universität wien

1. BACHELORARBEIT

Titel der Bachelorarbeit

Galoisgruppen von Trinomen

Verfasser

Matija Suvajdžić

angestrebter akademischer Grad

Bachelor of Science (BSc.)

Wien, im Monat Juli 2021

Studienkennzahl lt. Studienblatt:	UA 033 621
Studienrichtung lt. Studienblatt:	Bachelorstudium Mathematik UG2002
Betreuer:	Assoz. Prof. Dr. Dietrich Burde, Privatdoz.

Abriss

Das Ziel dieser Bachelorarbeits ist es, die vielfältigen Eigenschaften von Galoisgruppen und die bestimmten Trinome, aus denen sie hervorgehen, zu untersuchen. Es ist wohlbekannt, dass Polynome meist die symmetrische Gruppe als Galoisgruppe haben. Malle [9] hat sogar gezeigt, dass für Polynome des Primzahlgrades die symmetrischen Gruppen *fast immer* entstehen. Insbesondere analysieren wir die Primpolynome $X^p + aX^{p-1} + a \in \mathbb{Z}[X]$. Wir werden zeigen, dass für $a \neq \pm 1$ oder $p \not\equiv 2 \pmod 3$ die Galoisgruppe von $X^p + aX^{p-1} + a$ eine **transitive** Permutationsgruppe ist, die eine **Transposition** enthält, und daher ist sie auch die volle **symmetrische Gruppe** S_p.

Inhaltsverzeichnis

Kapitel 1

Grundlegende Galoistheorie

1.1 Gruppen

Gruppen sind mathematische Strukturen, die das Essenz der Symmetrie erfassen. In vorliegender Arbeit untersuchen wir sie in ihrer Rolle als Galoisgruppen von Polynomen. Von besonderem Interesse sind für uns einige Eigenschaften von primgradigen Trinomen in $\mathbb{Q}[X]$, die genau bestimmen, wann ihre Galoisgruppen die Symmetrische Gruppe S_n ist. In dieser Rolle entstehen auch in der Arbeit die folgenden Gruppen:

(i) Die **Zyklische Gruppe** C_n ist eine Gruppe der Ordnung n, die von einem Element a mit $a^n = 1$ erzeugt wird:

$$C_n = \{1, a, a^2, ..., a^{n-1}\}.$$

(ii) Die **Diedergruppe** D_n ist eine Gruppe der Ordnung $2n$, bestehend aus Symmetrien eines regulären n-Ecks, von denen n Reflexionen und n Rotationen sind:

$$\exists\ r, s \in C_n \text{ mit } r^n = s^2 = 1 \text{ und } s = rsr^{-1}, \text{ sodass:}$$
$$D_n =< r, s > .$$

(iii) Die **Frobenius Gruppe** F_n ist eine *transitive Permutationsgruppe* der Ordnung n, die auf eine Menge X operiert, in der nur das Identitätselement mehr als einen Punkt fixiert:

$$(\forall\ x, y \in X, x \neq y)(\forall\ g \in F_n) :\ gx = x \text{ und } gy = y \Longrightarrow g = 1.$$

Die Grundlage für die gesamte Gruppentheorie ist ein sehr intuitiver Satz von Lagrange.

Theorem 1.1. ***(Lagrange):*** *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Mit $(G : H)$ bezeichnen wir die Kardinalität der Menge $\{aH \mid a \in G\}$, also die Anzahl der disjunkten Linksnebenklassen von H. Dann gilt*

$$ord(G) = (G : 1) = (G : H) \cdot (H : 1).$$

Nach Lagrange konnten nur die Mengen, derer Kardinalität die Ordnung der Gruppe G teilt, Untegruppen von G sein. Der Satz von Lagrange wirft auch die folgende Frage auf: Gibt es eine Menge von Gruppen, aus der alle anderen endlichen Gruppen als Untergruppen bis auf Isomorphie hervorgehen? Diese Frage führt uns zu einer solchen Familie von "Übergruppen", der **Symmetrischen Gruppen** S_n.

Definition 1.1. (Symmetrische Gruppe): Sei X={1,2,3,...,n}. Dann ist die Menge aller Bijektionen $f : X \to X$ eine Gruppe bezüglich der Komposition von Abbildungen, die *symmetrische Gruppe* S_n heißt.

Es ist wohlbekannt, dass S_n aus $n!$ Elementen besteht. Ein Element $\pi \in S_n$ normalerweise beschreiben wir als Produkt von Zyklen, Permutationen der Gestalt $(i_1, i_2, ..., i_m)$ für $m \leq n$ und Zahlen $\{i_1, i_2, ..., i_m\} \subseteq X$, in welchen:

$$\pi(i_1) = i_2,\ \pi(i_2) = i_3,\ \dots\ ,\ \pi(i_m) = i_1.$$

Zyklen (ij), die also nur 2 Elementen permutieren, heißen **Transpositionen**. Insbesondere könnte S_n durch bestimmte Transpositionen und Zyklen von maximaler Länge erzeugt werden, wie z. B. (12) und $(1234...n-1n)$.

Theorem 1.2. *Jedes Element in S_n ist für $n \geq 2$ ein Produkt von Transpositionen.*

Beweis. [Burde [5], p. 19, Satz 2.4.5.] □

Sei $\pi = (12)(23) \in S_n$. Es besitzt eine gerade Anzahl von Transpositionen, daher nennen wir es **gerade**. (12)(23)(45)(45) ist auch eine Darstellung von π, also auch gerade. Man konnte erkennen, dass unabhängig von der Darstellung ein gerades Element immer gerade Anzahl der Zyklen besitzt. Genauso gilt für **ungerade** Elementen. Die **Signum Abbildung** zeigt uns, ob eine Permutation gerade oder ungerade ist.

Definition 1.2. (Signum): Sei $\pi \in S_n$. Das Signum von π definieren wir als:

$$sgn(\pi) := \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j}.$$

Signum ist daher ein Gruppenhomomorphismus: $S_n \to (\{\pm 1\}, \cdot) \cong C_2$, der geraden Elementen $+1$ und -1 ungeraden Elementen zuweist. Die Menge von geraden Permutation ist eine Untergruppe von S_n, die **Alternierende Gruppe** heißt.

Definition 1.3. (Alternierende Gruppe): Die alternierende Gruppe A_n definieren wir als Kern der Signum-Abbildung.

Wir können schlussfolgern, dass $ord(A_n) = \frac{n!}{2}$ ist. Da A_n der Kern von einem Gruppenhomomorphismus ist, ist A_n auch ein *Normalteiler* von S_n mit $(S_n : A_n) = 2$.
Sei $n \geq 3$ und seien i, j, k paarweise verschiedene Zahlen in $\{1, 2, ..., n\}$. Die Permutationen

$$(ijk) = (ij)(jk) \quad \text{und} \quad (ikj) = (ik)(kj)$$

gehören zu A_n. Daher ist es immer möglich, von einem beliebigen Punkt i zu einem anderen Punkt k oder j durch eine Permutation von A_n zu gelangen. Wenn eine Gruppe wie A_n diese Eigenschaft hat, nennen wir sie eine **transitive Gruppe**.

Definition 1.4. (Transitive Gruppe): Eine Untergruppe G von S_n heißt **transitiv**, wenn sie transitiv auf $\{1, 2, ..., n\}$ operiert, d.h.

$$(\forall\ i, j \in \{1, 2, ..., n\})(\exists\ g \in G) : gi = j.$$

Die symmetrische Gruppe S_n ist klarerweise immer transitiv, ebenso A_n für $n \geq 3$. Für $n = 4$ sind die transitiven Untergruppen von S_4 auch die zyklische Gruppe C_4, die Diedergruppe D_4 und das direktes Produkt $C_2 \times C_2$.

1.2 Körper

Als eine mathematische "Fortsetzung"von Gruppen verfügt der Körper über viele der gleichen Begriffen und Ideen, wie z.B. Teilkörper und Körpererweiterungen. Einer der Hauptantriebe der Körpertheorie ist die Frage: In welcher Körpererweiterung liegen die Nullstellen einer bestimmten Polynom?

Definition 1.5. (Teilkörper, Körpererweiterung, Zwischenkörper): Sei L ein Körper. Ein Unterring K von L, der auch Körper ist, heist Teilkörper. Dann ist L eine Körpererweiterung von K, schreiben wir: $L \mid K$. Falls ein Teilkörper M von L existiert, so dass K Teilkörper von M ist, dann ist M ein Zwischenkörper von $L \mid K$, schreiben wir: $L \mid M \mid K$.

In der Arbeit werden wir vor allem die endliche Körpererweiterungen von $\mathbb{Q}$ untersuchen, die **Zahlkörper** heißen. Eine der bekanntesten Beispiele von Zahlkörpern sind die von Grad 2 über Q, die sogenannten **Quadratische Zahlkörper**.

Beispiel 1.1. Sei $f = X^2 + 3 \in \mathbb{Q}[X]$. Wir suchen eine Körpererweiterung $L \mid \mathbb{Q}$ mit $\alpha \in L$, so dass $\alpha^2 = -3$. Da kein Element diese Gleichung in $\mathbb{Q}$ löst, brauchen wir ein neues:

$$\alpha := \sqrt{-3}.$$

Der gesuchte quadratische Zahlkörper ist

$$L = Q(\sqrt{-3}) = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Q}\}.$$

Es lässt sich leicht überprüfen, dass für jeden quadratischen Zahlkörper ein quadratfreies Element $d \in \mathbb{Z}$ gibt, so dass $K = \mathbb{Q}(d)$.

Da es in $\mathbb{Q}[X]$ ein Polynom $f \neq 0$ gibt, für das α eine Nullstelle ist, nennen wir α **algebraisch** über $\mathbb{Q}$. Insbesondere ist eine Körpererweiterung $L \mid K$ algebraisch genau dann, wenn jedes Element aus L algebraisch ist. Der Körpererweiterung aller algebraischen Elemente über einem Körper K wird **algebraischer Abschluss** von K gennant, schreiben wir

$$\overline{K} = \{\alpha \in \mathbb{C} \mid \exists\ f \in \mathbb{K}[X], f \neq 0 :\ f(\alpha) = 0\}.$$

Die Elemente, die nicht algebraish sind, heißen **transzendental**.
Eine Körpererweiterung, die Lösungsraum einer Gleichung ist, und selbst mit Lösungen der Gleichung erzeugt ist, heißt **Zerfällungskörper**.

Definition 1.6. (Zerfällungskörper): Sei K ein Körper, $f \in K[X]$ ein Polynom vom Grad $n \geqslant 1$, und $L \mid K$ eine Körpererweiterung von K. $L \mid K$ heist Zerfällungskörper(ZFK) von f über K, falls einige Elementen $\{\alpha_1, \alpha_2, ..., \alpha_n\} \in L$ und eine Konstante $C \in K$ existieren, sodass:

$$f = C \prod_{i=1}^{n} (X - \alpha_i) \quad \text{und} \quad L = K(\alpha_1, \alpha_2, ..., \alpha_n).$$

Jetzt betrachten wir einige wichtige Eigenschaften von Körpererweiterungen.

Definition 1.7. (Galoiserweiterung): Sei $L \mid K$ eine endliche Körpererweiterung.

(i) $L \mid K$ heißt **normal**, falls:

$$(\forall\ \alpha \in L) :\ \text{Minimalpolynom } \mu_\alpha \text{ in } K[X] \text{ von } \alpha \text{ über } K \text{ in L in Linearfaktoren zerfällt.}$$

(ii) Ein Polynom $f \in K[X]$ heißt **separabel**, wenn es über algebraischer Abschluss $\overline{K}$ von K in paarweise verschiedene Linearefaktoren zerfällt. $L \mid K$ heißt dann **separabel**, falls:

$$(\forall\ \alpha \in L):\ \text{Minimalpolynom } \mu_\alpha \text{ in } K[X] \text{ ist separabel.}$$

(iii) Eine algebraische Körpererweiterung, die auch *normal* und *separabel* ist, heißt **Galoiserweiterung**.

Beispiel 1.2. Sei $f = X^3 - 7 \in \mathbb{Q}[X]$. Lösungsmenge der Gleichung ist:

$$\{\sqrt[3]{7}, \sqrt[3]{7} \cdot \zeta_3, \sqrt[3]{7} \cdot \zeta_3^2\},$$

wobei $\zeta_n = e^{\frac{2i\pi}{n}}$ die primitive $n - te$ Einheitswurzel ist.

$\mathbb{Q}(\sqrt[3]{7})$ enthält klarerweise $\sqrt[3]{7}$, aber nicht die beiden anderen Polynomnullstellen, und f zerfällt nicht in $\mathbb{Q}(\sqrt[3]{7})$ in Linearfaktoren. $\mathbb{Q}(\sqrt[3]{7})$ ist nicht normal und daher **keine Galoiserweiterung.**

Ersetzen wir $\mathbb{Q}(\sqrt[3]{7})$ mit $\mathbb{Q}(\sqrt[3]{7}, \zeta_3)$. Diese Erweiterung ist dann normal und nach dem *Ableitungskriterium für mehrfache Nullstellen* auch separabel, weil $char(\mathbb{Q}) = 0$. $\mathbb{Q}(\sqrt[3]{7}, \zeta_3) \mid \mathbb{Q}$ ist also eine **Galoiserweiterung.**

Galoiserweiterungen sind aufgrund der folgenden Äquivalenz sehr wichtig für die Galoistheorie [Burde [5], p. 104, Satz 4.8.21.]:

$$L \mid K \text{ ist eine Galoiserweiterung} \iff |Aut(L, K)| = [L : K].$$

Definition 1.8. (Galoisgruppe einer Gleichung): Sei K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom. Sei L Zerfällungskörper von f über K. Dann definieren wir die Galoisgruppe von f bis auf Isomorphie als die Automorphismengruppe:

$$G_f := Gal(L, K) := Aut(L \mid K)$$

Nach der Definition ist jedem nicht-konstanten Polynom $f \in K[X]$ eine Galoisgruppe zugeordnet. Genauso wie die $L \mid K$ eine Galoisgruppe induziert, erzeugt auch so einer Zwischenkörper M von $L \mid K$ die Gruppe $Gal(M, K)$, die Untergruppe von $Gal(L, K)$ ist.
Wir können auch in umgekehrter Richtung feststellen, dass eine Untegruppe $H \leq Gal(L, K)$ ein Zwischenkörper der $L \mid K$

$$L^H := \{\alpha \in L \mid (\forall\ \sigma \in H):\ \sigma(\alpha) = \alpha\}$$

definiert, der **Fixkörper** heißt.

Im Zentrum der Galoistheorie steht eine wichtige Verbindung zwischen den beiden oben genannten Entitäten.

Theorem 1.3. ***(Hauptsatz der Galoistheorie):*** *Es sei $L \mid K$ eine endliche Galoiserweiterung und $G := Gal(L, K)$. Dann sind die Abbildungen zwischen Untegruppen von G und Zwischenkörpern von $L \mid K$*

$$Z(L \mid K) \to U(G),\ M \mapsto Gal(L, M)$$

$$U(G) \to Z(L \mid K),\ H \mapsto L^H$$

zueinander inverse Bijektionen.

Beweis. [Burde [5], p. 107, Satz 4.8.27.] □

1.3 Diskriminante von Zahlkörpern

Ein besonders wichtiger Bestandteil dieser Arbeit wird mit **Diskriminanten von Zahlkörpern** zu tun haben. Um diesen Begriff weiter zu diskutieren, müssen wir zunächst einige wichtige Definitionen im Bereich der Zahlkörpern einführen.

Definition 1.9. (Ganzheitsring): Sei K ein Zahlkörper. Der ganze Abschluss von $\mathbb{Z}$ in K heißt der Ganzheitsring $\mathcal{O}_K$ von K, und eine Basis von $\mathcal{O}_K \mid \mathbb{Z}$ heißt **Ganzheitsbasis.**

Ganzheitsringe sind als Ringe ganz abgeschlossen. Insbesondere ist $\mathbb{Z}$ der Ganzheitsring von $\mathbb{Q}$, schreiben wir $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Beispiel 1.3. Sei $d \in \mathbb{Z}$ eine quadratfreie Zahl und $K = \mathbb{Q}(\sqrt{d})$. $Gal(K, \mathbb{Q}) = \{id, \sigma\} \cong C_2$ mit $\sigma(\sqrt{d}) = -\sqrt{d}$. Sei $\alpha = a + b\sqrt{d} \in \mathcal{O}_d$ mit $a, b \in \mathbb{Q}$, und sei μ_α Minimalpolynom von α in $\mathbb{Z}[X]$. Betrachten wir das Polynom $Q \in \mathbb{Q}[X]$:

$$\begin{aligned} Q &= (X - \alpha)(X - \sigma(\alpha)) \\ &= X^2 - (\alpha + \sigma(\alpha))X + (\alpha\sigma(\alpha)) \\ &= X^2 - 2aX + (a^2 - b^2 d). \end{aligned}$$

Da $Q(\alpha) = 0$ gilt $Q \mid \mu_\alpha$, also hat Q nach Lemma von Gauss ganzzahlige Koeffizienten: $-2a \in \mathbb{Z}$, $a^2 - b^2 d \in \mathbb{Z}$, mit den folgenden Implikationen:

$$2a \in \mathbb{Z} \implies 4a^2 \in \mathbb{Z} \implies 4b^2 d \in \mathbb{Z} \implies 2b \in \mathbb{Z}.$$

Insgesamt haben wir dann entweder $a, b \in \mathbb{Z}$, oder $a, b \in \frac{1}{2} + \mathbb{Z}$. Schreiben wir $a = \frac{u}{2}$ und $b = \frac{v}{2}$ für $u, v \in \mathbb{Z}$. Dann ist:

$$a^2 - b^2 d = \frac{u^2 - v^2 d}{4} \in \mathbb{Z}.$$

(i) $d \equiv 2, 3 \pmod 4$: Nur $u^2, v^2 \equiv 0 \pmod 4$ möglich ist, daher auch $u, v \equiv 0 \pmod 2$ und $a, b \in \mathbb{Z}$. Ganzheitsbasis von $\mathcal{O}_d$ ist dann $\{1, \sqrt{d}\}$, also:

$$\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}.$$

(ii) $d \equiv 1 \pmod 4$: Auch $u^2, v^2 \equiv 1 \pmod 4$ moglich ist, daher auch $u, v \equiv 1 \pmod 2$ und $a, b \in \frac{1}{2} + \mathbb{Z}$. Ganzheitsbasis von $\mathcal{O}_d$ ist dann $\{1, \frac{1+\sqrt{d}}{2}\}$, also:

$$\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\frac{1 + \sqrt{d}}{2}.$$

Definition 1.10. (Norm und Spur): Sei $L \mid K$ eine algebraische Körpererweiterung und $\alpha \in L$. Es bezeichne $\mu(\alpha)$ das **Minimalpolynom** von α, also das normierte Polynom kleinsten Grades mit Koeffizienten in K und Nullstelle α. Die Linksmultiplikation mit α definiert eine K-lineare Abbildung:

$$l_\alpha : K(\alpha) \to K \ , \ x \mapsto \alpha x.$$

Die **Norm** von α ist definiert als $N_{L|K}(\alpha) = det(l_\alpha)$. Die **Spur** von α ist defniert durch $tr_{L|K}(\alpha) = tr(l_\alpha)$.

Definition 1.11. (Diskriminante von Körpererweiterung): Sei $B \supset A$ eine Ringerweiterung und B ein freier A-Modul mit Basis $\{x_1, ..., x_n\}$.
Sei $(tr_{B/A}(x_i x_j))_{i,j}$ die Fundamentalmatrix der symmetrischen Bilinearform $B \times B \to A$, $(x, y) \to tr_{B/A}(xy)$ bezüglich dieser Basis. Dann heißt

$$D(x_1, ..., x_n) = det((tr_{B/A}(x_i x_j)_{i,j})) \in A$$

die Diskriminante der Basis $\{x_1, ..., x_n\}$.

Beispiel 1.4. Sei d eine quadratfreie Ganzzahl, $L = \mathbb{Q}(\sqrt{d})$ ihre quadratischer Zahlkörper und sei $\alpha = a + b\sqrt{d} \in L$. Eine Basis für $L \mid \mathbb{Q}$ wäre $\{1, \sqrt{d}\}$, bezüglich derer die Linksmultiplikation l_α die folgende Matrixdarstellung

$$l_\alpha = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

besitzt. Dann ist $tr_{L|\mathbb{Q}}(\alpha) = tr(l_\alpha) = 2a$.

(i) $d \equiv 2, 3 \pmod 4$: Nach Bsp. 1.3. ist $\{1, \sqrt{d}\}$ eine Ganzheitsbasis für $\mathcal{O}_d$, d.h. $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$. Diskriminante von $L \mid \mathbb{Q}$ ist dann:

$$D_{L|\mathbb{Q}} = D(1, \sqrt{d}) = det \begin{pmatrix} tr(1) & tr(\sqrt{d}) \\ tr(\sqrt{d}) & tr(d) \end{pmatrix} = det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

(ii) $d \equiv 1 \pmod 4$: Nach Bsp. 1.3. ist $\{1, \frac{1+\sqrt{d}}{2}\}$ eine Ganzheitsbasis für $\mathcal{O}_d$, d.h. $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2}$. Diskriminante von $L \mid \mathbb{Q}$ ist dann:

$$D_{L|\mathbb{Q}} = D(1, \frac{1+\sqrt{d}}{2}) = det \begin{pmatrix} tr(1) & tr(\frac{1+\sqrt{d}}{2}) \\ tr(\frac{1+\sqrt{d}}{2}) & tr(\frac{1+2\sqrt{d}+d}{2}) \end{pmatrix} = det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

Lemma 1.4. *Sei $L \mid K$ eine endliche, separable Körpererweiterung vom Grad n und seien $\sigma_1, \sigma_2, ..., \sigma_n$ die K-Einbettungen $L \hookrightarrow \overline{K}$, und sei $\{x_1, ..., x_n\}$ eine Basis von $L \mid K$. Dann gilt:*

$$D(x_1, ..., x_n) = det((\sigma_i(x_j))_{i,j})^2 \neq 0.$$

Insbesondere ist $D_{L|K} \neq 0$.

Beweis. [Burde [4], p. 21, Lemma 2.4.7.] □

Definition 1.12. (Diskriminante von Polynomen): Sei $f = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$ mit $a_n \neq 0$ ein nicht-Null Polynom über einem Körper K. Die Diskriminante von f ist definiert als die um a_n reduzierte *Resultante* von f mit seiner Ableitung f':

$$D = \frac{1}{a_n}(-1)^{n(n-1)/2} Res(f, f'),$$

wobei $Res(f, f')$ die Determinante der $(2n-1) \times (2n-1)$ Matrix ist:

$$\begin{pmatrix} a_n & a_{n-1} & ... & a_1 & a_0 & 0 & ... & 0 \\ 0 & a_n & a_{n-1} & ... & a_1 & a_0 & ... & 0 \\ ... & ... & .... & ... & ... & ... & ... & 0 \\ 0 & 0 & 0 & a_n & a_{n-1} & ... & a_1 & a_0 \\ na_n & (n-1)a_{n-1} & ... & 1a_1 & 0 & 0 & ... & 0 \\ 0 & na_n & (n-1)a_{n-1} & ... & 1a_1 & 0 & ... & 0 \\ 0 & 0 & 0 & na_n & (n-1)a_{n-1} & ... & 1a_1 & 0 \\ 0 & 0 & 0 & 0 & na_n & (n-1)a_{n-1} & ... & 1a_1 \end{pmatrix}$$

Seien $(\alpha_1, \alpha_2, ..., \alpha_n)$ die Nullstellen vom vorherigen f in algebraischer Abschluss $\overline{K}$. Die Diskriminante von f könnten wir dann auch als das Produkt darstellen

$$D = \prod_{1 \leq i \leq j \leq n} (\alpha_i - \alpha_j)^2.$$

Beispiel 1.5. Zeigen wir einige der bekannten Diskriminanten pro Grad:

(i) $n = 2$: Ein quadratisches Polynom $aX^2 + bX + c$ mit $a \neq 0$ hat die Diskriminante

$$D_2 = b^2 - 4ac,$$

die zur Lösungen $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$ führt.

(ii) $n = 3$: Ein kubisches Polynom $aX^3 + bX^2 + cX + d$ mit $a \neq 0$ hat die Diskriminante

$$D_3 = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

Sie induziert die folgenden Äquivalenzen [Irving [7], p. 154, Exercise 10.14.]:

$$\begin{gathered} D_3 > 0 \Longleftrightarrow \text{Alle Nullstellen reelle sind.} \\ D_3 = 0 \Longleftrightarrow \text{Mindestens zwei Nullstellen gleich sind.} \\ D_3 < 0 \Longleftrightarrow \text{Es gibt eine reelle und zwei komplexe konjugierte Nullstellen.} \end{gathered}$$

(iii) $n = 4$: Ein quadratisches Polynom $aX^4+bX^3+cX^2+dX+e$ mit $a \neq 0$ hat die Diskriminante

$$\begin{gathered} D_4 = 256a^3e^3 - 192a^2bde^2 - 128a^2c^2e^2 + 144a^2cd^2e \\ -27a^2d^4 + 144ab^2ce^2 - 6ab^2d^2e - 80abc^2de \\ +18abcd^3 + 16ac^4e - 4ac^3d^2 - 27b^4e^2 \\ +18b^3cde - 4b^3d^3 - 4b^2c^3e + b^2c^2d^2. \end{gathered}$$

Die Anzahl der Terme in einer Diskriminante wächst mit dem Polynomgrad zu ungeheuren Größen. Die Diskriminante eines allgemeinen Polynoms hohen Grades ist sehr unpraktisch zu analysieren. Wenn $n = 3$ gilt insbesondere die Äquivalenz:

$$D_3 < 0 \Longleftrightarrow G_f \cong S_3,$$

aufgrund des folgenden Satzes:

Theorem 1.5. *Sei $f \in \mathbb{Q}[X]$ irreduzibles Polynom vom Grad p mit p prim. Falls f in $\mathbb{C}$ genau zwei nicht-reelle Nullstellen hat, dann ist:*

$$G_f \cong S_p.$$

Beweis. [Burde [5], p. 116, Satz 4.10.9.] □

Beispiel 1.6. (i) Das Trinom $f = X^3 + x + 1$ über $\mathbb{Q}$ hat zwei nicht-reelle Nullstellen. Die Galoisgruppe G_f von f ist dann

$$G_f \cong S_3,$$

die auflösbar ist. Trinom f ist daher durch Radikale auflösbar.

(ii) Das Trinom $g = X^5 - 4X + 2$ über $\mathbb{Q}$ hat zwei nicht-reelle Nullstellen. Die Galoisgruppe G_g von g ist

$$G_g \cong S_5,$$

die nicht auflösbar ist. Trinom g ist daher nicht durch Radikale auflösbar.

Insbesondere beschränken wir uns in der Arbeit auf die Analyse von Diskriminanten über Zahlkörpern. Der folgende Satz legt den Grundstein für die Analyse in Kapitel 3: Er verbindet die Diskriminante eines Polynomes mit der Diskriminante seines Zerfällungskörpers.

Theorem 1.6. ***(Diskriminante von Zahlkörpern):*** *Sei $L \mid K$ eine Erweiterung von Zahlkörpern vom Grad n und $L = K(\alpha)$ mit $\alpha \in L$. Dann ist die Diskriminante der Basis $D(1, \alpha, ..., \alpha^{n-1})$ auch die Diskriminante des Minimalpolynoms μ_α von α über K, und es gilt*

$$D(1, \alpha, ..., \alpha^{n-1}) = \prod_{1 \leq i \leq j \leq n} (\alpha_i - \alpha_j)^2,$$

wobei $\alpha_1, ..., \alpha_n$ die Konjugierten von α in $\overline{K}$ sind.

Beweis. Seien $\sigma_i : K(\alpha) \hookrightarrow K$ die K-Einbettungen. Nach Lemma 1.4. gilt

$$(1, \alpha, ..., \alpha^{n-1}) = det((\sigma_i(\alpha^{j-1}))_{i,j})^2,$$

wobei die Konjugierten von α genau die $\sigma_i(\alpha)$ sind, die Nullstellen von μ_α. Nach der Determinantenformel von Vandermonde ist dann

$$\begin{aligned} D(1, \alpha, ..., \alpha^{n-1}) &= det((\sigma_i(\alpha^{j-1}))_{i,j})^2 \\ &= det((\alpha_i^{j-1})_{i,j})^2 \\ &= \prod_{1 \leq i \leq j \leq n} (\alpha_i - \alpha_j)^2. \end{aligned}$$

□

Kapitel 2

Trinome

Wie wir bereits gesehen haben, werden die Formeln für die Diskriminante für Polynome höheren Grades ungeheuer groß. Genauso gilt für die Anzahl der möglichen Galoisgruppen. Es ist daher einfacher, Polynome mit weniger Termen zu analysieren und das daraus resultierende Wissen zu nutzen, um kompliziertere Fälle zu lösen. In der Arbeit werden wir eine solche Gruppe von Polynomen betrachten, die **Trinome**.

Definition 2.1. (Trinom): Sei K ein Zahlkörper, seien $a, b, c \in K$ und seien $p, s, q \in \mathbb{N}_0$ mit $p > s > q$. Dann ist jedes Trinom $\varphi(X)$ über K ein Polynom der Form

$$\varphi(X) = aX^p + bX^s + cX^q.$$

Für Polynome vom Grad $n \leq 4$ könnte gezeigt werden, dass die allgemeine Form des Polynoms immer auflösbar ist. Falls $n \geq 5$ sind aber nach einem Satz von Galois die symmetrischen Gruppen S_n nicht auflösbar [Burde [5], p. 41, Korollar 2.10.5.], und daher sind auch die allgemeinen Formen von diesen Polynomen über Zahlkörper nicht auflösbar. Wir beobachten daher die quintischen und sechstischen Trinome anstelle der allgemeinen quintischen und seschtischen Polynomen, um herauszufinden, wann die Auflösbarkeit auftritt.

2.1 Quintische Trinome

Sei $f = X^5 + aX^p + bX^s$ ein irreduzibel Trinom in $\mathbb{Q}[X]$, wobei $p, s \in \mathbb{N}_0,\ p < s < 5$. Da f irreduzibel ist, operiert die Galoisgruppe transitiv auf den Nullstellen von f. Es gibt bis auf Konjugation nur 5 transitive Untergruppen von S_5 [Cohen [6], p. 328, Algorithm 6.3.9.]:

1. Die Zyklische Gruppe C_5 der Ordnung $|C_5| = 5$, *(auflösbar)*
2. Die Diedergruppe D_5 der Ordnung $|D_5| = 10$, *(auflösbar)*
3. Die Frobenius Gruppe F_{20} der Ordnung $|F_{20}| = 20$, *(auflösbar)*
4. Die Alternierende Gruppe A_5 der Ordnung $|A_5| = 60$, *(nicht auflösbar)*
5. Die Symmetrische Gruppe S_5 selbst, der Ordnung $|S_5| = 120$. *(nicht auflösbar)*

Als Untergruppen von S_5 bis auf Isomorphie stellen diese Gruppen die folgende Kette dar:

$$C_5 \subset D_5 \subset A_5 \cap F_{20} \subset S_5.$$

In der folgenden Tabelle finden wir einige Beispiele für Trinome, die diese Gruppen induzieren:

Galoisgruppen von quintische Trinomen		
Trinom	Galoisgruppe	Auflösbar
$X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$	$G_5 \cong C_5$	ja
$X^5 - 5X + 12$	$G_{10} \cong D_5$	ja
$5X^5 - 10X^2 - 1$	$G_{20} \cong F_{20}$	ja
$X^5 + 20X + 16$	A_5	nein
$X^5 + 2X^4 + 2$	S_5	nein

Bemerkung: G_5, G_{10} und G_{20} sind Untergruppen von S_5, die durch die folgenden Permutationen nach $MAGMA^{TM}$ erzeugt werden:

$$G_5 =< (13452) >,$$
$$G_{10} =< (14)(25), (13)(45) >,$$
$$G_{20} =< (1534), (13)(45), (12354) > .$$

2.1.1 Quintische Trinome $X^5 + aX + b$

In [Brown [3], p. 30, Quintic Trinomials] werden Parametrisierungen für die Koeffizienten von $X^5 + aX + b$ gegeben, die paarweise verschiedene irreduzible und auflösbare Trinomen erzeugen:

$$a = \frac{5e^4(3 - 4\epsilon c)}{c^2 + 1} \; und \; b = \frac{-4e^5(11\epsilon + 2c)}{c^2 + 1},$$

wobei $\epsilon = \pm 1$ und $c, e \in \mathbb{Q}$, so dass $c \geq 0, e \neq 0$.
Einige Beispiele für solche Trinome sind:

Galoisgruppen von $X^5 + aX + b$			
a	b	Trinom	Galoisgruppe
11	$\frac{28}{5}$	$X^5 + 11X + \frac{28}{5}$	$G_{10} \cong D_5$
$-\frac{5}{2}$	-26	$X^5 - \frac{5}{2}X - 26$	$G_{20} \cong F_{20}$
$\frac{35}{2}$	18	$X^5 + \frac{35}{2}X + 18$	$G_{20} \cong F_{20}$

2.1.2 Quintische Trinome $X^5 + aX^2 + b$

Es gibt bis auf Skalierung nur 5 verschiedene irreduzible und auflösbare Trinomen der Form $X^5 + aX^2 + b$, die auch in [Brown [3], p. 30, Quintic Trinomials] angegeben sind:

Galoisgruppen von $X^5 + aX^2 + b$	
Trinom	Galoisgruppe
$X^5 + 5X^2 + 3$	$G_{10} \cong D_5$
$X^5 + 5X^2 - 15$	$G_{10} \cong D_5$
$X^5 + 25X^2 + 300$	$G_{10} \cong D_5$
$X^5 + 100X^2 + 1000$	$G_{20} \cong F_{20}$
$X^5 + 250X^2 + 625$	$G_{20} \cong F_{20}$

2.2 Sechstische Trinome

Mit einem höheren und nicht-prim Polynomgrad kommt auch eine höhere Komplexität in den Galoisgruppen. Bis auf Konjugation gibt es 16 transitive Teilgruppen von S_6, von denen wir nur *auflösbaren* nennen werden[Cohen [6], p. 329, Algorithm 6.3.10.]:

1. Die Zyklische Gruppe C_6 der Ordnung $|C_6| = 6$,
2. Die Symmetrische Gruppe S_3 der Ordnung $|S_3| = 6$,
3. Die Alternierende Gruppe A_4 der Ordnung $|A_4| = 12$,
4. Das direkte Produkt $C_3 \times D_3$ der Ordnung $|C_3 \times D_3| = 3 \cdot 6 = 18$,
5. Das direkte Produkt $A_4 \times C_2$ der Ordnung $|A_4 \times C_2| = 12 \cdot 2 = 24$,
6. Das direkte Produkt $D_3 \times D_3$ der Ordnung $|D_3 \times D_3| = 6 \cdot 6 = 36$.

2.2.1 Sechstische Trinome $X^6 + aX + b$

Stephen Brown hat sich in seiner Arbeit "*On the Galois Groups of Sextic Trinomials*" insbesondere mit den sechstischen Trinomen $X^6 + aX + b$ beschäftigt. Wir zeigen einige der Sätze über diese Familie von Trinomen, deren Beweis in der oben genannten Arbeit gegeben wird.

Theorem 2.1. *Sei K ein algebraischer Zahlkörper. Falls $f = X^6 + aX + b \in K[X]$ irreduzibel über $\mathbb{Q}$ ist und C_6, S_3 oder $C_3 \times D_3$ als Galoisgruppe hat, dann existieren u, v und w aus K mit $u, v \neq 0$, so dass:*

$$a = 4u(3u + 1)v^5,$$

$$b = -u(1 - 18u + u^2)v^6,$$

und

$$(3w^2 + 144)u^2 + (-672 + 4w^4 + 210w^2)u + 784 + 27w^2 = 0.$$

Beweis. [Brown [3], p. 57, Theorem 6.1.] □

Es ist in [Cohen [6]] auch nachgewiesen, dass das einzige Trinom des Grades 6, das die Galoisgruppe C_6 hat,

$$X^6 + 133X + 209$$

ist.
Als Folge des obigen Satzes können wir bestimmte Schlussfolgerungen über die Galoisgruppe von $X^6 + aX + b$ ziehen:

Korollar 2.2. *(i) Es gibt keine Trinomen $X^6+aX+b \in \mathbb{Q}[X]$ mit Galoisgruppe S_3 oder $C_3 \times D_3$.*

(ii) Es gibt nur eine normale sechstische Erweiterung von irreduziblen Trinomen mit rationalen Koeffizienten. Diese Erweiterung wird insbesondere aus jeder Nullstelle des zuvor genannten $X^6 + 133x + 209$ erzeugt.

(iii) Sei K ein Zahlkörper und seien $a, b \in K$ nicht-Null Koeffizienten, so dass X^6+aX+b irreduzibel über K ist. Die Menge von Trinomen $X^6 + aX + b$ mit Galoisgruppe C_6, S_3 oder $C_3 \times D_3$ ist endlich.

Brown hat alle Ergebnisse in Bezug auf auflösbare $X^6 + aX + b$ in der folgenden Tabelle ordentlich zusammengefasst:

Galoisgruppen von $X^6 + aX + b$	
Trinom	Galoisgruppe
$X^6 + 133X + 209$	C_6
Es gibt kein solches Trinom	S_3
Es gibt kein solches Trinom	A_4
Es gibt kein solches Trinom	$G_{18} \cong C_3 \times D_3$
Unendliche viele Trinome	$A_4 \times C_2$
Mindestens $X^6 + \frac{224}{3}X + \frac{2240}{27}$	$G_{36} \cong D_3 \times D_3$

Kapitel 3

Galoisgruppe von $X^p + aX^{p-1} + a$

Wie bereits erwähnt, Polynome über Zahlkörper haben eine transitive Galoisgruppe genau dann, wenn sie irreduzibel sind. Wir beschränken uns daher auf das Studium irreduzibler $X^p+aX^{p-1}+a \in \mathbb{Q}[X]$ mit p prim und $a \in \mathbb{Z}$, für welcher Irreduzibilitat auftritt, wenn $a \neq \pm 1$ oder $p \not\equiv 2 \pmod 3$ gilt:

Lemma 3.1. *Sei p prim und $a \in \mathbb{Z}$. Jedes Trinom $f = X^p + aX^{p-1} + a$ mit $a \neq \pm 1$ oder $p \not\equiv 2 \pmod 3$ ist irreduzibel in $\mathbb{Q}[X]$.*

Beweis. [Bensebaa et al. [2], p. 829-830] □

3.1 Diskriminante von $X^p + aX^{p-1} + a$

Sei α eine Nullstelle von $X^p + aX^{p-1} + a$, $K := \mathbb{Q}(\alpha)$ ein Zahlkörper und N normaler Abschluss von K über $\mathbb{Q}$. Diskriminante D von $X^p + aX^{p-1} + a$ vereinfacht [McEliece [10], Theorem 2] zu

$$D = (-1)^{\frac{p-1}{2}} a^{p-1}(p^p + (p-1)^{p-1}a^{p-1}).$$

Definieren wir $\delta := min(p, (p-1)v_p(a))$, $b := a/p^{v_p(a)}$ und D_0 durch:

$$D_0 := p^{p-\delta} + (p-1)^{p-1}b^{p-1}p^{(p-1)v_p(a)-\delta}. \tag{3.1}$$

Dann gilt:

$$D = (-1)^{\frac{p-1}{2}} b^{p-1}p^{(p-1)v_p(a)+\delta}D_0. \tag{3.2}$$

Wir haben bereits gezeigt, dass im Fall $p = 3$ die folgende Äquivalenz gilt:

$$D < 0 \iff G_f \cong S_3.$$

Im weiteren Verlauf dieser Arbeit werden wir dann $p > 3$ annehmen. Für D_0 können wir 3 Lemmas zu eine zusammenfassen:

Lemma 3.2. *(i) Sei l ein Primzahl. Wenn $v_l(D_0)$ ungerade ist, dann teilt l die Diskriminante von Zahlkörpern K nur einmal. [P. Llorente [11], Theorem 2]*

(ii) Dementsprechend wird die Trägheitsgruppe eines Primideals von N über l durch eine Transposition erzeugt. [A. Movahhedi [1], Lemma 5]

(iii) Falls eine transitive Permutationsgruppe des Primgrades p eine Transposition enthält, dann ist sie die volle symmetrische Gruppe S_p. [Jordan [8]]

Aus Lemma 3.2. können wir schlussfolgern: Wenn D_0 quadratfrei ist, ist die Galoisgruppe G_f von f:

$$G_f \cong S_p.$$

Wir untersuchen daher die Quadratfreiheit von D_0 durch Fälle per $v_p(a)$: [Bensebaa et al. [2], p. 826]

(i) **Fall** $v_p(a) \leq 1$**:** Es gilt $\delta = (p-1)v_p(a)$. Falls D_0 eine Quadratzahl ist, dann:

$$(\exists\ s \in \mathbb{N}):\ D_0 = p^{p-(p-1)v_p(a)} + (p-1)^{p-1}b^{p-1} = s^2.$$

Definieren wir eine $t \in \mathbb{Z}$, wobei t relativ prim zu ps und teilbar durch $p-1$ ist, sodass:

$$s - t = 1 \ \text{ und } \ s + t = p^{p-(p-1)v_p(a)}.$$

Daraus folgt aber eine Kontradiktion zwischen geraden und ungeraden Zahlen:

$$2t = p^{p-(p-1)v_p(a)} - 1 \iff 2\frac{t}{p-1} = 1 + p + ... + p^{(p-1)(1-v_p(a))},$$

wobei $2t/(p-1)$ gerade und $p^{(p-1)(1-v_p(a))}/(p-1)$ ungerade für $v_p(a) \leq 1$ ist. D_0 ist dann für $v_p(a) \leq 1$ keine Quadratzahl.

(ii) **Fall** $v_p(a) \geq 2$**:** Es gilt $\delta = p$. Falls D_0 eine Quadratzahl ist, dann:

$$(\exists\ s \in \mathbb{N}):\ s^2 - 1 = (p-1)^{p-1}b^{p-1}p^{(p-1)v_p(a)-p}.$$

Da $gcd(s-1, s+1) = 2$ gilt, dividiert irgendwelcher ungeraden Primteiler von $(p-1)b$ entweder $s-1$ oder $s+1$. Deswegen wählen wir relativ prim $u, v \in \mathbb{Z}$ mit $u^{p-1} \mid s+1$, $v^{p-1} \mid s-1$ und $(p-1)b = 2^\lambda uv$ für eine $\lambda \in \mathbb{N}$, sodass

$$s - 1 = 2^\eta v^{p-1}p^\gamma \ \text{ und } \ s + 1 = 2^\mu u^{p-1}p^\beta \tag{3.3}$$

für einige $\mu, \eta, \beta, \gamma \in \mathbb{N}$ ist, wobei $\mu + \eta = (p-1)\lambda$ und $\beta + \gamma = (p-1)v_p(a) - p$. Wegen $gcd(s-1, s+1) = 2$ folgt auch $min(\mu, \eta) = 1$ und $min(\beta, \gamma) = 0$.

(ii.1) **Nehmen wir** $\gamma = 0$ **an:** Dann ist $\beta > 0$ und $s \equiv -1 \pmod p$. Aus (3.1) folgt nun:

$$-2 \equiv 2^\eta \pmod p \implies \eta \neq 1.$$

Da $min(\mu, \eta) = 1$ ist, muss $\mu = 1$ gelten. Gleichungen (3.1) werden dann zu:

$$s - 1 = 2^\eta v^{p-1} \ \text{ und } \ s + 1 = 2u^{p-1}p^\beta,$$

woraus folgt

$$4 = 4u^{p-1}p^\beta - 2^{\eta+1}v^{p-1}. \tag{3.4}$$

Da $\eta + 1 = (p-1)\lambda$ ist, folgt aus der letzen Gleichung $4 \equiv -1 \pmod p \implies p = 5$. Gleichung (3.4) wird dann zu:

$$1 = u^4 5^\beta - 2^{4\lambda-2}v^4.$$

Es gilt dann aber $\lambda = 1$, weil u, v und β ungerade sind. Da $(p-1)b = 2uv$ kommen wir zu eine Kontradiktion.

(ii.2) **Nehmen wir** $\beta = 0$ **an:** Es gilt $\gamma > 0$, und die Gleichungen (3.3) sind:

$$s - 1 = 2^\eta v^{p-1}p^\gamma \ \text{ und } \ s + 1 = 2^\mu u^{p-1}.$$

Falls $\eta = 1$ haben wir $\mu = (p-1) - 1$, daher:

$$s - 1 \equiv 0 \pmod p \ \text{ und } \ 2(s+1) \equiv 1 \pmod p.$$

Für $p > 3$ ist das aber unmoglich. So muss $\mu = 1$ gelten, und:

$$s - 1 = 2^{\eta} v^{p-1} p^{\gamma} \quad \text{und} \quad s + 1 = 2^{u} p - 1.$$

Umschreiben wir $\eta = 2\kappa + 1$, um die Gleichung

$$1 = u^{p-1} - 2^{2\kappa} p^{\gamma} v^{p-1} \tag{3.5}$$

zu bekommen, die **die Basis aller weiteren Analyse der Diskriminante wird.**

3.2 Zahlentheoretische Bedeutung der Diskriminante

Für $p = 3$ oder $v_p(a) \leq 1$ haben wir schon gezeigt, dass D_0 quadratfrei ist. Die folgende Lemma nach B. Bensebaa zeigt, dass dies auch bei $p = 5$ der Fall ist.

Lemma 3.3. *Sei $\gamma \in Z, \gamma \geq 1$ und sei $\kappa \in \mathbb{N}$ ungerade. Die Gleichung*

$$1 = u^4 - 2^{2\kappa} 5^{y} v^4 \tag{3.6}$$

hat keine ganzzahlige Lösungen u, v mit $v \neq 0$.

Beweis. Seien u, v ganzzahlige Losungen von (3.6) mit $v \neq 0$. Da u ungerade ist, gilt $u^2 + 1 \equiv 2 \pmod 4$. Wir ordnen die Gleichung mit ganzzahligen w, t, δ *und* ϵ neu an:

$$u^2 - 1 = 2^{2\kappa - 1} 5^{\delta} w^4 \quad \text{und} \quad u^2 + 1 = 2 \cdot 5^{\epsilon} t^4, \tag{3.7}$$

wobei $gcd(10, wt) = gcd(w, t) = 1$, $min(\delta, \epsilon) = 0$ und $\delta + \epsilon = \gamma$.

(i) **Fall** $\delta = 0$: Es gilt $\epsilon = \gamma > 0$, also auch $u^2 + 1 \equiv 0 \pmod 5$. Dies in die erste Gleichung eingeben, bekommen wir:

$$u^2 - 1 \equiv -2 \equiv 2^{2\kappa - 1} \pmod 5.$$

Es gilt aber $2^{2\kappa - 1} \equiv 2 \pmod 5$, weil κ ungerade ist. Daher kommen wir zu einem Widerspruch.

(ii) **Fall** $\epsilon = 0$: Es gilt $\delta = \gamma > 0$. Die zweite Gleichung wird die *Ljunggren Gleichung*

$$u^2 + 1 = 2t^4.$$

Die Ljunggren Gleichung hat nur zwei ganzzahlige Lösungen []:

$$(u, t) = (1, 1) \quad \text{und} \quad (u, t) = (239, 13),$$

von denen aber keine (3.7) löst:

$$u^2 - 1 = 2^{2\kappa - 1} 5^{\gamma} w^4.$$

□

Von nun an gehen wir davon aus, dass $p > 5$ und $v_p(a) \geq 2$ hält. Die folgenden beiden Lemmata nach B. Bensebaa sind Hilfsätze für den Beweis unseres Hauptsatzes.

Lemma 3.4. *Sei $p > 5$ ein Primzahl. Die Gleichung:*

$$1 = u^{\frac{p-1}{2}} - 2^{2\kappa - 1} v^{p-1} \tag{3.8}$$

hat keine ganzzahlige Lösungen für $u, v, \kappa \geq 1$, so dass $p \nmid uv$.

Beweis. [Bensebaa et al. [2], p. 827, Lemma 3.1] □

Lemma 3.5. *Sei $p > 3$ ein Primzahl und $\gamma \geq 1$ ganzzahlig. Die Gleichung:*

$$1 = u^2 - p^{\gamma} v^{p-1} \tag{3.9}$$

hat keine ganzzahlige Lösungen u, v mit v ungerade.

Beweis. [Bensebaa et al. [2], p. 828, Lemma 3.2]. □

3.3 Hauptsatz der Arbeit

Schließlich beweisen wir schrittweise der Satz von B. Bensebaa, indem wir die zahlentheoretische Lemmata aus dem vorherigen Abschnitt verwenden.

Theorem 3.6. *Sei p eine Primzahl und $a \in \mathbb{Z}$. Gilt entweder $a \neq \pm 1$ oder $p \not\equiv 2 \pmod 3$, so ist der Trinom $f = X^p + aX^{p-1} + a$ irreduzibel in $\mathbb{Z}[X]$ und hat Galoisgruppe $G_f \cong S_p$.*

Beweis. Sei $p > 5$ und $v_p(a) \geq 2$, sei $\gamma > 0$ und seien $u, v \in \mathbb{Z}$ positive Lösungen von:

$$1 = u^{p-1} - 2^{2\kappa} p^{\gamma} v^{p-1}.$$

Schreiben wir (3.3) als:

$$(u^{\frac{p-1}{2}} + 1)(u^{\frac{p-1}{2}} - 1) = 2^{2\kappa} p^{\gamma} v^{p-1}.$$

Ordnen wir die Gleichung mit ganzzahligen w, t, μ, η, δ und ϵ neu an:

$$u^{\frac{p-1}{2}} + 1 = 2^{\eta} p^{\epsilon} t^{p-1} \quad \text{und} \quad u^{\frac{p-1}{2}} - 1 = 2^{\mu} p^{\delta} w^{p-1}, \tag{3.10}$$

wobei $gcd(2p, wt) = gcd(w, t) = 1$, $min(\mu, \eta) = 1$ und $\mu + \eta = 2\kappa$, $min(\delta, \epsilon) = 0$ und $\delta + \epsilon = \gamma > 0$. Nach Lemma 3.4. ist $\delta = 0$ in (3.10) unmöglich. So gilt $\delta = \gamma$, und die Gleichungen werden zu

$$u^{\frac{p-1}{2}} + 1 = 2^{\eta} t^{p-1} \quad \text{und} \quad u^{\frac{p-1}{2}} - 1 = 2^{\mu} p^{\gamma} w^{p-1}. \tag{3.11}$$

(i) **Fall** $\mu = 1$: Es gilt $\eta = 2\kappa - 1$. Aus (3.11) folgt jetzt:

$$1 = 2^{2\kappa-2} t^{p-1} - p^{\gamma} w^{p-1} = (2^{\kappa-1} t^{\frac{p-1}{2}})^2 - p^{\gamma} w^{p-1}.$$

Dies ist aber eine ganzzahlige Lösung der Gleichung (3.9), was nach Lemma 3.5. ein Widerspruch ist.

(ii) **Fall** $\eta = 1$: Es gilt $\mu = 2\kappa - 1$, und aus Gleichungen (3.11) folgt:

$$1 = t^{p-1} - 2^{2(\kappa-1)} p^{\gamma} w^{p-1}.$$

$(t, w, \kappa - 1)$ ist daher auch eine Lösung der urpsprünglichen Gleichung. Es gilt insbesondere für jede $\kappa \in \mathbb{N}$:

$$(t, w, \kappa) \text{ ist eine Losung von (3.3)} \implies (t, w, \kappa - 1) \text{ ist auch eine Lösung von (3.3).}$$

Nach Induktion per κ kommen wir eventuell zur $\kappa = 0$ und einige $t_0, w_0 \in \mathbb{Z}$, sodass:

$$1 = (t_0^{\frac{p-1}{2}})^2 - p^{\gamma} w_0^{p-1}.$$

Diese Gleichung hat aber nach Lemma 3.5. keine ganzzahlige Lösungen, also kommen wir noch einmal zu einem Widerspruch.

D_0 ist daher immer **quadratfrei**. G_f ist dann nach Lemma 3.2. eine **transitive** Permutationsgruppe, die eine **Transposition** enthält, und daher auch die volle **symmetrische Gruppe:**

$$G_f \cong S_p.$$

□

Betrachten wir ein Beispiel und ein Gegenbeispiel zu Theorem 3.6:

Beispiel 3.1. Sei $p = 13$, $a = 1$ und $f = X^{13} + X^{12} + 1 \in \mathbb{Z}[X]$. Es gilt $p \not\equiv 2 \pmod 3$ und $a \in \{\pm 1\}$, also ist eine der Bedingunen von Theorem 3.6. erfüllt. Die Galoisgruppe G_f von f ist dann isomorph zur symmetrischen Gruppe:

$$G_f \cong S_{13}.$$

Gegenbeispiel 3.2. Sei $p = 5$, $a = 1$. Dann ist f der Trinom $X^5 + X^4 + 1$, der über $\mathbb{Z}[X]$ in $(X^3 - X + 1)(X^2 + X + 1)$ zerfällt. G_f hat nach der $MAGMA^{TM}$ Rechner Ordnung 12, aber $|S_5| = 120$, daher:

$$G_f \ncong S_5.$$

Schließlich untersuchen wir die Konsequenzen von Theorem 3.6. in einigen weiteren Polynomgraden.

3.3.1 Septische Trinome $X^7 + aX^6 + a$

Es gilt $7 \equiv 1 \pmod 3$, also hat jeder Trinom $X^7 + aX^6 + a \in \mathbb{Z}[X]$ nach dem Theorem 3.6. die Galoisgruppe

$$G_f \equiv S_7.$$

Wir können diese Tatsache mit zufällig ausgewählten Koeffizienten $a \in \mathbb{Z} \setminus \{0\}$ und der $MAGMA^{TM}$ Rechner leicht überprüfen:

Galoisgruppen von $X^7 + aX^6 + a \in \mathbb{Z}[X]$		
a	Trinom	Galoisgruppe
1	$X^7 + X^6 + 1$	S_7
-1	$X^7 - X^6 - 1$	S_7
3	$X^7 + 3X^6 + 3$	S_7
7	$X^7 + 7X^6 + 7$	S_7
-10	$X^7 - 10X^6 + 10$	S_7
-25	$X^7 - 25X^6 - 25$	S_7
63	$X^7 + 63X^6 + 63$	S_7
1337	$X^7 + 1337X^6 + 1337$	S_7

3.3.2 Undecische Trinome $X^{11} + aX^{10} + a$

Es gilt $11 \equiv 2 \pmod 3$. Nach Theorem 3.6 hängt die Galoisgruppe vom Trinom $X^{11} + aX^{10} + a \in \mathbb{Z}[X]$ davon ab, ob der Koeffizient a in der Menge $\{\pm 1\}$ liegt.

Solche Fälle prüfen wir wieder mit zufällig ausgewählten Koeffizienten $a \in \mathbb{Z} \setminus \{0\}$ und der $MAGMA^{TM}$ Rechner:

Galoisgruppen von $X^{11} + aX^{10} + a \in \mathbb{Z}[X]$		
a	Trinom	Galoisgruppe
1	$X^{11} + X^{10} + 1$	$G_{725760} =$ $< (12), (34), (34567891011) >$
-1	$X^{11} - X^{10} - 1$	$G_{725760} =$ $< (12), (34), (34567891011) >$
-11	$X^{11} - 11X^{10} - 11$	S_{11}
37	$X^{11} + 37X^{10} + 37$	S_{11}
64	$X^{11} + 64X^{10} + 64$	S_{11}
-110	$X^{11} - 110X^{10} + 110$	S_{11}
625	$X^{11} + 625X^{10} + 625$	S_{11}
3200	$X^{11} + 3200X^{10} + 3200$	S_{11}

Literaturverzeichnis

[1] A. Movahhedi, A. S. (1996). The primitivity of the galois group of a trinomial. *J. London Math. Soc. (2) 53*, pages 433–440.

[2] Bensebaa, B., Movahhedi, A., and Salinier, A. (2009). The galois group of $x^p + ax^{p-1} + a$. *Journal of Number Theory*, 129(4):824–830.

[3] Brown, S. C. (2011). On the galois groups of sextic trinomials. *The University of British Columbia*.

[4] Burde, D. (2013). Algebraische zahlentheorie. *Lecture Notes*, pages 1–113.

[5] Burde, D. (2020). Algebra I und II. *Lecture Notes*, pages 1–137.

[6] Cohen, H. (1993). A course in computational algebraic number theory. *Springer, Berlin, Heidelberg*, pages XXI, 536.

[7] Irving, R. S. (2004). Integers, polynomials and rings. *Springer, New York, NY*, pages 1–288.

[8] Jordan, C. (1871). Théorèmes sur les groupes primitifs. *J. Math. (2) XVI*, pages 383–408.

[9] Malle, G. (2002). On the distribution of galois groups. *Journal of Number Theory*, 92(2):315–329.

[10] McEliece, R. J. (1969). Factorization of polynomials over finite fields. *American Mathematical Society, Mathematics of Computation*, 23.

[11] P. Llorente, E. Nart, N. V. (1984). Discriminants of number fields defined by trinomials. *Acta Arith. XLIII*, pages 367–363.