Universität Paderborn, Fakultät für Elektrotechnik, Informatik und Mathematik

Ausarbeitungen zum

Seminar Algebra

bei Dr. Christian Nelius

im WS 2003/2004

Teilnehmer:

Dennis Amelunxen,
Olga Anhalt,
Karin Büker,
Nadja Dvoretski,
Anna Hillebrand,
Ann–Kristin Malik,
José Sánchez–Romero,
Annemarie Schulz,
Johann Thiemeyer,
Dietrich Travkin,
Johann Wedel,
Alexander Willms

Inhaltsverzeichnis

1 Zerfällungskörper von Polynomen

In dieser Ausarbeitung soll auf „einfache“ Weise gezeigt werden, dass es zu einem Polynom $f \in K[T]$ für einen Körper K einen bis auf Isomorphie eindeutig bestimmten, kleinsten Oberkörper von K gibt, über dem f in Linearfaktoren zerfällt. Dabei baut diese Arbeit auf [2], Seiten 132 bis 142 auf.

1.1 Definition *Sei $L : K$ eine Körpererweiterung. L heißt Zerfällungskörper eines nicht-konstanten Polynoms $f \in K[T]$ (man sagt dann auch: L ist Zerfällungskörper von f über K, Kurzschreibweise: $\mathrm{ZFK}_K(f)$), wenn gilt:*

a) *f zerfällt über L in Linearfaktoren, d.h. es gibt $a_1, \ldots, a_n, b \in L$ mit $f = b \cdot (T - a_1) \cdot \ldots \cdot (T - a_n)$.*

b) *L ist minimal bzgl. der Eigenschaft in a), d.h. f zerfällt über keinem echten Zwischenkörper von $L : K$ in Linearfaktoren.*

1.2 Beispiele

a) *$\mathbb{C} \supset \mathbb{R}$ ist ein Zerfällungskörper des Polynoms $p := T^2 + 1 \in \mathbb{R}[T]$, denn die Nullstellen von p sind $i, -i \in \mathbb{C}$ und $\mathbb{R}(i) = \mathbb{C}$. Es gibt also keinen echten Zwischenkörper von $\mathbb{C} : \mathbb{R}$, über dem $p = T^2 + 1 = (T - i)(T + i)$ in Linearfaktoren zerfällt.*

b) *$\mathbb{Q}(i) \supset \mathbb{Q}$ ist ein Zerfällungskörper des Polynoms $p' := T^2 + 1 \in \mathbb{Q}[T]$. Hier gilt nämlich $i, -i \in \mathbb{Q}(i) = \mathbb{Q}(-i)$ und $\mathbb{Q}(i)$ ist der kleinste Zwischenkörper von $\mathbb{C} : \mathbb{Q}$, der $\mathbb{Q}$ und $\{i, -i\}$ enthält.*

Um die Existenz eines Zerfällungskörpers zu einem nicht-konstanten Polynom $f \in K[T]$ beweisen zu können, wird der folgende Satz von Kronecker benötigt.

1.3 Satz (von Kronecker) *Ist K ein Körper und f ein nicht-konstantes Polynom aus $K[T]$, so gibt es einen Oberkörper L von K und ein $\alpha \in L$ mit $f(\alpha) = 0$.*

Beweis: Weil $f \in K[T]$ nicht konstant ist, hat f einen Grad ≥ 1 und läßt sich nach [1] Satz 3.27 als Produkt von endlich vielen irreduziblen Polynomen darstellen. Sei $p \in K[T]$ eines dieser irreduziblen Polynome, d.h. $f = p \cdot q,\ q \in K[T]$. Da K ein Körper ist und p irreduzibel über K ist, ergibt sich aus [1] Satz 3.24 i) $\mathrm{grad}(p) \geq 1$. Dann ist $L := K[T]/(p)$ nach [1] Satz 3.34 ein Körper.

Betrachten wir nun die natürliche Abbildung $\nu : K[T] \to K[T]/(p)$ mit $\forall x \in K[T] : \nu(x) = [x]_{(p)}$. Diese Abbildung ist nach [1] Satz 1.18 ein surjektiver Ringhomomorphismus. Schränkt man ν auf K ein, d.h. wir betrachten $\nu|K : K \to L$, so ist diese Abbildung sogar ein Körperhomomorphismus, weil $L = K[T]/(p)$ und K Körper sind. Nach [1] Satz 2.10 ist jeder Körperhomomorphismus injektiv, was dann auch für $\nu|K$ gilt. Man kann also K in $L = K[T]/(p)$ einbetten und L (bis auf Isomorphie) als Oberkörper von K betrachten.

Sei $\alpha := \nu(T) = [T] \in L$ und $p \in K[T]$ habe die Form $p = \sum_{i=0}^{m} a_i T^i,\ a_i \in K$. Dann gilt

$$p(\alpha) = p([T]) = \sum_{i=0}^{m} a_i [T]^i = \sum_{i=0}^{m} a_i \left[T^i\right] = \sum_{i=0}^{m} \left[a_i T^i\right] = \left[\sum_{i=0}^{m} a_i T^i\right] = [p] = \nu(p)$$

Da $[p]$ aber die Restklasse von p nach dem Ideal (p) ist, also $p(\alpha) = [p]_{(p)}$ gilt, folgt $[p]_{(p)} = p + (p) = \{p + ap \mid a \in K[T]\} = [0]_{(p)}$ und damit auch $p(\alpha) = [p] = 0$. α ist also eine Nullstelle des Polynoms p und wegen $p \mid f$ ist α auch eine Nullstelle von f.

Es gilt also: L ist (bis auf Isomorphie) ein Oberkörper von K mit $f(\alpha) = 0,\ \alpha \in L$.
□

Nun kommen wir zu dem Beweis der Existenz eines Zerfällungskörpers zu einem nicht-konstanten Polynom.

1.4 Satz (Existenz) *Sei K ein Körper und $f \in K[T]$ ein nicht-konstantes Polynom. Dann gibt es einen Zerfällungskörper $Z = \mathrm{ZFK}_K(f)$ von f. Ist $L : K$ eine Körpererweiterung und zerfällt f über L in Linearfaktoren $T - a_1, \ldots, T - a_n$, so ist $K(a_1, \ldots, a_n) \supseteq K$ Zerfällungskörper von f.*

Beweis: Seien K ein Körper und $f \in K[T]$ ein nicht-konstantes Polynom, also ein Polynom mit $\mathrm{grad}(f) \geq 1$. Dann gibt es nach Satz 1.3 einen Oberkörper L_1 von K und ein $a_1 \in L_1$ mit $f(a_1) = 0$. Dann gilt nach [1] Lemma 3.12 $f = (T - a_1)q_1$ für ein geeignetes Polynom $q_1 \in L_1[T]$. Ist q_1 ein konstantes Polynom, so ist man fertig. Andernfalls — in diesem Fall gilt $\mathrm{grad}(q_1) \geq 1$ — kann man dieses Verfahren nochmal auf q_1 anwenden und erhält so einen Oberkörper L_2 von L_1 und ein Element $a_2 \in L_2$ mit $q_1(a_2) = 0 = f(a_2)$ und es gilt $q_1 = (T - a_2)q_2$ für ein geeignetes Polynom $q_2 \in L_2[T]$. Damit gilt also $f = (T - a_1)q_1 = (T - a_1)(T - a_2)q_2$. Für $\mathrm{grad}(f) = n$ läßt sich dieses Verfahren n-mal anwenden, und führt zu einem Oberkörper L_n von K und den Elementen $a_1, a_2, \ldots, a_n \in L_n$, sowie einem konstanten Polynom $q_n \in L_n[T]^* = L_n^*$ mit $f = (T - a_1)(T - a_2) \cdot \ldots \cdot (T - a_n)q_n$. Multipliziert man $(T - a_1) \cdot \ldots \cdot (T - a_n)$ aus, so hat man $f = q_n T^n + r$ für ein $r \in K[T]$, d.h. q_n ist der Leitkoeffizient von f und wegen $f \in K[T]$ liegt q_n sogar in $K \subseteq L_n$. Das Polynom $f \in K[T]$ zerfällt also über $K(a_1, a_2, \ldots, a_n)$ in Linearfaktoren.

Nun ist zu zeigen, dass $K(a_1, \ldots, a_n)$ sogar ein Zerfällungskörper von f ist.
Annahme: f zerfällt über einem Zwischenkörper L von $K(a_1, \ldots, a_n) : K$ in Linearfaktoren. Dann gibt es $b_1, b_2, \ldots, b_n \in L$ und ein $c \in K$ mit $f = (T - b_1)(T - b_2) \cdot \ldots \cdot (T - b_n)c$. Die Faktoren $T - a_i$ und $T - b_i$ für $i = 1, \ldots, n$ sind nach [1] Lemma 3.26 a) irreduzibel. Nach [1] Satz 3.27 läßt sich jedes Polynom $p \in K[T]$ vom Grad ≥ 1 als Produkt von endlich vielen irreduziblen Polynomen darstellen, wobei die Darstellung eindeutig ist bis auf Reihenfolge und Multiplikation mit Einheiten. Dieses gilt also auch für f, d.h. die Darstellungen $f = (T - a_1)(T - a_2) \cdot \ldots \cdot (T - a_n)q_n$ und $f = (T - b_1)(T - b_2) \cdot \ldots \cdot (T - b_n)c$ unterscheiden sich höchstens in der Reihenfolge der Faktoren und der Multiplikation mit einer Einheit. Zu jedem a_i, $i \in \{1, \ldots, n\}$ gibt es dann ein b_j, $j \in \{1, \ldots, n\}$ mit $T - a_i \sim T - b_j$ ($T - a_i$ ist assoziiert zu $T - b_j$), d.h. es gibt eine Einheit $d \in {L_n}^* = L_n \setminus \{0\}$ mit $d \cdot (T - a_i) = (T - b_j)$. Ein Koeffizientenvergleich führt zu $d = 1$ und damit zu $a_i = b_j$. Es gilt also $\{a_1, \ldots, a_n\} = \{b_1, \ldots, b_n\}$ und $q_n \sim c$. Dann gilt aber auch $K(b_1, \ldots, b_n) = K(a_1, \ldots, a_n)$. Wegen $K(b_1, \ldots, b_n) \subseteq L \subseteq K(a_1, \ldots, a_n)$ folgt dann $L = K(a_1, \ldots, a_n)$. Es gibt also keinen echten Zwischenkörper von $K(a_1, \ldots, a_n) : K$, über dem f in Linearfaktoren zerfällt, d.h. $K(a_1, \ldots, a_n) = \mathrm{ZFK}_K(f)$.
□

Die Konstruktion des Zerfällungskörpers $K(a_1, \ldots, a_n)$ von $f \in K[T]$ in dem letzten Beweis läßt auf eine interessante Eigenschaft der Körpererweiterung $K(a_1, \ldots, a_n) : K$ schließen.

1.5 Korollar *Seien K ein Körper, $f \in K[T]$ ein nicht-konstantes Polynom und Z ein Zerfällungskörper von f über K. Dann ist $Z : K$ eine endliche Körpererweiterung.*

Beweis: Nach Definition 1.1 zerfällt f über Z in Linearfaktoren, d.h. es gibt $a_1, \ldots, a_n, b \in Z$ mit $f = b \cdot (T - a_1) \cdot \ldots \cdot (T - a_n)$. Weiter gilt $a_1, \ldots, a_n \in K(a_1, \ldots, a_n) \subseteq Z$. Nach Satz 1.4 ist $K(a_1, \ldots, a_n)$ ein Zerfällungskörper von f über K. Da auch Z ein Zerfällungskörper von f über K ist und es nach Definition 1.1 keinen echten Zwischenkörper von $Z : K$ gibt, über dem f in Linearfaktoren zerfällt, folgt $Z = K(a_1, \ldots, a_n)$.

$f \in K[T]$ ist von Null verschieden und es gilt $f(a_i) = 0$ für alle $i = 1, \ldots, n$. Daraus folgt, dass a_i, $i = 1, \ldots, n$ algebraisch über K ist. Aus [1] Satz 5.14 folgt dann $K(a_1, \ldots, a_n) : K$ ist endlich, d.h. $Z : K$ ist endlich.

□

Bevor die Eindeutigkeit des Zerfällungskörpers $\mathrm{ZFK}_K(f)$ zu einem Polynom $f \in K[T]$ gezeigt wird, sollen noch einige Hilfsmittel bereitgestellt werden.

1.6 Satz *Seien K und K' Körper, $\varphi : K \to K'$ ein Isomorphismus und $\Phi : K[T] \to K'[T]$ der zugehörige Isomorphismus der Polynomringe. Ferner sei $f \in K[T]$ irreduzibel, α sei eine Nullstelle von f in einem Oberkörper von K und α' eine Nullstelle von $f' := \Phi(f) \in K'[T]$ in einem Oberkörper von K'.*

Dann gibt es genau einen Isomorphismus $\widehat{\varphi} : K(\alpha) \to K'(\alpha')$ mit $\widehat{\varphi}|K = \varphi$ und $\widehat{\varphi}(\alpha) = \alpha'$.

Beweis: f ist irreduzibel über K und damit gilt nach [1] Bemerkung 3.24 i) $f \neq 0$. α ist eine Nullstelle von $f \in K[T]$, $f \neq 0$ und damit ist α algebraisch über K. Nach [1] Satz 5.7 und [1] Satz 4.7 c_1) folgt dann $K(\alpha) = K[\alpha] = \{h(\alpha) \mid h \in K[T]\}$.

Eindeutigkeit von $\widehat{\varphi}$:
Angenommen, es gibt zwei Isomorphismen $\widehat{\varphi}, \widehat{\rho} : K(\alpha) \to K'(\alpha')$ mit den gewünschten Eigenschaften. Sei $a \in K(\alpha)$ beliebig. Dann gilt $a = g(\alpha)$ für ein $g \in K[T]$ wegen $K(\alpha) = \{h(\alpha) \mid h \in K[T]\}$. Sei g der Form $g = \sum_{i=0}^{m} a_i T^i$, $a_i \in K$. Dann gilt $\widehat{\varphi}(a) = \widehat{\varphi}(g(\alpha)) = \widehat{\varphi}(\sum_{i=0}^{m} a_i \alpha^i) = \sum_{i=0}^{m} \widehat{\varphi}(a_i \alpha^i) = \sum_{i=0}^{m} \widehat{\varphi}(a_i)\widehat{\varphi}(\alpha^i) = \sum_{i=0}^{m} \widehat{\varphi}(a_i)\widehat{\varphi}(\alpha)^i = \sum_{i=0}^{m} \varphi(a_i)(\alpha')^i$. Analog kommt man mit $\widehat{\rho}$ zu $\widehat{\rho}(a) = \widehat{\rho}(g(\alpha)) = \sum_{i=0}^{m} \widehat{\rho}(a_i)\widehat{\rho}(\alpha)^i = \sum_{i=0}^{m} \varphi(a_i)(\alpha')^i$. Das heißt $\forall a \in K(\alpha) : \widehat{\varphi}(a) = \widehat{\rho}(a)$ und damit $\widehat{\varphi} = \widehat{\rho}$. Es kann also höchstens einen Isomorphismus $\widehat{\varphi}$ mit den gewünschten Eigenschaften geben.

Existenz von $\widehat{\varphi}$:
Betrachtet man die Einsetzungshomomorphismen $E_\alpha : K[T] \to K(\alpha)$ definiert durch $E_\alpha(g) = g(\alpha)$ und $E_{\alpha'} : K'[T] \to K'(\alpha')$ definiert durch $E_{\alpha'}(g') = g'(\alpha')$ (siehe [1] Satz 3.10),

$$\begin{array}{ccc} K & \xrightarrow[\cong]{\varphi} & K' \\ \cap & & \cap \\ K[T] & \xrightarrow[\cong]{\Phi} & K'[T] \\ {\scriptstyle E_\alpha}\downarrow & & \downarrow{\scriptstyle E_{\alpha'}} \\ K(\alpha) & \xrightarrow{\widehat{\varphi}} & K'(\alpha') \end{array}$$

so gilt $E_\alpha(f) = f(\alpha) = 0$ und $E_{\alpha'}(f') = f'(\alpha') = 0$, da α eine Nullstelle von f und α' eine Nulstelle von f' ist. Es gilt also $f \in \mathrm{Kern}(E_\alpha)$ und $f' = \Phi(f) \in \mathrm{Kern}(E_{\alpha'})$.

Sei $m_\alpha \in K[T]$ das Minimalpolynom von α und $m_{\alpha'} \in K'[T]$ das Minimalpolynom von α'. Dann gilt nach [1] Satz 5.4 b) $m_\alpha | f$ und $m_{\alpha'} | f'$. Wegen $f(\alpha) = 0$ und weil f irreduzibel ist (aber nicht notwendigerweise normiert), folgt $m_\alpha \sim f$. Da $\Phi : K[T] \to K'[T]$ ein Isomorphismus ist, folgt, dass $f' = \Phi(f)$ irreduzibel in $K'[T]$ ist und damit

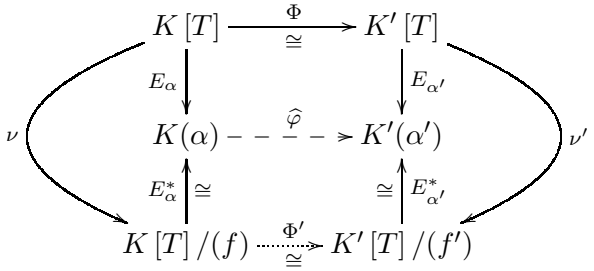
auch $m_{\alpha'} \sim f'$. Es folgt $(m_\alpha) = \{h \cdot m_\alpha \mid h \in K[T]\} = \{a \cdot h \cdot f \mid h \in K[T], a \in K^*\} = (f)$ und analog folgt auch $(m_{\alpha'}) = (f')$.

Behauptung: $(f) = \mathrm{Kern}(E_\alpha)$ und $(f') = \mathrm{Kern}(E_{\alpha'})$. Sei $g \in (f)$ beliebig. Dann hat g die Form $g = h \cdot f$ für ein geeignetes $h \in K[T]$. Weiter gilt wegen $f(\alpha) = 0$: $E_\alpha(g) = E_\alpha(h \cdot f) = E_\alpha(h) \cdot E_\alpha(f) = E_\alpha(h) \cdot f(\alpha) = 0$. Daraus folgt: $(f) \subseteq \mathrm{Kern}(E_\alpha)$. Analog gelangt man auch zu $(f') \subseteq \mathrm{Kern}(E_{\alpha'})$.

Sei jetzt umgekehrt $g \in \mathrm{Kern}(E_\alpha)$ beliebig. Dann gilt $0 = E_\alpha(g) = g(\alpha)$. Wegen $m_\alpha \sim f$ und $m_\alpha | g$ folgt dann $f|g$ und damit $g \in (f)$, d.h. $(f) \supseteq \mathrm{Kern}(E_\alpha)$. Analog zeigt man für ein beliebiges $g' \in \mathrm{Kern}(E_{\alpha'})$: $f'|g'$ und damit $g' \in (f')$, also $(f') \supseteq \mathrm{Kern}(E_{\alpha'})$. Damit ist die Behauptung $(f) = \mathrm{Kern}(E_\alpha)$ und $(f') = \mathrm{Kern}(E_{\alpha'})$ bewiesen.

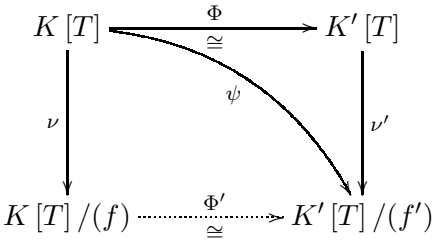
Weil α algebraisch über K ist, gilt $\mathrm{Bild}(E_\alpha) = \{E_\alpha(g) \mid g \in K[T]\} = \{g(\alpha) \mid g \in K[T]\} = K[\alpha] = K(\alpha)$. Mit $\mathrm{Kern}(E_\alpha) = (f)$ folgt dann nach dem Ringhomomorphiesatz in [1] Bemerkung 3.11 c), dass es einen Ringisomorphismus $E_\alpha^* : K[T]/(f) \to K(\alpha)$ gibt, definiert durch $[g]_{(f)} \mapsto E_\alpha(g) = g(\alpha)$ $(\forall g \in K[T])$. Analog läßt sich zeigen: $\mathrm{Bild}(E_{\alpha'}) = K'(\alpha')$ und es gibt einen Ringisomorphismus $E_{\alpha'}^* : K'[T]/(f') \to K'(\alpha')$, definiert durch $[g']_{(f')} \mapsto E_{\alpha'}(g') = g'(\alpha')$ $(\forall g' \in K'[T])$.

Nun soll gezeigt werden, dass es einen Isomorphismus $\Phi' : K[T]/(f) \to K'[T]/(f')$ gibt und damit der Isomorphismus $\widehat{\varphi} := E_{\alpha'}^* \circ \Phi' \circ E_\alpha^{*-1}$ existiert.



Nach [1] Satz 1.18 gibt es die natürliche Abbildung $\nu : K[T] \to K[T]/(f)$ und die natürliche Abbildung $\nu' : K'[T] \to K'[T]/(f')$, definiert durch $\nu(g) = [g]_{(f)}$ und $\nu'(g') = [g']_{(f')}$. Aus dem gleichen Satz ist bekannt, dass ν und ν' surjektive Ringhomomorphismen sind.

Sei nun $\psi : K[T] \to K'[T]/(f')$ definiert durch $\psi := \nu' \circ \Phi$.



Da Φ und ν' surjektive Ringhomomorphismen sind, ist ψ als Hintereinanderausführung dieser beiden Abbildungen ebenfalls ein surjektiver Ringhomomorphismus. Nach [1] Bemerkung 1.8 a) gilt dann $\mathrm{Bild}(\psi) = K'[T]/(f')$.

Behauptung: $\mathrm{Kern}(\psi) = (f)$. Es gilt offenbar $\psi(f) = (\nu' \circ \Phi)(f) = \nu'(\Phi(f)) = \nu'(f') = [f']_{(f')} = [0]_{f'}$, d.h. $f \in \mathrm{Kern}(\psi)$. Wegen $m_\alpha \sim f$ gilt für alle $g \in \mathrm{Kern}(\psi)$: $f|g$ und damit $g \in (f)$, d.h. $(f) \supseteq \mathrm{Kern}(\psi)$.

Andererseits gilt für alle $g \in (f)$: $g = h \cdot f$, für ein $h \in K[T]$ und $\psi(g) = \psi(h \cdot f) = \psi(h) \cdot \psi(f) = 0$, weil $f \in \mathrm{Kern}(\psi)$ gilt. Es folgt $g \in \mathrm{Kern}(\psi)$ und damit auch $(f) \subseteq \mathrm{Kern}(\psi)$. Die Behauptung $\mathrm{Kern}(\psi) = (f)$ ist damit gezeigt.

Mit $\text{Bild}(\psi) = K'[T]/(f')$ und $\text{Kern}(\psi) = (f)$ kann nun wieder der Ringhomomorphiesatz angewandt werden und es folgt: Es gibt einen Ringisomorphismus $\Phi' : K[T]/(f) \to K'[T]/(f')$, definiert durch $[g]_{(f)} \mapsto \psi(g) = \nu'(\Phi(g)) = [\Phi(g)]_{(f')}$. Diese Abbildung ist sogar ein Körperisomorphismus, denn weil f über K irreduzibel ist, gilt nach [1] Bemerkung 3.24 i) $\text{grad}(f) \geq 1$ und nach [1] Satz 3.34 ist $K[T]/(f)$ ein Körper. Analog zeigt man, dass $K'[T]/(f')$ ein Körper ist, da $f' = \Phi(f)$ irreduzibel in $K'[T]$ ist. Da $K(\alpha)$ und $K'(\alpha')$ ebenfalls Körper sind, folgt, dass auch E^*_α und $E^*_{\alpha'}$ Körperisomorphismen sind.

Die Abbildung $\widehat{\varphi} := E^*_{\alpha'} \circ \Phi' \circ {E^*_\alpha}^{-1}$ ist eine Hintereinanderausführung von Körperisomorphismen und damit selbst wieder ein Körperisomorphismus. Nun muss noch $\widehat{\varphi}|K = \varphi$ und $\widehat{\varphi}(\alpha) = \alpha'$ nachgewiesen werden.

Sei $a \in K$ beliebig. Dann gilt nach [1] Satz 3.10: $E^*_\alpha([a]_{(f)}) = E_\alpha(a) = a$ und damit $(E^*_\alpha)^{-1}(a) = [a]_{(f)}$. Es folgt dann $\widehat{\varphi}(a) = E^*_{\alpha'}(\Phi'((E^*_\alpha)^{-1}(a))) = E^*_{\alpha'}(\Phi'([a]_{(f)})) = E^*_{\alpha'}([\Phi(a)]_{(f')}) = E^*_{\alpha'}([\varphi(a)]_{(f')}) = E_{\alpha'}(\varphi(a)) = \varphi(a)$, d.h. $\widehat{\varphi}|K = \varphi$.

Für α gilt $\widehat{\varphi}(\alpha) = E^*_{\alpha'}(\Phi'((E^*_\alpha)^{-1}(\alpha))) = E^*_{\alpha'}(\Phi'([T]_{(f)})) = E^*_{\alpha'}([\Phi'(T)]_{(f')}) = E^*_{\alpha'}([T]_{(f')}) = E_{\alpha'}(T) = \alpha'$. Damit sind alle gewünschten Eigenschaften für $\widehat{\varphi}$ erfüllt und die Existenz bewiesen.

□

1.7 Korollar *Sei $L : K$ eine Körpererweiterung und seien $\alpha_1, \alpha_2 \in L$ algebraisch über K. Stimmen dann die Minimalpolynome von α_1 und α_2 über K überein, so gibt es genau einen Isomorphismus $\vartheta : K(\alpha_1) \to K(\alpha_2)$ mit $\vartheta|K = \text{id}_K$ und $\vartheta(\alpha_1) = \alpha_2$.*

Beweis: Wir können Satz 1.6 für $K = K'$ und $\varphi = \text{id}_K$ anwenden:
α_1 und α_2 sind Nullstellen des gemeinsamen Minimalpolynoms $m_{\alpha_1} = m_{\alpha_2} \in K[T]$, welches über K irreduzibel ist. ($\Phi(m_{\alpha_1})$ ist hier gerade m_{α_1} selbst und damit ist α_2 Nullstelle von $\Phi(m_{\alpha_1}) = m_{\alpha_1}$.) Dann gibt es nach Satz 1.6 genau einen Isomorphismus $\widehat{\varphi} : K(\alpha_1) \to K(\alpha_2)$ mit $\widehat{\varphi}|K = \text{id}_K$ und $\widehat{\varphi}(\alpha_1) = \alpha_2$. $\vartheta := \widehat{\varphi}$ ist also der gesuchte Isomorphismus.

□

1.8 Satz *Seien K und K' Körper, $\varphi : K \to K'$ ein Isomorphismus und $\Phi : K[T] \to K'[T]$ der zugehörige Isomorphismus der Polynomringe. Ferner sei $f \in K[T]$ nicht konstant.*

Ist dann $Z \supseteq K$ ein Zerfällungskörper von f und $Z' \supseteq K'$ ein Zerfällungskörper von $f' := \Phi(f)$, so gibt es einen (i.a. nicht eindeutig bestimmten) Isomorphismus $\psi : Z \to Z'$ mit $\psi|K = \varphi$, der die Menge der Nullstellen von f in Z auf die Menge der Nullstellen von f' in Z' abbildet.

Beweis: Der Beweis erfolgt durch vollständige Induktion über die Anzahl r der in $Z \setminus K$ liegenden Nullstellen von f:
Induktionsanfang: $\underline{r = 0:}$ Hier gilt $Z = K$, da f keine Nullstellen in $Z \setminus K$ hat und damit über K in Linearfaktoren zerfällt. Es gibt also $\alpha_1, \alpha_2, \ldots, \alpha_n, c \in K$ mit $f = c(T - \alpha_1) \cdot \ldots \cdot (T - \alpha_n)$. Damit gilt $f' = \Phi(f) = \Phi(c(T - \alpha_1) \cdot \ldots \cdot (T - \alpha_n)) = \Phi(c)\Phi(T - \alpha_1) \cdot \ldots \cdot \Phi(T - \alpha_n) = \varphi(c)(T - \varphi(\alpha_1)) \cdot \ldots \cdot (T - \varphi(\alpha_n))$. Die Nullstellen von f, nämlich $\alpha_1, \ldots, \alpha_n \in K$, werden auf die Nullstellen von $f' = \Phi(f)$, nämlich $\varphi(\alpha_1), \ldots, \varphi(\alpha_n) \in K'$, abgebildet. Damit erfüllt $\psi := \varphi$ die gewünschten Eigenschaften.

Induktionsannahme: Die Behauptung sei richtig für alle K, K', φ, f, Z, Z', die die Voraussetzungen des Satzes erfüllen und für die zusätzlich gilt, dass höchstens $r-1$ Nullstellen von f in $Z \setminus K$ liegen.
Induktionsschluss: $\underline{r \geq 1:}$ Falls nun K, K', φ, f, Z, Z' die Voraussetzungen des Satzes erfüllen und liegen r Nullstellen $\alpha_1, \ldots, \alpha_r$ von f in $Z \setminus K$, so betrachtet man das Minimalpolynom m_{α_1} von α_1 über K. Dieses ist nach [1] Satz 5.4 b) ein Teiler von f, sodass $m'_{\alpha_1} := \Phi(m_{\alpha_1})$ ein Teiler von $f' = \Phi(f)$ ist, denn es gilt $\Phi(f) = \Phi(m_{\alpha_1} \cdot q) = \Phi(m_{\alpha_1}) \cdot \Phi(q)$ für ein geeignetes Polynom $q \in K[T]$. Da f' in Z' in Linearfaktoren zerfällt, hat m'_{α_1} eine Nullstelle α'_1 in Z'. Nach Satz 1.6 gibt es dann einen Isomorphismus $\widehat{\varphi} : K(\alpha_1) \to K'(\alpha'_1)$ mit $\widehat{\varphi}|K = \varphi$ und $\widehat{\varphi}(\alpha_1) = \alpha'_1$. Für $K(\alpha_1), K'(\alpha'_1), \widehat{\varphi}, f, Z, Z'$ gilt nun, dass f höchstens $r-1$ Nullstellen in $Z \setminus K(\alpha_1)$ hat. Deswegen kann auf $K(\alpha_1), K'(\alpha'_1), \widehat{\varphi}, f, Z, Z'$ die Induktionsannahme angewandt werden und man erhält so unmittelbar die Behauptung, d.h. es gibt einen Isomorphismus $\psi : Z \to Z'$ mit $\psi|K(\alpha_1) = \widehat{\varphi}$, der die Menge der Nullstellen von f in Z auf die Menge der Nullstellen von f' in Z' abbildet.

□

Jetzt sind die benötigten Hilfsmittel für den Beweis der Eindeutigkeit eines Zerfällungskörpers $\mathrm{ZFK}_K(f)$ zu einem Polynom $f \in K[T]$ vorhanden, deswegen folgt nun der nachstehende Satz.

1.9 Satz (Eindeutigkeit) *Seien K ein Körper und $f \in K[T]$ ein nicht-konstantes Polynom. Sind $Z \supseteq K$ und $Z' \supseteq K$ Zerfällungskörper von f, so gibt es einen Isomorphismus $\psi : Z \to Z'$ mit $\psi|K = \mathrm{id}_K$, der die Menge der Nullstellen von f in Z auf die Menge der Nullstellen von f in Z' abbildet.*

Z ist also bis auf Isomorphie eindeutig und es kann von dem Zerfällungskörper eines nicht-konstanten Polynoms gesprochen werden.

Beweis: Setzt man $K = K'$ und $\varphi = \mathrm{id}_K$, so folgt aus Satz 1.8, dass es einen Isomorphismus $\psi : Z \to Z'$ gibt mit $\psi|K = \varphi = \mathrm{id}_K$, der die Menge der Nullstellen von f in Z auf die Menge der Nullstellen von f in Z' abbildet, denn es gilt $f' = \Phi(f) = \Phi(\sum_{i=0}^n a_i T^i) = \sum_{i=0}^n \varphi(a_i) T^i = \sum_{i=0}^n \mathrm{id}_K(a_i) T^i = \sum_{i=0}^n a_i T^i = f$, falls f die Form $f = \sum_{i=0}^n a_i T^i$, $a_i \in K$ hat. Das ist aber gerade die Behauptung.

□

1.10 Beispiele

a) *Sei $f := T^5 - 1 \in \mathbb{Q}[T]$ ein Polynom. Die Nullstellen von f sind dann $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ für $\alpha := e^{\frac{2\pi i}{5}} = \cos(\frac{2\pi}{5}) + i \sin(\frac{2\pi}{5})$. Damit läßt sich f wie folgt schreiben $f = (T-1)(T-\alpha)(T-\alpha^2)(T-\alpha^3)(T-\alpha^4)$, d.h. f zerfällt über $\mathbb{Q}(\alpha)$ in Linearfaktoren. Nach Satz 1.4 ist aber $\mathbb{Q}(1, \alpha, \alpha^2, \alpha^3, \alpha^4) = \mathbb{Q}(\alpha) \supset \mathbb{Q}$ ein Zerfällungskörper von f. Dieser ist nach Satz 1.9 eindeutig (bis auf Isomorphie).*

b) *Sei $g := 5T^5 + 15T^3 - 10T^2 - 30 \in \mathbb{Q}[T]$. g läßt sich nach dem Faktorisieren in $\mathbb{Q}$ ausdrücken durch $g = 5(T^3 - 2)(T^2 + 3)$ oder nach dem Faktorisieren in $\mathbb{C}$ durch $g = 5(T - \alpha_1)(T - \alpha_2)(T - \alpha_3)(T - \beta_1)(T - \beta_2)$ für $\alpha_1 := \sqrt[3]{2}$, $\alpha_2 := \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}}$, $\alpha_3 := \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}}$, $\beta_1 := i\sqrt{3}$ und $\beta_2 := -i\sqrt{3}$. Offensichtlich zerfällt g über $\mathbb{C}$ in Linearfaktoren, doch nach Satz 1.4 ist $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2) \subset \mathbb{C}$ ein Zerfällungskörper von g. Wegen $\alpha_3 = (\frac{\alpha_2}{\alpha_1})^2 \in \mathbb{Q}(\alpha_1, \alpha_2)$ und $\beta_2 = -\beta_1 \in \mathbb{Q}(\beta_1)$ gilt $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2) = \mathbb{Q}(\alpha_1, \alpha_2, \beta_1)$, das ist nach Satz 1.9 der (bis auf Isomorphie) eindeutig bestimmte Zerfällungskörper von g. Damit gibt es keinen echten Zwischenkörper von $\mathbb{Q}(\alpha_1, \alpha_2, \beta_1) : \mathbb{Q}$, über dem g in Linearfaktoren zerfällt.*

2 Separable und normale Körpererweiterungen

2.1 Definition *Eine Körpererweiterung $L : K$ heißt normal, wenn gilt:*

a) $L : K$ ist algebraisch.

b) Jedes irreduzible Polynom $f \in K[T]$, das in L eine Nullstelle hat, zerfällt über L in Linearfaktoren.

Bedingung *b)* ist offensichtlich gleichwertig damit, dass für jedes $a \in L$ gilt: Das Minimalpolynom von a über K zerfällt über L in Linearfaktoren.

2.2 Satz *Seien K und K' Körper, $\varphi : K \to K'$ ein Isomorphismus und $\Phi : K[T] \to K'[T]$ der zugehörige Isomorphismus der Polynomringe. Ferner sei f ein nicht-konstantes Polynom aus $K[T]$.*
Ist dann $Z \supseteq K$ ein Zerfällungskörper von f und $Z' \supseteq K'$ ein Zerfällungskörper von $f' := \Phi(f)$, so gibt es zu jeder Nullstelle α eines irreduziblen Faktors g von f in Z und zu jeder Nullstelle β von $g' := \Phi(g)$ in Z' einen Isomorphismus $\psi : Z \to Z'$ mit $\psi(\alpha) = \beta$ und $\psi(x) = \varphi(x)$ für alle $x \in K$, der die Menge der Nullstellen von f in Z auf die Menge der Nullstellen von f' in Z' abbildet.

Beweis: Da g irreduzibel ist, gibt es nach Satz 1.6 einen Isomorphismus $\widehat{\varphi} : K(\alpha) \to K'(\beta)$ mit $\widehat{\varphi}(x) = \varphi(x)$ für alle $x \in K$ und $\widehat{\varphi}(\alpha) = \beta$.
Da $Z \supseteq K(\alpha)$ ein Zerfällungskörper von f und $Z' \supseteq K'(\beta)$ ein Zerfällungskörper von f' ist, gibt es nach 1.8 einen Isomorphismus $\psi : Z \to Z'$ mit $\psi(x) = \widehat{\varphi}(x)$ für alle $x \in K(\alpha)$, der die Menge der Nullstellen von f in Z auf die Menge der Nullstellen von f' in Z' abbildet.
Das heißt, es gilt $\psi(x) = \widehat{\varphi}(x) = \varphi(x)$ für alle $x \in K$ und $\psi(\alpha) = \widehat{\varphi}(\alpha) = \beta$.

□

2.3 Satz *Für eine endliche Körpererweiterung $L : K$ sind folgende Aussagen äquivalent:*

1) $L : K$ ist normal.

2) $L \supseteq K$ ist Zerfällungskörper eines Polynoms $f \in K[T]$.

3) Ist $L' : L$ eine Körpererweiterung und $\varphi : L \to L'$ ein Körperhomomorphismus mit $\varphi | K = \mathrm{id}_K$, so gilt $\varphi(L) \subseteq L$.

Beweis: *1) ⇒ 2)* Da $L : K$ eine endliche Körpererweiterung ist, gibt es nach [1] Satz 5.14 über K algebraische Elemente $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$. Für jedes $i \in \{1, \ldots, n\}$ zerfällt das Minimalpolynom f_i von a_i nach Voraussetzung über L in Linearfaktoren. Ebenso zerfällt das Produkt $f := f_1 \cdot \ldots \cdot f_n \in K[T]$ über L in Linearfaktoren. Ist N die Menge aller Nullstellen von$f$ in L, so gilt:

$$L = K(a_1, \ldots, a_n) \subseteq K(N) \subseteq L.$$

Folglich ist $L = K(N)$ der Zerfällungskörper von f.
2) ⇒ 3) Wegen *2)* und 1.4 gibt es ein $f \in K[T]$ und $a_1, \ldots, a_n, b \in L$ mit $f = b \cdot (T - a_1) \cdot \ldots \cdot (T - a_n)$ und $L = K(a_1, \ldots, a_n)$. Haben L' und $\varphi : L \to L'$ die in *3)* verlangten Eigenschaften, so gilt $f(\varphi(a_i)) = \varphi(f(a_i)) = \varphi(0) = 0$ für jedes $i \in \{1, \ldots, n\}$, d.h. $\varphi(a_i)$ ist die Nullstelle des Polynoms $f \in K[T]$ für alle

$i \in \{1, \ldots, n\}$. Man erhält $\varphi(\{a_1, \ldots, a_n\}) \subseteq \{a_1, \ldots, a_n\}$. Sei nun $y \in \varphi(L)$ beliebig. Folglich existiert ein $x \in L$ mit $y = \varphi(x)$. Da $L = K(a_1, \ldots, a_n) = K[a_1, \ldots, a_n]$ nach [1] Korollar 5.8 gilt, existiert ein Polynom $g \in K[T_1, \ldots, T_n]$ mit $x = g(a_1, \ldots, a_n)$. Weil $\varphi(\{a_1, \ldots, a_n\}) \subseteq \{a_1, \ldots, a_n\}$ ist und φ nach Voraussetzung ein Körperhomomorphismus ist, erhält man $\varphi(x) = \varphi(g(a_1, \ldots, a_n)) = g(\varphi(a_1), \ldots, \varphi(a_n)) \in L$. Daraus folgt $\varphi(L) \subseteq L$.
3) ⇒ 1) Als endliche Körpererweiterung ist $L : K$ nach [1] 5.13 *a)* algebraisch. Sei f ein irreduzibles Element von $K[T]$, das eine Nullstelle a in L hat. Wählt man $a_1, \ldots, a_n \in L$ so, dass $L = K(a, a_1, \ldots, a_n)$ gilt und bezeichnet man für jedes i mit f_i das Minimalpolynom von a_i über K, so ist L ein Zwischenkörper des Zerfällungskörpers $L' \supseteq K$ von $g := f \cdot f_1 \cdot \ldots \cdot f_n$. f zerfällt natürlich über L' in Linearfaktoren. Ist aber $b \in L'$ eine Nullstelle von f, so gibt es nach 2.2 einen K-Automorphismus ψ von L' mit $\psi(a) = b$. Wendet man die Bedingung *3)* auf den Körperhomomorphismus $\psi|L : L \to L'$ an, so erhält man $b = \psi(a) \in L$; f zerfällt also schon über L in Linearfaktoren.

□

2.4 Beispiele
Da die Körpererweiterung $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ der Zerfällungskörper des Polynoms $T^2 - 2 \in \mathbb{Q}[T]$ ist, ist sie normal. Die Körpererweiterung $\mathbb{Q}(\sqrt[4]{2}) \supseteq \mathbb{Q}(\sqrt{2})$ ist als Zerfällungskörper des Polynoms $T^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[T]$ ebenfalls normal. Die Körpererweiterung $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ ist jedoch nicht normal, denn das Polynom $T^4 - 2 = (T^2 - \sqrt{2})(T^2 + \sqrt{2}) = (T - \sqrt[4]{2})(T + \sqrt[4]{2})(T - i\sqrt[4]{2})(T + i\sqrt[4]{2})$ ist ein irreduzibles Element von $\mathbb{Q}[T]$ und hat eine Nullstelle in $\mathbb{Q}(\sqrt[4]{2})$, es zerfällt über $\mathbb{Q}(\sqrt[4]{2})$ aber nicht in Linearfaktoren.

2.5 Definition *Sei K ein Körper und $Z \supseteq K$ der Zerfällungskörper eines nicht-konstanten Polynoms $f \in K[T]$. Ferner sei a ein Element von Z.*
Die natürliche Zahl

$$\mu(f; a) := \max\{n \in \mathbb{N} : (T - a)^n \text{ teilt } f \text{ in } Z[T]\}$$

heißt Vielfacheit von f in a.
Man nennt a eine einfache Nullstelle von f, wenn $\mu(f; a) = 1$ gilt. Im Falle $\mu(f; a) \geq 2$ heißt a mehrfache Nullstelle von f.

2.6 Definition *a) Sei K ein Körper. Ein nicht-konstantes Polynom $f \in K[T]$ heißt separabel, wenn jeder irreduzible Faktor von f in seinem Zerfällungskörper nur einfache Nullstellen hat.*

b) Sei $L : K$ eine Körpererweiterung. Ein Element $a \in L$ heißt separabel über K, wenn a Nullstelle eines separablen Polynoms $f \in K[T]$ ist.

c) Eine Körpererweiterung $L : K$ heißt separabel, wenn jedes $a \in L$ separabel über K ist.

d) Ein Körper K heißt vollkommen, wenn jedes nicht-konstante Polynom aus $K[T]$ separabel ist.

Ist $L : K$ eine Körpererweiterung, so ist ein über K algebraisches $a \in L$ offensichtlich genau dann separabel über K, wenn das Minimalpolynom von a über K separabel ist. In 2.12 werden wir sehen, dass jeder Körper der Charakterisitik Null vollkommen ist. Ebenso ist jeder endliche Körper vollkommen.

Mehrfache Nullstellen charakterisiert man in der Analysis durch das Verschwinden der Ableitung. Dieses Verfahren wird hier imitiert.

2.7 Definition *Sei $R[T]$ der Polynomring über einem kommutativen Ring. Die Abbildung*

$$D : R[T] \to R[T], \qquad \sum_{i=0}^{n} a_i T^i \mapsto \sum_{i=1}^{n} i a_i T^{i-1}$$

heißt formale Differentiation in $R[T]$. Sie ist (wie man leicht nachrechnet) eine Derivation von $R[T]$, d.h. es gilt

$$D(af + bg) = aD(f) + bD(g) \qquad \text{und} \qquad D(f \cdot g) = f \cdot D(g) + g \cdot D(f)$$

für alle $f, g \in R[T]$ und alle $a, b \in R$.

2.8 Lemma *Sei K ein Körper und $Z \supseteq K$ der Zerfällungskörper eines nicht-konstanten Polynoms $f \in K[T]$. Dann gilt für jedes $a \in Z$:*

1) $\mu(f; a) = 1 \Leftrightarrow f(a) = 0$ und $(Df)(a) \neq 0$.

2) $\mu(f; a) > 1 \Leftrightarrow f(a) = 0$ und $(Df)(a) = 0$.

Beweis: Sei $r := \mu(f; a)$, dann gibt es nach [1] Lemma 3.12 $g \in Z[T]$ mit $f = (T-a)^r g$ und $g(a) \neq 0$, und man erhält

$$D(f) = (T-a)^{r-1}(rg + (T-a)D(g)).$$

1) "$\Longrightarrow$" Aus $r = 1$ folgt $f = (T-a)g$ und $f(a) = 0$. Mit $Df = g + (T-a)D(g)$, erhält man $(Df)(a) = g(a) \neq 0$.
"$\Longleftarrow$" Falls $r \geq 2$ gilt, ist $(Df)(a) = 0$. Widerspruch!
2) ist die Negation von *1)*.

□

Ob ein Polynom über einem Körper K mehrfache Nullstellen in seinem Zerfällungskörper über K hat, kann man feststellen, ohne die Nullstellen zu kennen.

2.9 Lemma *Sei K ein Körper, f ein nicht-konstantes Polynom aus $K[T]$ und $Z \supseteq K$ sein Zerfällungskörper. Dann sind äquivalent:*

1) f hat in Z mehrfache Nullstellen.

2) f und Df haben in $K[T]$ einen nicht-konstanten gemeinsamen Teiler.

Beweis: *1) $\Rightarrow$ 2)* Sei $a \in Z$ mehrfache Nullstelle von f und g das Minimalpolynom von a über K. Wegen $f(a) = (Df)(a) \overset{2.8}{=} 0$ ist dann nach [1] 5.4 *b)* g ein gemeinsamer Teiler von f und Df.
2) $\Rightarrow$ 1) Sei $g \in K[T]$ ein gemeinsamer Teiler von f und Df mit $\operatorname{grad}(g) \geq 1$ und $a \in Z$ eine Nullstelle von g. Dann existieren f_1 und f_2 aus $K[T]$ mit $gf_1 = f$ und $gf_2 = Df$. Es gilt

$$g(a) \cdot f_1(a) = f(a) = 0 \qquad \text{und} \qquad g(a) \cdot f_2(a) = (Df)(a) = 0,$$

so dass nach 2.8 a eine mehrfache Nullstelle von f ist.

□

2.10 Satz *Sei K ein Körper. Ein irreduzibles Polynom $f \in K[T]$ ist genau dann separabel, wenn $Df \neq 0$ gilt.*

Beweis: Sei $Z \supseteq K$ der Zerfällungskörper von f. Ist $Df = 0$, so ist nach 2.8 jede Nullstelle von f in Z eine mehrfache Nullstelle. f ist dann also nach Definition 2.6 nicht separabel. Ist $Df \neq 0$, so ist f separabel. Denn andernfalls hätte f in seinem Zerfällungskörper nicht nur einfache Nullstellen, was nach Lemma 2.9 äquivalent dazu wäre, dass f und Df in $K[T]$ einen nicht-konstanten gemeinsamen Teiler g hätten. Da f irreduzibel in $K[T]$ ist, würde dies zum Widerspruch $\text{grad}(g) = \text{grad}(f) > \text{grad}\,(Df)$ führen.

□

2.11 Lemma *Sei K ein Körper und $f \in K[T]$.*
Im Falle $\text{char}(K) = 0$ gilt:

$$Df = 0 \Leftrightarrow f \text{ ist konstant.}$$

Im Falle $\text{char}(K) = p > 0$ gilt:

$$Df = 0 \Leftrightarrow \text{Es gibt } g \in K[T] \text{ mit } f(T) = g(T^p).$$

Beweis: Sei $\text{char}(K) = 0$.
"$\Longrightarrow$" **Annahme:** f ist nicht konstant, d.h. $f = \sum_{i=0}^{n} a_i T^i \in K[T]$ mit $n \geq 1$. Dann ist $Df = \sum_{i=1}^{n} i a_i T^{i-1} \in K[T]$ und nach Voraussetzng $Df = 0$. Daraus folgt $ia_i \overset{[1]}{\underset{\text{Aufg.11}}{=}} (i1_K) \cdot a_i = 0 \;\forall\, i \in \{1, \ldots, n\}$ mit $a_i \neq 0$. Dies führt zum Widerspruch, da $\text{char}(K) = 0$.
"$\Longleftarrow$" Es gilt $K[T] \ni f = c \neq 0$. Folglich, $Df = 0$.

Ist $p :=\text{char}(K) > 0$ und $f = \sum_{i=0}^{n} a_i T^i$, so ist $Df = 0$ gleichbedeutend damit, dass p für alle $i \in \{1, \ldots, n\}$ mit $a_i \neq 0$ ein Teiler von i ist, dass also f von der Gestalt

$$f = a_0 + a_p T^p + a_{2p} T^{2p} + \ldots + a_{mp} T^{mp}$$

ist. Das war aber zu zeigen.

□

Aus 2.10 und 2.11 folgt unmittelbar:

2.12 Korollar *Jeder Körper der Charakteristik Null ist vollkommen.*

Beweis: Seien K ein Körper mit $\text{char}(K) = 0$ und $f \in K[T]$ ein nicht-konstantes Polynom. Nach [1] Satz 3.27 läßt sich f als Produkt von (endlich vielen) irreduziblen Polynomen darstellen. Diese Darstellung ist eindeutig bis auf die Reihenfolge und Multiplikation mit Einheiten. Sei g ein beliebiger irreduzibler Faktor von f. Nach Lemma 2.11 gilt $Dg \neq 0$ und nach Satz 2.10 ist $g \in K[T]$ separabel und damit auch f.

□

In [1] Satz 7.6 haben wir eine Galoiserweiterung $L : K$ definiert durch die Bedingungen, dass $L : K$ endlich und K der Fixkörper von $\text{Gal}(L : K)$ ist. Aufgrund dieser Definition konnten wir den Hauptsatz der Galois-Theorie mit elementaren Hilfsmitteln der Linearen Algebra beweisen. Für die Anwendungen ist es jedoch wichtig, leichter nachprüfbare Kriterien für Galoiserweiterungen zu kennen.

2.13 Theorem *Für eine Körpererweiterung $L : K$ sind folgende Aussagen äquivalent:*

1) $L : K$ ist eine Galoiserweiterung.

2) Die Körpererweiterung $L : K$ ist endlich, normal und separabel.

3) $L \supseteq K$ ist Zerfällungskörper eines separablen Polynoms aus $K[T]$.

Bevor wir diesen Satz beweisen, notieren wir ein Lemma.

2.14 Lemma *Sei $L : K$ eine Galoiserweiterung und $a \in L$. $a_1, \ldots, a_n$ seien die paarweise verschiedenen Bilder von n K-Automorphismen $\sigma_i \in Gal(L : K)$ von a. Dann ist $f := (T - a_1) \cdot \ldots \cdot (T - a_n)$ das Minimalpolynom von a über K.*

Beweis: Sei $f = \sum_{i=1}^{n} b_i T^i \in L[T]$.
Zuerst zeigen wir, dass die Koeffizienten von f aus K sind, d.h. $f \in K[T]$. Sei $\tau \in \mathrm{Gal}(L : K)$ beliebig und $\bar{\tau} : L[T] \to L[T]$ der zugehörige Polynomringisomorphismus. Dann gilt

$$\bar{\tau}(f) = \bar{\tau}(\prod_{i=1}^{n}(T - \sigma_i(a))) = \prod_{i=1}^{n}(T - \tau(\sigma_i(a))) = \prod_{i=1}^{n}(T - \sigma_i(a)) = f.$$

Weiter erhält man

$$\bar{\tau}(f) = \sum_{i=0}^{n} \tau(b_i)T^i = \sum_{i=0}^{n} b_i T^i = f.$$

Der Koeffizientenvergleich ergibt $\tau(b_i) = b_i$ für alle $\tau \in \mathrm{Gal}(L : K)$, d.h. es gilt $b_i \in L^G \overset{[1]\ 7.6}{=} K$ für alle $i \in \{0, \ldots, n\}$. Weiterhin ist f normiert, a ist die Nullstelle von f, da $\mathrm{id}_L \in \mathrm{Gal}(L : K)$. Bleibt noch zu zeigen, dass f irreduzibel ist.
Angenommen, f ist reduzibel. Dann existieren Polynome g, h aus $K[T]$ mit $g \cdot h = f$ und $0 < \mathrm{grad}(g) < \mathrm{grad}(f)$. Da $g(a) \cdot h(a) = f(a) = 0$ gilt, folgt $g(a) = 0$ oder $h(a) = 0$. Sei o.B.d.A. $g(a) = 0$. Dann gibt es zu jedem $i \in \{1, \ldots, n\}$ ein ψ_i aus $\mathrm{Gal}(L : K)$ mit $a_i = \psi_i(a)$ und man erhält $g(a_i) = g(\psi_i(a)) = \psi_i(g(a)) = 0$ für jedes i. Da die Elemente $a_1, \ldots, a_n$ paarweise verschieden sind, besitzt g n Nullstellen, d.h. $\mathrm{grad}(g) \geq n$. Widerspruch!

□

Beweis:[von 2.13] *1) ⇒ 2)* Nach [1] Satz 7.6 ist jede Galoiserweiterung endlich. Nach 2.14 ist das Minimalpolynom jedes Elementes $a \in L$ über K endliches Produkt von paarweise verschiedenen Linearfaktoren aus $L[T]$. Die Körpererweiterung $L : K$ ist also auch normal und separabel.
2) ⇒ 3) Da die Körpererweiterung $L : K$ endlich und normal ist, ist sie nach 2.3 Zerfällungskörper eines Polynoms $f \in K[T]$. Wir wollen zeigen, dass f notwendigerweise separabel sein muss. Ist g ein irreduzibler Faktor von f und $a \in L$ eine Nullstelle von g, so ist g bis auf einen konstanten Faktor gleich dem Minimalpolynom von a über K. Da a separabel über K ist, ist g separabel.
3) ⇒ 1) Sei $L : K$ der Zerfällungskörper eines separablen Polynoms $f \in K[T]$. Mit $G :=\mathrm{Gal}(L : K)$ gilt $K \subseteq L^G$ und mit [1] Satz 7.3 folgt $|G| = \left[L : L^G\right] \leq [L : K] < \infty$. Nun zeigen wir durch die Induktion über die Anzahl r der Nullstellen von f in $L \backslash K$, dass auch $K \supseteq L^G$ gilt.
Im Falle $r = 0$ gilt $L = K$ und daher $L^G = K$. Sei nun $r \geq 1$ und $a \in L \backslash K$ eine Nullstelle von f. Das Minimalpolynom g von a über K ist ein Teiler von f in $K[T]$. Setzt man

$K' := K(a)$, so ist $L \supseteq K'$ der Zerfällungskörper des separablen Polynoms $f \in K'[T]$, das $r-1$ Nullstellen in $L \backslash K'$ hat. Nach Induktionsvoraussetzung ist daher $L : K'$ eine Galoiserweiterung, so dass es eine endliche Untergruppe G' von G gibt mit

$$K' = L^{G'} \qquad \text{und} \qquad G' = \mathrm{Gal}(L : K') \subseteq G.$$

Sei nun $x \in L^G \subseteq L^{G'} = K' = K(a)$. Ist $n :=\mathrm{grad}(g)$, so existiert eine K-Basis $\{1, a, a^2, \ldots, a^{n-1}\}$ von K' (wegen [1] 5.9) und es gilt

$$x = c_{n-1}a^{n-1} + \ldots + c_1 a + c_0,$$

wobei $c_0, \ldots, c_{n-1}$ die Elemente aus K sind. Sind $a = a_1, a_2, \ldots, a_n$ die Nullstellen von g in L, so gibt es nach 2.2 zu jedem $i \in \{1, \ldots, n\}$ ein $\varphi_i \in G$ mit $\varphi_i(a) = a_i$ und man erhält

$$x = \varphi_i(x) = c_{n-1}a_i^{n-1} + \ldots + c_1 a_i + c_0$$

für jedes i. Das Polynom

$$h := c_{n-1}T^{n-1} + \ldots + c_1 T + (c_0 - x) \in L[T]$$

hat daher die n Nullstellen $a_1, \ldots, a_n$. Wegen $\mathrm{grad}(h) \leq n-1$ folgt $h = 0$ und damit $x = c_0 \in K$.

□

Mit Hilfe von 2.12 folgt aus 2.13 sofort:

2.15 Korollar *Ist K ein Körper der Charakteristik Null, so ist eine Körpererweiterung $L : K$ genau dann eine Galoiserweiterung, wenn sie Zerfällungskörper eines Polynoms aus $K[T]$ ist.*

Beweis: Da $\mathrm{char}(K) = 0$, ist K nach 2.12 vollkommen. Und nach 2.13 ist $L : K$ genau dann eine Galoiserweiterung, wenn sie der Zerfällungskörper eines Polynoms aus $K[T]$ ist.

□

3 Die Galoisgruppe eines Polynoms

Im Folgenden bezeichne f ein rationales Polynom, $Z := \mathrm{ZFK}_{\mathbb{Q}}(f)$ sei der (bis auf Isomorphie eindeutig bestimmte) Zerfällungskörper von f über $\mathbb{Q}$. Ferner sei $G := \mathrm{Gal}_{\mathbb{Q}}(f) = \mathrm{Gal}(Z : \mathbb{Q})$ die Galoisgruppe von f. Die Frage ist, zu welcher (endlichen) Gruppe G isomorph ist. Dabei beschränken wir uns hier auf Polynome vom Grade ≤ 4. Daraus folgt, dass G auflösbar ist und dass die Nullstellen von f durch Radikale ausgedrückt werden können. Weiter werden wir annehmen, dass f normiert ist. Dieses kann bei einem beliebigen Polynom durch Teilen des Leitkoeffizienten, der $\neq 0$ ist, erreicht werden.
Zunächst beschreiben wir die generelle Struktur von G.

3.1 Satz *Sei $f \in \mathbb{Q}[T]$, $\mathrm{grad}(f) = n \geq 1$, $G := Gal_{\mathbb{Q}}(f)$ die Galoisgruppe von f und $N_f := \{\alpha_1, \ldots, \alpha_r\} \subseteq \mathbb{C}$ $(r \geq 1)$ die Nullstellenmenge von f. Dann gilt:*

a) G ist isomorph zu einer Untergruppe von S_r.

b) Ist f irreduzibel, so folgt

i) n teilt $|G|$.

ii) G ist isomorph zu einer transitiven Untergruppe von S_n.

Dabei heißt eine Untergruppe $U \leq S_n$ transitiv, falls $\forall\ i, j \in \{1, \ldots, n\}\ \exists\ \sigma \in U : \sigma(i) = j$.

Beweis: a) Sei $\alpha_i \in N_f$ beliebig $(1 \leq i \leq r)$ und sei $\sigma \in G$. Damit ist $\sigma(\alpha_i) \in N_f$. Also erzeugt jedes Element $\sigma \in G$ eine Permutation $\pi_\sigma \in S_r$.
Definiere

$$h :\ G \to S_r \quad , \quad \sigma \mapsto \pi_\sigma.$$

Es ist klar, dass h ein Homomorphismus ist. h ist außerdem injektiv. Dafür ist z.z., dass $\mathrm{Kern}(h) = \{\mathrm{id}_Z\}$ gilt. Sei also $\sigma \in G$ mit $h(\sigma) = \mathrm{id}_{S_r} \Rightarrow \sigma(\alpha_i) = \alpha_i\ \forall\ i \in \{1, \ldots, n\} \Rightarrow \sigma(c) = c\ \forall\ c \in Z \Rightarrow \sigma = \mathrm{id}_Z \Rightarrow h$ injektiv. Damit kann G also mit einer Untergruppe von S_r identifiziert werden.

b) i) Es gilt $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \mathrm{grad}(f) = n$. Damit folgt nach dem Gradsatz, dass $[\mathbb{Q}(\alpha_1) : \mathbb{Q}]$ ein Teiler von $[Z : \mathbb{Q}]$ ist. Da $Z : \mathbb{Q}$ aber eine Galoiserweiterung ist, folgt $[Z : \mathbb{Q}] = |G| \Rightarrow [\mathbb{Q}(\alpha_1) : \mathbb{Q}] \mid |G| \Rightarrow n \mid |G|$.
ii) Sei $i \neq j$ beliebig $(1 \leq i, j \leq n)$. Dann ex. nach (1.7) ein $\mathbb{Q}$-Isomorphismus $\sigma : \mathbb{Q}(\alpha_i) \xrightarrow{\cong} \mathbb{Q}(\alpha_j)$, $\sigma(\alpha_i) = \alpha_j$. Durch Fortsetzung dieses Isomorphismus erhält man einen $\mathbb{Q}$-Isomorphismus von Z. Damit existiert ein $\psi \in U \leq S_n$ mit $\psi(\alpha_i) = \alpha_j$, folglich ist U eine transitive Untergruppe von S_n.

□

Wir betrachten nun die trivialen Fälle, in denen der Grad von f 1 oder 2 ist.

$\underline{\mathrm{grad}(f) = 1:}$ $f = T + b \Rightarrow N_f = \{-b\} \subseteq \mathbb{Q} \Rightarrow Z = \mathbb{Q} \Rightarrow G = \{e\}$.

$\underline{\mathrm{grad}(f) = 2:}$ $f = T^2 + pT + q \Rightarrow N_f = \{-\frac{p}{2} \pm \sqrt{D}\}$, wobei $D = (\frac{p}{2})^2 - q$ ist $\Rightarrow Z = \mathbb{Q}(\sqrt{D}) \overset{f \text{ irred.}}{\Rightarrow} [Z : \mathbb{Q}] = 2 = |G| \Rightarrow G \cong S_2 \cong \mathbb{Z}_2$.

3.2 Definition *Sei $f \in \mathbb{Q}[T]$, grad$(f) = r$ und $N_f := \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{C}$ $(n \leq r)$ die Nullstellenmenge von f. Setze*

$$\triangle_f := \prod_{i<j}(\alpha_i - \alpha_j) = (\alpha_1 - \alpha_2) \cdot (\alpha_1 - \alpha_3) \cdot \ldots \cdot (\alpha_{n-1} - \alpha_n) \in Z.$$

Dann heißt $D_f := \triangle_f^2$ die Diskriminante von f.

3.3 Satz *Sei $f \in \mathbb{Q}[T]$ irreduzibel über $\mathbb{Q}$, grad$(f) = n$, $N_f := \{\alpha_1, \ldots, \alpha_n\}$. Dann gilt:*

a) $\triangle_f \neq 0$.

b) $\triangle_f \in \mathbb{Q} \iff G \leq A_n$.

c) Sei $U :=$ Gal$(Z : \mathbb{Q}(\triangle_f))$. Dann ist $U \leq A_n$.

Beweis: Setze $D := D_f$ und $\triangle := \triangle_f$. Klar ist $D \in \mathbb{Q}$, da jedes Element von G die Nullstellen von f permutiert und D somit fest lässt. Sei nun $\sigma \in G$ beliebig. Dann gilt: $D = \sigma(D) = \sigma(\triangle^2) = \sigma(\triangle)^2 \Rightarrow \sigma(\triangle) \in \{\pm\triangle\}$.

a) Annahme: $\triangle = 0 \Rightarrow$ es existieren $i \neq j$ mit $\alpha_i = \alpha_j \Rightarrow f$ ist nicht separabel, ein Widerspruch zu (2.12). Folglich $\triangle \neq 0$.

b) 1. $\triangle \in \mathbb{Q}$. Annahme: $\exists\ \sigma \in G$ mit sign$(\sigma) = -1 \Rightarrow \sigma(\triangle) = -\triangle$ $(\neq \triangle$, da $\triangle \neq 0) \Rightarrow \sigma$ lässt das Element $\triangle$ nicht fest, folglich kann $\triangle$ nicht im Grundkörper $\mathbb{Q}$ liegen, ein Widerspruch. Damit ist sign$(\sigma) = 1 \Rightarrow G \leq A_n$.
2. $\triangle \notin \mathbb{Q} \Rightarrow \exists\ \psi \in G : \psi(\triangle) = -\triangle \Rightarrow$ sign$(\psi) = -1 \Rightarrow G \not\leq A_n$.

c) $\mathbb{Q}(\triangle)$ ist ein Körper $\Rightarrow -\triangle \in \mathbb{Q}(\triangle)$. Darauf wende b) an.

□

Dieser Satz zeigt in Verbindung mit der vorherigen Definition, dass G genau dann eine Untergruppe von A_n ist, wenn D_f eine Quadratzahl ist (, welches äquivalent dazu ist, dass $\triangle \in \mathbb{Q}$).
Sei f nun ein über $\mathbb{Q}$ irreduzibles Polynom vom Grade 3. Nach (3.1) ist G isomorph zu einer transitiven Untergruppe von S_3. An dem Untergruppenverband dieser Gruppe sieht man leicht, dass hierfür nur die Gruppen A_3 und S_3 selbst in Frage kommen. Falls D_f eine Quadratzahl ist, folgt somit sofort $G \cong A_3 \cong \mathbb{Z}_3$, andernfalls $G \cong S_3$.
Folgendes Lemma gibt eine explizite Formel zur Berechnung von D_f in Abhängigkeit von den Koeffizienten von f an.

3.4 Lemma *Sei $f := T^3 + aT^2 + bT + c \in \mathbb{Q}[T]$ und D_f die Diskriminante von f. Dann hat das Polynom $g := f(T - \frac{a}{3})$ die Form $g = T^3 + pT + q \in \mathbb{Q}[T]$ und es gilt*

$$D_f = -4p^3 - 27q^2.$$

Beweis: (Idee) Zunächst zeigen wir, dass $D_f = D_g$ gilt. Dazu beobachte man, dass $D_g = \left(\alpha_1 - \frac{a}{3} - \alpha_2 + \frac{a}{3}\right)^2 \cdot \left(\alpha_1 - \frac{a}{3} - \alpha_3 + \frac{a}{3}\right)^2 \cdot \left(\alpha_2 - \frac{a}{3} - \alpha_3 + \frac{a}{3}\right)^2 = (\alpha_1 - \alpha_2)^2 \cdot (\alpha_1 - \alpha_3)^2 \cdot (\alpha_2 - \alpha_3)^2 = D_f$ gilt.

Sei nun $N_f = \{\alpha_1, \alpha_2, \alpha_3\} \Rightarrow f = (T - \alpha_1) \cdot (T - \alpha_2) \cdot (T - \alpha_3) = T^3 - (\alpha_1 + \alpha_2 + \alpha_3)T^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_2)T - \alpha_1\alpha_2\alpha_3$. Damit ergeben sich durch Koeffizientenvergleich folgende Beziehungen:

$$\alpha_1 + \alpha_2 + \alpha_3 = 0 \quad , \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p \quad , \quad \alpha_1\alpha_2\alpha_3 = -q.$$

Weiterhin gilt, da α_i Nullstelle von f ist, dass $\alpha_i^3 + p\alpha_i + q = 0 \iff \alpha_i^3 = -p\alpha_i - q$.

Diese beiden Bedingungen setzt man nun in die Formel für die Diskriminante ein und benutzt dabei die oben berechneten Abhängigkeiten.

□

Durch diese Formel ist es nun unter Berücksichtigung der vorherigen Überlegungen einfach, zu entscheiden, ob $G \cong \mathbb{Z}_3$ oder $G \cong S_3$ gilt. Beachtlich ist, dass man dafür nicht die Nullstellen von f kennen muss, sondern G von den Koeffizienten von f abhängt. Hierzu zwei

Beispiele

1. Sei $f = T^3 - 3T + 1 \in \mathbb{Q}[T]$. f ist über $\mathbb{Q}$ irreduzibel, da $f(1) \neq 0$ und $f(-1) \neq 0$. Weiter ist $D_f = -4 \cdot (-3)^3 - 27 \cdot 1^2 = 108 - 27 = 81 = 9^2 \Rightarrow G \cong \mathbb{Z}_3$.
2. Sei $g = T^3 + 3T^2 - T - 1 \in \mathbb{Q}[T]$. Wegen $g(1) \neq 0$ und $g(-1) \neq 0$ ist g ebenfalls irreduzibel über $\mathbb{Q}$. Durch die Substitution $T := U - \frac{3}{3} = U - 1$ erhält man das Polynom $h = U^3 - UT + 2$, wobei $D_h = -4 \cdot (-4)^3 - 27 \cdot 2^2 = 256 - 108 = 148 = D_g$, welches keine Quadratzahl ist. Folglich $G \cong S_3$.

Nun betrachten wir den Fall, dass $\text{grad}(f) = 4$ gilt, d.h. vorgelegt sei das normierte und irreduzible Polynom $f = T^4 + aT^3 + bT^2 + cT + d \in \mathbb{Q}[T]$.

Nach (3.1) kann G nur isomorph zu einer transitiven Untergruppe von S_4 sein. Diese sind S_4, A_4, D_4 (die Diedergruppe der Ordnung 8), $\mathbb{Z}_4$ und $V = \mathbb{Z}_2 \times \mathbb{Z}_2$, die Klein'sche Vierergruppe, welche in den folgenden Überlegungen eine wichtige Rolle spielen wird. Deshalb geben wir hier die Elemente von V explizit an:

$$V = \{(1),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

Diese Gruppe enthält also − neben dem neutralen Element − drei Permutationen, die ihrerseits aus je zwei disjunkten Transpositionen bestehen.

Insgesamt gibt es also fünf mögliche Gruppen, zu denen G isomorph sein kann. Wir werden zeigen, dass auch alle Möglichkeiten auftreten, es also zu jeder der obigen Gruppen auch ein Polynom 4. Grades gibt, dessen Galoisgruppe isomorph dazu ist.

Zunächst ist jedoch etwas Vorarbeit nötig. Ein, von f abhängiges Polynom, wird entscheidende Informationen über die Struktur von G liefern, die sogenannte *kubische Resolvente von f.*

3.5 Definition *Sei $f \in \mathbb{Q}[T]$, $grad(f) = 4$, $N_f = \{\alpha_1, \ldots, \alpha_4\}$. Setze*

$$x := \alpha_1 \cdot \alpha_2 + \alpha_3 \cdot \alpha_4 \quad , \quad y := \alpha_1 \cdot \alpha_3 + \alpha_2 \cdot \alpha_4 \quad , \quad z := \alpha_1 \cdot \alpha_4 + \alpha_2 \cdot \alpha_3.$$

Dann heißt das Polynom

$$f_{Res} := (T - x) \cdot (T - y) \cdot (T - z) \in \mathbb{Q}(x, y, z)[T]$$

die kubische Resolvente von f.

3.6 Lemma *Sei $f := T^4 + aT^3 + bT^2 + cT + d \in \mathbb{Q}[T]$. Dann ist*

$$f_{Res} = T^3 - bT^2 + (ac - 4d)T - a^2d + 4bd - c^2.$$

Insbesondere ist $f_{Res} \in \mathbb{Q}[T]$.

Beweis: (Idee) Sei $N_f = \{\alpha_1, \ldots, \alpha_4\} \subseteq Z \Rightarrow f = (T-\alpha_1)\cdot(T-\alpha_2)\cdot(T-\alpha_3)\cdot(T-\alpha_4)$. Nun multipliziere man die einzelnen Faktoren aus führe einen Koeffizientenvergleich mit der ausfaktorisierten Form $f = T^4 + aT^3 + bT^2 + cT + d$ durch.
Weiter betrachte man die kubische Resolvente $f_{Res} = (T - x) \cdot (T - y) \cdot (T - z)$ ebenfalls in ihrer ausfaktorisierten Form und nutze anschließend die Definitionen von x, y und z (siehe (3.5)).

□

3.7 Lemma *Sei $L : K$ eine Körpererweiterung und seien α_1, $\alpha_2 \in L$ algebraisch über K. Es existiere ein Isomorphismus $h : K(\alpha_1) \to K(\alpha_2)$ mit $h|K = id_K$ und $h(\alpha_1) = \alpha_2$. Dann stimmen die Minimalpolynome von α_1 und α_2 über K überein.*

Beweis: Sei $m_{\alpha_1} := \sum_{i=0}^{n} a_i T^i$ das Minimalpolynom von α_1 über K. Dann ist z.z., dass α_2 ebenfalls eine Nullstelle von m_{α_1} ist. Sei $\bar{h}$ der zu h gehörige Isomorphismus der Polynomringe $K(\alpha_1)[T]$ und $K(\alpha_2)[T]$. Dann gilt $\bar{h}(m_{\alpha_1}) = \bar{h}\left(\sum_{i=0}^{n} a_i T^i\right) = m_{\alpha_1}$, da $h|K = \mathrm{id}_K$. Weiter ist

$$m_{\alpha_1}(\alpha_2) = \sum_{i=0}^{n} a_i \cdot \alpha_2^i \overset{\text{Vor.}}{=} \sum_{i=0}^{n} a_i \cdot h(\alpha_1)^i = h\left(\sum_{i=0}^{n} a_i \cdot \alpha_1^i\right) = h\left(m_{\alpha_1}(\alpha_1)\right) = h(0) = 0,$$

also ist α_2 Nullstelle von m_{α_1}.

□

3.8 Lemma *Sei $f \in \mathbb{Q}[T]$ ein über $\mathbb{Q}$ irreduzibles Polynom, $grad(f) = 4$, f_{Res} die kubische Resolvente von f und $N_{f_{Res}} = \{x, y, z\}$ die Nullstellenmenge von f_{Res}. Es bezeichne $G := Gal_{\mathbb{Q}}(f)$ und V die Klein'sche Vierergruppe. Dann gilt:*

a) *In der bestehenden Galois-Korrespondenz der Körpererweiterung $Z : \mathbb{Q}$ entspricht der Zwischenkörper $\mathbb{Q}(x, y, z)$ der Untergruppe $G \cap V$.*

b) *$G \cap V$ ist Normalteiler in G.*

c) *$\mathbb{Q}(x, y, z) : \mathbb{Q}$ ist eine Galoiserweiterung.*

d) *$Gal(\mathbb{Q}(x, y, z) : \mathbb{Q}) \cong G/(G \cap V)$.*

Beweis: a) $Z : \mathbb{Q}$ ist eine Galoiserweiterung. Dann ist z.z., dass $\mathbb{Q}(x, y, z) = Z^{G \cap V}$ gilt. Aufgrund der bestehenden Galoiskorrespondenz können wir Behauptung aber auch gruppentheoretisch beschreiben und hierfür einen Beweis liefern. Es ist also äquivalent z.z., dass $G \cap V = \mathrm{Gal}(Z : \mathbb{Q}(x, y, z))$ gilt.
"$\subseteq$": Sei $\sigma \in G \cap V \Rightarrow \sigma \in V$. Damit liegen die Elemente x, y und z im Fixkörper von σ, welches man elementweise nachprüfen kann. Wähle z.B. das Element $\psi := (1\ 3)(2\ 4) \in V$ und das Element $x \in \mathbb{Q}(z)$. Dann gilt $\psi(x) = \alpha_3 \cdot \alpha_4 + \alpha_1 \cdot \alpha_2 = \alpha_1 \cdot \alpha_2 + \alpha_3 \cdot \alpha_4 \Rightarrow x \in \mathrm{Fix}(\psi)$. Insgesamt ist σ also nicht nur ein $\mathbb{Q}$-Automorphismus von Z, sondern sogar ein $\mathbb{Q}(x, y, z)$-Automorphismus von Z. Dies bedeutet aber, dass $\sigma \in \mathrm{Gal}(Z : \mathbb{Q}(x, y, z))$ gilt. Folglich ist $G \cap V \subseteq \mathrm{Gal}(Z : \mathbb{Q}(x, y, z))$.
"$\supseteq$": Sei $\sigma \notin G \cap V \Rightarrow \sigma \in G \backslash (G \cap V) \Rightarrow \forall\, \sigma :\ x \notin \mathrm{Fix}(\sigma)$ oder $y \notin \mathrm{Fix}(\sigma)$ oder $z \notin \mathrm{Fix}(\sigma)$, welches man leicht sieht. Damit ist σ <u>kein</u> $\mathbb{Q}(x, y, z)$-Automorphismus von Z, also gilt $\sigma \notin \mathrm{Gal}(Z : \mathbb{Q}(x, y, z)) \Rightarrow \mathrm{Gal}(Z : \mathbb{Q}(x, y, z)) \subseteq G \cap V$.
Insgesamt gilt damit die behauptete Gleichheit.

b) Klar ist $G \leq S_4$. Außerdem ist V Normalteiler in S_4, mithin ist auch $G \cap V \lhd G$.

c) und d) folgen direkt aus dem Hauptsatz der Galoistheorie.

□

3.9 Satz *Sei $f \in \mathbb{Q}[T]$ ein über $\mathbb{Q}$ irreduzibles Polynom, $grad(f) = 4$, $f_{Res} := (T - x)(T - y)(T - z) \in \mathbb{Q}[T]$ die kubische Resolvente von f. Bezeichne $m := [\mathbb{Q}(x, y, z) : \mathbb{Q}]$. Dann gilt:*

a) *$m = 6 \iff G \cong S_4$.*

b) *$m = 3 \iff G \cong A_4$.*

c) *$m = 1 \iff G \cong V$.*

d) *$m = 2 \iff \left\{ \begin{array}{ll} G \cong D_4 & , \text{falls } f \text{irreduzibel über } \mathbb{Q}(x, y, z) \text{ist} \\ G \cong \mathbb{Z}_4 & , \text{sonst} \end{array} \right\}$.*

Beweis: $\mathbb{Q}(x, y, z)$ ist ZFK von einem Polynom dritten Grades, also ist $[\mathbb{Q}(x, y, z) : \mathbb{Q}] \leq 3 \cdot 2 \cdot 1 = 6$. Weiter gilt nach dem Gradsatz:

$$[Z : \mathbb{Q}] = [Z : \mathbb{Q}(x, y, z)] \cdot [\mathbb{Q}(x, y, z) : \mathbb{Q}].$$

Wegen $[Z : \mathbb{Q}] = |G|$ und $[Z : \mathbb{Q}(x, y, z)] = |G \cap V|$ (3.8d) folgt sofort $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = \frac{|G|}{|G \cap V|}$, damit ist m ein Teiler von $[Z : \mathbb{Q}]$.
Insgesamt ergibt sich, dass $m \in \{1, 2, 3, 6\}$ gilt. Aufgrund dieser Feststellung und der Tatsache, dass alle möglichen Gruppen im Satz erwähnt werden, genügt es, in jedem Fall die Implikation "$\Leftarrow$" zu zeigen.

a) $G \cong S_4 \Rightarrow G \cap V = V \Rightarrow m = |G/V| = \frac{24}{4} = 6.$

b) $G \cong A_4 \Rightarrow G \cap V = V \Rightarrow m = |G/V| = \frac{12}{4} = 3.$

c) $G \cong V \Rightarrow G \cap V = G \Rightarrow m = |G/G| = \frac{4}{4} = 1.$

d) $G \cong D_4 \Rightarrow G \cap V = V \Rightarrow m = |G/V| = \frac{8}{4} = 2.$

$G \cong Z_4 \Rightarrow |G \cap V| = 2 \Rightarrow m = |G/V| = \frac{4}{2} = 2.$

Es bleibt nun der Fall $m = 2$, in dem die Äquivalenz der Aussagen tatsächlich gezeigt werden muss. Sei dazu $N_f = \{\alpha_1, \ldots, \alpha_4\} \subseteq Z$ und gelte ferner $G \cong D_4$. Damit ist $G \cap V = V$ und $V \cong \mathrm{Gal}(Z : \mathbb{Q}(x, y, z))$. Da V eine transitive Untergruppe von S_4 ist, gibt es nach (1.7) für alle $i,\ j \in \{1, 2, 3, 4\}$ ein $\sigma \in V$, so dass

$$\sigma : \ \mathbb{Q}(x, y, z)(\alpha_i) \ \longrightarrow \ \mathbb{Q}(x, y, z)(\alpha_j) \quad , \quad \sigma(\alpha_i) = \alpha_j$$

ein Isomorphismus ist. Nach (3.8) sind α_i und α_j damit Nullstellen des gleichen irreduziblen Polynoms $g \in \mathbb{Q}(x, y, z)$. Damit sind $\alpha_1, \ldots, \alpha_4$ Nullstellen von g und $\mathrm{grad}(g) \geq 4 \Rightarrow g = (T - \alpha_1) \cdot (T - \alpha_2) \cdot (T - \alpha_3) \cdot (T - \alpha_4) \cdot h$ für $h \in \mathbb{Q}(x, y, z)$ geeignet. Es folgt, dass f ein Teiler von g ist. Da g irreduzibel ist, ist $\mathrm{grad}(f) = 0$ oder $\mathrm{grad}(f) = \mathrm{grad}(g)$. Offensichtlich gilt $\mathrm{grad}(f) = \mathrm{grad}(g)$. Also ist $f \sim g$, welches die Irreduzibilität von f über $\mathbb{Q}(x, y, z)$ impliziert.
Gelte andererseits $G \cong \mathbb{Z}_4 \Rightarrow |G \cap V| = 2 \Rightarrow G \cap V$ ist <u>keine</u> transitive Untergruppe von S_4, es gibt also ein Paar $i \neq j$ mit der Eigenschaft, dass es <u>kein</u> $\sigma \in G \cap V$ mit $\sigma(\alpha_i) = \alpha_j$ gibt.
Analog zu oben gibt es nun wieder einen Isomorphismus

$$\vartheta : \ \mathbb{Q}(x, y, z)(\alpha_i) \ \longrightarrow \ \mathbb{Q}(x, y, z)(\alpha_j) \quad , \quad \vartheta(\alpha_i) = \alpha_j.$$

ϑ ist somit die Einschränkung eines $\mathbb{Q}(x, y, z)$-Automorphismus von Z. Solch ein Isomorphismus existiert jedoch nicht, da es in G kein Element π mit $\pi(i) = j$ gibt. Damit können α_i und α_j nicht die Nullstellen des gleichen über $\mathbb{Q}(x, y, z)$ irreduziblen Polynoms sein. Seien $g_1, g_2 \in \mathbb{Q}(x, y, z)$ zwei irreduzible und verschiedene Polynome, so dass $g_1(\alpha_i) = 0$ und $g_2(\alpha_j) = 0$ gilt. Dann folgt $f = g_1 \cdot g_2 \cdot h$, wobei $h \in \mathbb{Q}(x, y, z)$ geeignet gewählt ist. Also ist f reduzibel über $\mathbb{Q}(x, y, z)$.

Damit ist Satz (3.9) vollständig bewiesen.

□

Abschließend behandeln wir einige

Beispiele

1. Sei $f = T^4 - T + 1 \in \mathbb{Q}[T]$. f ist irreduzibel und die kubische Resolvente von f ist $f_{\text{Res}} = T^3 - 4T - 1$, welches ein über $\mathbb{Q}$ irreduzibles Polynom ist, da $f_{Res}(1) \neq 0$ und $f_{Res}(-1) \neq 0$. Weiter gilt $D_{f_{\text{Res}}} = 4^4 - 27 = 229$, welches kein Quadrat in $\mathbb{Q}$ ist. Folglich ist $\text{Gal}_{\mathbb{Q}}(f_{\text{Res}}) \cong S_3$ und damit ergibt sich nach (3.9), dass $m = 6$ gilt. Man erhält $G \cong S_4$.

2. Sei $f = T^4 - 6T^2 + 8T + 28 \in \mathbb{Q}[T]$. f hat keine rationale Nullstelle, da f normiert ist und für jeden Teiler t von 28 folgt, dass $f(t) \neq 0$ ist. Dass f keinen Teiler vom Grade 2 hat, zeigt man durch Koeffizientenvergleich (f lässt sich im Falle der Reduzibilität durch $(T^2 + aT + b) \cdot (T^2 + cT + d)$ darstellen, welches man zum Widerspruch führt). Also ist f irreduzibel über $\mathbb{Q}$. Weiter ist $f_{\text{Res}} = T^3 + 6T^2 - 112T - 736$. Substituiere mit $T := U - 2$. Man erhält das Polynom $g = U^3 - 124U - 496$, welches irreduzibel über $\mathbb{Q}$ ist, da es keine Teiler des Absolutglieds 496 als Nullstelle hat. Es ist $D_g = D_{f_{\text{Res}}} = 4 \cdot 124^3 - 27 \cdot 496^2 = (31 \cdot 32)^2$, also eine Quadratzahl. Damit ist $\text{Gal}_{\mathbb{Q}}(f_{\text{Res}}) \cong A_3 \Rightarrow m = 3 \Rightarrow G \cong A_4$.

3. Sei $f = T^4 + 1 \in \mathbb{Q}[T]$. Das Polynom $f(T + 1) = T^4 + 4T^3 + 6T^2 + 4T + 2$ ist nach Eisenstein ($p = 2$) irreduzibel über $\mathbb{Q}$, mithin ist auch f irreduzibel über $\mathbb{Q}$. Weiter ist $f_{\text{Res}} = T^3 - 4T = T \cdot (T - 2) \cdot (T + 2)$. Man sieht leicht, dass f_{Res} nur rationale Nullstellen hat, folglich ist $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 1$ und $G \cong V$.

4. Sei $f = T^4 - 2 \in \mathbb{Q}[T]$. f ist nach Eisenstein ($p = 2$) irreduzibel über $\mathbb{Q}$ und $f_{\text{Res}} = T^3 + 8T = T \cdot (T^2 + 8) = T \cdot (T + 2 \cdot \sqrt{2} \cdot i) \cdot (T - 2 \cdot \sqrt{2} \cdot i) \Rightarrow x = 0,\ y = 2 \cdot \sqrt{2} \cdot i,\ z = -2 \cdot \sqrt{2} \cdot i \Rightarrow \mathbb{Q}(x, y, z) = \mathbb{Q}(2 \cdot \sqrt{2} \cdot i) = \mathbb{Q}(\alpha)$ mit $\alpha = \sqrt{2} \cdot i$. $m_\alpha = T^2 + 2$ ist Minimalpolynom von α über $\mathbb{Q} \Rightarrow [\mathbb{Q}(\sqrt{2} \cdot i) : \mathbb{Q}] = 2$. Wegen $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2} \cdot i)$ ist f irreduzibel über $\mathbb{Q}(\sqrt{2} \cdot i)$. Folglich ist $G \cong D_4$.

5. Sei $f = T^4 + 4T^2 + 2 \in \mathbb{Q}[T]$. f ist nach Eisenstein irreduzibel über $\mathbb{Q}$ und $f_{\text{Res}} = T^3 - 4T^2 - 8T + 32 = (T - 4) \cdot (T^2 - 8) \Rightarrow x = 4,\ y = -\sqrt{8},\ z = \sqrt{8} \Rightarrow \mathbb{Q}(x, y, z) = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{2})$. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \Rightarrow G \cong D_4$ oder $G \cong \mathbb{Z}_4$. Die Substitution $U := T^2$ liefert das Polynom $\tilde{f} = U^2 + 4U + 2$ mit $N_{\tilde{f}} = \{-2 - \sqrt{2},\ -2 + \sqrt{2}\} \Rightarrow N_f = \{\pm\sqrt{-2 \pm \sqrt{2}}\} \Rightarrow f = \left(T^2 - (-2 + \sqrt{2})\right) \cdot \left(T^2 - (-2 - \sqrt{2})\right) \in \mathbb{Q}(\sqrt{2})[T] \Rightarrow f$ reduzibel über $\mathbb{Q}(\sqrt{2}) \Rightarrow G \cong \mathbb{Z}_4$.

4 Der Fundamentalsatz der Algebra

4.1 Satz *Ist K ein Körper, so sind folgende Aussagen äquivalent:*

1) Jedes nicht-konstante Polynom aus $K[X]$ hat eine Nullstelle in K.

2) Jedes nicht-konstante Polynom aus $K[X]$ zerfällt über K in Linearfaktoren, d.h, es gibt $a_1, ..., a_n, b \in K$ mit $f = b(X - a_1)...(X - a_n)$.

3) Ein Polynom aus $K[X]$ ist genau dann irreduzibel, wenn es den Grad 1 hat.

4) Ist $L \supset K$ eine algebraische Körpererweiterung, so gilt $L = K$.

Beweis:

1) $\Rightarrow$ 2) Sei $f \in K[X]$ nicht konstant,so gibt es nach 1) ein $a \in K$ mit $f(a) = 0$ und daher ein $g \in K[X]$ mit $f = (X - a)g$. Ist g konstant, so ist man fertig, anderfalls wendet man 1) auf g an und setzt das Verfahren fort, bis das Verfahren ein konstantes Polynom liefert. Das Verfahren terminiert, da der Grad des Faktorpolynoms immer um eins kleiner wird.

2) $\Rightarrow$ 3) ist klar

3) $\Rightarrow$ 4) Jedes $a \in L$ ist algebraisch über K, sein Minimalpolynom f über K ist irreduzibel und normiert und es gilt $f(a) = 0$. Wegen 3) gilt daher $f = X - a$, also $X - a \in K[X]$, so dass $a \in K$ folgt.

4) $\Rightarrow$ 1) Sei $f \in K[X]$ nicht konstant. Wegen 1.3 (Satz von Kronecker) gibt es einen Oberkörper L von K und ein $a \in L$ mit $f(a) = 0$. Die Körpererweiterung $K(a) \supset K$ ist nach 4.3 algebraisch und wegen 4) ist $K(a) = K \Rightarrow a \in K$. Also hat f eine Nullstelle in K.

4.2 Definition *Ein Körper K heisst <u>algebraisch</u> <u>abgeschlossen</u>, wenn er eine (und damit jede) der Bedingungen aus Satz 4.1 erfüllt.*

4.3 Satz *Sei $L \supset K$ eine Körpererweiterung. Dann gilt:*

1) Ist die Körpererweiterung $L \supset K$ endlich, so ist sie algebraisch und es gibt $a_1, ..., a_n \in L$ mit $L = K(a_1, ..., a_n)$.

2) Gibt es über K algebraische Elemente $a_1, ..., a_n \in L$ mit $L = K(a_1, ..., a_n)$, so ist die Körpererweiterung endlich und damit algebraisch.

Beweis:

1) Sei m die Dimension des K-Vektorraums L, so sind für jedes $a \in L$ die Elemente $1, a, a^2, ..., a^m$ linear abhängig über K. Zu jedem $a \in L$ gibt es daher ein Polynom $f \in K[X]\backslash\{0\}$ mit $f(a) = 0$. Ausserdem gilt $L = K(a_1, ..., a_m)$ für jede Basis $(a_1, ..., a_m)$ des K-Vektorraums L.

2) Es wird durch vollständige Induktion bewiesen. Ist $a \in L$ algebraisch über K und gilt $L = K(a)$, so folgt $[L : K] < \infty$, da ein Minimalpolynom von a über K existiert, das einen endlichen Grad besitzt, der gleich $[L : K]$ ist. Sei nun $n \in \mathbb{N} \setminus \{0\}$ und die Behauptung richtig für alle Körpererweiterungen $L' \supset K$, bei denen L' durch Adjunktion von n über K algebraischen Elementen an K entsteht. Gilt dann $L = K(a_1, ..., a_{n+1})$ mit über K algebraischen Elementen $a_1, ..., a_{n+1} \in L$ so folgt $[L : K] = [K(a_1, ..., a_n)(a_{n+1}) : K(a_1, ..., a_n)][K(a_1, ..., a_n) : K] < \infty$, da ein Minimalpolynom von a_{n+1} über $K(a_1, ..., a_n)$ existiert, das einen endlichen Grad besitzt, der gleich $[K(a_1, ..., a_n)(a_{n+1}) : K(a_1, ..., a_n)]$ ist, und wegen Voraussetzung $[K(a_1, ..., a_n) : K] < \infty$, denn a_{n+1} ist auch algebraisch über $K(a_1, ..., a_n)$.

4.4 Lemma *Jeder Körper der Charakteristik Null ist vollkommen.*

4.5 Satz *Sei $L \supset K$ eine Körpererweiterung.Gibt es über K separable Elemente $a_1, ..., a_n \in L$ mit $L = K(a_1, ..., a_n)$, so gilt:*

1) Die Körpererweiterung $L \supset K$ ist endlich und separabel.

2) Es gibt einen Oberkörper L' von L, so dass $L' \supset K$ eine Galoiskörpererweiterung ist.

Beweis:

Sei $L \supset K$ eine Körpererweiterung. Gibt es über K separable Elemente $a_1, ..., a_n \in L$ mit $L = K(a_1, ..., a_n)$. Wegen 4.3.2 ist die Körpererweiterung $L \supset K$ endlich. Für jedes $i \in \{1, ..., n\}$ ist ferner das Minimalpolynom f_i von a_i über K separabel, so dass auch das Polynom $f = f_1 \cdot ... \cdot f_n \in K[X]$ separabel ist. Sei L' der Zerfällungskörper von f über L, dann ist L' auch der Zerfällungskörper von f über K,da $L = K(a_1, ..., a_n)$ ist. Wegen 2.13 ist $L' \supset K$ eine Galoiserweiterung und auch separabel. $L \supset K$ ist daher auch separabel.

4.6 Definition *Sei G eine Gruppe, e ihr neutrales Element und p eine Primzahl.*

a) G heisst $\underline{p - Gruppe}$, wenn es zu jedem $a \in G$ ein (i.a. von a abhängiges) $k \in \mathbb{N}$ gibt mit $a^{p^k} = e$.

b) Eine Untergruppe H von G heisst $\underline{p - Untergruppe}$ von G, wenn H eine p-Gruppe ist.

c) Eine Untergruppe S von G heisst $\underline{p - Sylow - Gruppe}$ in G, wenn S eine maximale p–Untergruppe von G ist, d.h. wenn gilt:

i) S ist eine p–Untergruppe von G.

ii) Es gibt keine p–Untergruppe H von G mit $S \subsetneq H$.

4.7 Satz *Sei p eine Primzahl und seien k, m, n natürliche Zahlen mit $n = p^k m$ und $p \nmid m$. Dann ist p^{k-l+1} für kein $l \in \{1, ..., k\}$ Teiler von $\binom{n}{p^l}$.*

4.8 Lemma *Sei G eine endliche Gruppe und p eine Primzahl. $k, m \in \mathbb{N}$ seien so gewählt, dass $|G| = p^k m$ und $p \nmid m$ gilt. Dann gibt es zu jedem $l \in 0, ..., k$ eine Untergruppe H von G mit $|H| = p^l$.*

Beweis:

Sei $l \in \{1, ..., k\}$ fest gewählt und sei X die Menge aller Teilmengen von G der Ordnung p^l. Bekanntlich gilt $|X| = \binom{n}{p^l}$, wenn man die Ordnung von G mit n bezeichnet. Da im Falle $l = 0$ nichts zu beweisen ist, wird $l \neq 0$ vorausgesetzt. Die Abbildung $\tau : G \times X \longrightarrow X,\ (a, U) \mapsto aU := \{au : u \in U\}$ ist eine Operation von G auf X. Aus dem letzten Satz folgt, dass p^{k-l+1} kein Teiler der Ordnung von X ist, so dass es wegen der Bahnengleichung ein $U \in X$ mit $p^{k-l+1} \nmid |G(U)|$ gibt.

Es soll gezeigt werden, dass $H = Iso_\tau(G; U)$ eine Untergruppe der Ordnung p^l von G ist: Zunächst gibt es $r, v \in \mathbb{N}$ mit $|H| = p^r v$ und $p \nmid v$ und ebenso $s, w \in \mathbb{N}$ mit $[G : H] = p^s w$ und $p \nmid w$. Da τ eine Operation der Gruppe G auf die Menge X ist und $H = Iso_\tau(G; U)$ ist, dann gilt $[G : H] = |G(U)|$, also $s \leq k - l$, und aus $|G| = |H| \cdot [G : H]$ folgt $p^k m = p^{r+s} vw$, also $k = r + s \leq r + k - l$. Man erhält $l \leq r$, so dass p^l ein Teiler der Ordnung von H ist. Da für ein $u \in U$ die Abbildung $H \to U$, $a \mapsto au$, injektiv ist, hat man anderseits auch $|H| \leq |U| = p^l$.

4.9 Korollar *Sei G eine endliche Gruppe und p eine Primzahl, so gilt:*

1) Ist p ein Teiler der Ordnung von G, so gibt es ein $a \in G$ mit $ord(a) = p$.

2) G ist genau dann eine p–Gruppe, wenn die Ordnung von G eine Potenz von p ist.

3) Gilt $|G| = p^k m$ mit $k, m \in \mathbb{N}$ und $p \nmid m$, so ist jede Untergruppe von G der Ordnung p^k eine p–Sylow–Gruppe in G.

Beweis:

1) Ist p ein Teiler der Ordnung von G, so gibt es ein $k, m \in \mathbb{N}$ mit $k \neq 0$, $p \nmid m$ und $|G| = p^k m$. Nach 4.8 gibt es eine Untergruppe H der Ordnung p von G. Als Gruppe von Primzahlordnung ist H zyklisch und für jedes erzeugende Element a von H gilt $ord(a) = p$.

2) Ist e das neutrale Element von G und gilt $|G| = p^k$, so folgt $a^{p^k} = e$ für jedes $a \in G$ d.h. G ist eine p–Gruppe. Sei umgekehrt G eine endliche p–Gruppe. Im Fall $G = \{e\}$ ist alles klar. Gilt $G \neq \{e\}$ und ist q ein Primfaktor von $|G|$, so gibt es nach 1) ein $a \in G$ mit $ord(a) = q$. Da G eine p–Gruppe ist, ist $ord(a)$ eine Potenz von p, so dass $q = p$ folgt. Daher ist p der einzige Primfaktor von $|G|$.

3) Sei S eine Untergruppe der Ordnung p^k von G und H eine p–Untergruppe von G mit $S \subset H$. Nach 2) gibt es ein $l \in \mathbb{N}$ mit $|H| = p^l$ und aus $S \subset H$ folgt $k \leq l$. Da die Ordnung von H ein Teiler der Ordnung von G ist, erhält man $l = k$ und damit $H = S$.

4.10 Satz *Sei G eine endliche Gruppe, p eine Primzahl und $k \in \mathbb{N}$ so, dass die Ordnung von G durch p^k, aber nicht durch p^{k+1} teilbar ist. Ist dann S_0 eine p–Sylow–Gruppe in G mit $|S_0| = p^k$, so gibt es zu jeder p–Untergruppe H von G ein $b \in G$ mit $H \subset bS_0b^{-1}$.*

4.11 Satz (von Sylow) *Sei G eine endliche Gruppe und p eine Primzahl, so gilt:*

1) Eine Untergruppe S von G ist genau dann eine p–Sylow–Gruppe in G, wenn $|S| = p^k$ gilt und $|G|$ durch p^k, aber nicht durch p^{k+1} teilbar ist.

2) Zu jeder p–Untergruppe H von G gibt es eine p–Sylow–Gruppe S in G mit $H \subset S$.

Beweis:

1) Dass jede Untergruppe der Ordnung p^k eine p–Sylow–Gruppe in G ist, wenn $|G|$ durch p^k, aber nicht durch p^{k+1} teilbar ist, wurde in 4.9 bewiesen. Sei umgekehrt S eine p–Sylow–Gruppe in G und $|G|$ sei durch p^k, aber nicht durch p^{k+1} teilbar. Nach 4.8 gibt es eine Untergruppe S_0 der Ordnung p^k von G. S_0 ist wegen 4.9 eine p–Sylow–Gruppe in G. Wendet man den letzten Hilfsatz auf $H = S_0$ an, so erhält man $|S| = |S_0| = p^k$.

2) Nach 4.8 und 1) gibt es in G eine p–Sylow–Gruppe S_0. Daher folgt die Behauptung aus dem vorigen Hilfsatz und 1).

4.12 Lemma *Jede Galoiserweiterung ist einfach. Sei K ein Körper der Charakteristik 0, so ist jede endliche Körpererweiterung $L \supset K$ einfach.*

4.13 Satz *Ist $f \in \mathbb{R}[X]$ ein Polynom mit ungeradem Grad, so hat f mindestens eine reelle Nullstelle.*

Beweis:

Der Beweis ist eine Übungsaufgabe zur reelen Analysis, bei der der Zwischenwertsatz für stetige Funktionen benutzt wird, der auf der Vollständigkeit von $\mathbb{R}$ beruht.

4.14 Satz *Ist $f \in \mathbb{C}[X]$ ein Polynom vom Grad 2, so zerfällt f über $\mathbb{C}$ in Linearfaktoren.*

Beweis:

Zum Beweis dieses Satzes benutzt man eine Folgerung aus den Anordnungsaxiomen von $\mathbb{R}$, dass jede nicht negative reelle Zahl eine reelle Quadratwurzel besitzt. Auf Grund

dieser Tatsache kann man nämlich für jedes $z = x + iy \in \mathbb{C}$, $x, y \in \mathbb{R}$, die komplexe Zahl $w = \sqrt{\frac{x+\sqrt{x^2+y^2}}{2}} + i\sqrt{\frac{-x+\sqrt{x^2+y^2}}{2}}$, bilden. Wegen $w^2 = z$ falls $y \geq 0$ und $\bar{w}^2 = z$ falls $y < 0$ hat jede komplexe Zahl eine komplexe Quadratwurzel. Daher kann man zu jedem Polynom $f = aX^2 + bX + c \in \mathbb{C}[X]$ vom Grad 2 die komplexen Zahlen $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$ bilden. Diese sind die Nullstellen von f.

4.15 Satz (Fundamentalsatz der Algebra) *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

1. **Beweis:**

Wegen 4.1 genügt es zu zeigen, dass $\mathbb{C}$ keine algebraische Erweiterung gestattet. Es genügt sogar zu zeigen, dass $\mathbb{C}$ keine endliche Erweiterung gestattet. Angenommen, dass $\mathbb{C}$ keine endliche Erweiterung gestattet. Sei $\alpha \in K$ beliebig (K algebraische Erweiterung) $\Rightarrow \alpha$ ist algebraisch über $\mathbb{C} \Rightarrow \mathbb{C}(\alpha) : \mathbb{C}$ ist eine endliche Körpererweiterung $\Rightarrow \mathbb{C}(\alpha) = \mathbb{C}$ $\Rightarrow \alpha \in \mathbb{C}$, also $K = \mathbb{C}$.

Sei $K \supseteq \mathbb{C}$ endlich, dann wegen 4.3.4 ist K algebraisch mit $K = \mathbb{C}(a_1, ..., a_n)$ mit $a_i \in K$ und nach 4.4 ist K separabel über $\mathbb{C}$. Dann ist $K = \mathbb{R}(b_1, ..., b_m)$ auch separabel über $\mathbb{R}$ ($K \supseteq \mathbb{C} \supseteq \mathbb{R}$). Wegen 4.5 existiert eine Galois-Erweiterung $L \supseteq \mathbb{R}$ mit $L \supseteq K$. Also genügt es zu zeigen $L = \mathbb{C}$. Wir haben $\mathbb{R} \subseteq \mathbb{C} \subseteq K \subseteq L$. Da L eine Galois-Erweiterung ist und $[\mathbb{C} : \mathbb{R}]$ gleich 2 ist,ist 2 ein Teiler der Ordnung von G. Sei $G = Gal(L : \mathbb{R})$ und $p = 2$. Nach 4.8 existiert eine 2-Sylow-Gruppe S in G. Sei L^S der Fixkörper von S. Da L eine Galois-Erweiterung ist und L^S der Fixkörper von S ist $\Rightarrow [L^S : \mathbb{R}] = [G : S]$. $[G : S]$ ist ungerade wegen 4.11.1 (da S eine 2-Sylow-Gruppe in G ist). Nach 4.10 gibt es ein Element $a \in L$ mit $L^S = \mathbb{R}(a)$. Der Grad des Minimalpolynoms von a über $\mathbb{R}$ ist gleich $[L^S : \mathbb{R}]$, also folgt aus 4.13 $L^S = \mathbb{R}$ und damit $G = S$. Aus 4.13 folgt, dass es $b \in \mathbb{R}$ so dass $f(b) = 0$ existiert. Dann $L = \mathbb{R}(a) \supseteq \mathbb{R}(b) \supseteq \mathbb{R}$ und $[\mathbb{R}(a) : \mathbb{R}] = grad(f)$ und $1 = [\mathbb{R}(b) : \mathbb{R}]$. Da f das Minimalpolynom von a ist $\Rightarrow$ f ist irreduzibel $\Rightarrow$ f ist auch das Minimalpolynom von b $\Rightarrow [\mathbb{R}(b) : \mathbb{R}] = grad(f) \Rightarrow \mathbb{R}(a) = \mathbb{R}(b)$. G ist also eine 2-Gruppe. Da $H = Gal(L : \mathbb{C})$ eine Untergruppe von G ist, gibt es wegen des Satzes von Lagrange ein $r \in \mathbb{N}$ mit $ord(H) = 2^r$. Wäre $r > 0$, so gäbe es eine Untergruppe $H' \subset H$ mit $ord(H') = 2^{r-1}$. Sei $L' = Fix(L, H')$, so ist $[L' : \mathbb{C}] = [H : H'] = 2$. Das kann aber nicht sein nach 4.14 $\Rightarrow r = 0 \Rightarrow ord(H) = 1$ und also $|Gal(L : \mathbb{C})| = 1$. Nach dem Hauptsatz der Galois-Theorie ist $[L : \mathbb{C}] = 1$ und also $L = \mathbb{C}$.

2. **Beweis:**

Wegen 4.1 genügt es zu zeigen, dass jedes nicht-konstante $f \in \mathbb{C}[X]$ eine komplexe Nullstelle besitzt. Ist $\overline{f}$ das Polynom mit den komplexen konjugiert Koeffizienten, so hat $f \cdot \overline{f}$ reelle Koeffizienten. Sei $a \in \mathbb{C}$ eine Nullstelle von $f \cdot \overline{f}$, so ist a Nullstelle von f oder von $\overline{f}$. Im letzteren Fall gilt aber $0 = \overline{f}(a) = \overline{\overline{f}(a)} = f(\overline{a})$. Also ist $\overline{a} \in \mathbb{C}$ eine Nullstelle von f. Es genügt also zu zeigen, dass jedes nicht–konstante $f \in \mathbb{R}[X]$ eine komplexe Nullstelle besitzt. Sei $n = grad(f)$, so können wir $n = 2^l m$ mit ungeradem m schreiben und Induktion über l führen. Für $l = 0$ folgt die Behauptung aus Satz 4.13 (da n ungerade ist). Sei $l > 0$ und $K \supset \mathbb{C}$ der Zerfällunskörper von f und $f = (x - a_1) \cdot ... \cdot (x - a_n)$ mit $a_1, ..., a_n \in K$. Wir definieren $b_{rs} = a_r + a_s + \lambda a_r a_s$ für ein festes $\lambda \in \mathbb{R}$ und $r, s \in \{1, ..., n\}$ sowie $g = \prod_{1 \leq r \leq s \leq n}(x - b_{rs}) \in K[X]$. Für jedes $\varphi \in Gal(K : \mathbb{R})$ gilt $\varphi(\{a_1, ..., a_n\}) \subseteq \{a_1, ..., a_n\}$ wegen $f \in \mathbb{R}[X]$ und Satz 2.2. Die Koeffizienten von g sind invariant unter $Gal(K : \mathbb{R})$. Da ferner K der Zerfällungskörper von $(x^2 + 1)f$ über $\mathbb{R}$ ist, ist $K \supset \mathbb{R}$ eine Galois–Erweiterung (Korollar 2.15) und $\mathbb{R}$ ein Körper der Charakteristik Null ist, erhält man also $g \in \mathbb{R}[X]$. Weiter ist $grad(g) = \frac{1}{2}n(n+1) = 2^{l-1}m(n+1)$ und wegen $l \geq 1$ ist $m(n+1)$ ungerade (da $l \geq 1$ ist, ist n gerade und

damit $n+1$ ungerade). Nach Induktionsannahme hat g eine komplexe Nullstelle, d.h, es gibt zu unserem vorgegebenen $\lambda \in \mathbb{R}$ Indizes $r, s \in \{1, ..., n\}$ mit $r \leq s$, so dass $b_{rs} = a_r + a_s + \lambda a_r a_s$ in $\mathbb{C}$ liegt. Da es unendlich viele reelle Zahlen aber nur endlich viele solcher Indizen gibt, können wir $\lambda, \mu \in \mathbb{R}$ mit $\lambda \neq \mu$ und $r \leq s$ finden, so dass $a_r + a_s + \lambda a_r a_s$ und $a_r + a_s + \mu a_r a_s$ in $\mathbb{C}$ liegen. Daraus folgt $a_r \cdot a_s \in \mathbb{C}$ und $a_r + a_s \in \mathbb{C}$ (denn wenn man beides subtrahiert, erhält man $(\lambda - \mu) a_r a_s \in \mathbb{C}$ und damit $a_r a_s \in \mathbb{C}$), d.h, das Polynom $(x - a_r)(x - a_s) \in K[X]$ hat komplexe Koeffienten. Nach 4.14 sind a_r und a_s komplexe Zahlen. Also hat f eine komplexe Nullstelle.

Die Lemmata 4.4 und 4.12 und die Sätze 4.7 und 4.10 wurden in der Vorlesung Algebra bewiesen.

5 Einheitswurzeln und Kreisteilungspolynome

In dieser Ausarbeitung wird gezeigt, wie der Grad einer n-ten Einheitswurzel über $\mathbb{Q}$ bestimmt wird. Die Grundlage dafür bietet [2], Seiten 169 bis 175.

5.1 Definition *Sei K ein Körper und $n \in \mathbb{N} \setminus \{0\}$. Ein Element a eines Oberkörpers von K heißt n-te Einheitswurzel über K, wenn*

$$a^n = 1$$

gilt, d.h. wenn a Nullstelle (NS) des Polynoms $T^n - 1$ ist.

5.2 Bezeichnung *Sei K ein Körper, dann bezeichnet K_n den Zerfällungskörper (ZFK) von $T^n - 1$ über K und $E_n(K)$ die Menge der in K_n liegenden n-ten Einheitswurzeln (EW) über K.*

5.3 Bemerkung *Sei $n \in \mathbb{N} \setminus \{0\}$. Dann gilt:*

1. $E_n(\mathbb{Q}) = \left\{ e^{(\frac{2 \cdot \pi \cdot i \cdot k}{n})} \mid k \in \{0, \ldots, n-1\} \right\} \subset \mathbb{C}$.
2. $K_n = K(E_n)$.
3. *Ist K ein Körper der Charakteristik $p > 0$, so gilt $\forall m, n \in \mathbb{N} \setminus \{0\}$ mit $n = m \cdot p$:*

$$K_m = K_n \text{ und } E_n(K) = E_m(K).$$

4. *Für jeden Körper K ist $E_n(K)$ eine zyklische Untergruppe von $(K_n^*, \cdot)$. Ihre Ordnung ist n, wenn $char(K) \nmid n$ ist, d.h. das Polynom $T^n - 1 \in K[T]$ hat in diesem Fall keine mehrfache NS in seinem ZFK.*
5. *Für jeden Körper K ist $K_n : K$ eine Galois-Erweiterung (GE).*

Beweis: Zu 1) Trivial, denn es gilt $(e^{(\frac{2 \cdot \pi \cdot i \cdot k}{n})})^n = 1$.
Zu 2) Adjungiert man die Nullstellen, so erhält man den ZFK K_n.
Zu 3) Sei K_n der ZFK von $T^n - 1$. Dann gilt:

1. $\underbrace{(T^m - 1) \cdot \ldots \cdot (T^m - 1)}_{p-mal} = (T^m - 1)^p \overset{p \in \mathbb{P}}{=} (T^{mp} - 1) = T^n - 1$
2. $\varepsilon \in E_n(K) \Leftrightarrow \varepsilon^n - 1 = 0 = (\varepsilon^m - 1)^p \Leftrightarrow \varepsilon^m - 1 = 0 \Leftrightarrow \varepsilon \in E_m(K)$

$$\Rightarrow E_n(K) = E_m(K)$$

3. $K_n = ZFK_K(T^n - 1) = K(E_n(K)) = K(E_m(K)) = K_m$

Zu 4) Hierzu reicht es aus zu zeigen, dass $E_n(K)$ eine Untergruppe von K_n^* ist. Dazu sei $f = T^n - 1$.
U_1) $\varepsilon_1, \varepsilon_2 \in E_n(K) \Rightarrow \varepsilon_1 \cdot \varepsilon_2 \in E_n(K)$

$$(\varepsilon_1 \cdot \varepsilon_2)^n = \varepsilon_1^n \cdot \varepsilon_2^n = 1 \cdot 1 = 1 \Rightarrow \varepsilon_1 \cdot \varepsilon_2 \in E_n(K)$$

U_2) $1 \in E_n(K)$

$$f(1) = 1^n - 1 = 1 - 1 = 0 \Rightarrow 1 \in E_n(K)$$

U_3) $\varepsilon \in E_n(K) \Rightarrow \varepsilon^{-1} \in E_n(K)$

$$f(\varepsilon^{-1}) = (\varepsilon^{-1})^n - 1 = (\varepsilon^n)^{-1} - 1 = 1 - 1 = 0 \Rightarrow \varepsilon^{-1} \in E_n(K)$$

Da nun $E_n(K)$ eine endliche Untergruppe von $(K_n^*, \cdot)$ ist, folgt aus [1] Satz (3.39) , dass $E_n(K)$ zyklisch ist.
Es gilt $\mid E_n(K) \mid = n$, falls $char(K) \not\mid n$. Dazu sei $\varepsilon \in E_n(K)$. $f(\varepsilon) = 0 \Leftrightarrow \varepsilon^n - 1 = 0$ und $(Df)(\varepsilon) \neq 0 \Leftrightarrow n \cdot \varepsilon^{n-1} \neq 0$, denn $char(K) \not\mid n$. Daraus folgt aus (2.8) des Algebra-Seminars, f hat nur einfache Nullstellen, ist also seperabel.
Zu 5) Da nach 4) $T^n - 1$ für $char(K) \not\mid n$ separabel ist, können wir aus (2.13) des Algebra-Seminars schließen, dass $K_n : K$ eine GE ist. Mit Hilfe von 3) folgt diese Aussage auch für den Fall $char(K) \mid n$.

□

5.4 Definition *Sei $n \in \mathbb{N} \setminus \{0\}$.*
Die Gruppe $(\mathbb{Z}_n^*, \cdot)$ heißt die Einheitengruppe von $\mathbb{Z}_n$.

$$\mathbb{Z}_n^* = \{[a]_n \mid a \in \mathbb{Z}, ggT(a, n) = 1\}$$

Ist $\varphi(n)$ die Anzahl der natürlichen Zahlen m mit $1 \leq m \leq n$, die zu n teilerfremd sind, so heißt die Abbildung $\varphi : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}, n \mapsto \varphi(n)$ die Eulersche φ-Funktion.

5.5 Satz *1. Für jedes $n \in \mathbb{N} \setminus \{0\}$ gilt:*

$$\mathbb{Z}_n^* = \big\{m + n\mathbb{Z} \mid \ m \in \{0, \ldots, n-1\}, ggT(m, n) = 1\big\}.$$

2. Für jedes $n \in \mathbb{N} \setminus \{0\}$ gilt:

$$ord(\mathbb{Z}_n^*) = \varphi(n).$$

3. Für alle teilerfremden m,$n \in \mathbb{N} \setminus \{0\}$ gilt

$$\varphi(mn) = \varphi(m)\varphi(n).$$

4. Ist $n \in \mathbb{N} \setminus \{0, 1\}$ und gilt $n = p_1^{l_1} \cdot \ldots \cdot p_r^{l_r}$, wobei $p_1, \ldots, p_r$ die verschiedenen Primteiler von n sind, so gilt

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_r})$$

Beweis: Diese Beweise sind Wiederholungen aus [1] oder aus den Grundzügen der Algebra (GdA). Es wird dem ambitionierten Leser überlassen, diese nachzulesen.
Zu 1) GdA (6.14)
Zu 2) [1](1.23)
Zu 3) [1] Aufgabe 9a) und (1.25)
Zu 4) Zu zeigen: $\varphi(p^k) = p^k - p^{k-1}$.

$$ggT(a, p^k) = 1 \Leftrightarrow ggT(a, p) = 1 \Leftrightarrow p \not| a$$

Daher sind unter den Zahlen von 1 bis p^k genau p^{k-1} Zahlen nicht teilerfrend zu p^k. Daraus folgt, dass $\varphi(p^k) = p^k - p^{k-1}$ ist. Insgesamt erhält man für n mit seiner PFZ $n = p_1^{l_1} \cdot \ldots \cdot p_r^{l_r}$

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_r})$$

□

5.6 Definition *Sei K ein Körper und $n \in \mathbb{N}$ mit $char(K) \nmid n$.*
Eine n-te Einheitswurzel ε über K heißt primitiv, wenn sie die Gruppe $E_n(K)$ erzeugt. Die Menge der primitiven n-ten Einheitswurzeln über K bezeichnen wir mit $PE_n(K)$.

5.7 Bemerkung *Sei K ein Körper, $n \in \mathbb{N}$ und $char(K) \nmid n$. Dann gilt:*

1. $\varepsilon \in PE_n(K) \Rightarrow K_n = K(\varepsilon)$
2. $\varepsilon \in PE_n(K), m \in \mathbb{N}$, *so liegt ε^m in $PE_n(K)$ genau dann, wenn m und n teilerfremd sind. Daraus ergibt sich, dass es genau $\varphi(n)$ primitive n-te Einheitswurzeln über K gibt.*
3. *Für jeden Teiler d von n mit $d > 0$ ist $E_d(K) \subset E_n(K)$ und*
$$PE_d(K) = \{\varepsilon |\ \varepsilon \in E_n(K), ord(\varepsilon) = d\}.$$
4. *Die Mengen $PE_d(K)$ mit $d|n$ und $d > 0$ sind paarweise disjunkt und es gilt*
$$E_n(K) = \bigcup_{\substack{d|n \\ d>0}} PE_d(K).$$

Beweis: Zu 1)$K_n = K(PE_n(K)) = K(\{\varepsilon^d | 1 \leq d \leq n, ggT(d,n) = 1\} = K(\varepsilon)$
Zu 2) Diese Aussage gilt allgemein für endliche zyklische Gruppen. Da $\varphi(n)$ die Anzahl der zu n teilerfremden Zahlen angibt, gibt es genau $\varphi(n)$ primitive Einheitswurzel über K.
Zu 3) Hierzu sind 2 Richtungen zu zeigen.
" $\subseteq$ "$\varepsilon \in PE_d(K) \Rightarrow ord(\varepsilon) = d,\ \varepsilon \in E_n(K)$
" $\supseteq$ "$\varepsilon \in E_n(K), ord(\varepsilon) = d \Rightarrow \varepsilon^d = 1 \Rightarrow \varepsilon^n = 1 (da\ d|n) \Rightarrow \varepsilon \in E_n(K)$
z.z.: $\varepsilon \in PE_d(K)$. $\varepsilon^d = 1 \Rightarrow \varepsilon \in E_d(K)$. Das bedeutet, dass $< \varepsilon >$ eine Untergruppe von $E_d(K)$ sein muß. Da $| < \varepsilon > | = d$ ist, folgt sogar, dass ε ein erzeugendes Element ist.
Zu 4) " $\supseteq$ " Klar, denn die Menge der primitiven Einheitswurzeln, deren Ordnung teilerfremd zur Gruppenordnung ist, ist als zyklische Untergruppe immer enthalten.
" $\subseteq$ " Sei $\varepsilon \in E_n(K) \overset{2)}{\Rightarrow} ord(\varepsilon) = d$ mit $d|n \Rightarrow \varepsilon \in PE_d(K)$.

□

Den letzten Teil des Beweises kann man durch Umstellen nutzen, um die Anzahl der pimitive Einheitswurzeln auszurechnen. Denn

$$n = |E_n(K)| = |\bigcup_{d|n} PE_d(K)| = \sum_{d|n} |PE_d(K)| \overset{1)}{=} \sum_{d|n} \varphi(d)$$

5.8 Beispiele
Errechnen der n-ten (primitiven) Einheitswurzeln
a) $n = 8$
<u>EW</u> $\varepsilon := e^{(\frac{2 \cdot \pi \cdot i \cdot k}{8})}; k \in \{0, \ldots, 7\}$
<u>primitive EW</u> $\varphi(8) = |\ \{k \mid\ 1 \leq k < 8, ggT(k,8) = 1\}\ | = 4$

$$PE_8(K) = \{\varepsilon, \varepsilon^3, \varepsilon^5, \varepsilon^7\}$$

b) $n = 7$

EW $\varepsilon := e^{(\frac{2\cdot\pi\cdot i\cdot k}{7})}; k \in \{0,\ldots,6\}$
primitive EW $\varphi(7) = \mid \{k \mid 1 \leq k < 7, ggT(k,7) = 1\} \mid = 6$

$$PE_7(K) = \{\varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5, \varepsilon^6\}$$

5.9 Definition *Sei K ein Körper, $n \in \mathbb{N}$ und $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ seien die primitiven n-ten Einheitswurzeln über K. Das Polynom*

$$\Phi_n(T) := (T - \varepsilon_1) \cdot \ldots \cdot (T - \varepsilon_{\varphi(n)}) \in K_n[T]$$

heißt das n-te Kreisteilungspolynom (KTP) von K.

5.10 Satz *Sei K ein Körper, $n \in \mathbb{N}$ und $char(K) \nmid n$. Dann gilt für das n-te Kreisteilungspolynom Φ_n von K:*

1. $grad(\Phi_n) = \varphi(n)$
2. $T^n - 1 = \prod_{\substack{d|n \\ d>0}} \Phi_d$
3. *Die Koeffizienten von Φ_n sind von der Form $m \cdot 1_K$ mit $m \in \mathbb{Z}$, wobei 1_K das Einselement von K ist.*

Beweis: Zu 1) Klar, dass $grad(\Phi_n) = \varphi(n)$ gilt, denn wie in (5.7) gezeigt, existieren genau $\varphi(n)$ primitive n-te Einheitswurzeln.
Zu 2) Beh.: $T^n - 1 = \prod_{\substack{d|n \\ d>0}} \Phi_d$. Durch (5.7)3) kann ich den Ausdruck $\prod_{\substack{d|n \\ d>0}} \Phi_d$ umschreiben in $\prod_{d|n} \prod_{\varepsilon \in PE_d(K)} (T - \varepsilon^d)$. Zusammengefasst bedeutet das $\prod_{\varepsilon \in E_{n(K)}} (T - \varepsilon)$. Das ist eben genau der gewünschte Term $T^n - 1$.
Zu 3) Dieser Beweis wird mit vollständiger Induktion nach n geführt.
$IA : n = 1 : \Phi_1 = T - 1$ Klar!
IV: Sei $n > 1$ beliebig und die Beh. richtig für alle $k < n$, d.h. Φ_k hat ganzzahlige Koeffizienten für alle $k < n$.
IS: Es gilt $T^n - 1 = \Phi_n \cdot \prod_{\substack{d|n \\ n>d>0}} \Phi_d$. Nach IV ist $\prod \Phi_d$ ein Polynom mit ganzzahligen Koeffizienten. Division mit Rest in $\mathbb{Z}[T]$ ergibt, dasss auch Φ_n lauter ganzzahlige Koeffizienten hat.

□

Hieraus ergibt sich eine Formel für die rekursive Berechnung von Kreisteilungspolynomen, wie man in den folgenden Beispielen sieht.

5.11 Beispiele
Mit Hilfe von (5.10) 2) können wir nun rekursiv KTP berechnen:

$$T^n - 1 = \prod_{\substack{d|n \\ d>0}} \Phi_d = \Phi_n \cdot \prod_{\substack{d|n \\ n>d>0}} \Phi_d$$

$$\Phi_n = \frac{T^n - 1}{\prod_{\substack{d|n \\ n>d>0}} \Phi_d}$$

1. *Sei* $n = p,\ p \in \mathbb{P}$
$$\Phi_p = \frac{T^p - 1}{T - 1} = T^{p-1} + \ldots + T + 1$$

2. *Sei* $n = 6$
$$\Phi_6 = \frac{T^6 - 1}{(T-1)\cdot(T+1)\cdot(T^2+T+1)} = T^2 - T + 1$$

3. *KTP für* $n \leq 11$

n	Φ_n
1	$T - 1$
2	$T + 1$
3	$T^2 + T + 1$
4	$T^2 + 1$
5	$T^4 + T^3 + T^2 + T + 1$
6	$T^2 - T + 1$
7	$T^6 + T^5 + T^4 + T^3 + T^2 + T + 1$
8	$T^4 + 1$
9	$T^6 + T^3 + 1$
10	$T^4 - T^3 + T^2 - T + 1$
11	$T^{10} + T^9 + T^8 + T^7 + T^6 + T^5 + T^4 + T^3 + T^2 + T + 1$

5.12 Satz *Sei K ein Körper und $n \in \mathbb{N}$ und $char(K) \not| n$. Dann gibt es einen injektiven Gruppenhomomorphismus*
$$Gal(K_n : K) \to \mathbb{Z}_n^*$$
der Galois-Gruppe von $K_n : K$ in die Einheitengruppe $\mathbb{Z}_n^*$.
Die Galois-Gruppe von $K_n : K$ ist also insbesondere abelsch.

Beweis: Zuerst wird gezeigt, dass jedes $\sigma \in Gal(K_n : K)$ $E_n(K)$ auf sich abbildet. z.z.: $\varepsilon \in E_n(K) \Rightarrow \sigma(\varepsilon) \in E_n(K)$.
$\varepsilon^n = 1 \Rightarrow \sigma(\varepsilon^n) = \sigma(1) = 1 \Rightarrow (\sigma(\varepsilon^n)) = (\sigma(\varepsilon))^n = 1 \Rightarrow \sigma(\varepsilon) \in E_n(K)$. Da σ injektiv ist, folgt daraus, dass $\sigma(E_n(K)) = E_n(K)$ ist. Und wir erhalten die Abbildung $\sigma : E_n(K) \to E_n(K)$. Da σ ein bijektiver Gruppenhomomorphismus ist, gilt weiterhin, dass $ord(\varepsilon) = ord(\sigma(\varepsilon))$. Sei $\eta \in PE_n(K)$. Dann folgt $\sigma(\eta) \in PE_n(K)$ und es gibt ein zu n teilerfremdes m mit $\sigma(\eta) = \eta^m$. Gilt außerdem $\sigma(\eta) = \eta^l$ mit $l \in \mathbb{N}$, dann erhält man:
$$\eta^m = \eta^l \qquad | \cdot \eta^{-l}$$
$$\eta^m \eta^{-l} = 1_K$$
$$\eta^{m-l} = 1_K$$
Daraus folgt insgesamt, dass $n \mid (m - l)$, denn $ord(\eta) = n$.
Auf diese Weise erhält man eine Abbildung
$$h : (Gal(K_n : K), \circ) \to (\mathbb{Z}_n^*, \cdot)$$
$$\sigma \mapsto [m]_n = \{b \mid b \in \mathbb{Z}, b \equiv m \ (mod\ n)\}$$
Es bleibt nun noch zu zeigen, dass h ein injektiver Gruppenhomomorphismus ist.
Seien dazu $\tau, \sigma \in Gal(K_n : K)$ mit
$h(\tau \circ \sigma) = [m]_n$, falls $\eta^m = \tau(\sigma(\eta))$,

$h(\tau) = [l]_n$, falls $\eta^l = \tau(\eta)$ und
$h(\sigma) = [k]_n$, falls $\eta^k = \sigma(\eta)$
Z.z.: $h(\tau \circ \sigma) = h(\tau) \cdot h(\sigma)$, also $[l]_n \cdot [k]_n = [m]_n$

$$\eta^m = \tau(\sigma(\eta)) = \tau(\eta^k) \overset{\tau \text{ Körperhom.}}{=} (\tau(\eta))^k = (\eta^l)^k = \eta^{l \cdot k}$$

$$\eta^m = \eta^{l \cdot k} \qquad | \cdot \eta^{-m}$$

$$1_K = \eta^{l \cdot k - m}$$

$\Rightarrow ord(\eta) \mid l \cdot k - m \Rightarrow n \mid l \cdot k - m \Rightarrow [l \cdot k]_n = [m]_n \Rightarrow [l]_n \cdot [k]_n = [m]_n$.
h ist injektiv: Z.z.: $Kern(h) = \{id_{K_n}\}$.
$Kern(h) = \{\sigma \mid \sigma \in Gal(K_n : K), h(\sigma) = [1]_n\}$. Sei $h(\sigma) = [1]_n$.
Z.z.: $\sigma = id_{K_n}$, das ist gleichbedeutend mit $\sigma(\alpha) = \alpha \quad (\forall \alpha \in K_n)$
$h(\sigma) = [k]_n = [1]_n$, falls $\eta^k = \sigma(\eta)$

$$k = 1 + l \cdot n \qquad \text{für ein } l \in \mathbb{N}$$

$$\eta^k = \eta^{1+l \cdot n} = \eta \cdot (\eta^n)^l = \eta$$

$$\Rightarrow \sigma(\eta) = \eta.$$

$$\text{Sei } \alpha \in K_n = K(\eta) \Rightarrow \alpha = \sum_{i=0}^{\varphi(n)-1} a_i \eta^i \qquad \text{mit } a_i \in K = Fix(Gal(K_n : K))$$

$$\sigma(\alpha) = \sum \underbrace{\sigma(a_i)}_{=a_i} \underbrace{\sigma(\eta)}_{=\eta}{}^i = \sum a_i \eta^i = \alpha.$$

Es existiert also ein injektiver Gruppenhomomorphismus

$$Gal(K_n : K) \to \mathbb{Z}_n^*$$

Da $\mathbb{Z}_n^*$ abelsch ist, ist auch $Gal(K_n : K)$ abelsch.

□

Der Abschluss und gleichzeitig der Höhepunkt dieser Ausarbeitung soll nun die Verschärfung von (5.12) auf den Fall $K = \mathbb{Q}$ sein.

5.13 Satz *Sei $n \in \mathbb{N} \setminus \{0\}$, $\Phi_n \in \mathbb{Z}[T]$ das n-te KTP und $\mathbb{Q}_n$ der ZFK des Polynoms $T^n - 1$ über $\mathbb{Q}$. Dann gilt:*

1. *Φ_n ist irreduzibel über $\mathbb{Q}$.*
2. *$[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$.*
3. *Es gibt einen Gruppenisomorphismus $Gal(\mathbb{Q}_n : \mathbb{Q}) \to \mathbb{Z}_n^*$.*

Beweis: Da 2) und 3) aus 1) folgen, werde ich zunächst die Folgerungen aus 1) darlegen und dann auf 1) eingehen.
Zu 2) Aus 1) folgt, dass Φ_n irreduzibel und damit MP von jeder primitiven n-ten EW $\eta \in \mathbb{Q}_n$ ist.
Aus $\mathbb{Q}_n = \mathbb{Q}(\eta)$ folgt $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$.
Zu 3) Wegen $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n) =| \mathbb{Z}_n^* |$ folgt, dass der injektive Gruppenhomomorphismus $Gal(\mathbb{Q}_n : \mathbb{Q}) \to \mathbb{Z}_n^*$ aus (5.12) ein Gruppenisomorphismsus ist.

Zu 1) Es genügt zu zeigen, dass Φ_n irreduzibel über $\mathbb{Z}$ ist. Da $\mathbb{Z}[T]$ ein faktorieller Ring ist, besitzt Φ_n einen irreduziblen Faktor $f \in \mathbb{Z}[T]$ vom Grade ≥ 1, d.h. $\Phi_n = f \cdot g$ mit $f, g \in \mathbb{Z}[T]$ normiert, f irreduzibel. Wir beweisen zunächst die Behauptung:
$(*)$ Ist η eine beliebige Nullstelle von f, so gilt $f(\eta^d) = 0$ für alle $d \in \mathbb{N}$ mit $1 \leq d \leq n$ und $ggT(d, n) = 1$.
1.Fall: $d = p \in \mathbb{P}$, $ggT(p, n) = 1$, d.h. $p \nmid n$

$$f(\eta) = 0 \Rightarrow \Phi_n(\eta) = f(\eta) \cdot g(\eta) = 0 \Rightarrow \eta \in PE_n(\mathbb{Q}) \Rightarrow \eta^p \in PE_n(\mathbb{Q}) \Rightarrow$$
$$0 = \Phi_n(\eta^p) = f(\eta^p) \cdot g(\eta^p)$$

Annahme: $f(\eta^p) \neq 0$
Dann muss $g(\eta^p) = 0$ gelten, so dass η Nullstelle des Polynoms $h := g(T^p) \in \mathbb{Z}[T]$ ist.
Da f das MP von η über $\mathbb{Q}$ ist, folgt $f \mid h$ in $\mathbb{Q}[T]$ und daher auch in $\mathbb{Z}[T]$, da $f, h \in \mathbb{Z}[T]$.
Es existiert also ein $h_0 \in \mathbb{Z}[T]$ mit

$$h = f \cdot h_0 \quad (\text{in } \mathbb{Z}[T]).$$

Der natürliche Homomorphismus $\nu : \mathbb{Z} \to \mathbb{Z}_p$ induziert einen surjektiven Ringhomomorphismus

$$\bar{\nu} : \mathbb{Z}[T] \to \mathbb{Z}_p[T]$$
$$q = \sum_{j=0}^{r} b_i T^j \longmapsto \bar{q} = \sum_{j=0}^{r} [b_j] T^j.$$

Daher gilt in $\mathbb{Z}_p[T]$

$$\bar{h} = \overline{f \cdot h_0} = \bar{f} \cdot \bar{h_0}.$$

Wegen $char(\mathbb{Z}_p) = p$ folgt

$$\bar{g}(T^p) = (\bar{g}(T))^p$$

und damit

$$\bar{g}^p = \bar{h} = \bar{f} \cdot \bar{h_0}$$

Sei $\bar{\lambda} \in \mathbb{Z}_p[T]$ ein irreduzibler Faktor von $\bar{f}$. Dann ist $\bar{\lambda}$ auch ein Faktor von $\bar{g}^p$ und damit von $\bar{g}$. Also hat

$$\bar{f} \cdot \bar{g} = \overline{f \cdot g} = \bar{\Phi}_n$$

$\bar{\lambda}^2$ als Faktor. Da $\bar{\Phi}_n$ ein Teiler von $T^n - \bar{1} \in \mathbb{Z}_p[T]$ ist, hat dann $T^n - \bar{1}$ eine mehrfache Nullstelle im Widerspruch zu (4) aus (5.3).
Folglich gilt $f(\eta^p) = 0$.
2.Fall: Sei $d \in \mathbb{N}$ mit $1 \leq d \leq n$ und $ggT(n, d) = 1$ beliebig, d besitze die PFZ $d = p_1 \cdot \ldots \cdot p_s$. Dann folgt $ggT(p_j, n) = 1$ für alle $j = 1, 2, \ldots, s$, d.h. $p_j \nmid n$. Wegen $p_1 \nmid n$ ist nach dem 1. Fall η^{p_1} eine Nullstelle von f. Wegen $p_2 \nmid n$ ist dann auch

$$(\eta^{p_1})^{p_2} = \eta^{p_1 p_2}$$

eine Nullstelle von f, usw. Schließlich ist
$\eta^{p_1 \cdot p_2 \cdot \ldots \cdot p_s} = \eta^d$ eine Nullstelle von f. Damit ist $(*)$ bewiesen. f besitzt mindestens eine Nullstelle η ($grad(f) \geq 1$), die auch Nullstelle von Φ_n ist, d.h. η ist eine primitive n-te Einheitswurzel. Wegen $PE_n(\mathbb{Q}) = \{\eta^d | 1 \leq d \leq n, ggT(d, n) = 1\}$ ist nach $(*)$ jede primitive n-te Einheitswurzel Nullstelle von f, d.h.

$$grad(\Phi_n) \geq grad(f) \geq |PE_n(\mathbb{Q})| = \varphi(n) = grad(\Phi_n).$$

Daraus folgt $grad(f) = grad(\Phi_n)$.
Aus $\Phi_n = f \cdot g$ ergibt sich damit $grad(g) = 0$, also $g = 1$, da g normiert ist.
Folglich ist $\Phi_n = f$ irreduzibel über $\mathbb{Z}$ und damit auch irreduzibel über $\mathbb{Q}$.

□

6 Endliche Körper

In dieser Ausarbeitung wird gezeigt, dass endliche Körper als Zerfällungskörper geeigneter Polynome auftreten und dass endliche Körper bis auf Isomorphie eindeutig bestimmt sind. Dabei baut diese Arbeit auf [2], Seite 162 bis 166 auf.

6.1 Bemerkung *Ist K ein endlicher Körper und P sein Primkörper, so gilt*

$$|K| = (char(K))^{[K:P]}.$$

Die Anzahl der Elemente von K ist also eine Primzahlpotenz.

Beweis: Die Charakteristik eines endlichen Körpers ist nach [1] Bemerkung 2.14 immer eine Primzahl, so dass nach [1] Satz 2.13 *b*) gilt $P := P(K) \cong \mathbb{Z}_p$. Daraus folgt, dass der Primkörper von K genau p Elemente hat.
Da K ein endlicher Körper ist, ist auch der Grad der Körpererweiterung $K : P$ endlich. Der n-dimensionale P-Vektorraum K ist isomorph zu P^n, so dass
$|K| = |P^n| = |P|^n = p^n = (char(K))^{[K:P]}$ folgt.

□

6.2 Satz *Ist K ein endlicher Körper, so gilt*

$$\prod_{a \in K^*} a = -1$$

Beweis: Ist $M := \{a \in K^* : a = a^{-1}\} = \{a \in K : a^2 = 1\}$, so gilt

$$\prod_{a \in K^*} a = \prod_{a \in M} a,$$

da sich aufgrund der Kommutativität von K^* die Elemente, die nicht zu sich selbst invers sind, in dem Produkt gegenseitig aufheben.
Ein Element $a \in K$ liegt genau dann in M, wenn a Nullstelle des Polynoms $T^2 - 1 \in K[T]$ ist. Dieses hat aber nur die Nullstellen $+1$ und -1. Durch Einsetzen der Nullstellen ergibt sich die Behauptung.

□

6.3 Korollar *(Satz von Wilson) Für jede Primzahl p gilt*

$$(p-1)! \equiv -1 (mod \ \ p).$$

Beweis: Durch Anwendung von Satz 6.2 auf den endlichen Körper $\mathbb{Z}_p$ erhalten wir:

$$[-1]_p = \prod_{a \in Z_p^*} a = [p-1]_p \cdot [p-2]_p \cdot \ldots \cdot [1]_p = [(p-1) \cdot (p-2) \cdot \ldots \cdot 1]_p = [(p-1)!]_p$$

$$\Longleftrightarrow (p-1)! \equiv -1 (mod \ \ p).$$

□

6.4 Satz *Ist K ein Körper, so ist jede endliche Untergruppe von $(K^*, \cdot)$ zyklisch.*

Beweis: Wir betrachten die endliche abelsche Gruppe $(U, \cdot)$. Sei $n := |U|$.
Die Menge $\{ord(b)|b \in U\} \subseteq \mathbb{N}$ der Ordnungen aller Elemente aus U ist endlich und besitzt daher ein größtes Element m. Sei $a \in U$ mit $ord(a) = m$.
Wir zeigen anschließend

$$(*)\forall b \in U : ord(b)|m.$$

Hieraus ergibt sich dann die Behauptung: Aus $(*)$ folgt mit $ord(b) \cdot t = m$ $(t \in \mathbb{N})$

$$(**)\forall b \in U : b^m = (b^{ord(b)})^t = 1_K^t = 1_K.$$

Nun betrachten wir das Polynom $f := T^m - 1 \in K[T]$. Bezeichnet N die Menge der in K gelegenen Nullstellen von f, so gilt nach [1] Satz 3.14 $|N| \leq grad(f) = m$.
Für ein beliebiges $b \in U$ folgt wegen $(**)$ $f(b) = 0$, also $b \in N$.
Folglich $U \subseteq N$ und $|U| \leq |N| \leq m = ord(a) \leq |U|$, woraus sich $|U| = ord(a)$ ergibt.
Aus $< a > \subseteq U$ und $| < a > | = ord(a) = |U|$, folgt dann aber $U =< a >$, d.h. U ist zyklisch mit a als erzeugendem Element.

Nachweis von $(*)$: Wir nehmen an, dass ein Element $c \in U$ mit $ord(c) \not| m$ existiert. Sei $l := ord(c)$. Wegen der Möglichkeit der eindeutigen Primfaktorzerlegung muss eine Primzahl p geben, die als Faktor von l mit einer höheren Potenz vorkommt als als Faktor von m, d.h. $l = p^\lambda \cdot l'$ mit $ggT(p, l') = 1$, $m = p^\mu \cdot m'$ mit $ggT(p, m') = 1$, $\lambda > \mu$.
Es folgt

$$ord(a^{p^\mu}) = \frac{ord(a)}{p^\mu} = \frac{m}{p^\mu} = \frac{p^\mu m'}{p^\mu} = m', ord(c^{l'}) = \frac{ord(c)}{l'} = \frac{l}{l'} = \frac{p^\lambda l'}{l'} = p^\lambda.$$

Sei $d := a^{p^\mu} \cdot c^{l'} \in U$. Da a^{p^μ} und $c^{l'}$ vertauschbar und ihre Ordnungen teilerfremd sind, ergibt sich

$$ord(d) = ord(a^{p^\mu} \cdot c^{l'}) = ord(a^{p^\mu}) \cdot ord(c^{l'}) = m' \cdot p^\mu = m \cdot \underbrace{p^{\lambda-\mu}}_{\geq 2} > m = ord(a).$$

Dies steht im Widerspruch dazu, dass a als ein Element größter Ordnung aus U gewählt war. Damit ist die Gültigkeit von $(*)$ nachgewiesen.

□

6.5 Korollar *Ist K ein endlicher Körper mit q Elementen, so gilt:*

1. *$(K^*, \cdot)$ ist zyklisch.*
2. *Es gibt ein $a \in (K^*, \cdot)$, so dass $K = \{0, 1, a, \ldots, a^{q-2}\}$.*
3. *Jedes Element von K ist Nullstelle des Polynoms $T^q - T \in K[T]$.*

Beweis:
zu 1.) Da K ein endlicher Körper ist, ist K^* selbst eine Untergruppe von K^* und somit nach Satz 6.4 zyklisch.

zu 2.) Da K ein Körper mit q Elementen ist, folgt $|K^*| = q - 1$. Nach 1) ist K^* zyklisch, somit existiert ein Element $a \in K^*$ mit $< a >= \{1, a, \ldots, a^{q-2}\}$ und

$K = \{0, 1, a, \ldots, a^{q-2}\}$.

zu 3.) Ein Element a von K ist genau dann Nullstelle des Polynoms $T^q - T \in K[T]$, wenn $a^q = a$ gilt. Dies gilt für jedes Element von K, denn aus der Gruppentheorie wissen wir, dass $a^{q-1} = 1_K$ für alle $a \in K^*$ gilt, da $|K^*| = q - 1$.
Daraus folgt $a^q = a$ für alle $a \in K^*$ und somit auch für alle $a \in K$.

□

6.6 Bemerkung *Ist K ein Körper der Charakteristik $p > 0$, so ist die Abbildung*

$$\sigma_K : K \longrightarrow K, x \mapsto x^p$$

ein (injektiver) Körperhomomorphismus.
σ_K heißt Frobenius-Homomorphismus *von K.*

Beweis: Nach [1] Satz 2.10 ist jeder Körperhomomorphismus injektiv. Es genügt also zu zeigen, dass σ_K ein Körperhomomorphismus ist.
Da für jedes $k \in \{1, \ldots, p-1\}$ die Zahl $p \in \mathbb{P}$ ein Teiler des Binomialkoeffizienten $\binom{p}{k}$ ist, folgt mit Hilfe des binomischen Lehrsatzes $(x + y)^p = x^p + y^p$ für alle $x, y \in K$.
Trivialerweise gilt auch $(x \cdot y)^p = x^p \cdot y^p$ für alle $x, y \in K$ und $1_K^p = 1_K$. Dies ist gerade die Bedingung dafür, dass σ_K ein Körperhomomorphismus ist.

□

6.7 Bemerkung *Es gilt*

1. *Der Frobenius-Homomorphismus eines endlichen Körpers ist ein Automorphismus.*
2. *Für jede Primzahl p ist der Frobenius-Homomorphismus des Körpers $\mathbb{Z}_p$ die Identität.*

Beweis:
zu 1.) Der Frobenius-Homomorphismus ist als Körperhomomorphismus injektiv. Da jede injektive Abbildung einer endlichen Menge in sich auch surjektiv ist, folgt die Behauptung sofort.

zu 2.) Es ist zu zeigen, dass die Abbildung $\mathbb{Z}_p \longrightarrow \mathbb{Z}_p, [x]_p \mapsto [x^p]_p$ für jede Primzahl p die Identität ist.
Für alle $[x]_p \in \mathbb{Z}_p^*$ gilt $[x^p]_p = [x]_p^p = [x]_p \cdot [x]_p^{p-1} = [x]_p \cdot [1]_p = [x]_p$.
Außerdem wird das Nullelement bei einem Körperhomomorphismus immer auf das Nullelement geschickt.

□

6.8 Satz *Ein Körper K der Charakteristik $p > 0$ ist genau dann vollkommen, wenn sein Frobenius-Homomorphismus σ_K surjektiv ist.*

Beweis: Sei K ein Körper der Charakteristik $p > 0$.
" $\Rightarrow$ " Ist K vollkommen, so ist nach Definition für jedes $a \in K$ das Polynom
$f := T^p - a \in K[T]$ separabel.
Sei g ein in K[T] irreduzibler Faktor von f, $L \supseteq K$ sein Zerfällungskörper und $b \in L$ eine Nullstelle von g. Dann ist $b \in L$ auch eine Nullstelle von f und es folgt $b^p = a$. Dann gilt $f = T^p - b^p = (T - b)^p \in L[T]$, da $p \in \mathbb{P}$, so dass es ein $n \in \{1, \ldots, p\}$ mit $g = (T - b)^n$

gibt. Da f separabel ist, hat g nach Definition nur einfache Nullstellen in L. Daraus folgt $n = 1$ und $b \in K$. Zu jedem $a \in K$ gibt es also ein $b \in K$ mit $a = b^p = \sigma_K(b)$. Somit ist σ_K surjektiv.

" $\Leftarrow$ " Sei nun σ_K surjektiv.
Wir nehmen an, dass K nicht vollkommen ist. Dann existiert ein nicht-separables Polynom $f \in K[T]$. Daraus folgt, dass es einen irreduzbiblen Faktor $g \in K[T]$ von f gibt, der mehrfache Nullstellen in seinem Zerfällungskörper hat. Damit existiert ein irreduzibles Polynom $g \in K[T]$ mit mehrfachen Nullstellen im Zerfällungskörper.
Dann folgt nach Lemma 2.11, dass es ein Polynom $h \in K[T]$ mit $g(T) = h(T^p)$ gibt. Wir erhalten

$$g(T) = a_0 + a_1T^p + \ldots + a_{n-1}(T^p)^{n-1} + a_n(T^p)^n$$

mit $a_0, \ldots, a_n \in K$. Da nach Voraussetzung σ_K surjektiv ist, gibt es zu jedem $i \in \{0, \ldots, n\}$ ein $b_i \in K$ mit $b_i^p = a_i$. So erhalten wir

$$g(T) = b_0^p + b_1^pT^p + \ldots + b_n^p(T^p)^n = b_0^p + b_1^pT^p + \ldots + b_n^p(T^n)^p = \underbrace{(b_0 + b_1T + \ldots + b_nT^n)}_{=:t \in K[T], \text{ da } b_i \in K}{}^p$$

$\Rightarrow t|g$. t ist ein echter Teiler, da wir die trivialen Fälle grad(t)=0 oder grad(t)=grad(f) ausschließen können. Denn mit grad(t)=0 folgt $t = b_0$ und $g = b_0^p$ und somit ist g als konstantes Polynom nicht irreduzibel über K. Außerdem gilt grad(t)$\neq$ grad(f), denn grad(t)=n und grad(g)=$np > n$, da $p \in \mathbb{P}$. Somit führt dies zum Widerspruch, da g über K irreduzibel ist und damit keine echten Teiler besitzt. Also ist K vollkommen.

□

6.9 Korollar *Jeder endliche Körper ist vollkommen.*

Beweis: Nach Satz 6.8 ist ein endlicher Körper K genau dann vollkommen, wenn σ_K surjektiv ist. Wir wissen nach Bemerkung 6.7, dass σ_K ein Automorphismus und damit surjektiv ist.

□

6.10 Satz *Für jede Primzahl p und $n \in \mathbb{N} \setminus \{0\}$ gilt:*

1. *Ist $K \supseteq \mathbb{Z}_p$ der Zerfällungskörper des Polynoms $T^{p^n} - T \in \mathbb{Z}_p[T]$, so ist K ein Körper mit p^n Elementen.*
2. *Ist K ein Körper mit p^n Elementen und P sein Primkörper, so ist $K \supseteq P$ Zerfällungskörper des Polynoms $T^{p^n} - T \in P[T]$.*
3. *Je zwei Körper mit p^n Elementen sind isomorph.*

Beweis:
zu 1.) Sei M die Menge der Nullstellen von $f := T^{p^n} - T$ in K.
Wir zeigen zunächst, dass M ein Zwischenkörper von $K : \mathbb{Z}_p$ ist. Dann muss K mit dieser Menge übereinstimmen, denn nach Voraussetzung ist $K := ZFK_{\mathbb{Z}_p}(f)$ und somit der kleinste Körper, der alle Nullstellen von f enthält.
Da die Gruppe $\mathbb{Z}_p^*$ die Ordnung $p-1$ hat, gilt $a^{p-1} = 1$, also $a^p = a$ und $a^{p^n} = a$ für alle $a \in \mathbb{Z}_p^*$, damit auch für alle $a \in \mathbb{Z}_p$. Somit ist $\mathbb{Z}_p$ in M enthalten.
Sind $a, b \in M$, so erhalten wir $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} = a \pm b$ und $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n} = a \cdot b$.

Außerdem gilt $(b^{-1})^{p^n} = (\frac{1}{b})^{p^n} = \frac{1^{p^n}}{b^{p^n}} = \frac{1}{b} = b^{-1}$, falls $b \neq 0$ und somit $b^{-1} \in M$. M ist demnach ein Körper und stimmt mit K überein.
Wegen $D(f) = -1 \neq 0$ hat f nach Lemma 2.8 nur einfache Nullstellen in M.
Daraus folgt $|K| = |M| = grad(f) = p^n$. K ist also ein Körper mit p^n Elementen.

zu 2.) Da die Gruppe K^* die Ordnung $p^n - 1$ hat, gilt $a^{p^n-1} = 1$ und somit $a^{p^n} = a$ für alle $a \in K^*$, damit auch für alle $a \in K$. Daraus folgt, dass alle Elemente aus K Nullstellen von f sind.
Da das Polynom $T^{p^n} - T$ in einem Oberkörper von P höchstens p^n Nullstellen hat und $|K| = p^n$, ist K die Menge seiner Nullstellen im Zerfällungskörper.
$K \supseteq P$ ist daher Zerfällungskörper dieses Polynoms.

zu 3.) Sind K und K' Körper mit p^n Elementen, so gilt nach Bemerkung 6.1
$char(K) = p = char(K')$. Daraus folgt, dass die Primkörper $P := P(K)$ und
$P' := P(K')$ nach [1] Satz 2.13 isomorph sind zu dem Körper $\mathbb{Z}_p$ und somit auch zueinander isomorph sind.
Wir führen den weiteren Beweis mit Satz 1.8 durch: Sei $\varphi : P \longrightarrow P'$ ein Körperisomorphismus (dieser existiert!) und $\Phi : P[T] \longrightarrow P[T]'$ der zugehörige Isomorphismus der Polynomringe.
Nach 2) ist $K \supseteq P$ Zerfällungskörper des Polynoms $f := T^{p^n} - T \in P[T]$ und $K' \supseteq P'$ Zerfällungskörper des Polynoms $f' := T^{p^n} - T \in P'[T]$.
Um Satz 1.8 anwenden zu können, müssen wir noch zeigen, dass $\Phi(f) = f'$.

$$\Phi(f) = \Phi(T^{p^n} - T) = \Phi(1_P T^{p^n} + (-1_P)T) = \varphi(1_P)T^{p^n} + \varphi(-1_P)T$$

$$= \varphi(1_P)T^{p^n} - \varphi(1_P)T = 1_{P'}T^{p^n} - 1_{P'}T = T^{p^n} - T = f' \in P'[T].$$

Mit Satz 1.8 folgt nun $K \cong K'$. Ein Körper mit p^n Elementen ist also bis auf Isomorphie eindeutig bestimmt!

□

6.11 Bezeichnung *Ist p ein Primzahl und $n \in \mathbb{N} \setminus \{0\}$, so nennt man den bis auf Isomorphie eindeutig bestimmten Körper mit p^n Elementen manchmal das* Galois-Feld *mit p^n Elementen und bezeichnet ihn mit $GF(p^n)$.*

6.12 Satz *Ist p eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$,*
so gilt für jeden Körper K mit p^n Elementen und seinen Primkörper P:

1. *Die Körpererweiterung $K : P$ ist eine Galoiserweiterung.*
2. *Der Frobenius-Homomorphismus von K erzeugt die Automorphismengruppe von K. Diese stimmt mit der Galoisgruppe von $K : P$ überein.*

Beweis:
zu 1.) Nach Theorem 2.13 ist eine Körpererweiterung $K : P$ genau dann eine Galoiserweiterung, wenn $K \supseteq P$ Zerfällungskörper eines separablen Polynoms aus $P[T]$ ist.
Nach Satz 6.10 ist ein Körper K mit p^n Elementen Zerfällungskörper des Polynoms

$T^{p^n} - T \in P[T]$ über dem Primkörper P. Dieses ist separabel, da P als endlicher Körper vollkommen ist.

zu 2.) Zunächst zeigen wir, dass die Automorphismengruppe von K mit der Galoisgruppe von $K : P$ übereinstimmt.

" $\subseteq$ " Sei $\sigma \in Gal(K : P)$ beliebig, so folgt $\sigma \in Aut(K)$ und somit
$Gal(K : P) \subseteq Aut(K)$.

" $\supseteq$ " Sei $\sigma \in Aut(K)$ beliebig. Dann folgt $Fix(\sigma)$ ist ein Unterkörper von K und es gilt $\sigma(a) = a$ für alle $a \in Fix(\sigma)$. Da der Primkörper $P(K)$ der kleinste Unterkörper von K und somit auch ein Unterkörper von $Fix(\sigma)$ ist, folgt $\sigma(a) = a$ für alle $a \in P$.
σ ist also ein P-Automorphismus von K. Damit ist $\sigma \in Gal(K : P)$ und
$Gal(K : P) \supseteq Aut(K)$.

Nun müssen wir zeigen, dass der Frobenius-Homomorphismus σ_K von K die Automorphismengruppe von K erzeugt.
Nach Bemerkung 6.7 ist σ_K ein Automorphismus und daher ein Element der Automorphismengruppe von K.
Der Hauptsatz der Galois-Theorie liefert: $|Aut(K)| = |Gal(K : P)| = [K : P] = n$, da $K : P$ eine Galoiserweiterung ist. Demnach gilt $< \sigma_K >= Aut(K) \iff | < \sigma_K > | = n$.

Beh.: $< \sigma_K >= \{\sigma_K^0, \sigma_K^1, \ldots, \sigma_K^{n-1}\}$. Wir müssen nun zeigen, dass die Potenzen von σ_K paarweise verschieden sind.
Sei dazu a ein erzeugendes Element der Gruppe K^* (vgl. 6.5).
Wegen $\sigma^i(a) = a^{p^i}$ für alle i genügt es zu zeigen, dass die Elemente $a, a^p, \ldots, a^{p^{n-1}}$ paarweise verschieden sind.
Wir nehmen an, dass $a^{p^i} = a^{p^j}$ mit $i, j \in \{0, 1, \ldots, n-1\}, j < i$ ist. Dann folgt $a^{p^i} \cdot a^{-p^j} = 1 \iff a^{p^i - p^j} = 1$. Da $1 \leq p^i - p^j \leq p^i - 1 < p^n - 1$ führt dies zum Widerspruch, denn a hat als erzeugendes Element von K^* die Ordnung $p^n - 1$.
Somit sind die Elemente $a, \ldots, a^{p^{n-1}}$ wie auch die Elemente von $< \sigma_K >$ paarweise verschieden.
Dann folgt $ord(\sigma_K) = | < \sigma_K > | = n = |Aut(K)|$ und $< \sigma_K >= Aut(K)$.
Der Frobenius-Homomorphismus von K erzeugt also die Automorphismengruppe von K. Die Galoisgruppe von $K : P$ ist zyklisch!

□

6.13 Satz *Sei p eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$.*
Ist dann K ein Körper mit p^n Elementen und σ_K sein Frobenius-Homomorphismus, so sind die Fixkörper $K^{<\sigma_K^i>}$, $i|n$, $i \in \mathbb{N} \setminus \{0\}$ genau die Unterkörper von K.
Insbesondere gibt es zu jedem Teiler i von n genau einen Unterkörper mit p^i Elementen.

Beweis: Wir führen den Beweis zunächst mit Gruppentheorie.
Die Gruppen $< \sigma_K^i >$, $i|n$, $i \in \mathbb{N} \setminus \{0\}$ sind die einzigen Untergruppen der Automorphismengruppe von K, da $Aut(K) =< \sigma_K >$ nach Satz 6.12 zyklisch ist. Damit ist auch jede ihrer Untergruppen zyklisch und nach [GdA] Satz 3.25 gibt es zu jedem Teiler i von n genau eine Unterguppe mit $| < \sigma_K^i > | = \frac{n}{i}$.

Der Hauptsatz der Galois-Theorie liefert eine bijektive Korrespondenz zwischen den Untergruppen der Galoisgruppe und den Zwischenkörpern einer Galoiserweiterung.
Für jede Untergruppe $< \sigma_K^i >$ der Automorphismengruppe von K ist demnach $K^{<\sigma_K^i>}$ ein Zwischenkörper von $K : P$ und zu jedem Teiler i von n existiert genau ein Un-

terkörper.
Wir müssen noch zeigen, dass die Unterkörper genau p^i Elemente haben.
$K^{<\sigma_K^i>}$ ist ein Zwischenkörper der Körpererweiterung $K : P$. Nach Bemerkung 6.1 gilt für endliche Körper und ihre Primkörper $\left|K^{<\sigma_K^i>}\right| = (char(K))^{[K^{<\sigma_K^i>}:P]}$.
Wir suchen also den Grad der Körpererweiterung $K^{<\sigma_K^i>} : P$.
Mit dem Gradsatz erhalten wir

$$[K^{<\sigma_K^i>} : P] = \frac{[K : P]}{[K : K^{<\sigma_K^i>}]} = \frac{n}{| < \sigma_K^i > |} = \frac{n}{\frac{n}{i}} = i.$$

Damit folgt $\left|K^{<\sigma_K^i>}\right| = (char(K))^{[K^{<\sigma_K^i>}:P]} = p^i$.

□

7 Irreduzible Polynome über endlichen Körpern

In diesem Vortrag wird die Anzahl der irreduziblen normierten Polynome eines bestimmten Grades über einem endlichen Körper bestimmt. Damit kann gezeigt werden, dass es irreduzible Polynome beliebigen Grades über einem endlichen Körper gibt. Dies hat zur Folge, dass zu einer beliebigen Primzahlpotenz p^n ein Körper mit p^n Elementen konstruiert werden kann.

7.1 Satz *Ist K ein endlicher Körper mit q Elementen und ist f ein irreduzibles Polynom vom Grade n über K, so ist f genau dann ein Teiler von $T^{q^s}-T$, wenn n ein Teiler von s ist.*

Beweis: "$\Longleftarrow$" Es wird durch Induktion nach i gezeigt, dass f ein Teiler von $T^{q^{ni}}-T$ für alle $i \in \mathbb{N}$ ist:
(IA) $i=1$ $L := K[T]/(f)$ ist ein Körper mit q^n Elementen. Es ist $f([T]_{(f)}) = [f]_{(f)} = 0$, so dass $[T]_{(f)} \in L$ eine Nullstelle von f ist. Weil nach 6.4(3) alle Elemente von L Nullstellen des Polynoms $T^{q^n}-T$ sind, haben f und $T^{q^n}-T$ eine gemeinsame Nullstelle in L. Nach [1] Satz 3.19 existiert $h \in K[T]$ mit $h := ggT(f, T^{q^n}-T)$. Außerdem gibt es Polynome $w, v \in K[T]$ mit $h = w \cdot f + v \cdot (T^{q^n}-T)$. Dann gilt

$$h([T]_{(f)}) = w([T]_{(f)}) \cdot f([T]_{(f)}) + v([T]_{(f)}) \cdot ([T]_{(f)}^{q^n} - [T]_{(f)}) = 0,$$

d.h. h ist keine Einheit in $K[T]$. Da $h|f$ gilt und f irreduzibel ist, folgt daraus $h \sim f$. Somit ist f ein Teiler von $T^{q^n}-T$.
(IV) Für eine beliebige, aber feste natürliche Zahl i sei die Behauptung richtig.
(IB) f ist ein Teiler von $T^{q^{n(i+1)}}-T$.
(IS) $i \to i+1$

$$T^{q^{n(i+1)}} - T = T^{q^{ni}\cdot q^n} - T = T^{q^{ni}\cdot q^n} - T^{q^n} + T^{q^n} - T = (T^{q^{ni}} - T)^{q^n} + T^{q^n} - T$$

Dabei beachte man dass q Potenz der Charakteristik von K ist, so dass $T^{q^{ni}\cdot q^n} - T^{q^n} = (T^{q^{ni}} - T)^{q^n}$ ist. Nach (IV) und (IA) teilt f die Polynome $T^{q^{ni}}-T$ und $T^{q^n}-T$. Folglich ist f auch ein Teiler von $T^{q^{n(i+1)}}-T$. Ist also n ein Teiler von s, so ist f ein Teiler von $T^{q^s}-T$.

"$\Longrightarrow$" Es sei umgekehrt f ein Teiler von $T^{q^s}-T$. Ferner sei $s = un+r$ mit $0 \le r < n$. Z.z.: $r=0$, d.h. $n|s$. Aus

$$T^{q^s} - T = T^{q^{un+r}} - T = T^{q^{un}\cdot q^r} - T^{q^r} + T^{q^r} - T = (T^{q^{un}} - T)^{q^r} + T^{q^r} - T$$

folgt dann, dass f auch ein Teiler von $T^{q^r}-T$ ist.

Sei $g = \sum_{i=0}^{m} g_i T^i$ ein beliebiges Polynom über dem Körper K. Dann gilt

$$g^{q^r} = \left(g_0 + \sum_{i=1}^{m} g_i T^i\right)^{q^r} = g_0^{q^r} + \left(\sum_{i=1}^{m} g_i T^i\right)^{q^r} = g_0 + \left(g_1 T + \sum_{i=2}^{m} g_i T^i\right)^{q^r}$$

$$= g_0 + (g_1 T)^{q^r} + \left(\sum_{i=2}^{m} g_i T^i\right)^{q^r} = \ldots = g_0 + g_1 T^{q^r} + g_2 T^{2q^r} + \ldots + g_m T^{mq^r}$$

$$= g_0 + g_1 T^{q^r} + g_2 \left(T^{q^r}\right)^2 + \ldots + g_m \left(T^{q^r}\right)^m = g\left(T^{q^r}\right),$$

man beachte dabei, dass q eine Potenz der Charakteristik von K und wegen Lagrange $g_i^{q^r} = g_i$ für $g_i \in K \ \ \forall i \in \{0, 1, \ldots, m\}$ ist. Also gilt $g^{q^r} = g(T^{q^r})$ für alle $g \in K[T]$.

Da f das Polynom $T^{q^r} - T$ teilt, ist $\left[T^{q^r} - T\right]_{(f)} = [0]_{(f)}$, d.h. $\left[T^{q^r}\right]_{(f)} = [T]_{(f)}$. Daher ist $[g]_{(f)}^{q^r} = \left[g^{q^r}\right]_{(f)} = \left[g(T^{q^r})\right]_{(f)} = g(\left[T^{q^r}\right]_{(f)}) = g([T]_{(f)}) = [g]_{(f)}$ für alle $g \in K[T]$, d.h. $[g]_{(f)}^{q^r} - [g]_{(f)} = [0]_{(f)}$. Somit sind alle Elemente aus L Nullstellen von $T^{q^r} - T$. Wegen $q^r < q^n$ ist daher $T^{q^r} - T$ das Nullpolynom, so dass $q^r = 1$ und damit $r = 0$ ist. Folglich ist n ein Teiler von s.

□

7.2 Satz *Ist K ein endlicher Körper mit q Elementen und ist $f \in K[T]$ irreduzibel, so ist f^2 kein Teiler von $T^{q^s} - T$ für alle $s \in \mathbb{N}$.*

Beweis: Angenommen für $s \in \mathbb{N}$ gilt $f^2 \mid T^{q^s} - T$. Dann gibt es $g \in K[T]$ mit $T^{q^s} - T = f^2 g$. In K gilt $q^s \cdot 1_K = 0_K$, da q Potenz der Charakteristik von K ist. Ist D die formale Differentiation in $K[T]$ wie in 2.7, dann ist also $D(f^2 g) = f^2 Dg + 2gfDf = f(fDg + 2gDf) = q^s T^{q^s - 1} - 1 = -1$, so dass f eine Einheit ist im Widerspruch zur Irreduzibilität von f.

□

7.3 Satz *Bezeichnet $N_{n,q}$ die Anzahl der irreduziblen normierten Polynome vom Grade n über einem Körper K mit q Elementen, so ist $q^n = \sum_{d|n} dN_{d,q}$.*

Vorbemerkung: $N_{n,q}$ ist eine endliche Zahl.

Beweis: Sei f_d das Produkt über alle irreduziblen normierten Polynome vom Grade d über K und $f = \prod_{d|n} f_d$. Da jedes dieser Polynome irreduzibel und normiert ist, so sind sie paarweise teilerfremd. Nach 7.1 teilt jedes dieser Polynome das Polynom $T^{q^n} - T$. Folglich wird $T^{q^n} - T$ auch vom Polynom f geteilt. Dann gibt es ein Polynom $h \in K[T]$ mit $T^{q^n} - T = fh$.

Annahme: h ist ein nicht-konstantes Polynom. Nach [1] Satz 3.27 läßt sich h als Produkt von irreduziblen Polynomen darstellen. Sei h_1 ein irreduzibler Faktor von h. Nach Satz 7.1 ist der Grad von h_1 ein Teiler von n. Damit ist h_1 ein Teiler von f. Folglich teilt h_1^2 das Polynom $T^{q^n} - T$. Dies ist ein Widerspruch zu 7.2.
Also ist h konstant. Da f und $T^{q^n} - T$ normiert sind, ist $h = 1$, d.h. $f = T^{q^n} - T$. Daraus folgt: $q^n = \operatorname{grad}\left(T^{q^n} - T\right) = \operatorname{grad}(f) = \operatorname{grad}\left(\prod_{d|n} f_d\right) = \sum_{d|n} \operatorname{grad}(f_d) = \sum_{d|n} dN_{d,q}$.

□

Die folgenden Ergebnisse brauchen wir um die Anzahl der irreduziblen Polynome zu bestimmen.

7.4 Lemma *Es sei R die Menge aller Abbildungen von $\mathbb{N}$ in $\mathbb{R}$. Man definiert auf R eine Multiplikation $*$ durch*

$$(f * g)(n) = \sum_{xy=n} f(x)g(y) = \sum_{x|n} f(x)g\left(\frac{n}{x}\right) \qquad \forall f, g \in R, \quad \forall n \in \mathbb{N}.$$

Versieht man R noch mit der punktweise definierten Addition, so wird R zu einem Ring. Das Einselement ist die durch $\varepsilon(1) = 1$ und $\varepsilon(n) = 0$ für $n > 1$ definierte Abbildung ε.

Beweis: Die Addition auf R ist definiert durch $(f+g)(n) = f(n)+g(n) \quad \forall f,g \in R$.

Zuerst zeigen wir, dass $(R,+)$ eine abelsche Gruppe ist.

0) *Abgeschlossenheit* Seien $f,g \in R$ beliebig. Für alle $n \in \mathbb{N}$ gilt $(f+g)(n) = \underbrace{f(n)+g(n)}_{\in\mathbb{R}}$. Damit ist $f+g$ eine Abbildung von $\mathbb{N}$ in $\mathbb{R}$, d.h. $f+g \in R$.

1) *Assoziatives Gesetz* Seien $f,g,h \in R$ beliebig. Es gilt

$$((f+g)+h)(n) = (f+g)(n)+h(n) = (f(n)+g(n))+h(n) = f(n)+(g(n)+h(n))$$
$$= f(n)+(g+h)(n) = (f+(g+h))(n) \quad \forall n \in \mathbb{N}.$$

Also ist $(f+g)+h = f+(g+h)$.

2) *Kommutatives Gesetz* Seien $f,g \in R$ beliebig. Es gilt $(f+g)(n) = f(n)+g(n) = g(n)+f(n) = (g+f)(n) \quad \forall n \in \mathbb{N}$. Damit ist $f+g = g+f$.

3) *Existenz eines Nullelementes* Die Nullabbildung $o \in R$ ist definiert durch $o(n) = 0$ für alle $n \in \mathbb{N}$. Sei jetzt $f \in R$ beliebig. Es ist $(f+o)(n) = f(n)+o(n) = f(n) \quad \forall n \in \mathbb{N}$. Also gilt $f+o = f$, d.h. $o \in R$ ist das Nullelement in R.

4) *Existenz von negativen Elementen* Sei $f \in R$ beliebig. Die Abbildung $-f \in R$ ist definiert durch $(-f)(n) = -f(n) \quad \forall n \in \mathbb{N}$. Dann gilt $(f+(-f))(n) = f(n)+(-f)(n) = f(n)+(-f(n)) = 0 = o(n) \quad \forall n \in \mathbb{N}$. Also ist $f+(-f) = o$, d.h. $-f$ ist das Negative zu f.

Nun zeigen wir, dass $(R,*)$ eine kommutative Halbgruppe mit einem neutralen Element ist.

0) *Abgeschlossenheit* Seien $f,g \in R$ beliebig. Für alle $n \in \mathbb{N}$ gilt $(f*g)(n) = \underbrace{\sum_{xy=n} f(x)g(y)}_{\in\mathbb{R}}$. Damit ist $f*g$ eine Abbildung von $\mathbb{N}$ in $\mathbb{R}$, d.h. $f*g \in R$.

1) *Assoziatives Gesetz* Seien $f,g,h \in R$ beliebig. Es gilt

$$((f*g)*h)(n) = \sum_{xy=n}(f*g)(x)h(y) = \sum_{xy=n}\left(\sum_{mk=x} f(m)g(k)\right)h(y) = \sum_{mky=n} f(m)g(k)h(y)$$
$$= \sum_{ms=n}\left(\sum_{ky=s} f(m)g(k)h(y)\right) = \sum_{ms=n}\left(f(m)\sum_{ky=s} g(k)h(y)\right)$$
$$= \sum_{ms=n} f(m)(g*h)(s) = (f*(g*h))(n) \quad \forall n \in \mathbb{N}.$$

Damit ist $(f*g)*h = f*(g*h)$.

2) *Kommutatives Gesetz* Seien $f,g \in R$ beliebig. Für alle $n \in \mathbb{N}$ gilt $(f*g)(n) = \sum_{xy=n} f(x)g(y) = \sum_{yx=n} g(y)f(x) = (g*f)(n)$. Also ist $f*g = g*f$.

3) *Existenz eines Einselementes* Sei $f \in R$ beliebig. Es gilt $\sum_{xy=n} f(x)\varepsilon(y) = f(n)\varepsilon(1) = f(n) \quad \forall n \in \mathbb{N}$. Also ist $f*\varepsilon = f$, d.h. ε ist Einselement in R.

Es bleibt noch zu zeigen, dass in R die distributiven Gesetze gelten.

Seien $f,g,h \in R$ beliebig. Für alle $n \in \mathbb{N}$ gilt

$$(f*(g+h))(n) = \sum_{xy=n} f(x)(g+h)(y) = \sum_{xy=n} f(x)(g(y)+h(y))$$
$$= \sum_{xy=n}(f(x)g(y)+f(x)h(y)) = \sum_{xy=n} f(x)g(y) + \sum_{xy=n} f(x)h(y) = (f*g)(n)+(f*h)(n).$$

Somit ist $f*(g+h) = (f*g)+(f*h)$. Ferner gilt auch $(g+h)*f = f*(g+h) = (f*g)+(f*h) = (g*f)+(h*f)$, da R kommutativ bzgl. $*$ ist.

□

7.5 Bemerkung *Die Abbildung $j \in R$ sei definiert durch $j(n) = 1\ \forall n \in \mathbb{N}$. Dann gilt*

$$(j * f)(n) = \sum_{d|n} f(d) \quad \forall f \in R.$$

Beweis: Sei $f \in R$ beliebig. Dann gilt

$$(j * f)(n) = \sum_{ds=n} j(s)f(d) = \sum_{d|n} f(d).$$

□

7.6 Definition *Eine natürliche Zahl n heißt quadratfrei, falls für alle Primzahlen p gilt, dass p^2 kein Teiler von n ist.*

7.7 Bezeichnung *Mit $\alpha(n)$ bezeichnet man die Anzahl der Primteiler von n.*

7.8 Definition *Die Funktion $\mu \in R$ sei definiert durch*

$$\mu(n) = \begin{cases} (-1)^{\alpha(n)} & \text{, falls } n \text{ quadratfrei} \\ 0 & \text{, falls } n \text{ nicht quadratfrei.} \end{cases}$$

μ heißt die Möbiusfunktion.

7.9 Satz *Es gilt $\mu * j = \varepsilon$.*

Beweis: Es ist

$$(\mu * j)(1) = \sum_{d|1} \mu(d) = \mu(1) = (-1)^{\alpha(1)} = (-1)^0 = 1 = \varepsilon(1).$$

Sind m und n teilerfremde natürliche Zahlen, so folgt aus dem Satz von der eindeutigen Primfaktorzerlegung, dass

$$\{de \mid d, e \in \mathbb{N},\ d|m,\ e|n\} = \{f \mid f \in \mathbb{N},\ f|mn\}$$

ist. Da m und n teilerfremd sind, so ist $ggT(d, e) = 1$. Dann gilt

$$\mu(de) = (-1)^{\alpha(de)} = (-1)^{\alpha(d)+\alpha(e)} = (-1)^{\alpha(d)}(-1)^{\alpha(e)} = \mu(d) \cdot \mu(e).$$

Somit ist

$$(\mu * j)(mn) = \sum_{f|mn} \mu(f) = \sum_{de|mn} \mu(de) = \sum_{d|m} \sum_{e|n} \mu(d) \cdot \mu(e) = \left(\sum_{d|m} \mu(d)\right) \cdot \left(\sum_{e|n} \mu(e)\right)$$

$$= [(\mu * j)(m)]\,[(\mu * j)(n)]\,.$$

Es sei jetzt $1 < n \in \mathbb{N}$ und p ein Primteiler von n. Ferner sei $n = p^t m$ mit $ggT(p, m) = 1$. Dann ist also $(\mu * j)(n) = \left[(\mu * j)(p^t)\right]\,[(\mu * j)(m)]$. Wegen $(\mu * j)(p^t) = \sum_{k|p^t} \mu(k) = \mu(1) + \mu(p) = 1 - 1 = 0$ ist daher $(\mu * j)(n) = 0 = \varepsilon(n)$. Folglich ist $(\mu * j)(n) = \varepsilon(n)\ \forall n \in \mathbb{N}$, d.h. $\mu * j = \varepsilon$.

□

Der folgende Satz wurde für den Fall, dass q eine Primzahl ist, schon von R. Dedekind im Jahr 1857 bewiesen.

7.10 Satz *Es sei K ein endlicher Körper mit q Elementen. Ferner sei n eine natürliche Zahl und $p_1, p_2, ..., p_m$ seien alle Primteiler von n. Ist $I \subseteq \{1, 2, ..., m\}$ eine beliebige Teilmenge, so setzt man $n(I) = n \prod_{i \in I} p_i^{-1}$. Ist dann wieder $N_{n,q}$ die Anzahl der irreduziblen normierten Polynome vom Grade n über K, so ist*

$$N_{n,q} = n^{-1} \sum_{I} (-1)^{|I|} q^{n(I)},$$

wobei die Summe über alle Teilmengen $I \subseteq \{1, 2, ..., m\}$ zu erstrecken ist.

Beweis: Definiere $F, G \in R$ durch $F(n) = q^n$ und $G(n) = n \cdot N_{n,q}$ für alle $n \in \mathbb{N}$. Es gilt $F = j * G$, denn es ist $(j * G)(n) \overset{7.5}{=} \sum_{k|n} G(k) = \sum_{k|n} k \cdot N_{k,q} \overset{7.3}{=} q^n = F(n) \quad \forall n \in \mathbb{N}$.

Daraus folgt $G = \varepsilon * G \overset{7.9}{=} (\mu * j) * G = \mu * (j * G) = \mu * F$. Dann ist

$$nN_{n,q} = G(n) = (\mu * F)(n) = \sum_{de=n} \mu(d) F(e) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Da für jeden nicht quadratfreien Teiler d von n $\mu(d) = 0$ gilt, müssen wir also nur über die quadratfreie Teiler von n summieren.
Ist d ein quadratfreier Teiler von n, so ist $d = p_1^{t_1} \cdot \ldots \cdot p_m^{t_m}$ mit $t_i \in \{0, 1\} \ \forall i \in \{1, \ldots, m\}$. Sei die Menge $I = \{i \in \{1, \ldots, m\} \mid t_i = 1\} \subseteq \{1, \ldots, m\}$. Dann ist $\alpha(d) = |I|$ und $\frac{n}{d} = n(I)$. Damit gilt

$$nN_{n,q} = \sum_{\substack{d|n \\ d \text{ quadratfrei}}} \mu(d) F\left(\frac{n}{d}\right) = \sum_{\substack{d|n \\ d \text{ quadratfrei}}} (-1)^{\alpha(d)} q^{\frac{n}{d}} = \sum_{I \subseteq \{1,2,\ldots,m\}} (-1)^{|I|} q^{n(I)}.$$

Daraus folgt die Behauptung.

□

7.11 Beispiele
Wir bestimmen die Anzahl der irreduziblen Polynome vom Grade 9 und 12 über dem Körper $\mathbb{Z}_3$.

$$N_{9,3} = \frac{1}{9}((-1)^0 \cdot 3^9 + (-1)^1 \cdot 3^3) = 2184.$$

Dann ist die Anzahl aller irreduziblen Polynome vom Grade 9 über $\mathbb{Z}_3$ gleich $2 \cdot 2184 = 4368$. Insgesamt gibt es $2 \cdot 3^9 = 39366$ Polynome vom Grade 9 über $\mathbb{Z}_3$. Also ist ungefähr ein Neuntel aller Polynome vom Grade 9 irreduzibel über $\mathbb{Z}_3$.

$$N_{12,3} = \frac{1}{12}((-1)^0 \cdot 3^{12} + (-1)^1 \cdot 3^6 + (-1)^1 \cdot 3^4 + (-1)^2 \cdot 3^2) = 44220.$$

Dann ist die Anzahl aller irreduziblen Polynome vom Grade 12 über $\mathbb{Z}_3$ gleich $2 \cdot 44220 = 88440$. Insgesamt gibt es $2 \cdot 3^{12} = 1062882$ Polynome vom Grade 12 über $\mathbb{Z}_3$. Also ist ungefähr ein Zwölftel aller Polynome vom Grade 12 irreduzibel über $\mathbb{Z}_3$.

7.12 Korollar *Ist K ein Körper mit q Elementen und ist n eine beliebige natürliche Zahl, so gibt es irreduzible Polynome vom Grade n über K.*

Beweis: Gibt es kein solches Polynom, so ist $N_{n,q} = 0$, d.h., es ist $\sum_{I \subseteq M} (-1)^{|I|} q^{n(I)} = 0$, wobei $M = \{1, 2, ..., \alpha(n)\}$ ist. Dann ist $q^{n(M)} \sum_{I \subseteq M} (-1)^{|I|} q^{n(I)-n(M)} = 0$. Es folgt $\sum_{I \subseteq M} (-1)^{|I|} q^{n(I)-n(M)} = 0$, da $q^{n(M)} \neq 0$ ist. Nun gilt $n(I) \geq n(M)$, und $n(I) = n(M)$ genau dann, wenn $I = M$ ist. Dann ist

$$\sum_{I \subset M} (-1)^{|I|} q^{n(I)-n(M)} + (-1)^{|M|} q^{n(M)-n(M)} = 0.$$

Daraus folgt $\sum_{I \subset M} (-1)^{|I|} q^{n(I)-n(M)} = -(-1)^{\alpha(n)}$. Für $I \subset M$ gilt $n(I) > n(M)$ und somit $n(I) - n(M) \geq 1$. Dann ist

$$q(\sum_{I \subset M} (-1)^{|I|} q^{n(I)-n(M)-1}) = -(-1)^{\alpha(n)},$$

d.h., q ist ein Teiler von $(-1)^{\alpha(n)} = \pm 1$. Dies ist ein Widerspruch dazu, dass q eine Primzahlpotenz ist. Also ist $N_{n,q} \neq 0$.

□

7.13 Korollar *Ist p eine Primzahl, so gibt es zu jeder natürlichen Zahl $n \in \mathbb{N}$ einen und bis auf Isomorphie auch nur einen Körper mit p^n Elementen.*

Beweis: Wir setzen $K = \mathbb{Z}_p$. Nach 7.12 existiert ein Polynom $f \in \mathbb{Z}_p[T]$ vom Grade n, das irreduzibel über $\mathbb{Z}_p$ ist. Dann ist nach [1] Satz 3.37 $\mathbb{Z}_p[T]/(f)$ ein Körper mit p^n Elementen und nach 6.10(3) sind je zwei Körper mit p^n Elementen isomorph.

□

8 Ein Satz von Wedderburn

Ziel dieser Ausarbeitung soll es sein, den 1905 aufgestellten Satz von Wedderburn zu beweisen, der besagt, dass endliche Schiefkörper kommutativ sind. Diesbezüglich werden zur Motivation einige veranschaulichende Beispiele vorausgeschickt, die bezeugen, dass es sowohl abzählbar unendliche als auch überabzählbar unendliche Schiefkörper gibt, die nicht kommutativ sind.

8.1 Beispiel *Sei K ein Zwischenkörper von $\mathbb{Q}$ und $\mathbb{R}$. Dann ist*

$$\mathcal{M}_K := \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in K\,[i] \right\} \subseteq M_2(\mathbb{C})$$

ein nicht kommutativer Schiefkörper. Für $K = \mathbb{Q}$ ist $\mathcal{M}_{\mathbb{Q}}$ abzählbar unendlich. Für $K = \mathbb{R}$ ist $\mathcal{M}_{\mathbb{R}}$ überabzählbar unendlich.

Beweis: Im Folgenden ist zu zeigen: $\mathcal{M}_K$ ist ein nicht kommutativer Schiefkörper.
Es folgt leicht, daß $\mathcal{M}_K$ eine Untergruppe von $(\mathrm{M}_2(\mathbb{C}), +)$ ist.
Offensichtlich ist $\mathcal{M}_K$ abgeschlossen bzgl. der Matrixmultiplikation, denn es gilt:

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{b}c - \overline{a}\overline{d} & -\overline{b}d + \overline{ac} \end{pmatrix},$$

wobei $\overline{(ac - b\overline{d})} = \overline{ac} - \overline{b\overline{d}} = -\overline{b}d + \overline{ac}$ und $-\overline{(ad + b\overline{c})} = -\overline{a}\overline{d} - \overline{b}c$.

Nun ist zu zeigen, dass $\mathcal{M}_K \setminus \{0\}$ bezüglich der Matrizenmultiplikation eine Gruppe ist.
Für $A \in \mathcal{M}_K$ gilt

$$\det(A) = |a|^2 + |b|^2 \in \mathbb{R} \quad \text{und} \quad A \neq 0 \Leftrightarrow \det(A) \neq 0.$$

Also: $A, B \in \mathcal{M}_K \setminus \{0\} \implies \det(AB) = \det(A)\det(B) \neq 0$ und damit $AB \in \mathcal{M}_K \setminus \{0\}$.
Wegen $\mathcal{M}_K \subseteq M_2(\mathbb{C})$ gilt das Assoziativgesetz der Multiplikation.
Ferner ist $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{M}_K \setminus \{0\}$ Einselement bezüglich der Multiplikation.
Sei $A \in \mathcal{M}_K \setminus \{0\}$. Dann gilt

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix} \in \mathcal{M}_K \setminus \{0\}.$$

Desweiteren gelten die distributiven Gesetze.

Abschließend wird gezeigt, daß die Matrixmultiplikation auf $\mathcal{M}_K$ nicht kommutativ ist:

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

□

8.2 Definition und Satz *Der Schiefkörper*

$$\mathcal{M}_{\mathbb{R}} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in \mathbb{C} \right\}$$

heißt Quaternionenschiefkörper und wird mit $\mathbb{H}$ bezeichnet.
Die Elemente von $\mathbb{H}$ heißen Quaternionen. Für die Elemente

$$e := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ j := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ k := \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \in \mathbb{H} \text{ gilt:}$$

a) *$\{e, i, j, k\}$ ist eine Basis von $\mathbb{H}$ über $\mathbb{R}$.*

b) *Es gilt*

$$i^2 = j^2 = k^2 = ijk = -e$$
$$ij = -ji = k \quad , \quad ik = -ki = -j \quad , \quad jk = -kj = i.$$

c) *$\mathcal{Q} := \{+e, -e, +i, -i, +j, -j, +k, -k\}$ ist eine nicht abelsche Untergruppe von $(\mathbb{H}^\star, \cdot)$.*
($\mathcal{Q}$ heißt Quaternionengruppe).

d) *Bezeichnet Im $\mathbb{H}$ den von i, j, k erzeugten Unterraum von $\mathbb{H}$, so gilt*

$$x^2 \in \mathbb{R}e \text{ für alle } x \in \text{Im } \mathbb{H}.$$

e) *Für jede Quaternion $x = ae + bi + cj + dk \in \mathbb{H}$ gilt:*

$$x^2 = 2ax - (a^2 + b^2 + c^2 + d^2)e.$$

Beweis:
a) Offensichtlich sind e, i, j, k linear unabhängig. Es bleibt zu zeigen e, i, j, k bilden ein Erzeugendensystem. Diesbezüglich muss gelten:

$$\begin{aligned} \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} &= \alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \beta \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + \gamma \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + \delta \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \\ &= \begin{pmatrix} \alpha + \beta i & -\gamma - \delta i \\ \gamma - \delta i & \alpha - \beta i \end{pmatrix}. \end{aligned}$$

Da für $a = \alpha + \beta i$ gilt $\overline{a} = \alpha - \beta i$ und für $b = -(\gamma - \delta i)$ gilt $-\overline{b} = \gamma - \delta i$, gilt obrige Aussage nach Definition von $\overline{a}$ und $\overline{b}$.

b) Alle Aussagen sind leicht nachzurechnen.

c) Nach (8.2 b) ist klar, dass die Multiplikation abgeschlossen und offensichtlich nicht kommutativ ist. Des weiteren ist $e_{\mathbb{H}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{Q}$ und

$$e^{-1} = e\ ,\ -e^{-1} = -e\ ,\ i^{-1} = -i\ ,\ -i^{-1} = i\ ,\ j^{-1} = -j\ ,\ -j^{-1} = j\ ,\ k^{-1} = -k$$
$$\text{sowie} \quad -k^{-1} = k.$$

Damit ist $\mathcal{Q}$ abgeschlossen bezüglich Inversenbildung und erfüllt die Eigenschaften einer Untergruppe.

d) Sei $x \in \operatorname{Im}\mathbb{H}$, dann gilt $x = bi + cj + dk$ mit $b, c, d \in \mathbb{R}$. Dies liefert

$$\begin{aligned} x^2 &= (bi + cj + dk)^2 \\ &= b^2 \underbrace{i^2}_{-e} + c^2 \underbrace{j^2}_{-e} + d^2 \underbrace{k^2}_{-e} + bcij + bdik + \underbrace{cbji}_{-bcij} + cdjk + \underbrace{dbki}_{-bdik} + \underbrace{dckj}_{-cdjk} \\ &= e(-b^2 - c^2 - d^2) \end{aligned}$$

Da $b, c, d \in \mathbb{R}$ ist auch $(-b^2 - c^2 - d^2) \in \mathbb{R}$.

e) Sei $x = ae + bi + cj + dk$ mit $a, b, c, d \in \mathbb{R}$. Dann gilt

$$\begin{aligned} x^2 &= (ae)^2 + (bi)^2 + (cj)^2 + (dk)^2 + abi + acj + adk + bai + caj + dak + bcij \\ &\quad + bdik + cbji + cdjk + dbki + dckj \\ &= a^2e - b^2e - c^2e - d^2e + 2abi + 2acj + 2adk \\ &= 2abi + 2acj + 2adk + 2a^2e - a^2e - b^2e - c^2e - d^2e \\ &= 2a(ae + bi + cj + dk) - e(a^2 + b^2 + c^2 + d^2) \\ &= 2ax - e(a^2 + b^2 + c^2 + d^2) \end{aligned}$$

□

8.3 Exkurs *(Konsequenzen aus der Nichtkommutativität von $\mathbb{H}$) Wie in (8.2) gezeigt, handelt es sich bei $\mathbb{H}$ um einen Schiefkörper. Offensichtlich ist $\mathbb{H}$ nicht kommutativ. Dies hat ungewohnte Konsequenzen. So wurden beispielsweise Polynome in Bezug auf unseren bisherigen Wissenstand lediglich auf kommutativen Hintergründen betrachtet. An dieser Stelle stellt sich die Frage: Können Polynome über Schiefkörpern betrachtet werden, und welche Folgen kann das Fehlen der Nichtkommutativität haben. Die folgenden Punkte sollen diesbezüglich einen kleinen Einblick geben.*

a) *Polynome können nicht in gewohnter Art und Weise faktorisiert werden.*
Seien $x, y \in \mathbb{H}$. Dann gilt $(T - x)(T - y) = T^2 - xT - Ty + xy \neq T^2 - (x + y)T + xy$.

b) *Polynome können mehr Nullstellen haben, als ihr Grad ist. $T^2 + e = 0$ wird offensichtlich erfüllt von $i, -i, j, -j, k, -k$. Das Polynom $f := T^2 + e$ hat folglich mindestens 6 Nullstellen. Nach (8.2 d) hat f sogar unendlich viele Nullstellen, denn für jedes $u \in \operatorname{Im}\mathbb{H}$ mit Länge 1 gilt $u^2 = -\underbrace{(b^2 + c^2 + d^2)}_{=1} = e = -e$. Damit erfüllt jedes u obige Gleichung und es ist gezeigt, das Polynom f hat unendlich viele Nullstellen. Nun ist nach bisheriger Kenntnis ein Polynom über einem kommutativen Körper mit unendlich vielen Nullstellen das Nullpolynom. f jedoch ist offensichtlich nicht das Nullpolynom. Ein erster Widerspruch wird deutlich.*

c) *Es gibt kubische Polynome, die von allen Quaternionen anulliert werden. Auch dieses Beispiel spiegelt das in b) angesprochene Problem. Sei $g := T^2iTi + iT^2iT - iTiT^2 - TiT^2i$. Nach Voraussetzung wird das Polynom über einem nichtkommutativen Schiefkörper betrachtet. In Folge dessen handelt es sich offensichtlich nicht um das Nullpolynom. Einsetzen einer beliebigen Quaternion x, die nach (8.2 e) der Gleichung $x^2 = \alpha x + \beta e$ genügt, annulliert g jedoch. Gleichzeitig verdeutlicht sich an diesem Beispiel ein Problem in Bezug auf die Begriffbestimmung des Grades von Polynomen. Im ursprünglichen Sinn wurde der Grad eines Polynoms verstanden als die höchste Potenz desselben. Da die hier gewählte Multiplikation nicht kommutativ ist, müsste man von einem Polynom zweiten Gerades sprechen, obwohl man es eher als ein Polynom dritten Gerades auffassen würde.*

d) *Determinaten können nicht sinnvoll in herkömmlicher Weise definiert werden. Betrachtet man zwei Möglichkeiten der Definition der Determinante:*

$$det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \quad oder \quad det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - cb.$$

Im Folgenden wird jeweils ein Beispiel angeführt. Im ersten Fall erhält man

$$det\begin{pmatrix} i & j \\ i & j \end{pmatrix} = ij - ji = 2k.$$

Der zweite Fall liefert

$$det\begin{pmatrix} i & i \\ j & j \end{pmatrix} = ij - ji = 2k.$$

Nach Definition der Determinante ist diese jedoch alternierend, das heißt: Hat eine Matrix gleiche Zeilen bzw. Spalten, so ist ihre Determinante Null. In beiden Fällen jedoch ist $2k$ offensichtlich von Null verschieden.

8.4 Definition *Sei G eine Gruppe, $x, y \in G$. x heißt konjugiert zu y (in Zeichen $x \sim y$) wenn es ein $g \in G$ gibt mit $y = g^{-1}xg$.*

$$\mathcal{K}(x) := \{g^{-1}xg | g \in G\}$$

bezeichnet die Menge der zu x konjugierten Elemente. $\mathcal{K}(x)$ heißt Konjugationsklasse von x.

8.5 Bemerkung *Die Konjugation ist eine Äquivalenzrelation auf der Gruppe G.*

Beweis: Es muss gezeigt werden, dass die Konjugation reflexiv, symmetrisch und transitiv ist.

Reflexiblität: $a \sim a$, da $a = e^{-1}ae$.

Symmetrisch: $a \sim b \Leftrightarrow a = g^{-1}bg \Leftrightarrow b = gag^{-1}$. Da $(g^{-1})^{-1} = g$ folgt $b \sim a$.

Transitiv: Sei $a \sim b$ und $b \sim c$. Dann gilt $a = g^{-1}bg$ und $b = \tilde{g}^{-1}c\tilde{g}$. Einsetzen liefert $a = g^{-1}\tilde{g}^{-1}c\tilde{g}g = (\tilde{g}g)^{-1}c(\tilde{g}g)$. Daraus folgt $a \sim c$.

□

8.6 Definition *Sei G eine Gruppe, $g \in G$. Dann heißt*

$$\mathcal{C}_G(g) := \{x | x \in G, xg = gx\}$$

der Zentralisator von g in G.

8.7 Bemerkung *$\mathcal{C}_G(g)$ ist eine Untergruppe von G.*

Beweis: Klar ist, dass $e \in \mathcal{C}_G(g)$, da $eg = ge$ für alle $g \in G$.

Des Weiteren muss gelten:
Für $y, z \in \mathcal{C}_G(g)$ folgt $yz \in \mathcal{C}_G(g)$. Es gilt $(yz)g = y(zg) = (yg)z = g(yz) \Rightarrow yz \in \mathcal{C}_G(g)$.
Außerdem muss gelten, aus $x \in \mathcal{C}_G(g)$ folgt $x^{-1} \in \mathcal{C}_G(g)$. Aus $xg = gx$ folgt
$g = x^{-1}gx \Leftrightarrow gx^{-1} = x^{-1}g \Leftrightarrow x^{-1}g = gx^{-1}$. Daraus folgt $x^{-1} \in \mathcal{C}_G(g)$. Damit ist gezeigt, $\mathcal{C}_G(g)$ ist Untergruppe von G.

□

8.8 Definition *Sei G eine Gruppe. Dann heißt*

$$\mathcal{Z}(G) := \bigcap_{g \in G} \mathcal{C}_G(g)$$

das Zentrum von G.

8.9 Lemma *Für $x \in G$ gilt*

a)

$$\mathcal{Z}(G) = \{x | x \in G, gx = xg \ \text{ für alle } \ g \in G\}.$$

b)

$$|\mathcal{K}(x)| = 1 \Leftrightarrow x \in \mathcal{Z}(G).$$

Beweis:
a) klar
b) Sei $x \in \mathcal{Z}(G)$. Dann gilt $xg = gx$ für alle $g \in G \Leftrightarrow g^{-1}xg = x$ für alle $g \in G \Leftrightarrow \{x\} = \{g^{-1}xg \mid g \in G\} \Leftrightarrow \{x\} = K(x) \Leftrightarrow |K(x)| = 1$.

□

8.10 Definition *Sei G eine Gruppe, H eine Untergruppe von G und G/H die Menge der Rechtsnebenklassen von G bzgl. H. Dann heißt*

$$(G : H) := |G/H|$$

der Index von H in G.

8.11 Lemma *Sei G eine endliche Gruppe, S sei eine Konjugationsklasse.*
Für $g \in S$ gilt

$$|S| = (G : \mathcal{C}_G(g)),$$

d.h. es gibt genausoviele zu g konjugierte Elemente wie Rechtsnebenklassen von G bzgl. $\mathcal{C}_G(g)$.

Beweis: Um die Elementzahl von S zu bestimmen, muss überlegt werden, wann zwei zueinander konjugierte Elemente gleich sind. Seien $x, y \in G$, dann gilt

$$x^{-1}gx = y^{-1}gy \Leftrightarrow yx^{-1}g = gyx^{-1} \Leftrightarrow yx^{-1} \in \mathcal{C}_G(g) \Leftrightarrow y \in \mathcal{C}_G(g)x.$$

Da Nebenklassen entweder gleich oder disjunkt sind, ist $\mathcal{C}_G(g)x = \mathcal{C}_G(g)y$. Demnach sind zwei zueinander konjugierte Elemente genau dann gleich, wenn ihre Rechtsnebenklassen gleich sind. Es gibt also genau so viele zu g konjugierte Elemente, wie Rechtsnebenklassen von G bezüglich $\mathcal{C}_G(g)$, d.h. $|S| = (G : \mathcal{C}_G(g))$.

□

8.12 Satz *(Die Klassengleichung) Sei G eine endliche Gruppe. $S_1, ..., S_n$ seien sämtliche Konjugationsklassen mit mehr als einem Element. Für $g_i \in S_i, i = 1, ..., n$ gilt:*

$$|G| = |\mathcal{Z}(G)| + \sum_{i=1}^{n} (G : \mathcal{C}_G(g_i)).$$

Beweis: Sei $V := \{g_1, g_2, ..., g_d\}$ ein vollständiges Vertretersystem bezüglich Konjugation in G. Wähle $n \in \mathbb{N}$ so, dass $\{g_1, ..., g_n\} \notin \mathcal{Z}(G)$ und $\{g_{n+1}, ..., g_d\} \in \mathcal{Z}(G)$. Da die Konjugation nach (8.5) eine Äquivalenzrelation ist, ist G die disjunkte Vereinigung ihrer Äquivalenzklassen. Es gilt

$$G = \bigcup_{i=1}^{d} K(g_i).$$

Nach (8.9) besteht $\mathcal{Z}(G)$ aus denjenigen Elementen, deren Konjugationsklassen einelementig sind, woraus folgt

$$G = \mathcal{Z}(G) \cup (\bigcup_{i=1}^{n} K(g_i)) = \mathcal{Z}(G) \cup (\bigcup_{i=1}^{n} S_i).$$

Da es sich in beiden Fällen um disjunkte Vereinigungen handelt, ergibt die Betrachtung der Elementzahlen

$$|G| = |\mathcal{Z}(G)| + |\bigcup_{i=1}^{n} S_i| = |\mathcal{Z}(G)| + \sum_{i=1}^{n} |S_i|.$$

Nach (8.11) gilt $|S| = (G : \mathcal{C}_G(g))$ und es folgt $|G| = |\mathcal{Z}(G)| + \sum_{i=1}^{n} (G : \mathcal{C}_G(g_i))$.

□

8.13 Hilfsatz *(über Teilbarkeit) Es seien $q, m, n \in \mathbb{N}$. Ferner sei $q > 1$.*
Genau dann ist $q^m - 1$ ein Teiler von $q^n - 1$, wenn m ein Teiler von n ist.

Beweis: " $\Leftarrow$ " Im Folgenden wird gezeigt, aus m teilt n folgt $q^m - 1$ teilt $q^n - 1$. Aus $m|n$ folgt $n = ms$ für $s \in \mathbb{N}$. Einsetzen von ms für n liefert

$$q^n - 1 = q^{ms} - 1 = (q^m - 1) \cdot \frac{q^{ms} - 1}{q^m - 1}.$$

Durch Anwenden der geometrischen Summenformel erhält man

$$q^n - 1 = (q^m - 1) \sum_{i=0}^{s-1} q^{mi},$$

woraus $q^m - 1 | q^n - 1$ folgt.

" $\Rightarrow$ " Nun gelte $q^m - 1 | q^n - 1$. Im Folgenden ist zu zeigen $m|n$. Der Beweis wird durch Widerspruch geführt. Dazu nehmen wir an, dass $m \nmid n$ gilt. Dann folgt $n = ms + r$ mit $0 \leq r < m$. Ziel wird sein, zu zeigen, dass gilt $r = 0$, woraus $n = ms$ und $m|n$ folgt.
Weise zuerst folgende Behauptung nach:

$$q^m - 1 \mid q^n - 1 - q^r(q^{ms} - 1).$$

Nach Vorraussetzung gilt $q^m - 1 | q^n - 1$. Falls $(q^m - 1)$ auch $(q^{ms} - 1)$ teilt, so teilt $(q^m - 1)$ den gesamten Ausdruck nach Teilbarkeitsregeln.
Es genügt zu zeigen $q^m - 1 | q^{ms} - 1$. Es gilt $q^{ms} - 1 = q^{m^s} - 1$. Ein Anwenden der Binomischen Formel $a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}$ liefert

$$q^{ms} - 1 = (q^m - 1) \cdot (q^{s-1} + q^{s-2} + q^{s-3} + ... + q^{-1} + q^0) = (q^m - 1) \sum_{i=1}^{s} q^{s-i} \in \mathbb{N},$$

woraus $q^m - 1 | q^{ms} - 1$ folgt. Damit gilt nach obigen Ausführungen

$$q^m - 1 | \underbrace{q^n - 1 - q^r(q^{ms} - 1)}_{= q^r - 1}.$$

Durch Auflösen der Klammern und Vereinfachen erhält man $q^n - 1 - q^r(q^{ms} - 1) = q^r - 1$, und es folgt

$$q^m - 1 | q^r - 1 \quad \Rightarrow \quad q^m - 1 \leq q^r - 1.$$

Aus $0 \leq r < m$ lässt sich jedoch folgern

$$q^m - 1 > q^r - 1.$$

Dieser Widerspruch liefert $r = 0$, woraus $n = ms$ folgt, d.h. $m|n$.

□

8.14 Definition *Sei K ein Schiefkörper. Für $a \in K$ heißt*

$$\mathcal{C}(a) := \{x | x \in K, xa = ax\}$$

der Zentralisator von a in K.

8.15 Bemerkung *$\mathcal{C}(a)$ ist ein Unterkörper von K.*

Beweis: Im Folgenden ist zu zeigen $1_K \in \mathcal{C}(a)$, $\mathcal{C}(a)$ ist abgeschlossen bezüglich Multiplikation, Subtrakion und der Bildung von Inversen.
$1_K \in \mathcal{C}(a)$, da $1_K a = a = a 1_K$.
Seien $x, y \in \mathcal{C}(a)$. Dann gilt $(x-y)a = xa - ya = ax - ay = a(x-y) \Rightarrow (x-y) \in \mathcal{C}(a)$.
Des Weiteren gilt $(xy)a = x(ya) = x(ay) = (xa)y = a(xy) \Rightarrow (xy) \in \mathcal{C}(a)$.
Sei $y \in \mathcal{C}(a), y \neq 0$, dann folgt $ya = ay \Leftrightarrow ay^{-1} = y^{-1}a$. Damit gilt $y^{-1} \in \mathcal{C}(a)$.

□

8.16 Definition *Sei K ein Schiefkörper. Dann heißt*

$$\mathcal{Z}(K) := \bigcap_{a \in K} \mathcal{C}(a)$$

das Zentrum von K.

8.17 Bemerkung *$\mathcal{Z}(K)$ ist ein Unterkörper von K.*

Beweis: Nach (2.5) des Algebra-Skripts gilt, der Durchschnitt eines beliebigen Systems von Unterkörpern ist wieder ein Unterkörper.

□

8.18 Hilfsatz *Ist m ein Teiler von n mit $m < n$, so gibt es ein $g \in \mathbb{Z}[T]$ mit*

$$(T^m - 1) \cdot g = (T^n - 1).$$

Ferner ist Φ_n ein Teiler von $g \in \mathbb{Z}[T]$.

Beweis: Nach (5.10.2) gilt

$$T^n - 1 = \prod_{\substack{d|n \\ 0<d}} \Phi_d = \Phi_n \cdot \prod_{\substack{d|n \\ 0<d<n}} \Phi_d.$$

Sei im Folgenden $\{d_1, ..., d_r\}$ die Menge der von n verschiedenen Teiler von n.

$$T^n - 1 = \Phi_n \cdot \Phi_{d_1} \cdot \Phi_{d_2} \cdot ... \cdot \Phi_{d_{i-1}} \cdot \Phi_{d_i} \cdot \Phi_{d_{i+1}} \cdot ... \cdot \Phi_{d_r}.$$

Da $T^{d_i} - 1 = \Phi_{d_i} \cdot \prod_{\substack{f|d_i \\ 0<f<d_i}} \Phi_f$, gilt

$$T^n - 1 = \Phi_n \cdot \Phi_{d_1} \cdot \Phi_{d_2} \cdot ... \cdot \Phi_{d_{i-1}} \cdot \frac{T^{di} - 1}{\prod_{\substack{f|d_i \\ 0<f<d_i}} \Phi_f} \cdot \Phi_{d_{i+1}} \cdot ... \cdot \Phi_{d_r}.$$

$f|d_i$ und $d_i|n$, woraus folgt $f|n$. Infolgedessen lässt sich der Nenner des Bruches vollständig wegkürzen und man erhält

$$T^n - 1 = (T^{d_i} - 1) \underbrace{\bar{g} \cdot \Phi_n}_{:=g},$$

wobei $\bar{g}$ das Produkt über die übrig gebliebenen Kreisteilungspolynome ist. Da Kreisteilungspolynome ganzzahlige Koeffizienten haben folgt $\bar{g} \in \mathbb{Z}[T]$ und daraus $g \in \mathbb{Z}[T]$. Für $d_i = m$ erhält man $T^n - 1 = (T^m - 1)g$ mit $g \in \mathbb{Z}[T]$. Des Weiteren gilt $\Phi_n|g$, da $g = \Phi_n \cdot \bar{g}$ mit $\bar{g} \in \mathbb{Z}[T]$.

□

8.19 Satz *(von Wedderburn, 1905) Jeder endliche Schiefkörper ist kommutativ.*

Beweis: Der im Folgenden dargestellte Beweis stammt von E. Witt aus dem Jahr 1931 und wird durch Widerspruch geführt.

Annahme: Es gibt einen nichtkommutativen, endlichen Schiefkörper K.

Dann ist $\mathcal{Z}(K)$ ein Unterkörper und hat mindestens zwei Elemente. Nach Annahme gilt außerdem: K ist nicht kommutativ, d.h. $\mathcal{Z}(K) \subset K$, mit $\mathcal{Z}(K) \neq K$. Demnach lässt sich folgende Ungleichung aufstellen:

$$1 < |\mathcal{Z}(K)| := q < |K| \quad \text{mit} \quad q \geq 2.$$

$\mathcal{Z}(K)$ ist ein kommutativer Unterkörper von K. Betrachte im Folgenden K als Vektorraum über $\mathcal{Z}(K)$. Es gilt

$$\dim_{\mathcal{Z}(K)} K = [K : \mathcal{Z}(K)] =: n \quad \text{mit} \quad n > 1.$$

Hieraus folgt $K \cong \mathcal{Z}(K)^n$. Betrachtet man die Elementzahlen, so erhält man

$$|K| = |\mathcal{Z}(K)^n| = |\mathcal{Z}(K)|^n = q^n.$$

Um im weiteren Verlauf (8.11) und (8.12) anwenden zu können, betrachte $(K^*, \cdot)$, die multiplikative Gruppe von K.
Seien $S_1, ..., S_t$ die Konjugationsklassen von K^* mit mehr als einem Element. Sei $a_i \in S_i$.

Bestimme im Folgenden die Ordnung des Zentralisators $\mathcal{C}(a_i)$. $\mathcal{Z}(K)$ ist kommutativer Unterkörper von $\mathcal{C}(a_i)$. $\mathcal{C}(a_i)$ lässt sich demnach als Vektorraum über $\mathcal{Z}(K)$ betrachten. Es gilt

$$\dim_{\mathcal{Z}(K)} \mathcal{C}(a_i) = [\mathcal{C}(a_i) : \mathcal{Z}(K)] =: m_i \quad \text{für} \quad m_i \in \mathbb{N}.$$

Demnach gilt $\mathcal{C}(a_i) \cong \mathcal{Z}(K)^{m_i}$. Betrachtet man die Elementzahlen, so erhält man

$$|\mathcal{C}(a_i)| = |\mathcal{Z}(K)^{m_i}| = |\mathcal{Z}(K)|^{m_i} = q^{m_i}.$$

Für $a_i \neq 0$ ist offenbar $\mathcal{C}(a_i)^* = \mathcal{C}_{K^*}(a_i)$. Mit Anwendung obiger Ergebnisse gilt ferner $|\mathcal{C}(a_i)^*| = q^{m_i} - 1$, sowie $|K^*| = q^n - 1$. Nach (8.7) ist $\mathcal{C}(a_i)^*$ Untergruppe von K^* und es folgt mit Anwendung von (8.11)

$$|S_i| = (K^* : \mathcal{C}(a_i)^*) = \frac{|K^*|}{|\mathcal{C}(a_i)^*|} = \frac{q^n - 1}{q^{m_i} - 1} \in \mathbb{N} \quad (\text{da } |S_i| \in \mathbb{N}).$$

Folglich ist $q^{m_i} - 1$ ein Teiler von $q^n - 1$, wobei $q, m_i, n \in \mathbb{N}$ mit $q \geq 2$ gilt. Mit Anwendung von (8.13) folgt $m_i | n$ mit $m_i \leq n$. Im Folgenden wird gezeigt, dass $m_i < n$ für alle $i = 1, ..., t$ gilt.
Annahme: Sei $m_i = n$ für ein $i \in \{1, ..., t\}$. Dann folgt

$$|K^*| = q^n - 1 = |C(a_i)^*| \Rightarrow C(a_i)^* = K^*.$$

Demnach kommutiert jedes Element aus K^* mit $a_i \in S_i$. Dann kommutiert auch jedes $a_i \in S_i$ mit jedem Element aus K^*, woraus folgt $a_i \in \mathcal{Z}(K^*)$. Mit Anwendung von (8.9) ist $|S_i| = 1$. Dies ist ein Widerspruch zur Wahl der Konjugationsklasse S_i. Demnach gilt $m_i | n$ mit $m_i < n$.
Betrachte die Klassengleichung (8.12). Es gilt:

$$|K^*| = |\mathcal{Z}(K^*)| + \sum_{i=1}^{t} (K^* : \mathcal{C}(a_i)^*).$$

Einsetzen der oben bestimmten Beziehungen liefert

$$(\star) \qquad q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{m_i} - 1}.$$

Im Folgenden wird auf Kreisteilungspolynome zurückgegriffen und gezeigt, dass $\Phi_n(q)$ $q^n - 1$ und die Summe teilt. Anschließend folgt nach Teilbarkeitsregeln $\Phi_n(q) | q - 1$.

Zeige $\Phi_n(q) | q^n - 1$. Nach (5.10.2) gilt

$$T^n - 1 = \Phi_n \cdot \prod_{\substack{d|n \\ 0<d<n}} \Phi_d.$$

Einsetzen von q liefert

$$q^n - 1 = \Phi_n(q) \prod_{\substack{d|n \\ 0<d<n}} \Phi_d(q).$$

Da Kreisteilungspolynome ganzzahlige Koeffizienten haben, gilt $q^n - 1 \in \mathbb{N}$, $\Phi_n(q) \in \mathbb{Z}$ und $\prod_{\substack{d|n \\ 0<d<n}} \Phi_d(q) \in \mathbb{Z}$, woraus folgt $\Phi_n(q) | q^n - 1$.

Nach (8.18) gilt des Weiteren für $m_i|n$ mit $m_i < n$:
Es gibt ein $g \in \mathbb{Z}[T]$ mit $(T^{m_i} - 1)g = (T^n - 1)$ und $g = \Phi_n \cdot \tilde{g}$ mit $\tilde{g} \in \mathbb{Z}[T]$.

$$(T^{m_i} - 1) \cdot \Phi_n \cdot \tilde{g} = (T^n - 1).$$

Einsetzen von q liefert $(q^{m_i} - 1) \cdot \Phi_n(q) \cdot \tilde{g}(q) = q^n - 1$, woraus folgt

$$\Phi_n(q) \cdot \tilde{g}(q) = \frac{q^n - 1}{q^{m_i} - 1} = |S_i| \in \mathbb{N}.$$

Da Kreisteilungspolynome ganzzahlige Koeffizienten haben, gilt $\Phi_n(q), \tilde{g}(q) \in \mathbb{Z}$, woraus folgt $\Phi_n(q)|\dfrac{q^n - 1}{q^{m_i} - 1}$, und damit $\Phi_n(q)| \sum\limits_{i=1}^{t} \frac{q^n-1}{q^{m_i}-1}$.

Damit folgt aus $(\star)$ $\Phi_n(q)|q - 1$ und somit

$$(\star\star) \qquad |\Phi_n(q)| \leq q - 1.$$

Dies wird zum Wiederspruch geführt.
Es ist

$$\Phi_n(q) = \prod_{\lambda}(q - \lambda),$$

wobei λ alle primitiven n-ten Einheitswurzeln durchläuft. Nach (5.10.1) ist

$$\text{grad}(\Phi_n) = \phi(n).$$

Da $n > 1$ ist, ist $\lambda \neq 1$.
Desweiteren ist $\lambda = a + bi$ mit $a, b \in \mathbb{R}$ und es gilt $1 = |\lambda|^2 = a^2 + b^2$.
Es ist $|q - \lambda|^2 = |q - a - bi|^2 = (q - a)^2 + b^2 = q^2 - 2qa + \underbrace{a^2 + b^2}_{=1}$, woraus folgt

$$|q - \lambda|^2 = q^2 - 2qa + 1.$$

Da $\lambda \neq 1$ ist, ist $a < 1$. Dies liefert folgende Abschätzung

$$|q - \lambda|^2 = q^2 - 2qa + 1 > q^2 - 2q + 1 = (q - 1)^2.$$

Da $q \geq 2$ ist, ist $(q - 1) > 0$ und es folgt $|q - \lambda| > q - 1$. Also

$$|\Phi_n(q)| = \prod_{\lambda} |q - \lambda| > \prod_{\lambda}(q - 1) = (q - 1)^{\varphi(n)} \geq q - 1, \quad \text{da} \quad q - 1 \geq 1.$$

Zusammenfassend gilt $|\Phi_n(q)| > q - 1$ im Widerspruch zur vorherigen Aussage $|\Phi_n(q)| \leq q - 1$ (vergleiche $(\star\star)$).

Also ist jeder endliche Schiefkörper kommutativ.

□

9 Endlichdimensionale reelle Algebren

9.1 Definition a) *Eine* **(reelle) Algebra** *(oder auch $\mathbb{R}$–Algebra) $\mathcal{A}$ ist ein $\mathbb{R}$–Vektorraum, auf dem eine $\mathbb{R}$–bilineare Multiplikation*

$$\mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A} \quad , \quad (x, y) \longmapsto x \cdot y \quad (=: xy)$$

definiert ist.

b) *Eine reelle Algebra $\mathcal{A}$ heißt* **assoziativ**, *wenn die Multiplikation assoziativ ist.*

c) *Eine reelle Algebra $\mathcal{A}$ heißt* **kommutativ**, *wenn die Multiplikation kommutativ ist.*

d) *$e \in \mathcal{A}$ heißt* **Einselement der Algebra**, *wenn $x \cdot e = x = e \cdot x$ für alle $x \in \mathcal{A}$ gilt.*

e) $\dim \mathcal{A} := \dim_{\mathbb{R}}(\mathcal{A})$ *heißt die* **Dimension der reellen Algebra $\mathcal{A}$**.

f) *Eine reelle Algebra $\mathcal{A}$ heißt* **nullteilerfrei**, *wenn für alle $x, y \in \mathcal{A}$ gilt:*
$x \cdot y = 0 \implies x = 0$ *oder* $y = 0$.

g) *Eine reelle Algebra $\mathcal{A}$ heißt* **alternativ** *wenn für alle $x, y \in \mathcal{A}$ gilt:*
$x \cdot (x \cdot y) = x^2 \cdot y \quad$ *und* $\quad (x \cdot y) \cdot y = x \cdot y^2$.

9.2 Bemerkung a) *Bei einer reellen Algebra $\mathcal{A}$ treten insgesamt 5 Verknüpfungen auf, die zum Teil mit denselben Symbolen bezeichnet werden: Die Körperaddition und –multiplikation auf $\mathbb{R}$, die Addition und die Skalarmultiplikation auf dem Vektorraum $\mathcal{A}$ und die Multiplikation auf der Algebra $\mathcal{A}$. Diese Verknüpfungen sind in vielfacher Weise miteinander verzahnt, was durch die entsprechenden Körper–, Vektorraum– und Algebraeigenschaften zum Ausdruck kommt.*

b) *Die $\mathbb{R}$–Bilinearität der Multiplikation bedeutet in Formeln ausgedrückt:*

$$(\alpha x + \beta y) \cdot z = \alpha(x \cdot z) + \beta(y \cdot z)$$

$$x \cdot (\alpha y + \beta z) = \alpha(x \cdot y) + \beta(x \cdot z)$$

Dies muß für alle $\alpha, \beta \in \mathbb{R}$ und $x, y, z \in \mathcal{A}$ gelten.

c) *Aus b) folgt insbesondere $\quad \alpha(x \cdot y) = \alpha(x \cdot y) = x \cdot (\alpha y)$ für alle $\alpha \in \mathbb{R}$ und $x, y \in \mathcal{A}$.*

d) *Wenn eine Algebra ein Einselement besitzt, so ist dieses eindeutig bestimmt.*

e) *Die Eigenschaft "alternativ" ist eine Abschwächung der Assoziativität (ein besserer Name wäre wohl "halb–assoziativ"). Jede assoziative Algebra ist insbesondere alternativ.*

f) Verallgemeinerung: *An Stelle von $\mathbb{R}$ kann man allgemeiner auch einen beliebigen Körper K nehmen. Ein K–Vektorraum mit einer K–bilinearen Multiplikation heißt dann eine* **K–Algebra**.

9.3 Beispiele a) *$\mathbb{R}$ und $\mathbb{C}$ sind kommutative und assoziative reelle Algebren mit Einselement. Beide sind nullteilerfrei und besitzen die Dimension 1 bzw. 2.*

b) *$M_n(\mathbb{R})$ und $M_n(\mathbb{C})$ sind assoziative Algebren mit Einselement, die für $n \geq 2$ nicht kommutativ und nicht nullteilerfrei sind.* $\dim M_n(\mathbb{R}) = n^2$ *und* $\dim M_n(\mathbb{C}) = 2n^2$.

c) *Der Schiefkörper* $\mathbb{H} = \left\{ \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \;\middle|\; w, z \in \mathbb{C} \right\}$ *der Quaternionen ist eine 4–dimensionale, nullteilerfreie, assoziative und nichtkommutative $\mathbb{R}$–Algebra mit einem Einselement.*

d) *Es bezeichne $\times$ das* **äußere Produkt** *(oder Vektorprodukt) auf dem Anschauungsraum $\mathbb{R}^3$. Aus der Linearen Algebra I ist bekannt, daß das äußere Produkt $\mathbb{R}$–bilinear,*

nicht assoziativ und antikommutativ ist ($a \times b = -b \times a$). Daraus folgt $a \times a = 0$ für alle $a \in \mathbb{R}^3$. Folglich ist $\mathbb{R}^3$ eine nicht assoziative und nicht kommutative Algebra, die auch nicht nullteilerfrei ist.

e) *Es bezeichne $Sym_n(\mathbb{R}) \subseteq M_n(\mathbb{R})$ den Unterraum der symmetrischen Matrizen. Eine Multiplikation auf $Sym_n(\mathbb{R})$ sei definiert durch*

$$A \cdot B := \frac{1}{2}(AB + BA) \quad (A, B \in Sym_n(\mathbb{R}))$$

Man rechnet leicht nach, daß $Sym_n(\mathbb{R}))$ eine endlichdimensionale kommutative Algebra mit Einselement ist, die für $n \geq 2$ nicht assoziativ ist.

f) *Jeder reelle Vektorraum $V \neq 0$ läßt sich immer zu einer asoziativen und kommutativen Algebra mit Eins machen: Wähle zu einem festen Vektor $e \in V$ einen Unterraum $U \subseteq V$ mit $V = \mathbb{R}e \oplus U$. Zwei Elemente $x = \alpha e + u$, $x' = \alpha' e + u' \in V$ $(\alpha, \alpha' \in \mathbb{R}, u, u' \in U)$ werden dann nach der Vorschrift*

$$x \cdot x' := (\alpha\alpha')e + \alpha u' + \alpha' u$$

multipliziert. Diese Multiplikation hat die gewünschten Eigenschaften, insbesondere ist e das Einselement.

g) *Ein beliebiger $\mathbb{R}$–Vektorraum V wird durch die Multiplikation $x \cdot y := 0$ zu einer* **trivialen** *Algebra.*

h) *Der Polynomring $\mathbb{R}[T]$ ist ein unendlichdimensionaler $\mathbb{R}$–Vektorraum. Die Polynommultiplikation macht $\mathbb{R}[T]$ zu einer assoziativen, kommutativen und nullteilerfreien Algebra mit Einselement ($\mathbb{R}[T]$ ist Vektorraum und Integritätsbereich!).*

9.4 Definition *Ein Unterraum U einer $\mathbb{R}$–Algebra $\mathcal{A}$ heißt eine* **$\mathbb{R}$–Unteralgebra** *von $\mathcal{A}$, wenn gilt:*

$$x \cdot y \in U \quad \text{für alle } x, y \in U\,.$$

9.5 Beispiele a) $\left\{ \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$ *ist eine 2–dimensionale Unteralgebra von $M_2(\mathbb{R})$.*

b) *$\mathbb{H}$ ist eine 4–dimensionale Unteralgebra von $M_2(\mathbb{C})$.*

c) *Die Menge $\Delta_n(\mathbb{R})$ der oberen Dreiecksmatrizen ist eine $\frac{1}{2}n(n+1)$–dimensionale Unteralgebra von $M_n(\mathbb{R})$.*

d) *Die Menge $\Delta_n(\mathbb{C})$ der oberen Dreiecksmatrizen ist eine $n(n+1)$–dimensionale Unteralgebra von $M_n(\mathbb{C})$.*

9.6 Definition *$\mathcal{A}$ und $\mathcal{B}$ seien reelle Algebren. Eine Abbildung $f : \mathcal{A} \longrightarrow \mathcal{B}$ heißt ein* **$\mathbb{R}$–Algebrahomomorphismus**, *wenn gilt:*

i) *f ist $\mathbb{R}$–linear*

ii) $f(x \cdot y) = f(x) \cdot f(y)$ *für alle $x, y \in \mathcal{A}$.*

9.7 Beispiele $f : \mathbb{C} \longrightarrow M_2(\mathbb{R})$, $\alpha + i\beta \longmapsto \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$ *ist ein injektiver Algebrahomomorphismus, d.h. $\mathbb{C}$ ist algebra–isomorph zu einer Unteralgebra von $M_2(\mathbb{R})$.*

b) *Ist $\mathcal{A}$ eine Algebra mit Einselement e, so ist $f : \mathbb{R} \longrightarrow \mathcal{A}$, $\alpha \longmapsto \alpha e$ ein injektiver Algebrahomomorphismus.*

c) *Ist $\mathcal{A}$ eine eindimensionale Algebra mit Einselement, so folgt $\mathcal{A} \cong \mathbb{R}$.*

9.8 Satz *Jede eindimensionale reelle Algebra mit nichttrivialer Multiplikation besitzt ein Einselement und ist isomorph zu* $\mathbb{R}$.

Die Algebren $\mathbb{R}, \mathbb{C}$ und $\mathbb{H}$ besitzen alle ein Einselement und sind Schiefkörper, d.h. jedes Element $\neq 0$ besitzt ein multiplikatives Inverses. Wir wollen diese Eigenschaft von Algebren herausstellen, nehmen aber die Formulierung so vor, daß wir nicht die Existenz eines Einselementes voraussetzen müssen. Unter gewissen zusätzlichen Voraussetzungen folgt diese aber automatisch.

9.9 Definition *Eine reelle Algebra* $\mathcal{A} \neq 0$ *heißt* **reelle Divisionsalgebra**, *wenn für jedes* $a \in \mathcal{A} \setminus \{0\}$ *die Gleichungen*

$$ax = b \quad \textit{und} \quad ya = b$$

für alle $b \in \mathcal{A}$ *eindeutig in* $\mathcal{A}$ *lösbar sind.*

9.10 Beispiele a) $\mathbb{R}$ *und* $\mathbb{C}$ *sind Divisionsalgebren der Dimension 1 bzw. 2, die beide assoziativ, kommutativ und nullteilerfrei sind und die ein Einselement besitzen.*

b) $\mathbb{H}$ *ist eine 4–dimensionale Divisionsalgebra, die nicht kommutativ ist.*

c) $M_n(\mathbb{R})$ *und* $M_n(\mathbb{C})$ *sind für* $n > 1$ *keine Divisionsalgebren.*

d) *Der Quotientenkörper* $\mathbb{R}(T)$ *von* $\mathbb{R}[T]$ *ist eine unendlichdimensionale reelle Divisionsalgebra.*

e) *Jede Divisionsalgebra ist nullteilerfrei.*

9.11 Lemma *Jede alternative reelle Divisionsalgebra besitzt ein Einselement.*

9.12 Satz *Ist* $\mathcal{A}$ *eine assoziative reelle Divisionsalgebra, so ist* $(\mathcal{A} \setminus \{0\}, \cdot)$ *eine Gruppe und* $(\mathcal{A}, +, \cdot)$ *somit ein Schiefkörper.*

9.13 Bemerkung a) *Der Beweis von (9.12) läßt sich auch rein gruppentheoretisch ohne (9.11) beweisen. Es gilt nämlich der folgende Satz:*

Satz: *G sei eine nichtleere Menge mit einer assoziativen Verknüpfung* $\star$. *Genau dann ist* $(G, \star)$ *eine Gruppe, wenn gilt: Für beliebige* $a, b \in G$ *sind die Gleichungen* $a \star x = b$ *und* $y \star a = b$ *in G lösbar. (Beweis als Übungsaufgabe!)*

b) *Eine assoziative reelle Divisionsalgebra* $\mathcal{A}$ *ist ein Schiefkörper und enthält eine zu* $\mathbb{R}$ *isomorphe Unteralgebra.*

9.14 Satz *Für eine endlichdimensionale reelle Algebra* $\mathcal{A}$ *sind folgende Aussagen äquivalent:*

a) $\mathcal{A}$ *ist eine Divisionsalgebra*

b) $\mathcal{A}$ *ist nullteilerfrei.*

9.15 Satz *Jede endlichdimensionale reelle Divisionsalgebra* $\mathcal{A}$ *mit Einselement, deren Dimension eine* **ungerade** *Zahl ist, ist isomorph zu* $\mathbb{R}$.

Wir wollen uns jetzt kurz ein konstruktives Verfahren zur Bildung von reellen Algebren anschauen.

9.16 Bemerkung *Sei V ein n–dimensionaler $\mathbb{R}$–Vektorraum und $\{e_1, e_2, \ldots, e_n\}$ eine Basis von V. Eine Multiplikation ist eindeutig festgelegt, wenn man die n^2 Produkte*

$$e_\mu \cdot e_\nu \quad (\mu, \nu = 1, 2, \ldots, n)$$

vorgibt. Die $\mathbb{R}$–bilineare Multiplikation $V \times V \longrightarrow V$ ist dann durch die Vorschrift

$$x \cdot y := \sum_{\mu,\nu=1}^{n} (\alpha_\mu \alpha_\nu) e_\mu e_\nu \quad \text{für } x = \sum_{\mu=1}^{n} \alpha_\mu e_\mu \text{ und } y = \sum_{\nu=1}^{n} \alpha_\nu e_\nu$$

definiert. Um dabei etwa e_1 zum Einselement zu machen, muß man nur

$$e_1 e_\nu = e_\nu = e_\nu e_1 \quad (\text{für alle } \nu = 1, 2, \ldots, n)$$

setzen. Es gelten die beiden folgenden Sätze:

9.17 Satz *Die oben definierte Algebra ist genau dann assoziativ (kommutativ), wenn die Multiplikation der Basisvektoren assoziativ (kommutativ) ist.*

9.18 Satz *Ist W eine weitere reelle Algebra, so ist eine $\mathbb{R}$–lineare Abbildung $f : V \longrightarrow W$ genau dann ein Algebrahomomorphismus, wenn gilt:*

$$f(e_\mu e_\nu) \;=\; f(e_\mu) f(e_\nu) \quad (\text{für alle } \mu, \nu = 1, 2, \ldots, n)$$

9.19 Beispiel *Wir betrachten die kanonische Basis $\{e_1, e_2\}$ von $\mathbb{R}^2$, die aus den beiden Einheitsvektoren $e_1 := (1, 0)$ und $e_2 := (0, 1)$ besteht. Für die Basisvektoren legen wir die folgende Multiplikationstafel fest:*

	e_1	e_2
e_1	e_1	e_2
e_2	e_2	$-e_1$

Die dadurch definierte Multiplikation auf $\mathbb{R}^2$ ist nach den obigen Überlegungen assoziativ und kommutativ und besitzt e_1 als neutrales Element. Wir berechnen jetzt das Produkt $x \cdot y$ für $x = (\alpha_1, \alpha_2) = \alpha_1 e_1 + \alpha_2 e_2$ und $y = (\beta_1, \beta_2) = \beta_1 e_1 + \beta_2 e_2$ und benutzen dabei die obige Multiplikationstafel der Basisvektoren.

$$\begin{aligned} x \cdot y &= (\alpha_1 e_1 + \alpha_2 e_2)(\beta_1 e_1 + \beta_2 e_2) \\ &= \alpha_1\beta_1(e_1 e_1) + \alpha_1\beta_2(e_1 e_2) + \alpha_2\beta_1(e_2 e_1) + \alpha_2\beta_2(e_2 e_2) \\ &= \alpha_1\beta_1 e_1) + \alpha_1\beta_2 e_2 + \alpha_2\beta_1 e_2 - \alpha_2\beta_2 e_1 \\ &= (\alpha_1\beta_1 - \alpha_2\beta_2) e_1 + (\alpha_1\beta_2 + \alpha_2\beta_1) e_2 \\ &= (\alpha_1\beta_1 - \alpha_2\beta_2 \;,\; \alpha_1\beta_2 + \alpha_2\beta_1) \end{aligned}$$

Das Ergebnis entspricht genau der Multiplikation komplexer Zahlen, d.h. wir haben auf diesem Wege aus $\mathbb{R}^2$ den Körper der komplexen Zahlen gewonnen.

9.20 Beispiel **Die Quaternionenalgebra $\mathcal{H}$ bzw $\mathbb{H}$**

Sei $\{e_1, e_2, e_3, e_4\}$ die kanonische Basis von $\mathbb{R}^4$, die aus den Einheitsvektoren besteht.

Eine Multiplikation auf $\mathbb{R}^4$ *wird entsprechend (9.16) auf dieser Basis durch die folgende Tafel definiert:*

	e_1	e_2	e_3	e_4
e_1	e_1	e_2	e_3	e_4
e_2	e_2	$-e_1$	e_4	$-e_3$
e_3	e_3	$-e_4$	$-e_1$	e_2
e_4	e_4	e_3	$-e_2$	$-e_1$

Dadurch wird $\mathbb{R}^4$ *zu einer reellen Algebra, die wir mit* $\mathcal{H}$ *bezeichen (Hamilton'sche Algebra).*

Es sei $\mathbb{H}$ *der von den über* $\mathbb{R}$ *linear unabhängigen Matrizen* $E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $K := \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ *erzeugte reelle Unterraum von* $M_2(\mathbb{C})$*. Explizit ist* $\mathbb{H}$ *die folgende Menge:*

$$\begin{aligned} \mathbb{H} &= \{\alpha E + \beta I + \gamma J + \delta K \mid \alpha, \beta, \gamma, \delta \in \mathbb{R}\} \\ &= \left\{ \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \,\middle|\, w, z \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C}) \end{aligned}$$

Bezgl. der Matrizenaddition und –multiplikation ist $\mathbb{H}$ *ein nichtkommutativer Schiefkörper, und damit eine nichtkommutative, assoziative reelle Divisionsalgebra (Quaternionenalgebra aus (8.1)) . Die Matrizenprodukte von je zwei Matrizen der Basis* $\{E, I, J, K\}$ *sind in der folgenden Tafel zusammengefaßt:*

	E	I	J	K
E	E	I	J	K
I	I	$-E$	K	$-J$
J	J	$-K$	$-E$	I
K	K	J	$-I$	$-E$

Die durch lineare Fortsetzung definierte $\mathbb{R}$*–lineare Abbildung*

$$f : \mathcal{H} \longrightarrow \mathbb{H}$$

mit $e_1 \longmapsto E$, $e_2 \longmapsto I$, $e_3 \longmapsto J$, $e_4 \longmapsto K$ *ist ein* $\mathbb{R}$*–Algebraisomorphismus nach (9.16b), da sich die Basisvektoren aus der kanonischen Basis entsprechend multiplizieren wie die Matrizen der Basis* $\{E, I, J, K\}$ *. Dieser Isomorphismus ermöglicht es, in* $\mathbb{H}$ *gültige Rechenregeln nach* $\mathcal{H}$ *zu übertragen. Da z.B. die Matrizenmultiplikation auf* $\mathbb{H}$ *bekanntermaßen assoziativ ist, läßt sich sofort schließen, daß auch die Multiplikation auf* $\mathcal{H}$ *assoziativ ist. Dies erspart den recht langwierigen direkten Nachweis, daß die auf* $\mathcal{H}$ *definierte Multiplikation assoziativ ist.*

Es soll im folgenden auf zwei Punkte hingewiesen werden, die als Hilfsmittel für den Beweis des Satzes von Frobenius wichtig sind.

9.21 Bemerkung *Aus der Linearen Algebra ist bekannt, daß jede quadratische Matrix ihr charakteristisches Polynom erfüllt (Satz von Cayley–Hamilton). Ist also* $p_A \in \mathbb{C}[T]$ *das charakteristische Polynom einer Matrix* $A = \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \in \mathbb{H}$ *, so gilt* $p_A(A) = O$*. Für* p_A *gilt*

$$p_A \;=\; T^2 - spur(A)\,T + \det(A)$$

Nun ist $spur(A) = 2\Re(w) \in \mathbb{R}$ *und* $\det(A) = |w|^2 + |z|^2 \in \mathbb{R}$*, so daß sogar* $p_A \in \mathbb{R}[T]$ *richtig ist. Es folgt*

$$O \;=\; p_A(A) \;=\; A^2 - spur(A)\,A + \det(A)E$$

Damit gibt es zu jedem $A \in \mathbb{H}$ *Elemente* $\alpha, \beta \in \mathbb{R}$*, für die gilt* $A^2 - \alpha A - \beta E = O$*, oder*

$$A^2 = \alpha A + \beta E\ .$$

Eine solche Algebra wird später als **quadratisch** *bezeichnet, so daß wir sagen können:*

Satz: $\mathbb{H}$ *ist eine quadratische Algebra.*

9.22 Bemerkung $\mathbb{R}i$ *ist die Menge der rein–imaginären Elemente von* $\mathbb{C}$*, und es gilt*

$$\mathbb{C} = \mathbb{R}1 \oplus \mathbb{R}i\,.$$

Hier ist die Menge $Im\mathbb{C} := \mathbb{R}i$ *sogar ein Unterraum von* $\mathbb{C}$*, der sog.* **Imaginärraum von $\mathbb{C}$***.*

In der Quaternionenalgebra $\mathcal{H}$ *gilt*

$$\mathcal{H} \;=\; \mathbb{R}e_1 \oplus \underbrace{\mathbb{R}e_2 \oplus \mathbb{R}e_3 \oplus \mathbb{R}e_4}_{=:Im\mathcal{H}}$$

Hierbei heißt $Im\mathcal{H} = \mathbb{R}e_2 \oplus \mathbb{R}e_3 \oplus \mathbb{R}e_4$ *der* **Imaginärraum von $\mathcal{H}$***, dessen Elemente als* **rein–imaginär** *bezeichnet werden, also*

$$\mathcal{H} \;=\; \mathbb{R}e_1 \oplus Im\,\mathcal{H}$$

$Im\,\mathcal{H}$ *läßt sich auch basis–unabhängig definieren. Nach (8.1e) gilt für ein Element* $x = \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4 \in \mathcal{H}$

$$x^2 \;=\; 2\alpha x - (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)e_1\ .$$

Wegen $x \in Im\,\mathcal{H} \iff \alpha = 0$ *folgt* $x = 0$ *oder* $x \notin \mathbb{R}e_1$ *für ein Element* $x \in Im\,\mathcal{H}$ *und* $x^2 = (\beta^2 + \gamma^2 + \delta^2)e_1 \in \mathbb{R}e_1$*. Folglich*

$$Im\,\mathcal{H} \;=\; \{\, x \,|\, x \in Im\,\mathcal{H}\,,\, x \notin \mathbb{R}e_1 \setminus \{0\} \text{ und } x^2 \in \mathbb{R}e_1 \,\}$$

Jedes $x \in Im\,\mathcal{H}$ *läßt sich also eindeutig in der Form*

$$x \;=\; \alpha e_1 + u$$

darstellen, wobei αe_1 *der* **skalare Anteil** *oder der* **Realteil** *und* $u \in Im\,\mathcal{H}$ *der* **vektorielle Anteil** *oder der* **Imaginärteil** *von* x *ist.*

Es sei noch darauf hingewiesen, daß die Menge der rein–imaginären Elemente einer Algebra mit Eins i. a. **kein** *Unterraum zu sein braucht. Dies gilt jedoch, wenn $\mathcal{A}$ eine endlich–dimensionale alternative Divisionsalgebra ist, wie wir im 10. Vortrag sehen werden.*

9.23 Beispiel Die Oktavenalgebra $\mathbb{O}$ von Cayley *$\{e_1, e_2, \ldots, e_8\}$ sei die kanonische Basis von $\mathbb{R}^8$, die aus den Einheitsvektoren besteht. Eine Multiplikation auf $\mathbb{R}^8$ wird entsprechend (9.16) auf dieser Basis definiert:*

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8
e_1	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8
e_2	e_2	$-e_1$	e_4	$-e_3$	e_6	$-e_5$	$-e_8$	e_7
e_3	e_3	$-e_4$	$-e_1$	e_2	e_7	e_8	$-e_5$	$-e_6$
e_4	e_4	e_3	$-e_2$	$-e_1$	e_8	$-e_7$	e_6	$-e_5$
e_5	e_5	$-e_6$	$-e_7$	$-e_8$	$-e_1$	e_2	e_3	e_4
e_6	e_6	e_5	$-e_8$	e_7	$-e_2$	$-e_1$	$-e_4$	e_3
e_7	e_7	e_8	e_5	$-e_6$	$-e_3$	e_4	$-e_1$	$-e_2$
e_8	e_8	$-e_7$	e_6	e_5	$-e_4$	$-e_3$	e_2	$-e_1$

Dadurch wird $\mathbb{R}^8$ zu einer reellen Algebra, der sog. **Oktavenalgebra $\mathbb{O}$** *von Cayley. Dies ist eine endlichdimensionale, nicht assoziative, alternative, nichtkommutative Divisionsalgebra mit einem Einselement.*

Wir haben damit die wesentlichen Beispiele für reelle Divisionsalgebren zusammengestellt, wie die drei folgenden Eindeutigkeitssätze zeigen.

9.24 Satz Frobenius, 1877

Jede endlichdimensionale **assoziative** *reelle Divisionsalgebra ist zu $\mathbb{R}, \mathbb{C}$ oder $\mathbb{H}$ isomorph.*

9.25 Satz Zorn, 1933

Jede endlichdimensionale **alternative, nicht assoziative** *reelle Divisionsalgebra ist zu $\mathbb{O}$ isomorph.*

9.26 Satz Hopf, 1940

a) *Jede endlichdimensionale* **kommutative** *reelle Divisionsalgebra ist höchstens 2–dimensional.*

b) *Jede endlichdimensionale* **kommutative** *reelle Divisionsalgebra* **mit Einselement** *ist isomorph zu $\mathbb{R}$ oder $\mathbb{C}$.*

In diesem Seminar werden wir noch einen Beweis des Satzes von Frobenius kennenlernen (10. Vortrag), die Beweise der beiden anderen Sätze findet man ebenfalls in dem Buch von Ebbinghaus et al. Erstaunlicherweise werden bei dem Beweis des Satzes von Hopf topologische Methoden benötigt.

Einige historische Anmerkungen

Nachdem sich zu Beginn des 19. Jahrhunderts die komplexen Zahlen bei den Mathematikern durchgesetzt hatten, wurde versucht, $\mathbb{C}$ umfassende Systeme mit entsprechenden Recheneigenschaften ("hyperkomplexe Systeme") zu finden. Nach vergeblichen Versuchen kam man dahin, daß das "Permanenzprinzip" nicht mehr vollständig aufrechterhalten werden könnte, sondern daß man auf Eigenschaften wie Kommutativität oder Assoziativität der Multiplikation verzichten müßte . Gefunden wurden dann die nichtkommutativen Quaternionen von Hamilton und die nichtassoziativen Oktaven von Graves und Cayley. Erst viel später stellte sich dann heraus, daß es keine weiteren Strukturen dieser Art mehr geben kann (Sätze von Frobenius, Zorn und Hopf) .

1799	Fundamentalsatz der Algebra (Dissertation von Gauß)
1843	Einführung der Quaternionen duch Hamilton als Elemente des $\mathbb{R}^4$ mit einer speziellen Multiplikation
1843	Entdeckung der Oktaven durch John T. Graves, 1845 von Cayley wiedergefunden
1858	Einführung der Matrizen durch Cayley. Die Quaternionen werden dabei als spezielle (2×2)–Matrizen über $\mathbb{C}$ dargestellt
1877	Satz von Frobenius
1933	Satz von Zorn
1940	Satz von Hopf

Carl Friedrich Gauß	1777–1855
William Rowan Hamilton	1805–1865
Arthur Cayley	1821–1895
Ferdinand Georg Frobenius	1849–1917
Heinz Hopf	1894–1971
Max Zorn	1906–1993

10 Ein Satz von Frobenius

Ziel dieser Ausarbeitung soll sein, den 1877 aufgestellten Satz von Ferdinand Georg Frobenius zu beweisen, welcher Aufschluss darüber gibt, dass es weitaus weniger interessante reelle Algebren gibt, als Mathematikergenerationen, (unter anderem Hamilton) zuvor annahmen. Dieser Satz besagt, dass es bis auf Isomorphie nur drei reelle endlich-dimensionale, assoziative Divisonsalgebren gibt: $\mathbb{R}, \mathbb{C}$ und $\mathcal{H}$, die vierdimensionale Hamiltonsche Algebra der Quaternionen. Zuvor werden die Hilfsmittel erläutert, die zum Beweis des Satzes von Frobenius nötig sind. Zunächst werden zwei Definitionen angeführt, welche an die Inhalte der Vorträge 8 und 9 anknüpfen.

10.1 Definition *In einer Algebra $\mathcal{A}$ mit Einselement e nennt man drei Elemente u, v, w ein Hamiltonsches Tripel, wenn die neun Hamiltonschen Bedingungen erfüllt sind:*

$$u^2 = v^2 = w^2 = -e \quad , \quad w = uv = -vu \quad , \quad u = vw = -wv \quad , \quad v = wu = -uw.$$

10.2 Definition *Für jede Algebra $\mathcal{A}$ mit Einselement e ist*

$$Im\mathcal{A} := \{x \in \mathcal{A} \ : \ x^2 \in \mathbb{R}e \text{ und } x \notin \mathbb{R}e \setminus \{0\}\}$$

die Menge der rein-imaginären Elemente.

10.3 Bemerkung *a) Aus der Definition folgt $\mathbb{R}e \cap Im\mathcal{A} = 0$ und $u \in Im\mathcal{A} \Rightarrow \alpha u \in Im\mathcal{A}$ für jedes $\alpha \in \mathbb{R}$.*

b) Aus $u, v \in Im\mathcal{A}$ folgt nicht ohne weiteres $u + v \in Im\mathcal{A}$. Deswegen ist $Im\mathcal{A}$ im allgemeinen kein Untervektorraum von $\mathcal{A}$.

10.4 Lemma *(Unabhängigkeitslemma)*

a) Sind $u, v \in Im\mathcal{A}$ linear unabhängig, so sind auch e, u, v linear unabhängig.

b) Sind $u, v, u + v \in Im\mathcal{A}$, so folgt $uv + vu \in \mathbb{R}e$.

c) Ist $\mathcal{A}$ nullteilerfrei, so gibt es zu jedem $u \in Im\mathcal{A}$, $u \neq 0$ ein $\omega \in \mathbb{R}$, $\omega > 0$ mit $u^2 = -\omega e$.

Beweis: a) Im Folgenden soll ein Widerspruchsbeweis geführt werden. Man nehme an: e, u, v, linear abhängig. Wegen $u \in \mathrm{Im}\mathcal{A}$ lassen sich dann $\alpha, \beta \in \mathbb{R}$ finden mit:

$$v = \alpha e + \beta u$$

Des Weiteren gilt dann:

$$v^2 = (\alpha e + \beta u)^2 = \alpha e + \alpha e \beta u + \beta u \alpha e + \beta^2 u^2 = \alpha e + \alpha\beta e u + \alpha\beta u e + \beta^2 u^2$$

Weitere Umformungen ergeben:

$$2\alpha\beta u = v^2 - \alpha^2 e - \beta^2 u^2 \ \in \mathbb{R}e$$

Aus $v^2 - \alpha^2 e - \beta^2 u^2 \ \in \mathbb{R}e$ folgt $\alpha\beta = 0$, da u laut Definition ein Element aus der Menge der rein-imaginären Elemente ist. Daraus folgen die beiden Fälle $\alpha = 0$ und $\beta = 0$. Diese werden im Folgenden zu einem Widerspruch geführt: Aus $\alpha = 0$ folgt $v = \beta u$, im Widerspruch zur linearen Unabhängigkeit von v und u. Aus $\beta = 0$ folgt $v = \alpha e$, im Widerspruch dazu, dass $v \in \mathrm{Im}\mathcal{A}$ sein soll. Daraus folgt nun, dass u, v, e linear unabhängig sind.
b) Man forme $(u + v)^2 - u^2 - v^2 \ \in \mathbb{R}e$ um zu: $u^2 + uv + vu + v^2 - u^2 - v^2 = uv + vu$. Daraus folgt dann: $uv + vu \ \in \mathbb{R}e$.

c) Es ist lediglich zu beweisen, dass $\omega > 0$. Der Rest gilt laut vorangegangenen Definitionen. Im Folgenden soll ein Widerspruchsbeweis geführt werden.
Laut Definition gilt:

$$u^2 = \alpha e \quad \alpha \in \mathbb{R}$$

Man nehme an: $\alpha \geq 0$. Setze $\alpha = \beta^2, \quad \beta \in \mathbb{R}$. Dann ist $u^2 = \beta^2 e$, woraus folgt:

$$0 = u^2 - \beta^2 e = (u + \beta e)(u - \beta e)$$

Aus der Nullteilerfreiheit von $\mathcal{A}$ folgt: $(u + \beta e) = 0$ oder $(u - \beta e) = 0$.
Aus $u + \beta e = 0$ folgt jedoch $u = -\beta e \ \in \mathbb{R}e$ im Widerspruch dazu, dass laut Definition $u \in \mathrm{Im}\mathcal{A}$ gilt.
Aus $u - \beta e = 0$ folgt $u = \beta e \ \in \mathbb{R}e$, was aus eben genannten Gründen auch einen Widerspruch darstellt.
Daraus folgert man nun: $\alpha < 0$.

□

10.5 Bemerkung *Nach 9.4 c) kann man von jedem rein-imaginären Element $u' \neq 0$ durch skalare Multiplikation zu einem Element $u = \gamma u'$ mit $u^2 = -e$ übergehen.*

10.6 Satz *Ist u, v, w ein Hamiltonsches Tripel in $\mathcal{A}$, so gilt:*

a) *e, u, v, w sind linear unabhängig.*

b) *Die Abbildung $f : \mathcal{H} \ \to \mathcal{A}$, $(\alpha, \beta, \gamma, \delta) \ \mapsto \ \alpha e + \beta u + \gamma v + \delta w$ ist ein injektiver Algebra-Homomorphismus.*

c) *Es gilt $\mathbb{R}u + \mathbb{R}v + \mathbb{R}w \subset \mathrm{Im}\mathcal{A}$. Insbesondere enthält $\mathrm{Im}\mathcal{A}$ einen dreidimensionalen Untervektorraum.*

Beweis: a) Zunächst wird durch einen Widerspruchsbeweis gezeigt, dass u, v linear unabhängig sind.
Man nehme an, dass u, v linear abhängig sind. Dann ist $v \in \mathbb{R}u$ und $v = \alpha u$, $\alpha \in \mathbb{R}$. Daraus folgt:

$$vu = \alpha uu = \alpha(-e) = -\alpha e$$

und

$$uv = u\alpha u = \alpha(-e) = -\alpha e.$$

Also: $uv = vu$ woraus $-w = w$ folgt und somit auch $w = 0$, was im Widerspruch dazu steht, dass laut Hamiltonschen Bedingungen $w^2 = -e$ ist.
Demnach sind u, v linear unabhängig.
Aus (10.4.a) folgt nun: e, u, v sind linear unabhängig.
Nun ist noch zu zeigen, dass e, u, v, w linear unabhängig sind. Dazu nimmt man an, dass e, u, v, w linear abhängig sind. Dann gibt es eindeutig bestimmte Zahlen $\rho, \sigma, \tau \in \mathbb{R}$, so dass gilt:

$$w = uv = \rho e + \sigma u + \tau v$$

Linksmultiplikation mit u liefert: $u^2 v = \rho ue + \sigma u^2 + \tau uv$.

Unter Berücksichtigung von $u^2 = -e$ erhält man:

$$v = -\rho u + \sigma e - \tau w$$

Setzt man diese Gleichung in $w = uv = \rho e + \sigma u + \tau v$ ein, so erhält man für $\tau \neq 0$:

$$v = \frac{1}{\tau} w - \frac{\rho}{\tau} e - \frac{\sigma}{\tau} u$$

(Der Fall $\tau = 0$ muss nicht beachtet werden, da in diesem Fall gilt: $v = -\rho u + \sigma e$, was im Widerspruch dazu steht, dass v, u, e nach (10.4a) linear unabhängig sind.)
Führt man nun einen Koeffizientenvergleich für die Gleichungen $v = -\rho u + \sigma e - \tau w$ und $v = \frac{1}{\tau} w - \frac{\rho}{\tau} e - \frac{\sigma}{\tau} u$ durch, so erzwingt die Eindeutigkeit der Darstellung $-\tau = \frac{1}{\tau}$. Daraus folgt $\tau^2 = -1$. Da jedoch $\tau \notin \mathbb{R}$, hat man einen Widerspruch.
Daraus folgt: e, u, v, w sind linear unabhängig.
b) Nun ist zu zeigen, dass die Abbildung f ein injektiver Algebra-Homomorphismus ist.
Zunächst soll nachgewiesen werden, dass f ein Algebra-Homomorphismus ist:
Wegen:

$$f(e) = e, \quad f(i) = u, \quad f(j) = v, \quad f(k) = w$$

werden die Elemente der Basis $\{e, i, j, k\}$ von $\mathcal{H}$ auf Basiselemente aus $\mathcal{A}$ geschickt und f ist nach dem Satz über lineare Fortsetzung für alle Elemente definiert und $\mathbb{R}$-linear.
Die weiteren Eigenschaften für einen Algebra-Homomorphismus:

$$f(xy) = f(x)f(y) \quad \forall x, y \in \mathcal{A}$$

müssen laut (9.18) nur für die Basiselemente nachgewiesen werden.
Da $e, i, j, k \in \mathcal{H}$ denselben Verknüpfungsregeln entsprechen, wie $e, u, v, w \in \mathcal{A}$, ist dies klar. Somit ist f ein Algebra-Homomorphismus.
Die Injektivität von f ist äquivalent dazu, dass der Kern von f nur aus dem Nullelement von $\mathcal{H}$ besteht. $f(\alpha, \beta, \gamma, \delta)$ bildet genau dann auf das Nullelement von $\mathcal{H}$ ab, wenn $\alpha = \beta = \gamma = \delta = 0$. Dieser Fall tritt hier ein, da e, u, v, w linear unabhängig sind. Demnach ist f injektiv.
c) Zunächst ist zu zeigen: $\mathbb{R}u + \mathbb{R}v + \mathbb{R}w \subset \mathrm{Im}\mathcal{A}$. Dazu zeige man: $(\beta u + \gamma v + \delta w)^2 \in \mathbb{R}e$ mit $\beta, \gamma, \delta \in \mathbb{R}$:

$$\begin{aligned}(\beta u + \gamma v + \delta w)^2 &= \beta^2 u^2 + \beta\gamma uv + \beta\delta uw + \gamma^2 v^2 + \gamma\beta vu + \gamma\delta vw + \delta\beta wu + \delta\gamma wv + \delta^2 w^2 \\ &= -(\beta^2 + \gamma^2 + \delta^2)e \in \mathbb{R}e\end{aligned}$$

Nun ist noch zu zeigen, dass $\mathbb{R}u + \mathbb{R}v + \mathbb{R}w$ (im Folgenden als U bezeichnet) ein dreidimensionaler Untervektorraum von $\mathcal{A}$ ist. Dass der Unterraum nicht leer ist, da mindestens das Nullelement von $\mathcal{A}$ in ihm enthalten sein muss, ist klar. Es ist noch die Abgeschlossenheit bezüglich Addition und sklararer Multiplikation zu prüfen.
Dazu sei $x = (au + bv + cw) \quad a, b, c \in \mathbb{R}$ und $y = (du + fv + gw) \quad d, f, g \in \mathbb{R}$. Dann ist:

$$x + y = ((a + d)u + (b + f)v + (c + g)w) \in U$$

und somit die Abgeschlossenheit bezüglich der Addition gezeigt.
Sei nun $\alpha \in \mathbb{R}$ dann ist:

$$\alpha x = (\alpha a u + \alpha b v + \alpha c w) \in U$$

und somit auch die Abgeschlossenheit bezüglich skalarer Multiplikation gezeigt. Da $\{u, v, w\}$ eine Basis von U ist, ist $\dim(U)$=3.

□

10.7 Lemma *Sei U ein zweidimensionaler Untervektorraum von Im$\mathcal{A}$. Dann gibt es zu jedem $p \in U$ ein $q \in U \setminus \mathbb{R}p$, so dass gilt: $pq + qp = 0$.*

Beweis: Im Folgenden ist nur der Fall $p \neq 0$ zu betrachten. Der Fall $p = 0$ ist trivial, da $0q + q0 = 0$ für alle $q \in U$ gilt.
Sei also $p \neq 0$. Dann gilt $p^2 = \alpha e$ mit $\alpha \in \mathbb{R}$, $\alpha \neq 0$. Man wähle $x \in U$, so dass p und x linear unabhängig sind. Nach (10.4b) gilt dann:

$$px + xp = \beta e \quad \beta \in \mathbb{R}.$$

Durch Nachrechnen findet man heraus, dass $q := x + \xi p$ mit $\xi := -\beta(2\alpha)^{-1}$ die Gleichung erfüllt:

$$pq + qp = p(x - \frac{\beta}{2\alpha}p) + (x - \frac{\beta}{2\alpha}p)p = px - \frac{\beta}{2\alpha}p^2 + xp - \frac{\beta}{2\alpha}p^2 \overset{p^2=\alpha e}{=}$$

$$px - \frac{\beta}{2}e + xp - \frac{\beta}{2}e = px + xp - \beta e = \beta e - \beta e = 0$$

□

10.8 Satz *(Existenssatz für Hamiltonsche Tripel) Sei $\mathcal{A}$ eine assoziative, nullteilerfreie Algebra mit Einselement e und sei U ein zweidimensionaler Untervektorraum von Im$\mathcal{A}$. Dann gibt es zu jedem $u \in U$ mit $u^2 = -e$ ein $v \in U$, so dass u, v, uv ein Hamiltonsches Tripel bilden.*

Beweis: Nach (10.4) und (10.5) existiert ein $v \in U$ mit $v^2 = -e$. Nach (10.7) gibt es ein $u' \in U$ mit $u'v + vu' = 0$. Wähle $\gamma \in \mathbb{R}$ mit $u = \gamma u'$ und $u^2 = -e$. Dann ist auch $uv + vu = 0$.
Nun sind die Hamiltonschen Bedingungen für $u, v, w := uv$ zu zeigen:

$$1)\ vw = v(uv) = v(-vu) = eu = -u$$

$$2)\ wv = (uv)v = uv^2 = u(-e) = -u \quad \Rightarrow wv = -vw$$

$$3)\ wu = (uv)u = (-vu)u = -vu^2 = -v(-e) = v$$

$$-uw = -(u(uv)) = -(-ev) = v$$

$$\Rightarrow wu = -uw$$

Zudem gilt: $u^2 = v^2 = -e$. Nun ist also noch zu zeigen: $w^2 = -e$.
Es gilt: $-v = uw = (vw)w = vw^2$. Daraus folgt:

$$0 = vw^2 + v = vw^2 + ve = v(w^2 + e).$$

Da $\mathcal{A}$ nullteilerfrei ist, und $v \neq 0$ laut Definition, folgt aus dieser Gleichung: $w^2 = -e$. Damit sind alle Hamiltonschen Bedingungen gezeigt.

□

10.9 Definition *Eine Algebra $\mathcal{A}$ mit Einselement e heißt quadratisch, wenn jedes Element $x \in \mathcal{A}$ einer quadratischen Gleichung*

$$x^2 = \alpha e + \beta x$$

mit $\alpha, \beta \in \mathbb{R}$ genügt.

10.10 Lemma *(Lemma von Frobenius) Ist $\mathcal{A}$ eine quadratische Algebra, so ist Im$\mathcal{A}$ ein Untervektorraum von $\mathcal{A}$ und es gilt: $\mathcal{A} = \mathbb{R}e \bigoplus$ Im$\mathcal{A}$.*

Beweis: Hier ist zunächst zu zeigen, dass Im$\mathcal{A}$ ein Untervektorraum von $\mathcal{A}$ ist. Die erste nachzuprüfende Bedingung, dass der Untervektorraum U nicht leer ist, folgt direkt daraus, dass das Nullelement in Im$\mathcal{A}$ liegt, und somit auch in jedem Untervektorraum enthalten sein muss. Die Abgeschlossenheit bezüglich skalarer Multiplikation folgt auch direkt aus (10.3a). Es ist also nur noch die Abgeschlossenheit bezüglich der Addition nachzuprüfen.
Seien $u, v \in \text{Im}\mathcal{A}$ beliebig. Zu zeigen: $u+v \in \text{Im}\mathcal{A}$. Dazu werden zwei Fälle unterschieden:
1.Fall: u, v sind linear abhängig. Dann gilt: $v = \alpha u$, und es ist:

$$u + v = u + \alpha u = (1 + \alpha)u \ \in \text{Im}\mathcal{A}.$$

2.Fall: u, v sind linear unabhängig. Da $\mathcal{A}$ quadratisch ist, bestehen die Gleichungen:

$$(u + v)^2 = \alpha_1 e + \beta_1(u + v)\ ,\ (u - v)^2 = \alpha_2 e + \beta_2(u - v)\ \ (\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{R})$$

Addieren und Ausmultiplizieren liefert:

$$(u + v)^2 + (u - v)^2 = \alpha_1 e + \beta_1(u + v) + \alpha_2 e + \beta_2(u - v)$$

$$\Rightarrow 2u^2 + 2v^2 - (\alpha_1 + \alpha_2)e = (\beta_1 + \beta_2)u + (\beta_1 - \beta_2)v$$

$2u^2 + 2v^2 - (\alpha_1 + \alpha_2)e \ \in \mathbb{R}e$ lässt sich schreiben als τe mit $\tau \in \mathbb{R}$. Dann ist:

$$(\beta_1 + \beta_2)u + (\beta_1 + \beta_2)v - \tau e = 0.$$

Daraus folgt dann mit (10.4a) $\beta_1 + \beta_2 = \beta_1 - \beta_2 = \tau = 0$ und daraus auch $\beta_1 = \beta_2 = 0$. Weiter folgert man: $(u + v)^2 = \alpha_1 e \ \in \mathbb{R}e$.
Nun ist noch zu zeigen: $u + v \ \notin \mathbb{R}e$. Man führe dazu einen Widerspruchsbeweis durch: Annahme: $u + v \ \in \mathbb{R}e$ Daraus folgt: $u + v = \alpha e$ mit $\alpha \in \mathbb{R},\ \alpha \neq 0$. Also gilt auch: $u + v - \alpha e = 0$, was einen Widerspruch darstellt, da u, v, e linear unabhängig sind.
Insgesamt gilt: $u + v \in \text{Im}\mathcal{A}$.
Nun ist noch zu zeigen: $\mathcal{A} = \mathbb{R}e \bigoplus \text{Im}\mathcal{A}$.
$\mathbb{R}e \cap \text{Im}\mathcal{A} = \{0\}$ folgt direkt aus (10.3a). Es gilt also nur noch nachzuweisen:
$\mathcal{A} = \mathbb{R}e + \text{Im}\mathcal{A}$.
Zu zeigen ist also: Für jedes $x \in \mathcal{A}$ gilt: $x = \gamma e + v$ mit $\gamma \in \mathbb{R},\ v \in \text{Im}\mathcal{A}$. Hierzu werden zwei Fälle unterschieden:
1.Fall: Sei $x \in \mathbb{R}e \subseteq \mathcal{A}$. Dann gilt $x = \gamma e + 0$ mit $0 \in \text{Im}\mathcal{A}$.
2.Fall: Sei $x \in \mathcal{A},\ x \notin \mathbb{R}e$ beliebig. Es gilt $x^2 = \alpha e + 2\beta x$ mit $\alpha, \beta \in \mathbb{R}$, da $\mathcal{A}$ quadratisch ist. Man erhält:

$$(x - \beta e)^2 = x^2 - 2\beta x + \beta^2 e = \alpha e + 2\beta x - 2\beta x + \beta^2 e = \alpha e + \beta^2 e = (\alpha + \beta^2)e$$

Nun ist noch zu zeigen: $x - \beta e \notin \mathbb{R}e$, was im folgenden durch Widerspruch bewiesen wird.
Annahme: $x - \beta e \in \mathbb{R}e$, dann gilt: $x - \beta e = \tau e$ mit $\beta, \tau \in \mathbb{R}$. Dann gilt auch $x = (\tau + \beta)e$ und somit wäre $x \in \mathbb{R}e$ was ein Widerspruch ist, da laut Definition: $x \notin \mathbb{R}$.
Da $x - \beta e \notin \mathbb{R}e$ gilt $u := x - \beta e \in \mathrm{Im}\mathcal{A}$. Daraus folgt $x = \beta e + u$ und daraus $\mathcal{A} = \mathbb{R}e + \mathrm{Im}\mathcal{A}$.
□

10.11 Satz *Sei $\mathcal{A}$ eine assoziative Algebra mit Einselement e. Dann ist für jedes Element $x \in \mathcal{A}$ die Abbildung*

$$E_x : \mathbb{R}[T] \to \mathcal{A} \quad , \quad f \mapsto f(x)$$

ein Algebra-Homomorphismus (Einsetzungshomomorphismus).

Beweis: Dieser Beweis wird in der Algebravorlesung unter (3.10) geführt.
□

10.12 Satz *Jede endlich-dimensionale, assoziative Divisionsalgebra $\mathcal{A}$ ist quadratisch.*

Beweis: Da die Algebra $\mathcal{A}$ assoziativ ist, und nach Satz (9.11) des Vortrages über endlichdimensionale relle Algebren ein Einselement besitzt, ist E_x für jedes $x \in \mathcal{A}$ definiert. Da $\mathbb{R}$ ein Körper ist, ist $\mathbb{R}[T]$ ein Hauptidealbereich. Daher ist $\mathrm{Ker}(\mathrm{E}_x)$ ein Hauptideal von $\mathbb{R}[T]$.
Im Folgenden soll durch Widerspruch bewiesen werden: Aus $\dim \mathcal{A} < \infty$ folgt $\mathrm{Ker}(\mathrm{E}_x) \neq 0$.
Annahme: $\mathrm{Ker}(\mathrm{E}_x) = 0$. Dann ist

$$\mathrm{E}_x : \mathbb{R}(T) \to \mathcal{A}, f \mapsto f(x).$$

eine injektive $\mathbb{R}$-lineare Abbildung und $\mathbb{R}[T] \cong \mathrm{Bild}(\mathrm{E}_x)$ ist ein unendlichdimensionaler Unterraum von $\mathcal{A}$, was wegen $\dim\mathcal{A} < \infty$ nicht möglich ist. Aus diesem Widerspruch folgt dann $\mathrm{Ker}(\mathrm{E}_x) \neq 0$ und daraus $\mathrm{Ker}(\mathrm{E}_x) = (p)$ für ein $p \in \mathbb{R}(T),\ p \neq 0$.
Nach dem Ringhomomorphiesatz gilt:

$$\mathbb{R}[T]/\mathrm{Ker}(\mathrm{E}_x) = \mathbb{R}[T]/(p) \cong \mathrm{Bild}(\mathrm{E}_x) \subseteq \mathcal{A}$$

Da $\mathcal{A}$ nullteilerfrei ist, ist auch jeder Unterring von $\mathcal{A}$ nullteilerfrei, also auch $\mathrm{Bild}(\mathrm{E}_x)$, und daraus folgt dann die Nullteilerfreiheit des Faktorrings $\mathbb{R}[T]/(p)$. Aus der Nullteilerfreiheit des Faktorrings folgt wiederum die Irreduzibilität von p über $\mathbb{R}$, was im Folgenden durch Widerspruch bewiesen wird:
Annahme: p ist nicht irreduzibel. Dann gilt: $p = p_1 \cdot p_2$ mit $p_1, p_2 \in \mathbb{R}[T]$,
$0 < \mathrm{grad}(p_i) < \mathrm{grad}(p)$. Daraus folgt:

$$[p_1]_{(p)} \cdot [p_2]_{(p)} = [p]_{(p)} = [0]_{(p)} \text{ mit } [p_1]_{(p)} \neq [0]_{(p)} \text{ und } [p_2]_{(p)} \neq [0]_{(p)}$$

Demnach wäre der Faktorring nicht nullteilerfrei. Aus diesem Widerspruch folgt die Irreduzibilität von p über $\mathbb{R}$.
Über $\mathbb{R}$ kann ein irreduzibles Polynom nur den Grad 1 oder 2 haben.
<u>1.Fall:</u> $p = T^2 - \beta T - \alpha \in \mathrm{Ker}(E_x) \quad (\alpha, \beta \in \mathbb{R})$. Es gilt also $p(x) = 0$. Eingesetzt ergibt dies:

$$0 = x^2 - \beta x - \alpha e,$$

$$\Rightarrow x^2 = \beta x + \alpha e$$

2.Fall: $p = T + \gamma,\ \gamma \in \mathbb{R}$. $0 = p(x) = x + \gamma e$

$$\Rightarrow x = -\gamma e$$

$$\Rightarrow x^2 = \gamma^2 e = \gamma^2 e + 0x$$

Somit genügt jedes Element $x \in \mathcal{A}$ einer quadratischen Gleichung.

□

10.13 Lemma *(Quaternionenlemma) Jede endlich-dimensionale, assoziative reelle Divisionsalgebra $\mathcal{A}$ enthält im Falle $\dim(\mathcal{A}) \geq 3$ Hamiltonsche Tripel und eineUteralgebra $\mathcal{B}$ mit $e \in \mathcal{B}$, die zur Hamiltonschen Algebra $\mathcal{H}$ isomorph ist. Insbesondere gilt $\dim(\mathcal{A}) \geq 4$.*

Beweis: Zunächst ist die Existenz Hamiltonscher Tripel in $\mathcal{A}$ nachzuweisen.
Nach Satz (10.12) ist die Algebra $\mathcal{A}$ quadratisch. Nach Lemma (10.10) folgt daher: Im$\mathcal{A}$ ist ein Untervektorraum von $\mathcal{A}$ und es gilt $\dim(\text{Im}\mathcal{A}) \geq 2$ wegen $\dim(\mathcal{A}) \geq 3$.
Nach dem Existenzsatz (10.8) gibt es also Hamiltonsche Tripel in $\mathcal{A}$.
Nun ist noch die Existenz von Unteralgebren $\mathcal{B}$ in $\mathcal{A}$ mit $\mathcal{B} \cong \mathcal{H}$ nachzuweisen. Es wurde bereits die Existenz Hamiltonscher Tripel in $\mathcal{A}$ nachgewiesen. Nach Satz (10.6) gibt es einen injektiven Algebrahomomorphismus $f : \mathcal{H} \mapsto \mathcal{A}$. Folglich ist $\mathcal{B}$:=Bild(f) eine Unteralgebra von $\mathcal{A}$, die zu $\mathcal{H}$ isomorph ist. Natürlich gilt $e \in \mathcal{B}$.

□

10.14 Satz *(Frobenius, 1877) Sei $\mathcal{A}$ eine endlich-dimensionale, assoziative reelle Divisionsalgebra. Dann ist $\mathcal{A}$ entweder zu $\mathbb{R}$, $\mathbb{C}$ oder $\mathcal{H}$ isomorph.*

Beweis: Im Folgenden werden 3 mögliche Fälle unterschieden:
1.Fall: $\dim(\mathcal{A}) = 1$.
Nach Beispiel (9.7.c) des Vortrages über endlichdimensionale reelle Algebren gilt: Ist $\mathcal{A}$ eine eindimensionale Algebra mit Einselement, so folgt: $\mathcal{A} \cong \mathbb{R}$.
2.Fall: $\dim(\mathcal{A}) = 2$.
Nach Unabhängigkeitslemma (10.4) und Lemma von Frobenius (10.10) existiert ein $u \in \mathcal{A}$ mit $u^2 = -e$.
Im Folgenden soll gezeigt werden, dass die Abbildung

$$f : \mathbb{C} \to \mathcal{A} \quad 1 \mapsto e, i \mapsto u$$

ein Algebra-Isomorphismus ist. Da die Elemente der Basis$\{1, i\}$ von $\mathbb{C}$ auf Basiselemente aus $\mathcal{A}$ geschickt werden, ist f nach dem Satz über lineare Fortsetzung für alle Elemente definiert und somit ist f auch $\mathbb{R}$-linear. Da die Multiplikation auf $\mathbb{C}$ der Multiplikation auf $\mathcal{A}$ entspricht, ist f ein Algebrahomomorphismus. Die Bijektivität von f folgt aus $\dim(\mathbb{C})$ =$\dim(\mathcal{A})$, und somit gilt: $\mathcal{A} \cong \mathbb{C}$.

3.Fall: $\dim(\mathcal{A}) \geq 3$.
Nach dem Quaternionenlemma (10.13) existiert ein Hamiltonsches Tripel $u, v, w \in \mathrm{Im}\mathcal{A}$ mit $w = uv$.
Im Folgenden wird ein Beweis durch Widerspruch geführt.
Annahme: $\dim(\mathcal{A}) > 4$. Nach (10.6.c) enthält $\mathrm{Im}\mathcal{A}$ einen dreidimensionalen Untervektorraum, mit der Basis $\{u, v, w\}$. Nach dem Basisergänzungssatz existiert ein $x \in \mathrm{Im}\mathcal{A}$, so dass $\{u, v, w, x, \}$ linear unabhängig sind, da $\dim(\mathrm{Im}\mathcal{A}) > 3$. Nach Anwendung von Lemma (10.7) auf $U := \mathbb{R}u + \mathbb{R}x \subset \mathrm{Im}\mathcal{A}$ existiert ein $y \in U \backslash \mathbb{R}u$ mit $uy + yu = 0$ und $y = \rho u + \tau x \quad \tau, \rho \in \mathbb{R}, \tau \neq 0$.
Hieraus folgt: u, v, w, y sind linear unabhängig.
Wegen $v, w, y \in \mathrm{Im}\mathcal{A}$, gilt laut (10.4b) und (10.10): $v + y,\ w + y \in \mathrm{Im}\mathcal{A}$ und:

$$vy + yv = \alpha e \text{ und } wy + yw = \beta e \quad \alpha, \beta \in \mathbb{R}.$$

Da $\mathcal{A}$ assoziativ ist, folgt:

$$yw = y(uv) = (yu)v = -(uy)v = -u(yv) = -u(\alpha e - vy) = -\alpha u + wy = -\alpha u + \beta e - yw$$

$$\Rightarrow 2yw = -\alpha u + \beta e$$

Rechtsmultiplikation mit w ergibt:

$$2yw^2 = -\alpha uw + \beta w$$

$$\Rightarrow -2y = \alpha v + \beta w$$

Dies ist ein Widerspruch dazu, dass u, v, w, y linear unabhängig sind.
Daraus folgt: $\dim(\mathcal{A}) \leq 4$.
Aus dem Quaternionenlemma (10.13) folgt nun: $\dim(\mathcal{A}) = 4$. Da jede endlich-dimensionale, assoziative reelle Divisionsalgebra $\mathcal{A}$ mit $\dim(\mathcal{A}) \leq 3$ eine Unteralgebra $\mathcal{B}$ hat, die zu $\mathcal{H}$ isomorph ist, gilt in diesem Fall: $\mathcal{A} = \mathcal{B}$ und somit $\mathcal{A} \cong \mathcal{H}$.

□

11 Die Auflösbarkeit der symmetrischen Gruppen

Aus der Vorlesung Algebra (SS 03) wissen wir, daß ein Polynom $f \in \mathbb{Q}[T]$ genau dann durch Radikale auflösbar ist, wenn dessen Galoisgruppe auflösbar ist ($Satz 10.13$). Darum ist die Auflösbarkeit von Gruppen ein wichtiger und interessanter Begriff in der Algebra.

11.1 Definition *Sei G eine Gruppe und e ihr neutrales Element.*

1) *Ein $(n+1)$-Tupel $(G_0, G_1, ..., G_n)$ von Untergruppen von G heißt Normalreihe (der Länge n) in G, wenn gilt:*

   i) $G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_n = \{e\}$

   ii) *Für jedes $i \in \{0, ..., n-1\}$ ist G_{i+1} ein Normalteiler in G_i*

2) *Ist $(G_0, G_1, ..., G_n)$ eine Normalreihe in G, so heißen die Gruppen $G_i/G_{i+1}, i \in \{0, ..., n-1\}$ die Faktoren von $(G_0, G_1, ..., G_n)$*

11.2 Definition *Eine Gruppe G heißt auflösbar, wenn es in G eine Normalreihe mit abelschen Faktoren gibt.*

11.3 Beispiel

1) *Jede abelsche Gruppe ist auflösbar, aber nicht umgekehrt. $(G, \{e\})$ ist eine Normalreihe mit abelschen Faktoren.*

2) *S_3 ist auflösbar: $S_3 \supset A_3 \supset \{id\}$.*

3) *Die Diedergruppe D_n ist für $n \geq 2$ auflösbar. Dies ist die Gruppe der Drehungen und Spiegelungen eines regelmäßigen n-Ecks. Sei U_n die Menge aller Drehungen. Dann gilt $U_n \trianglelefteq D_n$ und D_n/U_n ist abelsch, weil gilt:*
   $[D_n : U_n] = 2, \forall\ n \geq 2$

Um eine Normalreihe in einer Gruppe zu konstruieren, gibt es das Verfahren der Kommutatorgruppenbildung. Dazu folgende Definitionen:

11.4 Definition *Sei G eine Gruppe. Für $a, b \in G$ wird das Produkt $[a, b] := aba^{-1}b^{-1}$ als Kommutator von a und b bezeichnet. Die von allen Kommutotoren erzeugte Untergruppe $K(G)$ von G heißt Kommutatorgruppe von G, $K(G) := \langle\{[a, b]/a, b \in G\}\rangle$.*

11.5 Bemerkung *G abelsch $\Leftrightarrow K(G) = \{e\}$.*

Beweis:
" $\Rightarrow$ " $K(G) = \langle\{[a, b]/a, b \in G\}\rangle = \langle\{aba^{-1}b^{-1}\}\rangle = \langle\{aa^{-1}bb^{-1}\}\rangle$, da G abelsch ist, also gilt: $K(G) = \{e\}$
" $\Leftarrow$ " $K(G) = \{e\}$, das heißt: $aba^{-1}b^{-1} = e\ \forall a, b \in G \Leftrightarrow ab = eba \Leftrightarrow G$ abelsch.

□

11.6 Satz

1) $K(G)$ ist Normalteiler in G ($K(G) \trianglelefteq G$).

2) G/N abelsch $\Leftrightarrow K(G) \subset N$

Beweis:
1) Zu zeigen: $K(G) \trianglelefteq G$

i) $K(G) \leq G$ nach Definition

ii) Zu zeigen: $aka^{-1} \in K(G)\ \forall a \in G, k \in K(G)$.
Sei $a \in G, k \in K(G)$ gegeben. Dann existieren $n \in \mathbb{N}$ und $x_1, ..., x_n, y_1, ..., y_n \in G$, mit $k = [x_1, y_1] * [x_2, y_2] * ... * [x_n, y_n]$, und es gilt:
$aka^{-1} = a([x_1, y_1] * [x_2, y_2] * ... * [x_n, y_n])a^{-1}$. Auf der rechten Seite kann man zwischen den Kommutatoren $a^{-1}a = e$ ergänzen und man erhält:
$a[x_1, y_1]a^{-1}a[x_2, y_2]a^{-1}...a[x_n, y_n]a^{-1}$. Jetzt innerhalb der Kommutatoren mit $a^{-1}a$ ergänzen
$(a(x_1y_1x_1^{-1}y_1^{-1})a^{-1} = ax_1a^{-1}ay_1a^{-1}ax_1^{-1}a^{-1}ay_1^{-1}a^{-1})$ und man kommt zu dem Ergebnis: $aka^{-1} = \underbrace{[ax_1a^{-1}, ay_1a^{-1}] * ... * [ax_na^{-1}, ay_na^{-1}]}_{\in K(G)}$,

da das Produkt aus Kommutatoren in $K(G)$ liegt.

2)" $\Rightarrow$ " Sei $\nu : G \to G/N$ der natürliche Gruppenhomomorphismus mit $a \mapsto aN$. Dann gilt: $\nu([a, b]) = \nu(aba^{-1}b^{-1}) = \nu(a)\nu(b)\nu(a^{-1})\nu(b^{-1}) = \nu(a)\nu(b)\nu(a)^{-1}\nu(b)^{-1} = \nu(a)\nu(a)^{-1}\nu(b)\nu(b)^{-1}$, da G/N abelsch ist. Daraus folgt: $\nu([a, b]) = \nu(e) = N\ \forall a, b \in G$, also gilt $[a, b] \in \ker(\nu) = N$ und damit ist $K(G) \subseteq N$

" $\Leftarrow$ " $K(G) \subseteq N \Rightarrow \forall a, b \in G$:
$(aN)(bN) = (ab)N = (ab[b^{-1}, a^{-1}])N = (abb^{-1}a^{-1}ba)N = (ba)N = (bN)(aN)$. Das heißt, die Faktorgruppe G/N ist abelsch.

□

11.7 Beispiel *1) $K(S_n) = A_n\ \forall n \geq 2$*
" $\subseteq$ " Aus $|S_n/A_n| = 2\ \forall n \geq 2$ folgt, daß die Faktorgruppe S_n/A_n immer zyklisch und insbesondere abelsch ist. Dann folgt nach 11.6.2, daß $K(S_n) \subseteq A_n$ gilt.
" $\supseteq$ " Da jedes Element aus A_n mit $n \geq 3$ ein endliches Produkt von Dreierzykeln aus S_n ist, macht man eine Fallunterscheidung und zeigt die Behauptung erst für $n = 2$ und dann für $n \geq 3$ allgemein.

i) $n = 2$: S_2 besteht aus zwei Elementen: $\{e, a\}$, mit $a = a^{-1}$. Somit wird die Kommutatorgruppe von S_2 von dem neutralen Element erzeugt und es gilt: $K(S_2) = \{e\} = A_2$

ii) $n \geq 3$*: Es gilt für alle paarweise verschiedenen* $i, j, k \in \{1, 2, ..., n\}$ *:*
$(i, j, k) = (i, k, j)^2 = (i, k, j)(i, k, j) = (i, k)(k, j)(i, k)(k, j)$*, da jede Permutation* $\pi \in S_n$ *darstellbar ist als Hintereinanderausführung von Transpositionen. Jede Transposition ist gleich ihrem Inversen, darum gilt:* $(i, k)(k, j)(i, k)(k, j) = (i, k)(k, j)(i, k)^{-1}(k, j)^{-1} = [(i, k), (k, j)]$*. Damit liegen alle Dreierzykeln in* $K(S_n)$ *und es gilt:* $A_n \subseteq K(S_n)$

2) $K(A_n) = A_n \ \forall n \geq 5$
Seien nun $i, j, k, l, m \in \{1, ..., n\}$ *paarweise verschieden, dann gilt:*
$(i, j, k) = (i, k)(k, j)(i, k)(k, j) = (i, k)(l, m)(k, j)(l, m)(i, k)(l, m)(k, j)(l, m) =: \star$*, da jede Transposition gleich ihrem Inversen ist und disjunkte Zykeln vertauschbar sind. Weiter gilt:* $\star = [(i, k)(l, m), (l, m)(k, j)] \in K(A_n)$
$\Rightarrow A_n \subseteq K(A_n)$ *und da trivialerweise auch* $K(A_n) \subseteq A_n$ *gilt, ist* $K(A_n) = A_n$

11.8 Definition *Sei* $n \in \mathbb{N}$*. Die n-te Ableitung* $K^n(G)$ *einer Gruppe G ist rekursiv definiert durch*
$K^0(G) := G$ *und* $K^n(G) := K(K^{n-1}(G))$ *für* $n \geq 1$
(Bezeichnung $K^n(G) =: G^{(n)}$*)*

11.9 Bemerkung *Mit diesem Verfahren erhält man eine absteigende Kette von Untergruppen von G:* $K^0(G) = G \supset K^1(G) \supset K^2(G) \supset ... \supset K^n(G)$*. Wegen (11.6) ist* $K^{i+1}(G) \trianglelefteq K^i$ *und die Gruppe* $K^i(G)/K^{i+1}(G)$ *ist abelsch für alle* $i \leq n, n \in \mathbb{N}$*.*

11.10 Satz *Für eine Gruppe G sind folgende Aussagen äquivalent:*

1) G ist auflösbar

2) Es gibt ein $n \in \mathbb{N}$ *mit* $K^n(G) = \{e\}$*.*

Beweis:
1) $\Rightarrow$ 2) Sei G auflösbar, das heißt es existert eine Normalreihe mit abelschen Faktoren: $G = G_0 \supset G_1 \supset ... \supset G_n = \{e\}$ mit $G_{i+1} \trianglelefteq G_i$ und G_i/G_{i+1} ist abelsch. Es genügt also zu zeigen: $K^m(G) \subseteq G_m \forall m \in \mathbb{N}$ durch vollständige Induktion.
Ind.-Anfang: $m = 0$ $K^0(G) = G \subseteq G = G_0$ ist trivial
Ind.-Voraussetzung: Es gelte für $m \in \mathbb{N}$: $K^m(G) \subseteq G_m$
Ind.-Schritt: $m \to m + 1$ Da G_m/G_{m+1} abelsch ist, folgt nach 11.6:
$K(G_m) \subseteq G_{m+1}$ und nach Ind.-Voraussetzung gilt $K^m(G) \subseteq G_m \Rightarrow K^{m+1}(G) = K(K^m(G)) \subseteq K(G_m) \subseteq G_{m+1}$. Folglich ist $K^n(G) \subseteq G_n = \{e\}$.
2) $\Rightarrow$ 1) $K^0(G) = G_0 \supseteq K^1(G) \supseteq ... \supseteq K^n(G) = \{e\}$ ist nach 11.9 eine Normalreihe mit abelschen Faktoren in G und damit ist G auflösbar.

□

11.11 Satz *Die symmetrischen Gruppen* S_n $(n \in \mathbb{N})$ *sind für* $n \leq 4$ *auflösbar und für* $n \geq 5$ *nicht auflösbar.*

Beweis: I) S_1 und S_2 sind zyklisch, also insbesondere abelsch und damit nach 11.3.1 auflösbar. S_3 ist ebenfalls nach 11.3 auflösbar. Sei nun $n = 4$: $S_4 \supseteq A_4 \supseteq V \supseteq \{id\}$ ist eine Normalreihe in S_4 (V ist hier die Kleinsche Vierergruppe). Es bleibt also zu zeigen, daß die Faktoren abelsch sind, um daraus die Auflösbarkeit von S_4 zu folgern.
1.Faktor: $|S_4/A_4| = 2 \Rightarrow S_4/A_4$ ist zyklisch $\Rightarrow$ abelsch
2.Faktor: $|A_4/V| = 3 \Rightarrow A_4/V$ ist zyklisch $\Rightarrow$ abelsch
3.Faktor: $|V/\{id\}| = 4 \Rightarrow V/\{id\}$ abelsch.

II) Sei $n \geq 5$. Nach 11.7 ist $K(S_n) = A_n$ aber $K^t(A_n) = A_n \ \forall\ t \geq 2$. Das heißt, alle Kommutatorgruppen von S_n sind von der trivialen Gruppe $\{id\}$ verschieden und daraus folgt: S_n ist für $n \geq 5$ nicht auflösbar.

□ Der folgende Satz ist von großer Bedeutung, weil dieser eine wesentliche Rolle im

Beweis von *Satz*10.13 (Algebra Vorlesung) spielt.

11.12 Satz *Eine endliche Gruppe G ist genau dann auflösbar, wenn es in G eine Normalreihe mit zyklischen Faktoren gibt.*

Beweis: " $\Leftarrow$ " Es existiert in G eine Normalreihe mit zyklischen Faktoren. Diese sind insbesondere abelsch und damit ist G auflösbar.

" $\Rightarrow$ " Sei G auflösbar. $\Rightarrow$ es existiert eine Normalreihe $G_0, ..., G_i, G_{i+1}, ...G_n$ mit $G_{i+1} \trianglelefteq G_i$, G_i/G_{i+1} ist abelsch und $G_n = \{e\}$.
Sei $U := G_i$, $V := G_{i+1}$ und $\nu : U \to U/V$ der natürliche Homomorphismus.
Sei $a \in U/V$ vom neutralen Element verschieden, dann ist $< a >$ die von a erzeugte zyklische Untergruppe von U/V. Da U/V abelsch ist und jede Untergruppe einer abelschen Gruppe auch Normalteiler ist, gilt: $< a > \trianglelefteq U/V$.
Definiere $\nu^{-1}(< a >) =: N$, dann gilt: $N \trianglelefteq U$, weil das Urbild eines Normalteilers wieder ein Normalteiler ist. Betrachte folgende Einschränkung von ν:
$\nu' : N \to < a >$ mit $\nu'(x) = xV \ \forall x \in N$.
Dann gilt: $ker(\nu') = N \cap ker(\nu) = N \cap V$. Außerdem gilt: $V = \ker(\nu) = \nu^{-1}(\{e\}) \subset \nu^{-1}(< a >) = N$.
Das bedeutet, V ist eine echte Teilmenge von N und es gilt: $\ker(\nu') = N \cap V = V$. Nun existiert nach dem Homomorphiesatz für Gruppen der durch ν' induzierte Gruppenhomomorphismus $f : N/\ker(\nu') \to < a >$. f ist injektiv.
Falls ν' surjektiv ist, gilt zusätzlich: $N/V \cong < a >$.

Also ist noch zu zeigen, daß es zu einem beliebigen $y \in < a >$ ein $z \in N$ existiert, für das gilt: $\nu'(z) = y$.
Sei $y = zV \in < a >$ und $\nu(z) = zV \in < a >$
$\Rightarrow z \in \nu^{-1}(< a >) = N \Rightarrow z \in N \Rightarrow \nu'(z) = zV = y$.

Bis zu diesem Punkt kann man zusammenfassen, daß man ein N gefunden hat, für welches gilt: $V \trianglelefteq N \trianglelefteq U$ mit zyklischem Faktor N/V.
Das heißt, die Normalreihe wurde zwischen zwei beliebigen Elementen U und V erweitert, durch ein Element N, sodaß der Faktor N/V zyklisch ist. Da das Ziel aber eine Normalreihe ist, in der jeder Faktor zyklisch ist, benutzt man hier den zweiten Isomorphiesatz: $U/N \cong (U/V)/(N/V)$.
Da U/V abelsch ist, ist U/N auch abelsch, und man kann die gesamte Konstruktion mit N statt V wiederholen. G ist nach Voraussetzung endlich, so daß dieses Verfahren

abbricht. Man erhält also Untergruppen $N_1, .., N_r$ von G mit

$$V \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_r \trianglelefteq U$$

und zyklischen Faktoren $N_1/V, N_2/N_1, ..., U/N_r$. Daraus folgt, daß in jeder endlichen Gruppe G eine Normalreihe mit zyklischen Faktoren existiert.

□

11.13 Beispiel *Die symmetrische Gruppe S_4 ist endlich und nach Satz 11.11 auflösbar. Wie man im Beweis sehen konnte, existiert folgende Normalreihe:*
$S_4 \supseteq A_4 \supseteq V \supseteq \{id\}$ mit zwei zyklischen Faktoren: $S_4/A_4, A_4/V$ und einem abelschen Faktor $V/\{id\}$. V ist die kleinsche Vierergruppe und besteht aus drei Elementen der Ordnung zwei und dem neutralen Element: $\{id\}$.
Sei $a \in V$ mit $a \neq \{id\}$, dann kann man die Normalreihe mit der von a erzeugten Untergruppe $< a >$ erweitern:

$$S_4 \supseteq A_4 \supseteq V \supseteq < a > \supseteq \{id\}$$

$< a >$ ist ein Normalteiler von V, da V abelsch ist und die Faktoren $V/ < a >$ und $< a > /\{id\}$ sind zyklisch, weil deren Ordnung eine Primzahl ist. Somit sind alle Faktoren aus $S_4 \supseteq A_4 \supseteq V \supseteq < a > \supseteq \{id\}$ zyklisch.

11.14 Satz *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*

1) *$\varphi(K(U)) = K(\varphi(U))$ für $U \leq G$.*
2) *$\varphi(K^n(G)) \subseteq K^n(H) \quad \forall n \in \mathbb{N} \setminus \{0\}$.*
3) *$\varphi(K^n(G)) = K^n(H) \quad \forall n \in \mathbb{N} \setminus \{0\}$, falls φ surjektiv.*

Beweis:
1) " $\subseteq$ " Sei $\varphi([u,v])$ mit u,$v \in U$ ein erzeugendes Element von $\varphi(K(U))$.Dann folgt:
$\varphi([u,v]) = \varphi(uvu^{-1}v^{-1}) = \varphi(u)\varphi(v)\varphi(u^{-1})\varphi(v^{-1}) = \varphi(u)\varphi(v)\varphi(u)^{-1}\varphi(v)^{-1} = [\varphi(u), \varphi(v)] \in K(\varphi(U))$, d.h. $\varphi(K(U)) \subseteq K(\varphi(U))$.
" $\supseteq$ " Sei $[\varphi(u), \varphi(v)]$ ein erzeugendes Element von $K(\varphi(U))$. Dann folgt:
$[\varphi(u), \varphi(v)] = \varphi(u)\varphi(v)\varphi(u)^{-1}\varphi(v)^{-1} = \varphi(u)\varphi(v)\varphi(u^{-1})\varphi(v^{-1}) = \varphi(uvu^{-1}v^{-1}) = \varphi([u,v]) \in \varphi(K(U))$, d.h. $\varphi(K(U)) \supseteq K(\varphi(U))$
2) Beweis durch vollständige Induktion
Ind.-Anfang: $n = 1$ $\quad \varphi(K(G)) = K(\varphi(G)) \subseteq K(H)$ ist klar
Ind.-Voraussetzung: Die Behauptung gelte für $n \in \mathbb{N}$, also $\varphi(K^n(G)) \subseteq K^n(H)$
Ind.-Schritt: $n \to n{+}1$ $\quad \varphi(K^{n+1}(G)) = \varphi(K(K^n(G))) \subseteq K(\varphi(K^n(G))) \subseteq K(K^n(H)) = K^{n+1}(H)$
3) Beweis durch vollständige Induktion. Sei φ surjektiv:
Ind.-Anfang: $n = 1$ $\quad \varphi(K(G)) = K(H)$ ist klar.
Ind.-Voraussetzung: Die Behauptung gelte für $n \in \mathbb{N}$, also $\varphi(K^n(G)) = K^n(H)$
Ind.-Schritt: $n \to n{+}1$ $\quad \varphi(K^{n+1}(G)) = \varphi(K(K^n(G))) = K(\varphi(K^n(G))) = K(K^n(H)) = K^{n+1}(H)$

□

11.15 Satz

1) Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.

2) Jede Faktorgruppe einer auflösbaren Gruppe ist auflösbar.

3) Jedes endliche Produkt von auflösbaren Gruppen ist auflösbar.

Beweis:
1) Sei $U \leq G$ und $i : U \to G$ die Inklusionsabbildung. Nach 11.14 (2) gilt:

$$K^n(U) = i(K^n(U)) \subseteq K^n(G) \qquad \forall n \in \mathbb{N} \setminus \{0\}$$

Da G auflösbar ist, gilt für ein festes $m \in \mathbb{N} : K^m(G) = \{e\}$ und damit ist auch $K^m(U) = \{e\}$, das heißt U ist auflösbar.

2) Sei $N \trianglelefteq G$ und $\nu : G \to G/N$ der natürliche Homomorphismus. Mit $K^m(G) = \{e\}$ für ein festes $m \in \mathbb{N}$ gilt auch $K^m(G/N) = \{e\}$, denn nach 11.14 (3) gilt: $N = \nu(\{e\}) = \nu(K^m(G)) = K^m(G/N)$

3) Zu zeigen: Wenn $K^m(G \times H) = \{e\}$, ist auch $K^m(G) \times K^m(H) = \{e\}$. Darum genügt es zu zeigen: $K^n(G \times H) = K^n(G) \times K^n(H)$
Beweis durch vollständige Induktion: Seien $a, b \in G$ und $c, d \in H$.

Ind.-Anfang: $n = 1$
$K(G\times H) = \langle [(a,c),(b,d)] \rangle = \langle (a,c)(b,d)(a,c)^{-1}(b,d)^{-1} \rangle = \langle (a,c)(b,d)(a^{-1},c^{-1})(b^{-1},d^{-1}) \rangle = \langle (aba^{-1}b^{-1}, cdc^{-1}d^{-1}) \rangle = \langle ([a,b],[c,d]) \rangle = K(G) \times K(H)$

Ind.-Voraussetzung: Die Behauptung gelte für $n \in \mathbb{N}$, also $K^n(G\times H) = K^n(G)\times K^n(H)$.

Ind.-Schritt: $n \to n+1$
$K^{n+1}(G \times H) = K(K^n(G \times H)) = K(K^n(G) \times K^n(H)) = K(K^n(G)) \times K(K^n(H)) = K^{n+1}(G) \times K^{n+1}(H)$

□

11.16 Satz

1) **(Satz von Burnside)** *Alle Gruppen der Ordnung $p^a q^b$ $(p, q \in \mathbb{P}, p \neq q, a, b \in \mathbb{N})$ sind auflösbar.*

2) **(Satz von Feit-Thompson)** *Alle endlichen Gruppen ungerader Ordnung sind auflösbar.*

11.17 Bemerkung *Der* **Satz von Feit-Thompson** *wurde bereits um die Jahrhundertwende von* **Burnside** *vermutet. Ein Beweis wurde jedoch erst im Jahre 1963 von den Amerikanern* **W. Feit** *und* **J. Thompson** *gefunden. Der Originalbeweis ist mit allen Hilfssätzen 274 Seiten lang.*

Aus dem dritten Vortrag dieses Seminars wissen wir, daß die Galoisgruppe eines Polynoms $f \in \mathbb{Q}[T]$ isomorph ist zu einer Untergruppe der symmetrischen Gruppe S_r, wobei r die Anzahl der verschiedenen Nullstellen von f ist. Zudem ist bekannt, daß ein solches Polynom $f \in \mathbb{Q}[T]$ genau dann durch Radikale auflösbarer ist, wenn dessen Galoisgruppe auflösbar ist (siehe Einleitung).
Daraus ergibt sich direkt folgender Satz:

11.18 Satz *Jedes Polynom $f \in \mathbb{Q}[T]$ vom Grade ≤ 4 ist durch Radikale auflösbar.*

Beweis: Sei $r \leq 4$ die Anzahl der verschiedenen Nullstellen von $f \in \mathbb{Q}[T]$, $Z := \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_r)$ der Zerfällungskörper von f ($Z = ZFK_{\mathbb{Q}}(f)$) und $G := Gal_{\mathbb{Q}}(f)$.
Dann gilt: $G \cong U$ mit $U \leq S_r$.
Nach Satz 11.11 ist S_r für $r \leq 4$ auflösbar.
$\Rightarrow$ nach Satz 11.14 ist auch jede Untergruppe von S_r auflösbar.
$\Rightarrow$ G ist auflösbar, weil G zu einer dieser Untergruppen isomorph ist.
$\Rightarrow$ das Polynom f ist durch Radikale auflösbar.

□

11.19 Bemerkung *Man kann zeigen, daß es zu jedem $n \in \mathbb{N}$ ein irreduzibles Polynom $f_n \in \mathbb{Q}[T]$ vom Grade n gibt, mit $Gal_{\mathbb{Q}}(f_n) \cong S_n$. Da S_n für $n \geq 5$ nicht auflösbar ist, gibt es also zu jedem $n \geq 5$ ein irreduzibles Polynom über $\mathbb{Q}$ vom Grade n, das nicht durch Radikale auflösbar ist. Folglich kann es keine allgemeingültigen Lösungsformeln für die Nullstellen von Polynomen vom Grade ≥ 5 geben.*

12 Die Konstruktion des regelmäßigen 17-Ecks

1796 gelang Gauß die Konstruktion des regelmäßigen 17-Ecks. Mit dieser erstaunlichen Entdeckung wollen wir uns nun näher beschäftigen. Dabei müssen wir von $\mathbb{Q}$ über die Zwischenkörper zu dem Kreisteilungskörper $L = \mathbb{Q}(\alpha)$ mit $\alpha = e^{\frac{2\pi i}{17}}$ aufsteigen. Als Grundlage werden die Seiten 223 bis 225 aus [**?**] benutzt.

12.1 Bemerkung *Die konstruierbaren Zahlen bilden einen Zwischenkörper von* $\mathbb{C} : \mathbb{Q}$. *Quadratwurzeln von konstruierbaren Zahlen sind wieder konstruierbar.*

Unser Ziel wird sein, dass wir einen Zwischenkörperverband $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_m \subseteq \mathbb{C}$ aufbauen, wobei $[K_j : Kj-1] \leq 2$ ist $\forall\ j = 1, 2, ..., m$ mit $z_1 := \alpha + \alpha^{16} \in K^m$. Nach der Algebra-Vorlesung haben wir dann nachgewiesen, dass in unserem Fall $z_1 = \alpha + \alpha^{16}$ konstruierbar ist. Mit der Formel $\alpha^k - \alpha^{17-k} = 2\cos(\frac{2\pi k}{17})$ erhalten wir $z_1 = \alpha + \alpha^{16} = 2\cos(\frac{2\pi}{17})$. Es gilt $\frac{z_1}{2} = \alpha = \cos(\frac{2\pi}{17})$, da $\alpha^{16} = \alpha^{-1}$ und Re α =Re $\alpha^{16} = \cos(\frac{2\pi}{17})$. Somit ist auch α konstruierbar, wobei α ein Eckpunkt des regelmäßigen 17-Ecks ist.

Sei $\alpha := e^{\frac{2\pi i}{17}} \in \mathbb{C}, L := \mathbb{Q}(\alpha), G := Gal(L : \mathbb{Q})$. Dann ist $f := T^{16}+T^{15}+...+T+1 \in \mathbb{Q}[T]$ das Minimalpolynom von $\alpha/\mathbb{Q}$ mit $NULL_{L:Q}(f) = \{\alpha, \alpha^2, ..., \alpha^{16}\}$. G besteht daher aus 16 $\mathbb{Q}$-Automorphismen $\sigma_1, \sigma_2, ..., \sigma_{16}$, die durch ihre Werte für α eindeutig festgelegt sind. Wir definieren ein $\sigma \in G$ mit $\sigma(\alpha) = \alpha^3$, wobei im Exponenten eine primitive Kongruenzwurzel modulo 17 steht. Dabei gilt modulo 17:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3^m \ mod\ 17$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Mit $\sigma^m(\alpha) = \alpha^{3^m \ mod\ 17}$ erhalten wir:

τ	$\tau(\alpha)$	$ord(\tau)$	τ	$\tau(\alpha)$	$ord(\tau)$
$\varepsilon = \sigma^{16}$	α	1	σ^8	α^{16}	2
σ	α^3	16	σ^9	α^{14}	16
σ^2	α^9	8	σ^{10}	α^8	8
σ^3	α^{10}	16	σ^{11}	α^7	16
σ^4	α^{13}	4	σ^{12}	α^4	4
σ^5	α^5	16	σ^{13}	α^{12}	16
σ^6	α^{15}	8	σ^{14}	α^2	8
σ^7	α^{11}	16	σ^{15}	α^6	16

Damit wird die Gruppe $G \cong (\mathbb{Z}_{17})^*$ von σ erzeugt und es gilt $G = \{\varepsilon, \sigma, \sigma^2, ..., \sigma^{15}\}$. Um die Zwischenkörper von G zu erhalten, müssen zunächst die Untergruppen von G bestimmt werden. Da G zyklisch, gibt es zu jedem Teiler der Gruppenordnung genau eine Untergruppe. $|G| = 16$. Nach Lagrange folgt, dass $|U| \in \{1, 2, 4, 8, 16\}$. Die Untergruppen von G sind $U_1 = \{\varepsilon\} =< \varepsilon >, U := U_2 = \{\varepsilon, \sigma^8\} =< \sigma^8 >, V := U_4 = \{\varepsilon, \sigma^8, \sigma^4, \sigma^{12}\} =< \sigma^{12} >, W := U_8 = \{\varepsilon, \sigma^8, \sigma^4, \sigma^{12}, \sigma^2, \sigma^6, \sigma^{10}, \sigma^{14}\} =< \sigma^{14} >, U_{16} = G$. Wir erhalten den Untergruppenverband

$$U_1 \subset U \subset V \subset W \subset U_{16}.$$

Da $L : \mathbb{Q}$ nach Bemerkung 5.3 (5. Vortrag) eine Galois-Erweiterung ist, gehört hierzu der Zwischenkörperverband

$$L = L^{<\varepsilon>} \supset L^W \supset L^V \supset L^U \supset L^G = \mathbb{Q}.$$

Nun wollen wir uns Schritt für Schritt von $\mathbb{Q}$ nach L hocharbeiten. Benötigt wird dazu nach Algebra-Vorlesung eine Basis von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$. Sei etwa $\{\alpha, \alpha^2, ..., \alpha^{16}\}$ die gewählte Basis von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$. Jetzt wollen wir den Zwischenkörper L^W bestimmen.

Uns ist die Spur-Abbildung von U aus der Algebra-Vorlesung bekannt, wobei U eine endliche Untergruppe der Gruppe $(Aut(L), \circ)$ aller Körperhomomorphismen von L ist. Die Abbildung $sp_U : L \longrightarrow L$ ist definiert durch $sp_U(\alpha) := \sum_{\sigma \in U} \sigma(\alpha)\ \forall \alpha \in L$. Es gilt nach Algebra-Vorlesung:

$$L^W = \mathbb{Q}(sp_W(\alpha), sp_W(\alpha^2), ..., sp_W(\alpha^{16}))$$

$sp_W(\alpha) = \varepsilon(\alpha) + \sigma^8(\alpha) + \sigma^4(\alpha) + \sigma^{12}(\alpha) + \sigma^2(\alpha) + \sigma^6(\alpha) + \sigma^{10}(\alpha) + \sigma^{14}(\alpha) = \alpha + \alpha^9 + \alpha^{13} + \alpha^{15} + \alpha^{16} + \alpha^8 + \alpha^4 + \alpha^2$

$sp_W(\alpha^2) = \varepsilon(\alpha^2)+\sigma^8(\alpha^2)+\sigma^4(\alpha^2)+\sigma^{12}(\alpha^2)+\sigma^2(\alpha^2)+\sigma^6(\alpha^2)+\sigma^{10}(\alpha^2)+\sigma^{14}(\alpha^2) = \alpha^2 + \alpha + \alpha^9 + \alpha^{13} + \alpha^{15} + \alpha^{16} + \alpha^8 + \alpha^4$

$sp_W(\alpha^3) = \varepsilon(\alpha^3)+\sigma^8(\alpha^3)+\sigma^4(\alpha^3)+\sigma^{12}(\alpha^3)+\sigma^2(\alpha^3)+\sigma^6(\alpha^3)+\sigma^{10}(\alpha^3)+\sigma^{14}(\alpha^3) = \alpha^3 + \alpha^{10} + \alpha^5 + \alpha^{11} + \alpha^{14} + \alpha^7 + \alpha^{12} + \alpha^6$

Durch weiteres Nachrechnen erhalten wir, dass $sp_W(\alpha^i)$ für $i = 1, ..., 16$ nur aus den beiden voneinader verschiedenen Elementen $x_1 := sp_W(\alpha)$ und $x_2 := sp_W(\alpha^3)$ bestehen. Dabei gilt

$x_1 = \alpha + \alpha^9 + \alpha^{13} + \alpha^{15} + \alpha^{16} + \alpha^8 + \alpha^4 + \alpha^2$

$x_2 = \alpha^3 + \alpha^{10} + \alpha^5 + \alpha^{11} + \alpha^{14} + \alpha^7 + \alpha^{12} + \alpha^6$

Es gilt $\mathbb{Q}(x_1, x_2) \supseteq \mathbb{Q}(x_1) \supseteq \mathbb{Q}$. Da $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}] = 2$ und $[\mathbb{Q}(x_1) : \mathbb{Q}] = 2$, folgt nach dem Gradsatz $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}(x_1)] = 1$. Somit ist $L^W = \mathbb{Q}(x_1, x_2) = \mathbb{Q}(x_1)$. x_1 hat unter den Automorphismen von G nur die Bilder x_1 und x_2. Nach Lemma 2.14 (2. Vortrag) ist dann $(T - x_1)(T - x_2)$ das Minimalpolynom von $x_1/\mathbb{Q}$. Durch leichtes Nachrechnen erhalten wir $x_1 + x_2 = -1$ und $x_1 x_2 = -4$. Daraus ergibt sich das Polynom

$$(T - x_1)(T - x_2) = T^2 - (x_1 + x_2)T + x_1 x_2 = T^2 + T - 4$$

Dabei verwende man, dass $x_1 = 2(\cos(\phi) + \cos(2\phi) + \cos(4\phi) + \cos(8\phi))$, $x_2 = 2(\cos(3\phi) + \cos(5\phi) + \cos(7\phi) + \cos(6\phi))$ ist, mit $\phi := \frac{2\pi}{17}$.

Die Nullstellen $x_1 = \frac{1}{2}(\sqrt{17} - 1)$ und $x_2 = -\frac{1}{2}(\sqrt{17} + 1)$ des Polynoms $T^2 + T - 4$ sind also nach Bemerkung 12.1 mit Zirkel und Lineal konstruierbar.

Als nächstes betrachten wir den Körper L^V, der über $\mathbb{Q}$ den Grad 4 hat, da $[L^V : \mathbb{Q}] = \frac{|\mathbb{Q}|}{|V|} = \frac{16}{4} = 4$. Es gilt nach der Algebra-Vorlesung:

$$L^V = \mathbb{Q}(sp_V(\alpha), sp_V(\alpha^2), ..., sp_V(\alpha^{16}))$$

Ausgeschrieben haben die $sp_V(\alpha^i)$ für $i = 1, ..., 16$ folgende Gestalt

$$y_1 = \alpha + \alpha^{13} + \alpha^{16} + \alpha^4$$
$$y_2 = \alpha^2 + \alpha^9 + \alpha^{15} + \alpha^8$$
$$y_3 = \alpha^3 + \alpha^5 + \alpha^{14} + \alpha^{12}$$
$$y_4 = \alpha^6 + \alpha^{10} + \alpha^{11} + \alpha^7$$

Nach Lemma 2.14 (2. Vortrag) erhalten wir das Polynom

$$(T - y_1)(T - y_2)(T - y_3)(T - y_4).$$

Damit ist $[y_1 : \mathbb{Q}] = [L^V : \mathbb{Q}] = 4$, da das Minimalpolynom den Grad 4 hat. y_1 erzeugt L^V über $\mathbb{Q}$, also auch über L^W. Somit erhalten wir $L^V = L^W(y_1)$. Es ergibt sich das Minimalpolynom von y_1/L^W

$$(T - y_1)(T - y_2) \text{ bzw. } (T - y_3)(T - y_4).$$

Durch Nachrechnen erhalten wir $y_1 + y_2 = x_1$, $y_1y_2 = x_1 + x_2 = -1, y_1 + y_1 = x_2$ und $y_3y_4 = -1$. Daraus folgt

$$(T - y_1)(T - y_2) = T^2 - (y_1 + y_2)T + y_1y_2 = T^2 - x_1T - 1$$
$$(T - y_3)(T - y_4) = T^2 - (y_3 + y_4)T + y_3y_4 = T^2 - x_2T - 1.$$

Die Nullstellen

$y_1 = \frac{x_1}{2} + \frac{1}{2}\sqrt{{x_1}^2 + 4}$, $y_2 = \frac{x_1}{2} - \frac{1}{2}\sqrt{{x_1}^2 + 4}$,
$y_3 = \frac{x_2}{2} + \frac{1}{2}\sqrt{{x_2}^2 + 4}$ und $y_4 = \frac{x_2}{2} + \frac{1}{2}\sqrt{{x_2}^2 + 4}$

sind also nach 12.1 mit Zirkel und Lineal kostruierbar.

Nun sind $\mathbb{Q}, L^W, L^V$ bekannt. Als nächstes betrachten wir den Körper L^U. Da die Vorgehensweise analog zu der Berechnung des Zwischenkörpers L^V verläuft, werden wir uns nun kürzer fassen. Die $sp_U(\alpha^i)$ für $i = 1, ...16$ haben folgende Gestalt

$z_1 = \alpha + \alpha^{16}$, $z_2 = \alpha^2 + \alpha^{15}$
$z_3 = \alpha^3 + \alpha^{14}$, $z_4 = \alpha^4 + \alpha^{13}$
$z_5 = \alpha^5 + \alpha^{13}$, $z_6 = \alpha^6 + \alpha^{11}$
$z_7 = \alpha^7 + \alpha^{10}$, $z_8 = \alpha^8 + \alpha^9$

Da das Minimalpolynom von z_1 über $\mathbb{Q}$ den Grad 8 hat und das Minimalpolynom von z_1 über $\mathbb{Q}(x_1, y_1)$ den Grad 2, haben alle diese Elemente den Grad 8 über $\mathbb{Q}$ und den Grad 2 über $\mathbb{Q}(x_1, y_1)$. L^U wird von z_1 über $\mathbb{Q}$ erzeugt, also auch über L^V. Damit ist $L^U = L^V(z_1)$. Das Minimalpolynom von z_1/L^V ist nach (2.14)

$$(T - z_1)(T - z_4) = T^2 - (z_1 + z_4)T + z_1z_4 = T^2 - y_1T + y_3$$

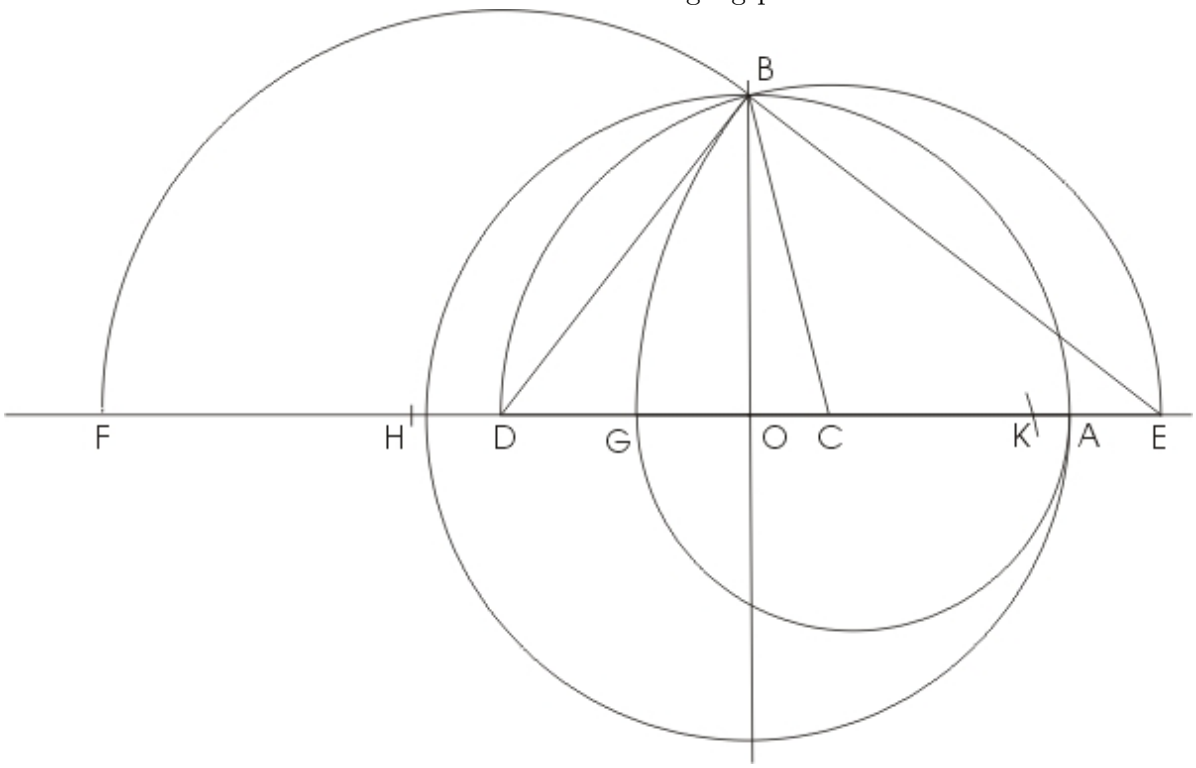
Die Nullstellen

$z_1 = \frac{y_1}{2} + \frac{1}{2}\sqrt{{y_1}^2 - 4y_3}$ und $z_4 = \frac{y_1}{2} - \frac{1}{2}\sqrt{{y_1}^2 - 4y_3}$

sind also nach 12.1 auch mit Zirkel und Lineal kostruierbar.

Das regelmäßige 17-Eck kann nun konstruiert werden, da $z_1 = \alpha + \alpha^{16} = 2\cos(\frac{2\pi}{17})$ konstruierbar ist. Es ergibt sich die folgende Konstruktion.

Die Grundfigur besteht aus zwei orthogonalen Geraden und einem Kreis um den Punkt O mit Radius $\overline{OA} = \overline{OB}$. Der Punkt O ist der Ausgangspunkt der Konstruktion.



Wir konstruieren zunächst den Wert $\sqrt{17}$. Dazu vierteln wir die Strecke $\overline{OA}$ und erhalten den Punkt C. Die Länge der Strecke $\overline{BC}$ entspricht somit dem Wert $\frac{1}{4}\sqrt{17}$. Nun schlagen wir einen Kreis um den Punkt C mit dem Radius $\overline{BC}$ und erhalten die Punkte D und E. Wir erhalten die Längen der Strecken $\overline{OD}$ bzw. $\overline{OE}$

$$\frac{1}{4}\sqrt{17} - \frac{1}{4} = \frac{x_1}{2} \quad \text{bzw.} \quad \frac{1}{4}\sqrt{17} + \frac{1}{4} = -\frac{x_2}{2}.$$

Nun schlagen wir einen Kreis um D mit dem Radius $\overline{BD}$ und erhalten den Punkt F und die Länge der Strecke $\overline{OF} = \overline{OD} + \overline{DF}$

$$\frac{x_1}{2} + \sqrt{(\frac{x_1}{2})^2 + 1} = y_1.$$

Analog schlagen wir einen Kreis um E mit den Radius $\overline{BE}$ und erhalten den Punkt G und die Länge der Strecke $\overline{OG} = \overline{EG} + \overline{EO}$

$$\sqrt{(\frac{x_2}{2})^2 + 1} - (-\frac{x_1}{2}) = y_3.$$

Jetzt halbieren wir die Strecke $\overline{OF}$ und erhalten den Punkt H. Dann errichten wir über $\overline{AG}$ den Thaleskreis und erhalten den Punkt J. Zuletzt schlagen wir einen Kreis um J mit dem Radius $\overline{OH}$ und erhalten den Punkt K. Somit erhalten wir die Länge der Strecke $\overline{HK} = \overline{HO} + \overline{OK}$

$$z_1 = \frac{y_1}{2} + \sqrt{(\frac{y_1}{2})^2 - y_3} = \alpha + \alpha^{16} = 2\cos(\frac{2\pi}{17}).$$

Zum Schluss werden wir schließen, dass

$$16\cos(\phi) = \sqrt{17} + 2\sqrt{(\frac{\sqrt{17}}{2} - \frac{1}{2})^2 + 4}$$

$$+4\sqrt{\sqrt{17} - 2\sqrt{(-\frac{\sqrt{17}}{2} - \frac{1}{2})^2 + 4} + (\frac{\sqrt{17}}{4} + \frac{\sqrt{(\frac{\sqrt{17}}{2} - \frac{1}{2})^2+4}}{2} - \frac{1}{4})2 + 1} - 1 := \xi$$

Benutzt wird dazu Maple. Also:

$$x_1 = \frac{\sqrt{17}}{2} - \frac{1}{2}, \quad x_2 = -\frac{\sqrt{17}}{2} - \frac{1}{2}$$

$$\Longrightarrow y_1 = \frac{\sqrt{17}}{4} + \frac{\sqrt{(\frac{\sqrt{17}}{2} - \frac{1}{2})^2+4}}{2} - \frac{1}{4}, \quad y_3 = \frac{\sqrt{(\frac{\sqrt{17}}{2} - \frac{1}{2})^2+4}}{2} - \frac{\sqrt{17}}{4} - \frac{1}{4}$$

$$\Longrightarrow 8z_1 = \xi = 16\cos(\phi)$$

Damit ist gezeigt, dass $16\cos(\phi)$ durch Wurzelziehen und rationale Rechenoperationen erreichbar ist. Dann gilt dasselbe für $\frac{16\cos(\phi)}{16} = \cos(\phi)$, also ist α konstruierbar.

13 Das Umkehrproblem der Galoistheorie

Dieser Vortrag beschäftigt sich mit folgender bis heute ungelösten Frage:
Gibt es zu einer beliebigen endlichen Gruppe G immer auch eine Körpererweiterung $L : \mathbb{Q}$, so dass die Galois-Gruppe von L über $\mathbb{Q}$ isomorph zu G ist?
Diese Frage ist der Kernpunkt des sogenannten **inversen Galois-Problems**, welches sich ganz natürlich aus den Anfängen der Galois-Theorie ergab, wo gezeigt wurde, dass sich einem beliebigen Polynom immer eine eindeutig bestimmte Gruppe zuordnen lässt. Die Frage wird sich als positiv zu beantworten herausstellen, falls G **abelsch** ist.
Als weiteres Ergebnis wird gezeigt, dass auch für die **symmetrische Gruppe** S_n geeignete Polynome konstruiert werdenen können.
Außerdem wird eine kleine historische Übersicht über die Entwicklung der Untersuchungen bezüglich des Inversen Galois-Problems gegeben, einige Ergebnisse vorgestellt und versucht, den derzeitigen „Stand der Dinge“ zu skizzieren.
Doch zunächst sei noch ein einfaches Ergebnis erwähnt, das klar macht, dass die Forderung „$\mathbb{Q}$ ist Grundkörper der gesuchten Galois-Erweiterung“ die eigentliche Schwierigkeit der Frage ausmacht ($\mathbb{Q}$ ist ja **Primkörper**):

13.1 Satz *Sei G eine beliebige endliche Gruppe.*
Dann gibt es Körper L und K mit $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$, so dass gilt: $Gal_K(L) \cong G$.

Beweis: Bekanntermaßen ist G isomorph zu einer Untergruppe $U \leq S_n$ (falls $|G| = n$). Im Laufe des Vortrags wird gezeigt, dass S_n als Galoisgruppe geeigneter Polynome über $\mathbb{Q}$ realisiert werden kann. Sei also f so ein Polynom (also $Gal_{\mathbb{Q}}(f) = S_n$) und $L := ZFK_{\mathbb{Q}}(f)$ der Zerfällungskörper von f über $\mathbb{Q}$. Definiere nun: $K := L^U$ der Fixkörper von L unter U. Nach dem Hauptsatz der Galois-Theorie gilt nun: $G \cong U \cong Gal_K(L)$.
□

Zunächst also die Untersuchung für abelsche Gruppen (mit einigen vorbereitenden (bekannten) Sätzen):

13.2 Satz (Chin. Restsatz)
Seien $n_1, \ldots, n_t \in \mathbb{N}$ mit $ggT(n_i, n_j) = 1$ für $i \neq j$, und $n := \prod_{i=1}^{t} n_i$.
Dann ist

$$\sigma : \mathbb{Z} \to \prod_{i=1}^{t} \mathbb{Z}_{n_i} \text{ mit } \sigma(x) = ([x]_{n_1}, [x]_{n_2}, \ldots, [x]_{n_t})$$

ein Ringhomomorphismus mit $Kern(\sigma) = n \cdot \mathbb{Z}$.
Mit anderen Worten:

$$\mathbb{Z}_n \cong \prod_{i=1}^{t} \mathbb{Z}_{n_i}$$

Beweis: siehe Vorlesung “Grundzüge der Algebra“ WS2002/2003 §8.1/8.2/8.3 (dort nur für Gruppen gezeigt, aber Übertragung auf Ringe klar (argumentiert wurde mithilfe des Gruppenhomomorphiesatzes, der in analoger Form auch für Ringe gilt (Übertragung auf Ringe mit „demselben“ Homomorphismus)
□

13.3 Satz (Dirichlet)
Seien $a, m \in \mathbb{N}$ mit $ggT(a,m) = 1$ und $A(a,m) := \{a + k \cdot m \mid k \in \mathbb{N}_0\}$ (arithmetische Folge).
Dann gilt: $A(a,m)$ enthält unendlich viele Primzahlen.

13.4 Folgerung *Für beliebiges $m \in \mathbb{N}$ enthält die arithmetische Folge $A(1,m)$ unendlich viele Primzahlen.*

Im weiteren wird nur die Folgerung aus dem Satz von Dirichlet gebraucht. Da jedoch selbst dieser Spezialfall einen sehr aufwendigen (und für unsere Zwecke nicht sehr erkenntnisreichen, da hauptsächlich zahlentheoretischen) Beweis bräuchte, wird darauf verzichtet.

Zur Erinnerung sei nun noch einmal ein wichtiges Ergebnis aus der Gruppentheorie erwähnt, das im Folgenden gebraucht wird:

13.5 Satz (Hauptsatz über endliche abelsche Gruppen)
Sei G eine endliche abelsche Gruppe.
Dann gilt: G ist isomorph zu einem direkten Produkt zyklischer Untergruppen von G (mit Primzahlpotenzordnung).

Der nächste Satz führt uns einen ersten Schritt in Richtung Kreisteilungskörper (dessen Galois-Gruppe ja nach (5.13) $(\mathbb{Z}_n)^*$ ist). Er besagt, dass man jede endliche abelsche Gruppe als Untergruppe von $(\mathbb{Z}_n)^*$ für ein geeignetes n wiederfindet.

13.6 Satz *Sei A eine endliche abelsche Gruppe der Ordnung m.*
Dann existiert ein $n \in \mathbb{N}$ mit $A \cong U \leq (\mathbb{Z}_n)^*$.

Beweis: Aus dem Hauptsatz über endliche abelsche Gruppen schließen wir zunächst:
es existieren $C_1, \dots C_t \leq A$, mit C_i zyklisch $\forall i$ und $A \cong \prod_{i=1}^t C_i$.
Setze: $m_i := |C_i|$. (Dann gilt: $m = |A| = \prod_{i=1}^t |C_i| = \prod_{i=1}^t m_i$).
Nach der o.g. Folgerung aus dem Satz von Dirichlet folgt nun: es ex. paarweise verschiedene $p_1, \dots, p_t$ prim mit $m \mid (p_i - 1)$ (da unendl. viele Primzahlen der Form $p = 1 + k \cdot m$ ex.). Setze $n := \prod_{i=1}^t p_i$.
Laut Chinesischem Restsatz gilt nun: $\mathbb{Z}_n \cong \prod_{i=1}^t \mathbb{Z}_{p_i}$.
Da gilt: $m \mid (p_i - 1)$, folgt: $m_i \mid (p_i - 1) \forall i$.
Aus dem 6. Vortrag (Satz 6.4) ist bekannt:$(\mathbb{Z}_{p_i})^*$ ist zyklisch der Ordnung $p_i - 1$.
Daraus folgt: es ex. (zyklische) Untergruppen $D_i \leq (\mathbb{Z}_n)^*$ mit $|D_i| = m_i$.
Da nun D_i und C_i jeweils zyklisch und derselben Ordnung, gilt: $C_i \cong D_i$.
Setze: $U := \prod_{i=1}^t D_i$. Insgesamt gilt nun:

$$A \cong \prod_{i=1}^t C_i \cong \prod_{i=1}^t D_i = U \text{ und } U = \prod_{i=1}^t D_i \leq \prod_{i=1}^t (\mathbb{Z}_{p_i})^* = \left(\prod_{i=1}^t \mathbb{Z}_{p_i} \right)^* \cong (\mathbb{Z}_n)^*$$

□

Da für unser angestrebtes Ziel, dem Beweis des Satzes von Kronecker-Weber, die zuletzt bewiesene Eigenschaft für Untergruppen abelscher Gruppen jedoch für Faktorgruppen gebraucht wird, zunächst noch folgender Satz:

13.7 Satz *Seien A eine endliche abelsche Gruppe und $U \leq A$ beliebig.*
Dann existiert eine Untergruppe $V \leq A$ mit $U \cong A/V$.

Beweis: Es gilt wieder: $A \cong \prod_{i=1}^{t} C_i$ mit C_i zyklisch.
Damit gilt für bel. $U \leq A$: $U \cong \prod_{i=1}^{t} U_i$ mit $U_i \leq C_i$.
Seien $u_i := |U_i|$ und $v_i := |C_i|/u_i$.
Da C_i zyklisch, existiert (genau) ein $V_i \leq C_i$ mit $|V_i| = v_i$ und da nun auch die Faktorgruppe C_i/V_i wieder zyklisch ist mit der Ordnung $|C_i|/v_i = u_i$, gilt: $U_i \cong C_i/V_i$.
Setze jetzt: $V := \prod_{i=1}^{t} V_i$. Dann gilt:

$$A/V \cong \prod_{i=1}^{t} C_i \,/\, \prod_{i=1}^{t} V_i = \prod_{i=1}^{t} (C_i/V_i) \cong \prod_{i=1}^{t} U_i \cong U$$

□

13.8 Folgerung *Sei A eine endliche abelsche Gruppe.*
Dann existieren ein $n \in \mathbb{N}$ und eine Untergruppe $B \leq (\mathbb{Z}_n)^*$, so dass $A \cong (\mathbb{Z}_n)^*/B$.

Jetzt haben wir genügend „Rüstzeug“ zusammen, um den ersten Teil des Vortrags abzuschließen mit dem:

13.9 Satz (Kronecker-Weber) *Sei A eine endliche abelsche Gruppe.*
Dann existiert eine Galois-Erweiterung $L : \mathbb{Q}$, so dass gilt: $A \cong Gal_{\mathbb{Q}}(L)$.

Beweis: Nach (5.13) gilt: $(\mathbb{Z}_n)^* \cong Gal_{\mathbb{Q}}(\mathbb{Q}_n) =: G$ ($\mathbb{Q}_n$: n-ter Kreisteilungskörper)
Nach der letzten Folgerung ex. jetzt ein $B \leq G$ mit $G/B \cong A$.
Setze: $L := \mathbb{Q}_n^B$ (also Fixkörper von B in $\mathbb{Q}_n$) und $\zeta := e^{2\pi i/n}$ (prime n-te Einheitswurzel).
Also: $\mathbb{Q} \subseteq L = \mathbb{Q}_n^B \subseteq \mathbb{Q}_n = \mathbb{Q}[\zeta]$. Definiere nun

$$f := \prod_{b \in B} (T - b(\zeta)) \in \mathbb{Q}_n[T]$$

Beh.: $f \in L[T]$ und f ist Minimalpolynom von ζ über L.
Sei $\sigma \in B$ beliebig und $\overline{\sigma}$ die kanonische Fortsetzung von σ auf $\mathbb{Q}_n[T]$. Dann gilt:

$$\overline{\sigma}(f) = \overline{\sigma}(\prod_{b \in B} (T - b(\zeta))) = \prod_{b \in B} (T - (\sigma \circ b)(\zeta)) = \prod_{b' \in B} (T - b'(\zeta)) = f$$

$$\text{Also: } \sum_{i=1}^{k} a_i T^i = f = \overline{\sigma}(f) = \sum_{i=1}^{k} \sigma(a_i) T^i$$

Koeffizienten-Vergleich ergibt: $\sigma(a_i) = a_i \forall i$.
Da $\sigma \in B$ beliebig gewählt war, folgt nun: $f \in L[T]$.
Zeige als nächstes: f ist irreduzibel
Gelte $f = g \cdot h$, $g, h \in L[T]$. Dann ist ζ Nullstelle von g oder h. (oBdA: $g(\zeta) = 0$).
Für bel. $b \in B$ gilt damit:

$$0 = b(0) = b(g(\zeta)) \overset{g \in L[T]}{=} g(b(\zeta))$$

Das heißt: alle Nullstellen von f liegen in g, woraus folgt, dass h konstant ist (da f quadratfrei (alle Nullstellen haben Vielfachheit 1)).

Damit ist f Minimal-Polynom von ζ über L.

Es gilt: $|A| \cdot |B| = |G/B| \cdot |B| = |G| = [\mathbb{Q}_n : \mathbb{Q}] = [\mathbb{Q}_n : L] \cdot [L : \mathbb{Q}] = |B| \cdot [L : \mathbb{Q}]$.
Daraus folgt: $|A| = [L : \mathbb{Q}]$.

Gezeigt wird jetzt: $A \cong Gal_{\mathbb{Q}}(L)$ (womit der Satz bewiesen wäre).
klar: $Gal_L(\mathbb{Q}_n) = B$
Falls $L : \mathbb{Q}$ auch Galoiserweiterung, so gilt nach dem 2. Teil des Haupts. der Galois-Theorie:

$$Gal_{\mathbb{Q}}(L) \cong G/B \ (\cong A)$$

Seien $g \in G, l \in L, b \in B$ bel.
Dann gilt: $b(g(l)) = (b \circ g)(l) \overset{G\,abelsch}{=} (g \circ b)(l) = g(b(l)) = g(l)$
$\Rightarrow g(l) \in L$. Also: G wirkt insgesamt nur auf L.
Nach dem 2.Teil des Haupts. der Galois-Theorie folgt, dass $L : \mathbb{Q}$ eine Galois-Erweiterung ist, womit jetzt alles bewiesen wäre.

□

Damit sei die Untersuchung für abelsche Gruppen abgeschlossen.
Beschäftigen wir uns nun mit der Frage, ob die symmetrische Gruppe S_n auch als Galois-Gruppe einer geeigneten Körpererweiterung von $\mathbb{Q}$ realisiert werden kann.
Die Idee ist dabei zunächst, eine Beziehung zu finden zwischen der (Ir)Reduzibilität eines Polynoms f über $\mathbb{Q}$ und über $\mathbb{Z}_p$. Es wird sich herausstellen, dass sich die Galoisgruppe von f über $\mathbb{Z}_p$ gerade als Untergruppe der Galoisgruppe über $\mathbb{Q}$ wiederfinden lässt.
Das Vorgehen ist dann schließlich, ein Polynom zu finden, das genügend Permutationen enthält, um ganz S_n zu erzeugen.

Zur Vorbereitung der Untersuchungen sind zunächst noch einige Aussagen über Polynome in mehreren Unbestimmten zu machen. Bewiesen werden wir dabei eher wenig, da die Aussagen schnell einzusehen, aber (insbesondere auch wegen der vielen Indizes) formale Beweise relativ mühsam sind.

13.10 Definition ((Elementar-)Symmetrische Polynome)
Ein symmetrisches Polynom in n Unbestimmten ist ein Polynom, das unter allen Permutationen der Unbestimmten invariant bleibt.
Eine besondere Art symmetrischer Polynome sind die elementar-symmetrischen Polynome. Sie haben die folgende Form:
$\sigma_k = \prod_{1 \le i_i < i_2 < \ldots < i_k \le n} T_{i_1} \cdot T_{i_2} \cdot \ldots \cdot T_{i_k}$.

In ausgeschriebener Form:
$\sigma_1 = T_1 + T_2 + \ldots + T_n$
$\sigma_2 = T_1T_2 + T_1T_3 + \ldots + T_1T_n + T_2T_3 + T_2T_4 + \ldots + T_2T_n + \ldots + T_{n-2}T_{n-1} + T_{n-2}T_n + T_{n-1}T_n$
$\sigma_3 = T_1T_2T_3 + T_1T_2T_4 + \ldots + T_1T_2T_n + T_1T_3T_4 + T_1T_3T_5 + \ldots + T_1T_3T_n + \ldots + T_{n-2}T_{n-1}T_n$
$_{(usw.)}$ $\vdots$
$\sigma_n = T_1 \cdot T_2 \cdot \ldots \cdot T_n$

Für $n = 5$ ergibt sich somit:
$\sigma_1 = T_1 + T_2 + T_3 + T_4 + T_5$
$\sigma_2 = T_1T_2 + T_1T_3 + T_1T_4 + T_1T_5 + T_2T_3 + T_2T_4 + T_2T_5 + T_3T_4 + T_3T_5 + T_4T_5$

$\sigma_3 = T_1T_2T_3 + T_1T_2T_4 + T_1T_2T_5 + T_1T_3T_4 + T_1T_3T_5 + T_1T_4T_5 + T_2T_3T_4 + T_2T_3T_5$
. $+T_2T_4T_5 + T_3T_4T_5$
$\sigma_4 = T_1T_2T_3T_4 + T_1T_2T_3T_5 + T_1T_2T_4T_5 + T_1T_3T_4T_5 + T_2T_3T_4T_5$
$\sigma_5 = T_1T_2T_3T_4T_5$

(In einfachen Worten: σ_k ist die Summe aller möglichen Zusammenstellungen von k Unbestimmten, wobei die Reihenfolge der Unbestimmten in der Zusammenstellung keine Rolle spielt (deshalb geordnet).)

13.11 Satz (Vieta) *Sei K ein beliebiger Körper, $f \in K[T]$ und $L \supseteq K$ der Zerfällungskörper von f. Gelte also:*

$$f(T) = \sum_{i=0}^{n} a_i T^i = a_n \cdot \prod_{i=1}^{n} (T - \alpha_i)$$

Dann gilt: $a_{n-k} = a_n \cdot (-1)^k \cdot \sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ für alle $k = 1, \ldots, n$

Beweis:
Die Verifikation dieser Aussage ergibt sich einfach durch Ausmultiplizieren des Ausdrucks $\prod_{i=1}^{n}(T - \alpha_i)$ und Koeffizientenvergleich mit $f(T) = \sum_{i=0}^{n} a_i T^i$.
Doch statt eines allzu technischen Induktionsbeweises, sollen uns einige Beispiele (n=2,3,4) genügen. Anschaulich sollte dann die Sache klar sein.
Bezeichne im Folgenden f_k ein allg. Polynom $k - ten$ Grades.
Also: $f_k(T) = \sum_{i=0}^{k} a_i T^i = a_k \cdot \prod_{i=1}^{k}(T - \alpha_i)$

$$\begin{aligned}
f_2(t) &= a_2\left((T-\alpha_1)(T-\alpha_2)\right) \\
&= a_2\left(T^2 - (\alpha_1+\alpha_2)T + \alpha_1\alpha_2\right) \\
f_3(t) &= a_3\left((T-\alpha_1)(T-\alpha_2)(T-\alpha_3)\right) \\
&= a_3\left(T^3 - (\alpha_1+\alpha_2+\alpha_3)T^2 + (\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)T - \alpha_1\alpha_2\alpha_3\right) \\
f_4(t) &= a_4\left((T-\alpha_1)(T-\alpha_2)(T-\alpha_3)(T-\alpha_4)\right) \\
&= a_4(T^4 - (\alpha_1+\alpha_2+\alpha_3+\alpha_4)T^3 + (\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4)T^2 \\
&\quad -(\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4)T + \alpha_1\alpha_2\alpha_3\alpha_4)
\end{aligned}$$

Bem.: Bei einem normierten Polynom ergeben sich also die Koeffizienten durch die Werte der elementar-symmetrischen Polynome in den Wurzeln des Polynoms (bis auf Vorzeichen).

□

13.12 Satz (Darstellungssatz symmetrischer Polynome) *Jedes symmetrische Polynom lässt sich als Polynom in den elementar-symmetrischen Polynomen darstellen.*

Bem.: Ein Beweis dieser Aussage lässt sich per absteigender Induktion nach dem Polynomgrad führen. Auch dieser Beweis ist hauptsächlich technisch und aufgrund der vielen Unbekannten relativ unübersichtlich. Deshalb wird auch hier auf einen formalen Beweis verzichtet.

An einem kleinen Beispiel wollen wir diese Möglichkeit der Darstellung aufzeigen:
Betrachte das Polynom

$$f(T_1, T_2) = (T_1 - 1)(T_2 - 1)(T_1 - 2)(T_2 - 2)$$

welches offensichtlich symmetrisch in den Unbekannten T_1 und T_2 ist.

Ausmultipliziert erhält man:

$$\begin{aligned} f(T_1,T_2) &= T_1^2\,T_2^2 - 3\,T_1^2\,T_2 - 3\,T_1\,T_2^2 + 9\,T_1\,T_2 + 2\,T_1^2 - 6\,T_1 + 2\,T_2^2 - 6\,T_2 + 4 \\ &= 2(T_1+T_2)^2 - 6(T_1+T_2) - 3(T_1+T_2)\cdot(T_1T_2) + (T_1T_2)^2 + 5(T_1T_2) + 4 \\ &= 2\sigma_1^2 - 6\sigma_1 - 3\sigma_1\cdot\sigma_2 + \sigma_2^2 + 5\sigma_2 + 4 \\ &= g(\sigma_1,\sigma_2) \end{aligned}$$

wobei

$$\sigma_1 = T_1 + T_2\ ,\ \sigma_2 = T_1\cdot T_2 \text{ und } g(U,V) = 2U^2 - 6U - 3UV + V^2 + 5V + 4$$

Dieses kleine Beispiel soll uns in diesem Zusammenhang reichen.

Kommen wir jetzt also zur Untersuchung des oben bereits angesprochenen Zusammenhangs:
Sei K ein Körper und $f \in K[T]$ normiert und quadratfrei mit $f = T^n + a_{n-1}T^{n-1} + \ldots + a_0 = \prod_{i=1}^{n}(T-\alpha_i)$ (im Zerfällungskörper $\overline{K}$ von f). Der Abkürzung halber definiere noch: $\alpha := (\alpha_i, \ldots, \alpha_n)$.
Seien $U = (U_i, \ldots, U_n)$ Unbestimmte.
Definiere nun, was es heißt, $\sigma \in S_n$ wirkt auf einen Ausdruck in den U_i bzw. α_i.
Sei $A(U) = A(U_1, \ldots, U_n)$ ein Ausdruck in den U_i's.
Dann sei für $\sigma \in S_n$: $\sigma_U(A(U)) := A(U_{\sigma(1)}, \ldots, U_{\sigma(n)})$.
Entsprechend auch für die α_i's: $\sigma_\alpha(A(\alpha)) := A(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$.

$$\text{Setze} \quad \vartheta := \sum_{i=1}^{n} U_i\cdot\alpha_i \quad \text{und} \quad F(T,U) := \prod_{\sigma\in S_n}(T - \sigma_U(\vartheta))$$

Damit ist $F(T,U) \in K[\alpha,U,T]$ symmetrisch in den α_i's, denn:

$$\pi_\alpha(F(T,U)) = \pi_\alpha\left(\prod_{\sigma\in S_n}(T-\sigma_U(\vartheta))\right) = \prod_{\sigma\in S_n}(T - \sigma_U(\pi_\alpha(\vartheta))) = \prod_{\sigma'\in S_n}(T-\sigma'_U(\vartheta)) = F(T,U)$$

und damit darstellbar als Polynom in den elementar-symmetrischen Polynomen mit „Unbestimmten“ α_i.
Nach dem Satz von Vieta entsprechen diese α_i gerade den Koeffizienten von f (bis auf Vorzeichen), so dass sich feststellen lässt:
$F(T,U)$ lässt sich als Polynom in den Koeffizienten von f darstellen.

$$\text{Also:} \quad F(T,U) \in K[U,T]$$

Zerlege nun $F(T,U)$ in $(K[U])[T]$ in irred. Faktoren (Es lässt sich zeigen, dass für einen faktoriellen Ring R der Polynomring $R[T]$ in einer Unbestimmten wieder ein faktorieller ist. Also folgt per Induktion, dass der Ring $(K[U])[T]$ faktoriell ist)
$F(T,U) = F_1(T,U)\cdot F_2(T,U)\cdot\ldots\cdot F_r(T,U)$

Beh.: Für einen Faktor F_{i_0} gilt: $\{\sigma \in S_n : \sigma_U(F_{i_0}) = F_{i_0}\}$ bildet eine Gruppe G (dies gilt für beliebiges i) mit $G \cong Gal_K(f)$.

Beweis: Zum 1. Punkt (Gruppeneigenschaften): Abgeschlossenheit, Assoziativität und Einselement sind klar.
Zum Inversen: $(\sigma^{-1})_U(F_i) = (\sigma^{-1})_U(\sigma_U(F_i)) = F_i$.

In $K[U,\alpha][T]$ zerfällt $F(T,U)$ in Linearfaktoren, denn $F(T,U) = \prod_{\sigma\in S_n}(T-\sigma_U(\vartheta))$
Sei i_0 nun so gewählt, dass F_{i_0} den Faktor $T-\sum_{i=1}^n U_i\alpha_i = T-\vartheta$ (also: $\sigma = id$) enthält.
Zur Abkürzung setze noch: L_{i_0}:= Menge der Linear-Faktoren von F_{i_0}.

$$\text{Aus} \quad (\sigma_U \circ \sigma_\alpha)(\vartheta) = \sum_{i=1}^{n} U_{\sigma(i)}\alpha_{\sigma(i)} = \vartheta \quad \text{folgt:} \quad \sigma_\alpha(\vartheta) = \sigma_U^{-1}(\vartheta)$$

Zwischenbeh.: $\sigma \in G \Leftrightarrow \sigma_U(T-\vartheta) \in L_{i_0}$
"$\Rightarrow$": Diese Richtung ist klar, denn für $\sigma \in G$ gilt: $\sigma_U(F_{i_0}) = F_{i_0}$ und damit, da $T-\vartheta \in L_{i_0}$: $\sigma_U(T-\vartheta) \in L_{i_0}$
"$\Leftarrow$": Da σ_U irred. Teiler von F in irred. Teiler von F überführt (denn: $\sigma_U(F_i \cdot F_j) = \sigma_U(F_i)\cdot\sigma_U(F_j)$), gilt: $\sigma_U(F_{i_0}) = F_j$ (j zunächst noch unbestimmt). Da nun $T-\vartheta$ in L_{i_0} liegt, muss $\sigma_U(F_{i_0}) = F_{i_0}$ gelten.

Nun charakterisiere noch die Elemente von $Gal_K(f)$ (aufgefasst als Untergr. von S_n):
Da F_{i_0} irreduzibel ist und den Faktor $T-\vartheta = T-\sum_{i=1}^n U_i\alpha_i$ enthält, ist der Zerfällungskörper von F_{i_0}: $(K[U,T])[\alpha]$. Da ja nun jeder Isomorphismus aus $Gal_K(f)$ durch eine Permutation der α_i's charakterisiert ist, ist dieser Isomorphismus genausogut durch Überführung von ϑ in ϑ' (Konjugierte von ϑ) charakterisiert.
Damit gibt $\sigma_\alpha = \sigma_U^{-1}$ einen Isomorphismus der beiden Gruppen an.

□

Dieses Ergebnis, was von reinem theoretischen Interesse ist, führt jetzt zu einem Korollar, das für die weiteren Untersuchungen von großem Interesse sein wird:

13.13 Korollar *Sei $f(T) \in \mathbb{Z}[T]$ normiert, p prim und $\overline{f}(T) := f(T)$ mod (p) beide quadratfrei.*
Dann gilt: $Gal_{\mathbb{Z}_p}(\overline{f}) \cong U \leq Gal_{\mathbb{Q}}(f)$.

Beweis:
Identifiziere im Folgenden wieder die Galois-Gruppen mit den entsprechenden Untergruppen von S_n.
Betrachte: $F(T,U) \in (\mathbb{Q}[U])[T]$ mit $F(T,U) = \prod_{\sigma\in S_n}(T-\sigma_U(\vartheta)) = F_1 \cdot \ldots \cdot F_r$ (F_i irreduzibel)
Nach dem Gauß-Lemma gilt nun: $F_i(T,U) \in (\mathbb{Z}[U])[T]$ (und damit natürlich auch: $F(T,U) \in (\mathbb{Z}[U])[T]$)
Betrachte nun: $(F(T,U) \bmod (p)) = (F_1 \bmod (p)) \cdot \ldots \cdot (F_r \bmod (p))$. (Beachte: $(F_i \bmod (p))$ ist nicht unbedingt irreduzibel.)
(Zur Abkürzung: Setze $\overline{F}_i := (F_i \bmod (p))$)
Sei nun $g \in Gal_{\mathbb{Z}_p}(\overline{f})$ bel.:
g(irred. Faktor von $\overline{F}_i$) =irred. Faktor von $\overline{F}_i$.
Und damit auch: g(irred. Faktor von F_i) =irred. Faktor von F_i.
Und damit ist nach obiger Überlegung: $g \in Gal_K(f)$.

□

Jetzt noch eine kurze Untersuchung, wie man mit möglichst wenig Permutationen die ganze Gruppe S_n erzeugen kann, und dann können wir uns auch schon geeignete Polynome konstruieren.

13.14 Satz *Eine transitive Untergruppe $U \leq S_n$, die eine Transposition und einen $(n-1)$-Zyklus enthält, ist ganz S_n.*

Beweis: Sei $(1, 2, \ldots, (n-1))$ der (n-1)-Zyklus (nach evtl. Umnummerierung der Zahlen $\{1, 2, \ldots, n\}$), und $\tau := (i, j)$ die Transposition.
Versuche jetzt eine Transposition der Form (k, n) zu finden. Falls $i = n$ oder $j = n$, so ist nichts mehr zu unternehmen, ansonsten führe folgende Konstruktion durch:
Da U transitiv, ex. ein $\sigma \in S_n$ mit $\sigma(j) = n$. Setze jetzt: $\nu := \sigma \circ \tau \circ \sigma^{-1}$.
Dann gilt: $\sigma(i) \xrightarrow{\sigma^{-1}} i \xrightarrow{\tau} j \xrightarrow{\sigma} \sigma(j) = n$
und: $\sigma(j) = n \xrightarrow{\sigma^{-1}} j \xrightarrow{\tau} i \xrightarrow{\sigma} \sigma(i)$.
Klar ist: $\nu(k) = k$ für alle $k \notin \{\sigma(i), n\}$, d.h. ν ist eine Transposition der Form (k, n).
Diese Transposition lässt sich nun mithilfe des Zyklus' $(1, 2, \ldots, (n-1))$ in (l, n) mit $l \in \{1, \ldots, n\}$ bel. umformen.
Damit enthält U alle Transpositionen dieser Form, die ein Erzeugendensystem für S_n bilden, sodass schließlich gilt: $U = S_n$.

□

Kommen wir nun zur Konstruktion eines Polynoms $\in \mathbb{Q}[T]$, das als Galoisgruppe die symmetrische Gruppe S_n hat.
Seien

- $f_1 \in \mathbb{Z}_2[T]$ irreduzibel vom Grade n
- $g_1, g_2 \in \mathbb{Z}_3[T]$ irreduzibel mit $grad(g_1) = n - 1$ und $grad(g_2) = 1$
- – n ungerade: $h_1, h_2 \in \mathbb{Z}_5[T]$ irreduzibel mit $grad(h_1) = 2$ und $grad(h_2) = n-2$
  – n gerade: $h_1, h_2, h_3 \in \mathbb{Z}_5[T]$ irreduzibel mit $grad(h_1) = 2$, $grad(h_2)$ ungerade, und $grad(h_1) + grad(h_2) + grad(h_3) = n$

Nach (7.12) sind diese Polynome alle zu finden.
Definiere nun:

- $f_2 := g_1 \cdot g_2$,
- $f_3 := h_1 \cdot h_2 \cdot h_3$,
- $f := 15f_1 + 10f_2 + 6f_3$.

Dann gilt:

$$f \equiv f_1 \pmod 2$$
$$f \equiv f_2 \pmod 3$$
$$f \equiv f_3 \pmod 5$$

(Es würde auch ein anderes f genügen, das diese 3 Kongruenzen erfüllt.)

Noch eine kurze Überlegung:
Nach (6.11) ist $Gal_{\mathbb{Z}_p}(P)$ zyklisch für bel. p prim und bel. $P \in \mathbb{Z}_p[T]$.
Außerdem gilt für bel. Polynom P: $Gal_K(P)$ ist transitiv $\Leftrightarrow$ P ist irreduzibel.
Zerfällt nun $P \in \mathbb{Z}_p[T]$ in der Art $P = P_1 \cdot P_2 \cdot \ldots \cdot P_r$ in irreduzible Faktoren und bezeichne $g_i := grad(P_i)$, so ergibt sich das Zykelformat der erzeugenden Permutation von $Gal_{\mathbb{Z}_p}(P)$ durch: $(1\,2 \ldots g_1)(g_1{+}1 \ \ldots \ g_2) \ \ldots \ (g_{r-1}{+}1 \ \ldots \ g_r)$.
Folgendes gilt deshalb für die Galois-Gruppe des gerade definierten f:

- '*mod* 2 - Zerfällung' $\Rightarrow$ $Gal_{\mathbb{Q}}(f)$ ist transitiv,
- '*mod* 3 - Zerfällung' $\Rightarrow$ $Gal_{\mathbb{Q}}(f)$ enthält einen $(n-1)$-Zyklus,

- '*mod* 5 - Zerfällung' $\Rightarrow$ $Gal_{\mathbb{Q}}(f)$ enthält eine Produkt aus einer Transposition und einem Zyklus (falls n ungerade) bzw. zwei Zyklen (falls n gerade) ungerader Ordnung (bildet man hiervon eine geeignete ungerade Potenz, so erhält man eine reine Transposition).

Nach obigem Satz gilt nun: Die Galois-Gruppe von f ist S_n.

Mithilfe dieses Ansatzes lässt sich sogar beweisen, dass **asymptotisch jedes** Polynom über $\mathbb{Q}$ vom Grade n und $(n \to \infty)$ die symmetrische Gruppe S_n als Galois-Gruppe hat. Dies beweist einmal mehr die Schwierigkeit des Inversen Galois-Problems.

Zur Illustration des Vorgangs wollen wir als kleines Beispiel die S_6 erzeugen:
Wähle folgende Polynome:

- $f_1 := T^6 + T^3 + 1$
- $g_1 := T^5 + T^3 + T^2 + 2 \parallel g_2 := T + 2$
- $h_1 := 2T^2 + T + 3 \parallel h_2 := T^3 + T^2 + 1 \parallel h_3 := 3T + 4$
- $f_2 := g1 \cdot g2 = T^6 + 2T^5 + T^4 + 3T^3 + 2T^2 + 2T + 4$
- $f_3 := h1 \cdot h2 \cdot h3 = 6T^6 + 17T^5 + 24T^4 + 31T^3 + 23T^2 + 13T + 12$
- $f := 15f_1 + 10f_2 + 6f_3 = 61T^6 + 122T^5 + 154T^4 + 231T^3 + 158T^2 + 98T + 127$

Mithilfe eines Computeralgebra-Systems (wie z.B. Maple) lassen sich die geforderten Eigenschaften an die Polynome einfach nachweisen und auch die Behauptung, dass f die S_6 erzeugt, verifizieren.

Eine andere Menge Polynome, die als Galois-Gruppen die symmetrischen Gruppen haben, sind die sogenannten Laguerre-Polynome, die sich sogar in geschlossener Form angeben lassen:

13.15 Satz (Issai Schur, 1930)

1. *Bedeutet L_n das n-te Laguerre-Polynom, also $L_n = \sum_{i=0}^{n} \binom{n}{i} \frac{(-T)^i}{i!}$, dann ist $Gal_{\mathbb{Q}}(L_n) \cong S_n$.*
2. *Für $E_n = \sum_{i=0}^{n} \frac{T^i}{i!}$ gilt:*
   Ist $n \equiv 0$ (mod 4), dann gilt: $Gal_{\mathbb{Q}}(E_n) \cong A_n$,
   für alle anderen n gilt: $Gal_{\mathbb{Q}}(E_n) \cong S_n$.

Zum Abschluss noch eine kleine historische Übersicht:

- **1830: François Evariste Galois** entwickelt eine Methode, einem Polynom eine endliche Gruppe zuzuordnen.
- **Ende 19. Jh.: Kronecker-Weber-Theorem** ist allgemein bekannt.
  Desweiteren sind einige Polynome bekannt, die abelsche Galois-Gruppen über $\mathbb{Q}$ besitzen. (Benutzt werden hierbei Gauss-Reihen, also ein rein zahlentheoretischer Ansatz.)

- **1892: David Hilbert** beginnt mit der ersten systematischen Studie des Inversen Galois-Problems. Mithilfe seines **Irreduzibilitäts-Theorems** beweist er folgende Aussage:
  Für beliebiges $n \geq 1$ lassen sich S_n und A_n als Galois-Gruppen über $\mathbb{Q}$ realisieren.

- **1916: Emmy Noether** beweist mithilfe von Hilberts Irreduzibilitäts-Theorems:
  Sei G eine beliebige endliche Gruppe der Ordnung n und $\mathbb{Q}[X_1, \ldots, X_n]^G$ der Fixkörper von $\mathbb{Q}[X_1, \ldots, X_n]$ unter den Permutationen der Unbestimmten mithilfe von G. Dann gilt:
  Falls $\mathbb{Q}[X_1, \ldots, X_n]^G/G$ rational (rein transzendent) ist, so ist G als Galois-Gruppe über $\mathbb{Q}$ zu realisieren.
  (**Bem.:** Nach Konstruktion ist $\mathbb{Q}[X_1, \ldots, X_n]/\mathbb{Q}[X_1, \ldots, X_n]^G$ galois mit Galois-Gruppe G.)
  „rational" bedeutet in diesem Zusammenhang, dass der Unterkörper relativ zum Oberkörper algebraisch abgeschlossen ist, d.h., dass es im Oberkörper nur transzendente Elemente gibt.

- **1937: A. Scholz** und **H. Reichhardt** beweisen folgende Aussage:
  Jede endliche p-Gruppe (p prim und $|G| = p^m$) kann als Galois-Gruppe über $\mathbb{Q}$ realisiert werden.
  Der Beweis war ein reiner Existenz-Beweis, ergab also keinen Algorithmus, wie man solche Polynome berechnen kann.

- **1950er** (vollst. Beweis erst 1989): **Shafarevich** beweist:
  Jede auflösbare Gruppe kann als Galois-Gruppe über $\mathbb{Q}$ realisiert werden.
  Auch dies war wieder ein reiner Existenzbeweis und außerdem auch hauptsächlich zahlentheoretisch, so dass sich die Idee nicht auf nicht-auflösbare Gruppen übertragen lässt.

- **1980**: Abschluss der **Charakterisierung von einfachen Gruppen**
  Aussage dieser Charakterisierung ist: *Es gibt genau **26 sporadische Gruppen** und **18 Familien einfacher Gruppen**.*
  Für die sporadischen Gruppen ist die Realisierbarkeit über $\mathbb{Q}$ bereits bewiesen (bis auf evtl. die Mathieu-Gruppe M_{23}).
  Dieses Ergebnis gab den Untersuchungen bzgl. des Inversen Galois-Problems eine neue Richtung, so dass es nun natürlich schien, sich erst auf die einfachen Gruppen zu konzentrieren und dann durch eine Art Induktion den Beweis auf alle Gruppen zu übertragen. Wie dieses Verfahren aber aussehen soll, ist noch nicht klar.

Ein letztes Ergebnis, was vielleicht besonders beeindruckend ist, ist folgendes:

- **1984: Thompson** beweist: *Die **Monster-Gruppe** kann als Galois-Gruppe über $\mathbb{Q}$ realisiert werden.*
  Warum ist dieses Ergebnis so beeindruckend? Nun, die 1980 entdeckte Monster-Gruppe beschreibt die Symmetrien eines 196883-dimensionalen Gitters und enthält insgesamt 10^{54} Elemente...

Literatur

[1] Christian Nelius: *Skript der „Algebra I“–Vorlesung*, Universität Paderborn, Sommersemester 2003

[2] G. Fischer und R. Sacher: *Einführung in die Algebra*, Teubner 1974

[3] Thomas W. Hungerford: *Algebra*, Springer 1980

[4] Heinz Lüneburg: *Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen*, B.I. 1979

[5] H. – D. Ebbinghaus et al.: *Zahlen*, Springer 1983

[6] Christian U. Jensen, Arno Ledet und Noriko Yui: *Generic Polynomials - Constructive Aspects of the Inverse Galois Problem*, Mathematical Sciences Research Institute Publications 2002