Diplomarbeit

# Über Sätze von Schur und Coleman aus der Galoistheorie

Orges Leka

27.05.2010

Betreuer: Prof. Dr. M. Lehn

Fachbereich 08 - Physik, Mathematik und Informatik
Johannes Gutenberg-Universität Mainz

# Inhaltsverzeichnis

**Einleitung** **4**

**1 Hilfssätze aus der algebraischen Zahlentheorie** **5**
1.1 Newton-Polygon . . . . . 5
1.2 Differente, Diskriminante, Dedekind . . . . . 8

**2 Hilfssätze aus der analytischen Zahlentheorie** **11**
2.1 Der Satz von Tschebyscheff-Bertrand . . . . . 11
2.2 Ein Satz von Schur-Sylvester . . . . . 14

**3 Hilfssätze aus der Gruppentheorie** **19**
3.1 Kranzprodukte und imprimitive Gruppen . . . . . 19
3.2 Transitive Gruppen . . . . . 21

**4 Die Galoisgruppe von $E_n(x)$ nach Schur** **24**
4.1 Allgemeine Sätze zur Berechnung von Galoisgruppen . . . . . 24
4.2 Konkrete Berechnungen zu $E_n(x)$ . . . . . 26

**5 Die Galoisgruppe von $E_n(x)$ nach Coleman** **30**

**6 Beobachtungen zu $C_n(x)$** **34**

# Einleitung

In dieser Arbeit werden wir zwei im wesentlichen verschiedene Wege vorstellen folgenden Satz von Schur zu beweisen:

> Die Galoisgruppe über $\mathbb{Q}$ des exponentiellen Taylorpolynoms $E_n(x) = \sum_{k=0}^{n} \frac{x^k}{k!}$ ist die symmetrische Gruppe $S_n$ falls $n \not\equiv 0 \mod (4)$ und die alternierende Gruppe $A_n$ sonst.

Die eigentliche Motivation in dieser Arbeit bestand darin die Galoisgruppen des Taylorpolynoms $C_n(x) = \sum_{k=0}^{n} \frac{x^{2k}}{(2k)!}$ zu berechnen. Eine Überprüfung für kleinere Grade n legt nämlich nahe zu vermuten die Galoisgruppe von $C_n(x)$ über $\mathbb{Q}$ ist $S_2 \wr S_n$, das Kranzprodukt aus $S_2$ mit $S_n$. Die Hoffnung, dass man dies beweisen könnte wurde durch den eben erwähnten Satz von Schur geweckt. Der Beweis von Schur benutzt einige Sätze aus der analytischen Zahlentheorie, die für sich genommen, bemerkenswert sind (etwa den Satz von Schur-Sylvester über die Teilbarkeit von aufeinanderfolgenden ganzen Zahlen durch gewisse Primzahlen) und Sätze von Dedekind aus der algebraischen Zahlentheorie. Dies erschwert den Zugang zum Satz über die Galoisgruppe, wenn man nur an diesen interessiert ist. Einen anderen Beweis des Schurschen Satzes über die Galoisgruppe von $E_n(x)$ fand Coleman. In diesem benutzt er Newton-Polygone und kommt relativ schnell zum gewünschten Ergebnis. Er vermeidet dadurch die Benutzung des Satzes von Schur-Sylvester aus der analytischen Zahlentheorie und auch die Benutzung der Sätze aus der algebraischen Zahlentheorie, die Schur verwendet. Beiden Zugängen, also denen von Schur und Coleman ist gemeinsam, dass sie den Satz von Tschebyscheff-Bertrand (Für $n \geq 8$ gibt es immer eine Primzahl $p, n/2 < p < n-2$) und einen Satz von Jordan aus der Gruppentheorie benutzen. Der Jordansche Satz gibt handliche Kriterien wann eine Gruppe $G$ die volle symmetrische Gruppe $S_n$ oder die alternierende Gruppe $A_n$ ist. Der Beweis, dass die Galoisgruppe von $C_n(x)$ über $\mathbb{Q}$ die Gruppe $S_2 \wr S_n$ ist, konnte leider im Rahmen dieser Arbeit nicht erbracht werden. Beim Versuch diese Vermutung zu beweisen stößt man unter anderem auf Schwierigkeiten zu zeigen, wann eine Untergruppe $G \leq S_2 \wr S_n$ die volle Gruppe $G = S_2 \wr S_n$ ist. Der Autor kennt leider keinen Satz über die $S_2 \wr S_n$, der handliche Kriterien dafür liefert, wie es der Jordansche Satz für die symmetrische Gruppe $S_n$ tut. Wir konnten jedoch mit den Methoden von Schur und Coleman zeigen, dass die Galoisgruppe von $\sum_{k=0}^{n} \frac{x^k}{(2k)!}$ über $\mathbb{Q}$ die alternierende oder die symmetrische Gruppe ist.

# Kapitel 1

# Hilfssätze aus der algebraischen Zahlentheorie

## 1.1 Newton-Polygon

Wir fangen mit der Definition und Eigenschaften von Newton-Polygonen an. (Siehe hierzu Neukirch, Algebraische Zahlentheorie oder Goueva, p-adic Numbers).

**Definition 1.1 (Newton-Polygon)** *Sei $v$ eine beliebige exponentielle Bewertung des Körpers $K$ und sei $f(x) = a_0+a_1x+\ldots+a_nx^n$ ein Polynom aus $K[x]$ mit $a_0a_n \neq 0$. Zu jedem Term $a_ix^i$ assoziieren wir einen Punkt $(i, v(a_i)) \in \mathbb{R}^2$ und ignorieren den Punkt $(i, \infty)$ falls $a_i = 0$. Nun nehmen wir die untere konvexe Hülle der Punkte $\{(0, v(a_0)), (1, v(a_1)), \ldots, (n, v(a_n))\}$. Dies liefert uns eine Polygon-Kette, welche als das Newton-Polygon von $f(x)$ bezeichnet wird.*

Beispielsweise ist das Newton-Polygonn von $f(x) = 6+9x+10x^3+12x^4$ bezüglich der Bewertung $v_2$ gegeben durch

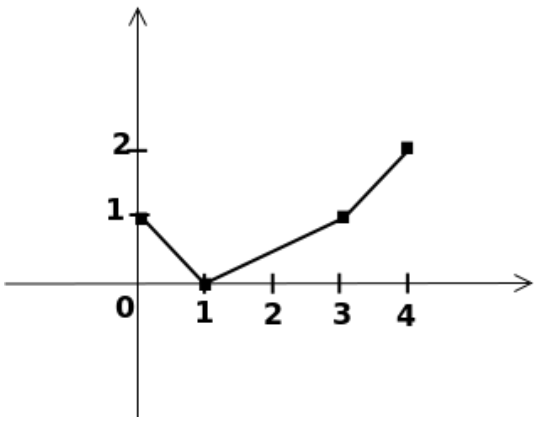


Abbildung 1.1: Newton-Polygon von $f(x) = 6 + 9x + 10x^3 + 12x^4$ bzgl. 2

Während das gleiche Polynom zur Bewertung $v_3$ das Newton-Polygon hat, welches in Abbildung 1.2 zu sehen ist.

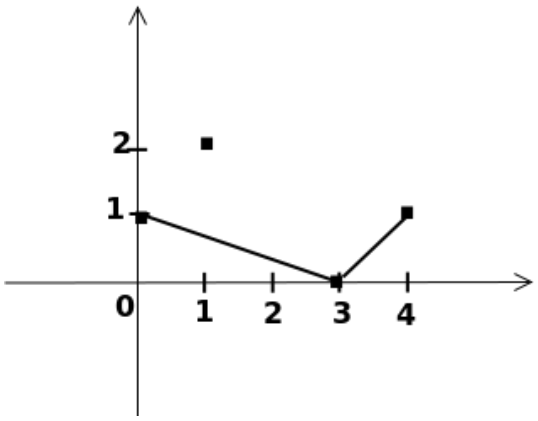


Abbildung 1.2: Newton-Polygon von $f(x) = 6 + 9x + 10x^3 + 12x^4$ bzgl. 3

Wie wir in diesem Beispiel sehen und wie man sich leicht überlegt besteht das Polygon aus Liniensegmenten $S_1, S_2, \ldots$ dessen Steigungen strikt monoton wachsen und die folgende Eigenschaft haben (siehe Neukirch):

**Satz 1.1 (Die Länge der Liniensegmente im Newton-Polygon)** *Sei $f(x) = a_0 + a_1x + \ldots + a_nx^n, a_0a_n \neq 0$ ein Polynom über dem Körper $K$, $v$ eine exponentielle Bewertung von $K$ und $w$ eine Erweiterung von $v$ zum Zerfällungskörper $L$ von $f$. Falls $(r, v(a_r)) - (s, v(a_s))$ ein Liniensegment mit Steigung $-m$ ist, welche im Newton-Polygon von $f$ auftaucht, dann hat $f(x)$ genau $s-r$ Nullstellen $\alpha_1, \ldots, \alpha_{s-r}$ mit Bewertung $w(\alpha_1) = \ldots = w(\alpha_{s-r}) = m$.*

Beweis:(zu finden bei Neukirch, Seite 145 / 146) Teilung durch $a_n$ bewegt das Polygon nur nach oben oder nach unten. Wir können also ohne Einschränkung $a_n = 1$ annehmen. Die Nullstellen $\alpha_1, \ldots, \alpha_n \in L$ von $f$ nummerieren wir so, dass gilt

$$\begin{aligned} w(\alpha_1) = \ldots = w(\alpha_{s_1}) &= m_1, \\ w(\alpha_{s_1+1}) = \ldots = w(\alpha_{s_2}) &= m_2, \\ \ldots \quad \ldots \quad \ldots & \\ w(\alpha_{s_t+1}) = \ldots = w(\alpha_n) &= m_{t+1} \end{aligned}$$

wobei $m_1 < m_2 < \ldots < m_{t+1}$. Wir betrachten die Koeffizienten $a_i$ als elementarsymmetrische Funktionen der Nullstellen $\alpha_j$ und stellen fest, dass

$$\begin{aligned} v(a_n) &= v(1) = 0, \\ v(a_{n-1}) &\geq \min_i\{w(\alpha_j)\} = m_1 \\ v(a_{n-2}) &\geq \min_{i,j}\{w(\alpha_i\alpha_j)\} = 2m_1 \\ \ldots \quad \ldots \quad \ldots & \\ v(a_{n-s_1}) &\geq \min_{i_1,\ldots,i_{s_1}}\{w(\alpha_{i_1} \cdots \alpha_{i_{s_1}})\} = s_1m_1 \end{aligned}$$

wobei die letzte Gleichung gilt, da die Bewertung von $\alpha_1 \cdots \alpha_{s_1}$ kleiner ist als die der anderen,

$$\begin{aligned} v(a_{n-s_1-1}) &\geq \min_{i_1,\ldots,i_{s_1+1}} \{w(\alpha_{i_1} \ldots \alpha_{i_{s_1+1}})\} = s_1 m_1 + m_2 \\ v(a_{n-s_1-2}) &\geq \min_{i_1,\ldots,i_{s_1+2}} \{w(\alpha_{i_1} \ldots \alpha_{i_{s_1+2}})\} = s_1 m_1 + 2m_2 \\ &\ldots \ \ldots \ \ldots \\ v(a_{n-s_2}) &\geq \min_{i_1,\ldots,i_{s_2}} \{w(\alpha_{i_1} \ldots \alpha_{i_{s_2}})\} = s_1 m_1 + (s_2 - s_1) m_2 \end{aligned}$$

und so weiter. Hieraus folgt, dass die Kanten des Newton-Polygons von rechts nach links gegeben sind durch $(n, 0), (n - s_1, s_1 m_1), (n - s_2, s_1 m_1 + (s_2 - s_1)m_2), \ldots$. Die Steigung der Kante ganz rechts ist dann gegeben durch

$$\frac{0 - s_1 m_1}{n - (n - s_1)} = -m_1$$

Betrachten wir die nächsten Kanten nach links, so haben diese die Steigung

$$\frac{(s_1 m_1 + \ldots + (s_j - s_{j-1})m_j) - (s_1 m_1 + \ldots + (s_{j+1} - s_j)m_{j+1})}{(n - s_j) - (n - s_{j+1})} = -m_{j+1}$$

□

**Lemma 1.1** *Wir behalten die Bezeichnungen des vorigen Satzes bei. Falls die Bewertung $v$ auf dem Zerfällungskörper $L$ von $f$ eindeutig fortgesetzt werden kann zur Bewertung $w$, so ist*

$$f(x) = \prod_{j=1}^{r} f_j(x)$$

*eine Faktorisierung über $K$, d.h. $f_j(x) = \prod_{w(\alpha_j)=m_j}(x - \alpha_i)$ ist ein Polynom aus $K[x]$.*

Beweis: Wir können annehmen, dass $a_n = 1$. Ist zunächst $f(x)$ irreduzibel, so hat man $\alpha_i = \sigma_i \alpha$ für ein $\sigma_i$ aus $G(L/K)$, wegen der Transitivität der Galoisgruppe $G(L/K)$ auf die Nullstellen von $f$. Da für jede Erweiterung $w$ von $v$, $w \circ \sigma_i$ ebenfalls eine Erweiterung von $v$ ist, folgt aus der Eindeutigkeit der Fortsetzung von $v$, dass $w(\alpha_i) = w(\sigma_i \alpha_i) = m_1$, also $f_1(x) = f(x)$ und die Behauptung ist bewiesen. Der allgemeine Fall folgt durch Induktion nach $n$. Für $n = 1$ ist nichts zu zeigen. Sei $p(x)$ das Minimalpolynom von $\alpha_1$ und $g(x) = \frac{f(x)}{p(x)} \in K[x]$. Da alle Nullstellen von $p(x)$ die gleiche Bewertung $m_1$ haben, ist $p(x)$ ein Teiler von $f_1(x)$. Sei $g_1(x) = \frac{f_1(x)}{p_1(x)}$. Die Faktorisierung von $g(x)$ ist nach dem vorigen Satz $(\ldots)$ gegeben durch

$$g(x) = g_1(x) \cdot \prod_{j=2}^{r} f_j(x)$$

Da $deg(g(x)) < deg(f(x))$, folgt dass $f_j(x)$ ein Polynom aus $K[x]$ ist für alle $j = 1, 2, \ldots, r$. □

**Lemma 1.2** *Sei $f(x)$ ein separables Polynom aus $k[x]$, $K$ der Zerfällungskörper von $f(x)$, $G = Gal(K/k)$. Weiterhin sei $f(x) = f_1(x) \cdots f_r(x)$ die Zerlegung von $f(x)$ in irreduzible Faktoren aus $k[x]$ und $n_i = deg(f_i(x))$ für $i = 1, 2 \ldots, r$. Dann ist jedes $n_i$ ein Teiler von $|G|$.*

Beweis: Sei $\Omega$ die Nullstellenmenge von $f(x)$ und $\Omega_i$ die Nullstellenmenge von $f_i(x)$. Dann ist $K_i := k(\Omega_i)$ der Zerfällungskörper von $f_i(x)$. Wegen $\Omega_i \subset \Omega$, ist $K_i = k(\Omega_i) \subset k(\Omega) = K$, d.h. $K_i$ ist ein Zwischenkörper von $K/k$. Die Behauptung folgt, weil $n_i = deg(f_i(x))$ ein Teiler von $[K_i : k]$ ist und da $[K : K_i] \cdot [K_i : k] = [K : k] = |Gal(K/k)| = |G|$. □

**Satz 1.2 (Hauptsatz über Newton-Polygone)** *Sei $p$ eine Primzahl und $f(x)$ ein Polynom aus $\mathbb{Q}_p[x]$ mit Ecken $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$ im Newton-Polygon von $f$. Dann ist die Zerlegung von $f(x)$ über $\mathbb{Q}_p$ gegeben durch*

$$f(x) = f_1(x) \cdot f_2(x) \cdots f_r(x),$$

*wobei der Grad von $f_j$ gleich $x_j - x_{j-1}$ ist und alle Nullstellen von $f_j(x)$ in $\bar{\mathbb{Q}}_p$ haben Bewertung*

$$-\frac{y_j - y_{j-1}}{x_j - x_{j-1}}$$

*Ist $f(x)$ separabel über $\mathbb{Q}_p$, so ist die Ordnung der Galoisgruppe über $\mathbb{Q}_p$ teilbar durch $x_j - x_{j-1}$.*

Beweis: Der erste Teil der Aussage folgt aus dem Lemma (1.1) und der zweite Teil folgt aus dem letzten Lemma. □

## 1.2 Differente, Diskriminante, Dedekind

**Lemma 1.3 (Transitivität von Differente und Diskriminante)** *Seien $K \subset K' \subset L$ endliche Erweiterungen von Zahlkörpern. Für die Differente $\mathcal{D}_{L/K}$ und die Diskriminante $D_{L/K}$ gelten folgende Formeln:*

$$\mathcal{D}_{L/K} = \mathcal{D}_{K'/K} \cdot \mathcal{D}_{L/K'}$$
$$D_{L/K} = (D_{K'/K})^{[L:K']} \cdot \mathcal{N}_{K'/K}(D_{L/K'})$$

Beweis: Seite 228, Kapitel 16, Proposition 3.
Leutbecher, Zahlentheorie, Eine Einführung in die Algebra, Springer 1996 □

**Satz 1.3 (Dedekindscher Differentensatz)** *Sei $K'/K$ eine Erweiterung von Zahlkörpern mit Relativdifferente $\mathcal{D}_{K'/K}$ und mit Ganzheitsringen $\mathbb{Z}_{K'}$ und $\mathbb{Z}_K$. Für jedes Primideal $\mathcal{P}' \neq 0$ von $\mathbb{Z}_{K'}$ mit dem in $\mathbb{Z}_K$ zugeordneten Primideal $\mathcal{P} = \mathcal{P}' \cap \mathbb{Z}_{K'}$ und dem Verzweigungsindex $e = e(\mathcal{P}'/\mathcal{P})$ gilt:*

$$v_{\mathcal{P}'}(\mathcal{D}_{K'/K}) = e - 1, \text{ falls } e \not\equiv 0 \mod p$$
$$v_{\mathcal{P}'}(\mathcal{D}_{K'/K}) \geq e, \text{ falls } e \equiv 0 \mod p$$

*Dabei ist $p$ die in $\mathcal{P}$ enthaltene rationale Primzahl.*

Beweis: Sei $L/K$ eine Galoiserweiterung, die $K'$ als Zwischenkörper enthält, $\mathbb{P}$ ein Primideal des Ganzheitsringes $\mathbb{Z}_L$ von $L$. Seien $G = Gal(L/K)$, $G' = Gal(L/K')$ die Galoisgruppen und seien $G_n$, $G'_n$ die Hilbertschen Verzweigungsgruppen (Ist $G_0 = \{\sigma \in G | \sigma(\mathbb{P}) = \mathbb{P}\}$ die Zerlegungsgruppe von $\mathbb{P}$, so ist für
$n \geq 0$, $G_n = \{\sigma \in G_0 | v_{\mathbb{P}}(\sigma(\alpha) - \alpha) \geq n+1 \ \forall \alpha \in \mathbb{Z}_L\}$)
des Primideals $\mathbb{P}$ bezüglich $K$ bzw. $K'$. Wie man sich überlegt ist $G'_n = G_n \cap G'$. Nach den Hilbertformel für die Verzweigungsgruppen (Leutbecher, Seite 234)gilt zudem

$$v_{\mathbb{P}}(\mathcal{D}_{L/K}) = \sum_{n=0}^{\infty} |G_n| - 1$$
$$v_{\mathbb{P}}(\mathcal{D}_{L/K'}) = \sum_{n=0}^{\infty} |G'_n| - 1$$

Wegen der Transitivität der Differente gilt $\mathcal{D}_{L/K} = \mathcal{D}_{L/K'} \cdot \mathcal{D}_{K'/K}$. Damit folgt nach Anwenden von $v_{\mathbb{P}}$ auf die letzte Gleichung:

$$\begin{aligned} v_{\mathbb{P}}(\mathcal{D}_{K'/K}) &= v_{\mathbb{P}}(\mathcal{D}_{L/K}) - v_{\mathbb{P}}(\mathcal{D}_{L/K'}) \\ &= \sum_{n=0}^{\infty} |G_n| - |G'_n| \end{aligned}$$

Die Ordnungen der Trägheitsgruppen $G_0$ bzw. $G'_0$ sind $e(\mathbb{P}|\mathcal{P})$ bzw. $e(\mathbb{P}|\mathcal{P}') = e'$ und wegen der Multiplikativität der Verzweigungsindizes ist $|G_0| = e(\mathbb{P}|\mathcal{P}')e(\mathcal{P}'|\mathcal{P}) = e'e$. Damit folgt

$$\begin{aligned} v_{\mathcal{P}'}(\mathcal{D}_{K'/K}) &= \frac{1}{e'} v_{\mathbb{P}}(\mathcal{D}_{K'/K}) \\ &= \frac{1}{e'} \sum_{n=0}^{\infty} |G_n| - |G'_n| \geq \frac{1}{e'}(|G_0| - |G'_0|) \\ &= \frac{1}{e'}(e'e - e') = e - 1 \end{aligned}$$

Die größte Potenz von $p$, die in $|G_0| = [G_0 : G_1] \cdot |G_1|$ bzw.$|G'_0| = [G'_0 : G'_1] \cdot |G'_1|$ aufgeht, ist $|G_1|$ bzw. $|G'_1|$ (siehe Zusatz zu Satz 11, Kapitel 15.8, Seite 223, Leutbecher). Wegen $[G_0 : G_1] \cdot |G_1| = [G'_0 : G'_1] \cdot |G'_1| \cdot e$, ist $e \not\equiv 0 \mod p$ genau dann wenn $|G_1| = |G'_1|$. In diesem Fall ist aber wegen $G'_n = G_n \cap G'$ und da die Folgen $G_n, G'_n$ monoton sind, auch $G_n = G'_n$ für $n \geq 1$. Hieraus folgt dann:

$$\begin{aligned} v_{\mathcal{P}'}(\mathcal{D}_{K'/K}) &= \frac{1}{e'} \sum_{n=0}^{\infty} |G_n| - |G'_n| \\ &= \frac{1}{e'}(|G_0| - |G'_0|) = e - 1 \end{aligned}$$

Ist aber $e \equiv 0 \mod p$, so ist nach dem eben Gesagtem $|G_1| < |G_1'|$ und es folgt $v_{\mathcal{P}'}(\mathcal{D}_{K'/K}) > e - 1$, also $v_{\mathcal{P}'}(\mathcal{D}_{K'/K}) \geq e$. □

Wir wollen noch einen anderen Satz von Dedekind erwähnen, den Schur braucht, um zu entscheiden ob die Diskriminante eines irreduziblen Polynoms durch eine höhere Potenz einer Primzahl geteilt wird als die Diskriminante eines Zahlkörpers, der durch hinzufügen einer beliebigen Nullstelle des Polynoms entsteht:

**Satz 1.4 (Dedekind-Kriterium)** *Sei $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n$ ein ganzzahliges, in $\mathbb{Q}[x]$ irreduzibles Polynom mit Diskriminante $\Delta$. Sei $D$ die Diskriminante des Körpers $\mathbb{Q}(\alpha)$ wobei $\alpha$ eine beliebige Nullstelle von $f$ ist. Sei $p$ eine Primzahl und es sei*

$$\bar{f}(x) \equiv \bar{f}_1(x)^{e_1} \cdots \bar{f}_r(x)^{e_r} \mod p$$

*die Primfaktorzerlegung von $f(x)$ in irreduzible Faktoren $\mod p$ und die Polynome $f_s(x)$ seien normiert (= höchster Koeffizient ist 1). Wird $m(x)$ definiert durch*

$$f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r} - p \cdot m(x)$$

*so sind folgende zwei Aussagen äquivalent:*

1. $v_p(\Delta) > v_p(D)$
2. a. $e_s > 1$ *für wenigstens ein* $f_s(x)$
   b. $m(x) \equiv 0 \mod (p, f_s(x))$ *(wobei mit $\mod (p, f_s(x))$ der endliche Körper $\mathbb{F}_p[x]/(f_s(x))$ gemeint ist.)*

Beweis: Für einen Beweis einer Version dieses Satzes siehe zum Beispiel Vorlesung - 'Algebraische Zahlentheorie', Peter Schmid, WS 2008 / 2009, Fassung vom September 2008, Kapitel 9 (Verzweigung und Diskriminante), Anhang (Dedekind-Kriterium), Seite 44. □

# Kapitel 2

# Hilfssätze aus der analytischen Zahlentheorie

In diesem Abschnitt werden wir, unter Zuhilfenahme einiger Ergebnisse von Tschebyscheff, Sätze beweisen, die von Schur benutzt werden um die Irreduzibilität von $E_n(x) = \sum_{k=0}^{n} \frac{x^k}{k!}$ über $\mathbb{Q}[x]$ zu zeigen. Wir werden auch den Satz von Tschebyscheff-Bertrand herleiten, weil er sowohl von Schur als auch von Coleman benutzt wird. Im folgenden sei $\pi(x)$ wie üblich die Anzahl der Primzahlen $p \leq x$ und $\vartheta(x)$ sei

$$\vartheta(x) = \sum_{\substack{p \leq x \\ p \text{ prim}}} \ln(p).$$

Weiterhin bezeichne $\Psi(x)$ die abbrechende Summe

$$\begin{aligned} \Psi(x) &= \vartheta(x) + \vartheta(x^{1/2}) + \vartheta(x^{1/3}) + ... \\ &= \sum_{m=1}^{\infty} \vartheta(x^{1/m}) \end{aligned}$$

Wie man sich leicht überlegt gilt auch $\Psi(x) = \sum_{p^m \leq x} \ln(p)$.

## 2.1 Der Satz von Tschebyscheff-Bertrand

**Satz 2.1 (Tschebyscheffsche Abschätzungen für $\Psi$ und $\vartheta$.)** *Sei* $a = \ln(\frac{2^{1/2}.3^{1/3}.5^{1/5}}{30^{1/30}}) = 0,92129\ldots$. *Dann gilt:*

$$\begin{aligned} &\textit{(i)}\ \vartheta(x) < \frac{6}{5}ax + 3\ln(x)^2 + 8\ln(x) + 5, \\ &\textit{(ii)}\ \vartheta(x) > ax - \frac{12}{5}a\sqrt{x} - \frac{3}{2}\ln(x)^2 - 13\ln(x) - 15 \\ &\textit{(iii)}\ \Psi(x) - \Psi(\frac{x}{6}) < ax + 5\ln(x) + 5 \end{aligned}$$

Beweis: Für (i) und (ii) siehe Landau, Handbuch der Lehre von der Verteilung der Primzahlen, Bd.I, S.91. Für den Beweis von (iii) siehe Landau, S. 95. □

**Satz 2.2 (Eine Abschätzung für $\pi$)** *Für $x \geq 2$ ist $\pi(x) < \frac{3}{2} \cdot \frac{x}{\ln(x)}$.*

Beweis: Die Ungleichung braucht nur für ganzzahlige $x$ bewiesen zu werden:
Sei nämlich die obige Ungleichung schon für ganzzahlige $x$ bewiesen und sei $x \in \mathbb{R}$, $x \geq 2$. Die Funktion $f(x) = \frac{3}{2} \cdot \frac{x}{\ln(x)}$ ist, wegen $f'(x) = \frac{3}{2} \cdot \frac{\ln(x)-1}{\ln(x)^2}$, für $x > e$ monoton steigend. Damit folgt nach Voraussetzung

$$\pi(x) = \pi(\lfloor x \rfloor) < \frac{3}{2} \cdot \frac{\lfloor x \rfloor}{\ln(\lfloor x \rfloor)} \leq \frac{3}{2} \cdot \frac{x}{\ln(x)}$$

und die Ungleichung ist auch für reelle $x \geq 2$ bewiesen. Die obige Ungleichung kann man ohne Weiteres für $2 \leq x \leq 6^5 = 7776$ mit einem Computer-Algebra-System (z.B. GAP, GP PARI) nachweisen (siehe Quellcode am Ende des Beweises). Wir müssen die Ungleichung dann nur noch für $x = 6^5 + 1, 6^5 + 2, ...$ nachweisen. Ist $x$ eine dieser Zahlen, so dürfen wir für ganzzahlige $\xi < x$, also insbesondere für $\xi = \lfloor \frac{x}{6} \rfloor$, die obige Ungleichung als bewiesen ansehen.
Wir haben

$$\begin{aligned}
\pi(x) - \pi(\frac{x}{6}) &= \sum_{\frac{x}{6} < p \leq x} \frac{\ln(p)}{\ln(p)} \\
&\leq \frac{1}{\ln(\frac{x}{6})} \sum_{\frac{x}{6} < p \leq x} \ln(p) \\
&= \frac{1}{\ln(\frac{x}{6})} \cdot (\vartheta(x) - \vartheta(\frac{x}{6})) \\
&\leq \frac{1}{\ln(\frac{x}{6})} \cdot (\Psi(x) - \Psi(\frac{x}{6})).
\end{aligned}$$

Nach Tschebyscheff (2.1, (iii)) ist aber

$$\Psi(x) - \Psi(\frac{x}{6}) < ax + 5\ln(x) + 5.$$

Das heißt wir erhalten

$$\pi(x) - \pi(\frac{x}{6}) \leq \frac{1}{\ln(\frac{x}{6})} \cdot (\Psi(x) - \Psi(\frac{x}{6})) < \frac{1}{\ln(\frac{x}{6})}(ax + 5\ln(x) + 5).$$

Da wir die zu beweisende Ungleichung für $\frac{x}{6}$ als bewiesen ansehen dürfen gilt zudem:

$$\pi(\frac{x}{6}) < \frac{1}{\ln(\frac{x}{6})} \cdot \frac{3}{2} \cdot \frac{x}{6}.$$

Also folgt

$$\begin{aligned}
\pi(x) &< \frac{1}{\ln(\frac{x}{6})}(\frac{3}{2} \cdot \frac{x}{6} + 0,93x + 5\ln(x) + 5) \\
&= \frac{1}{\ln(x) - \ln(6)}(1,18x + 5\ln(x) + 5).
\end{aligned}$$

Dies wird kleiner als $\frac{3}{2} \cdot \frac{x}{\ln(x)}$, wenn

$$\frac{3}{2} - 1,18 = 0,32 > \frac{3}{2} \cdot \frac{\ln(6)}{\ln(x)} + \frac{5\ln(x)}{x} + \frac{5}{x}$$

ist. Diese Ungleichung ist aber schon für $x = 6^5$ richtig. Denn wegen $\ln(6) < 2$ ist sogar

$$\frac{3}{2} \cdot \frac{1}{5} + \frac{25\ln(6) + 5}{7776} < 0,3 + \frac{55}{7776} < 0,31.$$

□

In GP Pari können die Zahlen $x = 2, 3, \ldots, 6^5$ beispielsweise wie folgt überprüft werden:

```
for(x=2,6^5,if(primepi(x)<3/2*x/log(x), , print("Ungleichung nicht
                        erfuellt fuer :", x)))
```

Falls die Ungleichung erfüllt wird, wird nichts ausgegeben, ansonsten wird die Zahl ausgegeben, welche die Ungleichung nicht erfüllt.

Wir kommen nun zu einem Hilfssatz, der Aussagen über die Existenz von Primzahl macht:

**Satz 2.3** *Für $x \geq 29$ gibt es Primzahlen $p$ mit $x < p \leq \frac{5x}{4}$.*

Beweis: Da für $y > 10$ gilt

$$3y^2 + 8y + 5 < 4y^2,$$
$$\frac{3}{2}y^2 + 13y + 15 < 3y^2,$$

folgt für $x > e^{10}$ und 2.1 (i), (ii), dass

$$\vartheta(x) < \frac{6}{5}ax + 4\ln(x)^2,$$
$$\vartheta(x) > ax - \frac{12}{5}a\sqrt{x} - 3\ln(x)^2.$$

Hieraus ergibt sich für $x > e^{10}$, dass

$$\vartheta(\frac{5x}{4}) - \vartheta x > \frac{1}{20}ax - \frac{12}{5}a\sqrt{\frac{5x}{4}} - 3\ln(\frac{5x}{4})^2 - 4\ln(x)^2.$$

Beachtet man, dass $\ln(1 + \frac{1}{4}) < \frac{1}{4}$, $\frac{12}{5}\sqrt{\frac{5}{4}} < \frac{14}{5}$ ist, so erhält man

$$\vartheta(\frac{5x}{4}) - \vartheta(x) > \frac{1}{20}g(x),$$

wobei $g(x) = ax - 56a\sqrt{x} - 140\ln(x)^2 - 30\ln(x) - 4$ zu setzen ist. Wird nun für $x > X > e^{10}$ der Ausdruck $g(x)$ positiv, so enthält unser Intervall $x > X$ mindestens eine Primzahl. Da aber $\frac{1}{x}g(x)$ schon für $x > e^x$ monoton wächst, genügt es, irgendeine Zahl $X > e^{10}$ anzugeben, für die $g(X) > 0$ wird. Eine einfache Rechnung zeigt, dass $X = e^{12}$ dieser Bedingung genügt. Für $x > e12$ gibt es also Primzahlen zwischen $x$ und $\frac{5x}{4}$. Die Werte $x$ zwischen 29 und $e^{12}$ können mit GP Pari überprüft werden:

```
for(x=29, floor(exp(12)),if(primepi(5.0/4.0*x)>primepi(x),
      ,print(‘‘Keine Primzahl gefunden fuer: ‘‘,x)))
```

□

**Satz 2.4 (Tschebyscheff-Bertrand)** *Für $n \geq 8$ existiert eine Primzahl $p$ mit $\frac{n}{2} < p < n - 2$.*

Beweis: Wir beweisen dies nur für $n \geq 58$. Sei $x = \frac{m}{2}$, also $x \geq 29$. Nach 2.3 gibt es eine Primzahl $p$ mit $x < p \leq \frac{5x}{4}$. Wie man leicht überprüft gilt $2x - 2 > \frac{5x}{4}$, also $\frac{5x}{4} < m - 2$. Hieraus folgt nun die Behauptung $\frac{n}{2} = x < p \leq \frac{5x}{4} < n - 2$. □

**Lemma 2.1** *Sind $a, b, c$ drei positive ganze Zahlen, so ist $\lfloor \frac{a+b}{c} \rfloor - \lfloor \frac{a}{c} \rfloor - \lfloor \frac{b}{c} \rfloor = 0$ oder 1.*

Beweis: Wir zeigen, dass für $x, y \in \mathbb{R}_{>0}$ gilt $\lfloor x + y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor = 0$ oder 1. Es ist nämlich $x = \lfloor x \rfloor + r_1, y = \lfloor y \rfloor + r_2$ für reelle Zahlen $0 \leq r_1 < 1, 0 \leq r_2 < 1$. Falls $r_1 + r_2 < 1$, folgt $\lfloor x + y \rfloor = \lfloor (\lfloor x \rfloor + \lfloor y \rfloor) + \underbrace{(r_1 + r_2)}_{<1} \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$. Ansonsten ist $r_1 + r_2 \geq 1$ und wegen $r_1 + r_2 < 2$ ist $r_1 + r_2 = 1 + r$ mit einer reellen Zahl $0 \leq r < 1$. Wir erhalten $\lfloor x + y \rfloor = \lfloor \lfloor x \rfloor + \lfloor y \rfloor + r_1 + r_2 \rfloor = \lfloor (\lfloor x \rfloor + \lfloor y \rfloor + 1) + r \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + 1$ und die Behauptung ist bewiesen. □

## 2.2 Ein Satz von Schur-Sylvester

**Satz 2.5 (Eine Ungleichung von Schur)** *Seien $h, k$ natürliche Zahlen mit der Eigenschaft, dass die $k$ aufeinanderfolgenden Zahlen $h+1, h+2, \ldots, h+k$ nur von Primzahlen $p \leq k$ geteilt werden. Dann ist*

$$(h + k + 1/2 - \pi(k)) \ln(h + k) < 7/6 + (h + 1/2) \ln(h) + (k + 1/2) \ln(k)$$

Beweis: Nach Voraussetzung wird die Zahl

$$(h+1) \cdot (h+2) \cdot \ldots \cdot (h+k) = \frac{(h+k)!}{h! \cdot k!} \cdot 1 \cdot 2 \cdot \ldots \cdot k = \binom{h+k}{k} \cdot k!$$

nur von Primzahlen $p \leq k$ geteilt, d.h. der Binomialkoeffizient $\binom{h+k}{k}$ wird als Teiler dieser Zahl auch nur von solchen Primzahlen geteilt und wir erhalten

$$\frac{(h+k)!}{h! \cdot k!} = \prod_{p \leq k, p \text{ prim}} p^{\mu_p}$$

wobei

$$\mu_p = \sum_\lambda \lfloor \frac{h+k}{p^\lambda} \rfloor - \lfloor \frac{h}{p^\lambda} \rfloor - \lfloor \frac{k}{p^\lambda} \rfloor$$

und die Summe läuft über $1 \leq \lambda \leq \lfloor \frac{\ln(h+k)}{\ln(p)} \rfloor$ . Nun ist aber $\lfloor \frac{a+b}{c} \rfloor - \lfloor \frac{a}{c} \rfloor - \lfloor \frac{b}{c} \rfloor = 0$ oder 1 für je drei natürliche Zahlen $a, b, c$. Damit folgt

$$\begin{aligned} \mu_p &= \sum_\lambda \overbrace{\lfloor \frac{h+k}{p^\lambda} \rfloor - \lfloor \frac{h}{p^\lambda} \rfloor - \lfloor \frac{k}{p^\lambda} \rfloor}^{=0 \text{ oder } 1} \leq \sum_\lambda 1 \\ &= \lfloor \frac{\ln(h+k)}{\ln(p)} \rfloor \leq \frac{\ln(h+k)}{\ln(p)} \end{aligned}$$

Setzen wir $T(n) = \ln(n!) = \ln(2) + \ln(3) + \ldots + \ln(n)$, so ist

$$\begin{aligned} \Delta &= T(h+k) - T(h) - T(k) = \ln(\frac{(h+k)!}{h! \cdot k!}) \\ &= \ln(\prod_{p \leq k, p \text{ prim}} p^{\mu_p}) = \sum_{p \leq k, p \text{ prim}} \mu_p \cdot \ln(p) \leq \sum_{p \leq k, p \text{ prim}} \frac{\ln(h+k)}{\ln(p)} \cdot \ln(p) \\ &= \sum_{p \leq k, p \text{ prim}} \ln(h+k) = \pi(k) \cdot \ln(h+k) \end{aligned}$$

d.h. $\Delta \leq \pi(k) \cdot \ln(h+k)$. Nach der Formel von Stirling ist $n! = \sqrt{2\pi} \cdot n^{n+1/2} \cdot e^{-n} \cdot e^{\frac{\vartheta(n)}{12n}}$ für ein $0 < \vartheta(n) < 1$.
Mit $R_n := \frac{\vartheta(n)}{12n}$ bekommen wir also:
$T(n) = \ln(n!) = (n+1/2)\ln(n) - n + \ln(\sqrt{(2\pi)}) + R_n$, wobei $0 < R_n < \frac{1}{12n} < 1/12$.
Setzen wir nacheinander $n = h+k$, $n = k$ und $n = k$ in die Gleichung von $T(n)$ ein, erhalten wir

$$\begin{aligned} T(h+k) &= (h+k+1/2)\ln(h+k) - (h+k) + \ln(\sqrt{2\pi}) + R_{h+k}, \\ T(h) &= (h+1/2)\ln(h) - h + \ln(\sqrt{2\pi}) + R_h, \\ T(k) &= (k+1/2)\ln(k) - k + \ln(\sqrt{2\pi}) + R_k. \end{aligned}$$

Hieraus folgt

$$\begin{aligned} \Delta &= T(h+k) - T(h) - T(k) \\ &= (h+k+1/2)\ln(h+k) - (h+1/2)\ln(h) - (k+1/2)\ln(k) - R' \ , \end{aligned}$$

wobei

$$\begin{aligned} R' &= \underbrace{\ln(\sqrt{2\pi})}_{<1} + \underbrace{R_h}_{<1/12} + \underbrace{R_k}_{<1/12} - \underbrace{R_{h+k}}_{>0} \\ &< 1 + 1/12 + 1/12 = 7/6 \ . \end{aligned}$$

Aus $\Delta \leq \pi(k)\ln(h+k)$ folgt dann

$$(h+k+1/2-\pi(k))\ln(h+k) < 7/6 + (h+1/2)\ln(h) + (k+1/2)\ln(k)$$

und die Behauptung ist bewiesen.

□

Der folgende Satz wird von Schur gebraucht, um die Irreduzibilität von $E_n(x)$ über $\mathbb{Q}[x]$ zu zeigen.

**Satz 2.6 (Schur-Sylvester, Aufeinanderfolgende natürliche Zahlen)** *Seien $h \geq k$ natürliche Zahlen. Dann gibt es unter den $k$ aufeinanderfolgenden Zahlen $h+1, h+2, \ldots, h+k$ eine Zahl, die durch eine Primzahl $q > k$ teilbar ist.*

Beweis: Zunächst reicht es den Satz für Primzahlen $k = p$ zu beweisen:
Ist nämlich der Satz schon für Primzahlen $k = p$ bewiesen, so folgt für eine allgemeine Zahl $k$, dass:
Sei $p$ die größte Primzahl $\leq k, h \geq k$. Dann gibt es unter den $p$ aufeinanderfolgenden Zahlen $h+1, h+2, \ldots, h+p$ eine Zahl, die durch eine Primzahl $q > p$ teilbar ist. Da $p$ die größte Primzahl $\leq k$ ist, folgt aus $q > p$, dass $q > k$. Die Primzahl $q > k$ teilt aber auch eine der Zahlen $h+1, h+2, \ldots, h+p, \ldots, h+k$ und der Satz ist bewiesen.
Wir zeigen den Satz also jetzt für eine Primzahl $k = p$:
Sei $p$ die $m$-te Primzahl und nehmen wir an die Zahlen
$h+1, h+2, \ldots, h+p$ würden nur von Primzahl $q \leq p$ geteilt werden. Dann folgt aus der Ungleichung von Schur, dass

$$(h+p+1/2-m)\ln(h+p) - (h+1/2)\ln(h) - (p+1/2)\ln(p) < 7/6.$$

Sei

$$\begin{aligned} S_1 &= (h+p+1/2-m)\ln(h+p), \\ S_2 &= (h+1/2)\ln(h), \\ S_3 &= (p+1/2)\ln(p) \text{ und} \\ S &= S_1 - S_2 - S_3 \end{aligned}$$

also $7/6 > S$ nach der vorherigen Ungleichung. Wir setzen $h = Qp$ in $\ln(h)$, $\ln(h+p)$ ein und beachten in $S_1$, dass $\ln(h+p) = \ln(Q+1) + \ln(p)$, $\ln(Q+1) = \ln(Q) + \ln(1+1/Q)$ ist. Damit erhalten wir:

$$\begin{aligned} S_1 &= (h+1/2)\ln(Q) + (h+1/2)\ln(1+1/Q) \\ &\quad +(h+1/2+p-m)\ln(p) + (p-m)\ln(Q+1), \\ S_2 &= (h+1/2)\ln(Q) + (h+1/2)\ln(p)), \\ S_3 &= (p+1/2)\ln(p), \text{ woraus} \end{aligned}$$

$$\begin{aligned} 7/6 > S &= S_1 - S_2 - S_3 \\ &= (h+1/2)\ln(1+1/Q) \\ &\quad -(m+1/2)\ln(p) + (p-m)\ln(Q+1) \end{aligned} \tag{2.1}$$

folgt. Wegen $h \geq p$ ist $Q \geq 1$, also
$\ln(1+1/Q) = 1/Q - \frac{1}{2Q^2} + \frac{1}{3Q^3} - \ldots > \frac{1}{Q} - \frac{1}{2Q^2}$ und damit

$$\begin{aligned}(h+1/2)\ln(1+1/Q) &> (h+1/2)(1/Q - \frac{1}{2Q^2}) \\ &= (Qp+1/2)(1/Q - \frac{1}{2Q^2}) \\ &= p - \frac{p}{2Q} + \frac{1}{2Q} - \frac{1}{4Q^2} \\ &> p - \frac{p}{2Q}.\end{aligned}$$

Lassen wir in (2.1) nur den Term $(p-m)\ln(Q+1)$ auf der kleineren Seite der Ungleichung stehen und beachten die letzte Ungleichung, so erhalten wir

$$\begin{aligned}(p-m)\ln(Q+1) &< 7/6 + (m+1/2)\ln(p) - (h+1/2)\ln(1+1/Q) \\ &< 7/6 + (m+1/2)\ln(p) + \frac{p}{2Q} - p \\ &= 7/6 + \frac{p}{2Q} + \ln(p)/2 + m\cdot\ln(p) - p\end{aligned} \tag{2.2}$$

Wir unterteilen den folgenden Beweis in zwei Teile $a$) und $b$). In Teil $a$) werden wir alle Primzahlen $p \geq 29$ betrachten, während wir in Teil $b$) die restlichen Primzahlen betrachten:
$a$) Für $p \geq 29$ ist die Aussage richtig:
Wir unterscheiden hier die Fälle, dass $h \leq 4p$ oder $h > 4p$:
Ist $h \leq 4p$, d.h. $Q \leq 4$, so auch
$\frac{h+p}{p} = 1 + \frac{p}{Qp} = 1 + 1/Q \geq 1 + 1/4 = 5/4$ und $h \geq p \geq 29$. Nach Satz 2.3 enthält das Intervall $h < P \leq \frac{5h}{4}$ mindestens eine Primzahl. Aus $5/4 \leq \frac{h+p}{h}$ folgt $\frac{5h}{4} \leq h+p$, d.h. für die Primzahl P gilt:

$$h+1 \leq P \leq \frac{5h}{4} \leq h+p \text{ und } p \leq h < P,$$

im Widerspruch zur Annahme, dass die Zahlen
$h+1, h+2, \ldots, h+p$ nur von Primzahlen $q \leq p$ geteilt werden.
Für den Fall, dass $h > 4p$, also $Q > 4$ folgt zunächst
$\ln(Q+1) > \ln(4+1) = \ln(5) > \frac{8}{5}$, $\frac{p}{2Q} < \frac{p}{2\cdot 4} = \frac{p}{8}$ und hieraus
$\frac{8}{5}(p-m) < (p-m)\ln(Q+1) \overbrace{<}^{(2.2)} \frac{7}{6} + \frac{p}{2Q} + \frac{\ln(p)}{2} + m\ln(p) - p$. Nach Satz 2.2 ist $m\ln(p) < \frac{3}{2}p$, also
$m\ln(p) - p < \frac{3}{2}p - p = \frac{p}{2}$ und wir bekommen

$$\begin{aligned}\frac{8}{5}(p-m) &< \frac{7}{6} + \underbrace{\frac{p}{2Q}}_{<\frac{p}{8}} + \frac{\ln(p)}{2} + \underbrace{m\ln(p) - p}_{<\frac{p}{2}} \\ &< \frac{7}{6} + \frac{5p}{8} + \frac{\ln(p)}{2}\end{aligned}$$

Nach Multiplikation der letzten Ungleichung mit $\frac{1}{p}$ und anschließendem Umordnen erhalten wir

$$\begin{aligned} \frac{39}{40} = \frac{8}{5} - \frac{5}{8} &< \frac{7}{6p} + \frac{\ln(p)}{2p} + \frac{8m}{5p} \\ &< \frac{7}{6p} + \frac{\ln(p)}{2p} + \frac{8}{5} \cdot \frac{3}{2} \frac{1}{\ln(p)} \end{aligned} \tag{2.3}$$

Die Funktion $g(x) = \frac{7}{6x} + \frac{12}{5\ln(x)}$ ist fallend für $x > 0$, während die Funktion $h(x) = \frac{\ln(x)}{2x}$ für $x \geq e$ fallend ist. Damit ist aber auch $f(p) = (\frac{7}{6p} + \frac{12}{5\ln(p)}) + \frac{\ln(p)}{2}$ erst recht fallend für $p \geq 29$, d.h. Ungleichung (2.3) müsste auch für $p = 29$ gelten: $\frac{39}{40} < \frac{7}{6 \cdot 29} + \frac{\ln(29)}{2 \cdot 29} + \frac{12}{5\ln(29)}$. Diese Ungleichung ist aber falsch, da beispielsweise $3 < \ln(29) < 4$, also $\frac{39}{40} < \frac{7}{6 \cdot 29} + \frac{4}{2 \cdot 29} + \frac{12}{5 \cdot 3} = \frac{791}{870} < \frac{39}{40}$. Es bleiben noch die Primzahlen $2, 3, 5, 7, 11, 13, 17, 23$ übrig. Wegen $Q \geq 1$ ist $\frac{p}{2Q} \leq \frac{p}{2}$ und aus der Ungleichung (2) erhalten wir

$$Q + 1 < e^{\frac{1}{p-m} \cdot (\frac{7}{6} - \frac{p}{2} + (m + \frac{1}{2}\ln(p)))}$$

und damit obere Schranken $K_p$ für $Q + 1$, die da sind

| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 |
|---|---|---|---|---|---|---|---|---|---|
| $K_p$ | 4 | 12 | 9 | 9 | 5 | 6 | 5 | 5 | 5 |

Wegen $h + p = Qp + p = (Q + 1)p < K_p \cdot p$ reicht es für jedes $p$ nur die Zahlen $h$ im Intervall $p \leq h < (K_p - 1) \cdot p$ zu untersuchen. Weiterhin sind die Primteiler $q > p$ von $\binom{h+p}{p}$ die gleichen, wie die Primteiler $q > p$ von $(h + 1) \cdot \ldots \cdot (h + p) = p! \binom{h+p}{p}$. Um diese Fälle nicht per Hand bearbeiten zu müssen, kann man ein Computeralgebra-System benutzen, wie beispielsweise GP Pari oder GAP, Group Theory. Im folgenden Pseudo-Code laufen wir mit $h$, zur gegebenen Prizahl $p$ und zugehörigen Schranke $K_p$, über alle Zahlen $p, p + 1, \ldots, (K_p - 1) \cdot p$. Wird zu einem solchen $h$ kein Primteiler $q > p$ von $\binom{h+p}{p}$ gefunden, so wird $h$ angezeigt:

```
for h = p, p+1,..., (K_p-1)p:
  gefunden := FALSE
  PD := primedivisors(binom(h+p,p))
  for q in PD:
     if q > p:
        gefunden := TRUE
  if gefunden == FALSE:
     print h
```

Eine Überprüfung mit dem Computer zeigt jedoch, dass es kein solches $h$ gibt, d.h. der Satz ist bewiesen. □

# Kapitel 3

# Hilfssätze aus der Gruppentheorie

In diesem Abschnitt wollen wir einige kleine gruppentheoretische Hilfssätze beweisen, die später gebraucht werden. Ein Beweis des Satzes von Jordan, in der Version, die bei Schur und Coleman gebraucht wird, würde aber den Rahmen dieser Arbeit sprengen. Wir werden aber einen Satz über imprimitive Gruppen beweisen, den wir zum Schluss dieser Arbeit brauchen, und der in etwa aussagt, dass imprimitive Gruppen Untergruppen von Kranzprodukten sind. Beim Aufbau und bei den Beweisen werden wir im Wesentlichen B. Huppert, Endliche Gruppen 1 folgen.

## 3.1 Kranzprodukte und imprimitive Gruppen

Wir fangen mit einer Definition an:

**Definition 3.1 (Kranzprodukt)** *Seien $G, H$ Gruppen, $H$ operiere auf die Menge $\Omega$. Dann ist das Kranzprodukt $G \wr H$ von $G$ mit $H$ die Menge*

$$\{(f, \sigma) | \sigma \in H, f \text{ Abbildung von } \Omega \text{ nach } G\}$$

*mit der Multiplikation*

$$(f_1, \sigma_1) * (f_2, \sigma_2) = (g, \sigma_1\sigma_2)$$

*mit $g(\alpha) = f_1(\alpha) f_2(\sigma_1 \cdot \alpha)$ für $\alpha \in \Omega$.*

Die so definierte Multiplikation ist assoziativ, hat $(f, 1)$ mit $f(\alpha) = 1$ für alle $\alpha \in \Omega$ als Eins in $G \wr H$, und das Inverse von $(f, \sigma)$ ist $(g, \sigma^{-1})$, wobei $g(\alpha) = f(\sigma^{-1} \cdot \alpha)^{-1}$ ist. Das macht $G \wr H$ zu einer Gruppe.
Die Struktur von $G \wr H$ wird durch folgenden Satz beschrieben:

**Satz 3.1 (Struktur von Kranzprodukten)** *Die Gruppe $H$ operiere auf $\Omega$ mit $|\Omega| = n$. Das Kranzprodukt $G \wr H$ besitzt den Normalteiler*

$$D = D_1 \times D_2 \times \ldots \times D_n$$

*mit $D_\alpha = \{(f, 1) | f(\beta) = 1 \text{ für } \alpha \neq \beta\} \simeq G$. Es ist $H* = \{(e, \sigma) | \sigma \in H, e(\alpha) = 1 \text{ für alle } \alpha \in \Omega\}$ ein zu $H$ isomorphes Komplement von $D$ in $G \wr H$. Also ist $|G \wr H| = |G|^n \cdot |H|$.*

Beweis: Sei $\Omega = \{1, 2, \ldots, n\}$. Wir setzen $D = \{(f, 1) | f : \Omega \to G\}$ und $D_\alpha = \{(f, \alpha) | f(\alpha) = 1 \text{ für } \beta \neq \alpha\}$. Offenbar gilt $D_\alpha \simeq G$ und $D = D_1 \times \ldots \times D_n$. Die Abbildung $\varepsilon : G \wr H \to H, (f, \sigma) \mapsto \sigma$ ist ein surjektiver Gruppenhomomorphismus mit $Kern(\varepsilon) = D$, d.h. $D$ ist ein Normalteiler von $G \wr H$. Wegen $(f, \sigma) = (f, 1) \cdot (e, \sigma)$ mit $e(\alpha) = 1$ für alle $\alpha \in \Omega$ ist die Gruppe $H* = \{(e, \sigma) | e(\alpha) = 1 \text{ für alle } \alpha \in \Omega\}$ ein Komplement von $D$ in $G \wr H$. □

Wir geben jetzt eine Operation von $G \wr H$ auf $\Omega \times \Gamma$ an, falls $H$ auf $\Omega$ und $G$ auf $\Gamma$ operieren.

**Lemma 3.1 (Kranzprodukte operieren auf kartesisches Produkt)** *Seien $G, H$ Gruppen, die auf den Mengen $\Gamma$ bzw. $\Omega$ operieren. Dann operiert das Kranzprodukt $G \wr H$ auf dem kartesischen Produkt $\Gamma \times \Omega$ durch*

$$(\alpha, \beta) \cdot (f, \sigma) = (f(\beta) \cdot \alpha, \sigma \cdot \beta)$$

*für $(\alpha, \beta) \in \Gamma \times \Omega$ und $(f, \sigma) \in G \wr H$.*

Beweis: Wir haben

$$\begin{aligned} ((\alpha, \beta) \cdot (f, \sigma)) \cdot (f', \sigma') &= (f(\beta)\alpha, \sigma\beta)(f', \sigma') \\ &= (f'(\sigma\alpha) f(\beta)\alpha, \sigma'\sigma\beta) \\ &= (\alpha, \beta) \cdot ((f, \sigma) \cdot (f', \sigma')). \end{aligned}$$

Da die von $(f, \sigma)$ auf $\Gamma \times \Omega$ bewirkte Abbildung ein Inverses besitzt, liefert die angegebene Vorschrift eine Operation von $G \wr H$ auf $\Gamma \times \Omega$. □

**Definition 3.2 (Imprimitive Gruppen)** *Eine Gruppe $G$, die transitiv auf $\Omega$ operiert, heißt imprimitiv, wenn es eine nichtleere Teilmenge $\Delta \not\subset \Omega$ gibt, so dass für alle $\sigma \in G$ gilt:*
*$\Delta \cap \sigma(\Delta) = \emptyset$ oder $\Delta = \sigma(\Delta)$. Wir nennen dann $\Delta$ einen Block von $G$. Ist $G$ transitiv und nicht imprimitiv, so heißt $G$ imprimitiv.*

**Satz 3.2 (Imprimitive Gruppen sind Untergruppen von Kranzprodukten)** *Sei $G$ imprimitiv auf die endliche Menge $\Omega$ und $\Delta$ ein Block von $G$. Sei $H = \{\sigma \in G | \sigma(\Delta) = \Delta\}$, und sei $G = \cup_{\tau \in L} \tau H$ die Nebenklassenzerlegung von $G$ nach $H$.*

- **a)** *Es ist $\Omega = \cup_{\tau \in L} \tau(\Delta)$ eine disjunkte Zerlegung von $\Omega$.*
- **b)** *Wir haben $|\Omega| = |\Delta| \cdot |L|$, d.h. insbesondere ist $|\Delta|$ ein Teiler von $\Omega$. Setzen wir $|\Delta| = k$ und $|L| = m$, so ist $G$ ähnlich zu einer Untergruppe des Kranzproduktes $S_k \wr S_m$ der symmetrischen Gruppen $S_k$ und $S_n$, aufgefasst im Sinne des vorhergehenden Lemmas als Operation vom Grad $km = |\Omega|$. Außerdem ist $|G|$ ein Teiler von $m!(k!)^m$.*
- **c)** *Die Untergruppe $H = \{\sigma \in G | \sigma(\Delta) = \Delta\}$ ist transitiv auf $\Delta$.*

Beweis:

**a)** Sei $\alpha_0 \in \Delta$ und $\alpha \in \Omega$. Wegen der Transitivität von $G$ gibt es ein $\sigma \in G$ mit $\alpha = \sigma(\alpha_0) \in \sigma(\Delta)$. Ist $\sigma = \tau\gamma$ mit $\gamma \in H$ und $\tau \in L$, so folgt $\alpha \in \tau\gamma(\Delta) = \tau(\Delta)$. Also gilt jedenfalls $\Omega = \cup_{\tau \in L}\tau(L)$. Aus $\tau(\Delta) \cap \tau'(\Delta) \neq \emptyset$ für $\tau, \tau' \in L$, folgt $\tau'^{-1}\tau(\Delta)) \neq \emptyset$ und da $\Delta$ ein Block ist, erhalten wir $\tau'^{-1}\tau(\Delta) = \Delta$. Daher haben wir $\tau'\tau \in H$ und somit $\tau = \tau'$. Offenbar ist mit $\Delta$ auch jedes $\sigma(\Delta), \sigma \in G$ ein Block von $G$.

**b)** Sei $|\Delta| = k, |G : H| = |L| = m$. Die Elemente in $\tau(\Delta)$ identifizieren wir in irgendeiner Weise mit den Paaren $(\alpha, \tau H)$ wobei $\alpha \in \Gamma = \{1, 2, \ldots, k\}$. Ist nun $\sigma \in G$, so auch $\tau\sigma = \gamma\tau'$ mit einem $\gamma$ aus $H$ und $\tau'$ aus $L$, und es folgt $\sigma(\tau(\Delta)) = \tau'(\Delta)$. Also permutiert $G$ die Mengen $\tau(\Delta)$ gemäß der von $G$ auf den Nebenklassen von $H$ bewirkten Operation von $G$. In der Schreibweise mit den Paaren heißt das
$\sigma((\alpha, \tau H)) = (\alpha', \sigma\tau H)$, wobei $\begin{pmatrix} \alpha \\ \alpha' \end{pmatrix}$ eine von $\sigma$ und $\tau H$ abhängende Permutation $\pi(\sigma, \tau H)$ auf $\Gamma = \{1, 2, \ldots, k\}$ ist. Also haben wir
$\sigma \cdot (\alpha, \tau H) = (\pi(\sigma, \tau H)\alpha, \sigma\tau H)$. Der Vergleich mit den Formeln in Lemma 3.1 ('Kranzprodukte operieren auf kartesisches Produkt') zeigt nun, dass $G$ zu einer Untergruppe des Kranzproduktes $S_k \wr S_m$, aufgefaßt als Permutationsgruppe auf der Produktmenge $\Gamma \times \{\tau H | \tau \in L\}$ ähnlich ist. Die restlichen Aussagen folgen sofort aus Satz 3.1 ('Struktur von Kranzprodukten').

**c)** Seien $\alpha, \beta$ aus $\Delta$. Wegen der Transitivität von $G$ gibt es ein $\sigma \in G$ mit $\sigma(\alpha) = \beta$. Dann ist $\beta \in \Delta \cap \sigma(\Delta)$, also $\Delta \cap \sigma(\Delta) \neq \emptyset$ und da $\Delta$ ein Block ist, folg $\Delta = \sigma(\Delta)$. Damit ist also $\sigma$ aus $H$ und die Transitivität von $H$ auf $\Delta$ ist gezeigt.

□

## 3.2 Transitive Gruppen

**Lemma 3.2 (Transitive Gruppen mit primitiven Untergruppen kleineren Grades)** *Sei $G$ transitiv auf $\Omega$, $U$ eine Untergruppe von $G$ und $\Delta \subset \Omega$ eine Bahn von $U$. Ist $U$ primitiv auf $\Delta$ und $|\Omega| < 2 \cdot |\Delta|$, so ist $G$ primitiv auf $\Omega$.*

Beweis: Angenommen es gibt einen Block $\Psi$ von $G$. Falls $\Psi \cap \Delta = \emptyset$, finden wir wegen der Transitivität von $G$ ein und $g \in G$ mit $g(\Psi) \cap \Delta \neq \emptyset$ und $g(\Psi)$ ist auch ein Block. Wir können also annehmen, dass $1 \leq |\Psi \cap \Delta|$. Da $G$ endlich ist, können wir $h \in G$ so wählen, dass $|g(\Psi) \cap \Delta| \leq |h(\Psi) \cap \Delta|$ für alle $g \in G$ ist. D.h wir können unseren Block $\Psi$ so wählen, dass $1 \leq |\Psi \cap \Delta|$ und $|g(\Psi) \cap \Delta| \leq |\Psi \cap \Delta|$ für alle $g \in G$. Setzen wir $\Lambda = \Psi \cap \Delta$ und ist $\Lambda \cap u(\Lambda) \neq \emptyset$ für ein $u \in U$, so ist auch $\emptyset \neq \Lambda \cap u(\Lambda) = (\Psi \cap \Delta) \cap (u(\Psi) \cap u(\Delta)) = (\Psi \cap u(\Psi)) \cap \Delta$ , also $\Psi \cap u(\Psi) \neq \emptyset$. Da $\Psi$ ein Block von $G$ ist, muss $u(\Psi) = \Psi$ sein, d.h. $u(\Lambda) = u(\Psi \cap \Delta) = u(\Psi) \cap u(\Delta) = \Psi \cap \Delta = \Lambda$. Aber $\Lambda$ kann kein Block von $U$ sein, da $U$ primitiv auf $\Delta$ ist. Es muss also $1 \not< |\Lambda| \not< |\Delta|$ sein und es bleiben die Fälle $\Lambda = \Delta$ und $1 = |\Lambda|$ übrig.
Im ersten Fall ist $\Delta \subset \Psi$ und nach Voraussetzung folgt $|\Omega| < 2 \cdot |\Delta| \leq 2 \cdot |\Psi|$.

Aber $|\Psi|$ ist nach Satz 3.2 ('Imprimitive Gruppen sind Untergruppen von Kranzprodukten') ein Teiler von $|\Omega|$, da $\Psi$ ein Block von $G$ ist. Es muss also $\Psi = \Omega$ sein, im Widerspruch zu $|\Psi| < |\Omega|$. Im zweiten Fall folgt für alle $g \in G$ dass $|g(\Psi) \cap \Delta| \leq |\Psi \cap \Delta| = |\Lambda| = 1$. Da $G$ transitiv auf $\Omega$ wirkt und $\Psi \neq \emptyset$, ist $\Omega = \cup_{g \in G} g(\Psi)$. D.h. für jedes $\alpha \in \Delta \subset \Omega$ existiert ein $g \in G$ mit $\alpha \in g(\Psi)$ und wegen $|g(\Psi) \cup \Delta| \leq 1$ muss $\{\alpha\} = g(\Psi) \cap \Delta$ sein. Sind nun $\alpha, \beta$ zwei verschiedene Elemente von $\Delta$, so gibt es $g, h \in G$ , mit $\{\alpha\} = g(\Psi) \cap \Delta$, $\{\beta\} = h(\Psi) \cap \Delta$ und es ist $g(\Psi) \not\subset h(\Psi)$, denn sonst wäre $g(\Psi) \cap h(\Psi) = g(\Psi)$ und wir erhielten einen Widerspruch $\emptyset = \{\alpha\} \cap \{\beta\} = (g(\Psi) \cap \Delta) \cap (h(\Psi) \cap \Delta) = (g(\Psi) \cap h(\Psi)) \cap \Delta = g(\Psi) \cap \Delta = \{\alpha\}$ Also gibt es mindestens $|\Delta|$ verschiedene $g(\Psi)$ und es folgt der Widerspruch
$|\Omega| \geq |\Delta| \cdot |\Psi| \geq |\Delta| \cdot 2 > |\Omega|$.
Somit hat $G$ keinen Block in $\Omega$ und ist primitiv auf $\Omega$.

□

**Satz 3.3 (Transitive Gruppen, die von einer genügend großen Primzahl geteilt werden)** *Sei $G$ eine transitive Gruppe vom Grad $n = |\Omega|$, $p$ eine Primzahl, die $|G|$ teilt und $\frac{n}{2} < p$. Dann ist $G$ primitiv und enthält einen $p-$Zyklus.*

Beweis:

1. Nach dem Satz von Cauchy enthält $G$ eine Permutation $\sigma \in S_n$ der Ordnung $p$. Wegen $2p > n$ muss $\sigma$ ein Zykel der Länge $p$ sein, d.h. wir können $\sigma = (\alpha_1, \alpha_2, \ldots, \alpha_p)$ als Zykel schreiben. Ist $U =< \sigma >$ und $\Delta = \{\alpha_1, \alpha_2, \ldots, \alpha_p\}$, so ist $\Delta$ eine Bahn von $U$, $U$ transitiv auf $\Delta$ vom Primzahlgrad $p = |\Delta|$. Nach ('Imprimitive Gruppen sind Untergruppen von Kranzprodukten') muss $U$ damit primitv auf $\Delta$ sein (sonst hätte es einen Block $\Psi$, $1 < |\Psi| < p$ gegeben, dessen Länge $|\Psi|$ ein Teiler von $|\Delta| = p$ wäre). Wegen $n < 2p = 2|\Delta|$, folgt die Behauptung aus dem vohergehenden Lemma.

2. Wie in 1. enthält $G$ ein $p$-Zykel. Angenommen $G$ sei nicht primitiv. Dann existiert ein Block $\Delta \subset \Omega$. Ist $k = |\Delta|$, so ist $1 < k < n$ und $k$ ist ein Teiler von $n$, d.h. $n = km$ für ein $m \in \mathbb{N}$ und es ist $|G|$ ein Teiler von $(k!)^m \cdot m!$ , nach Satz 3.2 ('Imprimitive Gruppen sind Untergruppen von Kranzprodukten'). Wir unterscheiden folgende Fälle:
   Falls $p \leq m$, so ist $\frac{n}{2} < p \leq m$, d.h. $mk = n < 2m$ und es muss $k = 1$ sein, im Widerspruch zu $k > 1$.
   Ist $p > m$, so kann $p$ kein Teiler von $m!$ sein. Nach Voraussetzung ist aber $p$ ein Teiler von $|G|$ und da $|G|$ ein Teiler von $|(k!)^m \cdot m!|$, muss $p$ ein Teiler von $k!$ sein, d.h. $p \leq k$. Wegen $mk = n > k$ folgt $m \geq 2$, d.h. $k = \frac{n}{m} \leq \frac{n}{2} < p \leq k$, Widerspruch.

□

Wir erwähnen hier ohne Beweis den Satz von Jordan zur symmetrischen Gruppe:

**Satz 3.4 (C.Jordan)** *Sei $G$ eine primitive Gruppe vom Grad $n$. Ist $|G|$ durch eine Primzahl $p$ teilbar und ist $\frac{n}{2} < p < n - 2$, so enthält $G$ die alternierende Gruppe vom Grad $n$.*

Der Beweis kan bei [Jordan72] und [Hall59] nachgelesen werden.

# Kapitel 4

# Die Galoisgruppe von $E_n(x)$ nach Schur

## 4.1 Allgemeine Sätze zur Berechnung von Galoisgruppen

**Satz 4.1** *Sei $K$ ein Zahlkörper $n$-ten Grades mit Diskriminante $D$, $L$ sei der zugehörige Galois-Körper mit Gruppe $G = Gal(L/\mathbb{Q})$. Ist $p$ eine Primzahl mit $v_p(D) \geq n$, so teilt $p$ die Gruppenordnung $g = |G|$.*

Beweis: Ist $D^*$ die Diskriminante von $L$ so gilt nach Lemma 1.3 (Transitivität der Differente und der Diskriminante)

$$\begin{aligned} D^* = D_{L/\mathbb{Q}} &= (D_{K/\mathbb{Q}})^{[L:K]} \cdot \mathcal{N}_{K/\mathbb{Q}}(D_{L/K}) \\ &= D^{\frac{g}{n}} \cdot \mathcal{N}_{K/\mathbb{Q}}(D_{L/K}) \end{aligned}$$

Da nach Voraussetzung $v_p(D) \geq n$ ist, folgt, dass $v_p(D^*) \geq n \cdot \frac{g}{n} = g$. Angenommen $p$ ist kein Teiler von $g$. Sei $\mathcal{P}$ ein Primideal in $L$, das in $p$ aufgeht mit Verzweigungsindex $e = e(\mathcal{P}|p)$, Restklassengrad $f$ und sei $r$ die Anzahl der Primideale aus $L$, die über $p$ verzweigen. Weil $p$ kein Teiler von $g = efr$ ist, folgt $e \not\equiv 0 \mod p$. Nach dem Dedekindschen Differentensatz (Satz 1.3) ist damit $v_{\mathcal{P}}(\mathcal{D}_{L/\mathbb{Q}}) = e - 1$ (wobei $\mathcal{D}_{L/\mathbb{Q}}$ die Relativdifferente von $L/\mathbb{Q}$ ist)und hieraus folgt $v_{\mathcal{P}}(D^*) = v_{\mathcal{P}}(\mathcal{N}_{L/\mathbb{Q}}(\mathcal{D}_{L/\mathbb{Q}})) = e - 1$. Somit ist die höchste in $D^*$ enthaltene Potenz von $p$ gleich

$$p^{(e-1)\cdot f\cdot r} = p^{efr - \frac{efr}{e}} = p^{g - \frac{g}{e}}$$

also kleiner als $p^g$, im Widerspruch zu $v_p(D^*) \geq g$. □

**Korollar 4.1** *Sei $K$ ein Zahlkörper $n$-ten Grades, $D$ seine Diskriminante und $p$ eine Primzahl mit $v_p(D) \geq n$, $\frac{n}{2} < p < n - 2$. Sei $L$ der Galois-Abschluss von $K$ mit Gruppe $G = Gal(L/k)$, welche als transitiv vom Grad $n$ vorausgesetzt sei. Dann ist $G$ die symmetrische oder die alternierende Gruppe $n$-ten Grades, wobei der zweite Fall eintritt, wenn $D$ eine Quadratzahl ist.*

Beweis: Wegen $v_p(D) \geq n$ folgt aus Satz 4.2, dass $p$ ein Teiler von $|G|$ ist. Weil $\frac{n}{2} < p < n-2$ folgt aus Satz 3.3 (Transitive Gruppen, die von einer großen Primzahl geteilt werden), dass $G$ primitiv sein muss. Nach dem Satz von Jordan über primitive Gruppen folgt hieraus, dass $G = A_n$ oder $G = S_n$. Wie aus der Galois-Theorie bekannt ist, wird $G = A_n$ sein, wenn $D$ eine Quadratzahl ist. □

**Satz 4.2 (Schur)** *Es sei*

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$$

*ein Polynom aus $\mathbb{Z}[x]$, welches folgende Eigenschaften hat:*

1. *Das Polynom $f(x)$ ist irreduzibel in $\mathbb{Q}[x]$.*
2. *Die Diskriminante $\Delta$ von $f(x)$ ist mindestens durch die $n$-te Potenz einer Primzahl $p$ teilbar.*
3. *Das konstante Glied $a_n$ ist durch $p$, aber nicht durch $p^2$ teilbar.*
4. *Es gilt eine Kongruenz der Form*

   $$\bar{f}(x) \equiv x^k \cdot \bar{g}(x) \mod p \ (k > 1)$$

   *wobei die Diskriminante $\Delta'$ des normierten Polynoms $g(x)$ nicht durch $p$ teilbar ist.*

*Dann hat die Galoissche Gruppe $G$ von $f(x)$ über $\mathbb{Q}$ eine durch $p$ teilbare Ordnung $|G|$. Ist insbesondere*

$$\frac{n}{2} < p < n-2,$$

*so ist $G$ die symmetrische oder die alternierende Gruppe. Der zweite Fall tritt ein, wenn $\Delta$ eine Quadratzahl ist.*

Beweis: Sei $D$ die Diskriminante eines Zahlkörpers $\mathbb{Q}(\alpha), \alpha$ eine Nullstelle von $f(x)$. Wir wollen zuerst zeigen, dass $v_p(\Delta) = v_p(D)$ :
Da die Diskriminante $\Delta'$ von $g(x)$ nicht durch $p$ teilbar ist, ist das Polynom $\bar{g}(x)$ separabel $\mod p$. Nach 4. ist damit $x$ der einzige irreduzible Faktor, der $\mod p$ mehrfach auftaucht. Definieren wir $m(x)$ durch

$$f(x) = x^k \cdot g(x) - p \cdot m(x)$$

und setzen wir im Dedekind-Kriterium (Satz 1.4) $f_s(x) = x$, also auch $e_s = k > 1$, so ist nach eben diesem Kriterium zu zeigen, dass

$$m(x) \not\equiv 0 \mod (p, x)$$

Angenommen, dies wäre falsch, d.h. $m(x) \equiv 0 \mod (p, x)$. Wir haben $a_n = f(0) = p \cdot m(0)$. Weil $m(0) \equiv m(x) \mod (x)$, folgt aus $m(x) \equiv 0 \mod (p, x)$, dass $m(0) \equiv 0 \mod p$, d.h. $a_n = p \cdot m(0)$ ist durch $p^2$ teilbar, im Widerspruch zu 3. Also ist $m(x) \not\equiv 0 \mod (p, x)$ und nach dem Dedekind-Kriterium folgt

$$v_p(\Delta) = v_p(D)$$

Wegen 2. ist damit $v_p(D) \geq n$ und wegen 1. ist die Galoisgruppe transitiv. Nach Satz 4.1 ist damit $|G|$ teilbar durch $p$ und nach Korollar 4.1 folgt der Rest. □

## 4.2 Konkrete Berechnungen zu $E_n(x)$

**Satz 4.3 (Ein Irreduzibilitätssatz von Schur)** *Ein Polynom der Form*

$$f(x) = 1 + g_1\frac{x^1}{1!} + g_2\frac{x^2}{2!} + \ldots + g_{n-1}\frac{x^2}{(n-1)!} + -\frac{x^n}{n!}$$

*mit ganzen Zahlen $g_1, g_2, \ldots, g_{n-1} \in \mathbb{Z}$ ist irreduzibel in $\mathbb{Q}[x]$.*

Beweis: Angenommen $f(x)$ sei nicht irreduzibel. Sei $A(x)$ ein irreduzibler Faktor von $f(x)$ vom Grad $k$, welcher ohne Einschränkung $\leq \frac{n}{2}$ sei (Ansonsten ist $k > \frac{n}{2}$, $f(x) = A(x) \cdot g(x)$ und das Polynom $g(x)$ habe Grad $l$, d.h. $k + l = n$. Es ist $l < \frac{n}{2}$. Wir wählen dann einen irreduziblen Faktor $\hat{A}(x)$ von $g(x)$ aus, welcher Grad $\deg(\hat{A}(x)) \leq \deg(g(x)) = l < \frac{n}{2}$ hat, und wir fahren mit $\hat{A}(x)$ fort an Stelle von $A(x)$). Nach Multiplikation von $f(x)$ mit $n!$ hat das resultierende Polynom höchsten Koeffizienten $+-1$, d.h. wir können ohne Einschränkung annehmen, dass $A(x)$ höchsten Koeffizienten 1 hat, d.h.

$$A(x) = x^k + a_1 \cdot x^{k-1} + \ldots + a_{k-1}x + a_k$$
$$(k \geq \frac{n}{2})$$

Wir teilen den Beweis in zwei Schritte:

1. Jeder Primteiler $p$ von $a_k$ ist $\leq k$.

2. Dies liefert einen Widerspruch zum Schur-Sylvesterschen Satz über aufeinanderfolgende Zahlen.

1. Sei $\alpha$ eine Nullstelle von $A(x)$, $S$ der ganze Abschluss von $\mathbb{Q}(\alpha)$. Da $A(x)$ irreduzibel über $\mathbb{Q}$ und normiert ist, ist $A(x)$ das Minimalpolynom von $\alpha$ über $\mathbb{Q}$, d.h. die Norm von $\alpha$ über $\mathbb{Q}(\alpha)$ ist $N(\alpha) = +- a_k \equiv 0 \mod p$ und die Hauptideale $(\alpha) = \alpha \cdot S$ und $(p) = p \cdot S$ sind somit nicht teilerfremd (da $N(\alpha) \in (p) \cap (\alpha)$). Sei $\mathcal{P}$ ein Primideal von $S$, dass $(\alpha)$ und $(p)$ teilt und es sei

   $$(\alpha) = \mathcal{P}^r\mathcal{M} \ , \ (p) = \mathcal{P}^s\mathcal{N}$$

   wobei $\mathcal{M}$ und $\mathcal{N}$ nicht mehr durch $\mathcal{P}$ teilbar sind. Da $(\alpha)$ und $(p)$ nicht teilerfremd sind, ist $1 \leq r$ , $1 \leq s$ und aus der bekannten Formel ($\sum_i e_i \cdot f_i = [L : K]$) für Verzweigungsindizes und Körpergrad folgt $s \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(A(x)) = k$. Wir erhalten also

   $$1 \leq r \ , \ 1 \leq s \leq k \tag{4.1}$$

   Aus $f(\alpha) = 0$ folgt, dass

   $$n! + n!g_1\frac{\alpha}{1!} + \ldots + n!g_{n-1}\frac{\alpha^{n-1}}{(n-1)!} + -n!\frac{\alpha^n}{n!} = 0 \tag{4.2}$$

Der erste Summand ist genau durch $p^{v_p(n!)}$ teilbar, wobei bekanntlich

$$v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor \dots \tag{4.3}$$

Es dürfen nicht alles Summanden

$$n! g_\nu \frac{\alpha^\nu}{\nu!} \ (\nu = 1, 2, \dots, n, g_n = +-1) \tag{4.4}$$

in (4.2) durch höhere Potenzen als $\mathcal{P}^{sv_p(n!)}$ teilbar sein (sonst wäre $sv_p(n!)$ nicht die höchste Potenz von $\mathcal{P}$, die in $n!$ aufgeht). Wegen

$$\begin{aligned} v_\mathcal{P}(n! g_\nu \frac{\alpha^\nu}{\nu!}) &= v_\mathcal{P}(n!) + v_\mathcal{P}(g_\nu) + \nu \cdot v_\mathcal{P}(\alpha) - v_\mathcal{P}(\nu!) \\ &\geq v_\mathcal{P}(n!) + \nu \cdot \underbrace{v_\mathcal{P}(\alpha)}_{=r} - v_\mathcal{P}(\nu!) \\ &= s \cdot v_p(n!) + r \cdot \nu - s \cdot v_p(\nu!) \end{aligned}$$

für $\nu = 1, 2, \dots, n, g_n = +-1$ ist jeder Summand

$$n! g_\nu \frac{\alpha^\nu}{\nu!}$$

mindestens durch $\mathcal{P}^{s \cdot v_p(n!) + r \cdot \nu - s \cdot v_p(\nu!)}$ teilbar. Für wenigstens ein $\nu \geq 1$ muss damit

$$\nu r \leq s \cdot v_p(\nu!) \tag{4.5}$$

gelten ( ansonsten wäre $\nu r - s v_p(\nu!) > 0$ für alle $\nu = 1, 2, \dots, n$ und jeder Summand wäre durch höhere Potenzen $sv_p(n!) + (\nu r - sv_p(\nu!)))$ als $sv_p(n!)$ von $\mathcal{P}$ teilbar). Andererseits ist

$$v_p(\nu!) = \lfloor \frac{\nu}{p} \rfloor + \lfloor \frac{\nu}{p^2} \rfloor \dots < \sum_{i=1}^{\infty} \frac{\nu}{p^i} = \frac{\nu}{p-1}$$

Aus (4.1) und (4.5) erhalten wir nun

$$\nu \overbrace{\leq}^{(4.1)} \nu r \overbrace{\leq}^{(4.5)} s v_p(\nu!) < s \cdot \frac{\nu}{p-1} \overbrace{\leq}^{(4.1)} \frac{k\nu}{p-1},$$

d.h. $p - 1 < k$ oder $p \leq k$.

2. Das Polynom $A(x)$ ist auch ein Teiler von

$$F(x) = +- n! f(x) = x^n + -g_1 n x^{n-1} + -g_2 n(n-1) x^{n-2} + - \dots$$

Für $l = 1, 2, \dots, n$ ist der Koeffizient vn $x^{n-l}$ gegeben durch

$$+- g_l n(n-1)(n-2) \cdots (n-l+1)$$

Ist daher $q$ eine Primzahl, die

$$n(n-1)(n-2)\cdots(n-l+1)$$
$$(l=1,2,\ldots,n)$$

teilt, so ist $F(x) \equiv x^{n-l+1}H(x) \mod q$ für ein ganzzahliges Polynom $H(x)$. Ist $F(x) = A(x)B(x)$, so auch $x^{n-l+1}H(x) \equiv F(x) \equiv A(x)B(x) \mod q$ und aus der Eindeutigkeit der Zerlegung in irreduzible Faktoren folgt:
Das Produkt der höchsten Potenzen von $x$, die $\mod q$ Teiler von $A(x)B(x)$ ist, muss mindestens $x^{n-l+1}$ sein. Insbesondere muss es für $l = k$ mindestens $x^{n-k+1} = x^{n-k}x^1$ sein. Da $\deg F(x) = n, \deg A(x) = k$, ist $B(x)$ genau vom Grad $n-k$, d.h. $A(x)$ ist $\mod q$ mindestens einmal durch $x$ teilbar. Wegen $A(x) = x^1(x^{k-1} + a_1x^{k-2} + \ldots + a_{k-1}) + a_k$ muss daher $a_k \equiv 0 \mod q$ sein, d.h. $q$ ein Teiler von $a_k$ und aus 1. folgt $q \leq k$. Setzen wir $h := n-k$, so ist $h \geq k$, da $k \leq \frac{n}{2}$, und die $k$ aufeinanderfolgenden Zahlen

$$h+1 = n-k+1, h+2 = n-k+2, \ldots, h+k = n$$
$$(h \geq k)$$

sind nur durch Primzahlen $q \leq k$ teilbar, im Widerspruch zum Satz von Schur-Sylvester über aufeinanderfolgende Zahlen.

□

**Lemma 4.1 (Die Diskriminante von $E_n(x)$)** *Sei $D_n$ die Diskriminante von $E_n(x)$. Dann gilt:*

1. $D_n = (-1)^{\frac{n(n-1)}{2}}(n!)^n$
2. *Ist $p$ eine Primzahl mit $\frac{n}{2} < p < n$, so ist $v_p(D_n) = n$.*
3. *$D_n$ ist ein Quadrat in $\mathbb{Q}$ genau dann wenn $n \equiv 0 \mod (4)$.*
4. *$D_n$ ist durch keine Primzahl $p > n$ teilbar.*

Beweis:

1. Sei $B_n(x) = n! \cdot E_n(x)$. Wegen $E_n(x) = E_{n-1}(x) + \frac{x^n}{n!} = E_n'(x) + \frac{x^n}{n!}$ gilt auch $B_n(x) = n!(E_n'(x) + \frac{x^n}{n!}) = B_n'(x) + x^n$. Sind $\alpha_1, \alpha_2, \ldots, \alpha_n$ die Nullstellen von $B_n(x)$, so folgt

$$\begin{aligned} D_n &= (-1)^{\frac{n(n-1)}{2}} \cdot \prod_{\alpha_i} B_n'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \cdot \prod_{\alpha_i} (\underbrace{B_n(\alpha_i)}_{=0} - {\alpha_i}^n) \\ &= (-1)^{\frac{n(n-1)}{2}} \cdot \prod_{\alpha_i} (-{\alpha_i}^n) = (-1)^{\frac{n(n-1)}{2}} \cdot B_n(0)^n = (-1)^{\frac{n(n-1)}{2}}(n!)^n \end{aligned}$$

2. Ist $\frac{n}{2} < p < n$, so ist $p < n < 2p < p^2$, d.h. $n!$ wird von $p$ aber nicht von $p^2$ geteilt, also $v_p(n!) = 1$. Hieraus folgt unter Benutzung von 1.), dass $v_p(D_n) = n \cdot v_p(n!) = n$.

3. Für $n \geq 7$ kann man die Aussage direkt aus 1.) bestätigen. Ist aber $n \geq 8$, so gibt es nach Tschebyscheff eine Primzahl $p$ mit $\frac{n}{2} < p < n-2$. Nach 2.) ist damit $v_p(D_n) = n$. Falls $n$ ungerade ist, so ist also auch $v_p(D_n) = n$ ungerade und $D_n$ kann keine Quadratzahl sein. Ist $n \equiv 2 \mod (4)$, so ist $(-1)^{\frac{n(n-1)}{2}} = -1$, d.h. $D_n < 0$ und $D_n$ kann somit keine Quadratzahl in $\mathbb{Q}$ sein. Falls nun $n \equiv 0 \mod (4)$ ist, so ist $D_n$ eine Quadratzahl.

4. Das ist klar nach 1., weil die Fakultät $n!$ nur durch Primzahlen $q \leq n$ geteilt wird.

□

**Satz 4.4 (Schur, Die Galoisgruppe von $E_n(x)$)** *Die Galoisgruppe von $E_n(x)$ über $\mathbb{Q}[x]$ ist die alternierende Gruppe, falls $n \equiv 0 \mod 4$, ansonsten die symmetrische Gruppe.*

Beweis: Wir behandeln nur die Fälle $n \geq 8$, da man die anderen Fälle leicht mit GP PARI oder Maple überprüfen kann. Sei $p$ eine Primzahl im Intervall $\frac{n}{2} < p < n-2$, was nach Tschebyscheff möglich ist. Wir wollen zeigen, dass man den letzten Satz auf das Polynom $B_n(x) = n! \cdot E_n(x)$ anwenden kann:

1. Nach dem Schurschen Irreduzibilitätssatz ist $B_n(x)$ irreduzibel in $\mathbb{Q}[x]$.

2. Wegen Lemma (4.1) ist die Diskriminante $D_n$ von $B_n(x)$ mindestens durch die $n$-te Potenz von $p$ teilbar.

3. Das konstante Glied $B_n(0) = n!$ ist wegen $p < n < 2p < p^2$ durch $p$, aber nicht durch $p^2$ teilbar.

4. Es sei $m = n - p$. Für $1 \leq r \leq n$ ist der Koeffizient bei $x^{n-r}$ von $B_n(x)$ gegeben durch

$$n(n-1)\cdots(n-r+1) \equiv \begin{cases} 0 \mod p & \text{, falls } r \geq n+1-p \\ m(m-1)\cdots(m-r+1) \mod p & \text{, falls } r < n+1-p \end{cases}$$

Wegen $p > m$ ist nach Lemma (4.1),4) die Diskriminante von $B_m$ nicht durch $p$ teilbar. Damit sind alle Kriterien des vorigen Satzes erfüllt und $G$ ist die alternierende oder die symmetrische Gruppe. Wegen Lemma (4.1) ist die Diskriminante $D_n$ ein Quadrat in $\mathbb{Z}$ genau dann wenn $n \equiv 0 \mod 4$ und der Satz ist bewiesen. □

# Kapitel 5

# Die Galoisgruppe von $E_n(x)$ nach Coleman

Wir wollen das Newton-Polygon von $E_n(x)$ ausrechnen und brauchen dazu folgendes Lemma:

**Lemma 5.1 (Die Bewertung der Fakultät)** *Sei $n$ eine natürliche Zahl und $n = a_0+a_1p+\ldots+a_sp^s$ die $p$-adische Entwicklung von $n$. Dann ist $v_p(n!) = \frac{n-(a_0+a_1+\ldots+a_s)}{p-1}$*

Beweis: Wir wissen, dass $v_p(n!) = \lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor \ldots + \lfloor\frac{n}{p^s}\rfloor$. Damit erhalten wir $v_p(n!)(p-1) = \lfloor\frac{n}{p}\rfloor \cdot p + (\sum_{i=2}^{s}\lfloor\frac{n}{p^i}\rfloor \cdot p - \lfloor\frac{n}{p^{i-1}}\rfloor) - \lfloor\frac{n}{p^s}\rfloor$.
Aber für $i = 2, 3, \ldots, s$ ist

$$\begin{aligned}\lfloor\frac{n}{p^i}\rfloor \cdot p - \lfloor\frac{n}{p^{i-1}}\rfloor &= (a_i + a_{i+1}p + \ldots + a_sp^{s-i}) \cdot p - (a_{i-1} + a_ip + \ldots + a_sp^{s-i+1}) \\ &= -a_{i-1}\end{aligned}$$

und wir erhalten

$$\begin{aligned}v_p(n!)(p-1) &= (n - a_0) - (a_1 + a_2 + \ldots + a_{s-1}) - a_s \\ &= n - (a_0 + a_1 + \ldots + a_s).\end{aligned}$$

□

**Bemerkung 5.1 (Untere konvexe Hülle)** *Seien $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$ Punkte im $\mathbb{R}^2$ mit $x_0 < x_1 < \ldots < x_n$. Das Polygon der unteren konvexen Hülle der obigen Punkte lässt sich induktiv folgendermaßen berechnen:*

1. *Der Eckpunkt am weitesten links ist $(x_0, y_0)$.*
2. *Sind $(x_{e_1}, y_{e_1}), (x_{e_2}, y_{e_2}), \ldots, (x_{e_{i-1}}, y_{e_{i-1}})$ die $(i-1)$ ersten Eckpunkte ($x_{e_1} < x_{e_2} < \ldots < x_{e_{i-1}}$), so kann man den $i$-ten Eckpunkt so bestimmen:*
   *Wähle $e_i, e_{i-1} + 1 \leq e_i \leq n$, so dass*
   *$\frac{y_{e_i}-y_{e_{i-1}}}{x_{e_i}-x_{e_{i-1}}} \leq \frac{y_j-y_{e_i}}{x_j-x_{e_i}}$ für alle $x_j > x_{e_{i-1}}$ gilt.*
   *Dann ist $(x_{e_i}, y_{e_i})$ der $i$-te Eckpunkte. Graphisch kann man das so veranschaulichen:*

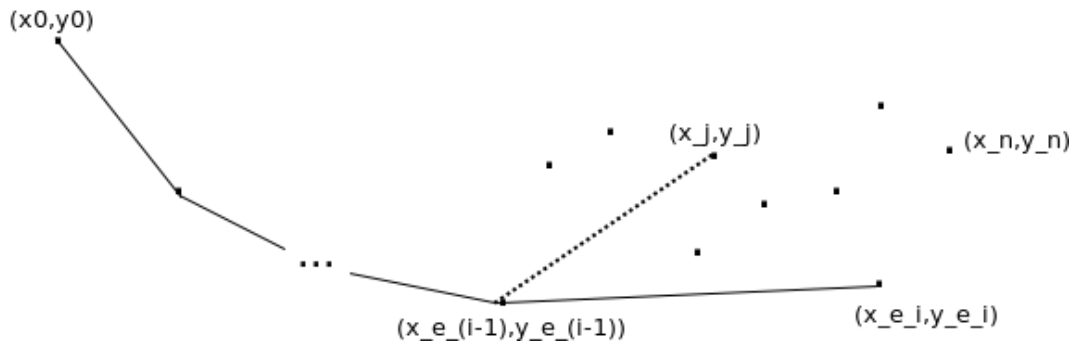


Abbildung 5.1: Untere konvexe Hülle

**Satz 5.1 (Das Newton-Polygon von $E_n(x)$)** *Sei $n = b_1p^{k_1} + b_2p^{k_2} + \ldots + b_sp^{k_s}$ die p-adische Entwicklung von n, $k_1 > k_2 > \ldots > k_s$ und $0 < b_i < p$ für $i = 1, 2, \ldots, s$. Dann sind die Eckpunkte des Newton-Polygons von $E_n(x)$ gegeben durch $(x_i, y_i)$ mit*

$$x_i = b_1p^{k_1} + b_2p^{k_2} + \ldots + b_ip^{k_i}$$
$$y_i = v_p(\frac{1}{x_i!}), 1 \leq i \leq s.$$

Beweis: Nach der vorigen Bemerkung ('Über die untere konvexe Hülle') müssen wir zeigen, dass
$\frac{y_i - y_{i-1}}{x_i - x_{i-1}} \leq \frac{y_j - y_{i-1}}{x_j - x_{i-1}}$ für alle $x_j > x_{i-1}, i > 0$. In unserem Fall ist $x_j = j$ und $y_j = v_p(\frac{1}{j!}) = -v_p(j!)$. Wegen $x_{i-1} < x_j \leq x_n = n$ und da $x_{i-1} = b_1p^{k_1} + \ldots + b_{i-1}p^{k_i-1}, k_1 > k_2 > \ldots > k_{i-1}$ , ist $x_j = b_1p^{k_1} + \ldots + b_{i-1} + c_rp^r + \ldots + cp + c_0$ die p-adische Entwicklung von $j = x_j$ und es ist $r < k_{i-1}$. Damit ist also $j - x_{i-1} = c_rp^r + \ldots + c_0, r < k_{i-1} < k_i$. Wir benutzen das Lemma 5.1 ('Über die Bewertung der Fakultät') und erhalten

$$\frac{y_j - y_{i-1}}{x_j - x_{i-1}} = \frac{x_{i-1} - j - (c_0 + \ldots + c_r)}{(p-1) \cdot (j - x_{i-1})}.$$

Beachtet man, dass $x_i - x_{i-1} = b_ip^{k_i}$ ist, so erhält man mit $y_i = -v_p(x_i!), y_{i-1} = -v_p(x_{i-1}!)$ wieder nach dem Lemma ('Über die Bewertung der Fakultät') folgendes

$$\frac{y_i - y_{i-1}}{x_i - x_{i-1}} = \frac{1 - p^{k_i}}{p^{k_i}(p-1)}.$$

Es ist also zu zeigen, dass

$$\frac{1 - p^{k_i}}{p^{k_i}(p-1)} \leq \frac{x_{i-1} - j - (c_0 + \ldots + c_r)}{(p-1) \cdot (j - x_{i-1})}.$$

für $j > x_{i-1}$ gilt. Wie man schnell einsieht ist letzte Ungleichung äquivalent zu $j - x_{i-} \leq p^{k_i}(c_0 + \ldots + c_r)$. Dies ist aber richtig, weil $j - x_{i-1} = c_rp^r + \ldots + c_1p + c_0$ und $r < k_i$. □

**Korollar 5.1 (Über die Teilbarkeit der Grade der Faktoren von $E_n(x)$)** *Sei $p^m$ ein Teiler von $n$. Dann teilt $p^m$ den Grad jedes irreduziblen Faktors von $E_n(x)$ über $\mathbb{Q}_p$*

Beweis: Nach Satz 5.1 ('Newton-Polygon von $E_n(x)$') hat eine Kante in dem Newton-Polygon von $E_n(x)$ die gekürzte Steigung

$$\frac{y_i - y_{i-1}}{x_i - x_{i-1}} = \frac{1 - p^{k_i}}{p^{k_i}(p-1)}.$$

Da $p^m$ ein Teiler von $n = b_1 p^{k_1} + \ldots + b_s p^{k_s}$ und $k_1 > k_2 > \ldots > k_s$ ist, muss $m < k_s < k_{s-1} < \ldots < k_1$ sein, d.h. $p^m$ ist auch ein Teiler jedes Nenners $p^{k_i}(p-1)$. Nach (...) ('Dem Hauptsatz über Newton-Polygone) teilt $p^m$ damit den Grad von jedem irreduziblen Faktor von $E_n(x)$ über $\mathbb{Q}_p$. □

**Korollar 5.2** *Sei $p^k \leq n$. Dann teilt $p^k$ den Grad des Zerfällungskörpers von $E_n(x)$ über $\mathbb{Q}_p$.*

Beweis: Da $p^k \leq n = b_1 p^{k_1} + b_2 p^{k_2} + \ldots + b_s p^{k_s}$ und $k_1 > k_2 > \ldots > k_s$ ist, muss $k \leq k_1$ sein. Wegen $m_1 = \frac{1-p^{k_1}}{p^{k_1}(p-1)}$ ist damit $p^k$ ein Teiler des Nenners $p^{k_1} \cdot (p-1)$ der Steigung $m_1$ der ersten Kante im Newton-Polygon von $E_n(x)$. Nach dem Hauptsatz über Newton-Polygone (Satz 1.2) teilt $p^k$ damit die Ordnung der Galoisgruppe von $E_n(x)$ über $\mathbb{Q}_p$, welche gleich dem Grad des Zerfällungskörpers ist. □

**Satz 5.2** *Das exponentielle Taylorpolynom $E_n(x)$ ist irreduzibel über $\mathbb{Q}$.*

Beweis: Sei $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ die Primfaktorzerlegung von $n$ und es sei $f(x) \in \mathbb{Q}[x]$ ein irreduzibler Faktor von $E_n(x)$. Wir wählen ein $i, 1 \leq i \leq s$ und fahren so fort:
Sei $f(x) = f_{i1}(x) \cdot \ldots \cdot f_{ir}(x)$ die Zerlegung von $f(x)$ in $\mathbb{Q}_{p_i}[x]$ in irreduzible Faktoren. Dann ist jedes $f_{ij}(x)$ $(1 \leq j \leq r)$ auch ein irreduzibler Faktor von $E_n(x)$ über $\mathbb{Q}_{p_i}$. Nach Korollar 5.1 ('Über die Teilbarkeit der Grade der Faktoren von $E_n(x)$') ist $p_i^{k_i}$ ein Teiler von jedem $degf_{ij}(x)$ (für $1 \leq j \leq r$), d.h. $p_i^{k_i}$ ist auch ein Teiler von $degf(x) = \sum_{j=1}^{r} degf_{ij}(x)$.
Wenn wir nun nacheinander $i = 1, i = 2, \ldots, i = s$ wie oben wählen, folgt:
Für jedes $i = 1, 2, \ldots, s$ ist $p_i^{k_i}$ ein Teiler von $degf(x) = \sum_{j=1}^{r} degf_{ij}(x)$. Also ist auch $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ ein Teiler $degf(x)$. Wegen $n = degE_n(x) \geq degf(x)$, folgt schließlich $degf(x) = n$ und hieraus die Irreduzibilität von $E_n(x) = f(x)$ über $\mathbb{Q}$. □

**Satz 5.3 (Die Galoisgruppe von $E_n(x)$ enthält prim-Zyklen und ist primitiv)** *Sei $p$ eine Primzahl, $\frac{n}{2} < p \leq n$ und $G$ die Galoisgruppe von $E_n(x) = 0$ über $\mathbb{Q}$. Dann enthält $G$ ein $p$-Zykel und ist primitiv.*

Beweis: Wegen $p^1 \leq n$ ist $p^1$ nach Korollar (5.3) ein Teiler des Grades des Zerfällungskörpers von $E_n(x)$ über $\mathbb{Q}_p$, welcher gleich dem Grad des Zerfällungskörpers von $E_n(x)$ über $\mathbb{Q}$ ist. Der Grad des Zerfällungskörpers von $E_n(x)$ über $\mathbb{Q}$ ist aber gleich der Ordnung $|G|$ der Galoisgruppe. Damit teilt $p$ also $|G|$. Wegen Satz 5.2 ist $E_n(x)$ irreduzibel über $\mathbb{Q}$ und damit ist $G$ transitiv. Nach Satz 3.3 ('Transitive Gruppen, die von einer genügend großen Primzahl geteilt werden) ist $G$ damit primitiv und enthält ein $p$-Zykel. □

**Lemma 5.2** *Sei $G$ die Galoisgruppe von $E_n(x) = 0$ über $\mathbb{Q}$. Dann ist $A_n \leq G$.*

Beweis: Für $n \leq 7$ kann man die Galoisgruppe mit einem CAS z.B. GP-PARI ausrechnen und stellt fest, dass die Behauptung stimmt. Für $n = 3$ kann man das in GP-PARI beispielsweise so ausrechnen:

```
polgalois(1/6*x^3 + 1/2*x^2 + x + 1)
```

Für $n \geq 8$ gibt es nach Tschebyscheff-Bertrand (2.4) eine Primzahl $p$, $\frac{n}{2} < p < n-2$. Nach 5.7 ist $G$ damit primitiv vom Grad $n$ und enthält einen $p$-Zykel. Nach dem Satz von Jordan enthält $G$ damit die alternierende Gruppe $A_n$. □

**Satz 5.4 (Die Galoisgruppe des exponentiellen Taylorpolynoms)** *Sei $G$ die Galoisgruppe von $E_n(x) = 0$ über $\mathbb{Q}$. Dann ist $G = S_n$, falls $n \not\equiv 0 mod 4$ und $G = A_n$ sonst.*

Beweis: Wie wir aus dem Abschnitt von Schur wissen (...) 'Die Diskriminante von $E_n(x)$' ist die Diskriminante $D_n = (-1)^{\frac{n(n+1)}{2}} \cdot (n!)^n$ von $E_n(x)$ genau dann ein Quadrat, wenn $n \equiv 0 mod(4)$ ist. Aus der Galois-Theorie wissen wir:
Enthält die Galoisgruppe die alternierende Gruppe, so ist $G = S_n$, falls die Diskriminante kein Quadrat ist und es ist $G = A_n$, falls die Diskriminante ein Quadrat ist. Da $A_n \leq G$ ist, folgt schließlich die Behauptung. □

# Kapitel 6

# Beobachtungen zu $C_n(x)$

Wir beginnen mit einer Eigenschaft von zusammengesetzten Polynomen (vgl. auch [Odoni184],[GeKlu]):

**Satz 6.1 (Imprimitivität und $f(x) = g(h(x))$)** *Sei $k$ ein Körper der Charakteristik 0, $f(x)$ ein irreduzibles Polynom aus $k[x]$ mit Nullstellenmenge $\Omega_f$ in einem algebraischen Abschluss. Weiter sei $K = k(\Omega_f)$ der Zerfällungskörper von $f(x)$ und $G = Gal(K/k)$ die Galoisgruppe. Folgende Aussagen sind äquivalent:*

*(1) Es gibt Polynome $g(x)$ aus $K[x]$ und $h(x)$ aus $k[x]$, beide vom Grad $\geq 2$ mit $f(x) = g(h(x))$.*

*(2) (a) $G$ ist imprimitiv mit einem Block $\Delta$,*

*(b) Ist $H = \{\sigma \in G | \sigma(\Delta) = \Delta\}$, $F$ der Fixkörper von $H$ und $b$ aus $\Delta$, so gilt:*
*$Irr(b, F, x) = h(x) - a$ für ein Polynom $h(x)$ aus $k[x]$ und $a$ aus $F$.*

Beweis: (1) $\Rightarrow$ (2)
$(a)$ Da $f(x)$ irreduzibel ist, ist zunächst $G$ transitiv auf $\Omega_f$. Sei $\Omega_g$ die Nullstellenmenge von $g$ in $K$. Dann ist $f(x) = g(h(x)) = \prod_{a \in \Omega_g} h(x) - a = \prod_{a \in \Omega_g} h_a(x)$, wobei $h_a(x) = h(x) - a$ für $a \in \Omega_g$. Da $f(x)$ als irreduzibles Polynom in $char(k) = 0$ auch separabel ist, ist auch jedes $h_a(x)$ separabel. Wir zeigen, dass für jedes $a \in \Omega_g$ die Nullstellenmenge $\Omega_a$ von $h_a(x)$ ein Block von $G$ ist. Zunächst ist klar, dass $\Omega_a \subset \Omega_f$ und wegen der Separabilität von $h_a(x)$ ist $|\Omega_a| = deg(h_a(x)) = deg(h(x)) \geq 2$. Andererseits ist $|\Omega_f| = deg(f(x)) = (deg(g(x))) \cdot (deg(h(x))) \geq 2 \cdot deg(h(x)) = 2 \cdot |\Omega_a| > |\Omega_a|$, also $1 < |\Omega_a| < |\Omega_f|$. Sei nun $\tau \in G$. Für jedes $b \in \Omega_a$ gilt dann $h(b) - a = 0$ und wenn wir $\tau$ auf die letzte Gleichung anwenden, erhalten wir wegen $h(x) \in k[x]$ folgendes:
$0 = \tau(h(b)) - \tau(a) = h(\tau(b)) - \tau(a)$.
Hieraus folgt $\tau(\Omega_a) = \Omega_{\tau(a)}$. Falls nun $\tau(a) = a$, so ist $\tau(\Omega_a) = \Omega_{\tau(a)} = \Omega_a$. Andernfalls ist $\tau(a) \neq a$ und es folgt $\tau(\Omega_a) \cap \Omega_a = \emptyset$.
$(b)$ Wir wählen ein $a \in \Omega_g$ und damit nach $(a)$ einen Block $\Delta := \Omega_a$ von $G$. Sei $H = \{\sigma \in G | \sigma(\Delta) = \Delta\}$, $F$ der Fixkörper von $H$ und sei $b$ aus $\Delta = \Omega_a$. Dann ist $b$ eine Nullstelle von $h(x) - a$. Da $H$ nach Satz 3.2 transitiv auf die Nullstellen $\Delta = \Omega_a$ von $h(x) - a$ wirkt, ist $h(x) - a$ irreduzibel in $F[x]$. Damit ist $Irr(b, F, x) = h(x) - a$.

(2) $\Rightarrow$ (1)
Sei also $\Delta$ ein Block von $G$, $H = \{\sigma \in G | \sigma(\Delta) = \Delta\}$ und sei $G = \cup_{\tau \in L} \tau H$ die Zerlegung von $G$ in Linksnebenklassen. Nach Satz 3.2 ist $H$ transitiv auf $\Delta$ und es gilt $\Omega_f = \cup_{\tau \in L} \tau(\Delta)$. Sei nun $b$ ein beliebiges Element aus $\Delta$. Nach Voraussetzung $(b)$ gibt es ein Polynom $h(x)$ aus $k[x]$ und ein $a$ aus $F$ mit $Irr(b, F, x) = h(x) - a$. Sei nun $\tau \in L$. Wir zeigen, dass jedes $\hat{b}$ aus $\tau(\Delta)$ eine Nullstelle von $h(x) - \tau(a)$ ist: Es ist $\hat{b} = \tau(b')$ für ein $b'$ aus $\Delta$. Da $H$ transitiv auf $\Delta$ ist, gibt es ein $\sigma \in H$ mit $b' = \sigma(b)$. Damit folgt
$h(\hat{b}) = h(\tau(b')) = h(\tau(\sigma(b))) = \tau(\sigma(h(b))) = \tau(\sigma(a)) = \tau(a)$, wobei die letzte Gleichheit gilt, da $a$ aus dem Fixkörper von $H$ und $\sigma$ aus $H$ ist. Weil $H = Gal(K/F)$ transitiv auf $\Delta$ operiert, ist das Polynom $\prod_{b' \in \Delta} x - b'$ irreduzibel in $F[x]$. Somit ist $\prod_{b' \in \Delta} x - b' = Irr(b, F, x) = h(x) - a$ und hieraus folgt $deg(h(x) - \tau(a)) = deg(h(x) - a) = |\Delta|$ für jedes $\tau$ aus $L$. Damit erhalten wir für jedes $\tau \in L$, dass $h(x) - \tau(a) = \prod_{\hat{b} \in \tau(\Delta)} x - \hat{b}$. Setzen wir $g(x) = \prod_{\tau \in L} x - \tau(a)$, so gilt also

$$\begin{aligned} g(h(x)) &= \prod_{\tau \in L} h(x) - \tau(a) = \prod_{\tau \in L} \Big( \prod_{\hat{b} \in \tau(\Delta)} x - \hat{b} \Big) \\ &= \prod_{b \in \Omega_f} x - b = f(x) \end{aligned}$$

□

Bemerkung: Die Aussagen (a) und (b) in (2) sind im Allgemeinen nich äquivalent, wie folgendes Beispiel zeigt: Seien $z_1, z_2, z_3, z_4$ transzendent über $\mathbb{C}$ und es sei $K := \mathbb{C}(z_1, \ldots, z_4)$. Die Diedergruppe $D_8$ erzeugt von $\tau = (1,2)(3,4)$ und $\sigma = (1,2,3,4)$ operiert transitiv auf die Nullstellenmenge $\Omega_f := \{z_1, z_2, z_3, z_4\}$ von $f(x) := (x - z_1) \cdot \ldots \cdot (x - z_4)$. Sei $k$ der Fixkörper von $D_8$ unter dieser Operation. Dann ist $D_8 = Gal(K/k)$. Wie man sich leicht überzeugt ist $\Delta = \{z_1, z_3\}$ ein Block von $\Omega_f$, d.h. $D_8$ operiert imprimitiv auf $\Omega_f$ und 2 (a) ist erfüllt. Sei nun $H = \{\alpha \in D_8 | \alpha(\Delta) = \Delta\}$ und $F$ der Fixkörper von $H$. Da $H$ nach Satz 3.2 transitiv auf $\Delta$ operiert, ist das Polynom $\prod_{b' \in \Delta} x - b' = (x - z_1) \cdot (x - z_3)$ irreduzibel in $F[x]$, somit das irreduzible Polynom von $b := z_1$ in $F$. Aber es ist nicht $h(x) - a = (x - z_1)(x - z_3) = x^2 - (z_1 + z_3)x + z_1 z_3$ für ein Polynom $h(x)$ aus $k[x]$, sonst wäre nämlich $h(x) = x^2 - (z_1 + z_3)x$ und hieraus würde folgen, dass $z_1 + z_3$ in $k = K^{D_8}$ liegt. Das ist aber nicht so, da zum Beispiel $\sigma(z_1 + z_3) = z_2 + z_4$ und die rechte Seite ist jedenfalls nicht gleich $z_1 + z_3$ (wäre sie das, so wären die $z_i$ wegen $z_1 + z_3 - z_2 - z_4 = 0$ nicht transzendent über $\mathbb{C}$).

**Korollar 6.1** *Sei $k$ ein Körper der Charakteristik 0, $f(x) = g(h(x))$ ein irreduzibles Polynom aus $k[x]$. Seien $g(x), h(x)$ Polynome aus $k[x]$ mit $deg(g(x)) = l$, $deg(h(x)) = m$, beide Grade $\geq 2$. Sei $K$ der Zerfällungskörper von $f(x)$ und $G = Gal(K/k)$ die Galoisgruppe. Dann ist $G$ eine Untergruppe von $S_m \wr S_l$.*

Beweis: Wie im Satz (6.1) ist $G$ imprimitiv mit einem Block $\Delta$ der Länge $m$. Aus Satz (3.2) b) folgt nun, dass $G$ eine Untergruppe von $S_m \wr S_l$ ist. □

**Korollar 6.2** *Die Galoisgruppe $G$ des Taylorpolynoms $C_n(x) = \sum_{k=0}^{n} \frac{x^{2k}}{(2k)!}$ über $\mathbb{Q}$ ist eine Untergruppe von $S_2 \wr S_n$.*

Beweis: Nach dem Schurschen Irreduzibilitätssatz ist das angegebene Polynom irreduzibel. Wir wenden dann Korollar (6.1) auf $C_n(x) = g(h(x))$ an, wobei $g(x) = \sum_{k=0}^{n} \frac{x^k}{(2k)!}$ und $h(x) = x^2$. □

**Lemma 6.1** *Sei $A = \{a_1, a_2, \ldots, a_n\}$ eine endliche Teilmenge von $k^*$ mit der Eigenschaft, dass für je zwei disjunkte Teilmengen $B, C \subset A$ das Element $\prod_{\substack{b\in B\\ c\in C}} \frac{b}{c}$ kein Quadrat in $k$ ist. Sei $\Lambda = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ wobei $\alpha_i$ eine Nullstelle von $x^2 - a_i$ ist und sei $\Lambda_i = \Lambda - \{\alpha_i\}$. Dann gilt für jedes i:*

*1) $x^2 - a_i$ ist irreduzibel über $k(\Lambda_i)$*

*2) $k(\alpha_i) \cap k(\Lambda_i) = k$*

*3) Die Galoisgruppe von $k(\Lambda)/k$ ist $C_2^n = C_2 \times \ldots \times C_2$.*

Beweis: Induktion nach $n$.
Für $n = 1$ sind alle Aussagen erfüllt, da in diesem Fall $\Lambda_1 = \emptyset$ und $x^2 - a_1$ irreduzibel über $k = k(\Lambda_1)$ ist und die Galoisgruppe von $k(\Lambda)/k = k(\alpha_1)/k$ ist die zyklische Gruppe $C_2$.
$n \to n+1$ :
Sei $A = \{a_1, \ldots, a_n, a_{n+1}\}$. Wir wollen zeigen, dass $x^2 - a_{n+1}$ irreduzibel in $k(\alpha_1, \ldots, \alpha_n)$ ist:
Angenommen es wäre $a_{n+1} = (A + B\alpha_n)^2$ für zwei $A, B$ aus $k(\alpha_1, \ldots, \alpha_{n-1})$. Dann ist $a_{n+1} = A^2 + a_n B^2, 0 = 2AB$.
Falls $A = 0$, so erhalten wir $B^2 - \frac{a_{n+1}}{a_n} = 0$. Nach Voraussetzung ist das Element $\hat{a}_n := \frac{a_{n+1}}{a_n}$ kein Quadrat in $k$. Die Menge $\{a_1, \ldots, a_{n-1}, \hat{a}_n\}$ erfüllt unsere Voraussetzungen, und da es $n$ Elemente hat, folgt per Induktion, dass $x^2 - \hat{a}_n$ irreduzibel über $k(\alpha_1, \ldots, \alpha_{n-1})$ ist im Widerspruch zu $B^2 - \hat{a}_n = 0$ und $B \in k(\alpha_1, \ldots, \alpha_{n-1})$.
Falls $B = 0$, dann ist $a_{n+1} = A^2$ ein Quadrat in $k(\alpha_1, \ldots, \alpha_{n-1})$. Per Induktion angewandt auf $\{a_1, \ldots, a_{n-1}, a_{n+1}\}$ ist das Polynom $x^2 - a_{n+1}$ irreduzibel über $k(\alpha_1, \ldots, \alpha_{n-1})$, im Widerspruch zu $A^2 - a_{n+1} = 0$ und $A \in k(\alpha_1, \ldots, \alpha_{n-1})$.
Also ist $x^2 - a_{n+1}$ irreduzibel über $k(\alpha_1, \ldots, \alpha_n)$ und per Induktion folgt, dass $\mathbb{B} = \{1, \alpha_1, \ldots, \alpha_{n+1}, \alpha_1 \cdot \alpha_2, \ldots, \alpha_1 \cdot \alpha_{n+1}, \ldots, \alpha_1 \cdot \ldots \cdot \alpha_{n+1}\}$ eine $k$-Basis von $k(\alpha_1, \ldots, \alpha_{n+1})$ ist.
Sei nun $A$ aus dem Schnitt $k(\alpha_{n+1}) \cap k(\alpha_1, \ldots, \alpha_n)$, also
$A = A_1 + A_2\alpha_{n+1} = B_1 + B_2\alpha_1 + \ldots + B_{n+1}\alpha_n + \ldots + B_m\alpha_1 \cdots \alpha_n$
wobei $A_i, B_i$ in $k$ liegen. Da $\mathbb{B}$ eine $k$-Basis ist, folgt dass $A = A_1 = B_1, A_2 = B_2 = \ldots = B_m = 0$, d.h. $A$ liegt in $k$.
Nach Corollary 1.15, p. 268, Lang (Algebra) folgt nun dass $G = G_1 \times \ldots \times G_n$ und da $G_i = Gal(k(\alpha_i)/k) = C_2$, ist die Behauptung bewiesen. □

**Bemerkung 6.1** *Die Voraussetzungen im obigen Lemma sind notwendig, wie folgendes einfache Beispiel zeigt:*
*Das Polynom $(x^2 - 2^2 \cdot 5) \cdot (x^2 - 3^2 \cdot 5)$ aus $\mathbb{Q}[x]$ hat $\mathbb{Q}(\sqrt{5})$ als Zerfällungskörper. Beide Zahlen $2^2 \cdot 5$ und $3^2 \cdot 5$ sind keine Quadrate in $\mathbb{Q}$, aber $\frac{2^2\cdot 5}{3^2\cdot 5} = (\frac{2}{3})^2$ ist ein Quadrat in $\mathbb{Q}$. Die Galois-Gruppe über $\mathbb{Q}$ ist aber $C_2$ und nicht $C_2 \times C_2$.*

**Bemerkung 6.2** *Die Eigenschaft*
*(1)* $B, C \subset A, B \cap C = \emptyset \Rightarrow \prod_{\substack{b\in B\\ c\in C}} \frac{b}{c}$ *kein Quadrat in* $k^*$
*im obigen Lemma ist äquivalent zur folgenden Eigenschaft:*
*(2)* $B \subset A \Rightarrow \prod_{b\in B} b$ *kein Quadrat in* $k^*$.

Beweis: (1) $\Rightarrow$ (2) : Wählen wir $C = \emptyset$, so ist $\prod_{c\in C} \frac{1}{c} = 1$.
(2) $\Rightarrow$ (1) : Seien $B, C \subset A, B \cap C = \emptyset$ und nehnem wir an $\prod_{\substack{b\in B\\ c\in C}} \frac{b}{c} = x^2$ sei ein Quadrat in $k^*$. Dann ist aber auch $\prod_{b\in B} b \cdot \prod_{c\in C} c = (x \cdot \prod_{c\in C} c)^2$ ein Quadrat in $k$, im Widerspruch dazu, dass das Produkt über die Teilmenge $D = B \cup C \subset A$ kein Quadrat in $k^*$ ist. □

**Bemerkung 6.3** *Sei* $f(x)$ *ein Polynom aus* $k[x], char(k) = 0, deg(f) = n$, $f$ *separabel mit Galois-Gruppe* $S_n$ *über* $k$. *Sei* $A = \{\alpha_1, \ldots, \alpha_n\}$ *die Nullstellenmenge von* $f$, $K = k(A)$ *der Zerfällungskörper. Für jede Teilmenge* $B \subset A$ *sei* $\prod_{b\in B} b$ *kein Quadrat in* $K$. *Dann hat das Polynom* $f(x^2)$ *Galois-Gruppe* $S_2 \wr S_n$ *über* $k$.

Beweis: Die Gruppe $S_n$ operiert $n$-transitiv auf $A$, also erst recht transitiv und $f(x)$ ist damit irreduzibel über $k$. Nach Voraussetzung ist $\alpha_i$ kein Quadrat in $k(\alpha_1, \ldots, \alpha_n)$, also ist erst recht $\alpha_i$ kein Quadrat in $k(\alpha_i)$ und $x^2 - \alpha_i$ damit irreduzibel über $k(\alpha_i)$. Wie man sich leicht überlegt (Gradformel für Körpererweiterungen und Minimalpolynom) ist auch $f(x^2)$ irreduzibel über $k$, hat also eine transititve Galoisgruppe $G = Gal(L/k)$, wobei $L$ der Zerfällungskörper von $f(x^2)$ ist. Ist $\Lambda = \{\beta_1, \ldots, \beta_n\}$, wobei $\beta_i$ eine Nullstelle von $x^2 - \alpha_i$ ist, so hat $K(\Lambda)/K$ nach dem vorigen Lemma (6.1) Galois-Gruppe $C_2^n$. Andererseits ist $K(\Lambda)$ der Zerfällungskörper von $(x^2 - \alpha_1) \cdots (x^2 - \alpha_n) = f(x^2)$, also $L = K(\Lambda)$. Damit folgt $|G| = [L : k] = [L : K] \cdot [K : k] = |Gal(L/K)| \cdot |Gal(K/k)| = 2^n \cdot n!$. Aus Korollar (6.2) folgt aber, dass $G$ eine Untergruppe von $S_2 \wr S_n$ ist. Die Behauptung folgt, weil $|G| = 2^n n! = |S_2 \wr S_n|$.

□

Ob man den letzten Satz dazu benutzen kann, um zu zeigen, dass $C_n(x)$ Galois-Gruppe $S_2 \wr S_n$ über $\mathbb{Q}$ hat, ist unklar. Rechnungen mit GP-Pari lassen jedoch vermuten, dass das Polynom $\sum_{k=0}^{n} \frac{x^k}{(2k)!}$ Galois-Gruppe $S_n$ über $\mathbb{Q}$ hat.

Angesichts der Schwierigkeiten auf die man stößt, wenn man versucht die Diskriminante von $C_n(x)$ zu berechnen, erscheint es sinnvoll darauf hinzuweisen, dass die Diskriminante von $C_n(x)$ nie ein Quadrat in $\mathbb{Q}$ ist. Dazu brauchen wir:

**Lemma 6.2** *Seien* $f(x), g(x)$ *Polynome aus* $k[x]$, $h(x) = f(g(x))$ *und* $\Delta_f$, $\Delta_h$ *die Diskriminante von* $f$ *bzw.* $h$. *Dann ist*

$$\Delta_h = \Delta_f^m \cdot Res(h, g') \cdot (-1)^{\frac{m\cdot n(mn-2+n)}{2}}$$

*wobei* $m = deg(g(x)), n = deg(f(x))$

Beweis: Wenn $\alpha$ über alle Nullstellen von $h$ läuft und $\beta$ über alle Nullstellen von $f$ läuft, so ist

$\Delta_f = (-1)^{\frac{n(n-1)}{2}} \cdot Res(f, f') = (-1)^{\frac{n(n-1)}{2}} \prod_\beta f'(\beta)$ und wegen $0 = h(\alpha) = f(g(\alpha))$ erhalten wir

$$\begin{aligned}\prod_\alpha f'(g(\alpha)) &= \prod_\beta f'(\beta)^{deg(g(x))} \\ &= (\prod_\beta f'(\beta))^m\end{aligned}$$

Damit folgt

$$\Delta_h = (-1)^{\frac{mn(mn-1)}{2}} Res(h, h') = (-1)^{\frac{mn(mn-1)}{2}} \prod_\alpha f'(g(\alpha)) \cdot g'(\alpha)$$

$$= (-1)^{\frac{mn(mn-1)}{2}} (\prod_\beta f'(\beta))^m \cdot \prod_\alpha g'(\alpha) = (-1)^{\frac{mn(mn-1)}{2}} \Delta_f^m Res(h, g') \cdot ((-1)^{\frac{n(n-1)}{2}})^m$$

□

Als Anwendung erhalten wir, dass die Diskriminante von $(2n)! \cdot C_n(x)$ für $n \geq 2$ kein Quadrat in $\mathbb{Z}$ ist:

**Korollar 6.3** *Sei $f(x) = (2n)! \sum_{k=0}^n \frac{x^k}{(2k)!}$, $h(x) = (2n)! \sum_{k=0}^n \frac{x^{2k}}{(2k)!}$, $\Delta_h$ die Diskriminante von $h(x)$ und $\Delta_f$ die Diskriminante von $f(x)$. Dann ist*

$$\Delta_h = \Delta_f^2 \cdot 2^{2n} \cdot (2n)! \cdot (-1)^{n(3n-2)}$$

*und $\Delta_h$ ist kein Quadrat in $\mathbb{Z}$.*

Beweis: Hier ist $g(x) = x^2$ im vorhergehenden Lemma und wegen
$Res(h, g') = \prod_\alpha g'(\alpha) = \prod_\alpha 2\alpha = 2^{2n} \cdot h(0) = 2^{2n} \cdot (2n)!$
folgt $\Delta_h = \Delta_f^2 \cdot 2^{2n} \cdot (2n)! \cdot (-1)^{n(3n-2)}$. Nach Tschebyscheff gibt es eine Primzahl $n < p < 2n$, also $v_p((2n)!) = 1$. Damit ist $v_p(\Delta_h) = 2v_p(\Delta_f) + v_p((2n)!) = 2v_p(\Delta_f) + 1$ ungerade und $\Delta_h$ kann kein Quadrat in $\mathbb{Q}$ sein. □

Es sei ab jetzt $D_n(x) = (2 \cdot n)! \cdot \sum_{k=0}^n \frac{x^k}{(2k)!}$ und $S_n(x) = (2n+1)! \cdot \sum_{k=0}^n \frac{x^k}{(2k+1)!}$. Nach dem Schurschen Irreduzibilitätssatz ist $D_n(x^2)$ irreduzibel über $\mathbb{Q}[x]$,d.h. auch $D_n(x)$ ist es. (Schur hat in einer späteren Arbeit mit ähnlichen Methoden wie im Irreduzibilitätssatz, d.h. unter Benutzung von zahlentheoretischen Sätzen, zeigen können, dass auch $S_n(x)$ irreduzibel über $\mathbb{Q}[x]$ ist. Eine Überprüfung für kleine Grade mit GP Pari lässt vermuten, dass auch $S_n(x)$ die symmetrische Galoisgruppe hat. Wir wollen hier aber nur auf die Eigenschaften von $S_n(x)$ eingehen, die uns helfen die Polynome $D_n(x)$ besser zu verstehen.)

**Lemma 6.3 (Die erste Seite von links im Newton-Polygon von $D_n(x)$)** *Es sei $p$ eine Primzahl im Intervall $\frac{n}{2} < p < n$. Dann hat die erste Seite von links im Newton-Polygon*

$$\textit{Länge } p \textit{ und Steigung } -\frac{2}{p}$$

Beweis: Multiplikation von $D_n(x)$ mit $\frac{1}{(2n)!}$ verschiebt das Newton-Polygon nur nach unten, d.h. wir können auch die erste Seite von

$$\frac{1}{(2n)!} \cdot D_n(x) = \sum_{j=0}^{n} \frac{x^j}{(2j)!}$$

berechnen:
Wie man durch Vergleich der Steigungen im Polygon einsieht, reicht es zu zeigen, dass

$$\frac{2}{p} \geq \frac{v_p((2j)!)}{j} \ (\forall j = 1, 2 \ldots n)$$

gilt. Wir wissen:

$$v_p((2j)!) = \lfloor \frac{2j}{p} \rfloor + \lfloor \frac{2j}{p^2} \rfloor \ldots + \lfloor \frac{2j}{p^r} \rfloor$$

für eine natürliche Zahl $r$ . Es reicht zu zeigen, dass $r = 1$ ist, weil dann folgt:

$$v_p((2j)!) = \lfloor \frac{2j}{p} \rfloor \leq \frac{2j}{p}$$

. Wir haben nach Voraussetzung an $j, n$ und $p$:

$$2j \leq 2n < 4p < p^2$$

, d.h. $\frac{2j}{p^2} < 1$, also auch $\lfloor \frac{2j}{p^2} \rfloor = 0$ und es folgt, dass $r = 1$.

□

**Satz 6.2** *Die Galoisgruppe von $D_n(x)$ ist entweder die alternierende oder die symmetrische Gruppe.*

Beweis: Da $D_n(x)$ irreduzibel über $\mathbb{Q}[x]$ ist, hat es eine transitive Galoisgruppe. Wegen dem letzten Lemma und aus dem Hauptsatz über Newton-Polygone ist die Ordnung der Gruppe durch eine Primzahl $p$ im Intervall $\frac{n}{2} < p < n$ teilbar. Eine solche Gruppe muss aber wegen Satz 3.3 ('Transitive Gruppen, die von einer großen Primzahl geteilt werden) schon primitiv sein. Nach dem Satz von Jordan folgt nun die Behauptung. □

**Lemma 6.4** *Sei nun $p$ eine Primzahl, $n < p < 2n$ und $r = n - \frac{p+1}{2}$, $t = n - \frac{p-1}{2}$. Dann ist*

$$D_n(x) \equiv x^{\frac{p+1}{2}} S_r(x) \mod p \tag{6.1}$$

$$S_n(x) \equiv x^{\frac{p-1}{2}} D_t(x) \mod p \tag{6.2}$$

Beweis: Wir beweisen nur die erste Aussage, da die zweite ähnlich zu beweisen ist: Es ist $D_n(x) = x^n + 2n(2n-1)x^{n-1} + 2n(2n-1)(2n-2)(2n-3)x^{n-2} + \ldots + (2n)!$. Für $0 \leq l \leq n$ sind die verschiedenen Glieder in $D_n(x)$ gegeben durch

$$2n(2n-1) \cdots (2l+1)x^{n-l}$$

Damit folgt

$$\begin{aligned} D_n(x) &\equiv x^n + 2n(2n-1)x^{n-1} + 2n(2n-1)(2n-2)(2n-3)x^{n-2} + \ldots + (2n)! \mod p \\ &\equiv x^{\frac{p+1}{2}}(x^r + (2r+1)(2r)x^{r-1} + (2r+1)(2r)(2r-1)(2r-2)x^{r-2} + \ldots + (2r+1)!) \mod p \\ &\equiv x^{\frac{p+1}{2}} S_r(x) \mod p \end{aligned}$$

□

**Satz 6.3** *Wir behalten die Bezeichnungen des vorigen Lemmas bei. Es sei $\alpha$ eine Nullstelle von $D_n(x)$, $\Delta_n$ die Diskriminante von $D_n(x)$ und $d_n$ die Diskriminante von $\mathbb{Q}(\alpha)$, $R$ der Ganzheitsring von $\mathbb{Q}(\alpha)$. Falls einer der äquivalenten Fälle eintritt*

1. *Außer $x$ hat $D_n(x)$ keine mehrfachen Nullstellen* mod $p$.
2. *Das Polynom $S_r(x)$ hat keine mehrfachen Nullstellen* mod $p$.
3. *Die Diskriminante von $S_r(x)$ ist nicht durch $p$ teilbar.*

*so ist die Galoisgruppe von $D_n(x)$ über $\mathbb{Q}[x]$ die symmetrische Gruppe.*

Beweis: Die Äquivalenz von 1. und 2. beweist man mit Hilfe der formalen Ableitung unter der Benutzung der Produktregel und der Gleichung (6.1). Die Äquivalenz von 2. und 3. dürfte eigentlich bekannt sein, basiert aber darauf, dass die Diskriminante eines Polynoms geschrieben werden kann als $(\prod_{i<j} \alpha_i - \alpha_j)^2$, wobe wir über die Nullstellen dieses Polynoms laufen.
Es sei nun 1. erfüllt. Da der konstante Koeffizient von $D_n(0) = (2n)!$ durch $p$ aber nicht durch $p^2$ teilbar ist, wird im Dedekind-Kriterium 2.$a$ mit $f_s(x) = x, e_s = \frac{p+1}{2}$ erfüllt, 2.$b$ dagegen nicht. Damit folgt nach eben diesem Kriterium, dass $v_p(\Delta_n) = v_p(d_n)$. Wegen $d_n = |R : \mathbb{Z}[\alpha]| \cdot \Delta_n$ ist $|R : \mathbb{Z}[\alpha]|$ nicht durch $p$ teilbar. Nach der Primfaktorzerlegung durch Kummer-Dedekind (siehe S.184, Kapitel 13.4, Satz 6, A.Leutbecher, Zahlentheorie) gibt es ein Primideal $\mathcal{P}$ von $R$, so dass $p$ mit Verzweigungsindex $e = \frac{p+1}{2}$ und Restklassengrad $f = \deg x = 1$ über diesen zerfällt. Offensichtlich ist $e = \frac{p+1}{2}$ nicht durch $p$ teilbar. Nach dem Dedekindschen (Differenten/) Diskriminanten-Satz (...) ist daher

$$v_{\mathcal{P}}(d_n) = e - 1 = \frac{p+1}{2} - 1 = \frac{p-1}{2}.$$

Damit ist die höchste in $d_n$ enthaltene Potenz von $p$ gleich

$$p^{f(e-1)} = p^{1 \cdot \frac{p-1}{2}} = p^{\frac{p-1}{2}}$$

Nun können wir nach einem Satz von Robert Breusch, der die Ideen von Tschebyscheff verfeinert, die Primzahl $p$ aus dem Intervall $n < p < 2n$ so wählen, dass $\frac{p-1}{2}$ ungerade ist. Damit ist aber auch

$$v_p(d_n) = \frac{p-1}{2}$$

ungerade und $d_n$ kann daher kein Quadrat in $\mathbb{Q}$ sein, d.h. die Galoisgruppe ist die symmetrische und nicht die alternierende Gruppe. □

# Literaturverzeichnis


[Schur20] I.Schur: *Beispiele für Gleichungen ohne Affekt.* Gesammelte Anhandlungen, Band III, No. 38, 280-285, 1920.

[Schur29I] I.Schur: *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen I.* Gesammelte Anhandlungen, Band III, No. 64, 140-151, 1929.

[Schur29II] I.Schur: *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen II.* Gesammelte Anhandlungen, Band III, No. 65, 370-391, 1929.

[Schur30] I.Schur: *Gleichungen ohne Affekt.* Gesammelte Anhandlungen, Band III, No. 67, 191-197, 1930.

[Schur31] I.Schur: *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome.* Gesammelte Anhandlungen, Band III, No. 70, 227-233, 1931.

[Hajir05] F.Hajir: *On the Galois group of generalized Laguerre polynomials.* Journal de Theorie des Nombres de Bordeaux, 17, 2005. (517-525)

[Hall59] M.Hall: *Theory of Groups.* Macmillan, 1959. (Theorems 5.6.2 and 5.7.2)

[Jordan72] C.Jordan: *Sur la limite de transitivite des groupes non alternes.* Bul. Soc. Math. France 1, (1872-1873), 40-71 (Theoreme 1)

[Landau] Landau: *Handbuch der Lehre von der Verteilung der Primzahlen.* Bd.I, S.91 und 1959.

[Coleman87] R.F.Coleman: *On the Galois groups of the exponential Taylor polynomials.* Enseign. Math (2) 33 (1987), no. 3-4, 183-189.

[Odoni84] R.W.K.Odoni: *The Galois Theory of Iterates and composites of polynomials.* Proc.London Math. Soc. (3), 51 (1985) 385-414. Lemma 4.1

[Gouvea97] F.Q.Gouvea: *p-adic numbers.* Sedond edition, Springer, Berlin, 1997.

[PARI] GP PARI: Version 2.3.4

[Huppert67] B.Huppert: *Endliche Gruppen I.* Springer-Verlag, Berlin, Heidelberg, New York,1967.

[Lang] S.Lang: *Algebraic Number Theory*. Springer, Second Edition, 1970.

[Lang02] S.Lang: *Algebra*. Graduate Texts in Mathematics, Revised 3rd Edition, Springer, 2002.

[Artin42] E.Artin: *Galois Theory*. Dover Publications, Inc, Mineola, New York, 1998.

[Leutbecher] A.Leutbecher: *Zahlentheorie, Eine Einführung in die Algebra*. Springer, 1991.

[Schmid08] P.Schmid: *Algebraische Zahlentheorie*. Vorlesung Tübingen, WS 2008 / 2009.

[Kolle02] M.Kölle: *Zur Berechnung von Galoisgruppen globaler Polynome durch Newton-Polygone*. Dissertation, Mathematische Fakultät, Eberhard-Karls-Universität zu Tübingen, Stuttgart, 2002.

[Neukirch] J.Neukirch: *Algebraic Number Theory*. Springer Verlag, Berlin, Heidelberg, 1999.

[GeKlu] K.Geissler, J.Klüners: *Galois Group Computation for Rational Polynomials*. J.Symbolic Computation (2000) 11, 1-23, Theorem 3.1.

# Danksagung

Ich bedanke mich an erster Stelle bei meiner Familie, die mich immer unterstützt hat bei dem was ich mache. Mein ehemaliger Lehrer Klaus Pullmann hat mich während der Schulzeit und während meines Studiums sehr unterstützt. Dafür möchte ich mich herzlichst bedanken. Weiterhin möchte ich mich bei meinem Betreuer Prof. Dr. M. Lehn bedanken, der mir stets geholfen hat falls ich nicht vorankam.


# Erklärung

Hiermit versichere ich, diese Diplomarbeit selbstständig und nur unter Verwendung der im Literaturverzeichnis angegebenen Hilfsmittel angefertigt zu haben.

Mainz, den 27.05.2010

Orges Leka