{m_1} \cdots a_n^{m_n} \text{ mit } c_{(m_1,\dots,m_n)} \in R$$

$$\text{und fast alle } c_{(m_1,\dots,m_n)} = 0\}.$$

Beweis. Sei

$$P = \{a \in S \colon a = \sum_{(m_1,\dots,m_n)\in\mathbb{N}^n} c_{(m_1,\dots,m_n)} a_1^{m_1} \cdots a_n^{m_n} \text{ mit } c_{(m_1,\dots,m_n)} \in R$$

$$\text{und fast alle } c_{(m_1,\dots,m_n)} = 0\}.$$

Dann ist P ein Unterring von S, der $a_1, \dots, a_n$ enthält. Ist P' ein weiterer Unterring von S mit dieser Eigenschaft, so gilt $P \subseteq P'$. Dies zeigt die Behauptung. □

Konstruktion 4.4. Sei R ein Ring und

$$R[X_1, \dots, X_n] =$$

$$\{(c_{(m_1,\dots,m_n)})_{(m_1,\dots,m_n)\in\mathbb{N}^n} : c_{(m_1,\dots,m_n)} \in R, \text{ fast alle } c_{(m_1,\dots,m_n)} = 0\}.$$

Definiere die Addition

$$(c_{(m_1,\dots,m_n)}) + (d_{(m_1,\dots,m_n)}) = (c_{(m_1,\dots,m_n)} + d_{(m_1,\dots,m_n)})$$

und die Multiplikation

$$(c_{(m_1,\dots,m_n)})(d_{(m_1,\dots,m_n)}) = (f_{(m_1,\dots,m_n)})$$

mit

$$f_{(m_1,\dots,m_n)} = \sum_{(s_1,\dots,s_n)+(t_1,\dots,t_n)=(m_1,\dots,m_n)} c_{(s_1,\dots,s_n)} d_{(t_1,\dots,t_n)}.$$

Sei

$$e_{(m_1,\dots,m_n)} = \begin{cases} 1 & (m_1, \dots, m_n) = (0, \dots, 0), \\ 0 & \text{sonst.} \end{cases}$$

Man rechnet nun nach, dass $R[X_1, \dots, X_n]$ ein Ring mit $1 = (e_{(m_1,\dots,m_n)})$ und $0 = (0)$ ist. Man nennt $R[X_1, \dots, X_n]$ den Polynomring in n Unbestimmten (Variablen) über R. Für $n = 1$ ist

$$R[X] = \{(c_m)_{m\in\mathbb{N}} \colon c_m \in R, \text{ fast alle } c_m = 0\}.$$

der übliche Polynomring in einer Variablen.

Satz 4.5. Sei R ein Ring. Dann entsteht der Ring $S = R[X_1, \dots, X_n]$ aus dem Ring

$$R \cong \{(a_{(m_1,\dots,m_n)} \colon a_{(m_1,\dots,m_n)} = 0 \text{ für } (m_1, \dots, m_n) \neq (0, \dots, 0), a_{(0,\dots,0)} \in R\}$$

durch Adjunktion der Elemente $X_i = (\delta^i_{(m_1,\dots,m_n)})$ mit

$$\delta^i_{(m_1,\dots,m_n)} = \begin{cases} 1 & \text{falls } (m_1, \dots, m_n) = \varepsilon_i, \\ 0 & \text{sonst.} \end{cases}$$

Beweis. Nachrechnen. □

Bemerkung 4.6. Jedes Element $f \in R[X_1, \dots, X_n]$ besitzt eine eindeutige Darstellung als Polynom

$$f = \sum_{(m_1,\dots,m_n)} a_{(m_1,\dots,m_n)} X_1^{m_1} \cdots X_n^{m_n}.$$

Satz 4.7. *(Die universelle Eigenschaft des Polynomrings)* Seien R und S Ringe, $\varphi \colon R \to S$ ein Ringhomomorphismus und $a_1, \dots, a_n \in S$. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\Phi \colon R[X_1, \dots, X_n] \to S$ mit

(i) $\Phi_{|R} = \varphi$,
(ii) $\Phi(X_i) = a_i$ für $i = 1, \dots, n$.

Ist insbesondere $S = R[a_1, \dots, a_n]$, so ist Φ ein Epimorphismus.

Beweis. Eindeutigkeit: Existiert Φ und ist

$$f = \sum_{(m_1,\dots,m_n)} a_{(m_1,\dots,m_n)} X_1^{m_1} \cdots X_n^{m_n} \in R[X_1, \dots, X_n],$$

so gilt

$$\begin{aligned} &\Phi(f) \\ &= \sum_{(m_1,\dots,m_n)} \Phi(a_{(m_1,\dots,m_n)}) \Phi(X_1)^{m_1} \cdots \Phi(X_n)^{m_n} \\ &= \sum_{(m_1,\dots,m_n)} \varphi(a_{(m_1,\dots,m_n)}) a_1^{m_1} \cdots a_n^{m_n}. \end{aligned}$$

Existenz: Definiere

$$\Phi(f) = \sum_{(m_1,\dots,m_n)} \varphi(a_{(m_1,\dots,m_n)}) a_1^{m_1} \cdots a_n^{m_n}$$

und rechnen nach, dass Φ eine Homomorphismus ist (dies folgt im Wesentlichen daraus, dass φ ein Homomorphismus ist). □

Korollar 4.8. Sei $n \in \mathbb{N}$ und R ein Ring. Dann gilt

$$R[X_1, \dots, X_n][X_{n+1}] \cong R[X_1, \dots, X_{n+1}].$$

Beweis. Sei $S = R[X_1, \dots, X_{n+1}]$. Betrachte den Monomorphismus (Einbettung)

$$\varphi \colon R \to S, \quad a \mapsto a.$$

Setze $a_1 = X_1, \dots, a_n = X_n$, dann existiert nach 4.7 ein eindeutiger Homomorphismus $\Phi \colon R[X_1, \dots, X_n] \to S$ mit

(i) $\Phi_{|R} = \varphi$,
(ii) $\Phi(X_i) = a_i$ für $i = 1, \dots, n$.

Man beachte, dass Φ injektiv ist. Nun betrachte den Homomorphismus

$$\varphi' = \Phi \colon R[X_1, \dots, X_n] \to S$$

und setze $a_1' = X_{n+1}$. Wieder nach 4.7 existiert ein eindeutig bestimmter Homomorphismus $\Phi' \colon R[X_1, \dots, X_n][X_{n+1}] \to S$ mit

(i) $\Phi'_{|R[X_1,\dots,X_n]} = \varphi' = \Phi$,
(ii) $\Phi(X_{n+1}) = a_1' = X_{n+1}$.

Φ' ist der gesuchte Isomorphismus. □

Definition 4.9. Sei R ein Ring und $S = R[X_1, \dots, X_n]$.

(i) Sei $\underline{m} = (m_1, \dots, m_n) \in \mathbb{N}^n$. Ein Element $X_1^{m_1} \cdots X_n^{m_n} \in S$ heißt *Monom*. Man nennt $(m_1, \dots, m_n)$ den *Multigrad* und $|\underline{m}| = m_1 + \cdots + m_n$ den *Totalgrad* von $X_1^{m_1} \cdots X_n^{m_n}$.
(ii) Sei $f = \sum_{(m_1,\dots,m_n)} a_{(m_1,\dots,m_n)} X_1^{m_1} \cdots X_n^{m_n} \in S$ beliebig. Definiere

$$\deg(f) = \begin{cases} \max\{m_1 + \ldots + m_n \colon a_{\underline{m}} \neq 0\} & f \neq 0, \\ -\infty & f = 0. \end{cases}$$

Dann heißt $\deg(f)$ der *Grad* von f.

Ist insbesondere $n = 1$ und $0 \neq f = \sum_{m \in \mathbb{N}} a_m X^m$. Dann gilt $\deg(f) = \max\{m \colon a_m \neq 0\}$. Das Element $a_{\deg(f)} = \mathrm{Leit}(f)$ heißt dann der *Leitkoeffizient*. f heißt *normiert*, wenn $\mathrm{Leit}(f) = 1$.

Bemerkung 4.10. Seien $f, g \in R[X]$, $\deg(f) = m$, $\deg(g) = n$, $a_m = \mathrm{Leit}(f)$ und $b_m = \mathrm{Leit}(g)$. Dann gilt:

(i) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$. Es gilt Gleichheit genau dann, wenn
  (a) $\deg(f) \neq \deg(g)$,
  (b) oder $f = g = 0$,
  (c) oder $\deg(f) = \deg(g)$ und $a_n + b_n \neq 0$.
(ii) $\deg(fg) \leq \deg(f) + \deg(g)$. Es gilt Gleichheit genau dann, wenn
  (a) $f = 0$ oder $g = 0$,
  (b) oder $f \neq 0$, $g \neq 0$ und $a_m b_n \neq 0$ (z.B. in einem Integritätsbereich).

Satz 4.11. Sei R ein Integritätsbereich. Dann gilt:

(i) $R[X_1, \dots, X_n]$ ist ein Integritätsbereich.
(ii) $E_{R[X_1,\dots,X_n]} = E_R$.

Beweis. Zu (i): Wir beweisen (i) durch eine Induktion nach n. Sei $n = 1$ und $0 \neq f, g \in R[X]$. Dann gilt nach 4.10, dass $\deg(fg) = \deg(f)\deg(g) \neq 0$ und daher $fg \neq 0$. Also ist $R[X]$ ein Integritätsbereich. Für $n > 1$ folgt die Aussage aus 4.8 und der Induktionsannahme wegen $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$.

Zu (ii): Auch (ii) wird durch eine Induktion bewiesen. Sei $n = 1$. Man beachte, dass für ein $0 \neq f \in R[X]$ gilt $\deg(f) = 0$ genau dann, wenn $f \in R$. Es gilt immer $E_R \subseteq E_{R[X]}$. Sei nun $f \in E_{R[X]}$. Dann ist $f \neq 0$ und es existiert ein $0 \neq g \in R[X]$ mit $1 = fg$. Also $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$. Somit ist $\deg(f) = \deg(g) = 0$

und daher $f, g \in R$, speziell $f, g \in E_R$. Für $n > 1$ folgt die Behauptung wieder aus 4.8 und der Induktionsannahme wegen

$$E_{R[X_1,\dots,X_n]} = E_{R[X_1,\dots,X_{n-1}][X_n]} = E_{R[X_1,\dots,X_{n-1}]} = E_R.$$

□

Satz 4.12. *(Division mit Rest)* Sei R ein Ring, $f, g \in R[X]$, $g \neq 0$ und $\mathrm{Leit}(g) \in E_R$. Dann existieren eindeutig bestimmte Polynome $q, r \in R[X]$ mit

(i) $f = qg + r$,
(ii) $\deg(r) < \deg(g)$.

Beweis. Existenz: Ist $f = 0$, so setze $q = r = 0$. Sei nun $f \neq 0$. Wir beweisen den Satz durch eine Induktion nach $\deg(f)$.

Sei $\deg(f) = 0$. Ist $\deg(g) = 0$, so gilt $g \in E_R$. Dann können wir $q = g^{-1}f$ und $r = 0$ wählen und erhalten $f = qg$. Ist $\deg(g) > 0$, dann sind $q = 0$ und $r = f$ die gesuchten Elemente mit $f = 0g + r$.

Sei nun $\deg(f) > 0$. Im Falle $\deg(f) < \deg(g)$, kann wieder $q = 0$ und $r = f$ gewählt werden. Betrachte also $\deg(f) \geq \deg(g)$. Sei $m = \deg(f)$, $n = \deg(g)$, $a_m = \mathrm{Leit}(f)$ und $b_n = \mathrm{Leit}(g)$. Definiere

$$q_1 = b_n^{-1} a_m X^{n-m} \text{ und } f_1 = f - q_1 g.$$

Dann ist $\deg(f_1) < \deg(f)$. Nach der Induktionsannahme existieren $q_2, r \in R[X]$ mit $f - q_1 g = f_1 = q_2 g + r$ und $\deg(r) < \deg(g)$. Somit

$$f = (q_1 + q_2)g + r.$$

Wähle nun $q = q_1 + q_2$.

Eindeutigkeit: Sei

$$f = q_1 g + r_1 = q_2 g + r_2 \text{ mit } \deg(r_1), \deg(r_2) < \deg(g).$$

Also $(q_1 - q_2)g = r_2 - r_1$. Es gilt $\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\} < \deg(g)$. Auf der anderen Seite ist $\deg((q_1 - q_2)g) = \deg(q_1 - q_2) + g$, da $\mathrm{Leit}(g) \in E_R$. Somit

$$\deg(g) + \deg(q_1 - q_2) = \deg(r_2 - r_1) < \deg(g).$$

Dies ist nur für $q_1 = q_2$ und $r_1 = r_2$ möglich. Dies zeigt die Eindeutigkeit. □

Korollar 4.13. Sei K ein Körper. Dann ist $K[X]$ zusammen mit der Abbildung deg ein euklidischer Ring. Insbesondere ist $K[X]$ ein Hauptidealring und faktoriell.

Definition 4.14. Sei $R \subseteq S$ eine Ringerweiterung und $0 \neq f = \sum_{m\in\mathbb{N}} a_m X^m \in R[X]$. Ein Element $b \in S$ heißt *Nullstelle* von f in S, wenn $f(b) = \sum_{m\in\mathbb{N}} a_m b^m = 0$ gilt, also ist f ist im Kern des Einsetzungshomomorphismus

$$R[X] \to S, \quad f \mapsto f(b).$$

Satz 4.15. Sei R ein Integritätsbereich und $0 \neq f \in R[X]$ ein Polynom vom Grad n.

(i) $b \in R$ ist genau dann eine Nullstelle von f, wenn $(X - b) | f$ in $R[X]$.
(ii) f besitzt höchstens n Nullstellen in R.

Beweis. Zu (i): Gilt $(X-b)|f$, so ist $f=(X-b)g$. Also $f(b)=(b-b)g=0$. Sei nun b eine Nullstelle von f. Teile f mit Division durch Rest durch $X-b$. Dann existieren $q,r\in R[X]$ mit $f=q(X-b)+r$ und $\deg(r)\leq 0$. Es gilt $0=f(b)=q(b)0+r(b)=r(b)$ und daher $r=0$, da $r\in R$ ein Widerspruch geben würde. Also gilt $(X-b)|f$.

Zu (ii): Wir beweisen die Aussage durch eine Induktion nach $\deg(f)$. Ist $\deg(f)=0$, so ist $f\in R$ und f kann keine Nullstellen besitzen. Sei nun $\deg(f)>0$. Falls f keine Nullstelle besitzt, ist nichts zu zeigen. Sei also b eine Nullstelle von f. Nach (i) gilt $f=(X-b)g$ für ein $g\in R[X]$ mit $\deg(g)=\deg(f)-1$. Nach der Induktionsannahme hat g höchstens $n-1$ Nullstellen in R. Da b' genau dann eine Nullstelle von f ist, wenn b' eine Nullstelle von $(X-b)$ oder von g ist, hat f höchstens $n-1+1=n$ Nullstellen. □

5. Der Satz von Gauß

Satz 5.1. *(Gauß)* Sei R ein faktorieller Ring, dann ist auch der Polynomring $R[X]$ faktoriell.

Korollar 5.2. Sei R ein faktorieller Ring, dann ist für $n\in\mathbb{N}, n\geq 1$ auch der Polynomring $R[X_1,\dots,X_n]$ faktoriell.

Beweis. Dies folgt aus 4.8 und 5.1. □

Bemerkung 5.3. Durch den Satz von Gauß sieht man, dass es faktorielle Ringe gibt, die keine Hauptidealringe sind. Z. B. ist für einen Körper K der Ring $K[X,Y]$ faktoriell. Dieser Ring ist aber kein Hauptidealring.

Lemma 5.4. Sei R ein faktorieller Ring, $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R. Dann besitzt jedes Element $0\neq x=\frac{a}{b}\in Q(R)$ eine eindeutige Darstellung

$$x=\varepsilon\prod_{p\in\mathcal{P}}p^{v_p(x)}$$

mit $\varepsilon\in E_R$, $v_p(x)\in\mathbb{Z}$ und fast alle $v_p(x)=0$. Insbesondere ist $x\in R$ genau dann, wenn alle $v_p(x)\in\mathbb{N}$.

Beweis. Existenz: Sei

$$a=\varepsilon_a\prod_{p\in\mathcal{P}}p^{v_p(a)}\text{ und }b=\varepsilon_b\prod_{p\in\mathcal{P}}p^{v_p(b)}$$

mit $\varepsilon_a,\varepsilon_b\in E_R$, $v_p(a),v_p(b)\in\mathbb{N}$ und fast alle $v_p(a)=0$ bzw. $v_p(b)=0$. Dann ist

$$x=\varepsilon_a\varepsilon_b^{-1}\prod_{p\in\mathcal{P}}p^{v_p(a)-v_p(b)}.$$

O.E. kann angenommen werden, dass immer $v_p(a)=0$ oder $v_p(b)=0$ gilt.

Eindeutigkeit: Sei

$$x=\varepsilon'\prod_{p\in\mathcal{P}}p^{v'_p(x)}$$

eine weitere Darstellung. Definiere

$$c = \prod_{p\in\mathcal{P}, v'_p(x)\geq 0} p^{v'_p(x)} \text{ und } d = \prod_{p\in\mathcal{P}, v'_p(x)<0} p^{-v'_p(x)}.$$

Dann ist $x = \frac{c}{d}$, also $ad = cb$. Wegen der Wahl von a, b, c, d und der Eindeutigkeit der Primfaktorzerlegung in R folgt nun $a = c$ und $b = d$ und damit die Behauptung. □

Definition 5.5. Sei R ein faktorieller Ring, $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R und $0 \neq f = \sum a_n X^n \in Q(R)[X]$. Dann:

(i) $v_p(f) = \min\{v_p(a_n)\colon a_n \neq 0\}$.
(ii) $I(f) = \prod_{p\in\mathcal{P}} p^{v_p(f)}$ heißt der *Inhalt* von f. Dieser Ausdruck ist definiert, aber abhängig von $\mathcal{P}$.
(iii) f heißt *primitiv*, wenn $I(f) \in E_R$ (d.h. der ggT der Koeffizienten ist 1).

Beispiel 5.6. Für normierte Polynome $f \in R[X]$ gilt, dass f primitiv ist.

Lemma 5.7. Sei R ein faktorieller Ring und $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R.

(i) Sei $a \in Q(R)$ und $f \in Q(R)[X]$. Dann ist $I(af) = I(a)I(f) = \varepsilon a I(f)$ für ein $\varepsilon \in E_R$. Ist $a = \prod_{p\in\mathcal{P}} p^{v_p(a)}$, so kann $\varepsilon = 1$ gewählt werden.
(ii) Sei $0 \neq f \in Q(R)[X]$. Dann gibt es ein $g \in R[X]$, g primitiv, $I(g) = 1$ und $f = I(f)g$.
(iii) Sei $f \in R[X]$ irreduzibel und $\deg(f) > 0$. Dann ist f primitiv.
(iv) Sei $f \in R[X]$ primitiv und in $Q(R)[X]$ irreduzibel. Dann ist f in $R[X]$ irreduzibel.

Beweis. Zu (i): Sei $f = \sum_{n\in\mathbb{N}} a_n X^n$ Dann ist $v_p(af) = \min\{v_p(aa_n)\colon a_n \neq 0\} = v_p(a) + v_p(f)$. Somit

$$I(af) = \prod_{p\in\mathcal{P}} p^{v_p(af)} = \prod_{p\in\mathcal{P}} p^{v_p(a)} \prod_{p\in\mathcal{P}} p^{v_p(f)} = \varepsilon a I(f)$$

für ein $\varepsilon \in E_R$. Ist $a = \prod_{p\in\mathcal{P}} p^{v_p(a)}$, so kann $\varepsilon = 1$ gewählt werden.

Zu (ii): Sei $g = I(f)^{-1}f$. Dann ist $f = I(f)g$. Ferner $I(g) = I(f)^{-1}I(f) = 1 \in E_R$ und somit ist g primitiv. Sei $f = \sum_{n\in\mathbb{N}} a_n X^n$. Es ist $v_p(I(f)^{-1}a_n) \geq 0$ für alle $p \in \mathcal{P}$, also ist $g \in R[X]$.

Zu (iii): Nach (ii) ist $f = I(f)g$ und $g \in R[X]$ primitiv. Außerdem $\deg(g) = \deg(f) > 0$. Da f irreduzibel ist, muss $I(f) \in E_{R[X]}$ gelten. Dann ist $I(f) \in E_R$ und somit f primitiv.

Zu (iv): Sei $f = gh$ mit $g, h \in R[X]$. Da f irreduzibel über $Q(R)[X]$ ist, muss $g \in Q(R) \setminus \{0\}$ oder $h \in Q(R) \setminus \{0\}$ gelten. Sei etwa $g \in Q(R) \setminus \{0\}$. Dann ist $\varepsilon g I(h) = I(gh) = I(f) \in E_R$. Da $I(h) \in R$ gilt, folgt $g \in E_R$. Dies war zu zeigen. □

Beispiel 5.8. Sei $f(X) = 2X$, also $I(f) = 2$. Dann ist f in $\mathbb{Q}[X]$ irreduzibel, aber nicht in $\mathbb{Z}[X]$, da hier 2 keine Einheit ist.

Lemma 5.9. *(Gauß)* Sei R ein faktorieller Ring und $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R. Seien $0 \neq f, g \in Q(R)[X]$. Dann gilt:

$$I(fg) = I(f)I(g).$$

Beweis. Sei $f = I(f)f_1$ und $g = I(g)g_1$ mit $f_1, g_1 \in R[X]$ primitiv und $I(f_1) = I(g_1) = 1$. Dann ist

$$fg = I(f)I(g)f_1g_1$$

und damit

$$I(fg) = I(f)I(g)I(f_1g_1)$$

Es genügt zu zeigen, dass $I(f_1g_1) = 1$ gilt. Wir können also o. E. annehmen, dass $f, g \in R[X]$ und $I(f) = I(g) = 1$ gilt.

Dann ist zu zeigen, dass für alle $p \in \mathcal{P}$ gilt $v_p(fg) = 0$. Sei $p \in \mathcal{P}$ fest gewählt, $\deg(f) = m$, $\deg(g) = n$

$$f = \sum_{i=0}^{m} a_i X^i, g = \sum_{j=0}^{n} b_j X^j, fg = \sum_{k=0}^{m+n} c_k X^k,$$

mit $c_{m+n} = a_m + b_n$. Es ist z. z., dass ein $k \in \{0, \dots, m+n\}$ existiert mit $v_p(c_k) = 0$, d.h $p \not| c_k$. Da $I(f) = 1$, existiert ein maximales $r \in \{0, \dots, n\}$ mit p teilt nicht a_r. Wähle analog $s \in \{0, \dots, m\}$ maximal mit p teilt nicht b_s. Dann ist

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = a_r b_s + \sum_{i>0} a_{r+i} b_{s-i} + \sum_{i>0} a_{r-i} b_{s+i}.$$

Für $i > 0$ gilt $p | a_{r+i} b_{s-i}$, da $p | a_{r+i}$. Für $i < 0$ gilt $p | a_{r-i} b_{s+i}$, da $p | b_{s+i}$. Da aber p nicht $a_r b_s$ teilt (p ist ein Primelement), folgt, dass p nicht c_{r+s} teilt. Dies zeigt die Behauptung. □

Korollar 5.10. Sei R ein faktorieller Ring. Seien $0 \neq f \in R[X]$ mit $\deg(f) > 0$. Dann sind folgende Aussagen äquivalent:

(i) f ist irreduzibel in $R[X]$,
(ii) f ist irreduzibel in $Q(R)[X]$ und f ist primitiv.

Beweis. (ii) $\Rightarrow$ (i): Dies wurde in 5.7 gezeigt.

(i) $\Rightarrow$ (ii): Nach 5.7 ist f primitiv. Insbesondere gilt $I(f) \in E_R$. Sei nun $f = gh$ mit $g, h \in Q(R)[X]$. Dann folgt $I(f) = I(g)I(h)$. Somit

$$I(f)^{-1} f = I(g)^{-1} g I(h)^{-1} h.$$

Da $I(f)^{-1}f$ irreduzibel in $R[X]$ und $I(g)^{-1}g, I(h)^{-1}h \in R[X]$ gilt, folgt o.E., dass $I(g)^{-1}g \in E_{R[X]} = E_R$. Also $g \in E_{Q(R)[X]} = Q(R) \setminus \{0\}$.

□

Korollar 5.11. Sei R ein faktorieller Ring. Seien $0 \neq f, g \in R[X]$, f primitiv, $h \in Q(R)[X]$ und $g = fh$. Dann gilt $h \in R[X]$. D. h. teilt f ein Element g in $Q(R)[X]$, dann teilt f das Element g in $R[X]$.

Beweis. Es ist $I(g) = I(f)I(h)$. Da f primitiv ist, gilt $I(f) \in E_R$. Also $I(h) = I(f)^{-1}I(g) \in R$ und daher $h \in R[X]$. □

Beweis. (Beweis des Satzes von Gauß) Sei R ein faktorieller Ring, $0 \neq f \in R[X] \setminus E_R$. Der Ring $Q(R)[X]$ ist ein euklidischer Ring, also faktoriell. Somit existieren $f_1, \dots, f_n \in Q(R)[X]$ irreduzibel mit $f = f_1 \cdots f_n$. Sei $c = \prod_{i=1}^{n} I(f_i)$ und $\tilde{f}_i = I(f_i)^{-1} f_i$. Dann folgt

$$I(\tilde{f}_i) = 1, \quad \tilde{f}_i \in R[X], \quad f = c \prod_{i=1}^{n} \tilde{f}_i \text{ mit } c = I(f) \in R.$$

c ist ein Produkt von Primelementen von R, die auch Primelemente von $R[X]$ sind (Übungsaufgabe).

$\tilde{f}_i$ ist primitiv und irreduzibel in $Q(R)[X]$. Nach 5.10 sind $\tilde{f}_i$ irreduzibel in $R[X]$. Es bleibt folgende Behauptung zu zeigen: Ist $f \in R[X]$ irreduzibel und primitiv, dann ist f ein Primelement.

Sei $g, h \in R[X]$ mit $f | gh$ in $R[X]$. Insbesondere gilt $f | gh$ in $Q(R)[X]$. Da f irreduzibel in $Q(R)[X]$ folgt, dass f ein Primelement in $Q(R)[X]$ ist. Somit $f | g$ oder $f | h$ in $Q(R)[X]$. Da f primitiv ist, folgt aus 5.11, dass $f | g$ oder $f | h$ in $R[X]$. Also ist f ein Primelement in $R[X]$. □

6. Irreduzibilitätskriterien für Polynome

Problem: Welche Polynome sind irreduzibel in $R[X]$ (bzw. in $Q(R)[X]$)? Teilt man durch den Inhalt, so kann o.E. angenommen werden, dass die Polynome primitiv sind.

Satz 6.1. *(Eisensteinsches Irreduzibilitätskriterium)* Sei R ein faktorieller Ring, $0 \neq f = \sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv, $\deg(f) = n > 0$. Weiter sei $p \in R$ ein Primelement mit $p \nmid a_n$, $p | a_i$ für $i = 0, \dots, n-1$, $p^2 \nmid a_0$. Dann ist f irreduzibel in $R[X]$ und somit auch in $Q(R)[X]$.

Beweis. Angenommen $f = gh$ mit $g = \sum_{i=0}^{n_g} b_i X^i$, $h = \sum_{i=0}^{n_h} c_i X^i$, $\deg(g) = n_g$ und $\deg(h) = n_h$. O.E. gilt $n_g, n_h > 0$, da f primitiv ist. (Wäre etwa $n_g = 0$, so würde aus $I(g)I(h) = I(f) \in E_R$ folgen, dass $g \in E_R$).

Da $p | a_0 = b_0 c_0$, folgt $p | b_0$ oder $p | c_0$. Sei o.E. $p | c_0$. Dann kann nicht $p | b_0$ gelten, da sonst $p^2 | a_0$ ein Widerspruch wäre. Da $p \nmid a_n = b_{n_g} c_{n_h}$ folgt, dass $p \nmid b_{n_g}$ und $p \nmid c_{n_h}$.

Sei nun $r = \min\{j : p \nmid c_j\}$. Es gilt $0 < r \leq n_h < n = n_h + n_g$. Betrachte

$$a_r = b_0 c_r + \sum_{i=1}^{r} b_i c_{r-i}.$$

Es gilt $p \nmid b_0 c_r$ und $p | b_i c_{r-i}$ für $i = 1, \dots r$ wegen der Wahl von r. Somit gilt $p \nmid a_r$. Dies ist ein Widerspruch zur Voraussetzung, da $0 < r < n$. □

Beispiel 6.2. Sei p eine Primzahl, dann ist $X^n - p$ irreduzibel in $\mathbb{Z}[X]$.

Lemma 6.3. Sei R ein Integritätsbereich. Dann gilt:

(i) Sei $\varphi : R \to R$ ein Automorphismus und $a \in R$. Dann ist a irreduzibel genau dann, wenn $\varphi(a)$ irreduzibel ist.

(ii) Sei $a \in R$ und $\varepsilon \in E_R$. Dann ist die Abbildung $\varphi\colon R[X] \to R[X], f(X) \mapsto f(\varepsilon X + a)$ ein Automorphismus. Insbesondere ist $f(X)$ irreduzibel genau dann, wenn $f(\varepsilon X + a)$ irreduzibel ist.

Beweis. Zu (i): Trivial.

Zu (ii): Man sieht leicht, dass φ ein Homomorphismus ist. Die Abbildung

$$\psi\colon R[X] \to R[X], \quad f(X) \mapsto f(\varepsilon^{-1}(X - a))$$

ist die Umkehrabbildung zu φ. Somit ist φ ein Automorphismus. □

Beispiel 6.4. Behauptung: Sei p eine Primzahl, dann ist $f(X) = \sum_{i=0}^{p-1} X^i$ irreduzibel in $\mathbb{Z}[X]$.

Die Behauptung ist äquivalent zu: $f(X+1) = \sum_{i=0}^{p-1}(X+1)^i$ ist irreduzibel in $\mathbb{Z}[X]$. Es gilt $(X-1)f(X) = X^p - 1$. Also $Xf(X+1) = (X+1)^p - 1$ und somit

$$f(X+1) = \frac{(X+1)^p - 1}{X} = \frac{\sum_{i=1}^{p} \binom{p}{i} X^i}{X} = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i.$$

Nun sieht man, dass $f(X+1)$ irreduzibel nach dem Eisensteinkriterium ist.

Satz 6.5. *(Reduktionsmethode)* Sei R faktoriell, $0 \neq f = \sum_{i=0}^{n} a_i X^i$ primitiv, $\deg(f) = n$, $P \subset R$ ein Primideal, $a_n \notin P$, $\overline{R} = R/P$ und $\overline{f} = \sum_{i=0}^{n} \overline{a_i} X^i \in \overline{R}[X]$ mit $\overline{a_i} = a_i + P$. Wenn $\overline{f}$ irreduzibel in $\overline{R}[X]$ ist, so folgt, dass f irreduzibel in $Q(R)[X]$ und $R[X]$ ist.

Beweis. Es genügt zu zeigen, dass f irreduzibel in $R[X]$ ist.

Angenommen: $f = gh$ mit $g, h \in R[X]$, $\deg(g) > 0$ und $\deg(h) > 0$. Der kanonische Epimorphismus $\varepsilon\colon R \to \overline{R}$ induziert einen Epimorphismus

$$\overline{\varepsilon}\colon R[X] \to \overline{R}[X], \quad \sum b_i X^i \mapsto \sum \overline{b_i} X^i.$$

Da nach Voraussetzung $\overline{a_n} \neq 0$ gilt folgt, dass $\deg(\overline{f}) = \deg(f) \geq 1$. Es ist $\deg(\overline{g}) \leq \deg(g)$ und $\deg(\overline{h}) \leq \deg(h)$. Da

$$\deg(f) = \deg(g) + \deg(h) \leq \deg(\overline{g}) + \deg(\overline{h}) = \deg(\overline{f}) = \deg(f),$$

folgt $\deg(\overline{g}) = \deg(g)$ und $\deg(\overline{h}) = \deg(h)$. Dann ist $\overline{f} = \overline{g}\,\overline{h}$ reduzibel ein Widerspruch zur Voraussetzung. □

Beispiel 6.6. Problem: Ist $f = X^4 + 3X + 1$ irreduzibel in $\mathbb{Q}[X]$ bzw. $\mathbb{Z}[X]$?

Betrachte Reduktion mod 2, also $\overline{f} = X^4 + X + 1$ in $\mathbb{Z}/2\mathbb{Z}[X]$.

X und $X+1$ sind die einzig möglichen Linearfaktoren in $\mathbb{Z}/2\mathbb{Z}[X]$. Da $\overline{f}(0) = \overline{f}(1) = 1$ besitzt f keine Linearfaktoren.

X^2, $X^2 + X$, $X^2 + 1$ und $X^2 + X + 1$ sind die einzigen möglichen quadratischen Polynome. Keines von diesen teilt $\overline{f}$ (ausrechnen).

Also ist $\overline{f}$ irreduzibel in $\mathbb{Z}/2\mathbb{Z}[X]$ und somit f irreduzibel in $\mathbb{Z}[X]$.

KAPITEL 3

Körpertheorie

1. Endliche und algebraische Körpererweiterungen

Definition 1.1. Sei L ein Körper und K ein Teilkörper.

(i) Dann heißt das Paar $K \subseteq L$ eine *Körpererweiterung*. Man schreibt hierfür L/K.

(ii) Die K-Vektorraumdimension $\dim_K(L) = [L\colon K]$ heißt der *Grad* von L über K. Die Körpererweiterung heißt *endlich* oder *unendlich*, je nachdem ob $[L\colon K]$ endlich oder unendlich ist.

Bemerkung 1.2. Sei L/K eine Körpererweiterung. Dann ist $L = K$ genau dann, wenn $[L\colon K] = 1$.

Satz 1.3. Seien L/K und M/L Körpererweiterungen. Dann gilt die Gradformel:

$$[M\colon K] = [M\colon L][L\colon K].$$

Beweis. Sei $[M\colon L] < \infty$ und $[L\colon K] < \infty$. Wähle eine L-Vektorraumbasis $v_1, \ldots, v_r$ von M und eine K-Vektorraumbasis $w_1, \ldots, w_s$ von L. Wir behaupten, dass $v_i w_j$, $i = 1, \ldots, r$, $j = 1, \ldots, s$ eine K-Vektorraumbasis von M ist. Daraus folgt dann die Gradformel.

Sei $x \in M$. Dann existieren $l_i \in L$ mit $x = \sum_{i=1}^{r} l_i v_i$. Für jedes l_i gibt es $a_{ij} \in K$ mit $l_i = \sum_{j=1}^{s} a_{ij} w_j$. Dann folgt

$$x = \sum_{i=1}^{r} \sum_{j=1}^{s} a_{ij} w_j v_i$$

und somit sind die Elemente $v_i w_j$ ein K-Vektorraumerzeugendensystem von M/K.

Seien $b_{ij} \in K$ mit

$$0 = \sum_{i=1}^{r} \sum_{j=1}^{s} b_{ij} v_i w_j = \sum_{i=1}^{r} (\sum_{j=1}^{s} b_{ij} w_j) v_i.$$

Da die v_i linear unabhängig über L sind, folgt für $i = 1, \ldots, r$

$$\sum_{j=1}^{s} b_{ij} w_j.$$

Da die w_j linear unabhängig über K sind, folgt für $i = 1, \ldots, r$ und $j = 1, \ldots, s$, dass $b_{ij} = 0$ gilt. Also sind die Elemente $v_i w_j$ linear unabhängig und sie bilden somit eine K-Basis von M.

Wir haben darüber hinaus gezeigt, dass mit $[M\colon L] \geq m$ und $[L\colon K] \geq n$ folgt $[M\colon K] \geq mn$. Ist somit $[M\colon L] = \infty$ oder $[L\colon K] = \infty$, dann ist auch $[M\colon K] = \infty$. □

Korollar 1.4. Seien L/K, M/L Körpererweiterungen und $[M\colon K]$ endlich. Dann ist $[L\colon K]$ endlich und $[L\colon K] | [M\colon K]$.

Korollar 1.5. Seien L/K, M/L Körpererweiterungen und $[M\colon K]$ eine Primzahl. Dann ist $L = M$ oder $L = K$.

Beispiel 1.6. Es ist $[\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 2$. Also besitzt $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ keine Zwischenkörper.

Definition 1.7. Sei L/K eine Körpererweiterung. Ein Element $a \in L$ heißt *algebraisch* über K, wenn ein $0 \neq f \in K[X]$ existiert mit $f(a) = 0$. Falls a nicht algebraisch ist, so heißt a *transzendent* über K.

Beispiel 1.8. Sei L/K eine Körpererweiterung.

(i) Alle Elemente $a \in K$ sind algebraisch über K, da für $f(X) = X - a$ gilt $f(a) = 0$.

(ii) Ist $K = \mathbb{Q}$ und $L = \mathbb{C}$, so ist $\sqrt{2}$ algebraisch und e transzendent über K.

Satz 1.9. Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Dann existiert ein eindeutig bestimmtes normiertes Polynom $f \in K[X]$ kleinsten Grades mit $f(a) = 0$. Ferner ist f ein Primelement und somit irreduzibel. f heißt das *Minimalpolynom* von a über K. Ist $g \in K[X]$ ein weiteres Polynom mit $g(a) = 0$, dann gilt $f | g$.

Beweis. Sei

$$\varphi\colon K[X] \to L, \quad g \mapsto g(a)$$

der Einsetzungshomomorphismus. Da a algebraisch ist folgt $\mathrm{Ker}(\varphi) \neq \{0\}$. Dann ist $\mathrm{Ker}(\varphi) = (f)$ für ein eindeutig bestimmtes normiertes Polynom $0 \neq f \in K[X]$. f ist das normierte Polynom kleinsten Grades mit der Eigenschaft $f(a) = 0$.

Nun ist $K[X]/(f) \subseteq L$ ein Unterring des Integritätsbereichs L. Daher ist (f) ein Primideal und somit f ein Primelement. □

Definition 1.10. Sei L/K eine Körpererweiterung und $a \in L$. Definiere

$$[a\colon K] = \begin{cases} \deg(f) & \text{falls } a \text{ algebraisch über } K \text{ ist mit Minimalpolynom } f, \\ \infty & \text{falls } a \text{ transzendent über } K \text{ ist.} \end{cases}$$

$[a\colon K]$ heißt der *Grad* von a über K.

Beispiel 1.11. Es ist $[\sqrt{2}\colon \mathbb{Q}] = 2$ und $[\sqrt{2}\colon \mathbb{C}] = 1$.

Lemma 1.12. Sei L/K eine Körpererweiterung und $\{a_i\}_{i \in I} \subseteq L$. Dann existiert ein kleinster Teilkörper $L' \subseteq L$ mit

(i) $K \subseteq L'$,

(ii) $a_i \in L'$ für $i \in I$.

Dieser wird mit $K(\{a_i\}_{i \in I})$ bezeichnet. Man sagt, dass $K(\{a_i\}_{i \in I})$ aus K durch Adjunktion der Elemente $\{a_i\}_{i \in I}$ entsteht.

Satz 1.13. Sei L/K eine Körpererweiterung und $a \in L$. Dann sind äquivalent:

(i) a ist algebraisch über K,

(ii) $K(a) = K[a]$,
(iii) $[K(a)\colon K] < \infty$.

Beweis. (i) $\Rightarrow$ (ii): Sei f das Minimalpolynom von a und

$$\varphi\colon K[X] \longrightarrow K[a], \quad g \mapsto g(a)$$

φ ist surjektiv, $\mathrm{Ker}(\varphi) = (f)$ und es folgt, dass $K[X]/(f) \cong K[a]$. Da f irreduzibel ist gilt, dass (f) ein maximales Ideal und somit $K[a]$ ein Körper ist.

Es gilt immer $K[a] \subseteq K(a)$. Da aber $K(a)$ der kleinste Körper mit a als Element ist, der K enthält, gilt $K[a] = K(a)$.

(ii) $\Rightarrow$ (iii): Es ist

$$K(a) = K[a] \cong K[X]/(g)$$

für ein $g = \sum_{i=0}^{n} a_i X^i \in K[X]$ mit $a_n = 1$. Hierbei ist $g \neq 0$, da $K[X]$ kein Körper ist ((0) ist kein maximales Ideal), und $\deg(g) > 0$.

Wir zeigen, dass (die Bilder von) $\{1, X, \ldots, X^{n-1}\}$ ein K-Vektorraum Erzeugendensystem von $K(a)$ bilden. Insbesondere ist dann $[K(a)\colon K] \leq n < \infty$. Da $K(a) = K[a]$, sind die X^i für $i \geq 0$ ein Erzeugendensystem von $K(a)$. Wir beweisen durch eine Induktion nach i, dass sich X^i als Linearkombination von $1, X, \ldots, X^{n-1}$ darstellen lässt. Daraus folgt die Behauptung

Für $i < n$ ist dies trivial, also sei nun $i \geq n$. Da $g(a) = 0$, existiert eine Gleichung

$$X^n = -\sum_{i=0}^{n-1} a_i X^i \text{ in } K[X]/(g).$$

Dann ist

$$X^i = X^n X^{i-n} = -\sum_{j=0}^{n-1} a_j X^j X^{i-n}.$$

Nach der Induktionsannahme lässt sich $X^j X^{i-n}$ als Linearkombination von $1, X, \ldots, X^{n-1}$ darstellen und daher auch X^i.

(iii) $\Rightarrow$ (i): Da $[K(a)\colon K] < \infty$ gilt, sind die Elemente $1, a, a^2, \ldots$ linear abhängig. Daher existieren $a_i \in K$ mit

$$\sum_{i=0}^{n} a_i a^i = 0$$

Definiere $f = \sum_{i=0}^{n} a_i X^i \in K[X]$. Dann ist a algebraisch über K. □

Korollar 1.14. Sei L/K eine Körpererweiterung und $a \in L$. Dann gilt:

$$[K(a)\colon K] = [a\colon K].$$

Beweis. Ist a transzendent über K, dann gilt $[a\colon K] = \infty$ nach Definition und $[K(a)\colon K] = \infty$ nach 1.13.

Sei nun a algebraisch über K mit Minimalpolynom $f = \sum_{i=0}^{n} a_i X$, $a_n = 1$. Dann ist per Definition $[a\colon K] = n$. Im Beweis von 1.13 wurde schon gezeigt, dass $K(a) = K + Ka + \ldots + Ka^{n-1}$. Es bleibt zu zeigen, dass $1, a, \ldots, a^{n-1}$ linear

unabhängig über K sind. Wären $1, a, \dots, a^{n-1}$ linear abhängig, so würden $b_i \in K$ existieren mit

$$\sum_{i=0}^{n-1} b_i a^i = 0.$$

Definiere $g = \sum_{i=0}^{n-1} b_i X^i \in K[X]$. Dann gilt $g(a) = 0$ und $\deg(g) < n = \deg(f)$. Dies ist ein Widerspruch, da f das Minimalpolynom von a ist. □

Beispiel 1.15. Betrachte die Körpererweiterung $\mathbb{R}/\mathbb{Q}$. Sei p eine Primzahl und $0 \neq n \in \mathbb{N}$. Dann ist nach dem Eisensteinschen Kriterium das Polynom $f = X^n - p$ irreduzibel und somit das Minimalpolynom von $\sqrt[n]{p}$. Daher ist $\sqrt[n]{p}$ algebraisch mit $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. Insbesondere kann $\mathbb{R}/\mathbb{Q}$ nicht endlich sein.

Definition 1.16. Sei L/K eine Körpererweiterung.

(i) L/K heißt *algebraisch*, wenn jedes Element $a \in L$ algebraisch über K ist.
(ii) L/K heißt *endlich erzeugt*, wenn $a_1, \dots, a_n \in L$ existieren mit

$$L = K(a_1, \dots, a_n).$$

(iii) L/K heißt eine *einfache Körpererweiterung*, wenn ein $a \in L$ existiert mit $L = K(a)$.

Bemerkung 1.17. Es gilt:

$$K(a_1, \dots, a_n) = Q(K[a_1, \dots, a_n]) = \{\frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} : f, g \in K[X_1, \dots, X_n], g \neq 0\}.$$

Satz 1.18. Sei L/K eine Körpererweiterung. Dann sind folgende Aussagen äquivalent:

(i) $[L : K] < \infty$ (d.h. L/K ist endlich),
(ii) L/K ist algebraisch und L/K ist endlich erzeugt.

Beweis. (i)⇒(ii): Ist L/K endlich, so existieren $a_1, \dots, a_n \in L$ mit

$$L = Ka_1 + \cdots + Ka_n.$$

Es folgt direkt, dass $L = K(a_1, \dots, a_n)$ endlich erzeugt ist.

Ist nun $a \in L$ beliebig, dann gilt nach der Gradformel $[K(a) : K] < \infty$. Dann ist a algebraisch über K nach 1.13.

(ii)⇒(i): Seien $a_1, \dots, a_n \in L$ mit $L = K(a_1, \dots, a_n)$. Für alle i ist

$$K(a_1, \dots, a_i)/K(a_1, \dots, a_{i-1})$$

einfach und algebraisch, da a_i bereits algebraisch über K ist. Daher gilt

$$[K(a_1, \dots, a_i) : K(a_1, \dots, a_{i-1})] = n_i < \infty.$$

Nun beweist man durch eine einfache Induktion

$$[L : K] = \prod_i n_i < \infty.$$

Daher ist L/K endlich. □

Korollar 1.19. Jede endliche Körpererweiterung ist algebraisch.

Bemerkung 1.20. Aus einer endlich erzeugten Körpererweiterungen L/K folgt nicht, dass L/K endlich ist. Betrachte etwa $\mathbb{Q}(e)/\mathbb{Q}$. Es gibt algebraische Körpererweiterungen, die nicht endlich sind.

Lemma 1.21. Sei L/K eine Körpererweiterung. Definiere

$$\overline{K} = \{a \in L \colon a \text{ algebraisch über } K\}.$$

Dann ist $\overline{K}$ ein Körper. Dieser heißt der *algebraische Abschluss* von K in L.

Beweis. Seien $a, b \in \overline{K}$ und $b \neq 0$. Behauptung: $a+b, a-b, ab, ab^{-1} \in \overline{K}$. Daraus folgt dann, dass $\overline{K}$ ein Körper ist.

Es gilt $a+b, a-b, ab, ab^{-1} \in K(a,b)$. Wir zeigen, dass $K(a,b)/K$ algebraisch ist. Daraus folgt die Behauptung.

Es genügt zu zeigen, dass $[K(a,b) : K] < \infty$ gilt. Da a algebraisch über K ist, gilt $[K(a) : K] < \infty$.

Sei $g \in K[X]$ das Minimalpolynom von b über K. Es gilt $g(b) = 0$. Ferner ist $g \in K(a)[X]$. Also ist b algebraisch über $K(a)$. Sei $f \in K(a)[X]$ das Minimalpolynom von b über $K(a)$. Wir wissen, dass $f|g$ in $K(a)[X]$. Daher gilt

$$[K(a,b) : K(a)] \leq [K(b) : K] < \infty$$

Nach der Gradformel folgt

$$[K(a,b) : K] = [K(a,b) : K(a)][K(a) : K] < \infty.$$

□

Beispiel 1.22. Sei etwa

$$\overline{\mathbb{Q}} = \{a \in \mathbb{C} \colon a \text{ algebraisch über } \mathbb{Q}\}.$$

Es ist $\overline{\mathbb{Q}}/\mathbb{Q}$ algebraisch. Aber $[\overline{\mathbb{Q}} \colon \mathbb{Q}] = \infty$, da etwa für eine Primzahl p und $0 \neq n \in \mathbb{N}$ immer $\sqrt[n]{p} \in \overline{\mathbb{Q}}$ mit $[\mathbb{Q}(\sqrt[n]{p}) \colon \mathbb{Q}] = n$ gilt.

Korollar 1.23. Seien M/L und L/K Körpererweiterungen. Dann sind folgende Aussagen äquivalent:

(i) M/K ist algebraisch,
(ii) M/L und L/K sind algebraisch.

Beweis. Ist M/K ist algebraisch, so folgt direkt, dass M/L und L/K algebraisch sind.

Seien nun M/L und L/K algebraisch. Wähle $a \in M$ beliebig. Da a algebraisch über L ist, existiert ein Polynom $0 \neq f = \sum_{i=0}^{n} a_i X^i \in L[X]$ mit $f(a) = 0$. Dann ist a bereits über dem Körper $K(a_0, \ldots, a_n)$ algebraisch. Daraus folgt

$$[K(a_0, \ldots, a_n, a) : K(a_0, \ldots, a_n)] < \infty.$$

Da L/K algebraisch ist, sind die Elemente a_i algebraisch über K. Eine Induktion zeigt

$$[K(a_0, \ldots, a_n) : K] < \infty.$$

Nach der Gradformel gilt nun

$$[K(a_0, \ldots, a_n, a) : K] = [K(a_0, \ldots, a_n, a) : K(a_0, \ldots, a_n)][K(a_0, \ldots, a_n) : K] < \infty,$$

also ist $K(a_0, \ldots, a_n, a)$ algebraisch über K. Dies bedeutet speziell, dass a algebraisch über K ist. □

2. Der algebraische Abschluss eines Körpers

Definition 2.1. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes Polynom $f \in K[X]$ mit $\deg(f) > 0$ eine Nullstelle in K besitzt.

Beispiel 2.2. *(Gauß)* Der Körper der komplexen Zahlen $\mathbb{C}$ ist algebraisch abgeschlossen.

Satz 2.3. Sei K ein Körper und $0 \neq f \in K[X]$ mit $\deg(f) > 0$. Dann gibt es eine endliche Körpererweiterung L/K und ein $a \in L$ mit $f(a) = 0$. Ist f irreduzibel, so kann $L = K[X]/(f)$ gewählt werden.

Beweis. Ist f nicht irreduzibel, so wähle einen irreduziblen Faktor von f.

Also kann o.E. angenommen werden, dass f irreduzibel ist. Dann ist (f) ein maximales Ideal und $L = K[X]/(f)$ ein Körper mit $[L : K] = \deg(f) < \infty$. Man bilde die Komposition von Abbildungen

$$K \hookrightarrow K[X] \xrightarrow{\varepsilon} K[X]/(f) = L,$$

wobei ε der kanonische Epimorphismus ist. Die resultierende Abbildung $K \longrightarrow L$ ist injektiv und wir können L als Erweiterungskörper von K auffassen, indem wir K mit seinem Bild in L identifizieren. Sei nun $a = \varepsilon(X)$. Ist $f = \sum_{i=0}^{n} b_i X^i \in K[X]$, dann gilt

$$f(a) = \sum_{i=0}^{n} b_i a^i = \varepsilon(\sum_{i=0}^{n} b_i X^i) = \varepsilon(f) = 0.$$

D.h. a ist Nullstelle von f. □

Satz 2.4. Sei K ein Körper. Dann sind folgende Aussagen äquivalent:

(i) K ist algebraisch abgeschlossen.
(ii) Jedes Polynom $f \in K[X]$ mit $\deg(f) > 0$ zerfällt in Linearfaktoren.
(iii) Falls $f \in K[X]$ irreduzibel ist, dann folgt $\deg(f) = 1$.
(iv) Ist L/K algebraisch, so folgt $L = K$.

Beweis. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii): Trivial.

(iii) $\Rightarrow$ (iv): Sei $a \in L$. Da a algebraisch über K ist, existiert ein Minimalpolynom $f \in K[X]$ mit $f(a) = 0$. Nun ist f irreduzibel, hat also nach Voraussetzung den Grad 1. Somit ist $f = X + b$ mit $b \in K$. Dann gilt

$$0 = f(a) = a + b \Leftrightarrow a = -b \in K.$$

Insgesamt folgt $L = K$.

(iv) $\Rightarrow$ (i): Sei $f \in K[X]$ mit $\deg(f) > 0$. Nach 2.3 existiert ein Körper L und ein $a \in L$ mit $f(a) = 0$. Nun ist $K(a)/K$ algebraisch, also $K(a) = K$ und insbesondere $a \in K$. □

Definition 2.5. Sei K ein Körper. Ein Körper $\overline{K}$ heißt *algebraischer Abschluss* von K, wenn gilt

(i) $\overline{K}/K$ ist algebraisch,

(ii) $\overline{K}$ ist algebraisch abgeschlossen.

Satz 2.6. Sei K ein Körper. Dann besitzt K einen algebraischen Abschluss.

Beweis. Wir beweisen den Satz in drei Schritten:

(i) Es existiert eine Körpererweiterung L_1/K, so dass alle $f \in K[X]$ mit $\deg(f) > 0$ eine Nullstelle in L_1 besitzen.

(ii) Betrachte die Kette

$$K \subseteq L_1 \subseteq \ldots \subseteq L_n \subseteq \ldots,$$

wobei alle $f \in L_n[X]$ mit $\deg(f) > 0$ eine Nullstelle in L_{n+1} besitzen. Definiere $L = \bigcup L_n$. Dann ist L ein algebraisch abgeschlossener Körper.

(iii) Sei $\overline{K}$ der algebraische Abschluss von K in L. Dann ist $\overline{K}$ ein algebraischer Abschluss von K.

Zu (i): Sei S die Menge der Polynome $f \in K[X]$ mit $\deg(f) > 0$ und $M = K[\{X_f\}_{f \in S}]$. Betrachte das Ideal $I = (f(X_f)\colon f \in S) \subseteq M$.

Behauptung: $I \neq M$. Angenommen $I = M$. Dann existieren $f_1, \ldots, f_n \in S$ und $g_1, \ldots, g_n \in M$ mit

$$1 = f_1(X_{f_1})g_1 + \cdots + f_n(X_{f_n})g_n.$$

In dieser Gleichung kommen nur endlich viele Variablen $X_1, \ldots, X_m$ vor und o.E. gilt $X_i = X_{f_i}$, also

$$1 = f_1(X_1)g_1(X_1, \ldots, X_m) + \cdots + f_n(X_n)g_n(X_1, \ldots, X_m).$$

Es gibt einen Körper N/K und Elemente $a_1, \ldots, a_n \in N$ mit $f_i(a_i) = 0$. Dann folgt jedoch der Widerspruch

$$1 = f_1(a_1)g_1(a_1, \ldots, a_n, X_{n+1} \ldots, X_m) + \cdots f_n(a_n)g_n(a_1, \ldots, a_n, X_{n+1} \ldots, X_m) = 0.$$

Also ist $I \neq M$. Daher existiert ein maximales Ideal $I \subseteq J \subseteq M$. Definiere

$$L_1 = M/J \text{ und } \varepsilon\colon M \longrightarrow L_1, \quad g \mapsto g + J.$$

Dann ist klar, dass L_1 ein Körper ist. Sei $f \in K[X]$ mit $\deg(f) > 0$. Dann gilt $f \in S$ und

$$f(X_f + J) = \varepsilon(f(X_f)) = 0.$$

Somit hat f die Nullstelle $X_f + J \in L_1$.

Zu (ii): Zu zeigen ist, dass L algebraisch abgeschlossen ist. Sei $f \in L[X]$ mit $\deg(f) > 0$. Das Polynom f besitzt nur endlich viele Koeffizienten $a_i \in L = \bigcup L_n$. Also gibt es ein n mit $f \in L_n[X]$. Nach Konstruktion existiert ein $a \in L_{n+1} \subseteq L$ mit $f(a) = 0$. Daher folgt die Behauptung.

Zu (iii): Da $\overline{K}/K$ algebraisch ist, bleibt zu zeigen, dass $\overline{K}$ algebraisch abgeschlossen ist.

Sei $f \in \overline{K}[X]$ mit $\deg(f) > 0$. f besitzt nur endlich viele Koeffizienten

$$c_0, \ldots, c_n \in \overline{K}.$$

Sei $M = K(c_0, \dots, c_n) \subseteq \overline{K}$. Dann ist M eine endliche algebraische Erweiterung von K, da die c_i algebraisch über K sind. Sei $a \in L$ eine Nullstelle von f. Dann ist a algebraisch über M. Es gilt

$$[M(a) : M] < \infty \text{ und } [M : K] < \infty.$$

Dann folgt nach der Gradformel

$$[M(a) : K] = [M(a) : M][M : K] < \infty.$$

Also ist $M(a)/K$ algebraisch und insbesondere ist a algebraisch über K. Somit ist $a \in \overline{K}$ eine Nullstelle von f.

Dies zeigt, dass $\overline{K}$ ein algebraischer Abschluss von K ist. □

Bemerkung 2.7. Wie werden später sehen, dass der algebraische Abschluss bis auf Isomorphie eindeutig ist.

Satz 2.8. Seien K, K' Körper, $\varphi\colon K \to K'$ ein Körperisomorphismus,

$$\Phi\colon K[X] \to K'[X], \quad \sum a_i X^i \mapsto \sum \varphi(a_i) X^i$$

der induzierte Isomorphismus, $f \in K[X]$ ein irreduzibles Polynom und $f' = \Phi(f)$ irreduzibel. Sei a eine Nullstelle von f in einem Erweiterungskörper von K und sei a' eine Nullstelle von f' in einem Erweiterungskörper von K'. Dann gibt es genau einen Körperisomorphismus $\overline{\varphi}\colon K(a) \to K'(a')$ mit

(i) $\overline{\varphi}_{|K} = \varphi$,
(ii) $\overline{\varphi}(a) = a'$.

Also ist folgendes Diagramm kommutativ:

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & K' \\ \downarrow & & \downarrow \\ K(a) & \xrightarrow[\overline{\varphi}]{} & K'(a') \end{array}$$

Beweis. Sei $\varepsilon\colon K[X] \to K(a), h(X) \mapsto h(a)$ der Einsetzungshomomorphismus. Da a algebraisch über K ist, folgt $K(a) = K[a]$ und daher ist ε surjektiv. Da $K[X]$ ein Hauptidealring ist, folgt $\operatorname{Ker}(\varepsilon) = (f)$, da f irreduzibel ist. Nach dem Isomorphiesatz induziert ε einen Isomorphismus

$$\varphi_1\colon K[X]/(f) \to K(a), \quad h(X) + (f(X)) \mapsto h(a).$$

Analog gibt es einen Isomorphismus

$$\varphi_2\colon K'[X]/(f') \to K'(a'), \quad h(X) + (f'(X)) \mapsto h(a').$$

Da Φ ein Isomorphismus ist und $\Phi(f) = f'$ gilt, wird ein Isomorphismus

$$\psi\colon K[X]/(f) \to K'[X]/(f')$$

induziert. Definiere den Isomorphismus

$$\overline{\varphi} = \varphi_2 \circ \psi \circ \varphi_1^{-1}\colon K(a) \to K'(a').$$

Da

$$\varphi_{1|K} = \mathrm{id}_{|K}, \quad \varphi_{2|K} = \mathrm{id}_{|K}, \quad \psi_{|K} = \varphi$$

gilt, folgt $\overline{\varphi}_{|K} = \varphi$. Ferner

$$\overline{\varphi}(a) = \varphi_2 \circ \psi \circ \varphi_1^{-1}(a) = \varphi_2 \circ \psi(X + (f)) = \varphi_2(X + (f')) = a'.$$

Sei λ ein weiterer solcher Isomorphismus. Ist $b \in K(a), b = \sum c_i a^i$ mit $c_i \in K$. Dann folgt

$$\lambda(b) = \lambda(\sum c_i a^i) = \sum \lambda(c_i)\lambda(a)^i = \sum \varphi(c_i)(a')^i = \overline{\varphi}(b).$$

□

Korollar 2.9. Seien k, L Körper, L algebraisch abgeschlossen, $0 \neq \sigma\colon k \longrightarrow L$ ein Körperhomomorphismus, a ein algebraisches Element von k in einem Erweiterungskörper von k und $f = \sum b_i X^i \in k[X]$ das Minimalpolynom von a über k. Dann ist die Anzahl der verschiedenen Fortsetzungen von σ auf $k(a)$, d.h. Körperhomomorphismen $\Sigma\colon k(a) \longrightarrow L$ mit $\Sigma_{|k} = \sigma$, gleich der Anzahl der verschiedenen Nullstellen von $f^\sigma = \sum \sigma(b_i)X^i$ in L. Insbesondere ist die Anzahl der Fortsetzungen kleiner oder gleich $[k(a) : k]$.

Beweis. Seien $a_1, \ldots, a_n$ die verschiedenen Nullstellen von f^σ. Nach 2.8 existieren Isomorphismen $\overline{\Sigma}_i\colon k(a) \longrightarrow k'(a_i)$ mit $k' = \sigma(k) \subseteq L$, $\overline{\Sigma}_i(a) = a_i$ und $\overline{\Sigma}_{i|k} = \sigma$. Dann haben die Abbildungen $\Sigma_i = Inklusion \circ \overline{\Sigma}_i\colon k(a) \longrightarrow L$ die gewünschten Eigenschaften. Für $i \neq j$ ist $\Sigma_i(a) = a_i \neq a_j = \Sigma_j(a)$, also $\Sigma_i \neq \Sigma_j$.

Sei nun Σ eine beliebige Fortsetzung von σ. Dann gilt

$$0 = \Sigma(f(a)) = f^\sigma(\Sigma(a)),$$

d.h. $\Sigma(a)$ ist eine Nullstelle von f^σ. Wegen der Eindeutigkeitsaussage in 2.8 gilt nun $\Sigma = \Sigma_i$ für ein i. □

Korollar 2.10. Seien k, L Körper, L algebraisch abgeschlossen, $0 \neq \sigma\colon k \longrightarrow L$ ein Körperhomomorphismus und K/k eine beliebige algebraische Körpererweiterung. Dann gibt es eine Fortsetzung $\Sigma\colon K \longrightarrow L$ von σ.

Beweis. Sei S die Menge aller Paare (F, τ) mit einem Zwischenkörper $k \subseteq F \subseteq K$ und $\tau\colon F \longrightarrow L$ ist Fortsetzung von σ. Wir definieren eine partielle Ordnung auf diesen Paaren.

$$(F, \tau) \leq (F', \tau') \Leftrightarrow F \subseteq F' \text{ und } \tau'_F = \tau.$$

Dann ist $(S, \leq)$ eine partiell geordnete nicht leere Menge, da $(k, \sigma) \in S$.

Sei $\{(F_i, \tau_i)\}$ eine vollständig geordnete Teilmenge von S. Definiere $F = \bigcup F_i$ und für $a \in F, a \in F_i$ $\tau(a) = \tau_i(a)$. Dann ist ist $(F, \tau) \in S$ eine obere Schranke der Teilmenge.

Nach dem Zornschen Lemma folgt, dass ein maximales Element $(E, \varphi) \in S$ existiert. Angenommen: $E \neq K$. Dann gibt es ein $a \in K \setminus E$. Da K/k algebraisch ist, folgt, dass a algebraisch über E ist. Sei f das Minimalpolynom von a über E und b eine Nullstelle von f^φ in L. Nach 2.9 gibt es eine Fortsetzung Φ von φ auf $E(a)$ mit $\Phi(a) = b$. Dies ist ein Widerspruch zu der Maximalität von (E, φ), da dann $(E, \varphi) < (E(a), \Phi)$.

Also ist $E = K$ und es folgt die Behauptung. □

Satz 2.11. Sei K ein Körper und $\overline{K}_1$ und $\overline{K}_2$ algebraische Abschlüsse von K. Dann gibt es einen Isomorphismus $\Sigma\colon \overline{K}_1 \longrightarrow \overline{K}_2$, welcher id_K fortsetzt.

Beweis. Betrachte die Abbildung

$$\varphi\colon K \longrightarrow \overline{K}_2.$$

Da $\overline{K}_2$ algebraisch abgeschlossen ist, existiert nach 2.10 eine Fortsetzung

$$\Sigma\colon \overline{K}_1 \longrightarrow \overline{K}_2$$

mit $\Sigma_{|K} = \mathrm{id}_K$.

Σ ist injektiv, da die Abbildung ein nicht trivialer Körperhomomorphismus ist. Mit $\overline{K}_1$ ist auch $\Sigma(\overline{K}_1)$ algebraisch abgeschlossen. Da $\overline{K}_2/\Sigma(\overline{K}_1)$ algebraisch ist, folgt daher $\overline{K}_2 = \Sigma(\overline{K}_1)$. Somit ist Σ ein Isomorphismus.

□

3. Zerfällungskörper, normale Körpererweiterungen

Definition 3.1. Seien L/K, L'/K Körpererweiterungen und $\varphi\colon L \longrightarrow L'$ ein Körperhomomorphismus. φ heißt ein *K-Homomorphismus*, wenn φ eine Fortsetzung der Identität von K ist, d. h. $\varphi_{|K} = \mathrm{id}_K$.

Definition 3.2. Sei K ein Körper und $f_1, \ldots, f_n \in K[X]$ mit $\deg(f_i) > 0$. Ein Erweiterungskörper L von K heißt *Zerfällungskörper* (über K) von $f_1, \ldots, f_n$, wenn folgendes gilt:

(i) Jedes f_i zerfällt über L vollständig in Linearfaktoren.
(ii) Die Körpererweiterung L/K wird von den Nullstellen der f_i erzeugt.

Bemerkung 3.3. Es gilt:

(i) Ist $f \in K[X]$ mit $\deg(f) > 0$ und sind $a_1, \ldots, a_n$ die Nullstellen von f in einem algebraischen Abschluss $\overline{K}$ von K, so ist $L = K(a_1, \ldots, a_n)$ ein Zerfällungskörper von K.
(ii) Sind $f_1, \ldots, f_n \in K[X]$ mit $\deg(f_i) > 0$, so ist der Zerfällungskörper von $f_1, \ldots, f_n$ gleich dem Zerfällungskörper von $f_1 \cdots f_n$. Also kann man o.E. voraussetzen, dass der Zerfällungskörper stets bzgl. eines Polynoms gewählt wird.

Satz 3.4. Seien K, K' Körper, $f \in K[X]$, $\deg(f) > 0$, $\varphi\colon K \longrightarrow K'$ ein Körperisomorphismus, L ein Zerfällungskörper von f über K und L' ein Zerfällungskörper von f^φ über K'. Dann besitzt φ eine Fortsetzung $\psi\colon L \longrightarrow L'$ und ψ ist ein Isomorphismus. Ferner:

(i) Jeder Isomorphismus $\psi\colon L \longrightarrow L'$, der φ fortsetzt, bildet die Nullstellen von f auf die Nullstellen von f^φ ab.
(ii) Sei g ein irreduzibler Faktor von f in $K[X]$, a eine Nullstelle von g in L und b eine Nullstelle von g^φ. Dann gibt es eine Fortsetzung $\psi\colon L \longrightarrow L'$ mit $\psi(a) = b$.

Beweis. Aus (i) und (ii) folgt insbesondere die Existenz einer Fortsetzung von φ.

Zu (i): Sei $\psi\colon L \longrightarrow L'$ ein Isomorphismus, der φ fortsetzt und a eine Nullstelle von f. Dann gilt

$$0 = \psi(0) = \psi(f(a)) = f^{\varphi}(\psi(a)).$$

Also ist $\psi(a)$ eine Nullstelle von f^{φ}.

Zu (ii): Nach 2.8 existiert ein Isomorphismus $\overline{\varphi}\colon K(a) \longrightarrow K(b)$, der φ fortsetzt mit $\overline{\varphi}(a) = b$.

Nun ist L auch ein Zerfällungskörper von f über $K(a)$ und L' ein Zerfällungskörper von f^{φ} über $K(b)$. Es ist $L/K(a)$ algebraisch, daher existiert nach 2.10 ein Fortsetzung $\psi\colon L \longrightarrow \overline{K}$ mit $L' \subseteq \overline{K}$ algebraisch abgeschlossen.

Seien $a_1, \ldots, a_n$ die Nullstellen von f. Dann sind $\psi(a_1), \ldots, \psi(a_n)$ die Nullstellen von f^{φ}. Ferner

$$\psi(L) = \psi(K(a_1, \ldots, a_n)) = K(\psi(a_1), \ldots, \psi(a_n)) = L'.$$

Dies bedeutet, das $\psi\colon L \longrightarrow L'$ ein Isomorphismus ist. □

Beispiel 3.5. Sei $f = (X^2 - 2)(X^2 + 1) \in \mathbb{Q}[X]$. Dann ist $\mathbb{Q}(i, \sqrt{2})$ ein Zerfällungskörper von f. Da $(X^2 - 2)$ irreduzibel über $\mathbb{Q}$ ist, existiert ein Isomorphismus

$$\varphi\colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}), \sqrt{2} \mapsto -\sqrt{2}.$$

Nun ist $X^2 + 1$ irreduzibel über $\mathbb{Q}(\sqrt{2})$, also existiert ein Isomorphismus

$$\psi\colon \mathbb{Q}(i, \sqrt{2}) \longrightarrow \mathbb{Q}(i, \sqrt{2}), i \mapsto -i,$$

der φ fortsetzt.

Korollar 3.6. Sei K ein Körper, $f \in K[X]$ mit $\deg(f) > 0$ und L, L' Zerfällungskörper von f. Dann existiert ein Isomorphismus $\psi\colon L \longrightarrow L'$, welcher id_K fortsetzt.

Beweis. Wende 3.4 auf $\varphi = \mathrm{id}_K$ an. □

Definition 3.7. Eine algebraische Körpererweiterung L/K heißt *normal*, wenn jedes irreduzible Polynom $f \in K[X]$, das in L eine Nullstelle besitzt, über L in Linearfaktoren zerfällt.

Beispiel 3.8. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist nicht normal. Denn das Polynom $f = X^4 - 2$ hat die Nullstellen $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$ und $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$.

Satz 3.9. Sei L/K eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent:

(i) L/K ist normal.
(ii) L ist Zerfällungskörper eines Polynoms $f \in K[X]$.
(iii) Falls L'/L eine Körpererweiterung und $\varphi\colon L \longrightarrow L'$ ein K-Homomorphismus ist, dann gilt $\varphi(L) \subseteq L$.

Beweis. Da L/K endlich ist folgt, dass L/K endlich erzeugt und algebraisch ist. D.h. $L = K(a_1, \ldots, a_n)$ mit a_i algebraisch über K. Sei $p_i \in K[X]$ das Minimalpolynom von a_i über K.

(i) $\Rightarrow$ (ii): Sei

$$f = p_1 \cdots p_n.$$

p_i zerfällt in L in Linearfaktoren, da L/K normal ist. Somit zerfällt auch f in L in Linearfaktoren. $a_1, \dots, a_n$ sind Nullstellen von f. Also ist L ein Zerfällungskörper von f.

(ii) $\Rightarrow$ (iii): Sei L Zerfällungskörper von f und $\varphi\colon L \longrightarrow L'$ ein K-Homomorphismus. Seien $a_1, \dots, a_n$ die Nullstellen von f. Dann sind $\varphi(a_1), \dots, \varphi(a_n)$ Nullstellen von f, da

$$0 = \varphi(f(a_i)) = f^{\varphi}(\varphi(a_i)) = f(\varphi(a_i))$$

gilt. Also

$$\varphi(L) = \varphi(K(a_1, \dots, a_n)) = K(\varphi(a_1), \dots, \varphi(a_n)) \subseteq L.$$

(iii) $\Rightarrow$ (i): Sei f irreduzibel und a eine Nullstelle von f. Dann ist

$$L = K(a_1, \dots, a_n) = K(a, a_1, \dots, a_n).$$

Sei $g = fp_1 \cdots p_n$, $L \subseteq L'$ ein Zerfällungskörper von g und b eine Nullstelle von f in L'. Wegen 3.4 existiert ein K-Homomorphismus $\varphi\colon L \longrightarrow L'$ mit $\varphi(a) = b$. Wegen der Voraussetzung gilt $\varphi(L) \subseteq L$ und somit $b \in L$. □

Bemerkung 3.10. Die Eigenschaft normal ist nicht transitiv. Die Körpererweiterungen $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ sind normal. Aber $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist nicht normal (siehe 3.8).

4. Der Hauptsatz der Galoistheorie

Definition 4.1. Sei K ein Körper und G eine Untergruppe von der Automorphismengruppe $\mathrm{Aut}(K)$ von K. Definiere

$$K^G = \{a \in K\colon \varphi(a) = a \text{ für alle } \varphi \in G\}.$$

Der Teilkörper $K^G \subseteq K$ heißt der *Fixkörper* von G.

Definition 4.2. Sei L/K eine Körpererweiterung. L/K heißt eine *Galoiserweiterung*, wenn eine endliche Untergruppe $G \subseteq \mathrm{Aut}(L)$ existiert mit $K = L^G$.

Beispiel 4.3. Betrachte:

(i) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist galoisch.

Beweis. Sei $f = X^2 - 2$. Die Nullstellen von f sind $\pm\sqrt{2}$. Also existiert ein $\mathbb{Q}$-Homomorphismus

$$\varphi\colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}), \quad \sqrt{2} \mapsto -\sqrt{2}.$$

Definiere $G = \langle\varphi\rangle$. Sei nun $x = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ beliebig. Es ist

$$\varphi(x) = x \Leftrightarrow a + b\sqrt{2} = a - b\sqrt{2} \Leftrightarrow b = 0 \Leftrightarrow x \in \mathbb{Q}.$$

Also ist $\mathbb{Q}(\sqrt{2})^G = \mathbb{Q}$. □

(ii) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht galoisch.

Beweis. Annahme: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist eine Galoiserweiterung, d.h. es existiert eine endliche Untergruppe $G \subseteq \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$ mit $\mathbb{Q}(\sqrt[3]{2})^G = \mathbb{Q}$.

Behauptung: $G = \{\mathrm{id}\}$. Dann folgt der Widerspruch

$$\mathbb{Q}(\sqrt[3]{2})^G = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}.$$

Es bleibt die Behauptung zu zeigen. Sei $\varphi \in G$ beliebig und $f = X^3 - 2$. Beachte, dass f irreduzibel ist und $\varphi_{|\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Es ist $\varphi(\sqrt[3]{2})$ eine Nullstelle von f. Die Nullstellen ungleich $\sqrt[3]{2}$ von f liegen in $\mathbb{C} \setminus \mathbb{R}$. Aber $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Also muss $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$ gelten. Dann ist $\varphi = \mathrm{id}$. □

Definition 4.4. Sei K ein Körper und G eine multiplikative Gruppe. Ein Gruppenhomomorphismus $\sigma : G \longrightarrow K^*$ heißt *Charakter* von G in K.

Satz 4.5. *(Lineare Unabhängigkeit der Charaktere)* Sei K ein Körper, G eine multiplikative Gruppe und $\sigma_1, \ldots, \sigma_n$ paarweise verschiedene Charaktere von G in K. Seien $a_1, \ldots, a_n \in K$ mit $\sum_{i=1}^n a_i \sigma_i(x) = 0$ für alle $x \in G$. Dann gilt $a_1 = \ldots = a_n = 0$.

Beweis. Wir beweisen den Satz durch eine Induktion nach n. Für $n = 1$ ist die Aussage trivial, da $\sigma_1(x) \neq 0$ für alle $x \in G$ gilt.

Sei nun $n > 1$. Es muss wegen der Voraussetzung ein $y \in G$ existieren mit $\sigma_1(y) \neq \sigma_n(y)$. Nun gelten folgende Gleichungen

$$\sum_{i=1}^{n} a_i \sigma_n(y) \sigma_i(x) = 0. \tag{1}$$

$$\sum_{i=1}^{n} a_i \sigma_i(y) \sigma_i(x) = 0. \tag{2}$$

(2)-(1) ergibt

$$\sum_{i=1}^{n-1} a_i (\sigma_i(y) - \sigma_n(y)) \sigma_i(x) = 0 \text{ für alle } x \in G.$$

Nach der Induktionsannahme ist nun $a_i(\sigma_i(y) - \sigma_n(y)) = 0$ für $i = 1, \ldots, n-1$. Da $\sigma_1(y) \neq \sigma_n(y)$, folgt $a_1 = 0$. Also ist

$$\sum_{i=2}^{n} a_i \sigma_i(x) = 0 \text{ für alle } x \in G.$$

Wieder nach der Induktionsannahme folgt, dass $a_2 = \ldots = a_n = 0$. □

Satz 4.6. Sei L/K eine Körpererweiterung und $\sigma_1, \ldots, \sigma_n$ paarweise verschiedene Körperhomomorphismen $K \longrightarrow L$. Dann gilt:

(i) Die Abbildungen $\sigma_i : K^* \longrightarrow L^*$ sind Charaktere und

$$U = \{a \in K : a = \sigma_i(a) \text{ für } i = 1, \ldots, n\}$$

ist ein Teilkörper von K.

(ii) Es gilt $[K : U] \geq n$.

Beweis. Zu (i): Trivial.

Zu (ii): Angenommen $[K : U] = r < n$. Sei $w_1, \dots, w_r$ eine U-Basis von K. Das lineare Gleichungssystem

$$\sum_{i=1}^{n} \sigma_i(w_k) X_i = 0 \text{ für } k = 1, \dots, r$$

besitzt eine nicht triviale Lösung $(a_1, \dots, a_n) \in L^n$, da $r < n$. Also gilt

$$\sum_{i=1}^{n} \sigma_i(w_k) a_i = 0 \text{ für } k = 1, \dots, r$$

Sei $x = \sum_{k=1}^{r} c_k w_k \in K^*$ beliebig mit $c_k \in U$. Dann gilt

$$\sigma_i(x) = \sum_{k=1}^{r} c_k \sigma_i(w_k), \text{ da } \sigma_i \ U\text{-linear ist.}$$

Dann ist

$$\sum_{i=1}^{n} \sigma_i(x) a_i = \sum_{i=1}^{n} \sum_{k=1}^{r} a_i c_k \sigma_i(w_k) = \sum_{k=1}^{r} c_k (\sum_{i=1}^{n} a_i \sigma_i(w_k)) = 0.$$

Dies ist ein Widerspruch zu 4.5. □

Satz 4.7. *(Artin)* Sei L ein Körper, $G \subseteq \mathrm{Aut}(L)$ eine endliche Untergruppe und $K = L^G$. Dann gilt

$$[L : K] = \mathrm{ord}(G)$$

Beweis. Wir beweisen den Satz in drei Schritten:

(i) $[L : K] \geq \mathrm{ord}(G)$.

(ii) Definiere die *Spurabbildung* :

$$S \colon L \longrightarrow L, \quad x \mapsto \sum_{\sigma \in G} \sigma(x).$$

Dann gilt:

(a) S ist K-linear.

(b) $\mathrm{Im}(S) \subseteq K \subseteq L$.

(iii) $[L : K] \leq \mathrm{ord}(G)$.

Zu (i): Die Elemente von G können als Charaktere $L^* \longrightarrow L^*$ aufgefasst werden. Aus 4.6 folgt dann

$$[L : K] \geq \mathrm{ord}(G).$$

Zu (ii) (a): Sei $\sigma \in G$, $a \in K$ und $x \in L$. Dann gilt

$$\sigma(ax) = \sigma(a)\sigma(x) = a\sigma(x).$$

Dies war zu zeigen.

Zu (ii) (b): Sei $\tau \in G$ und $x \in L$. Dann gilt

$$\tau(S(x)) = \sum_{\sigma \in G} \tau \circ \sigma(x) = \sum_{\sigma \in G} \sigma(x) = S(x).$$

Somit ist $S(x) \in L^G = K$. Die Abbildung $S\colon L \longrightarrow K$ wird die *Spurabbildung* genannt. Es gilt $S_{|K} = |\mathrm{ord}(G)|\mathrm{id}_K$.

Zu (iii): Sei $\mathrm{ord}(G) = n$ und $G = \{\sigma_1, \dots, \sigma_n\}$. Seien nun $y_1, \dots, y_{n+1} \in L$. Wir zeigen, dass $y_1, \dots, y_{n+1}$ linear abhängig über K sind. Daraus folgt dann $[L : K] \leq \mathrm{ord}(G)$.

Das lineare Gleichungssystem

$$\sum_{k=1}^{n+1} \sigma_i^{-1}(y_k) X_k, \quad i = 1, \dots, n$$

besitzt eine nicht-triviale Lösung $(a_1, \dots, a_{n+1}) \in L^{n+1}$. O.E. gelte etwa $a_1 \neq 0$. Beachte, dass mit $(a_1, \dots, a_{n+1})$ auch stets $(za_1, \dots, za_{n+1})$ eine Lösung des Gleichungssystems ist.

Wegen der linearen Unabhängigkeit der Charaktere existiert ein $x \in L$ mit $S(x) \neq 0$. Setzen wir $z = xa_1^{-1}$, so können wir o.E. $S(a_1) \neq 0$ annehmen.

Multipliziert man die i-te Gleichung des obigen linearen Gleichungssystems mit σ_i, so erhalten wir

$$0 = \sum_{k=1}^{n+1} y_k \sigma_i(a_k), \quad i = 1, \dots, n.$$

Dann ist

$$\sum_{k=1}^{n+1} y_k S(a_k) = \sum_{k=1}^{n+1} y_k \sum_{i=1}^{n} \sigma_i(a_k) = \sum_{i=1}^{n} (\sum_{k=1}^{n+1} y_k \sigma_i(a_k)) = 0$$

Es gilt $S(a_k) \in K$ und $S(a_1) \neq 0$. Also sind $y_1, \dots, y_{n+1}$ linear abhängig.

□

Definition 4.8. Sei L/K eine Körpererweiterung. Dann heißt

$$G(L/K) = \{\varphi \in \mathrm{Aut}(L)\colon \varphi_{|K} = \mathrm{id}_K\}$$

die *Galoisgruppe* von L/K.

Lemma 4.9. Sei L/K eine endliche Körpererweiterung. Dann ist

$$\mathrm{ord}(G(L/K)) \leq [L : K] < \infty.$$

Beweis. Seien $\sigma_1, \dots, \sigma_n \in G(L/K)$ paarweise verschieden und $U = L^G$. Dann gilt nach 4.6 $[L : U] \geq n$. Da aber $K \subseteq U$, folgt mit Hilfe der Gradformel

$$n \leq [L : U][U : K] = [L : K] < \infty,$$

dass

$$\mathrm{ord}(G(L/K)) \leq [L : K] < \infty$$

gilt. □

Lemma 4.10. Sei L/K eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent:

(i) L/K ist eine Galoiserweiterung.
(ii) $[L : K] = \mathrm{ord}(G(L/K))$.

Beweis. (i) $\Rightarrow$ (ii): Da L/K eine Galoiserweiterung ist, existiert eine endliche Untergruppe $G \subseteq \mathrm{Aut}(L)$ mit $K = L^G$. Da $G \subseteq G(L/K)$ gilt, folgt

$$L^G = K \subseteq L^{G(L/K)} \subseteq L^G = K.$$

Somit ist auch $K = L^{G(L/K)}$. Da $G(L/K)$ endlich ist, folgt dann aus 4.7.

$$[L : K] = [L : L^{G(L/K)}] = \mathrm{ord}(G(L/K)).$$

(ii) $\Rightarrow$ (i): Sei $U = L^{G(L/K)}$. Da $G(L/K)$ endlich ist, folgt aus 4.7 und der Voraussetzung

$$[L : U] = \mathrm{ord}(G(L/K)) = [L : K].$$

Nun ist aber $K \subseteq U$. Aus

$$[L : K] = [L : U][U : K]$$

sieht man, dass $[U : K] = 1$ gilt. Daher ist $K = U$ und L/K eine Galoiserweiterung. □

Satz 4.11. *(Hauptsatz der Galoistheorie)* Sei L/K eine endliche Galoiserweiterung, $\mathcal{K}$ die Menge der Zwischenkörper von L/K, $\mathcal{G}$ die Menge der Untergruppen von $G(L/K)$. Dann gilt, dass die Abbildungen

$$\alpha \colon \mathcal{K} \longrightarrow \mathcal{G}, \quad M \mapsto G(L/M)$$

und

$$\beta \colon \mathcal{G} \longrightarrow \mathcal{K}, \quad G \mapsto L^G$$

bijektiv und invers zueinander sind, d.h.

$$L^{G(L/M)} = M \text{ und } G(L/L^G) = G$$

für alle $M \in \mathcal{K}$ und $G \in \mathcal{G}$. Insbesondere besitzt eine endliche Galoiserweiterung nur endlich viele Zwischenkörper.

Beweis. Wir zeigen:

(i) $\beta \circ \alpha = id$.
(ii) $\alpha \circ \beta = id$.

Zu (i): Sei $M \in \mathcal{K}$ und $H = G(L/M)$. Wir müssen $M = L^H$ zeigen.

Es gilt $H \subseteq G(L/K)$. Sei $[G(L/K) : H] = r$ und $\varphi_1 H, \ldots, \varphi_r H$ die Linksnebenklassen von $G(L/K)/H$. Definiere

$$\psi_i = (\varphi_i)_{|M} \colon M \longrightarrow L.$$

Dann sind $\psi_1, \ldots, \psi_r$ paarweise verschiedene Körperhomomorphismen.

Es gilt

$$K \subseteq U = \{x \in M \colon x = \psi_1(x) = \ldots = \psi_r(x)\}.$$

Nach 4.6 gilt dann $[M : K] \geq [M : U] \geq r$. Dann folgt aus 4.10, dass

$$[L : M][M : K] = [L : K] = \mathrm{ord}(G(L/K)) = [G(L/K) : H]\mathrm{ord}(H)$$
$$= r[L : L^H] \leq [M : K][L : L^H].$$

Also $[L : M] \leq [L : L^H]$. Nun ist $M \subseteq L^H$ und es gilt immer $[L : M] \geq [L : L^H]$. Somit $[L : M] = [L : L^H]$ und daher $M = L^H$.

Zu (ii): Sei $H \in \mathcal{G}$ und $M = L^H$. Wir müssen $H = G(L/M)$ zeigen. Nun gilt trivialerweise $H \subseteq G(L/M)$. Nach (i) ist $M = L^{G(L/M)}$. Dann folgt aus 4.7

$$\operatorname{ord}(G(L/M)) = [L : M] = \operatorname{ord}(H),$$

also $H = G(L/M)$. □

Bemerkung 4.12. Es gilt:

(i) Für alle $M \in \mathcal{K}$ und $H \in \mathcal{G}$ ist

$$[L : M] = \operatorname{ord}(G(L/M)) \text{ und } [L : L^H] = \operatorname{ord}(H).$$

(ii) Ist L/K galoisch und $K \subseteq M \subseteq L$, so ist L/M galoisch. Dies gilt i. a. nicht für M/K.

(iii) Die Abbildungen α und β kehren die Inklusionen um, d.h.

$$M_1 \subseteq M_2 \Rightarrow G(L/M_1) \supseteq G(L/M_2)$$

und

$$H_1 \subseteq H_2 \Rightarrow L^{H_1} \supseteq L^{H_2}.$$

Beispiel 4.13. Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dann ist $[\mathbb{Q}(\sqrt{2}) : K] = 2$. Ferner $[L : \mathbb{Q}(\sqrt{2})] = 2$, da $X^2 - 3$ irreduzibel in $\mathbb{Q}(\sqrt{2})[X]$ ist. Insgesamt folgt

$$[L : K] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : K] = 4.$$

$G(L/K)$ besteht aus folgenden Abbildungen:

$$\begin{aligned}
&\mathrm{id}\colon \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}\\
&\tau_1\colon \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\\
&\tau_2\colon \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}\\
&\tau_3\colon \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}
\end{aligned}$$

(Es gilt $G(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Man sieht, dass $K = L^{G(L/K)}$ und L/K eine Galoiserweiterung ist.

Die Gruppe $G(L/K)$ hat die Untergruppen

$$G(L/K), \quad H_1 = \{\mathrm{id}, \tau_1\}, \quad H_2 = \{\mathrm{id}, \tau_2\}, \quad H_3 = \{\mathrm{id}, \tau_3\}, \quad \{\mathrm{id}\}.$$

Daher hat L/K folgende Zwischenkörper

$$L^{\{\mathrm{id}\}} = L, \quad L^{H_1}, \quad L^{H_2}, \quad L^{H_3}, \quad L^{G(L/K)} = K$$

mit den entsprechenden Inklusionen.

Aus Gradgründen gilt $L^{H_1} = \mathbb{Q}(\sqrt{2})$ und $L^{H_2} = \mathbb{Q}(\sqrt{3})$.

Behauptung: $L^{H_3} = \mathbb{Q}(\sqrt{6})$. Betrachte hierfür die Spurabbildung

$$S\colon L \to L^{H_3}, \quad x \mapsto \sum_{\sigma \in H_3} \sigma(x) = x + \tau_3(x).$$

Nun gilt

$$L^{H_3} = \frac{1}{2} S(L) = \mathbb{Q} + \mathbb{Q}S(\sqrt{2}) + \mathbb{Q}S(\sqrt{3}) + \mathbb{Q}S(\sqrt{6}).$$

Da aber

$$S(\sqrt{2}) = \sqrt{2} - \sqrt{2} = 0, \quad S(\sqrt{3}) = \sqrt{3} - \sqrt{3} = 0, \quad S(\sqrt{6}) = \sqrt{6} + \sqrt{6} = 2\sqrt{6},$$

gilt, folgt die Behauptung.

Satz 4.14. Sei L/K eine endliche Galoiserweiterung und $K \subseteq M \subseteq L$ ein Zwischenkörper. Dann sind folgende Aussagen äquivalent:

(i) M/K ist eine Galoiserweiterung.
(ii) Für alle $\sigma \in G(L/K)$ gilt $\sigma(M) = M$ (Elemente von M müssen hierbei nicht fixiert werden !).
(iii) $G(L/M) \triangleleft G(L/K)$.

Gelten die äquivalenten Bedingungen, so ist

$$G(M/K) \cong G(L/K)/G(L/M).$$

Beweis. (i) $\Rightarrow$ (ii): Sei M/K galoisch mit Galoisgruppe $G(M/K) = \{\varphi_1, \ldots, \varphi_n\}$. Definiere für $i = 1, \ldots, n$

$$\psi_i \colon M \xrightarrow{\varphi_i} M \hookrightarrow L.$$

Angenommen es existiert ein $\sigma \in G(L/K)$ mit $\sigma(M) \neq M$. Dann ist $\sigma \neq \psi_i$ für $i = 1, \ldots, n$. Es gilt

$$K \subseteq M' = \{x \in M \colon x = \psi_1(x) = \ldots = \psi_n(x) = \sigma(x)\}.$$

Dann ist aber nach 4.10

$$[M : K] \geq [M : M'] \geq n + 1.$$

Dies ist ein Widerspruch zu M/K galoisch mit

$$[M : K] = \mathrm{ord}(G(M/K)) = n.$$

(ii) $\Rightarrow$ (iii): Sei $\tau \in G(L/M)$ und $\sigma \in G(L/K)$. Wir müssen $\sigma\tau\sigma^{-1} \in G(L/M)$ zeigen. Sei $x \in M$ beliebig. Dann gilt

$$\sigma\tau\sigma^{-1}(x) = \sigma(\tau(\sigma^{-1}(x))) = \sigma(\sigma^{-1}(x)) = x,$$

da nach Voraussetzung $\sigma^{-1}(x) \in M$.

(iii) $\Rightarrow$ (i): 1. Behauptung: Sei $\sigma \in G(L/K)$, dann ist $\sigma_{|M} \in G(M/K)$. Sei $x \in M$ und $\tau \in G(L/M)$. Dann folgt aus der Voraussetzung, dass $\sigma^{-1}\tau\sigma \in G(L/M)$ und daher $x = \sigma^{-1}\tau\sigma(x)$. Also gilt

$$\sigma(x) = \tau\sigma(x) \text{ für alle } \tau \in G(L/M).$$

Nun ist L/M galoisch und $M = L^{G(L/M)}$ und somit ist $\sigma(x) \in M$. Dies zeigt die erste Behauptung.

Definiere

$$\varphi \colon G(L/K) \to G(M/K), \quad \sigma \mapsto \sigma_{|M}.$$

2. Behauptung: φ ist surjektiv. Es gilt $\mathrm{Ker}(\varphi) = G(L/M)$. Daher ist

$$\mathrm{ord}(\mathrm{Im}(\varphi)) = \mathrm{ord}(G(L/K))\mathrm{ord}(G(L/M))^{-1} = [L : K][L : M]^{-1} = [M : K].$$

Andererseits ist wegen 4.9

$$[M : K] = \mathrm{ord}(\mathrm{Im}(\varphi)) \leq \mathrm{ord}(G(M/K)) \leq [M : K].$$

Daher $\mathrm{ord}(\mathrm{Im}(\varphi)) = \mathrm{ord}(G(M/K))$ und $\mathrm{Im}(\varphi) = G(M/K)$.

Insbesondere folgt nun mit 4.10, dass M/K eine Galoiserweiterung ist.

Gelten die äquivalenten Aussagen, so ist φ surjektiv und es gilt nach dem Isomorphiesatz

$$G(M/K) \cong G(L/K)/G(L/M).$$

□

5. Separable Körpererweiterungen

Definition 5.1. Sei K ein Körper, $f \in K[X]$, $\deg(f) > 0$, L ein Zerfällungskörper von f und $a \in L$. Die Zahl

$$\mu(f, a) = \max\{n \in \mathbb{N}\colon (X-a)^n \text{ teilt } f\}.$$

heißt die *Vielfachheit* von a in f. Dann heißt a *Nullstelle* von f, wenn $\mu(f, a) > 0$ gilt. a heißt *einfache Nullstelle* von f, wenn $\mu(f, a) = 1$.

Definition 5.2. Sei K ein Körper und $f \in K[X]$ mit $\deg(f) > 0$. Das Polynom f heißt *separabel*, wenn jeder irreduzible Faktor von f nur einfache Nullstellen (in einem Zerfällungskörper von f) besitzt.

Bemerkung 5.3. Die Definition hängt nicht von der Wahl des Zerfällungskörpers ab. Ferner gilt, dass f genau dann separabel ist, wenn jeder irreduzible Faktor von f separabel ist.

Beispiel 5.4. Sei p eine Primzahl und K ein Körper der Charakteristik p. Sei $f = X^p - Y \in K(Y)[X]$. Dann ist f irreduzibel nach Eisenstein. Sei a eine Nullstelle von f in einem Zerfällungskörper von f. Dann gilt

$$(X-a)^p = X^p - a^p = X^p - Y = f.$$

Also ist a eine mehrfache Nullstelle von f und f ist nicht separabel.

Bemerkung 5.5. Sei K ein Körper. Definiere

$$D\colon K[X] \to K[X], \quad \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=1}^{n} i a_i X^{i-1}.$$

D heißt die *formale Differentiation* (oder 1. Ableitung). Es gilt:

(i) Für $a, b \in K$ und $f, g \in K[X]$ gilt $D(af + bg) = aD(f) + bD(g)$.
(ii) Für $f, g \in K[X]$ gilt $D(fg) = fD(g) + gD(f)$.

(Übungsaufgabe)

Satz 5.6. Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom. Dann sind folgende Aussagen äquivalent:

(i) f ist separabel,
(ii) $D(f) \neq 0$.

Beweis. Übungsaufgabe. □

Definition 5.7. Ein Körper K heißt *vollkommen*, wenn jedes Polynom $f \in K[X]$ mit $\deg(f) > 0$ separabel ist.

Satz 5.8. Ein Körper K ist vollkommen, wenn

(i) $\mathrm{char}(K) = 0$,
(ii) $\mathrm{char}(K) = p$ eine Primzahl und für alle $a \in K$ existiert ein $b \in K$ mit $a = b^p$ (d.h. $K = K^p$).

Beweis. Zu (i): Sei $\mathrm{char}(K) = 0$, $f \in K[X]$ irreduzibel mit $\deg(f) > 0$. Dann folgt $\deg(D(f)) = \deg(f) - 1 \geq 0$ und daher $D(f) \neq 0$. Also ist f separabel.

Zu (ii): Sei nun $\mathrm{char}(K) = p$ eine Primzahl und $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ irreduzibel mit $\deg(f) > 0$. Angenommen f ist nicht separabel. Dann gilt

$$0 = D(f) = \sum_{i=1}^{n} i a_i X^{i-1}.$$

Es folgt, dass $a_i = 0$ gilt, wenn p nicht i teilt. Also ist

$$f = \sum_{j} a_{jp} X^{jp}.$$

Nach Voraussetzung kann man die p-te Wurzel aus a_{jp} ziehen, d.h. $a_{jp} = b_{jp}^p$ für $b_{jp} \in K$. Somit ist

$$f = \sum_{j} b_{jp}^p X^{jp} = (\sum_{j} b_{jp} X^j)^p$$

ein Widerspruch, da f irreduzibel ist. □

Satz 5.9. Sei K ein Körper und L ein Zerfällungskörper eines separablen Polynoms $f \in K[X]$. Dann ist L/K eine Galoiserweiterung. Sei $\Gamma = G(L/K)$. Dann heißt Γ die Galoisgruppe von f und es ist $\mathrm{ord}(\Gamma) = [L : K]$.

Beweis. Es gilt

$$\mathrm{ord}(\Gamma) = [L : L^\Gamma] \leq [L : K].$$

Es bleibt zu zeigen, dass $L^\Gamma = K$. Sei r die Anzahl der Nullstellen von f in $L \setminus K$. Wir beweisen $L^\Gamma = K$ durch eine Induktion nach r.

$r = 0$: Dann ist $L = K$ und daher $L^\Gamma = K^\Gamma = K$.

$r > 0$: Sei $a \in L \setminus K$ eine Nullstelle von f und g das Minimalpolynom von a über K. Es folgt, dass $g | f$ in $L[X]$. Da f separabel ist, muss auch g separabel sein.

L ist auch Zerfällungskörper von $f \in K(a)[X]$. Ferner besitzt f in $L \setminus K(a)$ höchstens $r - 1$ Nullstellen. Also ist nach der Induktionsannahme $L/K(a)$ eine Galoiserweiterung. Sei $\Gamma' = G(L/K(a))$. Dann ist $\Gamma' \subseteq \Gamma$ eine Untergruppe und $L^\Gamma \subseteq L^{\Gamma'} = K(a)$.

Sei $x \in L^\Gamma$ beliebig. Wir zeigen, dass $x \in K$. Dann folgt $L^\Gamma \subseteq K$. Da immer $L^\Gamma \supseteq K$, ist $L^\Gamma = K$ bewiesen.

Ist $\deg(g) = n$, so lässt sich $x = c_0 + c_1 a + \ldots + c_{n-1} a^{n-1}$ schreiben mit $c_i \in K$. Seien $a = a_1, a_2 \ldots, a_n$ die paarweise verschiedenen Nullstellen von g. Dann gibt es wegen 3.4 Isomorphismen $\varphi_i \in \Gamma$ mit $\varphi_i(a) = a_i$ für $i = 1, \ldots, a_n$. Da $x \in L^\Gamma$, gilt

$$x = \varphi_i(x) = c_0 + c_1 a_i + \ldots + c_{n-1} a_i^{n-1}.$$

Daher sind $a_1, \ldots, a_n$ Nullstellen des Polynoms

$$h = \sum_{k=0}^{n-1} c_k X^K - x.$$

Aber $\deg(h) = n - 1$. Somit muss $h = 0$ gelten. Dann ist

$$x = c_0 \in K$$

und dies war zu zeigen. □

Bemerkung 5.10. Sei $f \in \mathbb{Q}[X]$ mit $\deg(f) > 0$. Dann ist f separabel, da $\mathrm{char}(\mathbb{Q}) = 0$ gilt. Ist L der Zerfällungskörper von f über $\mathbb{Q}$, so ist $L/\mathbb{Q}$ eine Galoiserweiterung.

Definition 5.11. Seie L/K eine Körpererweiterung.

(i) Ein Element a heißt *separabel* über K, wenn a Nullstelle eines separablen Polynoms $f \in K[X]$ ist.
(ii) L/K heißt *separabel*, wenn jedes Element $a \in L$ separabel über K ist.

Bemerkung 5.12. Ein Element $a \in L$ ist separabel genau dann, wenn a algebraisch über K ist und das Minimalpolynom von a separabel über K ist.

Satz 5.13. Sei L/K eine endliche Körpererweiterung, $\overline{K}$ der algebraische Abschluss von K und

$$S = \{\varphi \colon L \to \overline{K} \text{ mit } \varphi_{|K} = \mathrm{id}_K\}.$$

Dann gilt:

(i) $|S| \leq [L : K]$.
(ii) $|S| = [L : K]$ genau dann, wenn L/K separabel ist.

Beweis. Sei $L = K(a_1, \ldots, a_n)$, $[L\colon K] = \prod_{i=1}^{n} m_i$ mit

$$m_i = [K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})].$$

Nach 2.9 besitzt jede K-Einbettung

$$\sigma \colon K(a_1, \ldots, a_{i-1}) \to \overline{K}$$

genau so viele Fortsetzungen, wie das Minimalpolynom $f_i \in K(a_1, \ldots, a_{i-1})[X]$ von a_i verschiedene Nullstellen besitzt. Daher kann σ höchstens m_i Fortsetzungen haben und es folgt (id_K induktiv fortsetzen)

$$|S| \leq m_1 \cdots m_n = [L : K].$$

Sei nun L/K separabel, dann sind alle a_i separabel über K. Nun ist f_i Teiler des Minimalpolynoms g_i von a_i über K. Da g_i separabel ist, muss auch f_i separabel sein. Dann besitzt jede K-Einbettung

$$K(a_1, \ldots, a_{i-1}) \to \overline{K}$$

genau m_i Fortsetzungen und es folgt

$$|S| = m_1 \cdots m_n = [L : K].$$

Sei L/K nicht separabel und o. E. a_1 nicht separabel über K. Dann ist aber die Anzahl der Isomorphismen

$$K(a_1) \to \overline{K}$$

echt kleiner als m_1 und

$$|S| < m_1 \cdots m_n = [L : K].$$

□

Satz 5.14. Seien M/L und L/K endliche Körpererweiterungen. Dann sind folgende Aussagen äquivalent:

(i) M/K ist separabel.
(ii) M/L und L/K sind separabel.

Beweis. Sei $\overline{L}$ der algebraische Abschluss von L. Dann ist $\overline{L} = \overline{K}$ auch der algebraische Abschluss von K, da L/K endlich ist. Sei

$$S_1 = \{\sigma_1, \ldots, \sigma_n\}$$

die Menge der K-Einbettungen von L in $\overline{K}$,

$$S_2 = \{\tau_1, \ldots, \tau_m\}$$

die Menge der L-Einbettungen von M in $\overline{L}$ und S die Menge der K-Einbettungen von M in $\overline{K}$. Wir behaupten, dass

$$|S| = |S_1||S_2|$$

gilt. Dies beweist den Satz. Denn sind M/L und L/K separabel, dann folgt, dass

$$|S| = |S_1||S_2| = [L : K][M : L] = [M : K],$$

also ist M/K separabel. Ist umgekehrt M/K separabel, so folgt aus

$$|S| = [M : K] = [M : L][L : K] \geq |S_1||S_2| = |S|,$$

dass

$$[M : L] = |S_2| \text{ und } [L : K] = |S_1|.$$

Also sind M/L und L/K separabel.

Es bleibt die Behauptung $|S| = |S_1||S_2|$ zu zeigen. Wir beweisen:

(a) $|S| \geq |S_1||S_2|$.
(b) $|S| \leq |S_1||S_2|$.

Zu (a): Nach 2.10 existieren Fortsetzungen $\Sigma_i \colon \overline{L} \to \overline{L}$ von $\sigma_i \colon L \to \overline{L}$ für $i = 1, \ldots, n$. Dies sind Isomorphismen. Dann ist für $i = 1, \ldots, n$ und $j = 1, \ldots, m$ die Abbildung $\Sigma_i \circ \tau_j \colon M \to \overline{L}$ ein Element von S, da Σ_i und τ_j den Körper K fix lassen.

Angenommen: $\Sigma_i \circ \tau_j = \Sigma_k \circ \tau_l$. Dann folgt

$$\sigma_i = (\Sigma_i \circ \tau_j)_{|L} = (\Sigma_k \circ \tau_l)_{|L} = \sigma_k$$

und daher $i = k$. Nun gilt

$$\tau_j = \Sigma_i^{-1} \circ \Sigma_k \circ \tau_l = \tau_l.$$

Also $j = l$. Insgesamt habe wir $|S| \geq |S_1||S_2|$ bewiesen.

Zu (b): Sei $\tau \in S$ beliebig, d.h. $\tau\colon M \longrightarrow \overline{L}$ ist ein K-Homomorphismus. Nun ist $\tau_{|L} \in S_1$. D.h. $\tau_{|L} = \sigma_i$ für ein i. Dann ist aber $\Sigma_i^{-1} \circ \tau \in S_2$ (Σ_i wie oben eine Fortsetzung von σ_i), da

$$\Sigma_i^{-1} \circ \tau_{|L} = \mathrm{id}_L.$$

Es folgt, dass $\Sigma_i^{-1} \circ \tau = \tau_j$ für ein j ist. Also gilt

$$\tau = \Sigma_i \circ \tau_j$$

und daher

$$|S| \leq |S_1||S_2|.$$

□

Satz 5.15. Sei L/K eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent:

(i) L/K ist eine Galoiserweiterung.
(ii) L/K ist normal und separabel.
(iii) L ist der Zerfällungskörper eines separablen Polynoms $f \in K[X]$.

Beweis. (iii) $\Rightarrow$ (i): Dies wurde in 5.9 bewiesen.
(i) $\Rightarrow$ (ii): Sei

$$G(L/K) = \{\sigma_1, \ldots, \sigma_n\} \text{ mit } n = [L : K].$$

Sei $\overline{L}$ der algebraische Abschluss von L und K. Betrachte:

$$\psi_i\colon L \xrightarrow{\sigma_i} L \hookrightarrow \overline{L} \text{ für } i = 1, \ldots, n.$$

Dies sind n verschieden K-Einbettungen von L nach $\overline{L}$. Ist S die Menge aller K-Einbettungen von L nach $\overline{L}$, so gilt mit Hilfe von 5.13 (i), dass

$$|S| \geq n = [L : K] \geq |S|.$$

Also $|S| = [L : K]$. Es folgt aus 5.13 (ii), dass L/K separabel ist.

Ferner gilt für jede K-Einbettungen ψ_i von L nach $\overline{L}$ (das sind alle), dass $\psi_i(L) \subseteq L$. Also ist L/K normal nach 3.9.

(ii) $\Rightarrow$ (iii): Da L/K normal ist, folgt aus 3.9, dass L der Zerfällungskörper eines Polynoms $f \in K[X]$ ist. Sei g ein irreduzibler Faktor von f und a eine Nullstelle von g in L. Dann ist g das Minimalpolynom von a. Da L/K separabel ist, muss g separabel sein. Daher ist f separabel. □

Lemma 5.16. Sei G eine abelsche Gruppe und $a, b \in G$ mit endlicher Ordnung. Ist $\mathrm{ord}(a) = m$ und $\mathrm{ord}(b) = n$, so existiert in G ein Element der Ordnung $\mathrm{kgV}(m, n)$.

Beweis. Sei zunächst $\mathrm{ggT}(m, n) = 1$. Es gilt

$$(ab)^{mn} = (a^m)^n (b^n)^m = e$$

Ist

$$(ab)^t = e,$$

dann folgt aus

$$a^{nt} = a^{nt} b^{nt} = e,$$

dass $m|t$ wegen $\mathrm{ggT}(m,n)=1$. Analog $n|t$ und daher

$$\mathrm{ord}(ab) = mn.$$

Also ist ab ein Element der Ordnung $mn = \mathrm{kgV}(m,n)$.

Seien nun m, n beliebig. Sei

$$\mathrm{kgV}(m,n) = p_1^{a_1} \cdots p_r^{a_r}$$

eine Primfaktorzerlegung von $\mathrm{kgV}(m,n)$. Definiere

$$m_0 = \prod_{i, p_i | m} p_i^{a_i} \text{ und } n_0 = \prod_{j, p_j \text{ teilt nicht } m} p_j^{a_j}.$$

Dann gilt

$$m_0|m, \quad n_0|n, \quad \mathrm{kgV}(m,n) = m_0 n_0 \text{ und } \mathrm{ggT}(m_0, n_0) = 1.$$

Sei $m = m_0 m'$ und $n = n_0 n'$. Es folgt

$$\mathrm{ord}(a^{m'}) = m_0 \text{ und } \mathrm{ord}(b^{n'}) = n_0.$$

Dann hat das Element $a^{m'} b^{n'}$ die Ordnung $\mathrm{kgV}(m,n)$. □

Korollar 5.17. Sei K ein Körper und H eine endliche Untergruppe von K^*. Dann ist H zyklisch. Ist insbesondere K endlich, so ist K^* eine zyklische Gruppe.

Beweis. Sei $a \in H$ ein Element mit maximaler Ordnung m und H_m die Untergruppe von H, die aus allen Elementen besteht, deren Ordnung ein Teiler von m ist. Alle Elemente von H_m sind Nullstellen des Polynoms

$$X^m - 1,$$

so dass H_m höchstens m Elemente enthalten kann. Somit folgt

$$H_m = \langle a \rangle,$$

da $\langle a \rangle \subseteq H_m$. Wir behaupten, dass bereits $H = H_m$. Wäre $b \in H \setminus H_m$, so ist $\mathrm{ord}(b) = n$ kein Teiler von m. Dann besitzt H aufgrund von 5.16 ein Element der Ordnung $\mathrm{kgV}(m,n) > m$ im Widerspruch zu der Wahl von a und m. □

Satz 5.18. *(Satz vom primitiven Element)* Sei L/K eine endliche separable Körpererweiterung. Dann ist L/K einfach, d.h. es gibt ein Element $a \in L$ mit $L = K(a)$. Das Element a heißt *primitives Element* der Erweiterung.

Beweis. 1. Fall: $|K| < \infty$. Es folgt

$$|L| = [L:K]|K| < \infty,$$

da L/K endlich ist. Aus 5.17 folgt, dass

$$L^* = \langle a \rangle = \{1, a, a^2, \dots\}$$

zyklisch ist. Also $L = K(a)$.

2. Fall: $|K| = \infty$. Sei $L = K(a_1, \dots, a_n)$, f_i das Minimalpolynom von a_i über K und $f = \prod_i f_i$. Da die f_i separabel sind, ist auch f separabel. Sei $M \supseteq L$ ein Zerfällungskörper von f. Nach 5.15 ist M/K eine Galoiserweiterung, die nur

endlich viele Zwischenkörper besitzt. Daher besitzt auch L/K nur endlich viele Zwischenkörper.

Betrachte für $c \in L$ die Körper $K(a_1 + ca_2) \subseteq L$. Da $|K| = \infty$, existieren $c_1, c_2 \in K$ mit $c_1 \neq c_2$ und

$$K(a_1 + c_1 a_2) = K(a_1 + c_2 a_2) = N.$$

Aus $a_1 + c_1 a_2, a_1 + c_2 a_2 \in N$ folgt $(c_1 - c_2)a_2 \in N$. Da $c_1 - c_2 \neq 0$, ist $a_2 \in N$ und daher auch $a_1 \in N$. Dann ist aber bereits

$$L = K(a_1 + c_1 a_2, a_3, \ldots, a_n).$$

Eine Induktion ergibt die Behauptung $L = K(a)$ für ein $a \in L$. □

KAPITEL 4

Fortführung der Gruppentheorie

1. Gruppenoperationen

Definition 1.1. Sei G eine Gruppe und X eine Menge. Eine *Gruppenoperation* von G auf X ist eine Abbildung

$$G \times X \to X, \quad (a, x) \mapsto a(x),$$

mit:

(i) Ist e das neutrale Element von G, so gilt $e(x) = x$ für alle $x \in X$.
(ii) Für alle $a, b \in G$ und $x \in X$ gilt $(ab)(x) = a(b(x))$.

Man sagt G *operiert auf* X.

Beispiele 1.2. Es gilt:

(i) Für jede Menge X operiert $S(X)$ auf X.
(ii) Sei G eine Gruppe, dann operiert G auf sich selber durch

$$G \times G \to G, \quad (a, b) \mapsto ab.$$

Lemma 1.3. Sei G eine Gruppe und X eine Menge.

(i) Wenn G auf X operiert, dann gibt es genau einen Gruppenhomomorphismus $\varphi : G \to S(X)$ mit $\varphi(a)(x) = a(x)$ für alle $a \in G$ und $x \in X$.
(ii) Ist umgekehrt $\varphi : G \to S(X)$ ein Gruppenhomomorphismus, dann ist die Abbildung

$$G \times X \to X, \quad (a, x) \mapsto \varphi(a)(x)$$

eine Gruppenoperation.

Somit entsprechen Gruppenoperationen von G auf X umkehrbar eindeutig den Gruppenhomomorphismen $G \to S(X)$.

Beweis. Zu (i): Es ist zu zeigen, dass φ eine Abbildung von G nach $S(X)$ ist. Als erstes zeigen wir, dass $\varphi(a) \in S(X)$ für $a \in G$ ist.

$\varphi(a)$ ist injektiv: Seien $x_1, x_2 \in X$ mit $\varphi(a)(x_1) = \varphi(a)(x_2)$, d.h. $a(x_1) = a(x_2)$. Dann ist

$$x_1 = e(x_1) = (a^{-1}a)(x_1) = a^{-1}(a(x_1)) = a^{-1}(a(x_2)) = (a^{-1}a)(x_2) = e(x_2) = x_2.$$

Somit folgt die Behauptung.

$\varphi(a)$ ist surjektiv: Sei $y \in X$. Dann ist

$$\varphi(a)(a^{-1}(y)) = a(a^{-1}(y)) = (aa^{-1})(y) = e(y) = y.$$

Es folgt, dass $\varphi(a)$ eine bijektive Abbildung ist. Als nächstes muss gezeigt werden, dass φ ein Gruppenhomomorphismus ist. Seien $a, b \in G$. Es ist zu zeigen, dass $\varphi(ab) = \varphi(a)\varphi(b)$. Sei $x \in X$ beliebig, dann gilt

$$\varphi(ab)(x) = (ab)(x) = a(b(x)) = a(\varphi(b)(x)) = \varphi(a)(\varphi(b)(x)) = (\varphi(a)\varphi(b))(x).$$

Die Eindeutigkeit folgt durch die Definition.

Zu (ii): Sei e das neutrale Element von G. Dann folgt für $x \in X$

$$e(x) = \varphi(e)(x) = x, \text{da } \varphi(e) \text{ das neutrale Element von } S(X) \text{ ist.}$$

Seien $a, b \in G$ und $x \in X$, dann gilt

$$(ab)(x) = \varphi(ab)(x) = (\varphi(a)\varphi(b))(x) = \varphi(a)(\varphi(b)(x)) = a(b(x)).$$

□

Definition 1.4. Sei G eine Gruppe, die auf einer Menge X operiert.

(i) G operiert *treu* auf X, wenn der zugehörige Homomorphismus $\varphi\colon G \to S(X)$ injektiv ist (d.h. aus $a(x) = b(x)$ für alle $x \in X$ folgt $a = b$).

(ii) Zwei Elemente $x, y \in X$ heißen *G-äquivalent* ($x \sim y$), wenn ein $a \in G$ existiert mit $a(x) = y$.

(iii) Die Äquivalenzklassen ($Gx = \{ax\colon a \in G\}$) bzgl. $\sim$ heißen *Bahnen* von G in X.

(iv) G operiert *transitiv* auf X, wenn es genau eine Bahn von G in X gibt (d.h. für alle $x, y \in X$ existiert ein $a \in G$ mit $a(x) = y$).

Beispiele 1.5. Betrachte:

(i) Die multiplikative Gruppe der komplexen Zahlen vom Betrag 1 operiert auf der Gaußschen Zahlenebene ($\mathbb{C}$). Diese Operation ist treu. Die Bahnen sind die konzentrischen Kreise mit Mittelpunkt 0.

(ii) Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Durch Rechts- bzw. Linksmultiplikation wird eine Operation von H auf G erklärt:

$$R\colon H \to S(G), \quad R(a)(b) = ba,$$

$$L\colon H \to S(G), \quad L(a)(b) = ab.$$

Die Bahnen bzgl. der Rechts- bzw. Linksmultiplikation sind die Links- bzw. Rechtsnebenklassen von H.

Beispiel 1.6. Sei K ein Körper, Γ die Galoisgruppe eines separablen Polynoms $f \in K[X]$ mit $\deg(f) > 0$ und $N(f)$ die Nullstellen von f in einem Zerfällungskörper von f. Dann gilt:

(i) Γ operiert auf $N(f)$ und kann als Untergruppe von $S_{|N(f)|}$ interpretiert werden.

(ii) Seien $f_1, \ldots, f_n$ die irreduziblen Faktoren von f. Die Bahnen der Operation von Γ auf $N(f)$ sind die Teilmengen $N(f_i)$ für $i = 1, \ldots, n$.

(iii) Ist f irreduzibel, so operiert Γ transitiv auf $N(f)$.

Lemma 1.7. Sei G eine Gruppe, die auf einer Menge X operiert. Dann ist X die disjunkte Vereinigung der Bahnen von G.

Beweis. Da $X = \cup_{x \in X} Gx$ gilt, ist zu zeigen, dass für $x, y \in X$ aus $Gx \cap Gy \neq \emptyset$ schon $Gx = Gy$ folgt. Sei $z \in Gx \cap Gy$, etwa $z = ax = by$ für $a, b \in G$. Es folgt $x = a^{-1}by$ und somit $Gx \subseteq Gy$. Analog gilt $Gy \subseteq Gx$ und daher $Gx = Gy$. □

Definition 1.8. Sei G eine Gruppe, die auf einer Menge X operiert.

(i) Ein Element $x \in X$ heißt *Vertreter* der Bahn Gx.

(ii) Ein *Vertretersystem* einer Familie $(B_i)_{i \in I}$ paarweise disjunkter Bahnen ist eine Familie $(a_i)_{i \in I}$ mit $a_i \in B_i (B_i = Ga_i)$. Das Vertretersystem heißt *vollständig*, wenn $X = \cup_{i \in I} B_i$ gilt.

Definition 1.9. Sei G eine Gruppe, die auf einer Menge X operiert und $x \in X$. Die Untergruppe $G_x = \{a \in G \colon a(x) = x\}$ von G heißt die *Isotropiegruppe* (oder Standgruppe) von x.

Satz 1.10. *(Bahnengleichung)* Sei G eine Gruppe, die auf einer endlichen nicht leeren Menge X operiert und $x_1, \ldots, x_n$ ein vollständiges Vertretersystem der Bahnen von G. Dann gilt

$$|X| = \sum_{i=1}^{n} [G : G_{x_i}]$$

G ist hierbei nicht notwendigerweise endlich.

Beweis. Aus 1.7 folgt $X = \dot{\cup}_{i=1}^{n} Gx_i$ und daher gilt

$$|X| = \sum_{i=1}^{n} |Gx_i|.$$

Wir definieren für $i = 1, \ldots, n$ eine bijektive Abbildung $\alpha_i \colon G/G_{x_i} \longrightarrow Gx_i$. Dann folgt

$$|X| = \sum_{i=1}^{n} |G/G_{x_i}| = \sum_{i=1}^{n} [G : G_{x_i}].$$

Für $a \in G$ definiere $\alpha(aG_{x_i}) = a(x_i)$. Wir zeigen:

(1) α_i ist wohldefiniert: Sei $aG_{x_i} = bG_{x_i}$ und daher $b^{-1}a \in G_{x_i}$. Es folgt

$$b(x_i) = b(b^{-1}a(x_i)) = (bb^{-1}a)(x_i) = a(x_i)$$

und daher $\alpha(bG_{x_i}) = \alpha(aG_{x_i})$.

(2) α_i ist surjektiv: Sei $y \in Gx_i$ beliebig und $y = a(x_i)$ für ein $a \in G$. Dann ist $\alpha_i(aG_{x_i}) = y$.

(3) α_i ist injektiv: Seien $a, b \in G$ mit $\alpha(aG_{x_i}) = \alpha(bG_{x_i})$, d.h. $a(x_i) = b(x_i)$. Es folgt $x_i = b^{-1}a(x_i)$ und somit $b^{-1}a \in G_{x_i}$. Dies ist äquivalent zu

$$aG_{x_i} = bG_{x_i}$$

und daraus folgt die Behauptung.

□

Definition 1.11. Sei G eine Gruppe. Die Operation $G \times G \longrightarrow G, (a, b) \mapsto aba^{-1} = b^a$ heißt *Konjugation*. Die Bahnen der Konjugation heißen *Konjugationsklassen* von G. Zwei Elemente $a, b \in G$ sind *konjugiert*, wenn ein $c \in G$ existiert mit $b = a^c$.

Definition 1.12. Sei G eine Gruppe.

(i) Sei $S \subseteq G$. Die Untergruppe

$$Z_S = \{b \in G \colon aba^{-1} = b \text{ für alle } a \in S\}$$

heißt der *Zentralisator* von S in G.

(ii) Die Untergruppe

$$Z_G = \{b \in G \colon aba^{-1} = b \text{ für alle } a \in G\}$$

von G heißt das *Zentrum* von G.

Bemerkung 1.13. Z_G besteht aus allen Elementen von G, die mit allen Elementen von G kommutieren. Die Gruppe G ist abelsch $\Leftrightarrow G = Z_G$. Es ist

$$G_a = Z_{\{a\}} = \{b \in G \colon bab^{-1} = a\} = \{b \in G \colon ba = ab\}.$$

Satz 1.14. *(Klassengleichung)* Sei G eine endliche Gruppe mit Zentrum Z_G und $a_1, \ldots, a_n$ ein Vertretersystem der Bahnen in $G - Z_G$ unter der Konjugation. Dann gilt:

$$\operatorname{ord}(G) = \operatorname{ord}(Z_G) + \sum_{i=1}^{n} [G : Z_{\{a_i\}}].$$

Beweis. Es gilt

$$a \in Z_G \Leftrightarrow Z_{\{a\}} = G \Leftrightarrow [G : Z_{\{a\}}] = 1$$

Sei $a_1, \ldots, a_n, b_1, \ldots, b_m$ ein vollständiges Vertretersystem der Bahnen von G unter der Konjugation mit $a_1, \ldots, a_n \in G - Z_G$ und $b_1, \ldots, b_m \in Z_G$. Dann gilt nach 1.10

$$\operatorname{ord}(G) = \sum_{j=1}^{m} [G : Z_{\{b_j\}}] + \sum_{i=1}^{n} [G : Z_{\{a_i\}}] = \operatorname{ord}(Z_G) + \sum_{i=1}^{n} [G : Z_{\{a_i\}}].$$

□

Korollar 1.15. Sei p eine Primzahl und G eine Gruppe der Ordnung p^n für ein $n > 0$. Dann ist $Z_G \neq \{e\}$.

Beweis. Ist $G = Z_G$, so ist nichts zu zeigen. Sei nun $G \neq Z_G$ und $a \in G - Z_G$. Da $1 < [G : Z_{\{a\}}]$, ist $Z_{\{a\}}$ eine echte Untergruppe von G. Es folgt $[G : Z_{\{a\}}] | \operatorname{ord}(G) = p^n$ und daher $[G : Z_{\{a\}}] = p^m$ für ein $1 < m < n$. Sei nun $a_1, \ldots, a_n$ ein Vertretersystem der Bahnen in $G - Z_G$ unter der Konjugation. Dann existieren Zahlen $1 < m_i < n$ mit $[G : Z_{\{a_i\}}] = p^{m_i}$. Somit

$$p^n = \operatorname{ord}(G) = \operatorname{ord}(Z_G) + \sum_{i=1}^{n} [G : Z_{\{a_i\}}] = \operatorname{ord}(Z_G) + \sum_{i=1}^{n} p^{m_i}.$$

Es folgt $p | \operatorname{ord}(Z_G)$ und daher $Z_G \neq \{e\}$. □

2. Endlich erzeugte abelsche Gruppen

Bemerkung 2.1. Sei

$$G = \langle a_1, \dots, a_m \rangle = \{z_1 a_1 + \cdots + z_m a_m \colon z_i \in \mathbb{Z}\}$$

eine endlich erzeugte abelsche Gruppe. Auch wenn das Erzeugendensystem nicht verkürzbar ist, so ist die Darstellung der Elemente von G nicht eindeutig.

Sei etwa $G = \mathbb{Z}/n\mathbb{Z}$ und $a_1 = 1 + n\mathbb{Z}$. Dann gilt $G = \langle a_1 \rangle$ und für jedes Element $a \in G$ ist mit $a = za_1$ auch $a = (z+n)a_1$.

Definition 2.2. Sei G eine abelsche Gruppe.

(i) Ein Erzeugendensystem $\{a_i\}_{i \in I}$ von G heißt *Basis*, wenn sich jedes Element von G eindeutig als $\mathbb{Z}$-Linearkombination endlich vieler der $\{a_i\}_{i \in I}$ schreiben lässt.

(ii) G heißt *frei*, wenn G ein Basis besitzt.

Bemerkung 2.3. Für $n \in \mathbb{N}$ mit $n \geq 1$ sei $\mathbb{Z}^n$ die Menge der n-Tupel mit Koeffizienten aus $\mathbb{Z}$ und komponentenweiser Addition. Dann sind für $i = 1, \dots, n$ die Elemente $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ mit der 1 an der i-ten Position eine Basis von $\mathbb{Z}^n$. Daher ist $\mathbb{Z}^n$ frei.

Satz 2.4. Sei G eine endlich erzeugte abelsche Gruppe mit Erzeugendensystem $a_1, \dots, a_n$ und F eine freie abelsche Gruppe mit Basis $f_1, \dots, f_n$ (z.B. $\mathbb{Z}^n$). Dann gibt es einen Gruppenepimorphismus

$$\varphi \colon F \to G, \quad f_i \mapsto a_i.$$

Ist $H = \mathrm{Ker}(\varphi)$, so gilt $G \cong F/H$.

Beweis. Eindeutigkeit: Sei $f = \sum_{i=1}^n z_i f_i \in F$ mit $z_i \in \mathbb{Z}$. Dann gilt

$$\varphi(f) = \sum_{i=1}^n z_i \varphi(f_i) = \sum_{i=1}^n z_i a_i.$$

Existenz: Definiere

$$\varphi \colon F \to G, \quad \varphi(f) = \sum_{i=1}^n z_i a_i, \text{ wenn } f = \sum_{i=1}^n z_i f_i.$$

Die Abbildung ist wohldefiniert, da die Koeffizienten z_i durch f und die Basis f_i eindeutig bestimmt sind. Nun rechnet man leicht nach, dass φ ein Gruppenhomomorphismus ist.

Ist $H = \mathrm{Ker}(\varphi)$, so folgt $G \cong F/H$ aus dem Homomorphiesatz. □

Satz 2.5. Sei F eine endlich erzeugte abelsche Gruppe mit Basis $f_1, \dots, f_n$. Dann gilt $F \cong \mathbb{Z}^n$.

Beweis. Betrachte die Epimorphismen

$$\varphi \colon F \to \mathbb{Z}^n, \quad f_i \mapsto e_i \text{ für } i = 1, \dots, n$$

und

$$\psi \colon \mathbb{Z}^n \to F, \quad e_i \mapsto f_i \text{ für } i = 1, \dots, n.$$

Dann folgt $\varphi \circ \psi = \mathrm{id}_{\mathbb{Z}^n}$ und $\psi \circ \varphi = \mathrm{id}_F$. Daher sind die Abbildungen Isomorphismen und es gilt $F \cong \mathbb{Z}^n$. □

Satz 2.6. Seien $m, n \in \mathbb{N}$ mit $m, n \geq 1$. Dann gilt $\mathbb{Z}^m \cong \mathbb{Z}^n$ genau dann, wenn $m = n$.

Beweis. Ist $m = n$, so folgt direkt, dass $\mathbb{Z}^m \cong \mathbb{Z}^n$.

Sei nun

$$\varphi \colon \mathbb{Z}^m \to \mathbb{Z}^n$$

ein gegebener Gruppenisomorphismus. Definiere

$$\overline{\varphi} \colon \mathbb{Q}^m \to \mathbb{Q}^n, \quad (q_1, \ldots, q_n) \mapsto \sum_{i=1}^{m} q_i \varphi(e_i).$$

Dies ist eine $\mathbb{Q}$-lineare Abbildung. Behauptung: φ ist injektiv. Dann folgt aus der Linearen Algebra, dass $m \leq n$. Analog gilt $n \leq m$ und daher $m = n$.

Es bleibt die Behauptung zu zeigen. Sei

$$\overline{\varphi}(q_1, \ldots, q_n) = \sum_{i=1}^{m} q_i \varphi(e_i) = 0.$$

Schreibe $q_i = \frac{z_i}{t}$ mit $z_i \in \mathbb{Z}$ und einem Hauptnenner $t \in \mathbb{N}$ der q_i. Nach Multiplikation mit t folgt:

$$0 = \sum_{i=1}^{m} z_i \varphi(e_i) = \varphi(\sum_{i=1}^{m} z_i e_i).$$

Nun ist φ ein Isomorphismus, also $\sum_{i=1}^{m} z_i e_i = 0$. Da die Elemente e_i eine Basis für $\mathbb{Z}^m$ sind, folgt $z_i = 0$ für alle i und daher

$$(q_1, \ldots, q_n) = (0, \ldots, 0).$$

Dies war zu zeigen. □

Korollar 2.7. Sei F eine e. e. freie abelsche Gruppe mit Basis $f_1, \ldots, f_n$. Dann besitzt jede andere Basis von F ebenfalls die endliche Länge n. Man nennt n den *Rang* von F.

Beweis. Nach 2.5 ist $F \cong \mathbb{Z}^n$.

Angenommen F besitzt eine unendlichen Basis oder eine Basis mit mehr als n Elementen. Sei diese Basis $g_1, \ldots, g_n, g_{n+1}, \ldots$. Dann ist $g_1, \ldots, g_{n+1}$ eine Basis für $H = \langle g_1, \ldots, g_{n+1} \rangle$. Es folgt,

$$\mathbb{Z}^{n+1} \cong H \subseteq F \cong \mathbb{Z}^n.$$

Dann würde aber

$$\mathbb{Q}^{n+1} \subseteq \mathbb{Q}^n$$

als Inklusion von Vektorräumen folgen (analog zum vorherigen Beweis). Dies ist ein Widerspruch.

Daher muss die andere Basis die Gestalt $g_1, \ldots, g_m$ mit $m \leq n$ haben. Analog gilt jedoch $n \leq m$ und daher $m = n$. □

Definition 2.8. Seien $G_1, \dots, G_r$ Gruppen. Sei

$$G_1 \times \cdots \times G_r = \{(a_1, \dots, a_r) \colon a_i \in G_i\}.$$

Diese Menge ist mit der komponentenweise induzierten Verknüpfung eine Gruppe. Sie heißt das *direkte Produkt* von $G_1, \dots, G_r$.

Beispiel 2.9. Betrachte:

(i) $\mathbb{Z}^n \cong \mathbb{Z} \times \cdots \times \mathbb{Z}$.

(ii) Seien $G_1, G_2 \subseteq G$ Untergruppen von G. Genau dann wird durch

$$G_1 \times G_2 \longrightarrow G, \quad (a, b) \mapsto ab$$

ein Gruppenisomorphismus gegeben, wenn gilt:

(a) Für alle $a \in G$ existieren $b \in G_1$ und $c \in G_2$ mit $a = bc$.

(b) G_1, G_2 sind Normalteiler von G.

(c) $G_1 \cap G_2 = \{e\}$.

Beweis: Übungsaufgabe.

Man schreibt dann $G = G_1 \times G_2 = G_1 \oplus G_2$ und nennt dies die *innere direkte Summe* (Produkt) von G_1 und G_2.

Satz 2.10. *(Hauptsatz für abelsche Gruppen)* Sei F eine freie abelsche Gruppe vom Rang n und $U \subseteq F$ eine Untergruppe. Dann gibt es eine Basis $b_1, \dots, b_n$ von F, eine Zahl $p \leq n$ und Zahlen $\varepsilon_1, \dots, \varepsilon_p \in \mathbb{N}$ mit $\varepsilon_i | \varepsilon_{i+1}$ für $i = 1, \dots, p-1$, so dass $\varepsilon_1 b_1, \dots, \varepsilon_p b_p$ eine Basis von U ist. Insbesondere ist U eine freie abelsche Gruppe vom Rang $p \leq n$.

Beweis. Für $U = \{0\}$ ist nichts zu zeigen, also sei $U \neq \{0\}$.

Wir beweisen den Satz durch eine Induktion nach n. Sei $n = 1$, dann ist $F = \langle b_1 \rangle \cong \mathbb{Z}$ und es gilt $U \cong (\varepsilon_1) \subseteq \mathbb{Z}$ für ein Hauptideal (ε_1). Daher ist $U = \langle \varepsilon_1 b_1 \rangle$ und die Behauptung folgt in diesem Falle.

Sei $n > 1$ und der Satz für beliebige freie abelsche Gruppen vom Rang kleiner als n bewiesen. Sei $w_1, \dots, w_n$ eine beliebige Basis von F.

Für $u \in U$ existiert eine Darstellung

$$u = z_1^u w_1 + \cdots + z_n^u w_n \text{ mit } z_i^u \in \mathbb{Z}.$$

Es existieren $u \in U$ mit Koeffizienten $z_i^u > 0$. Sei $\varepsilon_1 \in \mathbb{N}$ die kleinste positive Zahl, die bei der Darstellung eines $u \in U$ bzgl. irgendeiner Basis von F als Koeffizient auftritt. Sei $w_1, \dots, w_n$ eine solche Basis von F und

$$u_1 = z_1 w_1 + \cdots + z_n w_n$$

ein solches Element. O.E. können wir $z_1 = \varepsilon_1$ annehmen. Definiere das Ideal

$$I_1 = (z_1^u \colon u \in U) \subseteq \mathbb{Z}.$$

Wegen der Wahl von ε_1 folgt $I_1 = (\varepsilon_1)$. Insbesondere teilt ε_1 jedes z_1^u für $u \in U$.

Nun teile die Koeffizienten z_i von u_1 für $i = 2, \dots, n$ durch ε_1 mit Rest, also

$$z_i = q_i \varepsilon_1 + r_i \text{ mit } q_i, r_i \in \mathbb{Z}, 0 \leq r_i < \varepsilon_1.$$

Bezüglich der Basis $w_1 + q_i w_i, w_2, \dots, w_n$ von F hat u_1 die Darstellung

$$u_1 = \varepsilon_1(w_1 + q_i w_i) + z_2 w_2 + \cdots + r_i w_i + \cdots + z_n w_n.$$

Nach Wahl von ε_1 muss dann aber $r_i = 0$ für $i = 2, \dots, n$ gelten, also $z_i = q_i\varepsilon_1$. Definiere $b_1 = w_1 + q_2w_2 + \cdots + q_nw_n$. Dann ist $b_1, w_2, \dots, w_n$ eine Basis von F und $\varepsilon_1 b_1 = u_1 \in U$. Wegen $I_1 = (\varepsilon_1)$ gilt

$$U = \mathbb{Z}\varepsilon_1 b_1 + (U \cap \langle w_2, \dots, w_n\rangle).$$

Die Summe ist direkt, da $b_1, w_2, \dots, w_n$ eine Basis ist. Wir können also schreiben

$$U = \mathbb{Z}\varepsilon_1 b_1 \oplus U_1 \text{ mit } U_1 = (U \cap \langle w_2, \dots, w_n\rangle).$$

Da U_1 Untergruppe der freien abelschen Gruppen $F_1 = \langle w_2, \dots, w_n\rangle$ vom Rang $n-1$ ist, gibt es eine Basis $b_2, \dots, b_n$ von F_1, ein $p \leq n$ und Zahlen $\varepsilon_2, \dots, \varepsilon_p \in \mathbb{N}$ mit $\varepsilon_i | \varepsilon_{i+1}$ für $i = 2, \dots, p$, so dass $\varepsilon_2 b_2, \dots, \varepsilon_p b_p$ eine Basis von U_1 ist.

Trivialerweise ist $b_1, \dots, b_n$ eine Basis von F und $\varepsilon_1 b_1, \dots, \varepsilon_p b_p$ eine von U. Es bleibt noch $\varepsilon_1 | \varepsilon_2$ zu zeigen. Betrachte $u = \varepsilon_1 b_1 + \varepsilon_2 b_2$ und teile ε_2 durch ε_1 mit Rest, d.h.

$$\varepsilon_2 = q\varepsilon_1 + r \text{ mit } q, r \in \mathbb{Z}, 0 \leq r < \varepsilon_1.$$

Da $b_1 + qb_2, b_2, \dots, b_n$ eine Basis von F ist und

$$u = \varepsilon_1(b_1 + qb_2) + rb_2$$

ist, folgt wegen der Wahl von ε_1, dass $r = 0$ gilt. Also $\varepsilon_1 | \varepsilon_2$. □

Korollar 2.11. Sei G eine e. e. abelsche Gruppe. Dann existieren Zahlen $r, \varepsilon_1, \dots, \varepsilon_p \in \mathbb{N}$ mit $\varepsilon_i | \varepsilon_{i+1}$ für $i = 1, \dots, p-1$ und ein Isomorphismus

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/\varepsilon_1\mathbb{Z} \times \cdots \times \mathbb{Z}/\varepsilon_p\mathbb{Z}.$$

Insbesondere ist G ein direktes Produkt zyklischer Gruppen.

Beweis. Aus 2.4 folgt, dass eine freie abelsche Gruppe F und eine Untergruppe $U \subseteq F$ existiert mit $G \cong F/U$.

Nach 2.10 existiert eine Basis $b_1, \dots, b_n$ von F und eine Zahl $p \leq n$ und Zahlen $\varepsilon_1, \dots, \varepsilon_p \in \mathbb{N}$ mit $\varepsilon_i | \varepsilon_{i+1}$ für $i = 1, \dots, p-1$, so dass $\varepsilon_1 b_1, \dots, \varepsilon_p b_p$ eine Basis von U ist. Also o.E.

$$F = \mathbb{Z}b_1 \times \cdots \times \mathbb{Z}b_n$$

und

$$U = \mathbb{Z}\varepsilon_1 b_1 \times \cdots \times \mathbb{Z}\varepsilon_p b_p \subseteq F.$$

Sei $r = n - p$, dann folgt

$$G \cong \mathbb{Z}/\varepsilon_1\mathbb{Z} \times \cdots \times \mathbb{Z}/\varepsilon_p\mathbb{Z} \times \mathbb{Z}^r$$

mit den gewünschten Eigenschaften. □

Bemerkung 2.12. Es gilt:

(i) Sei

$$T(G) = \{a \in G\colon \text{Es existiert ein } n \in \mathbb{N}, n > 0 \text{ mit } na = 0\}.$$

$T(G)$ ist eine Untergruppe von G und heißt die *Torsionsgruppe* von G. Es ist

$$G/T(G) \cong \mathbb{Z}^r$$

und daher $r = \mathrm{Rang}(G/T(G))$ eindeutig. Diese Zahl heißt der *Rang* von G.

(ii) Man kann zeigen, dass die Zahlen $\varepsilon_1, \ldots, \varepsilon_p$ ebenfalls eindeutig für G sind. Diese Zahlen heißen die *Elementarteiler* von G.

Korollar 2.13. Sei G eine e. e. abelsche Gruppe. Dann existieren Zahlen $r, r_1, \ldots, r_s \in \mathbb{N}$, Primzahlen $p_1, \ldots, p_s$ und ein Isomorphismus

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}.$$

Beweis. Nach dem chinesischen Restsatz lässt sich für $n \in \mathbb{Z}$ mit $n = \prod_{i=1}^{t} p_i^{s_i}$, wobei $p_1, \ldots, p_t$ Primzahlen sind und $s_1, \ldots, s_t \in \mathbb{N}$, jede Gruppe der Gestalt

$$\mathbb{Z}/n\mathbb{Z}$$

als Produkt

$$\mathbb{Z}/p_1^{s_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{s_t}\mathbb{Z}$$

zerlegen. Dieser Sachverhalt und 2.11 beweisen die Behauptung. □

3. p-Gruppen und die Sylowsätze

Im Folgenden sei p stets eine Primzahl.

Definition 3.1. Eine Gruppe G heißt *p-Gruppe*, wenn die Ordnung von jedem Element von G eine Potenz von p ist.

Satz 3.2. *(Cauchy)* Sei G eine endliche Gruppe mit $p|\mathrm{ord}(G)$. Dann gibt es ein Element mit $\mathrm{ord}(a) = p$.

Beweis. Wir beweisen den Satz durch eine Induktion nach $\mathrm{ord}(G)$. Ist $\mathrm{ord}(G) = p$, so folgt aus dem 1. Kapitel, dass $G = \langle a \rangle$ zyklisch ist mit $\mathrm{ord}(a) = p$.

Sei nun $\mathrm{ord}(G) > p$. Betrachte die Konjugation auf G ($G \times G \to G, (a, x) \mapsto axa^{-1}$). Sei $a_1, \ldots, a_n$ ein Vertretersystem der Bahnen (Konjugationsklassen) in $G \setminus Z_G$. Dann gilt die Klassengleichung 1.14

$$\mathrm{ord}(G) = \mathrm{ord}(Z_G) + \sum_{i=1}^{n} [G : Z_{\{a_i\}}].$$

und $1 < \mathrm{ord}(Z_{\{a_i\}}) < \mathrm{ord}(G)$. Existiert ein i mit $p|\mathrm{ord}(Z_{\{a_i\}})$, so folgt nach der Induktionsannahme, dass es ein $a \in Z_{\{a_i\}} \subseteq G$ gibt mit $\mathrm{ord}(a) = p$. Ansonsten teilt p keine der Zahlen $\mathrm{ord}(Z_{\{a_i\}})$. Wegen

$$\mathrm{ord}(G) = [G : Z_{\{a_i\}}]\mathrm{ord}(Z_{\{a_i\}})$$

und $p|\mathrm{ord}(G)$ muss dann $p|[G : Z_{\{a_i\}}]$ für alle i gelten. Dann folgt aus der Klassengleichung

$$p|\mathrm{ord}(Z(G)).$$

Ist $\mathrm{ord}(Z(G)) < G$, so kann wieder wegen der Induktionsannahme ein Element $a \in Z(G) \subseteq G$ der Ordnung p gefunden werden.

Es bleibt der Fall $Z(G) = G$ zu zeigen, d.h. G ist abelsch. Dann kann nach 2.13 o.E.

$$G = \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}.$$

mit $r_1, \ldots, r_s \in \mathbb{N}$ und Primzahlen $p_1, \ldots, p_s$ angenommen werden. Hierbei existiert kein freier Summand, da G endlich ist. Man sieht, dass $\operatorname{ord}(G) = \prod_{i=1}^{s} p_i^{r_i}$. Da $p|\operatorname{ord}(G)$, muss ein i existieren mit $p = p_i$. Sei $b \in G$ mit $\operatorname{ord}(b) = p^{r_i}$. Definiere $a = p_i^{r_i - 1} b$. Dann gilt $\operatorname{ord}(a) = p$. □

Korollar 3.3. Sei G eine endliche Gruppe. Dann sind äquivalent:

(i) G ist eine p-Gruppe.
(ii) $\operatorname{ord}(G)$ ist eine p-Potenz.

Beweis. (i) ⇒ (ii): Angenommen es existiert eine Primzahl $q \neq p$ mit $q|\operatorname{ord}(G)$. Dann existiert nach 3.2 ein Element $a \in G$ mit $\operatorname{ord}(a) = q$ im Widerspruch zur Annahme, dass G eine p-Gruppe ist.

(ii) ⇒ (i): Sei $a \in G$. Dann gilt $\operatorname{ord}(a)|\operatorname{ord}(G)$ und $\operatorname{ord}(a)$ muss daher eine Potenz von p sein. □

Korollar 3.4. Sei G eine endliche p-Gruppe. Dann besitzt G ein nicht triviales Zentrum Z_G.

Beweis. Dies folgt aus 1.15 und 3.3. □

Beispiel 3.5. Betrachte:

(i) Ist $\operatorname{ord}(G) = p$, so gilt $G \cong \mathbb{Z}/p\mathbb{Z}$.
(ii) Sei $\operatorname{ord}(G) = p^2$. Dann ist G zu einer der beiden abelschen Gruppen

$$\mathbb{Z}/p^2\mathbb{Z} \text{ oder } \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

isomorph (G ist abelsch und man kann den Hauptsatz der abelschen Gruppen anwenden).

Definition 3.6. Sei G eine Gruppe. Eine Untergruppe $H \subseteq G$ heißt *p-Sylowuntergruppe*, wenn gilt:

(i) H ist eine p-Gruppe.
(ii) Ist $H \subseteq Q \subseteq G$ eine p-Gruppe, so folgt $H = Q$.

Eine p-Sylowuntergruppe ist eine maximale p-Gruppe.

Bemerkung 3.7. Ist G eine endliche abelsche Gruppe, so kann man aus dem Hauptsatz für abelsche Gruppen folgern, dass genau eine p-Sylowuntergruppe H existiert. Es ist

$$H = \{a \in G \colon \operatorname{ord}(a) \text{ ist eine } p\text{-Potenz}\}.$$

Lemma 3.8. Sei G eine Gruppe. Dann existiert eine p-Sylowuntergruppe $H \subseteq G$.

Beweis. Sei $\mathcal{P}$ die Menge der p-Untergruppen von G. Dann ist $\mathcal{P} \neq \emptyset$, da $\{e\} \in \mathcal{P}$. Ferner ist $\mathcal{P}$ bzgl. der Inklusion partiell geordnet. Ist $\{H_i\}_{i \in I}$ eine vollständig geordnete Familie von p-Untergruppen von G, dann ist auch $H = \cup_{i \in I} H_i$ eine p-Gruppe und daher eine obere Schranke der Familie in $\mathcal{P}$. Nach dem Lemma von Zorn existiert in $\mathcal{P}$ ein maximales Element P. Dies ist dann eine p-Sylowuntergruppe von G. □

Lemma 3.9. Sei G eine endliche Gruppe, die auf einer Menge X operiert. Für ein $x \in X$ sei r die Anzahl der Elemente der Bahn Gx und $G_x = \{a \in G \colon a(x) = x\}$ die Isotropiegruppe von x. Dann gilt:

$$\operatorname{ord}(G) = \operatorname{ord}(G_x)r.$$

Beweis. Seien $a_1(x), \ldots, a_r(x)$ die verschiedenen Elemente der Bahn von x mit $a_i \in G$. Dann sind die Elemente

$$a_1 b, \ldots, a_r b \text{ mit } b \in G_x$$

alle verschieden. Denn wäre $a_i b = a_j b'$ für $b, b' \in G_x$, so ist

$$a_i(x) = a_i(b(x)) = a_i b(x) = a_j b'(x) = a_j(b'(x)) = a_j(x),$$

also $i = j$. Dann folgt $b = b'$. Wir haben

$$\operatorname{ord}(G) \geq \operatorname{ord}(G_x)r$$

bewiesen.

Ist $a \in G$ beliebig. Dann muss $a(x) = a_i(x)$ für ein $i \in \{1, \ldots, r\}$ gelten. Es folgt, dass $a_i^{-1} a \in G_x$ gilt, da

$$a_i^{-1} a(x) = a_i^{-1} a_i(x) = e(x) = x.$$

Also existiert ein $b \in U$ mit $a = a_i b$. Somit $\operatorname{ord}(G) \leq \operatorname{ord}(G_x)r$ und insgesamt

$$\operatorname{ord}(G) = \operatorname{ord}(G_x)r.$$

□

Lemma 3.10. *(Fundamentallemma)* Sei p eine Primzahl und G eine Gruppe mit $\operatorname{ord}(G) = p^n$, die auf einer endlichen Menge X operiert. Sei $X_0 = \{x \in X \colon a(x) = x, a \in G\}$ die Menge der Fixpunkte der Operation. Dann gilt

$$|X| \equiv |X_0| \mod p.$$

Beweis. Nach 1.7 ist X die disjunkte Vereinigung der Bahnen der Operation und daher

$$|X| = |X_0| + |Gx_1| + \cdots + |Gx_m|,$$

wobei Gx_i die Bahnen mit $|Gx_i| > 1$ durchläuft. Nach 3.9 ist $|Gx_i|$ ein Teiler von $\operatorname{ord}(G) = p^n$, also durch p teilbar. Daher folgt

$$|X| \equiv |X_0| \mod p.$$

□

Bemerkung 3.11. Sei G eine Gruppe und X die Menge aller Untergruppen von G. Dann ist die Abbildung $G \times X \longrightarrow X$, $(a, H) \mapsto aHa^{-1}$ eine Gruppenoperation von G auf X (Beachte, dass aHa^{-1} eine Gruppe ist). Diese heißt Konjugation. Ist $H \subseteq G$ eine Untergruppe, so heißt die Isotropiegruppe

$$N(H) = \{a \in G \colon aHa^{-1} = H\}$$

der *Normalisator* von H. Man sieht, das H ein Normalteiler von $N(H)$ ist. Ferner gilt $H \triangleleft G$ genau dann, wenn $G = N(H)$.

Lemma 3.12. Sei H eine p-Gruppe von G. Dann gilt

$$[N(H) : H] \equiv [G : H] \mod p.$$

Beweis. Definiere folgende Abbildung

$$H \times G/H \to G/H, \quad (a, bH) \mapsto abH.$$

Dies definiert eine Operation von H auf der Menge der Linksnebenklassen von H. Sei

$$X_0 = \{bH \in G/H : abH = bH \text{ für } a \in H\}$$

die Menge aller Fixpunkte dieser Operation. Es gilt

$$bH \in X_0 \Leftrightarrow abH = bH \text{ für alle } a \in H \Leftrightarrow b^{-1}ab \in H \text{ für alle } a \in H \Leftrightarrow$$

$$bab^{-1} \in H \text{ für alle } a \in H \Leftrightarrow bHb^{-1} = H \Leftrightarrow b \in N(H).$$

Also ist X_0 die Menge aller Linksnebenklassen bH mit $b \in N(H)$ und daher

$$|X_0| = [N(H) : H].$$

Ferner

$$|G/H| = [G : H]$$

und es folgt aus 3.10

$$[N(H) : H] \equiv [G : H] \mod p.$$

□

Korollar 3.13. Sei H eine p-Gruppe von G und $p|[G : H]$, dann ist $N(H) \neq H$.

Beweis. Aus 3.12 folgt

$$[N(H) : H] \equiv 0 \mod p$$

und daher $[N(H) : H] > 1$, also $N(H) \neq H$. □

Satz 3.14. *(1. Satz von Sylow)* Sei G eine endliche Gruppe mit $\text{ord}(G) = p^n m$ und p teilt nicht m. Dann gilt:

(i) Für $i = 0, \ldots, n$ besitzt G eine Untergruppe der Ordnung p^i.

(ii) Jede Untergruppe von G der Ordnung p^i mit $i \in \{0, \ldots, n-1\}$ ist Normalteiler in einer Untergruppe der Ordnung p^{i+1}.

Beweis. Für $n = 0$ sind die Aussagen trivial, also sei $n > 0$. Zu (i): Wir konstruieren induktiv eine Kette von Untergruppen

$$G_n \supset G_{n-1} \supset \ldots \supset G_0 = \{0\}$$

derart, dass $\text{ord}(G_i) = p^i$ und $G_i \triangleleft G_{i+1}$. Definiere $G_0 = \{e_G\}$. Sei nun schon die Existenz von $G_i, \ldots, G_0$ für $0 \leq i < n$ bereits gezeigt. Dann ist

$$[G : G_i] = \text{ord}(G)/\text{ord}(G_i) = p^{n-i}m.$$

Da $p|[G : G_i]$ folgt aus 3.13, dass $N(G_i) \neq G_i$. Beachte, dass $G_i \triangleleft N(G_i)$. Also ist $N(G_i)/G_i$ eine Gruppe mit $p|\text{ord}(N(G_i)/G_i)$ (siehe 3.12).

Nach dem Satz von Cauchy 3.2 besitzt $N(G_i)/G_i$ ein Element aG_i mit $\text{ord}(aG_i) = p$ für ein $a \in N(G_i)$. Definiere $\overline{G}_{i+1} = \langle aG_i \rangle$ mit $\text{ord}(\overline{G}_{i+1}) = p$. Sei

$$\varepsilon : N(G_i) \to N(G_i)/G_i$$

der kanonische Epimorphismus. Definiere

$$G_{i+1} = \varepsilon^{-1}(\overline{G}_{i+1})$$

Dann ist $G_{i+1} \subseteq N(G_i) \subseteq G$ eine Gruppe. Da $G_i \triangleleft N(G_i)$, gilt auch $G_i \triangleleft G_{i+1}$. Ferner $[G_{i+1} : G_i] = \mathrm{ord}(G_{i+1}/G_i) = p$. Daher

$$\mathrm{ord}(G_{i+1}) = [G_{i+1} : G_i]\mathrm{ord}(G_i) = pp^i = p^{i+1}.$$

Beachte, dass im Induktionsschritt auch (ii) bewiesen wurde. □

Korollar 3.15. Sei G eine endliche Gruppe mit $\mathrm{ord}(G) = p^n m$ und p teilt nicht m. Sei H eine p-Untergruppe von G. Dann sind folgende Aussagen äquivalent:

(i) H ist eine p-Sylowuntergruppe.
(ii) p teilt nicht $[G : H]$.
(iii) $\mathrm{ord}(H) = p^n$.

Insbesondere besitzt jede p-Sylowuntergruppen von G die Ordnung p^n.

Beweis. (i) ⇒ (ii): Angenommen: $p|[G : H]$. Dann ist $\mathrm{ord}(H) = p^i$ mit $0 \leq i < n$. Aus 3.14 folgt dann aber die Existenz einer p-Gruppe $P \supseteq H$ mit $P \neq H$. Dies ist ein Widerspruch und daher gilt (ii).

(ii) ⇒ (iii): Es gilt

$$p^n m = \mathrm{ord}(G) = [G : H]\mathrm{ord}(H).$$

Wegen der Voraussetzung muss $\mathrm{ord}(H) = p^n$ gelten.

(iii) ⇒ (i): Es kann keine p-Gruppe P geben mit $P \supseteq H$ geben und $P \neq H$, da dann $\mathrm{ord}(P) > p^n$ und $\mathrm{ord}(P)|\mathrm{ord}(G) = p^n m$ folgen würde. Dies ist aber nicht möglich, also ist H eine p-Sylowuntergruppe. □

Korollar 3.16. Sei G eine Gruppe der Ordnung p^n. Dann gibt es eine absteigende Kette von Untergruppen

$$G = G_n \supset G_{n-1} \supset \ldots \supset G_0 = \{0\}$$

derart, dass $\mathrm{ord}(G_i) = p^i$ und $G_i \triangleleft G_{i+1}$. Ferner ist G_{i+1}/G_i zyklisch.

Beweis. Aus dem Beweis von 3.14 folgt die Existenz einer Kette

$$G_n \supset \ldots \supset G_0 = \{0\}$$

mit $\mathrm{ord}(G_i) = p^i$ und $G_i \triangleleft G_{i+1}$. Nun ist

$$\mathrm{ord}(G_{i+1}/G_i) = [G_{i+1} : G_i] = p,$$

und daher ist G_{i+1}/G_i eine zyklische Gruppe. Schliesslich ist wegen $\mathrm{ord}(G) = p^n$ dann $G = G_n$. □

Bemerkung 3.17. Es gilt:

(i) Sei G eine endliche Gruppe, H eine p-Sylowuntergruppe und $a \in G$. Dann ist die Konjugierte aHa^{-1} wieder eine p-Sylowuntergruppe.
(ii) Besitzt G nur eine p-Sylowuntergruppe, so ist diese wegen (i) ein Normalteiler in G.

Beweis. Zu (i): Sei $H' = aHa^{-1}$. Dann ist $\mathrm{ord}(H') = \mathrm{ord}(H)$ eine p-Potenz. Wäre $P \supset H'$ eine p-Gruppe mit $P \neq H'$, dann würde

$$a^{-1}Pa \supset H$$

eine p-Gruppe mit $a^{-1}Pa \neq H$ sein. Dies ist ein Widerspruch, da H eine p-Sylowuntergruppe ist. Also muss auch H' eine p-Sylowuntergruppe sein.

Zu (ii): Wegen (i) muss

$$aHa^{-1} = H$$

für alle $a \in G$ gelten. Also ist $H \lhd G$. □

Satz 3.18. *(2. Satz von Sylow)* Sei G eine endliche Gruppe. Dann gilt:

(i) Zu jeder p-Untergruppe H von G und jeder p-Sylowuntergruppe P von G existiert ein $a \in G$ mit $aHa^{-1} \subseteq P$.
(ii) Je zwei p-Sylowuntergruppen sind konjugiert.

Beweis. Zu (i): Definiere folgende Abbildung

$$H \times G/P \longrightarrow G/P, \quad (a, bP) \mapsto abP.$$

Dies definiert eine Operation von H auf der Menge der Linksnebenklassen von P. Sei

$$X_0 = \{bP \in G/P \colon abP = bP \text{ für } a \in H\}$$

die Menge aller Fixpunkte dieser Operation. Aus 3.10 folgt

$$|X_0| \equiv |G/P| \mod p.$$

Aus 3.15 folgt, dass p nicht $[G : P] = |G/P|$ teilt. Daher ist $|X_0| \neq 0$. Es gibt dann ein $b \in G$ mit $abP = bP$ für alle $a \in H$. Dies ist äquivalent zu $b^{-1}ab \in P$ für alle $a \in H$. Somit gilt

$$b^{-1}Hb \subseteq P.$$

Dies zeigt die Behauptung.

Zu (ii): Seien P und P' zwei p-Sylowuntergruppen von G. Dann existiert nach (i) ein $a \in G$ mit

$$aPa^{-1} \subseteq P'.$$

Wegen 3.15 haben je zwei p-Sylowuntergruppen die gleiche Ordnung. Ausserdem gilt

$$\mathrm{ord}(P') = \mathrm{ord}(P) = \mathrm{ord}(aPa^{-1}).$$

Daher ist $P' = aPa^{-1}$ und dies war zu zeigen. □

Satz 3.19. *(3. Satz von Sylow)* Sei G eine endliche Gruppe. Sei s_p die Anzahl der verschiedenen p-Sylowuntergruppen von G. Dann gilt:

(i) $\mathrm{ord}(G) \equiv 0 \mod s_p$.
(ii) $s_p \equiv 1 \mod p$.

Beweis. Zu (i): Sei X die Menge aller Untergruppen von G. Definiere folgende Abbildung

$$G \times X \longrightarrow X, \quad (a, H) \mapsto aHa^{-1}.$$

Dies definiert eine Operation von G auf X. Sei P eine beliebige p-Sylowuntergruppe von G. Dann ist s_p nach 3.18 gerade die Anzahl der Elemente der Bahn von P unter der definierten Operation. Wegen 3.9 ist daher s_p ein Teiler von $\mathrm{ord}(G)$ und dies bedeutet

$$\mathrm{ord}(G) \equiv 0 \mod s_p.$$

Zu (ii): Sei X' die Menge aller p-Sylowuntergruppen von G und P wieder eine feste p-Sylowuntergruppe von G. Definiere die Operation

$$P \times X' \longrightarrow X', \quad (a, H) \mapsto aHa^{-1}.$$

Sei X'_0 die Menge aller Fixpunkte dieser Operation, also

$$X'_0 = \{H \in X' \colon aHa^{-1} = H \text{ für alle } a \in P\}.$$

Behauptung: $X'_0 = \{P\}$. Es ist $H \in X'_0$ genau dann, wenn $P \subseteq N(H)$, wobei

$$N(H) = \{a \in G \colon aHa^{-1} = H\}$$

der Normalisator von H ist. Es gilt immer $H \subseteq N(H)$. Da P, H p-Sylowuntergruppen von G sind, müssen sie dann auch p-Sylowuntergruppen von $N(H)$ sein. Nach 3.18 sind P und H in $N(H)$ konjugiert, also existiert ein $a \in N(H)$ mit

$$P = aHa^{-1}.$$

Aber nach Definition ist $aHa^{-1} = H$ und daher folgt $P = H$. Somit $X'_0 = \{P\}$. Dann folgt aus 3.10

$$s_p = |X'| \equiv |X'_0| \mod p \equiv 1 \mod p.$$

□

Satz 3.20. Seien p und q Primzahlen mit $p > q$ und $q \not| p-1$. Dann ist jede Gruppe der Ordnung pq zyklisch.

Beweis. Sei G eine Gruppe der Ordnung pq. Nach dem Satz von Cauchy 3.2 besitzt G ein Element a der Ordnung p und ein Element b der Ordnung q. Seien s_p bzw. s_q die Anzahl der verschiedenen p-Sylowuntergruppen bzw. q-Sylowuntergruppen. Nach 3.19 gilt $s_p | pq$ und $p | (s_p - 1)$. Es muss einer der folgenden Fälle gelten:

(i) $s_p = 1$
(ii) $s_p = p$
(iii) $s_p = q$
(iv) $s_p = pq$

Der Fall (ii) kann nicht auftreten, da p nicht $p-1$ teilt. (iii) bzw. (iv) sind nicht möglich, da $p > q$ und daher p nicht $q-1$ bzw. p nicht $pq-1$ teilt. Also muss $s_p = 1$ gelten. Dann ist aber $\langle a \rangle$ die einzige p-Sylowuntergruppe von G und diese muss nach 3.17 ein Normalteiler sein.

Analog ist s_q ein Teiler von pq und $s_q - 1$ ist durch q teilbar. q teilt nicht $pq - 1$ und $q - 1$. Ausserdem auch nicht $p - 1$ nach Voraussetzung. Daher muss $s_q = 1$ gelten. Somit ist auch $\langle b \rangle$ ein Normalteiler von G.

Es ist $\langle a \rangle \cap \langle b \rangle = \{e\}$. Sei $H = \langle a, b \rangle$. Es ist $H = \langle a \rangle \times \langle b \rangle$ (Übungsaufgabe). Da $\mathrm{ord}(H) \geq pq$, folgt

$$G = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}/(p) \times \mathbb{Z}/(q) \cong \mathbb{Z}/(pq).$$

□

Beispiel 3.21. Jede Gruppe der Ordnung $15 = 3 \cdot 5$ oder $33 = 3 \cdot 11$ ist zyklisch.

4. Permutationsgruppen

Sei stets $n \in \mathbb{N}$. In diesem Abschnitt untersuchen wir die Gruppe S_n.

Definition 4.1. Für $r \in \mathbb{N}$, $r \geq 2$ heißt ein $\sigma \in S_n$ ein *r-Zyklus*, wenn es Zahlen $j_1, \ldots, j_r$ gibt mit $\sigma(j_i) = j_{i+1}$ für $i = 1, \ldots, r-1$, $\sigma(j_r) = j_1$ und $\sigma(k) = k$ für $k \in \{1, \ldots, n\} \setminus \{j_1, \ldots, j_r\}$. Ein solcher Zyklus wird

$$(j_1, \ldots, j_r)$$

geschrieben. 2-Zyklen heißen auch *Transpositionen.*

Bemerkung 4.2. Es gilt:

(i) Eine Transposition (i, j) vertauscht i und j und lässt alle anderen Zahlen aus $\{1, \ldots, n\}$ fest. Es ist $(i, j)^{-1} = (i, j)$ und $(i, j)^2 = id$.

(ii) Sei $\sigma = (j_1, \ldots, j_r)$ ein r-Zyklus. Dann gilt

$$\mathrm{ord}(\sigma) = r \text{ und } \sigma^{-1} = (j_r, \ldots, j_1).$$

Für ein $\tau \in S_n$ rechnet man nach, dass

$$\tau\sigma\tau^{-1} = (\tau(j_1), \ldots, \tau(j_r))$$

gilt.

Definition 4.3. Zwei Permutationen $\sigma, \tau \in S_n$ heißen *disjunkt*, wenn alle Zahlen, die bei σ bzw. τ bewegt werden, bei τ bzw. σ fest bleiben.

Bemerkung 4.4. Es ist:

(i) Z.B. sind $(1, 2)$ und $(3, 4)$ disjunkt, aber $(1, 2)$ und $(2, 3)$ nicht.

(ii) Sind $\sigma, \tau \in S_n$ disjunkt, so gilt $\sigma \circ \tau = \tau \circ \sigma$.

Satz 4.5. Jede Permutation $\sigma \in S_n$ lässt sich eindeutig (bis auf Reihenfolge der Faktoren) als Produkt paarweiser disjunkter Zyklen zerlegen. Diese Zerlegung heißt die *Zyklenzerlegung* von σ.

Beweis. Sei $H = \langle \sigma \rangle \subseteq S_n$. Dann operiert H auf $\{1, \ldots, n\}$.

Existenz der Zerlegung: Seien $B_1, \ldots, B_l$ die Bahnen der Operation von H mit $|B_i| > 1$ für $i = 1, \ldots, l$. Definiere

$$\sigma_i(x) = \begin{cases} \sigma(x) \in B_i & \text{für } x \in B_i, \\ x & \text{für } x \notin B_i. \end{cases}$$

Dann gilt $\sigma_i \in S_n$. Da die Bahnen paarweise disjunkt sind folgt, dass auch die σ_i paarweise disjunkt sind. Ferner gilt per Definition

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_l.$$

Nun muss noch gezeigt werden, dass die σ_i Zyklen sind. Sei $|B_i| = r_i$ und für ein $x \in B_i$ sei $m > 0$ die kleinste Zahl mit $\sigma^m(x) = x$. Dann sind

$$x = \sigma^0(x), \sigma(x), \ldots, \sigma^{m-1}(x)$$

paarweise verschieden und für jedes $n \in \mathbb{Z}$ ist $\sigma^n(x) = \sigma^j(x)$ für ein $j \in \{0, \ldots, m-1\}$. Daher gilt

$$B_i = \{x, \sigma(x), \ldots, \sigma^{m-1}(x)\}.$$

und $m = r_i$. Ferner ist σ_i der r_i-Zyklus

$$(x, \sigma(x), \ldots, \sigma^{r_i-1}(x)).$$

Eindeutigkeit: Sei

$$\sigma = \sigma'_1 \circ \cdots \circ \sigma'_k.$$

eine weitere Zerlegungen von σ in ein Produkt paarweiser disjunkter Zyklen. Wir beweisen die Aussage durch eine Induktion nach $m = \min\{l, k\}$. Ist $m = 0$, so ist $\sigma = id_{S_n}$ und die Behauptung ist trivial. Sei nun $m > 0$. Wähle $x \in \{1, \ldots, n\}$ mit $\sigma(x) \neq x$. Dann muss $x \in B_i$ für ein i gelten. Ferner existiert ein eindeutiges $j \in \{1, \ldots, k\}$ mit $\sigma'_j(x) \neq x$. Ist

$$\sigma'_j = (j'_1, \ldots, j'_{r_j}),$$

dann muss $\{j'_1, \ldots, j'_{r_i}\}$ die Bahn von x sein, da jedes andere σ'_l das Element x festhält. Also $B_i = \{j'_1, \ldots, j'_{r_i}\}$. Dies bedeutet aber $\sigma'_j = \sigma_i$. Betrachte

$$\begin{aligned}\sigma \circ \sigma_i^{-1} &= \sigma_1 \circ \cdots \circ \sigma_{i-1} \circ \sigma_{i+1} \circ \cdots \circ \sigma_l. \\ &= \sigma'_1 \circ \cdots \circ \sigma'_{j-1} \circ \sigma'_{j+1} \circ \cdots \circ \sigma'_k.\end{aligned}$$

Nach der Induktionsannahme hat $\sigma \circ \sigma_i^{-1}$ eine eindeutige Zyklendarstellung und es folgt nach einer eventuellen Umnummerierung $l = k$ und $\sigma_j = \sigma'_j$ für $j = 1, \ldots, l$. □

Korollar 4.6. Jedes $\sigma \in S_n$ ist Produkt von Transpositionen.

Beweis. Sei $(j_1, \ldots, j_r) \in S_n$ ein beliebiger Zyklus. Dann gilt

$$(j_1, \ldots, j_r) = (j_1, j_2) \circ (j_2, j_3) \circ \cdots \circ (j_{r-1}, j_r).$$

Die Behauptung folgt aus diesem Sachverhalt und 4.5. □

Definition 4.7. Sei $\sigma \in S_n$. Die Abbildung

$$\operatorname{sign}(\sigma) = \prod_{j<i} \frac{\sigma(i) - \sigma(j)}{i - j} \in \{1, -1\}$$

heißt das *Signum* von σ. Ist $j < i$, aber $\sigma(j) > \sigma(i)$, so heißt (j, i) ein *Fehlstand* von σ. Ist $\operatorname{sign}(\sigma) = 1$ bzw. $\operatorname{sign}(\sigma) = -1$, dann heißt σ eine *gerade* bzw. *ungerade* Permutation.

Beispiel 4.8. Sei $\tau = (i, j) \in S_n$ eine Transposition, dann gilt $\operatorname{sign}(\tau) = -1$.

Satz 4.9. Sei $\sigma \in S_n$ beliebig und $\tau = (k,l) \in S_n$ mit $k < l$ eine Transposition. Dann gilt $\operatorname{sign}(\sigma \circ \tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau) = -\operatorname{sign}(\sigma)$.

Beweis. Es gilt

$$\begin{aligned}\operatorname{sign}(\sigma\circ\tau) &= \prod_{j<i}\frac{\sigma(\tau(i))-\sigma(\tau(j))}{i-j} = \prod_{j<i}\frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)}\prod_{j<i}\frac{\tau(i)-\tau(j)}{i-j}\\ &= \prod_{j<i}\frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)}\cdot\operatorname{sign}(\tau)\\ &= \prod_{j<i,\{j,i\}\cap\{k,l\}=\emptyset}\frac{\sigma(i)-\sigma(j)}{i-j}\cdot\frac{\sigma(k)-\sigma(l)}{k-l}\cdot\prod_{j<i,j=k,i>l}\frac{\sigma(i)-\sigma(l)}{i-l}\\ &\quad\prod_{j<i,j=l}\frac{\sigma(i)-\sigma(k)}{i-k}\prod_{j<i,j<k,i=l}\frac{\sigma(k)-\sigma(j)}{k-j}\prod_{j<i,i=k}\frac{\sigma(l)-\sigma(j)}{l-j}\cdot\operatorname{sign}(\tau)\\ &= \operatorname{sign}(\sigma)\cdot\operatorname{sign}(\tau) = -\operatorname{sign}(\sigma).\end{aligned}$$

□

Korollar 4.10. Es gilt:

(i) Ist $\sigma \in S_n$ Produkt von m Transpositionen, dann

$$\operatorname{sign}(\sigma) = (-1)^m.$$

(ii) Ist σ ein r-Zyklus, dann ist $\operatorname{sign}(\sigma) = (-1)^r$.

Beweis. Zu (i): Dies ist nun trivial.

Zu (ii): Ist $\sigma = (j_1, \ldots, j_r) \in S_n$, dann gilt

$$(j_1, \ldots, j_r) = (j_1, j_2) \circ (j_2, j_3) \circ \ldots \circ (j_{r-1}, j_r).$$

Die Behauptung folgt nun aus (i). □

Korollar 4.11. Die Abbildung

$$\operatorname{sign}\colon S_n \longrightarrow \{1,-1\}, \quad \sigma \mapsto \operatorname{sign}(\sigma)$$

ist ein Gruppenhomomorphismus.

Beweis. Wir müssen für alle $\sigma, \pi \in S_n$

$$\operatorname{sign}(\sigma \circ \pi) = \operatorname{sign}(\sigma)\operatorname{sign}(\pi).$$

zeigen. Aus 4.6 folgt, dass

$$\sigma = \tau_1 \circ \ldots \circ \tau_n, \quad \pi = \tau_{n+1} \circ \ldots \circ \tau_m,$$

mit Transpositionen τ_i. Wegen 4.9 gilt

$$\operatorname{sign}(\sigma) \cdot \operatorname{sign}(\pi) = (-1)^n(-1)^{m-n} = (-1)^m = \operatorname{sign}(\sigma \circ \pi).$$

□

Definition 4.12. Die Menge

$$A_n = \{\sigma \in S_n : \operatorname{sign}(\sigma) = 1\}$$

der geraden Permutationen heißt die *alternierende Gruppe* n-ten Grades.

Bemerkung 4.13. Es gilt:

(i) A_n ist ein Normalteiler von S_n, da A_n der Kern eines Gruppenhomomorphismus ist.
(ii) Für $n > 1$ gilt $S_n/A_n \cong \{1, -1\}$. Daher folgt

$$[S_n : A_n] = 2, \quad \operatorname{ord}(A_n) = \frac{1}{2}n!.$$

5. Auflösbare Gruppen

Definition 5.1. Sei G eine Gruppe. Eine Kette von Untergruppen

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

von G heißt *Normalreihe* von G, wenn $G_{i+1} \triangleleft G_i$ für $i = 0, \ldots, n-1$ ist. Die Faktorgruppen G_i/G_{i+1} heißen die *Faktoren* der Normalreihe. G heißt *auflösbar*, wenn G eine Normalreihe mit abelschen Faktoren besitzt.

Beispiel 5.2. Es gilt:

(i) Jede abelsche Gruppe ist auflösbar.
(ii) Besitzt eine nicht abelsche Gruppe keine Normalteiler, so ist sie nicht auflösbar.
(iii) Jede endliche p-Gruppe ist nach 3.16 auflösbar.

Definition 5.3. Sei G eine Gruppe. Für $a, b \in G$ heißt $[a, b] = aba^{-1}b^{-1}$ der *Kommutator* von a, b. Sei

$$[G, G] = \langle [a, b] \colon a, b \in G \rangle \subseteq G$$

die von allen Kommutatoren erzeugte Untergruppe von G. Sie heißt die *Kommutatorgruppe* von G (G ist abelsch genau dann, wenn $[G, G] = \{e\}$).

Bemerkung 5.4. Sei G eine Gruppe. Dann gilt:

(i) $[G, G]$ besteht aus endlichen Produkten von Kommutatoren aus G.
(ii) $[G, G] \triangleleft G$.
(iii) $G/[G, G]$ ist abelsch.
(iv) Ist $H \triangleleft G$ mit G/H abelsch, dann gilt $[G, G] \subseteq H$.

Beweis. (i), (ii) und (iii) rechnet man leicht nach (Übungsaufgabe).

Zu (iv): Seien $a, b \in G$. Dann gilt $a^{-1}b^{-1}H = b^{-1}a^{-1}H$, da G/H abelsch ist. Daher $[a, b] = aba^{-1}b^{-1} \in H$ und insgesamt folgt die Behauptung. □

Definition 5.5. Sei G eine Gruppe. Wir definieren induktiv

$$G^{(0)} = G \text{ und } G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

Die Gruppe $G^{(i)}$ heißt die *i-te iterierte Kommutatorgruppe* von G.

Bemerkung 5.6. Wegen 5.4 gilt:

(i) $G = G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(i)} \supseteq \ldots$
(ii) $G^{(i+1)} \triangleleft G^{(i)}$.
(iii) $G^{(i)}/G^{(i+1)}$ ist abelsch.

Satz 5.7. Eine Gruppe G ist genau dann auflösbar, wenn ein $n \in \mathbb{N}$ existiert mit $G^{(n)} = \{e\}$.

Beweis. Sei $G^{(n)} = \{e\}$ für ein $n \in \mathbb{N}$. Dann ist

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(n)} = \{e\}$$

wegen 5.6 eine Normalreihe mit abelschen Faktoren. Also ist G auflösbar.

Sei nun G auflösbar und

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

die zugehörige Normalreihe mit abelschen Faktoren. Wir zeigen per Induktion, dass $G^{(i)} \subseteq G_i$ für alle i gilt. Dann ist $G^{(n)} = \{e\}$.

Für $i = 0$ ist $G^{(0)} = G = G_0$. Sei nun $i > 0$ und $G^{(i)} \subseteq G_i$ bereits bewiesen. Da G_i/G_{i+1} abelsch ist, folgt aus 5.4, dass $[G_i, G_i] \subseteq G_{i+1}$. Dann

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1}.$$

□

Satz 5.8. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann gilt:

(i) Ist G auflösbar, so ist auch H auflösbar.
(ii) Gilt $H \triangleleft G$, dann ist G genau dann auflösbar, wenn H und G/H auflösbar sind.

Beweis. Sei G auflösbar. Dann existiert wegen 5.7 ein $n \in \mathbb{N}$ mit $G^{(n)} = \{e\}$. Da $H^{(i)} \subseteq G^{(i)}$, gilt $H^{(n)} = \{e\}$ und daher ist H auflösbar. Dies zeigt (i).

Sei nun H ein Normalteiler und

$$\varepsilon \colon G \to G/H$$

der kanonische Epimorphismus. Durch eine Induktion folgt

$$(G/H)^{(i)} = \varepsilon(G^{(i)})$$

für alle i. Dann ist $(G/H)^{(n)} = \{e\}$ und auch G/H ist auflösbar.

Sei nun $H \triangleleft G$ und H, G/H auflösbar. Dann existiert ein n mit $H^{(n)} = \{e\}$ und $(G/H)^{(n)} = \{e\}$. Da

$$\varepsilon(G^{(n)}) = (G/H)^{(n)} = \{e\},$$

gilt $G^{(n)} \subseteq H$. Dann ist $G^{(2n)} \subseteq H^{(n)} = \{e\}$. Somit ist auch G auflösbar. □

Lemma 5.9. Sei G eine endliche abelsche Gruppe. Dann existiert eine Normalreihe

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

mit zyklischen Faktoren G_i/G_{i+1} (mit einer Potenz einer Primzahl als Ordnung).

Beweis. Nach dem Hauptsatz für abelsche Gruppen hat G o.E. die Gestalt

$$G = \oplus_{i=1}^{r} \mathbb{Z}/(p_i^{s_i})$$

mit Primzahlen $p_1, \ldots, p_r$ und $s_1, \ldots, s_r \in \mathbb{N}$. Definiere

$$G_j = \oplus_{i=1}^{n-j} \mathbb{Z}/(p_i^{s_i}).$$

Dann ist

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

und

$$G_j/G_{j+1} \cong \mathbb{Z}/(p_{n-j}^{s_{n-j}})$$

ist zyklisch (mit einer Potenz einer Primzahl als Ordnung). Dies war zu zeigen. □

Satz 5.10. Sei G eine endliche auflösbare Gruppe. Dann lässt sich jede Normalreihe mit abelschen Faktoren zu einer Normalreihe mit zyklischen Faktoren (mit einer Potenz einer Primzahl als Ordnung) verfeinern.

Beweis. Sei

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

die vorgegebene Normalreihe mit abelschen Faktoren. Da G_i/G_{i+1} abelsch ist, existiert nach 5.9 eine Normalreihe

$$G_i/G_{i+1} = \overline{G_{i,0}} \supseteq \cdots \supseteq \overline{G_{i,n_i}} = \{e\}$$

mit zyklischen Faktoren (mit einer Potenz einer Primzahl als Ordnung). Sei

$$\varepsilon\colon G_i \longrightarrow G_i/G_{i+1}$$

der kanonische Epimorphismus. Definiere $G_{i,j} = \varepsilon^{-1}(\overline{G_{i,j}})$ für $j = 0, \ldots, n_i$. Beachte, dass wegen Kapitel 1, 2.8 stets $G_{i,j+1} \lhd G_{i,j}$ gilt. Dann ist

$$G_{i,j}/G_{i,j+1} \cong (G_{i,j}/G_{j+1})/(G_{i,j+1}/G_{j+1}) \cong \overline{G_{i,j}}/\overline{G_{i,j+1}}$$

zyklisch (mit einer Potenz einer Primzahl als Ordnung). Ferner $G_{i+1,0} = G_{i+1} = G_{i,n_i}$ und daher ist

$$G = G_0 = G_{1,0} \supseteq G_{1,1} \supseteq \ldots \supseteq G_{1,n_1} = G_2 = G_{2,0} \supseteq \ldots$$

eine Normalreihe von G mit zyklischen Faktoren (mit einer Potenz einer Primzahl als Ordnung). □

Satz 5.11. Sei $n \in \mathbb{N}$. Dann gilt:

(i) $[S_n, S_n] = A_n$ für $n \geq 2$.
(ii) $[A_n, A_n] = A_n$ für $n \geq 5$.
(iii) $[A_n, A_n] = \{\mathrm{id}\}$ für $n = 2, 3$.
(iv) $[A_4, A_4] \cong K_4 \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Hierbei ist K_4 die Kleinsche Vierergruppe.

Beweis. Zu (i): Da $A_n \lhd S_n$ und S_n/A_n abelsch, folgt aus 5.4 $[S_n, S_n] \subseteq A_n$. Da $A_2 = \{id\}$ folgt direkt $[S_2, S_2] = A_2$. Die Gruppe A_n wird für $n \geq 3$ von allen 3-Zyklen erzeugt (Übungsaufgabe). Sei nun $(i, j, k) \in A_n$ ein solcher Zyklus. Dann ist

$$(i, j, k) = (i, k)(j, k)(i, k)^{-1}(j, k)^{-1} = [(i, k), (j, k)] \in [S_n, S_n].$$

Daher gilt $A_n \subseteq [S_n, S_n]$ und somit $A_n = [S_n, S_n]$.

Zu (ii): Wähle paarweise verschiedene Zahlen $i, j, k, l, m \in \{1, \ldots, n\}$. Dann gilt

$$(i, j, k) = [(i, j, l), (i, k, m)] \in [A_n, A_n].$$

Es folgt $A_n \subseteq [A_n, A_n]$ und somit $A_n = [A_n, A_n]$.

Zu (iii): Die Gruppen $A_2 = \{id\}$ und $A_3 = \{\mathrm{id}, (1, 2, 3), (1, 3, 2)\} \cong \langle(1, 2, 3)\rangle \cong \mathbb{Z}/(3)$ sind beide abelsch und daher ist der Kommutator trivial.

Zu (iv): Dies folgt durch eine direkte Rechnung (Übungsaufgabe). □

Korollar 5.12. S_n ist auflösbar genau dann, wenn $n \leq 4$.

Beweis. Die Behauptung folgt aus 5.7 und 5.11. □

KAPITEL 5

Anwendungen der Galoistheorie

1. Der Fundamentalsatz der Algebra

Bemerkung 1.1. Folgende Eigenschaften des Körpers $\mathbb{R}$ werden in diesem Abschnitt benutzt:

(i) Jedes Polynom $f \in \mathbb{R}[X]$ ungeraden Grades hat eine Nullstelle in $\mathbb{R}$.
(ii) Jedes $a \in \mathbb{R}$ mit $a \geq 0$ hat eine Quadratwurzel. Hieraus folgt, dass jedes $z \in \mathbb{C}$ eine Quadratwurzel besitzt.

Die Aussagen über die reellen Zahlen lassen sich leicht mit dem Zwischenwertsatz beweisen. Eine Gleichung $z = x + iy = (a + ib)^2$ führt zu

$$a^2 = \frac{1}{2}x \pm \frac{1}{2}\sqrt{x^2 + y^2} \text{ und } b^2 = -\frac{1}{2}x \pm \frac{1}{2}\sqrt{x^2 + y^2}$$

und dies ist lösbar.

Satz 1.2. *(Gauß)* Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.

Beweis. Sei a algebraisch über $\mathbb{C}$. Wir müssen zeigen, dass $a \in \mathbb{C}$ gilt. Dies beweist die Behauptung.

Sei $L = \mathbb{C}(a)$. Da $[\mathbb{C} : \mathbb{R}] = 2$ und $[L : \mathbb{C}] < \infty$ folgt, dass $[L : \mathbb{R}] < \infty$. Daher ist a auch algebraisch über $\mathbb{R}$. Sei $g \in \mathbb{R}[X]$ das Minimalpolynom von a über $\mathbb{R}$. Sei K der Zerfällungskörper von $(X^2 + 1) \cdot g$. Dann ist $K/\mathbb{R}$ eine Galoiserweiterung, da $\mathbb{R}$ vollkommen ist, und $\mathbb{C} \subseteq K$. Wir zeigen, dass $K = \mathbb{C}$ gilt und hieraus folgt $a \in \mathbb{C}$.

Behauptung: $G(K/\mathbb{R})$ ist eine 2-Gruppe. Da $[\mathbb{C} : \mathbb{R}] = 2$, gilt

$$2 | [K : \mathbb{R}] = \text{ord}(G(K/\mathbb{R})).$$

Sei H eine 2-Sylowuntergruppe von $G(K/\mathbb{R})$ und $M = K^H$. Dann ist $H = G(K/M)$ und es folgt

$$[M : \mathbb{R}] = \frac{[K : \mathbb{R}]}{[K : M]} = \frac{\text{ord}(G(K/\mathbb{R}))}{\text{ord}(G(K/M))} = \frac{\text{ord}(G(K/\mathbb{R}))}{\text{ord}(H)} = [G(K/\mathbb{R}) : H].$$

Nun ist $[G(K/\mathbb{R}) : H]$ ungerade, weil H eine 2-Sylowuntergruppe von $G(K/\mathbb{R})$ ist. Somit ist $[M : \mathbb{R}]$ ungerade.

Nach dem Satz vom primitiven Element (Kapitel 3, 5.18) existiert ein $x \in M$ mit $M = \mathbb{R}(x)$. Sei $f \in \mathbb{R}[X]$ das Minimalpolynom von x über $\mathbb{R}$. Dann ist $\deg(f) = [M : \mathbb{R}]$ ungerade, besitzt also eine Nullstelle in $\mathbb{R}$. Da f irreduzibel ist, muss $\deg(f) = 1$ gelten. Also $M = \mathbb{R}$. Daher

$$H = G(K/M) = G(K/\mathbb{R})$$

und $G(K/\mathbb{R})$ ist eine 2-Gruppe. Sei $[K:\mathbb{R}] = \mathrm{ord}(G(K/\mathbb{R})) = 2^n$ für ein $n \geq 1$. Es ist $G(K/\mathbb{C}) \subseteq G(K/\mathbb{R})$ und

$$\mathrm{ord}(G(K/\mathbb{C})) = [K:\mathbb{C}] = [K:\mathbb{R}]/[\mathbb{C}:\mathbb{R}] = 2^{n-1}.$$

Angenommen es gilt $n > 1$. Dann gibt es nach dem 1. Satz von Sylow eine Untergruppe $\Gamma \subseteq G(K/\mathbb{C})$ mit $\mathrm{ord}(\Gamma) = 2^{n-2}$. Dann folgt

$$[K^\Gamma:\mathbb{C}] = [K:\mathbb{C}]/[K:K^\Gamma] = \mathrm{ord}(G(K/\mathbb{C}))/\mathrm{ord}(\Gamma) = 2.$$

Wieder nach dem Satz vom primitiven Element existiert ein $b \in K^\Gamma$ mit $K^\Gamma = \mathbb{C}(b)$. Sei $h \in \mathbb{C}[X]$ das Minimalpolynom von b über $\mathbb{C}$. Dann ist h irreduzibel und $\deg(h) = 2$. Ist $h = X^2 + pX + q$ mit $p, q \in \mathbb{C}$, dann existieren hierfür die Nullstellen

$$-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \in \mathbb{C}.$$

Daher ist h reduzibel. Dies ist ein Widerspruch und es muss $n = 1$ gelten. Dies bedeutet $[K:\mathbb{C}] = 1$ und

$$K = \mathbb{C}.$$

□

2. Konstruktionen mit Zirkel und Lineal

Sei $M \subseteq \mathbb{C}$. In diesem Abschnitt sind wir an "Konstruktionsproblemen mit Zirkel und Lineal" interessiert. Sei

(i) $G(M)$ die Menge aller Geraden g, die zwei verschiedene Punkte $z_0, z_1 \in M$ enthalten. Wir schreiben hierfür $g = g(z_0, z_1)$. Es gilt

$$g(z_0, z_1) = \{z_0 + r(z_1 - z_0) \colon r \in \mathbb{R}\}.$$

(ii) $K(M)$ die Menge aller Kreise k mit Mittelpunkt $z_0 \in M$ und Radius $r = |z_1 - z_2|$ für zwei verschiedene Punkte $z_1, z_2 \in M$. Ein Kreis wird mit $k = k(z_0, z_1, z_2)$ bezeichnet. Es gilt

$$k(z_0, z_1, z_2) = \{z \in \mathbb{C} \colon |z - z_0| = |z_1 - z_2|\}.$$

Wir nehmen an, dass wir jede Gerade aus $G(M)$ und jeden Kreis aus $K(M)$ konstruieren können. Durch folgende *elementare Konstruktionsschritte* lassen sich neue Punkte gewinnen:

(i) Schnittpunkt zweier verschiedener Geraden aus $G(M)$.
(ii) Schnittpunkte einer Geraden aus $G(M)$ und eines Kreises aus $K(M)$.
(iii) Schnittpunkte zweier verschiedener Kreise aus $K(M)$.

Definition 2.1. Sei $M \subseteq \mathbb{C}$. Dann ist $\mathrm{Kon}(M)$ die Menge der Punkte $z \in \mathbb{C}$ mit der Eigenschaft, dass eine Kette $M = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r$ existiert, so dass $z \in M_r$ und M_i entsteht aus M_{i-1} durch Hinzunahme der Punkte, die aus M_{i-1} durch einen elementaren Konstruktionsschritt gewonnen werden. $\mathrm{Kon}(M)$ heißt die aus M durch *Zirkel und Lineal konstruierbaren Punkte*.

Im Folgenden wollen wir stets $0, 1 \in M$ annehmen.

Bemerkung 2.2. Es gilt:

(i) $\mathrm{Kon}(\mathrm{Kon}(M)) = \mathrm{Kon}(M)$.
(ii) Mit $z \in \mathrm{Kon}(M)$ ist auch $|z| \in \mathrm{Kon}(M)$, da $|z|$ der Schnittpunkt der Geraden $g(0,1)$ mit dem Kreis $k(0,0,z)$ ist. Ferner ist $\frac{z}{|z|}$ als Schnittpunkt von $g(0,z)$ und $k(0,0,1)$ konstruierbar.
(iii) Ist $g(z_0,z_1)$ eine Gerade aus $G(M)$. Dann ist die orthogonale Gerade g' durch $z \in g(z_0,z_1) \cap \mathrm{Kon}(M)$ konstruierbar. O. E. sei $z = z_0$. Die Gerade $g(z_0,z_1)$ schneidet den Kreis $k(z_0,z_0,z_1)$ in zwei Punkten z_1, z_1'. Die Kreise $k(z_1,z_1,z_1')$ und $k(z_1',z_1,z_1')$ schneiden sich in einem Punkt w. Die Gerade g' ist dann gerade $g(z_0,w)$.

Satz 2.3. Sei $M \subseteq \mathbb{C}$ mit $0,1 \in M$. Dann ist $\mathrm{Kon}(M)$ ein Zwischenkörper von $\mathbb{C}/\mathbb{Q}(M \cup \overline{M})$ mit $\overline{M} = \{\overline{z} \in M : z \in M\}$.

Beweis. Wir zeigen:

(i) $z_1, z_2 \in \mathrm{Kon}(M) \Rightarrow z_1 + z_2 \in \mathrm{Kon}(M)$.
(ii) $z \in \mathrm{Kon}(M) \Rightarrow -z \in \mathrm{Kon}(M)$.
(iii) $z_1, z_2 \in \mathrm{Kon}(M) \Rightarrow z_1 \cdot z_2 \in \mathrm{Kon}(M)$.
(iv) $z \in \mathrm{Kon}(M), z \neq 0 \Rightarrow z^{-1} \in \mathrm{Kon}(M)$.
(v) $z \in \mathrm{Kon}(M) \Rightarrow \overline{z} \in \mathrm{Kon}(M)$.

Aus (i)-(iv) folgt, dass $\mathrm{Kon}(M)$ ein Körper ist. Dieser muss $\mathbb{Q}$ enthalten: Aus $1 \in \mathrm{Kon}(M)$ folgt $n \in \mathrm{Kon}(M)$ für alle $n \in \mathbb{N}$. Dann ist aber auch $-n \in \mathrm{Kon}(M)$ und schließlich $\frac{p}{q} \in \mathrm{Kon}(M)$ für alle $p, q \in \mathbb{Z}$. Durch (v) wird bewiesen, dass $\mathbb{Q}(M \cup \overline{M}) \subseteq \mathrm{Kon}(M)$ (Die folgenden Beweise sollten man sich durch Skizzen verdeutlichen).

Zu (i): Die Kreise $k(z_1,0,z_2)$ und $k(z_2,0,z_1)$ schneiden sich in $z_1 + z_2$ (Dies entspricht der Vektoraddition). Daher ist $z_1 + z_2 \in \mathrm{Kon}(M)$.

Zu (ii): Die Gerade $g(0,z)$ und der Kreis $k(0,0,z)$ schneiden sich in $-z$. Daher ist $-z \in \mathrm{Kon}(M)$.

Zu (iii): O.E. gilt $z_1 \neq 0$ und $z_2 \neq 0$. Es ist $z_1 z_2 = z_1 \frac{z_2}{|z_2|} |z_2|$. Daher reicht es, die beiden Fälle $|z_2| = 1$ und $z_2 \in \mathbb{R}^+$ zu betrachten.

Sei $|z_2| = 1$. Die Gerade $g(0,z_1)$ und der Kreis $k(0,0,1)$ schneiden sich in dem Punkt $\frac{z_1}{|z_1|}$. Der Kreis $k(\frac{z_1}{|z_1|}, 1, z_2)$ und der Kreis $k(0,0,1)$ schneiden sich in $\frac{z_1}{|z_1|} z_2$. Schliesslich schneiden sich die Gerade $g(0, \frac{z_1}{|z_1|} z_2)$ und der Kreis $k(0,0,z_1)$ in dem Punkt $z_1 z_2$.

Sei nun $z_2 \in \mathbb{R}^+$. Wir unterscheiden wieder zwei Fälle. Der erste Fall ist $z_1 \in \mathbb{R}^+$. Mit Hilfe von 2.2 (iii) lässt sich die Figur eines Strahlensatzes konstruieren: Betrachte die Punkte $1, z_2$ auf der Geraden $g(1,z_2)$. Dann wird (die Länge) z_1 auf der senkrechten Geraden zu $g(1,z_2)$ durch 1 abgetragen und man erhält einen Punkt z_3. Als nächstes wird eine Gerade durch 0 und z_3 gezogen. Schliesslich wird eine senkrechte Gerade zu $g(1,z_2)$ durch z_2 abgetragen um einen weiteren Punkt z_4 zu erhalten. Man erhält dann direkt, dass $z_1 z_2 \in \mathrm{Kon}(M)$ gilt, da dies die Länge der Strecke zwischen z_2 und z_4 ist.

Ist z_1 beliebig, dann ist $|z_1|$ und somit nach dem bisher bewiesenen $|z_1| z_2$ konstruierbar. Aber $z_1 z_2$ ist der Schnittpunkt des Kreises $k(0,0,|z_1| z_2)$ mit der Geraden $g(0,z_1)$, also auch konstruierbar.

Zu (iv): Es ist $z^{-1} = (\frac{z}{|z|})^{-1}|z|^{-1}$. Da mit z auch $\frac{z}{|z|}$ und $|z|$ konstruierbar sind, reicht es wieder die Fälle $|z| = 1$ und $z \in \mathbb{R}^+$ zu betrachten.

Sei $|z| = 1$. Der Kreis $k(0, 0, 1)$ und der Kreis $k(1, 1, z)$ schneiden sich in z^{-1} und dies zeigt die Behauptung.

Sei $z \in \mathbb{R}^+$. Dies behandelt man wieder mit einer geeigneten Anwendung des Strahlensatzes: Betrachte die Gerade durch $1, z$. Dann wird (die Länge) 1 auf der senkrechten Gerade zu $g(1, z)$ durch den Punkt z abgetragen und eine Gerade durch 0 und dem neu konstruierten Punkt gezogen. Schliesslich wird eine senkrechte Gerade zu $g(1, z_2)$ durch 1 abgetragen um einen weiteren Punkt z' zu erhalten. Die Länge der Strecke zwischen 1 und z' ist z^{-1} und daher gilt $z^{-1} \in \mathrm{Kon}(M)$.

Zu (v): Der Kreis $k(z, 1, z)$ schneidet die Gerade $g(1, 0)$ in 1 und einem weiteren Punkt z'. Dann ist $\overline{z}$ Schnittpunkt der Kreise $k(1, 1, z)$ und $k(z', 1, z)$ (Dies ist eine Spiegelung von z an $g(1, 0)$). □

Satz 2.4. Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$. Dann sind folgende Aussagen äquivalent:

(i) $z \in \mathrm{Kon}(M)$.

(ii) Es existiert eine Körperkette $\mathbb{Q}(M \cup \overline{M}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m \subseteq \mathbb{C}$ mit $z \in L_m$ und $[L_i : L_{i-1}] = 2$ für $i = 1, \ldots, m$.

(iii) Sei L der Zerfällungskörper des Minimalpolynoms von z über $\mathbb{Q}(M \cup \overline{M})$. Dann ist $[L : \mathbb{Q}(M \cup \overline{M})]$ eine Potenz von 2.

Korollar 2.5. Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$, $z \in \mathrm{Kon}(M)$ und f das Minimalpolynom von z über $\mathbb{Q}(M \cup \overline{M})$. Dann ist $\deg(f)$ eine Potenz von 2.

Beweis. Sei L der Zerfällungskörper von f. Dann gilt $\deg(f)|[L : \mathbb{Q}(M \cup \overline{M})]$, da

$$\deg(f) = [\mathbb{Q}(M \cup \overline{M})(z) : \mathbb{Q}(M \cup \overline{M})].$$

Dies und 2.4 beweisen die Behauptung. □

Beispiele 2.6. Durch die bisherigen Ergebnisse lässt sich bereits die Unlösbarkeit einiger klassischer Konstruktionsprobleme beweisen.

(i) (Quadratur des Kreises) Die Quadratur des Kreises ist nicht möglich, d.h. es ist nicht möglich zu einem gegebenen Kreis (Mittelpunkt und Radius) ein flächengleiches Quadrat mit Zirkel und Lineal zu konstruieren: Wir nehmen an, dass der Kreis den Mittelpunkt 0 und den Radius 1 hat. Sein Flächeninhalt ist dann π. Ein flächengleiches Quadrat hat die Kantenlänge $\sqrt{\pi}$. Sei $M = \{0, 1\}$. Dann gilt $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Es ist zu entscheiden, ob $\sqrt{\pi} \in \mathrm{Kon}(M)$ gilt. Nach 2.4 ist $\mathrm{Kon}(M)/\mathbb{Q}$ algebraisch. Aber $\sqrt{\pi}$ ist transzendent über $\mathbb{Q}$. Also ist die Quadratur des Kreises nicht möglich.

(ii) (Delische Problem der Würfelverdoppelung) Es ist nicht möglich zu einem gegebenen Würfel einen Würfel mit dem doppelten Volumen mit Zirkel und Lineal zu konstruieren: Der vorgegebene Würfel besitze die Kantenlänge 1. Sei wieder $M = \{0, 1\}$. Ein Würfel mit doppelten Volumen hat die Kantenlänge $\sqrt[3]{2}$. Das Minimalpolynom von $\sqrt[3]{2}$ ist $X^3 - 2$ und hat den Grad 3. Also ist die Würfelverdoppelung nach 2.5 nicht möglich.

(iii) (Dreiteilung eines Winkels) Im Allgemeinen ist es nicht möglich einen vorgegebenen Winkel mit Zirkel und Lineal in drei gleiche Teile zu zerlegen: Ein Winkel ist durch einen Punkt $z \in \mathbb{C}$ mit $|z| = 1$ gegeben. Wir zeigen, dass es z. B. nicht möglich ist, den 60°-Winkel dreizuteilen. Sei $M = \{0, 1\}$. Der 60°-Winkel ist aus M als Schnittpunkt des Einheitskreises $k(0, 0, 1)$ und $k(1, 0, 1)$ elementar konstruierbar. Wäre der 20°-Winkel konstruierbar, so müsste der Punkt $\cos(20°) + i \sin(20°)$ in $\mathrm{Kon}(M)$ liegen. Dann gilt aber auch $c = 2\cos(20°) \in \mathrm{Kon}(M)$. Wir zeigen, dass c das Minimalpolynom $f = X^3 - 3X - 1 \in \mathbb{Q}[X]$ hat. Dies ist dann ein Widerspruch. f ist irreduzibel wegen der Reduktionsmethode nach 2 und dem Satz von Gauß. Es gilt

$$c^3 - 3c - 1 = 8\cos^3(20°) - 6\cos(20°) - 1$$

$$= 2(4\cos^3(20°) - 3\cos(20°)) - 1 = 2\cos(60°) - 1 = 0,$$

da $4\cos^3(20°) - 3\cos(20°) = \cos(3x)$ (Additionstheoreme verwenden) und $2\cos(60°) - 1 = 0$. Dies zeigt die Behauptung.

Bevor wir 2.4 beweisen, stellen wir einige Hilfsmittel zusammen.

Satz 2.7. Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$ und $z \in \mathrm{Kon}(M)$. Dann ist auch $\sqrt{z} \in \mathrm{Kon}(M)$.

Beweis. O.E. ist $z \neq 0$. Mit z ist auch $|z|$ und $\frac{z}{|z|}$ ein Element von $\mathrm{Kon}(M)$. Ferner ist $\sqrt{z} = \sqrt{\frac{z}{|z|}} \cdot \sqrt{|z|}$. Daher reicht es, die Fälle $|z| = 1$ und $z \in \mathbb{R}^+$ zu betrachten.

Sei $|z| = 1$. Dann ist $\sqrt{z} = \frac{1+z}{|1+z|}$ (ausrechnen). Diese Zahl ist konstruierbar, denn mit $z, 1 \in \mathrm{Kon}(M)$ folgt $1 + z \in \mathrm{Kon}(M)$ und schliesslich $\sqrt{z} \in \mathrm{Kon}(M)$.

Sei $z \in \mathbb{R}^+$. Es ist z oder $\frac{1}{z}$ größer oder gleich 1. Ist eine der beiden Wurzeln konstruierbar, dann auch die andere, da $\mathrm{Kon}(M)$ ein Körper ist. Also können wir o.E. annehmen, dass $z > 1$ ($z = 1$ ist trivial). Beachte, dass $\frac{z}{2} \in \mathrm{Kon}(M)$.

Der Kreis $k(\frac{z}{2}, 0, \frac{z}{2})$ schneidet die senkrechte Gerade zu der Geraden $g(0, z)$ im Punkt 1 in einem Punkt $z' = 1 + iy$. Daher $z' \in \mathrm{Kon}(M)$ und $|z'| = \sqrt{1 + y^2}$. Nun liegt z' auf dem obigen Kreis und es gilt

$$(\frac{z}{2})^2 = (1 - \frac{z}{2})^2 + y^2 = 1 - z + (\frac{z}{2})^2 + y^2.$$

Daher $z = 1 + y^2$ und $\sqrt{z} = |z'| \in \mathrm{Kon}(M)$. □

Lemma 2.8. Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$. Dann gilt $\mathbb{Q}(M \cup \overline{M}) = \overline{\mathbb{Q}(M \cup \overline{M})}$.

Beweis. Sei $L = \mathbb{Q}(M \cup \overline{M})$. Dann ist $\overline{L} = \{z \in \mathbb{C} \colon \overline{z} \in L\}$ wieder ein Körper mit $\mathbb{Q}, M, \overline{M} \subseteq \overline{L}$. Daher $L \subseteq \overline{L}$. Nun gilt $\overline{L} \subseteq \overline{\overline{L}} = L$ und somit folgt die Behauptung. □

Lemma 2.9. Sei $L \subseteq \mathbb{C}$ ein Teilkörper mit $L = \overline{L}$. Dann gilt:

(i) Der Schnittpunkt zweier verschiedener Geraden aus $G(L)$ ist in L enthalten.

(ii) Die Schnittpunkte einer Geraden aus $G(L)$ mit einem Kreis aus $K(L)$ sind in $L(\sqrt{w})$ für ein $w \in L$ enthalten.

(iii) Die Schnittpunkte zweier verschiedener Geraden aus $K(L)$ sind in $L(\sqrt{w})$ für ein $w \in L$ enthalten.

Beweis. Zu (i): Sei z Schnittpunkt zweier verschiedener Geraden. Beachte, dass mit $q, q' \in L$ auch $q - q' \in L$ gilt. Daher existieren

$$z_0 = x_0 + iy_0, \quad z_1 = x_1 + iy_1, \quad w_0 = x_0' + iy_0', \quad w_1' = x_1' + iy_1' \in L.$$

und $r, s \in \mathbb{R}$ mit

$$z = z_0 + rz_1 = z_0' + sz_1'.$$

Zerlegt man dies in Realteil und Imaginärteil, so erhält man ein lineares Gleichungssystem in r und s

$$x_0 + rx_1 = x_0' + sx_1'$$
$$iy_0 + riy_1 = iy_0' + siy_1'.$$

in dem wegen $L = \overline{L}$ die Koeffizienten $x_0, x_1, x_0', x_1', iy_0, iy_1, iy_0', iy_1'$ alle Elemente von L sind. Dieses Gleichungssystem ist lösbar, also muss die Lösung auch in L liegen.

Zu (ii): Die Gerade sei durch $\{z_0 + rz_1 : r \in \mathbb{R}\}$ mit $z_0 = x_0 + iy_0, z_1 = x_1 + iy_1 \in L$ gegeben und der Kreis durch $k(w_0, w_1, w_2)$ mit $w_0 = x_0' + iy_0', w_1, w_2 \in L$. Beachte, dass $l^2 = |w_1 - w_2|^2$ auch ein Element von L ist. Sei z ein Schnittpunkt der Geraden und des Kreises. Dann ist $z = z_0 + rz_1$ für ein $r \in \mathbb{R}$. Es gilt die Kreisbedingung

$$(rx_1 + x_0 - x_0')^2 - (r(iy_1) + (iy_0) - (iy_0'))^2 = l^2.$$

Dies ist eine lineare oder quadratische Gleichung in r und auch hier sind wieder alle Koeffizienten Elemente von L. Im ersten Fall folgt $r \in L$ und daher $z \in L$. Man kann $w = 1$ setzen. Im zweiten Fall gilt eine Gleichung der Form

$$r^2 + pr + q = 0 \text{ mit } p, q \in L.$$

Dann ist

$$r = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Mit $w = \frac{p^2}{4} - q$ folgt, dass alle Schnittpunkte der Geraden und des Kreises in $L(\sqrt{w})$ enthalten sind.

Zu (iii): Mit $z = x + iy$ und analog zur Bezeichnung in (i) und (ii) erfülle z zwei Kreisgleichungen der Form

$$(x - x_0)^2 - (iy - iy_0)^2 = r_0^2$$
$$(x - x_0')^2 - (iy - iy_0')^2 = (r_0')^2$$

mit $x_0, x_0', iy_0, iy_0', r_0^2, (r_0')^2 \in L$. Durch eine Differenzbildung erhält man

$$ax + b(iy) = c \text{ mit } a, b, c \in L \text{ und } (a, b) \neq (0, 0),$$

da dies nach Voraussetzung verschiedene Kreise sind, die sich schneiden. Die letzte Gleichung beschreibt eine Gerade aus $G(L)$ und z ist ein Schnittpunkt dieser Geraden mit den Kreisen. Aus (ii) folgt dann die Behauptung. □

Lemma 2.10. Sei L/K eine Körpererweiterung mit $[L : K] = 2$. Dann existiert ein $a \in L$ mit $a^2 \in K$ und $L = K(a)$.

Beweis. Es existiert ein $b \in L \setminus K$ mit $L = K(b)$. Ist $f \in K[X]$ das Minimalpolynom von b, so gilt $\deg(f) = 2$. Daher ist $f = X^2 + pX + q$ mit $p, q \in K$. Dann ist aber $b = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}$ oder $b = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q}$. Sei $a = \sqrt{\frac{p^2}{4} - q}$. Dann ist $K(a) = K(b)$ und $a^2 \in K$. □

Lemma 2.11. Sei L/K eine endliche Körpererweiterung mit $L = K(a_1, \ldots, a_m)$ und $\overline{L}$ der algebraische Abschluss von L. Seien $\sigma_1, \ldots, \sigma_n$ die paarweise verschiedenen K-Homomorphismen von L nach $\overline{L}$. Definiere

$$L' = K(\sigma_i(a_j) \colon i = 1, \ldots, n \text{ und } j = 1, \ldots, m).$$

Dann gilt:

(i) L'/L ist eine endliche Körpererweiterung.
(ii) L'/K ist eine normale Körpererweiterung.

Beweis. Sei $f_i \in K[X]$ das Minimalpolynom von a_i über K für $i = 1, \ldots, m$. Sei $M \subseteq \overline{L} = \overline{K}$ ein Zerfällungskörper der $f_1, \ldots, f_m$. Dann ist M/K normal und M/L endlich. Wir zeigen $M = L'$.

Es gilt $f_j^{\sigma_i} = f_j$, da σ_i ein K-Homomorphismus ist. Ferner ist $\sigma_i(a_j)$ wieder eine Nullstelle von f_j. Daher gilt $L' \subseteq M$.

Ist nun $a \in M$ eine Nullstelle von einem f_j. Dann können wir einen K-Homomorphismus $\sigma : L \longrightarrow L'$ finden mit $\sigma'(a_j) = a$ (siehe Kapitel 3, 3.4). σ induziert eine Abbildung von L nach $\overline{L}$ und es gilt $a \in L'$. Insgesamt folgt $L' = M$. □

Beweis. (von 2.4) (i) $\Rightarrow$ (ii): Sei $z \in \mathrm{Kon}(M)$. Dann existiert eine Kette

$$M = M_0 \subseteq \cdots \subseteq M_m$$

von Teilmengen von $\mathbb{C}$ und M_i entsteht aus M_{i-1} durch Hinzunahme der Elemente, die aus einem elementaren Konstruktionsschritt gewonnen werden können. Wir beweisen durch eine Induktion nach i, dass eine Körperkette

$$L_0 = \mathbb{Q}(M_i \cup \overline{M_i}) \subseteq L_1 \subseteq \cdots \subseteq L_{2i+1} \subseteq L_{2i+2}$$

existiert mit $[L_{2j+2} : L_{2j+1}] \leq 2$, $[L_{2j+1} : L_{2j}] \leq 2$ und $L_{2j+2} = \overline{L_{2j+2}}$ für $j = 0, \ldots, i$, so dass $M_i \subseteq L_{2i+2}$ gilt. Sei nun die Aussage für $i - 1$ bewiesen. Sind z_0 und z_1 diejenigen Elemente mit $M_i = M_{i-1} \cup \{z_0, z_1\}$ (im Falle eines Elements einfach $z_0 = z_1$ setzen), so folgt aus 2.9, dass immer ein $w \in L_{2i}$ existiert mit $z_0, z_1 \in L_{2i}(\sqrt{w})$. Beachte, dass auch $\overline{w} \in \overline{L_{2i}} = L_{2i}$. Definiere $L_{2i+1} = L_{2i}(\sqrt{w})$ und $L_{2i+2} = L_{2i}(\sqrt{w}, \sqrt{\overline{w}})$. Dann gilt

$$[L_{2i+2} : L_{2i+1}] \leq 2, \quad [L_{2i+2} : L_{2i+1}] \leq 2, \quad \overline{L_{2i+2}} = L_{2i+2}.$$

Ferner $M_i \subseteq L_{2i+2}$. Für $i = m$ erhält man schliesslich (ii), wenn man noch diejenigen L_j mit $L_j = L_{j-1}$ entfernt.

(ii) $\Rightarrow$ (iii): Sei

$$\mathbb{Q}(M \cup \overline{M}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m \subseteq \mathbb{C}$$

die Körperkette mit $z \in L_m$ und $[L_i : L_{i-1}] = 2$ für $i = 2, \ldots, m$. Nach 2.10 existieren Elemente $a_i \in L_i$ mit $L_i = L_{i-1}(a_i)$ und $a_i^2 \in L_{i-1}$. Also entsteht $L_m = L_0(a_1, \ldots, a_m)$ durch sukzessive Adjunktion von Quadratwurzeln aus L_0.

Konstruiere zu der endlichen Körpererweiterung L_m/L_0 die Erweiterung L'/L_m aus 2.11. Sind $\sigma_1, \dots, \sigma_n$ die paarweise verschiedenen K-Homomorphismen von L_m nach $\overline{L_m} \subseteq \mathbb{C}$. Dann ist $L' = L_0(\sigma_i(a_j)\colon i = 1, \dots, n \text{ und } j = 1, \dots, m)$. Definiere $M_{0,m} = L_0$ und

$$M_{k,l} = L_0(\sigma_i(a_j)\colon 1 \leq i \leq k \text{ und } 1 \leq j \leq l)$$

für $k = 1, \dots, n$ und $l = 1, \dots, m$. Für $l > 1$ ist $M_{k,l} = M_{k,l-1}(\sigma_k(a_l))$ mit $\sigma_k(a_l)^2 \in M_{k,l-1}$. Ausserdem ist $M_{k,1} = M_{k-1,m}(\sigma_k(a_1))$ mit $\sigma_k(a_1)^2 \in M_{k-1,m}$. Daher

$$[M_{k,l} : M_{k,l-1}] = 2 \text{ und } [M_{k,1} : M_{k-1,m}] = 2$$

für die entsprechenden k, l. Dann ist

$$[L' : L_0] = \prod_{k=1}^{n} \prod_{l=2}^{m} [M_{k,l} : M_{k,l-1}] \cdot \prod_{k=1}^{n} [M_{k,1} : M_{k-1,m}]$$

eine Potenz von 2. Beachte, dass L'/L_0 normal und daher eine Galoiserweiterung ist.

Ist nun L der Zerfällungskörper des Minimalpolynoms von $z \in L_m \subseteq L'$, dann gilt $L \subseteq L'$, da L'/L_0 normal. Da $[L : L_0] | [L' : L_0]$, ist auch $[L : L_0]$ eine Potenz von 2 und dies war zu zeigen.

(iii) $\Rightarrow$ (i): Die Körpererweiterung $L/\mathbb{Q}(M \cup \overline{M})$ ist eine Galoiserweiterung und die Galoisgruppe $G = G(L/\mathbb{Q}(M \cup \overline{M}))$ hat als Ordnung eine Potenz von 2. Daher ist G eine 2-Gruppe und auflösbar. Nach Kapitel 4, 3.16 lässt sich eine Kette von Normalteilern

$$G = G_0 \supseteq \cdots \supseteq G_n = \{e\}$$

finden mit $G_i/G_{i+1} \cong \mathbb{Z}/2\mathbb{Z}$ zyklisch. Sei $K_i = L^{G_i}$. Dann entspricht die Normalreihe einer Kette von Zwischenkörpern

$$L = K_n \supseteq \cdots \supseteq K_0 = \mathbb{Q}(M \cup \overline{M})$$

mit

$$[K_i : K_{i-1}] = \frac{[L : K_{i-1}]}{[L : K_i]} = \frac{\operatorname{ord}(G(L/K_{i-1}))}{\operatorname{ord}(G(L/K_i))} = \frac{\operatorname{ord}(G_{i-1})}{\operatorname{ord}(G_i)} = 2.$$

Nach 2.10 ist $K_i = K_{i-1}(a_i)$ mit $a_i^2 \in K_{i-1}$. Wir zeigen per Induktion nach i, dass $K_i \subseteq \operatorname{Kon}(M)$ gilt. Für $i = 0$ ist dies trivial, also sei $i > 0$. Da $a_i^2 \in K_{i-1} \subseteq \operatorname{Kon}(M)$. ist nach 2.7 auch $a_i \in \operatorname{Kon}(M)$. Dann ist aber $K_i = K_{i-1}(a_i) \subseteq \operatorname{Kon}(M)$.

Somit ist $z \in K_n \subseteq \operatorname{Kon}(M)$. □

3. Einheitswurzeln

In diesem Abschnitt fixieren wir einen Körper K sowie einen algebraischen Abschluss $\overline{K}$ von K.

Definition 3.1. Sei $n \in \mathbb{N} \setminus \{0\}$. Ein Element $\zeta \in K$ heißt *n-te Einheitswurzel*, wenn ζ Nullstelle des Polynoms $X^n - 1 \in K[X]$ ist. $E_n(K)$ sei die Menge der n-ten Einheitswurzeln und K_n der Zerfällungskörper von $X^n - 1$.

Bemerkung 3.2. Beachte:

(i) Gilt $\operatorname{char}(K) \nmid n$, dann ist dass Polynom $X^n - 1$ separabel.

(ii) $E_n(K) \subseteq K^*$ ist eine Gruppe, da mit $a, b \in E_n(K)$ auch $ab^{-1} \in E_n(K)$ gilt.

Satz 3.3. Sei $n \in \mathbb{N} \setminus \{0\}$ und $\mathrm{char}(K) \nmid n$. Dann gilt:

(i) K_n/K ist eine Galoiserweiterung.
(ii) $E_n(K_n)$ ist zyklisch von der Ordnung n.

Beweis. Zu (i): Siehe Kapitel 3, 5.9.
Zu (ii): Siehe Kapitel 3, 5.17. □

Definition 3.4. Ein Element $\zeta \in E_n(K_n)$ heißt *primitive n-te Einheitswurzel*, wenn $E_n(K_n) = \langle \zeta \rangle = \{1, \ldots, \zeta^{n-1}\}$.

Beispiel 3.5. Sei $K = \mathbb{C}$ und $n = 4$. Dann ist $E_4 = \{\pm 1, \pm i\}$ und $\pm i$ sind die primitiven 4-ten Einheitswurzeln.

Definition 3.6. Sei $n \in \mathbb{N} \setminus \{0\}$. Die Abbildung

$$\varphi \colon \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}, \quad n \mapsto \varphi(n) = \mathrm{ord}((Z/n\mathbb{Z})^*)$$

heißt die Eulersche φ-Funktion. Hierbei ist $(Z/n\mathbb{Z})^*$ die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$.

Bemerkung 3.7. Es gilt

$$(Z/n\mathbb{Z})^* = \{a + n\mathbb{Z} \in Z/n\mathbb{Z} \colon \mathrm{ggT}(a, n) = 1\}$$

und daher

$$\varphi(n) = |\{a \in \{0, \ldots, n-1\} \colon \mathrm{ggT}(a, n) = 1\}|.$$

Lemma 3.8. Es gilt:

(i) Für teilerfremde Zahlen $m, n \in \mathbb{N}$ ist $\varphi(mn) = \varphi(m)\varphi(n)$.
(ii) Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{i=1}^{r} p_i^{s_i}$ und $s_i \geq 1$. Dann ist $\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{s_i - 1}$.

Beweis. Zu (i): Nach dem Chinesischen Restsatz existiert ein Ringisomorphismus

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Dieser induziert dann einen Isomorphismus

$$(\mathbb{Z}/mn\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*.$$

Dies beweist (i).

Zu (ii): Sei p eine Primzahl und $s \geq 1$. Die Elemente $a \in \mathbb{N}$ mit $0 \leq a < p^s$ und $\mathrm{ggT}(a, p) \neq 1$ sind von der Form

$$0 \cdot p, 1 \cdot p, \ldots, (p^{s-1} - 1)p.$$

Daher ist $\varphi(p^s) = p^s - p^{s-1} = (p-1)p^{s-1}$. Dies und (i) zeigen (ii). □

Satz 3.9. Sei $n \in \mathbb{N}$. Ein Element $\overline{a} = a + \mathbb{Z}$ erzeugt die additive zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ genau dann, wenn $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Ist $n \neq 0$, so enthält $\mathbb{Z}/n\mathbb{Z}$ genau $\varphi(n)$ Elemente, die $\mathbb{Z}/n\mathbb{Z}$ als zyklische Gruppe erzeugen.

Beweis. Ein Element $\overline{a}$ erzeugt $\mathbb{Z}/n\mathbb{Z}$ genau dann, wenn $\overline{1} \in \langle \overline{a} \rangle$. Dies ist genau dann der Fall, wenn ein $r \in \mathbb{Z}$ existiert mit $\overline{1} = r\overline{a} = \overline{ra}$. Letzteres ist äquivalent zu $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. □

Korollar 3.10. Sei $n \in \mathbb{N} \setminus \{0\}$ mit $\mathrm{char}(K) \nmid n$. Dann gilt:

(i) K_n enthält genau $\varphi(n)$ primitive n-te Einheitswurzeln.

(ii) Sei $\zeta \in E_n(K_n)$ eine primitive Einheitswurzel. Dann ist ζ^r für ein $r \in \mathbb{Z}$ genau dann eine primitive n-te Einheitswurzel, wenn $r + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$, d.h. $\mathrm{ggT}(r, n) = 1$.

Beweis. Zu (i): Nach 3.3 ist $E_n(K_n) \cong \mathbb{Z}/n\mathbb{Z}$. Die Behauptung folgt dann aus 3.9.

Zu (ii): Ist $\zeta \in E_n(K_n)$ eine primitive Einheitswurzel, dann existiert der Isomorphismus

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow E_n(K_n), \quad \overline{r} \mapsto \zeta^r.$$

Nun ist ζ^r genau dann eine primitive n-te Einheitswurzel, wenn $\overline{r} \in (\mathbb{Z}/n\mathbb{Z})^*$, also $\mathrm{ggT}(r, n) = 1$. □

Satz 3.11. Sei $n \in \mathbb{N} \setminus \{0\}$ mit $\mathrm{char}(K) \nmid n$. Dann gilt:

(i) Es gibt einen injektiven Gruppenhomomorphismus

$$G(K_n/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*.$$

(ii) K_n/K ist eine (abelsche) Galoiserweiterung mit $[K_n : K] | \varphi(n)$.

Beweis. Zu (i): Sei $\zeta \in K_n$ eine n-te primitive Einheitswurzel. Ist $\sigma \in G(K_n/K)$, dann gilt $\sigma(\zeta) = \zeta^m$ für ein $1 \leq m \leq n$, da $\sigma(\zeta)$ wieder eine Einheitswurzel und ζ primitiv ist. Da $\sigma\colon E_n(K_n) \longrightarrow E_n(K_n)$ ein Automorphismus ist, folgt dass $\sigma(\zeta)$ eine primitive n-te Einheitswurzel ist, d.h. $\mathrm{ggT}(m, n) = 1$. Wir können daher folgende Abbildung definieren

$$\alpha\colon G(K_n/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*, \quad \sigma \mapsto m + n\mathbb{Z}$$

wobei m durch $\sigma(\zeta) = \zeta^m$ gegeben wird (α ist wohldefiniert, da ζ die Gruppe $E_n(K_n) \cong \mathbb{Z}/n\mathbb{Z}$ erzeugt). α ist trivialerweise ein Gruppenhomomorphismus. Angenommen $\alpha(\sigma) = 1 + n\mathbb{Z}$, d.h. $\sigma(\zeta) = \zeta$. Dann ist $\sigma = \mathrm{id}$, da $K_n = K(\zeta)$.

Zu (ii): K_n/K ist eine Galoiserweiterung (wegen (i) ist diese abelsch). Ferner gilt $[K_n : K] = \mathrm{ord}(G(K_n/K)) | \mathrm{ord}(\mathbb{Z}/n\mathbb{Z})^*$ und $\mathrm{ord}(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$. □

Satz 3.12. Sei $n \in \mathbb{N} \setminus \{0\}$. Dann gilt $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$.

Beweis. Aus 3.11 folgt direkt $[\mathbb{Q}_n : \mathbb{Q}] \leq \varphi(n)$.

Sei nun $\zeta \in \mathbb{Q}_n$ eine n-te primitive Einheitswurzel und f das Minimalpolynom von ζ über $\mathbb{Q}$. Da $\mathbb{Q}_n = \mathbb{Q}(\zeta)$, gilt $\deg(f) = [\mathbb{Q}_n : \mathbb{Q}]$.

Behauptung 1: Alle primitiven Einheitswurzeln sind Nullstellen von f. Dann folgt $[\mathbb{Q}_n : \mathbb{Q}] \geq \varphi(n)$ und somit der Satz.

Sei $\eta \in \mathbb{Q}_n$ eine beliebige n-te primitive Einheitswurzel. Dann folgt $\eta = \zeta^m$ mit $\mathrm{ggT}(m, n) = 1$.

Behauptung 2: Sei ξ eine Einheitswurzel mit $f(\xi) = 0$ und p eine Primzahl mit $p \nmid n$. Dann ist $f(\xi^p) = 0$. Hieraus folgt die 1. Behauptung, denn ist $m = p_1 \cdots p_l$ mit Primfaktoren $p_i \nmid n$, dann kann die 2. Behauptung induktiv angewendet werden.

Angenommen die 2. Behauptung wäre falsch. Dann ist $f(\xi^p) \neq 0$. Es ist $X^n - 1 = f(X) \cdot h(X)$ mit $h(X) \in \mathbb{Q}[X]$. Da f normiert ist, ist auch h normiert und nach dem

Lemma von Gauß gilt $f(X), h(X) \in \mathbb{Z}[X]$. Aus

$$0 = (\xi^p)^n - 1 = f(\xi^p)h(\xi^p)$$

folgt nun $h(\xi^p) = 0$. Dann ist aber ξ eine Nullstelle von $h(X^p)$. Da f das Minimalpolynom von ξ war, ist dann $h(X^p) = f(X) \cdot g(X)$ mit $g(X) \in \mathbb{Z}[X]$. Wir betrachten die Reduktion modulo p. Hierbei sei für ein $r(X) \in \mathbb{Z}[X]$ das Element $\overline{r(X)} \in \mathbb{Z}/p\mathbb{Z}[X]$ die entsprechende Restklassen. Dann folgt

$$\overline{f(X)g(X)} = \overline{h(X^p)} = \overline{h(X)}^p.$$

Dann haben aber $\overline{f(X)}$ und $\overline{h(X)}$ einen gemeinsamen Faktor. Dies ist ein Widerspruch, da

$$X^n - 1 = \overline{f(X)h(X)}$$

separabel über $\mathbb{Z}/p\mathbb{Z}$ ist. □

Korollar 3.13. Sei $n \in \mathbb{N} \setminus \{0\}$. Dann ist $\mathbb{Q}_n/\mathbb{Q}$ eine (abelsche) Galoiserweiterung mit Galoisgruppe $G(\mathbb{Q}_n/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$.

Beweis. Dies folgt aus 3.11 und 3.12. □

Definition 3.14. Sei K ein Körper, $n \in \mathbb{N} \setminus \{0\}$ mit $\mathrm{char}(K) \nmid n$ und $\zeta_1, \ldots, \zeta_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln in K_n. Das Polynom

$$f_n = (X - \zeta_1) \cdots (X - \zeta_{\varphi_{(n)}})$$

heißt das *n-te Kreisteilungspolynom* (über K).

Satz 3.15. Sei $n \in \mathbb{N} \setminus \{0\}$. Dann gilt:

(i) $\deg(f_n) = \varphi(n)$.
(ii) $X^n - 1 = \prod_{d|n} f_d$
(iii) Die Koeffizienten von f_n sind von der Gestalt $z \cdot 1$ für $z \in \mathbb{Z}$, d.h. sie liegen im Primring von K.

Beweis. Zu (i): Dies folgt direkt aus der Definition von f_n.

Zu (ii): Sei $P_d = \{\zeta \in E_n(K_n) \colon \mathrm{ord}(\zeta) = d\}$ für alle $d \in \mathbb{N}$ mit $d|n$. Dann ist $E_n(K_n)$ die disjunkte Vereinigung der P_d und es folgt

$$X^n - 1 = \prod_{\zeta \in E_n(K_n)} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in P_d} (X - \zeta) = \prod_{d|n} f_d.$$

Zu (iii): Sei P der Primring von K. Wir beweisen die Aussage durch eine Induktion nach n. Der Fall $n = 1$ ist trivial, also sei $n > 1$. Dann ist

$$X^n - 1 = f_n \prod_{d|n, d \neq n} f_d.$$

Sei $g = \prod_{d|n, d \neq n} f_d$. Dann ist nach der Induktionsannahme $g \in P[X]$. Teile $X^n - 1$ durch g mit Rest in $P[X]$, also

$$X^n - 1 = qg + r$$

mit $q, r \in P[X]$ und $\deg(r) < \deg(g)$. In $K_n[X]$ gilt dann

$$r = X^n - 1 - qg = f_n g - qg = (f_n - q)g.$$

Wegen $\deg(r) < \deg(g)$ ist $r = 0$ und somit $f_n = q \in P[X]$. □

Beispiel 3.16. Sei p eine Primzahl. Dann gilt

$$X^p - 1 = (X-1)(X^{p-1} + \cdots + X + 1).$$

Hierbei ist $f_1 = X - 1$ und $f_p = X^{p-1} + \cdots + X + 1$. Ferner ist

$$G(\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$

Bemerkung 3.17. Der Satz gibt eine Möglichkeit f_n induktiv zu berechnen, da

$$f_n = \frac{X^n - 1}{\prod_{d|n, d\neq n} f_d}.$$

Zum Beispiel ist $f_1 = X - 1$ und $f_3 = X^2 + X + 1$. Dann folgt

$$f_9 = \frac{X^9 - 1}{(X-1)(X^2+X+1)} = \frac{X^8 + \cdots + X + 1}{X^2 + X + 1} = X^6 + X^3 + 1.$$

4. Auflösbarkeit algebraischer Gleichungen

Zur Vereinfachung sei in diesem Abschnitt K stets ein Körper mit $\mathrm{char}(K) = 0$. Dieser Abschnitt skizziert das Problem der Auflösbarkeit algebraischer Gleichungen.

Bemerkung 4.1. Eine Gleichung der Form

$$X^d + a_{d-1}X^{d-1} + \cdots + a_0 = 0$$

mit $a_i \in K$ heißt eine algebraische Gleichung vom Grad d. Für algebraische Gleichungen vom Grad 2 sind Formeln zur Auflösung leicht herzuleiten. Auch für Gleichungen vom Grad 3 und 4 ist dies noch möglich (Stichwort: Cardanosche Formeln). Für Gleichungen vom Grad ≥ 5 ist dies i.a. nicht mehr möglich, wie wir sehen werden.

Definition 4.2. Eine endliche Körpererweiterung L/K heißt durch *Radikale auflösbar* (Radikalerweiterung), wenn es zu L einen Erweiterungskörper E sowie eine Kette

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_m = E$$

gibt, so dass $E_{i+1} = E_i(a_i)$, wobei a_i Nullstelle eines Polynoms der Form $X^{n_i} - b_i \in E_i[X]$ für $n_i \in \mathbb{N}$ und $b_i \in E_i$ ist.

Bemerkung 4.3. Beachte, dass E/K separabel ist, da E_{i+1}/E_i separabel für $i = 0, \ldots, m-1$. Dann ist auch L/K separabel.

Sei eine Radikalerweiterung vorgegeben. Dann lässt $a \in E_m$ sich darstellen als $a = \sum_j c_j(\sqrt[n_m]{b_m})^j$ mit $c_j \in E_{m-1}$. Jedes c_j besitzt eine analoge Darstellung bzgl. b_{m-1}, usw. Die Elemente lassen sich also jeweils durch die Operationen $+, -, \cdot, /, \sqrt{}$ gewinnen. Z. B. $\sqrt[3]{1 - \sqrt[2]{5}}$.

Definition 4.4. Eine endliche Körpererweiterung heißt *auflösbar*, wenn eine Körpererweiterung $E \supseteq L$ existiert, so dass E/K eine endliche Galoiserweiterung mit auflösbarer (im Sinne von Kapitel 4, 5.1) Galoisgruppe ist.

Bemerkung 4.5. Eine endliche Galoiserweiterung L/K ist genau dann auflösbar, wenn die Galoisgruppe $G(L/K)$ auflösbar ist. Kann man L/K zu einer endlichen Galoiserweiterung E/K mit auflösbarer Galoisgruppe vergrößern, so ist $G(L/K) = G(E/K)/G(E/L)$ also Quotient einer auflösbaren Gruppe auflösbar.

Man kann nun zeigen, dass die beiden Auflösbarkeitkeitsbegriffe wie folgt zusammenhängen.

Satz 4.6. Eine endliche Körpererweiterung ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.

Definition 4.7. Sei $f \in K[X]$ mit $\deg(f) > 0$ und L ein Zerfällungskörper von f. Dann heißt f *auflösbar* bzw. durch *Radikale auflösbar*, wenn L/K auflösbar bzw. durch Radikale aufösbar ist.

Korollar 4.8. Sei $f \in K[X]$ mit $\deg(f) > 0$ und L ein Zerfällungskörper von f. Dann sind äquivalent:

(i) f ist durch Radikale auflösbar,
(ii) $G(L/K)$ ist auflösbar.

Korollar 4.9. Es gilt:

(i) Alle nicht konstanten Polynome vom Grad ≤ 4 sind durch Radikale auflösbar.
(ii) Polynome vom Grad ≥ 5 sind im Allgemeinen nicht durch Radikale auflösbar.

Beweis. Zu (i): Sei $f \in K[X]$ mit $n = \deg(f) > 0$ und L ein Zerfällungskörper von f. Die Galoisgruppe $G(L/K)$ von f kann als Untergruppe von S_n aufgefasst werden.

S_n ist genau dann auflösbar, wenn $n \leq 4$ (Kapitel 4, 5.12). Ist nun $n \leq 4$, dann folgt, dass $G(L/K)$ als Untergruppe ebenfalls auflösbar ist. Daher ist in diesem Falle L/K durch Radikale auflösbar. Dies zeigt (i).

Zu (ii). Zum Beispiel kann gezeigt werden, dass für $f = X^5 - 4X + 2$ gilt $G(L/K) \cong S_5$. Daher ist $G(L/K)$ nicht auflösbar. □

Literaturverzeichnis

[1] M. Artin, Algebra, Birkhäuser, Basel, 1993.
[2] S. Bosch, Algebra, Springer, Berlin, 2001.
[3] E. Kunz, Algebra, Vieweg, Braunschweig Wiesbaden, 1994.
[4] G. Scheja und U. Storch, Lehrbuch der Algebra 1 und 2, Teubner, Stuttgart, 1980.
[5] B. L. van der Waerden, Algebra I und II, Springer, Berlin, 1967.