Algebra

Helmut Schwichtenberg

Mathematisches Institut der Universität München
Wintersemester 1998/99

Inhaltsverzeichnis

Vorwort

Dieses Skriptum gibt den Inhalt einer Vorlesung über Algebra wieder, die ich im Wintersemester 1980/81 und dann noch einmal im Wintersemester 1998/99 am Mathematischen Institut der Universität München gehalten habe. Ziel dieser Vorlesung war es, die Galois-Theorie und ihre wichtigsten klassischen Anwendungen darzustellen. Die Vorlesung von 1980/81 wurde von Herrn Jürgen Werner ausgearbeitet, dem ich auch an dieser Stelle noch einmal danken möchte. Das vorliegende Skriptum ist eine Überarbeitung der damaligen Ausarbeitung.

Bei der Vorbereitung habe ich neben Vorlesungen über Algebra und lineare Algebra, die ich in Berlin bei Professor Grotemeyer gehört habe, hauptsächlich die Lehrbücher von Kunz (Algebra, Braunschweig 2-te Auflage 1994), Artin (Galoissche Theorie, Zürich 1965), Fischer/Sacher (Einführung in die Algebra, Stuttgart 1978), Jacobson (Basic Algebra I, San Francisco 1974) und Lang (Algebra, Reading 1965) verwendet.

Bedanken möchte ich mich bei Thomas Rudlof für seine Unterstützung bei der Vorbereitung der Vorlesung und der zugehörigen Übungen. Für die gute Zusammenarbeit und viele hilfreiche Anmerkungen bedanke ich mich bei den Übungsgruppenleitern und Korrektoren Mathias Flurl, Stefanie Kuntze, Sebastian Petersen und Christian Wittmann.

München, im Februar 1999
Helmut Schwichtenberg

Kapitel 1

Gruppen

1.1 Grundbegriffe

Definition 1.1.1. Sei G eine Menge und $\circ\colon G \times G \to G$ eine Abbildung. G (oder genauer $(G, \circ)$) heißt *Gruppe*, wenn gilt

1. $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$ für alle $\alpha, \beta, \gamma \in G$ (*Assoziativgesetz*).
2. Es gibt ein $e \in G$ (*neutrales Element* von G) mit folgenden Eigenschaften
   a. $e \circ \alpha = \alpha$ für alle $\alpha \in G$.
   b. Zu jedem $\alpha \in G$ gibt es ein $\alpha' \in G$ mit $\alpha' \circ \alpha = e$ (α' heißt *inverses Element* zu α).

G heißt *abelsch*, wenn außerdem noch gilt $\alpha \circ \beta = \beta \circ \alpha$ für alle $\alpha, \beta \in G$ (*Kommutativgesetz*).

Bemerkung. Sei G eine Gruppe.

1. Sei $e \in G$ neutrales Element und $\alpha, \alpha' \in G$ so daß $\alpha' \circ \alpha = e$. Dann gilt auch $\alpha \circ \alpha' = e$.
2. Sei $e \in G$ neutrales Element. Dann gilt $\alpha \circ e = \alpha$ für alle $\alpha \in G$.
3. Es gibt genau ein neutrales Element $e \in G$.
4. Zu jedem $\alpha \in G$ gibt es genau ein inverses Element $\alpha' \in G$, bezeichnet mit α^{-1}.

Beweis. 1. Wähle α'' mit $\alpha'' \circ \alpha' = e$. Dann gilt

$$\alpha \circ \alpha' = e \circ \alpha \circ \alpha' = \alpha'' \circ \alpha' \circ \alpha \circ \alpha' = \alpha'' \circ \alpha' = e.$$

2. $\alpha \circ e = \alpha \circ \alpha' \circ \alpha = e \circ \alpha = \alpha$.
3. Seien e, e^* neutrale Elemente von G. Dann gilt

$$e^* = e \circ e^* = e.$$

4. Seien α', α^* inverse Elemente zu $\alpha \in G$. Dann gilt

$$\alpha^* = \alpha^* \circ e = \alpha^* \circ \alpha \circ \alpha' = e \circ \alpha = \alpha'. \qquad \square$$

Lemma 1.1.2. *Sei G eine nicht leere Menge und $\circ\colon G\times G \to G$ eine Abbildung. G ist eine Gruppe genau dann, wenn gilt*

1. $(\alpha\circ\beta)\circ\gamma = \alpha\circ(\beta\circ\gamma)$ *für alle* $\alpha,\beta,\gamma\in G$.

2*. a. $\forall\alpha,\beta{\in}G\,\exists\gamma{\in}G\;\alpha\circ\gamma=\beta$.

   b. $\forall\alpha,\beta{\in}G\,\exists\delta{\in}G\;\delta\circ\alpha=\beta$.

Beweis. $\Longrightarrow$. Sei G eine Gruppe. Zu zeigen ist (2*). a. Setze $\gamma = \alpha^{-1}\circ\beta$. b. Setze $\delta = \beta\circ\alpha^{-1}$.

$\Longleftarrow$. G erfülle (1) und (2*). Zu zeigen ist (2). Wähle $\alpha_0\in G$ fest (hier wird benötigt, daß G nicht leer ist). Wähle e so, daß $e\circ\alpha_0=\alpha_0$ ist. a. Sei $\alpha\in G$ beliebig. Wähle $\gamma\in G$ mit $\alpha_0\circ\gamma=\alpha$. Dann gilt

$$e\circ\alpha = e\circ\alpha_0\circ\gamma = \alpha_0\circ\gamma=\alpha.$$

Teil (b) folgt aus (2*b). □

Bemerkung. Sei G eine Gruppe und $\alpha,\beta\in G$. Dann gilt

$$(\alpha^{-1})^{-1} = \alpha, \tag{1.1}$$

$$(\alpha\circ\beta)^{-1} = \beta^{-1}\circ\alpha^{-1}. \tag{1.2}$$

Beweis. (1.1). Es gilt $(\alpha^{-1})^{-1}\circ\alpha^{-1}=e$ und auch $\alpha\circ\alpha^{-1}=e$. Die Behauptung folgt aus der Eindeutigkeit des Inversen.

(1.2). $\beta^{-1}\circ\alpha^{-1}\circ\alpha\circ\beta = \beta^{-1}\circ e\circ\beta = e$. □

Beispiele. 1. $(\mathbb{Z},+)$ ist abelsche Gruppe. Das neutrale Element ist 0, und das inverse Element zu $n\in\mathbb{Z}$ ist $-n$. Ebenso sind $(\mathbb{Q},+)$ und $(\mathbb{R},+)$ abelsche Gruppen. Man beachte aber, daß $(\mathbb{N},+)$ *keine* Gruppe ist.

2. $(\mathbb{Q}^*,\cdot)$ mit $\mathbb{Q}^* := \mathbb{Q}\setminus\{0\}$ ist abelsche Gruppe. Das neutrale Element ist 1, und das inverse Element zu $\alpha\in\mathbb{Q}^*$ ist $\frac{1}{\alpha}$. Ebenso sind $(\mathbb{R}^*,\cdot)$ mit $\mathbb{R}^* := \mathbb{R}\setminus\{0\}$, $(\mathbb{Q}^*_+,\cdot)$ mit $\mathbb{Q}^*_+ := \{\,\alpha\in\mathbb{Q}\mid\alpha>0\,\}$ und $(\mathbb{R}^*_+,\cdot)$ mit $\mathbb{R}^*_+ := \{\,\alpha\in\mathbb{R}\mid\alpha>0\,\}$ abelsche Gruppe. Man beachte aber, daß $(\mathbb{Z}\setminus\{0\},\cdot)$ *keine* Gruppe ist, und ebenso $(\mathbb{N},\cdot)$ *keine* Gruppe ist.

3. Sei M eine Menge und $S(M)$ die Menge der bijektiven Abbildungen von M auf sich selbst. Dann ist $(S(M),\circ)$, wobei $\circ$ für die Verknüpfung von Abbildungen steht, eine Gruppe, die *symmetrische Gruppe* der Menge M. Man beachte, daß $S(M)$ i.a. nicht kommutativ ist. Im Spezialfall $M=\{1,\dots,n\}$ schreibt man S_n statt $S(M)$. Jede Abbildung $\sigma\in S_n$ heißt *Permutation* der Zahlen $1,\dots,n$.

Definition 1.1.3. Sei G eine Gruppe und $U\subseteq G$ eine Teilmenge von G. U heißt *Untergruppe* von G, wenn gilt

1. $xy\in U$ für alle $x,y\in U$,
2. $e\in U$,
3. $x^{-1}\in U$ für alle $x\in U$.

Bemerkung. U ist also genau dann eine Untergruppe von G, wenn die Gruppenstruktur auf G eine Gruppenstruktur auf U induziert.

Satz 1.1.4. *(Untergruppenkriterium). Sei G eine Gruppe und $U \subseteq G$ eine Teilmenge von G.*

1. *Dann ist U Untergruppe von G genau dann, wenn*
   a. *$U \neq \emptyset$,*
   b. *$xy^{-1} \in U$ für alle $x, y \in U$.*
2. *Sei U eine endliche Menge. Dann ist U Untergruppe von G genau dann, wenn*
   a. *$U \neq \emptyset$,*
   b. *$xy \in U$ für alle $x, y \in U$.*

Beweis. 1. $\Longrightarrow$. Dies folgt sofort aus der Definition 1.1.3. $\Longleftarrow$. Da $U \neq \emptyset$, existiert ein $x_0 \in U$. Damit gilt auch $e = x_0 x_0^{-1} \in U$, also (2). Sei $x \in U$. Dann ist auch $x^{-1} = ex^{-1} \in U$, woraus (3) folgt. Seien $x, y \in U$. Dann ist auch $y^{-1} \in U$ und damit gilt $xy = x(y^{-1})^{-1} \in U$, also (1).

2. $\Longrightarrow$. Dies folgt wieder sofort aus 1.1.3. $\Longleftarrow$. Sei $x \in U$. Betrachte die Abbildung

$$\hat{x} \colon U \longrightarrow U \text{ mit } \hat{x}(y) := xy.$$

Diese Abbildung ist wohldefiniert nach Bedingung (b). $\hat{x}$ ist injektiv, denn

$$\begin{aligned} \hat{x}(y) &= \hat{x}(z) \\ xy &= xz \\ x^{-1}xy &= x^{-1}xz \\ y &= z. \end{aligned}$$

Da U endlich ist, ist $\hat{x}$ damit schon bijektiv. Sei nun $x \in U$ beliebig, aber fest (die Existenz ist klar, da $U \neq \emptyset$). Da $\hat{x}$ bijektiv ist, existiert $y \in U$ mit $\hat{x}(y) = x$. Dann gilt $xy = x$ und somit $y = e$, also $e \in U$. Außerdem existiert $z \in U$ mit $\hat{x}(z) = e$; dann gilt $xz = e$ und damit $z = x^{-1}$, also $x^{-1} \in U$. Da $x \in U$ beliebig gewählt war, folgt die Behauptung. □

Definition 1.1.5. Seien G, H Gruppen und $f \colon G \to H$ eine Abbildung.

1. f heißt *Homomorphismus* für Gruppen, wenn für alle $x, y \in G$ gilt
$$f(xy) = f(x)f(y).$$
2. f heißt *Mono-, Epi- bzw. Isomorphismus* , wenn f Homomorphismus und injektiv, surjektiv bzw. bijektiv ist.
3. f heißt *Endo- bzw. Automorphismus* , wenn $G = H$ und f Homo- bzw. Isomorphismus ist.
4. G und H heißen *zueinander isomorph* ($G \cong H$), wenn es einen Isomorphismus $g \colon G \to H$ gibt.

Bemerkung 1.1.6. Seien G, H Gruppen und $f \colon G \to H$ ein Homomorphismus. Dann gilt

1. $f(e) = e$, und $f(x^{-1}) = f(x)^{-1}$ für alle $x \in G$.
2. Ist U Untergruppe von G, so ist $f(U)$ Untergruppe von H. Ist V Untergruppe von H, so ist $f^{-1}(V)$ Untergruppe von G. Insbesondere ist also $\mathsf{Kern}(f) := f^{-1}(\{e'\})$ (e' neutrales Element von H) eine Untergruppe von G.
3. $\mathsf{Kern}(f) = \{e\}$ genau dann, wenn f injektiv ist.
4. f ist Isomorphismus genau dann, wenn ein Homomorphismus $g\colon H \to G$ mit $g \circ f = \mathsf{id}_G$ und $f \circ g = \mathsf{id}_H$ existiert.

Beweis. 1. $f(e) = f(ee) = f(e)f(e)$, also $f(e) = e$. Außerdem ist $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e$ also $f(x^{-1}) = f(x)^{-1}$.

2. Sei U Untergruppe von G. Da $U \neq \emptyset$, folgt $f(U) \neq \emptyset$. Ferner gilt für alle $x, y \in U$

$$f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(U).$$

Also ist $f(U)$ nach dem Kriterium 1.1.4 Untergruppe von H.

Sei V Untergruppe von H. Dann gilt $f^{-1}(V) \neq \emptyset$, da $f(e) = e \in V$, also $e \in f^{-1}(V)$. Seien nun $x, y \in f^{-1}(V)$ und damit $f(x), f(y) \in V$. Da V Untergruppe ist, folgt $f(x)f(y)^{-1} = f(xy^{-1}) \in V$, also $xy^{-1} \in f^{-1}(V)$, und damit $f^{-1}(V)$ Untergruppe von G nach 1.1.4

3. $\Longrightarrow$. Seien $x, y \in G$ mit $f(x) = f(y)$. Dann gilt $e = f(x)f(y)^{-1} = f(xy^{-1})$ und somit $xy^{-1} = e$, also $x = y$.

$\Longleftarrow$. $f(e) = e$, also $e \in \mathsf{Kern}(f)$. Sei $x \in \mathsf{Kern}(f)$. Dann gilt $f(x) = e$ und damit $x = e$, da f injektiv ist; also $\mathsf{Kern}(f) = \{e\}$.

4. $\Longrightarrow$. Setze $g := f^{-1}$. Zu zeigen bleibt, daß f^{-1} ein Homomorphismus ist. Seien $x, y \in H$ mit $x = f(u), y = f(v)$ für $u, v \in G$. Dann gilt $f^{-1}(x)f^{-1}(y) = uv = f^{-1}(f(uv)) = f^{-1}(f(u)f(v)) = f^{-1}(xy)$. Also ist f^{-1} Homomorphismus.

$\Longleftarrow$. Klar, da aus der Existenz von g die Bijektivität von f folgt. ☐

Definition 1.1.7. Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe.

1. Sei $x \in G$. Dann heißt

   $$xU := \{\, xu \mid u \in U \,\}$$

   die von x erzeugte *Linksnebenklasse* bzgl. U. Analog heißt

   $$Ux := \{\, ux \mid u \in U \,\}$$

   die von x erzeugte *Rechtsnebenklasse* bzgl. U.
2. $G/U := \{\, xU \mid x \in G \,\}$. (Sprechweise: "$G$ modulo U").

Bemerkung 1.1.8. Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann gilt

1. $xU = yU$ genau dann, wenn $x^{-1}y \in U$. Definiert man für $x, y \in G$

   $$x \sim y :\Longleftrightarrow x^{-1}y \in U$$

   (Schreibweise: $x \equiv y \mod U$, "x kongruent y modulo U"), so ist also $\sim$ eine Äquivalenzrelation auf G.

2. $xU = \{ y \mid y \sim x \}$ (=: $[x]$, Äquivalenzklasse von x).

3. Wähle in jeder Linksnebenklasse ein Element (Repräsentant) x_i. $(x_i)_{i\in I}$ sei die Familie der Repräsentanten. Dann gilt

$$G = \bigcup_{i\in I} x_i U \quad \text{(disjunkte Vereinigung).}$$

Beweis. 1. Es genügt, die erste Aussage zu beweisen. $\Longrightarrow$. Da $y = ye \in yU = xU$, gilt $y = xu$ für ein $u \in U$. Damit folgt $x^{-1}y = u \in U$.

$\Longleftarrow$. $x^{-1}y = u \in U$, also $y = xu$. Dann folgt für alle $v \in U$, daß $yv = xuv \in xU$, also $yU \subseteq xU$. Wegen $(x^{-1}y)^{-1} = y^{-1}x$ folgt analog $xU \subseteq yU$.

2. $\subseteq$. Sei $u \in U$. Dann gilt $(xu)^{-1}x = u^{-1}x^{-1}x = u^{-1} \in U$, also $xu \sim x$.

$\supseteq$. Sei $y \sim x$, also $y^{-1}x \in U$. Dann gibt es ein $u \in U$ mit $y^{-1}x = u$; und folglich gilt $y = xu^{-1}$, also $y \in xU$.

3. Dies gilt bekanntlich für jede Äquivalenzrelation. □

Definition 1.1.9. 1. Sei G eine Menge. Dann ist $|G|$ die Anzahl der Elemente von G. ($|G| = \infty$ ist zugelassen).

2. Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe.

$$[G\colon U] := |G/U| \quad \text{heißt } \textit{Index} \text{ von } U \text{ in } G.$$

$[G\colon U]$ gibt die Anzahl der Linksnebenklassen an.

Satz 1.1.10. *(Lagrange). Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann gilt*

$$|G| = |U| \cdot [G\colon U].$$

Beweis. Falls $|U| = \infty$, so gilt die Behauptung. Falls $|U| < \infty$, genügt es zu zeigen $|xU| = |U|$ für alle $x \in G$ (mit Bemerkung 1.1.8(3) folgt dann die Behauptung). Betrachte die Abbildungen

$$\begin{aligned} \hat{x}\colon U &\to xU & \qquad \overline{x}\colon xU &\to U,\\ \hat{x}(u) &= xu & \overline{x}(v) &= x^{-1}v. \end{aligned}$$

($\overline{x}$ ist wohldefiniert, denn aus $v \in xU$ folgt $x^{-1}v \in U$). Dann ist $\overline{x} \circ \hat{x} = \mathsf{id}_U$ und $\hat{x} \circ \overline{x} = \mathsf{id}_{xU}$. Also ist $\hat{x}$ bijektiv, und damit $|xU| = |U|$. □

Folgerung 1.1.11. *(Kleiner Fermatscher Satz). Sei G eine endliche Gruppe. Dann gilt für alle $x \in G$*

$$x^{|G|} = e.$$

Beweis. Sei $x \in G$ beliebig, aber fest gewählt. $U := \{ x^i \mid i \in \mathbb{N} \}$ ist abelsche Untergruppe von G, da $U \neq \emptyset$ und $x^i \cdot x^j = x^{i+j} \in U$. (Untergruppenkriterium 1.1.4(3) für endliche Gruppen). Es gilt $x^{|U|} = e$, denn

$$\begin{aligned} \prod_{y\in U}(xy) &= x^{|U|}\prod_{y\in U} y & &\text{da } U \text{ abelsch,}\\ \prod_{y\in U}(xy) &= \prod_{y\in U} y, & &\text{da } \hat{x}\colon U \to U,\ \hat{x}(y) = xy \text{ bijektiv ist.} \end{aligned}$$

Also folgt $x^{|G|} = x^{|U|\cdot[G\,:\,U]} = (x^{|U|})^{[G\,:\,U]} = e$. □

1.2 Zyklische Gruppen

Definition 1.2.1. Sei $(G, \circ)$ eine Gruppe. G heißt *zyklisch*, wenn es ein $a \in G$ gibt mit $G = \{ a^i \mid i \in \mathbb{Z} \} =: \langle a \rangle$. a^i bedeutet dabei $\hat{a} \circ \hat{a} \circ \cdots \circ \hat{a}$ (i-mal),wobei

$$\hat{a} = \begin{cases} a & \text{für } i \geq 0, \\ a^{-1} & \text{für } i < 0. \end{cases}$$

Beispiele.

1. $\mathbb{Z}$ ist zyklisch, denn $\mathbb{Z} = \langle 1 \rangle$.
2. $n\mathbb{Z} := \{ nx \mid x \in \mathbb{Z} \}$ ($n \in \mathbb{N}$) ist ebenfalls zyklisch, denn $n\mathbb{Z} = \langle n \rangle$.
3. $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ ($n \in \mathbb{N}$, $n > 0$) mit der Addition modulo n als Gruppenverknüpfung ist zyklisch, denn $\mathbb{Z}_n = \langle 1 \rangle$.

Lemma 1.2.2. *(Bestimmung der Untergruppen von $\mathbb{Z}$). Die Untergruppen von $\mathbb{Z}$ sind genau alle $n\mathbb{Z}$, $n \in \mathbb{N}$.*

Beweis. Alle $n\mathbb{Z}$ sind offenbar Untergruppen von $\mathbb{Z}$. Sei nun $U \subseteq \mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$. Zu zeigen ist

$$\exists n{\in}\mathbb{N}\ U = n\mathbb{Z}.$$

Sei o.B.d.A. $U \neq \{0\}$ (sonst setze $n := 0$). Sei m die kleinste positive Zahl in U (da U Untergruppe ist, existieren positive Zahlen in U). Dann gilt $U = m\mathbb{Z}$. Begründung: Da $m \in U$ und U Untergruppe, gilt $m\mathbb{Z} \subseteq U$. Sei nun $x \in U$. Es existieren $s \in \mathbb{Z}$ und $r \in \{0, \ldots, m-1\}$ mit $x = s \cdot m + r$. Daraus folgt $r = x - s \cdot m \in U$, also $r = 0$ nach Wahl von m. Damit ist auch $x = s \cdot m \in m\mathbb{Z}$ und folglich $U \subseteq m\mathbb{Z}$, insgesamt also $U = m\mathbb{Z}$. □

Lemma 1.2.3. *(Bestimmung der zyklischen Gruppen). Sei G zyklische Gruppe. Dann gilt*

$$G \cong \mathbb{Z} \textit{ oder } G \cong \mathbb{Z}_n \textit{ für ein } n \in \mathbb{N},\ n > 0.$$

Beweis. Sei G eine zyklische Gruppe und $G = \langle a \rangle = \{ a^i \mid i \in \mathbb{Z} \}$. Betrachte die Abbildung

$$f\colon \mathbb{Z} \to \langle a \rangle, \quad f(i) = a^i.$$

f ist Homomorphismus, da $a^{i+j} = a^i \cdot a^j$. f ist surjektiv, denn $f(\mathbb{Z}) = \{ a^i \mid i \in \mathbb{Z} \} = \langle a \rangle$.

Fall 1. $\mathsf{Kern}(f) = \{0\}$. Nach Bemerkung 1.1.6(3) ist f dann injektiv, also bijektiv, und damit gilt $\mathbb{Z} \cong \langle a \rangle$.

Fall 2. $\mathsf{Kern}(f) \neq \{0\}$. Da $\mathsf{Kern}(f)$ Untergruppe von $\mathbb{Z}$ ist, existiert nach Lemma 1.2.2 ein $n > 0$ mit $\mathsf{Kern}(f) = n\mathbb{Z}$. Damit folgt $a^n = e$ und $a^m \neq e$ für alle $m \in \{1, \ldots, n-1\}$. Nun sind alle a^i für $i \in \{0, \ldots, n-1\}$ verschieden (denn für $0 \leq r < s < n$ ist $0 < s - r < n$, also $a^{s-r} \neq e$ und damit $a^r \neq a^s$). Also ist $\langle a \rangle = \{a^0, a^1, \ldots, a^{n-1}\}$. □

Definition 1.2.4. Sei G eine Gruppe und $a \in G$. Dann heißt

$$\mathsf{ord}(a) := \begin{cases} \text{kleinstes } n > 0 \text{ mit } a^n = e & \text{falls eines existiert,} \\ \infty & \text{sonst} \end{cases}$$

die *Ordnung* von a.

Satz 1.2.5. *Sei G eine endliche Gruppe und $a \in G$. Dann ist* $\mathsf{ord}(a)$ *Teiler der Gruppenordnung $|G|$. Ist $|G|$ eine Primzahl, so ist G zyklisch.*

Beweis. $\langle a \rangle$ ist eine Untergruppe von G. Mit dem Satz 1.1.10 von Lagrange folgt, daß $|\langle a \rangle|$ ein Teiler von $|G|$ ist, und es ist $|\langle a \rangle| = \mathsf{ord}(a)$. Falls $|G|$ Primzahl ist, so ist demnach $\mathsf{ord}(a) = |G|$ für alle $a \neq e$. Damit ist G zyklisch. □

Satz 1.2.6. *Jede Untergruppe einer zyklischen Gruppe ist zyklisch, und jedes homomorphe Bild einer zyklischen Gruppe ist zyklisch.*

Beweis. Sei G zyklisch, etwa $G = \langle a \rangle$.

1. Sei $U \subseteq G$ Untergruppe. Es existiert ein minimales $n > 0$ mit $a^n \in U$. Dann gilt $U = \langle a^n \rangle$.

2. Sei H eine weitere Gruppe und $f\colon G \to H$ ein Homomorphismus. Dann gilt $f(G) = \langle f(a) \rangle$. □

1.3 Normalteiler

Erstes Ziel dieses Paragraphen ist die Charakterisierung der Kerne von Gruppenhomomorphismen.

Bemerkung 1.3.1. Seien G, H Gruppen, $f\colon G \to H$ Homomorphismus und $N := \mathsf{Kern}(f)$. Dann gilt

$$xN = Nx \quad \text{für alle } x \in G.$$

Beweis. Sei $x \in G$ und $z \in N = \mathsf{Kern}(f)$. Es ist

$$\begin{aligned}
&f(xzx^{-1}) = f(x)f(z)f(x^{-1}) = f(xx^{-1}) = f(e) = e\\
&xzx^{-1} \in N\\
&xNx^{-1} \subseteq N\\
&xN \subseteq Nx.
\end{aligned}$$

Dann gilt auch $x^{-1}N \subseteq Nx^{-1}$ für alle $x \in G$, also $Nx \subseteq xN$. Insgesamt folgt $xN = Nx$ für alle $x \in G$. □

Definition 1.3.2. Sei G Gruppe und $N \subseteq G$ Untergruppe. N heißt *Normalteiler* (in G), wenn gilt

$$xN = Nx \quad \text{für alle } x \in G.$$

Satz 1.3.3. *(Konstruktion der* Faktorgruppe*). Sei G eine Gruppe und $N \subseteq G$ Normalteiler. Definiere*

$$\begin{aligned}
\mathsf{kan}\colon G &\to G/N\\
x &\mapsto xN.
\end{aligned}$$

Dann gibt es auf G/N genau eine Gruppenstruktur, so daß $\mathsf{kan}\colon G \to G/N$ *ein Homomorphismus wird. In diesem Fall gilt* $\mathsf{Kern}(\mathsf{kan}) = N$.

Beweis. Existenz. Für alle $x, y \in G$ gilt $xNyN = xyNN = xyN$. Also existiert eine assoziative Verknüpfung auf G/N mit neutralem Element eN; $x^{-1}N$ ist inverses Element zu xN. Demnach ist G/N Gruppe, kan ist Homomorphismus und $\mathsf{Kern}(\mathsf{kan}) = N$.

Eindeutigkeit. Eine Verknüpfung $\circ$ auf G/N, so daß kan Homomorphismus ist, müßte die Bedingung $xN \circ yN = xyN = xyNN = xN \cdot yN$ erfüllen. □

Satz 1.3.4. *Sei G Gruppe und $N \subseteq G$ Untergruppe. Dann sind äquivalent*

1. *N ist Normalteiler,*
2. *$xN \subseteq Nx$ für alle $x \in G$,*
3. *N ist Kern eines Gruppenhomomorphismus $f\colon G \to H$.*

Beweis. $1 \Longrightarrow 2$. Klar nach Definition des Normalteilers.

$2 \Longrightarrow 1$. Im Beweis zu Bemerkung 1.3.1 wurde gezeigt, daß aus $xN \subseteq Nx$ für alle $x \in G$ folgt $xN = Nx$.

$1 \Longrightarrow 3$. Siehe Satz 1.3.3

$3 \Longrightarrow 1$. Siehe Bemerkung 1.3.1. □

Satz 1.3.5. *(Universelle Eigenschaft der Faktorgruppe). Seien G und H Gruppen, $N \subseteq G$ Normalteiler, $f\colon G \to H$ Homomorphismus und $N \subseteq \mathsf{Kern}(f)$. Dann gibt es genau einen Homomorphismus $g\colon G/N \to H$ mit $g \circ \mathsf{kan} = f$.*

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\mathsf{kan}"'] & & H \\ & G/N \arrow[ur, "g"'] & \end{tikzcd}$$

Beweis. Existenz. Definiere

$$\begin{aligned} g\colon G/N &\to H \\ g(xN) &= f(x). \end{aligned}$$

g ist wohldefiniert:

$$\begin{aligned} xN &= yN \\ x &= yz && \text{für ein } z \in N \\ f(x) = f(yz) &= f(y)f(z) = f(y) && \text{da } z \in N \subseteq \mathsf{Kern}(f). \end{aligned}$$

g ist ein Homomorphismus, denn für alle $x, y \in G$ gilt

$$g(xNyN) = g(xyN) = f(xy) = f(x)f(y) = g(xN)g(yN).$$

Eindeutigkeit. Für eine Abbildung g mit den gewünschten Eigenschaften muß gelten

$$g(xN) = (g \circ \mathsf{kan})(x) = f(x) \qquad \text{für alle } x \in G.$$ □

Folgerung 1.3.6. *(Homomorphiesatz). Seien G, H Gruppen, $f\colon G \to H$ ein Epimorphismus und $N := \mathsf{Kern}(f)$. Dann gilt $G/N \cong H$.*

Beweis. Sei g wie in Satz 1.3.5 erklärt. Dann ist g surjektiv, da $f = g \circ \mathsf{kan}$ und f surjektiv ist. g ist auch injektiv, denn aus $g(xN) = e$ folgt $f(x) = e$, also $x \in N$ und damit $xN = N$. Insgesamt ist also g bijektiv, woraus $G/N \cong H$ folgt. □

Bemerkung 1.3.7. Seien G, H Gruppen und $f\colon G \to H$ ein Homomorphismus. Dann gilt

1. Ist M Normalteiler in H, so ist $f^{-1}(M)$ Normalteiler in G.
2. Ist N Normalteiler in G und f surjektiv, so ist $f(N)$ Normalteiler in H.

Beweis. 1. Betrachte die Abbildungen $f\colon G \to H$ und $\mathsf{kan}\colon H \to H/M$. Mit Satz 1.3.3 gilt $\mathsf{Kern}(\mathsf{kan}) = M$ und damit auch $\mathsf{Kern}(\mathsf{kan} \circ f) = f^{-1}(M)$. Also ist $f^{-1}(M)$ Normalteiler nach Satz 1.3.4.

2. Sei $y \in H$. Dann existiert ein $x \in G$ mit $y = f(x)$, da f surjektiv ist. Man erhält $yf(N) = f(x)f(N) = f(xN) = f(Nx) = f(N)f(x) = f(N)y$. □

Satz 1.3.8. *(Erster Isomorphiesatz von Noether). Sei G eine Gruppe, $U \subseteq G$ Untergruppe und $N \subseteq G$ Normalteiler. Dann ist $U \cap N$ Normalteiler in U, UN Untergruppe von G und es gilt*

$$U/(U \cap N) \cong UN/N.$$

Beweis. Zunächst wird gezeigt, daß UN Untergruppe von G ist. Es gilt $e \in U$, also $UN \neq \emptyset$. Da N Normalteiler ist, gilt außerdem $xN = Nx$ für alle $x \in G$; insbesondere also $UN = NU$. Seien $x, y \in UN$. Es existiert $u \in U, n \in N$ mit $y = un$. Es ist $y^{-1} = (un)^{-1} = n^{-1}u^{-1} \in NU = UN$ und damit auch $xy^{-1} \in UNUN = UUNN = UN$. Also ist UN nach 1.1.4 Untergruppe von G.

Betrachte nun die Abbildung $\mathsf{kan}: G \to G/N$. Durch Einschränkung erhält man $f\colon U \to \mathsf{kan}(U)$. Es gilt $\mathsf{Kern}(\mathsf{kan}) = N$, also $\mathsf{Kern}(f) = U \cap N$. Daraus folgt, daß $U \cap N$ Normalteiler in U ist. Also gilt nach dem Homomorphiesatz

$$U/(U \cap N) \cong \mathsf{kan}(U) = \{\, uN \mid u \in U \,\} = \{\, xN \mid x \in UN \,\} = UN/N. \qquad \square$$

Satz 1.3.9. *(Zweiter Isomorphiesatz von Noether). Seien G und H Gruppen, $f\colon G \to H$ Epimorphismus, $M \subseteq H$ Normalteiler und $N := f^{-1}(M)$. Dann gilt*

$$G/N \cong H/M.$$

Beweis. Betrachte die Abbildungen $f\colon G \to H$ und $\mathsf{kan}\colon H \to H/M$. $\mathsf{kan} \circ f$ ist Epimorphismus, und es gilt $\mathsf{Kern}(\mathsf{kan} \circ f) = f^{-1}(M) = N$. Also folgt mit dem Homomorphiesatz $G/N \cong H/M$. □

Bemerkung. Der Homomorphiesatz ist hierin als Spezialfall für $M = \{e\}$ enthalten.

Definition 1.3.10. Sei G eine Gruppe und $N \subseteq G$ Normalteiler. N heißt *maximaler* Normalteiler, wenn für alle M gilt

Aus $N \subseteq M \subseteq G$ und M Normalteiler folgt $M = N$ oder $M = G$.

N heißt *echter* Normalteiler, wenn $\{e\} \subsetneq N \subsetneq G$. Die Gruppe G heißt *einfach*, wenn G keine echten Normalteiler besitzt.

Bemerkung. Sei G eine einfache Gruppe. Dann läßt sich G durch Homomorphismen nicht echt verkleinern, d.h. ist $f\colon G \to H$ ein Epimorphismus, so ist f Isomorphismus oder $H = \{e\}$.

Beweis. Da G einfach und $\mathsf{Kern}(f)$ Normalteiler in G ist, folgt $\mathsf{Kern}(f) = \{e\}$ oder $\mathsf{Kern}(f) = G$. Also ist f Isomorphismus oder $H = \{e\}$. □

Lemma 1.3.11. *Sei G eine Gruppe und $N \subseteq G$ Normalteiler. N ist maximaler Normalteiler genau dann, wenn G/N einfach ist.*

Beweis. Betrachte die Abbildung $\mathsf{kan}\colon G \to G/N$.

$\Longrightarrow$. Sei $\overline{N} \subseteq G/N$ Normalteiler. Dann gilt $N \subseteq \mathsf{kan}^{-1}(\overline{N}) \subseteq G$, und $\mathsf{kan}^{-1}(\overline{N})$ ist Normalteiler in G. Daraus folgt $\mathsf{kan}^{-1}(\overline{N}) = N$ oder $\mathsf{kan}^{-1}(\overline{N}) = G$, also (indem man die kan-Bilder betrachtet) $\overline{N} = \{[e]\}$ oder $\overline{N} = G/N$. Damit ist G/N einfach.

$\Longleftarrow$. Sei $N \subseteq M \subseteq G$ und M Normalteiler. Daraus folgt $\{[e]\} \subseteq \mathsf{kan}(M) \subseteq G/N$ und $\mathsf{kan}(M)$ Normalteiler. Falls $\mathsf{kan}(M) = \{[e]\}$ ist, gilt $M \subseteq N$, also M = N. Falls $\mathsf{kan}(M) = G/N$, enthält M aus jeder Nebenklasse mindestens ein Element. Da $N \subseteq M$, gilt: aus $m \in M$ folgt $mN \subseteq M$. Also enthält M mit jedem Element gleich die ganze Nebenklasse. Insgesamt gilt also $M = N$ oder $M = G$. Daraus folgt, daß M maximaler Normalteiler ist. □

1.4 Operationen einer Gruppe auf einer Menge

Definition 1.4.1. Sei G eine Gruppe und p eine Primzahl. G heißt *p-Gruppe*, wenn $|G| = p^n$ für ein $n \geq 1$.

$$Z_G := \{\, y \in G \mid xy = yx \text{ für alle } x \in G \,\}$$

heißt das *Zentrum* von G.

Lemma 1.4.2. *Sei G eine Gruppe. Dann ist Z_G Normalteiler in G.*

Beweis. Seien $y, z \in Z_G$. Dann gilt $xyz = yxz = yzx$ für alle $x \in G$, also $yz \in Z_G$. Außerdem folgt mit $xe = ex$ auch $e \in Z_G$. Sei $y \in Z_G$. Dann gilt wiederum $xy = yx$ für alle $x \in G$, damit auch $y^{-1}x = xy^{-1}$ und schließlich $y^{-1} \in Z_G$. $xZ_G = Z_G x$ gilt sogar elementweise. Also ist Z_G Normalteiler in G. □

Es soll jetzt gezeigt werden, daß jede p-Gruppe ein nichttriviales Zentrum hat. (Dies wird in Abschnitt 1.5 gebraucht zum Beweis, daß jede p-Gruppe auflösbar ist). Dazu werden als Hilfsmittel die Operationen einer Gruppe auf einer Menge sowie die sog. Klassengleichung benötigt.

Definition 1.4.3. Sei G eine Gruppe, S eine Menge und $m\colon G \times S \to S$ eine Abbildung. (Abkürzung: $xs := m(x, s)$ für $x \in G$, $s \in S$)

1. m heißt *Operation* von G auf S, wenn gilt

$$\begin{aligned} (xy)s &= x(ys) && \text{für alle } s \in S \text{ und } x, y \in G,\\ es &= s && \text{für alle } s \in S. \end{aligned}$$

2. Sei m Operation von G auf S und $s \in S$.

$$\begin{aligned} Gs &:= \{ xs \mid x \in G \} && \text{heißt } \textit{Orbit} \text{ von } s, \\ G_s &:= \{ x \in G \mid xs = s \} && \text{heißt } \textit{Isotopiegruppe} \text{ von } s. \end{aligned}$$

Bemerkung. Sei G eine Gruppe, $m\colon G \times S \to S$ eine Operation und $s \in S$. Dann ist G_s Untergruppe von G.

Beweis. 1. Aus $es = s$ folgt $e \in G_s$.
2. Seien $x, y \in G_s$. Dann gilt $(xy)s = x(ys) = xs = s$ und damit $xy \in G_s$.
3. Sei $x \in G_s$. Dann gilt $xs = s$ und damit auch $x^{-1}s = x^{-1}(xs) = (x^{-1}x)s = s$. Daraus folgt $x^{-1} \in G_s$. □

Beispiele 1.4.4. 1. Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe.

$$\begin{aligned} &U \times G \to G \\ &(u, x) \mapsto ux \quad \text{(Verknüpfung in } G) \end{aligned}$$

ist Operation von U auf G.
2. Sei G eine Gruppe.

$$\begin{aligned} &G \times G \to G \\ &(x, y) \mapsto xyx^{-1} \quad \text{(Verknüpfung in } G) \end{aligned}$$

ist Operation von G auf G ("Konjugation").

Beweis. Sind $u, x, y \in G$, so gilt $(ux)y(ux)^{-1} = uxyx^{-1}u^{-1} = u(xyx^{-1})u^{-1}$. Außerdem ist $exe^{-1} = x$. □

3. Sei V ein endlichdimensionaler euklidischer Vektorraum und G eine Untergruppe der euklidischen Gruppe von V (also von $\{ g\colon V \to V \mid g \text{ Bewegung} \}$; eine Abbildung $g\colon V \to V$ heißt Bewegung (oder Kongruenz), falls es ein $f \in O(V)$ und ein $a \in V$ gibt, so daß für alle $x \in V$ gilt $g(x) = f(x) + a$). Die Abbildung

$$\begin{aligned} &G \times V \to V \\ &(x, v) \mapsto x(v) \end{aligned}$$

ist Operation. Im Spezialfall $G = O(V)$ gilt für beliebige $v \in V$

$$Gv = \{ xv \mid x \in G \} = \{ w \in V \mid \|w\| = \|v\| \} \quad \text{Orbit von } v.$$

Im Fall $\mathsf{dim}(V) = 2$ ist Gv der Kreis um den Ursprung mit Radius $\|v\|$, und im Fall $\mathsf{dim}(V) = 3$ ist Gv die Oberfläche einer Kugel um den Ursprung mit Radius $\|v\|$.

Satz 1.4.5. *Sei G eine Gruppe, S eine Menge und $m\colon G \times S \to S$ eine Operation.*

1. *S ist disjunkte Vereinigung von Orbits, also $S = \bigcup_{i \in I} Gs_i$ (disjunkte Vereinigung) für eine Familie $(s_i)_{i \in I}$ von Elementen aus S.*

2. *Sei G endlich. Dann gilt $|Gs| = [G : G_s]$ für jedes $s \in S$.*

Beweis. 1. Es gilt $s = es$ für jedes $s \in S$, also $S = \bigcup_{s \in S} Gs$. Noch zu zeigen ist, daß aus $Gs \cap Gs' \neq \emptyset$ folgt $Gs = Gs'$. Sei also $Gs \cap Gs' \neq \emptyset$. Dann existieren $x, y \in G$ mit $xs = ys'$ und damit $s = x^{-1}ys' \in Gs'$. Also ist $Gs \subseteq Gs'$. Aus Symmetriegründen gilt ebenso $Gs' \subseteq Gs$; insgesamt folgt also $Gs = Gs'$.

2. Betrachte die Abbildung

$$\begin{aligned} G/G_s &\to Gs \\ xG_s &\mapsto xs \end{aligned}$$

Folgende Aussagen sind äquivalent.

$$\begin{aligned} xG_s &= yG_s \\ x^{-1}y &\in G_s \\ x^{-1}ys &= s \\ ys &= xs. \end{aligned}$$

Daher ist die Abbildung wohldefiniert und injektiv. Nach Definition ist die Abbildung auch surjektiv, also bijektiv. □

Bemerkung 1.4.6. Sei G eine endliche Gruppe, S eine Menge, $m\colon G \times S \to S$ eine Operation und $s \in S$. Dann gilt

$$|G_s| \cdot |Gs| = |G|.$$

Beweis. Nach dem Satz von Lagrange (1.1.10) und dem Satz 1.4.5 gilt $|G| = |G_s| \cdot [G : G_s] = |G_s| \cdot |Gs|$. □

Folgerung 1.4.7. *Sei G eine endliche Gruppe, S eine Menge, $m\colon G \times S \to S$ eine Operation und $C \subseteq S$ so, daß $S = \bigcup_{s \in C} Gs$ (disjunkte Vereinigung). Dann gilt*

$$|S| = \sum_{s \in C} |Gs| = \sum_{s \in C} [G : G_s].$$ □

Im folgenden sei G eine Gruppe, und G operiere auf G mittels Konjugation.

Bemerkung 1.4.8. Das Zentrum Z_G von G besteht genau aus den Elementen von G, deren Isotopiegruppe G ist.

Beweis. Folgende Aussagen sind äquivalent.

$$\begin{aligned} &y \in Z_G \\ &xyx^{-1} = y \quad \text{für alle } x \in G \\ &G_y = \{\, x \in G \mid xyx^{-1} = y \,\} = G \end{aligned}$$ □

Satz 1.4.9. *(Klassengleichung). Sei $|G| < \infty$ und $C \subseteq G$ so, daß*

$$G = \bigcup_{y \in C} Gy \quad \textit{(disjunkte Vereinigung)}$$

($Gy = \{\, xyx^{-1} \mid x \in G \,\}$ bedeutet in diesem Fall das Orbit, nicht das Komplexprodukt). Dann gilt

$$|G| = |Z_G| + \sum_{\substack{y \in C \\ [G:G_y] \geq 2}} [G : G_y].$$

Beweis. Nach Bemerkung 1.4.8 ist $Z_G = \{ y \in C \mid [G : G_y] = 1 \}$. Die Behauptung folgt somit aus Folgerung 1.4.7. □

Satz 1.4.10. *Ist G p-Gruppe, so gilt $|Z_G| \geq p$.*

Beweis. p ist ein Teiler von $|G|$ und (wegen $|G| = p^n$) auch von $[G : G_y]$, falls $[G : G_y] \geq 2$ (siehe Bemerkung 1.4.6). Nach der Klassengleichung 1.4.9 ist dann p ein Teiler von $|Z_G|$, also $|Z_G| \geq p$. □

1.5 Auflösbare Gruppen

Sei G eine Gruppe und $M \subseteq G$ Teilmenge.

$$\langle M \rangle := \{ x_1^{\varepsilon_1} \cdot \cdots \cdot x_n^{\varepsilon_n} \mid n \geq 0, x_1, \ldots, x_n \in M, \varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\} \}$$

heißt *die von M erzeugte Untergruppe* von G. Nach Definition ist $\langle M \rangle$ die kleinste Untergruppe von G, die M enthält.

Definition 1.5.1. Sei G eine Gruppe und $x, y \in G$. Das $k \in G$ mit

$$xy = kyx, \quad \text{also} \quad k := xyx^{-1}y^{-1}$$

heißt *Kommutator* von x und y. k mißt die Abweichung vom kommutativen Gesetz.

$$K_G := \{ xyx^{-1}y^{-1} \mid x, y \in G \}$$

heißt *Kommutatormenge* von G. Die Gruppe $G' := \langle K_G \rangle$ heißt *Kommutatorgruppe* von G oder *erste Ableitung* von G.

Bemerkung. Sei G eine Gruppe. Dann gilt:

1. G ist genau dann abelsch, wenn $G' = \{e\}$.
2. $\langle K_G \rangle = \{ k_1 \cdot \cdots \cdot k_n \mid n \geq 0 \text{ und } k_1, \ldots, k_n \in K_G \}$

Beweis. 2. Es genügt zu zeigen, daß mit k auch k^{-1} in K_G liegt. Sei $k \in G$, also $k = xyx^{-1}y^{-1}$ mit $x, y \in G$. Es folgt $k^{-1} = yxy^{-1}x^{-1} \in K_G$. □

Satz 1.5.2. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann gilt*

$$G' \subseteq H \iff H \text{ ist Normalteiler mit abelscher Faktorgruppe } G/H.$$

Beweis. $\Longrightarrow$. Sei $x \in G$. Dann gilt $xhx^{-1}h^{-1} \in H$ für alle $h \in H$, da $G' \subseteq H$. Damit folgt $xhx^{-1} \in H$ und somit auch $xHx^{-1} \subseteq H$. Da $x \in G$ beliebig war, folgt nach Satz 1.3.4, daß H Normalteiler in G ist. Seien nun $Hx, Hy \in G/H$. Es ist

$$HxHy = Hxy = H(yxy^{-1}x^{-1})xy = Hyx = HyHx,$$

also G/H abelsch. Verwendet wurde hierbei $H = Hyxy^{-1}x^{-1}$; dies gilt wegen $yxy^{-1}x^{-1} \in G' \subseteq H$.

$\Longleftarrow$. Seien $x, y \in G$. Da H Normalteiler und G/H abelsch ist, gilt $HxHy = HyHx$, also $Hxy = Hyx$, somit $H = Hyxy^{-1}x^{-1}$ und damit auch $yxy^{-1}x^{-1} \in H$. Also ist $K_G \subseteq H$ und daher $G' \subseteq H$. □

Definition 1.5.3. Sei G eine Gruppe. Die *n-te Ableitung* $G^{(n)}$ von G wird rekursiv definiert durch

$$\begin{aligned} G^{(0)} &:= G, \\ G^{(n+1)} &:= (G^{(n)})'. \end{aligned}$$

Eine endliche Familie von Untergruppen $G_i \subseteq G$ $(i = 0, \ldots, n)$ heißt *Normalreihe* in G, wenn gilt

1. $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$.
2. G_{i-1} enthält G_i als Normalteiler $(i = 1, \ldots, n)$.

Die Gruppen G_{i-1}/G_i heißen *Faktoren* der Normalreihe

Satz 1.5.4. *Sei G eine Gruppe. Dann sind folgende Aussagen äquivalent.*

1. *Zu G gibt es eine Normalreihe mit abelschen Faktoren.*
2. *Für ein $n \in \mathbb{N}$ ist $G^{(n)} = \{e\}$.*

Beweis. $2 \Longrightarrow 1$. $G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(n)} = \{e\}$ ist Normalreihe mit abelschen Faktoren nach Satz 1.5.2.

$1 \Longrightarrow 2$. Sei $G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{e\}$ Normalreihe mit abelschen Faktoren. Nach Satz 1.5.2 gilt dann

$$\begin{array}{ll} H_1 \supseteq H_0' & \text{da } H_0/H_1 \text{ abelsch ist} \\ H_2 \supseteq H_1' & \text{da } H_1/H_2 \text{ abelsch ist} \\ \vdots & \\ \{e\} = H_{n-1}' & \text{da } H_{n-1}/H_n \cong H_{n-1} \text{ abelsch ist.} \end{array}$$

Da für Untergruppen $U, V \subseteq G$ aus $U \subseteq V$ stets folgt $U' \subseteq V'$, ergibt sich

$$\{e\} = H_{n-1}' \supseteq H_{n-2}^{(2)} \supseteq \cdots \supseteq H_0^{(n)} = G^{(n)},$$

also $\{e\} = G^{(n)}$. $\square$

Definition 1.5.5. Eine Gruppe G heißt *auflösbar*, wenn sie eine der beiden Bedingungen des letzten Satzes (und damit beide) erfüllt.

Bemerkung. Die Kommutatorgruppen werden nur eingeführt, um die zweite Charakterisierung zu haben, die z.B. beim Beweis, daß Untergruppen und homomorphe Bilder auflösbarer Gruppen wieder auflösbar sind, gebraucht wird.

Lemma 1.5.6. *Sei G eine Gruppe.*

1. *Ist $U \subseteq G$ eine Untergruppe, so gilt $U^{(n)} \subseteq G^{(n)}$.*
2. *Ist H eine weitere Gruppe und $f\colon G \to H$ ein Homomorphismus, so gilt $(f(G))^{(n)} = f(G^{(n)})$.*
3. *Ist $N \subseteq G$ Normalteiler, so gilt $(G/N)^{(n)} = G^{(n)}N/N$.*

Beweis. 1. Es gilt $U' \subseteq G'$, also folgt induktiv $U^{(n)} \subseteq G^{(n)}$.

2. Offenbar genügt es, die Behauptung für $n = 1$ zu zeigen; die allgemeine Aussage folgt dann durch Induktion. Zu zeigen ist also

$$(f(G))' = f(G'),$$

d.h.

$$\langle K_{f(G)} \rangle = f(\langle K_G \rangle).$$

Es gilt

$$\begin{aligned} f(\langle K_G \rangle) &= \{ f(k_1) \dots f(k_n) \mid k_1, \dots k_n \in K_G \} \\ &= \langle K_{f(G)} \rangle, \qquad \text{da } K_{f(G)} = \{ f(k) \mid k \in K_G \}. \end{aligned}$$

3. Dies ergibt sich aus (2) mit $\mathsf{kan}\colon G \to G/N$ für f. Gebraucht wird

$$\mathsf{kan}(U) = UN/N \quad \text{für jede Untergruppe } U \subseteq G$$

(vgl. Beweis zum ersten Isomorphiesatz 1.3.8). □

Satz 1.5.7. *Sei G eine auflösbare Gruppe. Dann gilt:*

1. *Jede Untergruppe von G ist auflösbar.*
2. *Jedes homomorphe Bild von G ist auflösbar.*

Beweis. 1. Sei $G^{(n)} = \{e\}$. Nach Lemma 1.5.6 gilt $U^{(n)} \subseteq G^{(n)}$, also $U^{(n)} = \{e\}$, d.h. U ist auflösbar.

2. Sei H eine Gruppe, $f\colon G \to H$ Epimorphismus und $G^{(n)} = \{e\}$. Dann gilt nach Lemma 1.5.6

$$H^{(n)} = (f(G))^{(n)} = f(G^{(n)}) = \{e\}.$$ □

Insbesondere ist also jeder Quotient einer auflösbaren Gruppe auflösbar. Satz 1.5.7 wird später für die Diskussion der Auflösbarkeit von Gleichungen durch Radikale gebraucht.

Satz 1.5.8. *Sei G eine Gruppe und $N \subseteq G$ Normalteiler. Sind dann N und G/N auflösbar, so ist auch G auflösbar.*

Beweis. Sind $n, m \in \mathbb{N}$ mit $N^{(n)} = \{e\}$ und $(G/N)^{(m)} = \{[e]\}$, so gilt $G^{(m)}N/N = \{[e]\}$ (siehe Lemma 1.5.6), also $G^{(m)}N = N$ und somit $G^{(m)} \subseteq N$. Es folgt $G^{(m+n)} \subseteq N^{(n)} = \{e\}$, also ist G auflösbar. □

Folgerung 1.5.9. *Jede p-Gruppe ist auflösbar.*

Beweis. Sei $|G| = p^n$, p Primzahl. Der Beweis wird durch vollständige Induktion über n geführt.

$n = 1$: Wegen $|G| = p$ ist G zyklisch nach Satz 1.2.5, damit auch abelsch und folglich auflösbar.

$n > 1$: Nach Satz 1.4.10 gilt $|Z_G| \geq p$. *Fall* 1. $G = Z_G$. Dann ist G abelsch und damit auflösbar. *Fall* 2. $G \supsetneq Z_G$. Wegen $|G| = p^n$ ist $|Z_G| = p^k$ mit $1 \leq k < n$ und $[G : Z_G] = p^{n-k}$. Nach Induktionsvoraussetzung sind Z_G und G/Z_G auflösbar, und nach Szta 1.5.8 ist also auch G auflösbar. □

Die Folgerung 1.5.9 wird später beim Beweis des Hauptsatzes über Konstruktionen mit Zirkel und Lineal benötigt.

Definition 1.5.10. Sei $G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m$ eine Normalreihe. Eine Normalreihe $H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n$ heißt eine *Verfeinerung* von $G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m$, wenn es eine ordnungstreue injektive Abbildung

$$\pi\colon \{0, 1, \ldots, m\} \to \{0, 1, \ldots, n\}$$

gibt, so daß für alle i gilt

$$G_i = H_{\pi(i)}.$$

Lemma 1.5.11. *Sei G eine Gruppe und $G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{e\}$ eine Normalreihe mit abelschen Faktoren. Dann hat jede Verfeinerung dieser Normalreihe ebenfalls abelsche Faktoren.*

Beweis. Betrachte $H_{i-1} = S_0 \supseteq S_1 \supseteq \cdots \supseteq S_k = H_i$ und $H_{i-1}/H_i = S_0/H_i \supseteq S_1/H_i \supseteq \cdots \supseteq S_k/H_i = \{[e]\}$. Da H_{i-1}/H_i abelsch ist, sind auch alle S_l/H_i abelsch. Der zweite Noethersche Isomorphiesatz 1.3.9 angewandt auf den Epimorphismus $S_{l-1} \to S_{l-1}/H_i$ liefert wegen $\mathsf{kan}^{-1}(S_l/H_i) = S_l$

$$S_{l-1}/S_l \cong (S_{l-1}/H_i)/(S_l/H_i).$$

Da $(S_{l-1}/H_i)/(S_l/H_i)$ als Faktorgruppe einer abelschen Gruppe selbst abelsch ist, ist auch S_{l-1}/S_l abelsch. □

Satz 1.5.12. *Jede endliche auflösbare Gruppe hat eine Normalreihe, deren Faktoren zyklische Gruppen von Primzahlordnung sind.*

Beweis. G hat eine Normalreihe mit abelschen Faktoren, da G auflösbar ist. Nun wird eine maximale Verfeinerung gebildet, d.h. es werden zwischen zwei Terme solange echte Normalteiler geschoben, bis dies nicht mehr geht. Da G endlich ist, bricht das Verfahren ab. Die Faktoren dieser maximalen Verfeinerung sind abelsch (nach Lemma 1.5.11) und einfach (da jeweils maximale Normalteiler vorliegen). Eine einfache abelsche Gruppen hat keine echten Untergruppen, ist also zyklisch und deshalb – da sie einfach ist – von Primzahlordnung. □

Dieser Satz wird gebraucht für die Diskussion der Auflösbarkeit von Gleichungen durch Radikale und für den Hauptsatz über Konstruktionen mit Zirkel und Lineal.

Wir wollen jetzt die Auflösbarkeit der symmetrischen Gruppen

$$S_n := \{\, f \mid f\colon \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ bijektiv} \,\}$$

untersuchen. Gezeigt wird, daß S_n für $n \geq 5$ nicht auflösbar ist.

Es wird sich als nützlich erweisen, die Elemente aus S_n als Produkte von sogenannten *Zykeln* darzustellen. Für verschiedene $i_1, \ldots, i_m \in \{1, \ldots, n\}$ bezeichnet man das $f \in S_n$ mit

$$\begin{aligned}
f(i_1) &= i_2, \\
f(i_2) &= i_3, \\
&\vdots \\
f(i_{m-1}) &= i_m, \\
f(i_m) &= i_1, \\
f(x) &= x \qquad \text{für } x \notin \{i_1, \ldots, i_m\}
\end{aligned}$$

mit

$$f = (i_1\ i_2 \ldots\ i_m)$$

und nennt es *m-Zykel.* Jedes Element von S_n läßt sich als Produkt von Zykeln darstellen, wobei keine Zahl in zwei Zykeln gleichzeitig vorkommt. Die Darstellung ist bis auf die Reihenfolge der Zykeln und zyklische Vertauschung der Zykeln eindeutig. (Alle diese Aussagen lassen sich leicht durch Induktion über n beweisen). Beispiel:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 6 & 4 & 2 & 8 & 7 & 9 & 1 \end{pmatrix} \quad \text{entspricht} \quad (1\ 3\ 6\ 8\ 9)\,(2\ 5).$$

Es soll nun gezeigt werden, daß für $n \geq 5$ die Gruppe S_n nicht auflösbar ist. Zur Vorbereitung dient das folgende Lemma.

Lemma 1.5.13. *Sei $n \geq 5$, $U \subseteq S_n$ Untergruppe, $\overline{U} \subseteq U$ Normalteiler und $U/\overline{U}$ abelsch. Enthält U alle 3-Zykeln, so müssen sie schon in $\overline{U}$ liegen.*

Beweis. Seien $i, k, l \in \{1, \ldots, n\}$ verschieden. Zu zeigen ist $(i\ l\ k) \in \overline{U}$. Seien zusätzlich noch $j, m \in \{1, \ldots, n\}$, so daß i, j, k, l, m verschieden sind (diese Wahl ist möglich, da $n \geq 5$). Bilde

$$x := (i\ j\ k) \quad \text{und} \quad y := (k\ l\ m).$$

Nach Voraussetzung sind $x, y \in U$. Betrachte $\mathsf{kan}\colon U \to U/\overline{U}$. Dann gilt

$$\mathsf{kan}(xyx^{-1}y^{-1}) = \mathsf{kan}(x)\mathsf{kan}(y)\mathsf{kan}(x)^{-1}\mathsf{kan}(y)^{-1} = [e], \quad \text{da } U/\overline{U} \text{ abelsch ist.}$$

Damit folgt $xyx^{-1}y^{-1} \in \overline{U}$. Andererseits ist

$$xyx^{-1}y^{-1} = (i\ j\ k)(k\ l\ m)(k\ j\ i)(m\ l\ k) = (i\ l\ k),$$

wie man leicht nachrechnet. Insgesamt folgt $(i\ l\ k) \in \overline{U}$. □

Satz 1.5.14. *S_n ist für $n \geq 5$ nicht auflösbar.*

Beweis. Sei $n \geq 5$. Nehmen wir an, S_n sei auflösbar. Dann existiert eine Normalreihe mit abelschen Faktoren, etwa $S_n = U_0 \supseteq U_1 \supseteq \cdots \supseteq U_r = \{e\}$. Es sind alle 3-Zykeln in $S_n = U_0$. Da U_0/U_1 abelsch ist, folgt mit dem Lemma vorher, daß alle 3-Zykeln in U_1 sind. Da U_1/U_2 abelsch ist, folgt ebenso, daß alle 3-Zykeln in U_2 liegen. Schließlich ergibt sich, daß alle 3-Zykeln in $U_r = \{e\}$ sind. Dies ist der gesuchte Widerspruch. □

Kapitel 2

Körper

2.1 Grundbegriffe

Definition 2.1.1. Sei K eine Menge und $+\colon K \times K \to K$, $\cdot\colon K \times K \to K$ Abbildungen (Schreibweise: $x + y := +(x, y), xy := \cdot(x, y)$). K (oder genauer $(K, +, \cdot)$) heißt Körper, wenn gilt

1. $(K, +)$ ist eine abelsche Gruppe. Ihr neutrales Element wird mit 0, das zu $x \in K$ inverse Element mit $-x$ bezeichnet.

2. $K^* := K \setminus \{0\}$ ist zusammen mit der auf K^* eingeschränkten Multiplikation eine abelsche Gruppe. Ihr neutrales Element wird mit 1, das zu $x \in K^*$ inverse Element mit x^{-1} bezeichnet.

3. $x(y + z) = (xy) + (xz)$ für alle $x, y, z \in K$.

Schreibweise. 1. '$\cdot$' bindet stärker als '$+$'; beispielsweise steht $xy + xz$ für $(xy) + (xz)$.

2. $x - y$ steht für $x + (-y)$, und $\frac{x}{y}$ für xy^{-1}.

3. nx steht für $\underbrace{x + x + \cdots + x}_{n\text{-mal}}$, und x^n steht für $\underbrace{x \cdot x \cdot \cdots \cdot x}_{n\text{-mal}}$.

Bemerkung. Sei K ein Körper. Dann gilt für alle $x, y \in K$:

1. $0 \cdot x = 0$.

2. Wenn $x \neq 0$ und $y \neq 0$, so ist $xy = 0$.

3. $-x = (-1)x$.

4. $(-x)(-y) = xy$.

Beweis. 1. $0x = (0 + 0)x = 0x + 0x$ und damit $0x = 0$.
2. Klar, da K^* eine Gruppe ist.
3. Es gilt $x + (-1)x = 1x + (-1)x = (1 + (-1))x = 0x = 0$, also $-x = (-1)x$.
4. Es ist $1 + (-1) = 0$ und damit $1(-1) + (-1)(-1) = 0$, also $(-1)(-1) = 1$. Daraus folgt $(-x)(-y) = (-1)x(-1)y = (-1)(-1)xy = xy$. □

Beispiele. $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind zusammen mit der üblichen Addition und Multiplikation Körper, aber $(\mathbb{Z}, +, \cdot)$ ist *kein* Körper.

Definition 2.1.2. Sei K ein Körper und $k \subseteq K$ eine Teilmenge. k heißt Unterkörper von K, wenn folgendes gilt.

1. Mit x und y liegen auch $x + y$ und xy in k.

2. k bildet zusammen mit den induzierten Verknüpfungen
$$\begin{aligned} k \times k &\to k & \qquad k \times k &\to k \\ (x, y) &\mapsto x + y & \qquad (x, y) &\mapsto x \cdot y \end{aligned}$$
einen Körper.

Ein Paar (K, k) bestehend aus einem Körper K und einem Unterkörper k heißt *Körpererweiterung*. Schreibweise: $K \supseteq k$ statt (K, k).

Bemerkung 2.1.3. (Unterkörperkriterium). Sei K ein Körper und $k \subseteq K$ eine Teilmenge. Dann ist k ein Unterkörper von K genau dann, wenn gilt

1. k enthält mindestens zwei Elemente.

2. $x - y \in k$ für alle $x, y \in k$.

3. Für alle $x, y \in k$ mit $y \neq 0$ ist $xy^{-1} \in k$.

Beweis. $\Longrightarrow$. Dies folgt direkt aus der Definition von Unterkörpern.
$\Longleftarrow$. Aus Bedingung (2) folgt mit dem Untergruppenkriterium 1.1.4, daß $(k, +)$ Untergruppe von $(K, +)$ ist. Nach Bedingung (1) gilt $k^* \neq \emptyset$, also folgt aus Bedingung (3), wieder mit 1.1.4, daß $(k^*, \cdot)$ Untergruppe von $(K^*, \cdot)$ ist. □

Definition 2.1.4. Sei $K \supseteq k$ eine Körpererweiterung. Dann ist K zusammen mit den Abbildungen
$$\begin{aligned} K \times K &\to K & \qquad k \times K &\to K \\ (x, y) &\mapsto x + y & \qquad (\alpha, x) &\mapsto \alpha x \end{aligned}$$
ein k-Vektorraum. $[K : k] := \mathsf{dim}_k(K)$ heißt *Grad* der Körpererweiterung $K \supseteq k$. Die Körpererweiterung $K \supseteq k$ heißt *endlich*, wenn $[K : k] < \infty$. Ein Körper L heißt *Zwischenkörper* der Körpererweiterung $K \supseteq k$, wenn k Unterkörper von L und L Unterkörper von K ist.

Bemerkung. Sei $K \supseteq k$ Körpererweiterung. Dann gilt $[K : k] = 1$ genau dann, wenn $K = k$.

Beweis. Folgende Aussagen sind äquivalent.
$$\begin{aligned} &[K : k] = 1 \\ &1 \ (\in K) \text{ ist Basis des } k\text{-Vektorraums } K \\ &K = k. \end{aligned}$$
□

Satz 2.1.5. *(Gradsatz). Sei $K \supseteq k$ Körpererweiterung, L ein Zwischenkörper. Dann gilt $[K : k] = [K : L] \cdot [L : k]$.*

Beweis. Fall $[K : k] < \infty$. Dann gilt auch $[K : L] < \infty$ und $[L : k] < \infty$, da man sonst genau wie in dem folgenden Argument eine unendliche k-linear unabhängige Teilmenge von K erhielte. Sei also

$x_1, \ldots, x_m$	Basis des k-Vektorraums L, und
$y_1, \ldots, y_n$	Basis des L-Vektorraums K.

Es wird gezeigt, daß dann

$$(x_i y_j)_{i \in \{1,\ldots,m\}, j \in \{1,\ldots,n\}}$$

Basis des k-Vektorraums K ist. Lineare Unabhängigkeit.

$$\begin{aligned}
&\sum_{i,j} \alpha_{ij} x_i y_j = 0 && \text{mit } \alpha_{ij} \in k \\
&\sum_j \Big(\sum_i \alpha_{ij} x_i\Big) y_j = 0 && \\
&\sum_i \alpha_{ij} x_i = 0 && \text{für alle } j \\
&\alpha_{ij} = 0 && \text{für alle } i, j.
\end{aligned}$$

Erzeugendensystem. Sei $z \in K$. Dann gilt

$$\begin{aligned}
z &= \sum_{j=1}^{n} u_j y_j && \text{mit } u_j \in L \\
u_j &= \sum_{i=1}^{m} \alpha_{ij} x_i && \text{mit } \alpha_{ij} \in k,
\end{aligned}$$

also

$$z = \sum_{i,j} \alpha_{ij} x_i y_j \, .$$

Fall $[K : k] = \infty$. Falls $[K : L] < \infty$ und $[L : k] < \infty$, so folgt wie im ersten Fall $[K : k] < \infty$. Also ist $[K : L] \cdot [L : k] = \infty$. □

Folgerung 2.1.6. *Ist $K \supseteq k$ eine Körpererweiterung und $[K : k]$ eine Primzahl, so gibt es keine echten Zwischenkörper. Insbesondere hat $\mathbb{C} \supseteq \mathbb{R}$ keine echten Zwischenkörper.* □

2.2 Monomorphismen zwischen Körpern

Definition 2.2.1. Seien K,$\bar{K}$ Körper und $\varphi\colon K \to \bar{K}$ eine Abbildung. φ heißt *Monomorphismus* von Körpern, wenn folgendes gilt.

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$ für alle $x, y \in K$.

2. $\varphi(K^*) \subseteq \bar{K}^*$ und $\varphi(xy) = \varphi(x)\varphi(y)$ für alle $x, y \in K^*$.

φ heißt *Isomorphismus*, wenn $\varphi(K) = \bar{K}$. Ein Isomorphismus $\varphi\colon K \to K$ heißt *Automorphismus*. K und $\bar{K}$ heißen *zueinander isomorph*, falls ein Isomorphismus $\varphi\colon K \to \bar{K}$ existiert; (Schreibweise: $K \cong \bar{K}$).

Bemerkung. Seien $K, \bar{K}$ Körper. Dann gilt:

1. Jeder Monomorphismus $\varphi\colon K \to \bar{K}$ ist injektiv.

2. Ist $\varphi\colon K \to \bar{K}$ Isomorphismus, so auch $\varphi^{-1}\colon \bar{K} \to K$.

Beweis. 1. φ ist ein Gruppenhomomorphismus von $(K, +)$ in $(\bar{K}, +)$. Wegen $\varphi(K^*) \subseteq \bar{K}^*$ ist $\mathsf{Kern}(\varphi) = \{0\}$ und somit φ injektiv.
2. Dies folgt aus der Bemerkung 1.1.6. □

Satz 2.2.2. *Seien K, $\bar{K}$ Körper. Sind $\varphi_1, \ldots, \varphi_n$ verschiedene Monomorphismen $K \to \bar{K}$, so sind $\varphi_1, \ldots, \varphi_n$ linear unabhängig im $\bar{K}$-Vektorraum aller Abbildungen von K in $\bar{K}$.*

Beweis. Induktion nach n.
$n = 1$. Gelte $\bar{\alpha}\varphi_1(x) = 0$ für alle $x \in K$. Dann ist $\bar{\alpha}\varphi_1(1) = \bar{\alpha} \cdot 1 = 0$ und damit $\bar{\alpha} = 0$.
$n > 1$. Seien $\varphi_1, \ldots, \varphi_n$ verschiedene Monomorphismen $K \to \bar{K}$. Gelte

$$\sum_{i=1}^{n} \bar{\alpha}_i \varphi_i(x) = 0 \quad \text{für alle } x \in K. \tag{2.1}$$

Dann gilt für beliebige $y \in K$

$$\sum_{i=1}^{n} \bar{\alpha}_i \varphi_i(y)\varphi_i(x) = 0 \quad \text{nach (2.1) angewandt auf } yx$$
$$\sum_{i=1}^{n} \bar{\alpha}_i \varphi_n(y)\varphi_i(x) = 0 \quad \text{aus (2.1) multipliziert mit } \varphi_n(y).$$

Subtraktion ergibt

$$\sum_{i=1}^{n-1} \bar{\alpha}_i(\varphi_n(y) - \varphi_i(y))\varphi_i(x) = 0.$$

Die Induktionsvoraussetzung liefert

$$\bar{\alpha}_i(\varphi_n(y) - \varphi_i(y)) = 0 \quad \text{für } i = 1, \ldots, n-1.$$

Wähle y so, daß $\varphi_n(y) \neq \varphi_1(y)$; daraus folgt $\bar{\alpha}_1 = 0$. Dann ergibt sich mit (2.1), daß $\sum_{i=2}^{n} \bar{\alpha}_i\varphi_i(x) = 0$ für alle $x \in K$. Nochmalige Anwendung der Induktionsvoraussetzung liefert $\bar{\alpha}_2 = \cdots = \bar{\alpha}_n = 0$. □

Bemerkung. Die Voraussetzungen des Satzes lassen sich wie folgt abschwächen. G sei eine multiplikative Gruppe und $\bar{K}$ ein Körper. Sind $\chi_1, \ldots, \chi_n$ verschiedene Gruppenhomomorphismen $G \to \bar{K}^*$ (sog. *Charaktere*), so sind $\chi_1, \ldots, \chi_n$ linear unabhängig im $\bar{K}$-Vektorraum aller Abbildungen von G in $\bar{K}$. Dies beweist man wie eben.

Satz 2.2.3. *Seien K und $\bar{K}$ Körper, $\varphi_1, \ldots, \varphi_n$ verschiedene Monomorphismen $K \to \bar{K}$ und $L := \{\, x \in K \mid \varphi_1(x) = \cdots = \varphi_n(x) \,\}$. Dann gilt:*

1. *L ist Unterkörper von K. (L heißt der* Inzidenzkörper *von $\varphi_1, \ldots, \varphi_n$. Im Fall $K = \bar{K}$ und* id *unter $\varphi_1, \ldots, \varphi_n$ nennt man L* Fixkörper*).*

2. *$[K : L] \geq n$.*

Beweis. 1. Es gilt:

a. $0, 1 \in L$.

b. Seien $x, y \in L$. Dann gilt $\varphi_i(x - y) = \varphi_i(x) - \varphi_i(y) = \varphi_j(x) - \varphi_j(y) = \varphi_j(x - y)$ für beliebige $i, j \in \{1, \ldots, n\}$, also auch $x - y \in L$.

c. Seien $x, y \in L$, $y \neq 0$. Dann gilt $\varphi_i(xy^{-1}) = \varphi_i(x)\varphi_i(y)^{-1} = \varphi_j(x)\varphi_j(y)^{-1} = \varphi_j(xy^{-1})$ für beliebige $i, j \in \{1, \ldots, n\}$, also auch $xy^{-1} \in L$.

Also ist nach dem Unterkörperkriterium 2.1.3 L ein Unterkörper von K.

2. Gezeigt wird, daß kein Erzeugendensystem $y_1, \ldots, y_r$ des L-Vektorraums K existiert der Länge $r < n$. Nehmen wir also an, $y_1, \ldots, y_r$ ist ein solches Erzeugendensystem. Dann gibt es $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$, die nicht alle verschwinden, mit

$$\sum_{i=1}^{n} \bar{\alpha}_i \varphi_i(y_j) = 0 \quad \text{für } j = 1, \ldots, r. \tag{2.2}$$

(lineares Gleichungssystem mit n Unbekannten und $r < n$ Gleichungen). Es genügt zu zeigen

$$\sum_{i=1}^{n} \bar{\alpha}_i \varphi_i(x) = 0 \quad \text{für alle } x \in K,$$

denn dies wäre ein Widerspruch zur linearen Unabhängigkeit von $\varphi_1, \ldots, \varphi_n$. Sei also $x \in K$. Da $y_1, \ldots, y_r$ Erzeugendensystem ist, gilt

$$x = \sum_{j=1}^{r} \beta_j y_j \quad \text{mit } \beta_j \in L.$$

Man erhält

$$\begin{aligned}
\sum_{i=1}^{n} \bar{\alpha}_i \varphi_i(x) &= \sum_i \bar{\alpha}_i \varphi_i\Big(\sum_j \beta_j y_j\Big) \\
&= \sum_{i,j} \bar{\alpha}_i \varphi_i(\beta_j) \varphi_i(y_j) \\
&= \sum_{i,j} \bar{\alpha}_i \varphi_j(\beta_j) \varphi_i(y_j) && \text{da } \varphi_i(\beta_j) = \varphi_j(\beta_j) \text{ wegen } \beta_j \in L \\
&= \sum_j \varphi_j(\beta_j) \sum_i \bar{\alpha}_i \varphi_i(y_j) \\
&= 0 && \text{wegen (2.2).}
\end{aligned}$$

□

Wir zeigen jetzt, daß im Spezialfall $K = \bar{K}$ und $\{\varphi_1, \ldots, \varphi_n\}$ Untergruppe der *Automorphismengruppe*

$$\mathsf{Aut}(K) := \{\, \varphi\colon K \to K \mid \varphi \text{ Automorphismus} \,\}$$

von K für den Fixkörper L von $\{\varphi_1, \ldots, \varphi_n\}$ sogar die Gleichheit gilt, also $[K : L] = n$.

Bevor wir dies beweisen, soll zunächst die Stelle isoliert werden, an der eingeht, daß G eine Gruppe ist.

Definition 2.2.4. Sei K ein Körper und G eine endliche Untergruppe von $\mathsf{Aut}(K)$. Dann heißt die Abbildung

$$\begin{aligned} \mathsf{sp}_G \colon K &\to K \\ x &\mapsto \sum_{\varphi \in G} \varphi(x) \end{aligned}$$

die G-*Spur* in K.

Lemma 2.2.5. *Sei K ein Körper, G eine endliche Untergruppe von $\mathsf{Aut}(K)$ und L der Fixkörper von G. Dann gilt*

$$\{0\} \neq \mathsf{sp}_G(K) \subseteq L.$$

Beweis. 1. Annahme: $\{0\} = \mathsf{sp}_G(K)$. Dann gilt $0 = \sum_{\varphi \in K} \varphi(x)$ für alle $x \in K$, im Widerspruch zur linearen Unabhängigkeit der Automorphismen aus G (siehe Satz 2.2.2).

2. Seien $\sum_{\varphi \in G} \varphi(x)$ mit $x \in K$ und $\psi \in G$ gegeben. Zu zeigen ist

$$\psi\Big(\sum_{\varphi \in G} \varphi(x)\Big) = \sum_{\varphi \in G} \varphi(x),$$

also

$$\sum_{\varphi \in G} (\psi \circ \varphi)(x) = \sum_{\varphi \in G} \varphi(x).$$

Dies ist aber richtig, da die Abbildung

$$\begin{aligned} G &\to G \\ \varphi &\mapsto \psi \circ \varphi \end{aligned}$$

bijektiv ist. □

Satz 2.2.6. *Sei K ein Körper, G endliche Untergruppe von $\mathsf{Aut}(K)$ und $L = \{\, x \in K \mid \varphi(x) = x$ für alle $\varphi \in G \,\}$ der Fixkörper von G. Dann gilt $[K : L] = |G|$.*

Beweis. Nach Satz 2.2.2 genügt $[K : L] \leq n := |G|$. Seien $y_1, \ldots, y_{n+1} \in K$. Es genügt zu zeigen, daß $y_1, \ldots, y_{n+1}$ linear abhängig über L sind. Es existieren $x_1, \ldots, x_{n+1} \in L$, die nicht alle verschwinden, mit

$$\sum_{i=1}^{n+1} x_i \varphi^{-1}(y_i) = 0 \quad \text{für jedes } \varphi \in G.$$

(lineares Gleichungssystem mit $n+1$ Unbekannten und n Gleichungen). Sei etwa $x_l \neq 0$. Wähle $w \in K$ mit $\mathsf{sp}_G(w) \neq 0$ (möglich nach Lemma vorher). Setze $z_i := \frac{w}{x_l} x_i$ für $i = 1, \ldots, n+1$. Dann gilt

$$\begin{aligned}
&\sum_{i=1}^{n+1} z_i \varphi^{-1}(y_i) = 0 && \text{für jedes } \varphi \in G \\
&\sum_i \varphi(z_i) y_i = 0 && \text{für jedes } \varphi \in G \\
&\sum_{\varphi \in G} \sum_i \varphi(z_i) y_i = 0 \\
&\sum_i \Big(\sum_{\varphi \in G} \varphi(z_i) \Big) y_i = 0 \\
&\sum_i \mathsf{sp}_G(z_i) y_i = 0.
\end{aligned}$$

Nun ist $\mathsf{sp}_G(z_l) = \mathsf{sp}_G(w) \neq 0$, und nach dem vorangehenden Lemma $\mathsf{sp}_G(z_i) \in L$ für alle $i \in \{1, \ldots, n+1\}$. □

2.3 Die Galoisgruppe, galoissche Erweiterungen

Definition 2.3.1. Sei $K \supseteq k$ eine Körpererweiterung und

$$\Gamma_k^K := \{ \varphi \in \mathsf{Aut}(K) \mid \varphi(x) = x \text{ für alle } x \in k \}.$$

Die Gruppe $(\Gamma_k^K, \circ)$ heißt die *Galoisgruppe* der Körpererweiterung $K \supseteq k$. Die Körpererweiterung $K \supseteq k$ heißt *galoissch*, wenn Γ_k^K endlich ist und

$$k = \mathsf{FK}(\Gamma_k^K) := \{ x \in K \mid \varphi(x) = x \text{ für alle } \varphi \in \Gamma_k^K \} \quad (= \text{Fixkörper von } \Gamma_k^K).$$

Man sagt in diesem Fall, daß K ist *galoissch* über k ist.

Mit dieser Begrifflichkeit läßt sich der letzte Satz 2.2.6 des vorangehenden Abschnitts besonders prägnant formulieren.

Satz 2.3.2. *Sei $K \supseteq k$ eine Körpererweiterung und Γ_k^K endlich. Dann gilt*

$$K \text{ ist galoissch über } k \text{ genau dann, wenn } [K:k] = |\Gamma_k^K|.$$

Beweis. Sei $K \supseteq k$ eine Körpererweiterung und Γ_k^K endlich.

$\Longrightarrow$. K ist galoissch über k, d.h. $k = \mathsf{FK}(\Gamma_k^K)$ und damit $[K:k] = |\Gamma_k^K|$ nach Satz 2.2.6.

$\Longleftarrow$. $[K:k]$ ist endlich nach Voraussetzung. Sei $L := \mathsf{FK}(\Gamma_k^K)$ und damit $K \supseteq L \supseteq k$. Nach dem Gradsatz gilt $[K:k] = [K:L] \cdot [L:k]$. Nach Voraussetzung ist $[K:k] = |\Gamma_k^K|$, und nach Satz 2.2.6 gilt $[K:L] = |\Gamma_k^K|$. Damit folgt $[L:k] = 1$ und somit $k = L$, also $k = \mathsf{FK}(\Gamma_k^K)$. Also ist K galoissch über k. □

Lemma 2.3.3. *Sei $K \supseteq k$ eine Körpererweiterung und L ein Zwischenkörper. Dann gilt: Ist $K \supseteq k$ galoissch, so ist auch $K \supseteq L$ galoissch.*

Beweis. Sei $K \supseteq k$ eine galoissche Körpererweiterung. Dann ist Γ_k^K endlich und nach dem vorangehenden Satz $[K:k] = |\Gamma_k^K|$. Nach dem Gradsatz gilt $[K:k] = [K:L]\cdot[L:k]$, und nach Satz von Lagrange ist $|\Gamma_k^K| = |\Gamma_L^K|\cdot[\Gamma_k^K:\Gamma_L^K]$. Es wird nun gezeigt

$$[K:L] \geq |\Gamma_L^K| \tag{2.3}$$

$$[L:k] \geq [\Gamma_k^K:\Gamma_L^K]. \tag{2.4}$$

Aus (2.3) und (2.4) zusammen folgt $[K:L] = |\Gamma_L^K|$, also $K \supseteq L$ galoissch nach Satz 2.3.2.

Zu (2.3). Sei $L' := \mathsf{FK}(\Gamma_L^K)$. Dann gilt $K \supseteq L' \supseteq L$, also

$$[K:L] = [K:L']\cdot[L':L] \geq [K:L'] = |\Gamma_L^K| \quad \text{nach Satz 2.2.6.}$$

Zu (2.4). Γ_k^K denke man sich durch die Untergruppe Γ_L^K in Linksnebenklassen zerlegt. Dann sind folgende Aussagen äquivalent.

$$\begin{aligned}
&\varphi, \psi \text{ sind aus einer Linksnebenklasse}\\
&\psi^{-1}\circ\varphi \in \Gamma_L^K\\
&(\psi^{-1}\circ\varphi)(x) = x \text{ für alle } x \in L\\
&\varphi(x) = \psi(x) \text{ für alle } x \in L\\
&\varphi \text{ und } \psi \text{ stimmen auf } L \text{ überein.}
\end{aligned}$$

Sei nun $\varphi_1, \ldots, \varphi_s$ ein Repräsentantensystem mit $s := [\Gamma_k^K:\Gamma_L^K]$. Betrachte

$$\Omega := \{\varphi_1{\restriction}L, \ldots, \varphi_s{\restriction}L\}.$$

Ω besteht aus s verschiedenen Monomorphismen $L \to K$. Dann ist k der Inzidenzkörper von Ω.

Begründung. $\subseteq$. Klar, da $k = \mathsf{FK}(\Gamma_k^K)$, also insbesondere $\varphi_1(x) = \cdots = \varphi_s(x)$ für alle $x \in k$. $\supseteq$. Sei $x \in L$, $\varphi_1(x) = \cdots = \varphi_s(x)$. Nach dem oben Gezeigten stimmen innerhalb einer Nebenklasse alle Abbildungen auf x überein. Da $\varphi_1, \ldots, \varphi_s$ ein Repräsentantensystem bilden, koinzidiert Γ_k^K auf x. Also gilt $x \in \mathsf{FK}(\Gamma_k^K) = k$.

Satz 2.2.3 liefert nun $[L:k] \geq s = [\Gamma_k^K:\Gamma_L^K]$, also (2.4). □

Satz 2.3.4. *(Hauptsatz der Galoistheorie). Sei $K \supseteq k$ eine Körpererweiterung und K galoissch über k. Dann gilt folgendes.*

1. *Die Zwischenkörper L und die Untergruppen von $U \subseteq \Gamma_k^K$ entsprechen einander eineindeutig vermöge der Zuordnungen*

$$\begin{aligned} L &\mapsto \Gamma_L^K\\ U &\mapsto \mathsf{FK}(U). \end{aligned}$$

Im folgenden sei L ein Zwischenkörper.

2. $[K:L] = |\Gamma_L^K|$ *und* $[L:k] = [\Gamma_k^K:\Gamma_L^K]$.

3. a. *Jeder Monomorphismus von L in einen Erweiterungskörper $K' \supseteq K$, welcher k elementweise festläßt, kann durch Einschränkung eines $\varphi \in \Gamma_k^K$ erhalten werden (hat also insbesondere sein Bild in K).*

b. *Genau die Elemente einer Nebenklasse von* Γ_L^K *in* Γ_k^K *liefern denselben (k elementweise festlassenden) Monomorphismus* $L \to K$.

c. *Weiter gilt für alle* $\varphi \in \Gamma_k^K$

$$\Gamma_{\varphi(L)}^K = \varphi \circ \Gamma_L^K \circ \varphi^{-1}.$$

4. *Folgende Bedingungen sind äquivalent.*

a. L *ist galoissch über* k.

b. $\varphi(L) = L$ *für alle* $\varphi \in \Gamma_k^K$.

c. Γ_L^K *ist Normalteiler in* Γ_k^K.

Falls eine der Bedingungen erfüllt ist (und damit alle), gilt $\Gamma_k^K / \Gamma_L^K \cong \Gamma_k^L$.

Beweis. 1. Es ist zu zeigen, daß beide Abbildungen zueinander invers sind.

a. Sei L Zwischenkörper. Da $K \supseteq L$ galoissch ist nach Lemma 2.3.3, gilt $\mathsf{FK}(\Gamma_L^K) = L$.

b. Sei $U \subseteq \Gamma_k^K$ Untergruppe und $L := \mathsf{FK}(U)$. Zu zeigen ist $\Gamma_L^K = U$. Es gilt

$$\begin{array}{ll} [K:L] = |U| & \text{nach Satz 2.2.6} \\ [K:L] = |\Gamma_L^K| & \text{da } K \supseteq L \text{ galoissch} \\ U \subseteq \Gamma_L^K & \text{wegen } L = \mathsf{FK}(U). \end{array}$$

Da beide Mengen endlich sind, folgt $\Gamma_L^K = U$.

2. Dies wurde im Beweis des Lemmas 2.3.3 gezeigt.

3a. Sei Ω die im Beweis von Lemma 2.3.3 definierte Menge von Monomorphismen $L \to K$. Sei $K' \supseteq K$ eine Körpererweiterung, Θ die Menge aller Monomorphismen $L \to K'$, die k elementweise festlassen, und k' der Inzidenzkörper von Θ. Es gilt

$$\begin{array}{ll} [L:k] = |\Omega| & \text{nach dem Beweis des Lemmas 2.3.3} \\ [L:k] \geq [L:k'] \geq |\Theta| & \text{nach dem Gradsatz bzw. Satz 2.2.3} \\ \Omega \subseteq \Theta & \text{da } K \subseteq K' \text{ und } k \subseteq k' \subseteq L. \end{array}$$

Also ist $|\Omega| \geq |\Theta|$ und daher $\Omega = \Theta$.

b. Siehe Beweis zu Lemma 2.3.3.

c. Sei $\varphi \in \Gamma_k^K$. Dann sind folgende Aussagen äquivalent.

$$\begin{array}{ll} \psi \in \Gamma_{\varphi(L)}^K & \\ \psi(\varphi(x)) = \varphi(x) & \text{für alle } x \in L \\ (\varphi^{-1} \circ \psi \circ \varphi)(x) = x & \text{für alle } x \in L \\ \varphi^{-1} \circ \psi \circ \varphi \in \Gamma_L^K & \\ \psi \in \varphi \circ \Gamma_L^K \circ \varphi^{-1}. & \end{array}$$

4. Folgende Aussagen sind äquivalent.

Γ^K_L ist Normalteiler in Γ^K_k		
$\Gamma^K_L = \varphi \circ \Gamma^K_L \circ \varphi^{-1}$	für alle $\varphi \in \Gamma^K_k$	
$\Gamma^K_L = \Gamma^K_{\varphi(L)}$	für alle $\varphi \in \Gamma^K_k$ (nach 3.)	
$L = \varphi(L)$	für alle $\varphi \in \Gamma^K_k$ (nach 1.)	
$\Gamma^L_k \supseteq \{\, \psi \mid \psi \colon L \to K \text{ Monom.}, \forall{\in}k\, \psi(x) = x \,\}$	(siehe unten)	(2.5)
$\lvert\Gamma^L_k\rvert = \lvert\{\, \psi \mid \psi \colon L \to K \text{ Monom.}, \forall{\in}k\, \psi(x) = x \,\}\rvert$	da oben $\subseteq$ stets gilt	
$\lvert\Gamma^L_k\rvert = [\Gamma^K_k : \Gamma^K_L]$	nach 3b	
$\lvert\Gamma^L_k\rvert = [L : k]$	nach 2	
$L \supseteq k$ ist galoissch	nach Satz 2.3.2.	

Für den letzten Schluß beachte man, daß Γ^L_k endlich ist nach 3a.

(2.5) sieht man wie folgt. $\Longleftarrow$. Sei $\varphi \in \Gamma^K_k$. Nach Voraussetzung ist $\varphi\restriction L \in \Gamma^L_k$, also $\varphi(L) = L$. $\Longrightarrow$. Die Behauptung folgt aus 3a und der Voraussetzung.

Noch zu zeigen ist, daß aus $L \supseteq k$ galoissch folgt $\Gamma^K_k/\Gamma^K_L \cong \Gamma^L_K$. Betrachte dazu die Abbildung

$$\begin{aligned} h\colon \Gamma^K_k &\to \Gamma^L_k \\ \varphi &\mapsto \varphi\restriction L. \end{aligned}$$

h ist wohldefiniert, da $\varphi(L) = L$ für alle $\varphi \in \Gamma^K_k$. h ist surjektiv nach 3a. Für $\varphi, \psi \in \Gamma^K_k$ gilt $(\varphi \circ \psi)\restriction L = (\varphi\restriction L) \circ (\psi\restriction L)$, also ist h Homomorphismus. Ferner ist $\mathsf{Kern}(h) = \Gamma^K_L$, denn folgende Aussagen sind für beliebige $\varphi \in \Gamma^K_k$ äquivalent.

$$\begin{aligned} &\varphi \in \mathsf{Kern}(h) \\ &\varphi\restriction L = \mathsf{id} \\ &\varphi \in \Gamma^K_L \end{aligned}$$

Der Homomorphiesatz liefert jetzt

$$\Gamma^K_k/\Gamma^K_L \cong \Gamma^L_k. \qquad \square$$

Kapitel 3

Ringe

3.1 Grundbegriffe

Definition 3.1.1. Sei A eine Menge und $+\colon A \times A \to A$, $\cdot\colon A \times A \to A$ Abbildungen. A (oder genauer $(A, +, \cdot)$) heißt *Ring*, wenn gilt

1. $(A, +)$ ist eine abelsche Gruppe.
2. $x(yz) = (xy)z$ für alle $x, y, z \in A$.
3. $x(y + z) = (xy) + (xz)$ und $(x + y)z = (xz) + (yz)$ für alle $x, y, z \in A$.

(Schreibweise wie bei Körpern). A heißt *kommutativ*, wenn $xy = yx$ für alle $x, y \in A$. Ein Element $1 \in A$ heißt *Einselement* von A, wenn für alle $x \in A$ gilt $1x = x1 = x$.

Zur Vereinfachung betrachten wir nur kommutative Ringe mit 1.

Bemerkung. Sei A ein kommutativer Ring mit 1. Dann besitzt A genau ein Einselement. (Beweis: Seien $1, 1^*$ Einselemente. Dann gilt $1 = 1 \cdot 1^* = 1^*$). Ferner gilt für alle $x, y \in A$:

1. $0 \cdot x = 0$
2. $-x = (-1) \cdot x$
3. $(-x) \cdot (-y) = xy$

Dies beweist man wie bei Körpern im Abschnitt 2.1.

Beispiele. 1. $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit 1.
2. Alle Körper sind insbesondere kommutative Ringe mit 1.
3. Sei A ein Ring, X eine nicht-leere Menge. Auf $A^X := \{ f\colon X \to A \mid f \text{ Abbildung} \}$ erklärt man $+, \cdot$ komponentenweise, also durch

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

für alle $x \in A$. Damit wird A^X zu einem kommutativen Ring mit 1. (Einselement ist die Abbildung $X \to A$, $x \mapsto 1$).

4. Sei $(G, +)$ eine abelsche Gruppe und $\mathsf{End}(G)$ die Menge aller Endomorphismen von G. Mit $+$ (übliche Addition) und $\circ$ (Hintereinanderausführung) wird $(\mathsf{End}(G), +, \circ)$ zwar ein Ring mit Einselement id_G, doch i.a. ist die Kommutativität *nicht* gegeben.

5. Auch $\mathbb{R}^{n\times n}$ ist ein Ring mit Einselement E, doch für $n \geq 2$ *nicht* kommutativ.

6. Seien $A_1, \ldots, A_n$ kommutative Ringe mit 1. Auf $A_1 \times \cdots \times A_n$ erkläre man $+, \cdot$ komponentenweise. Damit wird $A_1 \times \cdots \times A_n$ zu einem kommutativen Ring mit 1, dessen Einselement die Spalte aus lauter Einsen ist (*direktes Produkt* von $A_1, \ldots, A_n$).

7. $\{0\}$ ist ein kommutativer Ring mit Einselement 0.

Definition 3.1.2. Sei A ein kommutativer Ring mit 1. A heißt *Integritätsring* (oder *Integritätsbereich*), wenn gilt

1. $1 \neq 0$.
2. A ist nullteilerfrei, d.h. für alle $x, y \in A$ folgt aus $xy = 0$ stets $x = 0$ oder $y = 0$.

Beispiele. 1. Jeder Körper ist ein Integritätsring, ebenso der Ring $\mathbb{Z}$.

2. Sei A ein Integritätsring, X eine Menge mit mindestens zwei Elementen a und b. Dann ist A^X kein Integritätsring, denn betrachtet man die Abbildungen

$$f\colon X \to A, \qquad g\colon X \to A,$$

$$f(x) = \begin{cases} 0, & \text{falls } x = a \\ 1, & \text{falls } x = b \\ 0, & \text{sonst} \end{cases} \qquad g(x) = \begin{cases} 1, & \text{falls } x = a \\ 0, & \text{falls } x = b \\ 0, & \text{sonst} \end{cases}$$

so gilt $f, g \neq 0$, aber $f \cdot g = 0$.

Definition 3.1.3. Sei A ein kommutativer Ring mit 1 und $U \subseteq A$ eine Teilmenge. U heißt *Unterring* mit 1 von A, wenn gilt

1. $U \neq \emptyset$
2. $x + y, xy \in U$ für alle $x, y \in U$
3. U bildet zusammen mit den Abbildungen

$$\begin{aligned} U \times U &\to U \\ (x, y) &\mapsto x + y \end{aligned} \qquad \begin{aligned} U \times U &\to U \\ (x, y) &\mapsto xy \end{aligned}$$

   einen kommutativen Ring mit 1.

Definition 3.1.4. Seien A, B kommutative Ringe mit 1 und $f\colon A \to B$ eine Abbildung. f heißt *Homomorphismus* für Ringe, wenn für alle $x, y \in A$ gilt

1. $f(x + y) = f(x) + f(y)$,
2. $f(xy) = f(x)f(y)$,
3. $f(1) = 1$.

Die Begriffe *Mono-, Iso-, Endo-* und *Automorphismus* erklärt man wie für Gruppen.

Bemerkung 3.1.5. Seien A, B kommutative Ringe mit 1 und $f\colon A \to B$ ein Ringhomomorphismus. Dann gilt

1. Ist U Unterring von A, so ist $f(U)$ Unterring von B, und ist V Unterring von B, so ist $f^{-1}(V)$ Unterring von A.

2. Sei wieder $\mathsf{Kern}(f) := f^{-1}(0)$. Dann ist $\mathsf{Kern}(f) = \{0\}$ genau dann, wenn f injektiv ist.

3. f ist Isomorphismus genau dann, wenn ein Homomorphismus $g\colon B \to A$ existiert mit $g \circ f = \mathsf{id}_A$ und $f \circ g = \mathsf{id}_B$.

Beweis. 1. Nach Bemerkung 1.1.6 sind $f(U)$ bzw. $f^{-1}(V)$ additive Untergruppen. Ferner folgt aus $f(1) = 1$ stets $1 \in f(U)$ bzw. $1 \in f^{-1}(V)$. Seien nun $x, y \in f(U)$. Dann existieren $u, v \in U$ so daß $x = f(u)$ und $y = f(v)$, und es gilt $xy = f(u)f(v) = f(uv) \in f(U)$. Seien $w, z \in f^{-1}(V)$. Dann gilt $f(wz) = f(w)f(z) \in V$, also $wz \in f^{-1}(V)$. Daher sind $f(U)$ und $f^{-1}(V)$ Unterringe von B bzw. A.

2. Dies folgt direkt aus dem Beweis zu Bemerkung 1.1.6(3).

3. $\Longrightarrow$. $g := f^{-1}$ leistet nach Bemerkung 1.1.6(4) das Verlangte. Wegen $f^{-1}(1) = 1$ bleibt nur zu zeigen $f^{-1}(x)f^{-1}(y) = f^{-1}(xy)$ für alle $x, y \in B$. Seien dazu $x, y \in B$ und $x = f(u), y = f(v)$ (wobei $u, v \in A$). Dann gilt

$$f^{-1}(x)f^{-1}(y) = uv = f^{-1}(f(uv)) = f^{-1}(f(u)f(v)) = f^{-1}(xy).$$

$\Longleftarrow$. Klar, da aus der Existenz von g die Bijektivität von f folgt. ◻

Definition 3.1.6. Sei A ein kommutativer Ring mit 1 und $\mathfrak{a} \subseteq A$ eine Teilmenge. $\mathfrak{a}$ heißt *Ideal* von A, wenn gilt

1. $\mathfrak{a}$ ist Untergruppe der additiven Gruppe von A.

2. $A\mathfrak{a} \subseteq \mathfrak{a}$ (wobei $A\mathfrak{a} := \{\, yx \mid y \in A, x \in \mathfrak{a} \,\}$).

Beispiele. Sei A ein kommutativer Ring mit 1.
1. $\{0\}$ und A sind Ideale von A (triviale Ideale).
2. Ist $x \in A$, so ist $Ax := \{\, yx \mid y \in A \,\}$ ein Ideal von A.
3. $\mathfrak{a}$ ist Ideal von $\mathbb{Z}$ genau dann, wenn ein $m \in \mathbb{N}$ existiert mit $\mathfrak{a} = m\mathbb{Z}$.

Beweis zu (3). $\Longleftarrow$. Gilt nach (2). $\Longrightarrow$. $\mathfrak{a}$ ist eine Untergruppe von $(\mathbb{Z}, +)$, also $\mathfrak{a} = m\mathbb{Z}$ nach Lemma 1.2.2. ◻

Bemerkung 3.1.7. 1. Sei A kommutativer Ring mit 1. Dann ist $\mathfrak{a} \subseteq A$ Ideal von A genau dann, wenn $\mathfrak{a}$ Untermodul des A-Moduls A ist.

2. Sei K ein Körper. Dann sind $\{0\}$ und K die einzigen Ideale in K.

3. Seien A, B kommutative Ringe mit 1 und $f\colon A \to B$ Ringhomomorphismus. Dann gilt

a. Wenn $\mathfrak{b} \subseteq B$ Ideal von B ist, so ist auch $f^{-1}(\mathfrak{b})$ Ideal von A.

b. Wenn $\mathfrak{a} \subseteq A$ Ideal von A ist und f surjektiv ist, so ist auch $f(\mathfrak{a})$ Ideal von B.

Beweis. 2. Sei $\mathfrak{b} \neq \{0\}$ ein Ideal in K und $b \in \mathfrak{b}$, $b \neq 0$. Dann gilt $b^{-1} \cdot b = 1 \in \mathfrak{b}$, da $K \cdot \mathfrak{b} \subseteq \mathfrak{b}$. Also ist $K \subseteq \mathfrak{b}$ und damit $K = \mathfrak{b}$.

3. a. Nach Bemerkung 1.1.6 ist $f^{-1}(\mathfrak{b})$ Untergruppe von $(A, +)$. Noch zu zeigen ist $Af^{-1}(\mathfrak{b}) \subseteq f^{-1}(\mathfrak{b})$. Seien dazu $y \in A$ und $x \in A$ mit $f(x) \in \mathfrak{b}$. Dann gilt $f(yx) = f(y)f(x) \in \mathfrak{b}$, da $f(x) \in \mathfrak{b}$ und $\mathfrak{b}$ ein Ideal ist. Damit folgt $yx \in f^{-1}(\mathfrak{b})$.

b. Nach Bemerkung 1.1.6 ist $f(\mathfrak{a})$ Untergruppe von $(B, +)$. Noch zu zeigen ist $Bf(\mathfrak{a}) \subseteq f(\mathfrak{a})$. Seien dazu $x \in \mathfrak{a}$ und $y \in B$. Da f surjektiv ist, existiert ein $z \in A$ mit $f(z) = y$. Dann gilt $yf(x) = f(z)f(x) = f(zx) \in f(\mathfrak{a})$, da $zx \in \mathfrak{a}$. □

Im Spezialfall $\mathfrak{b} = \{0\}$ ergibt sich aus (3a), daß $\mathsf{Kern}(f)$ Ideal von A ist. Es soll jetzt die Umkehrung gezeigt werden, also daß jedes Ideal Kern eines Ringhomomorphismus ist.

Satz 3.1.8. *(Konstruktion des Restklassenrings). Sei A ein kommutativer Ring mit 1 und $\mathfrak{a} \subseteq A$ ein Ideal. Definiere $A/\mathfrak{a} := \{\, x + \mathfrak{a} \mid x \in A \,\}$ und*

$$\begin{aligned} \mathsf{kan}\colon A &\to A/\mathfrak{a}, \\ x &\mapsto x + \mathfrak{a}. \end{aligned}$$

Dann gibt es auf $A/\mathfrak{a}$ genau eine Struktur eines kommutativen Rings mit 1, so daß kan Ringhomomorphismus wird. In diesem Fall ist $\mathsf{Kern}(\mathsf{kan}) = \mathfrak{a}$.

Beweis. Existenz. $(A/\mathfrak{a}, +)$ ist nach Satz 1.3.3 eine abelsche Gruppe; + bedeutet die Komplexaddition, für die offenbar gilt $(x+\mathfrak{a})+(y+\mathfrak{a}) = (x+y)+\mathfrak{a}$. Definiere

$$\begin{aligned} \cdot\colon A/\mathfrak{a} \times A/\mathfrak{a} &\to A/\mathfrak{a}, \\ (x + \mathfrak{a}) \cdot (y + \mathfrak{a}) &= xy + \mathfrak{a}. \end{aligned}$$

$\cdot$ ist wohldefiniert: Seien $x + \mathfrak{a} = x' + \mathfrak{a}$ und $y + \mathfrak{a} = y' + \mathfrak{a}$, also $x - x' \in \mathfrak{a}$ und $y - y' \in \mathfrak{a}$. Dann folgt

$$xy - x'y' = xy - x'y + x'y - x'y' = \underbrace{(x - x')}_{\in\mathfrak{a}} y + x' \underbrace{(y - y')}_{\in\mathfrak{a}} \in \mathfrak{a},$$

also $xy+\mathfrak{a} = x'y'+\mathfrak{a}$. Offenbar gelten Assoziativ- und Kommutativgesetz. Es ist $(1+\mathfrak{a})(x+\mathfrak{a}) = x+\mathfrak{a}$, also ist $1+\mathfrak{a}$ Einselement. Ferner gilt das Distributivgesetz

$$\begin{aligned} (x + \mathfrak{a})[(y + \mathfrak{a}) + (z + \mathfrak{a})] &= (x + \mathfrak{a})[(y + z) + \mathfrak{a}] \\ &= x(y + z) + \mathfrak{a} \\ &= xy + xz + \mathfrak{a} \\ &= (xy + \mathfrak{a}) + (xz + \mathfrak{a}) \\ &= (x + \mathfrak{a})(y + \mathfrak{a}) + (x + \mathfrak{a})(z + \mathfrak{a}). \end{aligned}$$

Eindeutigkeit. Für + ist dies klar nach Satz 1.3.3. Eine Verknüpfung $\circ$ aus $A/\mathfrak{a}$, bzgl. der kan ein Ringhomomorphismus ist, muß die Bedingung $(x + \mathfrak{a}) \circ (y + \mathfrak{a}) = xy + \mathfrak{a} = (x + \mathfrak{a})(y + \mathfrak{a})$ erfüllen. Ferner ist $\mathsf{Kern}(\mathsf{kan}) = \mathfrak{a}$, da $0 + \mathfrak{a}$ Nullelement von $A/\mathfrak{a}$. □

Folgerung 3.1.9. *Sei A ein kommutativer Ring mit 1 und $\mathfrak{a} \subseteq A$ Teilmenge. $\mathfrak{a}$ ist Ideal genau dann, wenn $\mathfrak{a}$ Kern eines Ringhomomorphismus $f\colon A \to B$ ist.*

Beweis. Dies folgt aus Bemerkung 3.1.7 und Satz 3.1.8. ◻

Satz 3.1.10. *(Universelle Eigenschaft des Restklassenrings). Sind A, B kommutative Ringe mit 1, $f: A \to B$ ein Ringhomomorphismus und $\mathfrak{a} \subseteq A$ ein Ideal mit $\mathfrak{a} \subseteq \mathsf{Kern}(f)$, so gibt es genau einen Ringhomomorphismus $g: A/\mathfrak{a} \to B$ mit $g \circ \mathsf{kan} = f$.*

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\mathsf{kan}"'] & & B \\ & A/\mathfrak{a} \arrow[ur, "g"'] & \end{tikzcd}$$

Beweis. Es ist nur noch zu zeigen, daß der nach Satz 1.3.5 eindeutig bestimmte Gruppenhomomorphismus g auch ein Ringhomomorphismus ist. Dies sieht man wie folgt.

$$\begin{aligned} g((x+\mathfrak{a})(y+\mathfrak{a})) &= g(xy+\mathfrak{a}) \\ &= (g \circ \mathsf{kan})(xy) \\ &= f(xy) \\ &= f(x)f(y) \\ &= (g \circ \mathsf{kan})(x) \cdot (g \circ \mathsf{kan})(y) \\ &= g(x+\mathfrak{a}) \cdot g(y+\mathfrak{a}). \end{aligned}$$

Zudem gilt $g(1+\mathfrak{a}) = (g \circ \mathsf{kan})(1) = f(1) = 1$, d.h. g ist Ringhomomorphismus. ◻

Folgerung 3.1.11. *(Homomorphiesatz). Seien A, B kommutative Ringe mit 1, $f: A \to B$ ein surjektiver Ringhomomorphismus und $\mathfrak{a} := \mathsf{Kern}(f)$. Dann gilt $A/\mathfrak{a} \cong B$.*

Beweis. Der nach Satz 3.1.10 existierende Homomorphismus $g: A/\mathfrak{a} \to B$ ist nach dem Homomorphiesatz 1.3.6 für Gruppen bijektiv. ◻

Definition 3.1.12. Sei A ein kommutativer Ring mit 1.

1. Für Ideale $\mathfrak{a}, \mathfrak{b} \subseteq A$ definiert man

$$\begin{aligned} \mathfrak{a}+\mathfrak{b} &:= \{\, x+y \mid x \in \mathfrak{a}, y \in \mathfrak{b} \,\} \\ \mathfrak{a} \cap \mathfrak{b} &:= \{\, x \mid x \in \mathfrak{a}, x \in \mathfrak{b} \,\}. \end{aligned}$$

2. Für eine Teilmenge $M \subseteq A$ sei

$$(M) := \{\, x_1a_1 + \cdots + x_na_n \mid n \geq 0, a_1, \ldots, a_n \in M, x_1, \ldots, x_n \in A \,\}.$$

   Wir schreiben $(a_1, \ldots, a_n)$ für$(\{a_1, \ldots, a_n\})$.

Bemerkung. Unter der Voraussetzung der Definition gilt

1. $\mathfrak{a}+\mathfrak{b}$ und $\mathfrak{a}\cap\mathfrak{b}$ sind Ideale von A.

2. (M) ist das kleinste M umfassende Ideal von A, d.h. es gilt

   a. (M) ist ein Ideal.

   b. $(M)\supseteq M$.

   c. Ist $\mathfrak{a}\supseteq M$ Ideal von A, so gilt $\mathfrak{a}\supseteq(M)$.

3. Für $a,b\in A$ ist $(a)+(b)=(a,b)$.

Beweis. 1. Unter Benützung des Untergruppenkriteriums 1.1.4 läßt sich leicht zeigen, daß $\mathfrak{a}+\mathfrak{b}$ und $\mathfrak{a}\cap\mathfrak{b}$ Untergruppen von $(A,+)$ sind. Seien nun $a\in A$, $w\in\mathfrak{a}+\mathfrak{b}$, $z\in\mathfrak{a}\cap\mathfrak{b}$. Dann existieren $x\in\mathfrak{a}$ und $y\in\mathfrak{b}$ so, daß $w=x+y$ und es gilt $aw=a(x+y)=ax+ay\in\mathfrak{a}+\mathfrak{b}$, da $ax\in\mathfrak{a}$ und $ay\in\mathfrak{b}$ ($\mathfrak{a}$ und $\mathfrak{b}$ sind Ideale), sowie $az\in\mathfrak{a}\cap\mathfrak{b}$, da $az\in\mathfrak{a}$ und $az\in\mathfrak{b}$. Damit folgt, daß $\mathfrak{a}+\mathfrak{b}$ und $\mathfrak{a}\cap\mathfrak{b}$ Ideale von A sind.

2. Wieder folgt nach dem Untergruppenkriterium 1.1.4 sofort, daß (M) Untergruppe von $(A,+)$ ist. Seien $a\in A$ und $x=x_1a_1+\cdots+x_na_n\in(M)$. Dann folgt $ax=(ax_1)a_1+\cdots+(ax_n)a_n\in(M)$, da $ax_i\in A$ für alle i, also ist (M) ein Ideal. $(M)\supseteq M$ ist klar. Sei $\mathfrak{a}\supseteq M$ Ideal von A. Dann folgt $\mathfrak{a}\supseteq AM(:=\{\,yx\mid y\in A,x\in M\,\})$, da $\mathfrak{a}$ Ideal ist, und damit $\mathfrak{a}\supseteq(M)$, da $\mathfrak{a}$ Untergruppe von $(A,+)$ ist.

3. Seien $a,b\in A$. Es gilt $(a)\subseteq(a,b)$ und $(b)\subseteq(a,b)$, also $(a)+(b)\subseteq(a,b)$, da (a,b) Untergruppe von $(A,+)$ ist. Nach (1) ist $(a)+(b)$ ein Ideal und damit $(a)+(b)\supseteq(a,b)$ nach (2). Also gilt $(a)+(b)=(a,b)$. □

Beispiel. Im Ring $\mathbb{Z}$ der ganzen Zahlen betrachten wir die Ideale $(m),(n)$ mit $m,n\neq0$. OBdA können wir $m,n>0$ annehmen. Es gilt

1. $(m)\supseteq(n)$ genau dann, wenn $m|n$ $(:\Longleftrightarrow\exists x{\in}\mathbb{Z}\; mx=n)$.

2. $(m)+(n)=(m,n)=(d)$ für ein eindeutig bestimmtes $d>0$ (vgl. Lemma 1.2.2). (d) ist charakterisiert durch

$$\begin{aligned}&(d)\supseteq(m),(n),\\&\forall a{\in}\mathbb{Z}((a)\supseteq(m),(n)\Longrightarrow(a)\supseteq(d)),\end{aligned}$$

   und d ist charakterisiert durch

$$\begin{aligned}&d|m,n,\\&\forall a{\in}\mathbb{Z}(a|m,n\Longrightarrow a|d),\\&d>0.\end{aligned}$$

   Dieses d nennt man den *größten gemeinsamen Teiler* von m und n und bezeichnet ihn mit $\mathsf{ggT}(m,n)$.

3. $(m)\cap(n)=(v)$ für ein eindeutig bestimmtes $v>0$ (vgl. Lemma 1.2.2). (v) ist charakterisiert durch

$$\begin{aligned}&(m),(n)\supseteq(v),\\&\forall a{\in}\mathbb{Z}((m),(n)\supseteq(a)\Longrightarrow(v)\supseteq(a)),\end{aligned}$$

und v ist charakterisiert durch

$$
\begin{aligned}
&m, n | v, \\
&\forall a {\in} \mathbb{Z} (m, n | a \Longrightarrow v | a), \\
&v > 0.
\end{aligned}
$$

Dieses v nennt man das *kleinste gemeinsame Vielfache* von m und n und bezeichnet es mit $\mathsf{kgV}(m, n)$.

Diese hier für $\mathbb{Z}$ durchgeführte Betrachtung werden wir in Abschnitt 3.3 auf beliebige Hauptidealringe übertragen.

Definition 3.1.13. Sei A ein kommutativer Ring mit 1. Dann heißt $u \in A$ *Einheit*, wenn es ein $v \in A$ gibt mit $vu = 1$. Die Menge der Einheiten von A wird mit A^* bezeichnet.

Bemerkung. Sei A ein kommutativer Ring mit 1. Dann ist $(A^*, \cdot)$ eine Gruppe, die *Einheitengruppe* von A.

Beweis. Dies folgt unmittelbar aus der Gruppendefinition 1.1.1, denn 1 ist neutrales Element von A^* und zu jedem $u \in A^*$ gibt es nach Definition von Einheiten ein inverses Element. $\square$

Beispiele. 1. $\mathbb{Z}^* = \{1, -1\}$.
2. Sei K ein Körper. Dann gilt $K^* = K \setminus \{0\}$. Wie man sieht, ist dies mit der Definition von K^* in 2.1.1 verträglich.

Satz 3.1.14. *Sei A ein Integritätsring und $a, b \in A$. Dann gilt $(a) = (b)$ genau dann, wenn es ein $u \in A^*$ gibt mit $a = ub$.*

Beweis. $\Longrightarrow$. Im Fall $a = b = 0$ ist die Behauptung trivial. Sei also oBdA $a \neq 0$. Wegen $a \in (b)$ gibt es ein $u \in A$ mit $a = ub$. Wegen $b \in (a)$ gibt es ein $v \in A$ mit $b = va$. Also ist $a = uva$ und deshalb $a(1 - uv) = 0$. Da A ein Integritätsring ist und $a \neq 0$, folgt $1 - uv = 0$ und somit $1 = uv$, also $u \in A^*$.
$\Longleftarrow$. Sei $a = ub$ mit $u \in A^*$. Es gilt $(a) = Aa = Aub \subseteq Ab = (b)$ und damit $(a) \subseteq (b)$. Analog hat man $(b) \subseteq (a)$, da $b = u^{-1}a$. $\square$

Definition 3.1.15. Für $n > 0$ sei $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$. (Die in Abschnitt 1.2 ebenso bezeichnete Gruppe ist offenbar mit der hier definierten isomorph). Die Einheitengruppe $\mathbb{Z}_n^*$ von $\mathbb{Z}_n$ nennt man die *Gruppe der primen Restklassen modulo n*. Durch $\varphi(n) :=$Anzahl der zu n teilerfremden $m \in \{1, \ldots, n-1\}$ (d.h. für die gilt $\mathsf{ggT}(m, n) = 1$) wird die *Eulersche φ-Funktion* definiert.

Die Behandlung der Eulerschen φ-Funktion ordnet sich hier ein, da nach dem folgenden Satz $\varphi(n) = |\mathbb{Z}_n^*|$ gilt.

Satz 3.1.16. *Sei $n > 0$. Dann gilt*

1. $\mathbb{Z}_n^* = \{\, m + n\mathbb{Z} \mid m \in \{1, \ldots, n-1\}$ *und m, n teilerfremd*$\}$.
2. $|\mathbb{Z}_n^*| = \varphi(n)$.
3. *Sei noch $m > 0$ und m, n teilerfremd. Dann ist $\varphi(mn) = \varphi(m)\varphi(n)$.*
4. $\varphi(p^r) = p^{r-1}(p-1)$ *für p Primzahl und $r > 0$.*

Beweis. 1. Sei $m \in \{1, \ldots, n-1\}$. Dann sind folgende Aussagen äquivalent:

$$\begin{aligned}
&m + n\mathbb{Z} \in \mathbb{Z}_n^* \\
&\exists x{\in}\mathbb{Z}\ (m + n\mathbb{Z})(x + n\mathbb{Z}) = 1 + n\mathbb{Z} \\
&\exists x{\in}\mathbb{Z}\ mx + n\mathbb{Z} = 1 + n\mathbb{Z} \\
&\exists x, y{\in}\mathbb{Z}\ mx + ny = 1 \\
&m\mathbb{Z} + n\mathbb{Z} \ni 1 \\
&m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z} \\
&\mathsf{ggT}(m, n) = 1
\end{aligned}$$

2. Folgt aus (1) nach Definition der Eulerschen φ-Funktion.

3. Seien $n, m > 0$ und teilerfremd. Nach (2) genügt es zu zeigen, daß $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. (Hierbei ist das direkte Produkt von Gruppen gemeint: die Verknüpfung geschieht komponentenweise). Betrachte die Abbildung

$$\begin{aligned}
\mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\
x + mn\mathbb{Z} &\mapsto \begin{pmatrix} x + m\mathbb{Z} \\ x + n\mathbb{Z} \end{pmatrix}
\end{aligned}$$

Die Abbildung ist offenbar wohldefiniert. Sie ist ein Ringhomomorphismus, denn es gilt

$$(x + mn\mathbb{Z}) + (y + mn\mathbb{Z}) \mapsto \begin{pmatrix} x + y + m\mathbb{Z} \\ x + y + n\mathbb{Z} \end{pmatrix} = \begin{pmatrix} x + m\mathbb{Z} \\ x + n\mathbb{Z} \end{pmatrix} + \begin{pmatrix} y + m\mathbb{Z} \\ y + n\mathbb{Z} \end{pmatrix}$$

Dieselbe Rechnung kann man für $\cdot$ durchführen. Ferner gilt

$$1 + mn\mathbb{Z} \mapsto \begin{pmatrix} 1 + m\mathbb{Z} \\ 1 + n\mathbb{Z} \end{pmatrix}$$

Wir zeigen jetzt die Injektivität der Abbildung. Gelte $\binom{x+m\mathbb{Z}}{x+n\mathbb{Z}} = 0$. Dann folgt $x \in m\mathbb{Z}$ und $x \in n\mathbb{Z}$, also $x = mp$ und $x = nq$ für $p, q \in \mathbb{Z}$. Da m, n teilerfremd sind, existieren $y, z \in \mathbb{Z}$ mit $my + nz = 1$, damit auch $mpy + npz = p$, also $xy + npz = p$. Wegen $x = nq$ folgt $n|p$, also $mn|x$ und damit $x \in mn\mathbb{Z}$.

Da beide Mengen mn Elemente haben, ist die Abbildung auch bijektiv.

Damit wissen wir $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, also auch $\mathbb{Z}_{mn}^* \cong (\mathbb{Z}_m \times \mathbb{Z}_n)^*$. Zu zeigen bleibt $(\mathbb{Z}_m \times \mathbb{Z}_n)^* = \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Dies folgt aus der Äquivalenz der folgenden Aussagen.

$$\begin{aligned}
&\begin{pmatrix} x + m\mathbb{Z} \\ y + n\mathbb{Z} \end{pmatrix} \in (\mathbb{Z}_m \times \mathbb{Z}_n)^* \\
&\begin{pmatrix} x + m\mathbb{Z} \\ y + n\mathbb{Z} \end{pmatrix} \cdot \begin{pmatrix} x' + m\mathbb{Z} \\ y' + n\mathbb{Z} \end{pmatrix} = \begin{pmatrix} 1 + m\mathbb{Z} \\ 1 + n\mathbb{Z} \end{pmatrix} \quad \text{für geeignete } x', y' \in \mathbb{Z} \\
&\begin{cases} (x + m\mathbb{Z})(x' + m\mathbb{Z}) = 1 + m\mathbb{Z} & \text{für ein } x' \in \mathbb{Z} \\ (y + n\mathbb{Z})(y' + n\mathbb{Z}) = 1 + n\mathbb{Z} & \text{für ein } y' \in \mathbb{Z} \end{cases} \\
&\begin{cases} x + m\mathbb{Z} \in \mathbb{Z}_m^* \\ y + n\mathbb{Z} \in \mathbb{Z}_n^* \end{cases}
\end{aligned}$$

4. Betrachte
$$0 \dots p \dots 2p \dots lp \dots (l+1)p \dots p^{r-1}p.$$
Es genügt zu zeigen, daß jedes m mit $lp < m < (l+1)p$ zu p teilerfremd ist. (Denn da es genau p^{r-1} Intervalle $\{\, m \mid lp < m < (l+1)p \,\}$ gibt und in jedem $p-1$ Elemente liegen, folgt daraus $\varphi(p^r) = p^{r-1}(p-1)$). Nehmen wir $p|m$ an. Dann folgt $m = kp$ für ein $k \in \mathbb{Z}$ und damit $lp < kp < (l+1)p$; dies ist aber nicht möglich. □

Satz 3.1.17. *(Konstruktion des Quotientenkörpers). Sei A ein Integritätsring.*

1. *Auf $\{\,(x,y) \mid x,y \in A, y \neq 0\,\}$ wird durch $(x,y) \sim (x',y') :\Longleftrightarrow xy' = x'y$ eine Äquivalenzrelation erklärt.*
2. *Bezeichnet man mit $\frac{x}{y}$ die Äquivalenzklasse von (x,y) und mit $Q(A)$ die Menge aller Äquivalenzklassen, so gibt es Abbildungen*
$$\begin{aligned} +\colon Q(A) \times Q(A) &\to Q(A) & \cdot\colon Q(A) \times Q(A) &\to Q(A) \\ \frac{x_1}{y_1} + \frac{x_2}{y_2} &= \frac{x_1y_2 + x_2y_1}{y_1y_2}, & \frac{x_1}{y_1} \cdot \frac{x_2}{y_2} &= \frac{x_1x_2}{y_1y_2} \end{aligned}$$
für alle $x_1, x_2, y_1, y_2 \in A$ mit $y_1, y_2 \neq 0$.
3. *$(Q(A), +, \cdot)$ ist ein Körper; er heißt der* Quotientenkörper *von A.*
4. *Die Abbildung*
$$\begin{aligned} i\colon A &\to Q(A) \\ x &\mapsto \frac{x}{1} \end{aligned}$$
ist ein Ringmonomorphismus.

Beweis. 1. Es genügt, die Transitivität zu zeigen. Sei also $(x,y) \sim (x',y')$ und $(x',y') \sim (x'',y'')$, d.h. $xy' = x'y$ und $x'y'' = x''y'$. Dann folgt $xy'y'' = x'yy'' = x''yy'$ und damit $(xy'' - x''y)y' = 0$, also $xy'' = x''y$, da $y' \neq 0$ und A ein Integritätsring ist. Also gilt $(x,y) \sim (x'',y'')$.

2. Es ist die Wohldefiniertheit zu zeigen. Gelte $x_1y_1' = x_1'y_1$ und $x_2y_2' = x_2'y_2$. Dann folgt
$$\begin{aligned} (x_1y_2 + x_2y_1)y_1'y_2' &= x_1y_2y_1'y_2' + x_2y_1y_1'y_2' \\ &= x_1'y_2y_1y_2' + x_2'y_1y_1'y_2 \\ &= (x_1'y_2' + x_2'y_1')y_1y_2 \end{aligned}$$
und
$$\begin{aligned} (x_1'x_2')y_1y_2 &= x_1'y_1x_2'y_2 \\ &= x_1y_1'x_2y_2' \\ &= (x_1x_2)y_1'y_2'. \end{aligned}$$

3. Man rechnet leicht nach, daß $+$ assoziativ und kommutativ ist. $\frac{0}{1}$ ist neutrales Element, und $\frac{-x}{y}$ ist invers zu $\frac{x}{y}$. Ferner ist $\cdot$ assoziativ und kommutativ. $\frac{1}{1}$ ist neutrales Element, $\frac{1}{1} \neq \frac{0}{1}$; $\frac{y}{x} (x \neq 0)$ ist invers zu $\frac{x}{y}$. Es gelten die Distributivgesetze.

4. i ist ein Ringhomomorphismus mit $\mathsf{Kern}(i) = \{0\}$. □

Beispiele. 1. $\mathbb{Q}$ ist Quotientenkörper von $\mathbb{Z}$.

2. $K(X) := \{\, \frac{f}{g} \mid g \neq 0,\ f, g \in K[X] \,\}$ ist Quotientenkörper von $K[X]$.

Satz 3.1.18. *(Universelle Eigenschaft des Quotientenkörpers). Sei A ein Integritätsring, K ein Körper und $f\colon A \to K$ ein Ringmonomorphismus. Dann gibt es genau einen Körpermonomorphismus $\bar f\colon Q(A) \to K$ mit $\bar f \circ i = f$.*

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "i"'] & & K \\
& Q(A) \arrow[ur, "\bar f"'] &
\end{tikzcd}$$

Beweis. Existenz. Definiere

$$\bar f\colon Q(A) \to K,$$
$$\frac{m}{n} \mapsto \frac{f(m)}{f(n)}.$$

$\bar f$ ist wohldefiniert, denn aus $\frac{m}{n} = \frac{m'}{n'}$ folgt $mn' = m'n$ und somit $f(mn') = f(m'n)$, also

$$\frac{f(m)}{f(n)} = \frac{f(m')}{f(n')}.$$

$\bar f$ ist ein Homomorphismus, denn es gilt für alle $\frac{m}{n}, \frac{m'}{n'} \in Q(A)$

$$\begin{aligned}
\bar f\Big(\frac{m}{n} + \frac{m'}{n'}\Big) &= \bar f\Big(\frac{mn'+m'n}{nn'}\Big) \\
&= \frac{f(mn'+m'n)}{f(nn')} \\
&= \frac{f(m)}{f(n)} + \frac{f(m')}{f(n')} \\
&= \bar f\Big(\frac{m}{n}\Big) + \bar f\Big(\frac{m'}{n'}\Big)
\end{aligned}$$

und

$$\bar f\Big(\frac{m}{n} \cdot \frac{m'}{n'}\Big) = \bar f\Big(\frac{mm'}{nn'}\Big) = \frac{f(mm')}{f(nn')} = \frac{f(m)}{f(n)} \cdot \frac{f(m')}{f(n')} = \bar f\Big(\frac{m}{n}\Big) \cdot \bar f\Big(\frac{m'}{n'}\Big).$$

$\bar f$ ist injektiv, denn $\mathsf{Kern}(\bar f) = \{0\}$ sieht man wie folgt. Sei $\frac{m}{n} \in Q(A)$ mit $\bar f(\frac{m}{n}) = 0$. Dann folgt $\frac{f(m)}{f(n)} = 0$, damit auch $f(m) = 0$ und $m = 0$, also $\frac{m}{n} = 0$.

Eindeutigkeit. Sei $\bar f$ mit $\bar f \circ i = f$ gegeben. Dann gilt für alle $\frac{m}{n} \in Q(A)$

$$\bar f\Big(\frac{m}{n}\Big) = \bar f(i(m)i(n)^{-1}) = \bar f(i(m))\bar f(i(n))^{-1} = f(m)f(n)^{-1} = \frac{f(m)}{f(n)} \qquad \square$$

Bemerkung. Statt von $y \neq 0$ kann man allgemeiner ausgehen von $y \in N$, wobei N eine (feste) multiplikativ abgeschlossene Menge ist. Dann erhält man i.a. jedoch nur einen Quotientenring (s. Kunz, Algebra, Braunschweig 2-te Auflage 1994, §4.V).

3.2 Primideale und maximale Ideale

Im folgenden sei stets A ein kommutativer Ring mit 1.

Definition 3.2.1. Ein Ideal $\mathfrak{p} \subsetneq A$ heißt *Primideal*, wenn für alle $x, y \in A$ gilt

$$\text{Aus } xy \in \mathfrak{p} \text{ folgt } x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}.$$

Beispiel. Sei $A = \mathbb{Z}$, $\mathfrak{p} = p\mathbb{Z}$ mit $p \in \mathbb{N}, p \geq 2$. Dann sind folgende Aussagen äquivalent.

$$\begin{aligned}
&p\mathbb{Z} \text{ Primideal}\\
&\forall x, y{\in}\mathbb{Z}(xy \in p\mathbb{Z} \Longrightarrow x \in p\mathbb{Z} \text{ oder } y \in p\mathbb{Z})\\
&\forall x, y{\in}\mathbb{Z}(p|xy \Longrightarrow p|x \text{ oder } p|y)\\
&p \text{ Primzahl}
\end{aligned}$$

Definition 3.2.2. Ein Ideal $\mathfrak{m} \subsetneq A$ heißt *maximal*, wenn für alle Ideale $\mathfrak{a} \subseteq A$ gilt

$$\text{Aus } \mathfrak{m} \subseteq \mathfrak{a} \subseteq A \text{ folgt } \mathfrak{m} = \mathfrak{a} \text{ oder } \mathfrak{a} = A.$$

Beispiel. Sei $A = \mathbb{Z}$, $\mathfrak{m} = m\mathbb{Z}$ mit $m \in \mathbb{N}$ und $m \geq 2$. Dann sind folgende Aussagen äquivalent.

$$\begin{aligned}
&m\mathbb{Z} \text{ maximal}\\
&\forall n{\in}\mathbb{N}(m\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z} \Longrightarrow m = n \text{ oder } n = 1)\\
&\forall n{\in}\mathbb{N}(n|m \Longrightarrow n = m \text{ oder } n = 1)\\
&m \text{ Primzahl}
\end{aligned}$$

Satz 3.2.3. *1. Sei $\mathfrak{p} \subsetneq A$ ein Ideal. Dann gilt*

$$\mathfrak{p} \textit{ ist Primideal genau dann, wenn } A/\mathfrak{p} \textit{ ein Integritätsring ist.}$$

2. Sei $\mathfrak{m} \subsetneq A$ ein Ideal. Dann gilt

$$\mathfrak{m} \textit{ ist maximal genau dann, wenn } A/\mathfrak{m} \textit{ ein Körper ist.}$$

Beweis. Nach Satz 3.1.8 sind $A/\mathfrak{p}$ und $A/\mathfrak{m}$ kommutative Ringe mit 1.

1. Folgende Aussagen sind äquivalent.

$$\begin{aligned}
&\mathfrak{p} \text{ Primideal}\\
&\forall x, y{\in}A(xy \in \mathfrak{p} \Longrightarrow x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p})\\
&\forall x, y{\in}A(xy + \mathfrak{p} = \mathfrak{p} \Longrightarrow x + \mathfrak{p} = \mathfrak{p} \text{ oder } y + \mathfrak{p} = \mathfrak{p})\\
&\forall x, y{\in}A((x + \mathfrak{p})(y + \mathfrak{p}) = 0 + \mathfrak{p} \Longrightarrow x + \mathfrak{p} = 0 + \mathfrak{p} \text{ oder } y + \mathfrak{p} = 0 + \mathfrak{p})\\
&A/\mathfrak{p} \text{ Integritätsring}
\end{aligned}$$

2. $\Longrightarrow$. Sei $x + \mathfrak{m} \neq \mathfrak{m}$, also $x \notin \mathfrak{m}$. Dann gilt $\mathfrak{m} \subsetneq \mathfrak{m} + Ax$, also $\mathfrak{m} + Ax = A$, da $\mathfrak{m}$ maximal. Es gibt also $y \in A$ und $m \in \mathfrak{m}$ mit $m + yx = 1$. Damit folgt $yx \in 1 + \mathfrak{m}$ und somit $(y + \mathfrak{m})(x + \mathfrak{m}) = yx + \mathfrak{m} = 1 + \mathfrak{m}$. Also existiert zu $x + \mathfrak{m}$ ein inverses Element, und damit ist $A/\mathfrak{m}$ ein Körper.

$\Longleftarrow$. Sei $\mathfrak{a}$ ein Ideal mit $\mathfrak{m} \subsetneq \mathfrak{a} \subseteq A$ und $x \in \mathfrak{a}$, $x \notin \mathfrak{m}$. Dann gilt $x + \mathfrak{m} \neq \mathfrak{m}$. Sei weiterhin $z \in A$ beliebig. Zu zeigen ist $z \in \mathfrak{a}$. Da nach Voraussetzung $A/\mathfrak{m}$ ein Körper ist, existiert ein $y \in A$ mit $(y + \mathfrak{m})(x + \mathfrak{m}) = yx + \mathfrak{m} = z + \mathfrak{m}$. Also existiert ein $m \in \mathfrak{m}$ mit $yx + m = z$. Da $x \in \mathfrak{a}$ und $\mathfrak{a}$ Ideal ist, gilt $yx \in \mathfrak{a}$, also auch $z = yx + m \in \mathfrak{a}$. □

Folgerung 3.2.4. *Sei $\mathfrak{a} \subsetneq A$ ein Ideal. Dann gilt*

Ist $\mathfrak{a}$ maximal, so ist $\mathfrak{a}$ Primideal.

Beweis. $\mathfrak{a}$ ist maximal genau dann, wenn $A/\mathfrak{a}$ Körper ist. Also ist $A/\mathfrak{a}$ auch Integritätsring und demnach $\mathfrak{a}$ Primideal. □

Bemerkung. Die Umkehrung gilt im allgemeinen nicht. *Gegenbeispiel*: $\mathbb{Z}[X] :=$ Menge aller Polynome über $\mathbb{Z}$ in einer Unbekannten X. $\mathbb{Z}[X]$ ist ein kommutativer Ring mit 1. Betrachte das Ideal

$$(X) = \{\, a_n X^n + \cdots + a_1 X \mid n \geq 0, a_n, \ldots, a_1 \in \mathbb{Z} \,\}.$$

(X) ist ein Primideal: Seien $f, g \in \mathbb{Z}[X]$ und $f \cdot g \in (X)$, also

$$f \cdot g = (a_n X^n + \cdots + a_1 X + a_0)(b_m X^m + \cdots + b_1 X + b_0) \in (X).$$

Damit folgt $a_0 b_0 = 0$, also $a_0 = 0$ oder $b_0 = 0$ und somit $f \in (X)$ oder $g \in (X)$.

(X) ist aber nicht maximal, denn $(X) \subsetneq (X, 2) \subsetneq \mathbb{Z}[X]$, wobei

$$(X, 2) = \{\, a_n X^n + \cdots + a_1 X + 2a_0 \mid n \geq 0, a_n, \ldots, a_0 \in \mathbb{Z} \,\}.$$

Folgerung 3.2.5. *Sei p eine Primzahl. Nach Beispiel 3.2 ist $p\mathbb{Z}$ maximal, also gilt nach Satz 3.2.3, daß $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ ein Körper ist.* □

Definition 3.2.6. (Charakteristik eines Körpers). Sei K ein Körper. Betrachte

$$\begin{aligned} f \colon \mathbb{Z} &\to K \\ n &\mapsto n \cdot 1. \end{aligned}$$

f ist ein Ringhomomorphismus, und da $\mathsf{Kern}(f)$ ein Ideal in $\mathbb{Z}$ ist, existiert ein $p \geq 0$ mit $\mathsf{Kern}(f) = p\mathbb{Z}$. Die natürliche Zahl p heißt *Charakteristik* von K. Es gilt $p \neq 1$, da $0 \neq 1$ in K.

Wir wollen jetzt die verbleibenden Möglichkeiten für p diskutieren.

Fall $p = 0$. Dann gilt $\mathsf{Kern}(f) = \{0\}$; also ist f injektiv. Betrachte

$$\begin{aligned} \bar{f} \colon \mathbb{Q} &\to K \\ \frac{m}{n} &\mapsto \frac{m \cdot 1}{n \cdot 1}. \end{aligned}$$

$\bar{f}$ ist Monomorphismus, und $P := \bar{f}(\mathbb{Q}) \cong \mathbb{Q}$ ist der kleinste Unterkörper von K. Er heißt *Primkörper* von K.

Fall $p > 1$. $A := f(\mathbb{Z})$ ist Unterring von K, also Integritätsring, da K Körper ist. Der Homomorphiesatz liefert $\mathbb{Z}/p\mathbb{Z} \cong A$. Damit ist $p\mathbb{Z}$ Primideal (nach Satz 3.2.3), also p Primzahl. Folglich ist $\mathbb{Z}_p$ Körper, also ist auch A ein Körper. $P := A \cong \mathbb{Z}_p$ ist der kleinste Unterkörper von K. Er heißt wieder *Primkörper* von K.

3.3 Hauptidealringe

Definition 3.3.1. Sei A ein kommutativer Ring mit 1.

1. Ein Ideal $\mathfrak{a} \subseteq A$ heißt *Hauptideal*, wenn $\mathfrak{a} = (a)$ für ein $a \in A$.

2. A heißt *Hauptidealring*, wenn A Integritätsring ist und jedes Ideal von A ein Hauptideal ist.

Beispiele. 1. $\mathbb{Z}$ ist ein Hauptidealring, da jedes Ideal in $\mathbb{Z}$ die Gestalt $m\mathbb{Z}$ hat (vgl. Lemma 1.2.2).
2. $K[X]$ ist Hauptidealring für jeden Körper K (siehe Abschnitt 3.4).

Satz 3.3.2. *Sei A Hauptidealring, $a \in A$, $a \neq 0$ und a keine Einheit. Dann gilt*

(a) ist maximales Ideal genau dann, wenn (a) Primideal ist.

Beweis. $\Longrightarrow$. Siehe Folgerung 3.2.4.
$\Longleftarrow$. Gelte $(a) \subseteq (b) \subseteq A$ mit $b \in A$. Dann gilt $a \in (b)$, also existiert ein $x \in A$ mit $a = xb$. Es gilt $xb \in (a)$. Da (a) Primideal, folgt $x \in (a)$ oder $b \in (a)$.
Fall $x \in (a)$. Dann existiert $y \in A$ mit $x = ay$, d.h. $a = ayb$ und somit $a(1 - yb) = 0$. Damit folgt $yb = 1$, da $a \neq 0$ und A Integritätsring. Somit ist b Einheit, also $(b) = A$.
Fall $b \in (a)$. Dann gilt $(b) \subseteq (a)$, also $(b) = (a)$.
Insgesamt folgt, daß (a) maximales Ideal ist. □

Definition 3.3.3. Sei A ein Integritätsring. Ein $a \in A$ heißt *irreduzibel*, wenn $a \neq 0$ und keine Einheit ist und für alle $x, y \in A$ gilt

Aus $a = xy$ folgt, daß x Einheit ist oder y Einheit ist.

(d.h. a besitzt nur "triviale Zerlegungen").

Bemerkung 3.3.4. Sei A ein Integritätsring.

1. Dann gilt für alle $a \in A$: ist a irreduzibel und u Einheit, so ist ua irreduzibel.

2. Definiere für $x, y \in A$
$$x \sim y :\Leftrightarrow \exists u \in A^* \; x = uy.$$
Dann ist $\sim$ eine Äquivalenzrelation auf A; man nennt x und y *assoziiert*.

Teil (1) besagt, daß "irreduzibel" verträglich mit $\sim$ ist.

Satz 3.3.5. *Sei A ein Integritätsring, $a \in A$, $a \neq 0$ und a keine Einheit. Dann gilt*

Ist (a) Primideal, so ist a irreduzibel.

Beweis. Gelte $a = xy$, also $xy \in (a)$. Dann gilt $x \in (a)$ oder $y \in (a)$, da (a) Primideal.
Fall $x \in (a)$. Dann existiert ein $z \in A$ mit $x = az$, also $x = xyz$ und somit $yz = 1$, da $x \neq 0$ wegen $a \neq 0$ und A Integritätsring. Also ist y Einheit.
Fall $y \in (a)$. Man zeigt dann genauso, daß x Einheit ist.
Insgesamt ergibt sich, daß a irreduzibel ist. □

Unser nächstes Ziel ist die Formulierung von Bedingungen, unter denen eine Umkehrung dieses Satzes möglich ist.

Definition 3.3.6. Sei A ein Integritätsring.

1. Ein $a \in A$, $a \neq 0$, heißt *eindeutig zerlegbar in irreduzible Elemente*, wenn a eine Darstellung $a = up_1 \dots p_r$ besitzt mit einer Einheit $u \in A$ und irreduziblen Elementen $p_1, \dots, p_r \in A$, und wenn für je zwei solche Darstellungen $a = up_1 \dots p_r = vq_1 \dots q_s$ gilt $r = s$ und (evtl. nach Umnumerierung) $p_i = u_i q_i$ mit u_i Einheit $(i = 1, \dots r)$.

2. A heißt *faktoriell*, wenn jedes $a \in A$, $a \neq 0$ eindeutig zerlegbar in irreduzible Elemente ist.

Satz 3.3.7. *Sei A faktoriell, $a \in A$, $a \neq 0$ und a keine Einheit. Dann gilt*

$$(a) \text{ ist Primideal genau dann, wenn } a \text{ irreduzibel ist.}$$

Beweis. $\Longrightarrow$. Siehe Satz 3.3.5.

$\Longleftarrow$. Gelte $xy \in (a)$, d.h. $xy = az$ für ein $z \in A$. Betrachte die Zerlegungen von x und y in irreduzible Elemente. OBdA kommt a in der Zerlegung von x vor. Dann gilt $x \in (a)$. □

Wir wollen jetzt zeigen, daß jeder Hauptidealring faktoriell ist. Dazu wird zunächst der Begriff eines größten gemeinsamen Teilers auf beliebige kommutative Ringe mit 1 erweitert.

Definition 3.3.8. Sei A ein kommutativer Ring mit 1 und $a, b \in A$.

1. $a|b$ (gelesen *a teilt b*) gelte genau dann, wenn es ein $x \in A$ gibt mit $ax = b$.

2. Ein $d \in A$ heißt ein *größter gemeinsamer Teiler* von a und b, wenn gilt

$$\begin{aligned} &d|a, b, \\ &\forall x{\in}A(x|a, b \Longrightarrow x|d). \end{aligned}$$

3. Ein $v \in A$ heißt ein *kleinstes gemeinsames Vielfaches* von a und b, wenn gilt

$$\begin{aligned} &a, b|v, \\ &\forall x{\in}A(a, b|x \Longrightarrow v|x). \end{aligned}$$

Satz 3.3.9. *Sei A ein Hauptidealring und $a, b, d \in A$. Dann gilt $(a, b) = (d)$ genau dann, wenn d ein größter gemeinsamer Teiler von a, b ist.*

Beweis. Folgende Aussagen sind äquivalent.

$$\begin{aligned} &d \text{ ist größter gemeinsamer Teiler von } a, b \\ &\begin{cases} d|a, b \\ \forall x{\in}A(x|a, b \Longrightarrow x|d) \end{cases} \\ &\begin{cases} (d) \supseteq (a), (b) \\ \forall x{\in}A\big((x) \supseteq (a), (b) \Longrightarrow (x) \supseteq (d)\big) \end{cases} \\ &(a, b) = (d), \end{aligned}$$

wobei wir für die letzte Äquivalenz die Definition von (a, b) benutzt haben sowie die Voraussetzung, daß A Hauptidealring ist. □

Satz 3.3.10. *Jeder Hauptidealring ist faktoriell.*

Beweis. Sei A ein Hauptidealring. Gezeigt wird:

1. Es gibt keine unendliche aufsteigende Kette $(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \ldots$ von Idealen in A.

2. Jedes $b \in A$, $b \neq 0$, b keine Einheit, besitzt einen irreduziblen Teiler.

3. Jedes $a \in A$, $a \neq 0$ besitzt eine Zerlegung in irreduzible Elemente.

4. Diese Zerlegung ist eindeutig.

1. Annahme: Es existiert eine solche Kette $(a_1) \subsetneq \cdots \subsetneq (a_n) \subsetneq \ldots$. Dann ist $\bigcup_{n\in\mathbb{N}}(a_n)$ ein Ideal von A, und da A Hauptidealring ist, existiert ein $a \in A$ mit $(a) = \bigcup_{n\in\mathbb{N}}(a_n)$. Es folgt $a \in (a_n)$ für ein $n \in \mathbb{N}$, also $(a_n) \subseteq (a) \subseteq (a_n)$ im Widerspruch dazu, daß die Kette echt aufsteigt.

2. Annahme: Es existiert ein $b = b_0 \in A$, $b_0 \neq 0$ und keine Einheit, das keinen irreduziblen Teiler besitzt. Das bedeutet insbesondere, daß b_0 selbst reduzibel (d.h. nicht irreduzibel) ist. Sei also

$$b_0 = b_1 b_1' \text{ mit } b_1, b_1' \neq 0 \text{ und keine Einheiten.}$$

Nun ist b_1 auch reduzibel, da sonst b einen irreduziblen Teiler hätte, also

$$b_1 = b_2 b_2' \text{ mit } b_2, b_2' \neq 0 \text{ und keine Einheiten.}$$

Induktiv ergibt sich eine Folge b_n mit $(b_0) \subsetneq (b_1) \subsetneq (b_2) \subsetneq \ldots$, was im Widerspruch zu (1) steht. (Es gilt $\subsetneq$, denn aus $(b_{i-1}) = (b_i)$ würde nach Satz 3.1.14 folgen $b_{i-1} = b_i u$ mit $u \in A^*$, also $b_i' = u$ da A Integritätsring ist).

3. Ist $a =: a_0$ eine Einheit oder irreduzibel, so sind wir fertig. Andernfalls existiert nach (2) ein irreduzibler Teiler q_1 von a_0, also

$$a_0 = q_1 a_1.$$

Ist a_1 Einheit oder irreduzibel, so sind wir fertig. Andernfalls existiert nach (2) ein irreduzibler Teiler q_2 von a_1, also

$$a_1 = q_2 a_2.$$

Ist a_2 Einheit oder irreduzibel, so sind wir fertig. Dieses Verfahren setze man fort. Bricht es ab, so sind wir wieder fertig. Andernfalls erhalten wir eine Folge a_n mit $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$, im Widerspruch zu (1).

4. Wir bemerken zunächst, daß für irreduzibles $a \in A$ und beliebige $x, y \in A$ gilt

$$\text{Aus } a|xy \text{ folgt } a|x \text{ oder } a|y.$$

Dies sieht man wie folgt. Sei d ein größter gemeinsamer Teiler von a und x. Dann gilt $d|a$, also $dz = a$ für ein $z \in A$. Da a irreduzibel ist, ist d oder z Einheit.

Fall 1. d ist Einheit; oBdA sei $d = 1$. Dann gilt

$$\begin{aligned} 1 &= ba + cx && \text{für geeignete } b, c \in A \\ y &= bay + cxy && \\ a&|y && \text{da } a|xy. \end{aligned}$$

Fall 2. z ist Einheit. Dann gilt $d \sim a$, also $a|x$.

Nun der Beweis von 4. Gelte $a = p_1 \dots p_r = q_1 \dots q_s$ mit $p_1, \dots, p_r, q_1, \dots, q_s$ irreduzibel. Es gilt $p_1|a$, also $p_1|q_1 \dots q_s$. Nach der Vorbemerkung können wir $p_1|q_1$ annehmen. Dann ist $q_1 = u_1 p_1$ für ein $u_1 \in A^*$ und somit gilt $p_2 \dots p_r = u_1 q_2 \dots q_s$. Induktiv folgt nun die Behauptung. □

Folgerung 3.3.11. *Sei A ein Hauptidealring, $a \in A$, $a \neq 0$ und a keine Einheit. Folgende Aussagen sind äquivalent.*

(a) ist Primideal.

(a) ist maximales Ideal.

a ist irreduzibel. □

Bemerkung 3.3.12. Sei A ein faktorieller Ring. Betrachte die in Bemerkung 3.3.4 definierte Äquivalenzrelation $\sim$ (also $x \sim y$ genau dann, wenn ein $u \in A^*$ existiert mit $x = uy$). Wähle aus jeder Äquivalenzklasse, die ein irreduzibles Element enthält, ein p aus. P sei die Menge dieser p's. Dann gilt

1. Jedes $a \in A$, $a \neq 0$ läßt sich eindeutig darstellen in der Form
$$a = u \prod_{p \in P} p^{\nu_p(a)}$$
mit $\nu_p(a) \in \mathbb{N}$ und $\nu_p(a) = 0$ für fast alle p (d.h. alle bis auf endlich viele).

2. Alle Teilbarkeitseigenschaften lassen sich aus dieser Darstellung ablesen, z.B.:

   $a|b$ genau dann, wenn für alle $p \in P$ gilt $\nu_p(a) \leq \nu_p(b)$.

   d ist ein größter gemeinsamer Teiler von a und b genau dann, wenn für alle $p \in P$ gilt $\nu_p(d) = \min(\nu_p(a), \nu_p(b))$.

   v ist kleinstes gemeinsames Vielfaches von a und b genau dann, wenn für alle $p \in P$ gilt $\nu_p(v) = \max(\nu_p(a), \nu_p(b))$.

Beispiele. 1. $\mathbb{Z}$ mit P = Menge der Primzahlen.

2. $K[X]$ (wobei K Körper) mit P = Menge der irreduziblen Polynome mit Leitkoeffizienten 1; dies werden wir im nächsten Abschnitt beweisen.

3.4 Polynomringe

Wir wollen jetzt den Polynombegriff etwas genauer fassen und Polynome (in einer und mehreren Veränderlichen) über einem beliebigen kommutativen Ring A mit 1 einführen. Es wird sich zeigen, daß man wieder einen Ring erhält, und zwar den sogenannten Polynomring $A[X]$.

Jedem Polynom $f = \sum_{i=0}^n a_i X^i \in A[X]$ kann man eine Abbildung von A nach A zuordnen durch $x \mapsto \sum_{i=0}^n a_i x^i \in A$. Im allgemeinen bestimmt eine solche Abbildung jedoch *nicht* die Koeffizienten. Zum Beispiel für $A = \mathbb{Z}_2$ und $f = X^2 + X$ ist $f(0) = f(1) = 0$, also die zugeordnete Abbildung die Nullabbildung, obwohl die Koeffizienten nicht Null sind. Dies ist ein Grund, Polynome als formale Ausdrücke einzuführen.

Unser Ansatz zu einer genauen Fassung des Polynombegriffs ist es, daß ein formaler Ausdruck $a_n X^n + \dots + a_1 X + a_0$ eindeutig festgelegt ist durch die Folge $(a_0, a_1, \dots, a_n, 0, 0, \dots)$ der Koeffizienten.

Satz 3.4.1. *Sei A ein kommutativer Ring mit 1, $A[X]$ die Menge aller Folgen $(a_0, a_1, \ldots)$ von Elementen aus A, wobei $a_k = 0$ für fast alle $k \in \mathbb{N}$.*

1. *Definiere*

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0{+}b_0, a_1{+}b_1, \ldots)$$
$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (c_0, c_1, c_2, \ldots) \qquad \text{mit } c_k := \textstyle\sum_{i=0}^{k} a_i b_{k-i}.$$

Dann ist $(A[X], +, \cdot)$ ein kommutativer Ring mit Einselement $(1, 0, 0, \ldots)$, der Polynomring *über A in einer Unbestimmten.*

2. *Die Abbildung*

$$\begin{aligned} i\colon A &\to A[X] \\ a &\mapsto (a, 0, 0, \ldots) \end{aligned}$$

ist ein Ringhomomorphismus.

3. *Definiert man $X := (0, 1, 0, 0, \ldots) \in A[X]$ und identifiziert man $a \in A$ mit $i(a) = (a, 0, 0, \ldots) \in A[X]$, so läßt sich jedes $f \in A[X]$ schreiben als*

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{mit } a_i \in A.$$

(Addition und Multiplikation sind hier in $A[X]$ zu verstehen).

4. *Diese Darstellung ist im folgenden Sinn eindeutig. Gilt $\sum_{i=0}^{n} a_i X^i = \sum_{j=0}^{m} b_j X^j$ mit (etwa) $n \leq m$, so folgt $a_k = b_k$ für $0 \leq k \leq n$ und $b_k = 0$ für $n < k \leq m$.*

Beweis. 1. Leicht nachzurechnen: $(A[X], +)$ ist abelsche Gruppe mit neutralem Element $(0, 0, \ldots)$. Inverses Element zu $(a_0, a_1, \ldots)$ ist $(-a_0, -a_1, \ldots)$. Die Verknüpfung $\cdot$ ist assoziativ und kommutativ. Für $(a_0, a_1, \ldots) \in A[X]$ ist $(a_0, a_1, \ldots) \cdot (1, 0, 0, \ldots) = (a_0, a_1, \ldots)$.

3. Setze $X^0 := (1, 0, 0, \ldots)$. Durch Induktion über i sieht man leicht, daß

$$X^i = (\underbrace{0, \ldots, 0}_{i}, 1, 0, 0, \ldots).$$

Es folgt

$$a \cdot X^i = (a, 0, 0, \ldots) \cdot X^i = (\underbrace{0, \ldots, 0}_{i}, a, 0, 0, \ldots).$$

Sei jetzt $a_i = 0$ für $i > n$ und $f = (a_i)_{i \in \mathbb{N}}$. Dann gilt

$$\begin{aligned}(a_0, a_1, \ldots) &= (a_0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots) + \cdots + (0, \ldots, 0, a_n, 0, 0, \ldots) \\ &= \sum_{i=0}^{n} a_i X^i.\end{aligned}$$

Damit ist die Existenz der angegebenen Darstellung von $f \in A[X]$ gezeigt.

4. Die Eindeutigkeit dieser Darstellung folgt mit demselben Argument. $\square$

Bemerkung. Sei A ein kommutativer Ring mit 1 und $A[X]$ der Polynomring über A. Nach der vorigen Definition ist es möglich, A mit seinem Bild $i(A)$ in $A[X]$ zu identifizieren.

Satz 3.4.2. *(Universelle Eigenschaft des Polynomrings). Seien A, B kommutative Ringe mit 1, $A[X]$ der Polynomring über A, ferner $x \in B$ und $\varphi\colon A \to B$ ein Ringhomomorphismus. Dann existiert genau ein Ringhomomorphismus $\bar\varphi\colon A[X] \to B$ mit $\bar\varphi(X) = x$ und $\bar\varphi \circ i = \varphi$.*

$$\begin{tikzcd}
A \arrow[rr, "\varphi"] \arrow[dr, "i"'] & & B \\
& A[X] \arrow[ur, "\bar\varphi"'] &
\end{tikzcd}$$

Beweis. Existenz. Definiere

$$\bar\varphi\colon A[X] \to B$$
$$\bar\varphi\Big(\sum_{i=0}^{n} a_i X^i\Big) = \sum_{i=0}^{n} \varphi(a_i) x^i.$$

$\bar\varphi$ ist Ringhomomorphismus, wie man durch Nachrechnen leicht zeigt.

Eindeutigkeit. Für eine Abbildung $\bar\varphi$ mit den gewünschten Eigenschaften muß gelten

$$\bar\varphi\Big(\sum_{j=0}^{n} a_j X^j\Big) = \sum_{j=0}^{n} \bar\varphi(i(a_j)) \cdot \bar\varphi(X)^j = \sum_{j=0}^{n} \varphi(a_j) x^j. \qquad \square$$

Definition 3.4.3.

$$A[X_1, X_2] := (A[X_1])[X_2]$$
$$A[X_1, \dots, X_{n+1}] := (A[X_1, \dots, X_n])[X_{n+1}]$$

Bemerkung. Zu jedem $f \in A[X_1, \dots, X_n]$, $f \neq 0$ gibt es genau eine endliche Teilmenge $I \subseteq \mathbb{N}^n$ und eindeutig bestimmte $a_{i_1 \dots i_n} \in A \setminus \{0\}$, $(i_1, \dots, i_n) \in I$ mit

$$f = \sum_{(i_1, \dots, i_n) \in I} a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}.$$

Dies zeigt man leicht durch Induktion über n.

Definition 3.4.4. Für jedes $f \in A[X]$ sei der *Grad* definiert durch

$$\mathsf{deg}(f) := \begin{cases} n & \text{falls } f = \sum_{i=0}^{n} a_i X^i,\ a_n \neq 0 \\ -\infty & \text{falls } f = 0 \end{cases}$$

Gilt $f = \sum_{i=0}^{n} a_i X^i$ mit $a_n \neq 0$, so heißt a_n der *Leitkoeffizient* von f. Ein $f \in A[X]$, $f \neq 0$, heißt *normiert* oder *unitär*, wenn der Leitkoeffizient 1 ist.

Bemerkung 3.4.5. Seien $f, g \in A[X]$. Dann gilt

1. $\mathsf{deg}(fg) \leq \mathsf{deg}(f) + \mathsf{deg}(g)$.
2. Ist A Integritätsring, so gilt sogar $\mathsf{deg}(fg) = \mathsf{deg}(f) + \mathsf{deg}(g)$, wenn man $-\infty + n := -\infty$, $-\infty + (-\infty) := -\infty$ definiert.

Beweis. OBdA können wir $f, g \neq 0$ annehmen, denn im Fall $f = 0$ oder $g = 0$ ist $fg = 0$, und damit sind (1) und (2) erfüllt.

Sei $f = a_m X^m + \cdots + a_1 X^1 + a_0$ mit $a_m \neq 0$ und $g = b_n X^n + \cdots + b_1 X^1 + b_0$ mit $b_n \neq 0$. Dann ist $f \cdot g = c_{m+n} X^{m+n} + \cdots + c_1 X^1 + c_0$ mit $c_i = \sum_{k+l=i} a_k b_l$. Damit ist (1) gezeigt. Ist A Integritätsring, so folgt $c_{m+n} = a_m b_n \neq 0$ und damit auch (2). □

Bemerkung. Sei K ein Körper. Dann ist $K[X]^* = K^*$.

Beweis. $\supseteq$ ist klar. $\subseteq$. Sei $f = a_n X^n + \cdots + a_0 \in K[X]^*$ mit $a_n \neq 0$. Dann existiert ein $g \in K[X]$ mit $f \cdot g = 1$. Da K Integritätsring ist, folgt mit der vorigen Bemerkung $\mathsf{deg}(f) = 0$, also $n = 0$ und $a_0 \neq 0$. Da K Körper ist, ist a_0 eine Einheit. □

Satz 3.4.6. *(Division mit Rest). Sei A ein Integritätsring und $f \in A[X]$, etwa $f = a_n X^n + \cdots + a_1 X + a_0$ mit $a_n \neq 0$. $K = Q(A)$ sei der Quotientenkörper von A. Dann gibt es zu jedem $g \in A[X]$ eindeutig bestimmte $q, r \in K[X]$ mit*

$$g = qf + r \quad \textit{und} \quad \mathsf{deg}(r) < \mathsf{deg}(f).$$

Ferner lassen sich q, r darstellen in der Form

$$q = \frac{1}{a_n^k}\bar{q} \quad \textit{und} \quad r = \frac{1}{a_n^k}\bar{r}$$

mit $\bar{q}, \bar{r} \in A[X]$ und $k = \max(0, m - n + 1)$ mit $m := \mathsf{deg}(g)$.

Beweis. Existenz. Zu zeigen ist die Existenz von $\bar{q}, \bar{r} \in A[X]$ mit

$$a_n^k g = \bar{q} f + \bar{r} \quad \text{und} \quad \mathsf{deg}(\bar{r}) < \mathsf{deg}(f).$$

Wir beweisen dies durch Induktion nach m.

Fall $m = 0, n > 0$. Dann ist $k = 0$. Setze $\bar{q} = 0$, $\bar{r} = g$.

Fall $m \geq 0, n = 0$. Dann ist $k = m + 1$. Setze $\bar{q} = a_n^m g$, $\bar{r} = 0$.

Fall $m > 0, n > 0$. OBdA gilt $n \leq m$. (Sonst setze man $\bar{q} = 0$, $\bar{r} = a_n^k g$). Sei b_m der Leitkoeffizient von g. Es gibt ein $g_1 \in A[X]$ mit

$$a_n g = b_m X^{m-n} f + g_1 \quad \text{und} \quad \mathsf{deg}(g_1) < m.$$

Sei $k_1 := \max(0, \mathsf{deg}(g_1) - n + 1)$. Nach Induktionsvoraussetzung gibt es $\bar{q}_1, \bar{r} \in A[X]$ mit

$$a_n^{k_1} g_1 = \bar{q}_1 f + \bar{r} \quad \text{und} \quad \mathsf{deg}(\bar{r}) < n.$$

Man erhält

$$\begin{aligned} a_n^{k_1+1} g &= a_n^{k_1}(b_m X^{m-n} f + g_1) \\ &= a_n^{k_1} b_m X^{m-n} f + \bar{q}_1 f + \bar{r} \\ &= \bar{q} f + \bar{r} \quad \text{mit } \bar{q} := a_n^{k_1} b_m X^{m-n} + \bar{q}_1. \end{aligned}$$

Zu zeigen ist noch $k_1 + 1 \leq k$; dies genügt, denn dann folgt

$$a_n^k g = a_n^{k-(k_1+1)} \bar{q} f + a_n^{k-(k_1+1)} \bar{r}.$$

Wegen $n \leq m$ haben wir $k = m - n + 1$, also wegen $\mathsf{deg}(g_1) < m$ dann $k_1 = \max(0, \mathsf{deg}(g_1) - n + 1) < m - n + 1 = k$, d.h. $k_1 + 1 \leq k$.

Eindeutigkeit. Gelte $g = q_1 f + r_1 = q_2 f + r_2$ mit $\mathsf{deg}(r_i) < \mathsf{deg}(f)$. Dann ist auch $\mathsf{deg}(r_1 - r_2) < \mathsf{deg}(f)$ und $(q_1 - q_2) f = r_2 - r_1$. Bemerkung 3.4.5 liefert $\mathsf{deg}(r_2 - r_1) = \mathsf{deg}(f) + \mathsf{deg}(q_1 - q_2)$, also $\mathsf{deg}(q_1 - q_2) < 0$ und damit $q_1 = q_2$. Dann ist auch $r_1 = r_2$. □

Bemerkung. Wenn man im Satz voraussetzt, daß

- A kommutativer Ring mit 1 und f normiert ist, oder
- A ein Körper ist,

so gibt es zu jedem $g \in A[X]$ sogar eindeutig bestimmte $q, r \in A[X]$ mit $g = qf + r$ und $\mathsf{deg}(r) < \mathsf{deg}(f)$.

Satz 3.4.7. *Sei K ein Körper. Dann ist $K[X]$ Hauptidealring.*

Beweis. Nach Bemerkung 3.4.5 ist $K[X]$ ein Integritätsring. Sei $\mathfrak{a} \subseteq K[X]$ ein Ideal; oBdA $\mathfrak{a} \neq 0$. Sei $f \in \mathfrak{a}$ von minimalem Grad ≥ 0 und $g \in \mathfrak{a}$ beliebig, $g \neq 0$. Nach Satz 3.4.6 gibt es $q, r \in K[X]$ mit $g = qf + r$ und $\mathsf{deg}(r) < \mathsf{deg}(f)$. Es ist $r = g - qf \in \mathfrak{a}$, also $r = 0$ und damit $\mathfrak{a} = (f)$. □

Folgerung. *Sei K ein Körper. Dann ist $K[X]$ faktoriell.* □

Bemerkung 3.4.8. (Euklidischer Algorithmus). Sei K ein Körper und $f_0, f_1 \in K[X]$. Ein $d \in K[X]$ ist nach Satz 3.3.9 ein größter gemeinsamer Teiler von f_0, f_1 genau dann, wenn $(d) = (f_0, f_1)$.

Konstruktion eines größten gemeinsamen Teilers von f_0, f_1:

$$\begin{aligned}
f_0 &= q_1 f_1 + f_2 && \text{mit } \mathsf{deg}(f_2) < \mathsf{deg}(f_1) \\
f_1 &= q_2 f_2 + f_3 && \text{mit } \mathsf{deg}(f_3) < \mathsf{deg}(f_2) \\
&\vdots \\
f_{m-2} &= q_{m-1} f_{m-1} + f_m && \text{mit } \mathsf{deg}(f_m) < \mathsf{deg}(f_{m-1}) \\
f_{m-1} &= q_m f_m
\end{aligned}$$

Wir wollen uns jetzt überlegen, daß $(f_m) = (f_0, f_1)$, d.h. daß f_m größter gemeinsamer Teiler von f_0 und f_1 ist. Dies sieht man wie folgt.

$\supseteq$. Es gilt

$$\begin{gathered}
f_m | f_{m-1} \\
f_m | f_{m-2} \\
\vdots \\
f_m | f_1 \\
f_m | f_0.
\end{gathered}$$

Also ist $(f_m) \supseteq (f_1)$ und $(f_m) \supseteq (f_0)$, und damit $(f_m) \supseteq (f_0, f_1)$.

$\subseteq$. Gelte $(h) \supseteq (f_0), (f_1)$. Zu zeigen ist $(h) \supseteq (f_m)$. Es gilt $h | f_0, h | f_1$, also auch $h | f_2$ und schließlich $h | f_m$. Damit folgt $(h) \supseteq (f_m)$.

Definition 3.4.9. 1. Sei $f \in A[X]$, etwa $f = a_n X^n + \dots + a_1 X + a_0$. Ein $a \in A$ heißt *Nullstelle* von f, wenn gilt $f(a) := a_n a^n + \dots + a_1 a + a_0 = 0$.

2. Sei $f \in A[X_1, \dots, X_n]$. Ein $(a_1, \dots, a_n) \in A^n$ heißt Nullstelle von f, wenn $f(a_1, \dots, a_n) := \sum_{(i_1,\dots,i_n)\in I} a_{i_1 \dots i_n} a_i^{i_1} \cdots a_n^{i_n} = 0$.

Bemerkung. Wie schon oben bemerkt, ist es möglich, daß jedes $a \in A$ Nullstelle von $f \in A[X]$ ist, obwohl $f \neq 0$. Ein Beispiel ist $A = \mathbb{Z}_p$ und $f = X^p - X$.

Satz 3.4.10. *Sei K ein Körper und $f \in K[X]$, $f \neq 0$. Dann gilt*

1. *Ist $a \in K$ Nullstelle von f, so gilt $f = (X - a)g$ für ein $g \in K[X]$.*
2. *f hat höchstens $\mathsf{deg}(f)$ Nullstellen.*

Beweis. 1. Es gibt $g, r \in K[X]$ mit $f = (X - a)g + r$ und $\mathsf{deg}(r) < 1$. Wegen $0 = f(a) = r(a)$ ist $r = 0$.

2. Seien $a_1, \dots, a_m$ verschiedene Nullstellen von f. Mit (1) folgt induktiv $f = (X - a_1) \dots (X - a_m)g$ für ein $g \in K[X]$, $g \neq 0$, also $\mathsf{deg}(f) = m + \mathsf{deg}(g) \geq m$. □

Als Anwendung dieses Satzes soll nun gezeigt werden, daß jede endliche Untergruppe von $(K^*, \cdot)$ zyklisch ist. Zur Vorbereitung dienen die folgenden Lemmata.

Lemma 3.4.11. *Sei G eine abelsche Gruppe, $x, y \in G$, $\mathsf{ord}(x) = m$, $\mathsf{ord}(y) = n$ und $v = \mathsf{kgV}(m, n)$. Dann gibt es ein $z \in G$ mit $\mathsf{ord}(z) = v$.*

Beweis. Zuerst wird der Spezialfall m, n teilerfremd untersucht. Dann ist $v = mn$. Wähle $z = xy$. Es ist $z^{mn} = (x^n)^m (y^m)^n = e$, da G abelsch. Sei nun r mit $z^r = e$, also $(xy)^r = x^r y^r = e$. Dann ist $x^{mr} y^{mr} = y^{mr} = e$, also $n|mr$ und somit $n|r$, da n, m teilerfremd. Analog folgt $m|r$, also $nm|r$ und damit $\mathsf{ord}(z) = m \cdot n$.

Wir behandeln jetzt den allgemeinen Fall. Zunächst eine Vorbemerkung. Sei $\mathsf{ord}(z) = m$ und $d|m$. Dann ist $\mathsf{ord}(z^{\frac{m}{d}}) = d$, also existiert immer ein $u \in G$ mit $\mathsf{ord}(u) = d$.

Sei nun $m = p_1^{m_1} \dots p_r^{m_r}$ und $n = p_1^{n_1} \dots p_r^{n_r}$. Dann ist $v = p_1^{t_1} \dots p_r^{t_r}$ mit $t_i = \max(m_i, n_i)$. Nach der Vorbemerkung existieren $x_i, y_i \in G$ mit $\mathsf{ord}(x_i) = p_i^{m_i}$, $\mathsf{ord}(y_i) = p_i^{n_i}$, also existieren auch $z_i \in G$ mit $\mathsf{ord}(z_i) = p_i^{t_i}$. Setze $z = z_1 \dots z_r$. Nach (1) gilt dann $\mathsf{ord}(z) = p_1^{t_1} \dots p_r^{t_r} = v$. □

Lemma 3.4.12. *Sei G eine abelsche Gruppe. Gibt es in G ein Element x maximaler Ordnung m, so gilt $y^m = e$ für alle $y \in G$. (Falls G endlich ist, existiert immer ein solches x).*

Beweis. Sei x Element mit maximaler Ordnung m. Sei $y \in G$ beliebig, $\mathsf{ord}(y) := n$. Nach dem vorigen Lemma existiert ein $z \in G$ mit $\mathsf{ord}(z) := v := \mathsf{kgV}(m, n)$. Da m maximal ist und $v \geq m$, folgt $v = m$. Damit gilt $n|m$, also $kn = m$ für ein $k \in \mathbb{N}$ und somit $y^m = (y^n)^k = e$. □

Satz 3.4.13. *Sei K ein Körper und G eine endliche Untergruppe der multiplikativen Gruppe K^*. Dann ist G zyklisch.*

Beweis. G ist abelsch und endlich. Sei m die maximale Elementordnung. Es ist $m \leq |G|$, da $x^{|G|} = 1$ für alle $x \in G$. Nach Lemma 3.4.12 ist $x^m = 1$ für alle $x \in G$. Also hat das Polynom $X^m - 1 \in K[X]$ genau $|G|$ verschiedene Nullstellen. Damit gilt $|G| \leq m$. Insgesamt ist $|G| = m$, also gibt es ein Element in G der Ordnung $|G|$; damit ist G zyklisch. □

Kapitel 4

Algebraische Körpererweiterungen

4.1 Algebraische Elemente

Satz 4.1.1. *1. Seien A, R Ringe mit $A \subseteq R$, und $a \in R$. Betrachte*

$$\begin{aligned} \hat{a} \colon A[X] &\to R \\ f = \sum_{i=0}^{n} a_i X^i &\mapsto \sum_{i=0}^{n} a_i a^i =: f(a). \end{aligned}$$

$\hat{a}$ ist Ringhomomorphismus und $A[a] := \mathsf{Bild}(\hat{a})$ der kleinste Unterring von R, der A umfaßt und a als Element enthält. $A[a]$ heißt der durch Ringadjunktion *von $a \in R$ zu A entstehende Ring.*

2. Sei $k \subseteq K$ eine Körpererweiterung und $a \in K$. Dann ist

$$k(a) := \{ \frac{f(a)}{g(a)} \mid f, g \in k[X], g(a) \neq 0 \} \subseteq K$$

der kleinste Unterkörper von K, der k umfaßt und a als Element enthält. $k(a)$ heißt der durch Körperadjunktion *von $a \in K$ zu k entstehende Körper.*

Beweis. Nach Bemerkung 3.1.5 sind $A[a]$ bzw. $k(a)$ Unterringe von R bzw. K. Nach Definition ist $k(a)$ sogar Unterkörper. Nach Konstruktion ist $A[a]$ bzw. $k(a)$ der kleinste Unterring bzw. Unterkörper. □

Bemerkung. Sei $k \subseteq K$ eine Körpererweiterung, $a \in K$. Dann gilt $k[a] \subseteq k(a)$, und $k(a)$ ist der Quotientenkörper von $k[a]$.

Satz 4.1.2. *1. Seien A, R Ringe mit $A \subseteq R$ und $a_1, \ldots, a_n \in R$. Betrachte*

$$\begin{aligned} \widehat{(a_1, \ldots, a_n)} \colon A[X_1, \ldots, X_n] &\to R \\ f = \sum_{(i_1, \ldots, i_n) \in I} a_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n} &\mapsto \sum_{(i_1, \ldots, i_n) \in I} a_{i_1 \ldots i_n} a_1^{i_1} \cdots a_n^{i_n} \\ &=: f(a_1, \ldots, a_n). \end{aligned}$$

$\widehat{(a_1, \ldots, a_n)}$ *ist Ringhomomorphismus, und*

$$A[a_1, \ldots, a_n] := \mathsf{Bild}(\widehat{(a_1, \ldots, a_n)})$$

ist der kleinste Unterring von R, der $A \cup \{a_1, \ldots, a_n\}$ enthält.

2. Sei $k \subseteq K$ eine Körpererweiterung und $a_1, \ldots, a_n \in K$. Dann ist

$$k(a_1, \ldots, a_n) := \{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \mid f, g \in k[X_1, \ldots, X_n], g(a_1, \ldots, a_n) \neq 0 \}$$

der kleinste Unterkörper von K, der $k \cup \{a_1, \ldots, a_n\}$ enthält. □

Im Folgenden sei $k \subseteq K$ eine Körpererweiterung.

Lemma 4.1.3. *Seien $a_1, \ldots, a_n, b_1, \ldots, b_m \in K$. Dann gilt*

1. $k[a_1, \ldots, a_n][b_1, \ldots, b_m] = k[a_1, \ldots, a_n, b_1, \ldots, b_m]$.
2. $k(a_1, \ldots, a_n)(b_1, \ldots, b_m) = k(a_1, \ldots, a_n, b_1, \ldots, b_m)$.

Beweis. Dies folgt sofort aus 4.1.1 und der anschließenden Bemerkung. □

Beispiel. Es ist $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i)$. Wir werden im folgenden zeigen, daß dies kein Zufall ist: es liegt daran, daß i Nullstelle von $X^2 + 1 \in \mathbb{R}[X]$ ist.

Definition 4.1.4. 1. Ein $a \in K$ heißt *algebraisch* über k, wenn a Nullstelle eines Polynoms $f \neq 0$ über k ist.

2. Ein $a \in K$ heißt *transzendent* über k, wenn kein Polynom $f \neq 0$ über k das Element a als Nullstelle hat.

3. Eine Körpererweiterung $k \subseteq K$ heißt *algebraisch*, wenn jedes $a \in K$ algebraisch über k ist.

Satz 4.1.5. *Sei $a \in K$ algebraisch über k. Dann gilt*

1. $k[a] = k(a)$.
2. *Für normierte Polynome $f \in k[X]$, $f \neq 0$ mit $f(a) = 0$ sind folgende Aussagen äquivalent.*
   - *i. f hat unter allen Polynomen $g \in k[X]$, $g \neq 0$ mit $g(a) = 0$ den kleinsten Grad.*
   - *ii. $(f) = \mathsf{Kern}(\hat{a})$, d.h. (da $\subseteq$ nach Voraussetzung gilt) für jedes $g \in k[X]$ mit $g(a) = 0$ gibt es ein $q \in k[X]$ so daß $g = qf$.*
   - *iii. f ist irreduzibel.*

   Es gibt genau ein normiertes Polynom $f \in k[X]$, $f \neq 0$ mit $f(a) = 0$ und allen Eigenschaften (i) bis (iii). Dieses f heißt das Minimalpolynom *zu a. Es gilt $k(a) \cong k[X]/(f)$ mit $a \mapsto X + (f)$.*
3. *$k(a)$ hat $1, a, \ldots, a^{n-1}$ mit $n := \mathsf{deg}(f)$ als k-Basis.*

Beweis. 1. Betrachtet man die Abbildung $\hat{a}$ aus 4.1.1, so liefert der Homomorphiesatz $k[X]/\mathsf{Kern}(\hat{a}) \cong k[a]$. Nun ist $k[a]$ ($\subseteq K$) Integritätsring, also $\mathsf{Kern}(\hat{a})$ Primideal nach Satz 3.2.3. Ferner gilt $\{0\} \subsetneq \mathsf{Kern}(\hat{a})$, da a algebraisch über k ist. Da $k[X]$ Hauptidealring ist, ist nach Folgerung 3.3.11 $\mathsf{Kern}(\hat{a})$ maximales Ideal. Damit ist $k[a]$ ein Körper und $k[a] \supseteq k(a)$, also $k[a] = k(a)$.

2. Sei $f \in k[X]$ normiert, $f \neq 0$ und $f(a) = 0$.

$(i) \Longrightarrow (ii)$. Sei $g \in k[X]$ mit $g(a) = 0$. Falls $g = 0$, ist $g \in (f)$. Sei also $g \neq 0$. Division mit Rest liefert $g = qf + r$ mit $q, r \in k[X]$ und $\mathsf{deg}(r) < \mathsf{deg}(f)$. Wegen $g(a) = 0$ und $f(a) = 0$ folgt $r(a) = 0$, und damit auch $r = 0$ nach (i).

$(ii) \Longrightarrow (iii)$. Gelte $f = gh$ mit $g, h \in k[X]$. Es ist $0 = f(a) = g(a)h(a)$, also $g(a) = 0$ oder $h(a) = 0$. OBdA gelte $h(a) = 0$. Dann existiert $q \in k[X]$ mit $h = qf$, also $f = gqf$. Daraus folgt $gq = 1$, also ist g Einheit, und damit ist f irreduzibel.

$(iii) \Longrightarrow (i)$. Sei $g \in k[X]$, $g \neq 0$, $g(a) = 0$ und $\mathsf{deg}(g)$ minimal. Annahme: $\mathsf{deg}(g) < \mathsf{deg}(f)$. Division mit Rest liefert $f = qg + r$ mit $q, r \in k[X]$ und $\mathsf{deg}(r) < \mathsf{deg}(g)$. Da $f(a) = 0 = g(a)$ folgt $r(a) = 0$ und somit $r = 0$, da man sonst einen Widerspruch zur Minimalität von $\mathsf{deg}(g)$ erhielte. Also ist $f = qg$ mit $\mathsf{deg}(g) < \mathsf{deg}(f)$. Dies ist ein Widerspruch zur Irreduzibilität von f.

Beweis der *Existenz* von f: $k[X]$ ist ein Hauptidealring, also ist $\mathsf{Kern}(\hat{a})$ Hauptideal. Demnach ist $\mathsf{Kern}(\hat{a}) = (f)$ für ein $f \in k[X]$. f kann normiert angenommen werden (sonst dividiere man durch den Leitkoeffizienten).

Eindeutigkeit. Gelte $\mathsf{Kern}(\hat{a}) = (f) = (f_1)$. Dann gilt $f = uf_1$ für ein $u \in k[X]^*$. Da f und f_1 normiert sind, folgt $u = 1$, also $f = f_1$.

$k(a) \cong k[X]/(f)$ mit $a \mapsto X + (f)$ folgt aus $k[a] = k(a)$ und $(f) = \mathsf{Kern}(\hat{a})$.

3. Zu zeigen ist, daß $1, a, \ldots, a^{n-1}$ über k linear unabhängig sind und ein Erzeugendensystem von $k(a)$ bilden.

Lineare Unabhängigkeit. Gelte $\sum_{i=0}^{n-1} a_i a^i = 0$ mit $a_i \in k$. Setzt man $g := \sum_{i=0}^{n-1} a_i X^i \in k[X]$, so gilt $g(a) = 0$ und $\mathsf{deg}(g) < n$. Nach (2) folgt $g = 0$, also $a_i = 0$ für alle i.

Erzeugendensystem. Wegen (1) genügt es zu zeigen, daß jede Potenz a^m mit $m \geq 0$ aus $1, a, \ldots, a^{n-1}$ linear kombinierbar ist. Dies zeigen wir durch Induktion über m. Für $m < n$ ist die Behauptung trivial. Sei also $m \geq n$. Es ist

$$a^m = a^{m-n} \underbrace{f(a)}_{0} + (a^m - a^{m-n} f(a)).$$

Nun ist $a^m - a^{m-n} f(a)$ von der Form $\sum_{i=0}^{m-1} b_i a^i$ mit $b_i \in k$, und nach Induktionsvoraussetzung sind alle a^i $(i < m)$ linear kombinierbar. □

Beispiel. Betrachte $\mathbb{Q} \subseteq \mathbb{R}$ und $\sqrt[3]{2} \in \mathbb{R}$. $\sqrt[3]{2}$ ist algebraisch über $\mathbb{Q}$, da $\sqrt[3]{2}$ Nullstelle von $X^3 - 2$ ist.

Es ist $\sqrt[3]{2} \notin \mathbb{Q}$, sonst hätte man $\sqrt[3]{2} = p/q$ mit $p, q \in \mathbb{N}$, also $2q^3 = p^3$ im Widerspruch zur eindeutigen Zerlegbarkeit in Primfaktoren.

Wir wollen uns überlegen, daß $X^3 - 2$ das Minimalpolynom zu $\sqrt[3]{2}$ ist. Nach Satz 4.1.5 genügt es zu zeigen, daß $X^3 - 2$ irreduzibel über $\mathbb{Q}$ ist. Wäre $X^3 - 2$ reduzibel, so müßte es $a, a_0, a_1 \in \mathbb{Q}$ geben mit $X^3 - 2 = (X - a)(X^2 + a_1 X + a_0)$. Es folgte $a = \sqrt[3]{2} \in \mathbb{Q}$, im Widerspruch zur obigen Bemerkung.

Nach Definition ist

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

$$\mathbb{Q}(\sqrt[3]{2}) = \{\, \frac{b_2(\sqrt[3]{2})^2 + b_1\sqrt[3]{2} + b_0}{c_2(\sqrt[3]{2})^2 + c_1\sqrt[3]{2} + c_0} \mid b_i, c_i \in \mathbb{Q}, (c_0, c_1, c_2) \neq (0,0,0) \,\}.$$

In Satz 4.1.5 haben wir gezeigt, daß $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$ ist, was direkt nicht leicht einzusehen ist.

Bemerkung. Der (triviale) Spezialfall $a \in k$ in Satz 4.1.5 liefert $f = X - a$. Nach (2ii) läßt sich dann jedes $g \in k[X]$ mit $g(a) = 0$ in der Form $g = (X - a)h$ für ein $h \in k[X]$ darstellen. Dies hatten wir schon früher unter allgemeineren Voraussetzungen gezeigt.

Satz 4.1.6. *Sei $k \subseteq K$ eine Körpererweiterung. Dann sind folgende Aussagen äquivalent.*

1. *$[K : k]$ ist endlich.*

2. *K ist algebraische Erweiterung von k von der Form $K = k(a_1, \ldots, a_n)$.*

Beweis. (1) $\Longrightarrow$ (2). Wir zeigen zunächst, daß K eine algebraische Erweiterung von k ist. Sei also $a \in K$. Betrachte die Elemente $1, a, a^2, a^3, \ldots$. Wegen $[K : k] < \infty$ gibt es ein m so daß $1, a, \ldots, a^m$ linear abhängig sind. Dann existieren $b_i \in k$, die nicht alle verschwinden, mit $\sum_{i=0}^m b_i a_i = 0$. Setze $f := \sum_{i=0}^m b_i X^i \in k[X]$. Dann gilt $f \neq 0$ und $f(a) = 0$. Also ist a algebraisch über k.

Wir zeigen jetzt, daß K von der Form $K = k(a_1, \ldots, a_n)$ ist. Sei $a_1, \ldots, a_n$ eine k-Basis von K. Dann gilt $K = k(a_1, \ldots, a_n)$. Dies sieht man wie folgt. $\supseteq$ ist klar. $\subseteq$. Sei $a \in K$. Dann existieren $b_i \in K$ mit $a = \sum_{i=1}^n b_i a_i$, da $a_1, \ldots, a_n$ k-Basis von K ist. Damit folgt $a \in k(a_1, \ldots, a_n)$.

(2) $\Longrightarrow$ (1). Es gilt $k \subseteq k(a_1) \subseteq k(a_1)(a_2) \subseteq \cdots \subseteq k(a_1)(a_2)\cdots(a_n) = K$. Es folgt

$$[K{:}k] = [k(a_1)\cdots(a_n) : k(a_1)\cdots(a_{n-1})] \cdot \ldots \cdot [k(a_1)(a_2) : k(a_1)] \cdot [k(a_1) : k] < \infty,$$

da jeder einzelne Faktor endlich ist (denn $K \supseteq k$ ist algebraisch). □

Bemerkung. Ohne den Zusatz "von der Form $K = k(a_1, \ldots, a_n)$" gilt (2) $\Longrightarrow$ (1) nicht. *Gegenbeispiel.* Betrachte

$$\bar{\mathbb{Q}} := \{\, a \in \mathbb{C} \mid a \text{ algebraisch über } \mathbb{Q} \,\}.$$

Wir zeigen zunächst, daß $\bar{\mathbb{Q}}$ ein Körper ist. Seien $a, b \in \mathbb{Q}$, $b \neq 0$. Dann gilt $[\mathbb{Q}(a,b) : \mathbb{Q}] < \infty$ wegen $[\mathbb{Q}(a,b) : \mathbb{Q}] = [\mathbb{Q}(a)(b) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}]$. Nach dem Satz ist also $\mathbb{Q}(a,b)$ algebraisch über $\mathbb{Q}$. Wegen $a - b$ und $\frac{a}{b} \in \mathbb{Q}(a,b)$ sind also $a - b$ und $\frac{a}{b}$ algebraisch über $\mathbb{Q}$ und damit $\in \bar{\mathbb{Q}}$.

Also ist $\bar{\mathbb{Q}} \supseteq \mathbb{Q}$ eine algebraische Körpererweiterung. Andererseits gilt $[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$, denn es gibt irreduzible Polynome beliebig hohen Grades über $\mathbb{Q}$ (etwa die Kreisteilungpolynome aus Abschnitt 5.1).

Satz 4.1.7. *(Kronecker). Sei k ein Körper und $g \in k[X]$, g nicht konstant. Dann gibt es einen Erweiterungskörper $K \supseteq k$, in dem g mindestens eine Nullstelle besitzt.*

Beweis. Sei $g = ph$ mit $p, h \in k[X]$ eine Zerlegung von g, wobei p irreduzibel ist (eine solche Zerlegung ist nach Satz 3.3.10 möglich). Da p irreduzibel ist, ist (p) nach Folgerung 3.3.11 ein maximales Ideal, also $k[X]/(p)$ ein Körper. Betrachte die Abbildung

$$\begin{aligned}\varphi\colon k &\to k[X]/(p)\\ a &\mapsto a + (p).\end{aligned}$$

φ ist ein Ringhomomorphismus mit Kern $\{0\}$, also ein Ringmonomorphismus. Nach dem Homomorphiesatz ist das Bild isomorph zu k, kann also durch k ersetzt werden. Es entsteht $K \supseteq k$. Sei etwa $p = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in k$. Dann gilt

$$0 = p + (p) = \sum_{i=0}^{n} (a_i + (p))(X + (p))^i \in k[X]/(p),$$

also nach dem Ersetzen des Bildes von φ in $k[X]/(p)$ durch k

$$0 = \sum_{i=0}^{n} a_i (X + (p))^i \in K.$$

Also ist $X + (p) \in K$ Nullstelle von p und damit auch von g. □

Bemerkung. Für $k = \mathbb{R}$ sagt der sogenannte *Fundamentalsatz der Algebra* (siehe Abschnitt 5.6) mehr aus, nämlich daß jedes nicht konstante Polynom $g \in \mathbb{R}[X]$ (sogar $g \in \mathbb{C}[X]$) eine Nullstelle in $\mathbb{C}$ besitzt.

4.2 Zerfällungskörper

Ziel dieses Abschnitts ist es, zu einem Körper k und einem Polynom $f \in k[X]$ einen bis auf Isomorphie eindeutig bestimmten Erweiterungskörper $K \supseteq k$ zu finden, in welchem f in Linearfaktoren zerfällt, und der minimal bezüglich dieser Eigenschaft ist.

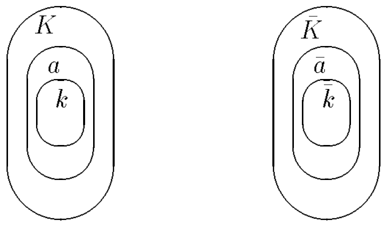
Lemma 4.2.1. *Seien $A, \bar{A}$ kommutative Ringe mit 1 und $\varphi\colon A \to \bar{A}$ ein Isomorphismus. Dann ist*

$$\begin{aligned}\hat{\varphi}\colon A[X] &\to \bar{A}[X]\\ \hat{\varphi}\Big(\sum_{i=0}^{n-1} a_i X^i\Big) &= \sum_{i=0}^{n-1} \varphi(a_i) X^i\end{aligned}$$

ein Isomorphismus mit $\hat{\varphi}\restriction A = \varphi$.

Beweis. Ergibt sich durch elementares Nachrechnen. □

Satz 4.2.2. *(Erster Erweiterungssatz). Seien $k \subseteq K$ und $\bar{k} \subseteq \bar{K}$ Körpererweiterungen, $a \in K$ und $\bar{a} \in \bar{K}$, ferner $p \in k[X]$ und $\bar{p} \in \bar{k}[X]$ irreduzibel mit $p(a) = 0$ und $\bar{p}(\bar{a}) = 0$. Weiter sei $\varphi\colon k \to \bar{k}$ ein Isomorphismus und $\hat{\varphi}(p) = \bar{p}$ ($\hat{\varphi}$ wie in Lemma vorher). Dann gibt es einen Isomorphismus $\bar{\varphi}\colon k(a) \to \bar{k}(\bar{a})$ mit $\bar{\varphi}\restriction k = \varphi$ und $\bar{\varphi}(a) = \bar{a}$.*



Beweis. Sei f das Minimalpolynom zu a. Wegen $p(a) = 0$ gilt $p = qf$ für ein $q \in k[X]$. Da p irreduzibel ist, muß q Einheit sein. Also gilt $(p) = (f)$, und ebenso $(\bar{p}) = (\bar{f})$, wobei $\bar{f}$ Minimalpolynom zu $\bar{a}$ ist. Es ist $\hat{\varphi}(p) = \bar{p}$, also $\hat{\varphi}((p)) = (\bar{p})$. Das folgende Diagramm ist kommutativ.

$$\begin{array}{ccc} k & \xrightarrow[\varphi]{\cong} & \bar{k} \\ \downarrow & & \downarrow \\ k[X] & \xrightarrow[\hat{\varphi}]{\cong} & \bar{k}[X] \\ \downarrow & & \downarrow \\ k(a) \cong k[X]/(p) & \xrightarrow[\bar{\varphi}]{\cong} & \bar{k}[X]/(\bar{p}) \cong \bar{k}(\bar{a}) \end{array}$$

Die Pfeile von oben nach unten stellen die kanonischen Abbildungen dar. In der unteren Zeile ergeben sich der erste und der letzte Isomorphismus aus Satz 4.1.5(2), und der mittlere Isomorphismus wird gegeben durch die Abbildung

$$\begin{aligned} k[X]/(p) &\to \bar{k}[X]/(\bar{p}) \\ g + (p) &\mapsto \hat{\varphi}(g) + (p), \end{aligned}$$

da $\hat{\varphi}$ Isomorphismus mit $\hat{\varphi}(p) = \bar{p}$ ist. $\bar{\varphi}$ ergibt sich nun als Hintereinanderschaltung dieser drei Abbildungen. Offenbar ist $\bar{\varphi}\restriction k = \varphi$, und $\bar{\varphi}(a) = \bar{a}$ ergibt sich aus $a \mapsto X + (p) \mapsto X + (\bar{p}) \mapsto \bar{a}$. $\square$

Folgerung 4.2.3. *Sei $k \subseteq K$ eine Körpererweiterung, $p \in k[X]$ irreduzibel, $a, b \in K$ und $p(a) = 0 = p(b)$. Dann gilt $k(a) \cong k(b)$.*

Beweis. Setze im ersten Erweiterungssatz $k = \bar{k}$ und $\varphi = \mathsf{id}_k$. $\square$

Beispiel. Betrachte die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{C}$ und das irreduzible Polynom $X^3 - 2 \in \mathbb{Q}[X]$. Seine Nullstellen sind $\sqrt[3]{2}$, $\sqrt[3]{2}\,e^{\frac{2\pi i}{3}}$ und $\sqrt[3]{2}\,e^{\frac{4\pi i}{3}}$. Aus der eben bewiesenen Folgerung ergibt sich

$$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}}) \cong \mathbb{Q}(\sqrt[3]{2}e^{\frac{4\pi i}{3}}).$$

Definition 4.2.4. Sei k ein Körper und $f \in k[X]$. Ein Erweiterungskörper $Z \supseteq k$ heißt ein *Zerfällungskörper* von f, wenn folgendes gilt.

1. f zerfällt in Z in Linearfaktoren, d.h. es gibt $a_1, \ldots, a_n \in Z$ mit $f = b(X - a_1) \cdots (X - a_n)$, $b \in k$.

2. Z ist minimal bezüglich der Eigenschaft (1), d.h. f zerfällt über keinem echten Zwischenkörper von $Z \supseteq k$ in Linearfaktoren.

Bemerkung. Sei $k \subseteq K$ eine Körpererweiterung. $f \in k[X]$ zerfalle in K in Linearfaktoren, etwa $f = b(X - a_1) \cdots (X - a_n)$ mit $a_1, \ldots, a_n \in K$ und $b \in k$. Dann ist $k(a_1, \ldots, a_n)$ ein Zerfällungskörper von f.

Beweis. (1) gilt nach Konstruktion, und (2) folgt aus der Eindeutigkeit der Zerlegung in irreduzible Faktoren und der Tatsache, daß $k(a_1, \ldots, a_n)$ der kleinste Körper ist, der $k \cup \{a_1, \ldots, a_n\}$ enthält. □

Satz 4.2.5. *Sei k ein Körper. Dann gibt es zu jedem Polynom $f \in k[X]$ einen Zerfällungskörper $Z \supseteq k$ so daß $[Z : k]$ endlich ist.*

Beweis. Nach dem Satz 4.1.7 von Kronecker gibt es einen Erweiterungskörper $K_1 \supseteq k$ und ein $a_1 \in K_1$ mit $f(a_1) = 0$ und $f = (X - a_1)f_1$, $f_1 \in K_1[X]$. OBdA kann man $K_1 = k(a_1)$ annehmen. Analog existiert $K_2 \supseteq K_1$ und ein $a_2 \in K_2$ mit $f_1(a_2) = 0$ und $f_1 = (X - a_2)f_2$, $f_2 \in K_2[X]$. Wieder kann man oBdA $K_2 = K_1(a_2)$ annehmen. Nach $\mathsf{deg}(f)$ Schritten bricht dieses Verfahren ab, und man erhält eine Körperfolge

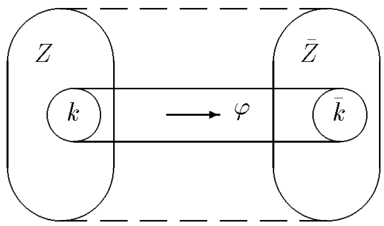
$$\begin{aligned}
&k \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n, \\
&K_n = k(a_1, \ldots, a_n) \quad (\text{da } k(a_1, \ldots, a_i)(a_{i+1}) = k(a_1, \ldots, a_i, a_{i+1})) \\
&K_n = k(a_1, \ldots, a_n) \text{ ist ein Zerfällungskörper von } f.
\end{aligned}$$

Weiter gilt $[K_{i+1} : K_i] = [K_i(a_{i+1}) : K_i] < \infty$, also

$$[K_n : k] = [K_n : K_{n-1}] \ldots [K_2 : K_1][K_1 : k] < \infty. \qquad \square$$

Satz 4.2.6. *(Zweiter Erweiterungssatz). Seien $k, \bar{k}$ Körper, $f \in k[X]$, $\bar{f} \in \bar{k}[X]$ und Z Zerfällungskörper von f, $\bar{Z}$ Zerfällungskörper von $\bar{f}$. Ferner sei $\varphi \colon k \to \bar{k}$ ein Isomorphismus mit $\hat{\varphi}(f) = \bar{f}$. Dann gibt es einen Isomorphismus $\tilde{\varphi} \colon Z \to \bar{Z}$ mit $\tilde{\varphi}\restriction k = \varphi$ und*

$$\tilde{\varphi}(\textit{Menge der Nullstellen von } f) = \textit{Menge der Nullstellen von } \bar{f}.$$



Bemerkung. $\tilde{\varphi}$ ist i.a. nicht eindeutig bestimmt. $\tilde{\varphi}$ liegt jedoch fest, wenn man die Werte auf den Nullstellen $a_1, \ldots, a_n$ von f kennt, da $Z = k(a_1, \ldots, a_n)$.

Beweis. Durch Induktion nach der Anzahl N der Nullstellen von f in $Z \setminus k$.

Fall $N = 0$. Dann ist $Z = k$, also $f = b(X-a_1) \cdots (X-a_n)$ mit $a_1, \ldots, a_n, b \in k$. Es folgt $\bar{f} = \hat{\varphi}(f) = \varphi(b)(X - \varphi(a_1)) \cdots (X - \varphi(a_n))$, also $\bar{Z} = \bar{k}$, und wir können $\tilde{\varphi} := \varphi$ setzen.

Fall $N > 0$. Wähle $a_1 \in Z \setminus k$ mit $f(a_1) = 0$. p_1 sei das Minimalpolynom zu a_1. Dann gilt $f = qp_1$, also $\bar{f} = \hat{\varphi}(f) = \hat{\varphi}(q)\hat{\varphi}(p_1)$. Da $\bar{Z}$ Zerfällungskörper von $\bar{f}$ ist, gibt es $\bar{a}_1, \ldots, \bar{a}_n \in \bar{Z}$ und $\bar{b} \in \bar{k}$ mit $\bar{f} = \bar{b}(X - \bar{a}_1) \cdots (X - \bar{a}_n)$. Da $\mathsf{deg}(\hat{\varphi}(q)) < \mathsf{deg}(\bar{f})$, kann man oBdA annehmen, daß $\bar{a}_1$ Nullstelle von $\hat{\varphi}(p_1)$ ist. Da p_1 als Minimalpolynom irreduzibel ist, muß auch $\hat{\varphi}(p_1)$ irreduzibel sein. Der erste Erweiterungssatz liefert einen Isomorphismus $\bar{\varphi}\colon k(a_1) \to \bar{k}(\bar{a}_1)$ mit $\bar{\varphi}{\restriction}k = \varphi$ und $\bar{\varphi}(a_1) = \bar{a}_1$. Es gilt also $f \in (k(a_1))[X]$, $\bar{f} \in (\bar{k}(\bar{a}_1))[X]$, $\hat{\bar{\varphi}}(f) = \bar{f}$ und f hat höchstens $N-1$ Nullstellen in $Z \setminus k(a_1)$. Die Behauptung folgt jetzt aus der Induktionsvoraussetzung. □

Folgerung 4.2.7. *Sei k Körper und $f \in k[X]$. Dann sind alle Zerfällungskörper von f isomorph; man spricht deshalb von* dem *Zerfällungskörper von f.* □

4.3 Separable Erweiterungen

Ziel dieses Abschnitts ist es, ein wichtiges Kriterium anzugeben, wann eine Körpererweiterung $k \subseteq K$ galoissch ist. Dazu wird die Galois-Theorie mit dem Polynombegriff in Verbindung gebracht.

Definition 4.3.1. Sei k ein Körper, $f \in k[X]$, $Z \supseteq k$ Zerfällungskörper von f und $a \in Z$. Dann heißt

$$\mu(f,a) := \text{ dasjenige } n \geq 0 \text{ mit } (X-a)^n | f,\ (X-a)^{n+1} \nmid f$$

die *Vielfachheit* von a als Nullstelle von f. a heißt *einfache Nullstelle* von f, wenn $\mu(f,a) = 1$.

Bemerkung. Sei k ein Körper, $p \in k[X]$ irreduzibel. Dann gilt: sind $Z, \bar{Z} \supseteq k$ Zerfällungskörper von p, und hat p in Z nur einfache Nullstellen, so auch in $\bar{Z}$.

Beweis. Nach dem zweiten Erweiterungssatz wird die Menge der Nullstellen von p in Z bijektiv auf die Menge der Nullstellen von p in $\bar{Z}$ abgebildet. Hat also p in Z lauter verschiedene Nullstellen, so auch in $\bar{Z}$. □

Definition 4.3.2. 1. Sei k ein Körper. Dann heißt $f \in k[X]$ *separabel*, wenn jeder irreduzible Faktor von f (in seinem Zerfällungskörper) nur einfache Nullstellen hat. (Dies ist nach der vorangegangenen Bemerkung wohldefiniert).

2. Sei $k \subseteq K$ eine Körpererweiterung. Dann heißt $a \in K$ *separabel* über k, wenn es ein separables Polynom $f \in k[X]$ gibt mit $f(a) = 0$.

3. Eine Körpererweiterung $k \subseteq K$ heißt *separabel* über k, wenn jedes $a \in K$ separabel über k ist.

Lemma 4.3.3. *Sei $k \subseteq K$ galoissch, $a \in K$ und $a_1, \ldots, a_n$ die verschiedenen Bilder von a unter den $\varphi \in \Gamma_k^K$. Dann gilt:*

1. *$p := (X - a_1) \cdots (X - a_n) \in k[X]$.*

2. *p ist separabel.*

3. *p ist das Minimalpolynom zu a.*

Beweis. 1. Sei $\varphi \in \Gamma_k^K$. Dann gilt $\hat{\varphi}(p) = (X - \varphi(a_1)) \cdots (X - \varphi(a_n))$. Da φ bijektiv ist, sind $\varphi(a_1), \ldots, \varphi(a_n)$ verschieden. Da die Nullstellen von p auch Nullstellen von $\hat{\varphi}(p)$ sind, folgt $\{a_1, \ldots, a_n\} = \{\varphi(a_1), \ldots, \varphi(a_n)\}$ und damit $\hat{\varphi}(p) = p$. Also sind die Koeffizienten von p aus dem Fixkörper von Γ_k^K und deshalb $p \in k[X]$, da $\mathsf{FK}(\Gamma_k^K) = k$ nach Voraussetzung.

2. Folgt aus der Definition von p.

3. Da $\mathsf{id}_K \in \Gamma_k^K$, ist a eines der a_i, also $p(a) = 0$. Sei noch $g \in k[X]$, $g \neq 0$ mit $g(a) = 0$ gegeben. Zu zeigen ist $\mathsf{deg}(g) \geq \mathsf{deg}(p)$. Es gilt $g(a) = 0$, und da $g \in k[X]$, gilt $0 = \varphi(g(a)) = g(\varphi(a))$ für alle $\varphi \in \Gamma_k^K$. g hat demnach mindestens n verschiedene Nullstellen, also $\mathsf{deg}(g) \geq n = \mathsf{deg}(p)$. ◻

Satz 4.3.4. *Sei $k \subseteq K$ eine Körpererweiterung. Dann sind folgende Aussagen äquivalent.*

1. *$k \subseteq K$ ist galoissch.*

2. *K ist Zerfällungskörper eines separablen Polynoms über k.*

Beweis. 1 $\Longrightarrow$ 2. $[K : k] < \infty$, also ist $K \supseteq k$ algebraisch von der Form $K = k(a_1, \ldots, a_n)$. Seien $p_1, \ldots, p_n$ die Minimalpolynome zu $a_1, \ldots, a_n$. Definiere $f := p_1 \ldots p_n$. Nach dem vorangegangenen Lemma ist f separabel und zerfällt in K. Zerfiele f schon in einem Zwischenkörper L, so wären $a_1, \ldots, a_n \in L$, also $k(a_1, \ldots, a_n) \subseteq L \subseteq K = k(a_1, \ldots, a_n)$ und damit $L = K$.

2 $\Longrightarrow$ 1. Sei $f \in k[X]$ separabel und $K \supseteq k$ Zerfällungskörper von f. Zu zeigen: $k \subseteq K$ ist galoissch. Es gilt: $[K : k] < \infty$, da K Zerfällungskörper von f ist. Daraus folgt $|\Gamma_k^K| < \infty$, da $|\Gamma_k^K| \leq [K : k]$ nach Satz 2.2.3. Wir zeigen $\mathsf{FK}(\Gamma_k^K) = k$ durch Induktion nach der Anzahl N der Nullstellen von f außerhalb von k.

Fall $N = 0$. Dann gilt $K = k$, und die Aussage ist gezeigt.

Fall $N > 0$. Sei $f = p_1 \ldots p_r$, mit $p_i \in k[X]$ irreduzibel. Da $N > 0$, existiert ein p_i mit $\mathsf{deg}(p_i) > 1$. Sei OBdA $\mathsf{deg}(p_1) = s \geq 2$. p_1 hat in K die verschiedenen Nullstellen $a_1, \ldots, a_s$ (da f separabel). Außerdem ist f, aufgefaßt als Element von $k(a_1)[X]$, separabel. f hat außerhalb von $k(a_1)$ höchstens $N-1$ Nullstellen, daher liefert die Induktionsvoraussetzung $\mathsf{FK}(\Gamma_{k(a_1)}^K) = k(a_1)$. (Da k beliebig war, kann für k in der Induktionsvoraussetzung auch $k(a_1)$ gesetzt werden). Sei nun $b \in \mathsf{FK}(\Gamma_k^K)$. Zu zeigen ist $b \in k$, denn $k \subseteq \mathsf{FK}(\Gamma_k^K)$ gilt immer. Es gilt $b \in \mathsf{FK}(\Gamma_{k(a_1)}^K) = k(a_1)$. Da $\mathsf{deg}(p_1) = s$ und p_1 irreduzibel, ist p Minimalpolynom zu a_1, also bilden $1, a_1, \ldots, a_1^{s-1}$ eine k-Basis von $k(a_1)$. Sei

$$b = \sum_{i=0}^{s-1} c_i a_1^i \quad \text{mit } c_i \in k.$$

Setze

$$g := \Big(\sum_{i=0}^{s-1} c_i X^i\Big) - b \in k(a_1)[X].$$

Es ist $g(a_1) = 0$. Nun genügt es zu zeigen, daß es $\tilde{\varphi}_1, \ldots, \tilde{\varphi}_s \in \Gamma_k^K$ gibt mit $\tilde{\varphi}_i(a_1) = a_i$. Dann folgt nämlich $0 = \tilde{\varphi}_i(g(a_1)) = g(\tilde{\varphi}_i(a_1))$ für alle i, da $c_i \in k$ und $b \in \mathsf{FK}(\Gamma_k^K)$. g hat also mindestens s Nullstellen, aber einen Grad $\leq s - 1$. Es folgt $g = 0$, also $b = c_0 \in k$.

Es ist also noch die Existenz der $\tilde{\varphi}_1, \ldots, \tilde{\varphi}_s$ zu zeigen. Da $p_1 \in k[X]$ irreduzibel ist und $p_1(a_1) = p_1(a_i) = 0$, kann der erste Erweiterungssatz auf die folgende Situation angewandt werden.

$$\begin{array}{ccc} k & \xrightarrow{\mathsf{id}_k} & k \\ \downarrow & & \downarrow \\ k(a_1) & \xrightarrow[\varphi_i]{\cong} & k(a_i) \end{array}$$

Man erhält Isomorphismen φ_i mit $\varphi_i \restriction k = \mathsf{id}_k$ und $\varphi_i(a_1) = a_i$. Man betrachte nun $f \in k[X]$ einmal als Element von $k(a_1)[X]$ und dann als Element von $k(a_i)[X]$. Dann gilt $\hat{\varphi}_i(f) = f$ (wegen $f \in k[X]$), und der zweite Erweiterungssatz liefert

$$\begin{array}{ccc} k(a_1) & \xrightarrow{\varphi_i} & k(a_i) \\ \downarrow & & \downarrow \\ K & \xrightarrow[\tilde{\varphi}_i]{\cong} & K \end{array}$$

Es ergibt sich die Existenz von s verschiedenen Automorphismen $\tilde{\varphi}_i$ mit $\tilde{\varphi}_i \restriction k = \mathsf{id}_k$ und $\tilde{\varphi}_i(a_1) = a_i$, was noch zu zeigen war. □

Es soll nun noch untersucht werden, wann die Eigenschaft "$f \in k[X]$ ist separabel" erfüllt ist. Dazu wird der Begriff der formalen Ableitung eingeführt, und es wird (wie in der Analysis) für eine Nullstelle a eines Polynoms folgendes gezeigt: a ist mehrfache Nullstelle von f genau dann, wenn $f'(a) = 0$. Sei also k ein Körper und $f \in k[X]$, etwa $f = a_n X^n + \cdots + a_1 X + a_0$. Dann heißt

$$f' := n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + a_1 \in k[X]$$

die *formale Ableitung* von f.

Lemma 4.3.5. *Sei k ein Körper und $f, g \in k[X]$. Dann gilt*

1. $(f+g)' = f' + g'$.
2. $(fg)' = f'g + fg'$.

Beweis. 1. Ergibt sich durch einfaches Nachrechnen. 2. Sei etwa

$$f = \sum_{i=0}^{m} a_i X^i \quad \text{und} \quad g = \sum_{j=0}^{n} b_j X^j.$$

Dann gilt

$$\begin{aligned} fg &= \sum_{l=0}^{m+n} c_l X^l & \text{mit } c_l = \textstyle\sum_{i+j=l} a_i b_j \\ (fg)' &= \sum_{l=0}^{m+n} l c_l X^{l-1} \\ f'g &= \Big(\sum_{i=0}^{m} i a_i X^{i-1}\Big)\Big(\sum_{j=0}^{n} b_j X^j\Big) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{l=0}^{m+n} d_l X^{l-1} && \text{mit } d_l = \textstyle\sum_{i+j=l} i a_i b_j \\
fg' &= \sum_{l=0}^{m+n} e_l X^{l-1} && \text{mit } e_l = \textstyle\sum_{i+j=l} j a_i b_j \\
f'g + fg' &= \sum_{l=0}^{m+n} (d_l + e_l) X^{l-1} && \text{mit } d_l + e_l = \textstyle\sum_{i+j=l} (i+j) a_i b_j, \\
& && \text{also } d_l + e_l = \textstyle\sum_{i+j=l} l a_i b_j .
\end{aligned}
$$

□

Satz 4.3.6. *Sei k ein Körper, $f \in k[X]$, $Z \supseteq k$ Zerfällungskörper von f und $a \in Z$ mit $f(a) = 0$. Dann gilt*

1. *$\mu(f, a) > 1$ genau dann, wenn $f'(a) = 0$.*
2. *$\mu(f, a) = 1$ genau dann, wenn $f'(a) \neq 0$.*

Beweis. Es genügt, jeweils $\Longrightarrow$ zu zeigen. Sei $\mu(f, a) =: n$, also $f = (X - a)^n g$ für ein $g \in Z[X]$ mit $g(a) \neq 0$. Dann folgt

$$f' = n(X - a)^{n-1} g + (X - a)^n g'.$$

Im Fall $n > 1$ folgt $f'(a) = 0$, und im Fall $n = 1$ ist $f'(a) = g(a) \neq 0$. □

Satz 4.3.7. *Sei k ein Körper und $q \in k[X]$ irreduzibel. Dann gilt*

1. *Ist $\mathsf{char}(k) = 0$, so hat q nur einfache Nullstellen.*
2. *Ist $\mathsf{char}(k) = p$ (p Primzahl), so hat q mehrfache Nullstellen genau dann, wenn q mindestens eine Nullstelle hat und von der Form $a_n X^{pn} + \cdots + a_1 X^p + a_0$ ist mit $a_0, \ldots, a_n \in k$.*

Beweis. Sei $Z \supseteq k$ Zerfällungskörper von q.

1. Sei $\mathsf{char}(k) = 0$. Angenommen, es existiert eine mehrfache Nullstelle $a \in Z$ von q. Dann gilt $q(a) = 0$ und $q'(a) = 0$. Da q bis auf einen konstanten Faktor aus k das Minimalpolynom von a ist (denn q ist irreduzibel) und $\mathsf{deg}(q') < \mathsf{deg}(q)$ gilt, folgt $q' = 0$. Also ist q konstant. Dies ist ein Widerspruch zur Irreduzibilität von q.

2. Sei $\mathsf{char}(k)$ eine Primzahl p.

$\Longrightarrow$. Sei $a \in Z$ mehrfache Nullstelle von q. Wie eben folgt $q' = 0$. Also muß q von der Form $a_n X^{pn} + \cdots + a_1 X^p + a_0$ sein.

$\Longleftarrow$. Sei umgekehrt q von der Form $a_n X^{pn} + \cdots + a_1 X^p + a_0$. Dann ist $q' = 0$, also q hat keine einfache Nullstelle. (Hätte nämlich q eine einfache Nullstelle a, so müßte $q'(a) \neq 0$ sein, also könnte $q' = 0$ nicht gelten). Da aber q mindestens eine Nullstelle besitzt, hat q eine mehrfache Nullstelle. □

Folgerung 4.3.8. *1. Über einem Körper der Charakteristik* 0 *ist jedes Polynom separabel.*

2. Über einem Körper der Charakteristik p ist ein Polynom genau dann separabel, wenn kein *irreduzibler Faktor die Form $a_n X^{pn} + \cdots + a_1 X^p + a_0$ hat.* □

4.4 Normale Körpererweiterungen

Der Begriff einer normalen Körpererweiterung liefert uns eine Charakterisierung der Zerfällungskörper von Polynomen, und außerdem eine weitere Charakterisierung der galoisschen Erweiterungen.

Definition 4.4.1. Eine Körpererweiterung $k \subseteq K$ heißt *normal*, wenn gilt:

1. $k \subseteq K$ ist algebraisch.

2. Jedes irreduzible Polynom $f \in k[X]$, das in K eine Nullstelle besitzt, zerfällt über K in Linearfaktoren.

Satz 4.4.2. *Sei $k \subseteq K$ eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent.*

1. *$k \subseteq K$ ist normal.*

2. *K ist Zerfällungskörper eines Polynoms $f \in k[X]$.*

3. *Ist $K \subseteq K'$ eine Körpererweiterung und $\varphi\colon K \to K'$ ein Homomorphismus mit $\varphi{\restriction}k = \mathsf{id}_k$, so gilt $\varphi(K) \subseteq K$.*

Beweis. $1 \Longrightarrow 2$. Da $k \subseteq K$ endlich ist, existieren $a_1, \ldots, a_n \in K$, a_i algebraisch über k, so daß $K = k(a_1, \ldots, a_n)$. Sei f_i Minimalpolynom zu a_i. Nach (1) zerfällt f_i über K in Linearfaktoren. Also ist K Zerfällungskörper von $f = f_1 \ldots f_n$.

$2 \Longrightarrow 3$. Sei $K = k(a_1, \ldots, a_n)$ und $f = b(X - a_1) \cdots (X - a_n) \in k[X]$. Sei $K \subseteq K'$ eine Körpererweiterung und $\varphi\colon K \to K'$ Homomorphismus mit $\varphi{\restriction}k = \mathsf{id}_k$. Wegen $f \in k[X]$ gilt $0 = \varphi(f(a_i)) = f(\varphi(a_i))$, also $\varphi(\{a_1, \ldots, a_n\}) \subseteq \{a_1, \ldots, a_n\}$. Demnach ist $\varphi(k(a_1, \ldots, a_n)) \subseteq k(a_1, \ldots, a_n)$, d.h. $\varphi(K) \subseteq K$.

$3 \Longrightarrow 1$. Da $k \subseteq K$ endlich ist, ist $k \subseteq K$ algebraisch. Sei $f \in k[X]$ irreduzibel und $a \in K$ Nullstelle von f. Wähle $a_1, \ldots, a_n \in K$ mit $K = k(a, a_1, \ldots, a_n)$. Sei $f_i \in k[X]$ das Minimalpolynom zu a_i und betrachte $g = f f_1 \cdots f_n$. Wähle $K' \supseteq K$ als Zerfällungskörper von g. f zerfällt in K' in Linearfaktoren. Sei $b \in K'$ Nullstelle von f. Wir zeigen $b \in K$, und betrachten dazu das folgende Diagramm.

$$\begin{tikzcd}
k \arrow[r, "\mathsf{id}_k"] \arrow[d] & k \arrow[d] \\
k(a) \arrow[r, "\varphi"] \arrow[d] & k(b) \arrow[d] \\
K' \arrow[r, "\psi"] & K'
\end{tikzcd}$$

Der erste Erweiterungssatz 4.2.2 liefert φ mit $\varphi(a) = b$ und $\varphi{\restriction}k = \mathsf{id}_k$; der zweite Erweiterungssatz 4.2.6 liefert ψ mit $\psi(a) = b$ und $\psi{\restriction}k = \mathsf{id}_k$. Wende die Voraussetzung (3) an auf $\psi{\restriction}K\colon K \to K'$; es ergibt sich $(\psi{\restriction}K)(K) \subseteq K$. Da $a \in K$ (wegen $K = k(a, a_1, \ldots, a_n)$), folgt $b = \psi(a) \in (\psi{\restriction}K)(K) \subseteq K$. Da nun b eine beliebige Nullstelle von f war, liegen alle Nullstellen von f in K. Also zerfällt f über K in Linearfaktoren, und damit ist $k \subseteq K$ normal. □

Beispiele. 1. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ ist normal, da $\mathbb{Q}(\sqrt{2})$ Zerfällungskörper von $X^2 - 2 \in \mathbb{Q}[X]$ ist.

2. $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ ist normal, da $\mathbb{Q}(\sqrt[4]{2})$ Zerfällungskörper von $X^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$ ist.

3. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ ist *nicht* normal. Dies sieht man wie folgt. Betrachte $X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2}) = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$. $X^4 - 2 \in \mathbb{Q}[X]$ ist irreduzibel (da auch die quadratischen Faktoren nicht in $\mathbb{Q}$ liegen) und hat eine Nullstelle in $\mathbb{Q}(\sqrt[4]{2})$, aber $X^4 - 2$ zerfällt in $\mathbb{Q}(\sqrt[4]{2})$ *nicht* in Linearfaktoren (denn mit $i \notin \mathbb{Q}(\sqrt[4]{2})$ folgt $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$).

Ergebnis. Aus $k \subseteq K$ normal und $K \subseteq K'$ normal kann im allgemeinen nicht auf die Normalität von $k \subseteq K'$ geschlossen werden.

Satz 4.4.3. *Sei $k \subseteq K$ eine Körpererweiterung. Dann sind folgende Aussagen äquivalent.*

1. *$k \subseteq K$ ist galoissch.*
2. *$k \subseteq K$ ist endlich, normal und separabel.*
3. *K ist Zerfällungskörper eines separablen Polynoms über k.*

Beweis. Die Äquivalenz von (1) und (3) wurde bereits in Satz 4.3.4 bewiesen.

$1 \Longrightarrow 2$. Da $k \subseteq K$ galoissch ist, ist $k \subseteq K$ endlich, also auch algebraisch. Sei $f \in k[X]$ irreduzibel und $f(a) = 0$ für ein $a \in K$. f ist also bis auf einen konstanten Faktor das Minimalpolynom zu a. Lemma 4.3.3 liefert $f = b(X - a_1) \cdots (X - a_n)$, wobei die a_i Bilder von a unter den $\varphi \in \Gamma_k^K$ sind, also $a_i \in K$. f zerfällt also in K, daher ist $k \subseteq K$ normal. Sei $a \in K$. Nach Lemma 4.3.3 existiert ein separables Polynom aus $k[X]$, das a als Nullstelle hat. Daher ist $k \subseteq K$ separabel.

$2 \Longrightarrow 3$. Nach Satz 4.4.2 ist K Zerfällungskörper eines Polynoms $f \in k[X]$. Es genügt zu zeigen, daß f separabel ist. Sei also g irreduzibler Faktor von f und $a \in K$ Nullstelle von g. Dann ist g bis auf einen konstanten Faktor das Minimalpolynom zu a, hat also nach – da $a \in K$ separabel ist – verschiedene Nullstellen. ∎

4.5 Teilbarkeit ganzzahliger Polynome

Sei $f \in \mathbb{Z}[X]$ nicht konstant. Um triviale Betrachtungen zu vermeiden, seien oBdA die Koeffizienten von f teilerfremd. (Dies kann durch Division durch den größten gemeinsamen Teiler immer erreicht werden).

Wenn f irreduzibel ist in $\mathbb{Q}[X]$, so ist offenbar f auch irreduzibel in $\mathbb{Z}[X]$. Der Satz von Gauß soll nun die Umkehrung liefern.

Lemma 4.5.1. *(Gauß). Seien $f, g \in \mathbb{Z}[X]$, beide nicht konstant. Sind dann sowohl die Koeffizienten von f als auch die Koeffizienten von g teilerfremd, so sind die Koeffizienten von fg teilerfremd.*

Beweis. Angenommen, es gibt eine Primzahl p, die alle Koeffizienten von fg teilt. Dann ist $fg \in (p\mathbb{Z})[X] := \{ h \in \mathbb{Z}[X] \mid \text{alle Koeffizienten von } h \text{ sind } \in p\mathbb{Z} \}$. $(p\mathbb{Z})[X]$ ist ein Ideal in $\mathbb{Z}[X]$.

Es reicht zu zeigen, daß $(p\mathbb{Z})[X]$ ein Primideal in $\mathbb{Z}[X]$ ist, denn dann folgt $f \in (p\mathbb{Z})[X]$ oder $g \in (p\mathbb{Z})[X]$ im Widerspruch zur Voraussetzung. Dafür genügt

$\mathbb{Z}[X]/(p\mathbb{Z})[X] \cong (\mathbb{Z}/p\mathbb{Z})[X]$, denn dann ist $(p\mathbb{Z})[X]$ Primideal, da $(\mathbb{Z}/p\mathbb{Z})[X]$ ein Integritätsring ist. Betrachte die Abbildung

$$\widehat{\mathsf{kan}}\colon \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$$
$$\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} (a_i + p\mathbb{Z}) X^i$$

$\widehat{\mathsf{kan}}$ ist ein Epimorphismus mit Kern $(p\mathbb{Z})[X]$. Der Homorphiesatz liefert also $\mathbb{Z}[X]/(p\mathbb{Z})[X] \cong (\mathbb{Z}/p\mathbb{Z})[X]$. ☐

Satz 4.5.2. *(Gauß). Sei $f \in \mathbb{Z}[X]$ nicht konstant. Ist f irreduzibel in $\mathbb{Z}[X]$, so auch in $\mathbb{Q}[X]$.*

Beweis. Angenommen, es existieren $g_1, h_1 \in \mathbb{Q}[X]$ mit $f = g_1 h_1$ und $0 < \mathsf{deg}(g_1), \mathsf{deg}(h_1) < \mathsf{deg}(f)$. Durch Herausziehen zuerst des Hauptnenners und anschließend für jedes der beiden Polynome des größten gemeinsamen Teilers der Koeffizienten beider Polynome erhält man $f = agh$ mit $a \in \mathbb{Q}$, $g, h \in \mathbb{Z}[X]$, $\mathsf{deg}(g) = \mathsf{deg}(g_1)$, $\mathsf{deg}(h) = \mathsf{deg}(h_1)$ und sowohl die Koeffizienten von g als auch die von h sind teilerfremd. Nach dem Lemma 4.5.1 von Gauß sind dann die Koeffizienten von gh auch teilerfremd. Damit folgt $a \in \mathbb{Z}$, denn wäre etwa $a = \frac{b}{pc}$ mit $p \nmid b$, p Primzahl, so würde p jeden Koeffizienten von gh teilen. Dies ist ein Widerspruch zur Irreduzibilität von f in $\mathbb{Z}[X]$. ☐

Es soll nun ein *Verfahren von Kronecker* zur Bestimmung aller Teiler in $\mathbb{Z}[X]$ eines gegebenen Polynoms $f \in \mathbb{Z}[X]$ entwickelt werden. Damit ist insbesondere eine Entscheidung möglich, ob f in $\mathbb{Z}[X]$ irreduzibel ist oder nicht.

Lemma 4.5.3. *Sei K ein Körper, $a_0, \dots, a_n \in K$ verschieden, $b_0, \dots, b_n \in K$. Dann gibt es genau ein $f \in K[X]$ mit $\mathsf{deg}(f) \le n$ und $f(a_i) = b_i$ für $0 \le i \le n$.*

Beweis. Eindeutigkeit. Seien f und g mit den gewünschten Eigenschaften gegeben. Dann gilt $(f-g)(a_i) = 0$ für $0 \le i \le n$ und $\mathsf{deg}(f-g) \le n$. Damit ist $f - g = 0$, also $f = g$.

Existenz. Es gibt zwei Möglichkeiten zur Berechnung:

1. Das Lagrangesche Interpolationspolynom

$$f = \sum_{i=0}^{n} b_i \frac{(X-a_0)\cdots(X-a_{i-1})(X-a_{i+1})\cdots(X-a_n)}{(a_i-a_0)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)}$$

hat die gewünschten Eigenschaften.

2. Wir verwenden den Ansatz

$$f = c_0 + c_1(X-a_0) + c_2(X-a_0)(X-a_1) + \cdots + c_n(X-a_0)\cdots(X-a_{n-1}).$$

Man berechne zunächst c_0 durch Einsetzen von a_0 für X. Hat man $c_0, \dots, c_{i-1}$ schon berechnet, so erhält man c_i durch Einsetzen von a_i für X $(i = 1, \dots, n)$ (Newtonsches Interpolationsverfahren). ☐

Das Verfahren von Kronecker kann man jetzt wie folgt beschreiben. Sei $f \in \mathbb{Z}[X]$ gegeben; oBdA seien die Koeffizienten von f teilerfremd. Gesucht sind alle Teiler $g \in \mathbb{Z}[X]$ von f. Dazu genügt es, alle Teiler $g \in \mathbb{Z}[X]$ mit $\mathsf{deg}(g) \le \frac{1}{2}\mathsf{deg}(f)$ zu bestimmen, denn die restlichen Teiler ergeben sich daraus durch Division.

Sei nun $s \in \mathbb{N}$, $s \leq \frac{1}{2}\mathsf{deg}(f)$. In den folgenden drei Schritten werden alle Polynome $g \in \mathbb{Z}[X]$ vom Grad s bestimmt, die f teilen:

Schritt 1. Wähle verschiedene $a_0, \ldots, a_s \in \mathbb{Z}$ mit $f(a_i) \neq 0$ für $0 \leq i \leq s$. Bestimme alle Teiler der $f(a_i)$.

Schritt 2. Zu jedem $(s+1)$-Tupel $(b_0, \ldots, b_s)$ mit $b_i | f(a_i)$ für $0 \leq i \leq s$ berechne man das Polynom $g \in \mathbb{Q}[X]$ mit $\mathsf{deg}(g) \leq s$ und $g(a_i) = b_i$ für alle i (nach Lemma 4.5.3).

Schritt 3. Diejenigen der in Schritt 2 erhaltenen Polynome, die in $\mathbb{Z}[X]$ liegen, untersuche man darauf, ob sie f in $\mathbb{Z}[X]$ teilen (z.B. durch Division mit Rest).

Beispiel.

$$f = X^6 - 5X^5 + 6X^4 - 3X^3 + 15X^2 - 17X - 3 \in \mathbb{Z}[X].$$

Falls ein Linearfaktor $X - a$ von f existiert, muß $a|3$ gelten, also $a = \pm 1, \pm 3$. Durch Probieren erhält man $f(3) = 0$. Division mit Rest liefert

$$f = (X-3)g \quad \text{mit} \quad g = X^5 - 2X^4 - 3X^2 + 6X + 1.$$

Es ist $g(1) \neq 0$ und $g(-1) \neq 0$, also ist von g kein Linearfaktor abspaltbar.

Mit dem Verfahren von Kronecker soll jetzt untersucht werden, ob ein quadratischer Faktor von g existiert.

Schritt 1.

$$\begin{array}{lll} a_0 = 0 & g(a_0) = 1 & \pm 1 \\ a_1 = 2 & g(a_1) = 1 & \pm 1 \\ a_2 = 1 & g(a_2) = 3 & \pm 1, \pm 3, \end{array}$$

wobei die letzte Spalte jeweils die Teiler darstellt.

Schritte 2 und 3. Es gibt 16 Tripel (b_0, b_1, b_2) mit $b_i | g(a_i)$. Sei oBdA $b_0 = 1$ (dann kennt man alle Polynome $h \in \mathbb{Q}[X]$ mit $h(a_0) = 1$, $h(a_1)|g(a_1)$ und $h(a_2)|g(a_2)$, so kennt man auch alle Polynome $q \in \mathbb{Q}[X]$ mit $q(a_0) = -1$, $q(a_1)|g(a_1)$ und $q(a_2)|g(a_2)$. Ist nämlich q ein solches Polynom, so kommt $-q$ unter den h vor). Wir bestimmen jeweils $h \in \mathbb{Q}[X]$ mit $h(0) = 1$, $h(2) = b_1$ und $h(1) = b_2$. Für den Schritt 3 untersuchen wir im Fall $h \in \mathbb{Z}[X]$, ob $h|g$ in $\mathbb{Z}[X]$.

(1) $b_1 = 1, b_2 = 1$, also $h = 1$. Es gilt dann $h|g \in \mathbb{Z}[X]$, aber h ist kein echter Teiler.

(2) $b_1 = 1$, $b_2 = -1$. Ansatz nach dem Newtonschen Interpolationsverfahren: $h = c_0 + c_1 X + c_2 X(X-2)$. Man erhält

$$\begin{array}{ll} h(0) = 1 & \Longrightarrow c_0 = 1 \\ h(2) = 1 & \Longrightarrow c_1 = 0 \\ h(1) = -1 & \Longrightarrow c_2 = 2. \end{array}$$

Also ist $h = 1 + 2X(X-2) = 2X^2 - 4X + 1$. Es ist $h \nmid g \in \mathbb{Z}[X]$, da g normiert ist.

(3) $b_1 = 1$, $b_2 = 3$. Analog zu (2) erhält man $h = 1 - 2X(X-2) = -2X^2 + 4X + 1$, also $h \nmid g \in \mathbb{Z}[X]$.

(4) $b_1 = 1$, $b_2 = -3$, also $h = 1 + 4X(X-2)$, also $h \nmid g \in \mathbb{Z}[X]$.

(5) $b_1 = -1$, $b_2 = 1$. Es muß gelten:

$$\begin{aligned} h(2) = -1 &\quad\Longrightarrow c_1 = -1 \\ h(1) = 1 &\quad\Longrightarrow c_2 = -1, \end{aligned}$$

also $h = 1 - X - X(X-2) = -X^2 + X + 1$. Es ist $h(-2)\nmid g(-2)$, also $h\nmid g \in \mathbb{Z}[X]$.

(6) $b_1 = -1$, $b_2 = -1$, also $h = 1 - X + X(X-2) = X^2 - 3X + 1$. Es ist $h(-1)\nmid g(-1)$, also $h\nmid g \in \mathbb{Z}[X]$.

(7) $b_1 = -1$, $b_2 = 3$, also $h = 1 - X - 3X(X-2)$, also $h\nmid g \in \mathbb{Z}[X]$.

(8) $b_1 = -1$, $b_2 = -3$, also $h = 1 - X + 3X(X-2)$, also $h\nmid g \in \mathbb{Z}[X]$.

Also ist $g = X^5 - 2X^4 - 3X^2 + 6X + 1$ irreduzibel in $\mathbb{Z}[X]$.

In Spezialfällen kommt man gelegentlich mit weniger Rechenaufwand ans Ziel.

Satz 4.5.4. *(Eisensteinsches Irreduzibilitätskriterium). Sei*

$$f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

mit teilerfremden Koeffizienten, $a_n \neq 0$, $n > 0$. Gibt es dann eine Primzahl p mit

$$p|a_0, \ldots, p|a_{n-1},\ p\nmid a_n,\ p^2\nmid a_0,$$

so ist f irreduzibel in $\mathbb{Z}[X]$.

Beweis. Gelte $f = a_n X^n + \cdots + a_0 = (b_k X^k + \cdots + b_0)(c_l X^l + \cdots + c_0) = gh$ mit $b_k, c_l \neq 0$. Aus $p|a_0$, $p^2\nmid a_0$ folgt, daß p entweder b_0 oder c_0 teilt. OBdA $p|b_0$ und $p\nmid c_0$. Aus $p\nmid a_n$ folgt $p\nmid b_k$. Sei j minimal mit $p\nmid b_j$. Dann gilt $1 \leq j \leq k$. Es ist

$$a_j = b_j c_0 + b_{j-1} c_1 + \cdots + b_0 c_j,$$

und $p|b_{j-1}, \ldots, p|b_0$, aber $p\nmid b_j$. $p\nmid c_0$. Also gilt $p\nmid a_j$. Nach Voraussetzung teilt p aber a_0 bis a_{n-1}. Damit ist $j = n$ und wegen $j \leq k \leq n$ auch $k = n$, d.h. $l = 0$ und $h = 1$. Also ist f irreduzibel in $\mathbb{Z}[X]$. □

Beispiel. $X^2 - 6X + 2$ ist irreduzibel in $\mathbb{Z}[X]$ (also auch in $\mathbb{Q}[X]$), ebenso $X^2 - 6X + 3$. Allgemein gilt: $X^n - p$ (mit $n \geq 2$, p Primzahl) ist irreduzibel in $\mathbb{Z}[X]$.

Satz 4.5.5. *(Reduktionsverfahren). Sei $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ mit teilerfremden Koeffizienten, $a_n \neq 0$, $n > 0$ und p eine Primzahl mit $p\nmid a_n$. $\rho\colon \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ sei die Fortsetzung des kanonischen Epimorphismus $\mathbb{Z} \to \mathbb{Z}_p$ auf die Polynomringe. Dann gilt:*

Ist $\rho(f)$ irreduzibel in $\mathbb{Z}_p[X]$, so ist f irreduzibel in $\mathbb{Z}[X]$.

Beweis. Gelte $f = gh$ mit $g, h \in \mathbb{Z}[X]$. Es ist $\rho(f) = \rho(g)\rho(h)$ und $\mathsf{deg}(\rho(f)) = n$, da $p\nmid a_n$. Daraus folgt $\mathsf{deg}(\rho(g)) = \mathsf{deg}(g)$ und $\mathsf{deg}(\rho(h)) = \mathsf{deg}(h)$. Da nun $\rho(f)$ irreduzibel ist in $\mathbb{Z}_p[X]$, gilt $\mathsf{deg}(\rho(g)) = 0$ oder $\mathsf{deg}(\rho(h)) = 0$, also $g = 1$ oder $h = 1$. Demnach ist f irreduzibel in $\mathbb{Z}[X]$. □

Beispiel. $f = X^5 - X^2 + 1$. Wähle $p = 2$. Dann ist $\rho(f) = X^5 + X^2 + 1$. Es genügt zu zeigen, daß $\rho(f)$ irreduzibel in $\mathbb{Z}_2[X]$ ist. Wegen $\rho(f)(0) = 1 \neq 0$ und $\rho(f)(1) = 1 \neq 0$ ist kein Linearfaktor abspaltbar. Als quadratische Funktionen kommen nur X^2+X+1, X^2+X, X^2+1 und X^2 in Frage. X^2+X und X^2 sind keine Teiler von $\rho(f)$, da sonst $\rho(f)(0) = 0$ sein müßte. X^2+1 ist kein Teiler von $\rho(f)$, da sonst $\rho(f)(1) = 0$ sein müßte. X^2+X+1 ist kein Teiler von $\rho(f)$, denn Division mit Rest ergibt $X^5 + X^2 + 1 = (X^2 + X + 1)(X^3 + X^2) + 1 \in \mathbb{Z}_2[X]$. Damit ist nach Satz 4.5.5 f irreduzibel in $\mathbb{Z}[X]$.

Kapitel 5

Anwendungen der Galois-Theorie

5.1 Einheitswurzeln

Die Nullstellen des Polynoms $X^n - 1$ nennt man n-te Einheitswurzeln. Zum Beispiel hat $X^3 - 1 \in \mathbb{Q}[X]$ in $\mathbb{C}$ die Nullstellen 1, $e^{\frac{2\pi i}{3}}$ und $e^{\frac{4\pi i}{3}}$. Hauptergebnis dieses Paragraphen wird sein, daß die Galoisgruppe von $X^n - 1 \in \mathbb{Q}[X]$, d.h. die Galoisgruppe $\Gamma_{\mathbb{Q}}^{Z}$ (Z Zerfällungskörper von $X^n - 1$), isomorph zu $\mathbb{Z}_n^*$ ist.

In diesem Abschnitt sei k ein Körper und n kein Vielfaches der Charakteristik von k.

Lemma 5.1.1. *$X^n - a$ mit $a \neq 0$ hat nur einfache Nullstellen.*

Beweis. Sei $f := X^n - a$. Dann ist $f' = nX^{n-1}$. Für $b \neq 0$ gilt $f'(b) = nb^{n-1} \neq 0$, also ist $b \neq 0$ höchstens einfache Nullstelle. 0 ist keine Nullstelle, denn $f(0) = -a$. □

Ein $\varepsilon \in k$ heißt *n-te Einheitswurzel*, wenn $\varepsilon^n = 1$.

Lemma 5.1.2. *Die n-ten Einheitswurzeln in k bilden eine multiplikative Gruppe.*

Beweis. Die Menge der n-ten Einheitswurzeln ist nicht leer, da 1 eine n-te Einheitswurzel ist. 0 ist keine n-te Einheitswurzeln, also sind alle n-ten Einheitswurzeln in k^*. Seien ε, η n-te Einheitswurzeln, also $\varepsilon^n = 1$ und $\eta^n = 1$. Dann gilt $(\frac{\varepsilon}{\eta})^n = \varepsilon^n \eta^{-n} = 1$. □

Im Rest des Abschnitts sei Z Zerfällungskörper von $X^n - 1 \in k[X]$. Man nennt Z den *Körper der n-ten Einheitswurzeln*.

Satz 5.1.3. *1. Die Gruppe der n-ten Einheitswurzeln in Z ist zyklisch von der Ordnung n. Ihre erzeugenden Elemente nennt man* primitive n-te Einheitswurzeln.

2. Sei $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ die Gruppe der n-ten Einheitswurzeln in Z. Dann gibt es genau $\varphi(n)$ primitive n-te Einheitswurzeln, und zwar genau alle ε^i mit i zu n teilerfremd ($1 \leq i \leq n-1$).

Beweis. 1. Die Gruppe der n-ten Einheitswurzeln ist eine endliche Untergruppe der multiplikativen Gruppe Z^*. Damit ist die Gruppe zyklisch nach Satz 3.4.13. Da alle Nullstellen von $X^n - 1$ einfach sind, gibt es genau n verschiedene n-te Einheitswurzeln.

2. a. Sei i zu n teilerfremd. Gelte $(\varepsilon^i)^j = 1$. Da ε primitive n-te Einheitswurzel ist, folgt $n|ij$, also $n|j$. Also ist ε^i primitive n-te Einheitswurzel.

b. Sei umgekehrt ε^i primitive n-te Einheitswurzel und $r = \mathsf{ggT}(i,n)$. Dann ist $(\varepsilon^{\frac{i}{r}})^n = (\varepsilon^i)^{\frac{n}{r}} = 1$. Da ε^i primitive n-te Einheitswurzel ist, folgt $r = 1$.

Primitive n-te Einheitswurzeln sind also genau alle ε^i $(1 \leq i \leq n-1)$ mit $\mathsf{ggT}(i,n) = 1$. Nach Satz 3.1.16 gibt es davon genau $\varphi(n)$ Stück. □

Bemerkung. Sei $\{a_1, \ldots, a_n\} \subseteq k^*$ endliche Untergruppe. Dann gilt: $a_i^n = 1$ für alle i, $1 \leq i \leq n$. Also ist a_i n-te Einheitswurzel in k und $\{a_1, \ldots, a_n\}$ die Gruppe der n-ten Einheitswurzeln, da höchstens n Einheitswurzeln existieren.

Satz 5.1.4. *Z ist galoissch über k, und Γ_k^Z ist isomorph zu einer Untergruppe der Gruppe $\mathbb{Z}_n^*$ (insbesondere also abelsch).*

Beweis. Nach Lemma 5.1.1 ist $X^n - 1$ separabel, also ist $Z \supseteq k$ galoissch, da Z Zerfällungskörper eines separablen Polynoms ist. Sei ε primitive n-te Einheitswurzel, also $Z = k(\varepsilon)$. Betrachte die Abbildung

$$\begin{aligned} \Gamma_k^Z &\to \mathbb{Z}_n^* \\ \varphi &\mapsto \text{dasjenige } i \text{ mit } \varphi(\varepsilon) = \varepsilon^i. \end{aligned}$$

Die Abbildung ist wohldefiniert, da $\varphi(\varepsilon)$ primitive n-te Einheitswurzel ist, also von der Form ε^i mit i,n teilerfremd. Die Abbildung ist ein Homomorphismus, denn hat man $\varphi, \psi \in \Gamma_k^Z$ mit $\varphi \mapsto i$ und $\psi \mapsto j$, so gilt

$$(\psi \circ \varphi)(\varepsilon) = \psi(\varepsilon^i) = (\psi(\varepsilon))^i = \varepsilon^{j \cdot i},$$

d.h. $\psi \circ \varphi \mapsto j \cdot i$. Die Abbildung ist außerdem injektiv, denn ist $\varphi \mapsto 1$, so gilt $\varphi(\varepsilon) = \varepsilon$; wegen $\varphi \restriction k = \mathsf{id}_k$ und $Z = k(\varepsilon)$ folgt $\varphi = \mathsf{id}_Z$. □

Unser Ziel ist es zu zeigen, daß im Fall $k = \mathbb{Q}$ sogar $\Gamma_k^Z \cong \mathbb{Z}_n^*$ ist. Als Hilfsmittel verwenden wir die sogenannten Kreisteilungspolynome und ihre Irreduzibilität.

Definition 5.1.5. Seien $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln in Z. Dann heißt

$$f_n := (X - \varepsilon_1) \cdots (X - \varepsilon_{\varphi(n)}) \in Z[X]$$

das n-te *Kreisteilungspolynom*.

Satz 5.1.6. *f_n ist ganzzahlig.*

Beweis. Induktion nach n. OBdA sei $n > 1$. Es gilt

$$X^n - 1 = \prod_{d|n} f_d.$$

Begründung: Jede n-te Einheitswurzel ε ist primitive d-te Einheitswurzel für $d = \mathsf{ord}(\varepsilon)$, und jede primitive d-te Einheitswurzel ist n-te Einheitswurzel, da $d|n$. Außerdem sind alle Wurzeln verschieden.

Nach Induktionsvoraussetzung ist jedes f_d mit $d < n$ und $d|n$ ganzzahlig. (Beachte: n ist hier kein Vielfaches von $\mathsf{char}(k)$, also auch d nicht). Wir schreiben jetzt

$$X^n - 1 = \Big(\prod_{d|n, d<n} f_d\Big) f_n.$$

Nun ist das Produkt aller f_d mit $d|n$ und $d < n$ ganzzahlig mit höchstem Koeffizienten 1. Durch Koeffizientenvergleich ergibt sich daraus, daß f_n ganzzahlig ist. □

Beispiele. Sei $k = \mathbb{Q}$ und $Z \subseteq \mathbb{C}$. Es ist $f_1 = X - 1$, $f_2 = X + 1$. Wie im Beweis vorher werden die folgenden Kreisteilungspolynome berechnet:

$$\begin{array}{ll}
X^3 - 1 = f_1 f_3 = (X-1) f_3, & \text{also } f_3 = X^2 + X + 1. \\
X^4 - 1 = f_1 f_2 f_4 = (X^2-1) f_4, & \text{also } f_4 = X^2 + 1. \\
X^5 - 1 = f_1 f_5 = (X-1) f_5, & \text{also } f_5 = X^4 + X^3 + X^2 + X + 1. \\
X^6 - 1 = f_1 f_2 f_3 f_6 = (X^4 + X^3 - X - 1) f_6, & \text{also } f_6 = X^2 - X + 1.
\end{array}$$

Allgemein gilt für Primzahlen $p > 2$

$$X^p - 1 = f_1 f_p = (X-1) f_p, \quad \text{also} \quad f_p = \sum_{i=0}^{p-1} X^i.$$

Satz 5.1.7. *$f_n \in \mathbb{Q}[X]$ ist irreduzibel.*

Beweis. Wir schreiben $f_n(X)$ statt f_n. Für $f(X) = f = \sum_{i=0}^n a_i X^i$ sei $f(X^p) = \sum_{i=0}^n a_i X^{ip}$. Sei ε eine primitive n-te Einheitswurzel. Es genügt zu zeigen: $f_n(X)$ ist das Minimalpolynom zu ε. Sei $f(X)$ das Minimalpolynom zu ε. Dann genügt $\mathsf{deg}(f(X)) \geq \varphi(n) = \mathsf{deg}(f_n(X))$. Dazu reicht es zu zeigen: $f(\varepsilon^i) = 0$ für alle zu n teilerfremden i. Es gilt $X^n - 1 = q(X) f(X)$ für ein $q(X) \in \mathbb{Q}[X]$. OBdA sei $f(x) \in \mathbb{Z}[X]$ (Multiplikation mit dem Hauptnenner), $f(X) = a_m X^m + \cdots + a_1 X + a_0$, $a_l \in \mathbb{Z}$, $a_m > 0$. Sei $i \in \mathbb{N}$. Betrachte $f(X^i)$. Der Satz 3.4.6 von der Division mit Rest ergibt $f(X^i) = q_i(X) f(X) + r_i(X)$, wobei im Nenner der Koeffizienten nur Primfaktoren vorkommen, die auch in a_m vorkommen.

Schritt 1. $r_{n+i}(X) = r_i(X)$ (es gibt also höchstens n verschiedene Reste). *Beweis.*

$$\begin{aligned}
f(X^{n+i}) - f(X^i) &= \sum_{\nu=0}^m a_\nu (X^{(n+i)\nu} - X^{i\nu}) \\
&= \sum_{\nu=0}^m a_\nu X^{i\nu} (X^{n\nu} - 1) \\
&= g(X) \cdot (X^n - 1), \qquad \text{da } X^n - 1 \mid X^{n\nu} - 1 \\
&= h(X) \cdot f(X).
\end{aligned}$$

Die Behauptung folgt mit der Eindeutigkeit der Division mit Rest.

Schritt 2. Sei p Primzahl, $p \nmid a_m$. Dann teilt p den Zähler jedes Koeffizienten von $r_p(X)$.

Beweis. $r_p(X)$ ist auch Divisionsrest von $f(X^p) - (f(X))^p$. Andererseits gilt

$$f(X^p) - (f(X))^p = p \cdot g(X) \quad \text{mit } g(X) \in \mathbb{Z}[X],$$

denn $f(X) = \sum \pm X^m$ (z.B. $2X^3 - 3X^5 = X^3 + X^3 - X^5 - X^5 - X^5$). Also

$$\begin{aligned}(a+b)^p &\equiv a^p + b^p \mod p\\ (a-b)^p &\equiv a^p + (-1)^p b^p \mod p\\ &\equiv a^p - b^p \mod p,\end{aligned}$$

denn im Fall $p = 2$ ist $-1 = 1 \mod p$, und sonst ist p ungerade. Sei $g(X) = q(X)f(X) + r_g(X)$. Also $r_p(X) = pr_g(X)$. Mit $p \nmid a_m$ folgt die Behauptung.

Schritt 3. Sei $M \in \mathbb{N}$ mit $M > |a_m|$, $M >$ Betrag der Zähler der Koeffizienten aller Polynome $r_i(X)$. Dann gilt $r_p(X) = 0$ für jede Primzahl $p > M$. *Beweis.* Dies folgt direkt aus Schritt 2.

Schritt 4.

$$\left.\begin{array}{l} r_i(X) = 0\\ r_j(X) = 0\end{array}\right\} \Longrightarrow r_{ij}(X) = 0.$$

Beweis.

$$\left.\begin{array}{l} f(X^i) = q_i(X)f(X)\\ f(X^j) = q_j(X)f(X)\end{array}\right\} \Longrightarrow f(X^{ij}) = q_i(X^j)f(X^j) = q_i(X^j)q_j(X)f(X).$$

Damit folgt $r_{ij}(X) = 0$.

Schritt 5. $r_i(X) = 0$ für jedes zu n teilerfremde i. *Beweis.* Sei i zu n teilerfremd. Betrachte

$$i_1 = i + n \cdot \prod_{\substack{p \text{ Primzahl}\\ p \le M,\ p \nmid i}} p.$$

Keine Primzahl $\le M$ teilt i_1. Also hat i_1 nur Primfaktoren $> M$. Damit folgt $r_{i_1}(X) = 0$ nach den Schritten 3 und 4 und somit $r_i(X) = 0$ nach Schritt 1.

Schritt 6. $f(\varepsilon^i) = 0$ für jedes zu n teilerfremde i. *Beweis.* $f(X^i) = q_i(X)f(X)$ nach Schritt 5 und somit $f(\varepsilon^i) = q_i(\varepsilon)f(\varepsilon) = 0$. □

Satz 5.1.8. *Sei Z Zerfällungskörper von $X^n - 1 \in \mathbb{Q}[X]$. Dann ist Z galoissch über $\mathbb{Q}$ und $\Gamma_{\mathbb{Q}}^Z$ ist isomorph zu $\mathbb{Z}_n^*$.*

Beweis. Z ist galoissch über $\mathbb{Q}$, da Z Zerfällungskörper eines separablen Polynoms ist. Sei ε primitive n-te Einheitswurzel, also $Z = \mathbb{Q}(\varepsilon)$. $f_n \in \mathbb{Q}[X]$ ist irreduzibel, also das Minimalpolynom zu ε. Man erhält dann $\varphi(n) = \mathsf{deg}(f_n) = [\mathbb{Q}(\varepsilon) : \mathbb{Q}] = |\Gamma_{\mathbb{Q}}^Z|$. Es war schon gezeigt, daß $\Gamma_{\mathbb{Q}}^Z$ isomorph zu einer Untergruppe von $\mathbb{Z}_n^*$ ist. Mit $|\mathbb{Z}_n^*| = \varphi(n)$ folgt $\Gamma_{\mathbb{Q}}^Z \cong \mathbb{Z}_n^*$. □

5.2 Reine Polynome

Definition 5.2.1. Ein Polynom der Gestalt $X^n - a \in A[X]$ (A kommutativer Ring mit 1) heißt *reines Polynom*.

Satz 5.2.2. *Sei $k \subseteq K$ eine Körpererweiterung und $n \geq 2$ kein Vielfaches der Charakteristik von k. Ferner enthalte k die n-ten Einheitswurzeln. Dann gilt:*

1. *Ist K Zerfällungskörper eines reinen Polynoms $X^n - a \in k[X]$ mit $a \neq 0$, so ist K galoissch über k mit zyklischer Galoisgruppe.*

2. *K ist Zerfällungskörper eines irreduziblen Polynoms $X^n - a \in k[X]$ mit $a \neq 0$ genau dann, wenn K galoissch ist über k mit zyklischer Galoisgruppe und zusätzlich gilt $[K : k] = n$.*

Beweis. 1. Sei $a \neq 0$ und K Zerfällungskörper des reinen Polynoms $X^n - a \in k[X]$. Nach Lemma 5.1.1 ist $X^n - a$ separabel, also K galoissch über k. Sei $b \in K$ Nullstelle von $X^n - a$, und ε eine primitive n-te Einheitswurzel. Dann sind $b, \varepsilon b, \varepsilon^2 b, \ldots, \varepsilon^{n-1} b$ alle Nullstellen von $X^n - a$. Da k alle n-ten Einheitswurzeln enthält, gilt $K = k(b)$. Sei $\varphi \in \Gamma_k^K$. Es ist $0 = \varphi(0) = \varphi(b^n - a) = (\varphi(b))^n - a$, daher ist $\varphi(b)$ Nullstelle von $X^n - a$, also von der Form $\varepsilon^i b$. Betrachte die Abbildung

$$\begin{aligned} \Gamma_k^K &\to \mathbb{Z}_n \\ \varphi &\mapsto \text{dasjenige } i \text{ mit } \varphi(b) = \varepsilon^i b. \end{aligned}$$

Die Abbildung ist ein Homomorphismus, denn hat man $\varphi, \psi \in \Gamma_k^K$ mit $\varphi \mapsto i$ und $\psi \mapsto j$, so gilt

$$(\psi \circ \varphi)(b) = \psi(\varepsilon^i b) = \varepsilon^i \psi(b) = \varepsilon^{i+j} b, \quad \text{da } \varepsilon \in k.$$

Die Abbildung ist außerdem injektiv, denn aus $\varphi \mapsto 0$ folgt $\varphi(b) = b$, also $\varphi = \mathsf{id}_K$ wegen $K = k(b)$. Folglich ist Γ_k^K isomorph zu einer Untergruppe von $\mathbb{Z}_n$ und damit selbst zyklisch.

2. $\Longrightarrow$. Folgt aus der Überlegung in (1), denn wir hatten dort $K = k(b)$ für eine Nullstelle b von $X^n - a$. Da nach Voraussetzung $X^n - a$ irreduzibel ist, ist es das Minimalpolynom zu b, also $[K : k] = n$.

$\Longleftarrow$. Nach Voraussetzung ist $K \supseteq k$ galoissch, Γ_k^K zyklisch und $[K : k] = n$. Sei $\Gamma_k^K = (\varphi)$, ε primitive n-te Einheitswurzel und $a \in K \setminus k$. Wegen $|\Gamma_k^K| = [K : k] = n$ folgt $\varphi^n = \mathsf{id}_K$. Wir betrachten jetzt die *Lagrangesche Resolvente*

$$(\varepsilon, a) := \sum_{i=0}^{n-1} \varepsilon^i \varphi^i(a).$$

Es gilt

$$\begin{aligned} \varphi((\varepsilon, a)) &= \sum_{i=0}^{n-1} \varepsilon^i \varphi^{i+1}(a) && \text{da } \varepsilon \in k \\ &= \varepsilon^{-1} \sum_{i=0}^{n-1} \varepsilon^{i+1} \varphi^{i+1}(a) \\ &= \varepsilon^{-1}(\varepsilon, a) && \text{da } \varepsilon^n = 1 \text{ und } \varphi^n = \mathsf{id}_K, \end{aligned} \tag{5.1}$$

also

$$\varphi((\varepsilon, a)^n) = \varepsilon^{-n}(\varepsilon, a)^n = (\varepsilon, a)^n. \tag{5.2}$$

Nach (5.2) ist $X^n - (\varepsilon, a)^n \in k[X]$. Wir betrachten die Körpererweiterung $k \subseteq k((\varepsilon, a)) \subseteq K$. Da $K \supseteq k$ galoissch ist, ist auch $K \supseteq k((\varepsilon, a))$ galoissch, Es gilt

$$\Gamma_{k((\varepsilon,a))}^K = \{\mathsf{id}_K\},$$

da nach (5.1) (ε, a) von allen $\psi \in \Gamma_k^K$, $\psi \neq \mathsf{id}_K$, bewegt wird. Also ist $K = k((\varepsilon, a))$ und demnach K Zerfällungskörper von $X^n - (\varepsilon, a)^n \in k[X]$. Weiterhin ist $X^n - (\varepsilon, a)^n \in k[X]$ das Minimalpolynom zu (ε, a), da $[k((\varepsilon, a)) : k] = n$. Daher ist $X^n - (\varepsilon, a)^n$ irreduzibel. $\square$

5.3 Auflösbarkeit von Polynomen durch Radikale

Definition 5.3.1. Sei k ein Körper, $f \in k[X]$. f heißt *auflösbar durch Radikale*, wenn es eine Körperfolge $L_0, L_1, \ldots, L_r$ gibt mit

1. $k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r$, wobei $L_i = L_{i-1}(\bar{a}_i)$ ist, $\bar{a}_i$ Nullstelle eines Polynoms $X^{n_i} - a_i \in L_{i-1}[X]$ und n_i Primzahl.
2. f zerfällt in L_r.

Hauptergebnis dieses Abschnitts wird sein, daß ein Polynom genau dann durch Radikale auflösbar ist, wenn seine Galoisgruppe auflösbar ist.

Satz 5.3.2. *Sei k ein Körper, $f \in k[X]$ auflösbar durch Radikale, wobei keine der Primzahlen n_i der Definition die Charakteristik von k teilt. Dann gibt es eine Körperfolge $M_0, M_1, \ldots, M_s$ mit*

1. *$k = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_s$, wobei $M_i = M_{i-1}(\bar{b}_i)$, $\bar{b}_i$ Nullstelle eines Polynoms $X^{m_i} - b_i \in M_{i-1}[X]$ und m_i Primzahl.*
2. *f zerfällt in M_s.*
3. *M_s ist galoissch über k.*
4. *$\{m_1, \ldots, m_s\} = \{n_1, \ldots, n_r\}$.*
5. *Jedes M_i ist Zerfällungskörper des separablen Polynoms*
$$X^{m_i} - b_i \in M_{i-1}[X],$$
insbesondere galoissch über M_{i-1}.

Beweis. Im Beweis gelten die Bezeichnungen aus der obigen Definition. Es werden zwei Körperfolgen nach dem Schema

$$\begin{array}{ccccccccccc}
k & = & L_0 & \subseteq & L_1 & \subseteq & L_2 & \subseteq & \ldots & \subseteq & L_r \\
 & & \cap\!\!| & & \cap\!\!| & & \cap\!\!| & & & & \\
 & & N_0 & \subseteq & N_1 & \subseteq & N_2 & \subseteq & \ldots & & \\
 & & \cap\!\!| & & \cap\!\!| & & \cap\!\!| & & & & \\
L_r & \subseteq & K_0 & \subseteq & K_1 & \subseteq & K_2 & \subseteq & \ldots & &
\end{array}$$

konstruiert. $L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r$ ist die nach Voraussetzung existierende Körperfolge.

Vorschritt. Wähle $K_0 \supseteq L_r$ so daß

$$f_0 := (X^{n_1} - 1) \cdots (X^{n_r} - 1) \in k[X]$$

in K_0 zerfällt. $N_0 \subseteq K_0$ sei Zerfällungskörper von f_0. Da nach Voraussetzung $n_i \nmid \mathsf{char}(k)$ für alle i, ist f separabel, also N_0 galoissch über k. Sei ε_i primitive n_i-te Einheitswurzel. Dann gilt $N_0 = k(\varepsilon_1, \ldots, \varepsilon_r)$ und

$$k \subseteq k(\varepsilon_1) \subseteq k(\varepsilon_1, \varepsilon_2) \subseteq \cdots \subseteq k(\varepsilon_1, \ldots, \varepsilon_r) = N_0.$$

Dann ist $k(\varepsilon_1, \ldots, \varepsilon_i)$ Zerfällungskörper des separablen Polynoms $X^{n_i} - 1$ über $k(\varepsilon_1, \ldots, \varepsilon_{i-1})$.

Schritt 1. Es ist $X^{n_1} - a_1 \in N_0[X]$, da $a_1 \in L_0 = k$. Ferner ist $\mathsf{FK}(\Gamma_k^{N_0}) = k$, da N_0 galoissch über k ist. Sei

$$g_1 := \prod_{\varphi(a_1) \text{ verschieden},\ \varphi \in \Gamma_k^{N_0}} (X^{n_1} - \varphi(a_1)) \in k[X].$$

(Da $a_1 \in \mathsf{FK}(\Gamma_k^{N_0})$, gilt $g_1 = X^{n_1} - a_1$; es wurde allerdings die allgemeine Darstellung gewählt, um die Analogie zu den anderen Schritten zu zeigen). Wähle $K_1 \supseteq K_0$ so, daß $f_1 := f_0 g_1 \in k[X]$ in K_1 zerfällt. $N_1 \subseteq K_1$ sei der Zerfällungskörper von f_1. N_1 ist galoissch über k, denn ist b eine Nullstelle von g_1, so sind $b, b\varepsilon_1, \ldots, b\varepsilon_1^{n_1-1}$ verschiedene Nullstellen, also g_1 und damit auch f_1 separabel. Ferner gilt

$$\begin{aligned} N_0 \subseteq N_1, &\quad \text{da } N_0 = k(\varepsilon_1, \ldots, \varepsilon_r),\ \varepsilon_1, \ldots, \varepsilon_r \in K_1 \text{ und } f_1(\varepsilon_i) = 0 \\ L_1 \subseteq N_1, &\quad \text{da } L_1 = L_0(\bar{a}_1),\ \bar{a}_1 \in L_1 \subseteq L_r \subseteq K_1 \text{ und } f_1(\bar{a}_1) = 0. \end{aligned}$$

Von N_0 kommt man zu N_1 durch Adjunktion einer Nullstelle des Polynoms $X^{n_1} - a_1$, da N_0 alle n_1-ten Einheitswurzeln enthält.

Schritt 2. Es ist $X^{n_2} - a_2 \in N_1[X]$, da $a_2 \in L_1 \subseteq N_1$. Ferner ist $\mathsf{FK}(\Gamma_k^{N_1}) = k$, da N_1 galoissch über k ist. Sei

$$g_2 := \prod_{\varphi(a_2) \text{ verschieden},\ \varphi \in \Gamma_k^{N_1}} (X^{n_2} - \varphi(a_2)).$$

Wie in Lemma 4.3.3 zeigt man $g_2 \in k[X]$. Wähle $K_2 \supseteq K_1$ so, daß $f_2 := f_1 g_2 \in k[X]$ in K_2 zerfällt. $N_2 \subseteq K_2$ sei der Zerfällungskörper von f_2. N_2 ist galoissch über k, denn mit b sind $b, b\varepsilon_2, b\varepsilon_2^2, \ldots, \varepsilon_2^{n_2-1}$ verschiedene Nullstellen, und für $\varphi(a_2) \neq \psi(a_2)$ ist keine Nullstelle von $X^{n_2} - \varphi(a_2)$ auch Nullstelle von $X^{n_2} - \psi(a_2)$; also ist g_2 und damit auch f_2 separabel. Ferner gilt

$$\begin{aligned} N_1 \subseteq N_2, &\quad \text{da } N_1 \text{ Zerfällungskörper von } f_1 \\ &\quad \text{und } N_2 \text{ Zerfällungskörper von } f_2 = f_1 g_2 \text{ ist}, \\ L_2 \subseteq N_2, &\quad \text{da } L_2 = L_1(\bar{a}_2),\ \bar{a}_2 \in L_2 \subseteq L_r \subseteq K_2 \text{ und } f_2(\bar{a}_2) = 0. \end{aligned}$$

Von N_1 kommt man zu N_2 durch sukzessive Adjunktion von je einer Nullstelle der $X^{n_2} - \varphi(n_2)$. Jede solche Adjunktion liefert einen Zerfällungskörper des jeweiligen $X^{n_2} - \varphi(a_2)$.

Nach r solchen Schritten bricht das Verfahren ab und man erhält die gesuchte Körperfolge. ∎

Man kann also oBdA annehmen, daß in der Definition 5.3.1 der Auflösbarkeit durch Radikale jeder Körper L_i galoissch ist über dem vorangehenden Körper L_{i-1} und ferner der letzte Körper L_r galoissch über k ist. Dies wird im Beweis des folgenden Satzes gebraucht.

Satz 5.3.3. *Sei k ein Körper mit $\mathsf{char}(k) = 0$ und $f \in k[X]$ nicht konstant. Dann sind folgende Aussagen äquivalent.*

1. *f ist auflösbar durch Radikale.*

2. *Γ_k^Z ist auflösbar, wobei Z Zerfällungskörper von f ist.*

Beweis. 1 $\Longrightarrow$ 2. Sei $k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r$ die laut Voraussetzung existierende Körperfolge. Nach dem vorangehenden Satz können wir annehmen, daß L_r galoissch über k ist. Die entsprechenden Gruppen nach dem Hauptsatz der Galois-Theorie sind

$$\Gamma_k^{L_r} \supseteq \Gamma_{L_1}^{L_r} \supseteq \cdots \supseteq \Gamma_{L_r}^{L_r} = \{e\}. \tag{5.3}$$

Es gilt

L_r ist galoissch über L_{i-1}	nach Lemma 2.3.3
$L_{i-1} \subseteq L_i \subseteq L_r$	
L_i ist galoissch über L_{i-1}	nach dem vorangehenden Satz
$\Gamma_{L_i}^{L_r}$ ist Normalteiler in $\Gamma_{L_{i-1}}^{L_r}$	nach dem Hauptsatz der Galois-Theorie
(5.3) ist eine Normalreihe.	

Wir zeigen jetzt, daß die Faktoren von (5.3) abelsch sind, also $\Gamma_k^{L_r}$ auflösbar ist.

$\Gamma_{L_{i-1}}^{L_r}/\Gamma_{L_i}^{L_r} \cong \Gamma_{L_{i-1}}^{L_i}$	nach dem Hauptsatz
$\Gamma_{L_{i-1}}^{L_i}$ ist zyklisch	nach Satz 5.2.2. da L_i Zerfällungskörper des reinen Polynoms $X^{n_i} - a_i \in L_{i-1}[X]$ ist
$\Gamma_{L_{i-1}}^{L_i}$ ist abelsch.	

Nun ist noch zu zeigen, daß auch Γ_k^Z auflösbar ist. Es gilt $k \subseteq Z \subseteq L_r$, und Z ist Zerfällungskörper von $f \in k[X]$. Da f separabel ist, ist Z galoissch über k, also liefert wiederum der Hauptsatz

$$\Gamma_k^Z \cong \Gamma_k^{L_r}/\Gamma_Z^{L_r}.$$

Daher ist Γ_k^Z als homomorphes Bild der auflösbaren Gruppe $\Gamma_k^{L_r}$ selbst auflösbar (nach Satz 1.5.7).

2 $\Longrightarrow$ 1. Wegen $\mathsf{char}(k) = 0$ ist f separabel, also Z galoissch über k. Also ist Γ_k^Z nicht nur auflösbar, sondern auch endlich. Dann gilt nach Satz 1.5.12, daß Γ_k^Z eine Normalreihe mit zyklischen Faktoren von Primzahlordnung hat, etwa

$$\Gamma_k^Z = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{e\}.$$

Der Hauptsatz liefert die entsprechende Körperfolge

$$k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r = Z.$$

Da G_i Normalteiler in G_{i-1} ist, erhält man

L_i ist galoissch über L_{i-1}

$\Gamma_{L_{i-1}}^{L_i} \cong \Gamma_{L_{i-1}}^Z/\Gamma_{L_i}^Z = G_{i-1}/G_i$ ist zyklisch von Primzahlordnung n_i

$[L_i : L_{i-1}] = n_i$

Um den Satz 5.2.2 anwenden zu können, braucht man noch geeignete Einheitswurzeln. Adjungiere zu Z je eine primitive n_i-te Einheitswurzel ε_i. Betrachte dann

$$k \subseteq k(\varepsilon_1) \subseteq \cdots \subseteq k(\varepsilon_1, \ldots, \varepsilon_r) \subseteq L_1(\varepsilon_1, \ldots, \varepsilon_r) \subseteq \cdots \subseteq Z(\varepsilon_1, \ldots, \varepsilon_r).$$

Es reicht nun zu zeigen, daß $L_i(\varepsilon_1, \ldots, \varepsilon_r)$ galoissch über $L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r)$ ist mit zyklischer Galoisgruppe und $[L_i(\varepsilon_1, \ldots, \varepsilon_r) : L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r)] =: m_i$, wobei $m_i = 1$ oder $m_i = n_i$ ist. Im Fall $m_i = 1$ sind wir dann fertig, und im Fall $m_i = n_i$ folgt nach Satz 5.2.2, daß $L_i(\varepsilon_1, \ldots, \varepsilon_r)$ Zerfällungskörper eines (sogar irreduziblen) Polynoms $X^{n_i} - a_i \in L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r)[X]$ ist, also $L_i(\varepsilon_1, \ldots, \varepsilon_r) = L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r)(\bar{a}_i)$, $\bar{a}_i$ Nullstelle von $X^{n_i} - a_i$. Also ist f auflösbar durch Radikale.

Zum Beweis betrachten wir die Körpererweiterungen

$$\begin{array}{ccccc} L_{i-1} & \subseteq & L_i & \subseteq & L_i(\varepsilon_1, \ldots, \varepsilon_r) \\ L_{i-1} & \subseteq & L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r) & \subseteq & L_i(\varepsilon_1, \ldots, \varepsilon_r) \end{array}$$

und setzen $[L_i(\varepsilon_1, \ldots, \varepsilon_r) : L_i] =: l_i$ und $[L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r) : L_{i-1}] =: s_i$. Der Gradsatz liefert

$$n_i l_i = s_i m_i.$$

Zunächst gilt

L_i ist galoissch über L_{i-1}
L_i ist Zerfällungskörper eines separablen Polynoms $g \in L_{i-1}[X]$
$L_i(\varepsilon_1, \ldots, \varepsilon_r)$ ist Zerfällungskörper von $(X^{n_1} - 1) \cdots (X^{n_r} - 1) \cdot g \in L_{i-1}[X]$
$L_i(\varepsilon_1, \ldots, \varepsilon_r)$ ist galoissch über L_{i-1}
$L_i(\varepsilon_1, \ldots, \varepsilon_r)$ ist galoissch über $L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r)$.

Zu zeigen ist also $m_i = n_i$ oder $m_i = 1$. Betrachte dazu die Abbildung

$$\begin{aligned} \Gamma_{L_i}^{L_i(\varepsilon_1, \ldots \varepsilon_r)} &\to \Gamma_{L_{i-1}}^{L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r)} \\ \varphi &\mapsto \varphi \restriction L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r) \end{aligned}$$

Die Abbildung ist wohldefiniert, denn für jedes $\varphi \in \Gamma_{L_i}^{L_i(\varepsilon_1, \ldots, \varepsilon_r)}$ gilt

$$\varphi(L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r)) = L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r).$$

Zum Beweis beachte man, daß mit ε_j auch $\varphi(\varepsilon_j)$ primitive n_j-te Einheitswurzel ist. Damit ist $\subseteq$ klar. Für die umgekehrte Inklusion $\supseteq$ genügt es zu zeigen, daß $\varepsilon_j \in \varphi(L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r))$. Da nun $\varphi(\varepsilon_j)$ primitive n_j-te Einheitswurzel ist, gilt $\varphi(\varepsilon_j)^l = \varepsilon_j$ für ein geeignetes l, also auch $\varphi(\varepsilon_j^l) = \varepsilon_j$.

Die Abbildung ist trivialerweise ein Homomorphismus. Sie ist auch injektiv, denn ist $\varphi \restriction L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r) = \mathsf{id}_{L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r)}$, so folgt wegen $\varphi \in \Gamma_{L_i}^{L_i(\varepsilon_1, \ldots, \varepsilon_r)}$ auch $\varphi \restriction L_i = \mathsf{id}_{L_i}$, also $\varphi = \mathsf{id}_{L_i(\varepsilon_1, \ldots, \varepsilon_r)}$.

Damit ist $|\Gamma_{L_i}^{L_i(\varepsilon_1, \ldots, \varepsilon_r)}|$ ein Teiler von $|\Gamma_{L_{i-1}}^{L_{i-1}(\varepsilon_1, \ldots, \varepsilon_r)}|$, also $l_i | s_i$, d.h. $m_i | n_i$ und damit $m_i = n_i$ oder $m_i = 1$. $\square$

5.4 Das allgemeine Polynom n-ten Grades

Definition 5.4.1. Sei k ein Körper und $k(U_1, \dots, U_n)$ der Quotientenkörper des Integritätsrings $k[U_1, \dots, U_n]$ (U_i sind Unbestimmte). Dann heißt das Polynom

$$f = X^n - U_1 X^{n-1} + U_2 X^{n-2} - \dots + (-1)^n U_n \in k(U_1, \dots, U_n)[X]$$

das *allgemeine Polynom n-ten Grades* (bzgl. k).

Satz 5.4.2. *Das allgemeine Polynom n-ten Grades ist separabel (bzgl. k). Seine Galoisgruppe ist isomorph zu S_n.*

Beweis. Sei Z Zerfällungskörper von f und $y_1, \dots, y_n$ die Nullstellen von f in Z. Dann gilt $f = (X - y_1) \cdots (X - y_n)$, also

$$\begin{aligned} U_1 &= \sum_{i=1}^{n} y_i \\ U_2 &= \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} y_i y_j \\ &\vdots \\ U_n &= \prod_{i=1}^{n} y_i \end{aligned}$$

Also ist $Z = k(y_1, \dots, y_n)$. Gesucht ist $\Gamma^{k(y_1,\dots,y_n)}_{k(U_1,\dots,U_n)}$. Jedes $\varphi \in \Gamma^{k(y_1,\dots,y_n)}_{k(U_1,\dots,U_n)}$ permutiert die $y_1, \dots, y_n$, denn aus $0 = f(y_i)$ folgt $0 = \varphi(f(y_i)) = f(\varphi(y_i))$, da $\hat{\varphi}(f) = f$; also ist $\varphi(y_i) = y_j$.

Es soll nun gezeigt werden, daß zu jeder Permutation der $y_1, \dots, y_n$ genau ein $\varphi \in \Gamma^{k(y_1,\dots,y_n)}_{k(U_1,\dots,U_n)}$ gehört (daraus folgt dann $\Gamma^{k(y_1,\dots,y_n)}_{k(U_1,\dots,U_n)} \cong S_n$). Zu diesem Zweck betrachten wir ein ähnliches Polynom, bei dem Nullstellen und Unbestimmte vertauscht sind. Seien also $Y_1, \dots, Y_n$ Unbestimmte und $g \in k(Y_1, \dots, Y_n)[X]$ definiert durch

$$g = (X - Y_1) \cdots (X - Y_n).$$

Dann gilt $g = X^n - u_1 X^{n-1} + \dots + (-1)^n u_n$ mit

$$\begin{aligned} u_1 &= \sum_{i=1}^{n} Y_i \\ u_2 &= \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} Y_i Y_j \\ &\vdots \\ u_n &= \prod_{i=1}^{n} Y_i \end{aligned}$$

g ist ein separables Polynom über $k(u_1, \dots, u_n)$. Sein Zerfällungskörper ist $k(Y_1, \dots, Y_n)$. Also ist $k(Y_1, \dots, Y_n)$ galoissch über $k(u_1, \dots, u_n)$. Jedes $\varphi \in$

$\Gamma^{k(Y_1,\dots,Y_n)}_{k(u_1,\dots,u_n)}$ permutiert die $Y_1,\dots,Y_n$. (Begründung: $0 = g(Y_i)$, $0 = \varphi(g(Y_i)) = g(\varphi(Y_i))$, da $\hat{\varphi}(g) = g$, damit $\varphi(Y_i) = Y_j$). Umgekehrt bestimmt jede Permutation der $Y_1,\dots,Y_n$ ein $\varphi \in \Gamma^{k(Y_1,\dots,Y_n)}_{k(u_1,\dots,u_n)}$: Es existiert ein Ringautomorphismus ψ: $k[Y_1,\dots,Y_n] \to k[Y_1,\dots,Y_n]$ mit $\psi\restriction k = \mathsf{id}_k$, $\psi(Y_i) = Y_j$ (universelle Eigenschaft). Erweiterung auf den Quotientenkörper liefert: φ: $k(Y_1,\dots,Y_n) \to k(Y_1,\dots,Y_n)$, $\varphi \in \mathsf{Aut}(k(Y_1,\dots,Y_n))$, $\varphi(Y_i) = Y_j$. $u_1,\dots,u_n$ bleiben dabei fest, da alle u_i symmetrisch in den Y_l sind, z.B. $\varphi(u_1) = \sum_{i=1}^n \varphi(Y_i) = \sum_{j=1}^n Y_j = u_1$. Also gilt: $\Gamma^{k(Y_1,\dots,Y_n)}_{k(u_1,\dots,u_n)} \cong S_n$.

Jetzt soll ein Isomorphismus konstruiert werden, der die Eigenschaften von g auf f überträgt. Dazu benötigt man zuerst folgendes

Lemma 5.4.3. *Sei $h \in k[U_1,\dots,U_n]$. Dann gilt:*

$$\textit{Aus } h(u_1,\dots,u_n) = 0 \textit{ folgt } h = 0.$$

Beweis.

$$0 = h(u_1,\dots,u_n) = h\Big(\sum_{i=1}^n Y_1, \sum_{i=1}^{n-1}\sum_{j=i+1}^n Y_iY_j, \dots, \prod_{i=1}^n Y_i\Big).$$

Man denke sich das Polynom nach $Y_1^{\mu_1}\dots Y_n^{\mu_n}$ geordnet. Alle Koeffizienten müssen verschwinden, also

$$0 = h\Big(\sum_{i=1}^n y_1, \sum_{i=1}^{n-1}\sum_{j=i+1}^n y_iy_j, \dots, \prod_{i=1}^n y_i\Big) = h(U_1,\dots,U_n) = 0. \qquad \square$$

Fortsetzung des Beweises von 5.4.2. Man hat den kanonischen Ringhomomorphismus

$$k[U_1,\dots,U_n] \to k[u_1,\dots,u_n].$$

Dieser Homomorphismus ist surjektiv, und nach dem Lemma vorher auch injektiv, also bijektiv. Es gilt

$$\begin{tikzcd}
k[U_1,\dots,U_n] \arrow[r, "\cong"] \arrow[d] & k[u_1,\dots,u_n] \arrow[d] \\
k(U_1,\dots,U_n) \arrow[r, "\cong", "\psi"'] \arrow[d] & k(u_1,\dots,u_n) \arrow[d] \\
k(y_1,\dots,y_n) \arrow[r, "\cong"] & k(Y_1,\dots,Y_n)
\end{tikzcd}$$

Die erste Erweiterung ist die auf die Quotientenkörper. Wegen $\widehat{\psi}(f) = g$ liefert der zweite Erweiterungssatz die zweite Erweiterung. Folglich ist f separabel, $k(y_1,\dots,y_n)$ galoissch über $k(U_1,\dots,U_n)$ und

$$\Gamma^{k(y_1,\dots,y_n)}_{k(U_1,\dots,U_n)} \cong \Gamma^{k(Y_1,\dots,Y_n)}_{k(u_1,\dots,u_n)} \cong S_n. \qquad \square$$

Satz 5.4.4 (Abel). *Sei k ein Körper der Charakteristik 0. Das allgemeine Polynom n-ten Grades (bzgl. k) ist genau dann durch Radikale auflösbar, wenn $n \leq 4$.*

Beweis. Aus Satz 5.2.2 und dem vorangehenden Satz ergibt sich, daß das allgemeine Polynom n-ten Grades genau dann auflösbar ist, wenn auch S_n auflösbar ist. Im Abschnitt 1.5 und in Aufgabe 32 der Übungen war gezeigt worden, daß S_n auflösbar ist genau dann, wenn $n \leq 4$. □

5.5 Konstruktionen mit Zirkel und Lineal

Es soll untersucht werden, ob folgende "klassische Probleme" mit Zirkel und Lineal lösbar sind.

1. Dreiteilung eines beliebigen Winkels.
2. Delisches Problem: Verdoppelung eines Würfels, d.h. Konstruktion der Kantenlänge eines Würfels, dessen Volumen doppelt so groß ist wie das Volumen eines gegebenen Würfels.
3. Konstruktion eines regelmäßigen 7-Ecks (allgemein: n-Ecks).
4. Quadratur des Kreises, d.h. Konstruktion der Kantenlänge eines Quadrats, dessen Inhalt so groß ist wie der Inhalt eines gegebenen Kreises.

Als erstes ist es nötig, den Begriff "konstruierbar mit Zirkel und Lineal" zu präzisieren. In der euklidischen Geometrie ist

- eine Gerade bestimmt durch zwei Punkte,
- ein Kreis bestimmt durch den Mittelpunkt und einen weiteren Punkt auf dem Umfang und
- ein Winkel bestimmt durch den Ausgangspunkt und zwei Punkten auf den Schenkeln.

Also werden die gegebenen und gesuchten Größen durch endlich viele Punkte bestimmt. Die gegebenen Punkte $P_1, \ldots, P_n$ der Ebene werden mit Zahlen $z_1, \ldots, z_n \in \mathbb{C}$ identifiziert. OBdA können wir annehmen, daß P_1, P_2 den Zahlen $0, 1$ entsprechen; dies ist durch geeignete Wahl des Koordinatensystems immer erreichbar.

Definition 5.5.1. Seien $z_1, \ldots, z_n \in \mathbb{C}$ mit $z_1 = 0$ und $z_2 = 1$. Wir setzen $M_1 := \{z_1, \ldots, z_n\}$ und $M_{r+1} := M_r \cup \{ z \mid z$ ist

(a) Schnittpunkt zweier Geraden, die verschiedene Punkte aus M_r verbinden oder

(b) Schnittpunkt einer Geraden wie in (a) und eines Kreises um einen Punkt aus M_r mit einem Radius gleich einem Abstand zweier Punkte aus M_r oder

(c) Schnittpunkt zweier Kreise wie in (b) $\}$

und $K(z_1, \ldots, z_n) := \bigcup_{r=1}^{\infty} M_r$. Ein $z \in \mathbb{C}$ heißt *aus $z_1, \ldots, z_n$ mit Zirkel und Lineal konstruierbar*, wenn $z \in K(z_1, \ldots, z_n)$.

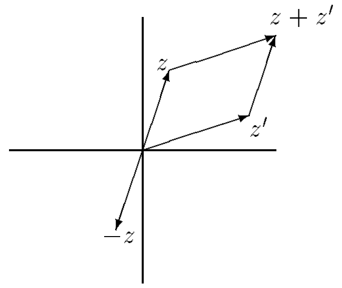
Bemerkung. Diese Definition stimmt mit dem üblichen unpräzisen Begriff “mit Zirkel und Lineal konstruierbar” überein. Fraglich ist höchstens die Wahl eines “beliebigen” Punktes in einem gegebenen Gebiet und die Wahl einer “beliebigen” Länge, die eine gegebene Ungleichung erfüllt. Doch auch dies ist durch die vorherige Definition abgedeckt, da $K(z_1, \ldots, z_n)$ in $\mathbb{C}$ dicht liegt.

Satz 5.5.2. *Seien $z_1, \ldots, z_n \in \mathbb{C}$ mit $z_1 = 0$ und $z_2 = 1$. Es ist $K(z_1, \ldots, z_n)$ der kleinste Unterkörper von $\mathbb{C}$, der $z_1, \ldots, z_n$ enthält und abgeschlossen ist gegen Ziehen von Quadratwurzeln und Konjugation, d.h. der*

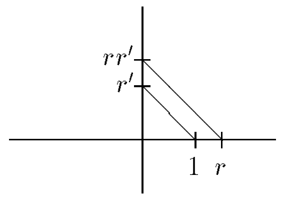
1. *$z_1, \ldots, z_n$ enthält,*
2. *mit z^2 stets auch z enthält,*
3. *mit z stets auch $\bar{z}$ enthält ($\bar{z} := x - iy$, falls $z = x + iy$, $x, y \in \mathbb{R}$).*

Beweis. Wir beginnen mit dem Beweis, daß $K(z_1, \ldots, z_n) \subseteq \mathbb{C}$ ein Unterkörper mit den angegebenen Eigenschaften ist. Seien also $z, z' \in K(z_1, \ldots, z_n)$.

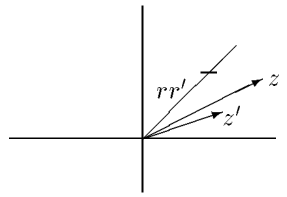
a. $z + z', -z \in K(z_1, \ldots, z_n)$ (siehe Zeichnung)



b. Sei $z = re^{i\nu}$, $z' = r'e^{i\nu'}$. Dann ist $zz' = rr'e^{i(\nu+\nu')} \in K(z_1, \ldots, z_n)$. Die Konstruktion kann man wie folgt durchführen.

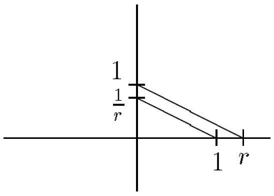


(Konstruktion der Parallele)



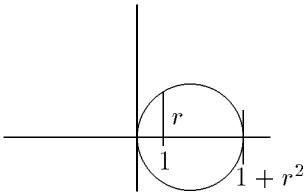
(Winkel werden addiert)

c. Sei $z = re^{i\nu}$. Um zu zeigen, daß $z^{-1} \in K(z_1, \ldots, z_n)$, reicht die Konstruktion von $\frac{1}{r}$, denn es ist $z^{-1} = \frac{1}{r}e^{-i\nu}$.



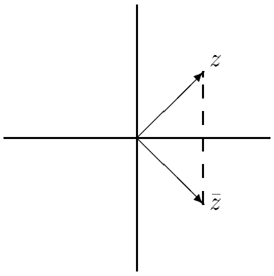
Aus (a) bis (c) folgt bereits, daß $K(z_1, \ldots, z_n)$ Unterkörper von $\mathbb{C}$ ist.

d. Wir zeigen jetzt, daß aus $z^2 \in K(z_1, \ldots, z_n)$ folgt $z \in K(z_1, \ldots, z_n)$. Sei $z = re^{i\nu}$, also $z^2 = r^2 e^{2i\nu}$. Es genügt zu zeigen, daß r aus r^2 konstruiert werden kann. Dies sieht man wie folgt.



Ist nämlich x der Radius, so gilt $r^2 + (x-1)^2 = x^2$, also $r^2 = 2x - 1$.

e. Mit z ist auch $\bar{z} \in K(z_1, \ldots, z_n)$.



Wir zeigen jetzt, daß $K(z_1, \ldots, z_n)$ der kleinste Unterkörper von $\mathbb{C}$ mit den angegebenen Eigenschaften (1)-(3) ist. Sei $K' \subseteq \mathbb{C}$ ein solcher Unterkörper. Es genügt zu zeigen

a. Schnittpunkte von Geraden, die durch Punkte in K' bestimmt sind, liegen in K'.

b. Schnittpunkte solcher Geraden mit Kreisen, deren Mittelpunkt in K' liegt und deren Radien gleich dem Abstand zweier Punkte in K' sind, liegen in K'.

c. Schnittpunkte zweier solcher Kreise liegen in K'.

Um den Beweis zu vereinfachen, wird zuerst gezeigt, daß für $x, y \in \mathbb{R}$ gilt

$$x + iy \in K' \text{ genau dann, wenn } x, y \in K'. \tag{5.4}$$

Es ist $i \in K'$ wegen $i^2 = -1 \in K'$. Damit ist $\Longleftarrow$ klar. $\Longrightarrow$. Es ist $x + iy$ und damit auch $x - iy \in K'$. Also folgt $2x \in K'$, somit auch $x \in K'$ und $iy \in K'$. Folglich ist auch $y \in K'$.

Mit (5.4) folgt. daß die Gleichung einer durch Punkte in K' bestimmten Geraden lautet

$$ax + by + c = 0 \qquad \text{mit } a, b, c \in \mathbb{R} \cap K'.$$

Die Gleichung von Kreisen mit Mittelpunkt in K' und Radius gleich dem Abstand zweier Punkte in K' lautet

$$x^2 + y^2 + dx + ey + f = 0 \qquad \text{mit } d, e, f \in \mathbb{R} \cap K'.$$

a. Die Koordinaten des Schnittpunktes zweier Geraden ergeben sich aus einem linearen Gleichungssystem, liegen also in K'.

b. *Fall* $b \neq 0$. Dann ist die Gerade durch eine Gleichung der Form $y = mx + r$ bestimmt. Falls Schnittpunkte existieren, ergeben sich die Abszissen aus der quadratischen Gleichung $x^2 + (mx + r)^2 + dx + c(mx + r) + f = 0$, liegen also in $\mathbb{R} \cap K'$. Die Ordinaten erhält man aus der Geradengleichung.

Fall $b = 0$, also $a \neq 0$. Wegen der Symmetrie in x und y kommt man wie im Fall 1 zum Ergebnis (Geradengleichung $x = s$).

c. Gesucht sind die Schnittpunkte von

$$\begin{aligned} &x^2 + y^2 + dx + ey + f = 0 \qquad \text{und} \\ &x^2 + y^2 + d'x + e'x + f' = 0. \end{aligned}$$

Diese sind dieselben wie die von

$$\begin{aligned} &x^2 + y^2 + dx + ey + f = 0 \qquad \text{und} \\ &(d - d')x + (e - e')y + (f - f') = 0. \end{aligned}$$

Also ergeben sich die Lösungen wie unter (b). □

Bemerkung. Es gilt $K(z_1, \ldots, z_n) \supseteq \{\, x + iy \mid x, y \in \mathbb{Q} \,\}$, also liegt $K(z_1, \ldots, z_n)$ dicht in $\mathbb{C}$.

Definition 5.5.3. Seien $z_1, \ldots, z_n \in \mathbb{C}$ mit $z_1 = 0$ und $z_2 = 1$. Setze

$$k := \mathbb{Q}(z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n).$$

Ein $z \in \mathbb{C}$ heißt *durch sukzessive Adjunktion von Quadratwurzeln konstruierbar* aus $z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n$, wenn es eine Folge $L_0, L_1, \ldots, L_r$ von Unterkörpern von $\mathbb{C}$ gibt mit

1. $k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r$, wobei $L_i = L_{i-1}(w_i)$ mit w_i Nullstelle eines Polynoms $X^2 - u_i \in L_{i-1}[X]$.

2. $z \in L_r$.

Satz 5.5.4. *Seien $z_1, \ldots, z_n \in \mathbb{C}$ mit $z_1 = 0$ und $z_2 = 1$. Ein $z \in \mathbb{C}$ ist in $K(z_1, \ldots, z_n)$ genau dann, wenn z durch sukzessive Adjunktion von Quadratwurzeln aus $z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n$ konstruierbar ist.*

Beweis. $\Longleftarrow$. $k \subseteq K(z_1, \ldots, z_n)$, da $K(z_1, \ldots, z_n)$ abgeschlossen ist gegen Konjugation. Es sind alle $L_i \subseteq K(z_1, \ldots, z_n)$, da $K(z_1, \ldots, z_n)$ abgeschlossen gegen das Ziehen von Quadratwurzeln ist.

$\Longrightarrow$. Für jeden Teilkörper $L \subseteq \mathbb{C}$ bestehe $\sqrt{L}$ aus allen Quadratwurzeln von Elementen aus L. Setze $K_0 := k$ und $K_{i+1} := K_i(\sqrt{K_i})$. Durch Induktion über i zeigen wir, daß jedes $z \in K_i$ aus k durch sukzessive Adjunktion von Quadratwurzeln konstruierbar ist. Für $i = 0$ ist nichts zu zeigen. Sei $v \in K_{i+1} = K_i(\sqrt{K_i})$. Es gibt dann $f, g \in K_i[X]$ und $w_1, \ldots, w_n \in \sqrt{K_i}$ mit

$$v = \frac{f(w_1, \ldots, w_n)}{g(w_1, \ldots, w_n)} \quad \text{und } g(w_1, \ldots, w_n) \neq 0.$$

Daraus folgt die Behauptung.

Es genügt zu zeigen, daß $K := \bigcup_i K_i$ ein Unterkörper von $\mathbb{C}$ ist, der gegen Konjugation und das Ziehen von Quadratwurzeln abgeschlossen ist. Aufgrund der Definition ist K gegen das Ziehen von Quadratwurzeln abgeschlossen. Wir beweisen durch Induktion über i, daß jedes K_i gegen Konjugation abgeschlossen ist. Für $K_0 = k$ gilt dies nach Definition. Im Induktionsschritt haben wir

$$\overline{K_{i+1}} = \overline{K_i(\sqrt{K_i})} = \overline{K_i}(\overline{\sqrt{K_i}}) = K_i(\sqrt{K_i}) = K_{i+1}$$

wegen

$$\begin{aligned}
\sqrt{K_i} &= \{\, w \mid w \text{ Nullstelle eines Polynoms } X^2 - u \in K_i[X] \,\} \\
\overline{\sqrt{K_i}} &= \{\, \overline{w} \mid w \text{ Nullstelle eines Polynoms } X^2 - u \in K_i[X] \,\} \\
&= \{\, \overline{w} \mid \overline{w} \text{ Nullstelle eines Polynoms } X^2 - \overline{u} \in K_i[X] \,\} \quad \text{da } K_i = \overline{K_i} \\
&= \sqrt{K_i}
\end{aligned}$$

□

Folgerung 5.5.5. *Seien $z_1, \ldots, z_n \in \mathbb{C}$, $z_1 = 0$, $z_2 = 1$ und*

$$k = \mathbb{Q}(z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n).$$

Ist $z \in \mathbb{C}$ aus $z_1, \ldots, z_n$ mit Zirkel und Lineal konstruierbar, so ist z algebraisch über k mit $[k(z) : k] = 2^s$ für ein $s \geq 0$.

Beweis. Sei $z \in K(z_1, \ldots, z_n)$, $k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r$, $L_i = L_{i-1}(w_i)$, w_i Nullstelle des Polynoms $X^2 - u_i \in L_{i-1}[X]$ und $z \in L_r$. Dann gilt: $[L_i : L_{i-1}] = 2$ oder 1, da entweder $X^2 - u_i \in L_{i-1}[X]$ irreduzibel und damit Minimalpolynom zu w_i ist oder schon $w_i \in L_{i-1}$ ist. Damit folgt $[L_r : k] = 2^r$ für ein $r \geq 0$. Wegen $[L_r : k] < \infty$ ist L_r algebraisch über k. Also ist z algebraisch über k und $k \subseteq k(z) \subseteq L_r$. Daher folgt aus dem Gradsatz $[k(z) : k] = 2^s$ für ein $s \geq 0$. □

Nach diesen Überlegungen können nun die am Anfang dises Abschnitts gestellten Probleme untersucht werden.

Folgerung 5.5.6. *Das Delische Problem ist mit Zirkel und Lineal* nicht *lösbar.*

Beweis. OBdA sei 1 die Kantenlänge des gegebenen Würfels. Dann müßte $\sqrt[3]{2}$ aus $0, 1$ konstruiert werden. Wir wenden die vorangehende Folgerung mit $k = \mathbb{Q}(0, 1, \bar{0}, \bar{1}) = \mathbb{Q}$ an. Es ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, da $X^3 - 2 \in \mathbb{Q}[X]$ irreduzibel ist, also das Minimalpolynom zu $\sqrt[3]{2}$ ist. Daher ist $\sqrt[3]{2}$ *nicht* mit Zirkel und Lineal konstruierbar. □

Folgerung 5.5.7. *Das regelmäßige 7-Eck ist* nicht *mit Zirkel und Lineal konstruierbar.*

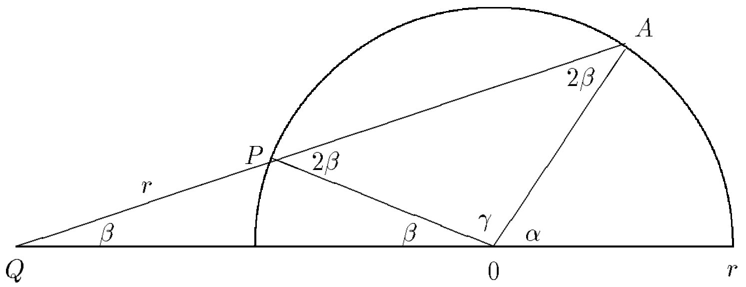
Beweis. Es müßte die erste Ecke des 7-Ecks, also $e^{\frac{2\pi i}{7}}$, aus $0, 1$ mit Zirkel und Lineal konstruiert werden. Wir verwenden Folgerung 5.5.5 mit $k = \mathbb{Q}$. Es gilt $[\mathbb{Q}(e^{\frac{2\pi i}{7}}) : \mathbb{Q}] = \varphi(n)$, da das n-te Kreisteilungspolynom f_n über $\mathbb{Q}$ irreduzibel ist. $\varphi(7) = 6$ ist keine Zweierpotenz, also ist $e^{\frac{2\pi i}{7}}$ aus $0, 1$ *nicht* mit Zirkel und Lineal konstruierbar. □

Mit derselben Überlegung ergibt sich: Ist $\varphi(n)$ keine Zweierpotenz, so ist $e^{\frac{2\pi i}{n}}$ aus $0, 1$ und damit das regelmäßige n-Eck nicht mit Zirkel und Lineal konstruierbar. In Satz 5.5.10 werden wir unter Einsatz der Galois-Theorie die Umkehrung beweisen.

Folgerung 5.5.8. *Die Quadratur des Kreises ist unmöglich.*

Beweis. OBdA habe der gegebene Kreis den Radius 1. Das gesuchte Quadrat hätte dann die Seitenlänge $\sqrt{\pi}$. Wir verwenden jetzt (hier ohne Beweis), daß π nicht algebraisch über $\mathbb{Q}$ ist; dies wurde zuerst von Lindemann 1882 bewiesen. Daher ist auch $\sqrt{\pi}$ nicht algebraisch über $\mathbb{Q}$, also aus $0, 1$ nicht mit Zirkel und Lineal konstruierbar. □

Bemerkung. Archimedes gab das folgende Verfahren zur Dreiteilung eines Winkels.



Dann ist

$$\begin{aligned} \gamma + 4\beta &= 180^\circ \\ \gamma + \beta + \alpha &= 180^\circ \\ 3\beta &= \alpha \end{aligned}$$

Aus dem gegebenen Winkel α erhält man nach obiger Skizze den Winkel $\beta = \frac{\alpha}{3}$. Allerdings handelt es sich dabei *nicht* um eine Konstruktion mit Zirkel und Lineal in unserem Sinne, da das Fixieren einer gegebenen Strecke auf dem Lineal und das Suchen der Punkte Q, P so, daß $\overline{QP} = r$ und Q, P und A auf einer Geraden liegen, nicht gestattet ist. Eine Dreiteilung eines Winkels meint vielmehr: Kann man aus den Punkten $z_1 = 0$, $z_2 = 1$ und $z_3 = \cos\alpha + i\sin\alpha$ den Punkt $z = \cos\frac{\alpha}{3} + i\sin\frac{\alpha}{3}$ konstruieren, d.h. ist $z \in K(z_1, z_2, z_3)$?

Folgerung 5.5.9. *Der Winkel von 60° läßt sich mit Zirkel und Lineal nicht in drei gleiche Teile teilen.*

Beweis. Sei $z_1 = 0$, $z_2 = 1$ und $z_3 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. Es gilt $K(z_1, z_2, z_3) = K(z_1, z_2)$, denn mit 3 liegt auch $\sqrt{3}$, also z_3 in $K(z_1, z_2)$. Läge also $z = \cos 20° + i \sin 20°$ in $K(0, 1)$, so wäre dies ein Eckpunkt des regelmäßigen 18-Ecks, dieses wäre also mit Zirkel und Lineal konstruierbar. Es ist aber $\varphi(18) = \varphi(2) \cdot \varphi(3^2) = 6$ keine Zweierpotenz, also ist das regelmäßige 18-Eck nicht mit Zirkel und Lineal konstruierbar aus $0, 1$. Daher ist auch der Winkel von 60° *nicht* mit Zirkel und Lineal in drei gleiche Teile teilbar. Es gibt also kein allgemeines Verfahren zur Dreiteilung eines Winkels. □

Im folgenden Satz wird nun die Galois-Theorie eingesetzt.

Satz 5.5.10. *Ist $\varphi(n)$ eine Zweierpotenz, so ist das regelmäßige n-Eck mit Zirkel und Lineal aus $0, 1$ konstruierbar.*

Beweis. Zu zeigen ist, daß $e^{\frac{2\pi i}{n}}$ aus $0, 1$ mit Zirkel und Lineal konstruierbar ist, d.h. $e^{\frac{2\pi i}{n}} \in K(0, 1)$. Dies soll unter Anwendung des Satzes 5.5.4 auf $k = \mathbb{Q}$ geschehen. f_n ist das Minimalpolynom zu $e^{\frac{2\pi i}{n}} \in \mathbb{C}$, und $\mathsf{deg}(f_n) = \varphi(n) = 2^s$ nach Voraussetzung. $Z := \mathbb{Q}(e^{\frac{2\pi i}{n}})$ ist Zerfällungskörper von $f_n \in \mathbb{Q}[X]$, also galoissch über $\mathbb{Q}$. Es ist $[Z : \mathbb{Q}] = 2^s$, also $|\Gamma^Z_{\mathbb{Q}}| = 2^s$. Daher ist $\Gamma^Z_{\mathbb{Q}}$ auflösbar, denn nach Folgerung 1.5.9 ist jede p-Gruppe auflösbar. Nach Satz 1.5.12 gibt es sogar eine Normalreihe mit zyklischen Faktoren von Primzahlordung, etwa

$$\Gamma^Z_{\mathbb{Q}} = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{\mathsf{id}_Z\}.$$

Da $[G_{i-1} : G_i]$ ein Teiler von $|G_0|$ ist, folgt $[G_{i-1} : G_i] = 2$, denn die Faktoren haben Primzahlordnung. Bilde mit dem Hauptsatz der Galois-Theorie die zugehörige Körperfolge

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_r = Z,$$

Dann ist $[L_i : L_{i-1}] = 2$. Der Satz 5.5.4 liefert die Behauptung, wenn noch gezeigt wird $L_i = L_{i-1}(w_i)$, w_i Nullstelle eines Polynoms $X^2 - u_i \in L_{i-1}[X]$. Sei dazu $x \in L_i \setminus L_{i-1}$. Wegen $[L_i : L_{i-1}] = 2$ sind $1, x, x^2$ linear abhängig über L_i. Es existieren also $a, b \in L_{i-1}$ mit $x^2 + ax + b = 0$. Damit gilt $(x + \frac{a}{2})^2 = (\frac{a^2}{4} - b) \in L_{i-1}$. Da $1, x$ linear unabhängig über L_{i-1}, also Basis von L_i sind, gilt $L_i = L_{i-1}(x) = L_{i-1}(x + \frac{a}{2})$. Setze $w_i = x + \frac{a}{2}$, $u_i = (x + a2)^2$. Dann ist $L_i = L_{i-1}(w_i)$ und w_i Nullstelle von $X^2 - u_i \in L_{i-1}[X]$. □

Es ist noch zu untersuchen, für welche n $\varphi(n)$ eine Zweierpotenz ist.

Satz 5.5.11. *Folgende Aussagen sind äquivalent:*

1. *Das regelmäßige n-Eck ist mit Zirkel und Lineal aus $0, 1$ konstruierbar.*

2. *$\varphi(n)$ ist eine Zweierpotenz.*

3. *$n = 2^s p_1 \cdots p_r$, wobei die p_i Primzahlen der Form $2^{2^{k_i}} + 1$ sind (sogenannte Fermatsche Primzahlen).*

Beweis. Die Äquivalenz von (1) und (2) ist schon gezeigt. Die Äquivalenz von (2) und (3) ergibt sich folgendermaßen. Sei $n = 2^s p_1^{m_1} \cdots p_r^{m_r}$, p_i Primzahlen > 2, $m_i \geq 1$. Dann ist nach Satz 3.1.16 $\varphi(n) = 2^{s-1} p_1^{m_1-1}(p_1 - 1) \cdots p_r^{m_r-1}(p_r - 1)$.

Also ist $\varphi(n)$ Zweierpotenz genau dann, wenn die p_i Primzahlen der Form 2^m+1 sind und $m_i = 1$.

Zu zeigen bleibt: Ist 2^m+1 Primzahl, so ist m eine Zweierpotenz. Annahme: $m = ab$ mit $a, b \in \mathbb{N}$ und $b > 1$ ungerade. Dann gilt

$$2^{ab} + 1 = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + - \cdots + 2^{a(b-b)}).$$

Wegen $1 < 2^a + 1 < 2^{ab} + 1$ ist dies ein Widerspruch zu: $2^{ab} + 1$ ist Primzahl. Also ist m Zweierpotenz. □

Bemerkung. Man kennt bisher nur folgende Primzahlen der Form $2^{2^k} + 1$:

$$3, 5, 17, 257, 65537 \quad (\text{für } k = 0, 1, 2, 3, 4).$$

Einige weitere Zahlen dieser Form sind keine Primzahlen, z.B. ist $2^{2^5} + 1$ durch 641 teilbar.

5.6 Fundamentalsatz der Algebra

Es soll gezeigt werden, daß jedes $f \in \mathbb{C}[X]$ in $\mathbb{C}[X]$ in Linearfaktoren zerfällt. Dafür genügt es zu zeigen, daß jedes $f \in \mathbb{C}[X]$ mit $\mathsf{deg}(f) \geq 1$ mindestens eine Nullstelle in $\mathbb{C}$ besitzt. Dies ist der sogenannte Fundamentalsatz der Algebra.

Lemma 5.6.1. *Jedes $f \in \mathbb{R}[X]$ mit $\mathsf{deg}(f)$ ungerade hat mindestens eine Nullstelle in $\mathbb{R}$.*

Beweis. Sei oBdA der Leitkoeffizient von f positiv. Dann ist

$$\lim_{x\to-\infty} f(x) = -\infty, \quad \lim_{x\to+\infty} f(x) = \infty.$$

Aus dem Zwischenwertsatz folgt die Behauptung. □

Lemma 5.6.2. *Jedes $f \in \mathbb{C}[X]$ mit $\mathsf{deg}(f) = 2$ zerfällt in $\mathbb{C}[X]$ in Linearfaktoren.*

Beweis. Für jedes $z = |z|e^{i\varphi} \in \mathbb{C}$ existiert ein $w \in \mathbb{C}$ mit $w^2 = z$ (etwa $w = \sqrt{|z|}e^{i\frac{\varphi}{2}}$). Also besitzt jedes $z \in \mathbb{C}$ in $\mathbb{C}$ eine Quadratwurzel. Sei nun $f \in \mathbb{C}[X]$ mit $\mathsf{deg}(f) = 2$ gegeben, etwa (oBdA) $f = X^2 + aX + b$. Dann sind

$$x_{1,2} = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b} \in \mathbb{C}$$

die Nullstellen von f in $\mathbb{C}$, und f zerfällt. □

Satz 5.6.3. *(Fundamentalsatz der Algebra). Jedes $f \in \mathbb{C}[X]$ zerfällt in $\mathbb{C}[X]$ in Linearfaktoren.*

Beweis. (Nach Lagrange). Wie schon erwähnt genügt es zu zeigen, daß jedes $f \in \mathbb{C}[X]$ mit $\mathsf{deg}(f) \geq 1$ mindestens eine Nullstelle in $\mathbb{C}$ besitzt. Sei $f \in \mathbb{C}[X]$. Wir betrachten das Polynom $f \cdot \bar{f}$, wobei

$$\begin{aligned} \bar{f} &= \bar{a}_n X^n + \cdots + \bar{a}_1 X + \bar{a}_0, \quad \text{falls} \\ f &= a_n X^n + \cdots + a_1 X + a_0. \end{aligned}$$

Es ist

$$f \cdot \bar{f} = \sum_{i=0}^{2n} c_i X^i \quad \text{mit } c_i = \textstyle\sum_{m+n=i} a_m \bar{a}_n.$$

Also gilt $c_i = \bar{c}_i$ und deshalb $f \cdot \bar{f} \in \mathbb{R}[X]$.

Sei $a \in \mathbb{C}$ eine Nullstelle von $f \cdot \bar{f}$. Dann ist a entweder Nullstelle von f oder von $\bar{f}$. Im letzten Fall ist $\bar{f}(a) = 0$ und deshalb $\overline{\bar{f}(a)} = f(\bar{a}) = 0$. Also ist entweder a oder $\bar{a}$ Nullstelle von f.

Es reicht also zu zeigen, daß jedes $f \in \mathbb{R}[X]$ mit $\mathsf{deg}(f) \geq 1$ mindestens eine Nullstelle in $\mathbb{C}$ hat. Sei also $f \in \mathbb{R}[X]$ und $\mathsf{deg}(f) = 2^l m$ mit m ungerade. Der Beweis wird durch Induktion über l geführt. *Fall* $l = 0$. Die Aussage ist nach Lemma 5.6.1 richtig. *Fall* $l > 0$. Sei $K \supseteq \mathbb{C}$ Zerfällungskörper von f über $\mathbb{C}$, also

$$f = (X - a_1) \cdots (X - a_n) \quad \text{mit } a_1, \ldots, a_n \in K.$$

Wegen $\mathsf{char}(\mathbb{C}) = 0$ ist f separabel, also $K \supseteq \mathbb{C}$ galoissch. Es ist sogar $K \supseteq \mathbb{R}$ galoissch, da K Zerfällungskörper von $(X^2+1)f$ über $\mathbb{R}$ ist. Betrachte für festes $\lambda \in \mathbb{R}$

$$\begin{aligned} b_{rs} &:= a_r + a_s + \lambda a_r a_s, && 1 \leq r, s \leq n \\ g &:= \prod_{1 \leq r \leq s \leq n} (X - b_{rs}) \in K[X]. \end{aligned}$$

Es gilt $\hat{\varphi}(g) = g$ für jedes $\varphi \in \Gamma_{\mathbb{R}}^{K}$, da φ die $a_1, \ldots, a_n$ permutiert (wegen $f \in \mathbb{R}[X]$), also jedes b_{rs} auf ein anderes $b_{r's'}$ wirft. Da K galoissch über $\mathbb{R}$ ist, folgt $g \in \mathbb{R}[X]$. Weiterhin gilt

$$\begin{aligned} \mathsf{deg}(g) &= |\{\, (r,s) \mid 1 \leq r \leq s \leq n \,\}| \\ &= n + (n-1) + \cdots + 1 \\ &= \tfrac{1}{2} n(n+1) \\ &= 2^{l-1} m(n+1) \end{aligned}$$

Da $m(n+1)$ ungerade ist, kann auf g die Induktionsvoraussetzung angewandt werden. g hat also eine Nullstelle in $\mathbb{C}$.

Für alle $\lambda \in \mathbb{R}$ gibt es also r, s mit $1 \leq r \leq s \leq n$, so daß $b_{rs} = a_r + a_s + \lambda a_r a_s \in \mathbb{C}$. Diese Paare (r,s) hängen von λ ab. Da es aber nur $\frac{n}{2}(n+1)$ solche Paare, aber unendlich viele reelle Zahlen gibt, findet man $\lambda, \mu \in \mathbb{R}$ mit $\lambda \neq \mu$ und r, s mit $1 \leq r \leq s \leq n$ so, daß

$$\begin{aligned} &a_r + a_s + \lambda a_r a_s \in \mathbb{C} \quad \text{und} \\ &a_r + a_s + \mu a_r a_s \in \mathbb{C}. \end{aligned}$$

Subtraktion ergibt $(\lambda - \mu) a_r a_s \in \mathbb{C}$, also auch $a_r a_s \in \mathbb{C}$. Damit gilt auch $a_r + a_s \in \mathbb{C}$. Also hat man $(X - a_r)(X - a_s) \in \mathbb{C}[X]$. Wendet man nun Lemma 5.6.2 an, so folgt $a_r, a_s \in \mathbb{C}$. Also hat f eine Nullstelle in $\mathbb{C}$. □

5.7 Endliche Körper

Bemerkung. Sei K ein endlicher Körper, $P \subseteq K$ sein Primkörper, $n := [K : P]$ und $p = \mathsf{char}(K)$. Dann gilt $|K| = p^n$.

Beweis. K ist P-Vektorraum der Dimension n, und $|P| = p$. □

Satz 5.7.1. *Für jede Primzahl p und jedes $n \geq 1$ gilt:*

1. *Sei $K \supseteq \mathbb{Z}_p$ Zerfällungskörper des Polynoms $X^{p^n} - X \in \mathbb{Z}_p[X]$. Dann ist K Körper mit p^n Elementen.*

2. *Sei K Körper mit p^n Elementen und P sein Primkörper. Dann ist K Zerfällungskörper des Polynoms $X^{p^n} - X \in P[X]$.*

3. *Je zwei Körper mit p^n Elementen sind isomorph. Man nennt den bis auf Isomorphie eindeutig bestimmten Körper mit p^n Elementen das* Galois-Feld *mit p^n Elementen. Schreibweise: $\mathsf{GF}(p^n)$ oder $\mathbb{F}_{p^n}$.*

Beweis. 1. Zunächst wird gezeigt: Die Menge M der Nullstellen von $X^{p^n} - X \in \mathbb{Z}_p[X]$ bildet einen Unterkörper von K. Dies sieht man wie folgt. Es gilt $M \subseteq K$ und $0, 1 \in M$. Seien $a, b \in M$, also $a^{p^n} = a$ und $b^{p^n} = b$. Dann gilt

$$(a - b)^{p^n} = a^{p^n} + (-1)^{p^n} b^{p^n} = a^{p^n} - b^{p^n} = a - b,$$

also $a - b \in M$ (die restlichen Terme des binomischen Ausdrucks fallen weg, da $\mathsf{char}(K) = p$. Für p ungerade gilt $(-1)^{p^n} = -1$, für $p = 2$ gilt $-1 = 1 \bmod 2$). Seien $a, b \in M$, $b \neq 0$. Dann gilt

$$\left(\frac{a}{b}\right)^{p^n} = \frac{a^{p^n}}{b^{p^n}} = \frac{a}{b},$$

also $\frac{a}{b} \in M$. Damit ist M Unterkörper von K. Nach Definition des Zerfällungskörpers gilt damit schon $K = M$. Das Polynom $X^{p^n} - X$ hat p^n Nullstellen, und diese sind wegen $(X^{p^n} - X)' = -1 \neq 0$ alle verschieden. Also hat M (bzw. K) p^n Elemente.

2. Da $|K^*| = p^n - 1$, gilt $a^{p^n} = a$ für alle $a \in K$ (nach Folgerung 1.1.11). Daher sind alle p^n Elemente von K Nullstellen von $X^{p^n} - X \in P[X]$. Da dieses Polynom nur p^n Nullstellen hat, sind damit schon alle Nullstellen gegeben. Also ist K der gesuchte Zerfällungskörper.

3. Seien K, K' Körper mit p^n Elementen und P, P' ihre Primkörper mit jeweils p Elementen. Dann gilt: $P \cong \mathbb{Z}_p \cong P'$. Nach (2) ist K Zerfällungskörper von $X^{p^n} - X \in P[X]$ und K' ist Zerfällungskörper von $X^{p^n} - X \in P'[X]$. Der zweite Erweiterungssatz liefert $K \cong K'$. □

Satz 5.7.2. *Sei K ein Körper der Charakteristik p. Dann ist die Abbildung*

$$\begin{aligned} K &\to K \\ a &\mapsto a^p \end{aligned}$$

ein Monomorphismus, der Frobenius-Homomorphismus *von K.*

Beweis. Seien $a, b \in K$. Es gilt $(ab)^p = a^p b^p$ und $(a + b)^p = a^p + b^p$, da die restlichen Terme des binomischen Ausdrucks wegfallen (wegen $\mathsf{char}(K) = p$). Außerdem folgt aus $a^p = 0$ offenbar $a = 0$, also ist die Abbildung injektiv. □

Bemerkung 5.7.3. 1. Für jeden endlichen Körper ist der Frobenius-Homomorphismus ein Automorphismus (da aus der Injektivität schon die Bijektivität folgt).

2. Für $\mathbb{Z}_p$ ist der Frobenius-Homomorphismus die Identität (denn $a^{p-1} = 1$ in $\mathbb{Z}_p$).

Satz 5.7.4. *Sei p eine Primzahl, $n \geq 1$, K ein Körper mit p^n Elementen und $P \subseteq K$ sein Primkörper. Dann gilt:*

1. *K ist galoissch über P.*
2. *$\Gamma_P^K = \langle \varphi \rangle$, wobei φ der Frobenius-Homomorphismus von K ist.*

Beweis. 1. K ist Zerfällungskörper eines separablen Polynoms (vgl. Satz 5.7.1), also ist K galoissch über P.

2. Es ist $[K : P] = n$, also $|\Gamma_P^K| = n$. Außerdem gilt $\varphi \in \Gamma_P^K$, da nach der Bemerkung vorher $\varphi \in \mathsf{Aut}(K)$ und $\varphi{\restriction}P = \mathsf{id}_P$. Es genügt also zu zeigen, daß $\varphi^0, \varphi^1, \ldots, \varphi^{n-1}$ verschieden sind. Sei a ein erzeugendes Element von K^* (da K^* zyklisch ist, existiert ein solches Element). Dann sind die $\varphi^i(a) = a^{p^i}$ verschieden für $i = 0, \ldots, n-1$. □

Bemerkung. Sei p eine Primzahl, $n \geq 1$, K ein Körper mit p^n Elementen und P sein Primkörper. Dann gilt $\Gamma_P^K = \mathsf{Aut}(K)$.

Beweis. Jedes $\psi \in \mathsf{Aut}(K)$ läßt P elementweise fest, da $\psi(1) = 1$ und daher $\psi(n \cdot 1) = n \cdot 1_K$ für alle $n = 0, \ldots, p-1$. □

Nun sollen noch die Unterkörper von $\mathbb{F}_{p^n}$ bestimmt werden.

Satz 5.7.5. *Sei p eine Primzahl, $n \geq 1$, K ein Körper mit p^n Elementen und φ sein Frobenius-Homomorphismus. Zu $i|n$, $1 \leq i \leq n$, gibt es genau einen Unterkörper von K mit p^i Elementen, nämlich $\mathsf{FK}(\langle \varphi^i \rangle)$, und dies sind sämtliche Unterkörper von K.*

Beweis. Die Untergruppen von $\Gamma_P^K = \langle \varphi \rangle$ sind genau die $\langle \varphi^i \rangle$ mit $i|n$, $1 \leq i \leq n$. Der Hauptsatz der Galois-Theorie liefert die Behauptung. □

Satz 5.7.6. *Sei K ein endlicher Körper. Dann gilt*

$$\prod_{a \in K^*} a = -1$$

.

Beweis. Falls $a \neq a^{-1}$, kommen a und a^{-1} im Produkt vor und heben sich auf. Mit $M := \{\, a \in K^* \mid a = a^{-1} \,\}$ gilt daher $\prod_{a \in K^*} a = \prod_{a \in M} a$. Jedes $a \in M$ ist Nullstelle von $X^2 - 1$, also $M = \{1, -1\}$. Damit folgt

$$\prod_{a \in K^*} a = 1 \cdot (-1) = -1$$ □

Folgerung 5.7.7 (Satz von Wilson). *Für jede Primzahl p gilt*

$$(p-1)! = -1 \bmod p.$$

Beweis. $K = \mathbb{Z}_p$. Der vorangehende Satz liefert $(p-1)! = -1 \bmod p$. □

Anhang A

Ein konstruktiver Beweis des Fundamentalsatzes

Wir beweisen konstruktiv den Fundamentalsatz der Algebra (nach Martin Kneser: Ergänzung zu einer Arbeit von Hellmuth Kneser über den Fundamentalsatz der Algebra, Math. Z. 177:1981, 285-287).

A.1 Ein Hilfssatz

Lemma A.1.1. *Für alle $n \in \mathbb{N}$ existiert ein $q \in \mathbb{Q}$ mit $0 < q < 1$, so daß für jedes normierte Polynom $f = \sum_{i=0}^{n} a_i \xi^i \in \mathbb{C}[\xi]$ mit $|a_0| > 0$ es ein $z \in \mathbb{C}$ gibt mit*

$$|z| \leq \left(\frac{|a_0|}{q}\right)^{\frac{1}{n}} \quad \textit{und} \quad |f(z)| \leq q|a_0|.$$

Aus dem Beweis wird sich ergeben, daß das $z \in \mathbb{C}$ von der *Darstellung* der Koeffizienten in $\mathbb{C}$ abhängt (also von der Wahl der Cauchyfolgen und Moduln). Dies ist auch zu erwarten, da es z.B. keine stetige Funktion $f\colon \mathbb{C} \to \mathbb{C}$ gibt mit $f(z)^2 = z$ (zur Auflösung der Mehrdeutigkeit der Wurzel benötigt man Riemannsche Flächen).

Beweis. Folgender Ansatz wird zum Ziel führen. Wir wählen eines der Glieder $a_1\xi, \ldots, a_n\xi^n = \xi^n$ aus, etwa $a_k\xi^k$, und bestimmen z so daß sich a_0 und $a_k z^k$ um einen negativen Faktor unterscheiden. Für den Betrag $|z| = r$ setzen wir zunächst nur voraus, daß er hinreichend klein ist, nämlich $|a_k|r^k \leq |a_0| + \varepsilon$. Dann folgt (siehe (A.7))

$$\begin{aligned} |f(z)| &\leq |a_0 + a_k z^k| + \sum_{i \neq 0,k} |a_i z^i| \\ &\leq |a_0| - |a_k|r^k + 2\varepsilon + \sum_{i \neq 0,k} |a_i| r^i. \end{aligned}$$

Es kommt also darauf an, k und r so zu wählen, daß die Glieder $|a_i|r^i$ $(i \neq 0, k)$ klein gegen $|a_k|r^k$ sind, dieses andereseits nicht zu klein gegen $|a_0|$ wird (siehe (A.6)).

Setze

$$q := 1 - \frac{1}{4 \cdot 3^{2n^2-1}} \quad \text{und} \quad \varepsilon := \min\Big(\frac{|a_0|}{2(n+1)} \cdot \frac{1}{4 \cdot 3^{2n^2-1}}, (q^{-1}-1)|a_0|\Big).$$

Diese Wahlen werden unten in den Schritten 6, 10 und 11 begründet.

Schritt 1. Sei

$$m(s) := \max\{\, |a_i| s^i \mid i = 1, \dots, n \,\}.$$

Wähle $t \in \mathbb{Q}$, $t > 0$, mit

$$\big| m(t) - |a_0| \big| \le \varepsilon. \tag{A.1}$$

Dies ist möglich nach dem Zwischenwertsatz, da $m(0) = 0 < |a_0|$ und wegen $s^n \le m(s)$ es ein $s > 0$ gibt mit $|a_0| < m(s)$.

Schritt 2. Wähle $y_i \in \mathbb{Q}$, $y_i > 0$, mit $|y_i - |a_i| t^i| \le \varepsilon$ für $i = 1, \dots, n$. Mit $y_{ij} := \frac{y_i}{3^{ij}}$ (für $j \in \mathbb{Z}$) erhält man

$$\Big| y_{ij} - |a_i| (\frac{t}{3^j})^i \Big| = \Big| \frac{y_i}{3^{ij}} - \frac{|a_i| t^i}{3^{ij}} \Big| \le \frac{\varepsilon}{3^{ij}}. \tag{A.2}$$

Schritt 3. Wähle nun $k_j \in \{1, \dots, n\}$ minimal so daß $y_{ij} \le y_{k_j j}$ für $i = 1, \dots, n$. Also

$$|a_i| \Big(\frac{t}{3^j}\Big)^i \le y_{ij} + \frac{\varepsilon}{3^{ij}} \le y_{k_j j} + \frac{\varepsilon}{3^{ij}} \le |a_{k_j}| \Big(\frac{t}{3^j}\Big)^{k_j} + \frac{\varepsilon}{3^{k_j j}} + \frac{\varepsilon}{3^{ij}}. \tag{A.3}$$

Schritt 4. Es gilt

$$k_j \ge k_{j+1}. \tag{A.4}$$

Dies sieht man wie folgt.

$$\begin{aligned}
y_{k_j(j+1)} &= \frac{1}{3^{k_j(j+1)}} y_{k_j} \\
&= \frac{1}{3^{k_j}} y_{k_j j} \\
&\ge \frac{1}{3^i} y_{ij} && \text{für } i \ge k_j \text{ wegen } y_{k_j j} \ge y_{ij} \\
&= \frac{1}{3^{i(j+1)}} y_i \\
&= y_{i(j+1)}.
\end{aligned}$$

Für $i \ge k_j$ ist also $y_{k_j(j+1)} \ge y_{i(j+1)}$. Nach Wahl von k_{j+1} (kleinstmöglich) folgt deshalb $k_{j+1} \le k_j$.

Schritt 5. Wähle $j \ge 0$ minimal, so daß $k_{j-1} = k_j = k_{j+1} =: k$. Wegen (A.4) gilt

$$n \ge k_{-1} \ge k_0 \ge k_1 \ge \dots \ge k_{j-1} = k_j = k_{j+1},$$

wobei von je zwei aufeinander folgenden $\ge$ (nach dem ersten) eines ein $>$ sein muß. Für $2i - 1 \le j$ gilt also $k_{2i-1} \le n - i$.

Fall 1. j ist von der Form $2i - 1$. Dann

$$\begin{aligned}
k_j &\le n - i = n - \frac{j+1}{2} \\
2k_j &\le 2n - j - 1 \\
j &\le 2(n - k_j) - 1
\end{aligned}$$

Fall 2. j ist von der Form $2i$. Dann

$$\begin{aligned} k_j = k_{j-1} &\le n - i = n - \frac{j}{2} \\ 2k_j &\le 2n - j \\ j &\le 2(n - k_j) \end{aligned}$$

Also hat man allgemein

$$j \le 2(n-k). \tag{A.5}$$

Schritt 6. Setze

$$r := \frac{t}{3^j} \in \mathbb{Q}.$$

Wir schätzen $|a_k|r^k$ gegen $|a_0|$ ab. Für $i = 1\ldots,n$ gilt

$$\begin{aligned} |a_k|r^k &= |a_k|\Big(\frac{t}{3^j}\Big)^k \\ &\ge |a_i|\Big(\frac{t}{3^j}\Big)^i - 2\varepsilon \quad \text{nach (A.3), da } k = k_j \\ &\ge \frac{1}{3^{nj}}|a_i|t^i - 2\varepsilon, \end{aligned}$$

also

$$\begin{aligned} |a_k|r^k &\ge \frac{1}{3^{nj}} m(t) - 2\varepsilon \qquad \text{da } m(t) = \max\{\, |a_i|t^i \mid i = 1,\ldots,n \,\} \\ &\ge \frac{1}{3^{nj}}|a_0| - 3\varepsilon \qquad \text{nach Wahl von } t \text{ in (A.1).} \end{aligned}$$

Nach (A.5) gilt $j \le 2(n-k)$, also $nj \le 2n(n-k) \le 2n^2 - k$ und deshalb

$$|a_k|r^k \ge \frac{1}{3^{2n^2-k}}|a_0| - 3\varepsilon. \tag{A.6}$$

Insbesondere ist $|a_k| > 0$ wegen $\varepsilon < \frac{|a_0|}{3} \cdot \frac{1}{3^{2n^2-1}}$.

Schritt 7. Wir bestimmen zunächst $z \in \mathbb{C}$ mit $|z| = r$ so, daß sich a_0 und $a_k z^k$ um einen negativen Faktor unterscheiden. Schreibe $a_0 = |a_0|e^{ix_0}$ und $a_k = |a_k|e^{ix_k}$ und setze $z = |r|e^{iy}$ mit y so, daß $x_0 + \pi = x_k + ky$.

Wir zeigen $|a_0 + a_k z^k| \le |a_0| - |a_k z^k| + 2\varepsilon$. Es gilt $a_k z^k = -ca_0$ mit $c \in \mathbb{R}$, $c \ge 0$, und nach Wahl von t in (A.1) auch $|a_k z^k| \le |a_0| + \varepsilon$. Daraus folgt

$$\begin{aligned} |a_k z^k| = c|a_0| &\le |a_0| + \varepsilon \\ 0 \le c &\le 1 + \frac{\varepsilon}{|a_0|}, \end{aligned}$$

also

$$\begin{aligned} a_0 + a_k z^k &= a_0(1-c) \\ |a_0 + a_k z^k| &= |a_0| \cdot |1-c| \\ &= |a_0| \max(1-c, c-1) \\ &= |a_0| \max(1-c, 1-c+2(c-1)) \\ &\le |a_0| \max\Big(1-c, 1-c+2\frac{\varepsilon}{|a_0|}\Big) \\ &= |a_0|(1-c) + 2\varepsilon \\ &= |a_0| - |a_k z^k| + 2\varepsilon. \end{aligned}$$

Man erhält jetzt

$$\begin{aligned} |f(z)| &\le |a_0 + a_k z^k| + \sum_{i\ne 0,k} |a_i z^i| \\ &\le |a_0| - |a_k z^k| + 2\varepsilon + \sum_{i\ne 0,k} |a_i z^i| \\ &= |a_0| - |a_k| r^k + 2\varepsilon + \sum_{i\ne 0,k} |a_i| r^i. \end{aligned} \tag{A.7}$$

Schritt 8. Abschätzung von $\sum_{1\le i<k} |a_i| r^i$. Sei $1 \le i < k$. Dann gilt

$$\begin{aligned} |a_i| r^i &= 3^i |a_i| \Big(\frac{r}{3}\Big)^i \\ &= 3^i |a_i| \Big(\frac{t}{3^{j+1}}\Big)^i \\ &\le 3^i \Big(|a_k| (\frac{t}{3^{j+1}})^k + \frac{\varepsilon}{3^{i(j+1)}} + \frac{\varepsilon}{3^{k(j+1)}} \Big) \quad \text{nach (A.3), da } k = k_{j+1} \\ &\le 3^i \Big(|a_k| (\frac{t}{3^j})^k \frac{1}{3^k} + 2\frac{\varepsilon}{3^i} \Big) \\ &= \frac{1}{3^{k-i}} |a_k| r^k + 2\varepsilon, \end{aligned}$$

also

$$\begin{aligned} \sum_{1\le i<k} |a_i| r^i &\le |a_k| r^k \sum_{1\le i<k} \frac{1}{3^{k-i}} + 2(k-1)\varepsilon \\ &= |a_k| r^k \Big(\frac{1}{3^{k-1}} + \cdots + \frac{1}{3} \Big) + 2(k-1)\varepsilon \\ &= |a_k| r^k \frac{\frac{1}{3} - \frac{1}{3^k}}{1 - \frac{1}{3}} + 2(k-1)\varepsilon \\ &= |a_k| r^k \frac{1}{2} \Big(1 - \frac{1}{3^{k-1}} \Big) + 2(k-1)\varepsilon. \end{aligned}$$

Es ergibt sich

$$\sum_{1\le i<k} |a_i| r^i \le |a_k| r^k \frac{1}{2} \Big(1 - \frac{1}{3^{k-1}} \Big) + 2(k-1)\varepsilon. \tag{A.8}$$

Schritt 9. Abschätzung von $\sum_{k<i\le n} |a_i| r^i$. Sei $k < i \le n$. Dann gilt

$$\begin{aligned} |a_i| r^i &= \frac{1}{3^i} |a_i| (3r)^i \\ &= \frac{1}{3^i} |a_i| \Big(\frac{t}{3^{j-1}}\Big)^i \\ &\le \frac{1}{3^i} \Big(|a_k| (\frac{t}{3^{j-1}})^k + \frac{\varepsilon}{3^{i(j-1)}} + \frac{\varepsilon}{3^{k(j-1)}} \Big) \quad \text{nach (A.3), da } k = k_{j-1} \\ &\le \frac{1}{3^i} \Big(|a_k| (\frac{t}{3^j})^k \cdot 3^k + 2\varepsilon \Big) \\ &\le \frac{1}{3^{i-k}} |a_k| r^k + 2\varepsilon, \end{aligned}$$

also

$$\begin{aligned}
\sum_{k<i\le n} |a_i| r^i &\le |a_k| r^k \sum_{k<i\le n} \frac{1}{3^{i-k}} + 2(n-k)\varepsilon \\
&= |a_k| r^k \Big(\frac{1}{3} + \cdots + \frac{1}{3^{n-k}}\Big) + 2(n-k)\varepsilon \\
&= |a_k| r^k \frac{\frac{1}{3} - \frac{1}{3^{n-k+1}}}{1-\frac{1}{3}} + 2(n-k)\varepsilon \\
&= |a_k| r^k \frac{1}{2}\Big(1 - \frac{1}{3^{n-k}}\Big) + 2(n-k)\varepsilon .
\end{aligned}$$

Es ergibt sich

$$\sum_{k<i\le n} |a_i| r^i \le |a_k| r^k \frac{1}{2}\Big(1 - \frac{1}{3^{n-k}}\Big) + 2(n-k)\varepsilon . \tag{A.9}$$

Schritt 10. Aus (A.7), (A.8) und (A.9) erhält man

$$\begin{aligned}
|f(z)| &\le |a_0| - |a_k| r^k + 2\varepsilon + \sum_{i\ne 0,k} |a_i| r^i \\
&\le 2n\varepsilon + |a_0| - |a_k| r^k + |a_k| r^k \frac{1}{2}\Big(1 - \frac{1}{3^{k-1}}\Big) + |a_k| r^k \frac{1}{2}\Big(1 - \frac{1}{3^{n-k}}\Big) \\
&\le 2n\varepsilon + |a_0| - \frac{1}{2}\cdot\frac{1}{3^{k-1}} |a_k| r^k \\
&\le 2n\varepsilon + |a_0| - \frac{1}{2\cdot 3^{k-1}}\Big(\frac{1}{3^{2n^2-k}} |a_0| - 3\varepsilon\Big) \quad \text{nach (A.6)} \\
&\le 2(n+1)\varepsilon + \Big(1 - \frac{1}{2\cdot 3^{2n^2-1}}\Big) |a_0| \\
&\le \underbrace{\Big(1 - \frac{1}{4\cdot 3^{2n^2-1}}\Big)}_{=:q} |a_0| \quad \text{für } \varepsilon \le \tfrac{|a_0|}{2(n+1)} \cdot \tfrac{1}{4\cdot 3^{2n^2-1}}
\end{aligned}$$

Schritt 11. Es ist $|z| = r$, also

$$|z|^n = r^n \le t^n \le m(t) \le |a_0| + \varepsilon \le q^{-1}|a_0|$$

wegen $\varepsilon \le (q^{-1} - 1)|a_0|$. Wie verlangt ist also

$$|z| \le (q^{-1}|a_0|)^{\frac{1}{n}} . \qquad \square$$

A.2 Beweis des Fundamentalsatzes

Nun geben wir den Beweis des Fundamentalsatzes der Algebra unter Verwendung des Hilfssatzes.

Satz A.2.1. *Für alle normierten Polynome*

$$g = \sum_{i=0}^{n} b_i \xi^i \in \mathbb{C}[\xi]$$

gibt es ein $z \in \mathbb{C}$ *mit* $g(z) = 0$.

Beweis. Wähle $c > 0$ mit $|b_0| \leq c$. Wir konstruieren rekursiv eine Folge komplexer Zahlen $(w_m)_{m\in\mathbb{N}}$ mit

$$|g(w_m)| \leq q^m c. \tag{A.10}$$

Als Basis der Folge wähle man $w_0 := 0$. Dann gilt (A.10) wegen

$$|g(w_0)| = |g(0)| = |b_0| \leq c = q^0 c.$$

Für den Schritt nehmen wir an, daß w_m mit (A.10) schon konstruiert ist. Betrachte das Polynom

$$f(\xi) := g(w_m + \xi) \in \mathbb{C}[\xi].$$

$f(\xi)$ ist normiert und hat den Grad n; das konstante Glied von $f(\xi)$ ist $g(w_m)$. Wegen $c > 0$ ist die folgende Fallunterscheidung zulässig.

Fall 1. $|g(w_m)| \leq q^{m+1}c$. Mit $w_{m+1} := w_m$ folgt dann (A.10) aus

$$|g(w_{m+1})| = |g(w_m)| \leq q^{m+1}c \quad \text{nach Fallunterscheidungsannahme.}$$

Fall 2. $|g(w_m)| \geq \frac{1}{2}q^{m+1}c > 0$. Der Hilfssatz angewandt auf $f(\xi)$ liefert ein $w \in \mathbb{C}$ mit

$$|w| \leq \left(\frac{|g(w_m)|}{q}\right)^{\frac{1}{n}} \quad \text{und} \quad |f(w)| \leq q|g(w_m)|.$$

Wegen (A.10) für w_m gilt $|g(w_m)| \leq q^m c$, also

$$|w| \leq (q^{m-1}c)^{\frac{1}{n}} \quad \text{und} \quad |f(w)| \leq q^{m+1}c.$$

Setze $w_{m+1} := w_m + w$. Dann folgt

$$|g(w_{m+1})| = |g(w_m + w)| = |f(w)| \leq q^{m+1}c,$$

d.h. (A.10) gilt auch für $m + 1$.

Wir zeigen jetzt

$$|w_{m+1} - w_m| \leq (q^{m-1}c)^{\frac{1}{n}}.$$

Im Fall $|g(w_m)| \leq q^{m+1}c$ folgt dies aus $w_{m+1} = w_m$, und im Fall $|g(w_m)| \geq \frac{1}{2}q^{m+1}c > 0$ haben wir

$$|w_{m+1} - w_m| = |w| \leq (q^{m-1}c)^{\frac{1}{n}}.$$

Es ergibt sich

$$\begin{aligned}
|w_{m+k} - w_m| &\leq |w_{m+k} - w_{m+k-1}| + \cdots + |w_{m+1} - w_m| \\
&\leq c^{\frac{1}{n}}\left(q^{\frac{m+k-2}{n}} + \cdots + q^{\frac{m-1}{n}}\right) \\
&\leq c^{\frac{1}{n}}(q^{\frac{1}{n}})^{m-1}(1 + q^{\frac{1}{n}} + (q^{\frac{1}{n}})^2 + \ldots).
\end{aligned}$$

Setzt man $z := \lim_{m\to\infty} w_m$, so folgt $g(z) = 0$ aus (A.10). $\square$

Index