Bachelorarbeit

Der Irreduzibilitätssatz von Hilbert

Betreuung
Prof. Dr. Jan Kohlhaase
Fakultät für Mathematik
Universität Duisburg-Essen

Erstkorrekteur: Prof. Dr. Jan Kohlhaase
Zweitkorrekteur: Prof. Dr. Georg Hain

vorgelegt von:
Mike Farniok

Datum der Abgabe: 19.06.2020

Inhaltsverzeichnis

1 Vorwort

In der inversen Galoistheorie wird man mit folgendem Problem konfrontiert:

Sei G eine endliche Gruppe und K ein Körper. Existiert dann dann eine endliche Galoiserweiterung $L|K$, sodass G isomorph zu $Gal(L|K)$ ist?
Mit anderen Worten: Lässt sich eine vorgegebene Gruppe G als Galoisgruppe über einem vorgegebenen Körper K realisieren?

Dabei handelt es sich um ein (noch) ungelöstes Problem in der Mathematik. Die Antwort ist für den Körper der rationalen Zahlen $\mathbb{Q}$, sowie auch viele andere Körper unbekannt.

Als Vorbereitung werden wir uns in Kapitel 2 mit der Diskriminanten eines Polynoms beschäftigen, welches sich vorallem in Kapitel 3 als nützliches Werkzeug erweisen wird. In Kapitel 3 befassen wir uns mit hilbertschen Körpern, die nach dem Mathematiker David Hilbert benannt sind und von zentraler Bedeutung in der inversen Galoistheorie. Ist K hilbertsch und eine Galoisgruppe über dem Funktionenkörper $K(x_1, \ldots, x_m)$ in m algebraisch unabhängigen Variablen realisierbar, so auch über K, was wir insbesondere am Ende von Kapitel 3 sehen werden.
In Kapitel 4 wollen wir konkret zeigen, dass der Körper $\mathbb{Q}$ hilbertsch ist. Dies publizierte Hilbert am Ende des 19. Jahrhunderts in Form eines Theorems, welches heute als *der Irreduzibilitätssatz von Hilbert* bekannt ist. Damit lassen sich Gruppen als Galoisgruppen über $\mathbb{Q}$ realisieren, wenn sie sich über $\mathbb{Q}(x_1, \ldots, x_m)$ realisieren lassen. In Kapitel 5 werden wir dies explizit für die symmetrische Gruppe S_n zeigen und abschließend einen kleinen Ausblick darüber geben, welche endlichen Gruppen über $\mathbb{Q}$ nach heutigem Kenntnisstand bereits realisiert wurden und welche noch nicht.

Für diese Arbeit setzen wir die elementaren Erkenntnisse der endlichen Galoistheorie, die in der Vorlesung „Algebra 1“ behandelt werden, voraus und beweisen alle Aussagen bis auf Satz 2.2 und Korollar 5.3.

2 Diskriminante

Wir befassen uns kurz mit der Diskriminate von Polynomen mit Koeffizienten aus einem Körper K. Wie sich im darauffolgenden Kapitel herausstellen wird, ist die Diskriminante ein fundamentales Werkzeug für die Realisierung von Gruppen als Galoisgruppen. Für die Herleitung der Diskriminante orientieren wir uns an Teilen des Kapitels 4.4 von [Bo] und beginnen mit der Definition eines symmetrischen Polynoms:

Definition 2.1
Sei R ein Ring und $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ ein Polynom in n Variablen. Dann heißt f *symmetrisch*, falls

$$f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n)$$

für alle $i, j \in \{1, \ldots, n\}$ mit $i \neq j$.

Bemerkung
Jede Permutation $\sigma \in S_n$ operiert auf der Menge $R[x_1, \ldots, x_n]$ über die Abbildung

$$\gamma_\sigma : R[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n],\ f(x_1, \ldots, x_n) \mapsto \gamma_\sigma(f) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Offensichtlich ist ein Polynom $f \in R[x_1, \ldots, x_n]$ genau dann symmetrisch, falls $\gamma_\tau(f) = f$ ist für alle Transpositionen $\tau \in S_n$. Da die symmetrische Gruppe durch alle Transpositionen erzeugt wird, ist insbesondere f genau dann symmetrisch, wenn f invariant unter allen Permutationen ist, das heißt $\gamma_\sigma(f) = f$ für alle $\sigma \in S_n$.

Beispiel
Für $0 \leq j \leq n$ sind die elementarsymmetrischen Polynome $s_0, \ldots, s_n \in R[x_1, \ldots, x_n]$ mit

$$s_j(x_1, \ldots, x_n) := \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=j}} \prod_{i \in I} x_i$$

symmetrisch. Es sind

$$\begin{aligned} s_0 &= 1, \\ s_1 &= x_1 + \ldots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n \\ &\ldots \\ s_n &= x_1 \cdot \ldots \cdot x_n \end{aligned}$$

die elementarsymmetrischen Polynome im Ring $R[x_1, \ldots, x_n]$.

Um die Diskriminante eines Polynoms definieren zu können, benötigen wir noch den Hauptsatz über symmetrische Polynome:

Satz 2.2 (Hauptsatz über symmetrische Polynome)
Sei R ein kommutativer Ring mit Eins und $R[t_1, \ldots, t_n]$ der zugehörige Polynomring in n Variablen.

(i) Sei $R[t_1, \ldots, t_n]^s := \{f \in R[t_1, \ldots, t_n] \mid f \text{ ist symmetrisch}\}$ die Menge der symmetrischen Polynome in $R[t_1, \ldots, t_n]$. Dann ist $R[t_1, \ldots, t_n]^s$ ein Unterring, der sowohl R als auch $s_1, \ldots, s_n$ enthält.

(ii) Sei $R[s_1, \ldots, s_n]$ der durch R und $\{s_1, \ldots, s_n\}$ erzeugte Unterring, also das Bild des Einsetzungshomomorphismus

$$\Psi_{\{s_1,\ldots,s_n\}} : R[t_1, \ldots, t_n] \to R[t_1, \ldots, t_n],\ t_i \mapsto s_i.$$

Dann ist $R[t_1, \ldots, t_n]^s = R[s_1, \ldots, s_n]$.

(iii) Die Elemente $s_1, \ldots, s_n$ sind algebraisch unabhängig über R.

Beweis vgl. [Bo], Kapitel 4.4, Satz 1, Seite 168-170. □

Wir betrachten nun den speziellen Fall $R = \mathbb{Z}$ und das Polynom

$$\Delta := \prod_{i<j} (t_i - t_j)^2 \in \mathbb{Z}[t_1, \ldots, t_n].$$

Man sieht, dass Δ ein symmetrisches Polynom ist. Mit Satz 2.2 (ii) und (iii) folgt $\Delta = \Delta(s_1, \ldots, s_n) \in \mathbb{Z}[s_1, \ldots, s_n]$, da wir $\mathbb{Z}[s_1, \ldots, s_n]$ als Polynomring in den n Variablen $s_1, \ldots, s_n$ betrachten können und dementsprechend auch das Polynom Δ.

Definition 2.3
Sei R ein Integritätsbereich und $\Delta \in \mathbb{Z}[s_1, \ldots, s_n]$ wie oben gewählt. Zudem sei $f = x^n + c_1 x^{n-1} + \ldots + c_n$ ein normiertes Polynom mit Koeffizienten in R. Dann heißt

$$\Delta_f := \Delta(-c_1, c_2, \ldots, (-1)^n c_n)$$

die *Diskriminante* von f. Hierbei fassen wir $\Delta = \Delta(s_1, \ldots, s_n)$ als Polynom in $s_1, \ldots, s_n$ auf und setzen $(-1)^j c_j$ für s_j ein.

Bemerkung
Für das Polynom

$$F(x) := \prod_{i=1}^{n} (x - t_i) = \sum_{j=0}^{n} (-1)^j s_j x^{n-j} \in \mathbb{Z}[t_1, \ldots, t_n][x] \tag{1}$$

ist $\Delta \in \mathbb{Z}[s_1, \ldots, s_n]$ die Diskriminante von F.
Seien R und f wie in Definition 2.3 gewählt. Seien und $a_1, \ldots, a_n$ die Nullstellen von f in einem algebraischen Abschluss des Quotientenkörpers von R und

definiere den zugrundeliegenden Ring $\tilde{R} := R[a_1, \ldots, a_n]$. Wir betrachten den Einsetzungshomomorphismus

$$\varphi' : \mathbb{Z}[t_1, \ldots, t_n] \to \tilde{R},\ t_i \mapsto a_i,$$

welcher den kanonischen Ringhomomorphismus $\varphi : \mathbb{Z} \to R,\ n \mapsto n \cdot 1_R$ fortsetzt. Wenden wir φ' auf die Koeffizienten von F (im Zeichen $\varphi'(F)$) an, so ist $\varphi'(F) = f$. Beachten wir zusätzlich noch (1), erhalten wir

$$c_j = (-1)^j s_j(a_1, \ldots, a_n). \tag{2}$$

Nach den obigen Erkenntnissen folgt direkt, dass $\Delta_f = \varphi'(\Delta)$ ist. Mit (2) folgt, dass φ' sich zu einer wohldefinierten Abbildung

$$\varphi'' : \mathbb{Z}[s_1, \ldots, s_n] \to R,\ s_j \mapsto (-1)^j c_j,$$

einschränkt. Dann gilt $\varphi''(\Delta) = \Delta_f$, sodass $\Delta_f \in R$ ist.
Für das normierte Polynom $1 \in R[x_1, \ldots, x_n]$ folgt $\Delta_1 = 1$, da leere Produkte per Konvention den Wert 1 haben.

Proposition 2.4
Sei R ein Integritätsbereich und $f = x^n + c_1 x^{n-1} + \ldots + c_n \in R[x]$ ein normiertes Polynom mit Diskriminante Δ_f. Schreiben wir $f = \prod_{i=1}^{n}(x - a_i)$ als Produkt von Linearfaktoren in $\tilde{R}$ (siehe obige Bemerkung), so ist

$$\Delta_f = \prod_{i<j}(a_i - a_j)^2.$$

Beweis (vgl [Bo], Kapitel 4.4, Bemerkung 3)
Sei

$$\varphi' : \mathbb{Z}[t_1, \ldots, t_n] \to \tilde{R},\ t_i \mapsto a_i$$

wie zuvor gegeben. Dann ist, wie wir gesehen haben, $\varphi'(F) = f$ und damit $\varphi'(\Delta) = \Delta_f$. Daraus ergibt sich dann

$$\Delta_f = \varphi'(\prod_{i<j}(t_i - t_j)^2) = \prod_{i<j}(\varphi'(t_i) - \varphi'(t_j))^2 = \prod_{i<j}(a_i - a_j)^2$$

was zu zeigen war. □

Beispiel
Wir wollen beispielhaft die Diskriminante für Polynome der Form $f(x) = x^2 + px + q \in \mathbb{Q}[x]$ bestimmen. Sind a_1 und a_2 die Nullstellen von f im algebraischen Abschluss $\bar{\mathbb{Q}}$, so ist

$$f(x) = (x - a_1) \cdot (x - a_2) = x^2 - (a_1 + a_2)x + a_1 a_2.$$

Also ist $p = -(a_1 + a_2) = -s_1(a_1, a_2)$ und $q = a_1 a_2 = s_2(a_1, a_2)$. Nach obiger Proposition ist die Diskriminante von f gegeben durch

$$\Delta_f = (a_1 - a_2)^2 = (a_1 + a_2)^2 - 4a_1 a_2 = p^2 - 4q.$$

Zum Abschluss dieses Abschnittes zeigen wir zwei Korollare, die wir im nächsten Abschnitt für den Beweis eines zentralen Lemmas benötigen. Wir erhalten folgendes Separabilitätskriterium:

Korollar 2.5
Sei $f \in K[x]$ ein normiertes Polynom mit Diskriminante Δ_f. Dann gilt

$$f \text{ ist separabel} \Leftrightarrow \Delta_f \neq 0$$

Beweis Jedes separable Polynom besitzt nur einfache Nullstellen in einem algebraischen Abschluss. Andersrum kann die Diskriminante nur gleich Null sein, wenn f mehrfache Nullstellen besitzt. □

Korollar 2.6
Seien f und Δ_f wie zuvor in 2.5. Wir schreiben $f(x) = x^n + c_1 x^{n-1} + \ldots + c_n$. Zudem sei $\omega : K \to K'$ ein Körperhomomorphismus und $\omega(f) = x^n + \sum_{j=0}^{n-1} \omega(c_j) x^{n-j} \in K'[x]$. Dann ist $\Delta_{\omega(f)} = \omega(\Delta_f)$.

Beweis Weil ω ein Ringhomomorphismus ist, folgt

$$\Delta_{\omega(f)} = \Delta(-\omega(c_1), \ldots, (-1)^n \omega(c_n)) = \omega(\Delta(-c_1, \ldots, (-1)^n c_n)) = \omega(\Delta_f),$$

was diesen Beweis und den kurzen Abschnitt über Diskriminanten abschließt. □

3 Realisierung von Galoisgruppen

3.1 Hilbertsche Körper

In diesem Abschnitt wollen wir uns mit sogenannten hilbertschen Körpern auseinandersetzen, welche von zentraler Bedeutung für die Realisierung von vorgegeben Gruppen als Galoisgruppen sind. Dabei werden wir uns an die Darstellung des Kapitels 1.1 von [Vö] orientieren.

Wir beschäftigen uns kurz mit der Betrachtungsweise von Polynomringen in mehreren Variablen über einem Körper K. Ist $K[x_1, \ldots, x_n]$ der Polynomring in n Variablen und ist $1 \leq i \leq n$ fest gewählt, so ist

$$R_i := K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n] \subseteq K[x_1, \ldots, x_n]$$

ein Unterring. Der R_i-lineare Einsetzungshomomorphismus $R_i[x_i] \to K[x_1, \ldots, x_n]$, der x_i auf x_i abbildet, ist offenbar bijektiv. Damit erhalten wir die übliche Identifikation $K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n][x_i] \cong K[x_1, \ldots, x_n]$. Falls wir im folgenden ein Polynom $f \in K[x_1, \ldots, x_n]$ ausschließlich als Polynom in der Variablen x_i betrachten wollen, schreiben wir $f \in K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n][x_i]$. Diese Betrachtungsweise stellt eine Grundlage für den weiteren Verlauf der Arbeit dar.

Definition 3.1
Ein Körper K heißt *hilbertsch*, falls für jedes irreduzible Polynom $f(x, y) \in K[x, y]$ unendlich viele $b \in K$ existieren, sodass $f(b, y) =: f_b(y) \in K[y]$ irreduzibel ist. Wir nennen $f_b(y)$ das *spezialisierte Polynom* von f bezüglich b.

Bemerkung
Aus der Definition eines hilbertschen Körpers folgt direkt, dass endliche Körper nicht hilbertsch sein können.
Ebenso können algebraisch abgeschlossene Körper nicht hilbertsch sein. Für einen algebraisch abgeschlossenen Körper K betrachte man das Polynom $f(x) = y^2 + x \in K[x, y]$. Wir fassen nach obiger Bemerkung f als Polynom in der Variablen y mit Koeffizienten im Ring $K[x]$ auf. Dieses ist irreduzibel nach dem Eisensteinkriterium, angewendet auf das Primideal (x). Allerdings ist für alle $b \in K$ das spezialisierte Polynom $f_b(y) = y^2 + b$ nicht irreduzibel, da K algebraisch abgeschlossen ist.

Proposition 3.2
Sei R ein Integritätsbereich, K sein Quotientenkörper und sei zudem $L|K$ eine separable Körpererweiterung mit $[L : K] = n$. Dann existiert ein $\alpha \in L$, sodass $L = K[\alpha]$ und $\mu_\alpha \in R[x]$, wobei wir mit μ_α das Minimalpolynom von α bzgl. K bezeichnen.

Beweis (vgl. [CZ], Proposition 2)
Da $L|K$ eine endliche und separable Körpererweiterung von Grad $[L : K] = n$ ist, liefert der Satz vom primitiven Element die Existenz eines Elements $\beta \in L$ mit

$L = K[\beta]$. Nun gilt es zu zeigen, dass ein weiteres Element $\alpha \in L$ existiert mit $K[\beta] = K[\alpha]$ und $\mu_\alpha \in R[x]$. Sei $\mu_\beta = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$ das Minimalpolynom von β über K. Da $K = \text{Quot}(R)$ ist, können wir die Koeffizienten $a_0, \ldots, a_{n-1}$ schreiben als

$$a_0 = \frac{b_0}{c_0}, \ldots, a_{n-1} = \frac{b_{n-1}}{c_{n-1}}$$

mit geeigneten $b_0, \ldots, b_{n-1} \in R$ und $c_0, \ldots, c_{n-1} \in R\backslash\{0\}$. Nun definiere $c := c_0 \cdot \ldots \cdot c_{n-1} \in R\backslash\{0\}$. Dann ist offensichtlich $c \cdot \mu_\beta \in R[X]$. Außerdem setzen wir $\alpha := c \cdot \beta$ und sehen, dass $K[\alpha] = K[\beta]$ ist, weil $c \in K\backslash\{0\}$ eine Einheit ist. Dann erhalten wir für das Polynom $\mu_\alpha(x) := c^n \cdot a_0 + c^{n-1} \cdot a_1 x + \ldots + c \cdot a_{n-1}x^{n-1} + x^n$, dass $\mu_\alpha(\alpha) = 0$ ist, weil

$$\begin{aligned}
\mu_\alpha(\alpha) &= \mu_\alpha(c \cdot \beta) \\
&= c^n \cdot a_0 + c^{n-1} \cdot a_1 \cdot c\beta + ... + c \cdot a_{n-1}(c\beta)^{n-1} + (c\beta)^n \\
&= c^n \cdot (a_0 + a_1\beta + ... + a_{n-1}\beta^{n-1} + \beta^n) \\
&= c^n \cdot \mu_\beta(\beta) \\
&= 0.
\end{aligned}$$

Da μ_α normiert ist vom Grad $n = [L : K] = [K[\beta] : K] = [K[\alpha] : K]$ folgt, dass μ_α das Minimalpolynom von α über K mit $\mu_\alpha \in R[x]$, was zu zeigen war. □

Bevor wir zum zentralen Lemma dieses Abschnittes kommen, möchten wir noch folgendes festhalten:

Lemma 3.3
Sei R ein Integritätsbereich mit $K = \text{Quot}(R)$ und $f, h \in R[x]$, wobei f normiert ist. Existiert ein $g \in K[x]$ mit $fg = h$, so ist $g \in R[x]$.

Beweis (vgl. [Vö], Lemma 1.5)
Wir schreiben zunächst

$$f = \sum_{i=0}^{n} a_i x^i,\ g = \sum_{i=0}^{m} b_i x^i \text{ und } h = \sum_{i=0}^{l} c_i x^i = \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i b_j) x^k = fg$$

mit $a_i, c_i \in R$ und $b_i \in K$ für alle i. Da f normiert ist, folgt für den Höchstkoeffizienten von h

$$R \ni c_l = c_{n+m} = a_n \cdot b_m = b_m,$$

weil f insbesondere normiert ist. Betrachtet man nun den zweithöchsten Koeffizienten von h, so erhält man

$$R \ni c_{n+m-1} = b_{m-1}a_n + b_m a_{n-1} = b_{m-1} + b_m a_{n-1}$$

und daraus

$$b_{m-1} = c_{n+m-1} - b_m a_{n-1} \in R,$$

da $c_{n+m-1}, b_m a_{n-1} \in R$ sind. Führt man dieses Schema induktiv fort, so kann man $c_{n+m-2}, \ldots, c_0$ bestimmen und sieht, dass diese ebenfalls in R liegen. □

Wir kommen nun zum zentralen Lemma dieses Abschnitts, welches bei der Realisierung von Gruppen als Galoisgruppen von grundlegender Bedeutung ist.

Lemma 3.4
Sei $L|K$ eine endliche Galoiserweiterung mit $[L : K] = n$ und Galoisgruppe $\mathrm{Gal}(L|K)$, R ein Unterring von K mit $K = \mathrm{Quot}(R)$. Wir wählen ein primitives Element $L = K[\alpha]$ mit $\mu_\alpha \in R[t]$ wie in Proposition 3.2. Außerdem sei $A \subset L$ endlich mit $\alpha \in A$ und invariant unter $\mathrm{Gal}(L|K)$, d.h.

$$\forall \beta \in A \ \forall \sigma \in \mathrm{Gal}(L|K) : \sigma(\beta) \in A.$$

Zu guter Letzt sei $R[A]$ der Unterring von L, erzeugt durch R und A.
Dann existiert ein $u \in R$, sodass für jeden Körper K' und jeden Ringhomomorphismus $\omega : R \to K'$ mit $\omega(u) \neq 0$ folgende Eigenschaften gelten:

(i) Es existiert eine endliche Körpererweiterung $L'|K'$, sodass ω zu einem Ringhomomorphimus $\tilde{\omega} : R[A] \to L'$ fortgesetzt werden kann.

(ii) L' ist eine endliche Galoiserweiterung von K' und wird durch $\tilde{\omega}(\alpha)$ erzeugt, das heißt es gilt $L' = K'(\tilde{\omega}(\alpha))$. Sei $\omega(\mu_\alpha) =: \mu'_\alpha$ das Polynom, dass durch Anwendung von ω auf die Koeffizienten von $\mu_\alpha \in R[X]$ entsteht. Dann ist $\mu'_\alpha(\tilde{\omega}(\alpha)) = 0$ für alle Fortsetzungen $\tilde{\omega}$ von ω und es gilt

$$[L' : K'] = [L : K] = n \Leftrightarrow \mu'_\alpha \text{ ist irreduzibel über } K'[X].$$

(iii) Nun sei μ'_α irreduzibel. Dann existiert für jede Fortsetzung $\tilde{\omega}$ von ω ein eindeutiger Isomorphismus $\mathrm{Gal}(L|K) \to \mathrm{Gal}(L'|K')$, $(\sigma \mapsto \sigma')$, sodass

$$\tilde{\omega}(\sigma(s)) = \sigma'(\tilde{\omega}(s))$$

für alle $\sigma \in \mathrm{Gal}(L|K)$ und $s \in R[A]$ gilt.

Beweis (vgl. [CZ] Lemma 2 und [Vö] Lemma 1.5)
Da der Beweis viele Behauptungen aufweist, werden wir diesen in einzelne Schritte unterteilen und anschließend die Behauptungen des Lemmas zeigen.
1.Schritt: Im ersten Schritt wollen wir $u \in R$ konstruieren. Nach Voraussetzung ist $L|K$ eine endliche Galoiserweiterung, sodass μ_α separabel ist. Somit besitzt μ_α keine doppelten Nullstellen in einem algebraischen Abschluss und es gilt $\Delta_{\mu_\alpha} \neq 0$ in R. Mit Korollar 2.6 erhalten wir für das Polynom $\omega(\mu_\alpha) =: \mu'_\alpha$ die Diskriminante $\Delta_{\mu'_\alpha} = \omega(\Delta_{\mu_\alpha})$. Wählen wir nun einen Homomorphismus $\omega : R \to K'$ mit $0 \neq w(\Delta_{\mu_\alpha}) = \Delta_{\mu'_\alpha}$, so ist μ'_α separabel nach Korollar 2.5. Das werden wir weiter unten brauchen. Sei nun $\varphi_\alpha : K[x] \to K(\alpha)$, $f \mapsto f(\alpha)$ der surjektive Einsetzungshomomorphismus. Dann existiert für alle $y \in A \subset L = K(\alpha)$ ein Polynom $g_y \in K[x]$ mit $y = g_y(\alpha)$. Da K der Quotientenkörper von R ist, finden wir ein $d_y \in R\backslash\{0\}$, sodass $d_y g_y \in R[x]$ ist. Definieren wir

$$d := \prod_{y \in A} d_y \in R\backslash\{0\} \text{ und } u := d \cdot \Delta_{\mu_\alpha} \in R\backslash\{0\},$$

so erhalten wir $dg_y \in R[x]$ für alle $y \in A$.
2. Schritt: Wir betrachten die Ringerweiterung $\tilde{R} := R[u^{-1}]$ von R in K, wobei wir $u \neq 0$ verwenden. Nach der universellen Eigenschaft von Lokalisierungen setzt sich der Ringhomomorphismus $\omega : R \to K'$ wegen $\omega(u) \neq 0$ zu einem Ringhomomorphismus $\omega_1 : \tilde{R} \to K'$ fort. Beachte auch, dass Δ_{μ_α} ein Teiler von μ_α in R ist. Aus $\omega(u) \neq 0$ folgt daher auch $\omega(\Delta_{\mu_\alpha}) \neq 0$, sodass μ'_α wie oben erwähnt separabel ist. Beachte schließlich, dass auch d in $\tilde{R}$ invertierbar ist wegen $d^{-1} = u^{-1}\Delta_{\mu_\alpha} \in \tilde{R}$.
3. Schritt: Wir zeigen, dass $\tilde{R}[A] = \tilde{R}[\alpha]$ ist, wobei die Inklusion „$\supseteq$“ trivial ist, da $\alpha \in A$. Für die Inklusion „$\subseteq$“ sei $y \in A$ und $g_y(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ wie in Schritt 1 gewählt. Dann ist

$$dy = dg_y(\alpha) = \sum_{i=0}^{n} da_i \alpha^i = \sum_{i=0}^{n} (\prod_{\substack{z \in A \\ z \neq y}} d_z)(d_y a_i)\alpha^i \in R[\alpha],$$

weil $d_y a_i, d_z \in R$ nach Wahl von d_y im ersten Schritt des Beweises. Außerdem ist $R[\alpha] \subset \tilde{R}[\alpha]$, sodass wir für $y \in A$ folgern können, dass $y = d^{-1}dy \in \tilde{R}[\alpha]$ ist. Insgesamt erhalten wir $A \subset \tilde{R}[\alpha]$ und damit folglich $\tilde{R}[A] \subseteq \tilde{R}[\alpha]$, was die Mengengleichheit zeigt. Nun können wir die Behauptungen (i)-(iii) zeigen.
(i): Wir beginnen mit der Konstruktion der Körpererweiterung L' von K' und wählen dafür einen irreduziblen Faktor g' von μ'_α in $K'[x]$. Dann definieren wir den Körper $L' := K'[x]/(g')$, der nach Konstruktion eine endliche Körpererweiterung von K' ist.
Im Folgenden konstruieren wir eine Abbildung $\chi : \tilde{R}[A] \to K'[x]/(g')$. Wir betrachten den surjektiven Einsetzungshomomorphismus

$$\phi : \tilde{R}[x] \to \tilde{R}[\alpha],\ f(x) \mapsto f(\alpha)$$

und behaupten $\ker(\phi) = (\mu_\alpha)$. Die Inklusion " $\supseteq$ " ist trivial, da μ_α das Minimalpolynom von α ist. Für die andere Inklusion " $\subseteq$ " wählen wir ein $h \in \tilde{R}[x] \subset K[x]$ mit $h(\alpha) = 0$. Nach Definition des Minimalpolynoms existiert ein $g \in K[x]$, sodass $h = g\mu_\alpha$. Nach Lemma 3.3 ist dann $g \in R[x]$, sodass insgesamt $h \in (\mu_\alpha)$ folgt, was wiederum die Mengengleichheit zeigt. Wir teilen den Kern heraus und erhalten den induzierten Isomorphismus

$$\bar{\phi} : \tilde{R}[x]/(\mu_\alpha) \to \tilde{R}[\alpha],\ f + (\mu_\alpha) \mapsto f(\alpha).$$

Sei nun $\omega : R \to K'$ ein fest gewählter Ringhomomorphimus mit $\omega(u) \neq 0$. Dann können wir nach Schritt 2 ω nach $\omega_1 : \tilde{R} \to K'$ fortsetzen und ω_1 lässt sich wiederum koeffizientenweise zu einem Ringhomomorphismus $\bar{\omega_1} : \tilde{R}[x] \to K'[x]$, $f \mapsto \omega(f)$ fortsetzen, sodass $\bar{\omega_1}(\mu_\alpha) = \mu'_\alpha$ gilt. Ist $\pi : K'[x] \to K'[x]/(\mu'_\alpha)$ die kanonische Restklassenabbildung, so induziert $\bar{\omega_1}$ einen wohldefinierten Homomorphismus

$$\Psi : R[x]/(\mu_\alpha) \to K'[x]/(\mu'_\alpha),\ f + (\mu_\alpha) \mapsto (\pi \circ \bar{\omega_1})(f) = \bar{\omega_1}(f) + (\mu'_\alpha).$$

Sei nun

$$\tilde{\pi} : K'[x]/(\mu'_\alpha) \to K'[x]/(g'),\ f + (\mu'_\alpha) \mapsto f + (g').$$

Dann ist $\tilde{\pi}$ wohldefiniert, weil g' ein Teiler von μ'_α ist. Ist nun

$$\chi := \tilde{\pi} \circ \Psi : \tilde{R}[x]/(\mu_\alpha) \to K'[x]/(g'),\ (f + (\mu_\alpha) \mapsto \bar{\omega_1}(f) + (g') = \tilde{\pi} \circ \bar{\omega_1}(f)),$$

so ist $\hat{\omega} := \chi \circ \bar{\phi}^{-1}$ die gesuchte Abbildung von $\tilde{R}[\alpha] = \tilde{R}[A]$ nach L'. Nun gilt es zu zeigen, dass $\hat{\omega}$ unser vorgegebenes ω fortsetzt. Sei dazu $r \in R$ gegeben. Dann ist

$$\begin{aligned}
\hat{\omega}(r) &= (\chi \circ \bar{\phi}^{-1})(r) \\
&= \chi(r + (\mu_\alpha)) \\
&= \tilde{\pi} \circ \bar{\omega_1}(r) \\
&= \tilde{\pi}(\bar{\omega_1}(r)) \\
&= \tilde{\pi}(\omega(r)) \\
&= \omega(r) + (g').
\end{aligned}$$

Unter der Inklusion $K' \to K'[x]/(g')$, $\beta \to \beta + (g')$, ist das einfach $\omega(r)$, wie behauptet. Abschließend setzen wir

$$\tilde{\omega} := \hat{\omega}\big|_{R[A]}$$

und erhalten die gesuchte Fortsetzung von ω, die in (i) gefordert war.
(ii): Wir zeigen, dass $L' = K'(\tilde{\omega}(\alpha))$ und $L'|K'$ eine Galoiserweiterung ist. Zunächst folgt aus der Bijektivität von $\bar{\phi}$

$$\bar{\phi}^{-1}(\alpha) = x + (\mu_\alpha).$$

Wir erhalten unmittelbar

$$\tilde{\omega}(\alpha) = (\chi \circ \bar{\phi}^{-1})(\alpha) = \chi(x + (\mu_\alpha)) = (\tilde{\pi} \circ \bar{\omega_1})(x) = \tilde{\pi}(x) = x + (g').$$

Nach Kontruktion von Körpererweiterungen ist

$$L' = K'[x]/(g') = K'(x + (g')) = K'(\tilde{\omega}(\alpha)),$$

sodass L von $\tilde{\omega}(\alpha)$ erzeugt wird. Nun gilt es zu zeigen, dass L' eine Galoiserweiterung von K' ist. Da μ'_α und somit auch g' separabel ist, reicht es zu zeigen, dass L' eine normale Körpererweiterung von K' ist. Seien dafür $\alpha_1, \ldots, \alpha_n$ die n paarweise verschiedenen Nullstellen von μ_α mit $\alpha_i := \alpha$ für ein fest gewähltes $i \in \{1, \ldots, n\}$. Schreiben wir $\mathrm{Gal}(L|K) = \{\sigma_1, \ldots, \sigma_n\}$, dann existiert, weil $L|K$ galoissch ist mit $L = K[\alpha]$, für alle α_j genau ein $\sigma_j \in Gal(L|K)$ mit $\sigma_j(\alpha) = \alpha_j$. Weil $\alpha \in A$ und A invariant unter der Galoisgruppe ist, müssen alle Nullstellen in A enthalten sein. Somit ist dann $\tilde{\omega}(\alpha_j) \in L'$ für alle $1 \leq j \leq n$. Schreiben wir $\mu_\alpha = x^n + c_1 x^{n-1} + \ldots + c_{n-1}x + c_n$ mit $c_1, \ldots c_n \in R$, so ist offensichtlich $\tilde{\omega}(\mu_\alpha) = \mu'_\alpha$ und $\tilde{\omega}(\alpha_j)$ eine Nullstelle von μ'_α für alle j, da

$$\begin{aligned}
\mu'_\alpha(\tilde{\omega}(\alpha_j)) &= \tilde{\omega}(\mu'_\alpha)(\tilde{\omega}(\alpha_j)) \\
&= x^n + \tilde{\omega}(c_1)(\tilde{\omega}(\alpha_j))^{n-1} + \ldots + \tilde{\omega}(c_{n-1})\tilde{\omega}(\alpha_j) + \tilde{\omega}(c_n) \\
&= \tilde{\omega}(x^n + c_1(\alpha_j)^{n-1} + \ldots c_{n-1}\alpha_j + c_n) \\
&= \tilde{\omega}(\mu_\alpha(\alpha_j)) \\
&= \tilde{\omega}(0) = 0.
\end{aligned}$$

Also muss μ'_α in L' vollständig in Linearfaktoren zerfallen, sodass L' ein endlicher Zerfällungskörper von μ'_α über K ist und die Behauptung ist gezeigt. Es gilt noch die Äquivalenz zu zeigen.
Für die Hinrichtung sei $[L' : K'] = [L : K] = n$. Dann ist L' eine n-dimensionale Körpererweiterung von K', sodass das Polynom g' Grad n besitzen muss. Da g' das Polynom μ'_α teilt,erhalten wir $g' = \mu'_\alpha$ und somit die Irreduzibilität von μ'_α.
Für die Rückrichtung nutzt man, dass μ'_α irreduzibel ist. Daraus folgt direkt $g' = \mu'_\alpha$ und somit $[L' : K'] = n$.
(iii): Sei μ'_α irreduzibel und $\tilde{\omega}$ eine fest gewählte Fortsetzung von ω. Dann ist nach (ii) $L' = K'[x]/(\mu'_\alpha)$ eine Galoiserweiterung von K' vom Grad n. Nun besitzt μ'_α, wie zuvor gesehen, die paarweise verschiedenen Nullstellen $\tilde{\omega}(\alpha_j) =: \alpha'_j \in L'$ für alle $1 \leq j \leq n$, was aus der Separabilität und der Irreduzibilität von μ'_α folgt. Schreiben wir $\mathrm{Gal}(L'|K') = \{\sigma'_1, \dots \sigma'_n\}$, so existiert für alle $1 \leq j \leq n$ genau ein $\sigma'_j \in Gal(L'|K')$ mit $\sigma'_j(\alpha') = \alpha'_j$, wobei $\alpha' := \alpha'_i = \tilde{\omega}(\alpha_i) = \tilde{\omega}(\alpha)$. Wir definieren die bijektive Abbildung

$$\varphi : \mathrm{Gal}(L|K) \to \mathrm{Gal}(L'|K'),\ (\sigma_i \mapsto \sigma'_i),$$

und zeigen, dass φ ein Isomorphismus ist. Dafür zeigen wir zunächst, dass für alle $s \in \tilde{R}[A]$ und für alle $\sigma_i \in \mathrm{Gal}(L|K)$ die Gleichung

$$\hat{\omega}(\sigma_i(s)) = \sigma'_i(\hat{\omega}(s)) \tag{3}$$

erfüllt ist. Wegen $\tilde{R}[A] = \tilde{R}[\alpha]$ reicht es die Behauptung für alle Elemente aus $\tilde{R}$ und das Element α zu überprüfen. Für $r \in \tilde{R} \subset K$ gilt

$$\hat{\omega}(\sigma_i(r)) = \hat{\omega}(r) = (\chi \circ \bar{\phi}^{-1})(r) = \chi(x + (\mu_\alpha)) = (\tilde{\pi} \circ \bar{\omega_1})(r) = \bar{\omega_1}(r) + (\mu'_\alpha),$$

weil $g' = \mu'_\alpha$ ist und somit $\tilde{\pi}$ die Identität ist. Außerdem ist $\bar{\omega_1}(r) \in K'$, woraus wir

$$\bar{\omega_1}(r) + (\mu'_\alpha) = \sigma'_i(\bar{\omega_1}(r) + (\mu'_\alpha)) = \sigma'_i(\hat{\omega}(r))$$

folgern können. Für α haben wir

$$\hat{\omega}(\sigma_i(\alpha)) = \hat{\omega}(\alpha_i) = \alpha'_i = \sigma'_i(\alpha') = \sigma'_i(\hat{\omega}(\alpha)),$$

also insgesamt die Behauptung für Elemente aus $\tilde{R}[\alpha]$. Da $R[A] \subset \tilde{R}[\alpha]$, gilt die Behauptung insbesondere für $\tilde{\omega}$. Um zu zeigen, das φ ein Gruppenhomomorphismus ist, bemerken wir $\sigma_i(\alpha) \in A$ für $1 \leq i \leq n$ und wenden (3) folgendermaßen an:

$$\begin{aligned}
\varphi(\sigma_i \circ \sigma_j)(\alpha') &= (\sigma_i \circ \sigma_j)'(\alpha') \\
&= (\sigma_i \circ \sigma_j)'(\tilde{\omega}(\alpha)) \\
&= \tilde{\omega}((\sigma_i \circ \sigma_j)(\alpha)) \\
&= \tilde{\omega}((\sigma_i(\sigma_j)(\alpha))) \\
&= \sigma'_i(\tilde{\omega}(\sigma_j(\alpha))) \\
&= \sigma'_i(\sigma'_j(\tilde{\omega}(\alpha))) \\
&= (\sigma'_i \circ \sigma'_j)(\tilde{\omega}(\alpha)) \\
&= (\sigma'_i \circ \sigma'_j)(\alpha') \\
&= (\varphi(\sigma_i) \circ \varphi(\sigma_j))(\alpha').
\end{aligned}$$

Dies schließt den Beweis ab. □

Konvention:
Für den Rest dieser Arbeit setzen wir voraus, dass alle betrachteten Körper Charakteristik 0 besitzen.

Erinnerung
Sei $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ und R ein faktorieller Ring. Dann nennen wir f *primitiv*, falls $\mathrm{ggT}(a_0, \ldots, a_n) = 1$ ist. Insbesondere sind normierte Polynome stets primitiv.

Lemma 3.5
Sei $f \in K[x_1, \ldots, x_n]$ und $1 \leq i \leq n$. Dann sind äquivalent:

(i) f ist irreduzibel in $K[x_1, \ldots, x_n]$

(ii) f ist irreduzibel und primitiv in $(K[x_1, \ldots, x_{i-1}, x_{i+1} \ldots, x_n])[x_i]$.

Insbesodere ist f genau dann irreduzibel in $K[x_1, \ldots, x_{i-1}, x_{i+1} \ldots, x_n][x_i]$, wenn f irreduzibel in $K(x_1, \ldots, x_{i-1}, x_{i+1} \ldots, x_n)[x_i]$ ist.

Beweis (vgl. [Vö], Lemma 1.4)
Wir definieren $R := K[x_1, \ldots, x_{i-1}, x_{i+1} \ldots, x_n]$.
"⇒": Sei f irreduzibel in $K[x_1, \ldots, x_n]$. Nehmen wir an, dass f reduzibel in $R[x_i]$ ist, so würde es eine Zerlegung $f = gh$ in $R[x_i]$ geben, sodass g und h keine Einheiten sind. Das bedeutet g oder h haben positiven Grad als Polynom in x_i oder sind Elemente aus $R \backslash R^\times$. In beiden Fällen ist g oder h keine Einheit in $K[x_1, \ldots, x_n]$, im Widerspruch zur Irreduzibilität von f.
"⇐": Sei $f = \sum_{j=0}^{m} a_j(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) x_i^j \in R[x_i]$ irreduzibel und primitiv, sodass $\mathrm{ggT}(a_0, \ldots, a_m) = 1$ ist. Falls wir dann $f = gh$ schreiben in $K[x_1, \ldots, x_n]$, so muss g oder h ein Element aus R sein. Wäre dies nicht so, wären g und h keine Einheiten in $R[x_i]$, aber dann wäre f nicht irreduzibel in $R[x_i]$. Wir können also ohne Einschränkung annehmen, dass $g \in R$ ist. Da f nach Voraussetzung primitiv ist, muss g eine Einheit in R sein, also ein Element aus K, was wiederum die Irreduzibilität in $K[x_1, \ldots, x_n]$ zeigt. Die letzte Behauptung folgt direkt aus dem Lemma von Gauß. □

Lemma 3.6
Sei K ein Körper und $f(x, y) \in K[x][y]$ ein separables Polynom, welches wir als Polynom in $K(x)[y]$ auffassen, wobei $K(x) = \mathrm{Quot}(K[x])$. Dann ist $f_b(y) \in K[y]$ separabel für alle bis auf endlich viele $b \in K$.

Beweis (vgl. [Vö], Lemma 1.6)
Wir können ohne Einschränkung annehmen, dass f als Polynom in der Variablen y normiert ist, da wir sonst f durch $a_n(x)^{n-1} \cdot f(\frac{x}{a_n(x)})$ ersetzen, wobei $a_n(x)$ der Höchstkoeffizient von f ist. Außer an den endlich vielen Nullstellen von $a_n(x)$ ändert das die Separabilität von $f_b(y)$ nicht. Nach Korollar 2.5 ist die Diskriminante

$\Delta_f(x) \in K[x]$ ein von 0 verschiedenes Polynom. Schreiben wir

$$f(x,y) = \sum_{i=0}^{n} a_i(x)y^i \in K[x][y] \text{ und } f_b(y) = \sum_{i=0}^{n} a_i(b)y^i \in K[y],$$

dann folgt aus der Definition der Diskriminante von f, dass

$$\Delta_{f_b} = \Delta((-1)^j a_j(b)) = \Delta((-1)^j a_j(x))(b) = \Delta_f(b).$$

Aus $\Delta_f(x) \in K[x]$ folgt, dass $\Delta_f(x)$ nur endlich viele Nullstellen in K besitzt. Somit ist $\Delta_{f_b} = \Delta_f(b) \neq 0$, falls $b \in K$ keine Nullstelle von $\Delta_f(x)$ ist, sodass $f_b(y)$ für alle $b \in K$, die keine Nullstellen der Diskriminate sind, separabel ist. □

Definition 3.7
Sei K ein Körper und G eine endliche Gruppe. Wir sagen, dass sich G als Galoisgruppe über K realisieren lässt, falls eine Galoiserweiterung $L|K$ existiert, sodass $G \cong \mathrm{Gal}(L|K)$ ist.

Bezüglich der Fragestellung, ob endliche Gruppen als Galoisgrruppen realisiert werden können, können wir nun folgende Aussage für hilbertsche Körper treffen:

Satz 3.8
Sei K hilbertsch und $E|K(x)$ eine endliche Galoiserweiterung mit $[E : K(x)] = n > 1$. Sei $\alpha \in E$ gewählt mit $E = K(x)[\alpha]$ und $\mu_\alpha(x,y) \in K[x][y]$ (vgl. Proposition 3.2). Dann ist $L := K[y]/(\mu_{\alpha,b}(y))$ eine endliche Galoiserweiterung von K für unendlich viele $b \in K$,wobei $\mu_{\alpha,b}(y) := \mu_\alpha(b,y)$. Zudem existiert ein Isomorphismus

$$\mathrm{Gal}(L|K) \cong \mathrm{Gal}(E|K(x)).$$

Insbesondere lässt sich eine endliche Gruppe G als Galoisgruppe über K realisieren, wenn sie sich als Galoisgruppe über $K(x)$ realisieren lässt.

Beweis (vgl. [CZ], Theorem 1)
Sei A die Nullstellenmenge des Polynoms $\mu_\alpha(x,y) \in K(x)[y]$ in einem geeigneten algebraischen Abschluss. Dann gilt $A \subseteq L$, weil $E|K(x)$ normal ist, und die Nullstellen des Minimalpolynoms werden von $\mathrm{Gal}(E|K(x))$ permutiert. Trivialerweise ist auch $\alpha \in A$, weil μ_α das Minimalpolynom von α ist. Sei

$$\varphi_b : K[y] \to K, \ (g \mapsto g(b)),$$

der Einsetzungshomomorphismus bezüglich $b \in K$ und $\Delta_{\mu_\alpha}(x) \in K[x]$ die Diskriminante von μ_α. Dann ist, wie wir im Beweis von Lemma 3.6 gesehen haben,

$$\varphi_b(\Delta_{\mu_\alpha}(x)) = \Delta_{\mu_\alpha}(b) = \Delta_{\mu_{\alpha,b}} \neq 0$$

für alle bis auf endlich viele $b \in K$, da μ_α separabel ist. In der Notation des Beweises von Lemma 3.4 ist auch $d \in K[x]\backslash\{0\}$ ein von Null verschiedenes Polynom.

Wegen $u = d \cdot \Delta_{\mu_\alpha}$ können wir durch Ausschluss der endlich vielen Nullstellen von d und Δ_{μ_α} sogar $\varphi_b(u) = u(b) \neq 0$ annehmen. Nach Lemma 3.4(i) lässt sich der Ringhomomorphismus $\varphi_b : K[x] \to K$ zu einem Ringhomomorphismus $\varphi_b' : K[x][A] \to L$ fortsetzen. Mit Lemma 3.4(ii) ist L eine Galoiserweiterung von K, wenn $\varphi_b(\mu_\alpha(x,y)) = \mu_{\alpha,b}(y)$ irreduzibel ist, was wiederum gegeben ist für unendlich viele $b \in K$, da K hilbertsch ist. Entfernen wir die $b \in K$, für die $\mu_{\alpha,b}(y)$ reduzibel ist, so ist nach Lemma 3.4(iii)

$$Gal(L|K) \cong Gal(E|K(x)).$$

□

Für die folgende Proposition wählen wir uns vorab einen hilbertschen Körper K und eine endliche Galoiserweiterung $E|K(x)$, die wir nach Proposition 3.2 schreiben als $E = K(x)[\alpha]$ mit Minimalpolynom $\mu_\alpha \in K[x][y]$.

Proposition 3.9
Sei $L|K$ eine endliche Körpererweiterung mit $L(x) \subset E$ und $h \in L[x][y]$ irreduzibel, sodass sämtliche Nullstellen in E liegen. Für alle bis auf endlich viele $b \in K$ gilt dann: Ist $\mu_{\alpha,b}(x)$ irreduzibel in $K[y]$, so ist $h_b(y)$ irreduzibel in $L[y]$.

Beweis (vgl [CZ]. Proposition 3)
Da $\mathrm{char}(K) = 0$ ist, finden wir nach dem Satz vom primitiven Element $\beta \in L$ mit $L = K[\beta]$. Um den Beweis übersichtlicher zu gestalten, unterteilen wir ihn in drei Schritte.
Schritt 1: Sei $\mu_\beta \in K(x)[y]$ das Minimalpolynom von β über $K(x)$. Wir definieren die Menge $A \subseteq E$, bestehend aus den Nullstellen von den Minimalpolynomen μ_α und μ_β, sowie den Nullstellen von h, die wir $\beta_1, \ldots, \beta_m$ nennen. Nun ist klar, dass A invariant unter $\mathrm{Gal}(E|K(x))$ ist, weil alle konjugierten Elemente ebenfalls in A liegen. Da h irreduzibel ist über $L[x][y]$, ist h auch separabel, denn $\mathrm{char}(L(x)) = 0$. Mit Lemma 3.6 ist auch h_b separabel für alle bis auf endlich viele $b \in K$. Wir entfernen an dieser Stelle diese endlich vielen b, um sicher zu stellen, dass h_b paarweise verschiedene Nullstellen besitzt. Sei nun wie im Beweis zuvor

$$\varphi_b : K[x] \to K$$

der Einsetzungshomomorphismus bezüglich b. Dann ist, wie wir gesehen haben, $\varphi_b(u) = u(b) \neq 0$ für alle bis auf endlich viele $b \in K$, sodass wir ohne Einschränkung $\varphi_b(u) \neq 0$ annehmen können. Wir fixieren nun ein solches b. Dann existiert nach Lemma 3.4 eine Galoiserweiterung E' von K, sowie eine Fortsetzung von φ_b, etwa

$$\tilde{\varphi}_b : K[x][A] \to E'.$$

Weil $\beta \in A$ ist, folgt offensichtlich $L \subset K[x][A]$, sodass die Einschränkung

$$\tilde{\varphi}_b\big|_L : L \to \tilde{\varphi}_b(L) =: \tilde{L}$$

ein Isomorphismus ist. Wir identifizieren $\tilde{L}$ mit L über diesen Isomorphismus und betrachten E' als Körpererweiterung von L. Wegen $L[x] = K(\beta)[x] \subset K[A][x] =$

$K[x][A]$ kann $L[x]$ als Teilmenge von $K[x][A]$ betrachtet werden. Wir schreiben $h(x,y) = \sum_{i=0}^{m} h_i(x)y^i$ und sehen, dass die Koeffizienten von $h \in L[x][y]$ in $K[x][A]$ enthalten sind. Sei

$$\chi_b : K[A][x][y] \to E'[y]$$

die koeffizientenweise definierte Erweiterung der Abbildung $\tilde{\varphi}_b$. Im Folgenden möchten wir das Polynom $\chi_b(h)$ näher untersuchen und insbesondere seine Nullstellen. Es gilt $\chi_b(h) = h_b$ in $L[y] \cong \tilde{L}[y] \subseteq E'[y]$. Die paarweise verschiedenen Nullstellen $\beta_1, \ldots, \beta_m$ von h sind in A enthalten und damit ihre Bilder $\tilde{\varphi}_b(\beta_1), \ldots, \tilde{\varphi}_b(\beta_m)$ in E'. Schreiben wir

$$h(x,y) = h_m(x)(y-\beta_1)\cdot\ldots\cdot(y-\beta_m) \in K[A][x][y],$$

so ist

$$\chi_b(h(x,y)) = h_b(y) = h_m(b)(y-\beta_1')\cdot\ldots\cdot(y-\beta_m') \in E'[y],$$

wobei $\beta_j' := \tilde{\varphi}_b(\beta_j)$ für jedes $j \in \{1,\ldots,m\}$ ist. Daraus folgt nun, dass h_b in E' in Linearfaktoren zerfällt.
Schritt 2: Im zweiten Schritt zeigen wir, dass $\mathrm{Gal}(E'|L)$ die Nullstellen von h_b transitiv permutiert. Nach Voraussetzung ist $h \in L[x][y]$ irreduzibel, und nach Lemma 3.5 insbesondere über $L(x)[y]$ irreduzibel. Nun ist $E|K(x)$ galoissch mit Zwischenkörper $L(x)$, sodass $E|L(x)$ galoissch ist. Außerdem sind die Nullstellen von h in E enthalten. Folglich muss der Zerfällungskörper des Polynoms h über $L(x)$, den wir an dieser Stelle als $\tilde{E}$ nennen, in E enthalten sein. Insbesondere ist $\tilde{E}|L(x)$ eine Galoiserweiterung und es folgt, dass $Gal(\tilde{E}|L(x))$ die Nullstellen von h transitiv permutiert. Weil $E|\tilde{E}$ algebraisch ist, kann jedes $\sigma \in Gal(\tilde{E}|L(x))$ fortgesetzt werden zu einem Homomorphismus $\tilde{\sigma} \in \mathrm{Gal}(E|L(x))$. Daraus können wir schließen, dass auch $\mathrm{Gal}(E|L(x))$ die Nullstellen von h transitiv permutiert. Nun ist K hilbertsch und E eine endliche Galoiserweiterung über $K(x)$ mit primitivem Erzeuger α und Minimalpolynom μ_α gewählt wie in Proposition 3.2. Nach Satz 3.8 und dem Beweis von Lemma 3.4 können wir $E' = K[y]/(\mu_{\alpha,b})$ wählen, und es gibt einen Gruppenisomorphismus

$$\varphi : Gal(E|K(x)) \to Gal(E'|K)$$

für alle $b \in K$, für die $\mu_{\alpha,b}(y)$ irreduzibel ist. Da K hilbertsch ist, existieren unendlich viele solcher b. Wir zeigen nun, dass $\varphi(\mathrm{Gal}(E|L(x))) = \mathrm{Gal}(E'|L)$ die Nullstellen $\beta_1', \ldots, \beta_m'$ von h transitiv permutiert. Wie wir gesehen haben, permutiert $Gal(E|L(x))$ die Nullstellen von h transitiv, sodass für zwei fest gewählte Nullstellen $\beta_i, \beta_j \in E$ mit $i \neq j$ ein $\sigma \in Gal(E|L(x))$ existiert, sodass $\sigma(\beta_i) = \beta_j$ gilt. Wenn $\sigma' = \varphi(\sigma)$ der zu σ korrespondierende Automorphismus ist, erhalten wir erneut mit Lemma 3.4(iii)

$$\sigma'(\beta_i') = \sigma'(\tilde{\varphi}_b(\beta_i)) = \tilde{\varphi}_b(\sigma(\beta_i)) = \varphi_b(\beta_j) = \beta_j',$$

was unsere Behauptung zeigt.
Schritt 3: Im letzten Schritt wollen wir zeigen, dass h_b irreduzibel in $L[y]$ ist. Wäre h_b nicht irreduzibel, so würde eine Zerlegung in nichttriviale Faktoren existieren,

und $\mathrm{Gal}(E'|L)$ würde die Nullstellen der nichttrivialen Faktoren von h_b jeweils einzeln permutieren. Dann könnte die Operation auf den Nullstellen von h_b aber nicht transitiv sein. Folglich ist h_b irreduzibel. □

Proposition 3.10
Sei $E|K(x)$ eine endliche Galoiserweiterung und $\alpha \in E$ gewählt mit $E = K(x)[\alpha]$ und $\mu_\alpha \in K[x][y]$ (siehe Proposition 3.2). Dann existieren endlich viele irreduzible Polynome $p_1(x,y), \ldots, p_k(x,y) \in K[x][y]$ mit $deg(p_i) > 1$ für alle $1 \leq i \leq k$ und unendlich viele $b \in K$, sodass folgende Behauptung erfüllt ist:
Haben alle spezialisierten Polynome $p_1(b,y), \ldots, p_k(b,y) \in K[y]$ keine Nullstelle in K, so ist das spezialisierte Polynom $\mu_{\alpha,b}(y)$ irreduzibel in $K[y]$.

Beweis (vgl. [Vö], Proposition 1.7(iii))
Schritt 1: Wir beginnen mit der Konstruktion der endlich vielen irreduziblen Polynome $p_1(x,y), \ldots, p_k(x,y) \in K[x][y]$. Nach Lemma 3.5 ist μ_α irreduzibel über $K(x)[y]$ und das Teilprodukt

$$\prod_{i \in I}(y - \alpha_i)$$

kann nicht in $K(x)[y]$ liegen, wenn I eine echte, nichtleere Teilmenge von $\{1, \ldots, n\}$ ist. Wählen wir eine feste Teilmenge $I \subset \{1, \ldots, n\}$, so folgt durch Ausmultiplizieren, dass das Teilprodukt mindestens einen Koeffizienten d_I haben muss mit $d_I \notin K(x)$. Wenn A die Nullstellenmenge von μ_α ist, so ist offensichtlich d_I eine Linearkombination aus Elementen aus der Menge A. Da alle α_i algebraisch über $K(x)$ sind, muss d_I ebenfalls algebraisch über $K(x)$ sein, was wiederum die Existenz eines irreduziblen Polynoms $p_I \in K(x)[y]$ mit $p_I(x, d_I) = 0$ und $\deg(p_I) > 1$ liefert. Mit der gleichen Argumentation wie im Beweis von Proposition 3.2 können wir ohne Einschränkung annehmen, dass $p_I \in K[x][y]$ ist. Beachte, dass nur endlich viele solcher Polynome p_I existieren können.
Schritt 2: Im Folgenden prüfen wir die Existenz der unendlich vielen $b \in K$ und zeigen die Behauptung. Da μ_α irreduzibel über $K[x][y]$ ist mit $\mathrm{char}(K(x)) = 0$, existieren nach Lemma 3.6 unendlich viele $b \in K$, sodass $\mu_{\alpha,b}$ separabel ist. Es gilt $\varphi_b(\Delta_{\mu_\alpha}) = \Delta_{\mu_\alpha}(b) \neq 0$ für alle bis auf endlich viele $b \in K$, wobei φ_b der Einsetzungshomomorphismus bezüglich b ist. Sei nun b dementsprechend gewählt und A die Nullstellenmenge von μ_α. Nach Lemma 3.4 existiert eine Galoiserweiterung $L|K$ und eine Fortsetzung $\tilde{\varphi}_b : K[x][A] \to L$ von φ_b. Ist α_i eine Nullstelle von μ_α, so ist $\tilde{\varphi}_b(\alpha_i) =: \alpha_i'$ eine Nullstelle von $\varphi_b(\mu_\alpha) = \mu_{\alpha,b}$. Wir können $\mu_{\alpha,b}$ in $L[y]$ schreiben als

$$\mu_{\alpha,b}(y) = \prod_{i=1}^{n}(y - \alpha_i').$$

Wir nehmen an, dass $\mu_{\alpha,b}$ reduzibel in $K[y]$ ist, das heißt es existieren nicht konstante Polynome $f, g \in K[y]$ mit $\mu_{\alpha,b} = fg$ in $K[y]$. Dann existiert eine echte, nichtleere Teilmenge $I \subset \{1, \ldots, n\}$, sodass

$$f = \prod_{i \in I}(y - \alpha_i')$$

geschrieben werden kann in $\overline{K}[y]$, wobei $\overline{K}$ ein algebraischer Abschluss von K ist. Betrachten wir für die gewählte Teilmenge I das Teilprodukt von μ_α, etwa $\prod_{i\in I}(y-\alpha_i)$, folgt mit Schritt 1 die Existenz eines Koeffizienten d_I mit $d_I \notin K(x)$. Allerdings ist $d_I \in K[x][A]$, sodass $c := \tilde{\varphi}_b(d_I)$ ein Koeffizient von f ist und nach Annahme in K liegt. Außerdem gilt nach Schritt 1 $p_I(x, d_I) = 0$ und daher

$$0 = \tilde{\varphi}_b(p_I(x, d_I)) = p_I(b, \tilde{\varphi}_b(d_I)) = p_I(b, c),$$

was einen Widerspruch darstellt, weil $c \in K$ eine Nullstelle von p_I ist. Da unsere Annahme falsch war, muss $\mu_{\alpha,b}$ irreduzibel sein.

□

Aus unseren Vorüberlegungen ergibt sich ingesamt:

Satz 3.11
Für einen Körper K sind äquivalent:

(i) K ist hilbertsch.

(ii) Für jede endliche Körpererweiterung $L|K$ und jede endliche Familie von irreduziblen Polynomen $h_1, \ldots, h_k \in L[x][y]$ existieren unendlich viele $b \in K$, sodass $h_{i,b}(y) := h_i(b, y) \in L[y]$ irreduzibel ist für $1 \leq i \leq k$.

(iii) Für jede endliche Familie $p_1(x, y), \ldots, p_j(x, y) \in K[x][y]$ von irreduziblen Polynomen mit $\deg(p_i) > 1$ existieren unendlich viele $b \in K$, sodass die spezialisierten Polynome $p_1(b, y), \ldots, p_j(b, y) \in K[y]$ keine Nullstellen in K besitzen.

Beweis (vgl. [Vö], Korollar 1.8)
(i)⇒(ii): Sei K hilbertsch, $L|K$ eine endliche Körpererweiterung und $\{h_1, \ldots, h_k\}$ eine endliche Menge von irreduziblen Polynomen aus $L[x][y]$. Nach Lemma 3.5 sind alle Polynome aus der obigen Menge ebenfalls irreduzibel über $L(x)[y]$. Wir definieren

$$h := \prod_{i=1}^{k} h_i$$

und betrachten einen Zerfällungskörper M von h in $L(x)$. Da $L|K$ endlich ist, ist $L(x)|K(x)$ ebenfalls endlich und mit dem Gradsatz erhalten wir, dass $M|K(x)$ endlich ist. Nun sei E eine normale Hülle von M über $K(x)$. Mit Proposition 3.2 können wir $\alpha \in E$ wählen mit $E = K(x)[\alpha]$ und $\mu_\alpha \in K[x][y]$. Nun enthält E die Nullstellen von h, also die Nullstellen von jedem h_i, und es gilt offensichtlich $L(x) \subset E$. Proposition 3.9, angewendet auf jedes h_i mit $1 \leq i \leq k$, liefert die Existenz von unendlich vielen $b \in K$, sodass $h_{i,b}(y)$ irreduzibel ist, wobei wir verwenden, dass K hilbertsch ist. Somit sind alle $h_{i,b}(y)$ gleichzeitig irreduzibel für unendlich viele $b \in K$.
(ii)⇒(iii): Wir setzen $L = K$ und $k = j$, dann folgt die Behauptung.
(iii)⇒(i): Sei $f(x, y) \in K[x][y]$ irreduzibel und $E|K(x)$ der Zerfällungskörper von f. Dann ist $E|K(x)$ endlich Galois, da f wegen $\mathrm{char}(K(x)) = 0$ separabel

ist. Wir wählen einen Erzeuger $E = K(x)[\alpha]$ mit $\mu_\alpha \in K[x][y]$ (vgl. Proposition 3.2). Voraussetzung (iii) zusammen mit Lemma 3.4 und Proposition 3.10 zeigt, dass es unendlich viele $b \in K$ gibt, sodass $\mu_{\alpha,b}$ irreduzibel ist und dass dann $L := K[y]/(\mu_{\alpha,b})|K$ endlich Galois ist mit $\mathrm{Gal}(E|K(x)) \cong \mathrm{Gal}(L|K)$. Wie in Proposition 3.9 folgt aus der Transitivität der Operation von $\mathrm{Gal}(E|K(x))$ auf der Nullstellenmenge von $f(x,y)$ auch die Transitivität der Operation von $\mathrm{Gal}(L|K)$ auf der Nullstellenmenge von $f_b(y)$. Wie dort impliziert das die Irreduzibilität von $f_b(y)$. □

Als unmittelbare Folgerung des Satzes ergibt sich noch folgendes Korollar:

Korollar 3.12
Sei K hilbertsch und $L|K$ eine endliche Körpererweiterung. Dann ist L hilbertsch.

Beweis
Die Bedingung in Satz 3.11(ii) ist invariant unter endlichen Körpererweiterungen. □

3.2 Kronecker-Spezialisierung

In diesem Abschnitt schauen wir uns die sogenannte Kronecker-Spezialisierung an, die wir im nächsten Abschnitt benötigen werden und orientieren uns an Kapitel 3 von [CZ].

Definition 3.13
Sei K ein Körper und $d, k \in \mathbb{Z}$ ganze Zahlen mit $d \geq 2$ und $k > 2$. Dann heißt der Homomorphismus von K-Algebren

$$S_d : K[x_1, ..., x_k] \to K[x, y],\ (f(x_1, ..., x_k) \mapsto f(x, y, y^d, ..., y^{d^{k-2}}))$$

eine d-Kronecker Spezialisierung.

Notation
Sei $f \in K[x_1, \ldots, x_n] \cong K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n][x_i]$. Dann definieren wir

$$deg_{x_i}(f)$$

als den Grad von f in der Variablen x_i.

Proposition 3.14
Sei K ein Körper und $k > 2$ gewählt. Wir definieren die Mengen

$$V_d := \{f \in K[x_1, ..., x_k] \mid deg_{x_i}(f) < d\ \forall i \in \{2, ..., k\}\},$$

$$W_d := \{f \in K[x, y] \mid deg_y(f) < d^{k-1}\}.$$

Dann induziert die d-Kronecker-Spezialisierung aus obiger Definition eine Bijektion

$$S_d\big|_{V_d} : V_d \to W_d.$$

Beweis (vgl. [CZ], Proposition 4)
Schritt 1: Zunächst untersuchen wir normierte Monome in V_d. Sei $f \in V_d$ ein Monom, etwa $f = x_1^{\alpha_1} \cdot ... \cdot x_k^{\alpha_k}$ mit $\alpha_1, ..., \alpha_k \in \mathbb{N}$ und $\alpha_i < d$ für alle $2 \leq i \leq k$. Wir setzen f in S_d ein und erhalten

$$S_d(f) = x^{\alpha_1} \cdot y^{\alpha_2 + \alpha_3 d + ... + \alpha_k d^{k-2}} \in K[x, y]$$

mit $\alpha_2 + \alpha_3 d + \ldots + \alpha_k d^{k-2} \leq (d-1) \cdot (1 + d + \ldots + d^{k-2}) = d^{k-1} - 1 < d^{k-1}$. Es folgt $S_d(f) \in W_d$, sodass die Abbildung für Monome wohldefiniert ist.
Schritt 2: Wir zeigen, dass $S_d\big|_{V_d}$ normierte Monome aus V_d bijektiv auf normierte Monome aus W_d abbildet. Für die Injektivität sei $g \in V_d$ ein normiertes Monom, etwa $g = x_1^{\beta_1} \cdot ... \cdot x_k^{\beta_k}$ mit $\beta_1, ..., \beta_k \in \mathbb{N}$ und $\beta_i < d$ für alle $2 \leq i \leq k$. Dann ist ebenfalls

$$S_d(g) = b x^{\beta_1} \cdot y^{\beta_2 + \beta_3 d + ... + \beta_k d^{k-2}} \in W_d$$

nach Schritt 1. Falls $S_d(f) = S_d(g)$ gilt, so folgt

$$x^{\beta_1} \cdot y^{\beta_2 + \beta_3 d + ... + \beta_k d^{k-2}} = x^{\alpha_1} \cdot y^{\alpha_2 + \alpha_3 d + ... + \alpha_k d^{k-2}},$$

das heißt

$$\beta_1 = \alpha_1 \text{ und } \beta_2 + \beta_3 d + ... + \beta_k d^{k-2} = \alpha_2 + \alpha_3 d + ... + \alpha_k d^{k-2}.$$

Da $0 \leq \alpha_i, \beta_i < d$ für alle $2 \leq i \leq k$, handelt es sich auf beiden Seiten der Gleichung um zwei d-adische Darstellungen bezüglich der Basis $\{1, \ldots, d^{k-2}\}$. Die Darstellung bezüglich dieser Art von Basen ist eindeutig, also folgt $\alpha_i = \beta_i$ für alle i. Insgesamt erhalten wir $f = g$ und somit die Injektivität für Monome in V_d. Jede Zahl in der Menge $\{1, ..., d^{k-1} - 1\}$ lässt sich durch eine Darstellung $\alpha_2 + \alpha_3 d + ... + \alpha_k d^{k-2}$ mit $0 \leq \alpha_i < d$ realisieren. Daraus folgt direkt die Surjektivität und damit die Bijektivität von Monomen in V_d auf Monome in W_d. *Schritt 3:* S_d ist ein Homomorphismus von K-Algebren und insbesondere K-linear. Die oben betrachteten Monome bilden K-Basen von V_d beziehungsweise W_d. Es folgt, dass $S_d\big|_{V_d} : V_d \to W_d$ ein Isomorphismus von K-Vektorräumen ist. □

Bemerkung
Da S_d ein Einsetzungshomomorphismus ist, folgt für $f, g \in V_d$ mit $fg \in V_d$

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

3.3 Endlich erzeugte Erweiterungen von Hilbertschen Körpern

In diesem Abschnitt orientieren wir uns Abschnitt 1.1.3 aus [Vö]. Ist K hilbertsch, so existieren per Definition für alle irreduziblen Polynome $f \in K[x,y]$ unendlich viele $b \in K$, sodass f_b stets irreduzibel in $K[y]$ bleibt. Wir wollen uns als erstes mit der Frage auseinandersetzen, ob diese Eigenschaft auch für Polynome mit mehr als zwei Variablen über einem hilbertschen Körper erhalten bleibt. Tatsächlich ist dies so, was wir im folgenden Satz zeigen und sehen werden:

Satz 3.15
Sei K ein hilbertscher Körper und $f \in K[x_1, ..., x_k]$ irreduzibel. Dann existieren unendlich viele $b \in K$, sodass $f(b, x_2, ..., x_k) =: f_b(x_2, \ldots, x_k) \in K[x_2, ..., x_k]$ irreduzibel ist.

Beweis (vgl [CZ], Theorem 4)
Schritt 1: Zuerst fassen wir unser irreduzibles Polynom $f \in K[x_1, \ldots, x_k]$ als Element in $K[x_1][x_2, \ldots, x_k]$ auf, das heißt f lässt sich als endliche Summe von Monomen der Form $a(x_1)x_2^{a_2} \cdot \ldots \cdot x_k^{a_k}$ schreiben mit $a(x_1) \neq 0$. Jeder von Null verschiedene Koeffizient $a(x_1)$ von $f \in K[x_1][x_2, \ldots, x_k]$ besitzt nur endlich viele Nullstellen in K. Insgesamt ist die Vereinigung der Nullstellenmengen der Koeffizienten von f in $K[x_1][x_2, \ldots, x_k]$ endlich und wir betrachten ab jetzt $b \in K$, die nicht in dieser Vereinigung enthalten sind.
Schritt 2: Betrachte nun f wie zu Beginn als Polynom in $K[x_1, \ldots, x_k]$ und sei $d \in \mathbb{Z}$ so gewählt, dass $deg_{x_i}(f) < d$ für alle $i \in \{1, ..., k\}$ gilt. Dann ist $f \in V_d$ und wir betrachten die zugehörige d-Kronecker-Spezialisierung $S_d(f)$. Nun fassen wir unser Polynom $S_d(f) \in K[x,y]$ nach geeigneter Umsortierung der einzelnen Monome als Polynom in der Variablen y mit Koeffizienten in $K[x]$ auf und finden eine eindeutige Primfaktorzerlegung von $S_d(f)$ in $K[x][y]$. Beachte, dass $K[x][y]$ nach dem Lemma von Gauß faktoriell ist. Das bedeutet, dass wir irreduzible Polynome $g_1(x,y), \ldots, g_n(x,y) \in K[x][y]$ und ein $g(x) \in K[x]$ finden mit

$$S_d(f)(x,y) = g(x) \cdot \prod_{i=1}^{n} g_i(x,y).$$

Nach Satz 3.11(ii) finden wir unendlich viele $b \in K$, sodass $g_i(b,y)$ irreduzibel ist für alle $1 \leq i \leq n$. Falls Nullstellen von $g(x)$ in diesen unendlich vielen $b \in K$ enthalten sein sollten, können wir diese entfernen und erhalten weiterhin eine unendliche Menge von Elementen aus K, für die alle $g_i(b,y)$ irreduzibel sind, da $g(x)$ nur endlich viele Nullstellen in K besitzt. Insgesamt erhalten wir dann

$$S_d(f)(b,y) = g(b) \prod_{i=1}^{n} g_i(b,y).$$

Wir nehmen an, dass $f(b, x_2, \ldots, x_k)$ reduzibel ist, sodass nicht konstante Polynome $u, v \in K[x_2, \ldots, x_k]$ existieren mit $f_b = uv$. Wir können f_b, u sowie v als

Elemente in $K[x_1, \ldots, x_k]$ betrachten. Dann sind $u, v \in V_d$ mit $uv = f_b \in V_d$, sodass

$$S_d(u)S_d(v) = S_d(uv) = S_d(f_b) = g(b) \cdot \prod_{i=1}^{n} g_i(b, y)$$

folgt. Wegen der Eindeutigkeit der Primfaktorzerlegungen existiert eine Partition $\{A, B\}$ von $\{1, \ldots, n\}$ und $\alpha, \beta \in K$ mit $\alpha\beta = g(b)$ und

$$S_d(u) = \alpha \prod_{i \in A} g_i(b, y) \text{ und } S_d(v) = \beta \prod_{i \in B} g_i(b, y).$$

Die Mengen A und B können nicht leer sein, weil u und v nicht konstante Polynome sind nach Annahme. An dieser Stelle setzen wir auch

$$U(x, y) := \prod_{i \in A} g_i(x, y) \text{ und } V(x, y) := \prod_{i \in B} g_i(x, y)$$

U und V sind als Teilprodukte von $S_d(f)$ offensichtlich in der Menge W_d enthalten, sodass wir nach der Bijektivität der Abbildung in Proposition 3.14 nicht konstante Polynome $\tilde{u}, \tilde{v} \in V_d$ finden mit $S_d(\tilde{u}) = U$ und $S_d(\tilde{v}) = V$. Anschließend beobachten wir

$$S_d(\tilde{u}_b) = S_d(\tilde{u})(b, y) = U(b, y) = \prod_{i \in A} g_i(b, y) = \alpha^{-1} S_d(u) = S_d(\alpha^{-1} u),$$

wobei in der letzten Gleichung die K-Linearität von S_d verwendet wird. Aus der Injektivität folgt nun, dass $\tilde{u}_b = \alpha^{-1} u$ gilt und mit einer analogen Rechnung erhält man $\tilde{v}_b = \beta^{-1} v$. Daraus erhalten wir

$$\tilde{u}_b \tilde{v}_b = \alpha^{-1}\beta^{-1} uv = (\alpha\beta)^{-1} uv = g(b)^{-1} uv = g(b)^{-1} f(b, x_2, \ldots, x_k).$$

Nun zeigen wir, dass $\tilde{u}\tilde{v} \notin V_d$ ist. Wir nehmen an, dass $\tilde{u}\tilde{v} \in V_d$ ist. Beachten wir, dass das Polynom $g(x) \in K[x]$ ebenfalls in der Menge W_d enthalten ist, so gilt für das Polynom $g(x_1) \in V_d$, dass $S_d(g(x_1)) = g(x)$. Insgesamt ist dann $g\tilde{u}\tilde{v} \in V_d$ und wir erhalten

$$S_d(g(x_1)\tilde{u}\tilde{v}) = S_d(g(x_1))S_d(\tilde{u})S_d(\tilde{v}) = gUV = S_d(f).$$

Aus der Injektivität folgt erneut $f = g\tilde{u}\tilde{v}$, was einen Widerspruch darstellt, weil $\tilde{u}, \tilde{v}$ keine konstanten Polynome in $K[x_1, \ldots, x_k]$ sind und f nicht irreduzibel wäre. Es folgt $\tilde{u}\tilde{v} \notin V_d$ und daher $\tilde{u}_b\tilde{v}_b \notin V_d$.

3. Schritt: Nun betrachten wir unser Polynom f erneut als Element im Polynomring $K[x_1][x_2, \ldots, x_k]$, wobei f als Summe von Monomen der Form $a(x_1)x_2^{a_2} \cdot \ldots \cdot x_k^{a_k}$ geschrieben werden kann. Weil $\tilde{u}\tilde{v}$ nicht in der Menge V_d enthalten ist, müssen $i \in \{2, \ldots, k\}$ und mindestens ein Monom von f existieren, sodass $a_i > d$ und $a(x_1) \neq 0$ gilt. Nun ist aber $\tilde{u}_b\tilde{v}_b = g(b)^{-1} f_b \in V_d$. Damit hier kein Widerspruch entsteht, muss jedes Monom $a(b)x_2^{a_2} \cdot \ldots \cdot x_k^{a_k}$ von f_b mit $a_i > d$ für ein $i \in \{2, \ldots, k\}$ verschwinden, weil f_b sonst nicht in V_d enthalten sein würde. Das bedeutet, dass b eine Nullstelle der Koeffizienten $a(x_1)$ dieser Monome ist. Jedoch haben wir diese im ersten Schritt des Beweises ausgeschlossen. Folglich ist f_b irreduzibel für alle $b \in K$, die nicht Nullstellen der Koeffizienten von f in $K[x_1][x_2, \ldots, x_k]$ sind. □

Abschließend kommen wir nach unserer ganzen Vorarbeit nun zwei Hauptsätzen für hilbertsche Körper. Zum einen erhält man folgendes Resultat:

Satz 3.16
Sei K hilbertsch und $L|K$ eine endlich erzeugte Körpererweiterung. Dann ist L hilbertsch.

Beweis (vgl [Vö], Korollar 1.11)
Schritt 1: Im ersten Schritt betrachten wir eine rein transzendente Körpererweiterung $L := K(x_1, \ldots, x_m)$ über K. Ohne Einschränkung können wir annehmen, dass die transzendenten Elemente $x_1, \ldots, x_m$ eine maximale, algebraisch unabhängige Familie bilden. Wir setzen $D := K[x_1, \ldots, x_m]$ und wählen ein irreduzibles $f(x, y) \in L[x, y]$. Hier können wir ebenfalls ohne Einschränkung annehmen, dass $f \in D[x, y]$ ist und betrachten anschließend f als Element in $L(x)[y]$. Mit Lemma 3.5 folgt, dass f irreduzibel in $L(x)[y]$ ist. Außerdem ist

$$L(x)(y) = K(x_1, \ldots, x_m)(x)(y) \cong K(x_1, \ldots, x_m, x, y),$$

und mit Lemma 3.5 ist f auch irreduzibel in $K[x_1, \ldots, x_m, x, y]$, wenn wir es als Element in diesem Polynomring auffassen. Nach Umsortierung der Variablen existieren mit Satz 3.16 unendlich viele $b \in K$, sodass $f(x_1, \ldots, x_m, b, y) = f_b$ irreduzibel in $K[x_1, \ldots, x_m, y] \cong K[x_1, \ldots, x_m][y] = D[y]$ ist. Insbesondere ist dann f_b dann auch irreduzibel in $L[y]$ nach Lemma 3.5, was wiederum zeigt, dass L hilbertsch ist.
Schritt 2: Nun betrachten wir eine beliebige, endlich erzeugte Körpererweiterung L über K. Aufgrund der Existenz von Transzendentbasen existiert ein Zwischenkörper $K \subseteq L' \subseteq L$, sodass $L'|K$ endlich erzeugt und rein transzendent und $L|L'$ endlich ist. Nach Schritt 1 ist L' hilbertsch und nach Korollar 3.12 ist L hilbertsch. □

Das folgende Hauptresultat dieser Arbeit wird insbesondere in Kapitel 5, in dem wir die symmetrische Gruppe als Galoisgruppe realisieren wollen, von großer Bedeutung sein. Mit unserer Vorarbeit können wir nun Satz 3.8 verallgemeinern und erhalten:

Satz 3.17
Sei K hilbertsch, $m \in \mathbb{N}$ und E eine Galoiserweiterung von $K(x_1, \ldots, x_m)$, wobei $x_1, \ldots, x_m$ algebraisch unabhängig über K sind. Dann existiert eine Galoiserweiterung $L|K$ mit

$$\mathrm{Gal}(E|K(x_1, \ldots, x_m)) \cong \mathrm{Gal}(L|K).$$

Insbesondere lässt sich eine endliche Gruppe G als Galoisgruppe über K realisieren, wenn sie als Galoisgruppe über $K(x_1, \ldots, x_m)$ realisiert werden kann.

Beweis (vgl. [CZ], Theorem 6)
Wir führen eine Induktion nach m durch. Der Fall $m = 1$ wurde in Satz 3.8

bewiesen. Wir nehmen also an, dass die Aussage für ein $m \in \mathbb{N}$ gelten würde. Nun gilt

$$K(x_1, \ldots, x_{m+1}) \cong K(x_1, \ldots, x_m)(x_{m+1})$$

und $K(x_1, \ldots, x_m)$ ist nach Satz 3.17 hilbertsch. Nach Satz 3.8 existiert eine Galoiserweiterung $E'|K(x_1, \ldots, x_m)$ mit

$$\mathrm{Gal}(E|K(x_1, \ldots, x_{m+1})) \cong \mathrm{Gal}(E'|K(x_1, \ldots, x_m)).$$

Nach Induktionsvorraussetzung existiert eine Galoiserweiterung $L|K$ mit

$$\mathrm{Gal}(E'|K(x_1, \ldots, x_m)) \cong \mathrm{Gal}(L|K).$$

Fügt man beides zusammen, erhält man

$$\mathrm{Gal}(E|K(x_1, \ldots, x_{m+1})) \cong \mathrm{Gal}(L|K),$$

was den Induktionsschritt abschließt.

□

4 Der Irreduzibilitätssatz von Hilbert

In diesem Abschnitt möchten wir das Haupttheorem dieser Bachelorarbeit, den *Irreduzibilitätssatz von Hilbert*, beweisen, welches wir schon im Vorwort kennengelernt haben. Dafür werden wir uns die zweite, äquivalente Bedingung eines hilbertschen Körpers von Nutzen machen, die man in Satz 3.11(iii) wiederfindet. Wir müssen also für jede Familie von irreduziblen Polynomen $f_1, \dots, f_r \in \mathbb{Q}[x, y]$ mit $\deg_y(f_i) > 1$ für alle $1 \leq i \leq r$, die wir als Polynome in $\mathbb{Q}[x][y]$ aufgefassen, überprüfen, ob unendlich viele $b \in \mathbb{Q}$ existieren, sodass die entsprechenden spezialisierten Polynome $f_{1,b}, \dots, f_{r,b} \in \mathbb{Q}[y]$ keine Nullstellen in $\mathbb{Q}$ besitzen. Wir orientieren uns erneut an [Vö], allerdings an Kapitel 1.2.1 bis Kapitel 1.2.3. Wir beschäftigen uns zuerst mit der sogenannten Analytizität von Nullstellen.

Satz 4.1
Sei $f(x, y) \in \mathbb{C}[x, y]$ mit $deg_y(f) \geq 1$. Sei $c_0 \in \mathbb{C}$ so gewählt, dass $f(c_0, y) \in \mathbb{C}[y]$ separabel ist. Dann existiert eine Umgebung $U(c_0)$ von c_0 und holomorphe Funktionen $\Psi_1, \dots, \Psi_n : U \to \mathbb{C}$, sodass für alle $c \in U(c_0)$ das Polynom $f(c, y)$ die n paarweise verschiedenen Nullstellen $\Psi_1(c), \dots, \Psi_n(c)$ besitzt.

Beweis (vgl. [Vö], Theorem 1.18)
Sind $\gamma_1, \dots, \gamma_n$ die paarweise verschiedenen Nullstellen von f_{c_0}, so müssen die holomorphen Funktionen, die wir im Anschluss konstruieren werden, paarweise verschieden sein, da f_{c_0} separabel ist. Somit genügt es für eine fest gewählte Nullstelle $\gamma := \gamma_i$ die entsprechende holomorphe Funktion zu konstruieren.
1. Schritt: Wir nehmen an, dass $c_0 = \gamma = 0$ gilt. Für die holomorphe Funktion $\Psi : U(0) \to \mathbb{C}$ muss also $\Psi(0) = 0$ und $f(t, \Psi(t)) = 0$ für alle $t \in U(0)$ gelten. Da holomorphe Funktionen analytisch sind, finden wir eine Potenzreihe mit Koeffizienten in $\mathbb{C}$, etwa

$$\Psi(t) = \sum_{i=0}^{\infty} a_i t^i,$$

die in jedem Punkt $u \in U(0)$ um den Entwicklungspunkt 0 gegen $\Psi(u)$ konvergiert. Aus $f(0, 0) = 0$ folgt, dass f von der Form

$$f(x, y) = ax + by + \text{Terme höherer Ordnung}$$

sein muss. Hierbei ist zu beachten, dass $b = (\partial f/\partial y)(0, 0) \neq 0$ ist, weil 0 eine einfache Nullstelle von $f(0, y)$ ist. Durch Multiplikation von f mit b^{-1} können wir ohne Einschränkung annehmen, dass $b = 1$ gilt. Wir definieren das Polynom

$$g(x, y) := y - f(x, y).$$

g besitzt keinen konstanten Term und ebenfalls keinen Term der Form ay. Außerdem gilt für jedes $t \in U$

$$g(t, \Psi(t)) = \Psi(t) - f(t, \Psi(t)) = \Psi(t). \tag{4}$$

Schreiben wir nun unser Polynom $g(x, y)$ in der Form

$$g(x,y) = \sum_{\substack{0 \le v_1 \le m \\ 0 \le v_2 \le n}} a_{v_1 v_2} x^{v_1} y^{v_2}$$

so können wir mit Hilfe von (4) die Koeffizienten von $\Psi(t)$ rekursiv bestimmen, indem wir $g(t, \Psi(t))$ als formale Potenzreihe um den Punkt 0 entwickeln. Da $\Psi(0) = 0$ ist, müssen wir also

$$g(t,\Psi(t)) = \sum_{\substack{0 \le v_1 \le m \\ 0 \le v_2 \le n}} a_{v_1 v_2} t^{v_1} (\sum_{i=1}^{\infty} a_i t^i)^{v_2} \stackrel{!}{=} \sum_{i=1}^{\infty} a_i t^i = \Psi(t) \tag{5}$$

lösen. Beachte, dass $a_{00} = a_{01} = 0$ gilt. Wir zeigen per Induktion nach $i \ge 1$, das Polynome $h_i = h_i(x_{00}, \ldots, x_{v_1 v_2}) \in \mathbb{Z}[x_{00}, \ldots, x_{v_1 v_2}]$ existieren, sodass $a_i = h_i(a_{00}, \ldots, a_{v_1 v_2})$ gilt, wobei $v_1, v_2 \ge 0$ und $v_1 + v_2 \le i$ erfüllt sind. Zudem sind die Koeffizienten von h_i nicht-negativ und h_i ist insbesondere ein Polynom in endlich vielen Variablen für alle i.
Für den Induktionsanfang $i = 1$ suchen wir auf der linken Seite der Gleichung (5) den Koeffizienten für t^1. Aus $a_0 = 0$ folgt, dass der niedrigste Term von $(\sum_{i=1}^{\infty} a_i t^i)^{v_2}$ vom Grad v_2 für $v_2 \ge 0$ ist. Damit folgt, dass $v_1 + v_2 \le 1$ gelten muss, sodass nur die Fälle [$v_1 = 0$ und $v_2 = 1$] oder [$v_1 = 1$ und $v_2 = 0$] in Frage kommen. Im ersten Fall erhalten wir den Koeffizienten $a_{01} a_1 = 0$, da $a_{01} = 0$ ist. Im zweiten Fall erhalten wir den Koeffizienten a_{10}. Insgesamt folgt $a_1 = a_{10}$ und man kann $h_1(x_{00}, x_{01}, x_{10}) := x_{10} \in \mathbb{Z}[x_{00}, x_{01}, x_{10}]$ definieren. Nun nehmen wir an, dass die Aussage für ein $i \in \mathbb{N}$ gelte, das heißt für alle $1 \le j \le i$ existieren Polynome $h_j \in \mathbb{Z}[x_{00}, \ldots, x_{v_{1,j}, v_{2,j}}]$ mit nicht-negativen Koeffizienten, sodass $a_j = h_j(a_{00}, \ldots, a_{v_{1,j} v_{2,j}})$ und $v_{1,j} + v_{2,j} \le j$ erfüllt sind.
Für den Koeffizienten a_{i+1} betrachten wir erneut die linke Seite der Gleichung (5). Beachte nun, dass für fest gewählte $v_1, v_2 \in \mathbb{N}$ im Ausdruck $a_{v_1 v_2} t^{v_1} \cdot (\sum_{i=1}^{\infty} a_i t^i)^{v_2}$ der Term mit minimalem Grad genau Grad $v_1 + v_2$ besitzt, da $a_0 = 0$ gilt. Somit gilt $v_1 + v_2 \le i + 1$, wenn wir auf der linken Seite von (5) den Koeffizienten von t^{i+1} bestimmen wollen. Ebenso kann der Koeffizient a_{i+1} nicht als Koeffizient von t^{i+1} auf der linken Seite der Gleichung auftauchen, da $a_{01} = 0$ ist. Es folgt, dass a_{i+1} als Summe von Elementen der Form $a_{mn} a_1^{j_1} \cdot \ldots \cdot a_i^{j_i}$ mit geeigneten $m, n, j_1, \ldots, j_i \in \mathbb{N}$ geschrieben werden kann, wobei $m + n \le i + 1$ immer erfüllt sein muss. Nach Induktionsvoraussetzung existiert für jeden Koeffizienten a_j mit $1 \le j \le i$ ein Polynom $h_j \in \mathbb{Z}[x_{00}, \ldots, x_{v_{1,j} v_{2,j}}]$ mit $v_{1,j} + v_{2,j} \le j$ und $a_j = h_j(a_{00}, \ldots, a_{v_{1,j} v_{2,j}})$. Wir fassen die Polynome $h_1, \ldots, h_i$ als Polynome in $\mathbb{Z}[x_{00}, \ldots, x_{v_1 v_2}]$ auf. Für jeden Summanden $a_{mn} a_1^{j_1} \cdot \ldots \cdot a_i^{j_i}$ von a_{i+1} definiere nun das entsprechende Polynom $x_{mn} h_1^{j_1} \cdot \ldots \cdot h_i^{j_i} \in \mathbb{Z}[x_{00}, \ldots, x_{v_1 v_2}]$ und h_{i+1} als die Summe dieser Polynome. Nach Konstruktion ist $h_{i+1}(a_{00}, \ldots, a_{v_1 v_2}) = a_{i+1}$. Jedes h_j besitzt nur nicht-negative Koeffizienten, sodass h_{i+1} ebenso ein Polynom mit nicht-negativen Koeffizienten in $\mathbb{Z}$ ist, was diese Induktion abschließt und die rekursive Darstellung der Koeffizienten von $\Psi(t)$ zeigt.
Nun gilt es noch zu zeigen, dass $\Psi(t)$ einen positiven Konvergenzradius besitzt. Sei C eine positive Konstante mit $|a_{v_1 v_2}| \le C$ für alle $(v_1, v_2) \in \{0, \ldots, m\} \times$

$\{0, \ldots, n\}$. Dann definieren wir die rationale Funktion

$$\tilde{g}(t,u) := C(-1-u+\frac{1}{(1-t)(1-u)}).$$

Lösen wir die Gleichung $u = \tilde{g}(t,u)$ nach u in Abhängigkeit von t, erhalten wir

$$u_1(t) = \frac{1}{2(C+1)}(1+\frac{\sqrt{4Ct(Ct-C+t-1)+(1-t)^2}}{t-1}),$$

$$u_2(t) = \frac{1}{2(C+1)}(1-\frac{\sqrt{4Ct(Ct-C+t-1)+(1-t)^2}}{t-1}).$$

Es folgt $u_1(0) = 0$ und $u_2(0) = 2$, wenn wir eine geeignete Umgebung für die Wurzelfunktion wählen, sodass $\sqrt{1} = 1$ gilt. Dementsprechend ist u_1 eine holomorphe Funktion, definiert in einer offenen Umgebung $U(0)$ um den Punkt 0, die zugleich

$$u_1(t) = \tilde{g}(t, u_1(t)) \tag{6}$$

erfüllt. Für $|t| < 1$ und $|u| < 1$ erhalten wir nach der geometrischen Reihe

$$\begin{aligned}\tilde{g}(t,u) &= C(-1-u+\frac{1}{(1-t)(1-u)}) \\ &= C(-1-u+(\sum_{k=0}^{\infty} t^k)\cdot(\sum_{h=0}^{\infty} u^h)) \\ &= C(-1-u+\sum_{\substack{k=0\\h=0}}^{\infty} t^k u^h),\end{aligned}$$

weil beide Reihen absolut konvergieren und nach der Cauchy-Produktformel miteinander multipliziert werden dürfen. Wir schreiben $u_1(t) = \sum_{i=0}^{\infty} b_i t^i$ mit geeigneten Koeffizienten aus $\mathbb{C}$. Aus (6) folgt, dass $\tilde{g}$ und u_1 dieselbe formale Gleichung erfüllen wie g und Ψ. Wir können also zur Darstellung des Koeffizienten b_i dasselbe Polynom h_i wählen. Da C nicht-negativ ist und alle Koeffizienten von $\tilde{g}$ gleich C sind, folgt $b_i = h_i(C, \ldots, C)$. Nun besitzen alle Polynome h_i nicht-negative Koeffizienten, sodass für $v_1 + v_2 \leq i$ nach der Dreiecksungleichung

$$|a_i| = |h_i(a_{00}, \ldots, a_{v_1 v_2})| \leq h_i(|a_{00}|, \ldots, |a_{v_1 v_2}|) \leq h_i(C, \ldots, C) = b_i$$

gilt. Da u_1 als holomorphe Funktion in $U(0)$ absolut konvergiert, folgt aus dem Majorantenkriterium die absolute Konvergenz von Ψ in $U(0)$.
Schritt 2: Im allgemeinen Fall ersetze $f(x,y)$ durch $f(x+c_0, y+\gamma)$, wobei γ eine Nullstelle von $f(c_0,y)$ ist. Betrachte hierfür die entsprechende Funktion Ψ : $U(0) \to \mathbb{C}$ aus Schritt 1 und ersetze sie durch

$$\overline{\Psi} : U(0) + c_0 \to \mathbb{C},\ \overline{\Psi}(x+c_0) := \overline{\Psi}(x) + \gamma.$$

□

Bemerkung
In diesem Beweis wurden die holomorphen Funktionen algebraisch konstruiert. Mit Hilfe des Satzes über implizite Funktionen kann man diesen Satz folgendermaßen unmittelbar folgern: Wir wählen $f \in \mathbb{C}[x,y]$ und $c_0 \in \mathbb{C}$ so, dass das spezialisierte Polynom $f(c_0,y) = f_{c_0}(y) \in \mathbb{C}[y]$ separabel ist. Dann besitzt f_{c_0} nur einfache Nullstellen in $\mathbb{C}$, und für jede Nullstelle γ gilt

$$\frac{\partial f_{c_0}}{\partial y}(\gamma) = \frac{\partial f}{\partial y}(c_0,\gamma) \neq 0,$$

da f_{c_0} separabel ist. Somit kann man den Satz über implizite Funktionen für holomorphe Funktionen anwenden und es existieren offene Umgebungen $U(c_0), U'(\gamma) \subset \mathbb{C}$ um c_0 und γ und eine holomorphe Abbildung $\Psi : U \to U'$ mit $\Psi(c_0) = \gamma$ und $f(c,\Psi(c)) = 0$ für alle $c \in U$.

Definition 4.2
Sei $M \subset \mathbb{N}$. M heißt *karg*, wenn eine reelle Zahl $\kappa \in (0,1)$ existiert, sodass

$$|M \cap \{1,\dots,n\}| \leq n^{\kappa}$$

für alle bis auf endlich viele $n \in \mathbb{N}$ gilt.

Proposition 4.3
Seien $M, M_1, \dots, M_n \subset \mathbb{N}$.

(i) Ist M eine endliche Teilmenge von $\mathbb{N}$, so ist M karg.

(ii) Sind $M_1,\dots,M_n$ karg, so ist auch $\bigcup_{i=1}^{n} M_i$ karg.

Beweis (i): Sei $M := \{m_1,\dots,m_n\} \subset \mathbb{N}$ endlich und $N := (\max M)^2$. Dann gilt $|M| \leq N^{1/2}$ und aus der Monotonie der Wurzelfunktion folgt die Behauptung für $N \to \infty$.

(ii): Sind $M_1,\dots,M_n$ karg, so existiert für jedes $1 \leq i \leq n$ ein $\kappa_i \in (0,1)$ und ein $n_i \in \mathbb{N}$, sodass $|M_i \cap \{1,\dots,N\}| < N^{\kappa_i}$ gilt für alle $N > n_i$. Zusätzlich existiert ein $\varepsilon > 0$, sodass $1 - \kappa_i > \varepsilon$ ist für alle i. Setzen wir $\tilde{n} := \max_{1\leq i\leq n} n_i$, so gilt für alle $N > \tilde{n}$

$$|M \cap \{1,\dots,N\}| = |\bigcup_{i=1}^{n} M_i \cap \{1,\dots,N\}| \leq \sum_{i=1}^{n} |M_i \cap \{1,\dots,n\}| < \sum_{i=1}^{n} N^{\kappa_i}.$$

Ist $\kappa := \max_{1\leq i\leq n} \kappa_i$, und N groß genug gewählt, sodass $n < N^{\varepsilon}$, so folgt weiter

$$\sum_{i=1}^{n} N^{\kappa_i} < n \cdot N^{\kappa} < N^{\epsilon} \cdot N^{\kappa} = N^{\epsilon+\kappa}.$$

Für $\kappa' := \epsilon + \kappa < 1$ folgt die Behauptung.

□

Satz 4.4
Sei $i_0 \in \mathbb{Z}$ und $\phi(t) = \sum_{i=i_0}^{\infty} a_i t^i$ eine Laurent-Reihe mit Koeffizienten in $\mathbb{C}$, die in einer punktierten, offenen Umgebung $U(0)\backslash\{0\} \subset \mathbb{C}$ um den Punkt 0 konvergiert. Sei

$$B(\phi) := \{b \in \mathbb{N} \mid \frac{1}{b} \in U(0) \text{ und } \phi(1/b) \in \mathbb{Z}\} \subset \mathbb{N}.$$

Dann ist B karg, sofern ϕ kein Laurant-Polynom ist.

Für den Beweis des Satzes benötigen wir:

Lemma 4.5
Sei $m \in \mathbb{N}_{>0}$, $t_0 < t_1 < \ldots < t_m$ reelle Zahlen und $f : [t_0, t_m] \to \mathbb{R}$ eine m-mal differenzierbare Funktion mit m-ter Ableitung $f^{(m)}$. Zusätzlich definieren wir

$$V_m := det(\begin{pmatrix} 1 & t_0 & \cdots & t_0^m \\ 1 & t_1 & \cdots & t_1^m \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_m & \cdots & t_m^m \end{pmatrix}) = \prod_{i>j} (t_i - t_j)$$

und

$$W_m := det(\begin{pmatrix} 1 & t_0 & \cdots & t_0^{m-1} & f(t_0) \\ 1 & t_1 & \cdots & t_1^{m-1} & f(t_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & t_m & \cdots & t_m^{m-1} & f(t_m) \end{pmatrix}).$$

Dann existiert ein $u \in (t_0, t_m)$, sodass

$$\frac{W_m}{V_m} = \frac{f^{(m)}(u)}{m!}.$$

Beweis (vgl. [CZ], Lemma 4)
Sei $g : [t_0, t_m] \to \mathbb{R}$ eine m-mal differenzierbare Funktion mit $g(t_i) = f(t_i)$ für alle $0 \leq i \leq m$. Dann ist $(g-f)(t_i) = (g-f)(t_{i+1}) = 0$ für alle $0 \leq i \leq m-1$. Nach dem Satz von Rolle, angewendet auf jedes Teilintervall (t_i, t_{i+1}) mit $i \in \{0, \ldots, m-1\}$, existiert $a_i \in (t_1, t_{i+1})$ mit $(g-f)^{(1)}(a_i) = 0$, also $g^{(1)}(a_i) = f^{(1)}(a_i)$. Wir erhalten m Punkte $a_0 < a_1 < \ldots < a_{m-1}$ mit $g^{(1)}(a_i) = f^{(1)}(a_i)$ für alle i. Wir wenden den Satz von Rolle erneut auf die Teilintervalle (a_i, a_{i+1}) an und erhalten $m-1$ Punkte $b_0 < \ldots < b_{m-2}$ mit $g^{(2)}(b_i) = f^{(2)}(b_i)$ für alle $0 \leq i \leq m-2$. Nach m-maligem Anwenden erhalten wir einen Punkt $u \in (t_0, t_m)$ mit $g^{(m)}(u) = f^{(m)}(u)$. Betrachte das lineare Gleichungssystem

$$\underbrace{\begin{pmatrix} 1 & t_0 & \cdots & t_0^m \\ 1 & t_1 & \cdots & t_1^m \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_m & \cdots & t_m^m \end{pmatrix}}_{=:A} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} f(t_0) \\ f(t_1) \\ \vdots \\ f(t_m) \end{pmatrix}.$$

Weil $t_i \neq t_j$ ist für $i \neq j$, gilt $det(A) = V_m = \prod_{i>j}(t_i - t_j) \neq 0$, sodass das Gleichungssystem eine eindeutige Lösung besitzt. Setzen wir $g(t) := \sum_{i=0}^{m} a_i t^i$, so ist g das eindeutig bestimmte Polynom von Grad kleiner gleich m mit $g(t_i) = f(t_i)$ für alle $0 \leq i \leq m$. Wie wir zuvor gesehen haben existiert ein $u \in (t_0, t_m)$ mit $f^{(m)}(u) = g^{(m)}(u) = m! \cdot a_m$, woraus

$$a_m = \frac{f^{(m)}(u)}{m!}$$

folgt. Nach der Cramerschen Regel, angewendet auf die letzte Spalte der Matrix A, folgt

$$a_m = \frac{W_m}{V_m},$$

was zu zeigen war. □

Beweis von Satz 4.4 (vgl. [Vö], Theorem 1.21)
Sei $\phi(t)$ eine Laurent-Reihe wie in Satz 4.4 gegeben. Zusätzlich nehmen wir an, dass $\phi(t)$ kein Laurent-Polynom ist.
Ist $B(\phi)$ endlich, so ist $B(\phi)$ nach Proposition 4.3(i) automatisch karg, sodass wir ohne Einschränkung annehmen, dass $B(\phi)$ eine unendliche Teilmenge von $\mathbb{N}$ ist.
Schritt 1: (vgl. [JLY], Seite 71, Zeile 2-4)
Wir behaupten, dass die Koeffizienten a_i von $\phi(t)$ reell sind.
Beweis: Angenommen $\phi(t)$ sei nicht reell, dann existiert ein minimales $j \in \mathbb{Z}$ mit $a_j \notin \mathbb{R}$. Da $B(\phi)$ eine unendliche Teilmenge von $\mathbb{N}$ ist, finden wir eine Folge $(b_n)_{n\in\mathbb{N}} \subset B(\phi)$ mit $b_n \to \infty$ für $n \to \infty$. Dann gilt aber

$$0 = \mathrm{Im}(\phi(\frac{1}{b_n}) \cdot b_n^j) = \mathrm{Im}(a_j + a_{j+1}\frac{1}{b_n} + \ldots) \overset{n\to\infty}{\to} \mathrm{Im}(a_j) \neq 0,$$

was einen Widerspruch darstellt, da die Nullfolge natürlich gegen 0 konvergiert. Es folgt, dass

$$\chi(s) := \phi(\frac{1}{s}) = \sum_{i=i_0}^{\infty} a_i s^{-i}$$

eine reellwertige Funktion für hinreichend große $s \in \mathbb{R}$ ist (sodass $1/s \in U(0)$).
Schritt 2: Wir behaupten folgende Aussage: *Es existiert ein $\lambda > 0$ und $m, S \in \mathbb{N}$, sodass für alle $s_0 \ldots, s_m \in \mathbb{Z}$ mit $\chi(s_0), \ldots, \chi(s_m) \in \mathbb{Z}$ und $S < s_0 < \ldots < s_m$ gilt, dass*

$$s_m - s_0 \geq s_0^{\lambda}.$$

Beweis: Sei $m > i_0$ gewählt. Dann hat die m-te Ableitung

$$\chi^{(m)}(s) = \sum_{i=n}^{\infty} d_i s^{-i}$$

nur noch Terme mit negativen Exponenten, das heißt $n \geq 0$. Da ϕ kein Laurent-Polynom ist, können wir $d_n \neq 0$ annehmen. Dann gilt

$$s^n \cdot \chi^{(m)}(s) = d_n + d_{n+1}\frac{1}{s} + \ldots \to d_n \text{ für } s \to \infty,$$

und aufgrund der Dreiecksungleichung existiert ein $S > 0$ mit

$$0 < |s^n \chi^{(m)}(s)| < |2d_n|$$

für alle $s \geq S$. Wählen wir $s_0, \ldots, s_m$ wie in der Behauptung vorgegeben, so existiert nach Lemma 4.5 ein Element $u \in (s_0, s_m)$ mit

$$W_m = \frac{V_m \chi^{(m)}(u)}{m!}.$$

Weil $s_i \neq s_j$ und $\chi(s_0), \ldots, \chi(s_m) \in \mathbb{Z}$ sind, ist $W_m \in \mathbb{Z}\backslash\{0\}$, also $|W_m| \geq 1$. Daraus ergibt sich $V_m \geq 1/|\chi^{(m)}(u)|$ und wir erhalten

$$(s_m - s_0)^{\frac{(m+1)(m+2)}{2}} \geq \prod_{i>j}(s_i - s_j) = V_m \geq \frac{1}{|\chi^{(m)}(u)|} \geq \frac{1}{|2d_n|}u^n \geq \frac{1}{|2d_n|}s_0^n$$

beziehungsweise

$$s_m - s_0 \geq (\frac{1}{|2d_n|})^{\frac{2}{(m+1)(m+2)}} s_0^{\frac{2n}{(m+1)(m+2)}}.$$

Durch Vergrößerung von S dürfen wir ohne Einschränkung $(\frac{1}{2|d_n|})^{1/n} \geq (\frac{1}{S})^{\frac{1}{2}}$ annehmen. Für $\lambda := \frac{n}{(m+1)(m+2)}$ gilt dann

$$s_m - s_0 \geq (\frac{1}{2|d_n|})^{\frac{2\lambda}{n}} s_0^{2\lambda} \geq (\frac{1}{S})^{\lambda} \cdot s_0^{2\lambda} \geq (\frac{1}{s_0})^{\lambda} \cdot s_0^{2\lambda} = s_0^{\lambda}$$

und die Behauptung folgt.
Schritt 3: Sei $\lambda > 0$ gegeben und $b_1 < b_2 < \ldots$ eine unendliche Folge von natürlichen Zahlen, sodass $b_{i+1} - b_i \geq b_i^{\lambda}$ ist für alle $i \in \mathbb{N}$. Dann ist die Menge $B := \{b_1, b_2, \ldots\}$ karg.
Beweis: Für jede natürliche Zahl $N \in \mathbb{N}$ definieren wir

$$N' := |\{b \in B \mid \sqrt{N} < b \leq N\}| < \infty$$

und schreiben $\{b \in B \mid \sqrt{N} < b \leq N\} = \{b_k, b_{k+1}, \ldots, b_{k+N'-1}\}$. Dann folgt aus der Monotonie der Funktion $(\cdot)^{\lambda}$

$$\begin{aligned}(N'-1)\sqrt{N}^{\lambda} &< \sum_{m=0}^{N'-2} b_{k+m}^{\lambda} \\ &\leq \sum_{m=0}^{N'-2} (b_{k+m+1} - b_{k+m} = \\ &= b_{k+N'-1} - b_K \\ &\leq b_{k+N'-1} < N\end{aligned}$$

beziehungsweise

$$N' - 1 < N^{1-\frac{\lambda}{2}}.$$

Daraus folgt nun, dass

$$|B \cap \{1, \ldots, N\}| \leq \sqrt{N} + N' \leq \sqrt{N} + N^{1-\frac{\lambda}{2}} + 1 < N^{\kappa}$$

für $N > 1$, sofern κ hinreichend nah an 1 ist. Somit folgt die Behauptung.
Schritt 4: Nun zeigen wir, dass $B(\phi) \subset \mathbb{N}$ karg ist.
Beweis: Zuerst eliminieren wir alle $b \in B(\phi)$ mit $b \leq S$, wobei S wie in Schritt 2 gewählt ist. Bei dieser Teilmenge von $B(\phi)$ handelt es sich um eine endliche Teilmenge, welche wiederum nach Proposition 4.3 karg ist. Außerdem bewirkt Schritt 2, dass wir die verbleibenden Elemente aus $B(\phi)$ nach geeigneter Sortierung als Vereinigung von m Teilmengen schreiben können, die alle nach Schritt 3 karg sind. Da alle Teilmengen, die wir hier betrachtet haben, karg sind, folgt mit Proposition 4.3(ii), dass auch $B(\phi)$ karg sein muss. □

Lemma 4.6
Sei $p(x, y) \in \mathbb{Q}[x][y]$ ein Polynom in der Variablen y, irreduzibel über $\mathbb{Q}(x)$ mit $\deg(p) =: r > 1$. Dann gilt für alle bis auf endlich viele $x_0 \in \mathbb{Z}$:

(a) Es existiert ein $\varepsilon > 0$ und holomorphe Funktionen $\Psi_1(t), \ldots, \Psi_r(t)$, sodass $\Psi_1(t), \ldots, \Psi_r(t)$ die Nullstellen des Polynoms $P(x_0+t, y) \in \mathbb{Q}[y]$ sind. Dabei sind die holomorphen Funktion $\Psi_i(t)$ für komplexe Zahlen $t \in \mathbb{C}$ mit $|t| < \epsilon$ definiert.

(b) Ist $\Psi_i(t)$ eine rationale Funktion (mit komplexen Koeffizienten) für ein $i \in \{1, \ldots, r\}$, so existieren nur endlich viele $q \in \mathbb{Q}$ mit $\Psi_i(q) \in \mathbb{Q}$.

(c) Sei $B(p, x_0) := \{b \in \mathbb{N} \mid p(x_0 + \frac{1}{b}, c) = 0 \text{ für ein } c \in \mathbb{Q}\}$. Dann ist $B(p, x_0)$ karg.

Beweis (vgl. [Vö], Lemma 1.22)
Zunächst folgt aus der Irreduzibilität von $p(x, y)$ über $\mathbb{Q}(x)[y]$ die Separabilität, weil $\mathbb{Q}(x)$ perfekt ist. Nach Lemma 3.6 gilt für fast alle $x_0 \in \mathbb{Z}$,dass $p(x_0, y)$ separabel in $\mathbb{Q}[y]$ ist. Betrachte im Folgenden ein solches $x_0 \in \mathbb{Z}$.
Die Behauptung (a) ist eine direkte Folgerung aus Satz 4.1.
Für (b) wählen wir zunächst ein $i \in \{1, \ldots, r\}$, sodass $\Psi_i(t)$ eine rationale Funktion ist und setzen $\Psi := \Psi_i$. Dann ist nach (a) $p(x_0 + t, \Psi(t)) = 0$ für alle t mit $|t| < \varepsilon$. Da $p(x_0 + t, \Psi(t))$ eine rationale Funktion in t ist, ergibt sich daraus unmittelbar $p(x_0 + x, \Psi(x)) = 0$ in $\mathbb{C}(x)$, wobei x transzendent über $\mathbb{C}$ ist. Da $p(x + x_0, y) \in \mathbb{Q}(x)[y]$ ungleich Null ist, ist $\Psi(x)$ algebraisch über $\mathbb{Q}(x)$, und ebenso über $\bar{\mathbb{Q}}(x)$, weil $\overline{\mathbb{Q}}(x)|\mathbb{Q}(x)$ algebraisch ist. Aber $\overline{\mathbb{Q}}(x)$ ist algebraisch abgeeschlossen in $\mathbb{C}(x)$ (vgl. [Vö], Lemma 1.1(ii)), sodass $\Psi(x) \in \overline{\mathbb{Q}}(x)$ sein muss.
Sei nun $\sigma \in Gal(\overline{\mathbb{Q}}|\mathbb{Q})$. Schreiben wir $\Psi(x) = f(x)/g(x)$, wobei $f(x), g(x) \in \overline{\mathbb{Q}}(x)$ sind und $g(x) \neq 0$ gilt, so definieren wir $\Psi^\sigma := \sigma(f)/\sigma(g) \in \overline{\mathbb{Q}}(x)$. Dann ist $\Psi^\sigma(q) = \Psi(q)$ für alle $q \in \mathbb{Q}$ mit $\Psi(q) \in \mathbb{Q}$. Nehmen wir an, dass es unendlich viele solcher $q \in \mathbb{Q}$ gibt, so folgt nach dem Identitätssatz für holomorphe Funktionen, dass $\Psi^\sigma = \Psi$ sein muss. Da σ beliebig gewählt wurde, folgt die Gleichheit für alle $\sigma \in Gal(\overline{\mathbb{Q}}|\mathbb{Q})$, woraus $\Psi \in \mathbb{Q}(x)$ folgt. Dann ist aber $p(x, \Psi(x - x_0)) = 0$, was der Irreduzibilität von $p(x, y)$ über $\mathbb{Q}(x)$ widerspricht, weil der Grad von p größer als 1 ist. Also muss die Anzahl der oben betrachteten $q \in \mathbb{Q}$ endlich sein, und die Behauptung in (b) ist gezeigt.
Nun kommen wir zu (c). Wir können wegen Proposition 4.3(i) erneut ohne Ein-

schränkung annehmen, das $B(p, x_0) \subset \mathbb{N}$ eine unendliche Teilmenge ist. Nach Multiplikation mit einem geeigneten Element $a \in \mathbb{Q}$ können wir ebenfalls ohne Einschränkung annehmen, dass $p(x, y) \in \mathbb{Z}[x][y]$ ist. Also finden wir für $p(x, y)$ eine Darstellung

$$p(x, y) = \sum_{i=0}^{r} p_i(x) y^i,$$

wobei $p_i(x) \in \mathbb{Z}[x]$ für alle $1 \leq i \leq r$ und $p_r(x) \neq 0$. Für die rationale Funktion $p(x_0 + \frac{1}{x}, y)$ existiert ein hinreichend großes $R > 0$, sodass

$$x^R p(x_0 + \frac{1}{x}, y) = \sum_{i=0}^{r} \underbrace{x^R p_i(x_0 + \frac{1}{x})}_{=:p_i'(x)} y^i \in \mathbb{Z}[x][y]$$

ist. Insbesondere ist $p_r'(x) \neq 0$ in $\mathbb{Z}[x]$. Wir definieren

$$p'(x, y) := y^r + \sum_{i=0}^{r-1} p_i'(x) p_r'(x)^{r-i-1} y^i \in \mathbb{Z}[x][y].$$

Wähle $b \in B(p, x_0)$ und ein zugehöriges $c \in \mathbb{Q}$ mit $p(x_0 + \frac{1}{b}, c) = 0$. Dann ist

$$\begin{aligned} p'(b, p_r'(b)c) &= (p_r'(b)c)^r + \sum_{i=0}^{r-1} p_i'(b) p_r'(b)^{r-i-1} \cdot (p_r'(b)c)^i \\ &= p_r'(b)^{r-1} \cdot (p_r'(b)c^r + \sum_{i=0}^{r-1} p_i'(b)c^i) \\ &= p_r'(b)^{r-1} \cdot b^R \cdot p(x_0 + \frac{1}{b}, c) = 0. \end{aligned}$$

Weil $p'(b, y) \in \mathbb{Z}[y]$ normiert ist, muss $p_r'(b)c$ ganz über $\mathbb{Z}$ sein. Jedoch ist $p_r'(b)c \in \mathbb{Q}$ und somit ein Element aus $\mathbb{Z}$, da $\mathbb{Z}$ ganzabgeschlossen ist.
Nehmen wir nun an, dass $|\frac{1}{b}| < \varepsilon$ ist, so existiert nach (a) ein $i \in \{1, \ldots, r\}$ und eine holomorphe Funktion $\Psi_i(t)$ mit $c = \Psi_i(\frac{1}{b})$, sodass insbesondere $p_r'(b)\Psi_i(\frac{1}{b}) \in \mathbb{Z}$ gilt.
Für $0 < |t| < \varepsilon$ und $1 \leq i \leq r$ setzen wir nun $\phi_i(t) := p_r'(t^{-1})\Psi_i(t)$. Für $b \in B(p, x_0)$ mit $|\frac{1}{b}| < \epsilon$ existiert also ein i mit $1 \leq i \leq r$, sodass $\phi_i(\frac{1}{b}) = h(b)\Psi_i(\frac{1}{b}) \in \mathbb{Z}$ ist. Da nur endlich viele $b \in \mathbb{N}$ existieren, sodass $|\frac{1}{b}| \geq \varepsilon$ ist, gilt

$$B(p, x_0) \subset \bigcup_{i=1}^{r} B(\phi_i),$$

wobei die Mengen $B(\phi_i)$ wie Satz 4.4 definiert sind. Wir unterscheiden nun zwei Fälle:

(1) Ist ϕ_i eine rationale Funktion, so ist $B(\phi_i)$ nach (b) endlich und somit insbesondere karg nach Proposition 4.3(i).

(2) Ist ϕ_i keine rationale Funktion, so kann ϕ_i insbesondere kein Laurent-Polynom sein. Somit ist $B(\phi_i)$ karg nach Satz 4.4. Mit Proposition 4.3(ii) folgt, dass die endliche Vereinigung der Mengen $B(\phi_i)$ ebenfalls karg sein muss.

Insgesamt folgt die Behauptung in (c).

□

Nun haben wir alle Hilfsmittel bewiesen, um das Hauptresultat dieser Bachelorarbeit beweisen zu können:

Der Irreduzibilitätssatz von Hilbert 4.7
Der Körper $\mathbb{Q}$ ist hilbertsch.

Beweis (vgl. [Vö], Theorem 1.23)
Sei $p_1(x,y),\dots,p_r(x,y) \in (\mathbb{Q}[x])[y]$ eine endliche Familie von irreduziblen Polynomen mit $\deg(p_i) > 1$ für alle $1 \le i \le r$. Nach Lemma 4.6 existieren unendlich viele $x \in \mathbb{Z}$, sodass die Behauptungen (a) - (c) auf $p_i(x,y)$ zutreffen für alle $1 \le i \le r$. Sei $x_0 \in \mathbb{Z}$ so gewählt, dass Lemma 4.6 für alle $p_1(x,y),\dots,p_r(x,y)$ erfüllt ist. Sei C die Menge aller $b \in \mathbb{N}$, sodass keines der spezialisierten Polynome $p_j(x_0 + \frac{1}{b}, y)$ eine Nullstelle in $\mathbb{Q}$ besitzt. Zudem definiere $B := \mathbb{N}\backslash C$. Dann ist nach Lemma 4.6(iii) und Proposition 4.3(ii)

$$B = \bigcup_{i=1}^{r} B(p_i, x_0)$$

karg in $\mathbb{N}$. Daraus folgt unmittelbar, dass C unendlich sein muss. Wäre C endlich, so wäre für $n \ge \max C$ stets $|B \cap \{1,\dots,n\}| = n - |C|$. Gäbe es $\kappa \in (0,1)$ mit $n - |C| < n^\kappa$ für fast alle n, so wäre die Funktion $n \mapsto n - n^\kappa$ beschränkt. Wegen $\kappa > 0$ gilt aber $\lim_{n\to\infty} n^{-\kappa} = 0$, und es würde sich

$$0 = \lim_{n\to\infty} n^{-\kappa}(n - n^{-\kappa}) = \lim_{n\to\infty} (n^{1-\kappa} - 1)$$

ergeben, im Widerspruch zu $\kappa < 1$. Aus Satz 3.11 folgt, dass $\mathbb{Q}$ hilbertsch ist.
□

5 Endliche Gruppen als Galoisgruppen

Für den Körper $\mathbb{Q}$ wissen wir nun, dass sich eine endliche Gruppe insbesondere als Galoisgruppe über $\mathbb{Q}$ realisieren lässt, wenn sie sich als Galoisgruppe über $\mathbb{Q}(x_1, \ldots, x_m)$ realisieren lässt. Als Anwendung geben wir an dieser Stelle ein paar Beispiele.

5.1 Die Symmetrische Gruppe

Als wichtiges Beispiel möchten wir die symmetrische Gruppe S_n für $n \in \mathbb{N}$ als Galoisgruppe über $\mathbb{Q}$ realisieren.

Korollar 5.1
Ist $n \in \mathbb{N}$ und $K|\mathbb{Q}$ eine endlich erzeugte Körpererweiterung, so kann S_n als Galoisgruppe über K realisiert werden. Insbesondere lässt sich S_n als Galoisgruppe über $\mathbb{Q}$ realisieren.

Beweis (vgl. [Vö], Beispiel 1.17)
Da $\mathbb{Q}$ hilbertsch ist, folgt mit Satz 3.17, dass K hilbertsch ist. Betrachte für K die endlich erzeugte Körpererweiterung $K(x_1, \ldots, x_n)$, wobei $x_1, \ldots, x_n$ algebraisch unabhängige Variablen über K sind. Sind $s_1, \ldots, s_n$ die elementarsymmetrischen Polynome in $K[x_1, \ldots, x_n]$, so ist $K(s_1, \ldots, s_n)$ ein Unterkörper von $K(x_1, \ldots, x_n)$. Betrachte das Polynom

$$f(y) = y^n - s_1 y^{n-1} + s_2 y^{n-2} \ldots + (-1)^{n-1} s_{n-1} y + (-1)^n s_n \in K(s_1, \ldots, s_n)[y].$$

Nach Gleichung (1) in Kapitel 2 ist

$$f(y) = \prod_{i=1}^{n} (y - x_i)$$

ein Produkt von Linearfaktoren in $K(x_1, \ldots, x_n)$. Somit ist die Körpererweiterung $K(x_1, \ldots, x_n)|K(s_1, \ldots, s_n)$ galoissch, weil sie der Zerfällungskörper von f ist.
Sei $\sigma \in S_n$. Dann operiert S_n auf der Menge $\{x_1, \ldots, x_n\}$ via

$$\sigma(x_i) := x_{\sigma(i)} \text{ für alle } i \in \{1, \ldots, n\}.$$

Insbesondere operiert jedes $\sigma \in S_n$ dann auf $K(x_1, \ldots, x_n)$ über die Abbildung

$$\varphi_i : K(x_1, \ldots, x_n) \to K(x_1, \ldots, x_n),\ f(x_1, \ldots, x_n) \mapsto \sigma(f) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Offensichtlich sind dies Körperautomorphismen mit $\varphi_i\big|_{K(s_1,\ldots,s_n)} = id_{K(s_1,\ldots,s_n)}$ für alle $1 \leq i \leq n$, was aus der Bemerkung nach Definition 2.1 folgt. Diese bilden eine Untergruppe H von $\mathrm{Gal}(K(x_1, \ldots, x_n)|K(s_1, \ldots, s_n))$, sodass wir den Fixkörper F^H betrachten können. Wegen der Bemerkung nach Definition 2.1 sind $s_1, \ldots, s_n \in F^H$ und es folgt

$$[K(x_1, \ldots, x_n) : F^H] = |H| = |S_n| = n!.$$

Auf der anderen Seite ist aber $K(x_1, \ldots, x_n)$ der Zerfällungskörper von f über $K(s_1, \ldots, s_n)$ und insbesondere gilt

$$[K(x_1, \ldots, x_n) : K(s_1, \ldots, s_n)] \leq n!.$$

Weil F^H ein Zwischenkörper ist, folgt $F^H = K(s_1, \ldots, s_n)$ und damit

$$Gal(K(x_1, \ldots, x_n)|K(s_1, \ldots, s_n)) \cong S_n.$$

Da nun $K(s_1, \ldots, s_n)$ eine endlich erzeugte Körpererweiterung von K ist, folgt mit Satz 3.18, dass sich S_n auch als Galoisgruppe über K realisieren lässt. Setzen wir $K = \mathbb{Q}$, so kann S_n insbesondere als Galoisgruppe über $\mathbb{Q}$ realisiert werden. □

Bemerkung
Der Beweis von Korollar 5.1 funktioniert ebenso für einen beliebigen hilbertschen Körper. Somit lässt sich die symmetrische Gruppe als Galoisgruppe über *jedem* hilbertschen Körper realisieren!

Aus Korollar 5.1 folgert man unmittelbar das folgende Korollar:

Korollar 5.2
Ist G eine endliche Gruppe, so existiert eine endliche Körpererweiterung $k|\mathbb{Q}$, sodass G als Galoisgruppe über k realisiert werden kann.

Beweis Da G endlich ist, existiert ein $n \in \mathbb{N}$ und ein injektiver Gruppenhomomorphismus

$$G \hookrightarrow S_n,$$

sodass G als Untergruppe von S_n aufgefasst werden kann. Nach Korollar 5.1 existiert eine Galoiserweiterung $K|\mathbb{Q}$ mit $Gal(K|\mathbb{Q}) \cong S_n$. Setze nun $k := K^G$. Dann folgt aus der Galoistheorie, dass

$$Gal(K|k) = Gal(K|K^G) \cong G.$$

□

Bemerkung
Es gibt auch elementare Verfahren, um S_n als Galoisgruppe über $\mathbb{Q}$ zu realisieren. Ist $K|\mathbb{Q}$ galoissch mit Galoisgruppe $G := Gal(K|\mathbb{Q})$, so existiert, wie wir im vorherigen Beweis gesehen haben, ein geeignetes $n \in \mathbb{N}$ und ein injektiver Gruppenhomomorphismus φ, sodass G als Untergruppe von S_n aufgefasst werden kann. Wir wenden das Theorem vom primitiven Element an und schreiben $K = \mathbb{Q}[\alpha]$ für ein geeignetes $\alpha \in K$. Sind $\alpha_1, \ldots, \alpha_n$ die Nullstellen des Minimalpolynoms von α über $\mathbb{Q}$, so operiert die Galoisgruppe auf der Menge $\{\alpha_1, \ldots, \alpha_n\}$. Die Operation ist transitiv, das heißt für alle α_i, α_j existiert ein $\sigma \in G$ mit $\sigma(\alpha_i) = \alpha_j$. Das Bild der Galoisgruppe unter φ ist eine transitive Untergruppe von S_n. Um S_n als Galoisgruppe über $\mathbb{Q}$ zu realisieren, gehen wir folgendermaßen vor:

(1) Wir wählen ein normiertes irreduzibles Polynom $f_1 \in \mathbb{F}_2[x]$ vom Grad n.

(2) Seien $g_1, \ldots, g_r \in \mathbb{F}_3[x]$ normiert, irreduzibel und paarweise koprim, wobei der Grad von g_1 gleich 2 und die Grade von $g_2, \ldots, g_r$ ungerade sind. Anschließend wählen wir $f_2 := g_1 \cdot \ldots \cdot g_r \in \mathbb{F}_3[x]$.

(3) Sei $f_3 \in \mathbb{F}_5[x]$ ein normiertes Polynom vom Grad n, dass in $\mathbb{F}_5[x]$ geschrieben werden kann als $f_3 = x \cdot g$, wobei g irreduzibel vom Grad $n-1$ ist.

Wähle nun ein normiertes Polynom $f(x) \in \mathbb{Z}[x]$ mit

$$\begin{aligned} f(x) &\equiv f_1(x) \pmod 2 \\ &\equiv f_2(x) \pmod 3 \\ &\equiv f_3(x) \pmod 5. \end{aligned}$$

Wählt man normierte Lifts $\tilde{f}_i \in \mathbb{Z}[x]$ der f_i, so kann zum Beispiel

$$f := -15\tilde{f}_1 + 10\tilde{f}_2 + 6\tilde{f}_3 \in \mathbb{Z}[x]$$

gewählt werden. Nach (1) ist $f(x)$ insbesondere irreduzibel über $\mathbb{Z}[x]$ und damit irreduzibel über $\mathbb{Q}[x]$ nach dem Lemma von Gauß. Dadurch operiert die Galoisgruppe transitiv auf der Menge der n paarweise verschiedenen Nullstellen von f. Um die Eigenschaften (2) und (3) auszunutzen, machen wir uns Korollar 41 aus [Du] in Kapitel 14.8 zunutze:

Korollar 5.3
(vgl. [DF], Sec. 14.8, Corollary 41)
Sei p prim, $f(x) \in \mathbb{Z}[x]$ mit $p \nmid \Delta_f$ und $\bar{f}(x) := f(x) \bmod p$. Ist

$$\bar{f}(x) = g_1^{n_1} \cdot \ldots \cdot g_k^{n_k}$$

die Zerlegung von $\bar{f}(x)$ in $\mathbb{F}_p[x]$, so enthält die Galoisgruppe des Zerfällungskörpers von $f(x)$ über $\mathbb{Q}$ eine Permutation $\sigma \in S_n$ mit Zyklentyp $(n_1, n_2, \ldots, n_k)$.

Wenden wir nun dieses Korollar auf das Polynom f und die Primzahlen $p = 3$ und $p = 5$ an, so sehen wir, dass die Galoisgruppe von f eine Transposition τ_{ij} an den Stellen i, j und eine Permutation σ mit Zyklentyp $(1, n-1)$ enthalten muss. Hierfür ist zu beachten, dass nach Konstruktion von f die Primzahlen 2, 3 und 5 die Diskriminante von f nicht teilen können. Ferner ist τ_{ij} eine ungerade Potenz des Zyklentyps von f_2, wobei wir verwenden, dass der Grad von g_1 gleich 2 und die Grade von $g_2, \ldots, g_r$ ungerade sind.
Nun gilt es noch zu zeigen, dass eine transitive Untergruppe von S_n, die eine Transposition und einen $(n-1)$-Zyklus enthält, schon ganz S_n ist. Einen Beweis für diese Aussage findet man in zum Beispiel in [We], Lemma A.3.2, Seite 201:
Beweis der Aussage: Wir nennen die transitive Untergruppe H und nennen τ_{ij} die Transposition an den Stellen $i \neq j$, die in H enthalten sein soll. Wir können nach geeigneter Umsortierung ohne Einschränkung annehmen, dass der $(n-1)$-Zyklus

von der Form $c = (2 \dots n)$ ist. Weil H transitiv ist, existiert $\sigma \in H$ mit $\sigma(i) = 1$. Daraus folgt

$$(\sigma\tau_{ij}\sigma_i^{-1})(1) = \sigma(\tau_{ij}(i)) = \sigma(j) =: k,$$

wobei $k \geq 2$ ist, weil $i \neq j$ und $\sigma(i) = 1$ gelten. Nun ist τ_{ij} eine Transposition, sodass die Konjugation $\sigma\tau_{ij}\sigma^{-1} =: \tau$ ebenfalls eine Transposition ist. Nach obiger Rechnung sieht man, dass $\tau = (1k)$ in H enthalten ist, weil σ und τ_{ij} in H enthalten sind. Wegen $c^i\tau c^{-i} = (1c^l(k)) \in H$ und $k \geq 2$ ist $\{(12), (13), \dots, (1n)\} =: H'$ eine Teilmenge von H. Aber H' erzeugt die gesamte Gruppe S_n, was aus

$$\tau_{1k}^{-1}\tau_{1j}\tau_{1k} = \tau_{jk}$$

folgt, und die Behauptung ist gezeigt.

5.2 Weitere Gruppen

Es stellt sich die Frage, welche weiteren endlichen Gruppen als Galoisgruppen über $\mathbb{Q}$ realisiert wurden, welche endlich erzeugte Körpererweiterung von $\mathbb{Q}$ verwendet und welche Polynome dafür betrachtet wurden. Wie sich zeigen wird, sind einige Realisierungen von endlichen Gruppen noch nicht bekannt. Eine gute Übersicht über bisherige Erkenntnisse liefern die Artikel [MZ] und [RR], sowie die Einführung in [JLY], an denen wir uns hier hauptsächlich orientieren werden. Bevor wir den Körper $\mathbb{Q}$ betrachen, werden wir zunächst den Fall des endlichen Körpers $\mathbb{F}_p$ mit Charakteristik p untersuchen. Für alle $n \in \mathbb{N}$ existiert (bis auf Isomorphie) genau ein Körper $\mathbb{F}_{p^n}$ der Charakteristik p mit genau p^n Elementen, sodass

$$[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$$

ist. Insbesondere ist die Körpererweiterung $\mathbb{F}_{p^n}|\mathbb{F}_p$ zyklisch mit Galoisgruppe

$$Gal(\mathbb{F}_{p^n}|\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z},$$

die erzeugt wird durch den Frobenius-Automorphismus. Somit sind alle endlichen zyklischen Gruppen über dem Körper $\mathbb{F}_p$ als Galoisgruppen realisierbar: Um eine zyklische Gruppe der Ordnung n über $\mathbb{F}_p$ zu realisieren, betrachtet man einfach den Zerfällungskörper des Polynoms $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ über $\mathbb{F}_p$.

Nun möchten wir den Körper $\mathbb{Q}$ untersuchen. Wir beginnen mit der Realisierung abelscher Gruppen und betrachten dazu das Kreisteilungspolynom Φ_n für ein $n \in \mathbb{N}$. Es ist bekannt, dass Φ_n das Minimalpolynom jeder primitiven n-ten Einheitswurzel ζ_n ist, und dass $\mathbb{Q}[\zeta_n]|\mathbb{Q}$ Galois ist mit Galoisgruppe $(\mathbb{Z}/n\mathbb{Z})^\times$. Ist nun G eine endliche abeslche Gruppe, so existieren natürliche Zahlen $n_1, \ldots, n_r$ mit

$$G \cong \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}.$$

Nach Dirichlets Satz von der arithmetischen Progression existieren paarweise verschiedene Primzahlen $p_1, \ldots, p_r$ mit $n_i \mid (p_i - 1)$ für $1 \leq i \leq r$. Für $n := \prod_{i=1}^{r} p_i$ lässt sich also G als Quotient

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i\mathbb{Z})^\times \cong \prod_{i=1}^{r} \mathbb{Z}/(p_i - 1)\mathbb{Z} \twoheadrightarrow \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} = G$$

auffassen. Der Hauptsatz der Galoistheorie liefert daher:

Theorem 1 (vgl. [MM1], Part 1 (The Rigidity Method), Theorem 5.1)
Jede endliche abelsche Gruppe G kann als Galoisgruppe über $\mathbb{Q}$ realisiert werden. Dabei kann G als Galoisgruppe eines Unterkörpers von $\mathbb{Q}[\zeta_n]$ realisiert werden, wobei ζ_n eine n-te primitive Einheitswurzel und $n \in \mathbb{N}$ geeignet gewählt sind.

Mit diesem Theorem lassen sich insbesondere alle endlichen, zyklischen Gruppen als Galoisgruppen über $\mathbb{Q}$ realisieren.

Nachdem der Mathematiker D. Hilbert am Ende des 19. Jahrhunderts seinen Irreduzibilitätssatz publiziert hatte, lieferte er 1892 Konstruktionen, mit Hilfe derer er die symmetrische Gruppe S_n (siehe Kapitel 5.1), sowie die alternierende Gruppe A_n (vgl. [MZ], Theorem 1.2) als Galoisgruppen über $\mathbb{Q}$ realisieren konnte. Einen Beweis für die alternierende Gruppe findet man ebenfalls in [Br]. Laut der Autoren der Quelle [MZ] konnte Im Jahr 1930 der Mathematiker I. Schur die ersten expliziten Polynome für die Realisierung der alternierenden Gruppe angeben. Für die alternierende Gruppe betrachtet man den Funktionenkörper $\mathbb{Q}(x)$ und das Polynom

$$p(x,t) := \begin{cases} t^n + \frac{(-1)^{\frac{n-1}{2}} x^2 - n^n}{n-1^{n-1}} & , n \text{ ungerade} \\ t^n + \frac{n^n}{(-1)^{\frac{n}{2}} x^2 + (n-1)^{n-1}} & , n \text{ gerade.} \end{cases}$$

Vergleiche hierzu [JLY], Corollary 3.3.12, Seite 78. Im Jahr 1937 wurden p-Gruppen mit $p > 2$ durch die Mathematiker A. Scholz und H. Reichardt realisiert:

Theorem 2, *veröffentlicht 1937* (vgl. [Sc] und [Re]):
Ist p prim und ungerade, so kann jede endliche p-Gruppe als Galoisgruppe über $\mathbb{Q}$ realisiert werden.

Es können auch allgemeiner auflösbare Gruppen als Galoisgruppen realisiert werden. Dies wurde vom russischen Mathematiker I. Shafarevich behauptet und vollständig im Jahr 1989 bewiesen:

Theorem 3, *korrigiert und bewiesen im Jahr 1989* (vgl. [JLY], Theorem 0.2.3)
Sei G eine endliche auflösbare Gruppe. Dann kann G als Galoisgruppe über $\mathbb{Q}$ realisiert werden.

Einen Beweis für Theorem 3 findet man unter anderem in [NSW], Chapter IX. Im Jahre 2008 konnte der Mathematiker J. Sonn konkrete Polynome für nicht-zyklische, endliche, auflösbare Gruppen angeben:

Theorem 4, *veröffentlicht 2008* (vgl. [So], Theorem 2.2)
[...] [J]ede nicht-zyklische, endliche, auflösbare Gruppe ist für ein Polynom $f \in \mathbb{Q}[x]$ als Galoisgruppe über $\mathbb{Q}$ realisierbar, falls f keine Nullstelle in $\mathbb{Q}$ aber eine Nullstelle in $\mathbb{Q}_p$ besitzt für alle Primzahlen p.

Nach heutigem Kenntnisstand konnten bislang nicht alle nicht-auflösbaren Gruppen über $\mathbb{Q}$ realisiert werden. Es konnten zum Beispiel, wie wir oben gesehen haben, die nicht-auflösbaren Gruppen A_n und S_n für $n \geq 5$ realisiert werden. Auch konnte die Diedergruppe D_{2n} für gewisse $n \in \mathbb{N}$ als Galoisgruppe über $\mathbb{Q}$ über realisiert werden, siehe dazu zum Beispiel [MM1], S. 502-514. Auf diesen Seiten findet man eine tabellarische Darstellung der Realisierung von gewissen endlichen Gruppen als Galoisgruppen über $\mathbb{Q}$, bei der zur Realisierung ein Polynom vom Grad kleiner gleich 15 genutzt werden kann. Eine allgemeine Aussage über Diedergruppen D_{2n} bleibt bisher aus.

Abschließend möchten wir uns noch mit der Realisierung endlicher, einfacher Gruppen beschäftigen. Der Mathematiker Shih konnte im Jahr 1974 die projektiven Gruppen $PSL(2,p)$ für einige ungerade Primzahlen realisieren, jedoch ebenfalls ohne konkrete Konstruktion von Polynomen (vgl. [JLY], Theorem 0.2.5 (a)). Diese wurden später von den Mathematikern Malle und Matzat über $\mathbb{Q}(t)$ konstruiert (vgl. [MM2], Satz 1 Seite 553). Ebenso konnten 25 der 26 einfachen, sporadischen Gruppen als Galoisgruppen über $\mathbb{Q}$ realisiert werden, darunter vier der fünf Mathieu-Gruppen (M_{11}, M_{12}, M_{22} und M_{24}) (vgl. [JLY], Theorem 0.2.6) und die sogenannte Monstergruppe (vgl. [0.2.7], Seite 4, oder [Th]).

Die Realisierung der fehlenden Mathieu-Gruppe M_{23} sowie die Realisierung einfacher Lie-Gruppen sind über $\mathbb{Q}$ nach heutigem Kenntnisstand noch nicht bekannt.

Mit Methoden, die im Rahmen dieser Arbeit nicht behandelt wurden, können noch andere Aussagen getroffen werden. So konnte zum Beispiel in Kapitel 2 aus [Vö] gezeigt werden, dass sich jede endliche Gruppe als Galoisgruppe über $\mathbb{C}(x)$ realisieren lassen kann. Dies wurde in *Riemanns Existenzsatz* festgehalten, welchen man in [Vö] in Theorem 2.13 und Remark 2.14(a) nachlesen kann.

Literatur

[Bo] Bosch, Siegfried: Algebra, 8. Auflage, Springer Verlag, 2013

[Br] Brink, D: On Alternating and Symmetric Groups as Galois Groups. Israel Journal Of Mathematics 142 ,2004: 47-60.

[CZ] Coleman, Rodney, und Laurent Zwald: Hilbertian Fields and Hilbert's Irreducibility Theorem, 2018. Abrufbar unter *https://arxiv.org/abs/1809.10977*, Stand: 18.06.2020

[DF] Dummit, David S., und Foote, Richard M. Abstract Algebra. 3. Auflage, Wiley Internat. ed. Hoboken, NJ: Wiley, 2004.

[JLY] Jensen, Christian U., Ledet, Arne, und Yui, Noriko: Generic Polynomials, Constructive Aspects of the Inverse Galois Problem. Cambridge University, 2002.

[MM1] Malle, Gunter, und Matzat, B. Heinrich. Realisierung von Gruppen $PSL_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$. Mathematische Annalen, 1985, Vol.272(4), S.549-565

[MM2] Malle, Gunter, und Matzat, B. Heinrich. Inverse Galois Theory, 2nd Edition, Springer-Verlag, 2018

[MZ] Michailov, Ivo M., und Nikola P. Ziapkov. On Realizability of p-groups as Galois Groups, 2011. Abrufbar unter *https://arxiv.org/abs/1112.1522*, Stand: 18.06.2020

[NSW] Neukirch, Jürgen, Schmidt, Alexander, und Wingberg, Kay. Cohomology of Number Fields, Springer, 2000.

[Re] Reichardt, Hans. Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung. Journal für die reine und angewandte Mathematik (Crelles Journal), 1937, Vol.1937(177), S.1-5

[RR] Ranjbar, Fariba, und Ranjbar, Saeed: Inverse Galois Problem and Significant Methods, 2015. Abrufbar unter *https://arxiv.org/ftp/arxiv/papers/1512/1512.08708.pdf*, Stand: 18.06.2020

[Sc] Scholz, Arnold. Konstruktion algebraischer Zahlenkörper mit beliebiger Gruppe von Primzahlpotenzordnung I, Math. Z. 42.1, 1937, S.161-168

[So] Sonn, J.: Polynomials with roots in $\mathbb{Q}_p$ for all p, Proc. AMS 136 (2008) 1955-1960. Abrufbar unter *https://arxiv.org/PS_ cache/math/pdf/0612/0612528v4.pdf*. Stand: 18.06.2020

[Th] Thompson, John G.: Some Finite Groups Which Appear As Gal L|K, where K $\subseteq$ Q(μ_n),1984, University of Cambridge, Journal of Algebra 89, 437-499.

[Vö] Völklein, Helmut: Groups as Galois Groups : An Introduction, Cambridge Studies in Advanced Mathematics 53, Digital Print, 2004

[We] Weintraub, Steven H. Galois Theory. New York, NY: Springer Science Business Media, LLC, 2009

Eidesstattliche Versicherung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Bachelorarbeit selbstständig und ohne Benutzung anderer, als der angegebenen Hilfsmittel, angefertigt habe. Die aus anderen Quellen direkt oder indirekt übernommenen Gedanken sind als solche gekennzeichnet.
Diese Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Essen, den 19.06.2020

Mike Farniok