Zur Berechnung von Galoisgruppen globaler Polynome durch Newton-Polygone

Dissertation

der Mathematischen Fakultät
der Eberhard-Karls-Universität zu Tübingen
zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von
Michael Kölle
aus Stuttgart

2002

Tag der mündlichen Prüfung: 13. August 2002
Dekan: Prof. Dr. Wolfgang Knapp
1. Berichterstatter: Prof. Dr. Peter Schmid
2. Berichterstatter: Prof. Dr. Wolfgang Knapp

Inhaltsverzeichnis

Einleitung

Sei $h \in K[X]$ ein separables Polynom vom Grade $n \geq 3$ über dem Körper K. Die Galoisgruppe $G = \mathrm{Gal}_K(h)$ von h ist die Gruppe aller K-Automorphismen "des" Zerfällungskörpers von h, aufgefasst als Permutationsgruppe auf der Wurzelmenge W_h von h. Wir erhalten also G als Untergruppe der symmetrischen Gruppe $\mathrm{Sym}(W_h) \simeq S_n$. Genau dann ist G transitiv, wenn h irreduzibel über K ist. Kein allgemeines Kriterium dieser Art ist bekannt zur Beschreibung der Primitivität. (Ausnahme sind die Monodromiegruppen, wo man den Satz von Lüroth ausnutzen kann.) Dies macht schon deutlich, auf welche Schwierigkeiten man bei der Berechnung von G im allgemeinen stößt. Diese sind durchaus vergleichbar mit dem Problem, zu vorgegebener endlicher Gruppe G ein Polynom zu finden mit G als Galoisgruppe (Umkehrproblem der Galoistheorie).

Abschätzungen nach oben für G erhält man in der Regel durch die Berechnung geeigneter Invarianten (vgl. Stauduhar [27], [28], Girstmair [7] oder Matzat [16], p.207 ff.). Wohlbekannt ist etwa, dass $G \leq A_n$ genau dann aus geraden Permutationen besteht, wenn die Diskriminante D_h von h ein Quadrat in K ist ($\mathrm{char}(K) \neq 2$).

Ebenso wie im Falle des Umkehrproblems der Galoistheorie ist die Entwicklung von Methoden zur Berechnung von $G = \mathrm{Gal}_K(h)$ über *Zahlkörpern* von Interesse. Sei also K ein algebraischer Zahlkörper und $\mathfrak{p}$ eine (endliche oder unendliche) Primstelle von K. Dann kann man G durch Übergang zur $\mathfrak{p}$-adischen Komplettierung $K_\mathfrak{p}$ studieren. Aus der Zerlegung von h über $K_\mathfrak{p}$ erhält man Informationen über die Zerlegungsgruppe $G_\mathfrak{P}$ einer Primstelle $\mathfrak{P}|\mathfrak{p}$ des Zerfällungskörpers L von h. Ist $\mathfrak{p}$ endlich und h $\mathfrak{p}$-ganz, so kann man die Reduktion h mod $\mathfrak{p}$ studieren. Ist diese Reduktion separabel (d.h $\mathfrak{p}$ ist kein Teiler von D_h), so verzweigt $\mathfrak{p}$ nicht in L, und $G_\mathfrak{P}$ ist isomorph zur Galoisgruppe von h mod $\mathfrak{p}$ als Permutationsgruppe der Wurzeln (Satz von Dedekind und Bauer). Ist die Reduktion inseparabel, so kann man stets das *Newton-Polygon* von h bzgl. $\mathfrak{p}$ betrachten: Aus den Steigungen der Seiten des Polygons erhält man Informationen über die Verzweigung und damit die Trägheitsgruppe $T_\mathfrak{P}$ von $\mathfrak{P}$.

Ursprünglich führte Newton Polygone zur Berechnung komplexer Kurven zweier Variablen ein. Die Entwicklung um singuläre Punkte führte zu den heutigen Puiseux-Reihen der Kurve (vgl. Brieskorn-Knörrer [1] für Details). Die Methode liefert analoge $\tilde{g}$-adische Entwicklungen nach Polynomen $\tilde{g}$ in einer Variablen. Solch eine Theorie (für ganzzahlige Polynome) wurde von Ore [22] in den 20-er Jahren des vergangenen Jahrhunderts entwickelt. In jüngerer Zeit wurde sie wiederentdeckt (siehe etwa [3], [10], [17], [18], [24]).

In dieser Arbeit wird das Newton-Polygon von h bzgl. einer endlichen Primstelle $\mathfrak{p}$ von K studiert. Sei h normiert ($a_0 = 1$),

$$h = X^n - a_1 X^{n-1} + - \cdots + (-1)^n a_n.$$

Das Newton-Polygon von h bzgl. $\mathfrak{p}$ (und $\tilde{g} = X$) ist die untere konvexe Hülle der Punkte $(i, v_{\mathfrak{p}}(a_i))$, $a_i \neq 0$, im euklidischen $\mathbb{R}^2$. In der Praxis ist es oft zweckmäßig, die Entwicklung von h nach anderen Polynomen $\tilde{g}$ zu betrachten, etwa solchen $\tilde{g}$, deren Reduktion mod $\mathfrak{p}$ irreduzible Faktoren von h mod $\mathfrak{p}$ sind. In der Theorie kann man sich aber auf die Untersuchung des obigen Standard-Polygons beschränken (nach Übergang zu einer geeigneten unverzweigten Erweiterung und eventueller Substitution $X \mapsto X + c$). Außerdem besteht das Newton-Polygon eines reduziblen Polynoms aus den Polygonen der Faktoren, indem man die Seiten nach wachsender Steigung ordnet. Wir setzen daher h als irreduzibel über K voraus. (Dies kann häufig aus dem Newton-Polygon abgelesen werden.) Dann kann das Verzweigungsverhalten von $\mathfrak{p}$ im Wurzelkörper $K[X]/(h)$ sinnvoll studiert werden.

Sei S_m eine Seite des Newton-Polygons von h bzgl. $\mathfrak{p}$ der Länge (Abszisse) E und Höhe (Ordinate) V mit nichtnegativer Steigung $m = \frac{V}{E}$. (Bei negativer Steigung ersetze man $h(X)$ durch $(-1)^n \frac{X^n}{a_n} h(X^{-1})$.) Wir setzen $d = \mathrm{ggT}(V, E)$ und $\nu = \frac{V}{d}$, $e = \frac{E}{d}$. Ferner sei $e_{\mathfrak{P}}$ der Verzweigungsindex von $\mathfrak{P}$ über $\mathfrak{p}$, $W_m = W_{h,m} = \{\theta \in W_h : v_{\mathfrak{P}}(\theta) = e_{\mathfrak{P}} m\}$ und

$$\hat{h}_m = \prod_{\theta \in W_m} (X - \theta).$$

Da $K_{\mathfrak{p}}$ henselsch und $m \geq 0$ ist, besitzt das Polynom $\hat{h}_m$ Koeffizienten im Ring der ganzen Zahlen von $K_{\mathfrak{p}}$ (Neukirch [21], II.6.4). Offenbar teilt e die Ordnung der Trägheitsgruppe $|T_{\mathfrak{P}}| = e_{\mathfrak{P}}$. Über $K_{\mathfrak{p}}$ zerfällt h in ein Produkt von paarweise teilerfremden $\hat{h}_m$ zu den Steigungen m der verschiedenen Seiten des Newton-Polygons.

Wir können $L_{\mathfrak{P}}$ mit $K_{\mathfrak{p}} L$ und $G_{\mathfrak{P}}$ mit der Galoisgruppe $\mathrm{Gal}(L_{\mathfrak{P}} | K_{\mathfrak{p}})$ identifizieren. Über $K_{\mathfrak{p}}$ zerfällt h in ein Produkt verschiedener normierter Primpolynome $\hat{h}_{\wp}$ der Grade $n_{\wp}$ (=Bahnenlängen von $G_{\mathfrak{P}}$ auf W_h). Sei $N = K(\theta)$ für eine feste Wurzel θ von h und $\mathcal{P}$ die Menge der Primideale $\wp | \mathfrak{p}$ von N. Nach einem Satz von van der Waerden ist

$$\mathfrak{p} R_N = \prod_{\wp \in \mathcal{P}} \wp^{e_{\wp}}$$

die Zerlegung von $\mathfrak{p}$ in N, und $f_\wp = n_\wp/e_\wp$ sind die Restklassengrade. Wir sagen, ein Primideal $\wp$ von N gehört zur Seite S_m des Newton-Polygons ($\wp \in \mathcal{P}_m$), falls $\hat{h}_\wp$ ein Teiler von $\hat{h}_m$ ist. Das bedeutet $\mathcal{P}_m = \{\wp \in \mathcal{P} : v_\wp(\theta) = e_\wp m\}$.

In der Praxis ist es meist schwierig, die *lokalen Polynome* $\hat{h}_\wp$ und $\hat{h}_m$ zu berechnen. Auch die Berechnung der Faktoren in $n_\wp = e_\wp f_\wp$ ist in der Regel nicht einfach. Die naheliegende Frage ist, ob man das Polynom $\hat{h}_m$, dessen Galoisgruppe G_m eine Untergruppe von $G_\mathfrak{P}$ und daher von G ist, durch ein *globales Polynom* $h_m \in K[X]$ mit derselben Galoisgruppe (über $K_\mathfrak{p}$) ersetzen kann. Dieses Polynom h_m sollte aus der Seite S_m des Newton-Polygons in einfacher Weise zu berechnen sein.

Die grundlegende Idee zur Definition von h_m stammt von Ore [22]. Die Seite S_m beginne etwa mit dem Punkt $(r, v_\mathfrak{p}(a_r))$ und ende bei $(s, v_\mathfrak{p}(a_s))$. Dann ist also $s - r = E$. Wir definieren h_m als das normierte Polynom vom Grade E mit Monomen $(-1)^k a_r^{-1} a_{r+k} X^{E-k}$, wobei nur solche k betrachtet werden, für welche $(r+k, v_\mathfrak{p}(a_{r+k}))$ auf der Seite S_m liegt. Dieses Polynom ist $\mathfrak{p}$-ganz und heißt der S_m oder m *zugeordnete Faktor* von h. Offenbar besteht das Newton-Polygon von h_m nur aus einer Seite S der Länge E und Steigung m, und alle Punkte liegen auf S. Sei π ein Element von K der Ordnung 1 bei $\mathfrak{p}$ ($v_\mathfrak{p}(\pi) = 1$). Wir können das Polynom h_m "kürzen", da nur Monome $\neq 0$ vorkommen, deren Grade Vielfache von e sind. Dann definieren wir das S_m oder S *zugeordnete Polynom* h_S als das normierte Polynom vom Grade d, dessen Monome $(-1)^{je} a_r^{-1} a_{r+je} \pi^{-je} X^{d-j}$ sind. Mit anderen Worten: h_m entsteht aus h_S durch die Substitution $X \mapsto \pi^{-\nu} X^e$ und anschließender Multiplikation mit $\pi^V = \pi^{d\nu}$.

Die Koeffizienten von h_S sind offenbar $\mathfrak{p}$-Einheiten in K. Wir bezeichnen die Seite S als *regulär*, falls die Reduktion h_S mod $\mathfrak{p}$ separabel ist. Zwar hängt h_S ab von der Wahl des Primelements π, nicht aber der Begriff der Regularität. Ist die Steigung $m = 0$, so gilt $e = 1$ und $h_S = h_m$. Im Falle der Regularität von S erhalten wir dann $e_\wp = 1$. (Liegt im Falle $m = 0$ keine Regularität vor, so ist eine geeignete Substitution der Variablen vorzunehmen.)

Zum Beispiel ist h genau dann ein Eisenstein-Polynom bzgl. $\mathfrak{p}$ (und damit irreduzibel über K), wenn das Newton-Polygon nur aus einer Seite S besteht und $h_m = X^n + (-1)^n a_n$ ein reines Polynom ist. In diesem Fall ist h_S linear, also S regulär.

Hauptsatz. *Sei $S = S_m$ eine reguläre Seite des Newton-Polygons von h bzgl. $\mathfrak{p}$ der Länge E mit nichtnegativer Steigung $m = \frac{\nu}{e}$ (gekürzt). Für eine feste Wurzel θ von h (irreduzibel über K) seien $\mathcal{P}_m$, $\hat{h}_m$, h_m, h_S wie oben erklärt.*

(a) *Die verschiedenen Primfaktoren $\bar{g}_\wp$ von h_S mod $\mathfrak{p}$ können so durch $\mathcal{P}_m$ indiziert werden, dass $f_\wp = \mathrm{grd}(\bar{g}_\wp)$ jeweils der Restklassengrad ist. Für alle $\wp \in \mathcal{P}_m$ ist $e = e_\wp$ der*

Verzweigungsindex über $\mathfrak{p}$.
(b) *Über* $K_{\mathfrak{p}}$ *hat* $h_m = \prod_{\wp \in \mathcal{P}_m} h_\wp$ *eine entsprechende Primfaktorzerlegung, wobei jeweils* $\mathrm{grd}(h_\wp) = e_\wp \cdot f_\wp$ *der Grad des Primfaktors* $\hat{h}_\wp$ *von* h *ist.*
(c) *Ist überdies* $\mathfrak{p}$ *kein Teiler von* e *(zahme Verzweigung), so haben* h_m *und* $\hat{h}_m$ *denselben Zerfällungskörper über* $K_{\mathfrak{p}}$ *(in einem festen algebraischen Abschluss) und ihre Galoisgruppe* G_m *hat isomorphe Permutationsdarstellungen auf den Wurzeln dieser Polynome.*

Der Beweis dieses Satzes steht im Mittelpunkt der Kapitel 1 und 2 dieser Dissertation. In Kapitel 3 geben wir auf der Grundlage dieses Satzes einige Anwendungen. Dabei können wir aktuelle Resultate, wie etwa die von Cohen, Movahhedi und Salinier [4], [5], [18], [19], Komatsu [12], [13] und Sase [25], verbessern.

Die Aussage (c) enthält das bekannte Resultat über total und zahm verzweigte Erweiterungen lokaler Körper ([21], II.7.7). In diesem Fall ist h ein Eisenstein-Polynom bzgl. $\mathfrak{p}$ und $e = n$. Ist $\mathfrak{p}$ kein Teiler von n, so ist $K_{\mathfrak{p}}(\theta) = K_{\mathfrak{p}}(\sqrt[n]{(-1)^{n+1}a_n})$ bei geeigneter Wahl der Wurzeln. Nach der Hilbert-Theorie ist dann $T_{\mathfrak{P}}$ zyklisch und wird daher von einem $n-$Zykel erzeugt.

Hier ein konkretes Beispiel: Sei p eine ungerade Primzahl, $K = \mathbb{Q}$ und $h = \Phi_p$ das $p-$te Kreisteilungspolynom ($n = p - 1$). Dann ist $N = \mathbb{Q}(\theta)$ der $p-$te Kreisteilungskörper. Da $X - 1 \bmod p$ ein mehrfacher Teiler von $h \bmod p$ ist, betrachten wir das Newton-Polygon von h bzgl. p und $\tilde{g} = X - 1$. Das Polynom $h(X+1)$ ist in der Tat ein Eisenstein-Polynom bzgl. p. Das Newton-Polygon besteht also aus einer Seite der Länge $E = p-1$ mit Steigung $m = \frac{1}{p-1}$. Wegen $\mathrm{ggT}(p, p-1) = 1$ liefert der Hauptsatz $\mathbb{Q}_p(\theta) = \mathbb{Q}_p(\sqrt[p-1]{-p})$. Da $\mathbb{Q}_p$ die $(p-1)$-ten Einheitswurzeln enthält, ist dies unabhängig von der Wahl der Wurzeln (vgl. Hasse [8], p.222, für einen anderen Zugang).

Wir geben noch ein Beispiel zur Illustration des Hauptsatzes, das später in Kapitel 3 noch eingehender studiert werden wird. Sei $K = \mathbb{Q}$, $n = p$ eine ungerade Primzahl und $h = X^p + aX + a$ mit einer durch p, aber nicht durch p^2 teilbaren ganzen Zahl a. Dies ist ein Eisenstein-Polynom bzgl. p, das von Komatsu [12], [13], Movahhedi [18] und vielen anderen Autoren untersucht worden ist. Bis heute ist offen, ob die Galoisgruppe von h immer die volle symmetrische Gruppe ist. Wie üblich sei $\theta \in W_h$, $N = \mathbb{Q}(\theta)$ und L der Zerfällungskörper von h. Aufgrund des Hauptsatzes ist $|T_{\mathfrak{P}}|$ durch p teilbar ($\mathfrak{P}$ ein Primideal von L über $\mathfrak{p}$). Es verzweigt p total und wild in N. Ist $\wp$ das Primideal von N über p, so ist θ ein Primelement in $N_\wp = \mathbb{Q}_p(\theta)$. Wir studieren das Newton-Polygon von $h_0(X) = h(X)/(X - \theta)$ bzgl. $\wp$ und bzgl. $\tilde{g} = X - \theta$, weil $\theta \bmod \wp$ eine Wurzel von $h_0 \bmod \wp$ ist. Dazu entwickeln wir $h_0(X + \theta)$ nach dem Satz von Taylor in ein Polynom in X und berechnen dann das übliche Newton-Polygon. Dies besteht aus einer Seite S der

Länge $E = p-1$ mit Steigung $m = \frac{p}{p-1}$. Es ist also $e = p-1$ $(d = 1)$, h_S linear, und der zugeordnete Faktor $(h_0)_m = X^{p-1} + a(1 + \frac{\theta^{p-1}}{a/p})$. Anwendung des Hauptsatzes liefert

$$N_\wp(\theta_0) = N_\wp(\sqrt[p-1]{-a})$$

für jede Wurzel θ_0 von h_0, denn $1 + \frac{\theta^{p-1}}{a/p}$ ist eine 1-Einheit in $N_\wp$ und daher eine $(p-1)$-te Potenz. Wir sehen, dass $T_\mathfrak{P}$ mindestens die Ordnung $p(p-1)$ hat. Da Galoisgruppen lokaler Körper stets auflösbar sind, muss diese Gruppe nach einem bekannten Satz von Galois die volle affine Gruppe $\mathrm{AGL}_1(p)$ der Ordnung $p(p-1)$ sein. Mit anderen Worten: $G_\mathfrak{P} = T_\mathfrak{P}$ ist isomorph zu $\mathrm{AGL}_1(p)$ (als Permutationsgruppe auf W_h). Die genauere Untersuchung dieses Polynoms liefert folgenden

Satz. *Die Galoisgruppe des Eisenstein-Polynoms $h = X^p + aX + a$ bzgl. der Primzahl p ist die volle symmetrische Gruppe, falls eine der folgenden Aussagen gilt ($a = pb$, $p \nmid b$):*

(i) $D_0 = p^{p-1} + b(p-1)^{p-1}$ *ist kein (positives ganzrationales) Quadrat.*

(ii) Es gibt einen Primteiler q von D_0 mit $q \not\equiv \pm 1$ mod p.

(iii) Die ganze Zahl b ist ein Quadrat oder eine p-te Potenz in $\mathbb{Q}$; b ist ungerade, $b \not\equiv 1$ mod p oder $b \leq p$.

(iv) Alle Primteiler q von b, die in $N = \mathbb{Q}(\theta)$ verzweigen ($\mathrm{ggT}(p, v_q(b)) = 1$) sind kongruent 1 mod p^2.

(v) $a \equiv 2$ mod 3 oder $a \equiv 1$ mod 3 und $p \equiv 2$ mod 3.

Wir werden im Anhang berechnen, dass die Galoisgruppe dieses Polynoms für alle $a < 10^9$ stets die volle symmetrische Gruppe ist.

An dieser Stelle möchte ich mich ganz herzlich bei Herrn Prof. Dr. P. Schmid für seine wertvollen Anregungen zur vorliegenden Arbeit und seine freundliche Betreuung bedanken. Die hervorragenden Arbeitsbedingungen waren mir eine große Hilfe. Desweiteren gilt mein besonderer Dank Herrn PD Dr. U. Riese für seine unermüdliche Diskussionsbereitschaft.
Als Doktorand wurde ich finanziell von der Landesgraduiertenförderung und der Konrad-Adenauer-Stiftung unterstützt; hierfür bedanke ich mich sehr herzlich.

Notationen

Stets sei K ein algebraischer Zahlkörper und $\mathbb{F}_p$ ein endlicher Körper mit p Elementen.

$W_h = \{\theta_i\}_{i=1}^n$	Wurzelmenge des Polynoms h
$N = K(\theta)$	Wurzelkörper einer ausgezeichneten Wurzel θ von h
L	Zerfällungskörper von h
R_K	Ring der ganzen Zahlen von K
$\mathfrak{p}$	eine endliche Primstelle von K
$\wp$	eine endliche Primstelle von N
$\mathfrak{P}$	eine endliche Primstelle von L
$G = \mathrm{Gal}(L\|K) = \mathrm{Gal}_K(h)$	Galoisgruppe des Polynoms h
$K_\mathfrak{p} \subseteq L_\mathfrak{P}$	Komplettierungen von K und L bzgl. der nicht-archimedischen Bewertungen $\|\cdot\|_\mathfrak{p}$ bzw. $\|\cdot\|_\mathfrak{P}$
$R_\mathfrak{p}$	topologischer Abschluß von R_K in $K_\mathfrak{p}$
$k_\mathfrak{p} = R_K/\mathfrak{p} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$	globaler und lokaler Restklassenkörper
$e_\mathfrak{P}$	Verzweigungsindex $e(\mathfrak{P}\|\mathfrak{p})$ in der Erweiterung L über K
$e_\wp$	Verzweigungsindex $e(\wp\|\mathfrak{p})$ in der Erweiterung N über K
$f_\mathfrak{P}$	Trägheitsgrad $f(\mathfrak{P}\|\mathfrak{p})$ in der Erweiterung L über K
$f_\wp$	Trägheitsgrad $f(\wp\|\mathfrak{p})$ in der Erweiterung N über K
$G_\mathfrak{P} = \mathrm{Gal}(L_\mathfrak{P}\|K_\mathfrak{p})$	Zerlegungsgruppe von $\mathfrak{P}$
$T_\mathfrak{P}$	Trägheitsgruppe von $\mathfrak{P}$
$\mathcal{P}$	Menge aller Primideale in einer festen Körpererweiterung N über dem Primideal $\mathfrak{p}$ von K
$\mathcal{P}_m \subseteq \mathcal{P}$	Menge aller Primideale $\wp\|\mathfrak{p}$ von $\mathcal{P}$ mit $v_\wp(\theta) = e_\wp \cdot m$
D_h	Diskriminante von h
D_K	Diskriminante des Zahlkörpers K
$i(h)$	Index $[R_N : \mathbb{Z}[\theta]]$ für $h \in \mathbb{Z}[X]$, $\theta \in W_h$
ε_m	primitive m-te Einheitswurzel
Φ_p	p-tes Kreisteilungspolynom
$\left(\frac{a}{p}\right)$	Legendre-Symbol für eine Primzahl $p \neq 2$, $p \nmid a, a \in \mathbb{Z}$
$\mathrm{AGL}_1(p)$	Gruppe der affinen Abbildungen (affine Gruppe) $\{\psi : \mathbb{F}_p \to \mathbb{F}_p, x \mapsto ax + b \ : a, b \in \mathbb{F}_p, a \neq 0\}$

Kapitel 1

Globale und lokale Polynome

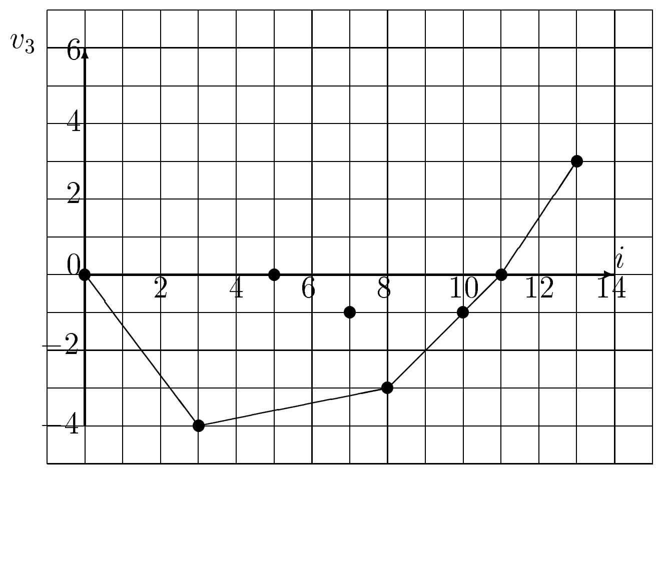
Wir schreiben für ein über K normiertes und separables Polynom

$$h(X) = \sum_{j=0}^{n} (-1)^j a_j X^{n-j} = X^n - a_1 X^{n-1} + - ... + (-1)^n a_n$$

und bezeichnen mit $W_h = \{\theta_i\}_{i=1}^n$ die Wurzelmenge von h im Zerfällungskörper L.

1.1 Definition. Ordne jedem Monom $\pm a_i X^{n-i} \neq 0$ von h den Punkt $(i, v_{\mathfrak{p}}(a_i))$ im euklidischen $\mathbb{R}^2$ zu. Die untere konvexe Hülle dieser Punkte heißt das *Newton-Polygon* von h bzgl. $(\mathfrak{p}, X)$. Es besteht aus geradlinigen Seiten S_{m_j} mit streng monoton wachsenden Steigungen $m_1 < m_2 < ... < m_t$.

1.2 Beispiel. Es sei $K = \mathbb{Q}$, $\mathfrak{p} = p = 3$ und $h(X) = X^{13} + \frac{5}{81}X^{10} + 25X^8 - \frac{20}{3}X^6 + \frac{10}{27}X^5 + \frac{5}{3}X^3 + 5X^2 + 135$. h ist ein Eisenstein-Polynom bzgl. 5 und daher irreduzibel über $\mathbb{Q}$. Das Newton-Polygon von h bzgl. $(3, X)$ hat die folgende Form.



1.1 Grundlagen

Wir bezeichnen mit S_{m_j} die Seiten des Newton-Polygons von h mit Steigungen m_j ($m_1 < m_2 < ... < m_t$). Ist $\mathfrak{p}$ eine endliche Primstelle des algebraischen Zahlkörpers K, d.h. ein Primideal des Rings der ganzen Zahlen R_K von K, so bezeichne $K_\mathfrak{p}$ die $\mathfrak{p}$-adische Komplettierung von K. Wir schreiben $\mathfrak{P}$ für ein Primideal von L über $\mathfrak{p}$ und $e_\mathfrak{P}$ bzw. $f_\mathfrak{P}$ für den Verzweigungsindex bzw. Trägheitsgrad von $\mathfrak{P}$ über $\mathfrak{p}$. Für $x \in K_\mathfrak{p}$ bezeichne $v_\mathfrak{p}(x)$ die $\mathfrak{p}$-adische Exponentialbewertung von x.

1.3 Satz *([21], II (6.3), (6.4)).*
Sei $m = m_j$ eine feste Steigung und $S_m : (r, v_\mathfrak{p}(a_r)) - (s, v_\mathfrak{p}(a_s))$ die dazugehörige Seite des Newton-Polygons von h, d.h. $r < s$ und

$$m = \frac{v_\mathfrak{p}(a_s) - v_\mathfrak{p}(a_r)}{s - r}.$$

(a) *h hat genau $s - r$ Wurzeln θ_{r+k} (in L) mit konstantem Wert $v_\mathfrak{P}(\theta_{r+k}) = e_\mathfrak{P} m, 1 \le k \le s - r$. Ferner gilt $(r + k, v_\mathfrak{p}(a_{r+k})) \in S_m$ genau dann, wenn $v_\mathfrak{p}(a_r^{-1} a_{r+k}) = km, \;\; 0 \le k \le s - r$.*

(b) *$h = \prod_{i=1}^t \hat{h}_{m_i}$ mit $\hat{h}_{m_i} = \prod_{v_\mathfrak{P}(\theta_j) = e_\mathfrak{P} m_i} (X - \theta_j)$ hat die Koeffizienten in $K_\mathfrak{p}$.*

Beweis. Es ist $v_\mathfrak{P}(xy) = v_\mathfrak{P}(x) v_\mathfrak{P}(y)$ für $x, y \in L_\mathfrak{P}^*$. Ferner gilt $v_\mathfrak{P}(x + y) \ge \min\{v_\mathfrak{P}(x), v_\mathfrak{P}(y)\}$, und wir erhalten das Gleichheitszeichen, falls $v_\mathfrak{P}(x) \ne v_\mathfrak{P}(y)$ ist (Ultrametrik). Es sind x, y nur dann $K_\mathfrak{p}-$konjugiert, wenn $v_\mathfrak{P}(x) = v_\mathfrak{P}(y)$. Für $x \in K_\mathfrak{p}$ gilt $v_\mathfrak{P}(x) = e_\mathfrak{P} v_\mathfrak{p}(x)$.

Wir ordnen die Wurzeln $\theta_1, ..., \theta_n$ von h in L total, mit der Maßgabe, dass $v_\mathfrak{P}(\theta_i) \le v_\mathfrak{P}(\theta_j)$ für $i < j$ ist. Nach Vieta sind die Koeffizienten von h elementarsymmetrische Polynome in den Wurzeln θ_j, und es gilt für $i = 1, ..., n$:

$$a_i = \sum_{1 \le k_1 < ... < k_i \le n} \theta_{k_1} \cdots \theta_{k_i}.$$

Folglich gilt $v_\mathfrak{P}(a_i) \ge v_\mathfrak{P}(\theta_1 \cdots \theta_i) = \sum_{k=1}^i v_\mathfrak{P}(\theta_k)$, und es gilt das Gleichheitszeichen im Falle $v_\mathfrak{P}(\theta_i) < v_\mathfrak{P}(\theta_{i+1})$. Sind also $\theta_{r+1}, ..., \theta_s$ die sämtlichen Wurzeln von h mit konstantem ganzzahligem Wert $v_\mathfrak{P}(\theta_s) = e_\mathfrak{P} \tilde{m}$ (etwa), so gilt $v_\mathfrak{P}(a_k) - v_\mathfrak{P}(a_r) \ge (k - r) v_\mathfrak{P}(\theta_s)$ für $r \le k \le s$, und wir erhalten das Gleichheitszeichen für $k = s$. Wegen $v_\mathfrak{P}(\theta_t) > v_\mathfrak{P}(\theta_s)$ für $t > s$ haben wir eine Seite des Newton-Polygons mit Steigung

$$m = \frac{v_\mathfrak{p}(a_s) - v_\mathfrak{p}(a_r)}{s - r} = \frac{1}{e_\mathfrak{P}} \cdot \frac{v_\mathfrak{P}(a_s) - v_\mathfrak{P}(a_r)}{s - r} = \frac{v_\mathfrak{P}(\theta_s)}{e_\mathfrak{P}},$$

d.h. $\tilde{m} = m$.

(a) Es ist $v_{\mathfrak{P}}(a_i) = v_{\mathfrak{P}}(\theta_1 \cdots \theta_i)$ für $i = r$ und $i = s$. Für $r \leq k \leq s$ gilt daher $(k, v_{\mathfrak{p}}(a_k)) \in S_m$ (sonst oberhalb) genau dann, wenn die behauptete Gleichung gilt.
(b) Es ist $\hat{h}_{m_i} \in K_{\mathfrak{p}}[X]$, denn nur solche Wurzeln θ_j von h sind konjugiert über $K_{\mathfrak{p}}$, für die $v_{\mathfrak{P}}(\theta_j)$ konstant ist. $\square$

Im Folgenden setzen wir h als irreduzibel über K voraus. Die Galoisgruppe $G{:=}\mathrm{Gal}(L|K)$ wirkt transitiv auf den Wurzeln W_h von h. Sei $N = K(\theta)$ für eine Wurzel θ von h und

$$\mathfrak{p}R_N = \wp_1^{e_{\wp_1}} \cdots \wp_r^{e_{\wp_r}}$$

die Zerlegung von $\mathfrak{p}$ in N. Wir bezeichnen mit $\mathcal{P} = \{\wp_1, ..., \wp_r\}$ die Menge der verschiedenen Primideale von N über $\mathfrak{p}$ ($\sum_{\wp_i \in \mathcal{P}} e_{\wp_i} f_{\wp_i} = n$).

1.4 Satz *(van der Waerden [34], Satz 1) .*
Sei h irreduzibel über K. Dann zerfällt die Wurzelmenge W_h unter $G_{\mathfrak{P}}$ in $r = |\mathcal{P}|$ Bahnen $W_{\wp_i}$ der Länge $e_{\wp_i} f_{\wp_i}$. Jede Bahn $W_{\wp_i}$ zerfällt unter der Trägheitsgruppe $T_{\mathfrak{P}}$ in $f_{\wp_i}$ Bahnen der Länge $e_{\wp_i}$.

Beweis. Da h irreduzibel über K ist, wirkt G transitiv auf $W = W_h$. Es ist $G_\theta = \mathrm{Gal}(L|K(\theta)) = \{\sigma \in G | \theta^\sigma = \theta\}$ und $G = \bigcup_{\sigma \in G} G_\theta \sigma$.

$$\begin{array}{lll} L & \mathfrak{P} \\ | & \\ K(\theta) & \wp \\ | & \\ K & \mathfrak{p} \end{array} \qquad \begin{array}{ll} G & [G_{\mathfrak{P}}] \\ | & \\ G_\theta & [(G_\theta)_{\mathfrak{P}}] \\ | & \\ \mathbf{1} & \end{array} \qquad \begin{array}{rl} & G \\ r & | \\ & G_{\mathfrak{P}} \\ f & | \\ & T_{\mathfrak{P}} \\ e & | \\ & \mathbf{1} \end{array}$$

Es ist $\mathfrak{P}^\sigma$, $\sigma \in G$, die Menge der Primideale von L über $\mathfrak{p}$ und es sei $\sigma_i \in G$ so gewählt, dass $\wp := \wp_1 = \mathfrak{P} \cap K(\theta)$ eines der Primideale $\mathfrak{P}^{\sigma_i^{-1}} \cap K(\theta) = \wp_i$ ist ($\sigma_1 = 1, \;\; i = 1, ..., r$). Die $G_{\mathfrak{P}}$- Bahnen von $W_{\wp_i}$ entsprechen als kleinste $G_{\mathfrak{P}}$-invariante Teilmengen von W, die $W_{\wp_i}$ enthalten, den verschiedenen (paarweise disjunkten) Doppelnebenklassen $G_\theta \sigma_i G_{\mathfrak{P}}$, d.h. $W_{\wp_i} = \{\theta^{\sigma_i \tau} | \tau \in G_{\mathfrak{P}}\}$. Es ist $G_\theta^{\sigma_i} = \{\tau \in G | \theta^{\sigma_i \tau} = \theta\}$, so dass für die Länge dieser Bahnen nach der Bahnengleichung

$$\left|W_{\wp_i}\right| = \left|G_{\mathfrak{P}} : \left(G_{\mathfrak{P}} \cap G_\theta^{\sigma_i}\right)\right| = \left|G_{\mathfrak{P}}^{\sigma_i^{-1}} : \left(G_{\mathfrak{P}}^{\sigma_i^{-1}} \cap G_\theta\right)\right| = \frac{|G_{\mathfrak{P}}|}{\left|(G_\theta)_{\mathfrak{P}^{\sigma_i^{-1}}}\right|}$$

gilt. Es ist $|G_{\mathfrak{P}}| = e_{\mathfrak{P}} f_{\mathfrak{P}}$ bzw. $\left|(G_\theta)_{\mathfrak{P}^{\sigma_i^{-1}}}\right| = e\big(\mathfrak{P}^{\sigma_i^{-1}} | \wp_i\big) f\left(\mathfrak{P}^{\sigma_i^{-1}} | \wp_i\right)$. Da $e_i' := e\big(\mathfrak{P}^{\sigma_i^{-1}} | \wp_i\big)$ ein Teiler von $e_{\mathfrak{P}}$ ist, also $e_{\mathfrak{P}} = e_i' e_{\wp_i}$ gilt und $f_i' := f\left(\mathfrak{P}^{\sigma_i^{-1}} | \wp_i\right)$ ein Teiler von $f_{\mathfrak{P}}$ ist, d.h. $f_{\mathfrak{P}} = f_i' f_{\wp_i}$ gilt, erhalten wir $|W_{\wp_i}| = e_{\wp_i} f_{\wp_i}$. Die Bahnenlängen der Trägheitsgruppen $T_{\mathfrak{P}}$

als Normalteiler von $G_{\mathfrak{P}}$ auf den Wurzeln $W_{\wp_i}$ sind alle gleich und es gilt daher

$$\left|T_{\mathfrak{P}} : \left(T_{\mathfrak{P}} \cap G_\theta^{\sigma_i}\right)\right| = \left|T_{\mathfrak{P}}^{\sigma_i^{-1}} : \left(T_{\mathfrak{P}}^{\sigma_i^{-1}} \cap G_\theta\right)\right| = \frac{e_{\mathfrak{P}}}{e_i^{'}} = e_{\wp_i}.$$

Die Behauptung folgt. □

Einen alternativen Beweis dieses Satzes von van der Waerden liefert Matzat [16], p.126. Wir werden vor allem die folgende aus dem Satz von van der Waerden zu folgernde Aussage benötigen.

1.5 Satz. *Sei h irreduzibel über K. h zerfällt über $K_{\mathfrak{p}}$ in ein Produkt von r paarweise verschiedenen normierten irreduziblen Polynomen $\hat{h}_{\wp_i}$ mit Graden* $\operatorname{grd}(\hat{h}_{\wp_i}) = e_{\wp_i} f_{\wp_i}$. *Wir sagen, $\wp_i$ gehöre zu $\hat{h}_{\wp_i}$ und schreiben dafür $h = \prod_{\wp_i \in \mathcal{P}} \hat{h}_{\wp_i}$.*
Zusatz: Wir können die Polynome $\hat{h}_{\wp_i}$ so anordnen, dass $\theta^{\sigma_i} \in W_{\hat{h}_{\wp_i}}$ genau dann gilt, wenn $\mathfrak{P}^{\sigma_i^{-1}} | \wp_i$ ist ($\sigma_i \in G$).

Beweis. Wir identifizieren $G_{\mathfrak{P}}$ mit der Galoisgruppe $\operatorname{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}})$, d.h. zwei Wurzeln von h sind genau dann $G_{\mathfrak{P}}-$konjugiert, wenn sie über $K_{\mathfrak{p}}$ konjugiert sind. Durch die Inklusionen $K(\theta) \hookrightarrow K(\theta)_{\wp_i}$ erhalten wir die Homomorphismen $K(\theta) \otimes_K K_{\mathfrak{p}} \to K(\theta)_{\wp_i}, a \otimes b \mapsto ab$, und damit einen kanonischen Isomorphismus $\varphi : K(\theta) \otimes_K K_{\mathfrak{p}} \to \prod_{i=1}^r K(\theta)_{\wp_i}$. Einem über $K_{\mathfrak{p}}$ irreduziblen Polynom $\hat{h}_{\wp_i}$ wird via $K_{\mathfrak{p}}[X]/(\hat{h}_{\wp_i}) \simeq K(\theta)_{\wp_i}$ genau ein $\wp_i$ zugeordnet. Wir erhalten folgendes kommutatives Diagramm von Isomorphismen.

$$\begin{array}{ccc}
K[X]/(h) \otimes_K K_{\mathfrak{p}} & \longrightarrow & \prod_{i=1}^r K_{\mathfrak{p}}[X]/(\hat{h}_{\wp_i}) \\
\Big\downarrow & & \Big\downarrow \\
K(\theta) \otimes_K K_{\mathfrak{p}} & \longrightarrow & \prod_{i=1}^r K(\theta)_{\wp_i}
\end{array}$$

Der Zusatz folgt direkt aus dem Beweis von Satz 1.4. □

Im Folgenden sei S_m eine feste Seite des Newton-Polygons mit den Eckpunkten $(r, v_{\mathfrak{p}}(a_r))$ und $(s, v_{\mathfrak{p}}(a_s))$, $r < s$. Wir schreiben $V := v_{\mathfrak{p}}(a_s) - v_{\mathfrak{p}}(a_r)$ und $E := s - r$, so dass $m = \frac{V}{E}$. Setzen wir $d = \operatorname{ggT}(E, V)$, so können wir $m = \frac{\nu}{e}$ schreiben, wobei $V = d\nu$ bzw. $E = de$ gilt ($\operatorname{ggT}(\nu, e){=}1$). Nach den Sätzen 1.3 und 1.5 gilt für die Faktorisierung von h über $K_{\mathfrak{p}}$

$$h = \prod_{j=1}^{t} \hat{h}_{m_j} = \prod_{\wp \in \mathcal{P}} \hat{h}_{\wp}.$$

Da die Faktoren der ersten Zerlegung nicht notwendig irreduzibel über $K_{\mathfrak{p}}$ sind, existiert eine Teilmenge $\mathcal{P}_m \subseteq \mathcal{P}$ mit $\hat{h}_m = \prod_{\wp \in \mathcal{P}_m} \hat{h}_{\wp}$. Wir bezeichnen $\mathcal{P}_m$ als die Menge aller Primideale von $\mathcal{P}$, die zur Seite S_m gehören.

1.6 Satz. *Ein Primideal $\wp \in \mathcal{P}$ gehört genau dann zu der Seite S_m, wenn $v_\wp(\theta) = e_\wp \cdot m$ ist.*

Beweis. Nach Satz 1.5 gehört $\wp$ genau dann zu S_m, wenn $\theta^\sigma \in W_{\hat{h}_\wp}$ für ein $\sigma \in G$ gilt, für welches $\mathfrak{P}^{\sigma^{-1}}$ über $\wp$ liegt. Wir erhalten

$$e\big(\mathfrak{P}^{\sigma^{-1}}|\wp\big)e(\wp|\mathfrak{p})m = e_\mathfrak{P}m = v_\mathfrak{P}\big(\theta^\sigma\big) = e\big(\mathfrak{P}^{\sigma^{-1}}|\wp\big)v_\wp(\theta)$$

für alle diese σ und es folgt $v_\wp(\theta) = e_\wp \cdot m$. □

1.7 Anwendung. Sei $K = \mathbb{Q}$ und $h \in \mathbb{Z}[X]$ ein irreduzibles normiertes Polynom von Primzahlgrad q. Ist p eine beliebige Primzahl, die genau einmal die Diskriminante D_h von h teilt, so ist die Galoisgruppe $G = \mathrm{Gal}_\mathbb{Q}(h)$ die volle symmetrische Gruppe S_q.

Beweis. Sei $\theta \in W_h$ und $N = \mathbb{Q}(\theta)$. Bezeichnen wir mit $i(h)$ den Index $[R_N : \mathbb{Z}[\theta]]$, dann gilt nach Voraussetzung und aufgrund der Beziehung $D_h = i(h)^2 D_N$, dass p genau einmal die Diskriminante D_N teilt. Für das Verzweigungsverhalten von N über $\mathbb{Q}$ gibt die Differente Aufschluss. Würde p wild verzweigen, so würde aufgrund von $v_p(D_N) = 1$ ein $e_{\wp_j}$ mit $e_{\wp_j} = 1$ existieren, was im Widerspruch zu $v_p(e_{\wp_j}) \geq 1$ steht. Also verzweigt p zahm in N und es gilt $\sum_{i=1}^r (e_{\wp_i} - 1) f_{\wp_i} = 1$ ([6], III §3, Theorem 26). Damit erhalten wir $f_{\wp_i} = 1$ für alle $i = 1, ..., r$, $e_{\wp_1} = 2$ (etwa) und $e_{\wp_i} = 1$ für alle übrigen i .
Wegen $f_{\wp_i} = 1$ für alle i ist $G_\mathfrak{P} = T_\mathfrak{P}$ und es wird $G_\mathfrak{P}$ nach Satz 1.4 durch eine Transposition auf W_h erzeugt ($pR_{\mathbb{Q}(\theta)} = \wp_1^2 \wp_2 \cdots \wp_r$). Als transitive Gruppe von Primzahlgrad ist G primitiv und daher die volle symmetrische Gruppe nach einem Satz von Jordan ([11], II Satz 1.3 und Satz 4.5 (b)). □

1.8 Korollar. *Ist h irreduzibel über $K_\mathfrak{p}$, so besteht das zugehörige Newton-Polygon bzgl. $(\mathfrak{p}, X)$ aus nur einer Strecke. Besteht umgekehrt das Newton-Polygon von h aus nur einer Strecke, dann müssen die Primfaktoren von h über $K_\mathfrak{p}$ den Grad ke, $1 \leq k \leq d$, besitzen.*

Beweis. Ersteres folgt direkt aus Satz 1.3. Wegen $h = \hat{h}_m = \hat{f}_m \hat{g}_m$ über $K_\mathfrak{p}$ müssen die Newton-Polygone bzgl. $(\mathfrak{p}, X)$ von $\hat{f}_m$ und $\hat{g}_m$ die gleiche Steigung haben wie das Newton-Polygon von $\hat{h}_m$. Sind b_n und c_n die konstanten Glieder von $\hat{f}_m$ und $\hat{g}_m$, so gilt aufgrund des Koeffizientenvergleichs

$$v_\mathfrak{p}(b_n) + v_\mathfrak{p}(c_n) = v_\mathfrak{p}(b_n c_n) = v_\mathfrak{p}(a_n).$$

Wegen $v_\mathfrak{p}(b_n), v_\mathfrak{p}(c_n) \in \mathbb{Z}$ müssen $\hat{f}_m$ und $\hat{g}_m$ eigene Eckpunkte besitzen, die auf S_m liegen. Die Behauptung folgt. □

1.2 Faktoren und zugeordnete Polynome

In diesem Abschnitt studieren wir die feste Seite S_m des Newton-Polygons genauer. Es seien wieder $(r, v_\mathfrak{p}(a_r))$ und $(s, v_\mathfrak{p}(a_s))$ die beiden Eckpunkte der Seite S_m mit $s - r = E$ und $v_\mathfrak{p}(a_r^{-1}a_s) = V$. Gilt etwa $m = \frac{v_\mathfrak{p}(a_s)-v_\mathfrak{p}(a_r)}{s-r} < 0$, so betrachten wir anstelle von $h(X)$ das Polynom

$$\begin{aligned}\frac{X^n}{(-1)^n a_n}h(X^{-1}) &= X^n - \frac{a_{n-1}}{a_n}X^{n-1} + -\ldots + (-1)^{n-1}\frac{a_1}{a_n}X + (-1)^n\frac{1}{a_n} \\ &=: \sum_{j=0}^{n}(-1)^j\tilde{a}_j X^{n-j}\end{aligned}$$

mit $\tilde{a}_j = \frac{a_{n-j}}{a_n}$. Setzen wir $n - s := \tilde{r}$ $(n - r = \tilde{r} + s - r)$, dann gilt

$$0 > \frac{v_\mathfrak{p}(a_s) - v_\mathfrak{p}(a_r)}{s-r} = \frac{v_\mathfrak{p}(\tilde{a}_{n-s}) - v_\mathfrak{p}(\tilde{a}_{n-r})}{s-r} = -\frac{v_\mathfrak{p}(\tilde{a}_{\tilde{r}+s-r}) - v_\mathfrak{p}(\tilde{a}_{\tilde{r}})}{s-r}.$$

Für die S_m entsprechende Seite dieses Polynoms mit gleicher Länge E und Steigung $\tilde{m}$ gilt also $\tilde{m} = -m > 0$.

Wir können also im Folgenden annehmen, dass $m \geq 0$ ist. Ferner gilt $\hat{h}_m = \prod_{i=r+1}^{s}(X - \theta_i)$ und nach Satz 1.3 erhalten wir für die Bewertungen der Wurzeln $v_\mathfrak{P}(\theta_i) = e_\mathfrak{P} \cdot m \geq 0$ für alle $i \in \{r+1, ..., s\}$. Die Koeffizienten von $\hat{h}_m$ sind elementarsymmetrische Polynome in den Wurzeln θ_i von h und damit Elemente des Rings der ganzen Zahlen von $K_\mathfrak{p}$. Wir können folglich annehmen, dass $\hat{h}_m \in R_\mathfrak{p}[X]$ ist.

Im allgemeinen ist $h \neq \hat{h}_m$, insbesondere $\hat{h}_m \notin K[X]$. Dennoch kann man das *lokale* Polynom $\hat{h}_m$ durch ein *globales* Polynom über K beschreiben, das aus der Form des Newton-Polygons erhalten werden kann. Die Grundidee geht dabei auf Ore [22] zurück.

1.9 Definition. Das Polynom

$$h_m = a_r^{-1} \sum_{\substack{k=0 \\ v_\mathfrak{p}(a_r^{-1}a_{r+k})=km}}^{E} (-1)^k a_{r+k} X^{E-k} \in K[X]$$

heißt der *Faktor* von h bzgl. S_m.

Bemerkung. Nach Satz 1.3 ist $v_\mathfrak{p}(a_r^{-1}a_{r+k}) \geq km$ für $k \geq 0$ und es gilt $v_\mathfrak{p}(a_r^{-1}a_{r+k}) = km$ genau dann, wenn $(r + k, v_\mathfrak{p}(a_{r+k})) \in S_m$. Der Faktor ist also ein normiertes Polynom, dessen Koeffizienten ausschließlich Punkte des Newton-Polygons von h berücksichtigt, die auf der Seite S_m liegen. h_m und $\hat{h}_m$ haben dasselbe Newton-Polygon bzgl. $(\mathfrak{p}, X)$ und es ist $h_m \in K[X]$, aber wegen $m \geq 0$ (vgl. obige Vorbemerkung) auch $h_m \in R_\mathfrak{p}[X]$.

Welche Koeffizienten von h spielen folglich bei der Betrachtung des Faktors eine Rolle? Da die Bewertungen $v_\mathfrak{p}(a_r^{-1}a_{r+k}) = km = \frac{k}{e}\cdot\nu$ ganze Zahlen sind, kommen nur Vielfache $k = je$ von e in Frage, für die $v_\mathfrak{p}(a_r^{-1}a_{r+k}) = j\nu$ gilt.

1.10 Definition. Es sei $\pi \in K$ ein Element der Ordnung 1 bzgl. $\mathfrak{p}$, d.h. $v_\mathfrak{p}(\pi) = 1$. Das Polynom

$$h_S = a_r^{-1} \sum_{\substack{j=0 \\ v_\mathfrak{p}(a_r^{-1}a_{r+je})=j\nu}}^{d} (-1)^{je} a_{r+je}\pi^{-j\nu}X^{d-j}$$

heißt das *der Seite S_m und h_m zugeordnete Polynom.*

Bemerkung. h_S ist ein normiertes Polynom mit $\mathfrak{p}$-Einheiten als Koeffizienten. Es gilt

$$\begin{aligned} h_S(\pi^{-\nu}X^e) &= a_r^{-1} \sum_{\substack{j=0 \\ v_\mathfrak{p}(a_r^{-1}a_{r+je})=j\nu}}^{d} (-1)^{je} a_{r+je}\pi^{-j\nu}\pi^{-\nu(d-j)}X^{e(d-j)} \\ &= a_r^{-1} \sum_{\substack{k=0 \\ v_\mathfrak{p}(a_r^{-1}a_{r+k})=\frac{k}{e}\nu}}^{ed} (-1)^{k} a_{r+k}\pi^{-\nu d}X^{E-k} = \pi^{-\nu d}h_m(X), \end{aligned}$$

so dass h_m aus h_S durch die Substitution $X \mapsto \pi^{-\nu}X^e$ und anschließender Multiplikation mit $\pi^{\nu d}$ entsteht.

Schreiben wir $\hat{h}_m(X) = \prod_{i=1}^{E}(X-\theta_i) =: \sum_{k=0}^{E}(-1)^k c_k X^{E-k} \in R_\mathfrak{p}[X]$, so können wir mittels derselben Vorgehensweise ein der Seite S_m und $\hat{h}_m$ zugeordnetes Polynom $\hat{h}_S$ definieren. Für dieses gilt dann nach Ignorieren aller nicht auf S_m liegenden Punkte und entsprechendem Kürzen der Koeffizienten zu $\mathfrak{p}$-Einheiten $\hat{h}_S(X) = \sum^{d}_{\substack{j=0 \\ v_\mathfrak{p}(c_{je})=j\nu}} (-1)^{je}\pi^{-j\nu}c_{je}X^{d-j}$. Wir erhalten also ausgehend von unserem Polynom h die folgende Situation.

$$\begin{tikzcd}[column sep=small]
 & h \in K[X] \arrow[dl] \arrow[dr] & \\
\text{Konstruktion} & & \text{Zerlegung über } K_\mathfrak{p} \\
K[X] \ni h_m \in R_\mathfrak{p}[X] \arrow[d, leftrightarrow] & \text{Fundamentallemma 1.11} & K[X] \not\ni \hat{h}_m \in R_\mathfrak{p}[X] \arrow[d, leftrightarrow] \\
h_S \arrow[rr, leftrightarrow] & & \hat{h}_S
\end{tikzcd}$$

Welcher Zusammenhang besteht zwischen dem *globalen* Faktor der linken und dem *lokalen* Polynom der rechten Seite des Diagramms? Eine Antwort liefert das folgende

1.11 Fundamentallemma. *h_m und $\hat{h}_m$ haben die gleichen Reduktionen mod $\mathfrak{p}$, insbesondere gilt*

$$h_S \bmod \mathfrak{p} = \hat{h}_S \bmod \mathfrak{p}.$$

Beweis. Wir zeigen, dass

$$v_{\mathfrak{p}}((a_r^{-1}a_{r+k} - c_k) \geq km + 1 \quad \text{für alle } k$$

gilt. Damit gilt insbesondere $\pi^{-km}c_k \equiv \pi^{-km}\frac{a_{r+k}}{a_r} \bmod \mathfrak{p}$ für alle k und die Behauptung des Fundamentallemmas 1.11 folgt. Wir können voraussetzen, dass $de = s - r < n$ ist, sonst folgt $s = n$, $r = 0$, also $c_k = a_k$ und es gilt $h = \hat{h}_m$ sowie $h_S \equiv \hat{h}_S \bmod \mathfrak{p}$ und die Behauptung ist offensichtlich. Nach Satz 1.3 gilt $v_{\mathfrak{p}}(c_k) \geq km$ bzw. $v_{\mathfrak{p}}(a_r^{-1}a_{r+k}) \geq km$ und wir erhalten das Gleichheitszeichen für $k = je,\ \ 0 \leq j \leq d$. Ordnen wir die Wurzeln von h wie im Beweis von Satz 1.3, dann gilt $v_{\mathfrak{P}}(\theta_i) < e_{\mathfrak{P}}m$ für $i \leq r$ und $v_{\mathfrak{P}}(\theta_i) > e_{\mathfrak{P}}m$ für $i > s$. Nach dem Hauptsatz über elementarsymmetrische Polynome gilt

$$c_k = \sum_{1\leq l_1<\ldots<l_k\leq s-r} \theta_{r+l_1}\cdots\theta_{r+l_k}.$$

Für $k = 1, ..., s-r$ betrachten wir $\rho_k := a_{r+k} - a_r c_k$.

1.Fall: $r = 0$. Es ist $a_0 = 1$ bzw. $v_{\mathfrak{P}}(a_0) = 0$.

Ferner ist

$$\begin{aligned}
\rho_k &= a_k - c_k = \sum_{1\leq j_1<\ldots<j_k\leq n} \theta_{j_1}\cdots\theta_{j_k} - \sum_{1\leq l_1<\ldots<l_r\leq s} \theta_{l_1}\cdots\theta_{l_k} \\
&= \sum_{\substack{1\leq i_1<\ldots<i_k\leq n \\ \text{mindestens ein } i_j>s}} \theta_{i_1}\cdots\theta_{i_k}
\end{aligned}$$

($i_j > s$ existiert, da nach Voraussetzung $s < n$). Dann ist also wegen der Anordnung der Wurzeln

$$\begin{aligned}
v_{\mathfrak{P}}(\rho_k) &\geq v_{\mathfrak{P}}(\theta_1\cdots\theta_{k-1}\theta_{s+1}) \\
&= v_{\mathfrak{P}}(\theta_1\cdots\theta_{k-1}) + v_{\mathfrak{P}}(\theta_{s+1}) + v_{\mathfrak{P}}(a_0)
\end{aligned}$$

und damit

$$\begin{aligned}
v_{\mathfrak{P}}(a_r^{-1}a_{r+k} - c_k) &= v_{\mathfrak{P}}(\rho_k) \\
&\geq (k-1)e_{\mathfrak{P}}m + (e_{\mathfrak{P}}m + 1) = ke_{\mathfrak{P}}m + 1.
\end{aligned}$$

Da $v_{\mathfrak{p}}(\rho_k)$ ganzzahlig ist, folgt die Behauptung.

2.Fall: $r \geq 1$.

Dann ist

$$\begin{aligned}
\rho_k &= a_{r+k} - a_r c_k \\
&= \sum_{1\leq j_1<\ldots<j_{r+k}\leq n} \theta_{j_1}\cdots\theta_{j_{r+k}} - \sum_{1\leq i_1<\ldots<i_r\leq n} \theta_{i_1}\cdots\theta_{i_r} \sum_{1\leq l_1<\ldots<l_k\leq s-r} \theta_{r+l_1}\cdots\theta_{r+l_k} \\
&= \sum_{1\leq j_1<\ldots<j_{r+k}\leq n} \theta_{j_1}\cdots\theta_{j_{r+k}} - \ ((\theta_1\cdots\theta_r) \sum_{1\leq l_1<\ldots<l_k\leq s-r} \theta_{r+l_1}\cdots\theta_{r+l_k} + \ z),
\end{aligned}$$

wobei offenbar

$$z = \sum_{1 \le i_1 < \ldots < i_r \le n} \theta_{i_1} \cdots \theta_{i_r} \sum_{1 \le l_1 < \ldots < l_k \le s-r} \theta_{r+l_1} \cdots \theta_{r+l_k} - (\theta_1 \cdots \theta_r) \sum_{1 \le l_1 < \ldots < l_k \le s-r} \theta_{r+l_1} \cdots \theta_{r+l_k}$$

gilt. Der Term $(\theta_1 \cdots \theta_r) \sum_{1 \le l_1 < \ldots < l_k \le s-r} \theta_{r+l_1} \cdots \theta_{r+l_k}$ verschwindet in der Differenz $a_{r+k} - a_r c_k$ und wir erhalten

$$\rho_k = a_{r+k} - a_r c_k = \sum_{\substack{\{1,\cdots,r\} \not\subseteq \{i_1,\cdots,i_{r+k}\} \text{ oder} \\ \{1,\cdots,r,s+i_1,\cdots,s+i_k\} \subseteq \{i_1,\cdots,i_{r+k}\}}} \theta_{i_1} \cdots \theta_{i_{r+k}},$$

wobei gewisse $i_j = i_l$ für $j \neq l$ auftreten können. Zwei Fälle müssen folglich betrachtet werden.

(a) Es sind höchstens $r-1$ Indizes $\le r$ und daher mindestens $k+1$ viele Indizes $\ge r+1$. Dann ist wegen $v_{\mathfrak{P}}(\theta_{r+1}) \ge v_{\mathfrak{P}}(\theta_r) + 1$

$$\begin{aligned} v_{\mathfrak{P}}(a_{r+k} - a_r c_k) &\ge v_{\mathfrak{P}}(\theta_1 \cdots \theta_{r-1} \theta_{r+1}^{k+1}) \ge v_{\mathfrak{P}}(\theta_1 \cdots \theta_r) + 1 + k \cdot v_{\mathfrak{P}}(\theta_{r+1}) \\ &= v_{\mathfrak{P}}(a_r) + 1 + k e_{\mathfrak{P}} m. \end{aligned}$$

Die Behauptung folgt aufgrund der Ganzzahligkeit von $v_{\mathfrak{p}}(\rho_k)$.

(b) r Indizes sind $\le r$ und k Indizes sind $\ge s+1$. In diesem Fall gilt wegen $v_{\mathfrak{P}}(\theta_{s+1}) \ge v_{\mathfrak{P}}(\theta_s) + 1$

$$\begin{aligned} v_{\mathfrak{P}}(a_{r+k} - a_r c_k) &\ge v_{\mathfrak{P}}(\theta_1 \cdots \theta_r \theta_{s+1}^k) = v_{\mathfrak{P}}(\theta_1 \cdots \theta_r) + k \cdot v_{\mathfrak{P}}(\theta_{s+1}) \\ &\ge v_{\mathfrak{P}}(a_r) + k(e_{\mathfrak{P}} m + 1) \end{aligned}$$

und die Behauptung folgt wie im ersten Fall. □

1.12 Beispiel. Sei $h(X) = \sum_{j=0}^n (-1)^j a_j X^{n-j} = X^n - a_1 X^{n-1} + -\ldots + (-1)^n a_n$ ein Eisenstein-Polynom bzgl. $\mathfrak{p}$. Dann ist $\hat{h}_m = h$, $h_m = X^n + (-1)^n a_n$ und $\hat{h}_S \bmod \mathfrak{p} = h_S \bmod \mathfrak{p} = X + (-1)^n \pi^{-1} a_n \bmod \mathfrak{p}$.

1.13 Satz. *Sei $\wp$ ein Primideal von $N = K(\theta)$, welches zur Seite S_m gehört, d.h. $\wp \in \mathcal{P}_m$. Dann ist $\bar{\theta} = \theta + \wp$ eine Wurzel von $\bar{h}_S = h_S \bmod \mathfrak{p}$ im Restklassenkörper $k_{\wp}$.*

Beweis. Aus der Konvexität des Newton-Polygons (nach unten) folgt offenbar

$$v_{\mathfrak{p}}(a_r^{-1} a_k) \ge (k-r) \cdot m$$

für alle $k = 1, \ldots, n$. Wir spalten das Polynom in zwei Bestandteile auf, wobei der erste alle Punkte auf dem Polygon und der zweite diejenigen Punkte, die oberhalb des Polygons liegen, berücksichtigt:

$$0 = h(\theta) = \sum_{v_{\mathfrak{p}}(a_r^{-1} a_k) = (k-r)m} (-1)^k a_k \theta^{n-k} + \sum_{v_{\mathfrak{p}}(a_r^{-1} a_k) > (k-r)m} (-1)^k a_k \theta^{n-k}.$$

Für den zweiten Summanden gilt mit Satz 1.6 sicherlich

$$\begin{aligned} v_\wp\left(\sum_{v_\wp(a_r^{-1}a_k)>e_\wp(k-r)m} (-1)^k a_k \theta^{n-k}\right) &> e_\wp(k-r)m + v_\wp(a_r) + (n-k)e_\wp m \\ &= (n-r)e_\wp m + 1 + v_\wp(a_r) \geq (s-r)e_\wp m + 1 + v_\wp(a_r) \\ &= e_\wp d\nu + 1 + v_\wp(a_r). \end{aligned}$$

Für den ersten Summanden kommt nur $k \in \{r+1, ..., s\}$ in Frage. Es folgt also

$$\begin{aligned} \infty &= v_\wp(h(\theta)) = v_\wp\left(h_m(\theta) + \sum_{v_\wp(a_r^{-1}a_k)>e_\wp(k-r)m} (-1)^k a_k \theta^{n-k}\right) \\ &\geq \min\left\{v_\wp(h_m(\theta)), v_\wp\left(\sum_{v_\wp(a_r^{-1}a_k)>e_\wp(k-r)m} (-1)^k a_k \theta^{n-k}\right)\right\}. \end{aligned}$$

Für die $\wp$-adische Exponentialbewertung von $h_m(\theta)$ folgt also

$$v_\wp(h_m(\theta)) \geq e_\wp d\nu + 1.$$

Dann gilt aber ($\tilde{k} = k - r \in \{1, ..., s-r\}$)

$$v_\wp\left(a_r^{-1} \sum_{\substack{\tilde{k}=0 \\ v_\mathfrak{p}(a_r^{-1}a_{r+\tilde{k}})=\tilde{k}m}}^{E} (-1)^{\tilde{k}} a_{r+\tilde{k}} \theta^{E-\tilde{k}}\right) + v_\wp(\pi^{-d\nu}) \geq 1$$

und es folgt ($\tilde{k} = je$)

$$v_\wp\left(a_r^{-1} \sum_{\substack{j=0 \\ v_\mathfrak{p}(a_r^{-1}a_{r+je})=j\nu}}^{d} (-1)^{je} \pi^{-j\nu} a_{r+je} \theta^{(d-j)e}\right) \geq 1.$$

Wegen $e \in \mathbb{N}$ gilt

$$v_\wp\left(a_r^{-1} \sum_{\substack{j=0 \\ v_\mathfrak{p}(a_r^{-1}a_{r+je})=j\nu}}^{d} (-1)^{je} \pi^{-j\nu} a_{r+je} \theta^{d-j}\right) \geq 1$$

und damit $v_\wp(h_S(\theta)) > 0$. Die Behauptung folgt. □

1.3 Regularität

Wir werden nun unter bestimmten Voraussetzungen den Zusammenhang zwischen Verzweigungsindizes bzw. Trägheitsgraden des Primideals $\mathfrak{p}$ in N und den lokalen und globalen Faktoren des Polynoms h aufzeigen.

Wir nehmen im Folgenden an, $\bar{h}_S = h_S \bmod \mathfrak{p}$ habe die Faktorisierung

$$\bar{h}_S = \bar{g}_1^{e_1} \cdots \bar{g}_t^{e_t} \tag{1.1}$$

über $k_\mathfrak{p}$, d.h. die Polynome $\bar{g}_i \in k_\mathfrak{p}[X]$ sind normiert, irreduzibel und paarweise verschieden. Nach dem Henselschen Lemma ([21], II 4.6) garantiert dies eine entsprechende Faktorisierung von

$$h_S = g_1 \cdots g_t$$

in normierte, paarweise teilerfremde Faktoren $g_i \in R_\mathfrak{p}[X]$ mit $g_i \equiv \bar{g}_i^{e_i} \bmod \mathfrak{p}$. Wir halten zunächst folgende Resultate fest.

1.14 Satz. *Mit den oben eingeführten Bezeichnungen gilt*

$$h_m = h_1 \cdots h_t, \tag{1.2}$$

wobei $h_i \in R_\mathfrak{p}[X]$ normierte, paarweise teilerfremde Polynome vom Grad $e{\cdot}\mathrm{grd}(g_i)$ sind. Das Newton-Polygon von h_i besteht aus einer Seite S_i mit Steigung m und zugeordnetem Polynom g_i $(1 \le i \le t)$.

Beweis. Nach Definition entsteht h_m aus h_S durch die Substitution $X \mapsto \pi^{-\nu} X^e$ und anschließender Multiplikation mit $\pi^{\nu\cdot\mathrm{grd}(h_S)}$. Aufgrund des Chinesischen Restesatzes gilt $K_\mathfrak{p}[X]/(h_S) \simeq \prod_{i=1}^t K_\mathfrak{p}[X]/(g_i)$. Die Polynome h_i entstehen also aus den Polynomen g_i durch die Substitution $X \mapsto \pi^{-\nu} X^e$ und anschließender Multiplikation mit $\pi^{\nu\cdot\mathrm{grd}(g_i)}$. Die Behauptung folgt. □

1.15 Satz. *Wie üblich sei $\hat{h}_m = \prod_{\wp \in \mathcal{P}_m} \hat{h}_\wp$ die Primfaktorzerlegung von $\hat{h}_m$ über $K_\mathfrak{p}$. Das Newton-Polygon von $\hat{h}_\wp$ besteht aus einer Seite $S_\wp$ mit Steigung m und Länge $\mathrm{grd}\big(\hat{h}_\wp\big) = e_\wp f_\wp$.*

Beweis. Die Behauptung folgt aus Satz 1.5. □

Um die Korrespondenz der Primfaktorzerlegung von h_m und $\hat{h}_m$ zu erreichen und Fundamentallemma 1.11 anwenden zu können, benötigen wir die Zerlegung von h_S in *irreduzible* Faktoren g_i. Dies führt zu folgender Definition.

1.16 Definition. Die Seite S_m des Newton-Polygons heißt *regulär*, falls $\mathfrak{p}$ nicht die Diskriminante von h_S teilt. Es ist dann also $h_S \bmod \mathfrak{p}$ separabel.

Bemerkung. Aus den Eigenschaften der Diskriminante folgt die Unabhängigkeit der Regularität von der Auswahl des Primelements π.

Ist also S_m regulär, dann gilt in der Faktorisierung (1.1) $e_i = 1$ für alle $i = 1, ..., t$. Nach dem Henselschen Lemma sind dann die Faktoren $g_i \in R_\mathfrak{p}[X]$ von h_S irreduzibel mit $\mathrm{grd}(\bar{g}_i) = \mathrm{grd}(g_i)$.

1.17 Satz. *Sei S_m regulär. Dann haben wir über $K_\mathfrak{p}$ die korrespondierenden Faktorisierungen*

$$h_m = \prod_{i=1}^{t} h_i \quad \text{und} \quad \hat{h}_m = \prod_{i=1}^{t} \hat{h}_{\wp_i}$$

in irreduzible, normierte Polynome $h_i, \hat{h}_{\wp_i} \in R_\mathfrak{p}[X]$. Ferner gilt:

(i) $\mathrm{grd}(h_i) = \mathrm{grd}(\hat{h}_{\wp_i}) = e_{\wp_i} f_{\wp_i}$

(ii) $e_{\wp_i} = e$ *für alle* $\wp_i \in \mathcal{P}_m$

(iii) $f_{\wp_i} = \mathrm{grd}(\bar{g}_i) = \mathrm{grd}(g_i)$.

Für den Beweis des Satzes 1.17 benötigen wir folgendes

1.18 Lemma. *Es sei $\theta \in W_h$ eine feste Wurzel von h und $N = K(\theta)$. Ferner sei $\hat{K}$ der topologische Abschluß von K in $N_\wp$. Ist $\bar{\theta} = \theta + \wp$ eine Wurzel eines irreduziblen Polynoms $\bar{\bar{g}} \in k_\mathfrak{p}[X]$ in $k_\wp$, dann existiert eine unverzweigte Erweiterung $\hat{M}$ von $\hat{K}$, wobei $\bar{\bar{g}}$ über dem Restklassenkörper von $\hat{M}$ in Linearfaktoren zerfällt und $\mathrm{grd}(\bar{\bar{g}})$ ein Teiler von $f_\wp$ ist.*

Beweis. Aus der Theorie der unverzweigten Erweiterungen für vollständige Körper ist bekannt, dass eine separable Erweiterung von festem Grad im Restklassenbereich eine bis auf Isomorphie eindeutige unverzweigte Erweiterung vom selben Grad im Urbildbereich garantiert. Die maximal unverzweigte Erweiterung in $N_\wp$ hat dabei den Grad $f_\wp$ über $\hat{K}$ ($[N_\wp : \hat{K}] = e_\wp f_\wp$) ([26], III §5, Theorem 2). Da aus der Irreduzibilität die Separabilität von $\bar{\bar{g}}$ folgt, garantiert der zu $K_\mathfrak{p}$ isomorphe Körper $\hat{K}$ die Existenz von $\hat{M}$ mit der gewünschten Eigenschaft. □

Beweis von Satz 1.17. Aufgrund der Regularität und Satz 1.14 gilt für die Zerlegung (1.2), dass die Polynome h_i irreduzibel vom Grad $\mathrm{grd}(h_i) = e \cdot \mathrm{grd}(g_i)$ sind. Nach Satz 1.5 und Fundamentallemma 1.11 ist $t = |\mathcal{P}_m|$ und damit

$$\hat{h}_m = \prod_{\wp \in \mathcal{P}_m} \hat{h}_\wp = \prod_{i=1}^{t} \hat{h}_{\wp_i}.$$

Wir halten fest, dass nach evtl. Umnummerierung nach dem Fundamentallemma 1.11 $\bar{g}_i = \bar{\hat{g}}_i$ ist, falls $\hat{h}_S \bmod \mathfrak{p} = \bar{\hat{g}}_1 \cdots \bar{\hat{g}}_t$ gilt. Da nach Satz 1.15 $\mathrm{grd}(\hat{h}_{\wp_i}) = e_{\wp_i} f_{\wp_i}$ gilt, ferner e nach Satz 1.6 ein Teiler von $e_{\wp_i}$ ist und $\mathrm{grd}(h_i) = e{\cdot}\mathrm{grd}(g_i) = e{\cdot}\mathrm{grd}(\bar{g}_i)$ gilt, bleibt zu zeigen, dass $\mathrm{grd}(\bar{g}_i)$ ein Teiler von $f_{\wp_i}$ ist. Dann ist nämlich $\mathrm{grd}(h_i)$ ein Teiler von $\mathrm{grd}(\hat{h}_{\wp_i})$ und aufgrund der Gleichheit von $\mathrm{grd}(h_m)$ und $\mathrm{grd}(\hat{h}_m)$ folgt aus der Teilbarkeit die Gleichheit $\mathrm{grd}(h_i) = \mathrm{grd}(\hat{h}_{\wp_i})$ für alle i.
Nach Satz 1.13 und obiger Bemerkung ist $\bar{\theta} = \theta + \wp$ eine Wurzel des globalen Polynoms $\bar{g}_i$, aber damit auch des lokalen Polynoms $\bar{\hat{g}}_i$. Nach voranstehendem Lemma 1.18 existiert aber eine unverzweigte Erweiterung vom Grade $\mathrm{grd}(\bar{g}_i) = \mathrm{grd}(\bar{\hat{g}}_i)|f_{\wp_i}$. Damit folgen (i), (ii) und (iii). □

1.19 Korollar. *Die Projektionskoordinaten E und V von S_m seien teilerfremd ($d = 1$).*

(i) Das S_m zugeordnete Polynom h_S ist linear, S_m damit regulär.

(ii) $\hat{h}_m$ und h_m sind irreduzibel über $K_\mathfrak{p}$ und die Erweiterungen durch einen Wurzelkörper sind total verzweigt vom Grade $e = E$. □

Der folgende Satz besagt, dass zu einem beliebig vorgegebenen Polynom ein Newton-Polygon konstruiert werden kann, das die Regularität eines modifizierten Polynoms garantiert, wobei die Galoisgruppen des ursprünglichen und des modifizierten Polynoms als Permutationsgruppen auf den Wurzeln isomorph sind.

1.20 Satz *(Ore [22], Satz 7).*
Sei h irreduzibel über K. Es existiert ein $\theta_0 \in R_{K(\theta)}$ mit $K(\theta) = K(\theta_0)$ und das Minimalpolynom h_0 von θ_0 über K besitzt ein Newton-Polygon bzgl. $(\mathfrak{p}, X)$, wobei das jeder Seite zugeordnete Polynom linear und damit jede Seite regulär ist.

Beweis. Sei etwa $\mathfrak{p}R_{K(\theta)} = \wp_1^{e_{\wp_1}} \cdots \wp_r^{e_{\wp_r}}$ und $t_{\wp_i}$ eine positive natürliche zu $e_{\wp_i}$ teilerfremde Zahl mit der Eigenschaft, dass

$$\frac{t_{\wp_1}}{e_{\wp_1}} < \frac{t_{\wp_2}}{e_{\wp_2}} < \dots < \frac{t_{\wp_r}}{e_{\wp_r}}.$$

Setze $m_{\wp_i} = \frac{t_{\wp_i}}{e_{\wp_i}}$. Aufgrund der Surjektivität der Exponentialbewertung und dem Chinesischen Restesatz gibt es ein $\theta_0 \in R_{K(\theta)}$ mit $v_{\wp_i}(\theta_0) = t_{\wp_i} = e_{\wp_i} m_{\wp_i}$ für jedes $i = 1, ..., r$. Nach dem Satz vom primitiven Element (Gauß) existiert ein $c \in \mathfrak{p}^{[m_{\wp_r}]+1} R_{K(\theta)}$, so dass $\theta_0 + c$ primitiv für $K(\theta)|K$ ist. Ferner erhalten wir aufgrund der Ultrametrik $v_{\wp_i}(\theta_0 + c) = v_{\wp_i}(\theta_0)$, denn es gilt $v_{\wp_i}(c) \geq ([m_{\wp_r}] + 1)e_{\wp_i} > t_{\wp_i}$ für alle i. Sei h_0 das Minimalpolynom von θ_0 über K ($h_0 \in R_K[X]$ ist normiert vom Grade n).

Nach Konstruktion hat dann das Newton-Polygon von h_0 bzgl. $\mathfrak{p}$ mindestens r verschiedene Seiten S_{m_i} mit den Steigungen $m_{\wp_i}$ (Satz 1.3). Nach Satz 1.5 sind dies auch alle Seiten, und die Primfaktorzerlegung von h_0 über $K_\mathfrak{p}$ ist

$$h_0 = (h_0)_{m_1} \cdots (h_0)_{m_r}.$$

Da $v_{\wp_i}(\theta_0) = t_{\wp_i}$ teilerfremd zu $e_{\wp_i}$ ist, hat die Seite S_{m_i} Steigung $m_{\wp_i}$, Länge $e_{\wp_i}$ und Höhe $t_{\wp_i}$. Es ist also jedes $(h_0)_{m_i}$ irreduzibel über $K_\mathfrak{p}$ und jedes einer Seite zugeordnete Polynom linear. □

1.21 Beispiel. Wir betrachten das über $\mathbb{Q}$ irreduzible Polynom $h(X) = X^2 + 12X + 4$ ($h(X) \equiv X^2 + 1 \bmod 3$ ist irreduzibel). Dann besteht das Newton-Polygon von h bzgl. $(2, X)$ aus einer Seite mit Steigung 1. Es ist $h_m(X) = X^2 + 4$ und $h_S(X) \equiv X^2 + 1 \equiv (X+1)^2 \bmod 2$ inseparabel oder nicht regulär. Für die Diskriminante von h gilt $D_h = 2^7$. Die durch h bestimmte quadratische Körpererweiterung ist $K = \mathbb{Q}(\sqrt{2})$ und das Minimalpolynom von $\theta_0 = \sqrt{2}$, das denselben Körper erzeugt wie h, ist $h_0(X) = X^2 - 2$. Dieses ist ein Eisenstein-Polynom bzgl. 2 und das der Seite zugeordnete Polynom ist linear und damit regulär.

1.22 Beispiel. Sei $h \in R_\mathfrak{p}[X]$ und $v_\mathfrak{p}(a_n) = 0$. Dann besteht das Newton-Polygon von h bzgl. $(\mathfrak{p}, X)$ nur aus einer Seite S mit Steigung $m = 0$. In diesem Fall entsteht $h_m = h_S$ aus h durch Weglassen der Monome $\pm a_i X^{n-i}$ mit $v_\mathfrak{p}(a_i) > 0$. Ist $h_S \bmod \mathfrak{p} = \bar{g}_1 \cdots \bar{g}_r$ separabel (Primfaktorzerlegung über $R_K/\mathfrak{p}$), so ist

$$h_m = h_S = g_1 \cdots g_r$$

mit irreduziblen, paarweise teilerfremden $g_i \in R_\mathfrak{p}[X]$ nach Hensels Lemma. Dann ist also $G_\mathfrak{P}$ isomorph zur Galoisgruppe von $h_S \bmod \mathfrak{p}$ als Permutationsgruppe der Wurzeln (Dedekind-Bauer). Ist $h_S \bmod \mathfrak{p}$ ($h \bmod \mathfrak{p}$) nicht separabel, so ist eine geeignete Substitution der Variablen durchzuführen, um das Polynom h zu modifizieren. Dies gilt insbesondere dann, wenn $\mathfrak{p}$ als verzweigend in $K[X]/(h)$ vermutet wird (vgl. Kapitel 2.2, 2.3 und Kapitel 3).

Kapitel 2

Verzweigung

In diesem Abschnitt richtet sich das Augenmerk auf die Verzweigung von $\mathfrak{p}$ in $N = K(\theta)$. Im Mittelpunkt steht dabei die Gleichheit der Galoisgruppen der im vorherigen Kapitel eingeführten "lokalen" und "globalen" Polynome über $K_\mathfrak{p}$ im Falle zahmer Verzweigung von $\mathfrak{p}$ in N (Kapitel 2.1). Wir untersuchen anschließend den Zusammenhang von totaler Verzweigung und Form des Newton-Polygons genauer (Kapitel 2.2) und zeigen dann die möglichen Änderungen des Newton-Polygons unter Homomorphismen vor dem Hintergrund der Existenz geeigneter unverzweigter Erweiterungen über $K_\mathfrak{p}$ auf (Kapitel 2.3).

2.1 Zahme Verzweigung

Wir halten an den Voraussetzungen und Bezeichnungen des vorherigen Kapitels fest. S_m ist also eine Seite des Newton-Polygons von h bzgl. $(\mathfrak{p}, X)$ mit nichtnegativer Steigung $m = \frac{\nu}{e}$. Wir nehmen in diesem Abschnitt zusätzlich zur Regularität von S_m an, dass $|e|_\mathfrak{p} = 1$ ist ($v_\mathfrak{p}(e) = 0$). Nach Satz 1.17 (ii) sind dann alle $\wp_i \in \mathcal{P}_m$ zahm verzweigt über $\mathfrak{p}$. Im Folgenden sei $\wp = \wp_i$ fest in $\mathcal{P}_m$ gewählt. Es seien $\hat{h}_\wp$ und h_{i_0} die zu diesem Primideal entsprechenden Primfaktoren von $\hat{h}_m$ und h_m, $\bar{g} = \bar{\hat{g}}$ das mod $\mathfrak{p}$ reduzierte zugeordnete Polynom. Wir bezeichnen mit $|\cdot|$ die Bewertung des algebraischen Abschlusses $\bar{K}_\mathfrak{p}$ von $K_\mathfrak{p}$, die $|\cdot|_\mathfrak{p}$ fortsetzt. Um die Gleichheit der Galoisgruppen der Polynome $\hat{h}_\wp$ und h_{i_0} über $K_\mathfrak{p}$ zu zeigen, wird als zentrales Hilfsmittel das folgende Lemma von Krasner benutzt.

Lemma von Krasner ([14], II §2, Proposition 3).
Es seien θ, β Elemente im algebraischen Abschluss von $K_\mathfrak{p}$ und β separabel über $K_\mathfrak{p}(\theta)$. Sind $\beta := \beta_1, \beta_2, \cdots, \beta_n$ die Konjugierten von β über $K_\mathfrak{p}$ und gilt

$$|\theta - \beta| < |\beta_i - \beta| \quad \text{für alle } \; i = 2, ..., n,$$

dann ist $K_\mathfrak{p}(\beta) \subseteq K_\mathfrak{p}(\theta)$. $\square$

Wir halten zunächst eine Vorbemerkung fest, die eine Reduktion des allgemeinenen Falls auf einen Spezialfall zulässt. Nach Lemma 1.18 zerfällt das Polynom $\bar{g}$ über dem Restklassenkörper der unverzweigten Erweiterung $\hat{M}$ vom Grad $\mathrm{grd}(\bar{g})$ in Linearfaktoren. h_{i_0} und $\hat{h}_\wp$ sind über $\hat{M}$ nicht mehr notwendig irreduzibel und haben entsprechende Zerlegungen. Ersetzen wir nun $\hat{h}_\wp$ durch den Faktor, der das Minimalpolynom von θ über $\hat{M}$ ist, h_{i_0} durch den entsprechenden Primfaktor über $\hat{M}$, dann haben nach Satz 1.14 und Satz 1.17 die zu erhaltenen Polynome dasselbe Newton-Polygon, bestehend aus einer Seite mit Steigung m, zugeordnetem linearem Polynom sowie teilerfremden Abszisse e und Ordinate ν. Ebenso nach Satz 1.17 liegt totale Verzweigung der Wurzelkörper vor. Durch Übergang zur unverzweigten Erweiterung $\hat{M}$ vom Grad $\mathrm{grd}(\bar{g})$ können wir im Folgenden also annehmen, dass $\bar{g}$ ein lineares Polynom ist und damit $K_\mathfrak{p}(\theta)$ bzw. $K_\mathfrak{p}(\beta)$ über $K_\mathfrak{p}$ total verzweigt vom Grad e.

2.1 Satz. *Es sei S_m regulär und $\mathfrak{p}$ zahm verzweigt in $K(\theta)$. Dann existiert zu jeder Wurzel θ von $\hat{h}_\wp$ eine Wurzel β von h_{i_0} mit*

$$K_\mathfrak{p}(\theta) = K_\mathfrak{p}(\beta).$$

Beweis. Nach obiger Vorbemerkung können wir annehmen, dass $K_\mathfrak{p}(\theta)$ bzw. $K_\mathfrak{p}(\beta)$ über $K_\mathfrak{p}$ total verzweigt vom Grade e. Es seien

$$\begin{aligned} h_{i_0} &= X^e + a_1 X^{e-1} + \cdots + a_{e-1}X - \pi^\nu u_{h_{i_0}}, \\ \hat{h}_\wp &= X^e + c_1 X^{e-1} + \cdots + c_{e-1}X - \pi^\nu u_{\hat{h}_\wp} \end{aligned}$$

mit $v_\mathfrak{P}(y_k) > e_\mathfrak{P} k m$ für alle $k = 1, ..., e-1$ und $y_k \in \{a_k, c_k\}$. Für die $\mathfrak{p}$-Einheiten $u_{h_{i_0}}, u_{\hat{h}_\wp}$ gilt nach Fundamentallemma 1.11 $u_{h_{i_0}} \equiv u_{\hat{h}_\wp} \mod \mathfrak{p}$, also insbesondere

$$\left| u_{\hat{h}_\wp} - u_{h_{i_0}} \right| < 1.$$

Bezeichnet $W_{h_{i_0}} = \{\beta_i\}_{i=1}^e$ die Wurzelmenge von h_{i_0}, so ist

$$\left| a_k \beta^{e-k} \right| < |\pi|^\nu \quad \text{bzw.} \tag{2.1}$$
$$\left| c_k \theta^{e-k} \right| < |\pi|^\nu \quad (k \in \{1, ..., e-1\}), \tag{2.2}$$

denn es gilt $v_\mathfrak{P}(c_k\theta^{e-k}) = v_\mathfrak{P}(a_k\beta^{e-k}) > (e-k)e_\mathfrak{P}m + e_\mathfrak{P}km = e_\mathfrak{P}\nu$. Da für die Bewertungen $\left|\pi^m\right| = |\theta| = |\beta|$ gilt, kann man für die Wurzeln

$$\begin{aligned} \theta^e &= \pi^\nu u \\ \beta^e &= \pi^\nu u_\beta \end{aligned}$$

mit $\mathfrak{p}$-Einheiten u, u_β schreiben. Wir halten fest, dass die Ungleichung

$$\begin{aligned} |\pi^\nu| |u - u_{\hat{h}_\wp}| &= |\theta^e - \pi^\nu u_{\hat{h}_\wp}| = \left|\sum_{i=1}^{e-1} c_i \theta^{e-i}\right| \\ &\leq \max_{1\leq i\leq e-1} \left\{ |c_i \theta^{e-i}| \right\} < |\pi|^\nu \end{aligned}$$

gilt und erhalten $|u - u_{\hat{h}_\wp}| < 1$. Aufgrund der Ultrametrik folgt dann

$$|u - u_{h_{i_0}}| \leq \max\{|u - u_{\hat{h}_\wp}|, |u_{\hat{h}_\wp} - u_{h_{i_0}}|\} < 1.$$

Betrachten wir h_{i_0} an der Stelle θ, so ist

$$\prod_{i=1}^{e} |\theta - \beta_i| < |\pi|^\nu \tag{2.3}$$

wegen

$$\begin{aligned} \prod_{i=1}^{e} |\theta - \beta_i| &= |h_{i_0}(\theta)| = \left|(\theta^e - \pi^\nu u_{h_{i_0}}) + \sum_{i=1}^{e-1} a_i \theta^{e-i}\right| \\ &\leq \max\{|\pi^\nu| |u - u_{h_{i_0}}|, \max_{i=1,\dots,e-1} \{|a_i| |\theta^{e-i}|\} \} < |\pi|^\nu. \end{aligned}$$

Da sicherlich die Beziehung

$$|\theta - \beta_i| \leq \max\{|\theta|, |\beta_i|\} = |\pi|^{\frac{\nu}{e}} \tag{2.4}$$

gilt, existiert wegen (2.3) und (2.4) eine Wurzel $\beta := \beta_1$ von h_{i_0} mit

$$|\theta - \beta| < |\pi|^{\frac{\nu}{e}}.$$

Wir zeigen, dass für dieses β die Behauptung gilt. Dazu betrachten wir zunächst die Ableitung des Polynoms h_{i_0} an der Stelle β und schließen aufgrund der zahmen Verzweigung

$$\begin{aligned} |h'_{i_0}(\beta)| &= \frac{1}{|\beta|} |e\beta^e + ((e-1)a_1 \beta^{e-1} + \cdots + a_{e-1}\beta)| \\ &\leq \max\left\{ |\pi|^{\frac{\nu}{e}(e-1)}, \max_{1\leq i\leq e-1} \left\{ \frac{1}{|\beta|} |(e-i) a_i \beta^{e-i}| \right\} \right\} \overset{(2.1)}{=} |\pi|^{\frac{\nu}{e}(e-1)}. \end{aligned}$$

Andererseits gilt unter Berücksichtigung der Ungleichung (2.4), die ebenso für β anstatt θ gilt, und mit Hilfe der Produktregel für h'_{i_0} an der Stelle β

$$|h'_{i_0}(\beta)| = \prod_{i=2}^{e} |\beta - \beta_i| \leq |\pi|^{\frac{\nu}{e}(e-1)}.$$

Da die Wurzeln β_i die Konjugierten von β sind, folgt mit (2.3)

$$|\beta_i - \beta| = |\pi|^{\frac{\nu}{e}} > |\theta - \beta|.$$

Das Lemma von Krasner liefert damit $K_{\mathfrak{p}}(\beta) \subseteq K_{\mathfrak{p}}(\theta)$ und aufgrund der Irreduzibilität der Polynome h_{i_0} und $\hat{h}_\wp$ über $K_{\mathfrak{p}}$, die denselben Grad haben, folgt die Gleichheit der Wurzelkörper. □

Wir können nun die Sätze 1.17 und 2.1 zusammenfassen zu dem in der Einleitung formulierten

2.2 Hauptsatz. *Sei $S = S_m$ eine reguläre Seite des Newton-Polygons von h bzgl. $\mathfrak{p}$ der Länge E mit nichtnegativer Steigung $m = \frac{\nu}{e}$ (gekürzt). Für eine feste Wurzel θ von h (irreduzibel über K) seien $\mathcal{P}_m$, $\hat{h}_m$, h_m, h_S wie üblich erklärt.*

(a) *Die verschiedenen Primfaktoren $\bar{g}_\wp$ von h_S mod $\mathfrak{p}$ können so durch $\mathcal{P}_m$ indiziert werden, dass $f_\wp = \mathrm{grd}(\bar{g}_\wp)$ jeweils der Restklassengrad ist. Für alle $\wp \in \mathcal{P}_m$ ist $e = e_\wp$ der Verzweigungsindex über $\mathfrak{p}$.*

(b) *Über $K_{\mathfrak{p}}$ hat $h_m = \prod_{\wp \in \mathcal{P}_m} h_\wp$ eine entsprechende Primfaktorzerlegung, wobei jeweils $\mathrm{grd}(h_\wp) = e_\wp \cdot f_\wp$ der Grad des Primfaktors $\hat{h}_\wp$ von h ist.*

(c) *Ist überdies $\mathfrak{p}$ kein Teiler von e (zahme Verzweigung), so haben h_m und $\hat{h}_m$ denselben Zerfällungskörper über $K_{\mathfrak{p}}$ (in einem festen algebraischen Abschluss) und ihre Galoisgruppe G_m hat isomorphe Permutationsdarstellungen auf den Wurzeln dieser Polynome.* □

2.3 Beispiel. Es seien a, b ganze Zahlen mit $\frac{(b-i)a}{b} \notin \mathbb{Z}$ für alle $i = 1, ..., b-1$. Gilt $v_{\mathfrak{p}}(b) = 0$, dann sind die Galoisgruppen der über K irreduziblen Polynome $\tilde{h}(X) = X^b + \pi^a u$ und $h(X) = X^b + \pi^{[\frac{a}{b}]} a_1 X^{b-1} + \pi^{[\frac{2a}{b}]} a_2 X^{b-2} + \cdots + \pi^{[\frac{(b-1)a}{b}]} a_{b-1} X + \pi^a u$ über $K_{\mathfrak{p}}$ identisch ($\pi \in K$ Primelement, u eine $\mathfrak{p}$-Einheit).

2.4 Beispiel. $\mathbb{Q}_p(\sqrt[p-1]{-p})$ ist der p-te Kreisteilungskörper über $\mathbb{Q}_p$ ($p \geq 3$ Primzahl).

Beweis. Sei $h(X) = \frac{(X+1)^p - 1}{(X+1)-1} = X^{p-1} + X^{p-2} + \cdots + p$. Ist $\theta = \varepsilon_p$ eine primitive p-te Einheitswurzel, so ist $\varepsilon_p - 1$ eine Wurzel von h. Das Newton-Polygon von h bzgl. (p, X) besteht aus einer Seite S der Länge $p-1$ mit Steigung $\frac{1}{p-1}$. (Dies entspricht dem Newton-Polygon des p-ten Kreisteilungspolynoms Φ_p bzgl. $(p, X-1)$ (vgl. Kapitel 2.3)). Da h_S linear ist, ist der Hauptsatz anwendbar. Es ist $h_m = X^{p-1} + p$. Da $\mathbb{Q}_p$ die $(p-1)$-ten Einheitswurzeln enthält, folgt die Behauptung. □

Dieses Resultat ist wohlbekannt (vgl. [8], Chapt. 15, Sect.3, p.222 für einen anderen Zugang).

2.5 Korollar. *Es sei h ein über $\mathbb{Q}$ irreduzibles Trinom der Form $h = X^n + aX^s + b \in \mathbb{Q}[X]$. Ferner sei p kein Teiler von n und das Newton-Polygon bzgl. (p, X) bestehe aus einer Seite mit $v_p(a) > \frac{v_p(b)}{n}(n - s)$. Dann existiert eine Wurzel $\theta \in W_h$ mit $\mathbb{Q}_p(\theta) \simeq \mathbb{Q}_p(\sqrt[n]{-b})$.*

Beweis. p verzweigt zahm in $L_{\mathfrak{P}}$ wegen $p \not| n$. Es ist $h_m = X^n + b$ und $h_S \equiv X^d + \frac{b}{p^{v_p(b)}}$ mod p separabel wegen $d =$ggT$(n, v_p(b)) \not| n$. Die Seite ist daher regulär und mit Hauptsatz 2.2 (c) folgt die Behauptung. □

2.2 Totale Verzweigung

Nach Hauptsatz 2.2 liegt totale Verzweigung im Wurzelkörper vor, wenn Abszisse und Ordinate des einseitigen Newton-Polygons teilerfremd sind. Das folgende Lemma zeigt einen Zusammenhang zwischen totaler Verzweigung und der Primfaktorzerlegung von h modulo eines Primideals $\mathfrak{p}$ auf ($h \in R_{\mathfrak{p}}[X]$).

2.6 Lemma. *Sei h irreduzibel über K. Verzweigt $\mathfrak{p}$ total im Wurzelkörper $N = K(\theta)$, so besteht das Newton-Polygon von h bzgl. $\mathfrak{p}$ nur aus einer Seite und für die Primfaktorzerlegung von h mod $\mathfrak{p}$ gilt*

$$h(X) \equiv (X + c)^n \mod \mathfrak{p}$$

für ein $c \in R_{\mathfrak{p}}$.

Beweis. Aufgrund der totalen Verzweigung gilt $\mathcal{P} = \mathcal{P}_m = \{\wp\}$. Das Newton-Polygon kann also aus nur einer Seite bestehen. Wegen $|\mathcal{P}_m| = 1$ ist h irreduzibel über $K_{\mathfrak{p}}$ und es gilt $e_\wp = n =$ grd(h) bzw. $1 = f_\wp =$grd$(\bar{g}_i)$. Daher zerfällt h mod $\mathfrak{p}$ in ein Produkt von Linearfaktoren ([6], III §3 Theorem 25), etwa $h(X) \equiv (X - c_1) \cdots (X - c_n)$ mod $\mathfrak{p}$. Angenommen, es gelte $c_i \neq c_j$ für ein $i \neq j$. Dann gilt

$$h(X) = (X - c_{i_0})^m + \mathfrak{p} \cdot \tilde{h}(X) \quad \text{bzw.} \quad h(X + c_{i_0}) \equiv X^m \bmod \mathfrak{p}$$

mit $m < n$ und grd$(\tilde{h}) = n$. Das Newton-Polygon von $h(X + c_{i_0})$ bzgl. $(\mathfrak{p}, X)$ besteht dann aber aus mindestens zwei Seiten mit den Eckpunkten $(0, 0), (n - m, 0)$ und $(n, v_{\mathfrak{p}}(a_n))$, was nach der Vorbemerkung nicht sein kann. □

2.7 Satz. *Sei $h = \sum_{j=0}^{q} (-1)^j a_j X^{q-j}$ ein über $\mathbb{Q}$ irreduzibles Polynom von Primzahlgrad q und p eine Primzahl mit $0 \leq \frac{v_p(a_q)}{q} \notin \mathbb{Z}$. Die Primzahl p verzweigt genau dann in N total, wenn das Newton-Polygon von (p, X) aus genau einer Seite besteht.*

Beweis. Verzweigt p total in N, so folgt die Behauptung mit Lemma 2.6. Besteht das Newton-Polygon aus einer Seite mit der angegebenen Koeffizientenbedingung, so gilt $m = \frac{v_p(a_q)}{q} \notin \mathbb{Z}$ und das der Seite zugeordnete Polynom h_S ist linear (ggT$(v_p(a_q), q)$=1).

Es ist h irreduzibel über $K_{\mathfrak{p}}$ (Korollar 1.8) und mit Hauptsatz 2.2 folgt $\mathcal{P} = \{\wp\}$, $e_\wp = q, f_\wp = 1$ und die Behauptung. □

Bemerkung. Satz 2.7 ist also eine Verallgemeinerung des Ergebnisses von Sase [25] Proposition 2, der totale Verzweigung von p für $m < 1$ behandelt.

Für $m \in \mathbb{Z}$, etwa $m = 0$, kann eine Primzahl nur im nichtregulären Fall total verzweigen. Beispiel hierfür ist das p-te Kreisteilungspolynom vom Grad $p-1$ bzgl. (p, X) (in $N = \mathbb{Q}(\varepsilon_p)$). Für Trinome können wir aber im allgemeinen zeigen, dass auch im nichtregulären Fall für $m = 0$ keine totale Verzweigung von p in N vorliegen kann.

2.8 Satz. *Sei h ein über $\mathbb{Q}$ irreduzibles Trinom vom Grad n (≥ 3), etwa $h(X) = X^n + aX^s + b \in \mathbb{Q}[X]$ und p eine Primzahl mit $v_p(a) \geq v_p(b) = 0$, d.h. $m = 0$ bzgl. (p, X).*

(a) Ist p kein Teiler von n, so verzweigt p nicht total im Wurzelkörper $N = \mathbb{Q}(\theta)$.

(b) Ist p ein Teiler von n, $v_p(a) = 0$ und $s \neq \frac{n}{2}$, so verzweigt p nicht total in N.

Zusatz. *Ist p ein Teiler von n, $v_p(a) > 0$ und existiert ein $i \in \{2, ..., \frac{n}{2}\}$ mit $p \nmid \binom{n}{i}$, dann verzweigt p nicht total im Wurzelkörper N.*

Beweis. Angenommen, p verzweige total in $\mathbb{Q}(\theta)$. Dann gilt nach Lemma 2.6

$$h(X) \equiv (X+c)^n = X^n + ncX^{n-1} + \cdots + nc^{n-1}X + c^n \mod p.$$

(a) Ist $c \equiv 0 \bmod p$, dann gilt $h(X) \equiv X^n \bmod p$, also $h(X) = X^n + p \cdot \tilde{h}(X)$ und daher $v_p(b) > 0$.
Sei also $c \not\equiv 0 \bmod p$, dann ist nc bzw. $nc^{n-1} \not\equiv 0 \bmod p$ und h kann kein Trinom sein.
(b) Aufgrund der Symmetrie des Binomialkoeffizienten muss für die Reduktion des Trinoms

$$h(X) \equiv X^n + \binom{n}{\frac{n}{2}} c^{\frac{n}{2}} X^{\frac{n}{2}} + c^n \mod p$$

gelten, was nur möglich ist, falls $v_p(a) > 0$.
Der Zusatz folgt aus der für totale Verzweigung notwendigen Bedingung

$$h(X) \equiv X^n + c^n \mod p,$$

die für $p \nmid \binom{n}{i}$ (i geeignet) nicht erfüllt ist. □

2.3 Das Newton-Polygon bzgl. eines Polynoms

Die gesamte bisherige Theorie basierte auf der Definition des Newton-Polygons bzgl. $(\mathfrak{p}, X)$. Nun lassen wir statt $\tilde{g} = X$ auch Entwicklungen nach allgemeineren Polynomen $\tilde{g}$ zu. Sinnvoll ist dies nur für (normierte) Polynome $\tilde{g}$, deren Reduktion mod $\mathfrak{p}$ ein Teiler von h mod $\mathfrak{p}$ ist ($h \in R_\mathfrak{p}[X]$). Sei

$$h(X) \equiv \bar{\tilde{g}}_1(X)^{e_1} \cdots \bar{\tilde{g}}_r(X)^{e_r} \mod \mathfrak{p}$$

die Primfaktorzerlegung von h mod $\mathfrak{p}$ und $\tilde{g}_i(X) \in R_\mathfrak{p}[X]$ ein normiertes Urbild von $\bar{\tilde{g}}_i(X) \in k_\mathfrak{p}[X]$. Wir schreiben $\tilde{g} = \tilde{g}_i$ für ein festes i und π für ein Primelement mit $v_\mathfrak{p}(\pi) = 1$.

2.9 Definition. Es sei $c := \operatorname{grd}(\tilde{g})$ der Grad von $\tilde{g}$. Dann bezeichne

$$h = \sum_{i=0}^{[\frac{n}{c}]} \widetilde{a_i}(X)\tilde{g}(X)^{[\frac{n}{c}]-i}$$

die Entwicklung von h bzgl. $\mathfrak{p}$ und $\tilde{g}$, wobei $\widetilde{a_i}(X) \in R_\mathfrak{p}[X]$ vom Grade $< c$. Ist $\widetilde{a_i}(X) \neq 0$, so sei π^{v_i} die größte Potenz von π, für die $\pi^{-\mathrm{v}_i}\widetilde{a_i}(X) \in R_\mathfrak{p}[X]$ ist. Die untere konvexe Hülle der Punkte $(i, \mathrm{v}_i) = (i, v_\mathfrak{p}(\widetilde{a_i}(X)))$ im euklidischen $\mathbb{R}^2$ bezeichnen wir als Newton-Polygon von h bzgl. $(\mathfrak{p}, \tilde{g}(X))$. Dieses besteht (ebenso wie das Newton-Polygon bzgl. $(\mathfrak{p}, X)$) aus geradlinigen Seiten S_{m_j} mit streng monoton wachsenden Steigungen $m_1 < m_2 < ... < m_t$.

Nach der Vorbemerkung zu Satz 2.1 können wir uns nach Übergang zur unverzweigten Erweiterung $\hat{M}$ vom Grad $\operatorname{grd}(\tilde{g})$ darauf beschränken, dass $K_\mathfrak{p}(\theta)$ über $K_\mathfrak{p}$ total verzweigt. Nach Lemma 2.6 haben wir dann die Situation

$$h(X) \equiv (X + c)^n \mod \mathfrak{p}, \ \ c \in R_\mathfrak{p}.$$

2.10 Satz. *Wir können die Entwicklung von h bzgl. $(\mathfrak{p}, \tilde{g}(X)) = (\mathfrak{p}, X + c)$ auf den Fall $(\mathfrak{p}, X)$ zurückführen.*

Beweis. Wir betrachten das Newton-Polygon $(\mathfrak{p}, X + c)$. Die Primfaktorzerlegung mod $\mathfrak{p}$ ist

$$h(X) \equiv (X + c)^n \mod \mathfrak{p}.$$

Die Entwicklung von $h(X)$ bzgl. $(\mathfrak{p}, X + c)$ entspricht wegen

$$h(X - c) \equiv X^n \mod \mathfrak{p}$$

der Entwicklung von $h(X-c) = h(-c) + h'(-c)X + \frac{h''(-c)}{2}X^2 + \cdots + \frac{h^{(n)}(-c)}{n!}X^n$ bzgl. $(\mathfrak{p}, X)$, d.h. das Newton-Polygon besteht aus der unteren konvexen Hülle der Punkte $(i, v_{\mathfrak{p}}(\frac{h^{(i)}(-c)}{i!}))$. □

Es stellt sich nun die Frage, wie sich das Newton-Polygon und damit der "Informationsgehalt" über die Primidealzerlegung bzw. Galoisgruppe eines Polynoms unter Einsetzungshomomorphismen ändern kann. Im Falle totaler Verzweigung genügt es, affine Transformationen zu betrachten. Dann können wir davon ausgehen, dass der Grad von $\hat{h}_m$ invariant unter affinen Transformationen ist. Wir untersuchen im Folgenden, wie sich die Steigung bzw. die Höhe der Seite unter diesen Homomorphismen ändern kann.

Wir schreiben für das Polynom h mit einseitigem Newton-Polygon

$$h(X) = h(0) + h'(0)X + \frac{h''(0)}{2!}X^2 + \cdots + X^E$$

und bezeichnen wie im vorherigen Kapitel $V = v_{\mathfrak{p}}(h(0))$. Gilt $\mathrm{ggT}(V, E) = 1$, so ist h irreduzibel über $K_{\mathfrak{p}}$ (und damit über K) und $\mathfrak{p}$ total verzweigt in $N = K(\theta)$. Die Frage ist folglich, ob sich durch affine Transformationen eine solche Aussage über die Verzweigung von $\mathfrak{p}$ treffen läßt, falls $\mathrm{ggT}(V, E) > 1$.

2.11 Satz. *Das Newton-Polygon von $h(X)$ bzgl. $(\mathfrak{p}, X)$ bestehe aus einer Seite mit nichtnegativer Steigung $m = \frac{V}{E}$. Besteht das Newton-Polygon von $h(aX+b)$ bzgl. $(\mathfrak{p}, X)$ ebenfalls aus einer Seite mit Länge E , dann gilt folgende Aussage ($a, b \in R_{\mathfrak{p}}$, $v_{\mathfrak{p}}(a) = 0$).*

(i) Ist $v_{\mathfrak{p}}(b) =: k > m$, dann stimmen die Newton-Polygone der beiden Polynome überein.

(ii) Ist $v_{\mathfrak{p}}(b) = k \leq m$, so hat die Steigung m' von $h(aX+b)$ einen Wert $\geq k$.

Zusatz *(Irreduzibiltätskriterium).*
Gilt $v_{\mathfrak{p}}\big(\frac{h^{(i)}(b)}{i!a^{E-i}}\big) > v_{\mathfrak{p}}\big(\frac{h^{(i)}(0)}{i!}\big)$ und $v_{\mathfrak{p}}\big(\frac{h(b)}{a^E}\big) = v_{\mathfrak{p}}(h(0)) + 1$ oder gilt $\mathrm{ggT}\big(\frac{h(b)}{a^E}, E\big) = 1$, dann ist h irreduzibel über $K_{\mathfrak{p}}$ und damit irreduzibel über K.

Beweis. Es ist $h(aX+b) = h(b) + h'(b)aX + \frac{h''(b)}{2!}a^2X^2 + \cdots + a^EX^E$. Nach Voraussetzung ist $v_{\mathfrak{p}}\big(\frac{h^{(i)}(0)}{i!}\big) \geq \frac{V}{E}(E-i)$ für alle $0 \leq i \leq E$, daher folgt für $h(b) = h(0) + h'(0)b + \frac{h''(0)}{2!}b^2 + \cdots + b^E$ insbesondere

$$v_{\mathfrak{p}}(h(b)) \geq \min_{0 \leq i \leq E} \left\{ \frac{V}{E}(E-i) + ki \right\} = \min_{0 \leq i \leq E} \left\{ V + i(k - \frac{V}{E}) \right\}. \tag{2.5}$$

Da das Newton-Polygon von $h(aX+b)$ ebenso aus einer Seite besteht, gilt sicherlich

$$v_{\mathfrak{p}}\left(\frac{h^{(i)}(b)}{a^{E-i}i!}\right) \geq \frac{v_{\mathfrak{p}}(h(b))}{E}(E-i) \qquad \text{für alle } 0 \leq i \leq E. \tag{2.6}$$

Wir setzen im Folgenden $m' := \frac{v_\mathfrak{p}(h(b))}{E}$. Mit der Spezialisierung $a = 1$ und $X = -b$ folgt

$$h(0) = h(b) - h'(b)b + \frac{h''(b)}{2!}b^2 - + \cdots + (-1)^E b^E.$$

Die Betrachtung der $\mathfrak{p}$-adischen Bewertung liefert dann

$$V = v_\mathfrak{p}(h(0)) \geq \min_{0\leq i\leq E}\left\{ v_\mathfrak{p}\left(\frac{h^{(i)}(b)}{i!}b^i\right)\right\}.$$

(i) Wegen (2.6) gilt

$$v_\mathfrak{p}\left(\frac{h^{(i)}(b)}{i!}b^i\right) \geq m'(E-i) + im = Em' + i(m-m')$$

für alle $1 \leq i \leq E-1$. Es folgt

$$V \geq \min_{1\leq i\leq E-1}\{Em', Em' + i(m-m'), Ev_\mathfrak{p}(b)\}$$

Angenommen $m' < m$, dann ist $V = Em'$ bzw. $m' = \frac{V}{E} = m$, was einen Widerspruch liefert. Gilt hingegen $m' > m$, dann ist $m' + (E-1)m > Em$ bzw. $Em' + (E-1)(m-m') = m' + \frac{E-1}{E}V > V$, was im Widerspruch zu $V \geq \min_{1\leq i\leq E-1}\{Em', Em' + i(m-m'), Ev_\mathfrak{p}(b)\}$ steht. Damit folgt $m = m'$.
(ii) Wegen (2.5) ist

$$v_\mathfrak{p}(h(b)) \geq \min_{0\leq i\leq E-1}\left\{V - i(\frac{V}{E} - k), Ek\right\} = Ek \qquad (2.7)$$

und wir erhalten $m' \geq k$.
Der Zusatz ist offensichtlich, denn entweder das Newton-Polygon von $h(X)$ oder das von $h(aX + b)$ besitzt teilerfremde Koordinatenprojektionen und die Irreduzibilität der Polynome über $K_\mathfrak{p}$ folgt. □

Im Folgenden bezeichne wie üblich $\wp$ ein Primideal über $\mathfrak{p}$ in $N = \mathbb{Q}(\theta)$.

2.12 Beispiel. Sei $\tilde{h} = X^p + \tilde{a}X + \tilde{a} \in \mathbb{Z}[X]$ ein Eisenstein-Polynom bzgl. p und θ eine Nullstelle von $\tilde{h}$. Dann ist θ ein Primelement von $N_\wp = \mathbb{Q}_p(\theta)$ ($v_\wp(\theta) = k = 1$). Es ist

$$\begin{aligned} h(X) = \frac{\tilde{h}(X)}{X-\theta} &= \tilde{h}'(\theta) + \frac{\tilde{h}''(\theta)}{2}(X-\theta) + \cdots + \frac{\tilde{h}^{(p)}(\theta)}{p!}(X-\theta)^{p-1} \\ &= h(0) + h'(0)X + \frac{h''(0)}{2!}X^2 + \cdots + X^{p-1}. \end{aligned}$$

Offensichtlich gilt $v_\wp(h(0)) = v_\wp\big(\tilde{h}'(\theta) - \frac{\tilde{h}''(\theta)}{2}\theta + \cdots + (-1)^{p-1}\frac{\tilde{h}^{(p)}(\theta)}{p!}\theta^{p-1}\big) = p-1$, d.h. $k = m = 1$ wegen $E = p-1$ und $v_\wp\big(\frac{h^{(i)}(\theta)}{i!}\big) \geq p$ für alle $i < p$. Die Steigung des Newton-Polygons von $h(X+\theta)$ beträgt $1 + \frac{1}{p-1}$, denn

$$v_\wp(h(\theta)) = v_\wp\big(\tilde{h}'(\theta)\big) = v_\wp\big(p\theta^{p-1} + \tilde{a}\big) = p = v_\wp(h(0)) + 1.$$

Nach Satz 2.11 kann daher durch die Verschiebung $X \mapsto X + \theta$ (d.h. $a = 1, b = \theta$) die Irreduzibilität von h über $N_\wp$ und damit über N gezeigt werden.

2.13 Beispiel. Sei $h(X)$ das p-te Kreisteilungspolynom, $h(X) = \Phi_p(X) = \frac{X^p-1}{X-1}$. Bezüglich (p, X) ist das Newton-Polygon ein Teil der x-Achse. Es ist $E = p-1$, $m = 0$, $v_p(1) = k = m = 0$ und $v_p(h(1)) = v_p(h(0))+1 = 1$. Nach Satz 2.11 ist damit h irreduzibel über $\mathbb{Q}_p$. In der Tat ist $h(X+1)$ ein Eisenstein-Polynom bezüglich p ($v_p\big(\frac{h^{(i)}(1)}{i!}\big) \geq 1$ für alle i, $m' = \frac{1}{p}$ und $a = b = 1$).

Diese Idee nutzt man auch aus, um lokale Galoisgruppen auszurechnen. Ist θ eine Nullstelle des über K irreduziblen Polynoms h, dann untersuchen wir das Polynom $h_0 = \frac{h(X)}{X-\theta}$ auf Irreduzibilität über $K(\theta)$, um eine Abschätzung über die Galoisgruppe von h nach unten zu bekommen (entsprechendes Verfahren für $h_1 = \frac{h_0(X)}{X-\theta_2}$ über $K(\theta, \theta_2)$ usw. im Falle der Reduzibilität von h_0 über $K(\theta)$ fortsetzen).

2.14 Satz. *Es sei $p > 3$ eine Primzahl und $h(X) = \sum_{j=0}^{p} (-1)^j a_j X^{p-j}$ ein Eisenstein-Polynom bzgl. p mit $v_p(a_{p-1}) = 1$. Dann ist* $\mathrm{Gal}_{\mathbb{Q}_p}(h) = \mathrm{AGL}_1(p) \leq \mathrm{Gal}_{\mathbb{Q}}(h)$.

Beweis. Wir halten zunächst fest, dass θ ein Primelement im Körper $N_\wp$ ist. Da die lokale Galoisgruppe als auflösbare Untergruppe der vollen symmetrischen Gruppe von Primzahlgrad die Ordnung $p(p-1)$ teilt, ist zu zeigen, dass das Polynom $h_0(X) = \frac{h(X)}{X-\theta}$ irreduzibel über $N_\wp$ ist. Es ist

$$h_0(X+\theta) = h'(\theta) + \frac{h''(\theta)}{2} X + \frac{h'''(\theta)}{3!} X^2 + \cdots + X^{p-1} \quad \text{mit}$$
$$\frac{h^{(i)}(\theta)}{i!} = \binom{p}{i} \theta^{p-i} - \binom{p-1}{i} a_1 \theta^{p-(i+1)} + - \cdots + (-1)^{p-i} a_{p-i}.$$

Wegen $p | a_{p-i}$ $(1 \leq i < p)$ gilt $v_\wp\big(\frac{h^{(i)}(\theta)}{i!}\big) \geq p$ für alle $1 \leq i < p$ und für $i = 1$ erhalten wir

$$\begin{aligned} v_\wp(h'(\theta)) &= v_\wp\big(p\theta^{p-1} - (p-1)a_1\theta^{p-2} + - \cdots + (-1)^{p-1} a_{p-1}\big) \\ &= p. \end{aligned}$$

Das einseitige Newton-Polygon von $h_0(X+\theta)$ bzgl. $(\wp, X)$ hat die Steigung $m = \frac{p}{p-1}$ mit teilerfremder Abszisse und Ordinate. h_0 ist daher irreduzibel über $N_\wp$ und es gilt

$$p(p-1) \geq [L_{\mathfrak{P}} : \mathbb{Q}_p] = [L_{\mathfrak{P}} : N_\wp][N_\wp : \mathbb{Q}_p] \geq (p-1)p.$$

Die Behauptung folgt. □

Bemerkung. Der zu h_0 gehörende Faktor über $N_\wp$ ist

$$(h_0)_m = X^{p-1} + h'(\theta) = X^{p-1} + a_1 \underbrace{\left(1 + (-1)^{p-2} \frac{2}{a_1} a_2 \theta + - \cdots - \frac{p-1}{a_1} a_{p-1} \theta^{p-2}\right)}_{=:u}.$$

Es ist u eine Einseinheit und damit eine $(p-1)$-te Wurzel in $N_\wp$ ([8], Chapter 15.2 II, p.217). Der lokale Zerfällungskörper dieses Polynoms ist demnach $L_\mathfrak{P} = \mathbb{Q}_p(\theta, \sqrt[p-1]{-a_1})$.

Um die Zerlegungsgruppe $G_\mathfrak{P}$ (als Untergruppe der Galoisgruppe von h) zu bestimmen, muss man die Zerlegung von h in Primfaktoren über $K_\mathfrak{p}(\theta)$ kennen. Im Falle totaler und wilder Verzweigung von $\mathfrak{p}$ erhalten wir für das Eisenstein-Polynom h aus Satz 2.14 die Irreduzibilität von h_0 über $N_\wp$ und damit $G_\mathfrak{P} = \mathrm{AGL}_1(p)$. Der folgende Satz zeigt jedoch, dass durch diese affine Transformation im Falle zahmer Verzweigung von $\mathfrak{p}$ in $N_\wp$ keine derartigen Erkenntnisse gewonnen werden können. Genauer:

2.15 Satz. *Sei h irreduzibel über K und $\mathfrak{p}$ total und zahm verzweigt im Wurzelkörper $N = K(\theta)$, d.h. θ ist ein Primelement in N mit Primideal $\wp$ über $\mathfrak{p}$ und $\mathfrak{p}$ teilt nicht $n = grd(h) = [N_\wp : K_\mathfrak{p}]$. Die Steigung des einseitigen Newton-Polygons bzgl. $(\mathfrak{p}, X)$ sei positiv. Zur Untersuchung von $[L_\mathfrak{P} : N_\wp]$ betrachten wir h über $N_\wp$, genauer $h_0 = \frac{h(X)}{X-\theta}$. Dann ist das Newton-Polygon von h_0 bzgl. $\wp$ invariant unter der affinen Transformation $X \mapsto X + \theta$.*

Beweis. Es gilt

$$h_0(X) = \frac{h(X)}{X-\theta} = h'(\theta) + \frac{h''(\theta)}{2}(X-\theta) + \frac{h'''(\theta)}{3!}(X-\theta)^2 + ... + (X-\theta)^{n-1} \quad \text{und}$$

$$h_0(X+\theta) = \frac{h(X+\theta)}{X} = h'(\theta) + \frac{h''(\theta)}{2}X + \frac{h'''(\theta)}{3!}X^2 + ... + X^{n-1}.$$

Wir erhalten

$$\frac{h^{(i)}(\theta)}{i!} = \binom{n}{i}\theta^{n-i} - \binom{n-1}{i}a_1\theta^{n-(i+1)} + - ... + (-1)^{n-i}a_{n-i}$$

für alle $i \geq 1$. Wegen $m > 0$ teilt $\mathfrak{p}$ die Koeffizienten a_i, $i \geq 1$. Daher gilt $v_\wp(h'(\theta)) = n-1$ ($\mathfrak{p}$ ist kein Teiler von n). Das Newton-Polygon von $h_0(X+\theta)$ (bzgl. $(\wp, X)$) besteht aus einer Seite mit Steigung $m = 1$ ($v_\wp\big(\frac{h^{(i)}(\theta)}{i!}\big) \geq n-i$ für alle $i = 1, \ldots, n-1$). Für den letzten Koeffizienten von $h_0(X)$ gilt $v_\wp\big(h'(\theta) - \frac{h''(\theta)}{2}\theta + \frac{h'''(\theta)}{3!}\theta^2 - + ... + (-1)^{n-1}\theta^{n-1}\big) = v_\wp\big(\sum_{i=1}^n (-1)^{i-1}\frac{h^{(i)}(\theta)}{i!}\theta^{i-1}\big) \geq v_\wp\big(h'(\theta)\big) = n-1$ und echt größer, nur falls $\mathfrak{p}$ ein Teiler von $\sum_{i=1}^n (-1)^{i-1}\binom{n}{i} = 1$ ist, was nicht sein kann. Da das Newton-Polygon von $h_0(X)$ bzgl. $(\mathfrak{p}, X)$ aufgrund der totalen Verzweigung von $\mathfrak{p}$ in N auch aus nur einer Seite besteht, besitzt dieses ebenso Steigung $m = 1$ und die Behauptung folgt. $\square$

Kapitel 3

Konkrete Berechnung von Galoisgruppen

In diesem Kapitel steht die Berechnung von Galoisgruppen von Polynomen im Vordergrund. Betrachten wir zunächst Beispiel 1.2 mit $h(X) = X^{13} + \frac{5}{81}X^{10} + 25X^8 - \frac{20}{3}X^6 + \frac{10}{27}X^5 + \frac{5}{3}X^3 + 5X^2 + 135$. Wir ordnen den vier Seiten des Newton-Polygons bzgl. $(3, X)$ mit $\tilde{m}_1 < m_2 < m_3 < m_4$ ihre zugeordneten Polynome zu (für $\tilde{m}_1$ betrachten wir die entsprechende Seite S_{m_1} des Polynoms $\frac{X^n}{(-1)^n a_n} h(X^{-1})$ mit $m_1 = -\tilde{m}_1 > 0$). Die Polynome h_{S_1}, h_{S_2} und h_{S_4} sind linear und das Polynom $h_{S_3} \equiv X^3 - X - 1 \bmod 3$ ist irreduzibel und damit separabel über $\mathbb{F}_3$. Es liegt also Regularität vor, so dass nach Hauptsatz 2.2

$$3R_N = \wp_1^3 \wp_2^5 \mathfrak{a} \wp_3^2$$

die Zerlegung von 3 in $N = \mathbb{Q}(\theta)$ ist, wobei $\mathfrak{a}$ ein Primideal oder ein Produkt von (höchstens drei) paarweise verschiedenen Primidealen in N ist. Ist $\mathfrak{P}$ ein Primideal über 3 im Zerfällungskörper L von h, so enthält die Trägheitsgruppe $T_{\mathfrak{P}}$ ein Element σ, das sich als Produkt aus einem 3-er, 5-er und 2-er Zykel (und Fixpunkten) schreiben läßt. Damit enthält $T_{\mathfrak{P}}$ auch eine Transposition (etwa σ^{15}) und es folgt $G = S_{13}$. Die Faktoren der Seite sind $h_{m_1} = X^3 + \frac{81}{5}$, $h_{m_2} = X^5 + 6$, $h_{m_3} = X^3 + \frac{9}{2}X + \frac{27}{2}$ und $h_{m_4} = X^2 + 27$, so dass $L_{\mathfrak{P}}$ zum Beispiel den 3-ten Kreisteilungskörper (über $\mathbb{Q}_3$) enthält, denn nach Hauptsatz 2.2 (c) existiert eine Wurzel $\theta_{i_0} \in W_h$ mit $\mathbb{Q}_3(\theta_{i_0}) = \mathbb{Q}_3(\sqrt{-27}) = \mathbb{Q}_3(\varepsilon_3)$ (Beispiel 2.4).

Während die Galoisgruppe reiner Polynome leicht zu bestimmen ist, treten schon bei der Bestimmung der Galoisgruppe von Trinomen im allgemeinen Schwierigkeiten auf. Im Folgenden sollen Galoisgruppen von über $\mathbb{Q}$ irreduziblen Trinomen der Form $h = X^n + aX^s + b$ untersucht werden. Zahlreiche Arbeiten haben sich bereits mit diesem Problem befaßt. Schon Wegner [36] zeigte für $n = p > 3$, $s = 1$ und $\mathrm{ggT}((p-1)a, pb) = 1$, dass die Galoisgruppe von h die volle symmetrische Gruppe vom Grade p ist.

Uchida ([31], [32] und [33]), Komatsu ([12], [13]) und Movahhedi [18] untersuchten ebenfalls vor allem den Fall $s = 1$. Dabei zeigt sich etwa, dass die Galoisgruppe des Polynoms $h = X^p + aX + a$ die volle symmetrische Gruppe ist, falls $\mathrm{ggT}(p, a) = 1$ und die volle symmetrische oder die affine Gruppe, falls h ein Eisenstein-Polynom bzgl. p ist.

In der jüngsten Arbeit von Hermez und Salinier [10] werden für $3 \leq s \leq n - 3$ und $n \geq 7$ Kriterien angegeben, so dass $G = \mathrm{Gal}_{\mathbb{Q}}(h)$ die alternierende Gruppe A_n ist.

Zahlreiche Fälle von Trinomen bleiben zu betrachten. Bei der Bestimmung der Galoisgruppe von Trinomen werden im Folgenden vor allem die Fälle $s \leq 2$ bzw. $s = n - 2$ im Vordergrund stehen. Das Hauptaugenmerk wird dabei auf das Eisenstein-Polynom $h = X^p + taX + a$ (bzgl. p) gelegt werden.

Bei der Beschreibung von Galoisgruppen ist es oftmals schon hilfreich, Aussagen über Primitivität oder Mehrfachtransitivität zu gewinnen. In jüngerer Zeit stand die Untersuchung von Trinomen auf diese Eigenschaften im Vordergrund (etwa [4], [19], [5]). Es soll daher zunächst ein Kriterium gezeigt werden, mit dessen Hilfe neue Resultate gewonnen werden können.

3.1 Primitivität von Galoisgruppen

Wir verwenden die üblichen Bezeichnungen. Die Galoisgruppe $G = \mathrm{Gal}_K(h)$ ist genau dann primitiv, wenn der Punktstabilisator $G_\theta = \mathrm{Gal}_{K(\theta)}(h)$ eine maximale Untergruppe von G ist. Anders ausgedrückt, G ist genau dann imprimitiv, wenn ein Zwischenkörper $K(\theta_1)$ existiert mit $\mathrm{Gal}_{K(\theta)}(h) < \mathrm{Gal}_{K(\theta_1)}(h) < G$.
Wir betrachten die Situation bei Imprimitivität ($n_0 n_1 = n$; $n_0, n_1 \notin \{1, n\}$).

$$\begin{array}{l|ll} & K(\theta) & \wp \\ n_0 & & \\ & K(\theta_1) & \tilde{\mathfrak{p}} \\ n_1 & & \\ & K & \mathfrak{p} \end{array}$$

Wegen $[K(\theta) : K(\theta_1)] = n_0 < n$ (genauer $n_0 | n$) ist h reduzibel über $K(\theta_1)$.
Es sei $\mathfrak{p}$ ein Primideal in K, $\tilde{\mathfrak{p}}$ ein über $\mathfrak{p}$ liegendes Primideal in $K(\theta_1)$ und $\wp$ ein über $\tilde{\mathfrak{p}}$ liegendes Primideal in $K(\theta)$. Für die Primidealzerlegungen von $\mathfrak{p}$ bzw. $\tilde{\mathfrak{p}}$ gelte

$$\begin{aligned}
\mathfrak{p}R_{K(\theta)} &= \wp_1^{e(\wp_1|\mathfrak{p})}\cdots\wp_s^{e(\wp_s|\mathfrak{p})}, \quad n=\sum_{r=1}^{s} e(\wp_r|\mathfrak{p})f(\wp_r|\mathfrak{p})\\
\mathfrak{p}R_{K(\theta_1)} &= \tilde{\mathfrak{p}}_1^{e(\tilde{\mathfrak{p}}_1|\mathfrak{p})}\cdots\tilde{\mathfrak{p}}_t^{e(\tilde{\mathfrak{p}}_t|\mathfrak{p})}, \quad n_1=\sum_{r=1}^{t} e(\tilde{\mathfrak{p}}_r|\mathfrak{p})f(\tilde{\mathfrak{p}}_r|\mathfrak{p})\\
\tilde{\mathfrak{p}}_iR_{K(\theta)} &= \wp_{i_1}^{e(\wp_{i_1}|\tilde{\mathfrak{p}}_i)}\cdots\wp_{i_u}^{e(\wp_{i_u}|\tilde{\mathfrak{p}}_i)}, \quad n_0=\sum_{r=i_1}^{i_u} e(\wp_r|\tilde{\mathfrak{p}}_i)f(\wp_r|\tilde{\mathfrak{p}}_i),
\end{aligned}$$

wobei $t,u\le s$ und $\{i_j|1\le j\le u\}\subseteq\{1,...,s\}$ für alle i. Bildet man unter Ausnutzen der Transitivität der Verzweigungsindizes und Trägheitsgrade das Produkt

$$e(\tilde{\mathfrak{p}}_i|\mathfrak{p})f(\tilde{\mathfrak{p}}_i|\mathfrak{p})n_0 = e(\tilde{\mathfrak{p}}_i|\mathfrak{p})f(\tilde{\mathfrak{p}}_i|\mathfrak{p})\sum_{r=i_1}^{i_u} e(\wp_r|\tilde{\mathfrak{p}}_i)f(\wp_r|\tilde{\mathfrak{p}}_i) = \sum_{r=i_1}^{i_u} e(\wp_r|\mathfrak{p})f(\wp_r|\mathfrak{p})$$

so erhält man

$$n_0=\frac{1}{e(\tilde{\mathfrak{p}}_i|\mathfrak{p})f(\tilde{\mathfrak{p}}_i|\mathfrak{p})}\sum_{r=i_1}^{i_u} e(\wp_r|\mathfrak{p})f(\wp_r|\mathfrak{p}).$$

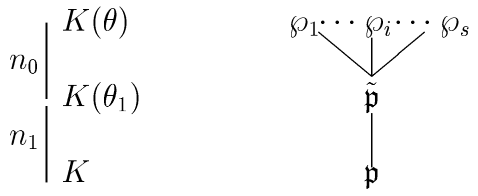
Wir bezeichnen im Folgenden

$$\begin{aligned}
\mathfrak{g} &:= \mathrm{ggT}(e(\wp_1|\mathfrak{p})f(\wp_1|\mathfrak{p}),\cdots,e(\wp_s|\mathfrak{p})f(\wp_s|\mathfrak{p})) \qquad \text{und}\\
\mathfrak{g}_i &:= \mathrm{ggT}(e(\wp_i|\mathfrak{p})f(\wp_i|\mathfrak{p}),\ n).
\end{aligned}$$

3.1 Satz. *Es gelten die Bezeichnungen von oben mit $s>1$. Ist $\mathfrak{p}$ träge in $K(\theta_1)$ ($f(\tilde{\mathfrak{p}}|\mathfrak{p})=n_1$) oder existiert ein Primideal von $R_{K(\theta_1)}$, das in $K(\theta)$ nicht zerfällt (insbesondere total verzweigt), dann sind die Zahlen $e(\wp_i|\mathfrak{p})f(\wp_i|\mathfrak{p})$ ($i=1,...,s$) und n nicht alle paarweise teilerfremd.*

Beweis.

(i) Sei $\mathfrak{p}$ träge in $K(\theta_1)$, also $\mathfrak{p}R_{K(\theta_1)}=\tilde{\mathfrak{p}}$. Wegen $e(\tilde{\mathfrak{p}}|\mathfrak{p})f(\tilde{\mathfrak{p}}|\mathfrak{p}) \mid e(\wp_i|\mathfrak{p})f(\wp_i|\mathfrak{p})$ für alle i gilt offensichtlich $e(\tilde{\mathfrak{p}}|\mathfrak{p})f(\tilde{\mathfrak{p}}|\mathfrak{p}) \mid \mathfrak{g}$.

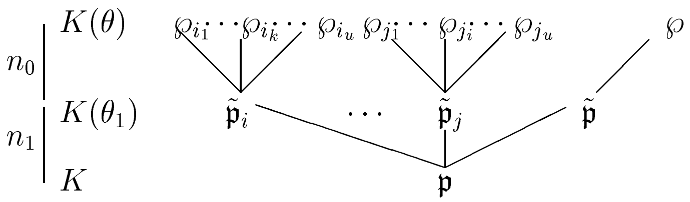


Dann ist

$$\begin{aligned}
n_0 &= \sum_{r=1}^{s} e(\wp_r|\tilde{\mathfrak{p}})f(\wp_r|\tilde{\mathfrak{p}}) = \frac{1}{e(\tilde{\mathfrak{p}}|\mathfrak{p})f(\tilde{\mathfrak{p}}|\mathfrak{p})}\sum_{r=1}^{s} e(\wp_r|\mathfrak{p})f(\wp_r|\mathfrak{p})\\
&= \frac{n}{e(\tilde{\mathfrak{p}}|\mathfrak{p})f(\tilde{\mathfrak{p}}|\mathfrak{p})} = \frac{n}{\tilde{\mathfrak{g}}} \quad \text{für} \quad \tilde{\mathfrak{g}}=e(\tilde{\mathfrak{p}}|\mathfrak{p})f(\tilde{\mathfrak{p}}|\mathfrak{p}).
\end{aligned}$$

Gilt also $n_0 \notin \{1, n\}$, dann ist $1 < \tilde{\mathrm{g}} < n$ und damit $\mathrm{g} > 1$. Die Zahlen $e(\wp_i|\mathfrak{p})f(\wp_i|\mathfrak{p})$ $(i = 1, ..., s)$ sind folglich nicht alle paarweise teilerfremd.

(ii) Sei $\tilde{\mathfrak{p}}$ ein nicht zerfallendes Primideal.



Dann gilt

$$n_0 = e(\wp|\tilde{\mathfrak{p}})f(\wp|\tilde{\mathfrak{p}}) = \frac{e(\wp|\mathfrak{p})f(\wp|\mathfrak{p})}{e(\tilde{\mathfrak{p}}|\mathfrak{p})f(\tilde{\mathfrak{p}}|\mathfrak{p})}.$$

Es ist also n_0 ein Teiler von $\mathrm{ggT}(e(\wp|\mathfrak{p})f(\wp|\mathfrak{p}),\ n)$. Gilt also $n_0 \notin \{1, n\}$, dann ist $\mathrm{g}_i > 1$ für ein i. □

3.2 Korollar. *Sind die Zahlen $e(\wp_i|\mathfrak{p})f(\wp_i|\mathfrak{p})$ $(i = 1, ..., s)$ und n paarweise teilerfremd, so ist die Galoisgruppe $\mathrm{Gal}_K(h)$ primitiv oder jedes Primideal des Zwischenkörpers in $K(\theta)$ zerfällt und $\mathfrak{p}$ ist nicht träge in $K(\theta_1)$.* □

3.3 Korollar *(Ore [23]). Sei $s \in \{2, 3\}$. Ist $\mathrm{g}{=}\mathrm{g}_i{=}1$ für alle $i \in \{1, 2, 3\}$, dann ist $G = \mathrm{Gal}_K(h)$ primitiv.*

Beweis. Offensichtlich, denn es tritt stets einer der Fälle (i) oder (ii) aus Satz 3.1 auf. □

Wie üblich schreiben wir im Folgenden für den Verzweigungindex von $\wp$ über $\mathfrak{p}$ wieder $e_\wp$, für den Trägheitsgrad entsprechend $f_\wp$. Für $h = X^n + aX^s + b$ können wir n und s als teilerfremd voraussetzen (sonst betrachten wir das Polynom $g(X) = h(X^{\mathrm{ggT}(n,s)})$). Da wir für eine beliebige Seite des Newton-Polygons $m \geq 0$ voraussetzen können, betrachten wir nun stets Polynome, deren Newton-Polygon bzgl. (p, X) aus Seiten mit ausschließlich nichtnegativen Steigungen besteht. Für die Form des Newton-Polygons bzgl. (p, X) existieren prinzipiell vier Möglichkeiten: Das Newton-Polygon besteht aus einer oder zwei Seiten, wobei jeweils unterschieden werden kann, ob eine Seite die Steigung $m = 0$ besitzt. Um die Resultate von Cohen, Movaheddi und Salinier [4], [5], [19] zu erweitern, betrachten wir daher diese möglichen Situationen (Satz 3.4 für das zweiseitige Newton-Polygon mit $m_1 m_2 = 0$, Satz 3.5 für $m_1 m_2 > 0$, Satz 3.6 für das einseitige Polynom mit $m = 0$ und Satz 3.7 für $m > 0$).

3.4 Satz. *Es sei $h(X) = X^n + aX^s + b \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$ und p eine Primzahl mit $v_p(b) > v_p(a) = 0$. $G{=}\mathrm{Gal}_\mathbb{Q}(h)$ ist primitiv, falls eine der folgenden Aussagen gilt ($\mathrm{ggT}(n, s) = 1$):*

(i) $n-s$ *ist eine* p*-Potenz,* $v_p(h(-a)) = \mathrm{ggT}(s, v_p(b)) = 1$.

(ii) $s = 2$, $n-2$ *ist eine* p*-Potenz und* $v_p(h(-a)) = 1$.

(iii) $s \in \{n-1, n-2\}$ *und* $\mathrm{ggT}(s, v_p(b)) = 1$.

Beweis. Im Fall (i) und (ii) gilt

$$h = X^n + aX^s + b \equiv X^s(X^{n-s} + a) \equiv X^s(X+a)^{n-s} \mod p.$$

Nach dem Henselschen Lemma gilt $h = \hat{h}_1 \cdot \hat{h}_2$ über $\mathbb{Q}_p$ mit inseparablen Polynomen $\hat{h}_1 \equiv X^s \bmod p$, $\hat{h}_2 \equiv (X+a)^{n-s} \bmod p$.
(i) Das Newton-Polygon von h bzgl. (p, X) besitzt die Eckpunkte $(0,0)$, $(n-s, 0)$ und $(n, v_p(b))$. Das der Seite S_m (mit positiver Steigung) zugeordnete Polynom ist linear, und nach Hauptsatz 2.2 verzweigt das über p liegende und zu S_m gehörende Primideal $\wp_1$ total in $\mathbb{Q}(\theta)_{\wp_1}$. Aufgrund der Inseparabilität von $\hat{h}_2 \equiv (X+a)^{n-2} \bmod p$ betrachten wir das Newton-Polygon $(p, X+a)$, welches sich wie üblich über die Taylorentwicklung von h bestimmen läßt. Es gilt

$$h(X-a) = h(-a) + h'(-a)X + \cdots + X^n \equiv (X-a)^s X^{n-s} \mod p.$$

Das Newton-Polygon von h bzgl. $(p, X+a)$ besitzt also die Eckpunkte $(0,0)$, $(s,0)$ und $(n,1)$. Das der Seite (mit positiver Steigung) zugehörige Polynom ist linear, man erhält auch hier totale Verzweigung für das der Seite zugehörige Primideal $\wp_2$. Nach Satz 1.4 und Hauptsatz 2.2 gilt für die Primidealzerlegung in $\mathbb{Q}(\theta)$ also

$$p_{\mathbb{Q}(\theta)} = \wp_1^s \ \wp_2^{n-s}$$

$(f_{\wp_i} = 1; i = 1,2)$. Wäre p ein Teiler von n, dann wäre p auch ein Teiler von s (wegen $n-s = p^t$ für ein $t > 0$) und $\mathrm{ggT}(n,s) > 1$. Daher sind $n, n-s$ und s paarweise teilerfremd und die Behauptung folgt nach Satz 3.1.
(ii) Ist $s = 2$ und $\mathrm{ggT}(s, v_p(b))$=2, so gilt für die Primidealzerlegung von p in $\mathbb{Q}(\theta)$

$$pR_{\mathbb{Q}(\theta)} = \wp_1^{n-2}\wp_2^2, \quad pR_{\mathbb{Q}(\theta)} = \wp_1^{n-2}\wp_2 \quad \text{oder} \quad pR_{\mathbb{Q}(\theta)} = \wp_1^{n-2}\wp_2\wp_3.$$

In den ersten beiden Fällen gilt $e_{\wp_2}f_{\wp_2} = 2$, im dritten Fall $e_{\wp_2}f_{\wp_2} = e_{\wp_3}f_{\wp_3} = 1$. Da n ungerade ist, sind die Zahlen n, $n-s$ (und 2) paarweise teilerfremd und die Behauptung folgt mit Satz 3.1.
(iii) Das Newton-Polygon von h bzgl. (p, X) hat die Eckpunkte $(0,0)$, $(n-s, 0)$ und $(n, v_p(b))$. Wegen $\mathrm{ggT}(s, v_p(b)) = 1$ ist das der Seite S_m mit positiver Steigung zugeordnete Polynom linear und für das dieser Seite zugehörige Primideal $\wp_1$ gilt $e_{\wp_1} = s$, $f_{\wp_1} = 1$. Existiert nur ein weiteres Primideal $\wp_2$ über p in $\mathbb{Q}(\theta)$, so gilt $e_{\wp_2}f_{\wp_2} \in \{1,2\}$, sind es

zwei weitere Primideale (nur im Fall $s = n-2$ möglich), so gilt $e_{\wp_2} f_{\wp_2} = e_{\wp_3} f_{\wp_3} = 1$. Die Behauptung folgt aufgrund der paarweisen Teilerfremdheit von n, s (und 2). □

Bemerkung. Die Aussage (i) ist nach [4], Theorem 2 und Lemma 3.2 bekannt. Wir werden in Satz 3.24 (ii) und Satz 3.25 (ii) zeigen, dass unter den Voraussetzungen von Satz 3.4 für ungerades n und $s \in \{2, n-2\}$ die Galoisgruppe G im allgemeinen die volle symmetrische Gruppe ist.

3.5 Satz. *Sei $h(X) = X^n + aX^s + b \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$ und p eine Primzahl mit $v_p(ba^{-1}) > 1 + \frac{s}{n-s}$ $(v_p(a) > 0)$. $G = \mathrm{Gal}_{\mathbb{Q}}(h)$ ist primitiv, falls eine der folgenden Aussagen gilt $(\mathrm{ggT}(n, s) = 1)$:*

(i) $\mathrm{ggT}(n-s, nsv_p(a)) = \mathrm{ggT}(s, v_p(ba^{-1})) = 1$.

(ii) $s \in \{1, 2\}$ *und* $\mathrm{ggT}(v_p(a), n-s) = 1$.

Beweis. Das Newton-Polygon von h bzgl. (p, X) besitzt die Eckpunkte $(0,0)$, $(s, v_p(a))$ und $(n, v_p(b))$.
(i) Aufgrund der Teilerfremdheit der Abszissen und Ordinaten der jeweiligen Seiten, sind die den Seiten zugeordneten Polynome linear und es gilt $e_{\wp_1} f_{\wp_1} = s$ bzw. $e_{\wp_2} f_{\wp_2} = n-s$. Da n, $n-s$ und s paarweise teilerfremd sind, folgt die Behauptung mit Satz 3.1.
(ii) Im Fall $s = 2$ existieren höchtens drei (und mindestens zwei) Primideale über p in $\mathbb{Q}(\theta)$ mit $e_{\wp_1} f_{\wp_1} = n-2$, $e_{\wp_2} f_{\wp_2} = 2$ oder $e_{\wp_1} f_{\wp_1} = n-2$, $e_{\wp_2} f_{\wp_2} = e_{\wp_3} f_{\wp_3} = 1$. Im Fall $s = 1$ gibt es genau zwei Primideale über p in $\mathbb{Q}(\theta)$ mit $e_{\wp_1} f_{\wp_1} = n-1$ und $e_{\wp_2} f_{\wp_2} = 1$. Satz 3.1 liefert die Behauptung (n ist im Fall $s = 2$ ungerade). □

3.6 Satz. *Sei $h(X) = X^n + aX^s + b \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$ und p eine Primzahl, bzgl. der (und X) das Newton-Polygon aus einer Seite mit Steigung $m = 0$ besteht $(v_p(a) \geq v_p(b) = 0)$. $G = \mathrm{Gal}_{\mathbb{Q}}(h)$ ist primitiv, falls eine der folgenden Aussagen gilt:*

(i) Es existiert ein $c \in \mathbb{Z}_p$ mit $\frac{h^{(i)}(c)}{i!} \equiv 0 \bmod p$ für genau alle $i = 0, ..., n-2$ und $v_p(h(c)) = 1$.

(ii) n ungerade, es existiert ein $c \in \mathbb{Z}_p$ mit $\frac{h^{(i)}(c)}{i!} \equiv 0 \bmod p$ für genau alle $i = 0, ..., n-3$ und $v_p(h(c)) = 1$.

Beweis. Es ist

$$h(X+c) = h(c) + h'(c)X + \frac{h''(c)}{2}X^2 + \cdots + \frac{h^{(n-2)}(c)}{(n-2)!}X^{n-2} + \frac{h^{(n-1)}(c)}{(n-1)!}X^{n-1} + X^n.$$

Im Fall (i) ergibt sich also

$$h(X+c) \equiv \frac{h^{(n-1)}(c)}{(n-1)!}X^{n-1} + X^n = X^{n-1}\left(X + \frac{h^{(n-1)}(c)}{(n-1)!}\right) \bmod p,$$

und im Fall (ii)

$$h(X+c) \equiv X^{n-2}\left(X^2 + \frac{h^{(n-1)}(c)}{(n-1)!}X + \frac{h^{(n-2)}(c)}{(n-2)!}\right) \mod p.$$

Das Newton-Polygon von $h(X+c)$ bzgl. (p, X) besteht im Fall (i) aus den Punkten $(0,0)$, $(1,0)$ und $(n, v_p(h(c)))$. Die Seite S_m $(m > 0)$ des Newton-Polygons hat teilerfremde Abszisse und Ordinate, so dass für das dieser Seite zugeordnete Primideal $e_{\wp_1} f_{\wp_1} = n-1$ gilt. Im Fall (ii) existieren höchstens drei (und mindestens zwei) Primideale über p in $\mathbb{Q}(\theta)$ mit $e_{\wp_1} f_{\wp_1} = n-2$, $e_{\wp_2} f_{\wp_2} = 2$ oder $e_{\wp_1} f_{\wp_1} = n-2$ und $e_{\wp_2} f_{\wp_2} = e_{\wp_3} f_{\wp_3} = 1$, denn die Eckpunkte des Newton-Polygons sind $(0,0)$, $(2,0)$ und $(n, v_p(h(c)))$. Die Behauptung folgt. □

3.7 Satz. *Sei $h(X) = X^n + aX^s + b \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$ und p eine Primzahl, bzgl. der (und X) das Newton-Polygon aus einer Seite mit Steigung $m > 0$ besteht ($v_p(a) \geq v_p(b) - \frac{s v_p(b)}{n} > 0$). G=$\mathrm{Gal}_{\mathbb{Q}}(h)$ ist primitiv, falls folgende Bedingungen erfüllt sind:*

(1) Es existiert ein $c \in \mathbb{Z}_p$ und ein $i \in \{1, ..., n-1\}$ mit

$$v_p\left(\frac{h^{(i)}(c)}{i!}\right) < \frac{v_p(h(c))(n-i)}{n},$$
$$v_p\left(\frac{h^{(j)}(c)}{j!}\right) \geq \frac{v_p\left(\frac{h^{(i)}(c)}{i!}\right)(n-j)}{n-i} \quad \text{für alle } j > i \text{ und}$$
$$v_p\left(\frac{h^{(j)}(c)}{j!}\right) \geq \left(1 - \frac{j}{i}\right) v_p(h(c)) + \frac{j}{i} v_p\left(\frac{h^{(i)}(c)}{i!}\right) \quad \text{für alle } j < i$$

(2) $\mathrm{ggT}\big(n-i, v_p\big(\frac{h^{(i)}(c)}{i!}\big)\big) = \mathrm{ggT}\big(i, v_p\big(\frac{h(c) i!}{h^{(i)}(c)}\big)\big) = 1,$

(3) $\mathrm{ggT}(n, i) = 1.$

Zusatz. *Für $i = 2$ bzw. $i = n-2$ kann auf die Bedingung $\mathrm{ggT}\big(2, v_p\big(\frac{2h(c)}{h''(c)}\big)\big) = 1$ bzw. $\mathrm{ggT}\big(2, v_p\big(\frac{h^{(n-2)}(c)}{(n-2)!}\big)\big) = 1$ in (2) verzichtet werden.*

Beweis. Wegen

$$h(X+c) = h(c) + h'(c) + \cdots + \frac{h^{(i)}(c)}{i!}X^i + \cdots + X^n$$

garantiert Bedingung (1), dass das Newton-Polygon von $h(X+c)$ bzgl. (p, X) aus zwei Seiten mit positiven Steigungen besteht. Analog zum Beweis von Satz 3.4 (i) (etwa) sind die zugeordneten Polynome wegen Bedingung (2) linear und es gilt $pR_N = \wp_1^{n-i}\wp_2^i$. Bedingung (3) liefert die notwendige Voraussetzung, um die Teilerfremdheit der Verzweigungsindizes zu garantieren (Satz 3.1). Der Zusatz folgt aus den Sätzen 3.4 (ii), (iii), 3.5 (ii) und 3.6 (ii). □

Bemerkung. Die Beweise bzw. Bedingungen der Sätze 3.6 und 3.7 zeigen, durch welche Voraussetzungen an affine Transformationen aus einseitigen Newton-Polygonen Polygone mit mehr als zwei Seiten konstruiert werden können. Die Teilerfremdheit der entsprechenden Abszissen, Ordinaten und n (zum Beispiel) liefert dann die Primitivität der Galoisgruppe von h.

3.2 Polynome der Form $h(X) = X^p + taX + a$

In diesem Abschnitt sei $p > 3$ eine Primzahl, b, t ganze Zahlen mit p teilt nicht bt und $a = pb$. Wir untersuchen die Galoisgruppe des Eisenstein-Polynoms $h = X^p + taX + a$. Für die Diskriminante von h gilt nach Swan ([30], Theorem 2) $D_h = D_0 \cdot D_1$, wobei $D_0 = p^{p-1} + bt^p(p-1)^{p-1}$ und $D_1 = (-1)^{\frac{p-1}{2}} p^p b^{p-1}$ teilerfremd sind und D_0 ungerade ist. Wie üblich ist L der Zerfällungskörper von h, $N = \mathbb{Q}(\theta)$ und $\theta \in W_h$. Für $t = 1$ hat Movahhedi [18] gezeigt, dass nur die affine oder volle symmetrische Gruppe als Galoisgruppe von h möglich sind. Bis heute gibt es kein Beispiel mit affiner Galoisgruppe.

3.8 Satz. *Sei q ein Primfaktor von D_0 und $\mathfrak{Q}$ ein Primideal in L über q.*

(a) Ist $v_q(D_0)$ ungerade, so verzweigt q zahm in L und $T_{\mathfrak{Q}}$ wird von einer Transposition erzeugt.

(b) Ist $v_q(D_0)$ gerade, so ist q unverzweigt in L und $G_{\mathfrak{Q}}$ hat entweder zwei Fixpunkte auf W_h, falls $-2D_0p(p-1)/q^{v_q(D_0)}$ ein Quadrat mod q ist, oder eine Bahn der Länge zwei sonst.

Beweis. Nach obiger Vorbemerkung ist q ungerade und q teilt $ta(p-1)$ nicht, also insbesondere $0 \not\equiv -\frac{p}{t(p-1)} =: u \bmod q$. Wir berechnen den größten gemeinsamen Teiler von h und h' mod q. Es ist $p \cdot h - X \cdot h' = ta(p-1)X + pa \not\equiv 1 \bmod q$. Folglich ist h mod q inseparabel und $X - u \bmod q = \mathrm{ggT}(h, h') \bmod q$. Mit Hilfe des Henselschen Lemmas erhalten wir eine Faktorisierung von $h = \hat{h}_1 \cdot \hat{h}_2$ über $\mathbb{Q}_q$ mit $\hat{h}_1 \bmod q = (X-u)^2 \bmod q$ und $\hat{h}_2 \bmod q$ ist separabel (und teilerfremd zu $X - u$).
Aufgrund der Inseparabilität von h mod q und da das Newton-Polygon von h bzgl. (q, X) mit einem Teil der x-Achse zusammenfällt, betrachten wir das wegen $v_q(h(u)) > 0$ nicht mit der x-Achse zusammenfallende Newton-Polygon von h bzgl. $(q, X-u)$, also

$$h(X+u) = h(u) + h'(u)X + \frac{h''(u)}{2!}X^2 + \cdots + X^n$$

(bzgl. (q, X); vgl. Satz 2.10). Wegen

$$\frac{h''(u)}{2!} = \frac{p(p-1)u^{p-2}}{2} = -\frac{p^{p-1}}{2t^{p-2}(p-1)^{p-3}}$$

teilt q den drittletzten Koeffizienten $\frac{h''(u)}{2!}$ nicht und $(p-2, 0)$ ist ein Punkt dieses Newton-Polygons. Ferner gilt

$$h'(u) = pu^{p-1} + ta = \frac{p^p + t^p pb(p-1)^{p-1}}{(t(p-1))^{p-1}} = \frac{pD_0}{(t(p-1))^{p-1}} \text{ und}$$

$$h(u) = -\frac{p^p}{(t(p-1))^p} - ta\frac{p}{t(p-1)} + a = -\frac{pD_0}{(t(p-1))^p}.$$

Wir erhalten folglich $v_q(D_0) = v_q(h(u)) = v_q(h'(u))$. Der zur Seite S_m (bestehend aus den Punkten $(p-2, 0)$ und $(p, v_q(D_0))$) gehörende Faktor ist $h_m = X^2 + \frac{2!h(u)}{h''(u)} = X^2 - c$ mit $c = -\frac{2D_0p(p-1)}{[tp^{\frac{p-1}{2}}(p-1)^2]^2}$. Damit ist $h_S = X - \frac{c}{q^{v_q(D_0)}}$, falls $v_q(D_0)$ ungerade ist und $h_S = X^2 - \frac{c}{q^{v_q(D_0)}}$ sonst. In beiden Fällen ist $\bar{h}_S = h_S \bmod q$ separabel und S_m regulär.

(a) Ist $v_q(D_0)$ ungerade, so hat das einzige der Seite mit positiver Steigung zugeordnete Primideal $\mathfrak{q}$ von N über q den Verzweigungsindex $e_{\mathfrak{q}} = 2$ und Trägheitsgrad $f_{\mathfrak{q}} = 1$. Alle anderen Primideale haben aufgrund der Separabilität von $\hat{h}_2$ Verzweigungsindex 1. Da q nach Voraussetzung ungerade ist, verzweigt $\mathfrak{q}$ zahm in N und in L (Kompositum von allen zahm verzweigten Erweiterungen [20], p.236). Daher ist die Trägheitsgruppe $T_{\mathfrak{Q}}$ zyklisch ([2], Chapter I, Section 8, Prop.1). Es ist $\hat{h}_1$ irreduzibel über $\mathbb{Q}_q$ und $T_{\mathfrak{Q}}$ von einer Transposition auf $W_{\hat{h}_1}$ erzeugt.

(b) Ist $v_q(D_0)$ gerade, so ist $e_{\mathfrak{q}} = e = 1$ für alle Primideale $\mathfrak{q}$ über q in N. Damit ist q unverzweigt in L ([21], II (7.3)). Es gilt ferner $c = \tilde{c}^2 \in \mathbb{Q}_q^{*2}$ genau dann, wenn $-2D_0p(p-1)q^{-v_q(D_0)}$ ein Quadrat mod q ist $\left(\left(\frac{-2D_0p(p-1)q^{-v_q(D_0)}}{q}\right) = 1\right)$. Genau dann ist aber h_S reduzibel mod q und die Zerlegungsgruppe $G_{\mathfrak{Q}}$ hat zwei Fixpunkte auf W_h. Die Behauptung folgt also mit dem Hauptsatz 2.2. □

3.9 Satz. *Sei q ein Primteiler von b, $\mathfrak{Q}$ ein Primideal über q in L.*

(i) Ist $v_q(b)$ nicht durch p teilbar, so verzweigt q in $\mathbb{Q}(\theta)$ total und zahm. Es ist $\mathbb{Q}_q(\theta) = \mathbb{Q}_q(\sqrt[p]{-a})$ und die Trägheitsgruppe $T_{\mathfrak{Q}}$ wird von einem p-Zykel auf W_h erzeugt.

(ii) Ist $v_q(b)$ durch p teilbar, so ist q unverzweigt in L und $L_{\mathfrak{Q}}$ der Zerfällungskörper von $X^p + a$ über $\mathbb{Q}_q$ ($\mathbb{Q}_q[X]/(h) \simeq \mathbb{Q}_q[X]/(X^p + a)$ als $\mathbb{Q}_q$-Algebren).

Beweis. Wir betrachten das Newton-Polygon von h bzgl. (q, X). Es besteht aus einer Seite mit Steigung $v_q(b)/p$ und zugeordnetem Faktor $h_m = X^p + a$. Im Fall (i) ist h_S linear, im Fall (ii) ist $h_S = X^p + \frac{a}{q^{v_q(a)}}$ separabel mod q, und die Behauptung liefert in beiden Fällen Hauptsatz 2.2. □

3.10 Korollar. *Es gelten die üblichen Bezeichnungen.*

(i) Für $|D_0| \notin \mathbb{N}^2$ *gilt* $G = S_p$.

(ii) Für $|D_0| \in \mathbb{N}^2$ *ist die Diskriminante des Zwischenkörpers* $D_N = (-1)^{(p-1)/2} p^p b_0^{p-1}$, *wobei* b_0 *das Produkt der verschiedenen in* $N = \mathbb{Q}(\theta)$ *verzweigenden Primteiler von* b *ist.*

Beweis. (i) Sei $|D_0|$ kein rationales Quadrat. Dann existiert eine Primzahl q, die D_0 teilt und sodass $v_q(D_0)$ ungerade ist. Nach Satz 3.8 (a) enthält G also eine Transposition. Als primitive Gruppe von Primzahlgrad ist G damit die volle symmetrische Gruppe.
(ii) Da D_N ein Teiler von $D_1 D_0$ ist und die Primteiler von D_N genau die in N verzweigenden Primzahlen sind, kommen als Primfaktoren von D_N nach Satz 3.8 (b) nur Teiler von D_1, also p oder Primteiler q von b mit $\mathrm{ggT}(v_q(b), p){=}1$ (Satz 3.9 (ii)) in Frage. Liegt ein Eisenstein-Polynom bzgl. q vor (wie etwa bei $q = p$), dann teilt q nicht den Index und damit gilt $v_q(D_N) = v_q(D_1)$ (vgl. [6], III §3, Theorem 24). In diesem Fall folgt also die Behauptung mit $b_0 = b$. Andernfalls folgt die Behauptung aus Satz 3.9 (i) aufgrund der zahmen und totalen Verzweigung der Primteiler q von b in N, denn dann ist die q-adische Bewertung der Differente genau $p - 1$ ([20], Chapter 4, §2, Theorem 4.8). □

Bemerkung. Es gilt also $v_q(b_0) = 1$ unabhängig von $v_q(b)$. Bezeichnet $i(h)$ den Index $[R_N : \mathbb{Z}(\theta)]$, so gilt $D_h = i(h)^2 \cdot D_N$ und es folgt $v_q(i(h)^2) = (p-1)(v_q(b) - v_q(b_0)) = (p-1)(v_q(b)-1)$. Daher gilt $v_q(i(h)) = \frac{1}{2}(p-1)(v_q(b)-1)$. Man kann folglich die q-adische Bewertung des Index an der Form des Newton-Polygons ablesen. Man zählt dazu lediglich die Gitterkästchen $((i, v_q(a_i)) \in \mathbb{Z} \times \mathbb{Z})$ echt unterhalb der Seite des Polygons (ohne die Punkte auf der x-Achse) ab (vgl. [22], Satz 8 und [15], Theorem 3).

Die nächsten beiden Sätze schließen das Resultat von Movahhedi ([18] Theorem 2.2, Theorem 3.1, Lemmata 4.1 und 4.2) für $t = 1$ ein.

3.11 Satz. *Sei* $\mathfrak{P}$ *ein Primideal über* p *in* L.

(i) Die Primzahl p *ist total und wild verzweigt in* $N = \mathbb{Q}(\theta)$.

(ii) $G_{\mathfrak{P}} = T_{\mathfrak{P}}$ *operiert auf* W_h *als affine Gruppe* $\mathrm{AGL}_1(p)$.

(iii) Es gilt $L_{\mathfrak{P}} = \mathbb{Q}_p(\theta, \sqrt[p-1]{-ta})$.

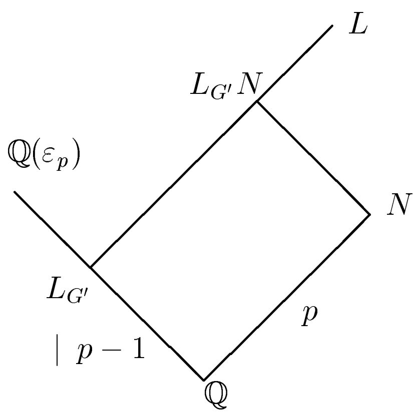
(iv) $G = S_p$ *oder* $G = \mathrm{AGL}_1(p)$.

Beweis. (i) Da h ein Eisenstein-Polynom bzgl. p ist, besteht das Newton-Polygon von h bzgl. (p, X) aus nur einer Seite mit Steigung $m = \frac{1}{p}$ und p verzweigt daher total und wild in N $(e_\wp = e = p)$.
(ii) Aufgrund der totalen Verzweigung ist $G_\mathfrak{P} = T_\mathfrak{P}$. Als auflösbare Gruppe ist $G_\mathfrak{P}$ in einer affinen Gruppe $\mathrm{AGL}_1(p)$ enthalten. Die Behauptung folgt mit Satz 2.14.
(iii) Die Behauptung folgt aus der Bemerkung nach Satz 2.14.
(iv) Die affine Gruppe von Primzahlgrad p ist eine maximale Untergruppe der vollen symmetrischen Gruppe S_p ([29], Satz 3.2.2). Damit folgt die Behauptung. □

3.12 Lemma. *Gilt $|D_0| \in \mathbb{N}^2$, so ist $D_0 > 0$.*

Beweis. Als Normalteiler der primtiven Gruppe G ist die Kommutatoruntergruppe G' von G transitiv auf der Wurzelmenge W_h ([11], II Satz 1.5). Sie enthält daher alle Elemente der Ordnung p von G. Ist $|D_0| \in \mathbb{N}^2$, so sind nach den Sätzen 3.8 und 3.9 die Trägheitsgruppen über sämtlichen Primzahlen mit Ausnahme der Primzahl p entweder die triviale Gruppe oder die zyklische Gruppe der Ordnung p. Die Kommutatorgruppe G' enthält folglich die Trägheitsgruppen aller Primideale von L, die nicht über p liegen. Der Hauptsatz der Galoistheorie liefert dann, dass im entsprechenden Fixkörper $L_{G'}$ (d.h. im maximal abelschen Teilkörper von L) nur die Primzahl p verzweigt. Da $[N : \mathbb{Q}] = p$ gilt, ist $L_{G'} \cap N = \mathbb{Q}$ oder $N \subseteq L_{G'}$. Letztere Möglichkeit entfällt, da $N|\mathbb{Q}$ nicht abelsch ist. Dann gilt aber $[L_{G'} : \mathbb{Q}] | (p-1)!$, der Grad der Erweiterung ist also insbesondere teilerfremd zu p. Nach dem Satz von Kronecker-Weber ist dieser Körper in $\mathbb{Q}(\varepsilon_{p^r})$ für ein $r \geq 1$ enthalten. Aufgrund der Teilerfremdheit des Erweiterungsgrades zu p kann man $r = 1$ wählen. Da nach dem Gaußschen Reziprozitätsgesetz $\mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}) = \mathbb{Q}(\sqrt{D_1 D_0})$ der einzig quadratische Zahlkörper in $\mathbb{Q}(\varepsilon_p)$ ist, folgt $D_0 > 0$. □

Wir haben also im Falle $|D_0| \in \mathbb{N}^2$ folgende Situation.



Im Falle $G = \mathrm{AGL}_1(p)$ ist nach Korollar 3.10 folglich $|D_0| \in \mathbb{N}^2$. Da die Ordnung der affinen Gruppe $p(p-1)$ ist und es einen Normalteiler der Ordnung p gibt, gilt also in diesem Fall $\mathbb{Q}(\varepsilon_p) = L_{G'}$ und $L = L_{G'}N$.

3.13 Satz. *Für $\mathfrak{P}|p$ enthält $L_{\mathfrak{P}}$ genau dann die p-ten Einheitswurzeln, wenn $tb \equiv 1$ mod p ist.*

Beweis. Nach Beispiel 2.4 und Satz 3.11 enthält $L_{\mathfrak{P}}$ genau dann die p-ten Einheitswurzeln, wenn

$$\mathbb{Q}_p(\sqrt[p-1]{-ta}) = \mathbb{Q}_p(\sqrt[p-1]{-p}).$$

Dies ist aber genau dann der Fall, wenn ein $c \in \mathbb{F}_p^*$ existiert mit

$$-ta = (-p)^m c^{p-1}$$

und ggT$(m, p-1)$=1. Ein p-adischer Vergleich der beiden Seiten der Gleichung liefert $m = 1$. Ferner gilt nach dem Satz von Fermat $0 \neq ta/p = c^{p-1} \equiv 1 \bmod p$. □

Bemerkung. Dieser Satz verallgemeinert [18], Lemma 4.2. Liegt $G = \mathrm{AGL}_1(p)$ vor, dann ist D_N nach Korollar 3.10 (ii) bekannt. Wegner [35] und Hasse [9] zeigen, dass im auflösbaren Fall (und unter der Annahme $L_{G'} = \mathbb{Q}(\varepsilon_p) \subseteq L$) eine ganze Zahl $b_1 \not\equiv 1$ mod p^2 mit $N = \mathbb{Q}(\sqrt[p]{b_1})$ existiert, deren Primteiler Teiler von b sind, die in $\mathbb{Q}(\theta)$ verzweigen (und damit nicht in p-ter Potenz in $\mathbb{Q}$ auftreten). Insbesondere kann also im Falle $G = \mathrm{AGL}_1(p)$ die Zahl b keine p-te Potenz in $\mathbb{Q}$ sein. Für den Zerfällungskörper L gilt ferner $L = \mathbb{Q}(\sqrt[p]{b_1}, \varepsilon_p)$.

3.14 Korollar. *Sind alle in $\mathbb{Q}(\theta)$ verzweigenden Primteiler q_i von b kongruent 1 mod p^2, so ist $G = S_p$.*

Beweis. Angenommen es gelte $G = \mathrm{AGL}_1(p)$. Dann wäre $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt[p]{b_1}$ mit $b_1 \not\equiv 1$ mod p^2 nach der Bemerkung des letzten Satzes. Damit folgt der Widerspruch zur Behauptung $(b_1 = \prod_i q_i)$. □

3.15 Satz. *Existiert ein Primteiler q von D_0 mit $q \not\equiv \pm 1$ mod p, so ist G stets die volle symmetrische Gruppe.*

Beweis. Wir nehmen an, G sei die affine Gruppe $\mathrm{AGL}_1(p)$. Dann ist wegen $D_0 \in \mathbb{N}^2$ und Satz 3.8 (a) q unverzweigt in L. Die Zerlegungsgruppe eines Primideals $\mathfrak{Q}$ über q in L besitzt ferner entweder zwei Fixpunkte auf W_h oder einen Orbit der Länge 2. Im ersten Fall folgt $G_{\mathfrak{Q}} = 1$ aus der Struktur der affinen Gruppe. Dann zerfällt q total in $\mathbb{Q}(\varepsilon_p) \subseteq L$. Daher ist $q \equiv 1 \bmod p$. Im zweiten Fall enthält $G_{\mathfrak{Q}}$ ein Produkt σ von $(p-1)/2$ disjunkten Transpositionen (und einem Fixpunkt). Die Einschränkung von σ auf $\mathbb{Q}(\varepsilon_p)$

ist der Frobenius $(q, \mathbb{Q}(\varepsilon_p)|\mathbb{Q})$ der Ordnung 2, also $q^2 \equiv 1 \bmod p$ ($q \not\equiv 1 \bmod p$) und daher $q \equiv -1 \bmod p$. □

Die bis hier gewonnenen Resultate sind unabhängig vom Parameter t. Im Folgenden spezifizieren wir den Wert von t. Wir setzen zunächst $t > 0$ voraus.

3.16 Satz. *Sei $t > 0$. Die Galoisgruppe des Polynoms $h = X^p + taX + a$ ist für negatives a stets die volle symmetrische Gruppe.*

Beweis. Das Polynom h hat einen Tiefpunkt an der Stelle $x_0 = \sqrt[p-1]{-tb}$ mit $h(x_0) = a(\frac{p-1}{p}t\sqrt[p-1]{-tb}+1) < 0$. Wir zeigen, dass h einen Hochpunkt an der Stelle $x_1 = -\sqrt[p-1]{-tb}$ mit $h(x_1) = a(-\frac{p-1}{p}t\sqrt[p-1]{-tb}+1) > 0$ hat. Dann besitzt h drei reelle Nullstellen und G kann daher nicht die affine Gruppe sein (für $x \to \pm\infty$ gilt $h(x) \to \pm\infty$). Für $t > 1$ hat h offensichtlich den gewünschten Hochpunkt. Für $t = 1$ können wir zunächst $b \in \{-1; -2\}$ aufgrund der notwendigen Annahme $b \equiv 1 \bmod p$ ausschließen (Satz 3.13). Sei also $b \leq -3$. Es gilt $(1 + \frac{1}{p-1})^{p-1} < 3$ wegen $\lim_{p\to\infty}(1 + \frac{1}{p-1})^{p-1} = e$ (=Eulersche Zahl). Also gilt $\sqrt[p-1]{-b} > \frac{p}{p-1}$ bzw. $\frac{p-1}{p}\sqrt[p-1]{-b} > 1$. Damit ist $h(x_1) > 0$ und die Behauptung folgt. □

3.17 Korollar. *Für $-1 \neq t < 0$ erhält man für positives a stets die volle symmetrische Gruppe.*

Beweis. Eine analoge Argumentation wie in Satz 3.16 führt zur Behauptung. □

3.18 Satz. *Sei $t > 0$. Ist $b = k^2t$ für ein $k \in \mathbb{Z}$, $(\mathrm{ggT}(k,p) = 1)$, dann ist $G = S_p$.*

Beweis. Wir zeigen durch Widerspruch, dass $D_0 \notin \mathbb{N}^2$ gilt. Ohne Beschränkung können wir voraussetzen, dass $k > 0$ ist. Wir nehmen also an, dass

$$D_0 = p^{p-1} + bt^p(p-1)^{p-1} = p^{p-1} + k^2t^{p+1}(p-1)^{p-1} = c^2$$

für ein $c \in \mathbb{N}$ gilt. Dann ist

$$p^{p-1} = c^2 - k^2t^{p+1}(p-1)^{p-1} = (c - kt^{\frac{p+1}{2}}(p-1)^{\frac{p-1}{2}})(c + kt^{\frac{p+1}{2}}(p-1)^{\frac{p-1}{2}})$$

mit teilerfremden Faktoren (sonst wäre der Teiler eine p-Potenz und damit $p|2c$ bzw. $p|c$, was nach Voraussetzung nicht sein kann). Da $c + kt^{\frac{p+1}{2}}(p-1)^{\frac{p-1}{2}} > 1$ ist, folgt also

$$c - kt^{\frac{p+1}{2}}(p-1)^{\frac{p-1}{2}} = 1, \tag{3.1}$$

$$c + kt^{\frac{p+1}{2}}(p-1)^{\frac{p-1}{2}} = p^{p-1}. \tag{3.2}$$

Betrachtet man die Differenz (3.2)-(3.1), so erhalten wir

$$\begin{aligned} p^{p-1} - 1 &= 2kt^{\frac{p+1}{2}}(p-1)^{\frac{p-1}{2}} \quad \text{bzw.} \\ k &= \frac{p^{p-1}-1}{2t^{\frac{p+1}{2}}(p-1)^{\frac{p-1}{2}}} \ . \end{aligned}$$

Wir setzen nun $B := \frac{p-1}{2} (\in \mathbb{N})$. Da $p \geq 5$ ist, gilt sicherlich $B \geq 2$. Für $p = 5$ oder $B = 2$ ist $k = \frac{5^4-1}{2t^{\frac{p+1}{2}} 4^2} \notin \mathbb{Z}$ für alle t. Für $B \geq 3$ erhalten wir

$$k = \underbrace{\frac{(2B+1)^{2B} - 1}{(2B)^3}}_{=:l} \cdot \frac{1}{2t^{\frac{p+1}{2}} (2B)^{B-3}} \quad .$$

Es bleibt zu zeigen, dass $l \notin \mathbb{Z}$ ist. Dann ist auch $k \notin \mathbb{Z}$ und die Annahme ($D_0 \in \mathbb{N}^2$) widerlegt, so dass wir $G = S_p$ erhalten. Es ist aber

$$\begin{aligned}
(2B+1)^{2B} - 1 &= (2B)^{2B} + (2B)(2B)^{2B-1} + \binom{2B}{2}(2B)^{2B-2} + \cdots \\
&\quad + \binom{2B}{2B-2}(2B)^2 + (2B)(2B) \\
&= (2B)^2 \left[(2B)^{2B-2} + (2B)^{2B-3} + \cdots + \frac{2B(2B-1)}{2} + 1 \right] \\
&\equiv (2B)^2 \left[\frac{2B(2B-1)}{2} + 1 \right] \\
&\equiv (2B)^2 [2B^2 - B + 1] \\
&\not\equiv 0 \mod (2B)^3,
\end{aligned}$$

denn sonst wäre $\frac{2B^2-B+1}{2B} = B - \frac{1}{2} + \frac{1}{2B} \in \mathbb{Z}$, was nicht möglich ist. Damit folgt die Behauptung. □

Bemerkung. Dieser Satz verallgemeinert das Resultat von Komatsu ([13], Theorem 3) auf beliebige $t > 0$ (statt $t = 1$).

Wählen wir nun $t \in 2\mathbb{Z} + 1$ als ungerade, so können wir folgendes Resultat gewinnen.

3.19 Satz. *Für ungerades a und ungerades t gilt stets $G = S_p$.*

Beweis. Wir nehmen an, dass $G = \mathrm{AGL}_1(p)$ ist. Wegen $h' = pX^{p-1} + ta$ ist $ph - Xh' = (p-1)taX + tap \equiv 1 \mod 2$ der größte gemeinsame Teiler von h und h' mod 2. Das Polynom $h \bmod 2 = X^p + X + 1$ ist daher separabel über $\mathbb{F}_2$, es hat zudem keine Wurzel in $\mathbb{F}_2$. Jede Permutation in $G = \mathrm{AGL}_1(p)$ ohne Fixpunkt ist aber ein p-Zykel. Dann ist $h \bmod 2$ irreduzibel über $\mathbb{F}_2$. Wegen $G = \mathrm{AGL}_1(p)$ enthält L den Körper $\mathbb{Q}(\varepsilon_p)$ und die Polynome $h_0 = h \cdot \Phi_p$ und h haben denselben Zerfällungskörper. Über $\mathbb{F}_2$ zerfällt Φ_p in paarweise verschiedene Primfaktoren des Grades $o(2 \bmod p) > 1$ ($2 \not\equiv 1 \mod p$), der ein Teiler von $p-1$ ist ([6], VI (1.12)). Betrachtet man G ($\supseteq G_{\mathfrak{P}}$) als Galoisgruppe von h_0, so existiert in ihr ein Element der Ordnung $\mathrm{kgV}(p, o(2 \bmod p)) = p \cdot o(2 \bmod p) > p$, was nach dem Satz von Fermat nicht möglich ist. Die Behauptung folgt. □

Mit weiteren Einschränkungen an den Parameter t lassen sich entsprechend obigem Beweis weitere Aussagen treffen, wann die Galoisgruppe die volle symmetrische Gruppe ist, so etwa der folgende

3.20 Satz. *Sei $t \equiv 1 \bmod 3$ und $a \equiv 2 \bmod 3$. Dann folgt $G = S_p$.*

Beweis. Wegen $\mathrm{ggT}(h, h') \bmod p = (p-1)taX + pta$ und da das Polynom $h \bmod 3 = X^p - X - 1$ keine Wurzel in $\mathbb{F}_3$ hat, ist $h \bmod 3$ separabel über $\mathbb{F}_3$. Angenommen, es gilt $G = \mathrm{AGL}_1(p)$, dann ist $h \bmod 3$ irreduzibel (jede Permutation in $G = \mathrm{AGL}_1(p)$ ohne Fixpunkt ist ein p-Zykel; analoge Argumentation wie in Satz 3.19). Da für die Ordnung $o(3 \bmod p) > 1$ gilt, folgt auch hier die Existenz eines Elements in $G = \mathrm{Gal}_{\mathbb{Q}}(h \cdot \Phi_p)$ der Ordnung $> p$, was nicht möglich ist. □.

3.21 Satz. *Wir betrachten den Fall $t = 1$, d.h. $h = X^p + aX + a$.*

(i) Für $p \equiv 2 \bmod 3$ und $a \equiv 1 \bmod 3$ ist $G = S_p$.

*(ii) Für $p \equiv 3 \bmod 4$ und $a \equiv 3 \bmod 5$ folgt $G = S_p$.
Ist $p \equiv 3 \bmod 5$ und $a \equiv 2 \bmod 5$, so gilt ebenfalls $G = S_p$.*

(iii) Ist q ein Teiler von D_0 und das mod q separable Polynom $\psi = X^{p-2} + 2X^{p-3} + 3X^{p-4} + \cdots + (p-2)X + (p-1)$ zerfällt über $\mathbb{F}_q$ nicht in $p-2$ verschiedene Linearfaktoren oder bis auf einen Linearfaktor in Primpolynome vom Grad 2, so ist die Galoisgruppe von h die volle symmetrische Gruppe. (Zusatz: Für $a = p(1 + kp), k \in \mathbb{N}$ gilt dies auch für alle $k \equiv \frac{-p^{p-2}}{(p-1)^{p-1}} - \frac{1}{p} \bmod q$).

(iv) Existiert eine Primzahl q, so dass $h \bmod q$ nicht in verschiedene Linearfaktoren zerfällt, irreduzibel ist oder bis auf einen Linearfaktor in verschiedene irreduzible Polynome gleichen Grades zerfällt, dann ist $G = S_p$.

Beweis. (i) Es ist $D_0 = p^{p-1} + b(p-1)^{p-1} \equiv 1 + b \equiv 0 \bmod 3$ und $3 \not\equiv \pm 1 \bmod p$ $(p \neq 2)$. Die Behauptung folgt mit Satz 3.15.
(ii) Im ersten Fall hat $h \equiv X^p + 3X + 3 \equiv X^3 + 3X + 3 \bmod 5$ keine Wurzel in $\mathbb{F}_5$ und unter der Annahme $G = \mathrm{AGL}_1(p)$ ist daher $h \bmod 5$ irreduzibel über $\mathbb{F}_5$. Eine analoge Argumentation wie im Beweis von Satz 3.19 (und Satz 3.20) liefert wegen $o(5 \bmod p) > 1$ den Widerspruch zur Annahme und die Behauptung folgt. Im zweiten Fall gilt $D_0 \equiv 1 + b \equiv 1 + 2 \cdot 3^{-1} \equiv 0 \bmod 5$, $5 \not\equiv \pm 1 \bmod p$ $(p > 3)$ und die Behauptung folgt nach Satz 3.15.
(iii) Es gilt genau dann $q | D_0 = p^{p-1} + \frac{a}{p}(p-1)^{p-1}$, wenn $\frac{a}{p} \equiv \frac{-p^{p-1}}{(p-1)^{p-1}}$ oder $k \equiv \frac{-p^{p-1}}{(p-1)^{p-1}} - \frac{1}{p}$ mod q ist. Der Beweis von Satz 3.8 zeigt, dass $h \equiv (X + \frac{p}{p-1})^2 \cdot \tilde{h} \bmod q$, wobei

$\tilde{h} \equiv X^{p-2} - 2(\frac{p}{p-1})X^{p-3} + 3(\frac{p}{p-1})^2 X^{p-4} - + \cdots - (p-1)(\frac{p}{p-1})^{p-2} \bmod q$ unabhängig von D_0 ist. Setzen wir $u := \frac{p}{p-1}$ und betrachten das Polynom $\psi(X) := \frac{\tilde{h}(-uX)}{-u^{p-2}}$, so ist ψ das im Satz erwähnte Polynom. Die Behauptung folgt bei Betrachtung der möglichen Permutationen von $G = \mathrm{AGL}_1(p)$.
(iv) Wie in (iii) existiert dann ein Zykel in G, der kein Element der affinen Gruppe sein kann. □

Wir können nun die bisherigen Ergebnisse zu dem in der Einleitung formulierten Satz zusammenfassen.

3.22 Satz. *Die Galoisgruppe G des Eisenstein-Polynoms $h = X^p + aX + a$ ist die volle symmetrische Gruppe, falls eine der folgenden Aussagen gilt ($a = pb$, $ggT(p, b) = 1$):*

(i) $D_0 = p^{p-1} + b(p-1)^{p-1}$ ist kein (positives ganzrationales) Quadrat.

(ii) Es gibt ein Primteiler q von D_0 mit $q \not\equiv \pm 1 \bmod p$.

(iii) Die ganze Zahl b ist ein Quadrat oder eine p-te Potenz in $\mathbb{Q}$; b ist ungerade, $b \not\equiv 1 \bmod p$ oder $b \leq p$.

(iv) Alle Primteiler q von b, die in $N = \mathbb{Q}(\theta)$ verzweigen ($\mathrm{ggT}(p, v_q(b)) = 1$) sind kongruent 1 mod p^2.

(v) $a \equiv 2$ mod 3 oder $a \equiv 1$ mod 3 und $p \equiv 2$ mod 3. □

Bemerkung. Aus Satz 3.21 (i) und (ii) wird deutlich, dass man beliebig weitere Bedingungen für $G = S_p$ konstruieren kann. Um $G = S_p$ für alle a und p zu zeigen, genügt es nach Satz 3.21 (iv) eine Primzahl q zu finden, die a nicht teilt und so dass die Reduktion $h \bmod q$ keine Wurzel in $\mathbb{F}_q$ hat und nicht irreduzibel (über $\mathbb{F}_q$) ist. Dann kann der Frobenius eines Primideals $\mathfrak{Q}|q$ von L nicht zur affinen Gruppe gehören. Nehmen wir zusätzlich $q \equiv 1 \bmod p$ an, so genügt es, dass $h \bmod q$ lediglich weder in Linearfaktoren zerfällt noch irreduzibel über $\mathbb{F}_q$ ist.

Im Anhang werden wir zeigen, dass für alle p und $a < 10^9$ die Galoisgruppe des Polynoms $h = X^p + aX + a$ stets die volle symmetrische Gruppe ist. Dabei bleibt nach den bisherigen Aussagen eine überschaubare Anzahl von Ausnahmen zu betrachten.

3.23 Beispiel. Sei $p = 5$ und $q|D_0 \in \mathbb{N}^2$ mit $q \equiv \pm 1 \bmod 5$. Dann ist $\psi(X) = X^3 + 2X^2 + 3X + 4$ und $D_\psi = -200 = -2^3 5^2$. Nach Swan ([30], Corollary 1) ist $D_\psi \in \mathbb{F}_q^2$ genau dann, wenn ψ irreduzibel ist oder in Linearfaktoren zerfällt mod q. Dies ist genau dann der Fall, wenn $-2 \in \mathbb{F}_q^2$ oder

$$\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = 1,$$

also genau dann, wenn $q \equiv 1$ oder 3 mod 8 ist. Wegen $p - 1 = 2^2$ und $p \equiv 1$ mod 4 gilt $\left(\frac{p-1}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\left(\frac{\pm 1}{q}\right) = 1$. Genau in diesem Fall ist also auch

$$\left(\frac{-2D_0 p(p-1)q^{-v_q(D_0)}}{q}\right) = \left(\frac{-2p(p-1)}{q}\right) = \left(\frac{-2}{q}\right)\left(\frac{p}{q}\right)\left(\frac{p-1}{q}\right) = \left(\frac{-2}{q}\right) = 1.$$

Ist also $\mathfrak{Q}$ ein über q liegendes Primideal in L, so besitzt die Zerlegungsgruppe $G_{\mathfrak{Q}}$ entweder einen Dreierzykel und zwei Fixpunkte oder fünf Fixpunkte, falls $q \equiv 1$ oder 3 mod 8 ist. Im Falle $q \equiv -1$ oder -3 mod 8 besitzt sie ein Produkt von zwei Transpositionen und einem Fixpunkt (vgl. Satz 3.8).

3.3 Polynome der Form $h(X) = X^n + aX^{n-2} + b$ und $h(X) = X^n + aX^2 + b$

Wir wollen nun abschließend noch konkrete Berechnungen für Galoisgruppen $G = \mathrm{Gal}_{\mathbb{Q}}(h)$ von über $\mathbb{Q}$ irreduziblen Trinomen der Form $h(X) = X^n + aX^{n-2} + b$ und $h(X) = X^n + aX^2 + b$ durchführen. Wir betrachten zunächst den Fall, dass das Newton-Polygon von h bzgl. (p, X) nicht vollständig oberhalb der $x-$Achse liegt.

3.24 Satz. *Sei $h(X) = X^n + aX^2 + b \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$ und p eine Primzahl mit $v_p(b) > v_p(a) = 0$.*

(i) Gilt $n = q$ für eine Primzahl q, $\mathrm{ggT}(p, q-2) = 1$ und $v_p(b) \equiv 1$ mod 2, so ist $G = S_q$.

(ii) Gilt n ungerade, $n-2$ ist eine p-Potenz, $v_p(b) \equiv 1$ mod 2 und $v_p(h(-a)) = 1$, so ist $G = S_n$.

Für $p \geq 3$ existiert eine Wurzel $\theta \in W_h$ mit $\mathbb{Q}_p(\theta) = \mathbb{Q}_p(\sqrt{-ba^{-1}})$.

Beweis. (i) Es gelten die üblichen Bezeichnungen. Ferner bezeichne t die Anzahl der über l liegenden Primideale in $\mathbb{Q}(\theta)$. Die Primfaktorzerlegung von h über $\mathbb{F}_p$ ist

$$h(X) = X^q + aX^2 + b \equiv X^2(X^{q-2} + a) \mod p.$$

Über $\mathbb{Q}_p$ gilt also die Faktorisierung $h = \hat{h}_1 \cdot \hat{h}_2$ mit $\hat{h}_1 \equiv X^2$ mod p und $\hat{h}_2$ separabel und teilerfremd zu $\hat{h}_1$. Das Newton-Polygon von h bzgl. (p, X) besitzt die Eckpunkte $(0,0)$, $(q-2, 0)$ und $(q, v_p(b))$. Das der Seite S_m (mit positiver Steigung) zugeordnete Polynom ist linear und nach Hauptsatz 2.2 verzweigt das über p liegende und zu S_m gehörende Primideal $\wp_1$ total in $\mathbb{Q}(\theta)_{\wp_1}$, so dass $e_{\wp_1} = 2$ und $e_{\wp_i} = 1$ $(i = 2, ..., t)$ wegen der Separabilität von $\hat{h}_2$. Ist $\mathfrak{P}$ ein über p liegendes Primideal in L, so enthält die Trägheitsgruppe $T_{\mathfrak{P}}$ (und damit G) eine Transposition. G ist als transitive Gruppe von Primzahlgrad primitiv und

die Behauptung folgt.
(ii) Die Primfaktorzerlegung über $\mathbb{F}_p$ ist

$$h(X) = X^n + aX^2 + b \equiv X^2(X^{n-2} + a) \equiv X^2(X+a)^{n-2} \mod p.$$

Wie wir im Beweis von Satz 3.4 (i) gezeigt haben, gilt für die Primidealzerlegung von p in $\mathbb{Q}(\theta)$

$$p_{\mathbb{Q}(\theta)} = \wp_1^2 \; \wp_2^{n-2}.$$

Die Galoisgruppe enthält wegen $n \equiv 1 \mod 2$ folglich eine Transposition. Da G primitiv ist, folgt $G = S_n$.
Für $p \geq 3$ verzweigt p zahm in $\mathbb{Q}(\theta)_{\wp_1}$ $(e_{\wp_1} = 2)$ und der Faktor zu dieser Seite ist $h_m = X^2 + ba^{-1}$. Nach Hauptsatz 2.2 (c) existiert daher eine Wurzel $\theta \in W_h$ mit $\mathbb{Q}_p(\theta) = \mathbb{Q}_p(\sqrt{-ba^{-1}})$. □

3.25 Satz. *Sei $h(X) = X^n + aX^{n-2} + b \in \mathbb{Q}[X]$ ein über $\mathbb{Q}$ irreduzibles Polynom mit $v_2(b) > v_2(a) = 0$ und $v_2(h(-1)) = 1$. Ferner sei $d :=$ ggT$(n-2, v_2(b))$.*

(i) Ist $n = q$ für eine Primzahl q (≥ 3), so gilt $G = S_q$.

(ii) Ist n ungerade und $d = 1$, so gilt $G = S_n$.

Beweis. Es sei wie üblich $\theta \in W_h$ und $\wp$ ein Primideal über 2 in $\mathbb{Q}(\theta)$. Nach Voraussetzung gilt

$$h(X) = X^n + aX^{n-2} + b \equiv X^{n-2}(X^2+1) \equiv X^{n-2}(X+1)^2 \mod 2.$$

Das Newton-Polygon $(2, X)$ besitzt die Eckpunkte $(0,0)$, $(2,0)$ und $(n, v_2(b))$. Das der Seite S_m $(m > 0)$ zugeordnete Polynom ist $h_S(X) = X^d + \frac{b}{2^{v_2(b)}}$, welches separabel mod 2 ist (d ist ungerade). Das Newton-Polygon $(2, X+1)$ besitzt wegen

$$h(X-1) = h(-1) + h'(-1)X + \frac{h''(-1)}{2}X^2 + \cdots + X^n \equiv X^2(X-1)^{n-2} \mod 2$$

die Eckpunkte $(0,0)$, $(n-2, 0)$ und $(n, v_2(h(-1)))$, wobei das der Seite mit positiver Steigung zugeordnete Polynom linear ist $(v_2(h'(-1)) \geq 1)$. Folglich gilt

$$2_{\mathbb{Q}(\theta)} = \wp_1^2 \wp_2^l \cdots \wp_t^l$$

mit $l := \frac{n-2}{d} \equiv 1 \mod 2$. Die Galoisgruppe G enthält also eine Transposition. Im Fall (i) folgt die Primitivität aufgrund des Primzahlgrades von h, im Fall (ii) mit Hilfe von Satz 3.4 (iii). Die Behauptung folgt. □

Wir betrachten nun abschließend den Fall, dass das zweiseitige Newton-Polygon bzgl. (p, X) aus Seiten mit ausschließlich positiven Steigungen besteht.

3.26 Satz. *Es sei $h(X) = X^n + aX^{n-2} + b \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$ mit $0 < v_p(a) \equiv 1$ mod 2 und $v_p(ba^{-1}) > \frac{n}{2}$. Ferner sei $d := \mathrm{ggT}(n-2, v_p(ba^{-1}))$.*

(i) Ist $n = q$ für eine Primzahl q (≥ 3) und p kein Teiler von d, dann gilt $G = S_q$.

(ii) Ist n ungerade und $d = 1$, so ist $G = S_n$.

Es existiert ferner eine Wurzel $\theta \in W_h$, so dass $\mathbb{Q}_p(\theta) = \mathbb{Q}_p(\sqrt{-a})$.

Beweis. Es seien $\wp_i$ die Primideale über p in $\mathbb{Q}(\theta)_{\wp_i}$. Aufgrund der Voraussetzung gilt

$$h(X) \equiv X^n \mod p.$$

Das Newton-Polygon (p, X) von h besteht aus den zwei Seiten S_1 bzw. S_2 mit den Eckpunkten $(0,0)$ und $(2, v_p(a))$ bzw. $(2, v_p(a))$ und $(n, v_p(b))$. Das der Seite S_1 zugeordnete Polynom ist linear, jenes der Seite S_2 zugeordnete

$$h_{S_2}(X) = X^d + \frac{b}{ap^{v_p(ba^{-1})}}.$$

Das Polynom h_{S_2} ist separabel mod p ($\mathrm{ggT}(p,d)$=1). Über $\mathbb{Q}_p$ läßt sich h als Produkt zweier Polynome $\hat{h}_{m_i}$ $(i = 1, 2)$ schreiben, also

$$h = \hat{h}_{m_1} \cdot \hat{h}_{m_2}$$

mit $\mathrm{grd}(\hat{h}_{m_1}) = 2$ und $\mathrm{grd}(\hat{h}_{m_2}) = n - 2$. Wegen $\mathrm{ggT}(v_p(a), 2) = 1$ ist das Polynom $\hat{h}_{m_1}$ irreduzibel über $\mathbb{Q}_p$. Der zu S_{m_1} gehörende Faktor ist $h_{m_1} = X^2 + a$. Gehört $\wp_1$ zur ersten Seite S_{m_1}, so verzweigt $\wp_1$ nach Hauptsatz 2.2 total in $\mathbb{Q}_p(\theta) = \mathbb{Q}_p(\sqrt{-a})$ (für eine Wurzel $\theta \in W_{\hat{h}_{m_1}}$). Es gilt also $e(\wp_1|p) = 2$. Die der Seite S_{m_2} zugeordneten Primideale $\wp_i$ haben nach Hauptsatz 2.2 den Verzweigungsindex $e(\wp_i|p) = \frac{n-2}{d} =: l$ und für die Primidealzerlegung von p in $\mathbb{Q}(\theta)$ gilt

$$p_{\mathbb{Q}(\theta)} = \wp_1^2 \ \wp_2^l \cdots \wp_t^l$$

mit $\sum_{i=2}^t f_{\wp_i} = d$. Ist $\mathfrak{P}$ ein Primideal in L über p, dann enthält die Zerlegungsgruppe $G_{\mathfrak{P}}$ folglich ein Produkt von l -Zykeln mit einer Transposition und damit eine Transposition (l ist ungerade).

(i) Als transitive Gruppe von Primzahlgrad ist G primitiv und damit die volle symmetrische Gruppe.

(ii) Da n ungerade ist, gilt $\mathrm{ggT}(2, n(n-2)v_p(a)) = 1$. Nach Satz 3.5 (i) ist G primitiv und die Behauptung folgt. Die Zusatzbemerkung folgt aus Hauptsatz 2.2 (c) aufgrund der zahmen Verzweigung des Primideals $\wp_1$ im entsprechenden Wurzelkörper. □

3.27 Korollar. *Es sei $h(X) = X^n + aX^2 + b \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$ mit ungeradem $v_p(ba^{-1}) > 1 + \frac{2}{n-2}$, ($v_p(a) > 0$). Ferner sei $d := \mathrm{ggT}(v_p(a), n-2)$.*

(i) Ist $n = q$ für eine Primzahl q (≥ 3) und p kein Teiler von d, dann ist $G = S_q$.

(ii) Ist n ungerade und $d = 1$, dann ist $G = S_n$.

Es existiert eine Wurzel $\theta \in W_h$ mit $\mathbb{Q}_p(\theta) = \mathbb{Q}_p(\sqrt{ba^{-1}})$.

Beweis. Das Newton-Polygon bzgl. (p, X) besitzt die Eckpunkte $(0,0)$, $(n-2, v_p(a))$ und $(n, v_p(b))$. Es ist h_{S_2} linear und

$$h_{S_1}(X) = X^d + \frac{a}{p^{v_p(a)}}$$

separabel mod p. Ferner ist $h_{m_2} = X^2 + ba^{-1}$ und damit $\mathbb{Q}_p(\theta) = \mathbb{Q}_p(\sqrt{ba^{-1}})$ für eine Wurzel $\theta \in W_{\hat{h}_{m_2}}$ (Hauptsatz 2.2 (c)). Analog zum Beweis von Satz 3.26 erhalten wir

$$p_{\mathbb{Q}(\theta)} = \wp_1^2 \wp_2^l \cdots \wp_t^l$$

mit $l = \frac{n-2}{d}$ und G enthält damit eine Transposition. Die Primitivität von G folgt in (i) wegen $n = q$ (q eine Primzahl) und in (ii) wegen $\mathrm{ggT}(n-2, 2nv_p(a)) = 1$ mit Hilfe von Satz 3.5 (i). $\square$

Anhang

Wir zeigen im Folgenden, dass für alle $a < 10^9$ die Galoisgruppe des Eisenstein-Trinoms $h = X^p + aX + a$ (bzgl. der Primzahl p) stets die volle symmetrische Gruppe ist. Für $p \geq 11$ existiert kein $a < 10^9$, so dass D_0 ein ganzrationales Quadrat ist[1]. Im Folgenden sind für $p = 5$ alle möglichen $a < 10^9$ mit $D_0 \in \mathbb{N}^2$, $a/5 \equiv 1 \bmod 5$ und $a \equiv 0 \bmod 6$ aufgelistet, für die für jeden Primteiler q von D_0 gilt $q \equiv \pm 1 \bmod 5$. Ferner werden für $p = 5$ nur diejenigen a betrachtet, für die das Polynom $X^3 + 2X^2 + 3X + 4$ modulo jeden Primteilers von D_0 kein irreduzibles Polynom ist (Sätze 3.15, 3.20 und 3.21 (i) und (iii)).

Entsprechend den Sätzen 3.15 und 3.21 (iii) sind für $p = 7$ alle $a < 10^9$ mit $D_0 \in \mathbb{N}^2$, $a/7 \equiv 1 \bmod 7$ aufgeführt, wobei für jeden Primteiler q von D_0 gilt $q \equiv \pm 1 \bmod 7$. Die Reduktion des Polynoms $X^5 + 2X^4 + 3X^3 + 4X^2 + 5X + 6$ modulo jeden Primteilers von D_0 zerfällt ferner in Linearfaktoren oder in drei Primpolynome, wobei zwei quadratisch und einer linear ist.

In den unten angeführten Tabellen bezeichnet PFZ die Primfaktorzerlegung einer ganzen Zahl, angegebene Faktorisierungen von Polynomen sind irreduzibel und die Behauptung für $p = 5$ und $p = 7$ folgt stets aus Satz 3.21 (iv).

p	a	PFZ von D_0	Begründung für $G = S_p$
5	1530	281^2	$h \bmod 31 = (X^3 + 28X^2 + 17X + 18)(X + 10)(X + 24)$
	44580	1511^2	$h \bmod 11 = (X + 5)(X + 8)(X^3 + 9X^2 + 8X + 9)$
	152130	2791^2	$h \bmod 7 = (X^3 + X^2 + 5X + 2)(X^2 + 6X + 3)$
	247380	3559^2	$h \bmod 13 = (X^3 + 2X^2 + 9X + 2)(X^2 + 11X + 8)$
	559230	5351^2	$h \bmod 17 = (X^3 + 16X^2 + 12X + 11)(X^2 + X + 6)$
	743280	$31^2 199^2$	$h \bmod 7 = (X^3 + X^2 + 5X + 2)(X^2 + 6X + 3)$
	2467080	11239^2	$h \bmod 13 = (X^3 + 4X^2 + X + 9)(X^2 + 9X + 2)$
	3718980	13799^2	$h \bmod 7 = (X^3 + X^2 + 5X + 2)(X^2 + 6X + 3)$
	5258880	$61^2 269^2$	$h \bmod 13 = (X^3 + 2X^2 + 9X + 2)(X^2 + 11X + 8)$

[1]Dies wurde mit dem Programm Maple 7 berechnet. Dazu genügt es wegen $0 < a/p \equiv 1 \bmod p$ und $\mathrm{Gal}_{\mathbb{Q}}(X^p + pX + p) = S_p$ ([13], Theorem 4) alle p mit $p(1+p) < 10^9$, d.h. $p < 31622$ zu betrachten.

p	a	PFZ von D_0	Begründung für $G = S_p$
5	5559180	16871^2	h mod 13=$(X^3+2X^2+9X+2)(X^2+11X+8)$
	6990780	18919^2	h mod 7=$(X^3+X^2+5X+2)(X^2+6X+3)$
	9052680	21529^2	h mod 23=$(X+16)(X^2+19X+17)(X+6)(X+5)$
	9445380	21991^2	h mod 103=$(X^3+21X^2+7X+97)(X^2+82X+22)$
	11772480	24551^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	17194680	29671^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	18096330	$61^2 499^2$	h mod 13=$(X^2+9X+2)(X^3+4X^2+X+9)$
	18770730	$29^2 1069^2$	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	19712280	31769^2	h mod 11=$(X+10)(X+3)(X^3+9X^2+7X+2)$
	21268230	32999^2	h mod 11=$(X+10)(X+3)(X^3+9X^2+7X+2)$
	28380030	38119^2	h mod 11=$(X+8)(X+5)(X^3+9X^2+8X+9)$
	34385880	41959^2	h mod 17=$(X^2+16X+10)(X^3+X^2+8X+15)$
	35313180	$101^2 421^2$	h mod 17=$(X^2+X+6)(X^3+16X^2+12X+11)$
	38709780	44519^2	h mod 13=$(X^2+9X+2)(X^3+4X^2+X+9)$
	44236380	47591^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	45770130	48409^2	h mod 13=$(X^2+11X+8)(X^3+2X^2+9X+2)$
	46647930	48871^2	h mod 13=$(X^2+6X+4)(X^3+7X^2+6X+1)$
	48125580	49639^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	51663030	51431^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	54266580	52711^2	h mod 11=$(X+10)(X+3)(X^3+9X^2+7X+2)$
	55859430	53479^2	h mod 13=$(X^2+11X+8)(X^3+2X^2+9X+2)$
	61335330	56039^2	h mod 13=$(X^2+6X+4)(X^3+7X^2+6X+1)$
	65433780	57881^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	70029180	59879^2	h mod 19=$(X+2)(X+10)(X^3+7X^2+10X+6)$
	71231880	$131^2 461^2$	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	79299030	63719^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	80578530	64231^2	h mod 23=$(X^2+10X+5)(X^3+13X^2+3X+20)$
	87129630	66791^2	h mod 11=$(X+10)(X+3)(X^3+9X^2+7X+2)$
	89144880	67559^2	h mod 7=$(X^2+6x+3)(X^3+X^2+5X+2)$
	90501180	68071^2	h mod 13=$(X^2+11x+8)(X^3+2X^2+9X+2)$
	99566730	71399^2	h mod 13=$(X^2+11x+8)(X^3+2X^2+9X+2)$
	103168680	72679^2	h mod 7=$(X^2+6x+3)(X^3+X^2+5X+2)$
	108318930	74471^2	h mod 7=$(X^2+6x+3)(X^3+X^2+5X+2)$
	110564580	75239^2	h mod 11=$(X+10)(X+3)(X^3+9X^2+7X+2)$
	114358530	76519^2	h mod 7=$(X^2+6x+3)(X^3+X^2+5X+2)$
	119777580	78311^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	134450280	$29^2 2861^2$	h mod 7=$(X^2+6x+3)(X^3+X^2+5X+2)$

p	a	PFZ von D_0	Begründung für $G = S_p$
5	135951780	83431^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	138466230	84199^2	h mod 17$=(X^2+10X+1)(X+3)(X+8)(X+13)$
	140320830	84761^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	144422880	85991^2	h mod 11$=(X+8)(X+5)(X^3+9X^2+8X+9)$
	160315980	90599^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	174193830	94439^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	174378330	$61^2 1549^2$	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	176087730	94951^2	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	181055280	96281^2	h mod 13$=(X^2+11X+8)(X^3+2X^2+9X+2)$
	185710830	97511^2	h mod 11$=(X+8)(X+5)(X^3+9X^2+8X+9)$
	185901330	97561^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	193593630	99559^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	200823480	$31^2 3271^2$	h mod 17$=(X^2+X+6)(X^3+16X^2+12X+11)$
	203877030	$71^2 1439^2$	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	205725030	$29^2 3539^2$	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	208815480	103399^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	230219280	$151^2 719^2$	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	235465230	$59^2 1861^2$	h mod 17$=(X^2+X+6)(X^3+16X^2+12X+11)$
	237666330	110311^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	243431880	111641^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	249045930	112921^2	h mod 13$=(X^2+11X+8)(X^3+2X^2+9X+2)$
	266272080	$59^2 1979^2$	h mod 11$=(X+8)(X+5)(X^3+9X^2+8X+9)$
	269556930	$29^2 4051^2$	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	271911630	117991^2	h mod 13$=(X^2+11X+8)(X^3+2X^2+9X+2)$
	278076180	119321^2	h mod 11$=(X+8)(X+5)(X^3+9X^2+8X+9)$
	283838730	120551^2	h mod 17$=(X^2+X+6)(X^3+16X^2+12X+11)$
	293564730	122599^2	h mod 11$=(X+8)(X+5)(X^3+9X^2+8X+9)$
	296262330	$79^2 1559^2$	h mod 17$=(X^2+X+6)(X^3+16X^2+12X+11)$
	331496430	130279^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	340678680	132071^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	347314230	133351^2	h mod 13$=(X^2+11X+8)(X^3+2X^2+9X+2)$
	351326280	$71^2 1889^2$	h mod 11$=(X+8)(X+5)(X^3+9X^2+8X+9)$
	354276780	134681^2	h mod 19$=(X+2)(X+10)(X^3+7X^2+10X+6)$
	360777330	135911^2	h mod 13$=(X^2+6X+4)(X^3+7X^2+6X+1)$
	367604880	137191^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	374766930	$71^2 1951^2$	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	381451980	$29^2 61^2 79^2$	h mod 11$=(X+8)(X+5)(X^3+9X^2+8X+9)$

p	a	PFZ von D_0	Begründung für $G = S_p$
5	395833080	$29^2 4909^2$	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	424817280	147481^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	428963730	148199^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	431932830	148711^2	h mod 13$=(X^2+6X+4)(X^3+7X^2+6X+1)$
	439693380	150041^2	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	444206130	$239^2 631^2$	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	447227430	389^4	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	451481580	152039^2	h mod 13$=(X^2+6X+4)(X^3+7X^2+6X+1)$
	459115530	153319^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	490600830	158489^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	501444780	160231^2	h mod 13$=(X^2+9X+2)(X^3+4X^2+X+9)$
	506263230	$131^2 1229^2$	h mod 13$=(X^2+9X+2)(X^3+4X^2+X+9)$
	509803830	161561^2	h mod 11$=(X+5)(X+8)(X^3+9X^2+8X+9)$
	514662180	$271^2 599^2$	h mod 17$=(X^2+X+6)(X^3+16X^2+12X+11)$
	517595880	162791^2	h mod 19$=(X+14)(X+15)(X^3+9X^2+4X+15)$
	525767430	164071^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	530701080	164839^2	h mod 11$=(X+5)(X+8)(X^3+9X^2+8X+9)$
	542302530	166631^2	h mod 13$=(X^2+11X+8)(X^3+2X^2+9X+2)$
	547639980	167449^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	550666080	167911^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	572710830	$109^2 1571^2$	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	581304780	172519^2	h mod 13$=(X^2+6X+4)(X^3+7X^2+6X+1)$
	593443830	174311^2	h mod 13$=(X^2+9X+2)(X^3+4X^2+X+9)$
	598684680	175079^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	619878480	178151^2	h mod 23$=(X^2+6X+10)(X^3+17X^2+3X+19)$
	661530330	184039^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	674475780	185831^2	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	683799330	187111^2	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	699219630	$431^2 439^2$	h mod 13$=(X^2+9X+2)(X^3+4X^2+X+9)$
	702638430	189671^2	h mod 17$=(X+13)(X+3)(X+8)(X^2+10X+1)$
	722109030	$59^2 3259^2$	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	727888980	$71^2 2719^2$	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	737573430	$29^2 6701^2$	h mod 7$=(X^2+6X+3)(X^3+X^2+5X+2)$
	776561730	199399^2	h mod 13$=(X^2+7X+7)(X^3+6X^2+3X+2)$
	786955680	$181^2 1109^2$	h mod 11$=(X+10)(X+3)(X^3+9X^2+7X+2)$
	800673930	202471^2	h mod 13$=(X^2+6X+4)(X^3+7X^2+6X+1)$
	817353030	$31^2 6599^2$	h mod 23$=(X^2+6X+10)(X^3+17X^2+3X+19)$

p	a	PFZ von D_0	Begründung für $G = S_p$
5	821049030	205031^2	h mod 17=$(X^2+3X+1)(X^3+14X^2+8X+13)$
	837533430	207079^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	848326380	208409^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	858369330	209639^2	h mod 11=$(X+10)(X+3)(X^3+9X^2+7X+2)$
	900809130	214759^2	h mod 17=$(X+13)(X+3)(X+8)(X^2+10X+1)$
	915904980	216551^2	h mod 13=$(X^2+11X+8)(X^3+2X^2+9X+2)$
	922413030	217319^2	h mod 23=$(X^2+10X+5)(X^3+13X^2+3X+20)$
	933310980	218599^2	h mod 11=$(X+5)(X+8)(X^3+9X^2+8X+9)$
	948675630	220391^2	h mod 17=$(X^2+16X+10)(X^3+X^2+8X+15)$
	955298880	221159^2	h mod 11=$(X+5)(X+8)(X^3+9X^2+8X+9)$
	955730880	221209^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	959727180	221671^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	971278230	269^2829^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
	988760730	71^23169^2	h mod 7=$(X^2+6X+3)(X^3+X^2+5X+2)$
7	11909065	281737^2	h mod 17=$(X+12)(X+9)(X+6)(X^4+7X^3+2X^2+6X+2)$
	13635090	301463^2	h mod 11=$(X^2+9X+10)(X^2+X+6)(X^3+X^2+9X+8)$
	265993420	1331497^2	h mod 13=$(X^3+2X^2+5X+2)(X^4+11X^3+12X^2+10X+2)$
	304581704	1424809^2	h mod 23=$(X+8)(X+14)(X^5+X^4+4X^3+7X^2+19X+17)$
	508569684	1841111^2	h mod 11=$(X^2+9X+10)(X^2+X+6)(X^3+X^2+9X+8)$

Nach Movahhedi [18] existieren für alle p unendlich viele a, so dass $D_0 \in \mathbb{N}^2$. Insbesondere liefert

$$a = p(r^2(p-1)^{p-1} + 2rp^{\frac{p-1}{2}}), \quad r \in \mathbb{Z}$$

stets ein solches D_0. Mit der Bedingung $b \equiv 1 \bmod p$ bleiben die Fälle $r \equiv \pm 1 \bmod p$ zu betrachten. Die folgenden Tabellen liefern für die Primzahlen 11, 13, 17, 19 und 23 mit den ersten 10 möglichen Werten für r weitere Beispiele für $G = S_p$. Die Zahlenangaben in der letzten Spalte geben die Reduktion bzgl. eines Primteilers q von D_0 sowie die Grade der mod q irreduziblen Primfaktoren von ψ (vgl. Satz 3.21 (iii)) wieder. (Beispiel: Ist etwa $p = 11$, ψ mod $3 = (X^7 + X^6 + 2X^4 + 2X^2 + 2X + 2)(X^2 + X + 2)$, so kürzen wir das 3; 7,2 ab.) Die Vermutung liegt also nahe, dass die Galoisgruppe des Polynoms $X^p + aX + a$ stets die volle symmetrische Gruppe ist, denn ein Gegenbeispiel ist bisher nicht gefunden worden.

p	a	PFZ von D_0	Begründung für $G = S_p$
11	110003543122	$3^2 37^2 90091541^2$	Satz 3.15

p	a	PFZ von D_0	Begründung für $G = S_p$
11	11000035431220	$3^2 7^2 1429^2 3332339^2$	Satz 3.15
	15840042517464	$17^2 683^2 10335041^2$	Satz 3.15
	48510074405562	$47^2 61^2 6053^2 12101^2$	Satz 3.15
	58190081491806	230000161051^2	230000161051; 7,1,1
	112640113379904	$131^2 211^2 11577011^2$	Satz 3.15
	127160120466148	$3^2 113333387017^2$	Satz 3.15
	203390152354246	$3^2 52919^2 2708543^2$	Satz 3.15
	222750159440490	$7^2 64285737293^2$	Satz 3.15
	320760191328588	$13^2 41538473927^2$	Satz 3.15
13	115909431324362	$5^2 37^2 113^2 426505873^2$	Satz 3.15
	16690941545099640	$727^2 421009^2 349567^2$	Satz 3.15
	22718225699114764	$79^2 619^2 2552614693^2$	Satz 3.15
	72443319279505850	$5829157^2 38239237^2$	Satz 3.15
	84497887336542030	$7^4 19^2 31^2 67^2 67993^2 1831^2$	Satz 3.15
	167373042383548924	$29^2 37^2 315761250569^2$	Satz 3.15
	185454894343606160	356644022757049^2	356644022757049; 1,8,2
	301480110857228862	$5^2 97623949^2 931577^2$	Satz 3.15
	325589246720307154	$71^2 1118038079^2 5953^2$	Satz 3.15
	474764524700545664	$17^2 6865718161^2 4889^2$	Satz 3.15

Für $p = 17, 19, 23$ geben wir keine vollständige Primfaktorzerlegung von D_0 an. Der in der rechten Spalte angegebene Primteiler (erste Zahlenangabe) ist ein quadratisch aufgehender Teiler von D_0 und die zweite Zahlenangabe ist wie für die Fälle $p = 11, 13$ zu verstehen.

p	a	Begründung für $G = S_p$
17	313594649490238130466	Satz 3.15
	80280230212578780680736	Satz 3.15
	101604666362261373854820	332041393333747686529; 15
	341504573044411728915810	Satz 3.15
	384153445343302563757990	Satz 3.15
	783986623144514731329700	Satz 3.15
	847959931592613807839976	Satz 3.15
	1407726380512887787922406	Satz 3.15
	1493024125110195106100778	Satz 3.15
	2212723845149530898693928	Satz 3.15

p	a	Begründung für $G = S_p$
19	747581753442896346448658	Satz 3.15
	242216488111746203699590980	Satz 3.15
	299032701372498928223534440	Satz 3.15
	1023439420446991937777430938	Satz 3.15
	1137071846968472862560286654	Satz 3.15
	2344416378759155574314937328	Satz 3.15
	2514865018541364699356705300	Satz 3.15
	4205147363048237113312110150	Satz 3.15
	4432412216091174438612790378	Satz 3.15
	6605632373314236554768949404	Satz 3.15
23	7852841179377093649371738683074	Satz 3.15
	3800775130818493077182946335831212	Satz 3.15
	4523236519321181748292748531016240	Satz 3.15
	15902003388238527858065020032753690	Satz 3.15
	17346926165243905112626126695042462	Satz 3.15
	36311537613439481348637095101369224	Satz 3.15
	38478921778947547186649506230761740	Satz 3.15
	65029377806421353548899171541677814	Satz 3.15
	67919223360432107970362887138174074	Satz 3.15
	102055523967184144458851249353679460	Satz 3.15

Literaturverzeichnis

[1] E. Brieskorn und H. Knörrer, “Ebene algebraische Kurven”, Birkhäuser, Basel - Boston - Stuttgart, 1981.

[2] J. W. S. Cassels und A. Fröhlich, “Algebraic Number Theory”, Academic Press London, New York 1967.

[3] H. Cohen, “A Course in Computational Algebraic Number Theory”, Graduate Texts in Mathematics **138**, Springer, Berlin - Heidelberg - New York, 1993.

[4] S. D. Cohen, A. Movahhedi und A. Salinier, Double transitivity of Galois groups of trinomials, *Acta Arith.* **82** (1997), 1-15.

[5] S. D. Cohen, A. Movahhedi und A. Salinier, Galois groups of trinomials, *J. Algebra* **222** (1999), 561-573.

[6] A. Fröhlich und M. J. Taylor, “Algebraic Number Theory”, Cambridge studies in advanced mathematics **27**. Cambridge 1991.

[7] K. Girstmair, On quadratic relations between roots of polynomials, *J. Algebra* **188** (1997), 692-700.

[8] H. Hasse, “Number Theory”, Grundlehren der mathematischen Wissenschaften **229**, Springer, Berlin - Heidelberg - New York, 1980.

[9] H. Hasse, Über die Diskriminante auflösbarer Körper von Primzahlgrad, *J. Reine Angew. Math.* **176** (1936), 12-17.

[10] A. Hermez und A. Salinier, Rational trinomials with the alternating group as Galois group, *J. Number Theory* **90** (2001), 113-129.

[11] B. Huppert, “Endliche Gruppen. Band 1”, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen **134**, Springer, Berlin - Heidelberg - New York, 1979.

[12] K. Komatsu, On the Galois group of $x^p + ax + a = 0$, *Tokyo J. Math.* **14** (1991), 227-229.

[13] K. Komatsu, On the Galois group of $x^p + p^t b(x+1) = 0$, *Tokyo J. Math.* **15** (1992), 351-356.

[14] S. Lang, "Algebraic Number Theory", Graduate Texts in Mathematics **110**, Springer, Berlin - Heidelberg - New York, 1986.

[15] P. Llorente, E. Nart und N. Vila, Discriminants of number fields defined by trinomials, *Acta Arith.* **43** (1984), 367-373.

[16] B. H. Matzat, "Konstruktive Galoistheorie", Lecture Notes in Mathematics **1284**, Springer, Berlin - Heidelberg - New York, 1986.

[17] J. Montes und E. Nart, On a theorem of Ore, *J. Algebra* **146** (1992), 318-334.

[18] A. Movahhedi, Galois group of $X^p + aX + a$, *J. Algebra* **180** (1996), 966-975.

[19] A. Movahhedi und A. Salinier, The primitivity of the Galois group of a trinomial, *J. London Math. Soc.* **53** (1996), 433-440.

[20] W. Narkiewics, "Elementary and Analytic Theory of Algebraic Numbers", 2.Edition, Springer, Berlin - Heidelberg - New York, 1990.

[21] J. Neukirch, "Algebraische Zahlentheorie", Springer, Berlin - Heidelberg - New York, 1992.

[22] Ö. Ore, Newtonsche Polygone in der Theorie der algebraischen Körper, *Math. Ann.* **99** (1928), 84-117.

[23] Ö. Ore, Kriterien für Gleichungen mit primitiven Gruppen, *Akademie der Wissenschaften Oslo. Mat.-nat. Klasse* **18**, Kristiania 1924.

[24] M. Pohst, A note on index divisors, *Computational Number Theory, Proc. Colloq.* **1989** (1991), 173-182.

[25] M. Sase, On a family of quadratic fields whose class numbers are divisible by five, *Proc. Japan Acad.* **15** (1998), 120-123.

[26] J. P. Serre, "Local Fields", Graduate Texts in Mathematics **67**, Springer, Berlin - Heidelberg - New York, 1979.

[27] R. P. Stauduhar, "The Automatic Determination of Galois groups", Ph.D.thesis, University of California, Berkeley 1969.

[28] R. P. Stauduhar, The determination of Galois groups, *Math. Comp.* **27** (1973), 981-996.

[29] S. Stodtko, “Die maximalen Untergruppen der alternierenden und symmetrischen Gruppe”, Diplomarbeit Tübingen 1997.

[30] R. G. Swan, Factorisations of polynomials over finite fields, *Pacific J. Math.* **12** (1962), 1099-1106.

[31] K. Uchida, Galois group of an equation $X^n - aX + b = 0$, *Tohoku Math. J.* **22** (1970), 670-678.

[32] K. Uchida, Unramified extensions of quadratic number fields, I, *Tohoku Math. J.* **22** (1970), 138-141.

[33] K. Uchida, Unramified extensions of quadratic number fields, II, *Tohoku Math. J.* **22** (1970), 220-224.

[34] B. L. van der Waerden, Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppe, *Math. Ann.* **111** (1935), 731-733.

[35] U. Wegner, Bestimmung eines auflösbaren Körpers von Primzahlgrad aus der Form seiner Diskriminante, *J. Reine Angew. Math.* **176** (1936), 1-11.

[36] U. Wegner, Über trinomische Gleichungen von Primzahlgrad, *Math. Ann.* **111** (1935), 738-742.

Lebenslauf

16.12.1972	geboren in Stuttgart
1979-1983	Besuch der Fuchsrain-Grundschule in Stuttgart
1983-1992	Besuch des ev. Heidehof-Gymnasiums in Stuttgart
30.5.1992	Abitur
1992-1993	Zivildienst an der Karl-Schubert-Schule in Stuttgart
1993-2000	Studium der Mathematik und Geographie in Tübingen (Lehramt Gymnasium, Hauptfach)
1997-1998	Auslandsstudienaufenthalt an der Universität La Sapienza in Rom
1999-2000	Staatsexamen in Mathematik, Geographie und Informatik
seit 1999	Lehrbeauftragter der Berufsakademie Horb
Mai 2000	Beginn der Dissertation bei Prof. Dr. P. Schmid
1.4.01-31.7.01	Stipendium nach dem Landesgraduiertenförderungsgesetz
seit 1.8.01	Stipendium der Konrad-Adenauer-Stiftung

Meine akademischen Lehrer in Mathematik waren die Herren Professoren und Dozenten

K. J. Engel, U. Felgner, H. Heyer, W. Knapp, C. Lubich, R. Nagel, F. Räbiger, U. Riese, H. Salzmann, P. Schmid.