Hilbert'scher Irreduzibilitätssatz

Diplomarbeit unter Anleitung von
Prof. Dr. D. Masser

Marcel Oehler
marcel.oehler@marcellosendos.ch
http://www.marcellosendos.ch/

23. Februar 2001

Zusammenfassung

Das Ziel dieser Diplomarbeit ist, einen klaren Beweis des Hilbert'schen Irreduzibilitätssatzes zu verfassen. Um dies zu erreichen, wird auf den Linearfaktorsatz sowie den Satz von Puiseux zurückgegriffen. Beide lassen sich ebenfalls kurz und verständlich beweisen. Als Zusatz folgt noch der Beweis des Galoisgruppensatzes mit dem Hilbert'schen Irreduzibilitätssatz.

"Ein auffälliger Zug aller Mathematik, der den Zugang zu ihr den Laien so sehr erschwert, ist der reichliche Gebrauch von Symbolen." – Hermann Weyl

"Immer mit den einfachsten Beispielen anfangen." – David Hilbert

Ein herzliches "Danggscheen" (in keiner bestimmten Reihenfolge) an

- ◇ *Prof. Dr. Masser* für die umfangreiche Betreuung,
- ◇ *Sandra* für die nette Gesellschaft,
- ◇ *Stephan* für die mathematische Hilfestellung,
- ◇ *Jolanda* für die ausführlichen Verbesserungsvorschläge,
- ◇ *Martin* für die LaTeXnischen Ratschläge,
- ◇ *Pamela* für die punktuelle Fehlerbehebung,
- ◇ *Oliver* für die scharfsinnigen Korrekturen,
- ◇ *Eva Maria* für die Liebe und den Sonnenschein.

Inhaltsverzeichnis

Einleitung **4**

1 Linearfaktorsatz **6**

2 Hilbert'scher Irreduzibilitätssatz **13**

3 Galoisgruppensatz **20**

A Satz von Puiseux **28**

Literaturverzeichnis **34**

Einleitung

Diese Arbeit hat ihren Ursprung in einem Seminar über den Hilbert'schen Irreduzibilitätssatz im Wintersemester 1998/99 bei Prof. Dr. D. Masser.

Definition

> Ein nicht-konstantes Polynom $F(x) \in k[x]$ heisst **irreduzibel** über k, falls aus $F(x) = G(x) \cdot H(x)$ und $G(x), H(x) \in k[x]$ folgt, dass entweder Grad $G = 0$ oder Grad $H = 0$ ist.

Inhalt

Zuerst wird in Kapitel 1 der, im Seminar so benannte, Linearfaktorsatz bewiesen.

Linearfaktorsatz

> Sei $F(x,t) \in \mathbb{Z}[x,t]$, normiert bezüglich x und sei $F(x,t) = 0$ ohne Lösung $x \in \mathbb{Q}(t)$.
>
> Dann gibt es unendlich viele $\tau \in \mathbb{Z}$, so dass $F(x,\tau) = 0$ keine Lösung $x \in \mathbb{Q}$ hat.

Dieser Satz entspricht in etwa dem Lemma 1 im Buch von Schinzel ([9], S. 180). Der Beweis folgt, abgesehen von einigen Fehlerkorrekturen, im Wesentlichen Schinzels Beweis ([9], S. 174-191). Lediglich das Lemma von Schwarz wurde von der Notation her vereinfacht und auf eine klarere Art bewiesen.

In Kapitel 2 folgt dann der Beweis des Hilbert'schen Irreduzibilitätssatzes mit Hilfe der Linearfaktorsatzes.

Hilbert'scher Irreduzibilitätssatz

> Sei $F(x,t) \in \mathbb{Q}[x,t]$ über $\mathbb{Q}(t)$ als Polynom in x irreduzibel.
>
> Dann existieren unendlich viele $\tau \in \mathbb{Z}$, so dass $F(x,\tau)$ über $\mathbb{Q}$ irreduzibel ist.

Dieser Satz entspricht Schinzels Theorem 33 ([9], S. 179) für den Fall $s = r = 1$ und $K = \mathbb{Q}$. Der Beweis weicht deshalb auch von Schinzels Version ab und benutzt eine alternative Form des Satzes von Mertens ([9], S. 85).

Mit Hilfe des Hilbert'schen Irreduzibilitätssatzes wird schliesslich in Kapitel 3 der, im Seminar so benannte, Galoisgruppensatz bewiesen.

Galoisgruppensatz

> Sei $F(x,t) \in \mathbb{Q}[x,t]$ *ohne Affekt* über $\mathbb{Q}(t)$.
>
> Dann gibt es unendlich viele $\tau \in \mathbb{N}$, so dass $F(x,\tau) \in \mathbb{Q}[x]$ *ohne Affekt* über $\mathbb{Q}$ ist.

Der Beweis weist, mit einer weiteren Variante des Merten'schen Satzes, gewisse Ähnlichkeiten zum Beweis der Variante im vorhergehenden Kapitel auf.

Der Satz von Puiseux, welcher für den Beweis des Linearfaktorsatzes wichtig ist, wird in Kapitel 1 formuliert. Da er aber nicht mehr zum eigentlichen Thema gehört, befindet sich sein Beweis in Anhang A.

Im Seminar haben wir den Versuch gemacht, diesen Satz wie Eichler [?] zu beweisen, was katastrophal endete. Für den Beweis verweist Schinzel [9] zwar auf Bliss [2], in dieser Arbeit verwenden wir aber van der Waerdens Variante [10], ergänzt mit dem Konvergenzaspekt.

Geschichte

Hilbert bewies 1892 [7] als erster den nach ihm benannten Satz für $\mathbb{Q}$. Er behauptete, dass der Beweis auch für jede Erweiterung von $\mathbb{Q}$ gelte, aber tatsächlich war sein Argument nur für normale Erweiterungen gültig.

Hilberts Beweis, welcher auf Puiseux-Erweiterungen basierte, wurde 1927 von Dörge [3] vereinfacht, aber die erste wirklich korrigierte Version des Beweises wurde 1931 von Franz [5] veröffentlicht. Bereits 1929 hatte Siegel eine andere Beweismethode skizziert.

Weitere Beweisverbesserungen folgten 1939 von Eichler [4] und 1974 von Fried [6]. 1965 leitete Schinzel [8] den Beweis für mehrere Variablen $x_1, \ldots, x_s, t_1, \ldots, t_r$ her. Später folgte von ihm [9] eine weitere Verallgemeinerung für beliebige endliche Erweiterungen von $\mathbb{Q}$.

Kapitel 1

Linearfaktorsatz

Zuerst werden wir einige Sätze formulieren, die für den Beweis des Linearfaktorsatzes notwendig sind.

Lemma von Schwarz (1882)

Sei $m \geq 1$, seien x_j reelle Zahlen mit $x_0 < \ldots < x_m$ und sei $\varphi(t)$ eine reelle Funktion m-mal differenzierbar im Intervall $x_0 \leq t \leq x_m$.

Dann existiert ein ξ, so dass $x_0 < \xi < x_m$ und

$$\frac{\varphi^{(m)}(\xi)}{m!} = \frac{1}{V_m} \begin{vmatrix} 1 & x_0 & \ldots & {x_0}^{m-1} & \varphi(x_0) \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_m & \ldots & {x_m}^{m-1} & \varphi(x_m) \end{vmatrix} \tag{1.1}$$

mit der Vandermonde-Determinante

$$V_m = \begin{vmatrix} 1 & x_0 & \ldots & {x_0}^m \\ \vdots & \vdots & & \vdots \\ 1 & x_m & \ldots & {x_m}^m \end{vmatrix} = \prod_{0 \leq i < j \leq m} (x_j - x_i). \tag{1.2}$$

Beweis

Für den Fall $m = 1$ entspricht dieses Lemma genau dem allgemeinen Mittelwertsatz

$$\varphi(x_1) - \varphi(x_0) = (x_1 - x_0)\varphi'(\xi). \tag{1.3}$$

Das bedeutet, dass eine an zwei Punkten differenzierbare Funktion verschwindet, ihre Ableitung an einem Punkt dazwischen eine Nullstelle hat.

Sei nun $A(t) = a_m t^m + \cdots + a_0$ und es gelte $A(x_j) = \varphi(x_j)$ $(0 \leq j \leq m)$. Diese Bedingungen definieren eine lineares Gleichungssystem

$$B \begin{pmatrix} a_0 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} \varphi(x_0) \\ \vdots \\ \varphi(x_m) \end{pmatrix} \qquad \text{mit } B = \begin{pmatrix} 1 & x_0 & \ldots & {x_0}^m \\ \vdots & \vdots & & \vdots \\ 1 & x_m & \ldots & {x_m}^m \end{pmatrix}. \tag{1.4}$$

Da $det(B) = V_m$ und die $x_0 < \ldots < x_m$ verschieden sind, ist $det(B)$ wegen der Produktformel (1.2) nicht Null. Die Matrix B ist deshalb invertierbar und es folgt durch Umformung

$$\begin{pmatrix} a_0 \\ \vdots \\ a_m \end{pmatrix} = B^{-1} \begin{pmatrix} \varphi(x_0) \\ \vdots \\ \varphi(x_m) \end{pmatrix}.$$

Sei nun $C(t) = A(t) - \varphi(t)$. Es gilt $C(t) = 0$ für $t = x_0, \ldots, x_m$.

Wir wenden den Mittelwertsatz an und erhalten

$$\begin{aligned} C'(t) &= A'(t) - \varphi'(t) = 0 \qquad \text{für } t = x'_0, \ldots, x'_{m-1} \text{ mit } x_j < x'_j < x_{j+1}, \\ C''(t) &= A''(t) - \varphi''(t) = 0 \qquad \text{für } t = x''_0, \ldots, x''_{m-2} \text{ mit } x'_j < x''_j < x'_{j+1}, \\ &\vdots \\ C^{(m)}(\xi) &= a_m \cdot m! - \varphi^{(m)}(\xi) = 0 \qquad \text{für } x_0 < \xi < x_m. \end{aligned} \tag{1.5}$$

a_m lässt sich nun aus der Gleichung (1.4) mittels der Cramer'schen Regel ([1], S. 30-32) bestimmen.

$$a_m = \frac{\begin{vmatrix} 1 & x_0 & \ldots & {x_0}^{m-1} & \varphi(x_0) \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_m & \ldots & {x_m}^{m-1} & \varphi(x_m) \end{vmatrix}}{det(B)}$$

Eingesetzt in die Gleichung (1.5) beweist dies das Lemma.

■

Satz von Dörge (1927)

Sei e eine positive ganze Zahl, sei $t_0 > 0$ eine reelle Zahl und sei

$$\varphi(t) = a_{-k} t^{\frac{k}{e}} + a_{-k+1} t^{\frac{k-1}{e}} + \cdots + a_{-1} t^{\frac{1}{e}} + a_0 + a_1 t^{\frac{-1}{e}} + \ldots$$

eine nach $t > t_0$ konvergierende Folge mit komplexen Koeffizienten, mit $\varphi(t) \notin \mathbb{Q}[t]$. Seien $t_1, t_2, \ldots \in \mathbb{N}$ mit $t_0 < t_1 < t_2 < \ldots$ und $\varphi(t_1), \varphi(t_2), \ldots \in \mathbb{Z}$.

(Wobei $t^{\frac{1}{e}}$ für $t \in \mathbb{N}$ hier die positive Wurzel bedeutet.)

Dann existiert ein $\lambda > 0$ in $\mathbb{R}$ und $m, I \in \mathbb{N}$, so dass

$$t_{i+m} - t_i > {t_i}^{\lambda}$$

für alle $i > I$.

Beweis

Wenn nicht alle Koeffizienten a_n reell sind, sei ℓ der kleinste Index, so dass $\mathrm{Im}(a_\ell)$ nicht Null ist.

Für alle $t \in \mathbb{R}$ gross genug haben wir

$$\left|\mathrm{Im}\left(\sum_{n=-k}^{\ell} a_n t^{-\frac{n}{e}}\right)\right| = \left|\mathrm{Im}\left(a_\ell t^{-\frac{\ell}{e}}\right)\right| > \left|\mathrm{Im}\left(\sum_{n=\ell+1}^{\infty} a_n t^{-\frac{n}{e}}\right)\right|$$

und deshalb gilt für ein i gross genug $\varphi(t_i) \notin \mathbb{R}$, was im Widerspruch zur Annahme steht. Deshalb genügt φ den Vorraussetzungen des Lemmas von Schwarz.

Weiter nehmen wir an, dass φ ein Polynom ist und deshalb in $\mathbb{R}[t]$ liegt. Nun ist $\varphi \notin \mathbb{Q}[t]$, also existiert ein kleinster Index ℓ, so dass $a_\ell \notin \mathbb{Q}$. Es ist klar, dass $\ell \leq 0$ und $e|\ell$ sind, und weiter $a_n = 0$ wenn $e\not|n$ ist.

Die Funktion

$$\varphi(t) - \sum_{n=-k}^{\ell-1} a_n t^{-\frac{n}{e}} = a_\ell t^{-\frac{\ell}{e}} + \cdots + a_0$$

hat rationale Werte für $t = t_1, t_2, \ldots$. Falls $\ell = 0$ ist, sind diese Werte alle gleich a_0 – ein Widerspruch!

Falls $\ell < 0$ ist, wenden wir das Lemma von Schwarz mit $m = -\frac{\ell}{e}$ auf diese Funktion an und erhalten Gleichheit mit a_ℓ auf der linken und eine rationale Zahl auf der rechten Seite – ein weiterer Widerspruch!

Es bleibt der Fall zu überprüfen, in dem $a_n \in \mathbb{R}$ für alle $n \geq -k$, aber $\varphi \notin \mathbb{R}[t]$. Wählen wir $m \geq 1$ so gross, dass $\varphi^{(m)}(t)$ nur Terme mit negativen Exponenten enthält (wahrscheinlich ist $m > \frac{k}{e}$). Nun gibt es eine reelle Zahl $\mu > 0$ und eine ganze Zahl $I \geq 0$ und $c > 0$, so dass

$$c^{-1}\tau^{-\mu} \geq \left|\varphi^{(m)}(\tau)\right| \geq \frac{1}{2}c^{-1}\tau^{-\mu} > 0$$

für alle $\tau \geq t_i$ mit $i > I$ gilt.

Jetzt wenden wir das Lemma von Schwarz an, mit $x_0 = t_i, x_1 = t_{i+1}, \ldots, x_m = t_{i+m}$ für alle $i > I$. Die Determinante im Zähler auf der rechten Seite von (1.1) ist eine ganze Zahl, und deshalb ist für $i > I$ der absolute Betrag der Determinante mindestens 1 und

$$\left|\frac{\varphi^{(m)}(\xi)}{m!}\right| \geq \frac{1}{V_m}.$$

Also ist für $i > I$

$$|V_m| \geq \frac{m!}{|\varphi^{(m)}(\xi)|} \geq \frac{m!\ c}{\xi^{-\mu}} = m!\ c \cdot \xi^{\mu} \geq m!\ c \cdot {t_i}^{\mu}.$$

Jede Differenz in der Formel für V_m ist als absoluter Betrag höchstens $t_{i+m} - t_i$, und deshalb ist

$$(t_{i+m} - t_i)^{\frac{m(m+1)}{2}} \geq |V_m| \geq m!\ c \cdot {t_i}^{\mu}$$

und der Satz folgt für alle $\lambda < \frac{2\mu}{m(m+1)}$.

■

Beispiel

Sei

$$\varphi(t) = (t+1)^{\frac{1}{2}} = t^{\frac{1}{2}} + \frac{1}{2}t^{-\frac{1}{2}} + \ldots.$$

Dann genügt $m = 1$ und

$$\varphi'(t) = \frac{1}{2}t^{-\frac{1}{2}} + \ldots.$$

Also gilt

$$\frac{2}{3}\tau^{-\frac{1}{2}} \geq |\varphi'(\tau)| \geq \frac{1}{3}\tau^{-\frac{1}{2}}$$

für alle $\tau \geq t_i$ und $i > I$. Nun impliziert der Mittelwertsatz (1.3) $\varphi(t_{i+1}) - \varphi(t_i) \neq 0$, und da wir uns in $\mathbb{Z}$ befinden, erhalten wir

$$t_{i+1} - t_i \geq \frac{1}{|\varphi'(\tau)|} \geq \frac{3}{2}\tau^{\frac{1}{2}} \geq \frac{3}{2}{t_i}^{\frac{1}{2}}$$

und daraus den Satz mit $\lambda = \frac{1}{2}$.
Natürlich ist $\varphi(\tau) \in \mathbb{Z}$ genau dann, wenn $t = 0, 3, 8, 15, \ldots, n^2 - 1, \ldots$.

Korollar

Seien φ und $\lambda > 0$ wie im Satz von Dörge.

Dann existiert ein $C = C(\varphi)$, so dass für ein beliebiges $T \geq 1$ die Anzahl $N(T)$ von $t > t_0$ in $\mathbb{Z}$ mit $\varphi(t) \in \mathbb{Z}$ und $t \leq T$ die Bedingung

$$N(T) \leq CT^{1-\lambda}$$

erfüllt, wenn $\lambda < 1$.

(Vergleiche dazu Schinzels Korollar ([9], S. 179). Seine Argumentation ergibt den Exponenten $\frac{1}{1-\lambda}$, was immer grösser als unser Exponent $1 - \lambda$ ist.)

Beweis

Zuerst ordnen wir die positiven ganzen Zahlen $t > t_0$ mit $\varphi(t) \in \mathbb{Z}$ so an, dass $t_0 < t_1 < t_2 < \ldots$. Seien m und I wie im Satz von Dörge und sei $t(j) = t_{I+1+mj}$ $(j = 0, 1, 2, \ldots)$. Weiter seien

$$\gamma = \frac{1}{1-\lambda} > 1 \qquad c = \min\left\{t(0), \left(2^{\gamma-1}\gamma\right)^{\gamma}\right\}.$$

Wir beweisen zuerst durch Induktion, dass

$$t(j) \geq c(j+1)^{\gamma} \qquad (j = 0, 1, 2, \ldots). \tag{1.6}$$

Der Fall $j = 0$ ist trivial. Angenommen die Behauptung stimmt für $j \geq 0$. Der Satz von Dörge impliziert nun, dass

$$t(j+1) - t(j) > t(j)^{\lambda}$$

und deshalb ist

$$t(j+1) > c(j+1)^{\gamma} + c^{\lambda}(j+1)^{\gamma-1}.$$

Durch Anwendung des Mittelwertsatzes (1.3) erhalten wir

$$(j+2)^{\gamma} - (j+1)^{\gamma} = \gamma\tau^{\gamma-1}$$

für ein τ mit $j+1 < \tau < j+2$. Also ist

$$(j+2)^{\gamma} - (j+1)^{\gamma} \leq \gamma(j+2)^{\gamma-1} \leq 2^{\gamma-1}, \gamma(j+1)^{\gamma-1}$$

und deshalb

$$t(j+1) \geq c(j+2)^{\gamma} - c2^{\gamma-1}\gamma(j+1)^{\gamma-1} + c^{\lambda}(j+1)^{\gamma-1} \geq c(j+2)^{\gamma},$$

weil $c^{1-\lambda} \geq \frac{1}{2^{\gamma-1}\gamma}$. Also folgt die Ungleichung (1.6) durch Induktion.

Nun sei $N = N(T)$ und wir haben $t_N \leq T$. Wir zeigen, dass

$$N < I + 1 + m\left(\frac{T}{c}\right)^{1-\lambda} \tag{1.7}$$

woraus das Korollar folgt.

Wenn $N \leq I$ gilt, folgt die Ungleichung (1.7) sofort. Sonst gibt es ein grösstes $j \geq 0$ mit $I + 1 + mj \leq N$ und es folgt, dass $t(j) \leq t_N \leq T$ ist.

Also impliziert die Ungleichung (1.6)

$$c(j+1)^{\gamma} \leq T.$$

Aber $I + 1 + m(j+1) > N$ und deshalb folgt die Ungleichung (1.7).

■

Beispiel

Sei

$$\varphi(t) = (t+1)^{\frac{1}{2}} = t^{\frac{1}{2}} + \frac{1}{2}t^{-\frac{1}{2}} + \dots .$$

Dann gilt die Bedingung im Korollar für $\lambda = \frac{1}{2}$ und wir erhalten $N(T) \leq CT^{\frac{1}{2}}$. Wie schon im letzten Beispiel gesagt, ist $\varphi(t) \in \mathbb{Z}$ für $t = 0, 3, 8, 15, \dots, n^2 - 1, \dots$ und so ist $N(n^2) \geq n - 1$.

Also ist der Exponent $\frac{1}{2}$ der bestmöglichste, während Schinzels Argumentation nur den Exponenten $\frac{2}{3}$ liefert.

Satz von Puiseux (1850)

> Sei $F(x,t) \in \mathbb{C}[x,t]$. Dann gibt es ein $t_0 > 0$ und $\varphi_1, \dots, \varphi_n$ wie im Satz von Dörge, konvergierend für alle komplexen t mit $|t| > t_0$, mit der folgenden Eigenschaft:
>
> Sei τ eine beliebige komplexe Zahl mit $|\tau| > t_0$. Dann gibt es für jedes komplexe ξ mit $F(\xi, \tau) = 0$ ein j mit $1 \leq j \leq n$, so dass $\xi = \varphi_j(\tau)$.

Dieser Satz wird hier nicht bewiesen, sondern erst in Anhang A.

Beispiel

Sei $F(x,t) = x^2 - t - 1 \in \mathbb{C}[x,t]$. Dann sind

$$\begin{aligned} \varphi_1(t) &= (t+1)^{\frac{1}{2}} = t^{\frac{1}{2}} + \frac{1}{2}t^{-\frac{1}{2}} + \dots \\ \varphi_2(t) &= -(t+1)^{\frac{1}{2}} = -t^{\frac{1}{2}} - \frac{1}{2}t^{-\frac{1}{2}} - \dots \end{aligned}$$

konvergierend für alle $|t| > 1$. Also gilt

$$\xi = \varphi_1(\tau) \qquad \text{oder} \qquad \xi = \varphi_2(\tau)$$

für jedes ξ mit $F(\xi, \tau) = \xi^2 - \tau - 1 = 0$ und τ beliebig mit $|\tau| > 1$.

Linearfaktorsatz

> Sei $F(x,t) \in \mathbb{Z}[x,t]$, normiert bezüglich x und sei $F(x,t) = 0$ ohne Lösung $x \in \mathbb{Q}(t)$.
>
> Dann gibt es unendlich viele $\tau \in \mathbb{Z}$, so dass $F(x,\tau) = 0$ keine Lösung $x \in \mathbb{Q}$ hat.

Beweis

Für jedes $\tau \in \mathbb{Z}$ hat das Polynom $F(x, \tau)$ die Form $x^n + b_1 x^{n-1} + \cdots + b_n$ mit $b_k \in \mathbb{Z}$, also sind alle rationalen Nullstellen ganze Zahlen. Nach dem Satz von Puiseux sind alle Lösungen von $F(x, \tau) = 0$ von der Form

$$\tau = \varphi(\tau) \quad \text{mit } \varphi = \varphi_1, \ldots, \varphi_n.$$

Nach Annahme ist $\varphi_i \notin \mathbb{Q}(t)$ und deshalb auch nicht in $\mathbb{Q}[t]$. Nach dem Korollar zum Satz von Dörge gibt es höchstens $O(T^\lambda)$ positive ganze Zahlen $t \leq T$, so dass $\varphi_i(t)$ eine ganze Zahl ist.

Weil $n \cdot O(T^\lambda) = O(T^\lambda)$ ist, existieren unendlich viele positive ganze Zahlen τ, für welche kein $\varphi_i(\tau)$ eine ganze Zahl ist, und deshalb ist für diese τ keine Nullstelle von $F(x, \tau)$ rational.

■

Kapitel 2

Hilbert'scher Irreduzibilitätssatz

Der Hilbert'sche Irreduzibilitätssatz kann mit Hilfe des Linearfaktorsatzes gezeigt werden. Dazu benötigen wir folgenden

Satz

Seien $n \geq 2$ und Variablen $\underline{t} = (t_1, \ldots, t_n), x$ gegeben. Dann existieren $N \geq 0$ und Polynome $Q_0(x, \underline{t}), \ldots, Q_N(x, \underline{t}) \in \mathbb{Z}[x, \underline{t}]$, normiert bezüglich x, mit der folgenden Eigenschaft.

Sei k ein beliebiger Körper mit Charakteristik Null. Dann ist für $\underline{\tau} = (\tau_1, \ldots, \tau_n) \in k^n$ das Polynom

$$P(x, \underline{\tau}) = x^n - \tau_1 x^{n-1} \pm \ldots + (-1)^n \tau_n$$

genau dann irreduzibel über k, wenn mindestens eines der Polynome $Q_0(x, \underline{\tau}), \ldots, Q_N(x, \underline{\tau}) \in k[x]$ über k keinen Linearteiler hat.

Beweis

Wir nehmen $N = \binom{n}{1}0 + \binom{n}{2}1 + \cdots + \binom{n}{n-1}(n-2)$, führen eine neue Variable $\underline{x} = (x_1, \ldots, x_n)$ ein und definieren für $r \in \mathbb{Z}$ $(0 \leq r \leq N)$

$$\begin{aligned} \tilde{Q}_r(x, \underline{x}) \quad = \quad & \prod_{1 \leq i_1 \leq n} (x - x_{i_1}) \prod_{1 \leq i_1 < i_2 \leq n} \Big(x - (x_{i_1} + x_{i_2}) - r x_{i_1} x_{i_2} \Big) \\ \cdots \quad & \prod_{1 \leq i_1 < \ldots < i_{n-1} \leq n} \Big(x - (x_{i_1} + \cdots + x_{i_{n-1}}) \\ & \qquad - r(x_{i_1} x_{i_2} + \cdots + x_{i_{n-2}} x_{i_{n-1}}) \\ & \qquad - r^2 (x_{i_1} x_{i_2} x_{i_3} + \cdots + x_{i_{n-3}} x_{i_{n-2}} x_{i_{n-1}}) \\ & \qquad - \ldots \\ & \qquad - r^{n-2} x_{i_1} \cdots x_{i_{n-1}} \Big) \qquad \in \mathbb{Z}[x, \underline{x}]. \end{aligned} \tag{2.1}$$

Dieses Polynom ist symmetrisch in $R[\underline{x}]$ für $R = \mathbb{Z}[x]$. Nach dem Hauptsatz über symmetrische Polynome ([1], S. 626-631) kann jedes symmetrische Polynom in den

elementarsymmetrischen Funktionen $s_1, \ldots, s_n$ geschrieben werden. Zuerst aber verbessern wir die Notation.

Sei $I \subseteq \mathcal{N} = \{1, \ldots, n\}$ mit $|I| = m$ $(1 \leq m \leq n)$ und sei ${s_j}^I(\underline{x})$ die j-te elementarsymmetrische Funktion $(1 \leq j \leq m)$ der x_i $(i \in I)$, zum Beispiel für $I = \mathcal{N}$:

$$\begin{array}{rcll} {s_1}^{\mathcal{N}}(\underline{x}) & = & x_1 + \cdots + x_n & (= s_1) \\ {s_2}^{\mathcal{N}}(\underline{x}) & = & x_1x_2 + \cdots + x_{n-1}x_n & (= s_2) \\ & \vdots & & \\ {s_n}^{\mathcal{N}}(\underline{x}) & = & x_1 \cdots x_n & (= s_n) \end{array}$$

oder für $I = \{1, 2\}$

$$\begin{array}{rcl} {s_1}^I(\underline{x}) & = & x_1 + x_2 \\ {s_2}^I(\underline{x}) & = & x_1x_2. \end{array}$$

Dann ist

$$\tilde{Q}_r(x, \underline{x}) = \prod_{m=1}^{n-1} \prod_{|I|=m} \Big(x - {s_1}^I(\underline{x}) - r{s_2}^I(\underline{x}) - \ldots - r^{m-1}{s_m}^I(\underline{x})\Big) \quad \in \mathbb{Z}[x, \underline{x}]$$

und es gibt $Q_r(x, \underline{t}) \in \mathbb{Z}[x, \underline{t}]$ mit $Q_r(x, \underline{t}) = \tilde{Q}_r(x, \underline{x})$. Dies definiert unsere Polynome

$$Q_r(x, \underline{t}) \quad \in \mathbb{Z}[x, \underline{t}] \qquad (0 \leq r \leq N).$$

Wir wollen zeigen:

> Das Polynom $P(x, \underline{\tau})$ ist genau dann irreduzibel, wenn mindestens ein $Q_r(x, \underline{\tau})$ $(0 \leq r \leq N)$ keinen Linearteiler hat.

Sei k ein Körper mit Charakteristik Null, sei $\tau \in k^n$, und seien $\xi_1, \ldots, \xi_n$ die Nullstellen von $P(x, \underline{\tau}) = 0$ im Abschluss $\overline{k}$ von k. Also

$$\begin{array}{rcl} P(x, \underline{\tau}) & = & (x - \xi_1) \cdots (x - \xi_n) \\ & = & x^n - \tau_1 x^{n-1} \pm \ldots + (-1)^n \tau_n. \end{array}$$

Wir überprüfen zuerst folgende Aussage:

> Wenn das Polynom $P(x, \underline{\tau}) \in k[x]$ über k reduzibel ist, dann hat jedes $Q_r(x, \underline{\tau})$ $(0 \leq r \leq N)$ einen Linearteiler über k.

Ist $P(x, \underline{\tau})$ über k reduzibel, dann hat es einen Faktor mit Grad m $(1 \leq m \leq n-1)$ in $k[x]$ und dieser Faktor hat Nullstellen ξ_i $(i \in I)$ für ein I mit $|I| = m$. Also liegen die elementarsymmetrischen Funktionen

$$\begin{array}{rcl} {s_1}^I(\underline{\xi}) & = & \xi_{i_1} + \cdots + \xi_{i_m} \\ {s_2}^I(\underline{\xi}) & = & \xi_{i_1}\xi_{i_2} + \cdots + \xi_{i_{m-1}}\xi_{i_m} \\ & \vdots & \\ {s_m}^I(\underline{\xi}) & = & \xi_{i_1} \cdots \xi_{i_m} \end{array}$$

alle in k. Es folgt, dass jedes $Q_r(x,\underline{\tau}) = \tilde{Q}_r(x,\underline{\xi})$ $(0 \le r \le N)$ einen Linearfaktor

$$x - {s_1}^I(\underline{\xi}) - r{s_2}^I(\underline{\xi}) - \ldots - r^{m-1}{s_m}^I(\underline{\xi})$$

in $k[x]$ hat.

In der anderen Richtung müssen wir beweisen, falls alle Polynome

$$Q_0(x,\underline{\tau}), \ldots, Q_N(x,\underline{\tau}) \quad \in k[x]$$

einen Linearfaktor über k haben, $P(x,\underline{\tau})$ reduzibel über k ist.

Angenommen, alle $Q_r(x,\underline{\tau})$ $(0 \le r \le N)$ haben einen Linearfaktor in $k[x]$. Seien $\xi_1, \ldots, \xi_n$ wieder die Nullstellen von $P(x,\underline{\tau}) = 0$, so dass

$$Q_r(x,\underline{\tau}) = \prod_{m=1}^{n-1} \prod_{|I|=m} \Big(x - {s_1}^I(\underline{\xi}) - r{s_2}^I(\underline{\xi}) - \ldots - r^{m-1}{s_m}^I(\underline{\xi})\Big).$$

Für jedes I sei q^I die Anzahl der r $(0 \le r \le N)$, so dass der Faktor

$$x - {s_1}^I(\underline{\xi}) - r{s_2}^I(\underline{\xi}) - \ldots - r^{m-1}{s_m}^I(\underline{\xi})$$

in $k[x]$ liegt. Dann ist

$$\sum_{m=1}^{n-1} \sum_{|I|=m} q^I \ge N+1.$$

Es folgt, dass ein I mit

$$q^I \ge m = |I| \tag{2.2}$$

existieren muss. Würde dies nicht gelten, so wäre $q^I \le m-1$ für alle I und wir würden

$$\begin{aligned} \sum_{m=1}^{n-1} \sum_{|I|=m} q^I &\le \sum_{m=1}^{n-1} \sum_{|I|=m} (m-1) \\ &= \sum_{m=1}^{n-1} (m-1) \sum_{|I|=m} 1 \\ &= \sum_{m=1}^{n-1} (m-1) \binom{n}{m} = N \end{aligned} \tag{2.3}$$

erhalten – ein Widerspruch. Somit ist die Ungleichung (2.2) geprüft.

Seien nun m und I wie in (2.2). Dann gibt es verschiedene $r_1, \ldots, r_m$, so dass

$$\begin{gathered} {s_1}^I(\underline{\xi}) + r_1{s_2}^I(\underline{\xi}) + \cdots + {r_1}^{m-1}{s_m}^I(\underline{\xi}) \\ \vdots \\ {s_1}^I(\underline{\xi}) + r_m{s_2}^I(\underline{\xi}) + \cdots + {r_m}^{m-1}{s_m}^I(\underline{\xi}) \end{gathered}$$

in k liegen. Dies lässt sich auch als Matrix schreiben:

$$\begin{pmatrix} 1 & r_1 & \dots & {r_1}^{m-1} \\ \vdots & \vdots & & \vdots \\ 1 & r_m & \dots & {r_m}^{m-1} \end{pmatrix} \begin{pmatrix} {s_1}^I(\underline{\xi}) \\ \vdots \\ {s_m}^I(\underline{\xi}) \end{pmatrix} = \begin{pmatrix} \kappa_1 \\ \vdots \\ \kappa_m \end{pmatrix}$$

mit $\kappa_1, \dots, \kappa_m \in k$.

Die Eliminierung von einzelnen Faktoren kann umgangen werden, wenn wir bemerken, dass die Vandermonde-Determinante

$$\begin{vmatrix} 1 & r_1 & \dots & {r_1}^{m-1} \\ \vdots & \vdots & & \vdots \\ 1 & r_m & \dots & {r_m}^{m-1} \end{vmatrix} = \prod_{1 \le i < j \le m} (r_j - r_i)$$

nicht Null ist, wenn $r_i \neq r_j$ für $i \neq j$. Aus der Produktformel ist dies leicht ersichtlich.

Nach der Cramer'schen Regel ([1], S. 30-32) liegen ${s_1}^I(\underline{\xi}), \dots, {s_m}^I(\underline{\xi})$ alle in k. Deshalb hat $P(x, \underline{\tau})$ den Faktor

$$\prod_{i \in I}(x - \xi_i) = x^m - {s_1}^I(\underline{\xi})x^{m-1} + \dots + (-1)^m {s_m}^I(\underline{\xi})$$

in $k[x]$ ist und ist somit reduzibel über k. Somit ist der Beweis beendet.

Die Rechnung (2.3) zeigt, dass die Wahl von

$$\begin{aligned} N &= \binom{n}{1}0 + \binom{n}{2}1 + \dots + \binom{n}{n-1}(n-2) \\ &= \frac{d}{dX}\left(\frac{(1+X)^n - 1}{X}\right)_{X=1} - (n-1) \\ &= (n-2)(2^{n-1} - 1) \end{aligned}$$

korrekt war.

■

Beispiele

Die Polynome $Q_0, \dots, Q_N$ können für kleine Werte von N vereinfacht werden.

n=2

Das Polynom $P(x, \underline{\tau}) = x^2 - \tau_1 x + \tau_2$ ist genau dann irreduzibel, wenn es einen Linearfaktor hat. Also können wir $N = 0$ und

$$Q_0(x, \underline{t}) = P(x, \underline{t})$$

nehmen.

n=3

Für diesen Fall gilt genau das Gleiche wie für den Fall $n = 2$.

n=4

Hier müssen wir zusätzlich quadratische Faktoren in Betracht ziehen. Tatsächlich reicht es aber, die sieben Polynome

$$(x - x_1 - x_2 + rx_1x_2) \cdots (x - x_3 - x_4 + rx_3x_4) \qquad (0 \leq r \leq 6)$$

als Polynome in den symmetrischen Funktionen $\underline{t} = (t_1, \ldots, t_4)$ von $\underline{x} = (x_1, \ldots, x_4)$ zu schreiben.

Eine Variante ersetzt $x - x_1 - x_2 + rx_1x_2$ durch $x - (x_1 + r)(x_2 + r)$. Dies führt zur folgenden, einfacher zu berechnenden Ausdrucksweise. Seien $S_1(\underline{t}), \ldots, S_6(\underline{t})$ die elementarsymmetrischen Funktionen von

$$x_1x_2 \quad x_1x_3 \quad x_1x_4 \quad x_2x_3 \quad x_2x_4 \quad x_3x_4$$

ausgedrückt in Termen mit $\underline{t} = (t_1, \ldots, t_4)$, mit

$$\begin{aligned} t_1 &= x_1 + x_2 + x_3 + x_4 \\ t_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ t_3 &= x_1x_2x_3 + x_1x_3x_4 + x_1x_2x_4 + x_2x_3x_4 \\ t_4 &= x_1x_2x_3x_4. \end{aligned}$$

Zum Beispiel sind

$$S_1(\underline{t}) = t_2 \qquad S_6(\underline{t}) = {t_4}^3$$

wobei $S_2(\underline{t}), \ldots, S_5(\underline{t})$ weitaus komplizierter zu berechnen sind. Aber mit der Hilfe von MAPLE findet man

$$\begin{aligned} S_2(\underline{t}) &= t_1t_3 - t_4 \\ S_3(\underline{t}) &= {t_3}^2 + {t_1}^2t_4 - 2t_2t_4 \\ S_4(\underline{t}) &= t_1t_3t_4 - {t_4}^2 \\ S_5(\underline{t}) &= t_2{t_4}^2. \end{aligned}$$

Sei nun

$$\begin{aligned} S(x, \underline{t}) &= x^6 - S_1(\underline{t})x^5 + S_2(\underline{t})x^4 - S_3(\underline{t})x^3 \\ &\quad + S_4(\underline{t})x^2 - S_5(\underline{t})x + S_6(\underline{t}). \end{aligned}$$

Dann können wir

$$Q_r(x, \underline{t}) = P(x, \underline{t})S(x, \underline{t}^{(r)}) \qquad (0 \leq r \leq 6)$$

mit $\underline{t}^{(r)} = ({t_1}^{(r)}, {t_2}^{(r)}, {t_3}^{(r)}, {t_4}^{(r)})$ nehmen, wobei $\underline{t}^{(r)}$ durch ersetzen von x_i durch $x_i + r$ in $\underline{t}$ entsteht. Also sind

$$\begin{aligned} {t_1}^{(r)} &= t_1 + 4r \\ {t_2}^{(r)} &= t_2 + 3rt_1 + 6r^2 \\ {t_3}^{(r)} &= t_3 + 2rt_2 + 3r^2t_1 + 4r^3 \\ {t_4}^{(r)} &= t_4 + rt_3 + r^2t_2 + r^3t_1 + r^4. \end{aligned}$$

Hilbert'scher Irreduzibilitätssatz

Sei $F(x, t) \in \mathbb{Q}[x, t]$ über $\mathbb{Q}(t)$ als Polynom in x irreduzibel.

Dann existieren unendlich viele $\tau \in \mathbb{Z}$, so dass $F(x, \tau)$ über $\mathbb{Q}$ irreduzibel ist.

Beweis

Wir nehmen zuerst

$$F(x, t) = x^n - f_1(t)x^{n-1} + \cdots + (-1)^n f_n(t) \in \mathbb{Z}[x, t]$$

irreduzibel über $\mathbb{Q}(t)$. Sei $\underline{f} = (f_1, \ldots, f_n)$. Nach vorherigem Satz mit $k = \mathbb{Q}(t)$ gibt es r $(0 \leq r \leq N)$, so dass

$$Q_r\left(x, \underline{f}(t)\right) = G(x, t)$$

keine Linearfaktoren über $\mathbb{Q}(t)$ hat.

Jetzt wenden wir den Linearfaktorsatz an und sehen, dass

$$G(x, \tau) = Q_r\left(x, \underline{f}(\tau)\right)$$

für unendlich viele $\tau \in \mathbb{Z}$ keine Linearfaktoren über $\mathbb{Q}$ hat.

Der Satz für $k = \mathbb{Q}$ zeigt nun, dass für diese τ

$$F(x, \tau) = x^n - f_1(\tau)x^{n-1} + \cdots + (-1)^n f_n(\tau) \in \mathbb{Q}[x]$$

irreduzibel über $\mathbb{Q}$ ist.

Im Allgemeinen können wir

$$F(x, t) = f_0(t)x^n - f_1(t)x^{n-1} \pm \ldots + (-1)^n f_n(t)$$

mit $f_0(t), \ldots, f_n(t) \in \mathbb{Z}[t]$ und $f_0(t) \neq 0$ nehmen. Wir führen dies mit einem Standard-Trick auf den vorhergehenden Fall zurück.

Wir haben nämlich

$$(f_0(t))^{n-1} F\left(\frac{x}{f_0(t)}, t\right) = \tilde{F}(x,t)$$

mit

$$\tilde{F}(x,t) = x^n - f_1(t)x^{n-1} + f_0(t)f_2(t)x^{n-2} \mp \ldots + (-1)^n f_0(t)^{n-1} f_n(t)$$

in $\mathbb{Z}[x,t]$. $\tilde{F}(x,t)$ bleibt irreduzibel über $\mathbb{Q}(t)$, also zeigt der vorhergehende Fall, dass $\tilde{F}(x,\tau)$ für unendlich viele $\tau \in \mathbb{Z}$ irreduzibel über $\mathbb{Q}$ ist.

Solange $f_0(\tau)$ nicht Null ist, folgt dass $F\left(\frac{x}{f_0(\tau)}, \tau\right)$ und darum auch $F(x,\tau)$ irreduzibel über $\mathbb{Q}$ ist. Somit wäre der Hilbert'sche Irreduzibiltätssatz bewiesen.

■

Kapitel 3

Galoisgruppensatz

Zuerst werden wir einige Definitionen und Sätze formulieren, die für den Beweis des Galoisgruppensatzes notwendig sind.

Definition

Sei k ein Körper mit Charakteristik Null, und sei $F(x) \in k[x]$ mit Grad $F = n \geq 1$.

Dann ist ein Körper $K \supseteq k$ ein **Zerfällungskörper** von $F(x)$, wenn

1. $\xi_1, \ldots, \xi_n \in K$ mit $F(x) = a_0 \prod_{i=1}^{n} (x - \xi_i)$ existieren,
2. $K = k(\xi_1, \ldots, \xi_n)$ ist.

Sind k und F gegeben, so existiert immer ein solches K ([1], S. 618).

Transitivitätslemma

Seien $\xi_1, \ldots, \xi_n$ die Nullstellen von einem Polynom $F(x)$ in einem Zerfällungskörper.

Dann ist $F(x)$ genau dann irreduzibel über k, wenn folgendes gilt:

(α) $\xi_1, \ldots, \xi_n$ sind paarweise verschieden.

(β) Seien i, j mit $1 \leq i, j \leq n$ gegeben.
Dann existiert ein Körper-Automorphismus

$$\sigma : k(\xi_1, \ldots, \xi_n) \to k(\xi_1, \ldots, \xi_n)$$

welcher k elementweise mit $\sigma(\xi_i) = \xi_j$ fixiert.

Beweis

Nehmen wir zuerst an, $F(x)$ sei irreduzibel über k. Dann ist (α) klar, weil k Charakteristik Null hat.

Sei σ ein Körper-Monomorphismus

$$\sigma : k(\xi_i) \to k(\xi_j)$$

mit $\sigma(\xi_i) = \xi_j$ ([1], S. 567). Nun ist $k(\xi_1, \ldots, \xi_n)$ eine endlich Erweiterung von $k(\xi_i)$ und σ kann nach $k(\xi_1, \ldots, \xi_n)$ erweitert werden. Die Werte werden nicht mehr in $k(\xi_i)$ liegen, aber jedes $\sigma(\xi_r)$ $(1 \leq r \leq n)$ ist auch eine Nullstelle von $F(x)$, also ein ξ_s $(1 \leq s \leq n)$. Deshalb bildet σ die Erweiterung $k(\xi_1, \ldots, \xi_n)$ nach sich selbst ab, und wir erhalten den in (β) verlangten Automorphismus.

Umgekehrt gelte (α) und (β) und angenommen, $F(x)$ sei nicht irreduzibel. Dann gilt

$$F(x) = G(x)H(x)$$

für G, H mit Grad grösser als Null über k. Wählen wir nun $i \neq j$ mit

$$G(\xi_i) = H(\xi_j) = 0.$$

Dann genügt σ aus (β) folgender Gleichung:

$$0 = \sigma(G(\xi_i)) = G(\sigma(\xi_i)) = G(\xi_j).$$

Also ist ξ_j ebenfalls eine Nullstelle von G was nach (α) unmöglich ist – ein Widerspruch. Somit ist $F(x)$ irreduzibel.

■

Definition

Sei k ein Körper mit Charakteristik Null und sei $F(x) \in k[x]$ mit Grad $F = n \geq 1$. Wir sagen, dass $F(x)$ **ohne Affekt** über k ist, wenn gilt:

(a) $F(x)$ ist irreduzibel über k.

(b) Seien $\xi_1, \ldots, \xi_n$ die verschiedenen Nullstellen von $F(x)$ in einem Zerfällungskörper.
Dann gibt es für jede Permutation

$$\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$$

in der symmetrischen Gruppe S_n einen Körper-Automorphismus

$$\sigma : k(\xi_1, \ldots, \xi_n) \to k(\xi_1, \ldots, \xi_n)$$

der k elementweise fixiert und die Bedingung

$$\sigma(\xi_i) = \xi_{\pi(i)} \qquad (1 \leq i \leq n)$$

erfüllt.

Beispiele

n=1

Jedes $F(x)$ mit Grad $F = 1$ ist trivialerweise *ohne Affekt*.

n=2

Hier ist (a) ausreichend. Ist π die identische Permutation, so können wir σ als identischen Automorphismus nehmen. Ansonsten ist $\pi = (12)$, und nach (β) gibt es ein $\sigma : k(\xi_1, \xi_2) \to k(\xi_1, \xi_2)$ mit $\sigma(\xi_1) = \xi_2$.

Aber ist $F(x) = ax^2 + bx + c$ $(a \neq 0)$, dann ist $\xi_1 + \xi_2 = -\frac{b}{a}$ und

$$\sigma(\xi_2) = \sigma\left(-\frac{b}{a} - \xi_1\right) = -\frac{b}{a} - \xi_2 = \xi_1.$$

n>2

Im Allgemeinen genügt (a) nicht. Zum Beispiel

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

und $\xi_1 = \cos\frac{\pi}{9}$ ist eine Nullstelle von $F(x) = 4x^3 - 3x - \frac{1}{2}$. Es ist einfach überprüft, dass F irreduzibel über $\mathbb{Q}$ ist.

Die anderen Nullstellen sind

$$\begin{aligned} \xi_2 &= \cos\frac{7\pi}{9} = -\cos\frac{2\pi}{9} \\ \xi_3 &= \cos\frac{13\pi}{9} = -\cos\frac{4\pi}{9}. \end{aligned}$$

Und wegen $\cos 2\theta = 2\cos^2\theta - 1$ gilt

$$\begin{aligned} \xi_2 &= 1 - 2{\xi_1}^2 \\ \xi_3 &= 1 - 2{\xi_2}^2. \end{aligned}$$

Es folgt

$$\sigma \text{ fixiert } \xi_1 \Rightarrow \sigma \text{ fixiert } \xi_2 \Rightarrow \sigma \text{ fixiert } \xi_3.$$

Deshalb kann $\pi = (23)$ nicht ein σ bestimmen und das Polynom $F(x)$ ist nicht *ohne Affekt*.

Grob gesagt, bedeutet *ohne Affekt*, dass die Nullstellen $\xi_1, \ldots, \xi_n$ so "unabhängig wie möglich" sind.

Lemma

Seien $\xi_1, \ldots, \xi_n$, paarweise verschieden, in einem Körper von Charakteristik Null, gegeben.

Dann existiert $r \in \mathbb{Z}$ mit

$$0 \leq r \leq N = (n-1)\frac{n!(n!-1)}{2}$$

so dass

$$\xi(\pi) = \xi_{\pi(1)} + r\xi_{\pi(2)} + \cdots + r^{n-1}\xi_{\pi(n)} \qquad (\pi \in S_n)$$

alle verschieden sind.

Beweis

Wenn $\xi(\pi)$ in der obigen Linearkombination vorkommt, dann sind die Gleichungen

$$\xi(\pi_1) = \xi(\pi_2) \qquad (\pi_1 \neq \pi_2 \in S_n)$$

$\frac{n!(n!-1)}{2}$ polynomiale Gleichungen in r, jede höchstens vom Grad $n-1$. Keine dieser Gleichungen ist identisch Null, sonst wäre $\pi_1 = \pi_2$, weil $\xi_1, \ldots, \xi_n$ paarweise verschieden sind.

Also hat jede Gleichung höchstens $n-1$ Nullstellen r. Deshalb ist mindestens eine der Zahlen r im Lemma keine Nullstelle, was bedeutet, dass für dieses r die $\xi(\pi)$ $(\pi \in S_n)$ verschieden sind.

■

Satz

Seien $n \geq 2$ und Variablen $\underline{t} = (t_1, \ldots, t_n), x$ gegeben. Dann existieren $N \geq 0$ und Polynome

$$Q_0(x, \underline{t}), \ldots, Q_N(x, \underline{t}) \quad \in \mathbb{Z}[x, \underline{t}]$$

mit der folgenden Eigenschaft.

Sei k ein beliebiger Körper mit Charakteristik Null. Dann ist für alle $\underline{\tau} = (\tau_1, \ldots, \tau_n) \in k^n$ das Polynom

$$P(x, \underline{\tau}) = x^n - \tau_1 x^{n-1} \pm \ldots + (-1)^n \tau_n \quad \in k[x]$$

ohne Affekt über k genau dann, wenn mindestens eines der Polynome $Q_0(x, \underline{\tau}), \ldots, Q_N(x, \underline{\tau})$ irreduzibel über k ist.

(Vergleiche dazu den Satz im Kapitel 2.)

Beweis

Der Beweis ist ähnlich zum Beweis des Satzes in Kapitel 2.

Wählen wir eine neue Variable $\underline{x} = (x_1, \ldots, x_n)$ und definieren

$$\begin{aligned} \tilde{Q}_r(x, \underline{x}) &= \prod_{\pi \in S_n} \left(x - x_{\pi(1)} - r x_{\pi(2)} - \ldots - r^{n-1} x_{\pi(n)} \right) \\ &= x^{n!} + \ldots \end{aligned}$$

in $\mathbb{Z}[x, \underline{x}]$ für $0 \leq r \leq N$. Wiederum lassen sich diese Polynome mit den elementarsymmetrischen Funktionen $\underline{s} = (s_1, \ldots, s_n)$ von $\underline{x} = (x_1, \ldots, x_n)$ ausdrücken. Deshalb ist

$$\tilde{Q}_r(x, \underline{x}) = Q_r(x, \underline{s}) \qquad (0 \leq r \leq N)$$

was unsere benötigten

$$Q_r(x, \underline{t}) \quad \in \mathbb{Z}[x, \underline{t}] \qquad (0 \leq r \leq N)$$

definiert.

Sei nun k ein Körper mit der Charakteristik Null, sei $\underline{\tau} \in k^n$ und angenommen, $P(x, \underline{\tau})$ sei *ohne Affekt* über k. Wir werden beweisen, dass ein $Q_r(x, \underline{\tau})$ irreduzibel über k ist.

Seien $\xi_1, \ldots, \xi_n$ die Nullstellen von $P(x, \underline{\tau})$ über einem Zerfällungskörper. Nach (a) ist $P(x, \underline{\tau})$ irreduzibel über k und es folgt, dass $\xi_1, \ldots, \xi_n$ verschieden sind. Nach dem Lemma können wir $r \in \mathbb{Z}$ $(0 \leq r \leq N)$ so wählen, dass die

$$\xi(\pi) = \xi_{\pi(1)} + r\xi_{\pi(2)} + \cdots + r^{n-1}\xi_{\pi(n)} \qquad (\pi \in S_n)$$

verschieden sind. Wir behaupten nun, dass dieses $Q_r(x, \underline{\tau})$ irreduzibel über k ist.

Diese Behauptung folgt aus dem Transitivitätslemma. (α) haben wir soeben bewiesen und (β) folgt sofort. Wenn nämlich $\pi_1, \pi_2 \in S_n$ sind, dann liefert (b) ein σ mit $\sigma(\xi_i) = \xi_{\pi(i)}$ mit $\pi = \pi_2 {\pi_1}^{-1}$, so dass

$$\sigma\xi(\pi_1) = \xi(\pi\, \pi_1) = \xi(\pi_2).$$

Somit wäre die erste Hälfte des Satzes bewiesen.

Die andere Hälfte ist ein wenig einfacher. Angenommen, ein $Q_r(x, \underline{\tau})$ sei irreduzibel über k. Dann sind im Speziellen die $\xi(\pi)$ $(\pi \in S_n)$ verschieden für dieses r. Also sind die $\xi_1, \ldots, \xi_n$ alle verschieden. Wir zeigen nun, dass $P(x, \underline{\tau})$ die Bedingung (b) der Definition von *ohne Affekt* erfüllt.

Sei $\pi \in S_n$. Nach (β) gibt es einen Automorphismus σ des Zerfällungskörpers von $Q_r(x, \underline{\tau})$ mit

$$\sigma\left(\xi_1 + r\xi_2 + \cdots + r^{n-1}\xi_n\right) = \xi_{\pi(1)} + r\xi_{\pi(2)} + \cdots + r^{n-1}\xi_{\pi(n)}$$

Dieser Zerfällungskörper ist ein Unterkörper von $k(\xi_1, \ldots, \xi_n)$, also kann σ, wie im Beweis des Transitivitätslemmas, zu einem Automorphismus von $k(\xi_1, \ldots, \xi_n)$ erweitert werden.

Weiter ist jedes $\sigma(\xi_i)$ ein ξ_j, was bedeutet, dass $\sigma(\xi_i) = \xi_{\rho(i)}$ für ein $\rho \in S_n$. Dies wiederum impliziert $\sigma(\xi(\varepsilon)) = \xi(\rho)$ und wir erhalten $\xi(\pi) = \xi(\rho)$. Also sind $\pi = \rho$ und $\sigma(\xi_i) = \xi_{\pi(i)}$ wie in (b).

Nun folgt (a) für $P(x, \underline{\tau})$, in dem wir π mit $\pi(i) = j$ nehmen, σ wie in (β) für $Q_r(x, \underline{\tau})$ konstruieren und das Transitivitätslemma für $P(x, \underline{\tau})$ benutzen. Dies beendet den Beweis.

■

Beispiele

n=2

Das Polynom $P(x, \underline{\tau}) = x^2 - \tau_1 x + \tau_2$ ist genau dann *ohne Affekt*, wenn es irreduzibel ist. Also können wir das einfache Polynom

$$Q_0(x, \underline{t}) = x^2 - t_1 x + t_2$$

mit $N = 0$ benutzen.

n=3

Die obige Konstruktion würde $N = 30$ bedeuten! Sie kann auf folgende Weise vereinfacht werden. Sei

$$\begin{aligned} \tilde{Q}_0(x, \underline{x}) &= (x - x_1 + x_2)(x - x_1 + x_3)(x - x_2 + x_3) \\ &\quad (x - x_2 + x_1)(x - x_3 + x_1)(x - x_3 + x_2) \end{aligned}$$

als ein Polynom $Q_0(x, \underline{t})$ in den elementarsymmetrischen Funktionen

$$\begin{aligned} t_1 &= x_1 + x_2 + x_3 \\ t_2 &= x_1 x_2 + x_2 x_3 + x_3 x_1 \\ t_3 &= x_1 x_2 x_3 \end{aligned}$$

ausgedrückt. Dann ist es wiederum nicht schwer zu überprüfen, dass $N = 0$ ausreichend ist.

Ist $Q_0(x, \underline{\tau})$ zum Beispiel irreduzibel, dann sind die Nullstellen ξ_1, ξ_2, ξ_3 von $P(x, \underline{\tau})$ verschieden und es existiert ein σ mit $\sigma(\xi_1 - \xi_2) = \xi_2 - \xi_1$. Also ist $\sigma = (12)$ und die symmetrische Gruppe wird durch Transposition erzeugt.

Wir finden weiter, dass

$$\begin{aligned} Q_0(x,\underline{t}) &= x^6 - S_1(\underline{t})x^5 + S_2(\underline{t})x^4 - S_3(\underline{t})x^3 \\ &\quad + S_4(\underline{t})x^2 - S_5(\underline{t})x + S_6(\underline{t}) \end{aligned}$$

mit

$$\begin{aligned} S_1 = S_3 = S_5 &= 0 \\ S_2 &= -2{t_1}^2 + 6t_2 \\ S_4 &= {t_1}^4 - 6{t_1}^2 t_2 + 9{t_2}^2 \\ S_6 &= -\Delta \end{aligned}$$

mit der Diskriminante

$$\Delta = -4{t_1}^3 t_3 + {t_1}^2{t_2}^2 + 18t_1t_2t_3 - 4{t_2}^3 - 27{t_3}^2$$

von $P(x,\underline{t})$. Mit anderen Symbolen: $x^3 - ax^2 + bx - c$ ist genau dann *ohne Affekt*, wenn

$$\begin{aligned} &x^6 - (2a^2 - 6b)x^4 + (a^4 - 6a^2b + 9b^2)x^2 \\ &\quad + (4a^3c - a^2b^2 - 18abc + 4b^3 + 27c^2) \end{aligned}$$

irreduzibel ist.

Aus der Galoistheorie erhalten wir ein noch einfacher aussehendes Kriterium, welches folgendes besagt:

> $P(x,\underline{\tau})$ ist genau dann *ohne Affekt*, wenn beide Polynome
>
> $$P(x,\underline{\tau}) \qquad x^2 - \Delta(\tau)$$
>
> irreduzibel sind.

Nun entspricht dies nicht ganz der Aussage aus unserem Satz, welcher verlangt, dass mindestens eines der Polynome Q_r $(0 \leq r \leq N)$ irreduzibel ist.

Galoisgruppensatz

Sei $F(x,t) \in \mathbb{Q}[x,t]$ *ohne Affekt* über $\mathbb{Q}(t)$.

Dann gibt es unendlich viele $\tau \in \mathbb{Z}$, so dass $F(x,\tau) \in \mathbb{Q}[x]$ *ohne Affekt* über $\mathbb{Q}$ ist.

Beweis

Wie im Beweis des Hilbert'schen Irreduzibilitätssatzes reicht es den Fall mit

$$F(x,t) = x^n - f_1(t)x^{n-1} \pm \ldots + (-1)^n f_n(t)$$

zu behandeln. Nach dem vorherigen Satz gibt es ein r $(0 \leq r \leq N)$, so dass $Q_r(x, \underline{f}(t))$ irreduzibel über $\mathbb{Q}(t)$ ist. Nach dem Hilbert'schen Irreduzibilitätssatz gibt es unendlich viele $\tau \in \mathbb{Z}$, so dass dieses $Q_r(x, \underline{f}(\tau))$ irreduzibel über $\mathbb{Q}$ ist.

Wieder nach dem gleichen Satz ist für jedes solches τ das Polynom $F(x, \tau)$ *ohne Affekt* über $\mathbb{Q}$. Dies beendet den Beweis.

■

Anhang A

Satz von Puiseux

In der Literatur existieren viele Beweise zum Satz von Puiseux, aber es gibt wenige, die kurz sind und den Konvergenzaspekt, welcher für unsere Anwendung wichtig ist, abdecken. Die folgende Ausführung folgt im Wesentlichen van der Waerdens Beweis ([10], S. 50-54) bei den formalen Puiseux-Reihen, ergänzt mit einigen zusätzlichen Betrachtungen, um die Konvergenz zu zeigen.

Im Folgenden bezeichnen wir mit $\|\cdot\|$ das Maximum der absoluten Werte der Koeffizienten eines Polynoms in $\mathbb{C}[x]$.

Lemma 1

Seien $P, Q \in \mathbb{C}[x]$ mit Grad $P = p \geq 1$ und Grad $Q = q \geq 1$. Sind P und Q teilerfremd, so existiert ein $c = c(P, Q)$ mit der folgenden Eigenschaft.

Für ein beliebiges $Z \in \mathbb{C}[x]$ mit Grad $Z \leq p + q - 1$ gibt es $X, Y \in \mathbb{C}[x]$ mit Grad $X \leq q - 1$ und Grad $Y \leq p - 1$, so dass gilt:

$$\begin{aligned} PX + QY &= Z \\ \max\{\|X\|, \|Y\|\} &\leq c\|Z\| \end{aligned} \tag{A.1}$$

Beweis

Wenn wir die Gleichung $PX + QY = Z$ ausschreiben und die Koeffizienten auf beiden Seiten vergleichen, erhalten wir ein System von $p + q$ linearen Gleichungen in den $p + q$ unbekannten Koeffizienten von X und Y.

Wenn die Determinante δ ungleich Null ist, könnten wir das System lösen, in dem wir die Cramer'sche Regel ([1], S. 30-32) benutzen. Die Koeffizienten von X und Y wären dann feste lineare Formen in den Koeffizienten von Z und die Abschätzung (A.1) würde sofort folgen.

Da δ eng mit der Resultanten von P und Q verbunden ist und P und Q teilerfremd sind, folgt daraus, das $\delta \neq 0$ ist.

Alternativ können wir auch wie folgt argumentieren: Angenommen δ sei gleich Null. Dann hat das zugehörige System von homogenen linearen Gleichungen eine nichttriviale Lösung. Das bedeutet, dass es $X, Y \in \mathbb{C}[x]$ nicht beide gleich Null gibt, mit Grad $X \leq q - 1$ und Grad $Y \leq p - 1$, mit $PX + QY = 0$.

Nun Q teilt PX, also teilt es X, da P und Q teilerfremd sind. Das bedeutet aber, dass $X = 0$ ist. Auf die gleiche Argumentationsweise erhalten wir $Y = 0$, was zum Widerspruch führt. Deshalb ist δ ungleich Null und der Beweis ist beendet.

■

Sei nun $\mathbb{C}[[z]]$ die Menge aller formalen Potenzreihen $\sum_{k=0}^{\infty} c_k z^k$ in einer Variablen z mit Koeffizienten $c_k \in \mathbb{C}$. Es ist bekannt, dass diese Menge ein Integritätsbereich ist.

Sei $R \subseteq \mathbb{C}[[z]]$ die Untermenge aller Potenzreihen, welche für ein genügend kleines $|z|$ konvergieren; oder äquivalent, für welche es ein $c > 0$ mit $|c_k| \leq c^k$ $k = (1, 2, \ldots)$ gibt. Diese Menge ist ein Unterring, welcher mit der Menge aller Funktionen, analytisch in der Nähe des Ursprungs, identifiziert werden kann.

Um später die Konvergenz zeigen zu können, benötigen wir nun das folgende

Lemma 2

Für $a > 0$, $b > 0$ und $c > 0$ definieren wir die Folge $u_1, u_2, \ldots$ durch $u_1 = ca$ und

$$u_k = ca^k + cb\,(u_1 u_{k-1} + \cdots + u_{k-1}u_1) \qquad (k \geq 2). \qquad \text{(A.2)}$$

Dann liegt $\sum_{k=1}^{\infty} u_k z^k$ in R.

Beweis

Formal erfüllt die Reihe $\Omega(z) = \sum_{k=1}^{\infty} u_k z^k \in \mathbb{C}[[z]]$ die Gleichung

$$\Omega(z) = \frac{caz}{1 - az} + cb\Omega^2(z) = caz + \ldots, \qquad \text{(A.3)}$$

wie aus der Berechnung der Koeffizienten von z^k ersichtlich ist. Die Funktion

$$\tilde{\Omega}(z) = \frac{-1 + \sqrt{1 - \frac{4c^2abz}{1-az}}}{2cb} = caz + \ldots$$

kann mit $\tilde{\Omega}(0) = 0$ als analytisch in der Nähe des Ursprungs definiert werden. Sie erfüllt die analoge Gleichung

$$\tilde{\Omega}(z) = \frac{caz}{1 - az} + cb\tilde{\Omega}^2(z). \qquad \text{(A.4)}$$

Subtrahieren wir (A.4) von (A.3) in $\mathbb{C}[[z]]$, erhalten wir $(\Omega - \tilde{\Omega})\Gamma = 0$ mit

$$\Gamma = 1 - cb\Omega - cb\tilde{\Omega} = 1 - 2c^2abz + \ldots \neq 0$$

Es folgt, dass $\Omega = \tilde{\Omega}$ in R liegt.

■

Das nächste Lemma ist van der Waerdens Version von Hensels Lemma ([10], S. 52), angepasst für Konvergenz-Zwecke.

Lemma 3

Für $p \geq 1$ und $q \geq 1$ sei $\Omega(x, z) \in R[x]$, normiert bezüglich x, mit Grad $Q = p+q$. Angenommen es gibt $P, Q \in \mathbb{C}[x]$, teilerfremd, mit Grad $P = p$ und Grad $Q = q$ und

$$\Omega(x, 0) = P(x)Q(x). \tag{A.5}$$

Dann gibt es $\Phi(x, z), \Psi(x, z) \in R[x]$ mit Grad $\Phi = p$ und Grad $\Psi = q$, $\Phi(x, 0) = P(x)$ und $\Psi(x, 0) = Q(x)$, und

$$\Omega(x, z) = \Phi(x, z)\Psi(x, z). \tag{A.6}$$

Beweis

Wir definieren $B_0 = P$ und $C_0 = Q$ und konstruieren $B_1, B_2, \ldots \in \mathbb{C}[x]$ mit Grad $B_1, B_2, \ldots \leq p - 1$ und $C_1, C_2, \ldots \in \mathbb{C}[x]$ mit Grad $C_1, C_2, \ldots \leq q - 1$ so, dass (A.6) mit

$$\begin{aligned} \Phi(x, z) &= B_0 + B_1 z + B_2 z^2 + \ldots \\ \Psi(x, z) &= C_0 + C_1 z + C_2 z^2 + \ldots \end{aligned}$$

korrekt ist. Gilt nun

$$\Omega(x, z) = A_0 + A_1 z + A_2 z^2 + \ldots$$

mit $A_0, A_2, \ldots \in \mathbb{C}[x]$, so ist dies äquivalent zum Gleichungssystem

$$B_0 C_0 = A_0 \tag{A.7}$$

$$B_0 C_1 + B_1 C_0 = A_1 \tag{A.8}$$

$$B_0 C_k + B_1 C_{k-1} + \cdots + B_{k-1} C_1 + B_k C_0 = A_k \qquad (k \geq 2). \tag{A.9}$$

Um das zu zeigen benutzen wir Induktion.

Wegen (A.5) ist (A.7) richtig. Angenommen $k \geq 1$ und $B_0, \ldots, B_{k-1}, C_0, \ldots, C_{k-1}$ sind so konstruiert, dass (A.8) und (A.9) für Werte kleiner als k stimmen. Das Polynom $Z = A_1$ bzw.

$$Z = A_k - B_1 C_{k-1} - \cdots - B_{k-1} C_1 \ (k \geq 2)$$

hat höchstens Grad $p + q - 1$, weil $k \geq 1$ und $\Omega(x, z)$ normiert ist.

Also gibt es nach Lemma 1 $X = C_k, Y = B_k \in \mathbb{C}[x]$ mit Grad $X \leq q - 1$ und Grad $Y \leq p - 1$, so dass (A.8) und (A.9) zutreffen. Dies beendet den Induktionsbeweis und es bleibt die Konvergenz zu prüfen.

Nun ist $\Omega(x, z) = A_0 + A_1 z + \ldots \in R[x]$. Es folgt, dass es ein $a > 0$ mit

$$\|A_k\| \leq a^k \ (k \geq 1)$$

gibt. Lemma 1 liefert nun

$$M_k \leq c\|Z\|$$

für $M_k = \max\{\|B_k\|, \|C_k\|\}$. Auch gilt $\|Z\| = \|A_1\|$ bzw.

$$\|Z\| \leq \|A_k\| + b\,(\|B_1\| \cdot \|C_{k-1}\| + \cdots + \|B_{k-1}\| \cdot \|C_1\|) \qquad (k \geq 2)$$

mit $b = \min\{p, q\}$. Es folgt, dass $M_1 \leq ca$ und

$$M_k \leq ca^k + cb\,(M_1 M_{k-1} + \cdots + M_{k-1} M_1) \qquad (k \geq 2).$$

Eine einfache Induktion zeigt, dass $0 \leq M_k \leq u_k$, mit u_k wie in Lemma 2, gilt. Weil $\sum_{k=1}^{\infty} u_k z^k$ in R liegt, folgt dass $\sum_{k=1}^{\infty} M_k z^k$ in R liegt. Also liegen $\sum_{k=1}^{\infty} B_k z^k$ und $\sum_{k=1}^{\infty} C_k z^k$ in $R[x]$ und dies impliziert das Gleiche für $\Phi(x, z)$ und $\Psi(x, z)$. Der Beweis ist somit beendet.

■

Wir können nun wie in van der Waerdens Beweis [10] das Hauptresultat der Puiseux-Erweiterungen herleiten.

Der Quotientenkörper K von R besteht bekannterweise aus allen Laurent-Reihen in z, welche mindestens endlich viele negative Potenzen enthalten und für genügend kleine $|z| > 0$ konvergent sind. Wenn wir formal z durch $z^{\frac{1}{e}}$ ersetzen, für ein $e \geq 1$ in $\mathbb{Z}$, erhalten wir einen neuen Körper K_e. Die Vereinigung L von allen Körpern K_e $(e \geq 1)$ ist ebenfalls ein Körper.

Satz (Puiseux)

Der Körper L ist algebraisch abgeschlossen.

Beweis

Es reicht zu überprüfen, dass für jedes

$$\Omega(x, z) = x^n + \Omega_1 x^{n-1} + \cdots + \Omega_n \in K[x]$$

ein $\omega \in L$ mit $\Omega(\omega, z) = 0$ existiert. Dann können wir z im allgemeinen Polynom in $L[x]$ durch ein z^e $(e \geq 1)$ ersetzen, indem wir bemerken, dass L unter der umgekehrten Operation abgeschlossen ist.

Die Argumentation erfolgt durch Induktion über n. Der Fall $n = 1$ ist klar, also können wir $n \geq 2$ annehmen. Indem wir x durch $x - \frac{1}{n}\Omega_1$ ersetzen, können wir vorraussetzen, dass $\Omega_1 = 0$ ist. Im Allgemeinen, wenn $\Omega_i \neq 0$ ist, setzen wir voraus, dass

$$\Omega_i = a_i z^{m_i} + \ldots \qquad (1 \leq i \leq n)$$

mit $a_i \neq 0$ in $\mathbb{C}$ und $m_i \in \mathbb{Z}$ sei. Ist $\Omega_i = 0$ für jedes i, so ist das Resultat mit $\omega = 0$ offensichtlich, ansonsten nehmen wir an, dass μ der kleinste Quotient $\frac{m_i}{i}$ mit $\Omega_i \neq 0$ ist. Wir definieren durch $x = \tilde{x} z^{\mu}$ eine neue Variable $\tilde{x}$ und erhalten

$$z^{-\mu n}\Omega(x,z) = \tilde{x}^n + \tilde{\Omega}_2(z)\tilde{x}^{n-2} + \cdots + \tilde{\Omega}_n(z) \tag{A.10}$$

mit $\tilde{\Omega}_i(z) = 0$ bzw.

$$\tilde{\Omega}_i(z) = a_i z^{m_i - \mu i} + \ldots$$

Weil im letzteren Fall $m_i \geq \mu i$ gilt, ist klar dass jedes $\tilde{\Omega}_i(z) \in \mathbb{C}\left[\left[z^{\frac{1}{e}}\right]\right]$ für ein $e \geq 1$ in $\mathbb{Z}$ ist (zum Beispiel für den Nenner von μ).

Wenden wir Lemma 3 auf

$$\tilde{\Omega}(\tilde{x},\tilde{z}) = \tilde{x}^n + \tilde{\Omega}_2(\tilde{z}^e)\tilde{x}^{n-2} + \cdots + \tilde{\Omega}_n(\tilde{z}^e) \tag{A.11}$$

an. Die Koeffizienten sind im Ring $\tilde{R}$ der konvergenten Potenzreihen in $\mathbb{C}[[\tilde{z}]]$. Und

$$\tilde{\Omega}(\tilde{x},0) = \tilde{x}^n + \tilde{\Omega}_2(0)\tilde{x}^{n-2} + \cdots + \tilde{\Omega}_n(0).$$

Es gibt aber i mit $\mu = \frac{m_i}{i}$ und für diesen Wert gilt $\tilde{\Omega}_i(0) = a_i \neq 0$. Also ist $\tilde{\Omega}(\tilde{x},0)$ ungleich $\tilde{x}^n$ und ebenfalls ungleich $(\tilde{x}-a)^n$ für ein $a \neq 0$, weil der Koeffizient von $\tilde{x}^{n-1}$ Null ist. Also hat $\tilde{\Omega}(\tilde{x},0)$ wie in (A.5) eine Faktorisation in teilerfremde, nichtkonstante Polynome in $\mathbb{C}[\tilde{x}]$.

Lemma 3 liefert deshalb eine Faktorisation (A.6) von $\tilde{\Omega}(\tilde{x},\tilde{z})$ in $\tilde{R}[\tilde{x}]$ in Faktoren mit kleinerem Grad. Die Induktionsannahme ergibt $\tilde{\omega}$ mit $\tilde{\Omega}(\tilde{\omega},\tilde{z}) = 0$. Wenn wir $\tilde{z}$ durch $z^{\frac{1}{e}}$ ersetzen, erhalten wir via (A.10) und (A.11) das benötigte $\omega \in L$ mit $\Omega(\omega,z) = 0$. Dies beendet den Beweis.

■

Nun können wir die Version aus Kapitel 1 herleiten. Sei $F(x,t) \in \mathbb{C}[x,t]$ mit $\mathrm{Grad}_x F = n$ und $\mathrm{Grad}_t F = r$. Dann ist $z^r F\left(x,\frac{1}{z}\right) = \Omega(x,z) \in \mathbb{C}[x,z] = \mathbb{C}[z][x] \subset L[x]$. $\Omega(x,z)$ zerfällt deshalb in

$$\Omega(x,z) = A(x-\omega_1)\cdots(x-\omega_n)$$

mit $A \neq 0$ in $\mathbb{C}[z]$ und $\omega_1,\ldots,\omega_n \in L$.

Nehmen wir nun an, dass $\tau \neq 0$ in $\mathbb{C}$ so gross ist, dass $\omega_1,\ldots,\omega_n$ in $z = \frac{1}{\tau}$ konvergieren. Wir schliessen

$$\begin{aligned} F(x,\tau) &= \tau^r \Omega\left(x,\frac{1}{\tau}\right) \\ &= \tau^r A\left(\frac{1}{\tau}\right)\left(x-\omega_1\left(\frac{1}{\tau}\right)\right)\cdots\left(x-\omega_n\left(\frac{1}{\tau}\right)\right). \end{aligned}$$

Nun sei $\xi \in \mathbb{C}$ eine beliebige Lösung von $F(\xi,\tau) = 0$. Wenn τ auch so gross ist, dass $A\left(\frac{1}{\tau}\right) \neq 0$ ist, beenden wir den Beweis, indem wir $x = \xi$ setzen und $\xi = \omega_i\left(\frac{1}{\tau}\right)$ für ein i $(1 \leq i \leq n)$ schliessen. Diese Werte haben dann die benötigte Form.

Beispiel

Sei $F(x,t) = x^4 - x - t$. Dann ist $\Omega(x,z) = x^4 - x - \frac{1}{z}$ im Beweis des Satzes von Puiseux. Also ist $\Omega_1 = \Omega_2 = 0$ und

$$\Omega_3 = -1 \qquad \Omega_4 = -\frac{1}{z}$$

mit $m_3 = 0$ und $m_4 = -1$. Somit ist $\mu = -\frac{1}{4}$ und wir können $e = 4$ nehmen.

Also sind $x = \tilde{x}z^{-\frac{1}{4}}$, $\tilde{z} = z^{\frac{1}{4}}$ und

$$\tilde{\Omega}(\tilde{x},\tilde{z}) = z\Omega(x,z) = \tilde{x}^4 - \tilde{z}^3\tilde{x} - 1.$$

Deshalb kann $\tilde{\Omega}(\tilde{x},0) = \tilde{x}^4 - 1$ zum Beispiel in $(\tilde{x}-1)Q(\tilde{x})$ faktorisiert werden. Hensels Lemma ergibt dann $\tilde{\Omega}(\tilde{x},\tilde{z}) = \Phi(\tilde{x},\tilde{z})\Psi(\tilde{x},\tilde{z})$ mit

$$\Phi(\tilde{x},\tilde{z}) = \tilde{x} - \tilde{\omega} \qquad \tilde{\omega}(\tilde{z}) = 1 + \ldots \in \mathbb{C}[[\tilde{z}]]$$

Wir $\Omega(\omega,z) = 0$ mit

$$\omega(z) = z^{-\frac{1}{4}}\tilde{\omega}\left(z^{\frac{1}{4}}\right) = z^{-\frac{1}{4}} + \ldots$$

im Körper k_4. Deshalb ist $F(\varphi_1,t) = 0$ mit

$$\varphi_1(t) = \omega\left(\frac{1}{t}\right) = t^{\frac{1}{4}} + \ldots.$$

Auf die gleiche Weise führen die Faktoren $\tilde{x} - i$, $\tilde{x} + 1$, $\tilde{x} + i$, $\tilde{x}^4 - 1$ zu den Folgen

$$\begin{aligned}\varphi_2(t) &= it^{\frac{1}{4}} + \ldots \\ \varphi_3(t) &= -t^{\frac{1}{4}} + \ldots \\ \varphi_4(t) &= -it^{\frac{1}{4}} + \ldots\end{aligned}$$

und schliesslich zu einer kompletten Faktorisierung

$$x^4 - x - t = (x - \varphi_1)(x - \varphi_2)(x - \varphi_3)(x - \varphi_4).$$

Literaturverzeichnis

[1] Michael Artin: *Algebra*
Birkhäuser (1993)

[2] G.A. Bliss: *Algebraic functions*
American Mathematical Society Colloquial Publications 16 (1933)

[3] Karl Dörge: *Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes*
Mathematische Annalen 96 (1927) pp. 176-182

[4] Martin Eichler: *Zum Hilbertschen Irreduzibilitätssatz*
Mathematische Annalen 116 (1939) pp. 742-748

[5] Wolfgang Franz: *Untersuchungen zum Hilbert'schen Irreduzibilitätssatz*
Mathematische Zeitschrift 33 (1931) pp. 275-293

[6] M. Fried: *On Hilbert's Irreducibility Theorem*
Journal of Number Theory (1974) pp. 211-232

[7] David Hilbert: *Über die Irreduciblität ganzer rationaler Functionen mit ganzzahligen Coefficienten*
Journal für Mathematik 110 (1892) pp. 104-129

[8] Andrzej Schinzel: *On Hilbert's Irreducibility Theorem*
Ann. Polon. Math. 16 (1965)

[9] Andrzej Schinzel: *Selected Topics on Polynomials*
Univercity of Michigan Press (1982)

[10] Bartel L. van der Waerden: *Einführung in die Algebraische Geometrie*
Springer (1939)