ulm university universität
uulm

Skript zur Vorlesung

Algebra

Wintersemester 2012/ 13

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

Institut für Zahlentheorie und Wahrscheinlichkeitstheorie
Universität Ulm

Inhaltsverzeichnis

Kapitel 1

Ringtheorie

1.1 Einführung

Wir setzen den Begriff des Rings und die Grundregeln für das Rechnen in Ringen als bekannt voraus. In dieser Vorlesung betrachten wir nur kommutative Ringe mit Eins. Im folgenden sei also $(R, +, \cdot)$ stets ein kommutativer Ring mit Eins.
Wir erinnern an folgende grundlegende Definition:

Definition 1.1.1. Es sei $(R, +, \cdot)$ ein (kommutativer) Ring (mit Eins).

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

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

iii) Der Ring R heißt Integritätsring, wenn R nullteilerfrei ist und $0_R \neq 1_R$ ist.

iv) Ein $\alpha \in R$ heißt Einheit, wenn es ein $\beta \in R$ mit $\alpha\beta = 1_R$ gibt. Die Menge der Einheiten von R wird mit R^* bezeichnet.

v) Ein Ring $(R, +, \cdot)$ heißt Körper, wenn $(R\backslash\{0\}, \cdot)$ eine abelsche Gruppe ist.

Bemerkung 1.1.1. Man zeigt leicht, dass $(R^*, \cdot)$ eine abelsche Gruppe ist. Sie heißt auch Einheitengruppe von R.

1.2 Homomorphismen und Ideale

Definition 1.2.1. Es sei R und R' Ringe.

i) Ein Homomorphismus $\varphi\colon R \to R'$ ist eine Abbildung mit

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b) \\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b) \quad \text{(Relationstreue)} \\ \varphi(1_R) &= 1_{R'}. \end{aligned}$$

ii) Ein Isomorphismus von Ringen ist ein bijektiver Homomorphismus.

iii) Gibt es einen Isomorphismus $R \to R'$, so heißen R und R' isomorph (Schreibweise: $R \cong R'$).

Definition 1.2.2. Es sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge $I \subset R$ heißt Ideal von R (Schreibweise: $I \triangleleft R$), wenn $(I, +)$ eine Untergruppe von R ist, und wenn für alle $r \in R$

$$a \in I \Rightarrow ar \in I$$

gilt.

Definition 1.2.3. Es sei $(R, +, \cdot)$ ein Ring und $I \triangleleft R$ ein Ideal. Unter R/I versteht man die Menge der (additiven) Nebenklassen von I:

$$R/I = \{r + I : r \in R\}.$$

Dann heißt $r + I$ auch Restklasse nach dem Ideal I.

Definition 1.2.4. i) Unter der Summe zweier Restklassen $r + I$ und $s + I$ versteht man das Komplexprodukt bzgl. $+$:

$$(r + I) + (s + I) = (r + s) + I.$$

ii) Unter dem Produkt zweier Restklassen $r + I$ und $s + I$ versteht man

$$(r + I) \cdot (s + I) = (rs) + I.$$

Satz 1.2.1. *Es sei $(R, +, \cdot)$ ein Ring und $I \triangleleft R$ ein Ideal. Dann ist $(R/I, +, \cdot)$ ein Ring. Die Abbildung $\Phi : R \to R/I$, $r \to r + I$ ist ein Epimorphismus (surjektiver Homomorphismus).*

Beweis. siehe Elemente der Algebra □

Definition 1.2.5. Der Ring $(R/I, +, \cdot)$ von 1.2.1 heißt Restklassenring von R nach I. Die Abbildung Φ heißt kanonischer Epimorphismus von R auf R/I.

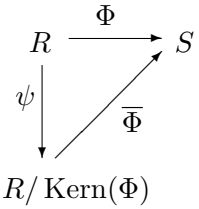
Satz 1.2.2. *Es seien R und R' Ringe sowie $\Phi : R \to R'$ ein Homomorphismus.*

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

ii) Die Abbildung

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

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



ist kommutativ.

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

Beweis. siehe Elemente der Algebra □

1.3 Der Chinesische Restsatz

Definition 1.3.1. Es seien $(R_1, +_1 \cdot_1), \ldots, (R_n, +_n, \cdot_n)$ Ringe. Unter dem direkten Produkt der Ringe $R_1, \ldots, R_n$ (Schreibweise: $R_1 \times R_2 \times \ldots \times R_n$ oder auch $\prod_{i=1}^n R_i$) versteht man den Ring, dessen Elemente die Elemente des kartesischen Produkts $R_1 \times \ldots \times R_n$ von Mengen sind, und für den Addition und Multiplikation komponentenweise definiert sind:

$$\begin{aligned}(r_1, \ldots, r_n) + (s_1, \ldots, s_n) &:= (r_1 +_1 s_1, \ldots, r_n +_n s_n)\\ (r_1, \ldots, r_n) \cdot (s_1, \ldots, s_n) &:= (r_1 \cdot_1 s_1, \ldots, r_n \cdot_n s_n).\end{aligned}$$

Das Einselement von $\prod R_i$ ist offenbar $(1_{R_1}, \ldots, 1_{R_n})$.

Definition 1.3.2. Es sei R ein Ring und $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ Ideale.

i) Unter der Summe von $\mathfrak{a}$ und $\mathfrak{b}$ versteht man

$$\mathfrak{a} + \mathfrak{b} := \{a + b \colon a \in \mathfrak{a},\ b \in \mathfrak{b}\}.$$

ii) Unter dem Durchschnitt von $\mathfrak{a}$ und $\mathfrak{b}$ versteht man

$$\mathfrak{a} \cap \mathfrak{b} := \{x \colon x \in \mathfrak{a},\ x \in \mathfrak{b}\}.$$

iii) Unter dem Produkt von $\mathfrak{a}$ und $\mathfrak{b}$ versteht man

$$\mathfrak{a} \cdot \mathfrak{b} := \{\sum a_i b_i \colon a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}\}.$$

Offenbar sind die in Definition 1.3.2 definierten Objekte ebenfalls Ideale, und es gilt $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Summen, Durchschnitte und Produkte können rekursiv auch für mehr als zwei Ideale definiert werden.

Definition 1.3.3. Es sei R ein Ring. Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ heißen komaximal, falls $\mathfrak{a} + \mathfrak{b} = R$ gilt.

Satz 1.3.1. *(Chinesischer Restsatz)*
Es sei R ein kommutativer Ring (mit Eins). Es seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq R$ paarweise komaximale Ideale von R, d.h. $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$. Dann gilt

i) $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.

ii) Es gibt eine Menge $\{e_1, \ldots, e_n\} \subseteq R$ mit

$$e_j \in \mathfrak{a}_i \quad \textit{falls } i \neq j \quad \textit{und} \quad e_j \equiv 1_R \bmod \mathfrak{a}_j. \tag{$*$}$$

Für $(r_1, \ldots, r_n) \in R^n$ ist das System von Kongruenzen

$$r \equiv r_1 \bmod \mathfrak{a}_1,\ r \equiv r_2 \bmod \mathfrak{a}_2, \ldots, r \equiv r_n \bmod \mathfrak{a}_n \tag{1}$$

zu der einzigen Kongruenz

$$r \equiv r_1 e_1 + \ldots r_n e_n \bmod \prod_{i=1}^n \mathfrak{a}_i \tag{2}$$

äquivalent.

iii) Die Abbildung

$$\Phi = \begin{cases} R/\prod_{i=1}^n \mathfrak{a}_i \to \prod_{i=1}^n (R/\mathfrak{a}_i) \\ r + \prod_{i=1}^n \mathfrak{a}_i \to (r + \mathfrak{a}_1, \ldots, r + \mathfrak{a}_n) \end{cases}$$

ist ein Isomorphismus von Ringen. Insbesondere ist

$$R/\prod_{i=1}^n \mathfrak{a}_i \cong R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n.$$

Beweis. i) Die Inklusion $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cdots \mathfrak{a}_n$ ist klar.
Wir zeigen die Umkehrung durch Induktion nach n.
Im Fall $n = 2$ gibt es eine Relation $1_R = a_1 + a_2$ mit $a_i \in \mathfrak{a}_i$. Dann gilt für $a \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ aber auch $a = a \cdot 1_R = a \cdot a_1 + a \cdot a_2 \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$.
Im Fall $n > 2$ hat man nach Induktionsvoraussetzung

$$(\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) \cdot \mathfrak{a}_n = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n,$$

wenn $R = \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} + \mathfrak{a}_n$ gilt. Nun hat man stetes Relationen $1_R = a_i + b_i$ mit $a_i \in \mathfrak{a}_i$ und $b_i \in \mathfrak{a}_n$ für $i \in \{1, \ldots, n-1\}$. Dann folgt durch Ausmultiplizieren

$$1_R = \prod_{i=1}^{n-1}(a_i + b_i) = \prod_{i=1}^{n-1} a_i + \sum_{i=1}^{n-1} b_i c_i \in \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} + \mathfrak{a}_n.$$

ii) Nach Voraussetzung gibt es für alle i, j mit $i \neq j$ Elemente $a_{ij} \in \mathfrak{a}_i$ und $b_{ij} \in \mathfrak{b}_j$ mit der Eigenschaft $1_R = a_{ij} + b_{ij}$. Wir setzen

$$e_j := \prod_{\substack{i=1 \\ i \neq j}}^{n} a_{ij} \in \mathfrak{a}_i$$

für alle i mit $i \neq j$. Es gilt weiter

$$e_j = \prod_{i=1}^{n}(1 - b_{ij}) \equiv 1_R \bmod \mathfrak{a}_j.$$

Aus $(*)$ folgt mit i) sofort die Äquivalenz der Kongruenzsystem (1) und (2).

iii) Für $(r_1, \ldots, r_n) \in R^n$ sei r durch (2) gegeben. Dann ist $(r+\mathfrak{a}_1, \ldots, r+\mathfrak{a}_n) = (r_1+\mathfrak{a}_1, \ldots, r_n+\mathfrak{a}_n)$, und r ist modulo $\prod_{i=1}^n \mathfrak{a}_i$ eindeutig bestimmt. Damit ist die Bijektivität von Φ gezeigt.

□

Wir erinnern an folgende Tatsachen aus der Elementaren Zahlentheorie:
Jedes Ideal von $\mathbb{Z}$ ist ein Hauptideal, d.h. es existiert ein $m \in \mathbb{Z}$ mit $I = (m) = \{m \cdot k \colon k \in \mathbb{Z}\}$.
Der größte gemeinsame Teiler $ggT(m, n) = g$ zweier Zahlen $m, n \in \mathbb{Z}$ kann stets als Linearkombination von m und n geschrieben werden: $g = x \cdot m + y \cdot n$ mit $x, y \in \mathbb{Z}$. Die Werte g, x und y können mittels des Euklidischen Algorithmus bestimmt werden.
Insbesondere sind (m) und (n) genau dann komaximal, wenn $ggT(m, n) = 1$ gilt.
Für $R = \mathbb{Z}$ lautet der Chinesische Restsatz dann folgendermaßen:

Satz 1.3.2. *Es seien $m_1, \ldots, m_n$ paarweise teilerfremde natürliche Zahlen und $m = m_1 \cdots m_n$. Dann gibt es für $1 \leq j \leq n$ Zahlen $l_j \in \mathbb{Z}$ mit $l_j \equiv 0 \bmod m_i$ für alle $i \neq j$ und $l_j \equiv 1 \bmod m_j$. Für ein beliebiges n- tupel $(r_1, \ldots, r_n) \in \mathbb{Z}^n$ ist das System von Kongruenzen*

$$r \equiv r_1 \bmod m_1, \ldots, r \equiv r_n \bmod m_n \tag{1}$$

zu der einzigen Kongruenz

$$r \equiv r_1 l_1 + \ldots r_n l_n \bmod m \tag{2}$$

äquivalent.
Die Abbildung

$$\Phi = \begin{cases} \mathbb{Z}/m\mathbb{Z} \to \prod_{i=1}^n (\mathbb{Z}/m_i\mathbb{Z}) \\ r + m\mathbb{Z} \to (r + m_1\mathbb{Z}, \ldots, r + m_n\mathbb{Z}) \end{cases}$$

ist ein Isomorphismus von Ringen. Insbesondere ist

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z}.$$

Beispiel 1.3.1. Es sei $m = m_1 \cdot m_2$ mit $m_1 = 5$ und $m_2 = 3$. Nach Satz 1.3.2 ist

$$\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Die Tafel, die Φ beschreibt, erhält man, indem für alle Restklassen $r + 15\mathbb{Z}$ das zugehörige Paar $(r_1 + 5\mathbb{Z}, r_2 + 3\mathbb{Z})$ berechnet wird. Veispielsweise gilt für $r = 7$:

$$\begin{aligned} r &\equiv 2 \bmod 5 \\ r &\equiv 1 \bmod 3, \end{aligned}$$

also $\Phi(7 + 15\mathbb{Z}) = (2 + 5\mathbb{Z}, 1 + 3\mathbb{Z})$. Wir bekommen

mod 3 \	0	1	2	3	4	mod 5
0	0	6	12	3	9	
1	10	1	7	13	4	
2	5	11	2	8	14	

Die Einträge sind nun alle modulo 15.

Die Idee des Chinesischen Restsatzes liegt der sogenannten "modularen Arithmetik" zugrunde, die Anwendung in der Informatik gefunden hat:
Zunächst wird jede Restklasse $r + m\mathbb{Z}$ durch ihr Bild $\Phi(r + m\mathbb{Z}) = (r_1 + m_1\mathbb{Z}, \ldots, r_n + m_n\mathbb{Z})$ ersetzt. Danach werden die Rechenschritte komponentenweise ausgeführt.

Beispiel 1.3.2. Berechne $(7 + 15\mathbb{Z}) \cdot (8 + 15\mathbb{Z})$.
Es ist

$$\begin{aligned} \Phi(7 + 15\mathbb{Z}) &= (2 + 5\mathbb{Z}, 1 + 3\mathbb{Z}) \\ \Phi(8 + 15\mathbb{Z}) &= (3 + 5\mathbb{Z}, 2 + 3\mathbb{Z}). \end{aligned}$$

Komponentenweise Rechnung ergibt $(2+5\mathbb{Z}, 1+3\mathbb{Z}) \cdot (3+5\mathbb{Z}, 2+3\mathbb{Z}) = (1+5\mathbb{Z}, 2+3Z) = \Phi(11+15\mathbb{Z})$. Also ist $(7 + 15\mathbb{Z}) \cdot (8 + 15\mathbb{Z}) = (11 + 15\mathbb{Z})$.

Zur algorithmischen Bestimmung der Zahlen l_j kann der Euklidische Algorithmus verwendet werden.

Beispiel 1.3.3. Man finde die Lösungsmenge des Systems

$$\begin{aligned} r &\equiv 2 \bmod 15 \\ r &\equiv 3 \bmod 23 \\ r &\equiv 5 \bmod 37. \end{aligned}$$

Lösung:
Es sei $m_1 = 15$, $m_2 = 23$ und $m_3 = 37$. Dann ist $m = m_1 \cdot m_2 \cdot m_3 = 12765$. Nach Satz 1.3.2 besteht die Lösungsmenge aus einer Restklasse modulo m. Wir bestimmen die Konstanten l_j. Dazu sei

$$M_j := \prod_{\substack{i=1 \\ i \neq j}}^{n} m_i$$

für $1 \leq i \leq 3$ gesetzt. Aus $l_j \equiv 0 \bmod m_i$ für alle $i \neq j$ und $l_j \equiv 1 \bmod m_j$ folgt $l_j = M_j x_j$ für $x_j \in \mathbb{Z}$. Es sind also x_j zu bestimmen, so dass $M_j x_j \equiv 1 \bmod m_j$ gilt.

- $j = 1$:
  Es ist
  $$23 \cdot 37x_1 \equiv 1 \bmod 15 \Rightarrow -4x_1 \equiv 1 \bmod 15.$$
  Zur Lösung der letzten Kongruenz genügt es, die Gleichung $-4x_1 + 15y_1 = 1$ mittels des Euklidischen Algorithmus (oder durch Erraten, was bei kleinen Koeffizienten einfach ist) zu lösen. Man findet
  $$\begin{aligned} 15 &= 3 \cdot 4 + 3 \\ 4 &= 3 + 1. \end{aligned}$$
  Also ist $1 = 4 - 3 = 4 - (15 - 3 \cdot 4) = 4 \cdot 4 - 15$ und $x - 1 = -4$ bzw. $l_1 = -4 \cdot 23 \cdot 37$.

- $j = 2$:
  Es ist
  $$15 \cdot 37x_2 \equiv 1 \bmod 23 \Rightarrow 3x_2 \equiv 1 \bmod 23,$$
  woraus sich $x_2 = 8$ bzw. $l_2 = 8 \cdot 15 \cdot 37$ ergeben.

- $j = 3$:
  Ausgehend von $15 \cdot 23 \equiv 1 \bmod 37$ haben wir
  $$\begin{aligned} 15 \cdot 23 &= 345 = 10 \cdot 37 - 25 \\ 37 &= 25 + 12 \\ 25 &= 2 \cdot 12 + 1. \end{aligned}$$
  Dies bedeutet

  $1 = 25 - 2 \cdot 12 = 25 - 2 \cdot (37 - 25) = 3 \cdot 25 - 2 \cdot 37 = 3 \cdot (10 \cdot 37 - 345) - 2 \cdot 37 = -3ßcdot345 + 28 \cdot 37.$

  Also ist $x_3 = -3$ und $l_3 = -3 \cdot 15 \cdot 23$. Nach Satz 1.3.2 ist das gegebene System an Kongruenzen zur einzigen Kongruenz
  $$r \equiv 2l_1 + 3l_2 + 5l_3 = 1337 \bmod 12765$$
  äquivalent.

Wir betrachten nun die Einheitengruppe eines direkten Produktes von Ringen. Man sieht unmittelbar die Gültigkeit von

Satz 1.3.3. *Es sei $R = R_1 \times \ldots \times R_n$. dann ist die Einheitengruppe durch das direkte Produkt*

$$R^* = R_1^* \times \ldots \times R_n^*$$

von Gruppen gegeben.

Satz 1.3.4. *Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann gilt*

$$a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^* \Leftrightarrow ggT(a, m) = 1.$$

Beweis. Es gilt

$$a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^* \Leftrightarrow \exists x \in \mathbb{Z} \colon ax + m\mathbb{Z} = 1 + m\mathbb{Z} \Leftrightarrow \exists x, y \in \mathbb{Z} \colon ax + my = 1,$$

was zu $ggT(a, m) = 1$ äquivalent ist. □

Definition 1.3.4. Es sei $m \in \mathbb{N}$. Die Restklasse $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})$ heißt teilerfremde Restklasse modulo m, wenn $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^*$ gilt.

Definition 1.3.5. Die Eulersche φ- Funktion ist die Funktion

$$\varphi = \begin{cases} \mathbb{N} \to \mathbb{N} \\ m \to |(\mathbb{Z}/m\mathbb{Z})^*|. \end{cases}$$

Bemerkung 1.3.1. Man sieht sofort, dass folgende Beschreibungen zu φ äquivalent sind:

i) die Anzahl der zu m teilerfremden Restklassen

ii) $|\{1 \leq a \leq m \colon ggT(a, m) = 1\}|$.

Beispiel 1.3.4. Von den Zahlen $\{a \colon 1 \leq a \leq 10\}$ sind $a = 1, 3, 7, 9$ zu 10 teilerfremd, also gilt $\varphi(10) = 4$.

Wir wollen eine Formel herleiten, die es erlaubt, die Eulersche φ- Funktion schnell zu berechnen.

Satz 1.3.5. *Es sei $m = m_1 \cdots m_r$ mit paarweise teilerfremden $m_i \in \mathbb{N}$. Dann gilt*

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/m_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/m_n\mathbb{Z})^*$$

und $\varphi(m) = \varphi(m_1) \cdots \varphi(m_r)$.

Beweis. Dies folgt aus den Sätzen 1.3.2 und 1.3.4. □

Satz 1.3.6. *Für $m \in \mathbb{N}$ gilt*

$$\varphi(m) = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right),$$

wobei sich das Produkt über alle Primzahlen erstreckt, die m teilen. Ist insbesondere $m = p^\alpha$ mit $\alpha \in \mathbb{N}$ und einer Primzahl p, so ist

$$\varphi(m) = p^\alpha - p^{\alpha-1} = p^\alpha \cdot \left(1 - \frac{1}{p}\right).$$

Beweis. Von den Repräsentanten $1, \ldots, p^\alpha$ von $\mathbb{Z}/p^\alpha\mathbb{Z}$ sind genau die Vielfachen von p, also $p, 2p, 3p, \ldots, p^\alpha$ zu p nicht teilerfremd. Also gilt

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \cdot \left(1 - \frac{1}{p}\right). \qquad (*)$$

Hat $m \in \mathbb{N}$ die Primfaktorzerlegung $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ mit $\alpha_j > 0$, so folgt mit Satz 1.3.5 und $(*)$ die Formel

$$\varphi(m) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}) = \prod_{i=1}^{r} p_i^{\alpha_i} \cdot \left(1 - \frac{1}{p}\right) = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

□

Beispiel 1.3.5. Bestimme $\varphi(360)$:
Es gilt mit $360 = 2^3 \cdot 3^2 \cdot 5$

$$\varphi(360) = \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(5) = 360 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 96.$$

Die folgenden zahlentheoretischen Aussagen, welche Folgerungen aus allgemeinen gruppentheoretischen Aussagen darstellen, waren schon lange vor der Entwicklung der Gruppentheorie bekannt.

Satz 1.3.7. *Es gilt:*

i) Euler, 18. Jahrhundert:
Es sei $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $ggT(a,n) = 1$. Dann ist $a^{\varphi(n)} \equiv 1 \bmod n$.

ii) "Kleiner Satz von Fermat", 17. Jahrhundert:
Es sei p eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist $a^{p-1} \equiv 1 \bmod p$.

Beweis. i) Dies ist ein Spezialfall $G = (\mathbb{Z}/n\mathbb{Z})^*$ aus der Gruppentheorie (siehe Elemente der Algebra).

ii) Dies ist wegen $\varphi(p) = p - 1$ für Primzahlen p ein Spezialfall von i).

□

Satz 1.3.8. *Es sei G eine endliche zyklsiche Gruppe, $G = \langle g \rangle$ und $|G| = |\langle g \rangle| = n$. Es sei $h = g^r$ mit $0 \leq r \leq n-1$. Dann gilt*

i) Es ist $|\langle h \rangle| = |\langle g^r \rangle| = \frac{n}{ggT(r,n)}$.
Weiter gilt genau dann $G = \langle h \rangle = \langle g^r \rangle$, wenn $ggT(r,n) = 1$ ist. Die Anzahl der Erzeugenden von G ist $\varphi(n)$.

ii) Die Menge der Untergruppen von G ist $\{U_d \colon d|n\}$ mit $U_d := \{x \in G \colon x^d = e\}$. Die Gruppe U_d ist zyklisch, und es gilt $|U_d| = d$.

iii) Es gibt genau $\varphi(d)$ Elemente $x \in G$ mit $|\langle x \rangle| = d$.

Beweis. i) Nach Elemente der Algebra Definition 1.3.3 ist $|\langle g^r \rangle| = \min\{m \geq 1 \colon g^{rm} = e\}$. Es gilt

$$g^{rm} = e \Leftrightarrow n|rm \Leftrightarrow \frac{n}{ggT(r,n)} \Big| m$$

nach Elementarer Zahlentheorie. Also gilt $|\langle g^r \rangle| = \frac{n}{ggT(r,n)}$ und $\langle g^r \rangle = G \Leftrightarrow ggT(r,n) = 1$.

ii) Es sei U eine Untergruppe von G. Nach dem Satz von Lagrange (Satz 1.7.3 in Elemente der Algebra) gilt $|U| = d$ mit einem Teiler $d|n$. Damit ist

$$U \subset U_d. \tag{1}$$

Es sei $h = g^{n/d}$ und $W_d = \langle h \rangle$. Nach Teil i) ist

$$|W_d| = |\langle h \rangle| = d, \tag{2}$$

also $x^d = e$ für alle $x \in W_d$. Somit ist

$$W_d \subset U_d. \tag{3}$$

Es sei $x = g^r \in U_d$, also $x^d = e$. Dann gilt $|\langle x \rangle| \big| d$ und damit nach Teil i)

$$\frac{n}{ggT(r,n)} \Big| d,$$

also $\frac{n}{d}|r$. Somit ist

$$x \in \langle h \rangle = W_d. \tag{4}$$

Aus (2), (3) und (4) folgt $U_d = W_d$ und $|U_d| = d$. Aus (1) folgt $U = U_d$. Damit ist ii) gezeigt.

iii) Dies folgt aus i) und ii).

□

Satz 1.3.9. *Es gilt*

$$\sum_{d|n} \varphi(d) = n.$$

Beweis. Dies folgt durch Anwendung von Satz 1.3.8 iii) auf die Gruppe $G = (\mathbb{Z}/n\mathbb{Z}, +)$. □

Satz 1.3.10. *Es sei G eine endliche abelsche Gruppe. Dann ist G genau dann zyklisch, wenn die folgende Aussage gilt:*

$$\textit{Für jedes } d \in \mathbb{N} \textit{ hat die Gleichung } x^d = e \textit{ höchstens } d \textit{ Lösungen.} \qquad (*)$$

Beweis. Es sei $|G| = n$.
"$\Rightarrow$":
Es sei G zyklisch. Dann folgt $(*)$ aus Satz 1.3.8.
"$\Leftarrow$":
Es sei $(*)$ erfüllt, und es genügt nun, die Existenz eines $g \in G$ mit $|\langle g \rangle| = n$ zu zeigen.
Es sei $F(d)$ die Anzahl der Elemente mit Ordnung d. Aus dem Satz von Lagrange folgt $F(d) = 0$ für $d \not| n$.
Wir zeigen, es gilt $F(d) = 0$ oder $F(d) = \varphi(d)$. Es sei $F(d) \neq 0$. Dann gibt es $x_d \in G$ mit $|\langle x_d \rangle| = d$. Für $U_d := \langle x_d \rangle$ gilt $|U_d| = d$ und $x^d = e$ für alle $x \in U_d$. Wegen $(*)$ folgt aus $|\langle x \rangle| = d$ auch $x \in U_d$. Nach Satz 1.3.8 ist $F(d) = \varphi(d)$. Aus der Existenz eines d mit $F(d) < \varphi(d)$ folgte

$$n = \sum_{d|n} F(d) < \sum_{d|n} \varphi(d) = n.$$

Also gilt $F(d) = \varphi(d)$ für alle $d|n$, und somit insbesobndere auch $F(n) = \varphi(n)$. Somit ist G zyklisch. □

Satz 1.3.11. *Es sei R ein Integritätsring und $f \in R[X]$ mit $\deg f = n \in \mathbb{N}_0$. Dann hat f höchstens n Nullstellen.*

Beweis. Induktion nach n:
Induktionsanfang: $n = 0$:
Es gilt $\deg f = 0$, also ist $f \equiv c \in R - \{0\}$, womit f keine Nullstelle hat.
$n = 1$:
Die Funktion $f(x) = a_1 x + a_0$ mit $a_1 \neq 0$ hat die einzige Nullstelle $x = -a_0 a_1^{-1}$.
Induktionsschritt: $n \to n + 1$:
Es sei $\deg f = n + 1$. Wir können annehmen, dass f mindestens eine Nullstelle $a_{n+1} \in R$ hat. Mittels des Divisionsalgorithmus erhalten wir $f(x) = (x - a_{n+1}) \cdot g(x)$ mit $\deg g = n$. Nach Induktionshypothese hat g die Nullstellen $\alpha_1, \ldots, \alpha_j$ mit $j \leq n$. Wegen der Nullteilerfreiheit von $R[X]$ folgt aus $f(\alpha) = 0$ entweder $\alpha = \alpha_{n+1}$ oder $\alpha \in \{\alpha - 1, \ldots, \alpha_j\}$. □

Satz 1.3.12. *Es sei R ein endlicher Integritätsring. Dann ist die Einheitengruppe R^* zyklisch. Ist insbesondere $(K, +, \cdot)$ ein endlicher Körper, so ist $K^* = (K - \{0_K\}, \cdot)$ zyklisch. Des Weiteren ist für eine Primzahl p die Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch.*

Beweis. Nach Satz 1.3.11 hat für jedes $d \in \mathbb{N}$ das Polynom $f = X^d - 1_R$ höchstens d Nullstellen im Ring R. Dann ist nach Satz 1.3.10 die Gruppe R^* zyklisch. □

Definition 1.3.6. Es sei $n \in \mathbb{N}$. Ein $r \in \mathbb{Z}$ mit $ggT(r, n) = 1$ heißt Primitivwurzel modulo n, falls $\langle r \bmod n \rangle = (\mathbb{Z}/n\mathbb{Z})^*$ gilt.

Beispiel 1.3.6. Es sei $n = 7$.
Es ist $3^1 \equiv 3 \bmod 7$, $3^2 \equiv 2 \bmod 7$, $3^3 \equiv 6 \bmod 7$, $3^4 \equiv 4 \bmod 7$, $3^5 \equiv 5 \bmod 7$ und $3^6 \equiv 1 \bmod 7$. Also ist $\langle 3 \bmod 7\rangle = (\mathbb{Z}/7\mathbb{Z})^*$, und 3 ist eine Primitivwurzel modulo 7.

Nach Satz 1.3.12 gibt es zu jeder Primzahl p eine Primitivwurzel modulo p. Wir geben ohne Beweis den folgenden Satz an:

Satz 1.3.13. *Es sei $n \in \mathbb{N}$. Dann ist $(\mathbb{Z}/n\mathbb{Z})^*$ genau dann zyklisch, d.h. es gibt eine Primitivwurzel modulo n, wenn $n \in \{1, 2, 4\}$, $n = p^\alpha$ oder $n = 2p^\alpha$ für eine ungerade Primzahl p und ein $\alpha \in \mathbb{N}$ ist. Für $k \geq 3$ ist $(\mathbb{Z}/2^k\mathbb{Z})^*$ das innere direkte Produkt der zyklischen Untergruppen $\langle 5 \bmod 2^k\rangle$ und $\langle(-1) \bmod 2^k\rangle$.*

1.4 Teilbarkeitstheorie

Wir rufen hier grundlegende Begriffe und Sätze der Vorlesung "Elemente der Algebra" in Erinnerung. Wir verzichten dabei auf eine Wiederholung der Beweise.
In diesem Abschnitt sei R stets ein Integritätsring.

Definition 1.4.1. Es seien $a, b, a' \in R$. es heißt a ein Teiler von b (oder a teilt b), wenn es ein $r \in R$ gibt mit $b = r \cdot a$ (Schreibweise: $a|b$). Ist a kein Teiler von b, so schreibt man $a \not| b$. Die Elemente a und a' heißen assoziiert, wenn es eine Einheit $u \in R^*$ mit $a' = ua$ gibt (Schreibweise: $a \sim a'$).

Folgende Teilbarkeitsregeln sind unmittelbar klar:

Satz 1.4.1. *Es sei R ein Integritätsring und $a, b, c, a', b_j \in R$. Dann gilt:*

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

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

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

iv) $a|b_1, \ldots, a|b_n \Rightarrow a|\sum_{i=1}^n b_i r_i$ *für alle* $r_i \in R$

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

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

Definition 1.4.2. Es sei R ein Integritätsring.

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

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

Bemerkung 1.4.1. Offenbar gilt: a prim $\Leftrightarrow$ $(a) = aR$ ist Primideal.

Satz 1.4.2. *Ist a prim, so ist a auch unzerlegbar.*

Bemerkung 1.4.2. Die Umkehrung gilt im Allgemeinen nicht.

Definition 1.4.3. Ein Ring R heißt ein Ring mit eindeutiger Faktorisierung oder faktoriell (oder Gaußscher Bereich), falls jede Nichteinheit eine im Wesentlichen eindeutige Faktorisierung in unzerlegbare Elemente besitzt.

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

Satz 1.4.3. *Ein Ring R ist faktoriell, falls*

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

ii) jedes irreduzible Element in R prim ist.

Die Umkehrung gilt trivialerweise.

Definition 1.4.4. Es sei R ein Integritätsring und $a, b \in R$ mit $a \neq 0$ oder $b \neq 0$. Das Element $c \in R$ heißt der größte gemeinsame Teiler von a und b (Schreibweise: $c = ggT(a, b)$), falls folgende Bedingungen gelten:

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

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

Das Element $x \in R$ heißt das kleinste gemeinsame Vielfache von a und b (Schreibweise: $x = kgV(a, b)$), falls folgende Bedingungen gelten:

1. $a|x$ und $b|x$,

2. $a|y$ und $b|y$ impliziert $x|y$.

Ist R faktoriell, so existieren der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache und sind bis auf Einheiten eindeutig bestimmt.

Definition 1.4.5. Es sei R ein Integritätsring.

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

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

Beispiel 1.4.1. Folgende Ringe sind Euklidisch:

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

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

Satz 1.4.4. *Es gilt:*

i) Ein Euklidischer Ring ist immer ein Hauptidealring.

ii) Ein Hauptidealring ist immer faktoriell.

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

Satz 1.4.5. *(Euklidischer Algorithmus)*
Es sei (R, δ) ein Euklidischer Ring und $r_1, r_2 \in R$ mit $r_2 \neq 0_R$. Konstruiere $q_i, r_i \in R$, so dass gilt:

$$
\begin{array}{lrcll}
(*) & r_1 & = & q_1 r_2 + r_3 & \text{mit} \quad \delta(r_3) < \delta(r_2) \\
& r_2 & = & q_2 r_3 + r_4 & \text{mit} \quad \delta(r_4) < \delta(r_3) \\
& \vdots & & \vdots & \vdots \\
& r_{n-1} & = & q_{n-1} r_n + r_{n+1} & \text{mit} \quad \delta(r_{n+1}) < \delta(r_n) \\
& r_n & = & q_n r_{n+1} + r_{n+2} & \text{mit} \quad r_{n+2} = 0_R
\end{array}
$$

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

Definition 1.4.6. Es sei R ein faktorieller Ring. Das Polynom $f = a_0 + a_1 X^1 + \cdots + a_{n-1} X^{n-1} + a_n X^n \in R[X]$ heißt primitiv, falls der größte gemeinsame Teiler von $a_0, \ldots, a_n$ gleich 1_R ist.

Satz 1.4.6. *(Gauß)*
Das Produkt zweier primitiver Polynome ist wieder primitiv (in $R[X]$, wobei R ein faktorieller Ring ist).

Satz 1.4.7. *Es sei R faktoriell, und K sei der Quotientenkörper von R. Ist $f \in R[X]$ irreduzibel, so ist f auch irreduzibel in $K[X]$.*

Satz 1.4.8. *Ist R faktoriell, so ist auch $R[X]$ faktoriell.*

Satz 1.4.9. *(Eisensteinkriterium)*
Es sei R faktoriell mit Quotientenkörper K und $f = a_0 + a_1 X^1 + \cdots + a_n X^n \in R[X]$ mit $a_n \neq 0$ für $n > 1$. Es sei weiter $p \in R$ prim, so dass $p \nmid a_n$ und $p | a_i$ für $i = n-1 \ldots 0$ und $p^2 \nmid a_0$.
Dann ist f irreduzibel in $K[X]$.

Satz 1.4.10. *Es sei R ein Ring und $I \trianglelefteq R$.*

i) Es ist R/I genau dann ein Integritätsring, wenn I ein Primideal ist.

ii) Es ist R/I genau dann ein Körper, wenn I maximal ist.

Kapitel 2

Galoistheorie

2.1 Grundlagen der Körpertheorie und Körpererweiterungen

Viele der Definitionen und Sätze in diesem Abschnitt wurden schon in der Vorlesung "Elemente der Algebra" behandelt. Wir verzichten daher weitgehend auf Beweise.

Definition 2.1.1. Es sei L ein Körper.

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

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

Beispiel 2.1.1. So sind etwa $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{R}$ Körpererweiterungen.

Definition 2.1.2. Es seien K_1 und K_2 Körper. Ein $\Phi\colon K_1 \to K_2$ heißt (Körper-)isomorphismus, falls es ein Ringisomorphismus ist. In diesem Fall heißen K_1 und K_2 isomorph (Schreibweise: $K_1 \cong K_2$).

Satz 2.1.1. *Es sei K ein Körper. Es gibt nun genau einen Ringhomomorphismus $\Phi\colon \mathbb{Z} \to K$ mit $\Phi(1) = 1_K$. Es gibt $p \in \mathbb{Z}$ mit $\mathrm{Kern}(\Phi) = p\mathbb{Z}$. Man unterscheidet zwei Fälle:*

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

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

Definition 2.1.3. Die Zahl p aus Satz 2.1.1 heißt Charakteristik von K (Schreibweise: $p = \mathrm{char}(K)$). Man nennt $\mathbb{F}_p$ den Primkörper der Charakteristik p. Der kleinste Unterkörper von K (d.h. der Durchschnitt aller Unterkörper von K) heißt Primkörper von K.

Definition 2.1.4. Es sei L/K eine Körpererweiterung und M eine Teilmenge von L. Man setzt

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

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

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

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

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

Definition 2.1.5. Es sei L eine Erweiterung eines Körpers K. Unter dem Grad von L über K (Schreibweise $[L\colon K]$) versteht man die Dimension von L als Vektorraum über K. Es handelt sich bei L um eine unendliche Erweiterung von K, falls $[L\colon K] = \infty$ ist, bzw. heißt L eine endliche Erweiterung von K, falls $[L\colon K] = n < \infty$ ist.

Satz 2.1.2. *(Gradsatz)*
Es seien L, K und M Körper sowie L/K und M/L Körpererweiterungen (Schreibweise: $M/L/K$).

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

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

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

Wir untersuchen nun einfache Körpererweiterungen auf Endlichkeit.

Definition 2.1.6. Es sei L/K eine Körpererweiterung. Ein $\alpha \in L$ heißt algebraisch über K, falls es ein Polynom $f \in K[X] - \{0\}$ mit $f(\alpha) = 0$ gibt. Ein $\alpha \in L$ heißt transzendent über K, falls es nicht algebraisch über K ist. Die Erweiterung L/K heißt algebraisch über K, falls alle $\alpha \in L$ algebraisch über K sind. Nicht algebraische Erweiterungen heißen transzendent. Eine komplexe Zahl $z \in \mathbb{C}$ heißt algebraisch (bzw. transzendent), falls z algebraisch (bzw. transzendent) über $\mathbb{Q}$ ist.

Bemerkung 2.1.1. Es sei $\alpha \in L$.

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

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

Definition 2.1.7. Unter einem normierten Polynom $f \in K[X]$ versteht man ein Polynom mit höchstem Koeffizienten 1_K, also

$$f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0.$$

Satz 2.1.3. *Es sei X eine Unbestimmte über K und L/K eine Körpererweiterung von K mit $\alpha \in L$. Der Ringhomomorphismus Φ sei durch $\Phi\colon K[X] \to K[\alpha]$, $f \to f(\alpha)$ gegeben.*

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

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

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

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

iii) Folgende Aussagen sind äquivalent:

(a) α ist algebraisch über K.

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

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

Definition 2.1.8. Es sei α algebraisch über dem Körper K. Das Polynom g des Satzes 2.1.3 heißt Minimalpolynom von α über K (Schreibweise: $m_K(\alpha, X)$). Der Grad $\deg(m_K(\alpha, X))$ des Minimalpolynoms heißt auch Grad von α über K (Schreibweise: $\deg_K(\alpha)$). Nach Satz 2.1.3 ist $\deg_K(\alpha) = [K(\alpha)\colon K]$. Offenbar gilt

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

Beispiel 2.1.2. Es sei $K = \mathbb{Q}$ und $L = \mathbb{R}$. Nach dem Zwischenwertsatz der Analysis hat das Polynom $g(X) = X^3 - 2$ in $L = \mathbb{R}$ genau eine Nullstelle, nämlich $\alpha = \sqrt[3]{2}$. Somit ist nach dem Eisensteinkriterium (Satz 1.4.9) g irreduzibel. Daher ist $m_{\mathbb{Q}}(\sqrt[3]{2}, X) = X^3 - 2$. Nach Satz 2.1.3 ist

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

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

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

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

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

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

Satz 2.1.4. *Es sei L/K eine Körpererweiterung. Folgende Eigenschaften sind äquivalent:*

i) L/K ist endlich.

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

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

Satz 2.1.5. *Es seien $M/L/K$ Körpererweiterungen. Ist M algebraisch über L und L algebraisch über K, so ist auch M algebraisch über K.*

2.2 Fortsetzung von Körperisomorphismen und Automorphismengruppen

Definition 2.2.1. Es seien L_1 und L_2 Erweiterungen eines Körpers K.
Ein Isomorphismus $\sigma\colon L_1 \to L_2$ heißt ein K-Isomorphismus, falls $\sigma(z) = z$ für alle $z \in K$ gilt.
Falls ein solcher K-Isomorphismus existiert, heißen L_1 und L_2 auch K-isomorph. Ist $L_1 = L_2$, so heißt σ auch K-Automorphismus von L.

Wir untersuchen zunächst die Frage, wann zwei einfache endliche Erweiterungen eines gegebenen Körpers K zueinander K-isomorph sind.

Definition 2.2.2. Es sei K ein Körper und α sowie β Elemente einer Erweiterung von K. Die Elemente α und β heißen konjugiert über K, wenn beide Elemente über K algebraisch sind und das gleiche Minimalpolynom über K besitzen. Dann heißt β auch die Konjugierte von α.

Beispiel 2.2.1. Es sei $\alpha = \sqrt[4]{2}$ und $K = \mathbb{Q}$.
Nach dem Eisensteinkriterium (Satz 1.4.9) ist $X^4 - 2$ in $\mathbb{Q}[X]$ irreduzibel und hat die Nullstelle α. Damit ist $m_{\mathbb{Q}}(\alpha, X) = X^4 - 2$. Im Körper $\mathbb{C}$ der komplexen Zahlen gilt dann

$$m_{\mathbb{Q}}(\alpha, X) = \left(X - \sqrt[4]{2}\right) \cdot \left(X + \sqrt[4]{2}\right) \cdot \left(X - i\sqrt[4]{2}\right) \cdot \left(X + i\sqrt[4]{2}\right).$$

Damit sind die Elemente $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = -\sqrt[4]{2}$, $\alpha_3 = i \cdot \sqrt[4]{2}$ und $\alpha_4 = -i \cdot \sqrt[4]{2}$ Konjugierte über dem Körper $\mathbb{Q}$. Diese vier Elemente sind alle Konjugierten von α in $\mathbb{C}$, da $m_{\mathbb{Q}}(\alpha, X)$ keine anderen Nullstellen besitzt. Die Elemente α_1 und α_2 sind auch wegen

$$m_{\mathbb{Q}(\sqrt{2})}(\alpha_1, X) = m_{\mathbb{Q}(\sqrt{2})}(\alpha_2, X) = X^2 - \sqrt{2}$$

über $\mathbb{Q}(\sqrt{2})$ konjugiert. Ebenso sind α_3 und α_4 über $\mathbb{Q}(\sqrt{2})$ konjugiert, da

$$m_{\mathbb{Q}(\sqrt{2})}(\alpha_3, X) = m_{\mathbb{Q}(\sqrt{2})}(\alpha_4, X) = X^2 + \sqrt{2}$$

gilt. Hingegen sind α_1 oder α_2 zu keinem der Elemente α_3 oder α_4 über $\mathbb{Q}(\sqrt{2})$ konjugiert.

Satz 2.2.1. *Es sei K ein Körper und α, β algebraisch über K.*
Falls α und β das gleiche Minimalpolynom über K besitzen, sind $K(\alpha)$ und $K(\beta)$ dann K-isomorph. Ein K-Isomorphismus wird dann durch die Zuordnung

$$\sum_{j=0}^{n-1} b_j \alpha^j \to \sum_{j=0}^{n-1} b_j \beta^j$$

für $n = \deg(\alpha) = \deg(\beta)$ mit $b_j \in K$ hergestellt.

In Hinblick auf weitere Anwendungen beweisen wir eine Verallgemeinerung dazu (Satz 2.2.2).

Definition 2.2.3. Es seien L bzw. $\overline{L}$ Erweiterungen von K bzw. $\overline{K}$.
Es sei σ ein Isomorphismus von K auf $\overline{K}$ und τ ein Isomorphismus von L auf $\overline{L}$.
Wir sagen, τ setzt σ fort, bzw. τ ist Fortsetzung von σ, falls $\tau(z) = \sigma(z)$ für alle $z \in K$ gilt, wenn also σ gerade die Einschränkung $\tau|_K$ von τ ist.

Satz 2.2.2. *Es sei α algebraisch über K und $g(X) = m_K(\alpha, X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$. Ferner sei $\overline{L}$ eine Erweiterung eines Körpers $\overline{K}$ und ein Isomorphismus $\sigma\colon K \to \overline{K}$ gegeben, sowie $g^{(\sigma)}(Y) = \sigma(a_0) + \sigma(a_1)Y + \cdots + \sigma(a_{n-1})Y^{n-1} + Y^n \in K[Y]$ mit einer Unbestimmten Y über $\overline{K}$ gesetzt.*

i) Es gibt genau dann einen Isomorphismus $\tau\colon K(\alpha) \to K'$ in einen Unterkörper $K' \leq \overline{L}$ der σ fortsetzt, wenn $g^{(\sigma)}$ mindestens eine Nullstelle in $\overline{L}$ besitzt.

ii) Sind $\beta_1, \ldots, \beta_r$ die verschiedenen Nullstellen von $g^{(\sigma)}$ in $\overline{L}$, so gibt es genau r derartige Fortsetzungen von σ. Dies sind die surjektiven Abbildungen $\tau_k\colon K(\alpha) \to \overline{K}(\beta_k)$ für $k = 1, \ldots, r$, welche durch

$$\tau_k\left(\sum_{j=0}^{n-1} b_j\alpha^j\right) = \sum_{j=0}^{n-1} \sigma(b_j)\beta_k^j$$

mit $n = [K(\alpha) : K]$ definiert sind.

Kurz ausgedrückt: Die Fortsetzungen $\tau_1, \ldots, \tau_r$ von σ sind den Nullstellen $\beta_1, \ldots, \beta_r$ von $g^{(\sigma)}(Y)$ in der Erweiterung $\overline{L}$ eindeutig zugeordnet. Die Abbildung τ_k ist durch die Forderung

$$\tau_k(\alpha) = \beta_k$$

eindeutig bestimmt, und es ist $[K(\alpha) : K] = [\overline{K}(\beta_k) : \overline{K}]$ für $k = 1, \ldots, r$.

Bemerkung 2.2.1. Satz 2.2.1 ergibt sich als Spezialfall von Satz 2.2.2, wenn $K = \overline{K}$ und $\sigma = id_K$ gesetzt wird.

Beweis. (Beweis von Satz 2.2.2)

i) Es sei $\tau\colon K(\alpha) \to K'$ ein Isomorphismus, der σ fortsetzt. Dann gilt

$$0 = \tau(g(\alpha)) = \sum_{j=0}^{n} \tau(a_j) \cdot \tau(\alpha)^j = \sum_{j=0}^{n} \sigma(a_j) \cdot \tau(\alpha)^j = g^{(\sigma)}(\tau(\alpha)),$$

also ist $\tau(\alpha)$ eine Nullstelle von $g^{(\sigma)}$ in $\overline{L}$. Durch die Kenntnis von $\beta = \tau(\alpha)$ ist τ vollständig bestimmt, denn für ein beliebiges $b \in K(\alpha)$ gilt

$$b = \sum_{j=0}^{n-1} b_j\alpha^j \quad \Rightarrow \quad \tau(b) = \sum_{j=0}^{n-1} \tau(b_j)\tau(\alpha^j) = \sum_{j=0}^{n-1} \sigma(b_j)\beta^j.$$

ii) Umgekehrt sei β eine beliebige Nullstelle von $g^{(\sigma)}(Y)$ in $\overline{L}$. Für ein beliebiges $b \in K(\alpha)$, etwa $b = \sum b_j\alpha^j$ mit $b_j \in K$, setzen wir

$$\tau(b) = \sum_{j=0}^{n-1} \sigma(b_j)\alpha^j.$$

Es bleibt nachzuweisen, dass τ ein Isomorphismus von $K(\alpha)$ auf $\overline{K}(\beta)$ ist, der σ fortsetzt. Dazu beachtet man zunächst, dass $g^{(\sigma)}(Y) = m_{\overline{K}}(\beta, Y)$ ist. Wie man leicht nachrechnet, ist die Abbildung

$$\omega\colon \sum b_jX^j \to \sum \sigma(b_j)Y^j$$

ein Isomorphismus $K[X] \to \overline{K}[Y]$ mit $\omega(g) = g^{(\sigma)}$.

Aus der Irreduzibilität von g in $K[X]$ folgt die Irreduzibilität von $g^{(\sigma)}$ in $\overline{K}[Y]$. Es sei

$$h\colon \sum b_j X^j + (g) \to \sum \sigma(b_j) Y^j + (g^{(\sigma)}).$$

Offenbar ist h ein Epimorphismus $h\colon K[x]/(g) \to \overline{K}[Y]/(g^{(\sigma)})$. Wir wollen zeigen, dass h auch injektiv und damit ein Isomorphismus ist. Dazu bestimmen wir Kern(h). Es sei

$$h\left(\sum b_j X^j + (g)) = 0_{\overline{K}[Y]} + (g^{(\sigma)}\right) = (g^{(\sigma)}).$$

Dann gilt $g^{(\sigma)} | \sum \sigma(b_j) Y^j$, also ist $\sum \sigma(b_j) Y^j = g^{(\sigma)} \cdot h^{(\sigma)}$ für ein $h^{(\sigma)} = \sum \sigma(d_j) Y^j = \omega(h)$ mit $h = \sum d_j X^j$. Anwendung von ω^{-1} ergibt dann $\sum b_j X^j = g \cdot h$, also $\sum b_j X^j + (g) = 0_{K[X]} + (g)$. Daraus folgt Kern$(h) = \{0_{K[X]/(g)}\}$. Nach Satz 2.1.3 sind die Abbildungen

$$\begin{aligned} \psi_1 &: K[\alpha] \to K[X]/(g), \quad \sum b_j \alpha^j \to \sum b_j X^j + (g) \\ \psi_2 &: \overline{K}[\beta] \to \overline{K}[Y]/(g^{(\sigma)}), \quad \sum \sigma(b_j) \beta^j \to \sum \sigma(b_j) Y^j + (g^{(\sigma)}) \end{aligned}$$

Isomorphismen. Daher ist auch $\tau = \psi_2^{-1} \circ h \circ \psi_1$ ein Isomorphismus und besitzt die gewünschten Eigenschaften.

□

Beispiel 2.2.2. Es sei $K = \overline{K} = \mathbb{Q}$ und $\overline{L} = \mathbb{C}$ mit $\sigma = id_{\mathbb{Q}}$ sowie $\alpha = \sqrt{2}$. Es liegt also der Spezialfall Satz 2.2.1 vor. Nach dem Eisensteinkriterium ist das Polynom $q(X) = X^2 - 2$ irreduzibel. Das Element $\alpha = \sqrt{2}$ hat daher das Minimalpolynom $q(X) = X^2 - 2$. Wegen $\sigma = id_{\mathbb{Q}}$ gilt $g^{(\sigma)} = Y^2 - 2$ mit den Nullstellen $\beta_1 = \sqrt{2}$ und $\beta_2 = -\sqrt{2}$ in $\overline{L} = \mathbb{C}$. Die Fortsetzungen τ_j mit $j = 1, 2$ von $\sigma = id$ sind also durch den Wert $\tau_j(\alpha) \in \{\beta_1, \beta_2\}$ bestimmt.

- Fall j=1:
  Die Festlegung $\tau_1\colon \sqrt{2} \to \sqrt{2}$ ergibt $\tau_1(b_0 + b_1\sqrt{2}) = b_0 + b_1\sqrt{2}$ für alle $b_0, b_1 \in \mathbb{Q}$, also insgesamt $\tau_1 = id_{\mathbb{Q}(\sqrt{2})}$.
- Fall j=2:
  Die Festlegung $\tau_2\colon \sqrt{2} \to -\sqrt{2}$ ergibt $\tau_2(b_0 + b_1\sqrt{2}) = b_0 - b_1\sqrt{2}$.

Beispiel 2.2.3. Es sei $K = \overline{K} = \mathbb{Q}(\sqrt{2})$ mit $\sigma_1 = id_K = \tau_1$ und $\sigma_2 = \tau_2$ aus dem vorigen Beispiel. Dazu sei $\alpha_1 = \sqrt[4]{2}$ und $\alpha_2 = i \cdot \sqrt[4]{2}$. Es ist $m_{\mathbb{Q}}(\alpha_1, X) = m_{\mathbb{Q}}(\alpha_2, X) = X^4 - 2$.
Also ist $\deg(\alpha_1) = \deg(\alpha_2) = 4$. Damit sind $\alpha_1, \alpha_2 \notin K$ wegen $[K\colon \mathbb{Q}] = 2$. Es ist

$$\begin{aligned} m_K(\alpha_1, X) &= X^2 - \sqrt{2} = g_1(X) \\ m_K(\alpha_2, X) &= X^2 + \sqrt{2} = g_2(X). \end{aligned}$$

- Die Fortsetzungen von σ_1:
  Die Fortsetzungen von σ_1 sind nach Satz 2.2.2 durch die Nullstellen $\beta_{1,1} = \sqrt[4]{2}$ und $\beta_{1,2} = -\sqrt[4]{2}$ von $g_1^{(\sigma_1)} = Y^2 - \sqrt{2}$ eindeutig bestimmt.
  Wir haben die Fortsetzungen

$$\begin{aligned} \sigma_{1,1} &: \sqrt[4]{2} \to \sqrt[4]{2}, \quad \text{d.h. } \sigma_{1,1} = id_{\mathbb{Q}(\sqrt[4]{2})} \\ \sigma_{1,2} &: \sqrt[4]{2} \to -\sqrt[4]{2}, \quad \text{d.h. } \sigma_{1,2}\colon b_0 + b_1\sqrt[4]{2} + b_2\sqrt[2]{2} + b_3(\sqrt[4]{2})^3 \to b_0 - b_1\sqrt[4]{2} + b_2\sqrt[2]{2} - b_3(\sqrt[4]{2})^3. \end{aligned}$$

- Die Fortsetzungen von σ_2:
  Die Fortsetzungen von σ_2 sind durch die Nullstellen von $g^{(\sigma_2)}(Y) = Y^2 - \sigma_2(\sqrt{2}) = Y^2 + \sqrt{2}$ gegeben: $\beta_{2,1} = i \cdot \sqrt[4]{2}$ und $\beta_{2,2} = -i \cdot \sqrt[4]{2}$.

$$\begin{aligned}
\sigma_{2,1} &: \quad \sqrt[4]{2} \to i \cdot \sqrt[4]{2}, \quad \text{d.h.} \\
\sigma_{2,1} &: \quad b_0 + b_1\sqrt[4]{2} + b_2\sqrt[2]{2} + b_3(\sqrt[4]{2})^3 \to b_0 + b_1(i \cdot \sqrt[4]{2}) - b_2\sqrt[2]{2} + b_3(i \cdot \sqrt[4]{2})^3 \quad \text{und} \\
\sigma_{2,2} &: \quad \sqrt[4]{2} \to -i \cdot \sqrt[4]{2}, \quad \text{d.h.} \\
\sigma_{2,2} &: \quad b_0 + b_1\sqrt[4]{2} + b_2\sqrt[2]{2} + b_3(\sqrt[4]{2})^3 \to b_0 - b_1(i \cdot \sqrt[4]{2}) - b_2\sqrt[2]{2} + b_3 \cdot i \cdot (\sqrt[4]{2})^3.
\end{aligned}$$

  Das heißt, dass σ_2 keine Fortsetzung zu Isomorphismen $\mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ besitzt, da $g^{(\sigma_2)}$ keine Nullstellen in $\mathbb{Q}(\sqrt[4]{2})$ hat.

Beispiel 2.2.4. Man finde sämtliche $\mathbb{Q}$-Automorphismen von $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

Lösung:
Der Körper L ist eine Erweiterung des in Beispiel 2.2.3 betrachteten Körpers $\mathbb{Q}(\sqrt[4]{2})$. Nach Satz 2.2.2 findet man sämtliche Automorphismen von L als Fortsetzungen der im vorigen Beispiel betrachteten Isomorphismen von $\mathbb{Q}(\sqrt[4]{2})$, deren Bilder in L liegen.

- Die Fortsetzungen der Isomorphismen $\sigma_{1,1}$ und $\sigma_{1,2}$:
  Wir wenden Satz 2.2.2 mit $K = \overline{K} = \mathbb{Q}(\sqrt[4]{2})$ an. Das Polynom $q(X) = X^2 + 1$ ist in $K[X]$ irreduzibel, da es in K keine Nullstelle besitzt. Also ist $m_K(i, X) = X^2+1 = (X+i)(X-i)$ und somit $[L : \mathbb{Q}] = 8$. Es ist $g^{(\sigma_{1,1})}(Y) = g^{(\sigma_{1,2})} = Y^2 + 1$. Die Fortsetzungen $\sigma_{1,1,1}$ und $\sigma_{1,1,2}$ von $\sigma_{1,1}$ bzw. $\sigma_{1,2,1}$ und $\sigma_{1,2,2}$ von $\sigma_{1,2}$ sind durch die Nullstellen i und $-i$ von $g^{(\sigma_{1,2})}(Y)$ bestimmt:

$$\begin{aligned}
\sigma_{1,1,1} &: \quad \sqrt[4]{2} \to \sqrt[4]{2}, \quad i \to i \\
\sigma_{1,1,2} &: \quad \sqrt[4]{2} \to \sqrt[4]{2}, \quad i \to -i \\
\sigma_{1,2,1} &: \quad \sqrt[4]{2} \to -\sqrt[4]{2}, \quad i \to i \\
\sigma_{1,2,2} &: \quad \sqrt[4]{2} \to -\sqrt[4]{2}, \quad i \to -i.
\end{aligned}$$

  Insbesondere ist $\sigma_{1,1,1} = id_L$.

- Die Fortsetzungen der Isomorphismen $\sigma_{2,1}$ und $\sigma_{2,2}$:
  Wir wenden Satz 2.2.2 mit $K = \mathbb{Q}(\sqrt[4]{2})$ und $\overline{K} = \mathbb{Q}(i \cdot \sqrt[4]{2})$ an. Wäre $i \in \overline{K}$, so wäre $L = \overline{K}$ im Widerspruch zu $[L\colon \mathbb{Q}] = 8$ und $[\overline{K} : \mathbb{Q}] = 4$. Damit besitzt g auch in $\overline{K}$ keine Nullstelle und ist in $\overline{K}[X]$ irreduzibel. Wiederum sind die Fortsetzungen von $\sigma_{2,1}$ und $\sigma_{2,2}$ durch die Nullstellen von $g^{(\sigma_{2,1})} = g^{(\sigma_{2,2})} = Y^2 + 1$ bestimmt:

$$\begin{aligned}
\sigma_{2,1,1} &: \quad \sqrt[4]{2} \to i \cdot \sqrt[4]{2}, \quad i \to i \\
\sigma_{2,1,2} &: \quad \sqrt[4]{2} \to i \cdot \sqrt[4]{2}, \quad i \to -i \\
\sigma_{2,2,1} &: \quad \sqrt[4]{2} \to -i \cdot \sqrt[4]{2}, \quad i \to i \\
\sigma_{2,2,2} &: \quad \sqrt[4]{2} \to -i \cdot \sqrt[4]{2}, \quad i \to -i.
\end{aligned}$$

  Damit sind alle Fortsetzungen von $id_{\mathbb{Q}}$ Automorphismen von L, es gibt also insgesamt acht Automorphismen von $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

Satz 2.2.2 gibt eine Methode, die schon in den obigen Beispielen illustriert wurde, um alle K-isomorphen Bilder einer endlichen Erweiterung $K(\alpha_1, \ldots, \alpha_n)$ von K in einer Erweiterung L von K zu finden. Durch wiederholte Anwendung von Satz 2.2.1 findet man zunächst alle Fortsetzungen von id_K zu K-Isomorphismen von $K(\alpha_1)$, dann alle Fortsetzungen dieser Isomorphismen zu K-Isomorphismen von $K(\alpha_1, \alpha_2)$ usw. Auf diese Weise gelingt es, insbesondere auch sämtliche K-Automorphismen einer endlichen Erweiterung von K zu finden. Diese sind unter den Körperisomorphismen von besonderem Interesse, da ihre Menge eine Gruppe bzgl. der Hintereinanderausführung $\circ$ bildet. In den folgenden Definitionen wird zunächst nicht vorausgesetzt, dass die betrachteten Körpererweiterungen endlich sind.

Definition 2.2.4. Es sei L/K eine Körpererweiterung.

i) Die Gruppe aller K-Automorphismen von L heißt die Galoisgruppe von L/K (Schreibweise: $G(L/K)$).

ii) Ein Körper Z mit $K \subseteq Z \subseteq L$ heißt Zwischenkörper von L/K (Schreibweise: $L/Z/K$).

iii) Ist U eine Untergruppe von $G(L/K)$, so heißt $L^U := \{z \in L \colon \sigma(z) = z,\ \forall \sigma \in U\}$ der Fixkörper zu U in L.

Die Galoistheorie (nach Evariste Galois) befasst sich mit der Beziehung zwischen den Untergruppen von $G(L/K)$ und den Zwischenkörpern von L/K. Es gibt zwei Zuordnungen. Die erste ist die Zuordnung $Z \to G(L/Z)$, die jedem Zwischenkörper die Untergruppe der Z-Automorphismen von L zuordnet. Die zweite ist die Zuordnung $U \to L^U$, die einer Untergruppe von $G(L/K)$ den zugehörigen Fixkörper in L zuordnet. In wichtigen Fällen, den sogenannten Galoisschen Erweiterungen, sind diese beiden Zuordnungen bijektiv und invers zueinander, also

$$G(L/L^U) = U \quad \text{und} \quad L^{G(L/Z)} = Z$$

für alle Untergruppen $U \leq G(L/K)$ und Zwischenkörper $L/Z/K$.

Beispiel 2.2.5. Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
Bestimme die Struktur von $G(L/K)$, ihre Untergruppen und deren Fixkörper.

Lösung:
Die Fortsetzungen von $id_{\mathbb{Q}}$ auf $\mathbb{Q}(\sqrt{2})$ sind durch

$$\begin{aligned} id_{\mathbb{Q}(\sqrt{2})} = \sigma_0 &: \quad \sqrt{2} \to \sqrt{2} \\ \sigma_1 &: \quad \sqrt{2} \to -\sqrt{2} \end{aligned}$$

bestimmt.
Annahme: $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.
Dann ist $\sqrt{3} = b_0 + b_1\sqrt{2}$ für $b_1, b_2 \in \mathbb{Q}$. Wegen $\sigma_1(\sqrt{3})^2 = \sigma_1((\sqrt{3})^2) = \sigma_1(3) = 3$ folgt nun auch $b_0 - b_1\sqrt{2} \in \{\sqrt{3}, -\sqrt{3}\}$. Damit ist $b_0 = \sqrt{3}$ oder $b_1 = \sqrt{3/2}$, was wegen $\sqrt{3}, \sqrt{3/2} \notin \mathbb{Q}$ unmöglich ist. Also $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Somit ist $m_{\mathbb{Q}(\sqrt{2})}(\sqrt{3}, X) = X^2 - 3 = (X - \sqrt{3})(X + \sqrt{3})$. Nach Satz 2.2.2 sind die Fortsetzungen von σ_0 und σ_1 durch

$$\begin{aligned} \sigma_{0,0} &: \quad \sqrt{2} \to \sqrt{2}, \quad \sqrt{3} \to \sqrt{3} \\ \sigma_{0,1} &: \quad \sqrt{2} \to \sqrt{2}, \quad \sqrt{3} \to -\sqrt{3} \\ \sigma_{1,0} &: \quad \sqrt{2} \to -\sqrt{2}, \quad \sqrt{3} \to \sqrt{3} \\ \sigma_{1,1} &: \quad \sqrt{2} \to -\sqrt{2}, \quad \sqrt{3} \to -\sqrt{3} \end{aligned}$$

gegeben.

Also gilt $\sigma_{k,l}\colon \sqrt{2} \to (-1)^k \cdot \sqrt{2}$, $\sqrt{3} \to (-1)^l \cdot \sqrt{3}$ für $k, l \in \{0, 1\}$.
Die Komposition zweier Automorphismen wird berechnet, indem ihre Wirkung auf die Elemente $\sqrt{2}$ und $\sqrt{3}$ untersucht wird. Es gilt

$$\begin{aligned}(\sigma_{k_1,l_1} \circ \sigma_{k_2,l_2})(\sqrt{2}) &= \sigma_{k_1,l_1}(\sigma_{k_2,l_2}(\sqrt{2})) = \sigma_{k_1,l_1}((-1)^{k_2}\sqrt{2}) \\ &= \sigma_{k_1,l_1}((-1)^{k_2})\sigma_{k_1,l_1}(\sqrt{2}) = (-1)^{k_2}\sigma_{k_1,l_1}(\sqrt{2}) = (-1)^{k_1+k_2} \cdot \sqrt{2}\end{aligned}$$

und

$$\begin{aligned}(\sigma_{k_1,l_1} \circ \sigma_{k_2,l_2})(\sqrt{3}) &= \sigma_{k_1,l_1}(\sigma_{k_2,l_2}(\sqrt{3})) = \sigma_{k_1,l_1}((-1)^{l_2}\sqrt{3}) \\ &= \sigma_{k_1,l_1}((-1)^{l_2})\sigma_{k_1,l_1}(\sqrt{3}) = (-1)^{l_2}\sigma_{k_1,l_1}(\sqrt{3}) = (-1)^{l_1+l_2} \cdot \sqrt{3}.\end{aligned}$$

Damit gilt $\sigma_{k_1,l_1} \circ \sigma_{k_2,l_2} = \sigma_{k_3,l_3}$, wobei (k_3, l_3) durch die Beziehungen $k_3 \equiv k_1 + k_2 \bmod 2$ und $l_3 \equiv l_1 + l_2 \bmod 2$ bestimmt ist. Diese Beziehungen legen nahe, die Beschreibung zu vereinfachen, indem man zur Indizierung der Automorphismen Restklassen modulo 2 verwendet.
Für $(r, s) \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ setzen wir $\sigma_{r,s}\colon \sqrt{2} \to (-1)^k \cdot \sqrt{2}$, $\sqrt{3} \to (-1)^l \cdot \sqrt{3}$ für beliebige $k \in r$ und $l \in s$. Wir erhalten die Beziehung $\sigma_{r_1,s_1} \circ \sigma_{r_2,s_2} = \sigma_{r_1+r_2,s_1+s_2}$.
Die Untergruppen von $G(L/K)$ sind dann

$$\begin{aligned}\left\langle \sigma_{\overline{0},\overline{0}} \right\rangle &= \{\sigma_{\overline{0},\overline{0}}\} = \{id_L\}, \\ \left\langle \sigma_{\overline{0},\overline{1}} \right\rangle &= \{\sigma_{\overline{0},\overline{0}}, \sigma_{\overline{0},\overline{1}}\}, \\ \left\langle \sigma_{\overline{1},\overline{0}} \right\rangle &= \{\sigma_{\overline{0},\overline{0}}, \sigma_{\overline{1},\overline{0}}\}, \\ \left\langle \sigma_{\overline{1},\overline{1}} \right\rangle &= \{\sigma_{\overline{0},\overline{0}}, \sigma_{\overline{1},\overline{1}}\}\end{aligned}$$

und $G(L/K)$ selbst, wobei $\overline{k}$ hier als die Restklasse k mod 2 zu verstehen ist.
Nach den Sätzen 2.2.1 und 2.2.2 ist

$$\begin{aligned}L &= \{b_0 + b_1\sqrt{2} + b_2\sqrt{3} + b_3\sqrt{6}\colon b_i \in \mathbb{Q}\}, \\ L^{\langle \sigma_{\overline{0},\overline{1}} \rangle} &= \{z \in L\colon \sigma_{\overline{0},\overline{0}}(z) = z,\ \sigma_{\overline{0},\overline{1}}(z) = z\}.\end{aligned}$$

Es ist $\sigma_{\overline{0},\overline{0}}(z) = z$ für alle $z \in L$. Andererseits ist

$$\sigma_{\overline{0},\overline{1}}(b_0 + b_1\sqrt{2} + b_2\sqrt{3} + b_3\sqrt{6}) = b_0 + b_1\sqrt{2} - b_2\sqrt{3} - b_3\sqrt{6},$$

und damit gilt

$$\sigma_{\overline{0},\overline{1}}(z) = z \Leftrightarrow z = b_0 + b_2\sqrt{2} \Leftrightarrow z \in \mathbb{Q}(\sqrt{2}),$$

d.h. $L^{\langle \sigma_{\overline{0},\overline{1}} \rangle} = \mathbb{Q}(\sqrt{2})$. Weiter folgt

$$\begin{aligned}\sigma_{\overline{1},\overline{0}}\colon b_0 + b_1\sqrt{2} + b_2\sqrt{3} + b_3\sqrt{6} &\to b_0 - b_1\sqrt{2} + b_2\sqrt{3} - b_3\sqrt{6} \\ \sigma_{\overline{1},\overline{1}}\colon b_0 + b_1\sqrt{2} + b_2\sqrt{3} + b_3\sqrt{6} &\to b_0 - b_1\sqrt{2} - b_2\sqrt{3} + b_3\sqrt{6},\end{aligned}$$

also gilt analog

$$\begin{aligned}\sigma_{\overline{1},\overline{0}}(z) = z &\Leftrightarrow z \in \mathbb{Q}(\sqrt{3}), \\ \sigma_{\overline{1},\overline{1}}(z) = z &\Leftrightarrow z \in \mathbb{Q}(\sqrt{6}).\end{aligned}$$

Insgesamt ergeben sich die zu den Untergruppen von $G(L/K)$ gehörenden Fixkörper mit

$$\begin{aligned} L^{\langle \sigma_{\bar{0},\bar{0}} \rangle} &= L, \\ L^{\langle \sigma_{\bar{1},\bar{0}} \rangle} &= \mathbb{Q}(\sqrt{3}), \\ L^{\langle \sigma_{\bar{0},\bar{1}} \rangle} &= \mathbb{Q}(\sqrt{2}), \\ L^{\langle \sigma_{\bar{1},\bar{1}} \rangle} &= \mathbb{Q}(\sqrt{6}), \\ L^{G(L/K)} &= K = \mathbb{Q}. \end{aligned}$$

Damit ist die Körpererweiterung L/K galoissch.
Die Zuordnungen zwischen Untergruppen von $G(L/K)$ und den Zwischenkörpern $L/Z/K$ lassen sich durch die folgenden Diagramme illustrieren:

$$\begin{array}{ccccc} \{\mathrm{id}\} & & & & L \\ \| & & & & \| \\ \langle\, \sigma_{\bar{0},\bar{0}} \,\rangle & & & & \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ / \quad | \quad \backslash & & U \longrightarrow L^U & & / \quad | \quad \backslash \\ \langle\, \sigma_{\bar{0},\bar{1}} \,\rangle \quad \langle\, \sigma_{\bar{1},\bar{0}} \,\rangle \quad \langle\, \sigma_{\bar{1},\bar{1}} \,\rangle & & & & \mathbb{Q}(\sqrt{2}) \quad \mathbb{Q}(\sqrt{3}) \quad \mathbb{Q}(\sqrt{6}) \\ \backslash \quad | \quad / & & G(L/Z) \longleftarrow Z & & \backslash \quad | \quad / \\ G(L/K) & & & & \mathbb{Q} \\ \| & & & & \| \\ G & & & & K \end{array}$$

Man beachte, dass die Enthaltenseinsbeziehungen in den beiden Diagrammen entgegengesetzt sind.

2.3 Zerfällungskörper und normale Erweiterungen

Wir wollen im folgenden ein Kriterium dafür erhalten, dass eine Körpererweiterung galoissch ist. Es wird lauten, dass eine Körpererweiterung L/K genau dann galoissch ist, wenn sie endlich, normal und separabel ist. Die Bedeutung des ersten Begriffs ist schon bekannt. In diesem und dem nächsten Abschnitt sollen die beiden anderen eingeführt werden. Eng mit dem Konzept der Normalität ist das des Zerfällungskörpers verbunden:

Definition 2.3.1. Es sei K ein Körper und $f \in K[X]$ mit $\deg(f) \geq 1$.
Eine algebraische Erweiterung L von K heißt Zerfällungskörper von f über K, wenn $L = K(\alpha_1, \ldots, \alpha_n)$ und $f = c \cdot (X - \alpha_1) \cdots (X - \alpha_n)$ mit $c \in K$ gilt.

Bemerkung 2.3.1. Man beachte, dass f nicht irreduzibel zu sein braucht.

Beispiel 2.3.1. Der Körper $\mathbb{Q}(\sqrt{2},\sqrt{3})$ aus Beispiel 2.3.1 ist ein Zerfällungskörper des Polynoms $f(X) = (X^2-2)\cdot(X^2-3)$ über $\mathbb{Q}$ denn es ist $f(X) = (X-\sqrt{2})(X-(-\sqrt{2}))(X-\sqrt{3})(X-(-\sqrt{3}))$ in $L[X]$, und $L = \mathbb{Q}(\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3})$.

Beispiel 2.3.2. Der Körper $\mathbb{C}$ ist Zerfällungskörper von X^2+1 über $\mathbb{R}$, da $X^2+1 = (X-i)(X-(-i))$ und $\mathbb{C} = \mathbb{R}(i,-i)$ ist.

Folgender Satz ist trivial:

Satz 2.3.1. *Es sei K ein Körper und $f \in K[X]$, sowie M ein Zerfällungskörper von f über K und Z ein Zwischenkörper, d.h. $M/Z/K$. Dann ist M auch ein Zerfällungskörper von f über Z.*

Wir werden im folgenden eine Aussage über Existenz und Eindeutigkeit von Zerfällungskörpern beweisen. In Beispiel 2.3.1 wurde der Zerfällungskörper L als Unterkörper von vorgegebenen großen Oberkörpern ($\mathbb{R}$ oder $\mathbb{C}$) erhalten, die mit Hilfsmitteln der Analysis (Cauchyfolgen) aus dem Körper $\mathbb{Q}$ konstruiert werden können. Im folgenden werden diese Zerfällungskörper mit rein algebraischen Hilfsmitteln konstruiert werden. In einem ersten Schritt konstruieren wir zu einem vorgegebenen Körper K und Polynom $f \in K[X]$ eine Körpererweiterung L/K, in der f mindestens eine Nullstelle besitzt.

Satz 2.3.2. *Es sei $g \in K[X]$ normiert und irreduzibel. Dann existiert eine einfache algebraische Erweiterung L/K mit $\alpha \in L$ und $m_K(\alpha, X) = g(X)$.*

Beweis. Der Satz 2.2.2 (ii) legt es nahe, den Restklassenring $\overline{L} = K[X]/(g)$ hierfür zu betrachten. Nach Satz 1.4.4 (iii) ist (g) ein maximales Ideal, womit $\overline{L}$ nach Satz 1.4.10 (ii) ein Körper ist.
Wir setzen $\alpha = X + (g) \in \overline{L}$.
Der Körper $\overline{L}$ enthält den zu K isomorphen Unterkörper $\overline{K} := \{z + (g) \colon z \in K\}$. Es sei $L = (\overline{L} - \overline{K}) \cup K$ und

$$\Phi := \begin{cases} z + (g) & \to \quad z \quad \text{falls} \quad z + (g) \in \overline{K} \\ z & \to \quad z \quad \text{falls} \quad z \in \overline{L} - \overline{K} \end{cases}$$

Wir definieren Addition und Multiplikation auf L durch

$$\Phi(z_1) + \Phi(z_2) := \Phi(z_1 + z_2), \quad \text{und} \quad \Phi(z_1) \cdot \Phi(z_2) := \Phi(z_1 \cdot z_2).$$

Dann ist $g(\alpha) = 0$, und L ist von der gewünschten Art. □

Der folgende Satz macht Aussagen über Existenz und Eindeutigkeit von Zerfällungskörpern.

Satz 2.3.3. *Es sei K ein Körper und $f \in K[X]$. Dann gibt es einen Zerfällungskörper L von f über K. Es sei $f(X) = c \cdot (X - \alpha_1) \cdots (X - \alpha_n)$ mit $c \in K$ und $\alpha_1, \ldots, \alpha_n \in L$. Ist $\overline{L}$ irgend ein Zerfällungskörper von f über K, so gibt es einen K-Isomorphismus $\sigma \colon L \to \overline{L}$, so dass $f(X) = c \cdot (X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_n))$ in $\overline{L}[X]$ ist. Insbesondere sind Zerfällungskörper von f über K stets K-isomorph.*

Beweis. Existenz:
Wir beweisen die Existenz eines Zerfällungskörpers L von f über K durch Induktion nach dem Grad $n = \deg(f)$.
$n = 1$:
Es gilt $f(X) = a_1 X + a_0$ mit $a_1 \neq 0$, also $f(X) = a_1 \cdot (X - (-a_0 a_1^{-1})$, d.h. K ist schon selbst Zerfällungskörper.
$n - 1 \to n$:
Es sei $f \in K[X]$ mit $\deg(f) = n$. Dann gibt es nach Satz 2.3.2 eine Körpererweiterung $K(\alpha_1)$ mit $m_K(\alpha_1, X) = f(X)$. Es ist $f(X) = c \cdot (X - \alpha_1) \cdot h(X)$ mit $c \in K$ für ein $h \in K(\alpha_1)[X]$ normiert und irreduzibel, sowie $\deg(h) = n - 1$. Nach Induktionshypothese gibt es eine algebraische Erweiterung $L = K(\alpha_1, \ldots, \alpha_n)$ von $K(\alpha_1)$, so dass $h(X) = (X - \alpha_2) \cdots (X - \alpha_n)$ in $L[X]$ gilt. Also ist L

Zerfällungskörper von f über K.
Eindeutigkeit: Die Eindeutigkeit bis auf K-Isomorphie ist ein Spezialfall des folgenden allgemeinen Satzes. □

Satz 2.3.4. *Es seien K und $\overline{K}$ Körper, X und Y Unbestimmte über K bzw. $\overline{K}$, und $\sigma\colon K \to \overline{K}$ ein Körperisomorphismus. Für $f(X) = a_nX^n + \cdots + a_0 \in K[X]$ sei $f^{(\sigma)}(Y) = \sigma(a_n)Y^n + \cdots + \sigma(a_0)$ gesetzt. Es sei L ein Zerfällungskörper von f über K mit $f(X) = c \cdot (X - \alpha_1) \cdots (X - \alpha_n)$, $c \in K$, $\alpha_1, \ldots, \alpha_n \in L$. Ferner sei $\overline{L}$ ein Zerfällungskörper von $f^{(\sigma)}$ über $\overline{K}$. Dann gibt es einen Isomorphismus $\tau\colon L \to \overline{L}$, der σ fortsetzt, und zwar mit $f^{(\sigma)} = \sigma(c) \cdot (Y - \tau(\alpha_1)) \cdots (Y - \tau(\alpha_m))$.*

Beweis. Wir beweisen die Behauptung durch Induktion nach $n = \deg(f)$:
$n = 1$:
Es gilt $f(X) = c \cdot (X - \alpha_1)$ mit $c, \alpha \in K$ und $f^{(\sigma)}(Y) = \sigma(c) \cdot (Y - \tau(\alpha_1))$. Die Behauptung gilt dann wegen $L = K$, $\overline{L} = \overline{K}$, wenn $\tau = \sigma$ gesetzt wird.
$n - 1 \to n$:
Die Behauptung sei schon für alle Grade $\leq n - 1$ gezeigt. Es sei $n = \deg(f)$, und es gelte $f(X) = c \cdot g_1(X) \cdots g_l(X)$ mit $c \in K$ und irreduziblen normierten $g_j \in K[X]$ für $1 \leq j \leq l$. Es sei α eine Nullstelle in L von $g_1(X)$. Damit gilt in $K(\alpha)[X]$

$$f(X) = c \cdot (X - \alpha)h(X) \cdot g_2(X) \cdots g_l(X) = (X - \alpha) \cdot k(X)$$

für ein $k \in K(\alpha)[X]$. Es sei β eine Nullstelle von $g_1^{(\sigma)}(Y)$ in $\overline{K}$. Dann gibt es nach Satz 2.2.2 einen Isomorphismus $\psi\colon K(\alpha) \to \overline{K}(\beta)$ mit $\psi(\alpha) = \beta$, der σ fortsetzt. Es gilt

$$f^{(\sigma)}(Y) = \sigma(c) \cdot (Y - \beta)h^{(\psi)}(Y) \cdot g_2^{(\psi)}(Y) \cdots g_l^{(\psi)}(Y) = (Y - \beta) \cdot k^{(\psi)}(Y).$$

Nun ist L Zerfällungskörper von k über $K(\alpha)$ und $\overline{L}$ Zerfällungskörper von $k^{(\psi)}$ über $\overline{K}$. Nach Induktionshypothese (mit $\deg(k) = n-1$) kann ψ zu einem Isomorphismus τ von L nach $\overline{L}$ fortgesetzt werden, so dass die gewünschten Eigenschaften gelten. □

Definition 2.3.2. Es sei f ein nicht konstantes Polynom aus $K[X]$.

i) Man hat alle Nullstellen von f zu K adjungiert, wenn man einen Zerfällungskörper von f über K betrachtet.

ii) Man hat eine Nullstelle von f zu K adjungiert, wenn man eine einfache Erweiterung $K(\alpha)$ von K mit $f(\alpha) = 0$ betrachtet.

iii) Ist α algebraisch über K, so heißt $\alpha_1, \ldots, \alpha_n$ ein volles System von Konjugierten zu α über K, wenn $\alpha_1 = \alpha$ ist und es eine Erweiterung L/K mit $\alpha_1, \ldots, \alpha_n \in L$ und $m_K(\alpha, X) = (X - \alpha_1) \cdots (X - \alpha_n)$ gibt.

Definition 2.3.3. Ein Körper L heißt normal über K (oder eine normale Erweiterung von K), wenn L eine algebraische Erweiterung von K ist, und jedes irreduzible Polynom aus $K[X]$, das in L mindestens eine Nullstelle besitzt, in lauter Linearfaktoren aus $L[X]$ zerfällt.

Beispiel 2.3.3. Die Erweiterung $L = \mathbb{Q}(\sqrt[4]{2})$ ist nicht normal über $\mathbb{Q}$, denn $f(x) = X^4 - 2$ ist in $\mathbb{Q}[X]$ irreduzibel, hat in $\mathbb{Q}(\sqrt[4]{2})$ eine Nullstelle $\alpha = \sqrt[4]{2}$, zerfällt jedoch nicht in Linearfaktoren aus $L[X]$, da die Nullstelle $\sqrt[4]{2} \cdot i \in \mathbb{C}$ nicht in L liegt.

Der folgende Satz sagt aus, dass endliche normale Erweiterungen und Zerfällungskörper ein und dasselbe sind:

Satz 2.3.5. *Ein Körper L ist genau dann eine normale und endliche Erweiterung von K, wenn L ein Zerfällungskörper eines Polynoms aus $K[X]$ über K ist.*

Beweis. $''\Rightarrow''$:
Es sei L eine normale und endliche Erweiterung von K. Dann ist $L = K(\alpha_1, \ldots, \alpha_n)$ für endlich viele $\alpha_1, \ldots, \alpha_n \in L$. Es sei $f(X) = m_K(\alpha_1, X) \cdots m_K(\alpha_n, X)$. Da jeder Faktor $m_K(\alpha_j, X)$ in Linearfaktoren aus $L[X]$ zerfällt, ist L ein Zerfällungskörper von f über K.
$''\Leftarrow''$:
Es sei L Zerfällungskörper eines Polynoms $f \in K[X]$ über K, etwa mit Zerfall

$$f(X) = c \cdot (X - \alpha_1) \cdots (X - \alpha_n)$$

in Linearfaktoren in $L[X]$, und $L = K(\alpha_1, \ldots, \alpha_n)$. Es sei $g \in L[X]$ normiert und irreduzibel mit $g(\beta) = 0$ für ein $\beta \in L$. Es ist zu zeigen, dass g in $L[X]$ in Linearfaktoren zerfällt. Dazu sei Z ein Zerfällungskörper von g über L. Ist $\overline{\beta}$ eine beliebige Nullstelle von g in Z, so bleibt $\overline{\beta} \in L$ zu zeigen. Wegen $g(X) = m_K(\beta, X) = m_K(\overline{\beta}, X)$ gibt es nach Satz 2.2.1 einen K-Isomorphismus $\sigma\colon K(\beta) \to K(\overline{\beta})$ mit $\sigma(\beta) = \overline{\beta}$. Da $L = L(\beta)$ ein Zerfällungskörper von f auch über $K(\beta)$ und $L(\overline{\beta})$ ein Zerfällungskörper von f über $K(\overline{\beta})$ ist, existiert nach Satz 2.3.4 ein Isomorphismus $\tau\colon L \to L(\overline{\beta})$, der σ fortsetzt. Wegen $0 = \tau(f(\alpha_j)) = f(\tau(\alpha_j))$ bilden die Elemente $\tau(\alpha_1), \ldots, \tau(\alpha_n)$ eine Permutation von $\alpha_1, \ldots, \alpha_n$.Für $\beta \in K(\alpha_1, \ldots, \alpha_n)$ gilt dann

$$\beta = p(\alpha_1, \ldots, \alpha_n)$$

mit $p \in K[X_1, \ldots, X_n]$. Daraus folgt

$$\overline{\beta} = p(\tau(\alpha_1), \ldots, \tau(\alpha_n)) \in K(\alpha_1, \ldots, \alpha_n) = L.$$

□

Satz 2.3.6. *Ist ein Körper L normal über K, so ist L normal über Z für jeden Zwischenkörper $L/Z/K$.*

Beweis. Es sei g ein irreduzibles und normiertes Polynom aus $Z[X]$ und $g(\alpha) = 0$ für ein $\alpha \in L$. Es gilt $g(X) = m_Z(\alpha, X)$, also $g(X) | m_K(\alpha, X)$ (Teilbarkeitsrelation in $Z[X]$). Da $m_K(\alpha, X)$ in $L[X]$ in Linearfakoren zerfällt, gilt das auch für den Teiler $g(X)$. □

2.4 Separabilität

Definition 2.4.1. Es sei L/K eine Körpererweiterung. Dann heißt $\alpha \in L$ eine r-fache Nullstelle eines Polynoms $f \in K[X]$ mit $r \in \mathbb{N}_0$, falls $(X - \alpha)^r | f(X)$ und $(X - \alpha)^{r+1} \nmid f(X)$ in $L[X]$ gilt.

Definition 2.4.2. Es sei f ein nicht konstantes Polynom aus $K[X]$ und L ein Zerfällungskörper von f über K.

i) Das Polynom f heißt separabel, wenn f nur einfache Nullstellen in L besitzt. Andernfalls heißt f inseparabel.

ii) Die Anzahl der verschiedenen Nullstellen von f in L wird der reduzierte Grad von f genannt.

Ein wichtiges Kriterium für die Separabilität eines Polynoms f kann mittels dessen Ableitung f' gewonnen werden.

Definition 2.4.3. Es sei

$$f(X) = \sum_{j=0}^{n} a_j X^j \in K[X]$$

beliebig. Unter der Ableitung f' von f versteht man das Polynom

$$f'(X) = \sum_{j=1}^{n} j \cdot a_j X^{j-1} \in K[X],$$

wobei j innerhalb der Summe als Abkürzung für $\Phi(j)$ mit dem Ringhomomorphismus $\Phi\colon \mathbb{Z} \to K$ aus Satz 2.2.1 zu verstehen ist. Man beweist leicht die Gültigkeit der Produktregel $(fg)' = f'g + fg'$.

Satz 2.4.1. *Es sei f ein nicht konstantes Polynom aus $K[X]$. Dann ist f genau dann separabel, wenn f und f' in $K[X]$ teilerfremd sind.*

Beweis. $''\Leftarrow''$:
Es sei α eine mehrfache Nullstelle von f in L. Dann gilt: $f(X) = (X-\alpha)^2 \cdot g(X)$ für ein $g \in L[X]$. Nach der Produktregel ist

$$f'(X) = 2(X-\alpha) \cdot g(X) + (X-\alpha)^2 \cdot g'(X),$$

also gilt $(X-\alpha) | f(X)$ und $(X-\alpha) | f'(X)$ in $L[X]$. Wären f und f' teilerfremd in $K[X]$, so folgte $(X-\alpha)|1$ in $L[X]$, ein Widerspruch.
$''\Rightarrow''$:
Es sei $f(X) = c \cdot (X-\alpha_1) \cdots (X-\alpha_n)$ mit $c \in K$, $\alpha_j \in L$ und alle a_j paarweise verschieden. Wir nehmen an, f und f' seien in $K[X]$ nicht teilerfremd. Da $L[X]$ faktoriell ist, folgt $g|f$ und $g|f'$ für ein irreduzibles $g \in L[X]$. Weiter folgt $g|(X-\alpha_j)$ für genau ein j, ein Widerspruch, da $(X-\alpha_j) \nmid f'$. □

Satz 2.4.2. *Es sei f ein irreduzibles Polynom in $K[X]$ mit $\mathrm{char}(K) = 0$. Dann ist f separabel.*

Beweis. Nach Satz 2.4.1 ist f genau dann inseparabel, wenn f und f' einen nicht konstanten größten gemeinsamen Teiler in $K[X]$ besitzen. Wegen der Irreduzibilität von f folgt: $f|f'$ oder $f'(X) \neq 0$. Ist $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ mit $a_n \neq 0$ und $n \geq 1$, so ist $f'(X) = a_1 + 2a_2 X + \cdots + n \cdot a_n X^{n-1} \neq 0$, da wegen $\mathrm{char}(K) = 0$ auch $n \neq 0$ für $n \geq 1$ gilt. □

Bemerkung 2.4.1. Für Körper K mit Primzahlcharakteristik p können irreduzible Polynome inseparabel sein.

Definition 2.4.4. Es sei K ein Körper.

i) Ein über K algebraisches Element α heißt separabel bzw. inseparabel über K, falls $m_K(\alpha, X)$ separabel bzw. inseparabel ist. Der reduzierte Grad von $m_K(\alpha, X)$ wird der reduzierte Grad von α über K genannt.

ii) Eine algebraische Erweiterung L/K heißt separabel (oder separable Erweiterung von K), falls alle $\alpha \in L$ über K separabel sind. Andernfalls heißt L inseparabel über K.

Satz 2.4.3. *Es ist stets K separabel über K. Ist L separabel über K, so ist L separabel über jedem Zwischenkörper $L/Z/K$.*

Beweis. Ist $\alpha \in K$, so ist $m_K(\alpha, X) = X - \alpha$ offensichtlich separabel. Es gilt $m_Z(\alpha, X) | m_K(\alpha, X)$ in $Z[X]$ für $\alpha \in L$. Aus der Separabilität von $m_K(\alpha, X)$ folgt daher die Separabilität von $m_Z(\alpha, X)$. □

Der folgende Satz ist für die Beziehung der Begriffe Normalität und Separabilität zur Galoistheorie von entscheidender Bedeutung:

Satz 2.4.4. *Es sei L/K endlich, $L = K(\alpha_1, \ldots, \alpha_r)$ und m_j der reduzierte Grad von α_j über $K(\alpha_1, \ldots, \alpha_{j-1})$ für $j = 1, \ldots, r$. Dann gilt $|G(L/K)| \leq m_1 \cdots m_r$. In dieser Ungleichung steht das Gleichheitszeichen, wenn L über K normal ist. Insbesondere ist stets $|G(L/K)| \leq [L\colon K]$.*

Beweis. Schritt 1:
Wir beweisen durch Induktion nach j folgende Behauptung, aus welcher für $j = r$ die erste Behauptung des Satzes folgt: Die Anzahl n_j der K-Isomorphismen von $K(\alpha_1, \ldots, \alpha_j)$ erfüllt $n_j \leq m_1 \cdots m_j$. Der Induktionsanfang $j = 0$ ist klar. Es sei nun $j > 0$ und die Behauptung für $j - 1$ schon gezeigt, d.h. es gibt n_{j-1} verschiedene K-Isomorphismen $\sigma_1, \ldots, \sigma_{n_{j-1}}$ von $L' = K(\alpha_1, \ldots, \alpha_{j-1})$ in L, wobei $n_{j-1} \leq m_1 \cdots m_{j-1}$ ist. Die K-Isomorphismen von $K(\alpha_1, \ldots, \alpha_j)$ werden nach Satz 2.2.2 aus den Fortsetzungen der σ_i erhalten. Es sei σ eines der σ_i, sowie $g(X) = m_{L'}(\alpha_j, X) = \sum a_k X^k$. und $g^{(\sigma)}(Y) = \sum \sigma(a_k) Y^k$. Nach Satz 2.2.2 sind die Fortsetzungen von σ durch die verschiedenen Nullstellen $\beta_1, \ldots, \beta_m$ von $g^{(\sigma)}(Y)$ in L über $\sigma(\alpha_j) = \beta_l$ charakterisiert. Es gibt also genau m' Fortsetzungen von σ, wobei $m' \leq \overline{m}_j$ ist für den reduzierte Grad $\overline{m}_j$ von $g^{(\sigma)}$. Da nach Satz 2.3.4 σ zu einem Isomorphismus eines Zerfällungskörpers von g über L' und einem Zerfällungskörper von $g^{(\sigma)}$ über $\sigma(L')$ fortgesetzt werden kann, gilt $\overline{m}_j = m_j$. Also folgt $n_j \leq n_{j-1} m_j \leq m_1 \cdots m_j$.

Schritt 2:
Es sei nun zusätzlich vorausgesetzt, dass L normal über K ist. Der Beweis für das Gleichheitszeichen wird wieder durch Induktion über j geführt. Die Induktionshypothese ist somit, dass es genau $m_1 \cdots m_{j-1}$ verschiedene K-Isomorphismen σ von $L' = K(\alpha_1, \ldots, \alpha_{j-1})$ gibt. Es ist zu zeigen, dass es zu jedem σ genau m_j Fortsetzungen zu einem Isomorphismus auf $K(\alpha_1, \ldots, \alpha_j)$ gibt. Dazu genügt es zu zeigen, dass $g^{(\sigma)}(Y)$ in $L[Y]$ vollständig in Linearfaktoren zerfällt. Wegen $g^{(\sigma)}(Y) = m_{L'}(\alpha_j, Y)$ gilt

$$h(X) = m_K(\alpha_j, X) = b_0 + b_1 X + \cdots + b_{m-1} X^{m-1} + b_m X^m = g(X) \cdot q(X),$$

mit $b_i \in K$ und $g, q \in K(\alpha_1, \ldots, \alpha_{j-1})[X]$. Dann ist

$$h(X) = \sigma(b_0) + \cdots + \sigma(b_{m-1}) X^{m-1} + X^m = g^{(\sigma)}(X) \cdot q^{(\sigma)}(X).$$

Da aber L normal über K ist, zerfällt auch h wegen $h(\alpha_j) = 0$ vollständig in Linearfaktoren in $L[X]$ und somit auch $g^{(\sigma)}$. Schließlich ist

$$\begin{aligned} [L\colon K] &= [K(\alpha_1)\colon K] \cdot [K(\alpha_1, \alpha_2)\colon K(\alpha_1)] \cdots [K(\alpha_1, \ldots, \alpha_r)\colon K(\alpha_1, \ldots, \alpha_{r-1})] \\ &\geq m_1 \cdots m_r \geq |G(L/K)|, \end{aligned}$$

woraus die letzte Behauptung des Satzes folgt. □

Satz 2.4.5. *Es sei L/K endlich. Dann gilt genau dann $|G(L/K)| = [L\colon K]$, wenn L/K normal und separabel ist.*

Beweis. "⇒"
Es sei L/K normal und separabel. Dann gilt im Beweis des vorigen Satzes

$$[L\colon K] = [K(\alpha_1)\colon K] \cdots [K(\alpha_1, \ldots, \alpha_r)\colon K(\alpha_1, \ldots, \alpha_{r-1})] = m_1 \cdots m_r = |G(L/K)|, \qquad (*)$$

wobei die vorletzte Gleichung wegen der Separablilität und gilt und die letzte wegen der Normalität von L/K.
"⇐"
Ist L/K nicht normal oder nicht separabel, so gilt in $(*)$ an mindestens einer Stelle eine strikte Ungleichung, weswegen $|G(L/K)| \neq [L\colon K]$ gilt. □

2.5 Endliche Körper

Satz 2.5.1. *Die Ordnung eines endlichen Körpers K ist stets eine Primzahlpotenz, also $|K| = p^m$ mit p prim und $m \in \mathbb{N}$.*

Beweis. Es sei $\mathbb{P}$ der Primkörper von K. Wäre nun $\operatorname{char} K = 0$, so wäre $\mathbb{P} \cong \mathbb{Q}$, damit also $|K| = \infty$. Nach Satz 2.1.1 ist $\operatorname{char} K = p$ für eine Primzahl p und $\mathbb{P} \cong \mathbb{Z}/p\mathbb{Z}$. Wegen $|K| < \infty$ ist außerdem $[K\colon \mathbb{P}] = m \in \mathbb{N}$. Also ist K ein Vektorraum der Dimension m über $\mathbb{P}$ mit einer Basis $\mathcal{B} = \{\gamma_1, \ldots, \gamma_m\}$.
Es ist $K = \{a_1\gamma_1 + \ldots + a_m\gamma_m \colon a_i \in \mathbb{P}\}$ die Menge aller Linearkombinationen der $\gamma_1, \ldots, \gamma_m$. Jeder Koeffizient a_i kann p Werte annehmen, woraus $|K| = p^m$ folgt. □

Es stellt sich nun die Frage, ob umgekehrt zu jeder Primzahlpotenz $q = p^m$ auch ein Körper K mit $|K| = q$ existiert. Der folgende Satz gibt einen Hinweis, wie ein solcher Körper zu konstruieren ist.

Satz 2.5.2. *Es sei $|K| = q = p^m$ mit einer Primzahl p, $m \in \mathbb{N}$ und dem Primkörper $\mathbb{P}$. Dann ist K ein Zerfällungskörper des Polynoms $f(X) = X^q - X$ über $\mathbb{P}$. Weiter ist K die Menge aller Nullstellen von f.*

Beweis. Da $(K\backslash\{0\}, \cdot)$ eine Gruppe mit $q-1$ Elementen ist, folgt $\alpha^{q-1} = 1$ für alle $\alpha \in K\backslash\{0\}$ und damit $\alpha^q - \alpha = 0$ für alle $\alpha \in K$. Damit ist K die Menge aller Nullstellen von f. Ist $K = \{\alpha_1, \ldots, \alpha_q\}$, so ist

$$f(X) = \prod_{i=1}^{q} (X - \alpha_i)$$

und $K = \mathbb{P}(\alpha_1, \ldots, \alpha_q)$. Nach Definition 2.3.1 ist K ein Zerfällungskörper von $f(X)$ über $\mathbb{P}$. □

Satz 2.5.3. *Ein Körper K mit $|K| = q$ existiert genau dann, wenn $q = p^m$ für eine Primzahl p und $m \in \mathbb{N}$ gelten. Der Körper K ist dann bis auf Isomorphie eindeutig bestimmt und isomorph zum Zerfällungskörper des Polynoms $f(X) = X^q - X$ über $\mathbb{Z}/p\mathbb{Z}$.*

Beweis. Die Behauptung folgt aus den Sätzen 2.5.1 und 2.5.2 sowie aus Satz 2.3.3 (Isomorphie von Zerfällungskörpern). □

Definition 2.5.1. Es sei $q = p^m$ eine Primzahlpotenz. Der nach Satz 2.5.3 bis auf Isomorphie eindeutig bestimmte Körper mit q Elementen wird mit $GF(q)$ oder $\mathbb{F}_q$ bezeichnet.

2.6 Symmetrische Funktionen

Es sei K ein Körper, $f \in K[X]$ separabel und L ein Zerfällungskörper von f über K. Es ist dann $f(X) = c \cdot (X - \alpha_1) \cdots (X - \alpha_n)$ mit paarweise verschiedenen $\alpha_i \in K$. Für jedes $\sigma \in G(L/K)$ ist $(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$ eine Permutation von $(\alpha_1, \ldots, \alpha_n)$.
Man kann nun auch umgekehrt fragen, welche Permutationen $\sigma \in S_n$ sich zu einem K- Automorphismus fortsetzen lassen.

Beispiel 2.6.1. Es sei $K = \mathbb{Q}$ und $f(X) = X^4 + X^3 + X^2 + X + 1$, das Kreisteilungspolynom der Ordnung 5. Es ist

$$f(X + 1) = X^4 + 5X^3 + 10X^2 + 10X + 5$$

in $\mathbb{Q}[X]$ nach dem Eisensteinkriterium mit $p = 5$ irreduzibel. Damit ist auch f in $\mathbb{Q}[X]$ irreduzibel.

Wegen $(X-1)\cdot f(X) = X^5 - 1$ ist

$$f(X) = \prod_{i=1}^{4}(X - \zeta^j)$$

mit $\zeta = \exp(\frac{2\pi i}{5})$. Es sei nun $L = K(\zeta)$. Nach Satz 2.2.1 ist $G(L/K) = \{\sigma_j \colon 1 \leq j \leq 4\}$, wobei σ_j durch $\sigma_j(\zeta) = \zeta^j$ eindeutig bestimmt ist. Von den 24 Permutationen der Nullstellen ζ^j können also nur vier zu K- Automorphismen von L fortgesetzt werden.

In diesem Abschnitt untersuchen wir einen Fall, in dem sich jede Permutation fortsetzen lässt.

Definition 2.6.1. Es seien $n \in \mathbb{N}$, R ein Ring und $u_1, \ldots, u_n$ unabhängige Unbestimmte über R. Für $f \in R[u_1, \ldots, u_n]$ und $\sigma \in S_n$ sei $f_\sigma(u_1, \ldots, u_n) = f(u_{\sigma^{-1}(1)}, \ldots, u_{\sigma^{-1}(n)})$.
Dann heißt $f \in R[u_1, \ldots, u_n]$ ein symmetrisches Polynom, wenn $f_\sigma = f$ für alle $\sigma \in S_n$ gilt. Sind $\alpha_1, \ldots, \alpha_n \in R$, so heißt $f(\alpha_1, \ldots, \alpha_n)$ ein symmetrisches Polynom von $\alpha_1, \ldots, \alpha_n$.

Definition 2.6.2. Es sei R ein Ring und $u_1, \ldots, u_n$ unabhängige Unbestimmte über R. Unter den elementarsymmetrischen Funktionen versteht man

$$\begin{aligned}
s_1 &= u_1 + u_2 + \ldots + u_n \\
s_2 &= u_1u_2 + u_1u_3 + \ldots + u_{n-1}u_n = \sum_{i<j} u_iu_j \\
s_3 &= \sum_{i<j<k} u_iu_ju_k \\
&\vdots \\
s_n &= u_1u_2 \cdots u_n.
\end{aligned}$$

Definition 2.6.3. Es sei $f(u_1, \ldots, u_n) = \sum a_{r_1,\ldots,r_n} u_1^{r_1} \cdots u_n^{r_n}$.
Unter dem Grad von f versteht man $\deg f = \max\{r_1 + \ldots + r_n \colon r_i \in \mathbb{N}\}$.

Bemerkung 2.6.1. Es ist $p(x) = (x-u_1)\cdot(x-u_2)\cdots(x-u_n) = x^n - s_1x^{n-1} + s_2x^{n-2} + \ldots + (-1)^n s_n$. Allgemein sind die Koeffizienten eines Polynoms bis auf das Vorzeichen die elementarsymmetrischen Funktionen seiner Nullstellen.

Satz 2.6.1. *(Hauptsatz über symmetrische Funktionen)*
Jedes symmetrische Polynom $g \in R[u_1, \ldots, u_n]$ lässt sich auf eindeutige Weise als Polynom in den elementarsymmetrischen Funktionen $s_1, \ldots, s_n$ schreiben.

Beweis. Existenz:
Der Beweis wird durch Induktion nach n geführt.
Induktionsanfang: $n = 1$:
Dies ist wegen $u_1 = s_1$ klar.
Induktionsschritt: $n \to n+1$:
Für $f \in R[u_1, \ldots, u_n]$ sei $f^0(u_1, \ldots, u_{n-1}) = f(u_1, \ldots, u_{n-1}, 0)$. Somit ist f^0 ein symmetrisches Polynom und lässt sich daher nach Induktionshypothese als Polynom in den elementarsymmetrischen Polynomen

$$s_1^0 = u_1 + \ldots + u_{n-1}, \ldots, s_{n-1}^0 = u_1 \cdots u_{n-1}$$

darstellen. Wir können also $f^0 = g(s_1^0, \ldots, s_{n-1}^0)$ schreiben. Es ist folglich $s_i^0 = s_i(u_1, \ldots, u_{n-1}, 0)$ für $i = 1, \ldots, n-1$. Wir setzen

$$p(u_1, \ldots, u_n) = f(u_1, \ldots, u_n) \cdot g(s_1, \ldots, s_{n-1}).$$

Als Differenz symmetrischer Funktionen ist auch das Polynom $p(x)$ symmetrisch. Jedes Monom, das in p vorkommt, ist durch u_n teilbar. Wegen der Symmetrie ist p durch jedes u_i und damit durch $s_n = u_1 \cdots u_n$ teilbar. Also gilt

$$f(u_1, \ldots, u_n) = g(s_1, \ldots, s_{n-1}) + s_n \cdot h(u_1, \ldots, u_n).$$

Durch eine weitere Induktion nach $\deg h$ können wir annehmen, dass h bereits als Polynom in den elementarsymmetrischen Funktionen dargestellt sei. Damit ergibt sich die Existenz auch für f.

Eindeutigkeit:
Die Eindeutigkeit ist gezeigt, wenn wir zeigen können, dass aus $\varphi(s_1, \ldots, s_n) = 0$ für $\varphi \in R[s_1, \ldots, s_n]$ die Aussage $\varphi = 0$ folgt. Wir führen den Beweis durch Induktion nach n.
Es sei $\varphi(s_1, \ldots, s_n) = 0$. Einsetzen von $u_n = 0$ ergibt $\varphi(s_1^0, \ldots, s_{n-1}^0, 0) = 0$. Nach Induktionshypothese folgt daraus $\varphi(s_1, \ldots, s_{n-1}, 0) = 0$, woraus sich dann $\varphi(s) = s_n\psi(s)$ ergibt. Also ist $0 = \varphi(s) = s_n\psi(s) = u_1 \cdots u_n\psi(s)$ und damit $\psi(s) = 0$. Der Beweis ergibt sich dann durch Induktion nach $\deg \psi$. □

Der Beweis des letzten Satzes ist konstruktiv, d.h. er liefert einen Algorithmus, der eine Darstellung liefert.

Beispiel 2.6.2. Man schreibe $f(u_1, \ldots, u_4) = u_1^2 + u_2^2 + u_3^2$ als Polynom in den elementarsymmetrischen Funktionen von $u_2, \ldots, u_4$.
Offenbar ist $u_4 = 0$. Wir bestimmen schrittweise $f(u_1, \ldots, u_n, 0, \ldots, 0)$ für $1 \leq n \leq 3$.
n=1:
Es gilt $f(u_1, 0, 0, 0) = u_1^3 = s_1(u_1, 0, 0, 0)^3$.
n=2:
Wir haben $f(u_1, u_2, 0, 0) = u_1^3 + u_2^3$ mit $s - 1(u_1, u_2, 0, 0)^3$. es gilt

$$s_1(u_1, u_2, 0, 0)^3 = (u_1 + u_2)^3 = u_1^3 + u_2^3 + 3u_1^2u_2 + 3u_1u_2^2,$$

also $f(u_1, u_2, 0, 0) = s_1(u_1, u_2, 0, 0)^3 - 3(u_1^2u_2 + u_1u_2^2)$.
Unterproblem:
Das Polynom $g(u_1, u_2) = u_1^2u_2 + u_1u_2^2$ ist nun als Polynom von $s_1(u_1, u_2)$ und $s_2(u_1, u_2)$ zu schreiben.
Es gilt $g(u_1, u_2) = u_1u_2(u_1 + u_2) = s_2(u_1, u_2, 0, 0)s_1(u_1, u_2, 0, 0)$,woraus

$$f(u_1, u_2, 0, 0) = s_1(u_1, u_2, 0, 0)^3 - 3s_1(u_1, u_2, 0, 0)s_2(u_1, u_2, 0, 0)$$

folgt.
n=3:
Es ist $f(u_1, u_2, u_3, 0) = u_1^3 + u_2^3 + u_3^3$. Mit

$$\begin{aligned} & s_1(u_1, u_2, u_3, 0)^3 - 3s_1(u_1, u_2, u_3, 0)s_2(u_1, u_2, u_3, 0) \\ = \; & u_1^3 + u_2^3 + u_3^3 + 3u_1^2u_2 + 3u_1u_2^2 + 3u_1u_3^2 + 3u_1^2u_3 + 3u_2^2u_3 + 3u_2u_3^3 + 6u_1u_2u_3 \\ & -3(u_1 + u_2 + u_3)(u_1u_2 + u_1u_3 + u_2u_3) \\ = \; & u_1^3 + u_2^3 + u_3^3 + 6u_1u_2u_3 - 9u_1u_2u_3 = u_1^3 + u_2^3 + u_3^3 - 3u_1u_2u_3. \end{aligned}$$

Dies ergibt schließlich

$$f(u_1, u_2, u_3, 0) = u_1^3 + u_2^3 + u_3^3 = s_1(u_1, u_2, u_3, 0)^3 - 3s_1(u_1, u_2, u_3, 0)s_2(u_1, u_2, u_3, 0) - 3s_3(u_1, u_2, u_3, 0).$$

Eine wichtige symmetrische Funktion der Nullstellen eines Polynoms ist die Diskriminante. Sie erlaubt zu überprüfen, ob ein Polynom separabel ist, also keine mehrfachen Nullstellen besitzt.

Definition 2.6.4. Es sei R ein Ring und $f \in R[X]$.
In einem Zerfällungskörper sei $f(X) = c \cdot (X - \alpha_1) \cdots (X - \alpha_n)$. Unter der Diskriminante von f versteht man

$$D(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Nach Satz 2.6.1 lässt sich $D(f)$ als Polynom in den elementarsymmetrischen Funktionen von $\alpha_1, \ldots, \alpha_n$ und damit als Funktion der Koeffizienten von f beschreiben. Zur Berechnung von $D(f)$ genügt somit die Kenntnis der Koeffizienten.

Satz 2.6.2. *i) Es sei $f(X) = X^2 + pX + q$ quadratisch. Dann gilt $D(f) = p^2 - 4q$.*

ii) Das Polynom f ist genau dann separabel, wenn $p^2 - 4q \neq 0$ ist.

iii) Es sei $f(X) = X^3 + pX + q$ kubisch. Dann gilt $D(f) = -4p^3 - 27q^2$.

Beweis. i) Es sei $f(X) = X^2 + pX + q$. Es ist $(\alpha_1 - \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2$. Aus $s_1(\alpha_1, \alpha_2) = \alpha_1 + \alpha_2 =: p$ und $s_2(\alpha_1, \alpha_2) =: q$ folgt die Behauptung (Satz von Vieta).

ii) Eine Nullstelle tritt genau dann mehrfach auf, wenn $D(f) = 0$ ist.

iii) Es sei $f(X) = (X - \alpha_1) \cdot (X - \alpha_2) \cdot (X - \alpha_3) = X^3 + pX + q$. Nach dem im Beweis von Satz 2.6.1 angegebenen Verfahren erhält man

$$(\alpha_1 - \alpha_2)^2 \cdot (\alpha_1 - \alpha_3)^2 \cdot (\alpha_2 - \alpha_3)^2 = s_1^2 s_2^2 - 4s_2^2 - 4s_1^3 s_3 - 27s_3^2 + 18 s_1 s_2 s_3.$$

Aus $s_1 = \alpha_1 + \alpha_2 + \alpha - 3 = 0$, $s_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p$ und $s_3 = \alpha_1\alpha_2\alpha_3 = q$ folgt die Behauptung.

□

Satz 2.6.3. *Es sei K ein Körper, $u_1, \ldots, u_n$ unabhängige Unbestimmte über K und $s_1, \ldots, s_n$ die elementarsymmetrischen Funktionen von $u_1, \ldots, u_n$. Weiter seien $K(u_1, \ldots, u_n)$ bzw. $K(s_1, \ldots, s_n)$ die Quotientenkörper von $K[u_1, \ldots, u_n]$ bzw. $K[s_1, \ldots, s_n]$. Dann sind auch $s_1, \ldots, s_n$ unabhängige Unbestimmte über K, der Körper $K(u_1, \ldots, u_n)$ ist eine Galoiserweiterung von $K(s_1, \ldots, s_n)$, und es gilt $[K(u_1, \ldots, u_n) \colon K(s_1, \ldots, s_n)] = n!$*

Beweis. Es sei $\sigma \in S_n$ und

$$r(u_1, \ldots, u_n) = \frac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)}.$$

Die Abbildung $\varphi \colon K(u_1, \ldots, u_n) \to K(u_1, \ldots, u_n)$,

$$\frac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)} = \frac{f_\sigma(u_1, \ldots, u_n)}{g_\sigma(u_1, \ldots, u_n)}$$

ist offenbar relationstreu und bijektiv mit Umkehrabbildung $\varphi(\sigma^{-1})$, also ein Automorphismus von $K(u_1, \ldots, u_n)$. Wegen

$$f(X) = X^n + s_1 X^{n-1} + \ldots + s_n = (X - u_1) \cdots (X - u_n)$$

ist $K(u_1, \ldots, u_n)$ ein Zerfällungskörper des Polynoms f über dem Körper K. Andererseits permutiert jeder $K(u_1, \ldots, u_n)$- Automorphismus von $K(s_1, \ldots, s_n)$ die Nullstellen $u_1, \ldots, u_n$ von f.
Damit ist $G(K(u_1, \ldots, u_n)/K(s_1, \ldots, s_n)) = \{\sigma \colon \sigma \in S_n\} \cong S_n$. Als Zerfällungskörper ist diese Körpererweiterung normal, ebenfalls endlich und separabel. Die Behauptung folgt mit $|S_n| = n!$. □

2.7 Galoiserweiterungen, Hauptsatz der Galoistheorie

Definition 2.7.1. Eine endliche Erweiterung L/K heißt Galoiserweiterung oder auch galoissch, wenn die Ordnung der Galoisgruppe mit dem Grad der Körpererweiterung übereinstimmt, das bedeutet $|G(L/K)| = [L\colon K]$.

Satz 2.7.1. *Eine Körpererweiterung L/K ist genau dann galoissch, wenn sie endlich, normal und separabel ist.*

Beweis. Es sei L/K endlich. Nach Satz 2.5.1 gilt genau dann $|G(L/K)| = [L\colon K]$, wenn L/K normal und separabel ist. □

Satz 2.7.2. *Ist L/K eine Galoiserweiterung, so ist auch L/Z eine Galoiserweiterung für jeden Zwischenkörper Z.*

Beweis. Nach den Sätzen 2.3.6 und 2.4.3 ist L/Z normal. Für jedes $\alpha \in L$ ist $m_{L^G}(\alpha, X)$ separabel. Damit ist L/L^G auch separabel. Nach Satz 2.7.1 ist L/L^G eine Galoiserweiterung. Die Behauptung folgt mit Definition 2.7.1. □

Satz 2.7.3. *Es sei L ein Körper, G eine endliche Gruppe von Automorphismen von L mit $|G| = n$. Dann ist L eine endliche Erweiterung des Fixkörpers L^G, und es ist $G(L/L^G) = G$. Weiter ist $|L\colon L^G] = n$.*

Beweis. Es sei $\alpha \in L$, und $r \in \mathbb{N}$ sei das maximale r, so dass eine Teilmenge $\{\sigma_1, \ldots, \sigma_r\} \subset G$ existiert, für die $\sigma_1\alpha, \ldots, \sigma_r\alpha$ verschieden sind. Wir behaupten, dass für $\tau \in G$ die Folge $(\tau\sigma_1\alpha, \ldots, \tau\sigma_r\alpha)$ eine Permutation der Folge $(\sigma_1\alpha, \ldots, \sigma_r\alpha)$ ist. Wäre nämlich $\tau\sigma_i\alpha \notin \{\sigma_1\alpha, \ldots, \sigma_r\alpha\}$, so wäre r nicht maximal, ein Widerspruch, da τ injektiv ist. Damit ist α eine Nullstelle des Polynoms

$$f(X) := \prod_{i=1}^{r}(X - \sigma_i\alpha) =: \sum_{j=0}^{r} a_j X^j$$

mit $a_j \in L$ und $a_r = 1$. Weil $(\tau\sigma_1\alpha, \ldots, \tau\sigma_r\alpha)$ eine Permutation der Folge $(\sigma_1\alpha, \ldots, \sigma_r\alpha)$ ist, gilt auch

$$f(X) = \prod_{i=1}^{r}(X - \tau\sigma_i\alpha),$$

und es gilt $a_j \in L^G$, da sie symmetrische Funktionen von $\sigma_i\alpha$ sind, also ist $f \in L^G[X]$. □

Satz 2.7.4. *(Hauptsatz der Galoistheorie)*
Es sei L eine Galoiserweiterung eines Körper K, und es sei $G = G(L/K)$ die zugehörige Galoisgruppe. Die Zuordnung $H \to L^H$ ist eine bijektive Abbildung von der Menge der Untergruppen von G auf die Menge der Zwischenkörper Z von L/K. Ihre Umkehrabbildung ist die Zuordnung $Z \to G(L/Z)$. Diese Zuordnung hat die Eigenschaft, dass für $H = G(L/Z)$ dann $|L\colon Z] = |H|$ und daher $[Z\colon K] = (G\colon H)$ gilt.

Beweis. Es sei Z ein Zwischenkörper und $H = G(L/Z)$. Nach Definition 2.2.4 (i) gilt $\sigma(z) = z$ für $\sigma \in H$ und für alle $z \in Z$, womit $Z \subset L^H$ gilt. Nach Satz 2.7.1 ist L eine Galoiserweiterung von Z, also $[L\colon Z] = |H|$ nach Definition 2.6.1. Andererseits ist $|H| = [L\colon L^H]$ nach Satz 2.7.3. Daraus folgt schließlich $Z = L^H$. □

Satz 2.7.5. *Es sei L/K eine Galoiserweiterung und Z ein Zwischenkörper. Es sei $H = G(L/Z)$ die entsprechende Untergruppe von $G = G(L/K)$.*

i) Es sei $\sigma \in G$. Dann ist $G(L/\sigma(Z)) = \sigma H \sigma^{-1}$.

ii) Es ist Z/K genau dann eine Galoiserweiterung, wenn H ein Normalteiler von G ist. In diesem Fall ist $G(Z/K)$ isomorph zur Faktorgruppe G/H.

Beweis. i) Es sei $\tau \in H = G(L/Z)$ und $\alpha' \in \sigma(Z)$. Dann ist $\sigma' = \sigma(\alpha)$ für ein $\alpha \in Z$. Weiter ist $\sigma\tau\sigma^{-1}(\alpha') = \sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \sigma'$, wobei die vorletzte Gleichung wegen $\tau \in H$ gilt. Somit ist $\sigma\tau\sigma^{-1} \in H' = G(L/\sigma(Z))$. Damit ist $\sigma H \sigma^{-1} \subset H'$.
Analog gilt $\sigma^{-1} H' \sigma \subset H$ oder $H' \subset \sigma H \sigma^{-1}$, woraus insgesamt $H' = \sigma H \sigma^{-1}$ folgt.

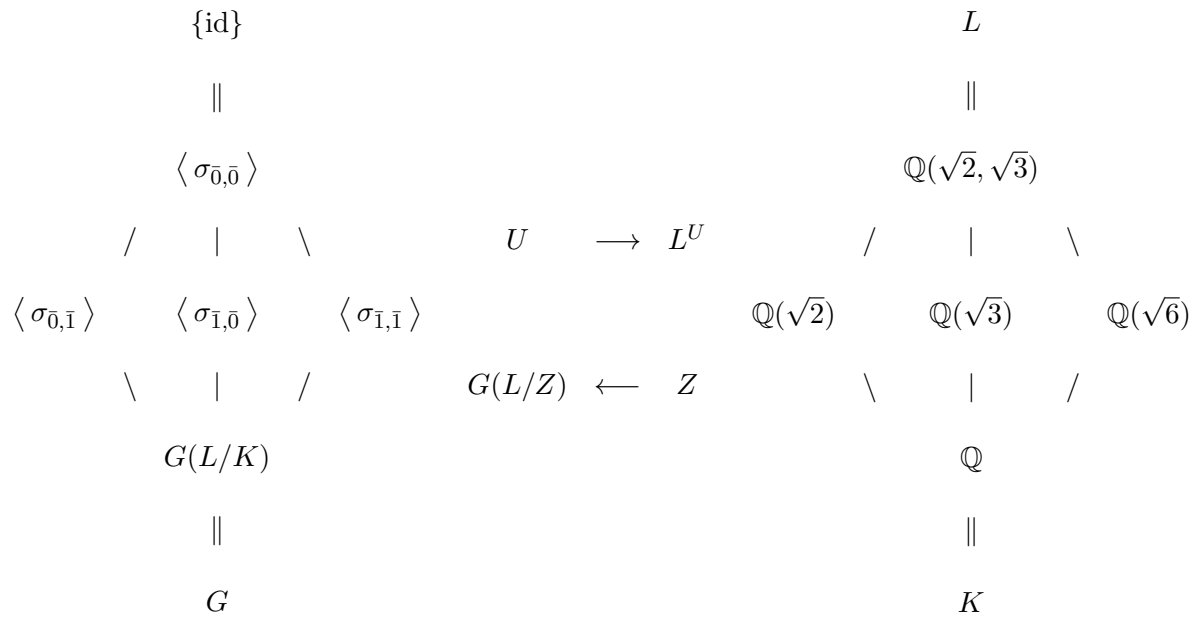
ii) "$\Leftarrow$":
Es sei $H \trianglelefteq G$. Dann ist $H = \sigma H \sigma^{-1}$ für alle $\sigma \in G$. Somit gilt $G(L/Z) = G(L/\sigma(Z))$ für alle $\sigma \in G$. Nach dem Hauptsatz der Galoistheorie (Satz 2.7.4) ist $\sigma(Z) = Z$ für alle $\sigma \in G$. Für $\sigma \in G$ ist also $\sigma_{|Z}$ ein K- Automorphismus von Z. Die Abbildung $\pi\colon G \to G(Z/K)$, $\sigma \to \sigma_{|Z}$ ist ein Homomorphismus. Weiter gilt

$$\sigma \in \mathrm{Kern}(\pi) \Leftrightarrow \sigma_{|Z} = id_{|Z} \Leftrightarrow \sigma \in G(L/Z).$$

Nach dem Homomorphiesatz (Elemente der Algebra) ist das Bild $\pi(G)$ isomorph zur Faktorgruppe G/H. Für den Grad der Erweiterung Z/K und die Ordnung von $G(Z/K)$ gilt dann $[Z\colon K] = |G/H| \leq |G(Z/K)|$. Da auch $|G(Z/K)| \leq [Z\colon K]$ gilt, folgt $G/H \cong G(Z/K)$.
"$\Rightarrow$":
Es sei Z/K galoissch. Dann ist Z ein Zerfällungskörper eines Polynoms $g \in K[X]$, das heißt $Z = K(\beta_1, \ldots, \beta_k)$, wobei β_i die Nullstellen von g in L sind. Weiter permutiert $\sigma \in G(L/K)$ diese Nullstellen, und damit ist $Z = \sigma(Z)$. Nach i) folgt $H = \sigma H \sigma^{-1}$, also $H \trianglelefteq G$.

□

Beispiel 2.7.1. Wir kehren zu Beispiel 2.2.5 zurück: $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Wir hatten gefunden, dass $G(L/K) = \{\sigma_{\bar{0},\bar{0}}, \sigma_{\bar{0},\bar{1}}, \sigma_{\bar{1},\bar{0}}, \sigma_{\bar{1},\bar{1}}\}$ (Restklassen modulo 2) mit $\sigma_{r,s}(\sqrt{2}) = (-1)^k\sqrt{2}$ mit $k \in r$ und $\sigma_{r,s}(\sqrt{3}) = (-1)^l\sqrt{3}$ mit $l \in s$ ist, und erhielten folgende Zuordnung zwischen Untergruppen von $G(L/K)$ und Zwischenkörpern $L/Z/K$:



Der Körper L ist Zerfällungskörper von $f(X) = (X^2 - 2) \cdot (X^2 - 3)$ über $\mathbb{Q}$, also ist L/K eine Galoiserweiterung. Aus dem Hauptsatz der Galoistheorie folgt, dass die Abbildungen $U \to L^U$ und $Z \to G(L/Z)$ zueinander invers sind. Insbesondere gibt es keine anderen Zwischenkörper, als diejenigen, die im obigen Diagramm aufgelistet sind.

Als nächstes diskutieren wir die Galoistheorie für endliche Körper:

Definition 2.7.2. Es sei K ein Körper mit $\mathrm{char}(K) = p$, wobei p eine Primzahl sei. Die Abbildung $\sigma_p \colon K \to K$, $z \to z^p$ heißt Frobeniushomomorphismus von K.

Satz 2.7.6. *i) Der Frobeniushomomorphismus σ_p ist ein Isomorphismus. Ist K endlich, so ist σ_p ein Automorphismus von K.*

ii) Es sei $q = p^m$ und $K \subset L$ mit $|K| = q$ und $|L| = q^n$.
Dann ist L/K galoissch und $G(L/K) = \langle \sigma_p^m \rangle$. Zu jedem Teiler $d|n$ gibt es genau einen Zwischenkörper Z_d mit $|Z_d| = q^d$. Weiter ist Z_d Zerfällungskörper und Nullstellenmenge von $f_d(X) = X^{q^d} - X$. Andere Zwischenkörper gibt es nicht.

Beweis. i) Es seien $x, y \in K$. Nach dem Binomialsatz ist

$$\sigma_p(x+y) = (x+y)^p = x^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-1-j} + y^p = x^p + y^p = \sigma_p(x) + \sigma_p(y),$$

weil $\binom{p}{j} = 0$ ist.
Nach Satz 2.5.3 können wir annehmen, dass $\mathbb{P} = \mathbb{Z}/p\mathbb{Z}$ der gemeinsame Primkörper von K und L ist. Weiter ist K die Menge der Nullstellen von $f(X) = X^q - X$ in L, und jedes $\alpha \in L$ ist Nullstelle von $g(X) = X^{p^n} - X$. Daher lässt $(\sigma_p)^m$ jedes $\alpha \in K$ fest.

ii) Es sei $G = \langle \sigma_p^m \rangle$ die von σ_p^m erzeugte zyklische Gruppe. Jedes $\sigma \in G$ ist ein K- Automorphismus. Wir wollen daher die Ordnung von G bestimmen. Ist $\sigma_p^{mk} = id$ für $k \in \mathbb{N}$, so sind alle $z \in L$ Nullstellen des Polynoms $f(X) = X^{p^{mk}} - X$. Daraus folgt $n|k$ und $|G| = n$. Für alle Körpererweiterungen gilt $G(L/K) \leq [L \colon K] = n$ ist und $G(L/K) = n$ genau für Galoiserweiterungen, woraus $G(L/K) = G = \langle \sigma_p^m \rangle$ folgt. Nach Satz 1.3.8 ist die Menge der Untergruppen von G durch $\{U_d \colon d|n\}$ mit $U_d = \{\sigma \in G \colon \sigma^d = id\}$ gegeben. Die Gruppe U_d ist zyklisch, und es gilt $U_d = \langle \sigma_p^{mn/d} \rangle$ sowie $|U_d| = d$. Nach Satz 2.7.4 (Hauptsatz der Galoistheorie) sind die Zwischenkörper die Fixkörper L^{U_d}, und wir haben genau dann $\alpha \in L^{U_d}$, wenn $(\sigma_p^m)^{n/d}(\alpha) = \alpha$ gilt. Somit ist L^{U_d} die Nullstellenmenge von $h_d(X) = (X^q)^{n/d} - X$. Die Substitution $d \to n/d$ ergibt die Behauptung.

□

Beispiel 2.7.2. Es sei $\zeta_5 = e^{\frac{2\pi i}{5}}$. Bestimme alle Unterkörper von $L = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$.
Lösung:
Es sei

$$f(X) = X^5 - 2 = \prod_{j=0}^{4} (X - \sqrt[5]{2}\zeta_5^j).$$

Dann ist L ein Zerfällungskörper von f über $\mathbb{Q}$. Also ist $L/\mathbb{Q}$ eine Galoiserweiterung, und wir bestimmen nun die Galosigruppe $G(L/\mathbb{Q})$.
Nach Satz 2.2.2 können die Automorphismen von L durch Fortsetzung der Isomorphismen von Unterkörpern gewonnen werden. Wir beginnen mit den Isomorphismen von $\mathbb{Q}(\sqrt[5]{2})$.
Ein anderer möglicher Weg wäre, zunächst die Isomorphismen von $\mathbb{Q}(\zeta_5)$ zu untersuchen.

Isomorphismen von $\mathbb{Q}(\sqrt[5]{2})$:
Nach dem Eisensteinkriterium ist

$$m_{\mathbb{Q}}(\sqrt[5]{2}, X) = X^5 - 2 = f(X) = \prod_{j=0}^{4}(X - \sqrt[5]{2}\zeta_5^j).$$

Die Isomorphismen von $\mathbb{Q}(\sqrt[5]{2})$ sind somit durch $\sigma_j \colon \mathbb{Q}(\sqrt[5]{2}) \to \mathbb{Q}(\sqrt[5]{2}\zeta_5^j)$ mit $0 \leq j \leq 4$ gegeben. Es ist $[\mathbb{Q}(\sqrt[5]{2}\zeta_5^j) \colon \mathbb{Q}] = 5$. Es sei $g(X) = X^4 + X^3 + X^2 + X + 1$. Dann ist $(X-1) \cdot g(X) = X^5 - 1$, also

$$g(X) = \prod_{k=1}^{4}(X - \zeta_5^k).$$

Das Polynom $g(X+1)$ und damit auch das Polynom $g(X)$ sind nach dem Eisensteinkriterium in $\mathbb{Q}[X]$ irreduzibel. Also gilt $[\mathbb{Q}(\zeta_5) \colon \mathbb{Q}] = 4$. Da L ein gemeinsamer Oberkörper von $\mathbb{Q}(\sqrt[5]{2})$ und $\mathbb{Q}(\zeta_5)$ ist, muss nach dem Gradsatz der Grad $[L \colon \mathbb{Q}]$ nun auch durch $\mathrm{kgV}(5,4) = 20$ teilbar sein. Wegen $m_{\mathbb{Q}(\sqrt[5]{2})}(\zeta_5, X) | g(X)$ folgt $g(X) = m_{\mathbb{Q}(\sqrt[5]{2})}(\zeta_5, X)$, $[L \colon \mathbb{Q}(\sqrt[5]{2})] = 4$ und $[L \colon \mathbb{Q}] = 20$, also auch $|G(L/\mathbb{Q})| = 20$. Nach Satz 2.2.2 sind die Fortsetzungen $\sigma_{k,j}$ der σ_j durch $\sigma_{k,j} \colon \sqrt[5]{2} \to \sqrt[5]{2}\zeta_5^j$, $\zeta_5 \to \zeta_5^k$ mit $0 \leq j \leq 4$ und $1 \leq k \leq 4$ gegeben. Wir bestimmen die Verknüpfungsregeln:

$$\begin{array}{ccccc} \sqrt[5]{2} & \underset{\sigma_{k_2,j_2}}{\to} & \sqrt[5]{2}\zeta_5^{j_2} & \underset{\sigma_{k_1,j_1}}{\to} & \sqrt[5]{2}\zeta_5^{j_1}\zeta_5^{j_2 k_1} \\ \zeta_5 & \underset{\sigma_{k_2,j_2}}{\to} & \zeta_5^{k_2} & \underset{\sigma_{k_1,j_1}}{\to} & \zeta_5^{k_2 k_1}. \end{array}$$

Also gilt $\sigma_{k_1,j_1} \circ \sigma_{k_2,j_2} = \sigma_{k_1 k_2, k_1 j_2 + j_1}$.
Auch Matrizen der Form

$$\begin{pmatrix} k & j \\ 0 & 1 \end{pmatrix}$$

haben ein analoges Verknüpfungsgesetz:

$$\begin{pmatrix} k_1 & j_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} k_2 & j_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} k_1 k_2 & k_1 j_2 + j_1 \\ 0 & 1 \end{pmatrix}.$$

Zur Beschreibung von $G(L/\mathbb{Q})$ eignet sich somit die Matrizengruppe

$$AG(5) = \left\{ \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} : r \in (\mathbb{Z}/5\mathbb{Z})^*,\ s \in \mathbb{Z}/5\mathbb{Z} \right\}.$$

Für

$$\mathcal{A} = \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \in AG(5)$$

sei $\sigma_{\mathcal{A}} \in G(L/\mathbb{Q})$ durch $\sigma_{\mathcal{A}} \colon \sqrt[5]{2} \underset{\sigma_{\mathcal{A}}}{\to} \sqrt[5]{2}\zeta_5^j$ mit $j \in s$ und $\zeta_5 \underset{\sigma_{\mathcal{A}}}{\to} \zeta_5^k$ mit $k \in r$ definiert. Nach der obigen Rechnung ist dann $\sigma_{\mathcal{A}} \circ \sigma_{\mathcal{B}} = \sigma_{\mathcal{AB}}$. Somit ist $\psi \colon AG(5) \to G(L/\mathbb{Q})$, $\mathcal{A} \to \sigma_{\mathcal{A}}$ ein Isomorphismus, also gilt $G(L/\mathbb{Q}) \cong AG(5)$. Beide Gruppen sind wiederum isomorph zur Gruppe der affinen Abbildungen $L(5) = \{\Phi_{\mathcal{A}} \colon \mathcal{A} \in AG(5)\}$ mit $\Phi_{\mathcal{A}} \colon \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$, $x \to rx + s$ und

$$\mathcal{A} = \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}.$$

Wir bestimmen nun die Untergruppen von $AG(5)$ und damit die von $G(L/\mathbb{Q})$. Durch vollständige Induktion beweist man leicht

$$\mathcal{A}^l = \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}^l = \begin{pmatrix} r^l & (r^{l-1} + r^{l-2} + \ldots + r + 1)s \\ 0 & 1 \end{pmatrix} \tag{1}$$

für alle $l \in \mathbb{N}$ und $\mathcal{A} \in AG(5)$.

Wir unterscheiden zwei Fälle:
Fall 1:
Die Untergruppe $U \leq AG(5)$ enthält eine Matrix

$$\begin{pmatrix} 1 & s_0 \\ 0 & 1 \end{pmatrix}$$

mit $s_0 \neq 0$, eine echte Translation. Es sei

$$\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \in U.$$

Durch Induktion zeigt man leicht

$$\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & s_0 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} r & mrs_0 + s \\ 0 & 1 \end{pmatrix}.$$

Wegen $r, s_0 \neq 0$ durchläuft $mrs_0 + s$ alle Elemente von $\mathbb{Z}/5\mathbb{Z}$. Also gilt

$$\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \in U \Rightarrow \begin{pmatrix} r & t \\ 0 & 1 \end{pmatrix} \in U \quad \forall t \in \mathbb{Z}/5\mathbb{Z}.$$

Damit hat U die Form

$$U = \left\{ \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} : r \in V,\ s \in \mathbb{Z}/5\mathbb{Z} \right\}$$

mit einer Untergruppe V von $(\mathbb{Z}/5\mathbb{Z})^*$.
Nun hat $(\mathbb{Z}/5\mathbb{Z})^* = \langle 2 \bmod 5 \rangle$ die Untergruppen $V_0 = (\mathbb{Z}/5\mathbb{Z})^*$, $V_1 = \langle 2^2 \bmod 5 \rangle = \{\pm 1 \bmod 5\}$ und $V_2 = \{1 \bmod 5\}$. Damit ergibt Fall 1 die drei Untergruppen

$$\begin{aligned} \tilde{N}_0 &= AG(5) \\ \tilde{N}_1 &= \left\{ \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} : r \equiv \pm 1 \bmod 5, s \in \mathbb{Z}/5\mathbb{Z} \right\} \\ \tilde{N}_2 &= \left\{ \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} : s \in \mathbb{Z}/5\mathbb{Z} \right\} \end{aligned}$$

mit $|\tilde{N}_1| = 10$ und $|\tilde{N}_2| = 5$. Man rechnet sofort nach, dass die $\tilde{N}_i$ Normalteiler von $AG(5)$ sind.

Fall 2:
Die Untergruppe $U \leq AG(5)$ enthält keine Matrix

$$\begin{pmatrix} 1 & s_0 \\ 0 & 1 \end{pmatrix}$$

mit $s_0 \neq 0$. Dann bildet

$$R(U) = \left\{ r : \exists \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \in U \right\}$$

eine Untergruppe von $(\mathbb{Z}/5\mathbb{Z})^*$. Es sei $R(U) = \langle \sigma_0 \rangle$ mit $|\langle \sigma_0 \rangle| = l_0$ und

$$\begin{pmatrix} r_0 & s_0 \\ 0 & 1 \end{pmatrix} \in U.$$

Es folgt dann aus (1) wegen

$$(r_0 - 1) \cdot (r_0^{l_0 - 1} + r_0^{l_0 - 2} + \ldots + r_0 + 1) \cdot s_0 = (r_0^{l_0} - 1) \cdot s_0 = 0$$

nun

$$\begin{pmatrix} r_0 & s_0 \\ 0 & 1 \end{pmatrix}^{l_0} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2}$$

Annahme:
Es existiert ein $l_1 \leq l_0$ mit

$$\mathcal{A}_{l_1} = \begin{pmatrix} r_0^{l_1} & s_1 \\ 0 & 1 \end{pmatrix} \in U \quad \text{und} \quad \mathcal{A}_{l_1} \neq \begin{pmatrix} r_0 & s_0 \\ 0 & 1 \end{pmatrix}^{l_1}.$$

Dann ist

$$\mathcal{B} = \mathcal{A}_{l_1} \begin{pmatrix} r_0 & s_0 \\ 0 & 1 \end{pmatrix}^{l_0 - l_1} \in U,$$

aber wegen (2)

$$\mathcal{B} = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

ein Widerspruch. Damit gilt

$$U = \left\langle \begin{pmatrix} r_0 & s_0 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Wir erhalten somit folgende Untergruppen:

$$\begin{aligned} U_{(-1,s)} &= \left\langle \begin{pmatrix} -1 & s \\ 0 & 1 \end{pmatrix} \right\rangle \\ U_{(2,s)} &= \left\langle \begin{pmatrix} 2 & s \\ 0 & 1 \end{pmatrix} \right\rangle \end{aligned}$$

mit $s \in \mathbb{Z}/5\mathbb{Z}$. Es ist dabei $|U_{(-1,s)}| = 2$ und $|U_{(2,s)}| = 4$.

Zur Berechnung der Fixkörper kann man die Darstellung der Körperelemente $\alpha \in L$ als Linearkombination der Basiselemente $\sqrt[5]{2}^g$ und ζ_5^h mit $0 \leq g \leq 4$ und $1 \leq h \leq 4$ benützen.

$$\begin{aligned} \alpha &= a_{0,0} + a_{0,1}\sqrt[5]{2} + \ldots + a_{0,4}(\sqrt[5]{2})^4 + a_{1,0}\zeta_5 + a_{1,1}\sqrt[5]{2}\zeta_5 + \ldots + a_{1,4}(\sqrt[5]{2})^4\zeta_5 \\ &\quad a_{2,0}\zeta_5^2 + a_{2,1}\sqrt[5]{2}\zeta_5^2 + \ldots + a_{2,4}(\sqrt[5]{2})^4\zeta_5^2 + a_{3,0}\zeta_5^3 + a_{3,1}\sqrt[5]{2}\zeta_5^3 + \ldots + a_{3,4}(\sqrt[5]{2})^4\zeta_5^3. \quad (2.1) \end{aligned}$$

Es seien N_i die zu den $\widetilde{N}_i$ isomorphen Normalteilern von $G(L/\mathbb{Q})$. Die Fixkörper L^{N_i} berechnen sich wie folgt:
Für

$$\mathcal{A} = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \in N_2$$

ist

$$\begin{aligned} \sigma_{\mathcal{A}}(\sqrt[5]{2}) &= \sqrt[5]{2}\zeta_5^s \\ \sigma_{\mathcal{A}}(\zeta_5) &= \zeta_5. \end{aligned}$$

Aus der Darstellung (2.1) folgt dann $\mathbb{Q}(\zeta_5) \subset L^{N_2}$. Wegen

$$[L^{N_2} \colon \mathbb{Q}] = (G(L/\mathbb{Q}) \colon N_2) = 4 = [\mathbb{Q}(\zeta_5) \colon \mathbb{Q}]$$

folgt $L^{N_2} = \mathbb{Q}(\zeta_5)$. Wegen $N_i \supset N_2$ für $0 \leq i \leq 1$ muss $L^{N_i} \subset L^{N_2} = \mathbb{Q}(\sqrt[5]{2})$ erfüllt sein. Es ist offenbar $L^{N_0} = \mathbb{Q}$, und es bleibt nur noch L^{N_1} zu bestimmen. Wir betrachten

$$\mathcal{A} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in N_1 - N_2$$

und $\sigma_{\mathcal{A}|_{\mathbb{Q}(\zeta_5)}}$ sowie $\sigma_{\mathcal{A}}(\zeta_5) = \zeta_5^{-1}$.

Es sei $\alpha = a_{0,0} + a_{1,0}\zeta_5 + a_{2,0}\zeta_5^2 + a_{3,0}\zeta_5^3 \in \mathbb{Q}(\zeta_5)$. Dann ist

$$\sigma_{\mathcal{A}}(\alpha) = a_{0,0} + a_{1,0}(-1 - \zeta_5 - \zeta_5^2 - \zeta_5^3) + a_{3,0}\zeta_5^2 + a_{2,0}\zeta_5^3.$$

Aus $\sigma_{\mathcal{A}}(\alpha) = \alpha$ folgt, dass die Bedingungen $a_{1,0} = 0$ und $a_{3,0} = a_{2,0}$ gelten.
Man kann Elemente des Fixkörpers von $\sigma_{\mathcal{A}}$ auch durch Angabe direkt finden, indem man die Elemente der Bahn eines Elements von $\sigma_{\mathcal{A}}$ summiert, d.h. die Spur des Elements bildet. Mit $\sigma_{\mathcal{A}}(\zeta_5) = \zeta_5^{-1}$ gilt

$$\eta_5 = \zeta_5 + \sigma_{\mathcal{A}}(\zeta_5) = \zeta_5 + \zeta_5^{-1}. \tag{3}$$

Man findet, dass η_5 Nullstelle des Polynoms $g(X) = X^2 + X - 1$ ist. Es ist

$$X^2 + X - 1 = (X - (\zeta_5 + \zeta_5^{-1})) \cdot (X - (\zeta_5^2 + \zeta_5^{-2})).$$

Somit ist $L^{N_1} = \mathbb{Q}(\eta_5)$ mit $\eta_5 = \zeta_5 + \zeta_5^{-1} \in \mathbb{R}$.

Der Fall 2 liefert fünf zyklische Untergruppen der Ordnung 4, die jeweils eine Untergruppe der Ordnung 2 erhalten.
Wir haben folgende Tabelle:

$\mathcal{A}$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}2&3\\0&1\end{pmatrix}$	$\begin{pmatrix}2&4\\0&1\end{pmatrix}$
$\mathcal{A}^2$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}$	$\begin{pmatrix}4&3\\0&1\end{pmatrix}$	$\begin{pmatrix}4&1\\0&1\end{pmatrix}$	$\begin{pmatrix}4&4\\0&1\end{pmatrix}$	$\begin{pmatrix}4&2\\0&1\end{pmatrix}$
$\mathcal{A}^3$	$\begin{pmatrix}3&0\\0&1\end{pmatrix}$	$\begin{pmatrix}3&2\\0&1\end{pmatrix}$	$\begin{pmatrix}3&4\\0&1\end{pmatrix}$	$\begin{pmatrix}3&1\\0&1\end{pmatrix}$	$\begin{pmatrix}3&3\\0&1\end{pmatrix}$
$\mathcal{A}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$
Untergruppen:					
	$U_0^{(4)}$	$U_1^{(4)}$	$U_2^{(4)}$	$U_3^{(4)}$	$U_4^{(4)}$
	$U_0^{(2)} = \left\langle \begin{pmatrix}4&0\\0&1\end{pmatrix} \right\rangle$	$U_1^{(2)} = \left\langle \begin{pmatrix}4&3\\0&1\end{pmatrix} \right\rangle$	$U_2^{(2)} = \left\langle \begin{pmatrix}4&1\\0&1\end{pmatrix} \right\rangle$	$U_3^{(2)} = \left\langle \begin{pmatrix}4&4\\0&1\end{pmatrix} \right\rangle$	$U_4^{(2)} = \left\langle \begin{pmatrix}4&2\\0&1\end{pmatrix} \right\rangle$
Fixkörper:					
$L^{U_j^{(4)}}$	$\mathbb{Q}(\sqrt[5]{2})$	$\mathbb{Q}(\sqrt[5]{2}\zeta_5^4)$	$\mathbb{Q}(\sqrt[5]{2}\zeta_5^3)$	$\mathbb{Q}(\sqrt[5]{2}\zeta_5^2)$	$\mathbb{Q}(\sqrt[5]{2}\zeta_5)$
$L^{U_j^{(2)}}$	$\mathbb{Q}(\sqrt[5]{2}, \eta_5)$	$\mathbb{Q}(\sqrt[5]{2}\zeta_5^4, \eta_5)$	$\mathbb{Q}(\sqrt[5]{2}\zeta_5^3, \eta_5)$	$\mathbb{Q}(\sqrt[5]{2}\zeta_5^2, \eta_5)$	$\mathbb{Q}(\sqrt[5]{2}\zeta_5, \eta_5)$

Die Berechnung der Fixkörper kann mit der Darstellung (2.1) erfolgen.
Wir geben die Rechnung nur für den Fall $U_1^{(4)}$ an. Die Automorphismen $\sigma_{\mathcal{A}^j}$ mit $1 \le j \le 4$ und

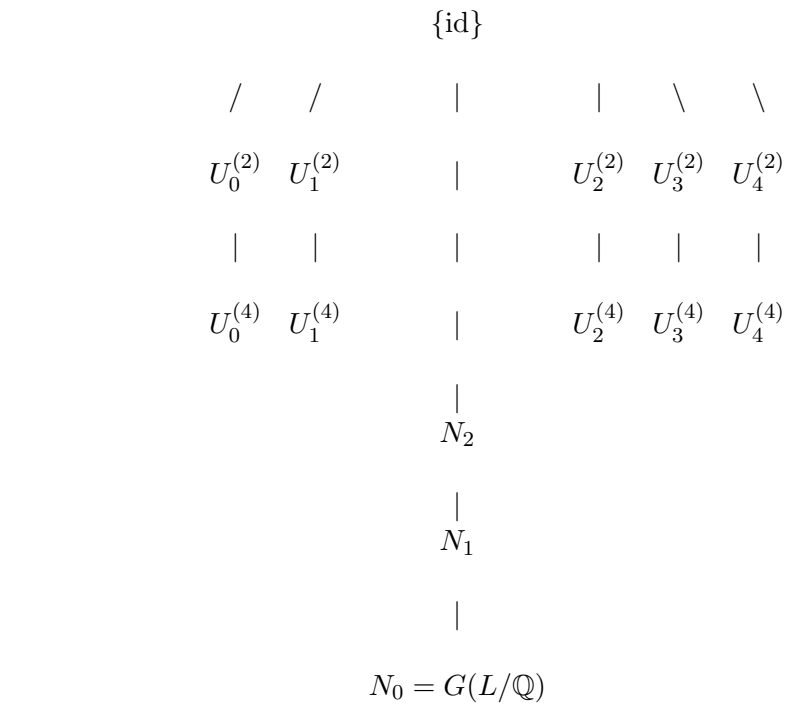
$$\mathcal{A} = \begin{pmatrix}2&1\\0&1\end{pmatrix}$$

haben folgende Wirkungen auf $\sqrt[5]{2}$:

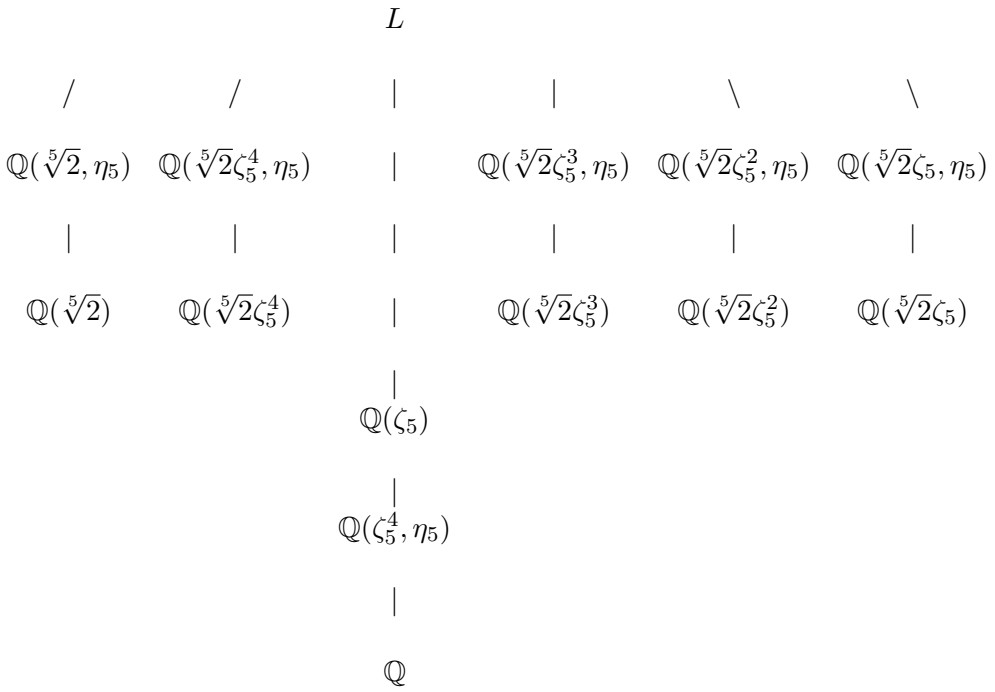
$$\begin{aligned}\sigma_{\mathcal{A}}(\sqrt[5]{2}) &= \sqrt[5]{2}\zeta_5,\\ \sigma_{\mathcal{A}^2}(\sqrt[5]{2}) &= \sqrt[5]{2}\zeta_5^2,\\ \sigma_{\mathcal{A}^3}(\sqrt[5]{2}) &= \sqrt[5]{2}\zeta_5^3.\end{aligned}$$

Damit folgt in (2.1) für $\alpha \in L^{U_1^{(4)}}$ die Bedingung $a_{0,1} = a_{1,1} = a_{2,1} = a_{3,1}$, und $L^{U_1^{(4)}}$ enthält somit das Element $\sqrt[5]{2}(1 + \zeta_5 + \zeta_5^2 + \zeta_5^3) = -\sqrt[5]{2}\zeta_5^4$.
Damit gilt $L^{U_1^{(4)}} = \mathbb{Q}(\sqrt[5]{2}\zeta_5^4)$.

Wir erhalten schließlich folgende Diagramme mit der Zuordnung $U \longrightarrow L^U$:



sowie



Beispiel 2.7.3. Es sei K ein Körper, $u_1, \ldots, u_n$ unabhängige Unbestimmte über K, $s_1, \ldots, s_n$ die elementarsymmetrischen Funktionen von $u_1, \ldots, u_n$ und $K(u_1, \ldots, u_n)$ bzw. $K(s_1, \ldots, s_n)$ die Quotientenkörper von $K[u_1, \ldots, u_n]$ bzw. $K[s_1, \ldots, s_n]$. Nach Satz 2.6.3 ist $K(u_1, \ldots, u_n)/K(s_1, \ldots, s_n)$ eine Galoiserweiterung.

2.8 Einheitswurzeln und Kreisteilungskörper

Definition 2.8.1. Es sei K ein Körper und $n \in \mathbb{N}$. Ein Zerfällungskörper des Polynoms $X^n - 1$ über dem Körper K wird mit $K^{(n)}$ bezeichnet und n- ter Kreisteilungskörper über K genannt. Die Nullstellen von $X^n - 1$ heißen die n- ten Einheitswurzeln von K, und ihre Menge wird mit $E^{(n)}$ bezeichnet. Wenn $K = K^{(n)}$ gilt, sagt man, dass K alle n- ten Einheitswurzeln enthält.

Beispiel 2.8.1. Zu jedem $n \in \mathbb{N}$ enthält $\mathbb{C}$ die n- ten Einheitswurzeln. Durch sie wird die Peripherie des Einheitskreises in n Stücke gleicher Länge geteilt, woher auch der Name "Kreisteilungskörper" resultiert.

Beispiel 2.8.2. Ein beliebiger Körper enthält stets die zweiten Einheitswurzeln, nämlich -1 und 1.

Satz 2.8.1. *Es sei $p = \mathrm{char}(K)$ und $n \in \mathbb{N}$ beliebig.*

i) Gilt $p|n$, also $n = mp^l$ mit $m, l \in \mathbb{N}$ und $p \nmid m$, so ist jede n- te Einheitswurzel eine m- te.

ii) Gilt $p \nmid n$, so ist $E^{(n)}$ mit der Multiplikation in $K^{(n)}$ eine zyklische Gruppe der Ordnung n.

Beweis. i) Nach Satz 2.7.6 ist die Abbildung $\psi\colon K \to K$, $z \to z^{p^l}$ als l- te Potenz des Frobeniushomomorphismus ein Monomorphismus, also insbesondere injektiv. Für $\zeta \in E^{(n)}$ gilt $\psi(\zeta^m) = (\zeta^m)^{p^l} = 1_K = \psi(1)$, also $\zeta^m = 1$ wegen der Injektivität von ψ.

ii) Das Polynom $f(X) = X^n - 1$ und seine Ableitung $f'(X) = nX^{n-1}$ sind wegen $p \nmid n$ teilerfremd. Nach Satz 2.4.1 ist f separabel und besitzt im Zerfällungskörper $K^{(n)}$ genau n verschiedene Nullstellen, d.h. $|E^{(n)}| = n$. Mit $\zeta, \eta \in E^{(n)}$ folgt stets $(\zeta\eta^{-1})^n = \zeta^n(\eta^n)^{-1} = 1_K$ und damit $\zeta\eta^{-1} \in E^{(n)}$. Da K ein Körper ist, hat für $d \in \mathbb{N}$ die Gleichung $x^d = 1_K$ höchstens d Lösungen $x \in E^{(n)}$. Nach Satz 1.3.10 ist $E^{(n)}$ zyklisch.

□

Definition 2.8.2. Es sei $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Dann heißt ein erzeugendes Element der zyklischen Gruppe $E^{(n)}$ eine primitive n- te Einheitswurzel über K.

Satz 2.8.2. *Es sei $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Dann gibt es genau $\varphi(n)$ verschiedene primitive n- te Einheitswurzeln. Ist ζ_n eine von ihnen, so sind die anderen durch ζ_n^k mit $1 \leq k \leq n$ und $ggT(k, n) = 1$ gegeben.*

Beweis. Dies folgt aus den Sätzen 2.8.1 und 1.3.8. □

Definition 2.8.3. Es sei $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und $\zeta_n \in K^{(n)}$ eine n- te primitive Einheitswurzel über K. Das Polynom

$$\Phi_n(X) = \prod_{\substack{j=1 \\ ggT(j,n)=1}}^{n} (X - \zeta_n^j) \in K^{(n)}[X]$$

heißt das n- te Kreisteilungspolynom über K.

Satz 2.8.3. *Es sei $\mathbb{P}$ der Primkörper von K und $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Dann ist $\Phi_n(X) \in \mathbb{P}[X]$. Ist $\mathbb{P} = \mathbb{Q}$, so gilt sogar $\Phi_n(X) \in \mathbb{Z}[X]$.*

Beweis. Es bezeichne $E_d^{(n)}$ die Menge aller Elemente von $E^{(n)}$ der Ordnung d. Dann ist

$$E^{(n)} = \bigcup_{d|n} E_d^{(n)}$$

eine Partition von $E^{(n)}$. Wegen $d|n$ enthält $E^{(n)}$ alle d- ten Einheitswurzeln, folglich ist $E_d^{(n)}$ die Menge der d- ten primitiven Einheitswurzeln aus $E^{(n)}$. Daher gilt

$$X^n - 1 = \prod_{\omega \in E^{(n)}} (X - \omega) = \prod_{d|n} \prod_{\omega \in E_d^{(n)}} (X - \omega) = \prod_{d|n} \Phi_d(X). \qquad (*)$$

Wir beweisen nun die Behauptung des Satzes durch Induktion nach n.
Für $n = 1$ ist $\Phi_1(X) = X - 1$.
Es sei nun $n > 1$ und die Behauptung für alle $d < n$ bewiesen. Dann folgt $(*)$ aus

$$\Phi_n(X) \cdot f(X) = X^n - 1$$

mit

$$f(X) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X).$$

und $f(X) \in \mathbb{P}[X]$ nach Induktionsvoraussetzung (für $\mathbb{P} = \mathbb{Q}$ sogar $f \in \mathbb{Z}[X]$).
Das Polynom $\Phi_n(X)$ kann aus $X^n - 1$ und $f(X)$ mittels "langer Division" gewonnen werden. Da der Divisor $f(X)$ normiert ist und seine Koeffizienten in $\mathbb{P}$ (und für $\mathbb{P} = \mathbb{Q}$ sogar in $\mathbb{Z}$) liegen, sieht man, dass dies auch für alle in der Division auftretenden Koeffizienten der Fall ist. □

Beispiel 2.8.3. Es sei $K = \mathbb{Q}$ und p eine Primzahl. Dann ist

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \ldots + X^{p-1}.$$

Für $n = 6$ ist

$$\Phi_6(X) = \frac{X^6 - 1}{\Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X)} = \frac{X^6 - 1}{(X - 1) \cdot (X + 1) \cdot (X^2 + X + 1)} = X^2 - X + 1.$$

Satz 2.8.4. *Für alle $n \in \mathbb{N}$ ist das n-te Kreisteilungspolynom $\Phi_n(X)$ über dem Körper $\mathbb{Q}$ in $\mathbb{Q}[X]$ irreduzibel.*

Beweis. Es genügt es, die Irreduzibilität von $\Phi_n(X)$ in $\mathbb{Z}[X]$ zu zeigen.
Wir nehmen das Gegenteil an: Es sei

$$\Phi_n(X) = f(X) \cdot g(X) \qquad (1)$$

mit einem irreduziblen (und damit auch primitiven) $f(X) \in \mathbb{Z}[X]$ und einem beliebigen $g(X) \in \mathbb{Z}[X]$.
Es sei ζ_n eine Nullstelle von $f(X)$ in $\mathbb{Q}^{(n)}$.
Es genügt zu zeigen, dass wenn p eine Primzahl mit $p \nmid n$ ist, ist ζ_n^p ebenfalls eine Nullstelle von $f(X)$.
Wir nehmen wieder das Gegenteil an und setzen

$$X^n - 1 = f(X) \cdot c(X) \qquad (2)$$

mit einem normierten $c(X) \in \mathbb{Z}[X]$. Dann ist ζ_n^p Nullstelle von $c(X)$, und damit ζ_n Nullstelle des Polynoms $c(X^p)$. Nach Elemente der Algebra gilt $f(X)|c(X^p)$ in $\mathbb{Q}[X]$, und wegen der Primitivität von $f(X)$ gilt sogar $f(X)|c(X^p)$ in $\mathbb{Z}[X]$, also

$$c(X^p) = f(X) \cdot h(X) \qquad (3)$$

für ein $h(X) \in \mathbb{Z}[X]$.

Wir ersetzen nun die Polynome in (3) durch Polynome in $(\mathbb{Z}/p\mathbb{Z})[Y]$, indem wir sämtliche Koeffizienten a durch die zugehörigen Restklassen $a \bmod p$ ersetzen und erhalten damit

$$\overline{c}(Y^p) = \overline{f}(Y) \cdot \overline{h}(Y),$$

also mit Anwendung des Homomorphismus $z \to z^p$

$$\overline{c}(Y)^p = \overline{f}(Y) \cdot \overline{h}(Y).$$

Damit sind $\overline{f}(Y)$ und $\overline{c}(Y)$ nicht teilerfremd. Aus (1) folgt

$$Y^n - (1 \bmod p) = \overline{f}(Y) \cdot \overline{c}(Y).$$

Damit ist $Y^n - (1 \bmod p)$ inseparabel, im Widerspruch zu $ggT(Y^n - (1 \bmod p), nY^{n-1}) = 1$. □

Satz 2.8.5. *Für $n \in \mathbb{N}$ ist $\mathbb{Q}^{(n)} = \mathbb{Q}(\zeta_n)$ mit einer primitiven n- ten Einheitswurzel.*
Dann ist $\mathbb{Q}^{(n)}/\mathbb{Q}$ eine Galoiserweiterung mit $[\mathbb{Q}^{(n)} : \mathbb{Q}] = \varphi(n)$. Die Galoisgruppe ist durch

$$G(\mathbb{Q}^{(n)}/\mathbb{Q}) = \{\sigma_j : 1 \leq r \leq n,\ ggT(r, n) = 1\}$$

mit $\sigma_j : \zeta_n \to \zeta_n^j$ gegeben. Es gilt $G(\mathbb{Q}^{(n)}/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Beweis. Nach Satz 2.2.2 sind sämtliche Isomorphismen von $\mathbb{Q}^{(n)} = \mathbb{Q}(\zeta_n)$ durch $\sigma_j : \zeta_n \to \alpha^{(j)}$ gegeben, wobei $\alpha^{(j)}$ die Nullstellen von $\Phi_n(X) = m_{\mathbb{Q}}(\zeta_n, X)$ sind.
Die Abbildung $\psi : G(\mathbb{Q}^{(n)}/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ mit $\psi(\sigma_j) = j \bmod n$ ist ein Isomorphismus, wie man leicht nachrechnet. □

2.9 Auflösbare Gruppen

Der Name auflösbar erklärt sich aus der Anwendung auf Fragen der Auflösbarkeit von algebraischen Gleichungen durch Radikale.

Definition 2.9.1. Es sei G eine Gruppe.

i) Unter einer Normalreihe von G versteht man eine Folge sukzessiver Normalteiler

$$G = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_k = \{1_G\}, \qquad (*)$$

so dass $N_i \triangleleft N_{i-1}$ ein Normalteiler von N_{i-1} ist. Die Faktorgruppen N_{i-1}/N_i heißen Faktoren der Normalreihe.

ii) Die Gruppe G heißt auflösbar, falls es eine Normalreihe von G der Form $(*)$ mit abelschen Faktoren N_{i-1}/N_i gibt.

iii) Eine Normalreihe der Form $(*)$ heißt Kompositionsreihe von G, wenn die Faktoren N_{i-1}/N_i einfach sind.

Definition 2.9.2. Es sei G eine Gruppe.

i) Für $g, h \in G$ heißt $[g, h] := ghg^{-1}h^{-1}$ der Kommutator von g und h.

ii) Die von allen Kommutatoren erzeugte Untergruppe $[G, G] := \langle\{[g, h] : g, h \in G\}\rangle$ heißt die Kommutatorgruppe von G.

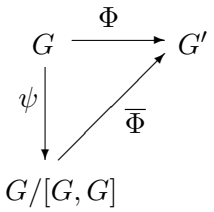
Satz 2.9.1. *Es sei G eine Gruppe.*

i) Es gilt $[G,G] = \{[a_1,b_1]\cdots[a_r,b_r]\colon a_i,b_i \in G,\ r \in \mathbb{N}\}$.

ii) Es ist $[G,G]$ ein Normalteiler von G.

iii) Es sei $N \trianglelefteq G$. Die Faktorgruppe G/N ist genau dann kommutativ, wenn $[G,G] \trianglelefteq N$ ist.

iv) Universelle Abbildungseigenschaft:
Es sei $\psi\colon G \to G/[G,G]$, $g \to g[G,G]$ der kanonische Epimorphismus von G auf $G/[G,G]$.
Für jeden Homomorphismus $\Phi\colon G \to G'$ von G in eine kommutative Gruppe G' existiert genau ein Homomorphismus $\overline{\Phi}\colon G/[G,G] \to G'$ mit $\Phi = \overline{\Phi} \circ \psi$, d.h.zu Φ gibt es stets ein $\overline{\Phi}$, so dass das Diagramm



kommutiert.

Beweis. i) Nach Elemente der Algebra ist

$$[G,G] = \{g_1\cdots g_l h_1^{-1}\cdots h_m^{-1}\colon g_j = [a_j,b_j],\ h_j^{-1} = [c_j,d_j],\ a_j,b_j,c_j,d_j \in G\}.$$

Es ist $h_j = (c_j d_j c_j^{-1} d_j^{-1})^{-1} = [d_j,c_j]$.

ii) Es seien $c \in [G,G]$ und $g \in G$, woraus $gcg^{-1} = gcg^{-1}c^{-1}c = [g,c]c \in [G,G]$ folgt.
Damit gilt $[G,G] \trianglelefteq G$.

iii) Es ist

$$G/N \text{ ist kommutativ} \Leftrightarrow N(gh) = N(hg)\ \forall g,h \in G \Leftrightarrow N[g,h] = N\ \forall g,h \in G \Leftrightarrow [G,G] \trianglelefteq N.$$

iv) Wir definieren $\overline{\Phi}$ durch

$$\overline{\Phi} := \begin{cases} G \to G/[G,G] \\ g[G,G] \to \Phi(g) \end{cases}$$

Die Abbildung $\overline{\Phi}$ ist wohldefiniert, denn wegen Teil (i) gilt

$$g_1[G,G] = g_2[G,G] \Rightarrow g_2^{-1}g_1 \in [G,G] \Rightarrow g_2^{-1}g_1 = [a_1,b_1]\cdots[a_r,b_r]$$

für $a_j,b_j \in G$. Daraus folgt nun

$$\Phi(g_2^{-1}g_1) = [\Phi(a_1),\Phi(b_1)]\cdots[\Phi(a_r),\Phi(b_r)] = 1_{G'}$$

da G' abelsch ist. Also ist $\Phi(g_1) = \Phi(g_2)$. Die übrigen Eigenschaften von $\overline{\Phi}$ sind klar.

□

Satz 2.9.2. *Für eine Gruppe G sind folgende Aussagen äquivalent:*

i) Die Gruppe G ist auflösbar.

ii) Es gibt ein $n \in \mathbb{N}$ mit $G^{(n)} = \{1\}$.
Dabei ist $G^{(n)}$ rekursiv durch $G^{(0)} := G$ und $G^{(i+1)} := [G^{(i)},G^{(i)}]$ definiert.

Beweis. $(i) \Rightarrow (ii)$:
Es sei $G = G_0 \triangleright \cdots \triangleright G_n = \{1\}$ eine Normalreihe mit abelschen Faktoren.
Wir zeigen $G^{(i)} \subseteq G_i$ durch Induktion nach i.
$\underline{i = 0}$:
Dies ist klar.
$\underline{(i-1) \to i}$:
Da G_{i-1}/G_i abelsch ist, folgt die Behauptung nach Satz 2.9.1 und der Induktionshypothese

$$G_i \supseteq [G_{i-1}, G_{i-1}] \supseteq [G^{i-1}, G^{i-1}] = G^{(i)}.$$

$(ii) \Rightarrow (i)$:
Nach Satz 2.9.1 ist $G = G^{(0)} \triangleright G^{(1)} \triangleright \cdots \triangleright G^{(n)}$ eine Normalreihe mit abelschen Faktoren. □

Satz 2.9.3. *Es sei G eine auflösbare Gruppe. Dann gilt:*

i) Jede Untergruppe $U \leq G$ ist auflösbar.

ii) Ist $\Phi\colon G \to G'$ ein Epimorphismus, so ist auch G' auflösbar.

Beweis. i) Dies folgt sofort nach Satz 2.9.2 (ii).

ii) Dies folgt wegen $\Phi(G)^{(i)} = \Phi(G^{(i)})$ aus Satz 2.9.2.

□

Die nächsten beiden Sätze können als Ergänzung zum Homomorphiesatz (Elemente der Algebra) betrachtet werden.

Satz 2.9.4. *(1. Isomorphiesatz)*
Es sei G eine Gruppe, $N \triangleleft G$ und $U \leq G$. Dann ist $UN \leq G$, $U \cap N \leq U$ und $UN/N \cong U/U \cap N$. Der Isomorphismus zwischen UN/N und $U/U \cap N$ ist durch $gN \to g(U \cap N)$ für alle $g \in H$ gegeben.

Beweis. Es gilt

$$(UN)(UN)^{-1} = UNN^{-1}U^{-1} = UNU \underset{N \triangleleft G}{=} UUN = UN,$$

also $UN \leq G$. Aus $N \triangleleft G$ folgt $N \triangleleft UN$. Es sei $\Phi\colon U \to UN/N$, $g \to gN$ für alle $g \in UN$ mit $\mathrm{Kern}(\Phi) = U \cap N$. Die Behauptung folgt mit dem Homomorphiesatz aus Elemente der Algebra. □

Satz 2.9.5. *(2. Isomorphiesatz)*
Es seien G und G' Gruppen. Weiter sei $\Phi\colon G \to G'$ ein Epimorphismus und $K = \mathrm{Kern}(\Phi)$.

i) Die Normalteiler von G, die K enthalten, entsprechen eineindeutig den Normalteilern von G' wie folgt:
Ist $\mathcal{N}$ die Menge der Normalteiler von G, die K enthalten, und $\mathcal{N}'$ die Menge der Normalteiler von G', so ist die Abbildung $\mathcal{N} \to \mathcal{N}'$, $N \to \Phi(N)$ bijektiv. Invers dazu ist die Abbildung

$$\psi\colon \mathcal{N}' \to \mathcal{N}, \quad N' \to \Phi^{-1}(N').$$

ii) Für jedes $N \in \mathcal{N}$ hat man den Isomorphismus $G/N \cong G'/\Phi(N)$ durch die Zuordnung

$$gN \to \Phi(g)\Phi(N)$$

für alle $g \in G$.

Beweis. i) Wir zeigen zunächst, dass $\Phi(N) \triangleleft G'$ für $N \triangleleft G$ und $N \supset K$ gilt. Offenbar ist $\Phi(N) \leq G'$.
Es sei nun $h \in G'$ mit $h = \Phi(g)$ für ein $g \in G$. Dann ist $h\Phi(N)h^{-1} = \Phi(gNg^{-1}) \subset \Phi(N)$, also $\Phi(N) \triangleleft G'$.
Wir behaupten nun, dass für $N' \in \mathcal{N}'$ die Aussage $\Phi^{-1}(N') \in \mathcal{N}$ gilt.
Es gilt $\Phi^{-1}(N') \supset \Phi'(\{e\}) = K$. Wegen

$$g, h \in \Phi^{-1}(N') = \Phi(gh^{-1}) = \Phi(g)\Phi(h)^{-1} \in N'$$

folgt $gh^{-1} \in \Phi^{-1}(N')$ bzw. $\Phi^{-1}(N') \leq G$.
Für $k \in G$ ist $\Phi(kgk^{-1}) = \Phi(k)\Phi(g)\Phi(k)^{-1} \in \mathcal{N}'$, also $kgk^{-1} \in \Phi^{-1}(N')$, woraus $\Phi^{-1}(N') \in \mathcal{N}$ folgt.
Die Abbildung τ sei durch $N' \to \Phi^{-1}(N')$ gegeben, also als eine Abbildung von $\mathcal{N}'$ nach $\mathcal{N}$.
Wir behaupten jetzt, dass τ zu ψ invers ist. Für $N \in \mathcal{N}$ gilt $(\tau \circ \psi)(N) = \Phi^{-1}(\Phi(N)) \supset N$.
Für $g \in \Phi^{-1}(\Phi(N))$ gilt

$$\Phi(g) \in \Phi(N) \Rightarrow \Phi(g) = \Phi(h) \Rightarrow \Phi^{-1}(\Phi(N)) \subset N \Rightarrow \Phi^{-1}(\Phi(N)) = N = \tau \circ \psi = id_{\mathcal{N}},$$

was zu zeigen war.

ii) Nach (i) gilt $\Phi(N) \triangleleft G'$, d.h. die Faktorgruppe $\Phi(N)/G'$ existiert. Es sei $\theta = \Omega \circ \Phi$ mit $\Omega\colon G' \to G'/\Phi(N)$ als kanonischer Epimorphismus. Somit ist θ ein Epimorphismus mit

$$\mathrm{Kern}(\Phi) = \theta^{-1}(\Phi(N)) = \Phi^{-1}(\Omega^{-1}(\Phi(N))) = \Phi^{-1}(\Phi(N)) = N.$$

Daher gilt $G/N \cong G'/\Phi(N)$ durch die Zuordnung $gN \to \theta(g) = \Phi(g)\Phi(N)$.

□

Satz 2.9.6. *(Kürzungsssatz)*
Es sei $K \triangleleft G$. Die Normalteiler von G, die K enthalten, entsprechen eineindeutig den Normalteilern von G/K wie folgt:
Ist $\mathcal{N}$ die Menge der Normalteiler von G, die K enthalten, und $\mathcal{N}'$ die Menge der Normalteiler von G/K, so ist die Abbildung $\mathcal{N} \to \mathcal{N}'$, $N \to N/K$ bijektiv.
Ist $N \in \mathcal{N}$, so ist $G/N \cong (G/K)/(N/K)$ durch die Zuordnung $gN \to (gK)(N/K)$ für alle $g \in G$.

Beweis. Es sei $\Phi\colon G \to G' = G/K$ der kanonische Epimorphismus. Dann gilt $\Phi(g) = gK$ für alle $g \in G$, und die Behauptung folgt mit dem 2. Isomorphiesatz. □

Satz 2.9.7. *Es sei G eine Gruppe, N ein Normalteiler von G und $\Phi\colon G \to G/N$ der kanonische Epimorphismus.*

i) Es seien

$$G/N = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_k = \{N\} \tag{1}$$

eine Normalreihe von G/N und

$$N = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_l = \{1\} \tag{2}$$

eine Normalreihe von N und $G_i := \Phi^{-1}(H_i)$ für $1 \leq i \leq k$. Dann ist

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = N = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_l = \{1\} \tag{3}$$

eine Normalreihe von G. Es ist $G_{i-1}/G_i \cong H_{i-1}/H_i$.

ii) Die Gruppe G ist genau dann auflösbar, wenn N und G/N auflösbar sind.

Beweis. i) Nach dem 2. Isomorphiesatz sind die $G_i = \Phi^{-1}(H_i)$ Normalteiler von G mit $N \trianglelefteq G_i$, und es ist $H_{i-1}/H_i = (G_{i-1}/N)/(G_i/N) \cong G_{i-1}/G_i$ nach dem Kürzungssatz.

ii) "$\Rightarrow$":
Dies folgt aus Satz 2.9.3.
"$\Leftarrow$":
Aus der Auflösbarkeit von G/N und N folgt die Existenz von Normalreihen der Form (1) und (2) mit abelschen Faktoren H_{i-1}/H_i und N_{i-1}/N_i. Wegen $G_{i-1}/G_i \cong H_{i-1}/H_i$ ist dann (3) eine Normalreihe von G mit abelschen Faktoren, d.h. G ist auflösbar.

□

Satz 2.9.8. *Ein endliche Gruppe $G \neq \{1\}$ ist genau dann auflösbar, wenn sie eine Kompositionsreihe besitzt, deren Faktoren zyklische Gruppen von Primzahlordnung sind.*

Beweis. "$\Leftarrow$":
Dies folgt sofort aus der Definition der Auflösbarkeit.
"$\Rightarrow$":
Wir nehmen an, die Aussage sei falsch. Es sei G ein "kleinster Verbrecher", d.h. $G \neq \{1\}$ sei eine Gruppe kleinster Ordnung, die zwar auflösbar ist, jedoch keine Normalreihe der beschriebenen Art besitzt. Wir nehmen nun an, G sei einfach. Dann ist $G \triangleright \{1\}$ die einzige Normalreihe von G. Also ist G abelsch, und damit nach Elemente der Algebra von Primzahlordnung, ein Widerspruch. Also ist G nicht einfach, d.h. es gibt $N \triangleleft G$ mit $\{1\} \triangleleft N \triangleleft G$. Dann sind nach Satz 2.9.4 (i) die Gruppen G/N und N auflösbar, und da G der kleinste Verbrecher ist, besitzen G/N und N Kompositionsreihen, deren Faktoren zyklisch von Primzahlordnung sind. Nach Satz 2.9.4 (i) lassen sich diese zu einer Kompositionsreihe von G zusammenfügen, erneut ein Widerspruch. □

Wir erwähnen ohne Beweis den wichtigen

Satz 2.9.9. *(Jordan-Hölder)*
Es seien

$$\begin{aligned} G &= G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{1\} \\ G &= H_0 \triangleright H_1 \triangleright \cdots \triangleright H_s = \{1\} \end{aligned}$$

zwei Kompositionsreihen einer Gruppe G. Dann ist $r = s$, und die Faktoren beider Kompositionsreihen sind bis auf die Reihenfolge isomorph, d.h. es existiert ein $\sigma \in \mathfrak{S}_r$ mit

$$G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}.$$

2.10 Auflösbarkeit durch Radikale

Definition 2.10.1. Für $n \in \mathbb{N}$ und $\alpha \in K$ bezeichne $\sqrt[n]{\alpha}$ eine beliebige, fest gewählte Nullstelle von $X^n - \alpha$ in einem Zerfällungskörper über K. Man nennt $\sqrt[n]{\alpha}$ eine n- te Wurzel von α über K oder ein Radikal vom Exponenten n über K. Ist $X^n - \alpha$ in $K[X]$ irreduzibel, so heißt $\sqrt[n]{\alpha}$ irreduzibles Radikal über K.

Das Symbol $\sqrt[n]{\alpha}$ ist im allgemeinen mehrdeutig und muss daher bei der jeweiligen Anwendung fixiert werden. Der nächste Satz gibt eine Aussage über das Ausmaß der Mehrdeutigkeit.

Satz 2.10.1. *Es sei $p = \mathrm{char}(K)$ und $\alpha \in K^* = K - \{0\}$. Für ein $n \in \mathbb{N}$ sei $n = k \cdot p^e$ mit $p \not| k$, falls $p \neq 0$ oder $n = k$ für $p = 0$ ist. Ferner sei L ein Zerfällungskörper von $X^n - \alpha$ über K und $\sqrt[n]{\alpha} \in L$ fest gewählt. Dann enthält L alle k- ten Einheitswurzeln, und sämtliche verschiedenen n-ten Wurzeln von α über K liegen in L und sind durch $\sqrt[n]{\alpha} \cdot \zeta^j$ für $j = 0, \ldots, k-1$ gegeben, wobei ζ eine primitive k- te Einheitswurzel in L bezeichne. Insbesondere ist $L = K(\sqrt[n]{\alpha}, \zeta)$.*

Beweis. Es sei $\beta = \sqrt[n]{\alpha}$. Da das Polynom $f(X) = X^n - \alpha \in K[X]$ in $L[X]$ linear zerfällt, tut es auch

$$\alpha^{-1} \cdot f(\beta X) = X^n - 1.$$

Nach Satz 2.8.1 sind die verschiedenen Nullstellen von $X^n - 1$ durch ζ^j mit $j = 0, \ldots k-1$ (für eine primitive k- te Einheitswurzel $\zeta \in L$) gegeben, die damit sämtlich in L liegen. Folglich sind die Nullstellen von $f(X)$ die Elemente $\beta \cdot \zeta^j$. □

Aus der Schule kennt man bereits die Lösungsformel für die quadratische Gleichung. Das Polynom $f(X) = a_2X^2 + a_1X + a_0 \in R[X]$ hat die Nullstellen

$$\alpha_{1,2} = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_2}.$$

Die Nullstellen liegen also in der Radikalerweiterung $\mathbb{R}(\sqrt{D})$ von $\mathbb{R}$, wobei D die Diskriminante $D = a_1^2 - 4a_0a_2$ ist. Der Körper $\mathbb{R}(\sqrt{D})$ ist der Zerfällungskörper von $f(X)$ über $\mathbb{R}$. Dies motiviert die folgende

Definition 2.10.2. Eine Erweiterung L/K mit $L = K(\sqrt[m]{\beta})$ für $m \in \mathbb{N}$ und ein $\beta \in K$ heißt Radikalerweiterung. Es sei $f(X)$ ein nicht konstantes Polynom aus $K[X]$ und L ein Zerfällungskörper von $f(X)$ über K. Man nennt $f(X)$ auflösbar über K, wenn es eine Erweiterung M/L gibt, für die eine endliche aufsteigende Folge $K = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M$ von Unterkörpern $M_j \subseteq M$ existiert, so dass $M_{j+1} = M_j(\sqrt[m_j]{\beta_j})$ für $m_j \in \mathbb{N}$ und $\beta_j \in M_j$ gilt.
Ist zudem für jedes j das Radikal $\sqrt[m_j]{\beta_j}$ über M_j irreduzibel, so heißt $f(X)$ durch irreduzible Radikale auflösbar.

Satz 2.10.2. *Es sei $n \in \mathbb{N}$ mit $\mathrm{char}(K) \not| n$ mit einem Körper K, der die n- ten Einheitswurzeln enthält. Dann gilt:*

i) Ist $L = K(\sqrt[n]{\beta})$ für ein $\beta \in K$, so ist L/K galoissch und $G(L/K)$ zyklisch. Weiter gilt $|G(L/K)| = m$ mit $m|n$. Es gilt genau dann $m = n$, wenn $\sqrt[n]{\beta}$ über K irreduzibel ist.

ii) Ist umgekehrt L/K galoissch mit zyklischer Galoisgruppe $G(L/K)$ der Ordnung n, so gibt es $\beta \in K$ mit $L = K(\sqrt[n]{\beta})$.

Zum Beweis dieses Satzes benötigen wir

Satz 2.10.3. *(Unabhängigkeitssatz)*
Es seien M und K Körper, $n \in \mathbb{N}$ sowie $\sigma_1, \ldots, \sigma_n \colon M \to K$ paarweise verschiedene Monomorphismen von Ringen. Dann gibt es zu jedem n- tupel $\vec{a} = (a_1, \ldots, a_n) \in K^n - \{\vec{0}\}$ ein $\alpha \in M$ mit

$$\sum_{j=1}^{n} a_j \cdot \sigma_j(\alpha) \neq 0_K.$$

Anders formuliert: aus verschiedenen Monomorphismen $\sigma_1, \ldots, \sigma_n$ lässt sich nicht die Nullabbildung kombinieren, sie sind über K linear unabhängig.

Beweis. Wir nehmen an, die Behauptung sei falsch, etwa mit einem nichttrivialen $\vec{a} \in K^n$ und (nach geeigneter Umnummerierung) einem $r \leq n$, so dass

$$\sum_{j=1}^{r} a_j \sigma_j(\alpha) = 0 \tag{1}$$

für alle $\alpha \in M$ gilt, d. h. die a_j kombinieren aus den σ_j die Nullabbildung. Es sei $r \leq n$ minimal mit dieser Eigenschaft. Zunächst ist $r \geq 2$, denn ansonsten wäre $a_1\sigma_1(\alpha) = 0$, also $\alpha = 0$. Es ist $\sigma_1 \neq \sigma_r$, es gibt also ein $\beta \in M$ mit $\sigma_1(\beta) \neq \sigma_r(\beta)$. Ersetzen wir α in (1) durch $\beta\alpha$, so folgt

$$a_1\sigma_1(\beta)\sigma_1(\alpha) + \ldots + a_r\sigma_r(\beta)\sigma_r(\alpha) = 0. \tag{2}$$

Wir multiplizieren (1) mit $\sigma_r(\beta)$, subtrahieren das Ergebnis von (2) und erhalten

$$a_1(\sigma_1(\beta) - \sigma_r(\beta)\sigma_1(\alpha) + \ldots + a_{r-1}(\sigma_{r-1}(\beta) - \sigma_r(\beta))\sigma_{r-1}(\alpha) + \underbrace{a_r(\sigma_r(\beta) - \sigma_r(\beta))\sigma_r(\alpha)}_{=0} = 0. \tag{3}$$

für alle $\alpha \in M$. Wegen $a_1(\sigma_1(\beta) - \sigma_r(\beta)) \neq 0$ widerspricht dies der Minimalität von r. □

Beweis. (Beweis von Satz 2.10.2)
Es sei ζ_n eine primitive n- te Einheitswurzel in K.

i) OBdA sei $\beta \neq 0$. In $L[X]$ haben wir die Zerlegung

$$X^n - \beta = (X - \sqrt[n]{\beta}\zeta_n^0) \cdot (X - \sqrt[n]{\beta}\zeta_n^1) \cdots (X - \sqrt[n]{\beta}\zeta_n^{n-1}).$$

Dann ist L ein Zerfällungskörper des seperablen Polynoms $X^n - \beta$ über K, also ist L/K galoissch. Da die Konjugierten von $\sqrt[n]{\beta}$ über K die Nullstellen von $X^n - \beta$ sind, folgt nun $G(L/K) = \{\sigma_1, \ldots, \sigma_m\}$ mit

$$\sigma_j(\sqrt[n]{\beta}) = \sqrt[n]{\beta} \cdot \eta_j$$

mit m verschiedenen n- ten Einheitswurzeln $\eta_j \in K$. Wir betrachten den Momonorphismus

$$\Phi = \begin{cases} G(L/K) \to E^{(n)} \\ \sigma_j \to \eta_j. \end{cases}$$

Die Injektivität von Φ ist klar. Die Relationstreue folgt aus

$$(\sigma_j \circ \sigma_k)(\sqrt[n]{\beta}) = \sigma_j(\sqrt[n]{\beta} \cdot \eta_k) = \sigma_j(\sqrt[n]{\beta}) \cdot \eta_k = \sqrt[n]{\beta} \cdot \eta_j \cdot \eta_k$$

und damit

$$\Phi(\sigma_j \circ \sigma_k) = \eta_j\eta_k = \Phi(\sigma_j)\Phi(\sigma_k).$$

Somit ist $G(L/K)$ zu einer Untergruppe der zyklischen Gruppe $E^{(n)}$ isomorph. Damit ist $G(L/K)$ zyklisch mit Ordnung $m|n$. Es gilt ferner

$$\sqrt[n]{\beta} \text{ irreduzibel} \Leftrightarrow X^n - \beta \in K[X] \text{ irreduzibel} \Leftrightarrow X^n - \beta = m_K(\sqrt[n]{\beta}, X)$$

mit $\deg(X^n - \beta) = n$ und $\deg(m_K(\sqrt[n]{\beta}, X)) = [L\colon K] = |G(L/K)| = m$. Das Minimalpolynom ist separabel, also ist $\sqrt[n]{\beta}$ genau dann irreduzibel, wenn $m = n$ gilt.

ii) Es sei L/K galoissch und $G(L/K) = \langle\sigma\rangle$ zyklisch vom Grad n. Für $\alpha \in L$ betrachten wir die Langrangesche Resolvente

$$\vartheta = \vartheta(\alpha) = \alpha + \zeta_n\sigma(\alpha) + \zeta_n^2\sigma^2(\alpha) + \ldots + \zeta_n^{n-1}\sigma^{n-1}(\alpha).$$

Nach dem Unabhängigkeitssatz gibt es $\alpha_0 \in L$ mit $\vartheta(\alpha_0) \neq 0$. Wir setzen $\vartheta_0 = \vartheta(\alpha_0)$. Dann ist

$$\vartheta_0 = \alpha_0 + \zeta_n\sigma(\alpha_0) + \ldots + \zeta_n^{n-1}\sigma^{n-1}(\alpha_0).$$

bzw.

$$\sigma(\vartheta_0) = \sigma(\alpha_0) + \zeta_n\sigma^2(\alpha_0) + \ldots + \zeta_n^{n-1}\sigma^n(\alpha_0) = \zeta_n^{-1}\vartheta_0$$

wegen $\sigma^n(\alpha_0) = \alpha_0$ und $\zeta_n^n = 1$. Es folgt induktiv $\sigma^k(\vartheta_0) = \zeta_n^{-k}\vartheta_0$. Also gilt

$$\sigma^k(\vartheta_0) = \vartheta_0 \Leftrightarrow n|k \Leftrightarrow \sigma^k = id$$

und damit $K(\vartheta_0) = L^{\langle\sigma^n\rangle} = L^{\{id\}} = L$. Für $\beta = \vartheta_0^n$ gilt

$$\sigma^k(\beta) = \sigma^k(\vartheta_0)^n = (\zeta_n^{-k}\vartheta_0)^n = \vartheta_0^n = \beta$$

für $k = 0, \ldots, n$. Also gilt $\beta \in L^{G(L/K)} = K$ und $L = K(\sqrt[n]{\beta})$.

□

Zum Verständnis der folgenden Definition machen wir folgende Vorbemerkungen: Es sei $f(X) \in K[X]$ ein separables Polynom und L ein Zerfällungskörper von $f(X)$ über K mit dem Zerfall

$$f(X) = (X - \alpha_1)\cdots(X - \alpha_n) \in L[X]$$

und der Nullstellenmenge $\mathcal{N} = \{\alpha_1, \ldots, \alpha_n\}$. Für ein $\sigma \in G(L/K)$ ist die Restriktion $\sigma_{|_\mathcal{N}}$ offenbar eine Permutation von $\mathcal{N}$, d.h. bis auf Isomorphie von der symmetrischen Gruppe S_n. Die Abbildung

$$\Phi = \begin{cases} G(L/K) \to S(\mathcal{N}) \\ \sigma \to \sigma_{|_\mathcal{N}} \end{cases}$$

ist ein Homomorphismus von Gruppen. Das Bild $\Phi(G(L/K)) =: G'(L/K)$ ist eine Untergruppe der vollen Permutationsgruppe $S(\mathcal{N}) \cong S_n$. Die Gruppen $G'(L/(K)$ (bzw. $G(L/K)$) operieren von links auf $\mathcal{N}$, womit $\mathcal{N}$ disjunkte Vereinigung seiner Bahnen ist.

Definition 2.10.3. Es sei $f(X) \in K[X]$ separabel sowie L ein Zerfällungskörper von $f(X)$ über K. Unter der Galoisgruppe von $f(X)$ über K (Schreibweise $G(f, K)$) versteht man die Gruppe $G(L/K)$ oder die ihr zugeordnete Permutationsgruppe $G'(L/K)$ der Nullstellenmenge von $f(X)$ in L.

Der nächste Satz enthüllt einige Eigenschaften von $G'(L/K)$:

Satz 2.10.4. *Es sei $f(X) \in K[X]$ normiert und separabel mit $\deg(f) = n > 0$ und der Nullstellenmenge $\mathcal{N} \subset L$ in einem Zerfällungskörper L von $f(X)$ über K. Dann gilt:*

i) Es ist $|G(L/K)|$ ein Teiler von $n!$.

ii) Es ist $G'(L/K)$ die Menge aller Permutationen $\sigma \in S(\mathcal{N})$ mit folgender Eigenschaft: Für ein beliebiges Polynom $h(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ gilt

$$h(\alpha_1, \ldots, \alpha_n) = 0 \Rightarrow h(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = 0.$$

iii) Ist $\mathcal{N} = \{\beta_1, \ldots, \beta_r\}\dot\cup\{\gamma_1, \ldots, \gamma_s\}\dot\cup\ldots$ die Zerlegung von $\mathcal{N}$ in Bahnen unter $G'(L/K)$, so ist $f(X) = g_1(X)g_2(X)\cdots$ mit

$$g_1(X) = (X - \beta_1)\cdots(X - \beta_r), \quad g_2(X) = (X - \gamma_1)\cdots(X - \gamma_s), \quad \ldots$$

die Zerlegung von $f(X)$ in irreduzible normierte Faktoren in $K[X]$. Insbesondere ist $f(X)$ genau dann in $K[X]$ irreduzibel, wenn $\mathcal{N}$ genau eine Bahn enthält. Man sagt dann, dass $G(L/K)$ bzw. $G'(L/K)$ transitiv auf $\mathcal{N}$ operiert.

Beweis. i) Wegen $G'(L/K) \leq S_n$ ist dies klar.

ii) Jedes $\sigma \in G(L/K)$ hat die genannte Eigenschaft wegen der Relationstreue bzgl. Addition und Multiplikation. Es sei nun umgekehrt $\sigma \in S(\mathcal{N})$ beliebig, so dass die Nullstelleneigenschaft unter Anwendung von σ in jedem n- stelligen Polynom $h(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ erhalten bleibt. Es ist noch zu zeigen, dass es einen K- Automorphismus $\tau \in G(L/K)$ mit $\tau_{|\mathcal{N}} = \sigma$ gibt. Da der Zerfällungskörper L von den Nullstellen $\alpha_1, \ldots, \alpha_n$ erzeugt wird, gibt es für jedes $\beta \in L$ ein Polynom $h_\beta(X_1, \ldots, X_n)$ über K mit $h_\beta(\alpha_1, \ldots, \alpha_n) = \beta$. Das gesuchte τ definieren wir wie über

$$\tau(\beta) := \tau(h_\beta(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))).$$

Dadurch wird die Wirkung der Permutation σ auf den Erzeugern auf L fortgesetzt. Es ist allerdings noch zu zeigen, dass die Definition unabhängig von der Wahl des Polynoms h_β zu β ist. Es seien also h_β und h'_β jeweils n- stellig über K mit $\beta = h_\beta(\alpha_1, \ldots, \alpha_n) = h'_\beta(\alpha_1, \ldots, \alpha_n)$. Dann ist die Differenz $d = h_\beta - h'_\beta$ ein n- stelliges Polynom mit $d(\alpha_1, \ldots, \alpha_n) = 0$. Nach der Wahl von σ ist auch $d(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = 0$, also $\tau(\beta) = h_\beta(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = h'_\beta(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$, d.h. die Definition ist gerechtfertigt. Die Relationstreue von τ folgt aus der Relationstreue der Zuordnung $K[X_1, \ldots, X_n] \to L$, $h \to h(\alpha_1, \ldots, \alpha_n)$ bzgl. der Addition und der Multiplikation. Es sei nun $|\langle\sigma\rangle| = m$. Dann gilt auch $\tau^m(\alpha) = h_\alpha(\sigma^m(\alpha_1), \ldots, \sigma^m(\alpha_n)) = h_\alpha(\alpha_1, \ldots, \alpha_n) = \alpha$, also $\tau^m = id$, d.h. die Abbildung τ^{m-1} ist das Inverse zu τ bzgl. der Operation $\circ$. Jedes $\alpha \in K$ wird durch das konstante Polynom $h_\alpha(X_1, \ldots, X_n) = \alpha$ dargestellt, woraus die K- Linearität von τ folgt. Ebenso wird jedes α_j durch $h_j(X_1, \ldots, X_n) = X_j$ dargestellt, woraus $\tau_{|\mathcal{N}} = \sigma$ folgt. Insgesamt ist τ ein K- Automorphismus von L.

iii) Es ist zu zeigen, dass $g_1(X)$, $g_2(X)$, etc. irreduzible Polynome in $K[X]$ sind. Wir dürfen uns auf $g_1(X)$ beschränken: durch jedes $\tau \in G(L/K)$ werden die Nullstellen $\beta_1, \ldots, \beta_r$ permutiert, also $g_1(X) \in L^{G(L/K)}[X] = K[X]$. Angenommen, es ist $g_1(X) = g(X)g'(X)$ eine Zerlegung in $K[X]$ mit $\deg(g(X)) \geq 1$, dann ist $g(\beta_j) = 0$ für mindestens eine Nullstelle β_j von $g_1(X)$. Wegen $g^\sigma(X) = g(X)$ sind dann aber auch alle anderen Elemente der Bahn $\{\beta_1, \ldots, \beta_r\}$ Nullstellen von $g(X)$, woraus $\deg(g'(X)) = 0$ folgt, d.h. $g_1(X)$ ist irreduzibel.

□

Satz 2.10.5. *Es sei $m \in \mathbb{N}$, $\mathrm{char}(K) \not| m$ und L/K eine galoissche Erweiterung mit $L^{(m)} \subseteq L$. Ferner sei $\beta \in L$ und $\beta_1, \ldots, \beta_r$ ein volles System von Konjugierten zu β über K in L. Dann ist*

$$M = L(\sqrt[m]{\beta_1}, \ldots, \sqrt[m]{\beta_r})$$

eine Galoiserweiterung von K.

Beweis. Ohne Einschränkung sei $\beta \neq 0$. Der Körper M ist Zerfällungskörper des Polynoms

$$h(X) = (X^m - \beta_1) \cdots (X^m - \beta_r) \in L[X]$$

über L. Zunächst ist $h(X)$ separabel, da seine Nullstellen die paarweise verschiedenen Elemente $\zeta_m^k \sqrt[m]{\beta_j}$ für $1 \leq j \leq r$ und $1 \leq k \leq m$ mit einer primitiven m- ten Einheitswurzel $\zeta_m \in L$ sind. Wir zeigen zunächst $h(X) \in K[X]$. Dazu sei $L' = K(\beta_1, \ldots, \beta_r)$, womit L' Zerfällungskörper des separablen Polynoms $m_K(\beta, X) \in K[X]$ und damit nach Satz 2.7.1 über K galoissch ist. Es sei $\sigma \in G(L'/K)$ und

$$h(X) = \sum_{j=0}^{r} a_j X^{jm}$$

mit $a_j \in L'$.

Dann gilt

$$h^{(\sigma)}(X) = \sum_{j=0}^{r} \sigma(a_j) X^{jm} = (X^m - \sigma(\beta_1)) \cdots (X^m - \sigma(\beta_r)) = (X^m - \beta_1) \cdots (X^m - \beta_r) = h(X),$$

da σ das Konjugiertensystem der β_j nur permutiert. Es folgt $\sigma(a_j) = a_j$ bzw. $a_j \in L'^{G(L'/K)} = K$. Also ist M Zerfällungskörper des separablen Polynoms $h(X) \in K[X]$ über K und folglich dann nach Satz 2.7.1 galoissch. □

Wir kommen nun zum 1. Hauptkriterium. Obwohl es unter allgemeineren Voraussetzungen gilt, behandeln wir es der Einfachheit halber nur für Körper der Charakteristik null.

Satz 2.10.6. *(1. Hauptkriterium)*
Es sei K ein Körper mit $\mathrm{char}(K) = 0$. *Ist ein separables Polynom $f(X) \in K[X]$ über K auflösbar, so ist $G(f, K)$ im Sinne von Definition 2.9.1 (ii) auflösbar.*

Beweis. Es sei L ein Zerfällungskörper von $f(X)$ über K. Wir beweisen die Auflösbarkeit von $G(L/K) = G(f, K)$. Nach Definition 2.10.2 bedeutet die Auflösbarkeit von $f(X)$ über K die Existenz einer Erweiterung M/L und einer endlichen Körperkette

$$K = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M \tag{1}$$

mit $M_{j+1} = M_j(\sqrt[m_j]{\beta_j})$ mit $\beta_j \in M_j$ und $m_j \in \mathbb{N}$. Diese Kette wird in zwei Schritten derart abgeändert, so dass Satz 2.10.2 über zyklische Erweiterungen angewendet werden kann, und das Endglied über K galoissch ist.

1. Schritt:
Um Satz 2.10.2 anwenden zu können, führen wir in die Körperkette (1) die nötigen Einheitswurzeln ein. Dazu sei $m = m_0 \cdot m_1 \cdots m_{r-1}$ und ζ_m eine primitive m- te Einheitswurzel über M. Mit der Abkürzung $L_j = M_j(\zeta_m)$ wird aus (1) die Kette

$$K \subseteq K(\zeta_m) = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r \tag{2}$$

mit $L_{j+1} = L_j(\sqrt[m_j]{\beta_j})$ und $\beta_j \in L_j$.

2. Schritt:
Wir erweitern die Körperkette (2) derart, dass ihr Endglied über K galoissch wird. Dabei wird induktiv jedes L_j durch ein $L'_j \supseteq L_j$ ersetzt, so dass L'_j/K galoissch ist. Im Fall $j = 0$ ist $L'_0 = L_0$ über K schon galoissch. Andernfalls sei L'_j/K bereits galoissch, und wir adjungieren zu L'_j sukzessive m_j- te Wurzeln von $\beta_j^{(k)}$ für $k = 1, \ldots, n_j$, wobei $\beta_j^{(1)} = \beta_j$ ist und $\beta_j^{(k)}$ sämtliche Konjugierten von β_j über K in L'_j bezeichnet. Dabei liegen diese auch wirklich in L'_j, da dieser Körper nach Konstruktion über K normal ist. Wir setzen

$$L'_{j,d} = L'_j\left(\sqrt[m_j]{\beta_j^{(1)}}, \ldots, \sqrt[m_j]{\beta_j^{(d)}}\right)$$

bzw. $L'_{j+1} = L'_{j,n_j}$ und erhalten die Kette

$$\ldots \subseteq L'_j \subseteq L'_{j,1} \subseteq L'_{j,2} \subseteq \ldots \subseteq L'_{j,n_j-1} \subseteq L'_{j+1} \subseteq L'_{j+1,1} \subseteq \ldots, \tag{3}$$

wobei nach Satz 2.10.5 die Erweiterungen L'_j/K galoissch sind. Damit ist auch jeweils $L'_{j+1}/L'_{j,k}$ für alle k galoissch. Dieser Körperfolge entspricht nach dem Hauptsatz der Galoistheorie die Folge von Gruppen

$$G(L'_{j+1}/L'_j) \triangleright G(L'_{j+1}/L'_{j,1}) \triangleright G(L'_{j+1}/L'_{j,2}) \triangleright \ldots \triangleright G(L'_{j+1})/L'_{j,n_j-1}) \triangleright G(L'_{j+1}/L'_{j+1}) \cong \{1\}. \tag{4}$$

Nach dem Hauptsatz der Galoistheorie und Satz 2.10.2 sind die Faktoren

$$G(L'_{j+1}/L'_{j,d})/G(L'_{j+1}/L'_{j,d+1}) \cong G(L'_{j,d+1}/L'_{j,d})$$

sämtlich zyklisch. Nach Definition 2.9.1 (ii) ist $G(L'_{j+1}/L'_j)$ für alle j auflösbar. Die Körperkette (2) ist also durch die Kette (3) mit

$$K \subseteq L'_0 \subseteq L'_1 \subseteq \ldots \subseteq L'_j \subseteq L'_{j+1} \subseteq \ldots \subseteq L'_r \tag{5}$$

ersetzt worden, wobei L'_j/K jeweils galoissch und $G(L'_{j+1}/L'_j)$ auflösbar ist. Der Kette (5) entspricht die Folge der Galoisgruppen

$$G(L'_r/K) \triangleright G(L'_r/L'_0) \triangleright G(L'_r/L'_1) \triangleright \ldots \triangleright G(L'_r/L'_r) \cong \{1\}. \tag{6}$$

Nach Satz 2.9.5 (ii) sind die Faktoren

$$G(L'_r/L'_j)/G(L'_r/L'_{j+1}) \cong G(L'_{j+1}/L'_j)$$

sämtlich auflösbar. Das Startglied $G(L'_r/K)/G(L'_r/L_0) \cong G(L'_0/K)$ ist zyklisch, also trivial oder auflösbar. Wiederholte Anwendung von Satz 2.9.7 ergibt, dass die Gruppe $G(L'_r/K)$ auflösbar ist. Nach Satz 2.9.3 (i) ist $G(f,K) = G(L/K)$ auflösbar. □

Zum Beweis des zweiten Hauptkriteriums, der Umkehrung des 1. Hauptkriteriums, benötigen wir als Vorbereitung folgenden Satz:

Satz 2.10.7. *Es sei L/K galoissch, sowie M eine Erweiterung von K, die mit L einen gemeinsamen Oberkörper besitzt. Dann ist $L(M)/M$ galoissch und $G(L(M)/M)$ zu einer Untergruppe von $G(L/K)$ isomorph.*

Beweis. Da L/K galoissch ist, ist $L = K(\alpha_1, \ldots, \alpha_n)$ Zerfällungskörper eines Polynoms $f \in K[X]$ mit $f(X) = (X - \alpha_1) \cdot (X - \alpha_2) \cdots (X - \alpha_n)$. Es gilt auch $f \in M(X)$ mit $L(M) = M(\alpha_1, \ldots, \alpha_m)$, d.h. $L(M)$ ist Zerfällungskörper von $L(M)$ über M. Jeder M- Automorphismus σ von $L(M)$ ist auch ein K- Automorphismus von $L(M)$. Die Einschränkung $\sigma_{|_L}$ ist ein K- Automorphismus von L. Da L/K galoissch ist, ist $\sigma_{|_L}$ ein K- Automorphismus von L. □

Bei der Formulierung des zweiten Hauptkriteriums beschränken wir uns wieder auf den Fall der Charakteristik null.

Satz 2.10.8. *(2. Hauptkriterium)*
Es sei $f(X)$ ein separables Polynoms in $K[X]$ mit $\mathrm{char}(K) = 0$*, so dass $G(f,K)$ auflösbar nach Definition 2.9.2 (ii) ist. Dann ist $f(X)$ über K auflösbar.*

Bemerkung 2.10.1. Mit etwas mehr Aufwand lässt sich zeigen, dass $f(X)$ über K dann sogar durch irreduzible Radikale auflösbar ist.

Beweis. Es sei L ein Zerfällungskörper von $f(X)$ über K und $|G(f,K)| = m$ sowie ζ_m eine primitive m- te Einheitswurzel über L. Es sei $K' = K(\zeta_m)$ bzw. $L' = L(\zeta_m)$. Nach Satz 2.10.7 ist L'/K' galoissch, und die Gruppe $G_0 = G(L'/K')$ ist isomorph zu einer Untergruppe von $G(L/K) = G(f,K)$. Nach Satz 2.9.3 (i) ist G_0 auflösbar und besitzt daher nach Satz 2.9.5 eine Normalreihe

$$G_0 \triangleright G_1 \triangleright \ldots \triangleright G_r \cong \{1\}.$$

deren Faktoren sämtlich zyklisch und von Primzahlordnung sind, wobei wir ohne Einschränkung $|G_0| > 1$, also $L' \neq K'$ annehmen.

Es bezeichne nun

$$K' = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = L'$$

die Reihe der zugehörigen Fixkörper in L'. Nach dem Satz 2.7.5 (ii) ist für $0 \leq j \leq r-1$ die Erweiterung K_{j+1}/K_j galoissch und

$$G(K_{j+1}/K_j) \cong G_j/G_{j+1}$$

zyklisch von Primzahlordnung, also etwa $|G(K_{j+1}/K_j)| = p_j$. Für alle j gibt es nach Satz 2.10.2 jeweils ein $\beta_j \in K_j$ mit $K_{j+1} = K_j(\sqrt[p_j]{\beta_j})$. Nach Definition 2.10.2 ist damit $f(X)$ über K auflösbar. □

Das 1. und 2. Hauptkriterium lassen sich folgendermaßen zusammenfassen:

Satz 2.10.9. *(Hauptsatz über die Auflösbarkeit von Polynomen)*
Es sei $\mathrm{char}(K) = 0$ *und* $f(X) \in K[X]$ *separabel. Dann gilt:*

$$f(X) \text{ ist über } K \text{ auflösbar (Definition 2.10.2)} \quad \Leftrightarrow \quad G(f,K) \text{ ist auflösbar (Definition 2.9.1).}$$

Kapitel 3

Moduln

3.1 Grundlegende Definitionen

Im folgenden sei R stets ein kommutativer Ring mit Einselement.

Definition 3.1.1. Ein R- Modul M ist eine abelsche Gruppe, deren Verknüpfung mit $+$ bezeichnet wird, zusammen mit einer skalaren Multiplikation $R \times M \to M$, $(r, m) \to rm$, für die

(M1) $1m = m$ (Unitarität)

(M2) $(rs)m = r(sm)$ (Assoziativgesetz)

(M3) $(r + s)m = rm + sm$ (1. Distributivgesetz)

(M4) $r(m + m') = rm + rm'$ (2. Distributivgesetz)

Beispiel 3.1.1. Der Modulbegriff ist eine Verallgemeinerung des Vektorraumbegriffs. Ist R ein Körper, so sind die R- Module gerade die Vektorräume über R.

Beispiel 3.1.2. Für $n \in \mathbb{N}$ ist $R^n = \{(r_1, \ldots, r_n) \colon r_j \in R\}$ mit der offensichtlichen Addition und Skalarmultiplikation ein R- Modul.

Beispiel 3.1.3. Es sei $(G, +)$ eine abelsche Gruppe. Dann wird G zu einem $\mathbb{Z}$- Modul, wenn die Skalarmultiplikation $\mathbb{Z} \times G \to G$, $(n, g) \to ng$ durch

$$ng = \underbrace{g + \ldots + g}_{n-\text{mal}}$$

für $n > 0$ und $ng = -(ng)$ für $n < 0$ sowie $0g = 0$ definiert ist.

Definition 3.1.2. Es sei M ein R- Modul. Eine Teilmenge $N \subset M$ heißt Untermodul von M (Schreibweise: $N \leq M$), wenn N bzgl. der auf M gegebenen Addition und Skalarmultiplikation ebenfalls ein R- Modul ist.

Beispiel 3.1.4. Es sei $M = R$ als R- Modul über sich selbst. Dann sind die Untermodule von R gerade die Ideale von R.

Definition 3.1.3. Es sei M ein R- Modul. Eine Teilmenge $\mathcal{M} \subset M$ heißt Erzeugendensystem eines Untermoduls N, falls

$$M = \bigcap_{\substack{\mathcal{M} \subset N \\ N \leq M}} N.$$

Wir schreiben $N = (\mathcal{M})$. Ist $\mathcal{M} = \{m\}$, so schreiben wir auch $N = (m)$ statt $N = (\{m\})$.

Definition 3.1.4. Es seien M und N zwei R- Moduln.
Eine Abbildung $\varphi\colon M \to N$ heißt (R- Modul)- Homomorphismus, wenn $\varphi(v+w) = \varphi(v) + \varphi(w)$ und $\varphi(rv) = r \cdot \varphi(v)$ für alle $v, w \in M$ und alle $r \in R$ gilt. Ein bijektiver Homomorphismus heißt Isomorphismus. Die Moduln M und N heißen isomorph, falls ein Isomorphismus $\psi\colon M \to N$ existiert. Die Menge $\operatorname{Kern}(\varphi) := \{v \in M\colon \varphi(v) = 0\}$ heißt der Kern von φ, und $\varphi(M) := \{\varphi(m)\colon m \in M\}$ heißt das Bild von φ.

Satz 3.1.1. *Es sei $\varphi\colon M \to N$ ein Homomorphismus. Dann ist $\operatorname{Kern}(\varphi)$ ein Untermodul von M und $\varphi(M)$ ein Untermodul von N.*

Beweis. Durch Nachprüfen der Moduleigenschaften. □

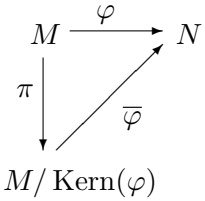
Bemerkung 3.1.1. Ist R ein Körper und M und N damit Vektorräume über R, so sind die Begriffe R- Modulhomomorphismus und lineare Abbildung äquivalent.

Definition 3.1.5. Es sei N ein Untermodul eines R- Moduls M.
Der Restklassen- oder Faktormodul M/N ist die additive Gruppe der Nebenklassen $\overline{v} := v+N$. Diese Menge wird durch $r\overline{v} = \overline{rv}$ ein R- Modul.

Satz 3.1.2. *i) Die in Definition 3.1.4 definierte Skalarmultiplikation ist wohldefiniert und macht $\overline{M} = M/N$ zu einem R- Modul.*

ii) Es ist $\pi\colon M \to \overline{M}$, $v \to \overline{v}$ ein surjektiver R- Modulhomomorphismus mit $\operatorname{Kern}(\pi) = N$.

iii) Es sei $\varphi\colon M \to N$ ein R- Modulhomomorphismus mit $N \subset \operatorname{Kern}(\varphi)$. Dann gibt es einen eindeutig bestimmten Homomorphismus $\overline{\varphi}\colon M/\operatorname{Kern}(\varphi) \to N$ mit $\varphi = \overline{\varphi} \circ \pi$. Das Diagramm



ist kommutativ.

iv) Isomorphiesatz:
Die Abbildung $\overline{\varphi}$ ist ein Isomorphismus von $M/\operatorname{Kern}(\varphi)$ auf $\varphi(M)$.

v) Es gibt eine bijektive Beziehung zwischen Untermoduln $\overline{U}$ von $M/\operatorname{Kern}(\varphi)$ und Untermoduln U von M, die $\operatorname{Kern}(\varphi)$ enthalten, definiert durch $U = \pi^{-1}(\overline{U})$ und $\overline{U} = \pi(U)$.
Es ist $M/U \cong (M/\operatorname{Kern}(\varphi))/\overline{U}$.

Beweis. ohne Beweis. □

3.2 Matrizen und Determinanten

Definition 3.2.1. Es seien $m, n \in \mathbb{N}$.
Unter $R^{(m,n)}$ verstehen wir die Menge aller Matrizen $\mathcal{A} = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ mit $a_i \in R$.

Der aus der Linearen Algebra bekannte Begriff der Determinante einer quadratischen Matrix über einem Körper kann auf beliebige kommutative Ringe mit Eins übertragen werden. Wir beschreiben nun eine von mehreren Möglichkeiten, den Begriff einzuführen.

Definition 3.2.2. i) Eine Abbildung $f\colon V^n \to R$, $(v_1,\ldots,v_n) \to f(v_1,\ldots,v_n)$ heißt n- fache Multilinearform (auf V), wenn f in jedem Argument linear ist, d.h. es gilt

$$f(v_1,\ldots,sv_j+tw_j,\ldots,v_n) = s\cdot f(v_1,\ldots,v_j,\ldots,v_n) + t\cdot f(v_1,\ldots,w_j,\ldots,v_n)$$

für alle $j\in\{1,\ldots,n\}$, alle $v_1,\ldots,v_n,w_j\in V$ und alle $s,t\in R$.

ii) Sie heißt alternierend, falls $f(v_1,\ldots,v_n)=0$, wenn es $i,j\in\{1,\ldots,n\}$ mit $v_i=v_j$ gibt.

Wie in der Linearen Algebra beweist man folgenden

Satz 3.2.1. *Es sei V ein R- Modul, $n\in\mathbb{N}$ und $f\colon V^n\to R$ eine n- fach alternierende Multilinearform auf V. Dann gibt es $v_1,\ldots,v_n\in V$ und $s\in R$ mit*

i) $f(v_1,\ldots,v_i,\ldots,v_j,\ldots,v_n) = -f(v_1,\ldots,v_j,\ldots,v_i,\ldots,v_n)$, wobei die Elemente an der i- ten und j- ten Stelle vertauscht werden.

ii) $f(v_1,\ldots,v_i+sv_j,\ldots,v_n) = f(v_1,\ldots,v_i,\ldots,v_n)$, falls $i\neq j$.

Beweis. Wie in der Linearen Algebra. □

Satz 3.2.2. *Es sei V ein R- Modul und f eine n- fach alternierende Multilinearform auf V. Weiter sei*

$$\begin{aligned} w_1 &= a_{11}v_1+\ldots+a_{1n}v_n \\ &\vdots \quad\quad \vdots \\ w_n &= a_{n1}v_1+\ldots+a_{nn}v_n \end{aligned}$$

mit $a_{ij}\in R$ und $v_i\in V$. Dann ist

$$f(w_1,\ldots,w_n) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)}\cdots a_{n,\sigma(n)} f(v_1,\ldots,v_n).$$

Beweis. Wir werten

$$f(w_1,\ldots,w_n) = f(a_{11}v_1+\ldots+a_{1n}v_n,\ldots,a_{n1}v_1+\ldots+a_{nn}v_n)$$

aus, indem wir die Linearität in jeder Variablen anwenden. Wir erhalten

$$f(w_1,\ldots,w_n) = \sum_{\tau} a_{1,\tau(1)}\cdots a_{n,\tau(n)} f(v_{\tau(1)},\ldots,v_{\tau(n)}),$$

wobei die Summe über alle Abbildungen $\tau\colon\{1,\ldots,n\}\to\{1,\ldots,n\}$ läuft. Da f alternierend ist, liefern nur die Permutationen unter den τ einen von null verschiedenen Beitrag. Damit gilt

$$f(w_1,\ldots,w_n) = \sum_{\sigma\in S_n} a_{1,\sigma(1)}\cdots a_{n,\sigma(n)} f(v_{\sigma(1)},\ldots,v_{\sigma(n)}).$$

Die Permutation σ kann durch eine gewisse Anzahl ν von Transpositionen τ_j erzeugt werden, wobei $(-1)^\nu = \operatorname{sgn}(\sigma)$ mit $\sigma=\tau_1\circ\ldots\circ\tau_\nu$ gilt. Jede Anwendung einer Transposition τ_j auf die Argumente von f erzeugt einen Faktor -1. □

Bei Determinanten handelt es sich um alternierende Multilinearformen auf R^n.

Definition 3.2.3. Es sei $n \in \mathbb{N}$. Unter einer $n \times n$- Determinante auf R verstehen wir eine Abbildung $\det\colon R^{(n,n)} \to R$ mit den folgenden Eigenschaften:

i) Werden die n Spalten $\vec{a}_1, \ldots, \vec{a}_n$ der Matrix $\mathcal{A} \in R^{(n,n)}$ als Elemente des R^n betrachtet, so ist det eine n- fach alternierende Multilinearform auf R^n.

ii) Für die Einheitsmatrix

$$\mathcal{E}_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

ist $\det \mathcal{E}_n = 1$

Es ist noch nicht klar, ob Determinanten existieren. Aus Satz 3.2.2 folgt jedoch, dass sie im Falle der Existenz eindeutig bestimmt sind.

Satz 3.2.3. *(Leibnizformel)*
Es sei det *eine $n \times n$- Determinante auf R und $\mathcal{A} = (a_{ij})_{1 \le i,j \le n} \in R^{(n,n)}$. Dann ist*

$$\det \mathcal{A} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}.$$

Beweis. Dies folgt durch Anwendung von Satz 3.2.2 mit $f = \det$ und $v_i = (0, \ldots, 1, \ldots, 0)$, wobei der Eintrag 1 in v_i an der i- ten Stelle steht. □

Satz 3.2.4. *Es sei $n \in \mathbb{N}$ und $\mathcal{A} \in R^{(n,n)}$.*

i) Die $n \times n$- Determinante ist eine n- fache alternierende Multilinearform in den Zeilen der Matrix.

ii) Es ist $\det \mathcal{A}^T = \det \mathcal{A}$.

Beweis. Es reicht offenbar, (ii) zu zeigen.
Aus Satz 3.2.3 folgt

$$\det \mathcal{A}^T = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}.$$

Die Substitution $\gamma = \sigma^{-1}$ liefert

$$\det \mathcal{A}^T = \sum_{\gamma \in S_n} \operatorname{sgn}(\gamma) a_{1,\gamma(1)} \cdots a_{n,\gamma(n)}.$$

□

Definition 3.2.4. Es sei $n \in \mathbb{N}$ und $\mathcal{A} \in R^{(n,n)}$. Unter dem Minor $\mathcal{A}_{ij}$ der Matrix $\mathcal{A}$ versteht man die Matrix, die aus $\mathcal{A}$ durch Streichen der i- ten Zeile und j- ten Spalte entsteht (mit $1 \le i, j \le n$). Die Adjungierte von $\mathcal{A}$ (Schreibweise: $\operatorname{Adj} \mathcal{A}$ ist die $n \times n$- Matrix, deren Einträge an der Stelle (i, j) gleich $(\operatorname{Adj})_{ij} = (1)^{i+j} \det \mathcal{A}_{ij}$ ist.

Satz 3.2.5. *(Existenz, Laplacescher Entwicklungssatz)*
Determinanten existieren. Für $n \geq 2$ gilt die Entwicklung nach der i- ten Zeile:

$$\det \mathcal{A} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}.$$

Beweis. Wir beweisen durch Induktion nach n, dass die rechte Seite die in Definition 3.2.3 angegebenen Eigenschaften besitzt:
$\underline{n = 1}$:
Die Funktion $\det\colon \mathbb{R} \to \mathbb{R}$, $a \to \det(a) = a$ hat die gewünschten Eigenschaften.
$\underline{n \to n+1}$:
Wir zeigen zuerst die Linearität in der k- ten Spalte der rechten Seite (für $1 \leq k \leq n$).
Für $j \neq k$ sind die Unterdeterminanten $\det \mathcal{A}_{ij}$ nach Induktionshypothese alle in der k- ten Spalte linear, während die a_{ij} von der k- ten Spalte nicht abhängen. Für $j = k$ sind die a_{ij} linear in der k- ten Spalte, während $\det \mathcal{A}_{ij}$ nicht davon abhängt.
Es bleibt noch zu zeigen, dass die rechte Seite alternierend ist.
Für $1 \leq k < l \leq n$ sei $\vec{a}_k = \vec{a}_l$. Nach Induktionshypothese liefern höchstens die Summanden für $j = k$ und $j = l$ einen von null verschiedenen Beitrag. Da $\mathcal{A}_{ik}$ aus $\mathcal{A}_{il}$ durch $l - k - 1$ Vertauschungen von Spaltenvektoren hervorgeht, gilt $\det \mathcal{A}_{ik} = (-1)^{l+k+1} \det \mathcal{A}_{il}$. Damit gilt

$$(-1)^{i+k} a_{ik} \det \mathcal{A}_{ik} + (-1)^{i+l} a_{il} \det \mathcal{A}_{il} = 0.$$

□

Satz 3.2.6. *(Cramersche Regel)*
Es sei $n \in \mathbb{N}$, $\vec{a}_1, \ldots, \vec{a}_n \in \mathbb{R}^n$ und $\mathcal{A} = (\vec{a}_1, \ldots, \vec{a}_n)$ die Matrix mit den Spalten $\vec{a}_i$. Es sei $\vec{b} = x_1\vec{a}_1 + \ldots + x_n\vec{a}_n$ mit $x_i \in R$ und $\mathcal{A}_i(\vec{b}) = (\vec{a}_1, \ldots, \vec{b}, \ldots, \vec{a}_n)$ mit dem Vektor $\vec{b}$ in der i- ten Spalte. Dann ist $x_i \det \mathcal{A} = \det \mathcal{A}_i(\vec{b})$

Beweis. Es ist

$$\det(\vec{a}_1, \ldots, \vec{b}, \ldots, \vec{a}_n) = \sum_{j=1}^{n} x_j \det(\vec{a}_1, \ldots, \vec{a}_j, \ldots, \vec{a}_n)$$

mit dem Vektor $\vec{a}_j$ an der i- ten Stelle. Für $j \neq i$ verschwinden aber die einzelnen Summanden. □

Satz 3.2.7. *(Determinantenmultiplikationssatz)*
Es sei $n \in \mathbb{N}$ und $\mathcal{A}, \mathcal{B} \in R^{(n,n)}$. Dann gilt $\det(\mathcal{AB}) = \det \mathcal{A} \cdot \det \mathcal{B}$.

Beweis. Für festes $\mathcal{B} \in R^{(n,n)}$ sei $f_{\mathcal{B}}(\vec{a}_1, \ldots, \vec{a}_n) = \det(\mathcal{AB})$. Man prüft leicht nach, dass $f_{\mathcal{B}}$ eine n-fache alternierende Multilinearform ist. Nach Satz 3.2.2 ist

$$f_{\mathcal{B}}(\vec{a}_1, \ldots, \vec{a}_n) = \det \mathcal{A} \cdot f_{\mathcal{B}}(\vec{e}_1, \ldots, \vec{e}_n) = \det \mathcal{A} \cdot \det \mathcal{B}.$$

□

Definition 3.2.5. Es sei $n \in \mathbb{N}$. Es heißt $\mathcal{A} \in R^{(n,n)}$ $\underline{\text{(in } R\text{) invertierbar}}$, wenn es $\mathcal{B} \in R^{(n,n)}$ mit $\mathcal{AB} = \mathcal{E}_n$ gibt.

Satz 3.2.8. *Es sei $n \in \mathbb{N}$. Für $\mathcal{A} \in R^{(n,n)}$ gilt*

$$\mathcal{A} \cdot (\operatorname{Adj} \mathcal{A}) = (\operatorname{Adj} \mathcal{A}) \cdot \mathcal{A} = \det \mathcal{A} \cdot \mathcal{E}_n.$$

Beweis. Nach Definition 3.2.4 und der Definition des Matrixprodukts ist

$$\mathcal{A} \cdot (\operatorname{Adj} \mathcal{A}) = (c_{ik})_{1 \leq i,k \leq n}$$

mit

$$c_{ik} = \sum_{j=1}^{n} a_{ij} \cdot (\operatorname{Adj} \mathcal{A}_{jk}) = \sum_{j=1}^{n} (-1)^{j+k} a_{ij} \det \mathcal{A}_{kj}.$$

Also gilt nach dem Laplaceschen Entwicklungssatz für $i \neq k$

$$c_{ik} = \det \begin{pmatrix} \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \vdots & \ddots & \vdots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \end{pmatrix} = 0,$$

wobei die angegebenen Zeilen die i- te und die k- te darstellen. Für $i = k$ ist $c_{ik} = \det \mathcal{A}$. Dann gilt

$$\mathcal{A} \cdot (\operatorname{Adj} \mathcal{A}) = \det \mathcal{A} \cdot \mathcal{E}_n.$$

Die zweite Gleichung $(\operatorname{Adj} \mathcal{A}) \cdot \mathcal{A} = \det \mathcal{A} \cdot \mathcal{E}_n$ folgt mittels Laplacescher Entwicklung nach Spalten. □

Satz 3.2.9. *Es sei $n \in \mathbb{N}$. Dann ist $\mathcal{A} \in R^{(n,n)}$ genau dann invertierbar, wenn $\det \mathcal{A} \in R^*$ ist. Es gibt genau dann ein $\mathcal{A}^{-1} \in R^{(n,n)}$ mit $\mathcal{A}^{-1}\mathcal{A} = \mathcal{A}\mathcal{A}^{-1} = \mathcal{E}_n$, nämlich*

$$\mathcal{A}^{-1} = (\det \mathcal{A})^{-1} \cdot \operatorname{Adj} \mathcal{A}. \qquad (*)$$

Die Menge der invertierbaren Matrizen im $R^{(n,n)}$ bildet eine Gruppe bzgl. der Matrixmultiplikation mit Einselement $\mathcal{E}_n$.

Beweis. Es sei $\det \mathcal{A} \in R^*$. Dann folgt die Invertierbarkeit von $\mathcal{A}$ und Gleichung $(*)$ aus Satz 3.2.8. Es sei $\mathcal{A}\mathcal{B} = \mathcal{E}_n$. Nach Satz 3.2.6 ist $1 = \det \mathcal{E}_n = \det \mathcal{A} \cdot \det \mathcal{B}$, also $\det \mathcal{A} \in R^*$. Die Assoziativität der Matrixmultiplikation folgt wie in der Linearen Algebra. Damit sind alle Gruppenaxiome erfüllt. Es folgt die Eindeutigkeit von $\mathcal{A}^{-1}$. □

Definition 3.2.6. Es sei $n \in \mathbb{N}$.
Die Gruppe aller invertierbaren Matrizen von $R^{(n,n)}$ wird mit $GL(n, R)$ bezeichnet. Für $\mathcal{A} \in GL(n, R)$ heißt das nach Satz 3.2.9 eindeutig bestimmte $\mathcal{A}^{-1} \in GL(n, R)$ mit $\mathcal{A}^{-1}\mathcal{A} = \mathcal{A}\mathcal{A}^{-1} = \mathcal{E}_n$ die Inverse von $\mathcal{A}$.

3.3 Freie Moduln und Basen

Definition 3.3.1. Es sei V ein R- Modul.
Dann heißt V endlich erzeugt, falls V ein endliches Erzeugendensystem besitzt. Die Vektoren $v_1, \dots, v_n$ heißen linear abhängig (l.a.), falls es $(r_1, \dots, r_n) \in R^n - \{(0, \dots, 0)\}$ gibt, so dass $r_1 v_1 + \dots + r_n v_n = 0$ gilt, andernfalls linear unabhängig (l.u.). Eine Menge $\mathcal{M}$ heißt linear unabhängig, wenn jede endliche Folge $v_1, \dots, v_n$ von verschiedenen $v_i \in \mathcal{M}$ linear unabhängig ist. Ein linear unabhängiges Erzeugendensystem von V heißt Basis von V. Weiter heißt V frei oder freier Modul (über R), falls V eine Basis besitzt.

Beispiel 3.3.1. Ist V ein endlichdimensionaler Vektorraum, d.h. ein endlich erzeugter R- Modul über einem Körper R, so ist aus der Linearen Algebra bekannt, dass V eine Basis besitzt und damit ein freier Modul ist.

Beispiel 3.3.2. Für jeden Ring R und $n \in \mathbb{N}$ ist $R^n = \{(r_1, \ldots, r_n) \colon r_i \in R\}$ ein freier Modul mit der Basis $\mathcal{B} = \{\vec{e}_1, \ldots, \vec{e}_n\}$, wobei $\vec{e}_i = (0, \ldots, 1, \ldots, 0)$ der i- te Einheitsvektor darstellt.

Beispiel 3.3.3. Es sei $(G, +)$ eine endliche abelsche Gruppe. Nach Beispiel 3.1.4 kann G nun als ein $\mathbb{Z}$- Modul aufgefasst werden. Für $g \in G$ ist $|G| \cdot g = 0$, also ist g linear abhängig. Daher besitzt G keine Basis. Der $\mathbb{Z}$- Modul G ist nicht frei.

Bei R- Homomorphismen zwischen freien Moduln mit endlichen Basen kann die aus der Linearen Algebra bekannte Methode der Beschreibung von linearen Abbildungen durch Matrizen angewandt werden.

Definition 3.3.2. Es seien V_1 bzw. V_2 endlich erzeugte Moduln mit Basen $\mathcal{B}_1 = \{\vec{b}_1, \ldots, \vec{b}_n\}$ bzw. $\mathcal{B}_2 = \{\vec{b}'_1, \ldots, \vec{b}'_n\}$. Weiter sei $\Phi \colon V_1 \to V_2$ ein Homomorphismus mit $\Phi(\vec{b}_j) = \sum_{i=1}^{m} a_{ij}\vec{b}'_i$ mit $a_{ij} \in R$. Dann heißt

$$\mathcal{M}(\Phi; \mathcal{B}_1, \mathcal{B}_2) = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

die Darstellungsmatrix von Φ bzgl. der Basen $\mathcal{B}_1$ und $\mathcal{B}_2$.

Wie in der Linearen Algebra beweist man folgenden Satz durch Nachrechnen:

Satz 3.3.1. *Es seien V_1, V_2 und V_3 jeweils R- Moduln mit endlichen Basen $\mathcal{B}_1$, $\mathcal{B}_2$ bzw. $\mathcal{B}_3$. Es seien $\psi \colon V_1 \to V_2$ bzw. $\Phi \colon V_2 \to V_3$ zwei R- Homomorphismen mit Darstellungsmatrizen $\mathcal{M}(\psi; \mathcal{B}_1, \mathcal{B}_2)$ bzw. $\mathcal{M}(\Phi; \mathcal{B}_2, \mathcal{B}_3)$. Dann gilt*

$$\mathcal{M}(\Phi \circ \psi; \mathcal{B}_1, \mathcal{B}_3) = \mathcal{M}(\Phi; \mathcal{B}_2, \mathcal{B}_3) \cdot \mathcal{M}(\psi; \mathcal{B}_1, \mathcal{B}_2).$$

Beweis. Wie in der Linearen Algebra. □

Definition 3.3.3. Es sei V ein endlich erzeugter freier R- Modul und $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$. Für $v \in V$ ist der Koordinatenvektor von v (bzgl. $\mathcal{B}$) das eindeutig bestimmte Element $\vec{\lambda} = (\lambda_1, \ldots, \lambda_n) \in R^n$, für das $v = \lambda_1\vec{b}_1 + \ldots + \lambda_n\vec{b}_n$ gilt.

Satz 3.3.2. *Es sei V ein endlich erzeugter freier R- Modul mit Basis $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$.*

i) Jede Basis von V hat die gleiche Anzahl an Elementen.

ii) Es sei $\mathcal{B}' = \{\vec{b}'_1, \ldots, \vec{b}'_n\}$ mit $\vec{b}'_i = \sum_{j=1}^{n} \alpha_{ij}\vec{b}_j$ und $\mathcal{A} = (\alpha_{ij})_{1 \le i,j \le n}$.
Dann ist $\mathcal{B}'$ genau dann eine Basis von V, wenn $\mathcal{A} \in GL(n, R)$ gilt.

Beweis. Wir beweisen (i). Die Überlegungen dazu werden auch einen Beweis für (ii) ergeben.
Es seien $\mathcal{B}_1 = \{\vec{b}_1, \ldots, \vec{b}_n\}$ und $\mathcal{B}_2 = \{\vec{c}_1, \ldots, \vec{c}_n\}$ zwei Basen von V.
Es sei

$$\begin{aligned} \vec{c}_1 &= \lambda_{1,1}\vec{b}_1 + \ldots + \lambda_{1,n}\vec{b}_n \\ &\vdots \quad\quad \vdots \\ \vec{c}_m &= \lambda_{m,1}\vec{b}_1 + \ldots + \lambda_{m,n}\vec{b}_n. \end{aligned}$$

und

$$\begin{aligned} \vec{b}_1 &= \mu_{1,1}\vec{c}_1 + \ldots + \mu_{1,m}\vec{c}_m \\ &\vdots \quad\quad \vdots \\ \vec{b}_n &= \mu_{n,1}\vec{c}_1 + \ldots + \mu_{n,m}\vec{c}_m. \end{aligned}$$

Es sei

$$\mathcal{L} = \begin{pmatrix} \lambda_{1,1} & \dots & \lambda_{1,n} \\ \vdots & & \vdots \\ \lambda_{m,1} & \dots & \lambda_{m,n} \end{pmatrix} \in R^{(m,n)}$$

und

$$\mathcal{M} = \begin{pmatrix} \mu_{1,1} & \dots & \mu_{1,m} \\ \vdots & & \vdots \\ \mu_{n,1} & \dots & \mu_{n,m} \end{pmatrix} \in R^{(n,m)}.$$

Dann ist

$$\begin{aligned} \vec{b}_1 &= \nu_{1,1}\vec{b}_1 + \ldots + \nu_{1,n}\vec{b}_n \\ \vdots & \quad \vdots \\ \vec{b}_n &= \nu_{n,1}\vec{b}_1 + \ldots + \nu_{n,n}\vec{b}_n. \end{aligned}$$

Es sei

$$\mathcal{N} = \begin{pmatrix} \nu_{1,1} & \dots & \nu_{1,n} \\ \vdots & & \vdots \\ \nu_{n,1} & \dots & \nu_{n,n} \end{pmatrix}.$$

Dann folgt $\mathcal{N} = \mathcal{M} \cdot \mathcal{L}$. Wegen der Basiseigenschaft der $\vec{b}_j$ folgt $\mathcal{M} \cdot \mathcal{L} = \mathcal{N} = \mathcal{E}_n$.
Wir nehmen nun $m \neq n$ an. Dazu sei O.B.d.A. $m < n$. Wir können $\mathcal{L}$ bzw. $\mathcal{M}$ zu quadratischen Matrizen

$$\tilde{\mathcal{L}} = \begin{pmatrix} \mathcal{L} \\ 0 \end{pmatrix} \quad \text{bzw.} \quad \tilde{\mathcal{M}} = \begin{pmatrix} \mathcal{M} & 0 \end{pmatrix}$$

ergänzen, indem wir sie durch Nullzeilen oder Nullspalten auffüllen. Es ist dann auch $\tilde{\mathcal{M}} \cdot \tilde{\mathcal{L}} = \mathcal{E}_n$ in Widerspruch zu Satz 3.2.9, da $\det \tilde{\mathcal{L}} = \det \tilde{\mathcal{M}} = 0$ gilt. Also ist $m = n$ und $\mathcal{L} = \mathcal{M}^{-1}$ mit $\mathcal{L}, \mathcal{M} \in GL(n, V)$. □

Definition 3.3.4. Es sei V ein freier R- Modul.

i) Es sei V endlich erzeugt. Die nach Satz 3.3.2 von der Basis unabhängige Anzahl der Basiselemente von V heißt der Rang von V (Schreibweise: $\operatorname{rg} V$).

ii) Ist V nicht endlich erzeugt, so ist $\operatorname{rg} V = \infty$.

Bemerkung 3.3.1. Ist V ein Modul über einem Körper, also ein Vektorraum, so ist, wie aus der Linearen Algebra bekannt ist, die Bezeichnung "Dimension" üblich. Aus historischen Gründen hat sich für allgemeine Moduln eine andere Bezeichnung durchgesetzt.

Definition 3.3.5. Es sei $k \in \mathbb{N}$, V ein R- Modul und $W_1, \ldots, W_k$ Untermoduln von V. Wir sagen, V ist die direkte Summe der W_i (Schreibweise: $V = W_1 \oplus \ldots \oplus W_k$), wenn folgende Eigenschaften gelten:

i) $V = W_1 + \ldots + W_k$

ii) die Untermoduln sind linear unabhängig.
Ist $w_1 + \ldots + w_k = 0$ mit $w_i \in W_i$, so ist $w_i = 0$ für alle i.

Man sieht sofort die Gültigkeit des folgenden Satzes:

Satz 3.3.3. *Es sei V ein freier R- Modul mit Basis $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$. Dann ist $V = (\vec{b}_1) \oplus \ldots \oplus (\vec{b}_n)$.*

Beweis. ohne Beweis. □

Satz 3.3.4. *Es sei W ein endlich erzeugter R- Modul. Dann ist W das homomorphe Bild des freien Moduls R^n. Jeder freie Modul vom Rang n ist isomorph zum R^n.*

Beweis. Es sei $\mathcal{E} = \{w_1, \ldots, w_n\}$ ein Erzeugendensystem von W. Dann ist ein surjektiver Homomorphismus $\Phi\colon R^n \to W$ durch $\Phi(\vec{e}_i) = w_i$ gegeben. Ist $\mathcal{E}$ eine Basis, so ist Φ ein Isomorphismus. □

3.4 Moduln über Hauptidealringen

Von nun an sei R stets als Hauptidealring vorausgesetzt.

Satz 3.4.1. *Es sei V ein endlich erzeugter freier Modul über R und U ein Untermodul von V. Dann ist auch U frei, und es ist* $\operatorname{rg} U \leq \operatorname{rg} V$.

Bemerkung 3.4.1. Die Behauptung gilt für beliebige freie Moduln über Hauptidealringen, jedoch ist der Beweis für den allgemeinen Fall komplizierter.

Beweis. (Beweis von Satz 3.3.4)
Es sei $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$ eine Basis von V und $U_r = U \cap (\{\vec{b}_1, \ldots, \vec{b}_r\})$.
Wir beweisen durch Induktion nach r, dass U_r frei und $\dim U_r \leq r$ ist.

Induktionsanfang: $r = 1$:
Es ist $U_1 = U \cap (\vec{b}_1)$ ein Untermodul von $(\vec{b}_1)$. Die Menge $J = \{r \in R\colon r\vec{b}_1 \in U_1\}$ ist offenbar ein Ideal von R und daher nach Voraussetzung ein Hauptideal (a). Damit gilt $V = (a\vec{b}_1)$, also ist dieser frei mit $\operatorname{rg} U_1 = 1$ oder $U_1 = \{0\}$.

Induktionsschluss: $r \to r + 1$:
Es sei J die Menge aller $s \in R$, so dass $\vec{u} \in U_{r+1}$ mit $\vec{u} = x_1\vec{b}_1 + \ldots + x_r\vec{b}_r + s\vec{b}_{r+1}$ und $x_i \in R$ existiert. Es ist J ein Ideal, also gilt nach Voraussetzung $J = (a_{r+1})$ für $a_{r+1} \in R$. Ist $a_{r+1} = 0$, so gilt $U_{r+1} = U_r$, und wir sind fertig.
Im Fall $a_{r+1} \neq 0$ sei $\vec{w} = a_{r+1}\vec{b}_{r+1} + y_r\vec{b}_r + \ldots + y_1\vec{b}_1 \in U_{r+1}$. Für alle $\vec{v} \in U_{r+1}$ gibt es ein $c = c(r) \in R$, so dass $\vec{v} - c\vec{w} \in U_r$ ist. Deshalb gilt $U_{r+1} = U_r + (\vec{w})$. Wegen $U_r \cap (\vec{w}) = \{0\}$ ist $U_{r+1} = U_r + (\vec{w})$.
Ist $\mathcal{U}_r$ eine Basis von U_r, so ist $\mathcal{U}_{r+1} = \mathcal{U} \cup \{\vec{w}\}$ eine Basis von U_{r+1}. □

Satz 3.4.2. *Der Untermodul eines endlich erzeugten Moduls M über R ist endlich erzeugt.*

Beweis. Nach Satz 3.3.4 gibt es $n \in \mathbb{N}$ und einen surjektiven Homomorphismus $\Phi\colon R^n \to M$. Weiter sei $U \leq M$ und $V = \Phi^{-1}(U)$. Dann ist nach Satz 3.4.1 auch V endlich erzeugt und damit auch $U = \Phi(V)$. □

Satz 3.4.3. *Es seien M und M' endlich erzeugte R- Moduln, und M' sei frei. Es sei $\Phi\colon M \to M'$ ein surjektiver Homomorphismus. Dann existiert ein freier Untermodul F von M, so dass $\Phi_{|_F}$ ein Isomorphismus von F nach M' ist und $M = F \oplus \operatorname{Kern}(\Phi)$ gilt.*

Beweis. Es sei $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$ eine Basis von M'. Für $1 \leq i \leq n$ sei $\vec{c}_i \in M$ mit $\Phi(\vec{c}_i) = \vec{b}_i$. Es sei $F = (\{\vec{c}_1, \ldots, \vec{c}_n\})$. Dann sind die $\vec{c}_i$ linear unabhängig und damit F frei.
Es sei $m \in M$. Dann gibt es $r_1, \ldots, r_n \in R$ mit $\Phi(m) = \sum_{i=1}^{n} r_i\vec{b}_i$, womit

$$m - \sum_{i=1}^{n} r_i\vec{c}_i \in \operatorname{Kern}(\Phi)$$

gilt. Somit gilt $M = \operatorname{Kern}(\Phi) + F$. Wegen $\operatorname{Kern}(\Phi) \cap F = \{0\}$ ergibt sich die Behauptung. □

Definition 3.4.1. Es sei T ein R- Modul.
Dann heißt T Torsionsmodul, wenn für alle $v \in T$ ein $r \in R - \{0\}$ mit $rv = 0$ existiert. Dieses Element v eines R- Moduls V heißt Torsionselement, wenn es ein $r \in R - \{0\}$ mit $rv = 0$ gibt.

Satz 3.4.4. *Es sei M ein R- Modul.*
Die Menge M_t aller Torsionselemente ist ein Untermodul von M.

Beweis. Es seien $v_1, v_2 \in M_t$. Dann gibt es $r_1, r_2 \in R - \{0\}$ mit $r_1 v_1 = r_2 v_2 = 0$. Es sei $w = s_1 v_1 + s_2 v_2$ für $s_1, s_2 \in R$. Dann ist $r_1 r_2 w = 0$, also $w \in M_t$. □

Definition 3.4.2. Der Untermodul M_t von Satz 3.4.4 heißt Torsionsuntermodul (kurz: Torsion) von M. Ist $M_t = \{0\}$, so heißt M torsionsfrei.

Satz 3.4.5. *Es sei M ein endlich erzeugter R- Modul. Dann ist M/M_t ein freier R- Modul. Es gibt einen freien Untermodul F von M, so dass $M = M_t \oplus F$ gilt. Der Rang von F ist eindeutig bestimmt.*

Beweis. Es ist M/M_t endlich erzeugt. Wir beginnen mit dem Beweis zweier Behauptungen.

i) Wir zeigen zunächst, dass M/M_t torsionsfrei ist.
Es sei $r \in R$ und $m \in M$, so dass $r(m + M_t) = 0 + M_t = M_t$ ist. Dann ist $rm \in M_t$. Also existiert ein $s \in R - \{0\}$ mit $srm = 0$. Deshalb ist $m \in M_t$, also $m + M_t = 0 + M_t$, also die Torsionsfreiheit.

ii) Wir zeigen nun, dass ein endlich erzeugter torsionsfreier Modul frei ist.
Es sei $\mathcal{C} = \{\vec{c}_1, \ldots, \vec{c}_m\}$ ein endliches Erzeugendensystem von V und $\mathcal{D} = \{\vec{d}_1, \ldots, \vec{d}_n\}$ eine maximale Teilmenge von $\mathcal{C}$, für die $\vec{d}_1, \ldots, \vec{d}_n$ linear unabhängig sind. Es sei $i \in \{1, \ldots, m\}$. Dann gibt es $(s, r_1, \ldots, r_m) \in R^{m+1} - \{(0, \ldots, 0)\}$ mit $s\vec{c}_i + r_1\vec{d}_1 + \ldots + r_n\vec{d}_n = 0$. Es ist $s \neq 0$, da sonst die $\vec{d}_1, \ldots, \vec{d}_n$ linear abhängig wären. Damit gilt $s\vec{c}_i \in (\{\vec{d}_1, \ldots, \vec{d}_n)\}$. Für $1 \leq j \leq m$ existieren also $s_j \neq 0_m$ mit $s_j\vec{c}_j \in (\{\vec{d}_1, \ldots, \vec{d}_n)\}$. Damit ist tV nach Satz 3.4.1 frei. Die Abbildung $\Phi\colon v \to tv$ ist injektiv, da V torsionsfrei ist. Also gilt $V \cong tV$, und damit ist auch V frei.

Wir wenden Satz 3.4.3 mit $M' = M/M_t$ und $\Phi\colon M \to M'$, $m \to m + M_t$, dem kanonischen Homomorphismus, an. Es ist $\mathrm{Kern}(\Phi) = M_t$. Nach Satz 3.4.3 existiert ein freier Untermodul F von M, so dass $M = F \oplus \mathrm{Kern}(\Phi) = F \oplus M_t$ gilt. Wegen $F \cong M/M_t$ ist der Rang von F eindeutig bestimmt. □

Definition 3.4.3. Es sei M ein R- Modul und $m \in M$.
Ist $\{r \in R\colon rm = 0\} = (s)$ mit $s \in R$, so heißt s eine Periode von m. Weiter heißt $c \in R$ Exponent für M (bzw. m), wenn $cM = \{0\}$ (bzw. $cm = 0$) gilt.
Es sei π ein Primelement von R. Dann sei $M(\pi)$ der Untermodul von M, der aus allen $l \in M$ besteht, für die ein r existiert, so dass π^r ein Exponent für l ist. Ein π- Untermodul von M ist ein Untermodul von $M(\pi)$.

Definition 3.4.4. Es sei M ein R- Modul und $y_1, \ldots, y_m \in M$. Wir sagen $y_1, \ldots, y_m$ sind unabhängig, wenn aus $r_1 y_1 + \ldots + r_m y_m = 0$ für $r_i \in R$ dann $r_i y_i = 0$ für alle $1 \leq i \leq m$ folgt.

Man beweist leicht

Satz 3.4.6. *Es sei M ein R- Modul und $y_1, \ldots, y_m \in R$. Die $y_1, \ldots, y_m$ sind genau dann unabhängig, wenn $(\{y_1, \ldots, y_m\}) = (y_1) \oplus \ldots \oplus (y_m)$ gilt.*

Beweis. ohne Beweis. □

Definition 3.4.5. Ein R- Modul M heißt zyklisch, falls $M \cong R/(a)$ für ein $a \in R$ gilt.

Beispiel 3.4.1. Abelsche Gruppen sind genau dann zyklische $\mathbb{Z}$- Moduln, wenn sie zyklische Gruppen sind. Sämtliche Isomorphietypen sind dann durch $(\mathbb{Z}/m\mathbb{Z}, +) \cong \mathbb{Z}/(m)$ bzw. $\mathbb{Z} \cong \mathbb{Z}/(0)$ gegeben.

Satz 3.4.7. *Es sei M ein Torsionsmodul mit Exponent π^r mit $r \geq 1$ und einem Primelement $\pi \in R$. Es sei $x_1 \in M$ ein Element mit Periode π^r. Es sei $\overline{M} = M/(x_1)$. Weiter seien $\overline{y_1}, \ldots, \overline{y_m}$ unabhängige Elemente von $\overline{M}$. dann gibt es für jedes i einen Repräsentanten $y_i \in \overline{y_i} = y_i + (x_1)$, so dass y_i dieselbe Periode wie $\overline{y_i}$ hat. Die Elemente $x_1, y_1, \ldots, y_m$ sind unabhängig.*

Beweis. Es habe $\overline{y} \in M$ die Periode π^n für $n \geq 1$. Es sei y ein Repräsentant von $\overline{y}$ in M, also $\overline{y} = y + (x_1)$. Dann ist $\pi^n y \in (x_1)$ und deshalb $\pi^n y = \pi^s c x_1$ mit $c \in R$ und $\pi \not| c$ für $s \leq r$.
Fall 1: $s = r$:
Dann hat y dieselbe Periode wie $\overline{y}$.
Fall 2: $s < r$:
Dann hat $\pi^s cx$ die Periode π^{r-s} und deshalb y die Periode π^{n+r-s}.
Es ist $n + r - s \leq r$, da π^r ein Exponent für M ist. Damit haben wir $n \leq s$, und $y - \pi^{s-n} c x_1$ ist ein Repräsentant für $\overline{y}$ mit Periode π^n.
Es seien $a, a_1, \ldots, a_m \in R$ mit $ax_1 + a_1 y_1 + \ldots + a_m y_m = 0$. Dann ist auch $a_1\overline{y_1} + \ldots + a_m\overline{y_m} = 0$. Nach Vorausetzung muss $a_i\overline{y_i} = 0$ für $1 \leq i \leq m$ gelten. Es sei π^{r_i} die Periode von $\overline{y_i}$. Dann ist $\pi^{r_i} | a_i$. Es folgt $a_i y_i = 0$ für alle i und damit auch $ax_1 = 0$, also die Unabhängigkeit von $x_1, y_1, \ldots, y_m$. □

Definition 3.4.6. Wir treffen jetzt für jedes Primelement π eine feste Wahl eines Repräsentanten aus der Klasse der Assoziierten von π. Es sei $m \in R$ mit $m \neq 0$. Mit M_m bezeichnen wir den Kern der Abbildung $x \to mx$. Es seien $r_1, \ldots, r_s \in \mathbb{N}$. Ein π- Modul M heißt vom Typ $(\pi^{r_1}, \ldots, \pi^{r_s})$, wenn $M \cong R/(\pi^{r_1}) \oplus \ldots \oplus R/(\pi^{r_s})$ gilt.

Satz 3.4.8. *Es sei M ein endlich erzeugter vom Nullmodul verschiedener Torsionsmodul. Dann gilt*

i) $M \cong \oplus_\pi M(\pi)$, wobei die direkte Summe über alle π erstreckt wird, für die $M(\pi) \neq 0$ gilt.

ii) Jedes $M(\pi)$ kann als direkte Summe geschrieben werden:

$$M(\pi) = M_1 \oplus \ldots \oplus M_u$$

mit $M_i \cong R/(\pi^{\nu_i})$ mit $1 \leq \nu_i \leq \ldots \leq \nu_u$.
Die Folge der $\nu_1, \ldots, \nu_u$ ist eindeutig bestimmt.

Beweis. i) Es sei a ein Exponent für M, und es gelte $a = bc$ mit $ggT(b, c) = 1$. Es seien $x, y \in R$ mit $xb + yc = 1$. Wir behaupten

$$M = M_b \oplus M_c. \tag{1}$$

Die Behauptung folgt dann durch Induktion, indem a als Produkt von Primelementen geschrieben wird. Es sei $v \in M$. Dann ist $v = xbv + ycv$, also $xbv \in M_c$ wegen $cxbv = xav = 0$. Analog zeigt man $ycv \in M_b$. Schließlich folgt $M_b \cap M_c = \{0\}$, woraus $M = M_b \oplus M_c$ folgt.

ii) Es sei s die Maximalzahl unabhängiger Elemente, wobei s auch existiert, da $M(\pi)$ endlich erzeugt ist. Wir führen den Beweis durch Induktion nach s:
Induktionsanfang: $s = 1$:
Es sei $x_1 \in M(\pi)$ mit maximaler Periode π^{ν_1}, und wir nehmen $M(\pi)/(x_1) \neq \{0\}$ an.
Dann gibt es ein unabhängiges $\overline{y_1} \in M(\pi)/(x_1)$. Nach Satz 3.4.7 gibt es einen Repräsentanten y_1 von $\overline{y_1}$, so dass x_1 und y_1 unabhängig sind, ein Widerspruch zu $s = 1$.
Damit gilt $M(\pi) = (x_1) \cong R/(\pi^{\nu_1})$.

Induktionsschritt: $\{1,\ldots,s-1\} \to s$:
Die Aussage sei für alle Werte kleiner gleich $s-1$ bewiesen. Es sei $x_1 \in M(\pi)$ mit maximaler Periode π^{ν_1}. Weiter seien $\overline{y_1},\ldots,\overline{y_m} \in M/(x_1)$ unabhängige Elemente, wobei m maximal gewählt ist. Nach Satz 3.4.7 gibt es Repräsentanten y_i von $\overline{y_i}$, die dieselben Perioden wie $\overline{y_i}$ haben, so dass $x_1, y_1, \ldots, y_m$ unabhängig sind. Also gilt $m \leq s-1$. Wir können dann auf $M/(x_1)$ die Induktionshypothese anwenden:

$$M/(x_1) \cong \overline{M_2} \oplus \ldots \oplus \overline{M_\nu}$$

mit $\overline{M_i} \cong R/(\pi^{\nu_i})$. Ist $\overline{M_i} = (\overline{z_i})$, so gibt es nach Satz 3.4.7 Repräsentanten z_i von $\overline{z_i}$, so dass $x_1, z_2, \ldots, z_u$ unabhängig sind. Damit gilt $M = (x_1) \oplus (z_2) \oplus \ldots \oplus (z_u)$ mit $(x_1) \cong R/(\pi^{\nu_1})$ und $(z_i) \cong R/(\pi^{\nu_i})$.
Damit ist alles bewiesen bis auf die Tatsache, dass die Folge der ν_i eindeutig bestimmt ist. Dies wird aber aus dem Beweis des kommenden Satzes folgen.

□

Satz 3.4.9. *Es sei $M \neq \{0\}$ ein endlich erzeugter Torsionsmodul.*
Dann gilt $M \cong R/(q_1) \oplus \ldots \oplus R/(q_s)$ mit $q_1,\ldots,q_s \in R\backslash\{0\}$ und $q_1|q_2|\ldots|q_s$. Die Folge der Ideale $(q_1),\ldots,(q_s)$ ist eindeutig bestimmt.

Beweis. Nach dem schon bewiesenen Teil von Satz 3.4.8 zerlegen wir den Torsionsmodul M in eine direkte Summe $M = M(\pi_1) \oplus \ldots \oplus M(\pi_l)$ und zerlegen dann jedes $M(\pi_i)$ in eine direkte Summe zyklischer Untermoduln mit Perioden $\pi_i^{s_{ij}}$. Wir erhalten folgendes Schema:

$$\begin{array}{rcl} M(\pi_1) & : & s_{11} \leq s_{12} \leq \ldots \\ M(\pi_2) & : & s_{21} \leq s_{22} \leq \ldots \\ \vdots & & \vdots \\ M(\pi_l) & : & s_{l1} \leq s_{l2} \leq \ldots \end{array}$$

Die Elemente q_i werden mit den Spalten der Matrix gebildet:

$$\begin{array}{rcl} q_1 & = & \pi_1^{s_{11}} \pi_2^{s_{21}} \ldots \pi_l^{s_{l1}} \\ q_2 & = & \pi_1^{s_{12}} \pi_2^{s_{22}} \ldots \pi_l^{s_{l2}} \\ \vdots & & \vdots \\ q_s & = & \pi_1^{s_{1s}} \pi_2^{s_{2s}} \ldots \pi_l^{s_{ls}}. \end{array}$$

Die für Satz 3.4.8 noch zu beweisende Eindeutigkeit des obigen Schemas wird dann aus der Eindeutigkeit der Folge der q_i folgen.
Wir zeigen zunächst, dass die Anzahl s der Idelae (q_i) eindeutig bestimmt ist.
Es sei $\pi \in R$ ein Primelement und $v_i \in M$ mit $v = v_1 + \ldots + v_s$ mit $v_i \in M_i \cong R/(q_i)$. Für alle i gilt genau dann $v \in M_\pi$, wenn $\pi v_i = 0$ ist. Damit ist $M_\pi = M_{1,\pi} \oplus \ldots \oplus M_{s,\pi}$. Wegen der Maximalität von (π) ist $R/(\pi)$ ein Körper, und M_π sowie die $M_{i,\pi}$ sind Vektorräume über $R/(\pi)$. Dann gilt

$$M_{i,\pi} = \begin{cases} 1, & \text{wenn } \pi|q_i \\ 0, & \text{wenn } \pi \not| q_i. \end{cases}$$

Damit ist

$$\dim M_\pi = |\{i \colon \pi|q_i\}|. \tag{1}$$

Ist π so gewählt, dass $\pi|q_1$ gilt, so folgt $\pi|q_i$ für alle i. Wegen (1) ist deshalb s eindeutig bestimmt.

Zum Abschluss des Beweises benötigen wir zunächst folgendes Ergebnis:
Für ein Primelement $\pi \in R$ und $b \in R - \{0\}$ ist

$$R/(\pi) \cong bR/(\pi b). \tag{2}$$

Dies folgt, weil (π) der Kern der Komposition $\Phi \circ \psi$ mit $\psi\colon R \to bR$, $r \to br$ und $\Phi\colon bR \to bR/(\pi b)$, $br \to br + (\pi b)$ ist.
Es sei $\Omega(q_s) = s_{1,s} + s_{2,s} + \ldots + s_{l,s}$ die Gesamtzahl der Primfaktoren von q_s. Es sei k das Maximum von $\Omega(q_s)$, gebildet über alle Darstellungen $M \cong R/(q_1) \oplus \ldots \oplus R/(q_s)$.
Wir beweisen nun die Eindeutigkeit durch Induktion nach k:
Induktionsanfang: $k = 1$:
Mit $M_i \cong R/(\pi)$ ist $M = M_1 \oplus \ldots \oplus M_s$. Da π die gemeinsame Periode aller $m \in M\backslash\{0\}$ ist, ist π eindeutig bestimmt.
Induktionsschritt: $\{1, \ldots, k\} \to k + 1$:
Es sei $q_i = \pi b_i$. Nach (2) gilt $\pi M \cong R/(b_1) \oplus \ldots \oplus R/(b_s)$ und $b_1 | \ldots | b_s$. Es seien $(b_1) = \ldots = (b_j) = (1)$ und $(b_{j+1}) \neq (1)$. Nach Induktionshypothese sind j und die $(b_{j+1}), \ldots, (b_s)$ eindeutig bestimmt. Damit sind auch die (q_i) eindeutig bestimmt. □

Definition 3.4.7. Eine abelsche Gruppe G heißt frei, falls sie ein freier $\mathbb{Z}$- Modul ist. Unter dem Rang von G versteht man den Rang des $\mathbb{Z}$- Moduls G.

Satz 3.4.10. *(Hauptsatz über endlich erzeugte abelsche Gruppen)*

i) Jede endlich erzeugte abelsche Gruppe ist das direkte Produkt einer endlichen abelschen Gruppe G und einer freien abelschen Gruppe F. Der Rang von F ist eindeutig bestimmt.

ii) Jede endliche abelsche Gruppe ist das direkte Produkt zyklischer Gruppen von Primzahlpotenzordnung. Die Ordnungen sind eindeutig bestimmt.

Beweis. i) Dies folgt aus Satz 3.4.5.

ii) Dies folgt aus Satz 3.4.8.

□

3.5 Anwendungen auf Endomorphismen von Vektorräumen

Definition 3.5.1. Es sei K ein Körper, t eine Unbestimmte über K, V ein Vektorraum über K mit $\dim V < \infty$ und φ ein Endomorphismus von V. Der von φ induzierte $K[t]$- Modul V ist wie folgt definiert:
Die Menge der Modulelemente ist V. Durch die auf dem Vektorraum V gegebene Addition wird V zu einer abelschen Gruppe. Es sei $p(t) = a_0 + a_1 t + \ldots + a_m t^m \in K[t]$ und $v \in V$. Dann setzen wir

$$p(t)v = a_0\varphi^0(v) + a_1\varphi(v) + \ldots + a_m\varphi^m(v)$$

mit $\varphi^0 = id$.

Satz 3.5.1. *Durch die in Definition 3.5.1 erklärten Operationen wird V zu einem endlich erzeugten $K[t]$- Modul.*

Beweis. Durch Nachrechnen. □

Satz 3.5.2. *Der von φ induzierte $K[t]$- Modul ist ein Torsionsmodul.*

Beweis. Es sei $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$ eine Basis von V. Da $\varphi^0(\vec{b}_i), \ldots, \varphi^n(\vec{b}_i)$ mit $1 \leq i \leq n$ linear abhängig sind, gibt es Polynome $p_i \in K[t] - \{0\}$ mit $p_i(t)\vec{b}_i = \vec{0}$. Für $f(t) = p_1(t) \cdots p_n(t)$ gilt dann $f(t) \cdot V = \{\vec{0}\}$. Wir wenden nun Satz 3.4.9 an. Die Primelemente von $K[t]$ sind zu irreduziblen Polynomen mit höchstem Koeffizienten 1 assoziiert. Nach Satz 3.4.9 hat V eine Zerlegung als direkte Summe zyklischer Moduln V_i, nämlich $V = V_1 \oplus \ldots \oplus V_s$ mit $V_i \cong K[t]/(p_i^{\nu_i})$ mit normierten und irreduziblen p_i. Sind $\mathcal{B}_1, \ldots, \mathcal{B}_s$ Basen der Unterräume V_i und $\mathcal{M}(\varphi_{|_{V_i}}; \mathcal{B}_i, \mathcal{B}_i)$ die Darstellungsmatrizen der Restriktionen $\varphi_{|_{V_i}}$ bzgl. der Basen $\mathcal{B}_i$, so ist $\mathcal{B} = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_s$ eine Basis von V, und die Darstellungsmtraix $\mathcal{M}(\varphi; \mathcal{B}, \mathcal{B})$ besteht aus den Kästchen $\mathcal{M}(\varphi_{|_{V_i}}; \mathcal{B}_i, \mathcal{B}_i)$ entlang der Diagonalen. Durch geeignete Wahl der Basen $\mathcal{B}_i$ können die Kästchen und damit auch die gesamte Matrix $\mathcal{M}(\varphi; \mathcal{B}, \mathcal{B})$ in eine kanonische Form gebracht werden. Es wird nun V_i von einem einzigen Element $w_i \in V_i$ erzeugt. Jedes $v \in V_i$ hat die Form $v = g(t)w_i$. Ist $g(t) = b_0 + \ldots + b_m\varphi^m(w_i)$, so erhalten wir $v = b_0w_i + b_1\varphi(w_i) + \ldots + b_m\varphi^m(w_i)$. Damit ist $\mathcal{M} = \{w_i, \varphi(w_i), \ldots, \varphi^k(w_i), \ldots\}$ ein Erzeugendensystem von V_i.
Die Abbildung $\Phi\colon K[t] \to V_i$, $g(t) \to g(t)w_i$ ist ein Homomorphismus. Nach dem Isomorphiesatz (Satz 3.1.2) gilt nun $\text{Kern}(\Phi) = (p_i^{\nu_i})$. Mit $f(t) = p_i(t)^{\nu_i} = a_0 + a_1t + \ldots + t^m$ und der Basis $\mathcal{B} = \{w_i, \varphi(w_i), \ldots, \varphi^{m-1}(w_i)\}$ hat $\mathcal{M}(\varphi_{|_{V_i}}; \mathcal{B}_i, \mathcal{B}_i)$ somit die Form

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & \ddots & \vdots \\ 0 & & & 1 & -a_{m-1} \end{pmatrix}. \qquad (*)$$

□

Satz 3.5.3. *(Rationale kanonische Form)*
Es sei φ ein Endomorphismus eines endlichdimensionalen Vektorraums V über einem Körper K. Dann gibt es eine Basis $\mathcal{B}$ für V, so dass $\mathcal{M}(\varphi; \mathcal{B}, \mathcal{B})$ aus Kästchen der Form $(*)$ des Satzes 3.5.2 entlang der Diagonalen besteht.
Für den Körper $\mathbb{C}$ der komplexen Zahlen kann eine einfachere Form, die Jordansche Normalform, erzielt werden.
Nach dem Fundamentalsatz der Algebra hat jedes nichtkonstante Polynom $f \in \mathbb{C}[t]$ eine Nullstelle. Somit sind die normierten irreduziblen Polynome gerade $p_i(t) = (t - \alpha_i)$ mit $\alpha_i \in \mathbb{C}$. Damit ergibt sich für einen Vektorraum über $\mathbb{C}$ die direkte Summe $V = V_1 \oplus \ldots \oplus V_s$ mit $V_i \cong \mathbb{C}[t]/(t-\alpha_i)^{\nu_i}$. Es sei wieder $v_i = (w_i)$. Wir definieren die Basis $\mathcal{B}_i = \{w_i^{(0)}, w_i^{(1)}, \ldots, w_i^{(\nu_i-1)}\}$ mit $w_i^{(j+1)} = (\varphi - \alpha_i \circ id)w_i^{(j)}$ für $0 \leq j \leq \nu_i - 2$. Wir erhalten $(\varphi - \alpha_i \circ id)w_i^{(\nu_j-1)} = 0$.
Damit wird $\mathcal{M}(\varphi_{|_{V_i}}; \mathcal{B}_i, \mathcal{B}_i)$ das Jordankästchen

$$\mathcal{M}(\varphi_{|_{V_i}}; \mathcal{B}_i, \mathcal{B}_i) = \begin{pmatrix} \alpha_i & & & 0 \\ 1 & \alpha_i & & \\ & \ddots & \ddots & \\ & & \ddots & \ddots \\ & 0 & & 1 & \alpha_i \end{pmatrix}$$

Beweis. ohne Beweis. □

Satz 3.5.4. *(Jordansche Normalform)*
Es sei φ ein Endomorphismus eines endlichdimensionalen Vektorraums V über $\mathbb{C}$. Dann gibt es eine Basis $\mathcal{B}$ für V, so dass $\mathcal{M}(\varphi;\mathcal{B},\mathcal{B})$ aus den Jordankästchen

$$\mathcal{M}(\varphi_{|_{V_i}};\mathcal{B}_i,\mathcal{B}_i) = \begin{pmatrix} \alpha_i & & & 0 & \\ 1 & \alpha_i & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & 0 & & 1 & \alpha_i \end{pmatrix}$$

entlang der Diagonalen besteht.

Beweis. ohne Beweis. □