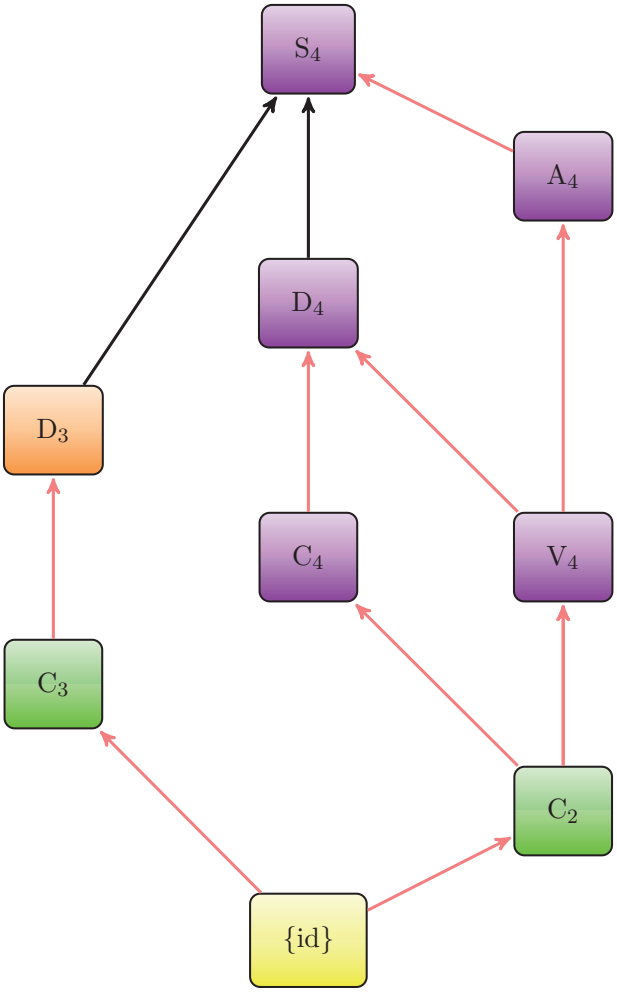
Max Feuerhake

Galoisgruppen von Polynomen vierten Grades



Universitätsdrucke Göttingen

Max Feuerhake

Galoisgruppen von Polynomen vierten Grades

Dieses Werk ist lizenziert unter einer
Creative Commons
Namensnennung - Weitergabe unter gleichen Bedingungen
4.0 International Lizenz.

erschienen in der Reihe der Universitätsdrucke
im Universitätsverlag Göttingen 2020

Max Feuerhake

Galoisgruppen von Polynomen vierten Grades

Universitätsverlag Göttingen
2020

Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über <http://dnb.dnb.de> abrufbar.

Masterarbeit im Masterstudiengang
Wirtschaftspädagogik mit Zweitfach Mathematik
an der Fakultät für Mathematik und Informatik
der Georg-August-Universität Göttingen

Autorenkontakt
Max Feuerhake
E-Mail: max.feuerhake.mf@gmail.com

Dieses Buch ist auch als freie Onlineversion über die Homepage des Verlags sowie über den Göttinger Universitätskatalog (GUK) bei der Niedersächsischen Staats- und Universitätsbibliothek Göttingen (https://www.sub.uni-goettingen.de) erreichbar. Es gelten die Lizenzbestimmungen der Onlineversion.

Satz und Layout: Max Feuerhake
Titelabbildung: Max Feuerhake: Untergruppen der S_4 bis auf Isomorphie (s. Abb. 1.1., S. 22 in diesem Band)

© 2020 Universitätsverlag Göttingen
https://univerlag.uni-goettingen.de
ISBN: 978-3-86395-440-6
DOI: https://doi.org/10.17875/gup2020-1248

Inhaltsverzeichnis

Abbildungsverzeichnis **7**

Tabellenverzeichnis **7**

Einleitung **9**

1 Grundlagen **11**

1 Die Struktur der symmetrischen Gruppe $\mathbf{S_4}$ 11

2 Galoistheorie 24

2 Galoisgruppen von Polynomen vierten Grades **31**

1 Begrifflichkeiten zur Klassifizierung 31

2 Klassifikationssatz 39

3 Flussdiagramm für $\mathbf{Grad}(\boldsymbol{p}(\boldsymbol{x})) = \mathbf{4}$ 49

4 Exkurs: Irreduzibilitätskriterien 51

5 Konkrete Beispiele für Satz 13 53

5.1 Fall (i) Galoisgruppe $\mathbf{S_4}$ 53

5.2 Fall (ii) Galoisgruppe $\mathbf{A_4}$ 57

5.3 Fall (iii) Galoisgruppe $\mathbf{V_4}$ 61

5.4 Fall (iv) Galoisgruppe $\mathbf{C_4}$ 65

5.5 Fall (v) Galoisgruppe $\mathbf{D_4}$ 69

5.6 Fall (i), (iv) und (v) Galoisgruppen $\mathbf{S_4}$, $\mathbf{C_4}$ und $\mathbf{D_4}$ . . 71

3 Galoisgruppen von biquadratischen Polynomen **75**

1 Irreduzibilitätskriterium biquadratischer Polynome . . 75

2 Flussdiagramm im Fall $\boldsymbol{p}(\boldsymbol{x}) = \boldsymbol{x}^4 + \boldsymbol{b}\boldsymbol{x}^2 + \boldsymbol{d}$ 82

3 Beispiele mit $\boldsymbol{p}(\boldsymbol{x}) = \boldsymbol{x}^4 + \boldsymbol{b}\boldsymbol{x}^2 + \boldsymbol{d}$ 84

3.1 Korollar 1, Fall (i) Galoisgruppe $\mathbf{V_4}$ 84

3.2 Korollar 1, Fall (ii) Galoisgruppe $\mathbf{C_4}$ 86
3.3 Korollar 1, Fall (iii) Galoisgruppe $\mathbf{D_4}$ 87

4 Implementierungen in Sage 91
1 Polynome vierten Grades 92
2 Statistik für Polynome vierten Grades 94
3 Biquadratische Polynome 96
4 Statistik für biquadratische Polynome 99

5 Anhang 101

Literaturverzeichnis 103

Index 105

Abbildungsverzeichnis

1.1 Untergruppen der S_4 bis auf Isomorphie 22
1.2 Alle Untergruppen der S_4 23

2.1 Klassifizierung von Polynomen vierten Grades 50

3.1 Klassifizierung von biquadratischen Polynomen . . . 83

Tabellenverzeichnis

1.1 Elemente der S_4 12
1.2 Untergruppen der S_4 15

4.1 Statistik für Polynome vierten Grades 96
4.2 Statistik für biquadratische Polynome 100

Einleitung

Im Zentrum der Arbeit stehen ein Satz über die Galoisgruppen von Polynomen vierten Grades und dessen Korollar für biquadratische Polynome. Mit deren Hilfe lassen sich die Galoisgruppen von Polynomen vierten Grades algorithmisch anhand der Koeffizienten bestimmen. Den Sätzen liegt das Paper „An Elementary Test for the Galois Group of a Quartic Polynomial“ von B. Warren und L.-C. Kappe [8, S. 133-137] zugrunde. Die vorliegende Arbeit ist ein Beispiel dafür, wie in einer konkreten Anwendung lineare Algebra, Gruppentheorie und Algebra zusammenspielen. In vielen Grundlagenwerken der Algebra wie jenen von Bosch [4], Karpfinger und Meyberg [9] oder dem von E. Artin [2] bzw. [3] werden die Galoisgruppen von Polynomen vierten Grades nicht systematisch klassifiziert. In den Monografien von M. Artin [1, S. 645] und G. Fischer [5, S. 401] werden hingegen die Galoisgruppen dieser Polynome fast vollständig klassifiziert. „Fast vollständig“ meint dabei, dass sich die Fälle der zyklischen Gruppe C_4 und der Diedergruppe D_4 dort nicht unterscheiden lassen.[1] Der in der vorliegenden Arbeit vorgestellte Satz aus dem Paper von Kappe und Warren [8, S. 133-137] vervollständigt die Klassifikation mittels eines Hilfspolynoms.

Um den Beweis des Satzes von Kappe und Warren [8, S. 134] vorzubereiten, werden einige Grundlagen benötigt, die in Kapitel 1 dargestellt werden. Die Galoisgruppen sind isomorph zu gewissen Untergruppen der symmetrischen Gruppe S_n, in unserem Falle der S_4. Daher werden in Kapitel 1 alle Untergruppen der S_4 vorgestellt und die Untergruppenbeziehungen in Abbildungen (siehe Abbildung 1.1 und Abbildung 1.2) illustriert. Die Sätze, die aus der Galoistheorie

[1] Beide Fälle fallen unter die dort angegebene Bedingung, dass die Diskriminante kein Quadrat und zugleich die kubische Resolvente reduzibel ist, und können damit nicht unterschieden werden.

im Beweis von Kappe und Warren [8, S. 135-136] verwendet werden, nämlich die Gradformel 7, das Fundamental-Lemma 1 und der Hauptsatz der Galoistheorie 10, werden in Kapitel 2 behandelt.
In Kapitel 2 folgt die Klassifizierung über Galoisgruppen von Polynomen vierten Grades mit ausführlichem Beweis (siehe Satz 13) [8, S.134-135]. In der Monographie von M. Artin [1, S. 645] wird ein anderes Kriterium für den Fall der Isomorphie der Galoisgruppe zur Kleinschen Vierergruppe V_4 angegeben. Wir weisen nach, dass dieses Kriterium mit dem analogen aus dem Paper von Kappe und Warren äquivalent ist. In Kapitel 3 erfolgt die Illustration des Satzes in einem Flussdiagramm. Bevor wir in Kapitel 5 zur Untersuchung der fünf Fälle des Satzes über die Galoisgruppen von Polynomen vierten Grades anhand von jeweils drei Beispielen übergehen, geben wir relevante Irreduzibilitätskriterien für Polynome in Kapitel 4 an.
In Kapitel 3 stehen anschließend Galoisgruppen von biquadratischen Polynomen im Fokus. Zunächst geben wir ein Irreduzibilitätskriterium speziell für biquadratische Polynome an, welches den Test auf Irreduzibilität für solche Polynome stark vereinfacht. Daraufhin folgt das Korollar, also die vereinfachte Klassifizierung der Galoisgruppen biquadratischer Polynome, mitsamt Beweis. Wiederum wird das Korollar mittels eines Flussdiagramms in Kapitel 2 illustriert.
In Kapitel 4 werden zwei selbstgeschriebene Programme zur Klassifizierung von Polynomen vierten Grades (s. Kapitel 1) und biquadratischen Polynomen (s. Kapitel 3) nach ihren Galoisgruppen in `Sage` präsentiert. Im Zuge der Implementierung und der Untersuchung der Beispiele kam die Frage nach der Häufigkeit der unterschiedlichen Galoisgruppen auf. Die Darstellung von je drei Beispielen zu jeder der fünf vorkommenden Galoisgruppen von Polynomen vierten Grades suggeriert womöglich eine gleichmäßig auftretende Häufigkeit aller fünf Fälle. Tatsächlich aber fand bereits Van der Waerden 1934 [14] beziehungsweise 1936 [15] heraus, dass der Fall der Isomorphie zur symmetrischen Gruppe S_n der häufigste Fall ist. Um dies zu verdeutlichen, werden abschließend die absoluten und relativen Häufigkeiten der Galoisgruppen von allgemeinen beziehungsweise biquadratischen Polynomen vierten Grades mit Koeffizienten aus einem vorgegebenen ganzzahligen Zahlenbereich (s. Kapitel 2 und 4) ermittelt.

1 Grundlagen

In diesem Kapitel werden gezielt die für den Klassifikationssatz von Polynomen vierten Grades notwendigen Grundlagen dargestellt. Galoisgruppen irreduzibler und separabler Polynome sind transitiv auf der Menge der Nullstelle operierende Untergruppen der symmetrischen Gruppe S_n vom Grad n. Deshalb wird in diesem Kapitel die symmetrische Gruppe S_4 mit allen und insbesondere auch mit diesen „transitiven“ Untergruppen vorgestellt. Im Anschluss werden drei Sätze der Galoistheorie, nämlich die Gradformel, das Fundamentallemma der Galoistheorie sowie der Hauptsatz der Galoistheorie, aufgeführt. Auf Beweise der zitierten Sätze wurde in diesem Kapitel bewusst verzichtet. Sie können der zitierten Literatur entnommen werden.

1 Die Struktur der symmetrischen Gruppe S_4

Im Folgenden werden die Definitionen der symmetrischen Gruppe samt ihrer Untergruppen angegeben.

Definition 1 (symmetrische Gruppe)**.** [5, S. 19][1, S. 46]
Eine Permutation von n Elementen einer endlichen Menge $M = \{\alpha_1, \ldots, \alpha_n\}$ mit $n \in \mathbb{N}$ ist eine bijektive Abbildung von M auf M. Die Menge

$$S_M := \{f : M \longrightarrow M \mid f \text{ ist bijektiv}\},$$

bildet eine Gruppe, die symmetrische Gruppe S_M von M. Die Verknüpfung in S_M ist die Komposition $\circ : S_M \longrightarrow S_M, (f, g) \mapsto f \circ g$ mit $(f \circ g)(x) := f(g(x))$ von Abbildungen. Für die Gruppenstruktur dieser Gruppe ist nur wichtig, dass $\alpha_1, \ldots, \alpha_n$ paarweise verschieden

sind. Meist rechnen wir daher o.B.d.A. mit $M = \{1, \ldots, n\}$ und sprechen von der symmetrischen Gruppe S_n.

Die Elemente der symmetrischen Gruppe stellen wir mit der Zykeldarstellung dar. Zur Erinnerung an die Zykeldarstellung geben wir ein Beispiel an.

Beispiel 1.
Sei $\tau \in S_6$, das heißt $\tau : \{1, 2, 3, 4, 5, 6\} \longrightarrow \{1, 2, 3, 4, 5, 6\}, k \mapsto \tau(k)$. Die Permutation sei durch folgende Zuordnungstabelle gegeben:

k	1	2	3	4	5	6
$\tau(k)$	5	4	3	6	1	2

.

Betrachten wir, wohin die Elemente von $\{1, 2, 3, 4, 5, 6\}$ durch τ verschoben werden: $1 \to 5 \to 1$ und $2 \to 4 \to 6 \to 2$ sowie $3 \to 3$. Dies führt zur kompakteren Zykeldarstellung der Permutation:
$\tau = (1, 5)(2, 4, 6) \in S_6$. Ein Element eines Zyklus wird auf das nächste Element abgebildet und das letzte Element eines Zyklus wird auf das erste Element abgebildet.

Alle 24 Elemente der S_4 sind in Tabelle 1.1 zu finden [5, S. 111].

Elemente von $\mathbf{S_4}$	Anzahl	Ordnung	Signum
id	1	1	+
$(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)$	6	2	−
$(1,2,3), (1,2,4), (1,3,4), (2,3,4),$ $(1,3,2), (1,4,2), (1,4,3), (2,4,3)$	8	3	+
$(1,2,3,4), (1,3,2,4), (1,4,2,3),$ $(1,2,4,3), (1,3,4,2), (1,4,3,2)$	6	4	−
$(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$	3	2	+
Summe	24		

Tabelle 1.1: Elemente der S_4

Wir wiederholen die Bezeichnungen der Untergruppen der S_4, die Definition einer Gruppenoperation und die Definition einer transitiven Gruppenoperation. Sämtliche Untergruppen der S_4 sind in Tabelle 1.2 auf Seite 15 zu finden.

Definition 2 (Signum einer Permutation)**.** [9, S. 126]
Zu $\sigma \in S_n$ betrachten wir

$$\operatorname{sign}(\sigma) = \prod_{1 \leqslant i < j \leqslant n-1} \frac{\sigma(i) - \sigma(j)}{i - j}$$

als das Signum von σ.

Bemerkung 1 (Rechenregel Signum einer Permutation)**.** [9, S. 126]
Eine Methode, um das Signum einer Permutation $\varphi \in S_n$ zu bestimmen, ist die Darstellung von φ als Produkt von k Transpositionen. Damit ist dann $\operatorname{sign}(\varphi) = (-1)^k$.

Beispiel 2.
Betrachte $(1,2,3)(4,5) \in S_5$. Diese Permutation können wir durch eine Verkettung von 3 Transpositionen darstellen:

$$(1,2,3)(4,5) = (1,3) \circ (1,2) \circ (4,5),$$

Daher ist

$$\operatorname{sign}\left((1,2,3)(4,5)\right) = (-1)^3 = -1.$$

Satz 1. [9, S. 126]
Die Abbildung $\operatorname{sign} : S_n \longrightarrow \{-1,+1\}, \varphi \mapsto \operatorname{sign}(\varphi)$ *ist ein Homomorphismus von Gruppen. Dabei wird* $\{-1,+1\} \subset \mathbb{Q}$ *als multiplikative Gruppe aufgefasst.*

Definition 3 (Normalteiler)**.** [1, S. 56]
Eine Untergruppe N einer Gruppe G heißt Normalteiler, wenn sie folgende Eigenschaft hat: Für jedes a aus N und jedes b aus G gilt $bab^{-1} \in N$. Wir schreiben dann $N \lhd G$.

Dies ist die formale Definition eines Normalteilers. Die wesentliche Eigenschaft ist, dass Normalteiler Kerne von Gruppenhomomorphismen sind. Denn es gilt:

Satz 2. [9, S. 55]
Ist $\varphi : G \longrightarrow H$ *ein Gruppenhomomorphismus, so ist* $\operatorname{Kern}(\varphi)$ *ein Normalteiler in* G.

Definition 4 (alternierende Gruppe)**.** [5, S. 33]
Die alternierende Gruppe A_n ist definiert als

$$\mathrm{Kern}(\mathrm{sign}) = \{\sigma \in \mathrm{S}_4 \mid \mathrm{sign}(\sigma) = +1\} =: A_n \lhd S_n.$$

Bemerkung 2.
Mit Bemerkung 1 erhalten wir, dass die Permutationen $\varphi \in \mathrm{A}_4$ gerade diejenigen sind, die sich durch eine Komposition einer geraden Anzahl von Transpositionen darstellen lassen.

Satz 3. [9, S. 127]
Für $n \geqslant 3$ wird A_n von den 3-Zyklen erzeugt.

Ein Dieder (übersetzt „Zweiflächner“) ist ein regelmäßiges n-Eck. Die Drehungen und Spiegelungen der Ebene, die ein Dieder in sich überführen, bilden die Diedergruppe. Deren Elemente denken wir uns als Permutationen der Eckpunkte $\{1, \ldots, n\}$. [5, S. 66]

Definition 5 (Diedergruppe)**.** [5, S. 66]
Sei $\sigma := (1, 2, \ldots, n)$ und $\tau = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & n & n-1 & \ldots & 2 \end{pmatrix}$. Dabei entspricht σ einer Drehung und τ einer Spiegelung. Diese beiden Abbildungen sind die Erzeuger der Diedergruppe.

$$D_n = \langle \sigma, \tau \rangle \subset S_n.$$

Bis auf Isomorphie ist die Diedergruppe D_n durch Erzeugende $\hat{\sigma}$ und $\hat{\tau}$ und die Relationen $\hat{\sigma}^n = \mathrm{id}$, $\hat{\tau}^2 = \mathrm{id}$ und $\hat{\tau}\hat{\sigma}\hat{\tau} = \hat{\sigma}$ bestimmt. Dass die in Definition 5 angegebenen Permutationen σ und τ diese Relationen erfüllen, rechnet man sofort nach.

Definition 6 (zyklische Gruppe)**.** [5, S. 69]
Eine Gruppe C heißt zyklisch, wenn es ein $a \in C$, sodass

$$C = \{a^k \mid k \in \mathbb{Z}\}.$$

Ist die Gruppe C endlich, mit $n \in \mathbb{N}$ Elementen so folgt

$$C = \left\{a^k \mid k \in \{0, \ldots, n-1\}\right\}.$$

Untergruppe der Ordnung 1		
id	id	$\{\mathrm{id}\}$
Untergruppe der Ordnung 2		
C_2	C_{21}	$\{\mathrm{id}, (1,2)(3,4)\}$
	C_{22}	$\{\mathrm{id}, (1,3)(2,4)\}$
	C_{23}	$\{\mathrm{id}, (1,4)(2,3)\}$
	C_{24}	$\{\mathrm{id}, (1,2)\}$
	C_{25}	$\{\mathrm{id}, (1,3)\}$
	C_{26}	$\{\mathrm{id}, (1,4)\}$
	C_{27}	$\{\mathrm{id}, (2,3)\}$
	C_{28}	$\{\mathrm{id}, (2,4)\}$
	C_{29}	$\{\mathrm{id}, (3,4)\}$
Untergruppe der Ordnung 3		
C_3	C_{31}	$\{\mathrm{id}, (1,2,3)(3,2,1)\}$
	C_{32}	$\{\mathrm{id}, (1,2,4)(1,4,2)\}$
	C_{33}	$\{\mathrm{id}, (1,3,4)(1,4,3)\}$
	C_{34}	$\{\mathrm{id}, (2,3,4)(4,3,2)\}$
Untergruppe der Ordnung 4		
C_4	C_{41}	$\{\mathrm{id}, (1,2,3,4), (1,4,3,2), (1,3)(2,4)\}$
	C_{42}	$\{\mathrm{id}, (1,3,2,4), (1,4,2,3), (1,2)(3,4)\}$
	C_{43}	$\{\mathrm{id}, (1,2,4,3), (1,3,4,2), (1,4)(2,3)\}$
V_4	V_4	$\{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$
	V_{41}	$\{\mathrm{id}, (1,2), (3,4), (1,2)(3,4)\}$
	V_{42}	$\{\mathrm{id}, (1,3), (2,4), (1,3)(2,4)\}$
	V_{43}	$\{\mathrm{id}, (1,4), (2,3), (1,4)(2,3)\}$
Untergruppe der Ordnung 6		
D_3	D_{31}	$\{\mathrm{id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$
	D_{32}	$\{\mathrm{id}, (1,2), (1,4), (2,4), (1,2,4), (1,4,2)\}$
	D_{33}	$\{\mathrm{id}, (1,3), (1,4), (3,4), (1,3,4), (1,4,3)\}$
	D_{34}	$\{\mathrm{id}, (2,3), (2,4), (3,4), (2,3,4), (2,4,3)\}$
Untergruppe der Ordnung 8		
D_4	D_{41}	$\{\mathrm{id}, (1,3), (2,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,3,4), (1,4,3,2)\}$
	D_{42}	$\{\mathrm{id}, (1,2), (3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,3,2,4), (1,4,2,3)\}$
	D_{43}	$\{\mathrm{id}, (1,4), (2,3), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,4,3), (1,3,4,2)\}$
Untergruppe der Ordnung 12		
A_4	A_4	$\{\mathrm{id}, (1,2,3), (1,2,4), (1,3,4), (2,3,4), (3,2,1), (4,2,1), (4,3,1),$ $(4,3,2), (1,2)(3,4), (1,3)(2,4), (2,3)(1,4)\}$
Untergruppe der Ordnung 24		
S_4	S_4	$\{\mathrm{id}, (1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2,3), (1,2,4),$ $(1,3,4), (2,3,4), (3,2,1), (4,2,1), (4,3,1), (4,3,2),$ $(1,2)(3,4), (1,3)(2,4), (2,3)(1,4)(1,2,3,4), (1,3,2,4),$ $(1,4,2,3), (1,2,4,3), (1,3,4,2), (1,4,3,2)\}$

Tabelle 1.2: Untergruppen der S_4

Eine zyklische Untergruppe der S_n wird von einem Zykel der Gestalt $\alpha = (a_1, \ldots, a_\ell)$ mit $1 \leqslant \ell \leqslant n$ erzeugt, wobei $\{a_1, \ldots, a_\ell\}$ eine ℓ-elementige Teilmenge von $\{1, \ldots, n\}$ ist und isomorph zu der Gruppe C_ℓ ist, die vom Zykel $\sigma = \{1, \ldots, \ell\} \in S_n$ erzeugt wird.[1]

Definition 7 (Kleinsche Vierergruppe)**.** [5, S. 19]
Die Kleinsche Vierergruppe ist definiert als:

$$\mathrm{V}_4 := \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (2,3)(1,4)\}.$$

In der Kleinschen Vierergruppe V_4 hat jedes Element die Ordnung 2. Bis auf Isomorphie ist V_4 dadurch charakterisiert, dass sie drei Elemente der Ordnung 2 enthält und das Produkt zweier dieser Elemente das jeweils dritte ergibt. Somit ist die Kleinsche Vierergruppe V_4 isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Notation 1.
Die Gruppen in Tabelle 1.2 bezeichnen wir so, dass der erste Index zum Namen (der Isomorphieklasse) der Gruppe gehört und der zweite Index die konkrete Gruppe nummeriert.

Wir wollen nun nachweisen, dass in Tabelle 1.2 alle Untergruppen der S_4 aufgelistet sind.

Satz 4 (Satz von Cauchy)**.** [9, S. 108]
Ist p ein Primteiler der Ordnung einer endlichen Gruppe, so besitzt diese ein Element der Ordnung p.

Für den nächsten Satz benötigen wir die Definition einer p-Sylowgruppe.

Definition 8. [9, S. 108]
Es sei p Primteiler der Ordnung einer endlichen Gruppe G und $|G| = p^r m$ mit $p \nmid m$ und $r \in \mathbb{N}$. Dann nennt man jede Untergruppe der Ordnung p^r von G eine p-Sylowgruppe von G.

Nachfolgender Satz folgt aus dem 2. Satz von Sylow [9, S. 110].

[1] Zeige, dass die Abbildung σ auf α ein Isomorphismus von Gruppen induziert.

Satz 5 (2. Satz von Sylow). [9, S. 110, Teil b]
Sei p Primteiler der Ordnung einer endlichen Gruppe G. Es gelte $|G| = p^r m$ mit $p \nmid m$ und $r \in \mathbb{N}$. Die Anzahl aller p-Sylowgruppen in G teilt m.

Satz 6 (Bestimmung aller Untergruppe der S_4).
Die Liste der Untergruppen von S_4 in Tabelle 1.2 auf Seite 15 ist vollständig.

Beweis. Zu überprüfen, dass die aufgeführten Mengen Gruppen sind, überlassen wir dem Leser. Nach dem Satz von Lagrange teilt die Ordnung einer beliebigen Untergruppe die Gruppenordnung, hier also 24.
Wir klassifizieren nun die Untergruppen nach ihrer Ordnung und beginnen mit der höchsten Ordnung.

„**Ordnung 24**“:
Offensichtlich haben wir nur eine Untergruppe der Ordnung 24, nämlich die S_4 selbst.

„**Ordnung 12**“:
Zu zeigen ist, dass es keine weitere Untergruppe der Ordnung 12 bis auf die A_4 gibt.
Sei also G eine Untergruppe der Ordnung 12. Dann ist $[S_4 : G] = 2$ und daher ist G ein Normalteiler in S_4 mit Restklassengruppe
$S_4/G \cong \mathbb{Z}^* = \{+1, -1\}$.
Für $a, b \notin G$ entsprechen die zugehörigen Restklassen $\bar{a}$ und $\bar{b}$ der -1 und $a \cdot b$ entspricht dann $(-1) \cdot (-1) = +1$. Es folgt also $a \cdot b \in G$. Insbesondere ist sowohl für $g \in G$ als auch für $g \notin G$ stets $g^2 \in G$. Für alle $s \in S_4$ erhalten wir $s^2 \in G$. Sei $s \in S_4$ mit $\operatorname{ord}(s) = 3$, dann ist $s^2 = s^{-1}$ also $s^{-1} \in G$. Da G eine Untergruppe von S_4 ist, muss auch $s \in G$ liegen. Also enthält G alle Dreierzykel. Diese erzeugen schon die A_4 nach Satz 3. Also ist $A_4 \subseteq G$. Wegen $|A_4| = 12$ folgt $G = A_4$.

„**Ordnung 8**“:
Sei $|G| = 8$, so ist G eine 2-Sylow-Gruppe von S_4, denn $24 = 2^3 \cdot 3$ (siehe Definition 8). Nach dem 2. Satz von Sylow (siehe Satz 5) teilt die Anzahl der 8-Sylow-Gruppen 3 und ist deshalb maximal 3. Das heißt, die Auflistung in der Tabelle 1.2 in der Zeile D_4 ist vollständig.

„**Ordnung 6**“:
Sei $|G| = 6$, so gibt es nach dem Satz von Cauchy (siehe Satz 4) Elemente $g, h \in G$ mit $|g| = 3$ und $|h| = 2$. Dann haben $g, h \in S_4$ Zykeldarstellungen etwa $g = (i, j, k)$ und $h = (\ell, m)$.
Falls $\{\ell, m\} \subset \{i, j, k\}$, folgt $G = S_{\{i,j,k\}}$, denn ein Zykel der Länge n und eine Transposition in der Zykeldarstellung nebeneinanderstehender Elemente erzeugen nach [9, S. 129] und [10, S. 51] schon die S_n. In dem Zykel (i, j, k) stehen alle Elemente nebeneinander. So erhalten wir die in Tabelle 1.2 in Zeile D_3 aufgezählten Gruppen.
Falls $\{\ell, m\} \not\subset \{i, j, k\}$ ist eine der Zahlen ℓ oder m nicht in $\{i, j, k\}$. Sei o.B.d.A. $m \notin \{i, j, k\}$. Da $\{i, j, k, m\} = \{1, 2, 3, 4\}$ und $\ell \neq m$ ist, folgt $\ell \in \{i, j, k\}$. Wir können o.B.d.A. $\ell = i$ wählen, da
$(i, j, k) = (k, i, j) = (j, k, i)$.
Wir rechnen $(i, m) \circ (i, j, k) = (i, j, k, m) \in G$. Dies steht im Widerspruch dazu, dass G kein Element der Ordnung 4 enthalten kann, da $4 \nmid |G|$.
Die Auflistung in Tabelle 1.2 in Zeile D_3 ist also vollständig.

„**Ordnung 4**“:
Sei $|G| = 4$. Wenn G ein Element φ der Ordnung 4 enthält, wird G von φ erzeugt und G ist isomorph zur zyklischen Gruppe C_4. Ein $g \in S_4$ der Ordnung 4 hat stets die Gestalt $(1, i, j, k)$ mit
$\{i, j, k\} = \{2, 3, 4\}$. Es gibt also $3! = 6$ solche g. Die Gruppe $\langle(1, i, j, k)\rangle$ enthält stets $(1, i, j, k)^{-1} = (1, k, j, i)$.
Das heißt $(1, 4, 3, 2) \in \overbrace{\langle(1, 2, 3, 4)\rangle}^{C_{41}}$, $(1, 4, 2, 3) \in \overbrace{\langle(1, 3, 2, 4)\rangle}^{C_{42}}$ und $(1, 3, 4, 2) \in \overbrace{\langle(1, 2, 4, 3)\rangle}^{C_{43}}$. Das heißt die unter $C_{4\bullet}$ aufgeführten Gruppen in Tabelle 1.2 enthalten bereits alle Elemente der Ordnung 4. Die Aufzählung der zyklischen Gruppen der Ordnung 4 in Tabelle 1.2 ist

also vollständig.
Betrachten wir nun nicht-zyklische Gruppen der Ordnung 4. Jedes Element einer solchen Gruppe G muss (wegen $3 \nmid |G|$) Ordnung 2 haben. In Tabelle 1.1 sind alle 9 Elemente der Ordnung 2 zu sehen. Die „Doppeltranspositionen“ $(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$ sind in der letzten Zeile aufgeführt. Sie bilden zusammen mit id die Kleinsche Vierergruppe V_4.
Alle anderen nicht-zyklischen Gruppen G der Ordnung 4 müssen also mindestens eine Transposition (i,j) mit $i,j \in \{1,2,3,4\}, i \neq j$ enthalten. Wäre nun $(i,k) \in G$ mit $k \notin \{i,j\}$, so wäre
$(i,k) \circ (i,j) = (i,j,k) \in G$ ein Element der Ordnung 3, Widerspruch $\lightning$, da $3 \nmid |G|$. Analog führt $(i,j) \circ (j,k) = (i,j,k)$ zum Widerspruch. Weitere Elemente von G können nur noch $(i,j)(k,\ell)$ oder (k,ℓ) mit $\{k,\ell\} = \{1,2,3,4\} \setminus \{i,j\}$ sein. Zusammen mit der Identität muss G also somit genau die Elemente $G = \{\mathrm{id}, (i,j), (k,\ell), (i,j)(k,\ell)\}$ enthalten und ist durch (i,j) eindeutig festgelegt.
Die unter V_4 aufgelisteten Gruppen V_{41}, V_{42} und V_{43} in Tabelle 1.2 sind daher neben der V_4 alle weiteren nicht-zyklischen Untergruppen der Ordnung 4.

„**Ordnung 3**“:
Untergruppen G der Ordnung 3 von S_4 sind zyklisch, da 3 eine Primzahl ist.
G wird durch ein Element der Ordnung 3 erzeugt, das heißt,
$G = \langle (i,j,k) \rangle$, wobei o.B.d.A. $i = \min\{i,j,k\}$ mit paarweise verschiedenen $i,j,k \in \{1,2,3,4\}$ sei. Es ergibt sich
$G = \{\mathrm{id}, (i,j,k), (i,j,k)^2 = (i,k,j)\}$. Es gibt 8 Elemente der Ordnung 3 in S_4 (siehe Tabelle 1.1). Da jede Gruppe G der Ordnung 3 neben id zwei Elemente der Ordnung 3 enthält, die beide G erzeugen, gibt es genau die vier Untergruppen C_{41}, C_{42}, C_{43} und C_{44} der S_4 der Ordnung 3.

„**Ordnung 2**“:
Die Untergruppen der Ordnung 2 von S_4 bestehen aus der Identität und einem Element der Ordnung 2. Es gibt $\binom{4}{2} = 6$ Möglichkeiten für Transpositionen (i,j) mit $\{i,j\} \subset \{1,2,3,4\}$ und $i \neq j$. Wir kön-

nen jede Transposition (i,j) ergänzen zum Element $(i,j)(k,\ell) \in S_4$ mit $(k,\ell) = \{1,2,3,4\} \setminus \{i,j\}$. Wegen $(i,j)(k,\ell) = (k,\ell)(i,j)$ führen je zwei der 6 Ergänzungen zur selben Permutation. Wir haben also drei Elemente der Ordnung 2, die auch in A_4 liegen. Insgesamt gibt es daher 9 Elemente der Ordnung 2 und damit 9 Untergruppen der Ordnung 2 (siehe Tabelle 1.1).

„**Ordnung 1**“:
Jede Gruppe muss die Identität id enthalten, womit es nur eine Untergruppe der Ordnung 1, nämlich $\{\mathrm{id}\}$, geben kann.

Es gibt also insgesamt 28 nicht-triviale Untergruppen der S_4. □

Definition 9 (Operation)**.** [1, S. 197]
Eine Gruppe $(G,\circ)$ operiert auf einer Menge $M \neq \emptyset$, wenn jedem Paar $(g,m) \in G \times M$ ein Element $g \cdot m \in M$ zugeordnet wird. Diese Operation von G auf M muss dabei folgende Axiome erfüllen:

$$1 \cdot m = m \;\forall\; m \in M, \text{ wobei } 1 \in G \text{ das neutrale Element ist;}$$
$$\forall g, g' \in G, m \in M \text{ gilt } (g \circ g') \cdot m = g \cdot (g' \cdot m) \text{ Assoziativgesetz.}$$

In der multiplikativen Schreibweise werden oft $\circ$ und $\cdot$ weggelassen, wenn keine Verwechselungsgefahr besteht.

Definition 10 (transitive Operation)**.** [5, S. 103]
Man sagt eine Gruppe G operiert transitiv auf einer Menge M, wenn G auf M operiert und wenn es zu je zwei Elementen $x, y \in M$ ein $g \in G$ gibt mit

$$g(x) = y.$$

Beispielsweise operiert für eine endliche Menge M die Gruppe S_M auf der Menge M.

Definition 11 (transitive Untergruppe von S_n)**.** [1, S. 640]
Sei M eine endliche Menge und $G \subset S_M$ eine Untergruppe der symmetrischen Gruppe, dann nennen wir G eine transitive Untergruppe von S_M, wenn G transitiv auf M operiert.

In Abbildung 1.1 auf Seite 22 sind die Untergruppen der S_4 bis auf Isomorphie zu sehen. Auf denselben Höhen sind jeweils (Isomorphieklassen von) Untergruppen identischer Ordnung zu finden. Ein Pfeil bedeutet: die Gruppe, von der der Pfeil ausgeht, ist isomorph zu einer Untergruppe der Gruppe, auf die der Pfeil zeigt. Ein Pfeil ist rot eingezeichnet, falls die kleinere Gruppe isomorph zu einem Normalteiler der größeren Gruppe ist. Die transitiven Gruppen sind in Lila dargestellt. Für die nicht-transitiven Gruppen sind folgende Farben gewählt. Die zyklischen Gruppen sind in Grün, die Diedergruppen in Orange, die nicht-transitiven zur Kleinschen Vierergruppe V_4 isomorphen Gruppen in Blau und die einelementige Gruppe $\{id\}$ ist in Gelb dargestellt.
In Abbildung 1.2 auf Seite 23 sind alle 30 Untergruppen der S_4 inklusive der trivialen Untergruppen $\{id\}$ und S_4 aufgeführt. Auf denselben Höhen sind wiederum Untergruppen identischer Ordnung dargestellt. In diesem Diagramm bedeutet ein Pfeil „ist Untergruppe von“. Wiederum sind die transitiven Gruppen in Lila dargestellt. Für die nicht-transitiven Gruppen sind folgende Farben gewählt. Die zyklischen Gruppen sind in Grün, die Diedergruppen in Orange, die nicht-transitiven zur Kleinschen Vierergruppe V_4 isomorphen Gruppen in Blau und die einelementige Gruppe $\{id\}$ in Gelb dargestellt. Die Pfeile sind mit Rot gezeichnet, falls die Untergruppe ein Normalteiler der oberen Gruppe ist. Dabei ist zu beachten, dass die Normalteilerrelation im Allgemeinen nicht transitiv ist.

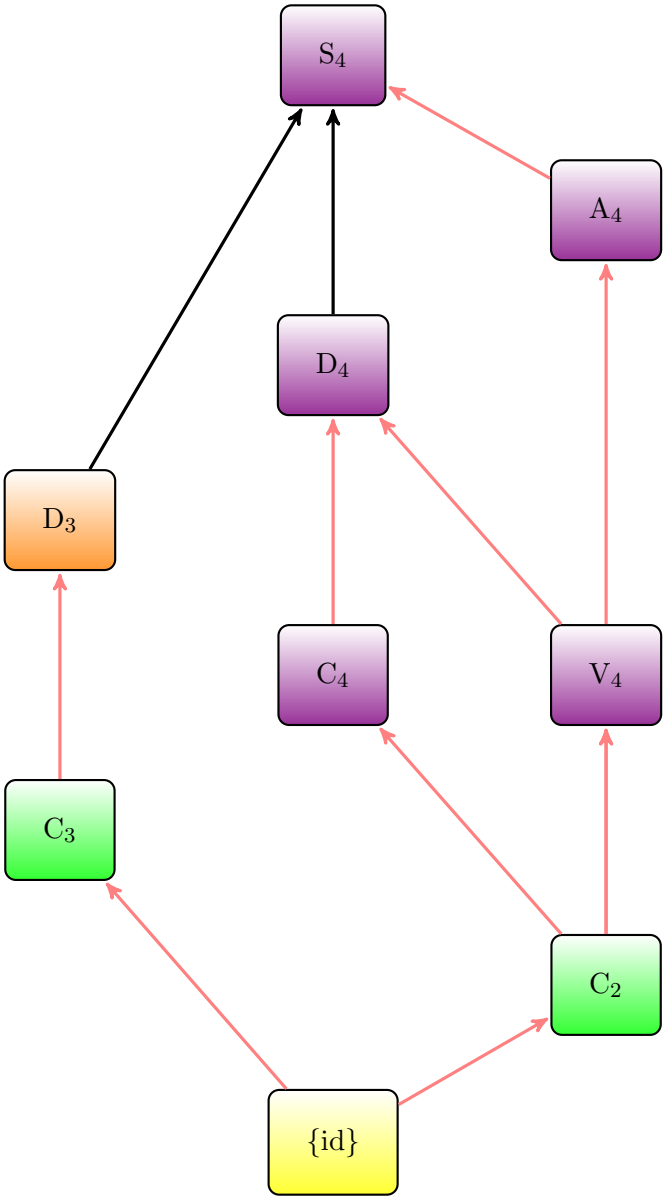


Abbildung 1.1: Untergruppen der S_4 bis auf Isomorphie
Quelle: Eigene Grafik erstellt mit TikZ

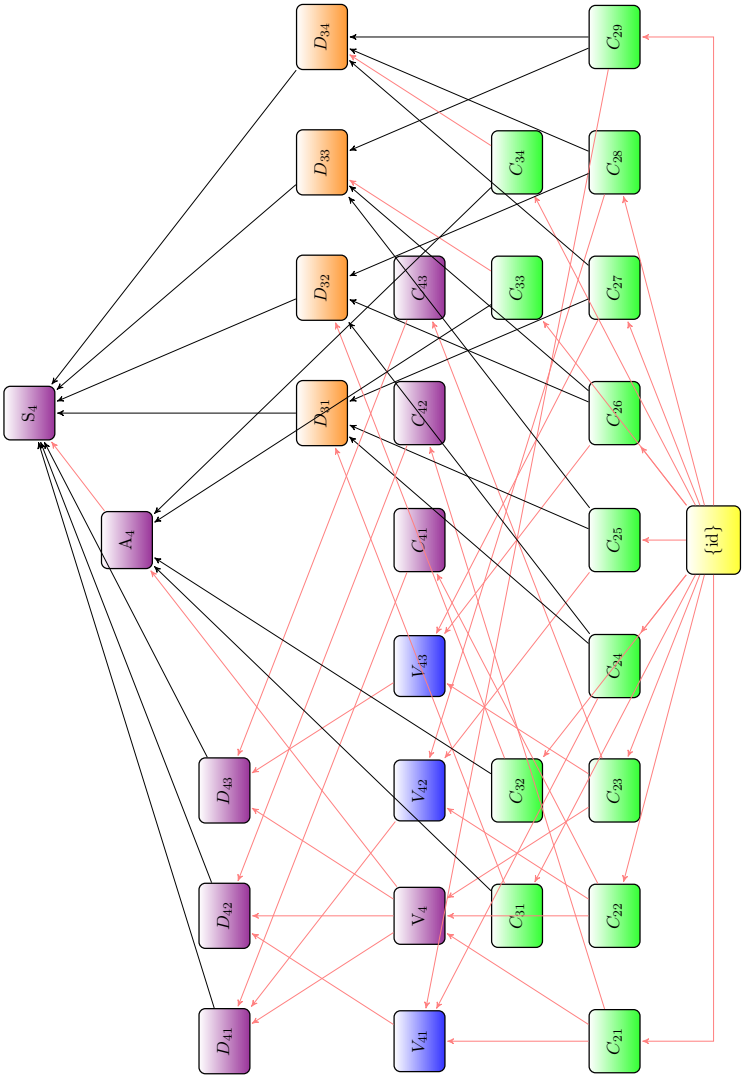


Abbildung 1.2: Alle Untergruppen der S_4
Quelle: Eigene Grafik erstellt mit TikZ

2 Galoistheorie

Für den Beweis des Klassifikationssatzes für Galoisgruppen von Polynomen vierten Grades werden wir den Gradsatz, das Fundamentallemma der Galoistheorie und den Hauptsatz der Galoistheorie benötigen. Daher geben wir in diesem Kapitel nun die Sätze an.

Definition 12 (Charakteristik eines Ringes)**.** [1, S. 409]
Sei R ein Ring mit Einselement 1_R, dann gibt es einen Homomorphimus von Ringen $\varphi : \mathbb{Z} \to R$, der durch $1 \mapsto 1_R$ induziert wird. Die Charakteristik eines Ringes R ist die nichtnegative Zahl n, die den Kern von φ erzeugt.

Definition 13 (Körpererweiterung)**.** [9, S. 271]
Sei $K \subseteq E$ und K, E Körper, wobei $+, \cdot$ in K die gleichen Verknüpfungen wie in E sind. Dann heißt K Unterkörper von E und E Erweiterungskörper von K. Wir nennen die Inklusion $K \subseteq E$ eine Körpererweiterung, die wir als E/K notieren.

Definition 14 (endlich erzeugte Körpererweiterung)**.** [9, S. 271]
Sei $K \subseteq E$ eine Körpererweiterung und seien $\alpha_1, ..., \alpha_n \in E$. Wir definieren $K(\alpha_1, ..., \alpha_n)$ als den kleinsten Unterkörper von E, welcher K und $\alpha_1, ..., \alpha_n$ enthält. Wir nennen $K(\alpha_1, ..., \alpha_n)$ die aus K durch Adjungieren von $\alpha_1, ..., \alpha_n \in E$ erzeugte Körpererweiterung. Der „kleinste“ Unterkörper bedeutet hier die Schnittmenge aller Unterkörper $E' \subseteq E$, die K und $\alpha_1, ..., \alpha_n$ enthalten.

$$K(\alpha_1, ..., \alpha_n) = \bigcap_{\{K \cup \{\alpha_1, ..., \alpha_n\}\} \subseteq E' \subseteq E} E'$$

Definition 15 (algebraisches Element)**.** [6, S. 127]
Sei $E \supset K$ eine Körpererweiterung. Ein Element $\alpha \in E$ heißt algebraisch über K, wenn es Nullstelle eines Polynoms aus $K[x] \setminus \{0\}$ ist.

Definition 16 (algebraische Körpererweiterung)**.** [6, S. 130]
Sei $E \supset K$ eine Körpererweiterung. Sind alle Elemente von E über K algebraisch, dann spricht man von einer algebraischen Körpererweiterung.

Sei K ein Körper. Dann können wir eine Körpererweiterung E als Vektorrauam über K ansehen und definieren:

Definition 17 (Grad einer Körpererweiterung)**.** [1, S. 568]
Sei E eine endliche Körpererweiterung von K. Die Dimension $\dim_K E$ des Vektorraumes E über K heißt Grad der Körpererweiterung. Wir schreiben

$$\mathrm{Grad}(E/K) := [E : K] := \dim_K E.$$

Satz 7 (Gradformel)**.** [1, S. 569]
Seien $K \subseteq E \subseteq F$ drei Körper, wobei $K \subseteq E$ und $E \subseteq F$ zwei endliche Körpererweiterungen sind. Dann gilt:

$$\mathrm{Grad}(F/K) = \mathrm{Grad}(E/K) \cdot \mathrm{Grad}(F/E).$$

Definition 18 (endliche Körpererweiterung)**.** [6, S. 125]
Sei $E \supset K$ eine Körpererweiterung. Wir sagen die Körperweiterung ist endlich, wenn
$\mathrm{Grad}(E/K) < \infty$, dass heißt, E ist ein endlich dimensionaler Vektorraum über K.

Satz 8. [6, S. 130]
Sei $E \supset K$ eine Körpererweiterung. Dann gilt:

(i) *Ist die Körpererweiterung $E \supset K$ endlich, so ist sie algebraisch und es gibt $\alpha_1, \ldots, \alpha_n \in E$ mit $E = K(\alpha_1, \ldots, \alpha_n)$.*

(ii) *Gibt es über K algebraische Elemente $\alpha_1, \ldots, \alpha_n \in E$ mit*

$E = K(\alpha_1, \ldots, \alpha_n)$, so ist die Körpererweiterung endlich und damit algebraisch.

Bemerkung 3.
Wir werden nur Nullstellen von Polynomen aus $K[x]$ adjungieren. Dadurch entstehen stets algebraische Körpererweiterungen.

Definition 19 (Minimalpolynom). [6, S. 129]
Sei $E \supset K$ eine Körpererweiterung und $\alpha \in K$ algebraisch über K, dann gibt es ein eindeutig bestimmtes normiertes Polynom
$f_\alpha \in K[x] \setminus \{0\}$ minimalen Grades mit $f_\alpha(\alpha) = 0$. Dieses wird als Minimalpolynom bezeichnet.[2]

Definition 20 (Zerfällungskörper). [1, S. 618]
Gegeben ist ein Körper K und ein normiertes nicht konstantes Polynom $f(x) \in K[x]$ vom Grad n. Ein Erweiterungskörper E von K heißt Zerfällungskörper von f über K, wenn folgende Eigenschaften gelten:

(i) Das Polynom f zerfällt in E vollständig in Linearfaktoren, das heißt, es gibt

$$\alpha_1, \ldots, \alpha_n \in E \text{ mit } f(x) = \prod_{i=1}^{n} (x - \alpha_i).$$

(ii) Es ist

$$E = K(\alpha_1, ..., \alpha_n),$$

das heißt, E ist minimal mit der Eigenschaft (i).

Der Zerfällungskörper ist bis auf Isomorphie eindeutig.

Definition 21 (separables Polynom). [11, S. 131]
Ein Polynom $f(x) \in K[x]$ heißt separabel, wenn jeder irreduzible Faktor von f keine mehrfachen Nullstellen in einem Zerfällungskörper von f besitzt.

[2] Unsere Definition ist eine der zur Definition des Minimalpolynoms laut Fischer [5, S. 299] äquivalenten Definition. So vermeiden wir die Verwendung von Idealen.

Definition 22 (normale Körpererweiterung). [9, S. 321]
Sei K ein Körper und $E \supset K$ eine Körpererweiterung, dann heißt E normal über K, wenn E Zerfällungskörper eines Polynoms f in K ist.

Für jeden Körper K bildet die Menge

$$\mathrm{Aut}(K) := \{\varphi : K \to K \mid \varphi \text{ Automorphismus}\}$$

zusammen mit der Hintereinanderschaltung von Abbildungen als Verknüpfung eine Gruppe. Sei $K \subset F$ eine Körpererweiterung, so ist

$$\mathrm{Aut}(F; K) := \{\varphi \in \mathrm{Aut}(F) \mid \varphi(x) = x \text{ für alle } x \in K\}$$

eine Untergruppe von $\mathrm{Aut}(F)$. Die Gruppe $\mathrm{Aut}(K)$ heißt Automorphismengruppe von K und die Gruppe $\mathrm{Aut}(F; K)$ heißt Gruppe der relativen Automorphismen von F/K [5, S. 364] .

Definition 23 (Galoisgruppe). [5, S. 364]
Sei K ein Körper und sei $f(x) \in K[x]$ ein normiertes Polynom. Ist $F \supset K$ Zerfällungskörper von $f(x) \in K[x]$, so nennt man

$$\mathrm{Gal}(f; K) := \mathrm{Aut}(F; K)$$

die Galoisgruppe von f über K.

Definition 24 (galoissche Körpererweiterung). [11, S. 131]
Sei K ein Körper und $E \supset K$ eine endliche Körpererweiterung. Sei $G := \mathrm{Gal}(f; K)$ die Galoisgruppe von E über K. Dann heißt E Galoiserweiterung von K oder galoissch über K, falls
$\mathrm{ord}(G) = [E : K]$ gilt.

Satz 9. [11, S. 131]
Für eine endliche Körpererweiterung $E \supset K$ sind äquivalent:

(a) *E ist galoissch über K.*

(b) *E ist Zerfällungskörper eines separablen Polynoms aus $K[X]$.*

Lemma 1 (Fundamental-Lemma). [5, S. 364]
Sei K ein Körper, $f \in K[x]$ mit $n := \mathrm{Grad}(f) \geqslant 1$. Weiter sei $F \supset K$ Zerfällungskörper von f und $G := \mathrm{Gal}(f; K) = \mathrm{Aut}(F; K)$. Ferner bezeichne N die Menge der paarweise verschiedenen Nullstellen von f, das heißt, $N = \{x_1, \ldots, x_r\} \subset F$ mit $r \leqslant n$. Wir identifizieren $S_{\{x_1,\ldots,x_r\}}$ wie in Definition 1 mit S_r. Dann gelten:

(a) *Für alle $\varphi \in G$ ist $\varphi(N) = N$ und der dadurch induzierte Homomorphismus*

$$\tau : G \to S_r\,,\ \varphi \mapsto \varphi|_N$$

ist injektiv. Man kann also G als Untergruppe von S_r ansehen. Insbesondere folgt

$$\mathrm{ord}(G) \text{ teilt } r!\,,$$

folglich ist G endlich.

(b) *Ist f irreduzibel, so ist die Operation von G auf N transitiv. Insbesondere folgt*

$$r \text{ teilt } \mathrm{ord}(G)$$

und n teilt $\mathrm{ord}(G)$, falls f separabel ist.

(c) *Ist f das Minimalpolynom des erzeugenden Elements $u \in F$ einer einfachen Erweiterung $F = K(u) \supset K$, so ist*

$$\mathrm{ord}(G) = r.$$

Ist f separabel, so folgt

$$\mathrm{ord}(G) = \mathrm{Grad}(f) = n.$$

(d) *Ist K endlich oder $\mathrm{char}(K) = 0$, so gilt für jedes $f \in K[x]$ mit Zerfällungskörper $F \supset K$*

$$\mathrm{ord}(G) = [F : K].$$

Satz 10 (Hauptsatz der Galoistheorie). [11, S. 133]
Sei F/K eine galoissche Körpererweiterung mit Galoisgruppe G. Dann gelten:

(a) *Es gibt eine bijektive Beziehung zwischen den Untergruppen*

$H \subset G$ und den Zwischenkörpern $K \subset L \subset F$, welche Inklusionen umkehrt. Sei $H \subset G$ eine Untergruppe. Dieser Untergruppe ordnen wir den Körper

$$F^H := \{f \in F \mid \varphi(f) = f \text{ für alle } \varphi \in H\}$$

zu. Umgekehrt ordnen wir jedem Zwischenkörper L die Untergruppe $H \subset G$, welche alle Elemente von L invariant lässt, zu. Das ist $\mathrm{Aut}_L(F)$.

$$\begin{array}{ccccccccc} \{id\} & \subset & H_1 & \subset & H_2 & \subset \ldots \subset & H_n & = & G \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ F & \supset & L_1 & \supset & L_2 & \supset \ldots \supset & L_n & = & K \end{array} \quad \begin{array}{c} \textit{aufsteigende Kette} \\ \textit{von Untergruppen} \\ \\ \textit{absteigende Kette} \\ \textit{von Zwischenkörpern} \end{array}$$

mit $L_i = F^{H_i}$ und $H_i = \mathrm{Aut}_{L_i}(F)$.

(b) *Die einzigen Elemente von F, welche unter allen Automorphismen $\varphi \in G$ invariant sind, sind die Elemente von K. Mit der Notation:*

$$F^G := \{f \in F \mid \varphi(f) = f \text{ für alle } \varphi \in G\},$$

ist also $F^G = K$.

Beweis. Teil (a) ist in [11, S. 133, 16.1] die Hauptaussage.
Ebenfalls dort wird für $Z \in \{L_1, \ldots, L_n\}$ die Gleichung

$$[Z : K] = \frac{|G|}{|G(F/Z)|}$$

gezeigt.

Zum Beweis von Teil (b) betrachten wir $Z = F^G$. Dann gilt trivialerweise $G(F/Z) = G$, da Z gerade als die Menge der Elemente, die unter G invariant bleiben, definiert ist. Daraus folgt

$$[Z : K] = \dim_K Z = 1 \Longrightarrow F^G = Z = K. \qquad \square$$

2 Galoisgruppen von Polynomen vierten Grades

Sei $p(x) = x^4 + ax^3 + bx^2 + cx + d$ ein Polynom über einem Grundkörper K mit Zerfällungskörper F und $p(x) = \prod_{i=1}^{4}(x - \alpha_i)$, wobei $\alpha_1, \ldots, \alpha_4 \in F$ seien. Bezeichne $K^2 = \{k^2 \mid k \in K\}$ die Menge aller Quadrate in K. Falls $p(x)$ irreduzibel und separabel ist, ist $|\{\alpha_1, \ldots, \alpha_4\}| = 4$ und die Galoisgruppe $\mathrm{Gal}(F/K)$ wirkt transitiv auf den vier Nullstellen (siehe Fundamental-Lemma 1 Teil b). Deshalb muss $\mathrm{Gal}(F/K)$ isomorph zu einer der transitiven Untergruppen der S_4 sein:

(i) der Kleinschen Vierergruppe V_4 der Ordnung 4,

(ii) der zyklischen Gruppe C_4 der Ordnung 4,

(iii) der Diedergruppe D_4 der Ordnung 8,

(iv) der alternierenden Gruppe A_4 der Ordnung 12,

(v) oder der symmetrischen Gruppe S_4 der Ordnung 24.

Nachfolgend wird angenommen, dass die Charakteristik des Grundkörpers K nicht 2 ist. Dies stellt sicher, dass das Polynom $p(x)$, falls es irreduzibel ist, separabel ist, da $p(x) = x^4 + \ldots$ und daher $p'(x) = 4x^3 + \ldots \neq 0$ für $\mathrm{char}(K) \neq 2$ ist (vgl. [8, S. 133-134]).

1 Begrifflichkeiten zur Klassifizierung

Bemerkung 4 (elementarsymmetrische Funktionen)**.**
Die Koeffizienten a, b, c, d von $p(x)$ lassen sich über die sogenannten

elementarsymmetrischen Funktionen in $\alpha_1, \ldots, \alpha_4$ ausdrücken.[1]

$$a = -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) \tag{2.1}$$

$$b = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 \tag{2.2}$$

$$c = -(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4) \tag{2.3}$$

$$d = \alpha_1\alpha_2\alpha_3\alpha_4 \tag{2.4}$$

Beweis. Es ist:

$$\begin{aligned}
\prod_{i=1}^{4}(x - \alpha_i) &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4) \\
&= (x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2) \cdot (x^2 - (\alpha_3 + \alpha_4)x + \alpha_3\alpha_4) \\
&= x^4 \\
&\quad - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)x^3 \\
&\quad + ((\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) + (\alpha_3\alpha_4 + \alpha_1\alpha_2))x^2 \\
&\quad - ((\alpha_1 + \alpha_2)\alpha_3\alpha_4 + \alpha_1\alpha_2(\alpha_3 + \alpha_4))x \\
&\quad + \alpha_1\alpha_2\alpha_3\alpha_4 \\
&= x^4 \\
&\quad - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)x^3 \\
&\quad + (\alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_1\alpha_2 + \alpha_3\alpha_4)x^2 \\
&\quad - (\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4)x \\
&\quad + \alpha_1\alpha_2\alpha_3\alpha_4 \\
&= x^4 + ax^3 + bx^2 + cx + d \\
&= p(x).
\end{aligned}$$

Koeffizientenvergleich ergibt die Behauptung. □

Definition 25 (kubische Resolvente)**.** [8, S. 134]
Das Polynom

$$r(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$$

[1] Die Bezeichnung kommt daher, dass diese Polynome unter Permutationen der Indizes, also einer Operation der symmetrischen Gruppe, invariant sind.

heißt die kubische Resolvente von $p(x)$. Wir schreiben $r(x)$ auch als

$$r(x) = x^3 - bx^2 + Bx - A$$
$$\text{mit } A = a^2d - 4bd + c^2 \text{ und } B = ac - 4d.$$

Definition 26 (Diskriminante eines Polynoms)**.** [9, S. 417]
Sei K ein Körper. Für ein Polynom $f(x) \in K[x]$ mit Zerfällungskörper F und der Darstellung

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i) \text{ mit } \alpha_1, \ldots, \alpha_n \in F$$

wird die Diskriminante definiert durch:

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

Bemerkung 5. [9, S. 417]
Mit den Bezeichnungen aus der Definition 26 gilt $D_f \in K$.

Wir zeigen, dass die kubische Resolvente $r(x)$ dieselbe Diskriminante wie $p(x)$ hat.

Definition 27.
Seien t_1, t_2 und t_3 wie folgt definiert:

$$t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4,$$
$$t_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 \text{ und}$$
$$t_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Bemerkung 6 (Nullstellen der kubischen Resolvente)**.**
Die Nullstellen der kubischen Resolvente $r(x)$ sind t_1, t_2 und t_3 aus Definition 27.

Beweis. Wir zeigen, dass $r(x)$ die Darstellung

$$r(x) = (x - t_1)(x - t_2)(x - t_3)$$

besitzt.[2] Sei

$$\begin{aligned}\tilde{r}(x) :=&(x-t_1)(x-t_2)(x-t_3)\\ =&(x^2-(t_1+t_2)x+t_1t_2)(x-t_3)\\ =&x^3-(t_1+t_2)x^2+t_1t_2x-t_3x^2+(t_1+t_2)t_3x-t_1t_2t_3\\ =&x^3-(t_1+t_2+t_3)x^2+(t_1t_2+t_1t_3+t_2t_3)x-t_1t_2t_3.\end{aligned}$$

Die kubische Resolvente ist:

$$\begin{aligned}r(x) &= x^3-bx^2+Bx-A\\ &= x^3-bx^2+(ac-4d)x-(a^2d-4bd+c^2).\end{aligned}$$

Nach Koeffizientenvergleich gilt $r(x)=\tilde{r}(x)$ genau dann, wenn die Koeffizienten übereinstimmen, das heißt, wenn gilt

$$b = t_1+t_2+t_3, \tag{2.5}$$

$$B = ac-4d = t_1t_2+t_1t_3+t_2t_3 \text{ und} \tag{2.6}$$

$$A = a^2d-4bd+c^2 = t_1t_2t_3. \tag{2.7}$$

Es wird nachgerechnet, dass die Bedingungen (2.5),(2.6) und (2.7) erfüllt sind. Dann ist $r(x)=(x-t_1)(x-t_2)(x-t_3)$ und damit sind t_1, t_2 und t_3 Nullstellen von $r(x)$. Aus Bemerkung 4 folgt

$$\begin{aligned}(2.5): b &= \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4\\ &= \alpha_1\alpha_2+\alpha_1\alpha_4+\alpha_1\alpha_3+\alpha_2\alpha_4+\alpha_1\alpha_4+\alpha_2\alpha_3\\ &= t_1+t_2+t_3.\end{aligned}$$

Aus Bemerkung 4 und Definition 25 folgt

$$\begin{aligned}(2.6): B = &-(\alpha_1+\alpha_2+\alpha_3+\alpha_4)\\ &\cdot(-(\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4))\\ &-4\cdot\alpha_1\alpha_2\alpha_3\alpha_4\end{aligned}$$

[2] Es ließe sich auch direkt nachrechnen, dass t_1, t_2 und t_3 Nullstellen von $r(x)$ sind. Für t_1 wird dies im Anhang ausgeführt.

$$
\begin{aligned}
&= \alpha_1^2\alpha_2\alpha_3 + \alpha_1^2\alpha_2\alpha_4 + \alpha_1^2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2^2\alpha_3 \\
&\quad + \alpha_1\alpha_2^2\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_4 + \alpha_2^2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3^2 + \alpha_1\alpha_2\alpha_3\alpha_4 \\
&\quad + \alpha_1\alpha_3^2\alpha_4 + \alpha_2\alpha_3^2\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_4^2 + \alpha_1\alpha_3\alpha_4^2 \\
&\quad + \alpha_2\alpha_3\alpha_4^2 - 4\cdot\alpha_1\alpha_2\alpha_3\alpha_4 \\
&= \alpha_1^2\alpha_2\alpha_3 + \alpha_1^2\alpha_2\alpha_4 + \alpha_1^2\alpha_3\alpha_4 + \alpha_1\alpha_2^2\alpha_3 \\
&\quad + \alpha_1\alpha_2^2\alpha_4 + \alpha_2^2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3^2 + \alpha_1\alpha_3^2\alpha_4 \\
&\quad + \alpha_2\alpha_3^2\alpha_4 + \alpha_1\alpha_2\alpha_4^2 + \alpha_1\alpha_3\alpha_4^2 + \alpha_2\alpha_3\alpha_4^2 \\
&= \alpha_1^2\alpha_2\alpha_3 + \alpha_1\alpha_2^2\alpha_4 + \alpha_1\alpha_3^2\alpha_4 + \alpha_2\alpha_3\alpha_4^2 \\
&\quad + \alpha_1^2\alpha_2\alpha_4 + \alpha_1\alpha_2^2\alpha_3 + \alpha_1\alpha_3\alpha_4^2 + \alpha_2\alpha_3^2\alpha_4 \\
&\quad + \alpha_1^2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3^2 + \alpha_1\alpha_2\alpha_4^2 + \alpha_2^2\alpha_3\alpha_4 \\
&= (\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_1\alpha_3 + \alpha_2\alpha_4) \\
&\quad + (\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_1\alpha_4 + \alpha_2\alpha_3) \\
&\quad + (\alpha_1\alpha_3 + \alpha_2\alpha_4)(\alpha_1\alpha_4 + \alpha_2\alpha_3) \\
&= t_1t_2 + t_1t_3 + t_2t_3.
\end{aligned}
$$

Aus Bemerkung 4 und Definition 25 folgt

$$
\begin{aligned}
(2.7) : A &= \big(-(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)\big)^2\alpha_1\alpha_2\alpha_3\alpha_4 \\
&\quad - 4(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4) \\
&\quad \cdot \alpha_1\alpha_2\alpha_3\alpha_4 + \big(-(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4)\big)^2 \\
&= (\alpha_1^2 + 2\,\alpha_1\alpha_2 + \alpha_2^2 + 2\,\alpha_1\alpha_3 + 2\,\alpha_2\alpha_3 + \alpha_3^2 + 2\,\alpha_1\alpha_4 \\
&\quad + 2\,\alpha_2\alpha_4 + 2\,\alpha_3\alpha_4 + \alpha_4^2)\cdot\alpha_1\alpha_2\alpha_3\alpha_4 \\
&\quad - 4(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4)\alpha_1\alpha_2\alpha_3\alpha_4 \\
&\quad + \alpha_1^2\alpha_2^2\alpha_3^2 + \alpha_1^2\alpha_2^2\alpha_4^2 + \alpha_1^2\alpha_3^2\alpha_4^2 + \alpha_2^2\alpha_3^2\alpha_4^2 \\
&\quad + 2\alpha_1^2\alpha_2^2\alpha_3\alpha_4 + 2\alpha_1^2\alpha_2\alpha_3^2\alpha_4 + 2\alpha_1\alpha_2^2\alpha_3^2\alpha_4 \\
&\quad + 2\alpha_1^2\alpha_2\alpha_3\alpha_4^2 + 2\alpha_1\alpha_2^2\alpha_3\alpha_4^2 + 2\alpha_1\alpha_2\alpha_3^2\alpha_4^2 \\
&= \alpha_1^3\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2^3\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3^3\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_4^3 \\
&\quad + \alpha_1^2\alpha_2^2\alpha_3^2 + \alpha_1^2\alpha_2^2\alpha_4^2 + \alpha_1^2\alpha_3^2\alpha_4^2 \\
&= (\alpha_1^2\alpha_2\alpha_3 + \alpha_1\alpha_2^2\alpha_4 + \alpha_1\alpha_3^2\alpha_4 + \alpha_2\alpha_3\alpha_4^2)\cdot(\alpha_1\alpha_4 + \alpha_2\alpha_3)
\end{aligned}
$$

$$
\begin{aligned}
&= (\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_1\alpha_3 + \alpha_2\alpha_4)(\alpha_1\alpha_4 + \alpha_2\alpha_3) \\
&= t_1 t_2 t_3. \qquad \square
\end{aligned}
$$

Satz 11.
Die kubische Resolvente $r(x)$ und das Polynom $p(x)$ besitzen dieselbe Diskriminante, das heißt,

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \prod_{i<j} (t_i - t_j)^2.$$

Beweis.

$$
\begin{aligned}
D &= \prod_{i<j} (t_i - t_j)^2 \\
&= (t_1 - t_2)^2 \cdot (t_1 - t_3)^2 \cdot (t_2 - t_3)^2 \\
&= (\alpha_1\alpha_2 + \alpha_3\alpha_4 - \alpha_1\alpha_3 - \alpha_2\alpha_4)^2 \\
&\quad \cdot (\alpha_1\alpha_2 + \alpha_3\alpha_4 - \alpha_1\alpha_4 - \alpha_2\alpha_3)^2 \\
&\quad \cdot (\alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_4 - \alpha_2\alpha_3)^2 \\
&= \big(\alpha_1(\alpha_2 - \alpha_3) - \alpha_4(\alpha_2 - \alpha_3)\big)^2 \\
&\quad \cdot \big(\alpha_1(\alpha_2 - \alpha_4) - \alpha_3(\alpha_2 - \alpha_4)\big)^2 \\
&\quad \cdot \big(\alpha_1(\alpha_3 - \alpha_4) - \alpha_2(\alpha_3 - \alpha_4)\big)^2 \\
&= (\alpha_1 - \alpha_4)^2 \cdot (\alpha_2 - \alpha_3)^2 \cdot (\alpha_1 - \alpha_3)^2 \\
&\quad \cdot (\alpha_2 - \alpha_4)^2 \cdot (\alpha_1 - \alpha_2)^2 \cdot (\alpha_3 - \alpha_4)^2 \\
&= \prod_{i<j} (\alpha_i - \alpha_j)^2. \qquad \square
\end{aligned}
$$

Satz 12.
Die Diskriminante lässt sich durch
$D = -4b^3A + b^2B^2 + 18bBA - 4B^3 - 27A^2$
mit $A = a^2d + c^2 - 4bd$ *und* $B = ac - 4d$ *ausdrücken.*[3]

Beweis. Es gilt:

$$
\begin{aligned}
D &= \big((t_1 - t_2)(t_1 - t_3)(t_2 - t_3)\big)^2 \\
&= \big((t_1^2 - t_1t_2 - t_1t_3 + t_2t_3)(t_2 - t_3)\big)^2 \\
&= (t_1^2t_2 - t_1t_2^2 - t_1t_2t_3 + t_2^2t_3 - t_1^2t_3 + t_1t_2t_3 + t_1t_3^2 - t_2t_3^2)^2 \\
&= (t_1^2t_2 - t_1t_2^2 + t_2^2t_3 - t_1^2t_3 + t_1t_3^2 - t_2t_3^2)^2 \\
&= \big(t_1^2(t_2 - t_3) + t_2^2(t_3 - t_1) + t_3^2(t_1 - t_2)\big)^2 \\
&= t_1^4(t_2 - t_3)^2 + t_2^4(t_3 - t_1)^2 + t_3^4(t_1 - t_2)^2 \\
&\quad + 2t_1^2(t_2 - t_3)t_2^2(t_3 - t_1) + 2t_1^2(t_2 - t_3)t_3^2(t_1 - t_2) \\
&\quad + 2t_2^2(t_3 - t_1)t_3^2(t_1 - t_2) \\
&= t_1^4t_2^2 - 2t_1^4t_2t_3 + t_1^4t_3^2 + t_2^4t_3^2 - 2t_2^4t_1t_3 + t_2^4t_1^2 + t_3^4t_1^2 \\
&\quad - 2t_3^4t_1t_2 + t_3^4t_2^2 - 2t_1^2t_2^2t_3^2 - 2t_1^3t_2^3 + 2t_1^2t_2^3t_3 + 2t_1^3t_2^2t_3 + 2t_1^3t_2t_3^2 \\
&\quad - 2t_1^2t_2^2t_3^2 - 2t_1^3t_3^3 + 2t_1^2t_2t_3^3 + 2t_1t_2^2t_3^3 - 2t_2^3t_3^3 - 2t_1^2t_2^2t_3^2 + 2t_1t_2^3t_3^2 \\
&= t_1^4t_2^2 + (2-4)t_1^4t_2t_3 + t_1^4t_3^2 + t_2^4t_3^2 + (2-4)t_2^4t_1t_3 + t_2^4t_1^2 \\
&\quad + t_3^4t_1^2 + (2-4)t_3^4t_1t_2 + t_3^4t_2^2 + (15 + 54 - 27 - 24 - 24)t_1^2t_2^2t_3^2 \\
&\quad + (2-4)t_1^3t_2^3 + (2-4)t_1^3t_3^3 + (2-4)t_2^3t_3^3 \\
&\quad + (18 + 8 - 12 - 12)t_1^2t_2^3t_3 + (18 + 8 - 12 - 12)t_1^3t_2^2t_3 \\
&\quad + (18 + 8 - 12 - 12)t_1^3t_2t_3^2 + (18 + 8 - 12 - 12)t_1^2t_2t_3^3 \\
&\quad + (18 + 8 - 12 - 12)t_1t_2^2t_3^3 + (18 + 8 - 12 - 12)t_1t_2^3t_3^2 \\
&= \underline{-4\,t_1^4t_2t_3 - 12\,t_1^3t_2^2t_3 - 12\,t_1^2t_2^3t_3 - 4\,t_1t_2^4t_3 - 12\,t_1^3t_2t_3^2} \\
&\quad \underline{-24\,t_1^2t_2^2t_3^2 - 12\,t_1t_2^3t_3^2 - 12\,t_1^2t_2t_3^3 - 12\,t_1t_2^2t_3^3 - 4\,t_1t_2t_3^4}
\end{aligned}
$$

[3] Im Artikel von Warren und Kappe [8, S. 134] wird fälschlicherweise die Formel $D = -4b^3A + b^2B^2 + 18dBA - B^3 - 27A^2$ verwendet, obwohl dort auf die Monografie von Jacobson verwiesen wurde [7, S. 251], in der die Formel für die Diskriminante korrekt steht. Die Summanden sind nämlich $18bBA$ statt $18dBA$ und $-4B^3$ statt $-B^3$.

$$
\begin{aligned}
&+ t_1^4t_2^2 + 2\,t_1^3t_2^3 + t_1^2t_2^4 + 2\,t_1^4t_2t_3 + 8\,t_1^3t_2^2t_3 + 8\,t_1^2t_2^3t_3 + 2\,t_1t_2^4t_3\\
&+ t_1^4t_3^2 + 8\,t_1^3t_2t_3^2 + 15\,t_1^2t_2^2t_3^2 + 8\,t_1t_2^3t_3^2 + t_2^4t_3^2 + 2\,t_1^3t_3^3 + 8\,t_1^2t_2t_3^3\\
&+ 8\,t_1t_2^2t_3^3 + 2\,t_2^3t_3^3 + t_1^2t_3^4 + 2\,t_1t_2t_3^4 + t_2^2t_3^4\\
&+18\,t_1^3t_2^2t_3 + 18\,t_1^2t_2^3t_3 + 18\,t_1^3t_2t_3^2 + 54\,t_1^2t_2^2t_3^2\\
&+18\,t_1t_2^3t_3^2 + 18\,t_1^2t_2t_3^3 + 18\,t_1t_2^2t_3^3\\
&-4\,t_1^3t_2^3 - 12\,t_1^3t_2^2t_3 - 12\,t_1^2t_2^3t_3 - 12\,t_1^3t_2t_3^2 - 24\,t_1^2t_2^2t_3^2\\
&-12\,t_1t_2^3t_3^2 - 4\,t_1^3t_3^3 - 12\,t_1^2t_2t_3^3 - 12\,t_1t_2^2t_3^3 - 4\,t_2^3t_3^3 - 27\,t_1^2t_2^2t_3^2\\
\overset{(1)}{=}\ &\underline{-4(t_1^3 + 3\,t_1^2t_2 + 3\,t_1t_2^2 + t_2^3 + 3\,t_1^2t_3 + 6\,t_1t_2t_3}\\
&\underline{+3\,t_2^2t_3 + 3\,t_1t_3^2 + 3\,t_2t_3^2 + t_3^3)(t_1t_2t_3)}\\
&+ (t_1^2 + 2\,t_1t_2 + t_2^2 + 2\,t_1t_3 + 2\,t_2t_3 + t_3^2)\\
&\cdot (t_1^2t_2^2 + 2\,t_1^2t_2t_3 + 2\,t_1t_2^2t_3 + t_1^2t_3^2 + 2\,t_1t_2t_3^2 + t_2^2t_3^2)\\
&+18(t_1 + t_2 + t_3)(t_1^2t_2^2t_3 + t_1^2t_2t_3^2 + t_1t_2^2t_3^2)\\
&-4(t_1^3t_2^3 + 3\,t_1^3t_2^2t_3 + 3\,t_1^2t_2^3t_3 + 3\,t_1^3t_2t_3^2 + 6\,t_1^2t_2^2t_3^2\\
&\qquad +3\,t_1t_2^3t_3^2 + t_1^3t_3^3 + 3\,t_1^2t_2t_3^3 + 3\,t_1t_2^2t_3^3 + t_2^3t_3^3) - 27(t_1t_2t_3)^2\\
=\ &-4t_1t_2t_3(t_1^3 + 3\,t_1^2t_2 + 3\,t_1t_2^2 + t_2^3 + 3\,t_1^2t_3\\
&\qquad + 6\,t_1t_2t_3 + 3\,t_2^2t_3 + 3\,t_1t_3^2 + 3\,t_2t_3^2 + t_3^3)\\
&+ (t_1^2 + 2\,t_1t_2 + t_2^2 + 2\,t_1t_3 + 2\,t_2t_3 + t_3^2)\\
&\quad \cdot (t_1^2t_2^2 + 2\,t_1^2t_2t_3 + 2\,t_1t_2^2t_3 + t_1^2t_3^2 + 2\,t_1t_2t_3^2 + t_2^2t_3^2)\\
&+ 18(t_1 + t_2 + t_3)(t_1^2t_2^2t_3 + t_1^2t_2t_3^2 + t_1t_2^2t_3^2)\\
&- 4(t_1^3t_2^3 + 3\,t_1^3t_2^2t_3 + 3\,t_1^2t_2^3t_3 + 3\,t_1^3t_2t_3^2 + 6\,t_1^2t_2^2t_3^2\\
&+ 3\,t_1t_2^3t_3^2 + t_1^3t_3^3 + 3\,t_1^2t_2t_3^3 + 3\,t_1t_2^2t_3^3 + t_2^3t_3^3) - 27(t_1t_2t_3)^2\\
=\ &-4(t_1 + t_2 + t_3)^3(t_1t_2t_3) + (t_1 + t_2 + t_3)^2(t_1t_2 + t_1t_3 + t_2t_3)^2\\
&+ 18(t_1 + t_2 + t_3)(t_1t_2t_3)(t_1t_2 + t_1t_3 + t_2t_3)\\
&- 4(t_1t_2 + t_1t_3 + t_2t_3)^3 - 27(t_1t_2t_3)^2\\
=\ &-4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2.
\end{aligned}
$$

Zur Vervollständigung des Beweises zeigen wir, dass die nicht unterstrichenen Terme bei (1) übereinstimmen.

$$
\begin{aligned}
&(\underline{t_1^2} + \underline{\underline{t_2^2}} + \underset{\sim}{t_3^2} + \underset{---}{2t_1t_2} + \underset{\cdots\cdot}{2t_1t_3} + 2t_2t_3) \\
&\cdot (t_1^2t_2^2 + t_1^2t_3^2 + t_2^2t_3^2 + 2t_1^2t_2t_3 + 2t_1t_2^2t_3 + 2t_1t_2t_3^2) \\
= {} & \underline{t_1^4t_2^2 + t_1^4t_3^2 + t_1^2t_2^2t_3^2 + 2t_1^4t_2t_3 + 2t_1^3t_2^2t_3 + 2t_1^3t_2t_3^2} \\
& \underline{\underline{+t_1^2t_2^4 + t_1^2t_2^2t_3^2 + t_2^4t_3^2 + 2t_1^2t_2^3t_3 + 2t_1t_2^4t_3 + 2t_1t_2^3t_3^2}} \\
& \utilde{+t_1^2t_2^2t_3^2 + t_1^2t_3^4 + t_2^2t_3^4 + 2t_1^2t_2t_3^3 + 2t_1t_2^2t_3^3 + 2t_1t_2t_3^4} \\
& +2t_1^3t_2^3 + 2t_1^3t_2t_3^2 + 2t_1t_2^3t_3^2 + 4t_1^3t_2^2t_3 + 4t_1^2t_2^3t_3 + 4t_1^2t_2^2t_3^2 \\
& +2t_1^3t_2^2t_3 + 2t_1^3t_3^3 + 2t_1t_2^2t_3^3 + 4t_1^3t_2t_3^2 + 4t_1^2t_2^2t_3^2 + 4t_1^2t_2t_3^3 \\
& + 2t_1^2t_2^3t_3 + 2t_1^2t_2t_3^3 + 2t_2^3t_3^3 + 4t_1^2t_2^2t_3^2 + 4t_1t_2^3t_3^2 + 4t_1t_2^2t_3^3 \\
= {} & t_1^4t_2^2 + 2t_1^3t_2^3 + t_1^2t_2^4 + 2t_1^4t_2t_3 + 8t_1^3t_2^2t_3 + 8t_1^2t_2^3t_3 \\
& + 2t_1t_2^4t_3 + t_1^4t_3^2 + 8t_1^3t_2t_3^2 + 15t_1^2t_2^2t_3^2 + 8t_1t_2^3t_3^2 + t_2^4t_3^2 \\
& + 2t_1^3t_3^3 + 8t_1^2t_2t_3^3 + 8t_1t_2^2t_3^3 + 2t_2^3t_3^3 + t_1^2t_3^4 + 2t_1t_2t_3^4 + t_2^2t_3^4 \qquad \square
\end{aligned}
$$

Der Vorteil dieser Darstellung der Diskriminante ist, dass die im Allgemeinen unbekannten Nullstellen der Polynome nicht darin auftreten. Sie hängt nur von den Koeffizienten ab.
Nach den Vorbereitungen kommen wir zum Klassifikationssatz für Galoisgruppen von Polynomen vierten Grades. Dieser stammt aus dem Paper von Warren und Kappe [8, S. 134]. Der Beweis wird in der vorliegenden Arbeit deutlich ausführlicher behandelt, als er dort ausgeführt ist.

2 Klassifikationssatz

Satz 13 (Klassifikationssatz für Galoisgruppen von Polynomen vierten Grades)**.** [8, S. 134-135]
Sei K ein Körper der Charakteristik ungleich 2.
Sei $p(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ irreduzibel über K. Be-

zeichne F den Zerfällungskörper von $p(x)$ mit $p(x) = \prod_{i=1}^{4}(x - \alpha_i)$ mit $\alpha_i \in F$ und $i \in \{1, 2, 3, 4\}$.
Sei weiter $r(x) := x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$ die kubische Resolvente von $p(x)$ und E ein Zerfällungskörper von $r(x)$. Ferner sei D die Diskriminante von $p(x)$.[4] *Dann gelten*

(i) $\mathrm{Gal}(F/K) \cong \mathrm{S}_4$ *genau dann, wenn $r(x)$ irreduzibel über K ist und $D \notin K^2$,*

(ii) $\mathrm{Gal}(F/K) \cong \mathrm{A}_4$ *genau dann, wenn $r(x)$ irreduzibel über K ist und $D \in K^2$,*

(iii) $\mathrm{Gal}(F/K) \cong \mathrm{V}_4$ *genau dann, wenn $r(x)$ über K in drei Linearfaktoren zerfällt,*

(iv) $\mathrm{Gal}(F/K) \cong \mathrm{C}_4$ *genau dann, wenn $r(x)$ genau eine Nullstelle $t \in K$ hat und*

$g(x) := (x^2 - tx + d)(x^2 + ax + (b - t))$ *in $E[x]$ zerfällt und*

(v) $\mathrm{Gal}(F/K) \cong \mathrm{D}_4$ *genau dann, wenn $r(x)$ genau eine Nullstelle t in K hat und $g(x)$ nicht in $E[x]$ zerfällt.*

Beweis. Sei $\mathrm{V}_4 = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Der Zerfällungskörper E der kubischen Resolvente $r(x)$ ist in F enthalten, da die t_1, t_2 und t_3 sich additiv und multiplikativ aus den Nullstellen $\alpha_1, \alpha_2, \alpha_3$ und α_4 wie in Definition 25 zusammensetzen. Da $p(x)$ separabel und irreduzibel ist, ist die gemeinsame Diskriminante nicht Null und damit hat auch $r(x)$ paarweise verschiedene Nullstellen.
Eine Permutation δ der Nullstellen $\alpha_1, \ldots, \alpha_4$ von $p(x)$ induziert eine Permutation $\sigma \in \mathrm{S}_4$ der dazugehörigen Indizes: $\delta(\alpha_i) = \alpha_{\sigma(i)}$, da die Nullstellen paarweise verschieden sind. Umgekehrt induziert $\sigma \in \mathrm{S}_4$ eine Permutation δ_σ mit $\delta(\alpha_i) := \alpha_{\sigma(i)}$. Im Folgenden rechnen wir nach, dass eine Permutation δ der Nullstellen $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ genau dann alle drei Nullstellen von $r(x)$ festhält, wenn die von δ induzierte Permutation der Subindizes der α_i in V_4 ist. Dazu zeigen wir nun:

$$\sigma \in \mathrm{V}_4 \iff \delta_\sigma(t_i) = t_i, \text{ für } i \in \{1, 2, 3\}. \tag{2.8}$$

[4] Oder wahlweise die Diskriminante von $r(x)$ nach Satz 11.

„$\Longleftarrow$“
Wir zeigen dies durch Kontraposition. Angenommen $\sigma \notin \mathrm{V}_4$. Für diese 20 Elemente, welche nicht zu V_4 gehören, aber Elemente der S_4 sind (siehe Tabelle 1.1), zeigen wir im Folgenden, dass immer für (mindestens) ein $i \in \{1, 2, 3\}$ gilt, dass die Bedingung $\delta(t_i) = t_i$ nicht erfüllt ist, wobei $\delta := \delta_\sigma$ sei.
Für alle Elemente σ der Ordnung 2, die nicht als Elemente der Kleinschen Vierergruppe vorkommen, finden wir jeweils ein t_i mit
$i \in \{1, 2, 3\}$ mit $\delta(t_i) \neq t_i$:

$$\sigma = (1,2) : \delta(t_2) = \alpha_{\sigma(1)}\alpha_{\sigma(3)} + \alpha_{\sigma(2)}\alpha_{\sigma(4)} = \alpha_2\alpha_3 + \alpha_1\alpha_4 = t_3 \neq t_2,$$
$$\sigma = (1,3) : \delta(t_1) = \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} = \alpha_3\alpha_2 + \alpha_1\alpha_4 = t_3 \neq t_1,$$
$$\sigma = (1,4) : \delta(t_2) = \alpha_{\sigma(1)}\alpha_{\sigma(3)} + \alpha_{\sigma(2)}\alpha_{\sigma(4)} = \alpha_4\alpha_3 + \alpha_2\alpha_1 = t_1 \neq t_2,$$
$$\sigma = (2,3) : \delta(t_2) = \alpha_{\sigma(1)}\alpha_{\sigma(3)} + \alpha_{\sigma(2)}\alpha_{\sigma(4)} = \alpha_1\alpha_2 + \alpha_3\alpha_4 = t_1 \neq t_2,$$
$$\sigma = (2,4) : \delta(t_3) = \alpha_{\sigma(1)}\alpha_{\sigma(4)} + \alpha_{\sigma(2)}\alpha_{\sigma(3)} = \alpha_1\alpha_2 + \alpha_4\alpha_3 = t_1 \neq t_3,$$
$$\sigma = (3,4) : \delta(t_3) = \alpha_{\sigma(1)}\alpha_{\sigma(4)} + \alpha_{\sigma(2)}\alpha_{\sigma(3)} = \alpha_1\alpha_3 + \alpha_2\alpha_4 = t_2 \neq t_3.$$

Für alle Elemente σ der Ordnung 3 rechnen wir $\delta(t_1) \neq t_1$ nach:

$$\begin{aligned}
\sigma = (1,2,3) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_2\alpha_3 + \alpha_1\alpha_4 \\
&= t_3 \neq t_1, \\
\sigma = (1,2,4) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_2\alpha_4 + \alpha_3\alpha_1 \\
&= t_2 \neq t_1, \\
\sigma = (1,3,4) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_3\alpha_2 + \alpha_4\alpha_1 \\
&= t_3 \neq t_1, \\
\sigma = (2,3,4) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_1\alpha_3 + \alpha_4\alpha_2 \\
&= t_2 \neq t_1, \\
\sigma = (3,2,1) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_3\alpha_1 + \alpha_2\alpha_4 \\
&= t_2 \neq t_1, \\
\sigma = (4,2,1) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_4\alpha_1 + \alpha_3\alpha_2 \\
&= t_3 \neq t_1, \\
\sigma = (4,3,1) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_4\alpha_2 + \alpha_1\alpha_3 \\
&= t_2 \neq t_1, \\
\sigma = (4,3,2) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_1\alpha_4 + \alpha_2\alpha_3 \\
&= t_3 \neq t_1.
\end{aligned}$$

Auch für alle Elemente der Ordnung 4 finden wir jeweils ein t_i mit $i \in \{1,2,3\}$ mit $\delta(t_i) \neq t_i$:

$$\begin{aligned}
\sigma = (1,2,3,4) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_2\alpha_3 + \alpha_4\alpha_1 = t_3 \neq t_1, \\
\sigma = (1,3,2,4) : \delta(t_2) &= \alpha_{\sigma(1)}\alpha_{\sigma(3)} + \alpha_{\sigma(2)}\alpha_{\sigma(4)} \\
&= \alpha_3\alpha_2 + \alpha_4\alpha_1 = t_3 \neq t_2, \\
\sigma = (1,4,2,3) : \delta(t_3) &= \alpha_{\sigma(1)}\alpha_{\sigma(4)} + \alpha_{\sigma(2)}\alpha_{\sigma(3)} \\
&= \alpha_4\alpha_2 + \alpha_3\alpha_1 = t_2 \neq t_3, \\
\sigma = (1,2,4,3) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_2\alpha_4 + \alpha_1\alpha_3 = t_2 \neq t_1, \\
\sigma = (1,3,4,2) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_3\alpha_1 + \alpha_4\alpha_2 = t_2 \neq t_1, \\
\sigma = (1,4,3,2) : \delta(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} \\
&= \alpha_4\alpha_1 + \alpha_2\alpha_3 = t_3 \neq t_1.
\end{aligned}$$

„$\Longrightarrow$“
Für $\mathrm{id} \in \mathrm{V}_4$ erhalten wir

$$\begin{aligned}
\delta_{\mathrm{id}}(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} = t_1, \\
\delta_{\mathrm{id}}(t_2) &= \alpha_{\sigma(1)}\alpha_{\sigma(3)} + \alpha_{\sigma(2)}\alpha_{\sigma(4)} = t_2, \\
\delta_{\mathrm{id}}(t_3) &= \alpha_{\sigma(1)}\alpha_{\sigma(4)} + \alpha_{\sigma(2)}\alpha_{\sigma(3)} = t_3.
\end{aligned}$$

Für $\sigma = (1,3)(2,4) \in \mathrm{V}_4$ erhalten wir

$$\begin{aligned}
\delta_\sigma(t_1) &= \alpha_{\sigma(1)}\alpha_{\sigma(2)} + \alpha_{\sigma(3)}\alpha_{\sigma(4)} = \alpha_3\alpha_4 + \alpha_1\alpha_2 = t_1, \\
\delta_\sigma(t_2) &= \alpha_{\sigma(1)}\alpha_{\sigma(3)} + \alpha_{\sigma(2)}\alpha_{\sigma(4)} = \alpha_1\alpha_3 + \alpha_2\alpha_4 = t_2, \\
\delta_\sigma(t_3) &= \alpha_{\sigma(1)}\alpha_{\sigma(4)} + \alpha_{\sigma(2)}\alpha_{\sigma(3)} = \alpha_3\alpha_2 + \alpha_4\alpha_1 = t_3.
\end{aligned}$$

Für $\tau = (1,2)(3,4) \in \mathrm{V}_4$ gelten

$$\begin{aligned}
\delta_\tau(t_1) &= \alpha_{\tau(1)}\alpha_{\tau(2)} + \alpha_{\tau(3)}\alpha_{\tau(4)} = \alpha_2\alpha_1 + \alpha_4\alpha_3 = t_1,\\
\delta_\tau(t_2) &= \alpha_{\tau(1)}\alpha_{\tau(3)} + \alpha_{\tau(2)}\alpha_{\tau(4)} = \alpha_2\alpha_4 + \alpha_1\alpha_3 = t_2,\\
\delta_\tau(t_3) &= \alpha_{\tau(1)}\alpha_{\tau(4)} + \alpha_{\tau(2)}\alpha_{\tau(3)} = \alpha_2\alpha_3 + \alpha_1\alpha_4 = t_3.
\end{aligned}$$

Für $\varphi = (1,4)(2,3) \in \mathrm{V}_4$ sind

$$\begin{aligned}
\delta_\varphi(t_1) &= \alpha_{\varphi(1)}\alpha_{\varphi(2)} + \alpha_{\varphi(3)}\alpha_{\varphi(4)} = \alpha_4\alpha_3 + \alpha_2\alpha_1 = t_1,\\
\delta_\varphi(t_2) &= \alpha_{\varphi(1)}\alpha_{\varphi(3)} + \alpha_{\varphi(2)}\alpha_{\varphi(4)} = \alpha_4\alpha_2 + \alpha_3\alpha_1 = t_2,\\
\delta_\varphi(t_3) &= \alpha_{\varphi(1)}\alpha_{\varphi(4)} + \alpha_{\varphi(2)}\alpha_{\varphi(3)} = \alpha_4\alpha_1 + \alpha_3\alpha_2 = t_3.
\end{aligned}$$

Somit lassen id, σ, τ und φ alle Nullstellen fest.
Für alle $\sigma \in \mathrm{V}_4$ und alle $i \in \{1,2,3\}$ gilt somit $\sigma(t_i) = t_i$.
Wir zeigen nun: Es ist $\mathrm{Gal}(F/E) = \mathrm{Gal}(F/K) \cap \mathrm{V}_4$.

„$\subseteq$“ Sei $\delta_\sigma \in \mathrm{Gal}(F/E) \Longrightarrow \delta_\sigma|_E = \mathrm{id}_E$. Da $\sigma \in \mathrm{V}_4$ gilt $\delta_\sigma(t_i) = t_i$ für $i \in \{1,2,3\}$ nach (2.8). Aus $K \subseteq E$ folgt $\mathrm{Gal}(F/E) \subseteq \mathrm{Gal}(F/K)$ und damit ist wegen $\sigma \in \mathrm{Gal}(F/E)$ auch $\sigma \in \mathrm{Gal}(F/K)$.

„$\supseteq$“ Sei $\delta_\sigma \in \mathrm{Gal}(F/K) \cap \mathrm{V}_4$, dann ist $\delta_\sigma \in \mathrm{Gal}(F/K)$, also $\delta_\sigma|_K = \mathrm{id}_\mathrm{K}$. Da $\sigma \in \mathrm{V}_4$, ist gilt nach (2.8), dass $\delta_\sigma(t_i) = t_i$ mit $i \in \{1,2,3\}$. Da die $t_i \in E$ den Körper E erzeugen, folgt $\delta_\sigma|_E = \mathrm{id}_E$ und somit $\sigma \in \mathrm{Gal}(F/E)$.
Daraus leitet sich ab:

(a) $r(x)$ zerfällt vollständig in Linearfaktoren über K genau dann, wenn $\mathrm{Gal}(F/K) \cong \mathrm{V}_4$,

(b) $r(x)$ ist irreduzibel über K genau dann,

wenn $|\mathrm{Gal}(F/K)| = |\mathrm{Gal}(F/E)| \cdot \overbrace{|\mathrm{Gal}(E/K)|}^{\overset{(1),(c)}{=}3}$ durch 3 teilbar ist.

Da $p(x)$ irreduzibel ist, ergibt das Fundamentallemma der Galoistheorie 1 Teil (b), dass

$4 \mid |\mathrm{Gal}(F/K)|$ und $|\mathrm{Gal}(F/K)| \geqslant 4$.
Im Fall (a) ergibt sich $\mathrm{Gal}(F/K) \cong \mathrm{V}_4$. Die Klassifizierung (iii) ist damit gezeigt.

Im Fall (b) ist $|\mathrm{Gal}(F/K)|$ durch 12 teilbar, also ist $\mathrm{Gal}(F/K) \cong \mathrm{S}_4$ oder $\mathrm{Gal}(F/K) \cong \mathrm{A}_4$.
Im Folgenden sehen wir, dass $\mathrm{Gal}(F/K) \cong \mathrm{S}_4$, falls die Diskriminante $D = \prod_{i<j} (\alpha_i - \alpha_j)^2$ kein Quadrat in K ist, und $\mathrm{Gal}(F/K) \cong \mathrm{A}_4$, falls D ein Quadrat in K ist.

„$\mathrm{Gal}(F/K) \cong \mathrm{S}_4$“: Sei nun D kein Quadrat in K, dass heißt, $\sqrt{D} \notin K$. Für jedes $\sigma \in \mathrm{A}_4$ folgt $\delta_\sigma(\sqrt{D}) = \sqrt{D}$, denn der Ausdruck $\sqrt{D} = \prod_{i<j} (\alpha_i - \alpha_j)$ ändert für jede Vertauschung $\alpha_i \leftrightarrow \alpha_j$ das Vorzeichen und wegen $\sigma \in \mathrm{A}_4$ lässt sich δ_σ nach Bemerkung 2 durch eine gerade Anzahl an Vertauschungen darstellen. Nach Voraussetzung ist $\sqrt{D} \notin K$, nach dem Hauptsatz der Galoistheorie 10 Teil (b) ist $K = \mathrm{Fix}(\mathrm{Gal}(F/K))$ und wir erhalten $\sqrt{D} \notin \mathrm{Fix}(\mathrm{Gal}(F/K))$. Daher gibt es ein $\delta_\sigma \in \mathrm{Gal}(F/K)$ mit $\delta_\sigma(\sqrt{D}) \neq \sqrt{D}$. Damit ist das dazugehörige $\sigma \notin \mathrm{A}_4$. Dies impliziert $\mathrm{Gal}(F/K) \ncong \mathrm{A}_4$, also $\mathrm{Gal}(F/K) \cong \mathrm{S}_4$.

„$\mathrm{Gal}(F/K) \cong \mathrm{A}_4$“: Sei D ein Quadrat in K, dass heißt, $\sqrt{D} \in K$. Dann gilt für $\sigma \in \mathrm{S}_4$ mit $\mathrm{sign}(\sigma) = -1$:

$$\delta_\sigma(\sqrt{D}) = -\sqrt{D} \neq \sqrt{D}.$$

Da $p(x)$ separabel ist, ist $D \neq 0$ und da K nicht Charakteristik zwei hat, ist $\sqrt{D} \neq -\sqrt{D}$. Damit wäre $\delta_\sigma|_K \neq \mathrm{id}_\mathrm{K}$ und es folgt

$$\delta_\sigma \notin \mathrm{Gal}(F/K) \Longrightarrow \mathrm{Gal}(F/K) \ncong \mathrm{S}_4 \Longrightarrow \mathrm{Gal}(F/K) \cong \mathrm{A}_4.$$

Damit sind (i) und (ii) gezeigt. Wir zeigen nun (iv) und (v). Habe nun im folgenden $r(x)$ genau eine Nullstelle t in K. Nach möglicher Umnummerierung der Nullstellen α_i von $p(x)$ können wir $t := t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$ annehmen. Wir zeigen nun Nummer (iv) nämlich, dass $\mathrm{Gal}(F/K)$ zu C_4 isomorph ist.

Betrachten wir nun das Polynom $g(x) = (x^2 - tx + d)(x^2 + ax + (b-t))$ über K.
Die Nullstellen des ersten Faktors sind $\alpha_1\alpha_2$ und $\alpha_3\alpha_4$:

$$\begin{aligned}
x^2 - tx + d\big|_{x=\alpha_1\alpha_2} &= (\alpha_1\alpha_2)^2 - t(\alpha_1\alpha_2) + d \\
&= (\alpha_1\alpha_2)^2 - (\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_1\alpha_2) + \alpha_1\alpha_2\alpha_3\alpha_4 \\
&= 0, \\
x^2 - tx + d\big|_{x=\alpha_3\alpha_4} &= (\alpha_3\alpha_4)^2 - t(\alpha_3\alpha_4) + d \\
&= (\alpha_3\alpha_4)^2 - (\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_3\alpha_4) + \alpha_1\alpha_2\alpha_3\alpha_4 \\
&= 0.
\end{aligned}$$

Die Nullstellen des zweiten Faktors sind zum einen $\alpha_1 + \alpha_2$, denn

$$\begin{aligned}
x^2 + ax + (b-t)\big|_{x=\alpha_1+\alpha_2} &= (\alpha_1 + \alpha_2)^2 + a(\alpha_1 + \alpha_2) + (b - t) \\
&\overset{(2.1),(2.2)}{=} (\alpha_1 + \alpha_2)^2 + (-\alpha_1 - \alpha_2 - \alpha_3 - \alpha_4) \\
&\quad \cdot (\alpha_1 + \alpha_2) + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 \\
&\quad + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 \\
&\quad - (\alpha_1\alpha_2 + \alpha_3\alpha_4) \\
&= \alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2 - \alpha_1^2 \\
&\quad - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_1\alpha_4 - \alpha_1\alpha_2 \\
&\quad - \alpha_2^2 - \alpha_2\alpha_3 - \alpha_2\alpha_4 + \alpha_1\alpha_2 \\
&\quad + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 \\
&\quad + \alpha_3\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 \\
&= 0
\end{aligned}$$

und sind zum anderen $\alpha_3 + \alpha_4$, denn

$$\begin{aligned}
x^2 + ax + (b-t)\big|_{x=\alpha_3+\alpha_4} &= (\alpha_3+\alpha_4)^2 + a(\alpha_3+\alpha_4) + (b-t) \\
&\overset{(2.1),(2.2)}{=} (\alpha_3+\alpha_4)^2 + (-\alpha_1-\alpha_2-\alpha_3-\alpha_4) \\
&\quad \cdot (\alpha_3+\alpha_4) + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 \\
&\quad + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 \\
&\quad - (\alpha_1\alpha_2 + \alpha_3\alpha_4) \\
&= \alpha_3^2 + 2\alpha_3\alpha_4 + \alpha_4^2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 - \alpha_3^2 \\
&\quad - \alpha_3\alpha_4 - \alpha_1\alpha_4 - \alpha_2\alpha_4 - \alpha_3\alpha_4 - \alpha_4^2 \\
&\quad + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 \\
&\quad + \alpha_2\alpha_4 + \alpha_3\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 \\
&= 0.
\end{aligned}$$

„$\mathrm{Gal}(F/K) \cong \mathrm{C}_4$“: Falls $\mathrm{Gal}(F/K) \cong \mathrm{C}_4$ gilt, gibt es genau eine Untergruppe der Ordnung zwei, denn die zyklische Gruppe
$\mathrm{C}_4 = \langle(1,2,3,4)\rangle$ hat genau eine Untergruppe der Ordnung zwei, nämlich $\langle(1,3)(2,4)\rangle$. Entsprechend gibt es nach dem Hauptsatz der Galoistheorie 10 Teil (a) nur eine quadratische Körpererweiterung von K. Also ist E die einzige quadratische Körpererweiterung von K, welche in F enthalten ist. Somit zerfallen beide quadratische Faktoren von $g(x)$ in E in Linearfaktoren.
Nehmen wir umgekehrt an, dass $g(x)$ über E vollständig in Linearfaktoren zerfällt, dann hat das Polynom $k(x) = x^2 - (\alpha_1+\alpha_2)x + \alpha_1\alpha_2$, welches die Nullstellen α_1 und α_2 besitzt, Koeffizienten in E. Sei M der Zerfällungskörper von $k(x)$ über E. Damit ist $E \subseteq M \subseteq F$. Es sind α_1, α_2 sowie $t = t_1, t_2$ und $t_3 \in E$ in M.
Da $\alpha_3 + \alpha_4 = -a - (\alpha_1 + \alpha_2)$ ist, folgt $\alpha_3 + \alpha_4 \in M$. Außerdem impliziert $\alpha_1 - \alpha_2 \neq 0$ zusammen mit $(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) = t_2 - t_3$, dass die Differenz $\alpha_3 - \alpha_4$ in M enthalten ist. Somit ist $\alpha_3, \alpha_4 \in M$, da $\mathrm{char}(K) \neq 2$ ist.[5]
Dies ergibt $F = M$, damit ist $|\mathrm{Gal}(F/M)| = 1$ und wegen der Grad-

[5] Das Gleichungssystem $\alpha_3+\alpha_4 = k_1 \wedge \alpha_3-\alpha_4 = k_2$ ist für $\mathrm{char}(K) \neq 2$ eindeutig lösbar in K, da die Determinante der Koeffizientenmatrix ungleich Null ist.

formel 7

$$\begin{aligned}|\mathrm{C}_4| &\leqslant |\mathrm{Gal}(F/K)| \\ &= |\mathrm{Gal}(F/M)| \cdot |\mathrm{Gal}(M/E)| \cdot |\mathrm{Gal}(E/K)| \\ &\leqslant 1 \cdot 2 \cdot 2 = 4 < 8 = |\mathrm{D}_4|\end{aligned}$$

muss $\mathrm{Gal}(F/K)$ isomorph zu C_4 sein. Damit ist (iv) gezeigt.
„$\mathrm{Gal}(F/K) \cong \mathrm{D}_4$“: Die Bedingung für (v) für D_4 ist die einzige verbleibende Möglichkeit und folgt daher durch wechselseitigen Ausschluss. □

Bemerkung 7.
Unter den Voraussetzungen des Klassifikationssatzes lässt sich die Bedingung (iii) auch folgendermaßen charakterisieren:

(iii)' $\mathrm{Gal}(F/K) \cong \mathrm{V}_4$ genau dann, wenn $r(x)$ über K reduzibel ist und $D \in K^2$.

Beweis. Wir zeigen die Äquivalenz dieser Bedingung zu (iii). Da (iii) und (iii)' die selben Voraussetzungen haben ($\mathrm{Gal}(F/K) \cong \mathrm{V}_4$), müssen wir nur noch zeigen, dass genau dann $r(x)$ über K reduzibel und zugleich $D \in K^2$ ist, wenn $r(x)$ in drei Linearfaktoren zerfällt.
(iii) $\Longrightarrow$ (iii)‘: Zerfällt $r(x)$ in drei Linearfaktoren, das heißt, $r(x) = (x - t_1)(x - t_2)(x - t_3)$ mit $t_1, t_2, t_3 \in K$, dann ergibt sich:

$$D = \underbrace{(t_1 - t_2)}_{\in K}{}^2 \underbrace{(t_1 - t_3)}_{\in K}{}^2 \underbrace{(t_2 - t_3)}_{\in K}{}^2 \in K^2.$$

(iii)‘ $\Longrightarrow$ (iii): Die kubische Resolvente $r(x) = (x - t_1)(x - t_2)(x - t_3)$ ist nach Definition 25 in $K[x]$. Wir müssen zeigen, dass $t_1, t_2, t_3 \in E$ bereits in K liegen. Durch Ausmultiplizieren erhalten wir
$r(x) = x^3 - (t_1 + t_2 + t_3)x^2 + (t_1t_2 + t_1t_3 + t_2t_3)x - t_1t_2t_3 \in K[x]$.
Wir wissen also bereits die Bedingungen

$$t_1 + t_2 + t_3 \in K, \tag{2.9}$$

$$t_1t_2 + t_1t_3 + t_2t_3 \in K, \tag{2.10}$$

$$t_1t_2t_3 \in K. \tag{2.11}$$

Nach Voraussetzung ist $r(x)$ reduzibel. Also gilt $t_i \in K$ für ein $i \in \{1, 2, 3\}$. Sei etwa $t_3 \in K$, dann gilt

$$t_3 \in K \overset{(2.9)}{\Longrightarrow} t_1 + t_2 \in K, \tag{2.12}$$

$$t_1 t_2 + \underbrace{(t_1 + t_2)}_{\in K \text{ nach } (2.12)} \cdot \underbrace{t_3}_{\in K} \in K \overset{(2.10)}{\Longrightarrow} t_1 \cdot t_2 \in K. \tag{2.13}$$

Aus der Voraussetzung $D \in K^2$ folgt $\sqrt{D} \in K$ und wir erhalten zusammen mit den obigen Bedingungen:

$$\begin{aligned}\sqrt{D} &= (t_1 - t_2)(t_1 - t_3)(t_2 - t_3)\\ &= (t_1 - t_2)(t_1 t_2 - t_1 t_3 - t_2 t_3 + t_3^2)\\ &= (t_1 - t_2)(\underbrace{t_1 t_2}_{\in K} - \underbrace{(t_1 + t_2)}_{\in K} \cdot \underbrace{t_3}_{\in K} + \underbrace{t_3^2}_{\in K}) \in K.\end{aligned}$$

Es folgt also $t_1 - t_2 \in K$. Mit $t_1 + t_2 \in K$ und $\mathrm{char}(K) \neq 2$ folgt $t_1, t_2 \in K$. □

Bemerkung 8.
Aus Bemerkung 7 ergibt sich: Wenn $r(x)$ reduzibel und zugleich $D \notin K^2$ ist, so ist
$\mathrm{Gal}(F/K) \cong \mathrm{C}_4$ oder $\mathrm{Gal}(F/K) \cong \mathrm{D}_4$.

3 Flussdiagramm für Grad($p(x)$) = 4

In Abbildung 2.1 ist ein Flussdiagramm zur Illustration des Klassifikationssatzes dargestellt.

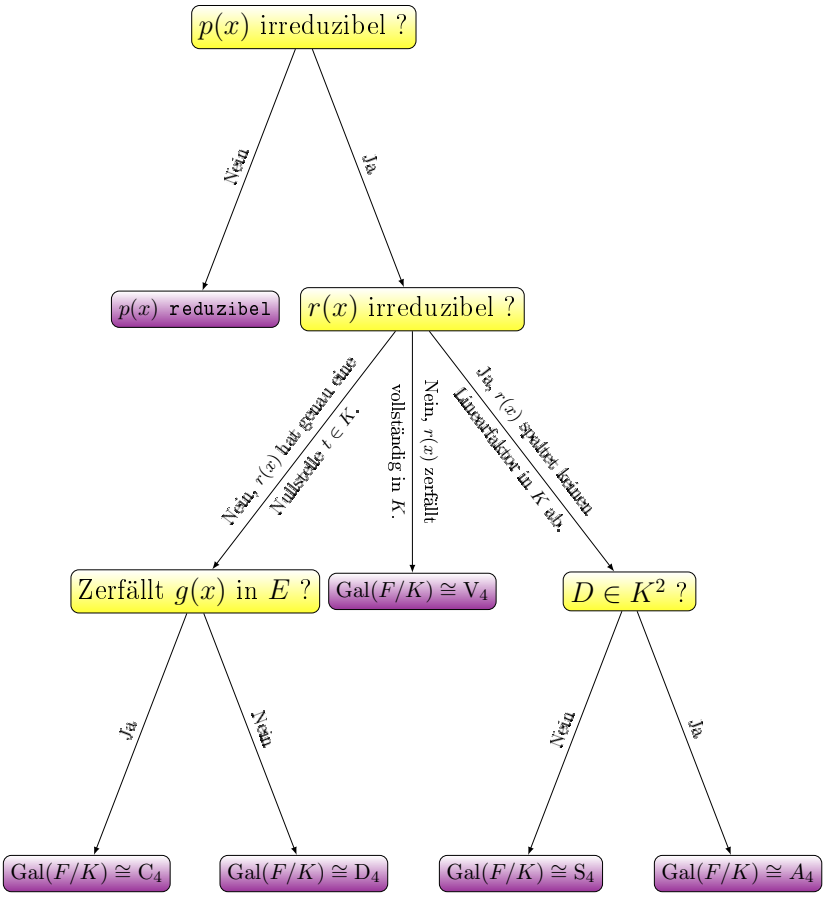


Abbildung 2.1: Klassifizierung von Polynomen vierten Grades
Quelle: Eigene Grafik erstellt mit TikZ

4 Exkurs: Irreduzibilitätskriterien

Bevor wir viele Beispiele mithilfe des Klassifikationssatzes für Polynome vierten Grades untersuchen, benötigen wir Kriterien, um zu entscheiden, ob ein Polynom irreduzibel ist. Deshalb werden im Folgenden die in den Beispielen verwendeten Irreduzibilitätskriterien bis auf das spezielle Irreduzibilitätskriterium für biquadratische Polynome, welches später vorgestellt wird, angegeben. Die meisten der Kriterien sind aus Fischer [5, S. 250-258] entnommen.

Kriterium 1 (Gaußkriterium). [5, S. 250]
Ist $f(x) \in \mathbb{Z}[x]$ *mit* $\mathrm{Grad}(f(x)) \geqslant 1$ *in* $\mathbb{Z}[x]$ *irreduzibel, so bleibt es in* $\mathbb{Q}[x]$ *irreduzibel.*

Es gilt sogar:

Kriterium 2 (Irreduzibilitätssatz). [5, S. 253]
Sei R *ein faktorieller Ring mit Quotientenkörper* $K := \mathrm{Quot}(R)$ *und* $f(x) \in R[x]$ *primitiv*[6].
Dann ist $f(x)$ *irreduzibel in* $R[x]$ *genau dann, wenn* $f(x)$ *irreduzibel in* $K[x]$ *ist.*

Kriterium 3 (Nullstellenkriterium). [5, S. 256]
Sei R *ein faktorieller Ring und* $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ *primitiv mit* $n \geqslant 2$ *und* $a_n \neq 0$ *und* $\mathrm{Grad}(f(x)) = 2$ *oder* $\mathrm{Grad}(f(x)) = 3$, *dann gilt:*

$$f(x) \text{ irreduzibel in } R[x] \iff f(x) \text{ hat keinen Linearfaktor in } R[x].$$

Zusammen mit dem Irreduzibilitätssatz 2 *ergibt sich sogar*

$$f(x) \text{ irreduzibel in } \mathrm{Quot}(R)[x] \iff \begin{array}{l} f(x) \text{ hat keinen} \\ \text{Linearfaktor in } R[x]. \end{array}$$

[6] d.h. $\mathrm{ggT}(a_0, \ldots, a_n) = 1$ [9, S. 254]

Kriterium 4 (Reduktionskriterium). [5, S. 257]
Sei R ein faktorieller Ring und

$$f(x) := a_n x^n + \ldots + a_1 x + a_0 \in R[x]$$

ein primitives Polynom vom Grad $n \geqslant 1$ sowie $\mathfrak{P} \subset R$ ein Primideal derart, dass $a_n \notin \mathfrak{P}$. Ist außerdem

$$\overline{R} := R/\mathfrak{P} \text{ und } \rho : R[x] \longrightarrow \overline{R}[x], f(x) \longmapsto \bar{f}(x)$$

der kanonische Homomorphismus, so gilt

$$\bar{f}(x) \text{ irreduzibel in } \overline{R}[x] \Longrightarrow \begin{array}{l} f(x) \text{ irreduzibel in } R[x] \text{ und in} \\ \mathrm{Quot}(R)[x] \text{ wegen Kriterium } 2 \end{array} .$$

Wir verwenden dieses Kriterium für $R = \mathbb{Q}$ und $\bar{f}(x) \in \mathbb{Q}[x]$ normiert. Dann ist $\overline{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper und in $\overline{Z}[x]$ gibt es zu jedem Grad nur endlich viele Polynome, also auch nur endlich viele Kandidaten für Faktoren von $\bar{f}(x)$.

Kriterium 5 (Eisensteinkriterium). [5, S. 257] *Sei R ein faktorieller Ring und*

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$$

ein primitives Polynom vom Grad $n \geqslant 1$. Wenn es ein Primelement $p \in R$ gibt, sodass

$$p \mid a_0, \ldots, p \mid a_{n-1}, \text{ aber } p \nmid a_n \text{ und } p^2 \nmid a_0$$

gilt, so ist $f(x)$ irreduzibel in $R[x]$ und wegen des Irreduzibilitätssatzes 2 gilt dies auch im Polynomring $\mathrm{Quot}(R)[x]$ über dem Quotientenkörper $\mathrm{Quot}(R)$ von R.

Wir verwenden dieses Kriterium für $R = \mathbb{Z}$ und für normierte Polynome, welche automatisch primitiv sind.

Kriterium 6 (Substitutionskriterium). [11, S. 90]
Zum Nachweis der Irreduzibilität von $f(x) \in \mathbb{Z}[x]$ genügt es, zu zeigen, dass $f(x-a)$ irreduzibel ist für ein passendes $a \in \mathbb{Z}$.

5 Konkrete Beispiele für Satz 13

Es folgen drei Beispiele zu jedem der fünf Fälle des Klassifikationssatzes 13 zur Bestimmung der Galoisgruppe von Polynomen vierten Grades. In den Fällen (iii)-(v) ist jeweils das zweite Beispiel ein biquadratisches Polynom, welches im darauffolgenden Kapitel 3 zu biquadratischen Polynomen erneut untersucht wird. Abschließend folgt noch ein allgemeineres Beispiel. Der Grundkörper der nachfolgenden Polynome sei stets $K = \mathbb{Q}$.[7]

5.1 Fall (i) Galoisgruppe S_4

Beispiel 3.
Untersuchung der Galoisgruppe des Polynoms
$p_1(x) = x^4 + 2x^3 + 2x^2 + 2x + 2$.

Es ist $p_1(x) = x^4 + 2x^3 + 2x^2 + 2x + 2$ irreduzibel nach dem Eisensteinkriterium 5 mit $p = 2$. Es ist $a = b = c = d = 2$ und die kubische Resolvente lautet

$$\begin{aligned} r_1(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 2x^2 + (2 \cdot 2 - 4 \cdot 2)x - (2^2 \cdot 2 - 4 \cdot 2 \cdot 2 + 2^2) \\ &= x^3 - 2x^2 - 4x + 4. \end{aligned}$$

Das Polynom $r_1(x)$ ist vom Grad 3. Nach dem Nullstellenkriterium 3 müssen wir für die Irreduzibilität von $r_1(x)$ über $\mathbb{Q}$ nur zeigen, dass keine ganzzahlige Nullstelle existiert. Wir zeigen, dass modulo 3 keine Nullstelle existiert (und folglich auch in $\mathbb{Z}$).

$$\begin{aligned} r_1(x) &= x^3 - 2x^2 - 4x + 4 \\ &\equiv x^3 + x^2 - x + 1 \mod 3 \end{aligned}$$

[7] Die nachfolgenden Beispielpolynome wurden meist so gewählt, dass das Eisensteinkriterium 5 anwendbar ist.

und es ist

$$\begin{aligned} r_1(0) &= 0^3 + 0^2 - 0 + 1 = 1 \neq 0 \mod 3 \\ r_1(1) &= 1^3 + 1^2 - 1 + 1 = 2 \neq 0 \mod 3 \\ r_1(-1) &= (-1)^3 + (-1)^2 - 1 + 1 = 2 \neq 0 \mod 3. \end{aligned}$$

Das Polynom $r_1(x)$ hat keine Nullstelle in $\mathbb{Z}$. Für die Diskriminante ergibt sich:

$$\begin{aligned} A &= a^2d + c^2 - 4bd = 2^2 \cdot 2 + 2^2 - 4 \cdot 2 \cdot 2 = -4 \\ B &= ac - 4d = 2 \cdot 2 - 4 \cdot 2 = -4 \\ D &= -4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2 \\ &= -4 \cdot 2^3(-4) + 2^2 \cdot (-4)^2 + 18 \cdot 2 \cdot (-4)(-4) - 4(-4)^3 - 27 \cdot (-4)^2 \\ &= 592. \end{aligned}$$

Es ist $24^2 = 576 < 592 < 625 = 25^2$. Also gilt $592 \neq \mathbb{Q}^2$.
Nach dem Klassifikationssatz 13, Fall (i) gilt $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{S}_4$.

Beispiel 4.
Untersuchung der Galoisgruppe des Polynoms
$p_2(x) = x^4 - 2x^3 + x^2 - x - 1$.

Die möglichen ganzzahligen Nullstellen sind Teiler des absoluten Gliedes. Daher kommen hier nur ± 1 in Frage.

$$\begin{aligned} p_2(1) &= 1^4 - 2 \cdot 1^3 + 1^2 - 1 - 1 = 1 - 2 + 1 - 1 = -1 \neq 0 \\ p_2(-1) &= (-1)^4 - 2 \cdot (-1)^3 + (-1)^2 - (-1) - 1 = 4 \neq 0. \end{aligned}$$

Somit spaltet $p_2(x)$ keinen Linearfaktor ab. Für die Irreduzibilität von $p_2(x)$ bleibt noch zu zeigen, dass $p_2(x)$ in $\mathbb{Z}[X]$ nicht Produkt zweier Polynome vom Grad zwei ist. Dazu zeigen wir, dass der Ansatz

$$\begin{aligned} p_2(x) &= x^4 - 2x^3 + x^2 - x - 1 \\ &= (x^2 + Tx + U)(x^2 + Vx + W) \\ &= x^4 + (T + V)x^3 + (U + W + TV)x^2 + (UV + TW)x + UW \end{aligned}$$

mit $T, U, V, W \in \mathbb{Z}$ zum Widerspruch führt. Mit Koeffizientenvergleich folgt:

$$T + V = -2, \tag{2.14}$$
$$U + W + TV = +1, \tag{2.15}$$
$$UV + TW = -1, \tag{2.16}$$
$$UW = -1. \tag{2.17}$$

Aus (2.17) $UW = -1$ folgt $U = -1 \wedge W = 1$ (Fall 1)
oder $U = 1 \wedge W = -1$ (Fall 2).
Im ersten Fall folgt aus (2.16) $-1 = -V + T$ und mit (2.14), dass $-3 = 2T$ ↯, da $2 \nmid -3$.
Im zweiten Fall folgt aus (2.16) $V - T = -1$ und mit (2.14) $2V = -3$ ↯, denn -3 ist ungerade.
In beiden Fällen zerfällt $p_2(x)$ also nicht in zwei quadratische Polynome über $\mathbb{Z}$. Das Polynom $p_2(x)$ ist damit irreduzibel in $\mathbb{Z}$ und nach dem Gaußkriterium 1 in $\mathbb{Q}$.
Für die kubische Resolvente ergibt sich mit $a = -2, b = 1$,
$c = -1, d = -1$

$$\begin{aligned} r_2(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 1x^2 + (-2 \cdot (-1) - 4 \cdot (-1))x \\ &\quad - ((-2)^2 \cdot (-1) - 4 \cdot 1 \cdot (-1) + (-1)^2)) \\ &= x^3 - x^2 + 6x - 1. \end{aligned}$$

Wieder prüfen wir die möglichen Nullstellen ± 1.

$$\begin{aligned} r_2(1) &= 1^3 - 1^2 + 6 \cdot 1 - 1 = 5 \neq 0 \\ r_2(-1) &= (-1)^3 - (-1)^2 + 6 \cdot (-1) - 1 = -9 \neq 0. \end{aligned}$$

Damit hat $r_2(x)$ keine Nullstellen und ist nach dem Nullstellenkriterium 3 irreduzibel.

Es bleibt zu prüfen, ob die Diskriminante eine Quadratzahl ist. Es ist

$$\begin{aligned}
A &= a^2d + c^2 - 4bd = (-2)^2 \cdot (-1) + (-1)^2 - 4 \cdot 1 \cdot (-1) = 1 \\
B &= ac - 4d = -2 \cdot (-1) - 4 \cdot (-1) = 6 \\
D &= -4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2 \\
&= -4 \cdot 1^3 \cdot 1 + 1^2 \cdot 6^2 + 18 \cdot 1 \cdot 1 \cdot 6 - 4 \cdot 6^3 - 27 \cdot 1^2 \\
&= -751.
\end{aligned}$$

Die Diskriminante der gemeinsamen kubischen Resolvente ist also negativ und damit insbesondere keine Quadratzahl in $\mathbb{Q}$.
Nach dem Klassifikationssatz 13, Fall (i) gilt $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{S}_4$.

Beispiel 5.
Untersuchung der Galoisgruppe des Polynoms
$p_3(x) = x^4 + 3x^3 + 3x^2 + 3$.

Es ist $p_3(x) = x^4 + 3x^3 + 3x^2 + 3$ irreduzibel nach dem Eisensteinkriterium 5 mit $p = 3$. Es ist $a = 3, b = 3, c = 0$ sowie $d = 3$ und die kubische Resolvente lautet

$$\begin{aligned}
r_3(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\
&= x^3 - 3x^2 + (3 \cdot 0 - 4 \cdot 3)x - (3^2 \cdot 3 - 4 \cdot 3 \cdot 3 + 0^2) \\
&= x^3 - 3x^2 - 12x + 9.
\end{aligned}$$

Das Polynom $r_3(x)$ ist vom Grad 3. Nach dem Nullstellenkriterium 3 müssen wir für die Irreduzibilität von $r_3(x)$ über $\mathbb{Q}$ lediglich zeigen, dass keine ganzzahlige Nullstelle existiert. Wir zeigen, dass modulo 2 keine Nullstelle existiert (und folglich auch in $\mathbb{Z}$).

$$\begin{aligned}
r_3(x) &= x^3 - 3x^2 - 12x + 9 \\
&\equiv x^3 + x^2 + 1 \mod 2
\end{aligned}$$

und es ist

$$\begin{aligned}
r_3(0) &= 0^3 + 0^2 + 1 = 1 \neq 0 \mod 2 \\
r_3(1) &= 1^3 + 1^2 + 1 = 1 \neq 0 \mod 2.
\end{aligned}$$

Das Polynom $r_3(x)$ hat daher keine Nullstelle in $\mathbb{Z}$.
Es bleibt zu prüfen, ob die Diskriminante eine Quadratzahl ist. Es ist

$$\begin{aligned}
A &= a^2d + c^2 - 4bd = 3^2 \cdot 3 + 0^2 - 4 \cdot 3 \cdot 3 = -9 \\
B &= ac - 4d = 3 \cdot 3 - 4 \cdot 3 = -3 \\
D &= -4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2 \\
&= -4 \cdot 3^3 \cdot (-9) + 3^2 \cdot (-3)^2 + 18 \cdot 3 \cdot (-9) \cdot (-3) \\
&\quad - 4 \cdot (-3)^3 - 27 \cdot (-9)^2 \\
&= 432.
\end{aligned}$$

Es ist

$$20^2 = 400 < D = 432 < 441 = 21^2.$$

Somit ist $D = 432 \notin \mathbb{Q}^2$.
Nach dem Klassifikationssatz 13, Fall (i) gilt $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{S}_4$.

5.2 Fall (ii) Galoisgruppe $\mathbf{A_4}$

Beispiel 6.
Untersuchung der Galoisgruppe des Polynoms
$p_4(x) = x^4 - 2x^3 + 2x^2 + 2$.

Das Polynom $p_4(x) = x^4 - 2x^3 + 2x^2 + 2$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 2$.
Für die kubische Resolvente ergibt sich mit $a = -2, b = 2, c = 0, d = 2$:

$$\begin{aligned}
r_4(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\
&= x^3 - 2x^2 + ((-2) \cdot 0 - 4 \cdot 2)x - ((-2)^2 \cdot 2 - 4 \cdot 2 \cdot 2 + 0^2) \\
&= x^3 - 2x^2 - 8x + 8.
\end{aligned}$$

Wie in den vorherigen Beispielen zeigen wir die Irreduzibilität von $r_4(x)$, indem wir zeigen, dass modulo einer Primzahl, hier 3, keine

Nullstellen existieren.

$$\begin{aligned} r_4(x) &= x^3 - 2x^2 - 8x + 8 \\ &\equiv x^3 + x^2 + x + 2 \mod 3 \end{aligned}$$

Wir prüfen alle Restklassen aus $\mathbb{Z}/3\mathbb{Z}$

$$\begin{aligned} r_4(0) &= 0^3 + 0^2 + 0 + 2 = 2 \neq 0 \mod 3, \\ r_4(-1) &= (-1)^3 + (-1)^2 + (-1) + 2 = 1 \neq 0 \mod 3, \\ r_4(1) &= 1^3 + 1^2 + 1 + 2 = 2 \neq 0 \mod 3. \end{aligned}$$

Also ist $r_4(x)$ nach dem Nullstellenkriterium 3 irreduzibel über $\mathbb{Q}$. Es bleibt zu überprüfen, ob die Diskriminante eine Quadratzahl ist. Für die gemeinsame Diskriminante D von $r_4(x)$ bzw. $p_4(x)$ ergibt sich

$$\begin{aligned} A &= a^2d + c^2 - 4bd = (-2)^2 \cdot 2 + 0^2 - 4 \cdot 2 \cdot 2 = -8, \\ B &= ac - 4d = -2 \cdot 0 - 4 \cdot 2 = -8, \\ D &= -4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2 \\ &= -4 \cdot 2^3(-8) + 2^2 \cdot (-8)^2 + 18 \cdot 2 \cdot (-8) \cdot (-8) - 4 \cdot (-8)^3 \\ &\quad - 27 \cdot (-8)^2 \\ &= 3136 = 56^2 \in \mathbb{Q}^2. \end{aligned}$$

Nach dem Klassifikationssatz 13, Fall (ii) gilt $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{A}_4$.

Beispiel 7.
Untersuchung der Galoisgruppe des Polynoms
$p_5(x) = x^4 + 2x^3 + 6x^2 + 4x + 2$.

Das Polynom $p_5(x) = x^4 + 2x^3 + 6x^2 + 4x + 2$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 2$.

Für die kubische Resolvente ergibt sich mit $a = 2, b = 6, c = 4, d = 2$:

$$\begin{aligned} r_5(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 6x^2 + (2 \cdot 4 - 4 \cdot 2)x - (2^2 \cdot 2 - 4 \cdot 6 \cdot 2 + 4^2) \\ &= x^3 - 6x^2 + 24. \end{aligned}$$

Da $r_5(x)$ vom Grad 3 ist, ist die Irreduzibilität nach dem Nullstellenkriterium 3 gleichbedeutend damit, dass kein Linearfaktor abgespalten wird, also keine ganzzahlige Nullstelle existiert. Dies verifizieren wir, indem wir $r_5(x)$ modulo 5 betrachten.
Es ist $r_5(x) = x^3 - 6x^2 + 24 \equiv x^3 - x^2 - 1 \mod 5$ und

$$\begin{aligned} r_5(0) &= 0^3 - 0^2 - 1 = -1 \not\equiv 0 \mod 5 \\ r_5(1) &= 1^3 - 1^2 - 1 = -1 \not\equiv 0 \mod 5 \\ r_5(2) &= 2^3 - 2^2 - 1 = 3 \not\equiv 0 \mod 5 \\ r_5(-1) &= (-1)^3 - (-1)^2 - 1 = -3 \not\equiv 0 \mod 5 \\ r_5(-2) &= (-2)^3 - (-2)^2 - 1 = 2 \not\equiv 0 \mod 5. \end{aligned}$$

Damit ist $r_5(x)$ irreduzibel in $\mathbb{Q}$.
Es bleibt zu überprüfen, ob die Diskriminante eine Quadratzahl ist.
Für die Diskriminante D von $r_5(x)$ bzw. $p_5(x)$ ergibt sich

$$\begin{aligned} A &= a^2d + c^2 - 4bd = 2^2 \cdot 2 + 4^2 - 4 \cdot 6 \cdot 2 = -24 \\ B &= ac - 4d = 2 \cdot 4 - 4 \cdot 2 = 0 \\ D &= -4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2 \\ &= -4 \cdot 6^3(-24) + 6^2 \cdot 0^2 + 18 \cdot 6 \cdot (-24) \cdot 0 - 4 \cdot 0^3 - 27 \cdot (-24)^2 \\ &= 5184 = 72^2 \in \mathbb{Q}^2. \end{aligned}$$

Nach dem Klassifikationssatz 13, Fall (ii) gilt $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{A}_4$.

Beispiel 8.
Untersuchung der Galoisgruppe des Polynoms
$p_6(x) = x^4 + 2x^3 + 2x^2 - 4x + 2$.

Das Polynom $p_6(x) = x^4 + 2x^3 + 2x^2 - 4x + 2$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 2$.

Für die kubische Resolvente ergibt sich mit
$a = 2, b = 2, c = -4, d = 2$

$$\begin{aligned} r_6(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 2x^2 + (2 \cdot (-4) - 4 \cdot 2)x - (2^2 \cdot 2 - 4 \cdot 2 \cdot 2 + (-4)^2) \\ &= x^3 - 2x^2 - 16x - 8. \end{aligned}$$

Das Polynom $r_6(x)$ ist vom Grad 3. Nach dem Nullstellenkriterium 3 müssen wir für die Irreduzibilität von $r_6(x)$ über $\mathbb{Q}$ lediglich zeigen, dass keine ganzzahlige Nullstelle existiert. Wir zeigen, dass modulo 3 keine Nullstelle existiert (und folglich auch in $\mathbb{Z}$).

$$\begin{aligned} r_6(x) &= x^3 - 2x^2 - 16x - 8 \\ &\equiv x^3 + x^2 - x + 1 \mod 3 \end{aligned}$$

und es ist

$$\begin{aligned} r_6(0) &= 0^3 + 0^2 - 0 + 1 = 1 \not\equiv 0 \mod 3, \\ r_6(-1) &= (-1)^3 + (-1)^2 - (-1) + 1 = 2 \not\equiv 0 \mod 3, \\ r_6(1) &= 1^3 + 1^2 - 1 + 1 = 2 \not\equiv 0 \mod 3. \end{aligned}$$

Also ist $r_6(x)$ irreduzibel in $\mathbb{Q}$.
Es bleibt zu überprüfen, ob die Diskriminante eine Quadratzahl ist. Für die gemeinsame Diskriminante D von $r_6(x)$ bzw. $p_6(x)$ ergibt sich

$$\begin{aligned} A &= a^2d + c^2 - 4bd = 2^2 \cdot 2 + (-4)^2 - 4 \cdot 2 \cdot 2 = 8 \\ B &= ac - 4d = 2 \cdot (-4) - 4 \cdot 2 = -16 \\ D &= -4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2 \\ &= -4 \cdot 2^3 \cdot 8 + 2^2 \cdot (-16)^2 + 18 \cdot 2 \cdot 8 \cdot (-16) - 4 \cdot (-16)^3 - 27 \cdot 8^2 \\ &= 10816 = 104^2 \in \mathbb{Q}^2. \end{aligned}$$

Nach dem Klassifikationssatz 13, Fall (ii) gilt $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{A}_4$.

5.3 Fall (iii) Galoisgruppe V_4

Beispiel 9.
Untersuchung der Galoisgruppe von $p_7(x) = x^4 + 4x^3 + 6x^2 + 4x + 2$.

Das Polynom $p_7(x) = x^4 + 4x^3 + 6x^2 + 4x + 2$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 2$.
Für die kubische Resolvente ergibt sich mit $a = 4, b = 6, c = 4, d = 2$

$$\begin{aligned} r_7(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 6x^2 + (4 \cdot 4 - 4 \cdot 2)x - (4^2 \cdot 2 - 4 \cdot 6 \cdot 2 + 4^2) \\ &= x^3 - 6x^2 + 8x \\ &= x(x-2)(x-4). \end{aligned}$$

Also zerfällt $r_7(x)$ schon über $\mathbb{Q}$ in Linearfaktoren und es liegt Fall (iii) des Klassifikationssatzes 13 vor. Damit ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{V}_4$.
Falls nur die Reduzibilität der kubischen Resolvente bekannt ist, können wir alternativ untersuchen, ob $D \in \mathbb{Q}^2$ ist, anstatt zu prüfen, ob die anderen beiden Nullstellen auch in K liegen. Für die Diskriminante D von $r_7(x)$ bzw. $p_7(x)$ ergibt sich

$$\begin{aligned} A &= a^2d + c^2 - 4bd = 4^2 \cdot 2 + 4^2 - 4 \cdot 6 \cdot 2 = 0 \\ B &= ac - 4d = 4 \cdot 4 - 4 \cdot 2 = 8 \\ D &= -4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2 \\ &= -4 \cdot 6^3 \cdot 0 + 6^2 \cdot 8^2 + 18 \cdot 6 \cdot 0 \cdot 8 - 4 \cdot 8^3 - 27 \cdot 0^2 \\ &= 16^2 \in \mathbb{Q}^2. \end{aligned}$$

Aus der Bemerkung 7, Fall (iii)' folgt dann, dass $\mathrm{Gal}(F/K) \cong \mathrm{V}_4$.

Beispiel 10.
Untersuchung der Galoisgruppe von $p_8(x) = x^4 + 6x^2 + 4$.

Über Substitution und die p-q–Formel können wir die Nullstellen in den komplexen Zahlen angeben. Substitution $u := x^2$ ergibt $u^2 + 6u + 4 = 0$ und damit

$$u = -3 \pm \sqrt{9-4} = -3 \pm \sqrt{5} \notin \mathbb{Q}.$$

Somit spaltet $p_8(x)$ keinen Linearfaktor ab. Für die Irreduzibilität von $p_8(x)$ bleibt noch zu zeigen, dass $p_8(x)$ in $\mathbb{Z}[X]$ nicht Produkt zweier Polynome vom Grad zwei ist. Dazu zeigen wir, dass der Ansatz

$$\begin{aligned} p_8(x) &= x^4 + 6x^2 + 4 \\ &= (x^2 + Tx + U)(x^2 + Vx + W) \\ &= x^4 + (T+V)x^3 + (U + W + TV)x^2 + (UV + TW)x + UW \end{aligned}$$

mit $T, U, V, W \in \mathbb{Z}$ zum Widerspruch führt. Mit Koeffizientenvergleich folgt

$$T + V = 0, \tag{2.18}$$

$$U + W + TV = 6, \tag{2.19}$$

$$UV + TW = 0, \tag{2.20}$$

$$UW = 4. \tag{2.21}$$

Sei $V = 0$, dann folgt aus (2.18), dass $T = 0$ ist. Gleichung (2.19), also $U + W = 6$, eingesetzt in (2.21), ergibt $U(6 - U) = 4$, also $-U^2 + 6U - 4 = 0$. Daraus folgt $U = 3 \pm \sqrt{5}$ ↯, im Widerspruch zu $U \in \mathbb{Z}$.
Sei nun $V \neq 0$, dann folgt aus Gleichung (2.18) also $T = -V$ eingesetzt in (2.20), dass $UV = VW$, also $U = W$ ist. Aus (2.21) folgt dann $U = W = 2$ (Fall 1) oder $U = W = -2$ (Fall 2).
Im ersten Fall folgt aus (2.18), eingesetzt in (2.19), dass $V = \pm\sqrt{-2}$, was im Widerspruch zu $V \in \mathbb{Z}$ steht.
Im zweiten Fall folgt aus (2.18), eingesetzt in (2.19), dass $V = \pm\sqrt{-10}$, was im Widerspruch zu $V \in \mathbb{Z}$ steht.
Damit zerfällt $p_8(x)$ nicht in zwei quadratische Polynome über $\mathbb{Z}$. Das Polynom $p_8(x)$ ist damit irreduzibel in $\mathbb{Z}$ und nach dem Gaußkriterium 1 auch in $\mathbb{Q}$.

Mit $a = 0, b = 6, c = 0, d = 4$ ergibt sich für die kubische Resolvente

$$\begin{aligned} r_8(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 6x^2 + (0 \cdot 0 - 4 \cdot 4)x - (0^2 \cdot 4 - 4 \cdot 6 \cdot 4 + 0^2) \\ &= x^3 - 6x^2 - 16x + 96 \\ &= (x + 4)(x - 4)(x - 6). \end{aligned}$$

Die kubische Resolvente $r_8(x)$ zerfällt somit vollständig in Linearfaktoren in $\mathbb{Q}$.
Nach dem Klassifikationssatz 13, Fall (iii) gilt $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{V}_4$. Falls nur die Reduzibilität der kubsichen Resolvente bekannt ist, können wir alternativ untersuchen, ob $D \in \mathbb{Q}^2$ ist, anstatt zu prüfen, ob die anderen beiden Nullstellen auch in K liegen. Für die Diskriminante D von $r_8(x)$ bzw. $p_8(x)$ ergibt sich

$$\begin{aligned} A &= a^2d + c^2 - 4bd = 0^2 \cdot 4 + 0^2 - 4 \cdot 6 \cdot 4 = -96 \\ B &= ac - 4d = 0 \cdot 0 - 4 \cdot 4 = -16 \\ D &= -4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2 \\ &= -4 \cdot 6^3 \cdot (-96) + 6^2 \cdot (-16)^2 + 18 \cdot 6 \cdot (-96) \cdot (-16) - 4 \cdot (-16)^3 \\ &\quad - 27 \cdot (-96)^2 \\ &= 160^2 \in \mathbb{Q}^2. \end{aligned}$$

Aus der Bemerkung 7, Fall (iii)' folgt dann, dass $\mathrm{Gal}(F/K) \cong \mathrm{V}_4$.
Später dient das Polynom $p_8(x)$ auch als Beispiel für ein vereinfachtes Verfahren für biquadratische Polynome.

Beispiel 11.
Untersuchung der Galoisgruppe des Polynoms
$p_9(x) = x^4 - 4x^3 + 2x^2 + 4x - 2$.

Das Polynom $p_9(x) = x^4 - 4x^3 + 2x^2 + 4x - 2$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 2$.
Mit $a = -4, b = 2, c = 4, d = -2$ ergibt sich für die kubische Resolvente

$$\begin{aligned} r_9(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 2x^2 + (-4 \cdot 4 - 4 \cdot (-2))x - ((-4)^2 \cdot (-2) \\ &\quad - 4 \cdot 2 \cdot (-2) + 4^2) \\ &= x^3 - 2x^2 - 8x \\ &= (x-4)x(x+2). \end{aligned}$$

Die kubische Resolvente $r_9(x)$ zerfällt vollständig in Linearfaktoren in $\mathbb{Q}$.
Nach dem Klassifikationssatz 13, Fall (iii) gilt $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{V}_4$.
Falls nur die Reduzibilität der kubsichen Resolvente bekannt ist, können wir alternativ untersuchen, ob $D \in \mathbb{Q}^2$ ist, anstatt zu prüfen, ob die anderen beiden Nullstellen auch in K liegen. Für die Diskriminante D von $r_9(x)$ bzw. $p_9(x)$ ergibt sich

$$\begin{aligned} A &= a^2d + c^2 - 4bd = (-4)^2 \cdot (-2) + 4^2 - 4 \cdot 2 \cdot (-2) = 0 \\ B &= ac - 4d = (-4) \cdot 4 - 4 \cdot (-2) = -8 \\ D &= -4b^3A + b^2B^2 + 18bAB - 4B^3 - 27A^2 \\ &= -4 \cdot 2^3 \cdot 0 + 2^2 \cdot (-8)^2 + 18 \cdot 2 \cdot 0 \cdot (-8) - 4 \cdot (-8)^3 - 27 \cdot 0^2 \\ &= 48^2 \in \mathbb{Q}^2. \end{aligned}$$

Aus der Bemerkung 7, Fall (iii)' folgt dann, dass $\mathrm{Gal}(F/K) \cong \mathrm{V}_4$.

5.4 Fall (iv) Galoisgruppe $\mathbf{C_4}$

Beispiel 12.
Untersuchung der Galoisgruppe des Polynoms
$p_{10}(x) = x^4 + x^3 + x^2 + x + 1$.[8]

Wir zeigen auf zwei Weisen die Irreduziblität von $p_{10}(x)$ über $\mathbb{Q}$.

(i) Setzen wir $x = \tilde{x} + 1$, ergibt sich

$$\begin{aligned} p_{10}(\tilde{x}+1) &= (\tilde{x}+1)^4 + (\tilde{x}+1)^3 + (\tilde{x}+1)^2 + (\tilde{x}+1) + 1 \\ &= \tilde{x}^4 + 4\tilde{x}^3 + 6\tilde{x}^2 + 4\tilde{x} + 1 + \tilde{x}^3 + 3\tilde{x}^2 + 3\tilde{x} + 1 \\ &\quad + \tilde{x}^2 + 2\tilde{x} + 1 + \tilde{x} + 1 + 1 \\ &= \tilde{x}^4 + 5\tilde{x}^3 + 10\tilde{x}^2 + 10\tilde{x} + 5. \end{aligned}$$

Das Polynom $p_{10}(\tilde{x}+1)$ irreduzibel nach dem Eisensteinkriterium 5 mit $p = 5$. Nach dem Substitutionskriterium 6 ist $p_{10}(x)$ irreduzibel über $\mathbb{Q}$.

(ii) Es ergibt sich

$$\begin{aligned} p_{10}(1) &= 1^4 + 1^3 + 1^2 + 1 + 1 = 5 \neq 0 \\ &= (-1)^4 + (-1)^3 + (-1)^2 + (-1) + 1 = 1. \end{aligned}$$

Somit spaltet $p_{10}(x)$ keinen Linearfaktor ab. Für die Irreduzibilität von $p_{10}(x)$ bleibt noch zu zeigen, dass $p_{10}(x)$ nicht in zwei Polynome zweiten Grades zerfällt. Dazu zeigen wir, dass der Ansatz

$$\begin{aligned} p_{10}(x) &= x^4 + x^3 + x^2 + x + 1 \\ &= (x^2 + Tx + U)(x^2 + Vx + W) \\ &= x^4 + (T+V)x^3 + (U + W + TV)x^2 \\ &\quad + (UV + TW)x + UW \end{aligned}$$

[8] Das Polynom $p_{10}(x) = x^4 + x^3 + x^2 + x + 1$ ist das Kreisteilungspolynom für fünfte Einheitswurzeln.

mit $T, U, V, W \in \mathbb{Z}$ zum Widerspruch führt. Mit Koeffizientenvergleich folgt

$$T + V = 1 \tag{2.22}$$
$$U + W + TV = 1 \tag{2.23}$$
$$UV + TW = 1 \tag{2.24}$$
$$UW = 1. \tag{2.25}$$

Aus (2.25) $UW = 1$ folgt $U = 1 \wedge W = 1$ (Fall 1) oder $U = -1 \wedge W = -1$ (Fall 2).

Im ersten Fall ist $V \neq 0$, denn falls $V = 0$ wäre, folgt aus (2.22), dass $T = 1$. Dies steht im Widerspruch zu (2.23), da $1+1+1\cdot 0 = 2 \neq 1$ ist. Wir können also $V \neq 0$ annehmen. Dann folgt aus (2.23) $T = \frac{-1}{V}$, eingesetzt in (2.22), dass $\frac{-1}{V} + V = 1$.

Daraus folgt $V^2 - V - 1 = \left(V - \frac{1}{2} + \frac{\sqrt{5}}{2}\right)\left(V - \frac{1}{2} - \frac{\sqrt{5}}{2}\right) = 0$ ↯, da $-\frac{1}{2} \pm \frac{\sqrt{5}}{2} \neq \mathbb{Z}$.

Im zweiten Fall ist $V \neq 0$, denn falls $V = 0$ wäre, folgt aus (2.22), dass $T = 1$. Dies steht im Widerspruch zu (2.23), da $-1+-1+1\cdot 0 = -2 \neq 1$ ist. Wir können also $V \neq 0$ annehmen. Dann folgt aus (2.23) $T = \frac{-3}{V}$, eingesetzt in (2.22), dass $\frac{-3}{V} + V = 1$.

Daraus folgt $V^2 - V - 3 = \left(V - \frac{1}{2} + \frac{\sqrt{13}}{2}\right)\left(V - \frac{1}{2} - \frac{\sqrt{13}}{2}\right) = 0$ ↯, da $-\frac{1}{2} \pm \frac{\sqrt{13}}{2} \neq \mathbb{Z}$.

In beiden Fällen zerfällt $p_{10}(x)$ also nicht in zwei quadratische Polynome über $\mathbb{Z}$. Das Polynom $p_{10}(x)$ ist damit irreduzibel in $\mathbb{Z}$ und nach dem Gaußkriterium 1 in $\mathbb{Q}$.

Für die kubische Resolvente ergibt sich

$$\begin{aligned} r_{10}(x) &= x^3 - 1 \cdot x + (1 \cdot 1 - 4 \cdot 1) \cdot x - (1^2 \cdot 1 - 4 \cdot 1 \cdot 1 + 1^2) \\ &= x^3 - x^2 - 3x + 2 \\ &= (x-2)(x^2 + x - 1) \end{aligned}$$

mit den Nullstellen $t_1 = 2, t_{2,3} = -\frac{1}{2} \pm \frac{\sqrt{5}}{2}$ und Zerfällungskörper $E = \mathbb{Q}(\sqrt{5})$.
Das Hilfspolynom $g_{10}(x)$ wird zu

$$\begin{aligned} g_{10}(x) &= (x^2 - tx + d)(x^2 + ax + (b - t)) \\ &= (x^2 - 2x + 1)(x^2 + x + (1 - 2)) \\ &= (x^2 - 2x + 1)(x^2 + x - 1) \\ &= (x - 1)^2 \left(x + \frac{1}{2} + \frac{\sqrt{5}}{2}\right)\left(x + \frac{1}{2} - \frac{\sqrt{5}}{2}\right) \in \mathbb{Q}(\sqrt{5})[x]. \end{aligned}$$

Damit zerfällt $g_{10}(x)$ vollständig in Linearfaktoren über E.
Nach dem Klassifikationssatz 13, Fall (iv) ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{C}_4$.

Beispiel 13.
Untersuchung der Galoisgruppe des Polynoms $p_{11}(x) = x^4 + 4x^2 + 2$.

Das Polynom $p_{11}(x) = x^4 + 4x^2 + 2$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 2$.
Mit $a = 0, b = 4, c = 0, d = 2$ ergibt sich für die kubische Resolvente

$$\begin{aligned} r_{11}(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 4x^2 + (0 \cdot 0 - 4 \cdot 2)x - (0^2 \cdot 2 - 4 \cdot 4 \cdot 2 + 0^2) \\ &= x^3 - 4x^2 - 8x + 32 = (x - 4)(x^2 - 8) \\ &= (x - 4)(x - 2\sqrt{2})(x + 2\sqrt{2}). \end{aligned}$$

Der Zerfällungskörper von $r_{11}(x)$ ist somit $E = \mathbb{Q}(\sqrt{2})$ und die kubische Resolvente hat genau eine rationale Nullstelle $t = 4$.
Das Hilfspolynom $g_{11}(x)$ wird zu

$$\begin{aligned} g_{11}(x) &= (x^2 - tx + d)(x^2 + ax + (b - t)) \\ &= (x^2 - 4x + 2)(x^2 + 0 \cdot x + (4 - 4)) \\ &= (x^2 - 4x + 2)x^2 \\ &= (x - 2 + \sqrt{2})(x - 2 - \sqrt{2})x^2 \in \mathbb{Q}(\sqrt{2})[x]. \end{aligned}$$

Es zerfällt vollständig in Linearfaktoren über E.

Nach dem Klassifikationssatz 13, Fall (iv) ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{C}_4$.
Später dient das Polynom $p_{11}(x)$ auch als Beispiel für ein vereinfachtes Verfahren für biquadratische Polynome.

Beispiel 14.
Untersuchung der Galoisgruppe des Polynoms
$p_{12}(x) = x^4 + 10x^3 + 10x^2 - 5x - 5$.

Das Polynom $p_{12}(x) = x^4 + 10x^3 + 10x^2 - 5x - 5$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 5$.
Mit $a = 10, b = 10, c = -5, d = -5$ ergibt sich für die kubische Resolvente

$$\begin{aligned} r_{12}(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 10x^2 + (10 \cdot (-5) - 4 \cdot (-5))x \\ &\quad - (10^2 \cdot (-5) - 4 \cdot 10 \cdot (-5) + (-5)^2) \\ &= x^3 - 10x^2 - 30x + 275 \\ &= (x-5)(x^2 - 5x - 55) \\ &= (x-5)\left(\frac{5}{2} - \frac{7\sqrt{5}}{2}\right)\left(\frac{5}{2} + \frac{7\sqrt{5}}{2}\right). \end{aligned}$$

Der Zerfällungskörper von $r_{12}(x)$ ist somit $E = \mathbb{Q}(\sqrt{5})$ und die kubische Resolvente hat genau eine rationale Nullstelle $t = 5$.
Das Hilfspolynom $g_{12}(x)$ wird zu

$$\begin{aligned} g_{12}(x) &= (x^2 - tx + d)(x^2 + ax + (b - t)) \\ &= (x^2 - 5x - 5)(x^2 + 10 \cdot x + (10 - 5)) \\ &= (x^2 - 5x - 5)(x^2 + 10x + 5) \\ &= \left(x - \frac{5}{2} + \frac{3\sqrt{5}}{2}\right) \cdot \left(x - \frac{5}{2} - \frac{3\sqrt{5}}{2}\right) \cdot \\ &\quad \left(x + 5 + 2\sqrt{5}\right) \cdot \left(x + 5 - 2\sqrt{5}\right) \in \mathbb{Q}(\sqrt{5})[x]. \end{aligned}$$

Es zerfällt vollständig in Linearfaktoren über E. Nach dem Klassifikationssatz 13, Fall (iv) ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{C}_4$.

5.5 Fall (v) Galoisgruppe $\mathbf{D_4}$

Beispiel 15.
Untersuchung der Galoisgruppe von $p_{13}(x) = x^4 + 5x^3 + 5x^2 + 5x - 5$.

Das Polynom $p_{13}(x)$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 5$.
Mit $a = 5, b = 5, c = 5, d = -5$ ergibt sich für die kubische Resolvente

$$\begin{aligned}
r_{13}(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\
&= x^3 - 5x^2 + (5 \cdot 5 - 4 \cdot (-5))x - (5^2 \cdot (-5) - 4 \cdot 5 \cdot (-5) + 5^2) \\
&= x^3 - 5x^2 + 45x \\
&= x(x^2 - 5x + 45) \\
&= x\left(\left(x - \frac{5}{2}\right)^2 + \frac{155}{4}\right) \\
&= x\left(x - \frac{1}{2}(5 + i\sqrt{155})\right)\left(x - \frac{1}{2}(5 - i\sqrt{155})\right) \in \mathbb{Q}(i\sqrt{155})[x]
\end{aligned}$$

mit den Nullstellen $t = t_1 = 0, t_2 = -\frac{1}{2}\big(5 + i\sqrt{155}\big)$ und $t_3 = -\frac{1}{2}\big(5 - i\sqrt{155}\big)$. Der Zerfällungskörper ist somit $E = \mathbb{Q}\big(i\sqrt{155}\big)$.
Das Hilfspolynom $g_{13}(x)$ lautet

$$\begin{aligned}
g_{13}(x) &= (x^2 - tx + d)(x^2 + ax + (b - t)) \\
&= (x^2 - 0 \cdot x + (-5))(x^2 + 5x + (5 - 0)) \\
&= (x^2 - 5)(x^2 + 5x + 5) \\
&= (x - \sqrt{5})(x + \sqrt{5}) \\
&\quad \cdot \left(x + \frac{5}{2} - \frac{\sqrt{5}}{2}\right)\left(x + \frac{5}{2} + \frac{\sqrt{5}}{2}\right) \in \mathbb{Q}\big(\sqrt{5}\big)[x].
\end{aligned}$$

Die Zerfällungskörper der Polynome $g_{13}(x)$ und $r_{13}(x)$ stimmen damit offensichtlich nicht überein und $g_{13}(x)$ zerfällt nicht über $E = \mathbb{Q}\big(i\sqrt{155}\big)$ in Linearfaktoren, da $\sqrt{5} \notin \mathbb{Q}\big(i\sqrt{155}\big)$ ist. Wir zeigen $\sqrt{5} \notin \mathbb{Q}\big(i\sqrt{155}\big)$ durch Widerspruch: Angenommen es gäbe $a, b \in \mathbb{Q}$,

dann folgt aus $\sqrt{5} = a + bi\sqrt{155}$, dass $5 = a^2 - 155b^2 + 2abi\sqrt{155}$. Also muss $a = 0$ oder $b = 0$ sein. Im Falle von $a = 0$ folgt $\frac{-5}{155} = b^2$ im Widerspruch zu $b \in \mathbb{Q}$. Im Falle von $b = 0$ folgt $5 = a^2$ im Widerspruch zu $a \in \mathbb{Q}$.
Damit ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{D}_4$ nach dem Klassifikationssatz 13 Fall (v).

Beispiel 16.
Untersuchung der Galoisgruppe von $p_{14}(x) = x^4 + 2x^2 + 2$.

Das Polynom $p_{14}(x) = x^4 + 2x^2 + 2$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 2$. Mit $a = 0, b = 2, c = 0, d = 2$ ergibt sich für die kubische Resolvente

$$\begin{aligned} r_{14}(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 2x^2 + (0 \cdot 0 - 4 \cdot 2)x - (0^2 \cdot 2 - 4 \cdot 2 \cdot 2 + 0^2) \\ &= x^3 - 2x^2 - 8x + 16 \\ &= (x - 2)(x^2 - 8) \\ &= (x - 2)(x - 2\sqrt{2})(x + 2\sqrt{2}) \end{aligned}$$

mit den Nullstellen $t = t_1 = 2 \in \mathbb{Q}, t_2 = 2\sqrt{2} \notin \mathbb{Q}$ und $t_3 = -2\sqrt{2} \notin \mathbb{Q}$. Der Zerfällungskörper ist somit $E = \mathbb{Q}\big(\sqrt{2}\big)$.
Das Hilfspolynom $g_{14}(x)$ lautet

$$\begin{aligned} g_{14}(x) &= (x^2 - tx + d)(x^2 + ax + (b - t)) \\ &= (x^2 - 2 \cdot x + 2)(x^2 + 0 \cdot x + (2 - 2)) \\ &= (x^2 - 2x + 2)x^2 \\ &= (x - 1 - i)(x - 1 + i)x^2 \in \mathbb{Q}(i)[x]. \end{aligned}$$

Die Zerfällungskörper der Polynome $g_{14}(x)$ und $r_{14}(x)$ stimmen damit offensichtlich nicht überein und $g_{14}(x)$ zerfällt nicht über $E = \mathbb{Q}(i)$ in Linearfaktoren, da $\sqrt{2} \notin \mathbb{Q}(i)$ ist.
Damit ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{D}_4$ nach dem Klassifikationssatz 13, Fall (v).
Später dient das Polynom $p_{14}(x)$ auch als Beispiel für ein vereinfachtes Verfahren für biquadratische Polynome.

Beispiel 17.
Untersuchung der Galoisgruppe von $p_{15}(x) = x^4 - 4x^3 + 4x^2 + 6$.

Das Polynom $p_{15}(x) = x^4 - 4x^3 + 4x^2 + 6$ ist irreduzibel nach dem Eisensteinkriterium 5 mit $p = 2$.
Mit $a = -4, b = 4, c = 0, d = 6$ ergibt sich für die kubische Resolvente

$$\begin{aligned} r_{15}(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 4x^2 + ((-4) \cdot 0 - 4 \cdot 6)x - ((-4)^2 \cdot 6 - 4 \cdot 4 \cdot 6 + 0^2) \\ &= x(x^2 - 4x - 24) \end{aligned}$$

mit den Nullstellen $t = t_1 = 0 \in \mathbb{Q}, t_2 = 2 - 2\sqrt{7} \notin \mathbb{Q}$ und $t_3 = 2 + 2\sqrt{7} \notin \mathbb{Q}$. Der Zerfällungskörper ist somit $E = \mathbb{Q}(\sqrt{7})$.
Das Hilfspolynom $g_{15}(x)$ lautet

$$\begin{aligned} g_{15}(x) &= (x^2 - tx + d)(x^2 + ax + (b - t)) \\ &= (x^2 - 0 \cdot x + 6)(x^2 - 4x + (4 - 0)) \\ &= (x^2 + 6)(x - 2)^2 \\ &= \left(x - \sqrt{6}i\right)\left(x + \sqrt{6}i\right)(x - 2)^2 \end{aligned}$$

und zerfällt wegen $\pm\sqrt{6}i \notin \mathbb{Q}(\sqrt{7})$ nicht über $E = \mathbb{Q}(\sqrt{7})$ in Linearfaktoren. Damit ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{D}_4$ nach dem Klassifikationssatz 13, Fall (v).

5.6 Fall (i), (iv) und (v) Galoisgruppen S_4, C_4 und D_4

Beispiel 18. [8, S. 136]
Sei p eine Primzahl. Untersuchung der Galoisgruppe des Polynoms $f(x) = x^4 + px + p$.

Das Polynom $f(x) = x^4 + px + p$ ist irreduzibel nach dem Eisensteinkriterium 5.
Mit $a = 0, b = 0, c = p, d = p$ ergibt sich für die kubsiche Resolvente

$$\begin{aligned} r(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - 0 \cdot x^2 + (0 \cdot p - 4 \cdot p)x - (0^2 \cdot p - 4 \cdot 0 \cdot p + p^2) \\ &= x^3 - 4px - p^2. \end{aligned}$$

Da $r(x)$ ein normiertes Polynom ist, ist $r(x)$ genau dann irreduzibel,

wenn es keine ganzzahligen Nullstellen besitzt. Als mögliche Nullstellen kommen alle Teiler von $-p^2$ in Frage. Es ist

$$\begin{aligned}
r(1) &= 1^3 - 4p \cdot 1 - p^2 = 1 - 4p - p^2 \\
r(-1) &= (-1)^3 - 4p(-1) - p^2 = -1 + 4p - p^2 \\
r(p) &= p^3 - 4p \cdot p - p^2 = p^3 - 5p^2 = p^2(p-5) \\
r(-p) &= (-p)^3 - 4p \cdot (-p) - p^2 = -p^3 + 4p^2 - p^2 = -p^3 + 3p^2 \\
&= p^2(3-p) \\
r(p^2) &= \left(p^2\right)^3 - 4p \cdot p^2 - p^2 = p^6 - 4p^3 - p^2 = p^2(p^4 - 4p - 1) \\
r(-p^2) &= \left(-p^2\right)^3 - 4p\left(-p^2\right) - p^2 = -p^6 + 4p^3 - p^2 \\
&= p^2(-p^4 + 4p - 1).
\end{aligned}$$

Daraus folgt, dass $r(x)$ genau dann irreduzibel ist, wenn $p \notin \{3, 5\}$ ist, denn für $p = 3$ ist $r(-p) = r(-3) = 0$ und

für $p = 5$ ist $r(p) = r(5) = 0$.

1. Allgemeiner Fall: $p \notin \{3, 5\}$:[9]
Für die Diskriminante von $f(x)$ bzw. $r(x)$ ergibt sich

$$\begin{aligned}
A &= a^2d + c^2 - 4bd = 0^2 \cdot p + p^2 - 4 \cdot 0 \cdot p = p^2 \\
B &= ac - 4d = 0 \cdot p - 4 \cdot p = -4p \\
D &= -4b^3A + b^2B^2 + 18bBA - 4B^3 - 27A^2 \\
&= -4 \cdot 0^3 \cdot p^2 + 0^2 \cdot (-4p)^2 + 18 \cdot 0(-4p)p^2 - 4(-4p)^3 - 27\left(p^2\right)^2 \\
&= 256p^3 - 27p^4 \\
&= p^2(p(256 - 27p)).
\end{aligned}$$

[9] Im Artikel von Kappe und Warren [8, S. 136] steht als Folge des in Fußnote 3 erwähnten Fehlers der falsche Ausdruck $D = -p^3(99p - 64)$ für die Diskriminante.

Es ist also $D \in \mathbb{Q}^2$ genau dann, wenn $p(256-27p) \in \mathbb{Q}^2$. Es ist [10]

$$\begin{aligned} 400 = 20^2 \leqslant 2{\cdot}(256-27\cdot 2) &= 404 \leqslant 21^2 = 441 \\ 441 = 21^2 \leqslant 7{\cdot}(256-27\cdot 7) &= 469 \leqslant 22^2 = 484 \\ 11{\cdot}(256-27\cdot 11) &= -451 < 0 \notin \mathbb{Q}^2. \end{aligned}$$

Für $p \notin \{2,3,5,7\}$ ist $256-27p < 0$, also $p(256-27p) < 0$, und damit ist $D \notin \mathbb{Q}^2$. Für $p \notin \{3,5\}$ ist also $r(x)$ irreduzibel und D kein Quadrat in $\mathbb{Q}$. Nach dem Klassifikationssatz 13, Fall (i) ist also $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{S}_4$.

2. Fall: $p = 5$

Es ergibt sich für die kubische Resolvente

$$\begin{aligned} r(x) &= x^3 - 4\cdot 5\cdot x - 5^2 \\ &= x^3 - 20x - 25 \\ &= (x-5)(x^2+5x+5) \end{aligned}$$

mit den Nullstellen $t_1 = 5 \in \mathbb{Q}$ und $t_{2,3} = \frac{1}{2}\big(-5 \pm \sqrt{5}\big) \notin \mathbb{Q}$. Der Zerfällungskörper von $r(x)$ ist also $E = \mathbb{Q}\big(\sqrt{5}\big)$ und das Hilfspolynom

$$\begin{aligned} g(x) &= (x^2 - tx + d)(x^2 + ax + (b-t)) \\ &= (x^2 - 5x + 5)(x^2 + 0x + (0-5)) \\ &= (x^2 - 5x + 5)(x^2 - 5) \\ &= \big(x - \sqrt{5}\big)\big(x + \sqrt{5}\big) \\ &\quad \cdot (x - \frac{1}{2}\big(5+\sqrt{5}\big))(x - \frac{1}{2}\big(5-\sqrt{5}\big)) \in \mathbb{Q}\big(\sqrt{5}\big)[x] \end{aligned}$$

zerfällt über E vollständig in Linearfaktoren. Nach dem Klassifikationssatz 13, Fall (iv) ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{C}_4$.

[10] Selbst für $p \in \{3,5\}$ ist $p(256-27p) \notin K^2$, jedoch ist $p \in \{3,5\}$ im betrachteten Fall ohnehin ausgeschlossen.

3. Fall: $p = 3$
Die kubische Resolvente lautet

$$\begin{aligned} r(x) &= x^3 - 4 \cdot 3 \cdot x - 3^2 \\ &= x^3 - 12x - 9 \\ &= (x+3)(x^2 - 3x - 3) \end{aligned}$$

mit den Nullstellen $t_1 = -3$ und $t_{2,3} = \frac{1}{2}(3 \pm \sqrt{21})$.
Der Zerfällungskörper von $r(x)$ ist also $E = \mathbb{Q}(\sqrt{21})$ und das Hilfspolynom $g(x)$ lautet

$$\begin{aligned} g(x) &= (x^2 - tx + d)(x^2 + ax + (b - t)) \\ &= (x^2 - (-3)x + 3)(x^2 + 0x + (0 - (-3))) \\ &= (x^2 + 3x + 3)(x^2 + 3) \\ &= \left(\left(x + \frac{3}{2}\right)^2 + \frac{3}{4}\right)\left(x^2 + 3\right) > 0 \ \forall\, x \in \mathbb{Q}. \end{aligned}$$

Damit hat $g(x)$ noch nicht einmal wegen $E = \mathbb{Q}(\sqrt{21}) \subset \mathbb{R}$ eine reelle Nullstelle. Die kubische Resolvente $r(x)$ hat genau eine Nullstelle in $\mathbb{Q}$ und $g(x)$ zerfällt nicht über E in Linearfaktoren. Nach dem Klassifikationssatz 13, Fall (v) ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{D}_4$.

3 Galoisgruppen von biquadratischen Polynomen

Betrachten wir nun biquadratische Polynome, das heißt Polynome $p(x) = x^4+ax^3+bx^2+cx+d$ mit $a = 0, c = 0$. Die Nullstellen im Zerfällungskörper nennen wir weiterhin $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Da $p(x) = p(-x)$ ist mit a_i auch $-a_i$ eine Nullstelle. Nach geeigneter Umbenennung $\alpha, \beta \in F$ in $\alpha_1 = \alpha$,$\alpha_2 = -\alpha$,$\alpha_3 = \beta$,$\alpha_4 = -\beta$ gilt

$$\begin{aligned} p(x) &= x^4 + bx^2 + d \\ &= (x-\alpha)(x+\alpha)(x-\beta)(x+\beta) \\ &= (x^2-\alpha^2)(x^2-\beta^2) \\ &= x^4 - (\alpha^2+\beta^2)x^2 + \alpha^2\beta^2 \end{aligned}$$

und wir erhalten $-b = \alpha^2 + \beta^2$ und $d = \alpha^2\beta^2$ durch Koeffizientenvergleich. Wir hätten beide Gleichungen auch aus den elementarsymmetrischen Funktionen von $p(x)$ erhalten (siehe Bemerkung 4).

1 Irreduzibilitätskriterium biquadratischer Polynome

Satz 14 (Irreduzibilitätskriterium für biquadratische Polynome)**.** [8, S. 135]
Sei $p(x) = x^4 + bx^2 + d$ ein Polynom über K mit $\mathrm{char}(K) \neq 2$ *und seien $\pm\alpha, \pm\beta$ die Nullstellen von $p(x)$. Dann sind die folgenden drei Aussagen äquivalent:*

(i) *$p(x)$ ist irreduzibel über K,*

(ii) $\alpha^2 \notin K \ \wedge\ \alpha + \beta \notin K \ \wedge\ \alpha - \beta \notin K$,

(iii) $b^2 - 4d \notin K^2 \ \wedge \ -b + 2\sqrt{d} \notin K^2 \ \wedge \ -b - 2\sqrt{d} \notin K^2$.

Beweis. Das Polynom $p(x)$ hat keinen irreduziblen kubischen Faktor.[1] Es kann höchstens in zwei quadratische Faktoren zerfallen. Auf diese Faktoren müssen sich die Linearfaktoren $x \pm \alpha, x \pm \beta \in F[x]$ von $p(x)$ verteilen. Daher ist $p(x)$ reduzibel über K genau dann, wenn für mindestens eine der drei Faktorisierungen

$$\begin{aligned}
p(x) &= \underline{(x-\alpha)(x+\alpha)}(x-\beta)(x+\beta) \\
&= \underline{(x^2-\alpha^2)}(x^2-\beta^2) \\
p(x) &= \underline{(x-\alpha)}(x+\alpha)\underline{(x-\beta)}(x+\beta) \\
&= \underline{(x^2-(\alpha+\beta)x+\alpha\beta)}(x^2+(\alpha+\beta)x+\alpha\beta) \\
p(x) &= \underline{(x-\alpha)}(x+\alpha)(x-\beta)\underline{(x+\beta)} \\
&= \underline{(x^2-(\alpha-\beta)x-\alpha\beta)}(x^2+(\alpha-\beta)x-\alpha\beta)
\end{aligned}$$

alle Koeffizienten in K liegen. Die drei Faktorisierungen erhalten wir, indem wir je zwei Faktoren der Darstellung
$p(x) = (x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$ multiplizieren.
„$(i) \Longrightarrow (ii)$“: Wir zeigen dies durch Kontraposition. Es gelte also

$$\underbrace{\alpha^2 \in K}_{\text{Bed.1}} \ \vee \ \underbrace{\alpha+\beta \in K}_{\text{Bed.2}} \ \vee \ \underbrace{\alpha-\beta \in K.}_{\text{Bed.3}} \tag{3.1}$$

Angenommen, Bedingung 1 ist erfüllt, also $\alpha^2 \in K$. Dann folgt mit $\alpha^2+\beta^2 = -b \in K$, dass $\beta^2 \in K$ ist. Somit ist $p(x) = (x^2-\alpha^2)(x^2-\beta^2)$ eine Faktorisierung in $K[x]$, das heißt, $p(x)$ ist reduzibel.
Angenommen, Bedingung 2 oder Bedingung 3 ist erfüllt, also
$\alpha \pm \beta \in K$. Dann gilt die Folgerung

$$(\alpha \pm \beta)^2 = \alpha^2 + \beta^2 \pm 2\alpha\beta = -b \pm 2\alpha\beta \in K \Longrightarrow 2\alpha\beta \in K.$$

[1] Falls $p(x)$ einen kubischen irreduziblen Faktor hätte, dann gilt $p(x) = x^4 + bx^2 + d = (x-\xi)(x^3+...) = x^4 - \xi x^3 + ...$ dann muss $\xi = 0$ sein. Das Polynom $p(x)$ besitzt die Nullstelle $x = 0$. Dann folgt $d = 0$ und $p(x)$ hat mindestens eine doppelte Nullstelle bei $x = 0$, im Widerspruch dazu, dass es nur einen Linearfaktor gibt.

Wegen $\mathrm{char}(K) \neq 2$ folgt $\alpha\beta \in K$. Im Falle von $\alpha + \beta \in K$ besitzt $p(x)$ die Faktorisierung

$$p(x) = (x^2 - (\alpha + \beta)x + \alpha\beta)(x^2 + (\alpha + \beta)x + \alpha\beta)$$

und im Falle von
$\alpha - \beta \in K$ die Faktorisierung

$$p(x) = (x^2 - (\alpha - \beta)x - \alpha\beta)(x^2 + (\alpha - \beta)x - \alpha\beta).$$

Falls eine der Bedingungen
$\alpha^2 \in K \vee \alpha + \beta \in K \vee \alpha - \beta \in K$ erfüllt ist, ist $p(x)$ reduzibel.
„(ii) $\Longrightarrow$ (i)“: Es ist bei allen drei möglichen Faktorisierungen mindestens einer der Koeffizienten nicht in K, somit ist $p(x)$ irreduzibel.
„(iii) $\Longleftrightarrow$ (ii)“: Wir zeigen $\neg$(iii) $\Longleftrightarrow$ $\neg$(ii). Angenommen es gelte $\neg$(ii), also (3.1). Falls Bedingung 1, das heißt $\alpha^2 \in K$ erfüllt ist, erhalten wir

$$\begin{aligned}\alpha^2 \in K &\Longrightarrow b + 2\alpha^2 \in K \Longrightarrow \left(b + 2\alpha^2\right)^2 \in K^2 \\ &\Longrightarrow b^2 + 4b\alpha^2 + 4\alpha^4 = b^2 - 4((\alpha^2 + \beta^2)\alpha^2 - \alpha^4) \\ &= b^2 - 4\alpha^2\beta^2 = b^2 - 4d \in K^2.\end{aligned}$$

Falls Bedingung 2 oder Bedingung 3 erfüllt ist, erhalten wir

$$\begin{aligned}\alpha \pm \beta \in K &\Longrightarrow (\alpha \pm \beta)^2 \in K^2 \\ &\Longrightarrow (\alpha \pm \beta)^2 = \alpha^2 + \beta^2 \pm 2\sqrt{d} = -b \pm 2\sqrt{d} \in K^2.\end{aligned}$$

In jedem Fall folgt eine der Bedingungen von $\neg(iii)$

$$b^2 - 4d \in K^2 \ \vee \ -b + 2\sqrt{d} \in K^2 \ \vee \ -b - 2\sqrt{d} \in K^2.$$

Angenommen es gilt:

$$b^2 - 4d \in K^2 \vee -b + 2\sqrt{d} \in K^2 \vee -b - 2\sqrt{d} \in K^2.$$

Ist $b^2 - 4d \in K^2$, dann folgt

$$\begin{aligned} b^2 - 4d &= b^2 - 4\alpha^2\beta^2 = b^2 - 4((\alpha^2 + \beta^2)\alpha^2 - \alpha^4) \\ &= b^2 + 4b\alpha^2 + 4\alpha^4 = \left(b + 2\alpha^2\right)^2 \in K^2. \end{aligned}$$

Deswegen liegt $b+2\alpha^2 \in K$, woraus $2\alpha^2 \in K$ und wegen $\mathrm{char}(K) \neq 2$ folglich $\alpha^2 \in K$ ist.
Ist hingegen $-b \pm 2\sqrt{d} \in K^2$, so erhalten wir

$$-b \pm 2\alpha\beta \in K^2 \Longrightarrow \alpha^2 \pm 2\alpha\beta + \beta^2 = (\alpha \pm \beta)^2 \in K^2 \Longrightarrow \alpha \pm \beta \in K.$$

In jedem Fall folgt eine der Bedingungen $\alpha^2 \in K \ \vee \ \alpha + \beta \in K \ \vee \ \alpha - \beta \in K$ von $\neg(ii)$. □

Beispiel 19.
Sei $K = \mathbb{Q}$ der Grundkörper für die nachfolgenden Polynome. Wir untersuchen mit Hilfe des Irreduzibilitätskriteriums für biquadratische Polynome 14 die folgenden Polynome auf Irreduzibilität.

(i) Sei $p_{16}(x) = x^4 - 13x^2 + 36$. Es ist $b = -13$ und $d = 36$. Es gilt

$$b^2 - 4d = (-13)^2 - 4 \cdot 36 = 169 - 144 = 25 = 5^2 \in \mathbb{Q}^2.$$

Eine der Bedingungen des Satzes 14 von Teil (iii) ist nicht erfüllt. Es gelten im übrigen auch

$$\begin{aligned} -b + 2\sqrt{d} &= -(-13) + 2\sqrt{36} = 13 + 2 \cdot 6 = 25 = 5^2 \in \mathbb{Q}^2 \\ -b - 2\sqrt{d} &= -(-13) - 2\sqrt{36} = 13 - 2 \cdot 6 = 1 = 1^2 \in \mathbb{Q}^2. \end{aligned}$$

Es sind sogar alle drei Aussagen nicht erfüllt. Das Polynom $p_{16}(x)$ reduzibel nach Teil (i) des Satzes 14.

Es ergibt sich für $p_{16}(x)$ die Faktorisierung

$$p_{16}(x) = x^4 - 13x^2 + 36 = (x-3)(x+3)(x-2)(x+2).$$

(ii) Sei $p_{17}(x) = x^4 + 4x^2 - 32$. Es ist $b = 4$ und $d = -32$. Es ist

$$b^2 - 4d = 4^2 - 4 \cdot (-32) = 144 = 12^2 \in \mathbb{Q}^2.$$

Eine der drei Teilbedingungen von Teil (iii) des Satzes 14 ist nicht erfüllt. Damit ist $p_{17}(x)$ nach Teil (i) des Satzes 14 reduzibel über $\mathbb{Q}$. In diesem Fall wären die anderen beiden Bedingungen allerdings erfüllt

$$\begin{aligned} -b + 2\sqrt{d} &= -4 + 2\sqrt{-32} \notin \mathbb{Q}^2 \\ -b - 2\sqrt{d} &= -4 - 2\sqrt{-32} \notin \mathbb{Q}^2. \end{aligned}$$

Es ergibt sich nämlich

$$p_{17}(x) = x^4 + 4x^2 - 32 = (x^2+8)(x-2)(x+2).$$

(iii) Sei $p_{18}(x) = x^4 - 3x^2 + 3$. Es ist $b = -3$ und $d = 3$. Es ist

$$\begin{aligned} b^2 - 4d &= (-3)^2 - 4 \cdot 3 = -3 \notin \mathbb{Q}^2 && \wedge \\ -b + 2\sqrt{d} &= -(-3) + 2\sqrt{3} = 3 + 2\sqrt{3} \notin \mathbb{Q}^2 && \wedge \\ -b - 2\sqrt{d} &= -(-3) - 2\sqrt{3} = 3 - 2\sqrt{3} \notin \mathbb{Q}^2. \end{aligned}$$

Keine der Bedingungen von Teil (iii) des Satzes 14 ist erfüllt. Damit ist $p_{18}(x)$ nach Teil (i) des Satzes 14 irreduzibel über $\mathbb{Q}$.

Für biquadratische Polynome kann also mit Hilfe dieses Kriteriums 14 recht einfach die Irreduzibilitätsuntersuchung durchgeführt werden. Daher halten wir folgende Bemerkung fest:

Bemerkung 9.
Zur Untersuchung der Irreduziblität von $p(x)$ kann und sollte das Irreduzibilitätskriterium für biquadratische Polynome 14 verwendet werden.

Korollar 1 (Galoisgruppen von biquadratischen Polynomen). [8, S. 134]
Sei $p(x) = x^4 + bx^2 + d$ irreduzibel über K und sei K ein Körper der Charakteristik ungleich 2. Bezeichne F den Zerfällungskörper und $\pm\alpha, \pm\beta$ die Nullstellen von $p(x)$. Dann gilt

(i) $\mathrm{Gal}(F/K) \cong \mathrm{V}_4 \iff d \in K^2 \iff \alpha\beta \in K$,

(ii) $\mathrm{Gal}(F/K) \cong \mathrm{C}_4 \iff d(b^2 - 4d) \in K^2 \iff K(\alpha\beta) = K(\alpha^2)$,

(iii) $\mathrm{Gal}(F/K) \cong \mathrm{D}_4 \iff d \notin K^2 \wedge d(b^2 - 4d) \notin K^2 \iff \alpha\beta \notin K(\alpha^2)$.

Beweis. Die kubische Resolvente von $p(x)$ ist

$$\begin{aligned} r(x) &= x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) \\ &= x^3 - bx^2 + (0 \cdot 0 - 4d)x - (0^2 \cdot d - 4bd + 0^2) \\ &= x^3 - bx^2 - 4dx + 4bd \\ &= (x - b)(x^2 - 4d) \\ &= (x - b)\left(x - 2\sqrt{d}\right)\left(x + 2\sqrt{d}\right). \end{aligned}$$

Nach dem Klassifikationssatz 13, Fall (iii)-(v) ist die Galoisgruppe von $h(x)$ isomorph zu $\mathrm{V}_4, \mathrm{C}_4$ oder D_4. Ebenso folgt aus dem Klassifikationssatz 13, dass genau dann $\mathrm{Gal}(F/K) \cong \mathrm{V}_4$, wenn die kubische Resolvente $r(x)$ über K zerfällt.
Wenn $r(x)$ über K zerfällt, ist also $\sqrt{d} = \alpha\beta \in K$ und damit auch $d = \alpha^2\beta^2 \in K^2$ und Bedingung i ist gezeigt.
Angenommen, es ist $\sqrt{d} \notin K$, dann hat $r(x)$ genau eine Nullstelle, nämlich $t_1 = b$ in K, und wir befinden uns im Fall (iv) oder (v) des Klassifikationssatzes 13.

Das Hilfspolynom $g(x)$, welches zu $p(x)$ gehört, lautet

$$\begin{aligned} g(x) &= (x^2 - tx + d)(x^2 + ax + (b - t)) \\ &= (x^2 - bx + d)(x^2 + 0 \cdot x + (b - b)) \\ &= (x^2 - bx + d)x^2 \\ &= \left(x - \frac{1}{2}(b + \sqrt{b^2 - 4d})\right)\left(x - \frac{1}{2}(b - \sqrt{b^2 - 4d})\right)x^2. \end{aligned}$$

Die nichtnegativen Nullstellen von $g(x)$ lauten $-\alpha^2 = \frac{1}{2}\big(b+\sqrt{b^2 - 4d}\big)$ und
$-\beta^2 = \frac{1}{2}\big(b - \sqrt{b^2 - 4d}\big)$, denn aus dem Beweis des Satzes 13 folgt, dass $\alpha_1\alpha_2 = -\alpha\alpha = -\alpha^2$ und $\beta_1\beta_2 = -\beta\beta = -\beta^2$ auch Nullstellen von $p(x)$ sind. Da nun $p(x)$ irreduzibel ist, sind diese Nullstellen nicht in K. Nach Satz 13 gilt $\mathrm{Gal}(F/K) \cong \mathrm{C}_4$ genau dann, falls $g(x)$ in $E = \mathbb{Q}(\sqrt{d})$ zerfällt. Diese Aussage ist äquivalent dazu, dass $K\big(\sqrt{b^2 - 4d}\big) = K\big(\sqrt{d}\big)$ oder $K(\alpha^2) = K(\alpha\beta)$ ist. Zwei quadratische Körpererweiterungen sind genau dann gleich, falls das Produkt ihrer Diskriminanten ein Quadrat im Körper ist. Die Diskriminante von $\sqrt{b^2 - 4d}$ ist $4(b^2 - 4d)$ und die Diskriminante von $\sqrt{d}$ ist $4d$. Somit ist die letzte Bedingung äquivalent dazu, dass

$$4(b^2 - 4d) \cdot 4d \in K^2 \iff 4^2 \cdot d(b^2 - 4d) \in K^2 \iff d(b^2 - 4d) \in K^2$$

gilt. Daraus folgt Bedingung ii, Bedingung iii folgt durch wechselseitigen Ausschluss. □

Bemerkung 10.
Die Bedingungen $d \in K^2$ und $d(b^2 - 4d) \in K^2$ schließen sich für irreduzible Polynome aus. Dies folgt aus Satz 14 Teil (iii).

Wir zeigen, dass die Bedingung $d \in K^2$ für die Isomorphie zur Kleinschen Vierergruppe im Falle der biquadratischen Polynome zur Bedingung $D \in K^2$ aus Bemerkung 7 äquivalent ist.

Bemerkung 11.
Für biquadratische Polynome gilt nämlich

$$d \in K^2 \Longleftrightarrow D = -4b^3A + b^2B^2 + 18bBA - 4B^3 - 27A^2 \in K^2$$
$$\text{mit } A = -4bd, B = -4d.$$

Beweis. Es gilt

$$\begin{aligned}
D &= -4b^3A + b^2B^2 + 18bBA - 4B^3 - 27A^2 \\
&= -4b^3(-4bd) + b^2(-4d)^2 + 18b(-4d)(-4bd) - 4(-4d)^3 - 27(-4bd)^2 \\
&= 16b^4d + 16b^2d^2 + 18 \cdot 16b^2d^2 + 16^2d^3 - 27 \cdot 16b^2d^2 \\
&= 4^2 \cdot (b^4 - 8b^2d + 16d^2) \cdot d \\
&= \underbrace{4^2}_{\in K^2} \cdot \underbrace{(b^2 - 4d)^2}_{\in K^2} \cdot d.
\end{aligned}$$

□

2 Flussdiagramm im Fall $p(x) = x^4 + bx^2 + d$

In Abbildung 3.1 ist ein Flussdiagramm zur Illustration des Korollars über die Galoisgruppen von biquadratischen Polynomen dargestellt.

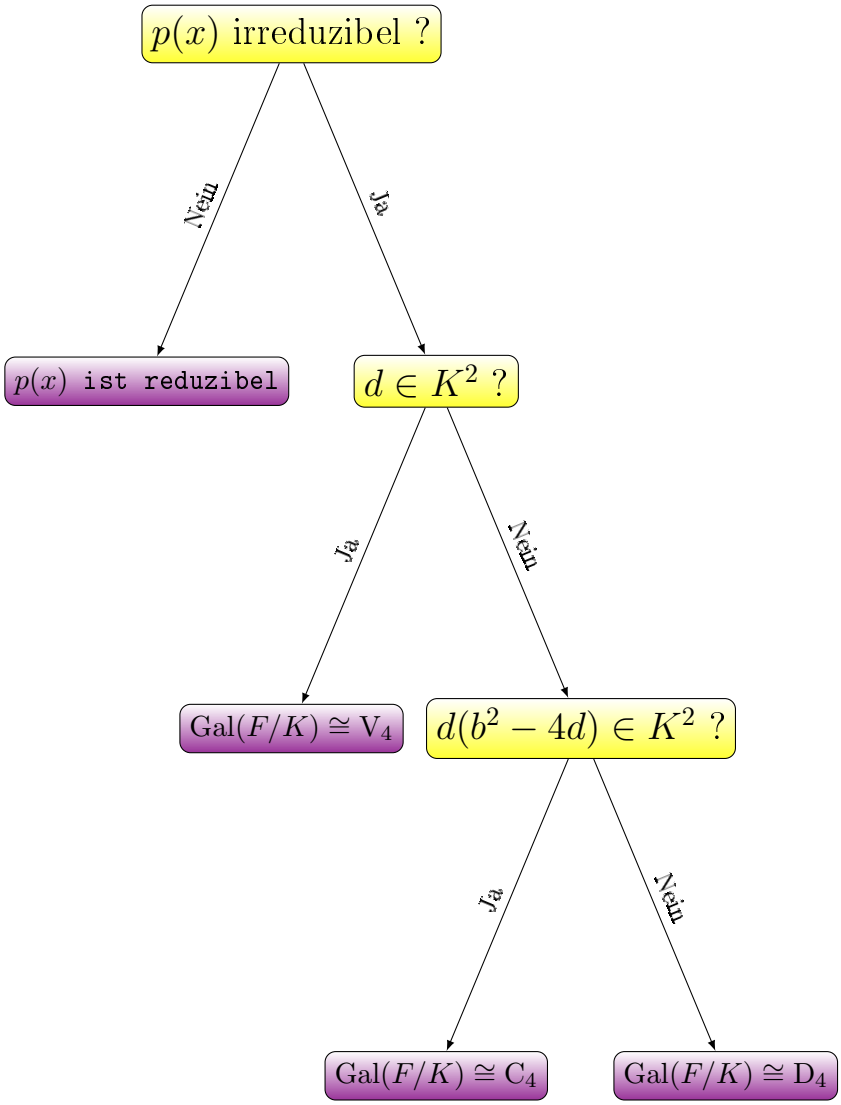


Abbildung 3.1: Klassifizierung von biquadratischen Polynomen
Quelle: Eigene Grafik erstellt mit TikZ

3 Beispiele mit $p(x) = x^4 + bx^2 + d$

Es folgen zu jedem der drei Fälle des Korollars 1 drei Beispiele. Beim zweiten Beispiel des jeweiligen Falles handelt es sich um ein Polynom, dessen Galoisgruppe bereits bestimmt wurde. Anhand dieser Beispiele kann sich der Leser vom Nutzen des Korollars 1 für Galoisgruppen von biquadratischen Polynomen überzeugen. Im Vergleich zum Verfahren des Klassifikationssatzes 13 erleichtert es die Rechnungen erheblich. Die Galoisgruppen werden also erneut untersucht, dieses Mal allerdings mit Hilfe des Irreduziblitätskriteriums für biquadratische Polynome 14 und des Korollars 1 für biquadratische Polynome. Beim dritten Beispiel des jeweiligen Falles handelt es sich um allgemeine Beispiele. Bei allen Beispielen sei $K = \mathbb{Q}$ der Grundkörper für die nachfolgenden Polynome.

3.1 Korollar 1, Fall (i) Galoisgruppe V_4

Beispiel 20.
Untersuchung der Galoisgruppe von $p_{19}(x) = x^4 + x^2 + 9$.

Es ist $b = 1$ und $d = 9$. Es ist

$$\begin{aligned} b^2 - 4d &= 1^2 - 4 \cdot 9 = -35 \notin \mathbb{Q}^2 && \wedge \\ -b + 2\sqrt{d} &= -1 + 2\sqrt{9} = 5 \notin \mathbb{Q}^2 && \wedge \\ -b - 2\sqrt{d} &= -1 - 2\sqrt{9} = -7 \notin \mathbb{Q}^2. \end{aligned}$$

Nach Satz 14, Teil (i) ist $p_{19}(x)$ irreduzibel.
Es ist

$$d = 9 = 3^2 \in \mathbb{Q}^2$$

und damit ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{V}_4$ nach Korollar 1, Fall (i).

Beispiel 21.
Betrachten wir nun erneut das Polynom $p_8(x) = x^4 + 6x^2 + 4$ aus Beispiel 10 und untersuchen von diesem die Galoisgruppe mit Hilfe des Irreduziblitätskriterium 14 und des Korollars 1 für biquadratische Polynome.

Es ist $b = 6$ und $d = 4$ und es gilt

$$\begin{aligned} b^2 - 4d &= 6^2 - 4 \cdot 4 = 20 \notin \mathbb{Q}^2 && \wedge \\ -b + 2\sqrt{d} &= -6 + 2\sqrt{4} = -2 \notin \mathbb{Q}^2 && \wedge \\ -b - 2\sqrt{d} &= -6 - 2\sqrt{4} = -10 \notin \mathbb{Q}^2, \end{aligned}$$

daher ist $p_8(x)$ nach Satz 14, Teil (i) irreduzibel.
Es ist

$$d = 4 = 2^2 \in \mathbb{Q}^2$$

und damit ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{V}_4$ nach Korollar 1, Fall (i).

Beispiel 22. [8, S. 136]
Seien k und j unterschiedliche quadratfreie ganze Zahlen und seien $r \in \mathbb{Q} \setminus \{0\}$ sowie $s \in \mathbb{Q}$. Untersuchung der Galoisgruppe von

$$p_{20}(x) = x^4 - 2(r^2k + s^2j)x^2 + (r^2k - s^2j)^2.$$

Es ist $b = -2(r^2k+s^2j)$ und $d = (r^2k-s^2j)^2$ und $p_{20}(x)$ ist irreduzibel über $\mathbb{Q}$, denn es ist

$$\begin{aligned} b^2 - 4d &= (-2(r^2k + s^2j))^2 - 4(r^2k - s^2j)^2 \\ &= 4r^4k^2 + 8r^2ks^2j + 4s^4j^2 - 4r^4k^2 \\ &\quad - 4r^4k^2 + 8r^2ks^2j - 4s^4j^2 \\ &= 16r^2s^2kj \notin \mathbb{Q}^2 && \wedge \\ -b + 2\sqrt{d} &= -(-2(r^2k + s^2j)) + 2\sqrt{(r^2k - s^2j)^2} \\ &= 2r^2k + 2s^2j + 2r^2k - 2s^2j \\ &= 4r^2k \notin \mathbb{Q}^2 && \wedge \\ -b - 2\sqrt{d} &= -(-2(r^2k + s^2j)) - 2\sqrt{(r^2k - s^2j)^2} \\ &= 2r^2k + 2s^2j - 2r^2k + 2s^2j \\ &= 4s^2j \notin \mathbb{Q}^2. \end{aligned}$$

Nach Korollar 1, Fall (i) folgt, dass $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{V}_4$, da

$$d = (r^2k - s^2j)^2 \in \mathbb{Q}^2.$$

3.2 Korollar 1, Fall (ii) Galoisgruppe C_4

Beispiel 23.
Untersuchung der Galoisgruppe von $p_{21}(x) = x^4 + 5x^2 + 5$.

Es ist $b = 5$ und $d = 5$ und es folgt

$$\begin{aligned} b^2 - 4d &= 5^2 - 4 \cdot 5 = 5 \notin \mathbb{Q}^2 && \wedge \\ -b + 2\sqrt{d} &= -5 + 2\sqrt{5} \notin \mathbb{Q}^2 && \wedge \\ -b - 2\sqrt{d} &= -5 - 2\sqrt{5} \notin \mathbb{Q}^2. \end{aligned}$$

Also ist $p_{21}(x)$ nach Satz 14, Teil (i) irreduzibel über $\mathbb{Q}$.
Es ist $d = 5 \notin \mathbb{Q}^2$ und es gilt

$$d(b^2 - 4d) = 5(5^2 - 4 \cdot 5) = 5^2 \in \mathbb{Q}^2.$$

Damit ist $\mathrm{Gal}(F/\mathbb{Q}) \cong C_4$ nach Korollar 1, Fall (ii).

Beispiel 24.
Betrachten wir nun erneut das Polynom $p_{11}(x) = x^4 + 4x^2 + 2$ aus Beispiel 13 und untersuchen von diesem die Galoisgruppe mit Hilfe des Irreduziblitätskriterium 14 und des Korollars 1 für biquadratische Polynome.

Es ist $b = 4$ und $d = 2$ und es folgt

$$\begin{aligned} b^2 - 4d &= 4^2 - 4 \cdot 2 = 8 \notin \mathbb{Q}^2 && \wedge \\ -b + 2\sqrt{d} &= -4 + 2\sqrt{2} \notin \mathbb{Q}^2 && \wedge \\ -b - 2\sqrt{d} &= -4 - 2\sqrt{2} \notin \mathbb{Q}^2. \end{aligned}$$

Also ist $p_{11}(x)$ nach Satz 14, Teil (i) irreduzibel über $\mathbb{Q}$.
Es ist $d = 2 \notin \mathbb{Q}^2$ und es gilt

$$d(b^2 - 4d) = 2(4^2 - 4 \cdot 2) = 4^2 \in \mathbb{Q}^2.$$

Damit ist $\mathrm{Gal}(F/\mathbb{Q}) \cong C_4$ nach Korollar 1, Fall (ii).

Beispiel 25. [8, S. 136-137]
Seien $m \in \mathbb{Z}$ und $n \in \mathbb{Z}$ mit $m^2 + n^2 \notin \mathbb{Q}^2$. Wir untersuchen die

Galoisgruppe von

$$p_{22}(x) = x^4 - 2(m^2+n^2)x^2 + n^2(m^2+n^2).$$

Es ist $b = -2(m^2+n^2)$ und $d = n^2(m^2+n^2)$. Das Polynom $p_{22}(x)$ ist nach Satz 14 Teil (i) irreduzibel über $\mathbb{Q}$, da

$$\begin{aligned}
b^2 - 4d &= (-2(m^2+n^2))^2 - 4(n^2(m^2+n^2)) \\
&= 4m^4 + 8m^2n^2 + 4n^4 - 4m^2n^2 - 4n^4 \\
&= 4m^4 + 4m^2n^2 \\
&= 4m^2(m^2+n^2) \notin \mathbb{Q}^2 && \wedge \\
-b + 2\sqrt{d} &= -(-2(m^2+n^2)) + 2\sqrt{n^2(m^2+n^2)} \\
&= 2(m^2+n^2) + 2n\sqrt{m^2+n^2} \notin \mathbb{Q}^2 && \wedge \\
-b - 2\sqrt{d} &= -(-2(m^2+n^2)) - 2\sqrt{n^2(m^2+n^2)} \\
&= 2(m^2+n^2) - 2n\sqrt{m^2+n^2} \notin \mathbb{Q}^2.
\end{aligned}$$

Es ist $d = n^2(m^2+n^2) \notin \mathbb{Q}^2$, da $m^2+n^2 \notin \mathbb{Q}^2$ ist.
Nach Voraussetzung und nach Korollar 1 Fall (ii) ist $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{C}_4$, da

$$\begin{aligned}
d(b^2-4d) &= n^2(m^2+n^2)((-2(m^2+n^2))^2 - 4n^2(m^2+n^2)) \\
&= n^2(m^2+n^2)(4m^4 + 8m^2n^2 + 4n^4 - 4n^2m^2 - 4n^4) \\
&= \left(2nm(m^2+n^2)\right)^2 \in \mathbb{Q}^2.
\end{aligned}$$

3.3 Korollar 1, Fall (iii) Galoisgruppe D_4

Beispiel 26.
Untersuchung der Galoisgruppe von $p_{23}(x) = x^4 - x^2 - 3$.

Es ist $b = -1$ und $d = -3$ und es folgt

$$\begin{aligned}
b^2 - 4d &= (-1)^2 - 4\cdot(-3) = 13 \notin \mathbb{Q}^2 && \wedge \\
-b + 2\sqrt{d} &= -(-1) + 2\sqrt{-3} = 1 + 2\sqrt{-3} \notin \mathbb{Q}^2 && \wedge \\
-b - 2\sqrt{d} &= -(-1) - 2\sqrt{-3} = 1 - 2\sqrt{-3} \notin \mathbb{Q}^2.
\end{aligned}$$

Also ist $p_{23}(x)$ nach Satz 14, Teil (i) irreduzibel über $\mathbb{Q}$. Es gilt

$$\begin{aligned} d &= -3 \notin \mathbb{Q}^2 && \wedge \\ d(b^2 - 4d) &= (-3)((-1)^2 - 4 \cdot (-3)) = -39 \notin \mathbb{Q}^2. \end{aligned}$$

Aus Korollar 1, Teil (iii) folgt, dass $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{D}_4$.

Beispiel 27.
Betrachten wir nun erneut das Polynom $p_{14}(x) = x^4 + 2x^2 + 2$ aus Beispiel 16 und untersuchen von diesem die Galoisgruppe mit Hilfe des Irreduziblitätskriterium 14 und des Korollars 1 für biquadratische Polynome.

Es ist $b = 2$ und $d = 2$ und es folgt

$$\begin{aligned} b^2 - 4d &= 2^2 - 4 \cdot 2 = -4 \notin \mathbb{Q}^2 && \wedge \\ -b + 2\sqrt{d} &= -2 + 2\sqrt{2} \notin \mathbb{Q}^2 && \wedge \\ -b - 2\sqrt{d} &= -2 - 2\sqrt{2} \notin \mathbb{Q}^2. \end{aligned}$$

Also ist $p_{14}(x)$ nach Satz 14, Teil (i) irreduzibel über $\mathbb{Q}$.
Es gilt

$$\begin{aligned} d &= 2 \notin \mathbb{Q}^2 && \wedge \\ d(b^2 - 4d) &= 2(2^2 - 4 \cdot 2) = -8 \notin \mathbb{Q}^2. \end{aligned}$$

Aus Korollar 1, Teil (iii) folgt, dass $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{D}_4$.

Beispiel 28. [8, S. 137]
Seien p und q verschiedene ungerade Primzahlen. Wir untersuchen die Galoisgruppe von

$$p_{24}(x) = x^4 - px^2 + q.$$

Es ist $b = -p$ und $d = q$. Wir zeigen die Irreduzibilität von $p_{24}(x)$ über $\mathbb{Q}$. Es ist

$$\begin{aligned} b^2 - 4d &= (-p)^2 - 4q = p^2 - 4q && \wedge \\ -b + 2\sqrt{d} &= -(-p) + 2\sqrt{q} \notin \mathbb{Q}^2 && \wedge \end{aligned}$$

$$-b - 2\sqrt{d} = -(-p) - 2\sqrt{q} \notin \mathbb{Q}^2.$$

Also ist $p_{24}(x)$ genau dann irreduzibel über $\mathbb{Q}$, wenn $p^2 - 4q \notin \mathbb{Q}^2$ ist. Hier werden zwei Beweise dafür angegeben, weshalb $p^2 - 4q$ kein Quadrat in $\mathbb{Q}$ ist.[2]

(i) Wir können annehmen, dass $p^2 - 4q > 0$, da negative Zahlen keine Quadratzahlen sein können. Angenommen es gäbe ein $t \in \mathbb{N}$ mit $p^2 - 4q = t^2$, dann ist t ungerade und jeder Faktor von $4q = (p+t)(p-t)$ ist gerade. Da q eine Primzahl ist und $0 < p - t < p + t$, muss gelten, dass $p - t = 2$ und $p + t = 2q$. Hieraus folgt, $p = q + 1$. Das steht im Widerspruch zur Annahme, dass p und q beide ungerade sind.

(ii) Wegen $2 \nmid p, q$ gibt es $k, \ell \in \mathbb{Z}$ mit $p = 2k + 1$ und $q = 2\ell + 1$. Es ist dann

$$\begin{aligned} p^2 - 4q &= (2k+1)^2 - 4(2\ell+1) \\ &= 4k^2 + 4k + 1 - 8\ell - 4 \\ &\equiv 4(k^2 + k) + 5 \mod 8 \\ &= 4(\overbrace{k(k+1)}^{\text{gerade}}) + 5 \equiv 5 \mod 8. \end{aligned}$$

Wiederum ist $p^2 - 4q$ ungerade. Für beliebige ungerade Zahlen $2k + 1$ mit $k \in \mathbb{Z}$ gilt

$$(2k+1)^2 = 4k^2 + 4k + 1 \equiv 1 \mod 8.$$

Somit kann $p^2 - 4q \equiv 5 \mod 8$ kein Quadrat in $\mathbb{Q}$ sein.

Aus Korollar 1, Teil (iii) folgt, dass $\mathrm{Gal}(F/\mathbb{Q}) \cong D_4$, da

$$\begin{aligned} d = q &\notin \mathbb{Q}^2 \qquad \wedge \\ d(b^2 - 4d) = q(p^2 - 4q) &\notin \mathbb{Q}^2. \end{aligned}$$

[2] Der Beweis im Fall i ist angelehnt an den Artikel von Kappe und Warren [8, S. 137], der zweite Beweis im Fall ii wurde selbst verfasst.

4 Implementierungen in SAGE

Der Klassifikationssatz für Galoisgruppen (siehe Satz 13) von Polynomen vierten Grades und dessen Korollar 1 für biquadratische Polynome beschreiben Verfahren, um die Galoisgruppe anhand der Koeffizienten zu bestimmen. Es bietet sich an, dies in ein Computeralgebrasystem zu implementieren. Dafür wurde SAGE verwendet. SAGE bietet die Vorteile, frei und benutzerfreundlich zu sein [13, S. 5]. Es ist dabei hauptsächlich in Python implementiert und auch die in SAGE verwendete Kommandosprache ist im Wesentlichen Python und sollte nicht ausschließlich für Informatiker gut lesbar sein. Ein Hauptvorteil des Computeralgebrasystems SAGE ist, dass es viele mathematische Funktionen besitzt, die bei Berechnungen hilfreich sind [13, S. 91-92].
Es wird ein Programm `classify` geschrieben, welches für ein Polynom dessen Galoisgruppe klassifiziert. Mit diesem Programm lassen sich dann alle Polynome mit einer speziellen Galoisgruppe für Koeffizienten aus einem vorgegebenen ganzzahligen Bereich angeben. Dies kann bei der Erstellung von Übungsaufgaben hilfreich sein und war bei der Suche nach Beispielen eine enorme Hilfe. Es kam die Frage auf, wie häufig die unterschiedlichen Gruppen vorkommen. Um dies zu untersuchen, wurden die absoluten und relativen Häufigkeiten der Galoisgruppen im vorgegebenen ganzzahligen Koeffizientenbereich berechnet.

1 Polynome vierten Grades

Nachfolgend wird die Klassifikation von Galoisgruppen von Polynomen vierten Grades in SAGE implementiert.

1. Grundlegende Definitionen
Wir rechnen im Polynomring über $\mathbb{Z}$ der von der Unbestimmten x erzeugt wird.

```
R = ZZ['x']
x = R.gen()
```

2. Anzahl der Faktoren der Faktorisierung von $g(x) \in \mathbb{Z}[x]$
Zur Berechnung wird die Faktorisierung (z.B. $(x-3)^2 * (x^2+x+2)$) in ein „Dictionary“ umgewandelt (hier dann $\{x-3:2, x^2+x+2:1\}$) und die rechten Seiten (die "Values") werden aufsummiert.

```
def factor_anz(g):
  return sum(dict(g.factor()).values())
```

3. Implementierung des Satzes 13
Für die Irreduzibilitätsuntersuchung greifen wir auf den in SAGE bereits vorhandenen Befehl zu.

```
def classify(a,b,c,d):
    f=x^4 + a*x^3 + b*x^2 +c*x+d
    if (not f.is_irreducible()):
      return("Red")
    A=a^2*d+c^2-4*b*d
    B=a*c-4*d
    D=-4*b^3*A+b^2*B^2+18*b*A*B-4*B^3-27*A^2
    r=x^3-b*x^2+(a*c-4*d)*x-(a^2*d-4*b*d+c^2)
    rfak=factor_anz(r)
    if(rfak==3):
      return("V4")
    if(rfak==1):
      return("A4" if is_square(D) else "S4") # r irreduzibel
    # Ab hier zerfällt r in einen linearen und einenquadratischen Faktor.
    rfac=r.factor()
    (lin,quad) = rfac[0][0],rfac[1][0]
    t=-lin.constant_coefficient()   # Rationale Nst. von r.
    # Durch den quadratischen Faktor erzeugter Zahlenkörper
    Nf.<s>=NumberField(quad)
    # Polynomring über dem Zerfällungskörper
    K.<X>=Nf[]
    g=(X^2-t*X+d)*(X^2+a*X+b-t)
    if(factor_anz(g)==4):
      return("C4")
    else:
      return("D4")
    return("err")
    # Hier sollten alle Fälle abgehandelt sein!
```

Zum Beispiel gibt der Aufruf `classify(1,1,1,1)` mit den Koeffizienten des fünften Kreisteilungspolynoms (siehe Beispiel 12), den String „C4“, also die Galoisgruppe C_4, zurück.

4. Ausgabe aller Polynome vierten Grades mit festgelegter Galoisgruppe im vorgegebenen Koeffizientenbereich
Mit der Funktion `classify` lassen sich auch alle Polynome mit einer vorgegebenen Galoisgruppe in einem vorgegebenen ganzzahligen Zahlenbereich auflisten.

```
timer=cputime(subprocesses=True)
In=range(-2,3)
for (a,b,c,d) in cartesian_product_iterator([In,In,In,
                                             In]):
  kl=classify(a,b,c,d)
  if(kl=="C4"):
    print(a,b,c,d),cputime(timer)
```

Beispielsweise gibt obige Eingabe alle Polynome mit Galoisgruppe C_4, deren Koeffizienten $a, b, c, d \in \{-2, -1, 0, 1, 2\}$ liegen, an.

2 Statistik für Polynome vierten Grades

Auch wenn zu jedem der fünf Fälle des Klassifikationssatzes 13 hier jeweils drei Beispiele präsentiert wurden, soll dies dem Leser nicht suggerieren, dass alle fünf Fälle gleichermaßen häufig auftreten. Der Fall $\mathrm{Gal}(F/K) \cong \mathrm{S}_4$, also Fall (i) aus dem Klassifikationssatz 13, ist der gewöhnliche Fall. Um dies zu illustrieren, werden alle Polynome mit ganzzahligen Koeffizienten in vorgegebenen Bereichen betrachtet und das Vorkommen unterschiedlicher Galoisgruppen gezählt. Dazu wird folgendes Programm geschrieben:

5. Statistikprogramm zur Bestimmung der absoluten und relativen Häufigkeiten der Galoisgruppen von Polynomen vierten Grades

```
timer=cputime(subprocesses=True)
In=range(-10,11)
Stat=dict({"err":0,"A4":0,"C4":0,"D4":0,"S4":0,"V4":0,
           "Red":0})
Anz=0
for (a,b,c,d) in cartesian_product_iterator([In,In,In,
                                             In]):
  Anz+=1
  kl=classify(a,b,c,d)
  Stat[kl]=Stat[kl]+1
Anz,[[i,Stat[i],(Stat[i]/Anz).n()]
     for i in Stat.keys()],cputime(timer)
```

Die obige Eingabe gibt die absoluten und relativen Häufigkeiten der Galoisgruppen für alle Polynome, deren Koeffizienten $a, b, c, d \in \{-10, -9, -8, \ldots, 8, 9, 10\}$ liegen, an.
Die entstehende Ausgabe wurde in Tabelle 4.1 zusammengefasst. Der Zahlenbereich wurde nicht noch weiter vergrößert, da dies zu rechenintensiv ist.
Mit Vergrößerung des zulässigen Zahlenbereiches steigt die relative Häufigkeit, dass die Galoisgruppe eines beliebig gewählten Polynoms die Galoisgruppe S_4 ist, an. Tatsächlich bewies Van der Waerden in den Artikeln „Die Seltenheit der Gleichungen mit Affekt.“ [14, S. 13-16] und „Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt.“ [15, S. 133-147], dass „der Bruchteil der Gleichungen, deren Galoissche Gruppe die symmetrische ist, mit wachsendem Koeffizientenbereich gegen Eins strebt.“ [15, S. S.133] Mit Affekt bedeutet hierbei, dass die Galoisgruppe nicht die S_4 ist.

Galoisgruppe	S_4	A_4	V_4	C_4	D_4	reduzibel
Bereich	**von 0 bis 1**					
absolute Häufigkeit	4	0	1	1	0	10
relative Häufigkeit	25	0	6.25	6.25	0	62.5
Bereich	**von -1 bis 1**					
absolute Häufigkeit	20	0	2	2	10	47
relative Häufigkeit	24.69	0	2.47	2.47	12.35	58.02
Bereich	**von -2 bis 2**					
absolute Häufigkeit	274	2	6	2	70	271
relative Häufigkeit	43.84	0.32	0.96	0.32	11.20	43.36
Bereich	**von -5 bis 5**					
absolute Häufigkeit	10382	16	46	28	774	3395
relative Häufigkeit	70.91	0.11	0.31	0.19	5.29	23.19
Bereich	**von -10 bis 10**					
absolute Häufigkeit	163588	182	218	108	5118	25267
relative Häufigkeit	84.12	0.09	0.11	0.06	2.63	12.99
Bereich	**von -12 bis 12**					
absolute Häufigkeit	338466	276	326	156	8378	43023
relative Häufigkeit	86.66	0.07	0.08	0.04	2.14	11.01
Bereich	**von -20 bis 20**					
absolute Häufigkeit	2601346	962	994	406	31296	190757
relative Häufigkeit	92.06	0.03	0.04	0.01	1.11	6.75

Tabelle 4.1: Statistik für Polynome vierten Grades

3 Biquadratische Polynome

Wir passen das Programm naiv für biquadratische Polynome an.

6. Naive Anpassung der Funktion `classify` für biquadratische Polynome

```
def classifybi(b,d):
  f=x^4 + b*x^2 +d
  if (not f.is_irreducible()):
    return("Red")
  if is_square(d):
    return("V4")
  if is_square(d*(b^2-4*d)):
    return("C4")
  else:
    return("D4")
  return("err")
```

Obige Implementierung verwendet für die Irreduzibilitätsuntersuchung weiterhin den in
SAGE bereits vorhandenen Befehl. Wenn wir statt `is_irreducible()` den Irreduzibilitätstest für biquadratische Polynome verwenden, lässt sich die Rechenzeit erheblich, und zwar um mehr als die Hälfte, verkürzen. Dies setzen wir im Folgenden um.

7. Irreduzibilitätstest für biquadratische Polynome

```
def bq_is_irreduzible(b,d):
  if is_square(b^2-4*d):
    return(false)
  if is_square(d):
    return(true)
  wD=sqrt(d)
  if is_square(-b+2*wD):
    return(false)
  if is_square(-b-2*wD):
    return(false)
  return(true)
```

8. Programm für biquadratische Polynome

```
def classifybi(b,d):
  if (not bq_is_irreduzible(b,d)):
    return("Red")
  if is_square(d):
    return("V4")
  if is_square(d*(b^2-4*d)):
    return("C4")
  else:
    return("D4")
  return("err")
```

Beispielsweise gibt der Aufruf für die Eingabe `classifybi(1,9)` den String „V4“ zurück, der für die Galoisgruppe V_4 steht.
Wie bereits im allgemeinen Fall kann es auch für biquadratische Polynome von Interesse sein, beispielsweise um Übungsaufgaben zu erstellen, Polynome mit einer vorgegebenen Galoisgruppe in einem vorgegebenen ganzzahligen Zahlenbereich zu finden. Durch den Geschwindigkeitsvorteil können wir größere Koeffizientenbereiche nach interessanten Beispielen absuchen.

9. Ausgabe aller biquadratischen Polynome mit bestimmter Galoisgruppe im vorgegebenen Koeffizientenbereich

```
timer=cputime(subprocesses=True)
In=range(-2,3)
for (b,d) in cartesian_product_iterator([In,In]):
    kl=classifybi(b,d)
    if(kl=="D4"):
      print(b,d),cputime(timer)
```

Obige Eingabe gibt alle Polynome mit Galoisgruppe D_4 mit Koeffizienten $b, d \in \{-2, -1, 0, 1, 2\}$ an.

4 Statistik für biquadratische Polynome

Wie bereits im allgemeinen Fall werden auch im Fall der biquadratischen Polynomen die absoluten und relativen Häufigkeiten der Galoisgruppen untersucht. Dies realisieren wir in SAGE wie folgt.

10. Statistikprogramm zur Bestimmung der absoluten und relativen Häufigkeiten von Galoisgruppen biquadratischer Polynome

```
timer=cputime(subprocesses=True)
In=range(-50,51)
Stat=dict({"err":0,"C4":0,"D4":0,"V4":0,"Red":0})
Anz=0
for (b,d) in cartesian_product_iterator([In,In]):
  Anz+=1
  kl=classifybi(b,d)
  Stat[kl]=Stat[kl]+1
Anz,[[i,Stat[i],(Stat[i]/Anz).n()]
      for i in Stat.keys()],cputime(timer)
```

Das Programm für biquadratische Polynome `classifybi` ist wesentlich schneller als das Programm `classify` für allgemeine Polynome vierten Grades. Dementsprechend können viel größere Koeffizientenbereiche zur Bestimmung der relativen und absoluten Häufigkeiten der Galoisgruppen untersucht werden. In Tabelle 4.2 sind absolute und relative Häufigkeiten der Galoisgruppen von biquadratischen Polynomen in den vorgegebenen ganzzahligen Zahlenbereichen, die mit der obigen Eingabe berechnet wurden, dargestellt. In Tabelle 4.2 ist zu sehen, dass der Fall der biquadratischen Polynomen $\mathrm{Gal}(F/K) \cong \mathrm{D}_4$ am häufigsten auftritt. Die zyklische Gruppe C_4 scheint wie auch schon im allgemeinen Fall am seltensten vorzukommen. Wir können zeigen, dass bei Vergrößerung der Koeffizientenbereiche die relative Häufigkeit des Vorkommens der Galoisgruppe C_4 gegen Null geht, denn aus Korollar 1 wissen wir,

$$\mathrm{Gal}(F/K) \cong \mathrm{C}_4 \Longleftrightarrow d \in K^2.$$

Die Anzahl der Quadratzahlen in $\{-n, -n+1, \ldots, n-1, n\}$ ist

$\lfloor\sqrt{n}\rfloor+1$, weil negative Zahlen keine Quadratzahlen sein können. Die relative Häufigkeit, nennen wir sie h, der Quadratzahlen innerhalb der Menge $\{-n, -n+1, \ldots, n-1, n\}$ der Galoisgruppe C_4 wird dann beschrieben durch

$$h = \frac{\lfloor\sqrt{n}\rfloor + 1}{2n+1}.$$

Somit ergibt sich

$$\lim_{n\to\infty} \frac{\lfloor\sqrt{n}\rfloor + 1}{2n+1} = 0.$$

Galoisgruppe	$\mathbf{V_4}$	$\mathbf{C_4}$	$\mathbf{D_4}$	**reduzibel**
Bereich	**von -50 bis 50**			
absolute Häufigkeit	597	40	8968	596
relative Häufigkeit	5.85	0.39	87.91	5.85
Bereich	**von -100 bis 100**			
absolute Häufigkeit	1790	84	37190	1337
relative Häufigkeit	4.43	0.21	92.05	3.31
Bereich	**von -200 bis 200**			
absolute Häufigkeit	5181	146	152524	2950
relative Häufigkeit	3.22	0.09	94.85	1.84
Bereich	**von -1000 bis 1000**			
absolute Häufigkeit	59940	582	3925494	17985
relative Häufigkeit	1.50	0.01	98.04	0.45
Bereich	**von -2000 bis 2000**			
absolute Häufigkeit	171888	1016	15796302	38795
relative Häufigkeit	1.07	0.01	98.68	0.24
Bereich	**von -5000 bis 5000**			
absolute Häufigkeit	689738	2150	99221774	106339
relative Häufigkeit	0.69	0.00	99.20	0.11
Bereich	**von -10000 bis 10000**			
absolute Häufigkeit	1979389	3582	397830176	226854
relative Häufigkeit	0.49	0.00	99.45	0.06

Tabelle 4.2: Statistik für biquadratische Polynome

5 Anhang

Einsetzen von t_1 in die kubische Resolvente (s. Fußnote 2):

$$
\begin{aligned}
r(t_1) = r(\alpha_1\alpha_2 + \alpha_3\alpha_4) &= (\alpha_1\alpha_2 + \alpha_3\alpha_4)^3 - (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 \\
&\quad + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4) \cdot (\alpha_1\alpha_2 + \alpha_3\alpha_4)^2 + ((\alpha_1 + \alpha_2 + \alpha_3 \\
&\quad + \alpha_4)(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4) - 4\alpha_1\alpha_2\alpha_3\alpha_4) \\
&\quad \cdot (\alpha_1\alpha_2 + \alpha_3\alpha_4) - ((\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^2(\alpha_1\alpha_2\alpha_3\alpha_4) \\
&\quad - 4(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4)(\alpha_1\alpha_2\alpha_3\alpha_4) \\
&\quad + (\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4)^2) \\
&= \alpha_1^3\alpha_2^3 + 3\alpha_1^2\alpha_2^2\alpha_3\alpha_4 + 3\alpha_1\alpha_2\alpha_3^2\alpha_4^2 + \alpha_3^3\alpha_4^3 - \alpha_1^3\alpha_2^3 - \alpha_1^3\alpha_2^2\alpha_3 \\
&\quad - \alpha_1^2\alpha_2^3\alpha_3 - \alpha_1^3\alpha_2^2\alpha_4 - \alpha_1^2\alpha_2^3\alpha_4 - 3\alpha_1^2\alpha_2^2\alpha_3\alpha_4 - 2\alpha_1^2\alpha_2\alpha_3^2\alpha_4 \\
&\quad - 2\alpha_1\alpha_2^2\alpha_3^2\alpha_4 - 2\alpha_1^2\alpha_2\alpha_3\alpha_4^2 - 2\alpha_1\alpha_2^2\alpha_3\alpha_4^2 - 3\alpha_1\alpha_2\alpha_3^2\alpha_4^2 \\
&\quad - \alpha_1\alpha_3^3\alpha_4^2 - -\alpha_2\alpha_3^3\alpha_4^2 - \alpha_1\alpha_3^2\alpha_4^3 - \alpha_2\alpha_3^2\alpha_4^3 - \alpha_3^3\alpha_4^3 + \alpha_1^3\alpha_2^2\alpha_3 \\
&\quad + \alpha_1^2\alpha_2^3\alpha_3 + \alpha_1^2\alpha_2^2\alpha_3^2 + \alpha_1^3\alpha_2^2\alpha_4 + \alpha_1^2\alpha_2^3\alpha_4 + \alpha_1^3\alpha_2\alpha_3\alpha_4 \\
&\quad + \alpha_1\alpha_2^3\alpha_3\alpha_4 + 2\alpha_1^2\alpha_2\alpha_3^2\alpha_4 + 2\alpha_1\alpha_2^2\alpha_3^2\alpha_4 + \alpha_1\alpha_2\alpha_3^3\alpha_4 \\
&\quad + \alpha_1^2\alpha_2^2\alpha_4^2 + 2\alpha_1^2\alpha_2\alpha_3\alpha_4^2 + 2\alpha_1\alpha_2^2\alpha_3\alpha_4^2 + \alpha_1^2\alpha_3^2\alpha_4^2 + \alpha_2^2\alpha_3^2\alpha_4^2 \\
&\quad + \alpha_1\alpha_3^3\alpha_4^2 + \alpha_2\alpha_3^3\alpha_4^2 + \alpha_1\alpha_2\alpha_3\alpha_4^3 + \alpha_1\alpha_3^2\alpha_4^3 + \alpha_2\alpha_3^2\alpha_4^3 \\
&\quad - \alpha_1^3\alpha_2\alpha_3\alpha_4 - \alpha_1\alpha_2^3\alpha_3\alpha_4 - \alpha_1\alpha_2\alpha_3^3\alpha_4 - \alpha_1\alpha_2\alpha_3\alpha_4^3 \\
&\quad - 2\alpha_1^2\alpha_2^2\alpha_3\alpha_4 - 2\alpha_1^2\alpha_2\alpha_3^2\alpha_4 - 2\alpha_1^2\alpha_2\alpha_3\alpha_4^2 - 2\alpha_1\alpha_2^2\alpha_3^2\alpha_4 \\
&\quad - 2\alpha_1\alpha_2^2\alpha_3\alpha_4^2 - 2\alpha_1\alpha_2\alpha_3^2\alpha_4^2 + 4\alpha_1^2\alpha_2^2\alpha_3\alpha_4 + 4\alpha_1^2\alpha_2\alpha_3^2\alpha_4 \\
&\quad + 4\alpha_1\alpha_2^2\alpha_3^2\alpha_4 + 4\alpha_1^2\alpha_2\alpha_3\alpha_4^2 + 4\alpha_1\alpha_2^2\alpha_3\alpha_4^2 + 4\alpha_1\alpha_2\alpha_3^2\alpha_4^2 \\
&\quad - \alpha_1^2\alpha_2^2\alpha_3^2 - 2\alpha_1^2\alpha_2^2\alpha_3\alpha_4 - 2\alpha_1^2\alpha_2\alpha_3^2\alpha_4 - 2\alpha_1\alpha_2^2\alpha_3^2\alpha_4 \\
&\quad - \alpha_1^2\alpha_2^2\alpha_4^2 - 2\alpha_1^2\alpha_2\alpha_3\alpha_4^2 - 2\alpha_1\alpha_2^2\alpha_3\alpha_4^2 - \alpha_1^2\alpha_3^2\alpha_4^2 \\
&\quad - 2\alpha_1\alpha_2\alpha_3^2\alpha_4^2 - \alpha_2^2\alpha_3^2\alpha_4^2 = 0.
\end{aligned}
$$

Literaturverzeichnis

[1] Artin, Michael: Algebra. 1. Auflage, Birkhäuser, 1998.

[2] Artin, Emil: Galoissche Theorie. 3. unveränderte Auflage, Harri Deutsch Thun, 1998.

[3] Artin, Emil: Algebra with Galois Theory. Courant Institute of Mathematical Sciences, New York University, 2012.

[4] Bosch, Siegfried: Algebra. 8., korrigierte Auflage, Springer Spektrum, 2013.

[5] Fischer, Gerd: Lehrbuch der Algebra. 4. wesentlich überarbeitete und erweiterte Auflage, Springer Spektrum, 2017.

[6] Fischer, Gerd & Sacher, Reinhard: Einführung in die Algebra. 2. überarbeitete Auflage., B. G. Teubner, Stuttgart, 1983.

[7] Jacobson, Nathan: Basic Algebra I. W. H. Freeman and Company, 1974.

[8] Kappe, Luise-Charlotte & Warren, Bette: An Elementary Test for the Galois Group of a Quartic Polynomial. The American Mathematical Monthly, 1989, Volume 96, Issue 2, pp. 133-137, `www.jstor.org/stable/2323198` letzter Zugriff: 07.06.2019.

[9] Karpfinger, Christian & Meyberg, Kurt: Algebra. 4. Auflage, Springer Spektrum, 2017.

[10] Karpfinger, Christian & Meyberg, Kurt: Algebra Lösungen. 4. Auflage, Springer Spektrum, 2017. www.springer.com/de/book/9783662547212 letzter Zugriff: 30.07.2019.

[11] Kersten, Ina: Algebra. 1. Auflage, Universitätsdrucke Göttingen, 2006.

[12] O'Connor J. J. & Robertson, E. F.: Evariste Galois. Universität Sankt Andrews, 1996 http://mathshistory.st-andrews.ac.uk/Biographies/Galois.html letzter Zugriff: 07.06.2019.

[13] The Sage Group: Sage Tutorial Release 8.8. http://doc.sagemath.org/pdf/de/tutorial/SageTutorial-de.pdf letzter Zugriff 27.06.2019.

[14] Waerden, Bartel Leendert: Die Seltenheit der Gleichungen mit Affekt. Mathematische Annalen, 1934, Band 109, S. 13-16.

[15] Waerden, Bartel Leendert: Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt. Monatshefte für Mathematik und Physik, Dezember 1936, Band 43, Heft 1, S. 133-147.

Index

algebraische Körpererweiterung, 24
algebraisches Element, 24
alternierende Gruppe, 14
Automorphismengruppe Aut(K), 27

Beispiele Galoisgruppe A_4, 57
Beispiele Galoisgruppe C_4, 65, 71, 86
Beispiele Galoisgruppe D_4, 69, 71, 87
Beispiele Galoisgruppe S_4, 53, 71
Beispiele Galoisgruppe V_4, 61, 84
Beispiele zum Irreduzibilitätskriterium für biquadratische Polynome, 78

Charakteristik eines Ringes, 24

Diedergruppe, 14
Diskriminante eines Polynoms, 33, 36

Eisensteinkriterium, 52
elementarsymmetrische Funktion, 31
Elemente der S_4, 12
endlich erzeugte Körpererweiterung, 24
endliche Körpererweiterung, 25

Flussdiagramm Galoisgruppen von biquadratischen Polynomen, 82, 83
Flussdiagramm Galoisgruppen von Polynomen vierten Grades, 50
Fundamental-Lemma, 28

Galoisgruppe, 27
Galoisgruppen von biquadratischen Polynomen, 80
galoissche Körpererweiterung, 27
Gaußkriterium, 51
Grad einer Körpererweiterung, 25
Gradformel, 25
Grafik Alle Untergruppen der S_4, 23
Grafik Untergruppen der S_4 bis auf Isomorphie, 22
Gruppe der relativen Automorphismen, 27

Häufigkeiten der Galoisgruppen von Polynomen vierten

Grades, 96
Häufigkeiten von Galoisgruppen biquadratischer Polynome, 100
Hauptsatz der Galoistheorie, 29

Implementierung des Irreduzibilitätstestes für biquadratische Polynome, 97
Irreduzibilitätskriterium für biquadratische Polynome, 75
Irreduzibilitätssatz, 51

Körpererweiterung, 24
Klassifikationssatz der Galoisgruppen von Polynomen vierten Grades, 39
Kleinsche Vierergruppe, 16
kubische Resolvente, 33, 34, 36

Minimalpolynom, 26

normale Körpererweiterung, 27
Normalteiler, 13
Normalteiler als Kerne von Gruppenhomomorphismen, 13
Nullstellen der kubischen Resolvente, 33
Nullstellenkriterium, 51

Operation, 20

primitives Polynom, 51
Programm Ausgabe aller biquadratischen Polynomen mit festgelegter Galoisgruppe im vorgegebenen Koeffizientenbereich, 98
Programm Ausgabe von Polynomen vierten Grades mit festgelegter Galoisgruppe im vorgegebenen Koeffizientenbereich, 94
Programm Galoisgruppen von biquadratischen Polynomen, 98
Programm Galoisgruppen von Polynomen vierten Grades, 92

Rechenregel Signum einer Permutation, 13
Reduktionskriterium, 52

Satz Bestimmung aller Untergruppen der S_4, 17
Satz von Cauchy, 16
Satz von Sylow, 17
separables Polynom, 26
Signum einer Permutation, 13
Statistikprogramm zur Bestimmung der Häufigkeiten der Galoisgruppen von biquadratischen Polynomen, 99

Statistikprogramm zur Bestimmung der Häufigkeiten der Galoisgruppen von Polynomen vierten Grades, 94
Substitutionskriterium, 52
Sylowgruppe, 16
symmetrische Gruppe, 11
Symmetrische Gruppe S_4, 12

transitive Operation, 20
transitive Untergruppe von S_n, 20

Untergruppen der S_4, 15

Zerfällungskörper, 26
zyklische Gruppe, 14

Die Galoistheorie genießt als Abschluss vieler Algebravorlesungen den Ruf, nur Experten zugänglich zu sein. Dieses Buch wendet sich an alle, die schon lange das Wesen der Galoistheorie begreifen wollten, aber vor der Komplexität in anderen Büchern zurückgeschreckt sind. Im Zentrum steht ein konkreter Satz über die Galoisgruppen von Polynomen vierten Grades und ein Korollar für biquadratische Polynome. Bei der Arbeit mit diesen Aussagen, deren Beweise ausführlich dargestellt und die mit Beispielen illustriert werden, lernt der/die Lesende viele Grundbegriffe und Methoden der Galoistheorie kennen. Auf sehr konkretem Niveau werden die nötigen Grundlagen zur Gruppentheorie sowie die benötigten Begriffe dieser eingeführt. Bewusst wird auf die volle Allgemeinheit zugunsten der Anschaulichkeit verzichtet. Abschließend werden die gefundenen Algorithmen realisiert, indem sie in Programmen implementiert und damit elementare Untersuchungen durchgeführt werden.

GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

ISBN: 978-3-86395-440-6

Universitätsdrucke Göttingen