Konstruktive Galoistheorie für Polynome kleinen Grades über $\mathbb{Q}$

September 16, 2013

von

Manuel Erdorf

zur Erlangung des Grades

des Bachelor of Science

angefertigt

am Lehrstuhl von Prof. Dr. Gekeler

Hiermit bestätige ich, dass ich die Bachelorarbeit selbstständig und nur mit Hilfe der angegebenen Hilfsmittel geschrieben habe.

Vorwort

Vor über 180 Jahren hat Evariste Galois, ein junger frazösischer Mathematiker, jedem Polynom $f(X)$ über einem Körper K, das ausschließlich einfache Nullstellen besitzt, eine endliche Gruppe G zugeordnet.
Wenn n der Grad von $f(X)$, α_1, α_2, ..., α_n die Nullstellen von $f(X)$, $L := K(\alpha_1, ..., \alpha_n)$ der Zerfällungskörper von $f(X)$ über K und

$$R := \{g(X_1, ..., X_n) \in K[X_1, ..., X_n] \mid g(\alpha_1, ..., \alpha_n) = 0\}$$

die Menge der K- rationalen Relationen zwischen den Nullstellen ist, dann bildet

$$Gal(f) := \left\{\sigma \in S_n \mid g\left(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(n)}\right) = 0,\ g(X_1, ..., X_n) \in R\right\}$$

eine Untergruppe der symmetrischen Gruppe S_n.
$Gal(f)$ wird als Galoisgruppe des Polynoms $f(X)$ bezeichnet. Diese Gruppe hängt von der Nummerierung der Nullstellen ab.
Des Weiteren ist

$$Gal(f) \cong Gal(L \mid K),$$

die Gruppe der K-Automorphismen des Körpers L.
Die Galoisgruppe enthält viele Informationen über die Struktur der Körpererweiterung $L \mid K$. Zum Beispiel ist die Ordnung der Galoisgruppe gleich dem Grad der Körpererweiterung $L \mid K$.

Ich möchte in dieser Arbeit Methoden angeben mit denen man die Galoisgruppe eines irreduziblen Polynoms bis zum Grad 5 über dem Körper der rationalen Zahlen explizit berechnen kann. Des Weiteren werden zusätzlich für jede transitive Untergruppe der symmetrischen Gruppe eine Familie von Polynomen angegeben, die diese als Galoisgruppe besitzt.

Im ersten Kapitel werden die grundlegenden Begriffe und Sätze der Galoistheorie angegeben.

Das nachfolgende Kapitel beschäftigt sich mit irreduzible Polynome dritten Grades. In diesem kurzen Kapitel soll man ein Gefühl für die Vorgehensweise zur Bestimmung der Galoisgruppe bekommen.

In Kapitel 3 werden irreduzible Polynome vierten Grades betrachtet. Hier wird deutlich, dass die Bestimmung der Galoisgruppe schon wesentlich schwieriger ist als bei Polynome dritten Grades. Um die Galoisgruppe bestimmen zu können, wird hierzu der Begriff der kubischen Resolvente eingeführt.

Im 4. Kapitel geht es um irreduzible Polynome fünften Grades. Zuerst muss man sich überlegen, welche Gruppen als Galoisgruppe in Frage kommen. Danach wird eine Methode angegeben, wie man die Galoisgruppe eines irreduziblen Polynoms fünften Grades bestimmt. Dabei tritt ein Problem auf. Mit dieser Methode lässt sich nicht zwischen der Diedergruppe mit 10 Elementen und der zyklischen Gruppe mit 5 Elementen unterscheiden.
Um zumindest mit großer Sicherheit sagen zu können, dass die Galoisgruppe die zyklische Gruppe ist, verwendet man den Satz von Cebotarev und den χ^2- Anpassungstest.

Inhaltsverzeichnis

1 Grundlagen

In diesem Kapitel möchte ich die wichtigsten Begriffe und Sätze der Galoistheorie angeben. Da ich diese Sätze und Begrifflichkeiten voraussetze, werden die Sätze größtenteils ohne Beweis wiedergegeben. Zuerst möchte ich die grundlegenden Bezeichnungen einführen, die in der gesamten Arbeit gelten.
Es bezeichne

- $\mathbb{N} = \{0,1,2,...\}$ die Menge der natürlichen Zahlen;
- $\mathbb{Z} = \{...,-2,-1,0,1,2,...\}$ die Menge der ganzen Zahlen;
- $\mathbb{Q} = \{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$ die Menge der rationalen Zahlen;
- $\mathbb{P} = \{2,3,5,...\}$ die Menge der Primzahlen;
- $\mathbb{F}_p = \{0, 1, ..., p-1\}$ der endliche Körper mit p Elementen, wobei $p \in \mathbb{P}$;
- $(\mathbb{Q}^*)^2 = \left\{a^2 \mid a \in \mathbb{Q}, a \neq 0\right\}$ die Menge der Quadrate in $\mathbb{Q}$.

Da wir uns in dieser Arbeit nur mit Polynomen über $\mathbb{Q}$ beschäftigen, werden alle Sätze und Definitionen nur im Fall des rationalen Körpers $\mathbb{Q}$ angegeben.

1.1 Definition:

Es sei $f \in \mathbb{Q}[X]$ ein nichtkonstantes Polynom. Das Polynom f heißt separabel, falls f keine mehrfachen Nullstellen besitzt.

1.2 Satz:

Sei $f \in \mathbb{Q}[X]$ irreduzibel vom Grad n$\geq$1. Dann ist f separabel.

1.3 Definition:

Eine algebraische Körpererweiterung $L \mid \mathbb{Q}$ heißt galoissch, wenn sie normal und separabel ist. In diesem Fall heißt die Gruppe

$$Gal(L \mid \mathbb{Q}) = Aut(L \mid \mathbb{Q}) = \{\sigma : L \longrightarrow L \mid \ \sigma \mid_{\mathbb{Q}} = id\}$$

die Galois-Gruppe von $L \mid \mathbb{Q}$.
Setzen wir voraus, dass L als Teilkörper von $\overline{\mathbb{Q}}$, dem algebraischen Abschluss von $\mathbb{Q}$, gegeben ist, so ist

$$Gal(L \mid \mathbb{Q}) = \{\ \sigma\colon\ L \longrightarrow \mathbb{Q} \mid \sigma \text{ ist } \mathbb{Q}\text{–Einbettung }\}.$$

1.4 Satz: (Hauptsatz der Galois-Theorie)

Es ist $L \mid \mathbb{Q}$ eine endliche galoissche Körpererweiterung und $G = Gal(L \mid \mathbb{Q})$. Dann ist $\#G = [L : \mathbb{Q}]$ und

$$\left\{ M \mid \begin{array}{c} M \text{ ist Zwischenkörper} \\ \text{von } L \mid \mathbb{Q} \end{array} \right\} = \mathcal{M} \underset{\psi}{\overset{\phi}{\underset{\longrightarrow}{\longleftarrow}}} \mathcal{H} = \left\{ H \mid \begin{array}{c} H \text{ ist} \\ \text{Untergruppe von } G \end{array} \right\}$$

$$M \longmapsto H = Gal(L \mid M)$$

$$M = L^H \longleftarrow H$$

sind inverse ordnungsvertauschende Bijektionen.
Ein $M \in \mathcal{M}$ ist galoissch über $\mathbb{Q}$ genau dann, wenn $H = Gal(L \mid M)$ normal ist in G. In diesem Fall ist

$$\begin{array}{c} G \longrightarrow Gal(M \mid \mathbb{Q}) \\ \sigma \longmapsto \sigma \mid_M \end{array}$$

surjektiv mit Kern H, das heißt

$$G/H \xrightarrow{\cong} Gal(M \mid \mathbb{Q}).$$

1.5 Definition:

Eine endliche Körpererweiterung $L \mid \mathbb{Q}$ heißt auflösbar, falls $L \mid \mathbb{Q}$ galoissch ist mit auflösbarer Galoisgruppe $Gal(L \mid \mathbb{Q})$.

1.6 Definition:

Für ein separables Polynom $f(X) \in \mathbb{Q}[X]$ sei $Gal(f)$ die Galoisgruppe von L über $\mathbb{Q}$, wobei L der Zerfällungskörper von f ist, also

$$Gal(f) = Gal(L \mid \mathbb{Q}).$$

1.7 Bemerkung:

Sei $\{\alpha_i \mid 1 \leq i \leq n\}$ die Menge der Wurzeln von f in dem algebraischen Abschluss $\overline{\mathbb{Q}}$.
Die Galoisgruppe $G = Gal\,(f)$ permutiert die α_i, und damit operiert G, nach *Wahl der Nummerierung*, auf der Menge $\{1, 2, ..., n\}$ der Indizes.
Somit können wir G als Untergruppe der symmetrischen Gruppe $S_n = Sym\{1, 2, ..., n\}$ auffassen.

Durch das folgende Lemma wird das Kriterium angegeben, welche Galoisgruppen wir im späteren Verlauf der Arbeit betrachten werden.

1.8 Lemma:

Ist $f \in \mathbb{Q}[X]$ separabel und irreduzibel, so operiert $Gal(f)$ transitiv auf der Menge der Wurzeln $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ von f in $\mathbb{Q}$.

Da wir im Folgenden nur irreduzible Polynome über $\mathbb{Q}$ betrachten, sind für uns nur die transitiven Untergruppen von S_n relevant.

1.9 Erinnerung:

Eine Gruppe $H \in S_n$ heißt transitiv, wenn H auf $\{1, 2, ..., n\}$ transitiv operiert, das heißt es existiert nur eine Bahn $H\sigma$ mit $\sigma \in S_n$.

Nun möchte ich die Definition der Diskriminante angeben, die wir verwenden werden, da die Diskriminante in der Literatur nicht einheitlich definiert ist.

1.10 Definition:

Für ein normiertes Polynom$f(X) = \prod_{1 \leq i \leq n} (X - \alpha_i) \in \mathbb{Q}[X]$ mit $\alpha_i \in \overline{\mathbb{Q}}$ vom Grad n sei

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

die Diskriminante von f.

1.11 Bemerkung:

(i) Die Diskriminante $D(f)$ liegt in $\mathbb{Q}$ und ist eine Invariante von f, das heißt $D(f)$ ist unabhängig von der Nummerierung der α_i.

(ii) Wie oben erwähnt definieren einige Autoren die Diskriminante anders. Sie definieren sie wie folgt: $D^*(f) = \prod_{1 \leq i \neq j \leq n} (\alpha_i - \alpha_j)$.

Dann ist

$$D^*(f) = (-1)^{\frac{n(n-1)}{2}} D(f).$$

(iii) Für $f(X) = X^2 + aX + b \in \mathbb{Q}[X]$ gilt: $D(f) = a^2 - 4b$. (Das heißt unsere Definition ist "die richtige").

1.12 Satz:

Sei $f(X) \in \mathbb{Q}[X]$ und schreibe

$$f(X) = a_0X^n + a_1X^{n-1} + ... + a_n \ (a_0 = 1)$$

$$f`(X) = b_0X^{n-1} + b_1X^{n-2} + ... + b_{n-1} \ (b_0 = n) \ .$$

Es bezeichne $det(M)$ die Determinante von M.
Dann ist

$$D(f) = (-1)^{\frac{n(n-1)}{2}} det(M) \text{ mit } M \in \mathbb{Q}^{(2n-1)\times(2n-1)}, \text{ wobei}$$

$$M = \begin{pmatrix}
a_0 & ... & ... & ... & a_n & 0 & & & 0 \\
0 & a_0 & & & a_{n-1} & a_n & 0 & & \\
\vdots & & & & & & & & \\
\vdots & & & & & & & & 0 \\
0 & ... & & & a_2 & a_3 & ... & ... & ... & a_n \\
b_0 & b_1 & & b_{n-1} & 0 & ... & ... & ... & ... & 0 \\
0 & b_0 & b_1 & & b_{n-1} & 0 & & & & \vdots \\
\vdots & & & & & & & & & \vdots \\
\vdots & & & & & & & & & 0 \\
0 & ... & 0 & b_0 & b_1 & b_2 & ... & ... & ... & b_{n-1}
\end{pmatrix}.$$

Da wir in den folgenden Kapiteln von einigen Polynomen die Diskriminante berechnen werden, gebe ich an dieser Stelle für allgemeine Polynome mit bestimmter Form die Formeln für diese Diskriminanten an.

1.13 Korollar:

Sei $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$. Dann ist

$$D(f) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

Beweis:

Nach Satz 1.12 gilt: $D(f) = (-1)^{\frac{n(n-1)}{2}} det(M) = (-1)\, det(M)$.
Die Ableitung von $f(X)$ ist gegeben durch $f'(X) = 3X^2 + 2aX + b$.
Es gilt:

$$
\begin{aligned}
det(M) &= det\begin{pmatrix} 1 & a & b & c & 0 \\ 0 & 1 & a & b & c \\ 3 & 2a & b & 0 & 0 \\ 0 & 3 & 2a & b & 0 \\ 0 & 0 & 3 & 2a & b \end{pmatrix} \\
&= det\begin{pmatrix} 1 & a & b & c & 0 \\ 0 & 1 & a & b & c \\ 0 & -a & -2b & -3c & 0 \\ 0 & 3 & 2a & b & 0 \\ 0 & 0 & 3 & 2a & b \end{pmatrix} \\
&= det\begin{pmatrix} 1 & a & b & c & 0 \\ 0 & 1 & a & b & c \\ 0 & 0 & -2b+a^2 & -3c+ab & ac \\ 0 & 0 & -a & -2b & -3c \\ 0 & 0 & 3 & 2a & b \end{pmatrix} \\
&= det\begin{pmatrix} -2b+a^2 & -3c+ab & ac \\ -a & -2b & -3c \\ 3 & 2a & b \end{pmatrix} \\
&= (-2b+a^2)(-2b)b + (-3c+ab)(-3c)3 + ac(-a)2a \\
&\quad -3(-2b)ac - 2a(-3c)(-2b+a^2) - b(-a)(-3c+ab) \\
&= 4b^3 - 2a^2b^2 + 27c^2 - 9abc - 2a^3c + 6abc - 12abc \\
&\quad +6a^3c - 3abc + a^2b^2 \\
&= -a^2b^2 + 4b^3 + 4a^3c + 27c^2 - 18abc.
\end{aligned}
$$

Also ist die Diskriminante gegeben durch:

$$D(f) = (-1)\, det(M) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

□

1.14 Korollar:

Es sei $f(X) = X^4 + aX^2 + bX + c \in \mathbb{Q}[X]$. Dann ist

$$D(f) = 16a^4c - 4a^3b^3 - 128a^2c^2 + 144ab^2c + 256c^3 - 27b^4.$$

Beweis:

Die Ableitung von $f(X)$ ist gegeben durch $f'(X) = 4X^3 + 2aX + b$.
Es gilt:

$$det(M) = det \begin{pmatrix} 1 & 0 & a & b & c & 0 & 0 \\ 0 & 1 & 0 & a & b & c & 0 \\ 0 & 0 & 1 & 0 & a & b & c \\ 4 & 0 & 2a & b & 0 & 0 & 0 \\ 0 & 4 & 0 & 2a & b & 0 & 0 \\ 0 & 0 & 4 & 0 & 2a & b & 0 \\ 0 & 0 & 0 & 4 & 0 & 2a & b \end{pmatrix}$$

$$= det \begin{pmatrix} 1 & 0 & a & b & c & 0 & 0 \\ 0 & 1 & 0 & a & b & c & 0 \\ 0 & 0 & 1 & 0 & a & b & c \\ 0 & 0 & -2a & -3b & -4c & 0 & 0 \\ 0 & 0 & 0 & -2a & -3b & -4c & 0 \\ 0 & 0 & 4 & 0 & 2a & b & 0 \\ 0 & 0 & 0 & 4 & 0 & 2a & b \end{pmatrix}$$

$$= det \begin{pmatrix} 1 & 0 & a & b & c & 0 & 0 \\ 0 & 1 & 0 & a & b & c & 0 \\ 0 & 0 & 1 & 0 & a & b & c \\ 0 & 0 & 0 & -3b & 2a^2 - 4c & 2ab & 2ac \\ 0 & 0 & 0 & -2a & -3b & -4c & 0 \\ 0 & 0 & 0 & 0 & -2a & -3b & -4c \\ 0 & 0 & 0 & 4 & 0 & 2a & b \end{pmatrix}$$

$$= det \begin{pmatrix} -3b & 2a^2 - 4c & 2ab & 2ac \\ -2a & -3b & -4c & 0 \\ 0 & -2a & -3b & -4c \\ 4 & 0 & 2a & b \end{pmatrix}$$

$$= -3b \cdot det \begin{pmatrix} -3b & -4c & 0 \\ -2a & -3b & -4c \\ 0 & 2a & b \end{pmatrix} + 2a \cdot det \begin{pmatrix} 2a^2 - 4c & 2ab & 2ac \\ -2a & -3b & -4c \\ 0 & 2a & b \end{pmatrix}$$

$$-4 \cdot det \begin{pmatrix} 2a^2 - 4c & 2ab & 2ac \\ -3b & -4c & 0 \\ -2a & -3b & -4c \end{pmatrix}$$

$$
\begin{aligned}
&= -3b\left[9b^3 - 32abc\right] + 2a\left[-2a^2b^2 + 12b^2c + 8a^3c - 32ac^2\right] \\
&\qquad -4\left[16a^2c^2 - 64c^3 - 6ab^2c\right] \\
&= -27b^4 + 96ab^2c - 4a^3b^2 + 24ab^2c + 16a^4c - 64a^2c^2 \\
&\qquad -64a^2c^2 + 256c^3 + 24ab^2c \\
&= 16a^4c - 4a^3b^2 - 128a^2c^2 + 144ab^2c + 256c^3 - 27b^4.
\end{aligned}
$$

Nach Satz 1.12 gilt:

$$D(f) = (-1)^{\frac{4(4-1)}{2}} det(M) = det(M).$$

□

1.15 Korollar:

Sei $f(X) = X^5 + aX + b \in \mathbb{Q}[X]$. Dann gilt:

$$D(f) = 4^4a^5 + 5^5b^4 \ .$$

Beweis:

Nach Satz 1.12 gilt:

$$D(f) = (-1)^{\frac{5(5-1)}{2}} det(M) = det(M).$$

Die Ableitung von $f(X)$ ist gegeben durch $f'(X) = 5X^4 + a$.
Daraus folgt:

$$
det(M) = \begin{pmatrix}
1 & 0 & 0 & 0 & a & b & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & a & b & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & a & b & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & a & b \\
5 & 0 & 0 & 0 & a & 0 & 0 & 0 & 0 \\
0 & 5 & 0 & 0 & 0 & a & 0 & 0 & 0 \\
0 & 0 & 5 & 0 & 0 & 0 & a & 0 & 0 \\
0 & 0 & 0 & 5 & 0 & 0 & 0 & a & 0 \\
0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & a
\end{pmatrix}
$$

$$
= det \begin{pmatrix}
1 & 0 & 0 & 0 & a & b & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & a & b & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & a & b & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & a & b \\
0 & 0 & 0 & 0 & -4a & -5b & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -4a & -5b & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -4a & -5b & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -4a & -5b \\
0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & a
\end{pmatrix}
$$

$$= -4a \cdot det \begin{pmatrix} -4a & -5b & 0 & 0 \\ 0 & -4a & -5b & 0 \\ 0 & 0 & -4a & -5b \\ 0 & 0 & 0 & a \end{pmatrix} + 5 \cdot det \begin{pmatrix} -5b & 0 & 0 & 0 \\ -4a & -5b & 0 & 0 \\ 0 & -4a & -5b & 0 \\ 0 & 0 & -4a & -5b \end{pmatrix}$$

$$= -4a \left[-4a \cdot det \begin{pmatrix} -4a & -5b & 0 \\ 0 & -4a & -5b \\ 0 & 0 & a \end{pmatrix} \right]$$

$$+5 \left[-5b \cdot det \begin{pmatrix} -5b & 0 & 0 \\ -4a & -5b & 0 \\ 0 & -4a & -5b \end{pmatrix} + 4a \cdot det \begin{pmatrix} 0 & 0 & 0 \\ -4a & -5b & 0 \\ 0 & -4a & -5b \end{pmatrix} \right]$$

$$= -4a \left[-4a \left(-4a \right) \left(-4a \right) a \right] + 5 \left[-5b \left(-5b \right) \left(-5b \right) \left(-5b \right) \right]$$
$$= 4^4 a^5 + 5^5 b^4.$$

Somit gilt:

$$D(f) = 4^4 a^5 + 5^5 b^4.$$

□

Nun kommen wir zu einem wichtigen Satz, der ein sehr wichtiges Hilfsmittel ist, um die Galoisgruppe eines Polynoms zu bestimmen.

1.16 Satz: (Diskriminantenkriterium)

Sei $f(X) \in \mathbb{Q}[X]$ ein normiertes, separables Polynom vom Grad n .
Bezüglich einer Nummerierung $\alpha_1, \alpha_2, ..., \alpha_n$ der Nullstellen von f im algebraischen Abschluss $\overline{\mathbb{Q}}$ betrachten wir $Gal(f)$ als Untergruppe von S_n .
Es gilt:

$$Gal(f) \subset A_n \Leftrightarrow D(f) \text{ ist ein Quadrat in } \mathbb{Q}.$$

Ein weiteres wichtiges Instrument zur Bestimmung der Galoisgruppe eines Polynoms über $\mathbb{Q}$ ist der folgende Satz:

1.17 Satz:

Sei $f \in \mathbb{Z}[X]$ vom Grad n , irreduzibel über $\mathbb{Q}$, und $p \in \mathbb{P}$, wobei

(a) $p \nmid L(f)$[1], das heißt die Reduktion $\overline{f_p}(X) \in \mathbb{F}_p[X]$ hat Grad n ;

(b) $\overline{f_p}$ ist separabel.

Sei $\overline{f_p} = f_1 ... f_r$ die Primfaktorzerlegung von $\overline{f_p}$ in $\mathbb{F}_p[X]$, $deg(f_i) = n_i$
$(\rightsquigarrow \sum_{1 \leq i \leq r} n_i = n)$.
Dann enthält $Gal\,(f) \subset S_n$ eine Permutation vom Typ $(n_1, n_2, ..., n_r)$, das heißt $\sigma = \tau_1 \tau_2 .. \tau_r$, wobei τ_i $(1 \leq i \leq r)$ Zykel der Länge n_i sind.

Da wir nun in den folgenden Kapiteln immer entscheiden müssen, ob ein Polynom über $\mathbb{Q}$ irreduzibel ist, werde ich nun aus [Pillot] und [Lang] zwei Kriterien angeben, mit denen man die Irreduzibilität eines Polynoms über $\mathbb{Q}$ überprüfen kann.

1.18 Satz: (Lemma von Gauß)

Seien $f, g \in \mathbb{Q}[X]$ zwei normierte Polynome, und für ihr Produkt gelte $fg \in \mathbb{Z}[X]$.
Dann sind die Polynome $f, g \in \mathbb{Z}[X]$.

Daraus ergibt sich das folgende Lemma:

1.19 Lemma:

Ist $f \in \mathbb{Z}[X]$ und $p \in \mathbb{P}$, so dass die Reduktion $\overline{f} \in \mathbb{F}_p[X]$ von f modulo p den gleichen Grad hat wie f und irreduzibel ist, so ist f irreduzibel in $\mathbb{Q}[X]$.

1.20 Satz: (Eisensteinkriterium)

Sei $f(X) = \sum_{0 \leq i \leq n} a_i X^i \in \mathbb{Z}[X]$ ein Polynom von Grad n.
Sei $p \in \mathbb{Z}$ ein Primelement mit $p \nmid a_n$, $p \mid a_j$ für $0 \leq j \leq n-1$, $p^2 \nmid a_0$.
Dann ist f in $\mathbb{Q}[X]$ irreduzibel.

Nun werde ich noch ein Irreduzibilitätskriterium aus [KaWa] angeben, das speziell für Polynome der Form $f(X) = X^4 + bX^2 + d \in \mathbb{Q}[X]$ gilt.

[1] $L(f)$ ist der Leitkoeffizient von f

1.21 Satz:

Sei $f(X) = X^4 + bX^2 + d$ ein Polynom über $\mathbb{Q}$ und seien $\pm\alpha, \pm\beta$ die Wurzeln von $f(X)$.
Dann sind die folgenden Bedingungen äquivalent:

(i) $f(X)$ ist irreduzibel über $\mathbb{Q}$;

(ii) $\alpha^2, \alpha + \beta, \alpha - \beta \notin \mathbb{Q}$;

(iii) $b^2 - 4d, -b + 2\sqrt{d}, -b - 2\sqrt{d} \notin \mathbb{Q}^2$.

2 Polynome 3. Grades

Die einzigen möglichen Galoisgruppen eines irreduziblen Polynoms dritten Grades über $\mathbb{Q}$ sind S_3 und A_3 , wobei

- $S_3 = \{id, (12), (13), (23), (123), (132)\}$ die symmetrische Gruppe mit 6 Elementen, und
- $A_3 = \{id, (123), (132)\}$ die alternierende Gruppe ist.

Dies sind die einzigen Galoisgruppen, die in Betracht kommen, da nach Lemma 1.8 die Galoisgruppe $Gal(f)$ transitiv auf den Wurzeln von f operiert und es außer S_3 und A_3 keine weiteren transitiven Untergruppen von S_3 gibt.
Zur Bestimmung der Galoisgruppe eines irreduziblen Polynoms 3.Grades genügt das folgende Diskriminantenkriterium, das aus Satz 1.16 folgt.

2.1 Korollar:

Es sei $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ irreduzibel. Dann gilt

$$\begin{cases} Gal(f) = S_3 \text{ , falls } D(f) \text{ kein Quadrat in } \mathbb{Q} \text{ ist.} \\ Gal(f) = A_3 \text{ , falls } D(f) \text{ ein Quadrat in } \mathbb{Q} \text{ ist.} \end{cases}$$

Beweis:

Folgt direkt aus Satz 1.16.

□

Im Folgenden werden Familien von Polynome angegeben, die als Galoisgruppe S_3 bzw. A_3 besitzen.

2.2 Satz:

Sei $p \in \mathbb{P}$.
Die Polynome $f_p(X) \in \mathbb{Q}[X]$ mit

$$f_p(X) = X^3 + pX + p$$

besitzen als Galoisgruppe die symmetrische Gruppe S_3.

Beweis:

Nach dem Eisensteinkriterium ist $f_p(X)$ irreduzibel und somit auch separabel.
Des Weiteren gilt nach Korollar 1.13:

$$D(f_p) = -4p^3 - 27p^2 = -p^2 (4p + 27) .$$

Somit ist die Diskriminante $D(f_p)$ kein Quadrat in $\mathbb{Q}$.
Also folgt nach Satz 2.1, dass $Gal(f) = S_3$ ist.

□

2.3 Satz:

Sei $a = n^2 + n + 7$ mit $n \in \mathbb{Z}$.
Das Polynom

$$f(X) = X^3 - aX + a$$

hat die alternierende Gruppe A_3 als Galoisgruppe.

Beweis:

Da a ungerade ist, gilt:

$$X^3 - aX + a \equiv X^3 + X + 1\,(2)\,.$$

Das Polynom $X^3 + X + 1$ ist irreduzibel über $\mathbb{F}_2[X]$.
Somit ist nach dem Lemma von Gauß auch $f(X) = X^3 - aX + a$ über $\mathbb{Q}$ irreduzibel.
Nach Korollar 1.13 ist die Diskriminante $D(f)$ gegeben durch

$$\begin{array}{rcc} D(f) & = & -4\,(-a)^2 - 27a^2 \\ & = & a^2(4a - 27) \\ & \overset{(a=n^2+n+7)}{=} & (n^2+n+7)^2(4(n^2+n+7) - 27) \\ & = & (n^2+n+7)^2(4n^2+4n+1) \\ & = & (n^2+n+7)^2(2n+1)^2. \end{array}$$

Damit ist $D(f)$ ein Quadrat in $\mathbb{Q}$ und nach Satz 2.1 ist $Gal(f) = A_3$.

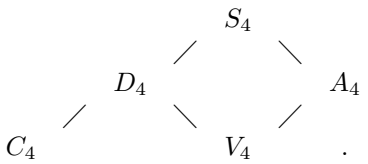
□

3 Polynome 4. Grades

In diesem Abschnitt muss man sich zuerst überlegen, welche Gruppen relevant sind.
Wir definieren für das gesamte Kapitel $\sigma := (1234)$ und $\tau := (12)(34)$.
Es bezeichne in diesem Kapitel

- $S_4 = < \sigma, (12) >$ die symmetrische Gruppe mit 24 Elementen;
- $A_4 = < (123), \tau >$ die alternierende Gruppe mit 12 Elementen;
- $D_4 = < \tau, (13) >$ die Diedergruppe mit 8 Elementen;
- $V_4 = < \tau, (13)(24) >$ die Kleinsche Vierergruppe;
- $C_4 = < \sigma >$ die zyklische Gruppe mit 4 Elementen.

Das Gruppendiagramm sieht wie folgt aus:



Wir betrachten im Folgenden ausschließlich irreduzible Polynome vierten Grades über $\mathbb{Q}$.
Nach Bemerkung 1.7 permutiert $Gal(f)$ die Nullstellen des Polynoms f.
Damit operiert $Gal(f)$, nach *Wahl der Nummerierung*, transitiv auf der Menge {1,2,3,4} der Indizes. Somit können wir $Gal(f)$ als transitive Untergruppe der symmetrischen Gruppe S_4 auffassen.

3.1 Satz:

Die transitiven Untergruppen von S_4 sind bis auf Konjugation die S_4, A_4, D_4, V_4 und C_4.

Beweis:

Die transitiven Untergruppen von S_4 besitzen alle eine Gruppenordnung, die durch 4 teilbar ist. Damit kommen die Gruppenordnungen 24, 12, 8 und 4 in Betracht.
Die Gruppe mit 24 Elementen ist die symmetrische Gruppe S_4 und die Gruppe mit Ordnung 12 ist die alternierende Gruppe A_4.
Nach den Sätzen von Sylow gibt es genau drei 2-Sylowuntergruppen der Ordnung 8 in S_4. Diese sind alle zueinander konjugiert. Also ist D_4, bis auf Konjugation, die einzige transitive Untergruppe mit 8 Elementen in S_4.
Zyklische Gruppen der Ordnung 4 sind alle zueinander konjugiert und werden

von einem 4er-Zykel erzeugt. Deshalb ist bis auf Konjugation C_4 die einzige zyklische Untergruppe mit 4 Elementen in S_4. Nichtzyklische, transitive Untergruppen mit der Ordnung 4 enthalten bis auf das
Einselement nur Elemente der Ordnung 2, der Form $(ab)(cd)$.
Somit sind diese Gruppen isomorph zu der kleinschen Vierergruppe V_4.

□

Anhand des Diagramms erkennt man nun, dass man nur mit Hilfe der Diskriminante nicht mehr entscheiden kann, welche Galoisgruppe ein irreduzibles Polynom vierten Grades besitzt.
Denn wenn die Diskriminante ein Quadrat in $\mathbb{Q}$ ist, dann ist die Galoisgruppe entweder A_4 oder V_4.
Andernfalls, das heißt die Diskriminante ist kein Quadrat in $\mathbb{Q}$, ist die Galoisgruppe S_4, D_4 oder C_4.
Um nun entscheiden zu können welche Galoisgruppe ein irreduzibles Polynom 4.Grades über $\mathbb{Q}$ besitzt, verwendet man die kubische Resolvente.

3.2 Definition:

Sei L der Zerfällungskörper eines Polynoms $f(X) = X^4 + aX^3 + bX^2 + cX + d$ über $\mathbb{Q}$. Desweiteren seien α_1, α_2, α_3 und α_4 die Nullstellen von f in L. Dann heißt das Polynom

$$g\,(Y) = [Y - (\alpha_1\alpha_2 + \alpha_3\alpha_4)]\,[Y - (\alpha_1\alpha_3 + \alpha_2\alpha_4)]\,[Y - (\alpha_1\alpha_4 + \alpha_2\alpha_3)]$$

die kubische Resolvente von $f(X)$.

3.3 Korollar:

Es sei $f(X) = X^4 + aX^3 + bX^2 + cX + d$ ein Polynom über $\mathbb{Q}$ und $g(Y)$ die kubische Resolvente von $f(X)$. Dann gilt:

$$g(Y) = Y^3 - bX^2 + (ac - 4d)Y - (a^2d + c^2 - 4bd).$$

Beweis:

Nach Voraussetzung gilt:

$$\begin{aligned} f(X) &= (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4) \\ &= (X^2-(\alpha_1+\alpha_2)X+\alpha_1\alpha_2)(X-\alpha_3)(X-\alpha_4) \\ &= (X^3-(\alpha_1+\alpha_2+\alpha_3)X^2+(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)X-\alpha_1\alpha_2\alpha_3) \\ &\quad (X-\alpha_4) \\ &= X^4-(\alpha_1+\alpha_2+\alpha_3+\alpha_4)X^3 \\ &\quad +(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4)X^2 \\ &\quad -(\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_3\alpha_4+\alpha_1\alpha_2\alpha_4+\alpha_2\alpha_3\alpha_4)X+\alpha_1\alpha_2\alpha_3\alpha_4 \\ &= X^4-s_1X^3+s_2X^2-s_3X+s_4, \end{aligned}$$

wobei s_1, s_2, s_3 und s_4 elementarsymmetrische Funktionen sind.
Man erkennt sofort, dass $g(Y)$ symmetrisch ist.
Somit lassen sich die Koeffizienten von $g(Y)$ durch elementarsymmetrische Funktionen darstellen. Also lassen sich die Koeffizienten von $g(Y)$ durch Koeffizienten von $f(X)$ ausdrücken.
Betrachte nun die kubische Resolvente und setze $g(Y)=Y^3+AY^2+BY+C$.
Es gilt:

$$\begin{aligned} g(Y) &= [Y-(\alpha_1\alpha_2+\alpha_3\alpha_4)]\,[Y-(\alpha_1\alpha_3+\alpha_2\alpha_4)]\,[Y-(\alpha_1\alpha_4+\alpha_2\alpha_3)] \\ &= [Y-(\alpha_1\alpha_2+\alpha_3\alpha_4+\alpha_1\alpha_3+\alpha_2\alpha_4)\,Y+(\alpha_1\alpha_2+\alpha_3\alpha_4)\,(\alpha_1\alpha_3+\alpha_2\alpha_4)] \\ &\quad [Y-(\alpha_1\alpha_4+\alpha_2\alpha_3)] \\ &= Y^3-(\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_1\alpha_2+\alpha_3\alpha_4+\alpha_1\alpha_3+\alpha_2\alpha_4)\,Y^2 \\ &\quad +[(\alpha_1\alpha_2+\alpha_3\alpha_4)(\alpha_1\alpha_4+\alpha_2\alpha_3)+(\alpha_1\alpha_3+\alpha_2\alpha_4)(\alpha_1\alpha_4+\alpha_2\alpha_3) \\ &\quad +(\alpha_1\alpha_2+\alpha_3\alpha_4)(\alpha_1\alpha_3+\alpha_2\alpha_4)]Y \\ &\quad -(\alpha_1\alpha_2+\alpha_3\alpha_4)\,(\alpha_1\alpha_3+\alpha_2\alpha_4)\,(\alpha_1\alpha_4+\alpha_2\alpha_3)\,. \end{aligned}$$

Durch Koeffizientenvergleich erhält man:

$$\begin{aligned} A &= -(\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_1\alpha_2+\alpha_3\alpha_4+\alpha_1\alpha_3+\alpha_2\alpha_4), \\ B &= (\alpha_1\alpha_2+\alpha_3\alpha_4)(\alpha_1\alpha_4+\alpha_2\alpha_3)+(\alpha_1\alpha_3+\alpha_2\alpha_4)(\alpha_1\alpha_4+\alpha_2\alpha_3) \\ &\quad +(\alpha_1\alpha_2+\alpha_3\alpha_4)(\alpha_1\alpha_3+\alpha_2\alpha_4), \\ C &= -(\alpha_1\alpha_2+\alpha_3\alpha_4)(\alpha_1\alpha_3+\alpha_2\alpha_4)(\alpha_1\alpha_4+\alpha_2\alpha_3). \end{aligned}$$

Man sieht sofort, dass $A=-s_2=-b$ ist.
Es bleiben somit noch B und C übrig. Es gilt:

$$
\begin{aligned}
B &= \alpha_1^2\alpha_2\alpha_4 + \alpha_1\alpha_2^2\alpha_3 + \alpha_1\alpha_3\alpha_4^2 + \alpha_2\alpha_3^2\alpha_4 \\
&\quad +\alpha_1^2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3^2 + \alpha_1\alpha_2\alpha_4^2 + \alpha_2^2\alpha_3\alpha_4 \\
&\quad +\alpha_1^2\alpha_2\alpha_3 + \alpha_1\alpha_2^2\alpha_4 + \alpha_1\alpha_3^2\alpha_4 + \alpha_2\alpha_3\alpha_4^2 \\
&= \alpha_1^2\alpha_2\alpha_4 + \alpha_1\alpha_2^2\alpha_3 + \alpha_1\alpha_3\alpha_4^2 + \alpha_2\alpha_3^2\alpha_4 + \alpha_1^2\alpha_3\alpha_4 \\
&\quad +\alpha_1\alpha_2\alpha_3^2 + \alpha_1\alpha_2\alpha_4^2 + \alpha_2^2\alpha_3\alpha_4 + \alpha_1^2\alpha_2\alpha_3 + \alpha_1\alpha_2^2\alpha_4 \\
&\quad \alpha_1\alpha_3^2\alpha_4 + \alpha_2\alpha_3\alpha_4^2 + 4\alpha_1\alpha_2\alpha_3\alpha_4 - 4\alpha_1\alpha_2\alpha_3\alpha_4 \\
&= (\alpha_1+\alpha_2+\alpha_3+\alpha_4)(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4) \\
&\quad -4\alpha_1\alpha_2\alpha_3\alpha_4 \\
&= s_1s_3 - 4s_4 \\
&= ac - 4d.
\end{aligned}
$$

Und für C gilt:

$$
\begin{aligned}
C &= -(\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)(\alpha_1\alpha_4 + \alpha_2\alpha_3) \\
&= -[\alpha_1^3\alpha_2\alpha_3\alpha_4 + \alpha_1^2\alpha_2^2\alpha_3^2\alpha_4 + \alpha_1\alpha_2\alpha_3^3\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_4^3 \\
&\quad +4\alpha_1^2\alpha_2^2\alpha_3\alpha_4 + 4\alpha_1^2\alpha_2\alpha_3^2\alpha_4 + 4\alpha_1^2\alpha_2\alpha_3\alpha_4^2 \\
&\quad +4\alpha_1\alpha_2^2\alpha_3^2\alpha_4 + 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 + \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 -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] \\
&= -[(\alpha_1^2 + 2\alpha_1\alpha_2 + 2\alpha_1\alpha_3 + 2\alpha_1\alpha_4 + \alpha_2^2 + 2\alpha_2\alpha_3 + 2\alpha_2\alpha_4 + \alpha_3^2 \\
&\quad +2\alpha_3\alpha_4 + \alpha_4^2)\alpha_1\alpha_2\alpha_3\alpha_4 + \alpha_1^2\alpha_2^2\alpha_3^2 + 2\alpha_1^2\alpha_2^2\alpha_3\alpha_4 \\
&\quad +2\alpha_1^2\alpha_2\alpha_3^2\alpha_4 + 2\alpha_1\alpha_2^2\alpha_3^2\alpha_4 + \alpha_1^2\alpha_2^2\alpha_4^2 + 2\alpha_1^2\alpha_2\alpha_3\alpha_4^2 \\
&\quad +2\alpha_1\alpha_2^2\alpha_3\alpha_4^2 + \alpha_1^2\alpha_3^2\alpha_4^2 + 2\alpha_1\alpha_2\alpha_3^2\alpha_4^2 + \alpha_2^2\alpha_3^2\alpha_4^2 \\
&\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] \\
&= -[(\alpha_1+\alpha_2+\alpha_3+\alpha_4)^2\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 \\
&\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] \\
&= -\left(s_1^2s_4 + s_3^2 - 4s_2s_4\right) \\
&= -\left(a^2d + c^2 - 4bd\right).
\end{aligned}
$$

Daraus folgt:

$$g(Y) = Y^3 - bY^2 + (ac-4d)Y - (a^2d + c^2 - 4bd).$$

□

3.4 Korollar:

Sei $f(X) = X^4 + aX^3 + bX^2 + cX + d$ ein Polynom über $\mathbb{Q}$ und sei $g(Y)$ die kubische Resolvente von $f(X)$.
Dann gilt:

$$D(g) = D(f).$$

Beweis:

Es seien t_1, t_2 und t_3 die Nullstellen von $g(Y)$. Es gilt:

$$\begin{aligned} D(g) &= \prod_{1\leq i\lneq j\leq 3}(t_i - t_j)^2 \\ &= \begin{matrix}[(\alpha_1\alpha_2+\alpha_3\alpha_4)-(\alpha_1\alpha_3+\alpha_2\alpha_4)]^2 \\ [(\alpha_1\alpha_2+\alpha_3\alpha_4)-(\alpha_1\alpha_4+\alpha_2\alpha_3)]^2 \\ [(\alpha_1\alpha_3+\alpha_2\alpha_4)-(\alpha_1\alpha_4+\alpha_2\alpha_3)]^2\end{matrix} \\ &= [(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)]^2[(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)]^2[(\alpha_1-\alpha_2)(\alpha_3-\alpha_4)]^2 \\ &= (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_1-\alpha_4)^2(\alpha_2-\alpha_3)^2(\alpha_2-\alpha_4)^2(\alpha_3-\alpha_4)^2 \\ &= \prod_{1\leq i\lneq j\leq 4}(\alpha_i-\alpha_j)^2 \\ &= D(f). \end{aligned}$$

Somit ist $D(g) = D(f)$.

□

Insbesondere ist $g(Y)$ separabel, wenn $f(X)$ separabel ist.
Mit Hilfe der kubischen Resolvente kann man nun die Galoisgruppe eines irreduziblen Polynoms über $\mathbb{Q}$ bestimmen.

3.5 Satz:

Es sei $f(X) = X^4 + aX^3 + bX^2 + cX + d$ ein irreduzibles Polynom über $\mathbb{Q}$ mit Zerfällungskörper L. Weiter sei $g(Y)$ die kubische Resolvente von $f(X)$ mit Zerfällungskörper E. Dann gilt:

(i) $Gal(f) \cong S_4$, falls $g(Y)$ irreduzibel über $\mathbb{Q}$ ist und $D(f) \notin (\mathbb{Q}^*)^2$;

(ii) $Gal(f) \cong A_4$, falls $g(Y)$ irreduzibel über $\mathbb{Q}$ ist und $D(f) \in (\mathbb{Q}^*)^2$;

(iii) $Gal(f) \cong V_4$, falls $g(Y)$ reduzibel über $\mathbb{Q}$ ist und $D(f) \in (\mathbb{Q}^*)^2$;

(iv) $Gal(f) \cong C_4$ oder D_4, falls $g(Y)$ reduzibel über $\mathbb{Q}$ ist und $D(f) \notin (\mathbb{Q}^*)^2$.

Beweis:

Sei $V = \{id, (12)(34), (13)(24), (14)(23)\}$ die einzige transitive Untergruppe von S_4, die isomorph zu V_4 ist.
Der Zerfällungskörper E von der $g(Y)$ ist im Zerfällungskörper L von $f(X)$ enthalten.
Da nun $f(X)$ irreduzibel und somit separabel über $\mathbb{Q}$ ist, ist die Diskriminante $D(f) \neq 0$. Nach Korollar 3.4 ist also auch $D(g) \neq 0$.
Das bedeutet, dass $g(Y)$ unterschiedliche Wurzeln besitzt, unabhängig davon

ob $g(Y)$ irreduzibel ist oder nicht.
Seien nun $\alpha_1, \alpha_2, \alpha_3$ und α_4 die Wurzeln von $f(X)$ und $t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $t_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$ und $t_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$ die Wurzeln von $g(Y)$.
In der nachfolgenden Tabelle erkennt man, dass eine Permutation von den Wurzeln von $f(X)$ die Wurzeln von $g(Y)$ fixiert genau dann, wenn die Permutation ein Element von V_4 ist.
Permutationstabelle:

$\sigma \in S_4$	t_1	t_2	t_3
id	t_1	t_2	t_3
(12)(34)	t_1	t_2	t_3
(13)(24)	t_1	t_2	t_3
(14)(23)	t_1	t_2	t_3
(123)	t_3	t_1	t_2
(132)	t_2	t_3	t_1
(124)	t_2	t_3	t_1
(142)	t_3	t_1	t_2
(134)	t_3	t_1	t_2
(143)	t_2	t_3	t_1
(234)	t_2	t_3	t_1
(243)	t_3	t_1	t_2
(12)	t_1	t_3	t_2
(13)	t_3	t_2	t_1
(14)	t_2	t_1	t_3
(23)	t_2	t_1	t_3
(24)	t_3	t_2	t_1
(34)	t_1	t_3	t_2
(1234)	t_3	t_2	t_1
(1243)	t_2	t_1	t_3
(1324)	t_1	t_3	t_2
(1342)	t_2	t_1	t_3
(1423)	t_1	t_3	t_2
(1432)	t_3	t_2	t_1

Deshalb gilt:

$$Gal(L \mid E) = Gal(E \mid \mathbb{Q}) \cap V_4.$$

Man sieht nun:

(1) $g(Y)$ zerfällt in Linearfaktoren über $\mathbb{Q}$ genau dann, wenn $Gal(L \mid \mathbb{Q}) = Gal(f) \subset V_4$;

(2) $g(Y)$ ist irreduzibel über $\mathbb{Q}$ genau dann, wenn $\#Gal(L \mid \mathbb{Q}) = \#Gal(L \mid E) \cdot \#Gal(E \mid \mathbb{Q})$ durch 3 teilbar ist.

Da nun $f(X)$ irreduzibel ist, operiert die Galoisgruppe $Gal(f) = Gal(L \mid \mathbb{Q})$ transitiv auf den Wurzeln von $f(X)$. Also ist $\#Gal(L \mid \mathbb{Q})$ durch 4 teilbar. Demnach ist die Ordnung mindestens 4. Somit gilt im Fall (1):

$$Gal(f) \cong V_4,$$

also (iii).

Im Fall (2) ist $\#Gal(L \mid \mathbb{Q})$ durch 12 teilbar. Also ist $Gal(L \mid \mathbb{Q})$ isomorph zu A_4 oder S_4.Nach dem Diskriminantenkriterium 1.15 ist $Gal(f) \cong A_4$, falls $D(f)$ ein Quadrat in $\mathbb{Q}$ ist. Falls $D(f)$ kein Quadrat in $\mathbb{Q}$ ist, dann ist $Gal(f) \cong S_4$.
Somit gelten (i) und (ii).

Es bleibt noch (iv) zu zeigen.
Sei dazu $D(f) \notin (\mathbb{Q}^*)^2$ und $g(Y)$ reduzibel über $\mathbb{Q}$.
Da die Diskriminante $D(f)$ kein Quadrat in $\mathbb{Q}$ ist, ist $Gal(f)$ isomorph zu S_4, D_4 oder C_4.
Man zeigt nun, dass $Gal(f)$ nicht isomorph zu S_4 ist. Man betrachtet dazu einen 3er-Zykel. Denn die einzige Gruppe von S_4, D_4 und C_4, die einen 3er-Zykel enthält, ist die symmetrische Gruppe S_4.
Deshalb macht man folgende Annahme: $(123) \in Gal(f)$.
Dann gilt $(\star)$:

- $(123)t_1 = t_3$,
- $(123)t_3 = t_2$,
- $(123)t_2 = t_1$.

Die Wurzeln t_1, t_2 und t_3 sind alle verschieden, da $g(Y)$ separabel ist.
Die kubische Resolvente $g(Y)$ ist nach Voraussetzung reduzibel, folglich liegt mindestens eine Wurzel von $g(Y)$ in $\mathbb{Q}$. Das bedeutet aber nach $(\star)$, dass $t_1 = t_2 = t_3$ gelten muss. Dies ist aber ein Widerspruch zur Separabilität von $g(Y)$. Somit ist $Gal(f)$ nicht isomorph zu S_4 und es gilt:

$$Gal(f) \cong D_4 \text{ oder } C_4.$$

□

Der folgende Satz verwendet man um zu entscheiden, ob ein Polynom die Galoisgruppe D_4 oder C_4 besitzt.

3.6 Satz:

Sei $f(X) = X^4 + aX^3 + bX^2 + cX + d$ irreduzibel über $\mathbb{Q}$ und $D(f) \notin (\mathbb{Q}^*)^2$.
Weiter sei die kubische Resolvente $g(Y)$ reduzibel über $\mathbb{Q}$ mit
$g(Y) = \left(Y^2 - t_1\right)\left(Y^2 + sY + t\right) \in \mathbb{Q}[Y]$, wobei $Y^2 + sY + t \in \mathbb{Q}$ irreduzibel ist.
Setze $E = \mathbb{Q}\left(\sqrt{s^2 - 4t}\right)$.
Dann ist $Gal(f) \cong C_4$ genau dann, wenn die beiden Polynome

$$r_1(X) = X^2 - t_1X + d \text{ und } r_2(X) = X^2 + cX + (b - t_1)$$

in E zerfallen.

Beweis:

Setze $t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4 \in \mathbb{Q}$. Dann gilt:

$$\begin{aligned} X^2 - t_1X + d &= X^2 - (\alpha_1\alpha_2 + \alpha_3\alpha_4)X + \alpha_1\alpha_2\alpha_3\alpha_4 \\ &= (X - \alpha_1\alpha_2)(X - \alpha_3\alpha_4) \end{aligned}$$

und

$$X^2 + aX + b - t_1 = [X - (\alpha_1 + \alpha_2)][X - (\alpha_3 + \alpha_4)].$$

Falls $Gal(f) \cong C_4$ ist, dann ist E die einzige quadratische Erweiterung von $\mathbb{Q}$ im Zerfällungskörper L von $f(X)$.
Um zu zeigen, dass $Gal(f) \cong C_4$ ist, reicht es zu zeigen, dass $[L : \mathbb{Q}] \leq 4$ ist.
Das heißt man muss $\#Gal(L \mid \mathbb{Q}) \leq 4$ zeigen.
Betrachte dazu das Polynom $k(X) = X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2 \in E$ mit Wurzeln α_1 und α_2.
Sei nun $E(\alpha_1, \alpha_2)$ der Zerfällungskörper von $k(X)$ über E.
Es ist $\mathbb{Q} \subseteq E \subseteq E(\alpha_1, \alpha_2) \subseteq L$.
Daraus folgt, dass α_1, α_2, t_1, t_2 und t_3 in $E(\alpha_1, \alpha_2)$ liegen. Da
$\alpha_3 + \alpha_4 = -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) - (\alpha_1 + \alpha_2) = -a - (\alpha_1 + \alpha_2)$ ist, ist
$\alpha_3 + \alpha_4 \in E(\alpha_1, \alpha_2)$.
Da f separabel ist, ist $\alpha_1 - \alpha_2 \neq 0$. Ferner gilt:

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

Also ist $\alpha_3 - \alpha_4 \in E(\alpha_1, \alpha_2)$.
Daraus folgt, dass α_3 und α_4 in $E(\alpha_1, \alpha_2)$ liegen.
Also ist $L = E(\alpha_1, \alpha_2)$. Somit ist $[L : E(\alpha_1, \alpha_2)] = 1$ und folglich ist
$\#Gal(L \mid E(\alpha_1, \alpha_2)) = 1$.
Da nun $\alpha_1 + \alpha_2$ und $\alpha_1\alpha_2$ in E liegen, gilt $[E(\alpha_1, \alpha_2) : E] \leq 2$.
Das heißt $\#Gal(E(\alpha_1, \alpha_2) \mid E) \leq 2$. Nun gilt:

$$\begin{aligned} \#Gal(f) &= \#Gal(L \mid \mathbb{Q}) \\ &= \#Gal(L \mid E(\alpha_1, \alpha_2)) \cdot \#Gal(E(\alpha_1, \alpha_2) \mid E) \cdot \#Gal(E \mid \mathbb{Q}) \\ &\leq 1 \cdot 2 \cdot 2 \\ &= 4 \\ &< 8 \\ &= \mid D_4 \mid . \end{aligned}$$

Somit muss $Gal(f)$ isomorph zu C_4 sein.

□

3.7 Korollar:

Es sei $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ irreduzibel. Dann gilt:

(i) Falls $b \in (\mathbb{Q}^*)^2$, dann ist $Gal(f) \cong V_4$;

(ii) Falls $b \notin (\mathbb{Q}^*)^2$, aber $b\left(a^2 - 4b\right) \in (\mathbb{Q}^*)^2$, dann ist $Gal(f) \cong C_4$;

(iii) Falls $b \notin (\mathbb{Q}^*)^2$ und $b\left(a^2 - 4b\right) \notin (\mathbb{Q}^*)^2$, dann ist $Gal(f) \cong D_4$.

Beweis:

Sei $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ irreduzibel.
Dann hat die kubische Resolvente die Form

$$g(Y) = Y^3 - aY^2 - 4bY + 4ab = (Y - a)\left(Y^2 - 4b\right).$$

Falls $b \in (\mathbb{Q}^*)^2$ ist, gilt:

$$\begin{array}{rcl} D(f) & \overset{(1.14)}{=} & 16a^4b - 128a^2b^2 + 256b^3 \\ & = & 16b\left(a^4 - 8a^2b + 16b^2\right) \\ & = & 16b\left(a^2 - 4b\right)^2 \\ & = & \square. \end{array}$$

Somit ist nach Satz 3.5 (iii) $Gal(f) \cong V_4$.
Betrachte nun $b \notin (\mathbb{Q}^*)^2$.
Dann gilt nach Satz 3.5 (iv):

$$Gal(f) \cong D_4 \text{ oder } C_4.$$

Betrachte nun die Polynome $r_1(X)$ und $r_2(X)$ aus Satz 3.6. Diese Polynome haben hier folgende Gestalt:

$$r_1(X) = X^2 - aX + b \text{ und } r_2(X) = X^2.$$

Es gilt:

$$\begin{array}{lcl} Gal(f) \cong C_4 & \overset{(3.6)}{\Leftrightarrow} & \frac{\left(-a \pm \sqrt{a^2-4b}\right)}{2} \in \mathbb{Q}\left(\sqrt{4b}\right) = \mathbb{Q}\left(\sqrt{b}\right) \\ & \Leftrightarrow & \sqrt{a^2 - 4b} \in \mathbb{Q}\left(\sqrt{b}\right) \\ & \overset{(a^2-4b) \notin (\mathbb{Q}^*)^2}{\Leftrightarrow} & b\left(a^2 - 4b\right) \in (\mathbb{Q}^*)^2. \end{array}$$

Falls nun $b\left(a^2 - 4b\right) \notin (\mathbb{Q}^*)^2$, dann ist $Gal(f) \cong D_4$.

□

Im Folgenden werden Familien von Polynomen angegeben, die als Galoisgruppen S_4, A_4, V_4, D_4 oder C_4 besitzen.

3.8 Satz:

Für $p \in \mathbb{P} \setminus \{3, 5\}$ besitzt das Polynom

$$f(X) = X^4 + pX + p \in \mathbb{Q}[X]$$

die Galoisgruppe S_4.

Beweis:

Das Polynom $f(X)$ ist nach dem Eisensteinkriterium irreduzibel über $\mathbb{Q}$.
Die kubische Resolvente von $f(X)$ lautet:

$$g(Y) = Y^3 - 4pY - p^2.$$

Da nun $g(Y)$ ein ganzzahliges Polynom dritten Grades ist, kommen nur die Teiler von $-p^2$ als Nullstellen in Betracht.
Es gilt:

- $g(-1) = -1 + 4p - p^2$,
- $g(1) = 1 - 4p - p^2$,
- $g(-p) = -p^3 + 4p^2 - p^2 = p^2\,(3 - p)$,
- $g(p) = p^3 - 4p^2 - p^2 = p^2\,(p - 5)\,,$
- $g(-p^2) = p^6 + 4p^3 - p^2 = p^2\left(-p^4 + 4p - 1\right)$,
- $g(p^2) = p^6 - 4p^3 - p^2 = p^2\left(p^4 - 4p - 1\right)$.

Somit ist $g(Y)$ irreduzibel über $\mathbb{Q}$, falls $p \neq 3, 5$ ist.
Für die Diskriminante gilt nach Korollar 1.14:

$$D(f) = 256p^3 - 27p^4 = p^3\,(256 - 27p)\,.$$

Man erkennt, dass der Ausdruck $(256 - 27p)$ ab $p = 11$ negativ wird. Und da $p^3 > 0$ ist, ist $D(f)$ kein Quadrat für $p \geq 11$.
Nun muss man noch die Fälle $p = 2$ und $p = 7$ überprüfen.
Für $p = 2$ gilt:

$$D(f) = 8 \cdot 202 = 2^4 \cdot 101 \neq \square.$$

Für $p = 7$ gilt:

$$D(f) = 7^3\,(256 - 189) = 7^3 \cdot 67 \neq \square.$$

Somit ist die $D(f)$ kein Quadrat in $\mathbb{Q}$ für alle $p \in \mathbb{P} \setminus \{3, 5\}$.
Nach Satz 3.5 (i) ist $Gal(f) \cong S_4$, falls $p \in \mathbb{P} \setminus \{3, 5\}$.

□

3.9 Satz:

Sei $n \equiv 11 \pmod{20}$. Dann besitzt das Polynom

$$f(X) = X^4 - \frac{6\left(n^3-54\right)}{n^3-27n+27}X^2 - 8X + \frac{9\left(n^3-54\right)^2 - 12\left(n^3+27\right)\left(n^3-27n+27\right)}{\left(n^3-27n+27\right)^2}$$

A_4 als Galoisgruppe über $\mathbb{Q}$.

Beweis:

Man kann das Polynom f folgendermaßen schreiben:

$$\begin{aligned} f(X) &= \left(n^3-27n+27\right)^2 X^4 - 6\left(n^3-54\right)\left(n^3-27n+27\right)X^2 \\ &\quad -8\left(n^3-27n+27\right)^2 X + 9\left(n^3-54\right)^2 - 12\left(n^3+27\right)\left(n^3-27n+27\right) \\ &= \left(n^3-27n+27\right)^2 X^4 - 6\left(n^3-54\right)\left(n^3-27n+27\right)X^2 \\ &\quad -8\left(n^3-27n+27\right)^2 X + (n-1)\left(n^5+6n^4-72n^3+108n^2+648n+972\right). \end{aligned}$$

Das Polynom $f(X)$ ist nach dem Eisensteinkriterium ($p = 2$) irreduzibel über $\mathbb{Q}$. Denn es gilt:

- $n^3 - 27n + 27 \equiv n^3 + n + 1 \pmod{2} \equiv 1 \pmod{2}$ für alle $n \in \mathbb{Z}$;
- $2 \mid \left[-6\left(n^3-54\right)\left(n^3-27n+27\right)\right]$;
- $2 \mid \left[-8\left(n^3-27n+27\right)^2\right]$;
- $2 \mid (n-1)\left(n^5+6n^4-72n^3+108n^2+648n+972\right)$ für alle $n \equiv 11 \pmod{20}$;
- $2^2 \nmid (n-1)\left(n^5+6n^4-72n^3+108n^2+648n+972\right)$ $(\star)$.

Beweis von $(\star)$:
Annahme: $(\star)$ gilt nicht.
Dann ist

$$(n-1)\left(n^5+6n^4-72n^3+108n^2+648n+972\right) \equiv 0 \pmod{4}.$$

Dies gilt falls:

$$n \equiv 1 \pmod{4} \text{ oder } n^5 + 2n^4 \pmod{4} \equiv 0 \pmod{4} \text{ ist.}$$

Die zweite Kongruenzbedingung ist erfüllt, wenn

$$n \equiv 0 \pmod{4} \text{ oder } n \equiv 2 \pmod{4} \text{ ist.}$$

Dies ist aber ein Widerspruch zur Bedingung, dass $n \equiv 11 \pmod{20}$.
Diese Bedingung beinhaltet $n \equiv 3 \pmod{4}$.
Somit ist die Annhme falsch. Das heißt $(\star)$ gilt.

Für die Diskriminante ergibt sich aus Korollar 1.14:

$$\begin{aligned} D(f) &= 16a^4c - 4a^3b^2 - 128a^2c^2 + 144ab^2c + 256c^3 - 27b^4 \\ &= (2^{12}\cdot 3^{12}n^6 - 18\cdot 2^{12}\cdot 3^{12}n^5 + 81\cdot 2^{12}\cdot 3^{12}n^4 + 54\cdot 2^{12}\cdot 3^{12}n^3 \\ &\quad -486\cdot 2^{12}\cdot 3^{12}n^2 + 729\cdot 2^{12}\cdot 3^{12})(n^3 - 27n + 27)^{-4} \\ &= 2^{12}\cdot 3^{12}(n^3 - 9n^2 + 27)^2(n^3 - 27n + 27)^{-4} \end{aligned}$$

Also ist $D(f) \in (\mathbb{Q}^*)^2$.
Daraus folgt, dass $Gal(f) \cong A_4$ oder V_4 ist.
Wenn $Gal(f)$ einen 3er-Zykel enthält, dann ist $Gal(f) \cong A_4$, da V_4 keine 3er-Zykel enthält.
Für $n \equiv 1 \pmod 5$ gilt:

$$\begin{aligned} f(X) &\equiv X^4 + 3X^2 + 2X \pmod 5 \\ &\equiv X\left(X^3 + 3X + 2\right) \pmod 5 . \end{aligned}$$

Das Polynom $X^3 + 3X + 2$ ist irreduzibel in $\mathbb{F}_5[X]$.
Nach Satz 1.17 enthält $Gal(f)$ einen 3er-Zykel.
Also ist $Gal(f) \cong A_4$.

□

3.10 Satz:

Das Polynom

$$f(X) = X^4 - 2(n^2p + m^2q)X^2 + (n^2p - m^2q)^2 \in \mathbb{Q}[X]$$

mit $2 < p,\ q \in \mathbb{P},\ p \neq q,\ 0 \neq m, n \in \mathbb{Q}$, hat die Galoisgruppe V_4.

Beweis:

Das Polynom $f(X)$ ist irreduzibel über $\mathbb{Q}$. Denn es gilt:

- $b^2 - 4d = 2^2(n^2p + m^2q)^2 - 4(n^2p - m^2q)^2 = 16m^2n^2pq \notin \mathbb{Q}^2$;
- $-b + 2\sqrt{d} = 2(n^2p + m^2q) + 2(n^2p - m^2q) = 4n^2p \notin \mathbb{Q}^2$;
- $-b - 2\sqrt{d} = 2(n^2p + m^2q) - 2(n^2p - m^2q) = 4m^2q \notin \mathbb{Q}^2$.

Somit ist nach Satz 1.21 das Polynom $f(X)$ irreduzibel.
Da nun $f(X)$ irreduzibel über $\mathbb{Q}$ ist und $(n^2p - m^2q)^2 \in (\mathbb{Q}^*)^2$ gilt, folgt aus Korollar 3.7, dass $Gal(f) \cong V_4$ ist .

□

3.11 Satz:

Sei $2 < p \in \mathbb{P}$ mit $p-1 \notin \mathbb{Q}^2$ und sei $s \neq np$ für alle $n \in \mathbb{N}$.
Dann hat

$$f(X) = X^4 - 2spX^2 + s^2p(p-1) \in \mathbb{Q}[X]$$

die Galoisgruppe D_4.

Beweis:

Durch das Eisensteinkriterium sieht man sofort, dass $f(X)$ irreduzibel über $\mathbb{Q}$ ist.
Denn $p \nmid 1$, $p \mid (-2sp)$, $p \mid s^2p(p-1)$, $p^2 \nmid s^2p(p-1)$.
Berechnung der Diskriminante liefert:

$$\begin{aligned} D(f) &\overset{(1.14)}{=} 16(-2sp)^4 s^2p(p-1) - 128(-2sp)^2(s^2p(p-1))^2 \\ &\qquad +256(s^2p(p-1))^3 \\ &= 4^4 s^6 p^5(p-1) - 2 * 4^4 s^6 p^4 (p-1)^2 + 4^4 s^6 p^3 (p-1)^3 \\ &= 4^4 s^6 p^3 (p-1)\left[p^2 - 2p(p-1) + (p-1)^2\right] \\ &= 4^4 s^6 p^3 (p-1)\left[p^2 - 2p^2 + 2p + p^2 - 2p + 1\right] \\ &= 4^4 s^6 p^3 (p-1). \end{aligned}$$

$D(f)$ ist also kein Quadrat in $\mathbb{Q}$.
Die kubische Resolvente von $f(X)$ ist reduzibel. Denn

$$\begin{aligned} g(Y) &= Y^3 + 2spY^2 - 4s^2p(p-1)Y - 8s^3p^2(p-1) \\ &= (Y + 2sp)\left[Y^2 - 4s^2p(p-1)\right]. \end{aligned}$$

Nach Satz 3.5 (iv) ist $Gal(f) \cong D_4$ oder C_4.
Nun ist aber $s^2p(p-1) \notin (\mathbb{Q}^*)^2$, da $p(p-1)$ kein Quadrat ist. Des Weiteren gilt:

$$\begin{aligned} s^2p(p-1)(4s^2p^2 - 4s^2p(p-1)) &= 4s^4p^2(p-1)(p-p+1) \\ &= 2^2 s^4 p^2 (p-1) \notin (\mathbb{Q}^*)^2. \end{aligned}$$

Nach Korollar 3.7 (iii) ist $Gal(f) \cong D_4$.

□

3.12 Satz:

Ist $1 + n^2 \in \mathbb{P}$ mit $n \in \mathbb{N} \setminus \{0\}$ und $0 \neq s \neq 1 + n^2$, so besitzt das Polynom

$$f(X) = X^4 - 2s(1+n^2)X^2 + s^2n^2(1+n^2) \in \mathbb{Q}[X]$$

als Galoisgruppe C_4.

Beweis:

Wähle $p = 1 + n^2 \in \mathbb{P}$. Dann gilt:
$p \nmid 1$, $p \mid (-2s(1+n^2))$, $p \mid s^2n^2(1+n^2)$, $p^2 \nmid s^2n^2(1+n^2)$.
Somit ist $f(X)$ irreduzibel über $\mathbb{Q}$ nach dem Eisensteinkriterium.
Für die kubische Resolvente ergibt sich:

$$\begin{aligned} g(Y) &= Y^3 + 2s(1+n^2)Y^2 - 4s^2n^2(1+n^2)Y - 8s^3n^2(1+n^2)^2 \\ &= \left[Y + 2s(1+n^2)\right]\left[Y^2 - 4s^2n^2(1+n^2)\right]. \end{aligned}$$

Also ist $g(Y)$ reduzibel über $\mathbb{Q}$. Es gilt nun:

$$\begin{aligned} D(f) &= D(g) \\ &\overset{(1.13)}{=} 4^3s^6n^4(1+n^2)^4 + 4^4s^6n^6(1+n^2)^3 + 4^4s^6n^2(1+n^2)^5 \\ &\quad -27 * 4^3s^6n^4(1+n^2)^4 + 18 * 4^3s^6n^4(1+n^2)^4 \\ &= -8 * 4^3s^6n^4(1+n^2)^4 + 4^4s^6n^6(1+n^2)^3 + 4^4s^6n^2(1+n^2)^5 \\ &= 4^4s^6n^2(1+n^2)^3\left[-2n^2(1+n^2) + n^4 + (1+n^2)^2\right] \\ &= 4^4s^6n^2(1+n^2)^3(-2n^2 - 2n^4 + n^4 + n^4 + 2n^2 + 1) \\ &= 4^4s^6n^2(1+n^2)^3 \\ &\neq \square. \end{aligned}$$

Nach Satz 3.4 (iv) ist $Gal(f) \cong D_4$ oder C_4.
Weiter gilt:
$s^2n^2(1+n^2) \notin (\mathbb{Q}^*)^2$, da $(1+n^2)$ kein Quadrat in $\mathbb{Q}$ ist und

$$\begin{aligned} s^2n^2(1+n^2)(4s^2(1+n^2)^2 - 4s^2n^2(1+n^2)) &= 4s^4n^2(1+n^2)^3 - 4s^4n^4(1+n^2)^2 \\ &= 4s^4n^2(1+n^2)^2\left[(1+n^2) - n^2\right] \\ &= 2^2s^4n^2(1+n^2)^2 \in (\mathbb{Q}^*)^2. \end{aligned}$$

Aus Korollar 3.7 folgt, dass $Gal(f) \cong C_4$ ist.

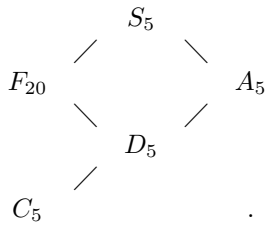
□

4 Polynome 5. Grades

In diesem Kapitel bezeichne

- $S_5 = < (12345), (12) >$ die symmetrische Gruppe mit 120 Elementen;
- $A_5 = < (12345), (123) >$ die alternierende Gruppe mit 60 Elementen;
- $F_{20} = < (12345), (1254) >$ die Frobeniusgruppe mit 20 Elementen;
- $D_5 = < (12345), (15)(24) >$ die Diedergruppe mit 10 Elementen;
- $C_5 = < (12345) >$ die zyklische Gruppe mit 5 Elementen.

Das Gruppendiagramm sieht folgendermaßen aus:



Wie in Kapitel 3 muss man sich zuerst überlegen, welche Galoisgruppen für irreduzible Polynome fünften Grades in Betracht kommen.
Sei dazu $f(X) \in \mathbb{Q}[X]$ ein irreduzibles Polynom 5.Grades. Nach Bemerkung 1.7 permutiert $Gal(f)$ die Nullstellen des Polynoms f. Damit operiert $Gal(f)$, *nach Wahl der Nummerierung,* transitiv auf der Menge {1,2,3,4,5} der Indizes. Somit können wir $Gal(f)$ als transitive Untergruppe der symmetrischen Gruppe S_5 auffassen.

4.1 Satz:

Die transitiven Untergruppen von S_5 sind bis auf Konjugation die S_5, A_5, F_{20}, D_5 und C_5.

Beweis:

Die transitiven Untergruppen von S_5 haben Gruppenordnungen, die durch 5 teilbar sind.
Also kommen folgende Gruppenordnungen in Betracht: 120, 60, 40, 30, 20, 15, 10 und 5.
Die Gruppe mit 120 Elementen ist die symmetrische Gruppe S_5. Des Weiteren ist die alternierende Gruppe A_5 die einzige Gruppe, die Ordnung 60 besitzt.
Falls es eine Untergruppe von A_5 mit Ordnung 30 geben würde, dann wäre diese normal in A_5. Aber da A_5 einfach ist, kann es keine Gruppe G mit Ordnung 30 existieren.
Die Gruppe G mit 30 Elementen besitzt eine Untergruppe $G \cap A_5$ mit Ordnung 15. Aber nach den Sätzen von Sylow gibt es bis auf Isomorphie nur eine

einzige Untergruppe mit der Ordnung 15. Diese ist zyklisch und insbesondere abelsch. Aber die Elemente mit Ordnung 5 kommutieren nicht mit Elemente mit Ordnung 3 in S_5, da zum Beispiel $(12345)(123) = (13245) \neq (13425) = (123)(12345)$. Somit gibt es keine Untergruppe der Ordnung 15 in S_5, und damit auch keine Untergruppe der Ordnung 30.
Untergruppen G mit 5 Elementen sind alle zu C_5 konjugiert.
Betrachte nun den Fall, dass $\mid G \mid = 10$ ist.
Sei dazu $\sigma = (12345)$ und $\tau_3 = (15)(24)$. Dann ist $\sigma^2 = (13524)$, $\sigma^3 = (14253)$, $\sigma^4 = \sigma^{-1} = (15432)$, $\sigma^5 = id$ und $\tau_3^2 = id$.
Weiter gilt:
$\tau_3\sigma\tau_3^{-1} = (15)(24)(12345)(15)(24) = (15432) = \sigma^{-1}$. Dies ist äquivalent zu $\tau_3\sigma = \sigma^{-1}\tau_3$.
Somit erzeugen σ und τ_3 die D_5.
Bis auf Konjugation ist dies die einzige Untergruppe von S_5 mit der Ordnung 10. Denn es gilt:
$\sigma = (12345) = (23451) = (34512) = (45123) = (51234)$. Dazu gehören nun $\tau_3 = (15)(24)$, $\tau_4 = (12)(35)$, $\tau_5 = (14)(23)$, $\tau_1 = (25)(34)$ und $\tau_2 = (13)(45)$.
Wähle jetzt $\tau \in S_5$ mit der Ordnung 2 so, dass $< \sigma, \tau >$ Ordnung 10 besitzt.
Nun reicht es zu zeigen, dass $\tau_x \in D_5$ für alle $x \in \{1, 2, 3, 4, 5\}$. Es gilt:

- ${}^{\sigma}\tau_1 = (\sigma 2\sigma 5)(\sigma 3\sigma 4) = (31)(45) = \tau_2 \in D_5$;
- ${}^{\sigma}\tau_2 = (\sigma 1\sigma 3)(\sigma 4\sigma 5) = (24)(51) = \tau_3 \in D_5$;
- ${}^{\sigma}\tau_3 = (\sigma 1\sigma 5)(\sigma 2\sigma 4) = (21)(35) = \tau_4 \in D_5$;
- ${}^{\sigma}\tau_4 = (\sigma 2\sigma 1)(\sigma 3\sigma 5) = (32)(41) = \tau_5 \in D_5$;
- ${}^{\sigma}\tau_5 = (\sigma 3\sigma 2)(\sigma 1\sigma 4) = (34)(25) = \tau_1 \in D_5$.

Somit ist D_5 bis auf Konjugation die einzige Untergruppe von S_5 mit Ordnung 10.
Sei jetzt G eine Untergruppe der Ordnung 20 von S_5. Und sei $U = \{id, \tau_1, \tau_2, \tau_3\}$ eine 2-Sylow-Untergruppe von G.
Zeige nun zuerst, dass U in G nicht normal ist.
Annahme: U ist normal in G.
Dann ist $\sigma\tau\sigma^{-1} \neq \tau$ $(\star)$ für alle 5er-Zykel σ, denn 5er-Zykel kommutieren nicht mit Elementen der Ordnung 2 in S_5.
Deshalb kann man voraussetzen, dass

$$(\sigma\tau\sigma^{-1} = \tau_1 \text{ und } \sigma^{-1}\tau\sigma = \tau_1) \text{ oder } (\sigma\tau\sigma^{-1} = \tau_2 \text{ und } \sigma^{-1}\tau\sigma = \tau_2).$$

Daraus folgt:

$$\sigma\tau\sigma^{-1} = \sigma^{-1}\tau\sigma \Leftrightarrow \sigma^2\tau\sigma^{-2} = \tau.$$

Dies ist ein Widerspruch zur Normalität von U, denn
$\sigma^2\tau\sigma^{-2} = \tau \overset{(\star)}{\Leftrightarrow} \sigma\tau\sigma^{-1} = \tau$.
Betrachte nun den 2. Fall:

$$\sigma\tau\sigma^{-1} = \tau_2 = \sigma^{-1}\tau\sigma \Leftrightarrow \sigma^2\tau\sigma^{-2} = \tau.$$

Dies führt ebenfalls zu einem Widerspruch. Also ist U nicht normal in G.
Folglich muss man zwei Fälle betrachten:

$$G \nsubseteq A_5 \text{ und } G \subset A_5.$$

Betrachte zuerst den Fall $G \nsubseteq A_5$.
Dann wird jede 2-Sylow-Gruppe von G durch einen 4er-Zykel erzeugt und $G \cap A_5$ wird durch σ und τ^2 erzeugt.
Sei nun $\sigma = (12345)$ und τ lässt das Element 3 fest. Dann ist
$\tau^2 = \tau_3 = (15)(24)$.
Aus den vorherigen Überlegungen weiß man, dass $G \cap A_5 = D_5$ ist.
Somit hat man nur zwei Möglichkeiten für τ:

$$\tau = (1254) \text{ oder } \tau = (1452), \text{ wobei } (1254)(1452) = id = (1452)(1254).$$

Also hat man nur eine Möglichkeit für τ. Sei also $\tau = (1254)$.
Dann gilt:

$$\tau\sigma\tau^{-1} = (1254)(12345)(1452) = (14253) = \sigma^3.$$

Somit ist F_{20} bis auf Konjugation die einzige Untergruppe von S_5, die die Ordnung 20 besitzt und nicht in A_5 liegt.
Sei nun $G \subset A_5$.
Nach den vorherigen Überlegungen weiß man, dass es keine 2-Sylow-Gruppe in A_5 gibt, die normal ist.
Betrachte jetzt die 5-Sylow-Gruppe von G.
Nach den Sätzen von Sylow gilt für die Anzahl a_5 der 5-Sylow-Gruppen:

$$a_5(G) \equiv 1(5) \text{ und } a_5(G) \mid 4.$$

Daraus folgt, dass $a_5(G) = 1$ sein muss. Also existiert genau eine normale 5-Sylow-Untergruppe von G.
Sei nun $\sigma = (12345) \in G$ der Erzeuger einer normalen Untergruppe von G und $\tau \in G$ ein Element mit der Ordnung 2.
Man zeigt nun, dass $\tau \in D_5$. Man setzt voraus, dass τ die Zahl 3 festhält.
Annahme: $\tau \neq \tau_3$.
Dann ist τ entweder (12)(45) oder (14)(25).
Da nun $< \sigma >$ normal in G ist, muss für eine der beiden Möglichkeiten für τ gelten:

$$\tau\sigma\tau^{-1} \in < \sigma >.$$

Es gilt:

1. $(12)(45)(12345)(12)(45) = (13542) \notin < \sigma >$;
2. $(14)(25)(12345)(14)(25) = (12453) \notin < \sigma >$.

Somit ist die Annahme falsch, das heißt $\tau = \tau_3$. Also ist $\tau \in D_5$.
Folglich gibt es keine Untergruppe mit der Ordnung 20 in A_5, da G von σ und Elemente mit der Ordnung 2 erzeugt werden würde.
Es fehlt noch die Gruppenordnung 40.
Solch eine Untergruppe G gibt es nicht in S_5, denn sonst würde eine Untergruppe $G \cap A_5$ in A_5 mit Ordnung 20 existieren.
Wie oben gesehen, gibt es solch eine Gruppe nicht.

□

Sei nun $f(X) = X^5 + aX^4 + bX^3 + cX^2 + dX + e \in \mathbb{Q}[X]$ ein irreduzibles Polynom.
Mit Hilfe des Diskriminantenkriteriums (1.16) können wir nur unterscheiden ob $Gal(f) = S_5$ oder F_{20} ist oder ob $Gal(f) = A_5$, D_5 oder C_5 ist.
Um die Galoisgruppe eines irreduziblen Polynoms fünften Grades genauer bestimmen zu können, müssen wir überprüfen ob das Polynom auflösbar durch Radikale ist.
Wir wissen nämlich, dass F_{20}, D_5 und C_5 auflösbare Gruppen und S_5 und A_5 nicht auflösbare Gruppen sind.
Der fogende Satz ist von Seite 279 aus dem Buch [Lorenz].

4.2 Satz:

Ein Polynom ist auflösbar durch Radikale genau dann, wenn die Galoisgruppe dieses Polynoms auflösbar ist.

"□"

Da es im Allgemeinen sehr schwierig ist zu entscheiden, ob ein Polynom fünften Grades auflösbar durch Radikale ist oder nicht, verwenden wir die Weber-Resolvente.

4.3 Definition:

Sei $f(X) = X^5 + aX^4 + bX^3 + cX^2 + dX + e \in \mathbb{Q}[X]$ irreduzibel. Das Polynom

$$G(Z) = \left(Z^3 + b_4Z^2 + b_2Z + b_0\right)^2 - 2^{10}D(f)Z \in \mathbb{Q}[Z]$$

heißt Weber-Resolvente von f, wobei

$$\begin{aligned}
b_0 &= -64c^4 - 176b^2d^2 + 28b^4d - 16a^2b^2c^2 - 1600a^2e^2 - 64acd^2 - 80b^2ce \\
&\quad +384a^3de + 640ac^2e - 192a^2bce - 1600cde - 128a^2c^2d + 48ab^3e \\
&\quad -640abde + 64a^3bcd + 64abc^3 + 224a^2bd^2 + 224bc^2d + 8ab^4c \\
&\quad -112ab^2cd - 16a^2b^3d - 16b^3c^2 - 64a^4d^2 + 4000be^2 - b^6 + 320d^3, \\
b_2 &= 3b^4 - 16ab^2c + 16a^2c^2 + 16a^2bd - 64a^3e + 16bc^2 \\
&\quad -8b^2d - 112acd + 240abe + 240d^2 - 400ce, \\
b_4 &= -3b^2 + 8ac - 20d \ .
\end{aligned}$$

Es gilt:

$$\begin{aligned} G(Z) &= \left(Z^3 + b_4Z^2 + b_2Z + b_0\right)^2 - 2^{10}D(f)Z \\ &= Z^6 + 2b_4Z^5 + 2b_2Z^4 + 2b_0Z^3 + 2b_2b_4Z^3 \\ &\quad +2b_0b_4Z^2 + 2b_0b_2Z + b_4^2Z^4 + b_2^2Z^2 + b_0^2 - 2^{10}D(f)Z \\ &= Z^6 + 2b_4Z^5 + \left(2b_2 + b_4^2\right)Z^4 + 2\left(b_0 + b_2b_4\right)Z^3 \\ &\quad + \left(2b_0b_4 + b_2^2\right)Z^2 + \left(2b_0b_2 - 2^{10}D(f)\right)Z + b_0^2. \end{aligned}$$

Wir verwenden von Seite 41 aus dem Buch [GenPol] den folgenden Satz:

4.4 Satz:

$Gal(f)$ ist auflösbar genau dann, wenn die Weber-Resolvente $G(Z)$ von f eine Wurzel in $\mathbb{Q}$ besitzt.

Dieser Satz gilt auch für beliebige Körper K, aber wir betrachten hier nur den Fall $K = \mathbb{Q}$.
Wir erhalten nun das Korollar 4.5.

4.5 Korollar:

Sei $f(X) = X^5 + aX^4 + bX^3 + cX^2 + dX + e \in \mathbb{Q}[X]$ ein irreduzibles Polynom. Dann gilt:

(i) $Gal(f) \cong S_5$, falls $D(f) \notin (\mathbb{Q}^*)^2$ und $f(X)$ ist nicht auflösbar durch Radikale;

(ii) $Gal(f) \cong F_{20}$, falls $D(f) \notin (\mathbb{Q}^*)^2$ und $f(X)$ ist auflösbar durch Radikale;

(iii) $Gal(f) \cong A_5$, falls $D(f) \in (\mathbb{Q}^*)^2$ und $f(X)$ ist nicht auflösbar durch Radikale;

(iv) $Gal(f) \cong D_5$ oder C_5, falls $D(f) \in (\mathbb{Q}^*)^2$ und $f(X)$ ist auflösbar durch Radikale.

Beweis:

Dieses Korollar ergibt sich direkt aus dem Diskriminantenkriterium 1.16 und Satz 4.2 mit dem Wissen, dass S_5 und A_5 nicht auflösbar beziehungsweise F_{20}, D_5 und C_5 auflösbar sind.

□

Falls das Polynom f die Form $f(X) = X^5 + aX + b \in \mathbb{Q}[X]$ besitzt, gilt folgender Satz:

4.6 Satz von Weber:

Sei $f(X) = X^5 + aX + b \in \mathbb{Q}[X]$ irreduzibel.
Falls $a = 0$ ist, dann ist $Gal(f) \cong F_{20}$. Andernfalls gilt:
$Gal(f) \cong D_5$ (bzw. F_{20}) genau dann, wenn die folgenden zwei Bedingungen erfüllt sind:

(i) $D(f) \in (\mathbb{Q}^*)^2$ (bzw. $D(f) \notin (\mathbb{Q}^*)^2$) und

(ii) a und b haben die folgende Form:

$$a = \frac{5^5\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)},\ b = a\mu,$$

für einige $\lambda, \mu \in \mathbb{Q}$ mit $\lambda \neq 1$ und $\mu \neq 0$.

Beweis:

Für den Fall $a = 0$ ist die Aussage klar, da $D(f) \overset{(1.15)}{=} 5^5b^4 \notin (\mathbb{Q}^*)^2$ und $G(Z) = Z^6$. Das heißt $f(X)$ ist auflösbar durch Radikale nach Satz 4.4.
Nach Korollar 4.5 ist $Gal(f) \cong F_{20}$. (Mit der Kummertheorie erhält man $Gal(f) \cong F_{20}$ auch direkt. Für $a = 0$ ist $f(X) = X^5 + b$. Somit ist der Körper M, der fünften Einheitswurzeln, im Zerfällungskörper L von f enthalten. Nach der Kummertheorie muss $[L : M] = 5$ sein. Somit ist
$[L : \mathbb{Q}] = [L : M] \cdot [M : \mathbb{Q}] = 5 \cdot 4 = 20$. Also ist $Gal(f) \cong F_{20}$.)
Sei jetzt $a \neq 0$.
In diesem Fall hat die Weber-Resolvente die Form

$$G(Z) = \left(Z^3 - 20aZ^2 + 240a^2Z + 320a^3\right)^2 - 2^{10}\left(4^4a^5 + 5^5b^4\right)Z.$$

Da man nur entscheiden muss, ob $G(Z)$ in $\mathbb{Q}$ eine Nullstelle besitzt, kann man eine Transformation $H(Z)$ von $G(Z)$ betrachten:

$$H(Z) = 2^{-12}G(4Z) = (Z-a)^4(Z^2 - 6aZ + 25a^2) - 5^5b^4Z.$$

Sei r eine rationale Wurzel von $H(Z)$.
Schreibe $r = a\lambda$ und $b = a\mu$. Dann gilt:

$$\begin{aligned}
H(r) = 0 &\Leftrightarrow (a\lambda - a)^4(a^2\lambda^2 - 6a^2\lambda + 25a^2) - 5^5a^4\mu^4a\lambda = 0\\
&\Leftrightarrow a^6(\lambda-1)^4(\lambda^2 - 6\lambda + 25) - 5^5a^5\lambda\mu^4 = 0\\
&\Leftrightarrow a^5(a(\lambda-1)^4(\lambda^2 - 6\lambda + 25) - 5^5\lambda\mu^4) = 0\\
&\Leftrightarrow a(\lambda-1)^4(\lambda^2 - 6\lambda + 25) - 5^5\lambda\mu^4 = 0\\
&\Leftrightarrow a = \tfrac{5^5\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)},\ \lambda \neq 1.
\end{aligned}$$

Wenn nun zusätzlich $D(f) \in (\mathbb{Q}^*)^2$ ist, dann ist $Gal(f) \cong D_5$.
Denn $Gal(f) \cong C_5$ ist für Polynome $f(X) = X^5 + aX + b \in \mathbb{Q}[X]$ nicht möglich, da solche Polynome immer mindestens ein Paar komplexer Nullstellen besitzt.
Falls $D(f) \notin (\mathbb{Q}^*)^2$ ist und a und b von der obigen Form sind, dann besitzt $G(Z)$ eine Nullstelle.
Somit ist $Gal(f)$ auflösbar. Also ist $Gal(f) \cong F_{20}$. □

Für irreduzible Polynome $f(X) = X^5 + aX + b \in \mathbb{Q}[X]$ kommt $Gal(f) \cong C_5$ nicht in Frage, da solche Polynome mindestens ein Paar komplexer Nullstellen haben.
Somit können wir für solche Polynome die Galoisgruppe genau bestimmen.

Für allgemeine Polynome fünften Grades, das heißt
$f(X) = X^5 + aX^4 + bX^3 + cX^2 + dX + e \in \mathbb{Q}[X]$, können wir nicht explizit entscheiden ob $Gal(f) \cong C_5$ oder D_5 ist.
Falls $Gal(f) \cong C_5$ ist, dann können wir dies nicht zu 100% bestimmen.
Wenn aber $Gal(f) \cong D_5$ ist, dann können wir dies mit Hilfe von Satz 1.17 bestimmen.
Falls wir also eine Primzahl finden, so dass $\overline{f}(X)$ so zerfällt, dass
$\overline{f}(X) = f_1 f_2 f_3$ mit $n_1 = 1$, $n_2 = n_3 = 2$ ist, dann hat die Galoisgruppe von f nach Satz 1.17 ein Element σ mit Zykelstruktur (1,2,2).
Dann ist $Gal(f) \cong D_5$, falls $Gal(f) \cong D_5$ oder C_5 ist.
Dies liegt daran, dass C_5 kein Element σ mit Zykelstruktur (1,2,2) besitzt.

Wenn wir jetzt in der Situation sind, dass $Gal(f) \cong C_5$ oder D_5 ist, dann können wir, mit dem Satz von Cebotarev von Seite 569 aus [Neuk] und dem χ^2-Anpassungstest aus der Wahrscheinlichkeitstheorie, mit hoher Wahrscheinlichkeit sagen, dass $Gal(f) \cong C_5$ ist und nicht D_5.

4.7 Satz von Cebotarev:

Sei $f \in \mathbb{Z}[X]$ irreduzibel über $\mathbb{Q}$, $G = Gal(f) \subset S_n$, $n = deg(f)$ und
$P_\pi = \{\sigma \in S_n \text{ mit Zykelstruktur } \pi\}$.

(i) Für fast alle $p \in \mathbb{P}$ (endlich viele Ausnahmen) ist die Reduktion $\overline{f_p}$ von f in $\mathbb{F}_p[X]$ separabel vom Grad n;

(ii) Sei π eine Partition von n. Es gilt

$$\lim_{x\to\infty} \frac{\#\{p \in \mathbb{P} \mid p \le x,\ \overline{f_p} \text{ zerfällt entsprechend } \pi\}}{\#\{p \in \mathbb{P} \mid p \le x\}} = \frac{\#(P_\pi \cap G)}{\#G}.$$

Wir fassen $\frac{\#(P_\pi \cap G)}{\#G}$ als Wahrscheinlichkeitsmaß auf $\mathbb{P}' := \mathbb{P} \setminus \{\text{verzweigte } p\}$ auf, wobei es kein "echtes" Wahrscheinlichkeitsmaß ist, da keine σ-Additivität vorliegt.
Die Primzahlen, die wir betrachten, sind unverzweigt im Zerfällungskörper von f.
Die Menge der verzweigten Primzahlen ist endlich, das heißt das Maß ist 0.

Somit gilt für die Wahrscheinlichkeiten der einzelnen Zykelstrukturen in D_5 und C_5:
D_5:

- (1,1,1,1,1): P($\{(1,1,1,1,1)\}$)=$\frac{1}{10}$ =10%
- (2,2,1): P($\{(2,2,1)\}$)=$\frac{5}{10}$ =50%
- (5): P($\{(5)\}$)=$\frac{4}{10}$ =40% .

C_5:

- (1,1,1,1,1): P($\{(1,1,1,1,1)\}$)=$\frac{1}{5}$ =20%
- (5): P($\{(5)\}$)=$\frac{4}{5}$ =80% .

Kommen wir nun zum $\chi^2 -$ Anpassungstest.
Beim χ^2- Anpassungstest sind die Zufallsvariablen $X_1, ..., X_n$ *unabhängig* und *identisch* verteilt. X_1 kann K verschiedene Werte annehmen.
Sei nun p_k die Wahrscheinlichkeit dafür, dass X_1 den k-ten Wert annimmt, wobei $1 \leq k \leq K$. Der Vektor $v = (p_1, ..., p_K)$ ist unbekannt.
Aus Beobachtungen $(x_1, ..., x_n)$ soll die Hypothese getestet werden, dass v gleich einem vorgegebenen $v_o = (p_1^o, ..., p_K^o)$ ist.

In unserem Fall ist $K = 3$ und X_1 kann die Zykelstrukturen (1,1,1,1,1) oder (1,2,2) oder (5) annehmen. Wir setzen:

k	k-te Wert
1	(1,1,1,1,1)
2	(1,2,2)
3	(5)

Als Hypothese verwenden wir $Gal(f) \cong D_5$ und als Alternative $Gal(f) \cong C_5$.
Das heißt, falls die Hypothese nicht gilt, dann gilt die Alternative.
Wir testen also die Hypothese

$$v = (p_1^o;\ p_2^o;\ p_3^o) = (0,1;\ 0,5;\ 0,4)\,.$$

Dabei ist

- 0,1 = 10 % die Wahrscheinlichkeit für das Auftreten eines Zykeltyps von der Form (1,1,1,1,1) in $Gal(f)$;
- 0,5 = 50 % die Wahrscheinlichkeit für das Auftreten eines Zykeltyps von der Form (1,2,2) in $Gal(f)$;
- 0,4 = 40 % die Wahrscheinlichkeit für das Auftreten eines 5er-Zykeltyps in $Gal(f)$.

Sei nun n_k die empirische Häufigkeit des k-ten Wertes in den n Beobachtungen. Ferner ist np_k^o die erwartete Häufigkeit für den k-ten Wert unter der Hypothese $v = v_o$.
Als Testgröße betrachtet man:

$$T := \sum_{1 \leq k \leq K} \frac{(n_k - np_k^o)^2}{np_k^o}.$$

Die Faustregel besagt nun, falls $np_k^o \geq 5$ für alle $1 \leq k \leq K$ ist, dann ist es vertretbar, die Verteilung von T unter der Hypothese durch die χ^2- Verteilung mit $(K-1)$ Freiheitsgraden zu approximieren.
Somit wählt man in unserer Situation den Stichprobenumfang n so aus, dass die Bedingung $0,1 \cdot n \geq 5$ erfüllt ist.
In unserem Fall, wählt man zum Beispiel die ersten 100 unverzweigten Primzahlen aus, um das Zerfällungsverhalten von f mod p und damit die Zykelstrukturen zu erhalten.
Man verwirft die Hypothese und nimmt die Alternative an, falls gilt:

$$T \geq \chi^2_{K-1,\, 1-\alpha}.$$

Dabei ist $\chi^2_{K-1,\, 1-\alpha}$ das $(1-\alpha)$ Quantil der χ^2-Verteilung mit $K-1$ Freiheitsgraden.
In unserer Situation verwerfen wir die Hypothese $(Gal(f) \cong D_5)$,
falls $T \geq \chi^2_{2,\, 1-\alpha}$ ist.
Wenn dies erfüllt ist, dann hat man die Hypothese zu unrecht mit einer Wahrscheinlichkeit von höchstens α % verworfen.
Falls α sehr klein gewählt ist, dann kann man mit einer hohen Sicherheit sagen, dass $Gal(f) \cong C_5$ ist.

Im Folgenden werden Beispiele von Familien von Polynomen angegeben, die als Galoisgruppe S_5, F_{20}, A_5 und D_5 haben.

4.8 Satz:

Sei $2 < p \in \mathbb{P}$. Dann besitzt

$$f(X) = X^5 - pX^4 + p \in \mathbb{Q}[X]$$

die Galoisgruppe S_5.

Beweis:

Man erkennt mit dem Eisensteinkriterium sofort, dass $f(X)$ irreduzibel über $\mathbb{Q}$ ist.
Nach Satz 1.12 gilt:

$$D(f) = (-1)^{\frac{5(5-1)}{2}} det(M) = det(M)$$

mit

$$M = \begin{pmatrix} 1 & -p & 0 & 0 & 0 & p & 0 & 0 & 0 \\ 0 & 1 & -p & 0 & 0 & 0 & p & 0 & 0 \\ 0 & 0 & 1 & -p & 0 & 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 & -p & 0 & 0 & 0 & p \\ 5 & -4p & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & -4p & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & -4p & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & -4p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & -4p & 0 & 0 & 0 \end{pmatrix}.$$

Es ist nun:

$$det(M) = det \begin{pmatrix} 1 & -p & 0 & 0 & 0 & p & 0 & 0 & 0 \\ 0 & 1 & -p & 0 & 0 & 0 & p & 0 & 0 \\ 0 & 0 & 1 & -p & 0 & 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 & -p & 0 & 0 & 0 & p \\ 0 & p & 0 & 0 & 0 & -5p & 0 & 0 & 0 \\ 0 & 5 & -4p & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & -4p & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & -4p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & -4p & 0 & 0 & 0 \end{pmatrix}$$

$$= det \begin{pmatrix} 1 & -p & 0 & 0 & 0 & p & 0 & 0 & 0 \\ 0 & 1 & -p & 0 & 0 & 0 & p & 0 & 0 \\ 0 & 0 & 1 & -p & 0 & 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 & -p & 0 & 0 & 0 & p \\ 0 & 0 & p^2 & 0 & 0 & -5p & -p^2 & 0 & 0 \\ 0 & 0 & p & 0 & 0 & 0 & -5p & 0 & 0 \\ 0 & 0 & 5 & -4p & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & -4p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & -4p & 0 & 0 & 0 \end{pmatrix}$$

$$= det \begin{pmatrix} 1 & -p & 0 & 0 & 0 & p & 0 & 0 & 0 \\ 0 & 1 & -p & 0 & 0 & 0 & p & 0 & 0 \\ 0 & 0 & 1 & -p & 0 & 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 & -p & 0 & 0 & 0 & p \\ 0 & 0 & 0 & p^3 & 0 & -5p & -p^2 & -p^3 & 0 \\ 0 & 0 & 0 & p^2 & 0 & 0 & -5p & -p^2 & 0 \\ 0 & 0 & 0 & p & 0 & 0 & 0 & -5p & 0 \\ 0 & 0 & 0 & 5 & -4p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & -4p & 0 & 0 & 0 \end{pmatrix}$$

$$= det \begin{pmatrix} 1 & -p & 0 & 0 & 0 & p & 0 & 0 & 0 \\ 0 & 1 & -p & 0 & 0 & 0 & p & 0 & 0 \\ 0 & 0 & 1 & -p & 0 & 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 & -p & 0 & 0 & 0 & p \\ 0 & 0 & 0 & 0 & p^4 & -5p & -p^2 & -p^3 & -p^4 \\ 0 & 0 & 0 & 0 & p^3 & 0 & -5p & -p^2 & -p^3 \\ 0 & 0 & 0 & 0 & p^2 & 0 & 0 & -5p & -p^2 \\ 0 & 0 & 0 & 0 & p & 0 & 0 & 0 & -5p \\ 0 & 0 & 0 & 0 & 5 & -4p & 0 & 0 & 0 \end{pmatrix}$$

$$= det \begin{pmatrix} 1 & -p & 0 & 0 \\ 0 & 1 & -p & 0 \\ 0 & 0 & 1 & -p \\ 0 & 0 & 0 & 1 \end{pmatrix} det \begin{pmatrix} p^4 & -5p & -p^2 & -p^3 & -p^4 \\ p^3 & 0 & -5p & -p^2 & -p^3 \\ p^2 & 0 & 0 & -5p & -p^2 \\ p & 0 & 0 & 0 & -5p \\ 5 & -4p & 0 & 0 & 0 \end{pmatrix}$$

$$= 5 \cdot det \begin{pmatrix} -5p & -p^2 & -p^3 & -p^4 \\ 0 & -5p & -p^2 & -p^3 \\ 0 & 0 & -5p & -p^2 \\ 0 & 0 & 0 & -5p \end{pmatrix} - (-4p) \cdot det \begin{pmatrix} p^4 & -p^2 & -p^3 & -p^4 \\ p^3 & -5p & -p^2 & -p^3 \\ p^2 & 0 & -5p & -p^2 \\ -p & 0 & 0 & -5p \end{pmatrix}$$

$$\begin{aligned} = \quad & 25 \cdot 125p^4 + 4p^5 \cdot det \begin{pmatrix} -5p & -p^2 & -p^3 \\ 0 & -5p & -p^2 \\ 0 & 0 & -5p \end{pmatrix} - 4p^4 \cdot det \begin{pmatrix} -p^2 & -p^3 & -p^4 \\ 0 & -5p & -p^2 \\ 0 & 0 & -5p \end{pmatrix} \\ & +4p^3 \cdot det \begin{pmatrix} -p^2 & -p^3 & -p^4 \\ -5p & -p^2 & -p^3 \\ 0 & 0 & -5p \end{pmatrix} + 4p^2 \cdot det \begin{pmatrix} -p^2 & -p^3 & -p^4 \\ -5p & -p^2 & -p^3 \\ 0 & -5p & -p^2 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} = \quad & 125 \cdot 25p^4 + 4p^5(-5p)^3 - 4p^4(-p^2)25p^2 + 4p^3p^4(-5p) \\ & -(-5p)^2(-p^3) + 4p^2(-p^2)^3 + 4p^2(-p^4)(-5p)^2 \\ & -4p^2(-5p)(-p^3)(-p^2) - 4p^2(-p^2)(-5p)(-p^3) \end{aligned}$$

$$
\begin{aligned}
= \quad & 25 \cdot 125p^4 - 20p^8 + 100p^8 - 20p^8 + 25p^5 - 4p^8 - 100p^8 \\
& +20p^8 + 20p^8 \\
= \quad & 25 \cdot 125p^4 + 25p^5 - 4p^8 \\
= \quad & 25p^4(125 + p) - 4p^8 \\
= \quad & p^4 \left[25(125 + p) - 4p^4\right].
\end{aligned}
$$

Sei nun $h(p) = 25(125 + p) - 4p^4$. Dann gilt:

- $h(3) = 2876 = 2^2 \cdot 719 \notin (\mathbb{Q}^*)^2$;
- $h(5) = 750 = 2 \cdot 3 \cdot 5^3 \notin (\mathbb{Q}^*)^2$;
- $h(7) = -6304 \notin (\mathbb{Q}^*)^2$.

Für alle $7 \leq p \in \mathbb{P}$ ist $h(p)$ negativ. Also ist $D(f)$ kein Quadrat in $\mathbb{Q}$.
Somit ist $Gal(f) \cong S_5$ oder F_{20}.
Wenn nun die Galoisgruppe einen 3er-Zykel enthält, dann ist $Gal(f) \cong S_5$, da F_{20} keine 3er-Zykel besitzt.
Es gilt:

$$
\begin{aligned}
X^5 - pX^4 + p \quad & \equiv \quad X^5 + X^4 + 1 \,(\mathrm{mod}\, 2) \\
& \equiv \quad \left(X^2 + X + 1\right)\left(X^3 + X + 1\right) \,(\mathrm{mod}\, 2).
\end{aligned}
$$

Nach Satz 1.17 enthält $Gal(f)$ einen Zykel mit Struktur (2,3).
Demnach besitzt $Gal(f)$ auch einen 3er-Zykel, da

- $(123)(12345) = (1352) \in Gal(f)$;
- $(123)(45)(1352) = (345) \in Gal(f)$.

Daraus folgt, dass $Gal(f) \cong S_5$ ist.

□

4.9 Satz:

Sei $p \in \mathbb{P}$. Dann besitzt das Polynom

$$f(X) = X^5 + p \in \mathbb{Q}[X]$$

als Galoisgruppe F_{20}.

Beweis:

Nach dem Eisensteinkriterium ist das Polynom $f(X) = X^5 + p$ irreduzibel über $\mathbb{Q}$.
Somit ist nach dem Satz von Weber (4.6) $Gal(f) \cong F_{20}$.

□

4.10 Satz:

Das Polynom

$$f(X) = X^5 + 5\left(5a^2 - 1\right)X - 4\left(5a^2 - 1\right) \in \mathbb{Q}[X]$$

mit $a \equiv 1 \pmod{21}$ besitzt als Galoisgruppe A_5.

Beweis:

Es gilt:

$$f(X) \equiv X^5 + 2X + 2 \pmod{3}.$$

Das Polynom $X^5 + 2X + 2$ ist irreduzibel in $\mathbb{F}_3[X]$.
Somit ist nach dem Lemma von Gauß das Polynom f irreduzibel über $\mathbb{Q}$.
Die Diskriminante ist

$$\begin{array}{rcc} D(f) & \overset{(1.15)}{=} & 5^5(-4)^4(5a^2-1)^4 + 4^4(5a^2-1)^5 * 5^5 \\ & = & (5a^2-1)^4 5^5 4^4 (1 + 5a^2 - 1) \\ & = & (5a^2-1)^4 5^6 4^4 a^2. \end{array}$$

Also ist $D(f)$ ein Quadrat in $\mathbb{Q}$. Weiter gilt:

$$\begin{array}{rcc} f(X) & \equiv & X^5 + 6X + 5 \pmod{7} \\ & \equiv & (X+4)(X+5)(X^3 + 5X^2 + 5X + 2) \pmod{7}. \end{array}$$

Nach Satz 1.17 beinhaltet $Gal(f)$ einen 3er-Zykel.
Da die Diskriminante ein Quadrat in $\mathbb{Q}$ ist, ist $Gal(f) \cong A_5$ oder D_5 oder C_5.
Die einzige dieser Gruppen, die einen 3er-Zykel enthält, ist A_5.
Deswegen ist $Gal(f) \cong A_5$.

□

Der folgende Satz ist aus [PaFa], aber die Bedingung für α ist verändert .

4.11 Satz:

Das Polynom $f(X) = X^5 + aX + b \in \mathbb{Q}[X]$ besitzt als Galoisgruppe D_5, falls

$$a = \frac{5\alpha^4}{4}\left(\beta^2+1\right)^2\left(\beta^2+\beta-1\right)\left(\beta^2-\beta-1\right)$$

und

$$b = \frac{\alpha^5}{2}\left(\beta^2+1\right)^3\left(\beta^2+\beta-1\right)(2\beta-1)(\beta+2)$$

ist, wobei $\alpha, \beta \in \mathbb{Q}$ mit $\beta \neq \frac{1}{2}, -2, \left(\beta^2+\beta-1\right) \in \mathbb{P}$ und $\alpha \neq 0$
mit $\alpha \neq \left(\beta^2+\beta-1\right)$.

Beweis:

Sei $f(X) = X^5 + aX + b \in \mathbb{Q}[X]$.
Nach dem Eisensteinkriterium $\left(p = (\beta^2 + \beta - 1) \in \mathbb{P}\right)$ ist $f(X)$ irreduzibel über $\mathbb{Q}$.
Die notwendigen und hinreichenden Bedingungen für $Gal(f) \cong D_5$ sind:

(i) $D(f) \overset{(1.15)}{=} 4^4a^5 + 5^5b^4 \in (\mathbb{Q}^*)^2$;

(ii) $f(X)$ ist auflösbar durch Radikale.

Die Notwendigkeit ist klar. Diese Bedingungen sind auch hinreichend, da aus (i) folgt, dass $Gal(f) \subseteq A_5$.
Bedingung (ii) schließt A_5 aus. Da $f(X) = 5X^4 + a$ zwei imaginäre Nullstellen besitzt, ist $Gal(f) \neq C_5$.
Also muss $Gal(f) \cong D_5$ sein.
Satz von Weber (4.6) besagt, dass $X^5 + aX + b$ auflösbar durch Radikale ist genau dann wenn a und b von der folgenden Form sind:

$$a = \frac{5^5\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)},\ b = \frac{5^5\lambda\mu^5}{(\lambda-1)^4(\lambda^2-6\lambda+25)}$$

mit $\lambda,\ \mu \in \mathbb{Q},\ \lambda \neq 1,\ \mu \neq 0$.
Setze

$$\lambda = 5\frac{u+1}{u-1} \text{ und } v = \frac{5\mu}{\lambda-1}.$$

Dadurch erhält man:

$$\begin{aligned}
a &= \frac{5^4\mu^4 5\lambda}{(\lambda-1)^4(\lambda^2-6\lambda+25)} \\
&= v^4\frac{25(u+1)}{(u-1)\left(25\frac{(u+1)^2}{(u-1)^2}-30\frac{(u+1)}{(u-1)}+25\right)} \\
&= \frac{5(u+1)}{5\frac{(u+1)^2}{(u+1)}-6(u+1)+5(u-1)}v^4 \\
&= \frac{5(u+1)(u-1)}{5(u+1)^2-6(u+1)(u-1)+5(u-1)^2}v^4 \\
&= \frac{5(u+1)(u-1)}{5u^2+10u+5-6u^2+6+5u^2-10u+5}v^4 \\
&= \frac{5(u+1)(u-1)}{4u^2+16}v^4 \\
&= \frac{5(u+1)(u-1)}{4(u^2+4)}v^4
\end{aligned}$$

und

$$
\begin{aligned}
b &= \frac{5^5\mu^5(\lambda-1)\lambda}{(\lambda-1)^5(\lambda^2-6\lambda+25)} \\
&= v^5\frac{5(u+1)\left(5\frac{(u+1)}{(u-1)}-1\right)(u-1)}{5(4u^2+16)} \\
&= \frac{(u+1)(u-1)(5u+5-u+1)}{(4u^2+16)(u-1)}v^5 \\
&= \frac{(u+1)(4u+6)}{4(u^2+4)}v^5 \\
&= \frac{2(u+1)(2u+3)}{4(u^2+4)}v^5 \\
&= \frac{(u+1)(2u+3)}{2(u^2+4)}v^5.
\end{aligned}
$$

Die Diskriminante von $f(X)$ ist dann gegeben durch:

$$
\begin{aligned}
D(f) &\overset{(1.15)}{=} 4^4a^5+5^5b^4 \\
&= 4^4\left(\tfrac{5}{4}\right)^5\frac{(u+1)^5(u-1)^5}{(u^2+4)^5}v^{20}+5^5\frac{(u+1)^4(2u+3)^4}{2^4(u^2+4)^4}v^{20} \\
&= \frac{5^5(u+1)^4\left[4(u+1)(u-1)^5+(2u+3)^4\left(u^2+4\right)\right]}{2^4(u^2+4)^5}v^{20} \\
&= \frac{5^5(u+1)^4\left(20u^6+80u^5+300u^4+600u^3+925u^2+880u+320\right)}{2^4(u^2+4)^5}v^{20} \\
&= \frac{5^6(u+1)^4\left(4u^6+16u^5+60u^4+120u^3+185u^2+176u+64\right)}{2^4(u^2+4)^5} \\
&= \frac{5^6(u+1)^4\left(2u^3+4u^2+11u+8\right)^2}{2^4(u^2+4)^5}v^{20}.
\end{aligned}
$$

Man sieht nun, dass $D(f)$ genau dann ein Quadrat ist, wenn u^2+4 ein Quadrat ist.
Wählt man

$$u=\beta-\frac{1}{\beta}\text{ und }v=\alpha\left(\beta^2+1\right),$$

dann ist

$$u^2+4=\beta^2-2+\frac{1}{\beta^2}+4=\beta^2+2+\frac{1}{\beta^2}=\left(\beta+\frac{1}{\beta}\right)^2.$$

Weiter erhählt man:

$$
\begin{aligned}
a &= \frac{5(u+1)(u-1)}{4(u^2+4)}v^4 \\
&= \frac{5}{4}\frac{\left(\beta-\frac{1}{\beta}+1\right)\left(\beta-\frac{1}{\beta}-1\right)}{\left(\beta-\frac{1}{\beta}\right)^2+4}\alpha^4\left(\beta^2+1\right)^4 \\
&= \frac{5\alpha^4}{4}\frac{\left(\beta-\frac{1}{\beta}+1\right)\left(\beta-\frac{1}{\beta}-1\right)\left(\beta^2+1\right)^4}{\frac{1}{\beta^2}\left(\beta^4+2\beta^2+1\right)} \\
&= \frac{5\alpha^4}{4}\frac{\beta^2\left(\beta-\frac{1}{\beta}+1\right)\left(\beta-\frac{1}{\beta}-1\right)\left(\beta^2+1\right)^4}{\left(\beta^2+1\right)^2} \\
&= \frac{5\alpha^4}{4}\left(\beta^2+1\right)^2\left(\beta^2+\beta-1\right)\left(\beta^2-\beta-1\right).
\end{aligned}
$$

und

$$
\begin{aligned}
b &= \frac{(u+1)(2u+3)}{2(u^2+4)}v^5 \\
&= \frac{\left(\beta-\frac{1}{\beta}+1\right)\left(2\beta-\frac{2}{\beta}+3\right)}{2\frac{1}{\beta^2}\left(\beta^2+1\right)^2}\alpha^5\left(\beta^2+1\right)^5 \\
&= \frac{\alpha^5}{2}\left(\beta^2+1\right)^3\left(\beta^2+\beta-1\right)\left(2\beta^2+3\beta-2\right) \\
&= \frac{\alpha^5}{2}\left(\beta^2+1\right)^3\left(\beta^2+\beta-1\right)(2\beta-1)(\beta+2).
\end{aligned}
$$

Somit ist $D(f)$ ein Quadrat in $\mathbb{Q}$ und nach dem Satz von Weber ist $f(X)$ auflösbar durch Radikale.
Also ist $Gal(f) \cong D_5$.

□

Kommen wir nun zu einem Beispiel für ein Polynom, das mit hoher Wahrscheinlichkeit C_5 als Galoisgruppe hat.

4.12 Beispiel:

Es sei

$$f(X) = X^5 - 10X^3 + 5X^2 + 10X + 1 \in \mathbb{Q}[X].$$

Es ist

$$f(X) \equiv X^5 + X^2 + 1 \pmod 2.$$

Das Polynom $X^5 + X^2 + 1$ ist irreduzibel in $\mathbb{F}_2[X]$.
Nach dem Lemma von Gauß ist $f(X)$ irreduzibel über $\mathbb{Q}$.
Nach Satz 1.12 gilt:

$$D(f) = (-1)^{\frac{5(5-1)}{2}} det(M) = det(M)$$

mit

$$M = \begin{pmatrix} 1 & 0 & -10 & 5 & 10 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -10 & 5 & 10 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -10 & 5 & 10 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -10 & 5 & 10 & 1 \\ 5 & 0 & -30 & 10 & 10 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & -30 & 10 & 10 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & -30 & 10 & 10 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 & -30 & 10 & 10 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & -30 & 10 & 10 \end{pmatrix}.$$

Also:

$$D(f) = det(M) = 5^8 7^2 \in (\mathbb{Q}^*)^2.$$

Betrachten wir nun die Weber-Resolvente von $f(X)$.
Für b_0, b_2 und b_4 aus (4.3) ergibt sich:

$$b_0 = 0,\ b_2 = 40000 \text{ und } b_4 = -500.$$

Daraus folgt:

$$\begin{aligned} G(Z) &= Z^6 - 1000Z^5 + 330000Z^4 - 40000000Z^3 \\ &\quad +1600000000Z^2 - 2^{10}5^87^2Z \\ &= Z(Z^5 - 1000Z^4 + 330000Z^3 - 40000000Z^2 \\ &\quad +1600000000Z - 2^{10}5^87^2). \end{aligned}$$

Somit ist $f(X)$ auflösbar durch Radikale.
Nach Korollar 4.5 ist $Gal(f) \cong D_5$ oder C_5.
Man sieht anhand von $D(f)$, dass 5 und 7 verzweigt sind.
Mit dem Computer-Programm PARI habe ich nun die Faktorisierung für die ersten 100 unverzweigten Primzahlen von $f(X)$ mod $p \in \mathbb{P} \setminus \{5, 7\}$ dargestellt.

p	Faktorisierung von $f(X)$ mod p
2	$X^5 + X^2 + 1$
3	$X^5 + 2X^3 + 2X^2 + X + 1$
11	$X^5 + X^3 + 5X^2 + 10X + 1$
13	$X^5 + 3X^3 + 5X^2 + 10X + 1$
17	$X^5 + 7X^3 + 5X^2 + 10X + 1$
19	$X^5 + 9X^3 + 5X^2 + 10X + 1$
23	$X^5 + 13X^3 + 5X^2 + 10X + 1$
29	$X^5 + 19X^3 + 5X^2 + 10X + 1$
31	$X^5 + 21X^3 + 5X^2 + 10X + 1$
37	$X^5 + 27X^3 + 5X^2 + 10X + 1$
41	$X^5 + 31X^3 + 5X^2 + 10X + 1$
43	$(X + 3)(X + 7)(X + 19)(X + 24)(X + 33)$
47	$X^5 + 37X^3 + 5X^2 + 10X + 1$
53	$X^5 + 43X^3 + 5X^2 + 10X + 1$
59	$X^5 + 49X^3 + 5X^2 + 10X + 1$
61	$X^5 + 51X^3 + 5X^2 + 10X + 1$
67	$X^5 + 57X^3 + 5X^2 + 10X + 1$
71	$X^5 + 61X^3 + 5X^2 + 10X + 1$
73	$X^5 + 63X^3 + 5X^2 + 10X + 1$
79	$X^5 + 69X^3 + 5X^2 + 10X + 1$
83	$X^5 + 73X^3 + 5X^2 + 10X + 1$
89	$X^5 + 79X^3 + 5X^2 + 10X + 1$
97	$X^5 + 87X^3 + 5X^2 + 10X + 1$
101	$(X + 24)(X + 36)(X + 63)(X + 83)(X + 97)$
103	$X^5 + 93X^3 + 5X^2 + 10X + 1$
107	$(X + 18)(X + 21)(X + 40)(X + 55)(X + 80)$
109	$X^5 + 99X^3 + 5X^2 + 10X + 1$
113	$X^5 + 103X^3 + 5X^2 + 10X + 1$
127	$X^5 + 117X^3 + 5X^2 + 10X + 1$
131	$X^5 + 121X^3 + 5X^2 + 10X + 1$
137	$X^5 + 127X^3 + 5X^2 + 10X + 1$
139	$X^5 + 129X^3 + 5X^2 + 10X + 1$
149	$(X + 16)(X + 91)(X + 100)(X + 104)(X + 136)$
151	$(X + 15)(X + 38)(X + 60)(X + 86)(X + 103)$
157	$(X + 6)(X + 52)(X + 54)(X + 88)(X + 114)$
163	$X^5 + 153X^3 + 5X^2 + 10X + 1$
167	$X^5 + 157X^3 + 5X^2 + 10X + 1$
173	$X^5 + 163X^3 + 5X^2 + 10X + 1$
179	$X^5 + 169X^3 + 5X^2 + 10X + 1$
181	$X^5 + 171X^3 + 5X^2 + 10X + 1$
191	$X^5 + 181X^3 + 5X^2 + 10X + 1$
193	$(X + 16)(X + 96)(X + 135)(X + 164)(X + 168)$
197	$X^5 + 187X^3 + 5X^2 + 10X + 1$

p	Faktorisierung von $f(X)$ mod p
199	$(X+27)(X+118)(X+138)(X+155)(X+159)$
211	$X^5+201X^3+5X^2+10X+1$
223	$X^5+213X^3+5X^2+10X+1$
227	$X^5+217X^3+5X^2+10X+1$
229	$X^5+219X^3+5X^2+10X+1$
233	$X^5+223X^3+5X^2+10X+1$
239	$X^5+229X^3+5X^2+10X+1$
241	$X^5+231X^3+5X^2+10X+1$
251	$(X+65)(X+155)(X+156)(X+181)(X+196)$
257	$(X+5)(X+26)(X+105)(X+143)(X+235)$
263	$X^5+253X^3+5X^2+10X+1$
269	$X^5+259X^3+5X^2+10X+1$
271	$X^5+261X^3+5X^2+10X+1$
277	$X^5+267X^3+5X^2+10X+1$
281	$X^5+271X^3+5X^2+10X+1$
283	$X^5+273X^3+5X^2+10X+1$
293	$(X+82)(X+95)(X+191)(X+223)(X+288)$
307	$(X+7)(X+20)(X+59)(X+100)(X+121)$
311	$X^5+301X^3+5X^2+10X+1$
313	$X^5+303X^3+5X^2+10X+1$
317	$X^5+307X^3+5X^2+10X+1$
331	$X^5+321X^3+5X^2+10X+1$
337	$X^5+327X^3+5X^2+10X+1$
347	$X^5+337X^3+5X^2+10X+1$
349	$(X+18)(X+38)(X+54)(X+270)(X+318)$
353	$X^5+343X^3+5X^2+10X+1$
359	$X^5+349X^3+5X^2+10X+1$
367	$X^5+357X^3+5X^2+10X+1$
373	$X^5+363X^3+5X^2+10X+1$
379	$X^5+369X^3+5X^2+10X+1$
383	$X^5+373X^3+5X^2+10X+1$
389	$X^5+379X^3+5X^2+10X+1$
397	$X^5+387X^3+5X^2+10X+1$
401	$(X+82)(X+120)(X+277)(X+345)(X+379)$
409	$X^5+399X^3+5X^2+10X+1$
419	$X^5+409X^3+5X^2+10X+1$
421	$X^5+411X^3+5X^2+10X+1$
431	$X^5+421X^3+5X^2+10X+1$
433	$X^5+423X^3+5X^2+10X+1$
439	$X^5+429X^3+5X^2+10X+1$
443	$(X+178)(X+209)(X+225)(X+349)(X+368)$
449	$(X+118)(X+128)(X+160)(X+190)(X+302)$
457	$(X+67)(X+303)(X+313)(X+340)(X+348)$

p	Faktorisierung von $f(X)$ mod p
461	$X^5 + 451X^3 + 5X^2 + 10X + 1$
463	$X^5 + 453X^3 + 5X^2 + 10X + 1$
467	$X^5 + 457X^3 + 5X^2 + 10X + 1$
479	$X^5 + 469X^3 + 5X^2 + 10X + 1$
487	$X^5 + 477X^3 + 5X^2 + 10X + 1$
491	$X^5 + 481X^3 + 5X^2 + 10X + 1$
499	$(X + 83)(X + 108)(X + 150)(X + 300)(X + 357)$
503	$X^5 + 493X^3 + 5X^2 + 10X + 1$
509	$X^5 + 499X^3 + 5X^2 + 10X + 1$
521	$X^5 + 511X^3 + 5X^2 + 10X + 1$
523	$X^5 + 513X^3 + 5X^2 + 10X + 1$
541	$X^5 + 531X^3 + 5X^2 + 10X + 1$
547	$X^5 + 537X^3 + 5X^2 + 10X + 1$
557	$(X + 187)(X + 259)(X + 345)(X + 360)(X + 520)$

Jetzt können wir Satz 1.17, Satz von Cebotarev und den χ^2-Anpassungstest anwenden.
Wir wählen uns nun als asymptotisches Niveau 0,5 %.
Es bezeichne

- n_1 die Anzahl der 5er-Zykel aus der Stichprobe mit Umfang $n = 100$;
- n_2 die Anzahl der (1,2,2)er-Zykel aus der Stichprobe;
- n_3 die Anzahl der (1,1,1,1,1)er-Zykel aus der Stichprobe.

Unsere Hypothese und Alternative lautet:
H: $v = (p_1^o,\, p_2^o,\, p_3^o) = (0,1;\, 0,5;\, 0,4)$, das heißt $Gal(f) \cong D_5$;
A: $v \neq (0,1; 0,5; 0,4)$, das heißt $Gal(f) \cong C_5$.
Aus der obigen Tabelle ergibt sich:

$$n_1 = 19,\ n_2 = 0 \text{ und } n_3 = 81.$$

Berechnen wir jetzt die Teststatistik:

$$\begin{aligned} T(x) &= \sum_{1 \le k \le 3} \frac{\left(n_k - np_k^0\right)^2}{np_k^0} \\ &= \frac{(19-100\cdot 0,1)^2}{100\cdot 0,1} + \frac{(0-100\cdot 0,5)^2}{100\cdot 0,5} + \frac{(81-100\cdot 0,4)^2}{100\cdot 0,4} \\ &= \frac{81}{10} + \frac{2500}{50} + \frac{41^2}{40} \\ &= 100,125. \end{aligned}$$

Aus der Tabelle mit den $(1-\alpha)$-Quantilen der χ^2-Verteilung von Seite 248 aus [Krengel] ergibt sich für das 99,5 % - Quantil der χ^2-Verteilung mit
2 Freiheitsgraden:

$$\chi^2_{2,\,0{,}995} = 10,60.$$

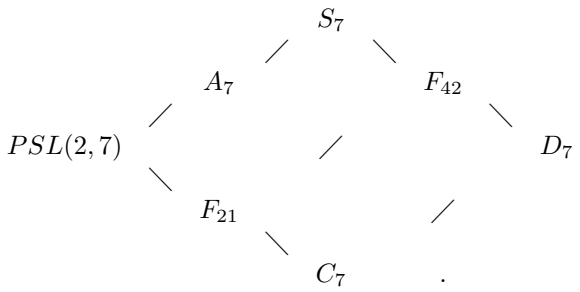
Also gilt:

$$T(x) = 100,125 > 10,60 = \chi^2_{2,\,0{,}995}.$$

Folglich verwerfen wir die Hypothese ($Gal(f) \cong D_5$) zum (asymptotischen) Niveau von 0,5 %.
Da nun 100,125 viel größer ist als 10,60, kann man ein noch viel kleineres Niveau α wählen als 0,5 %.
Das heißt mit sehr hoher Wahrscheinlichkeit ist $Gal(f) \cong C_5$.

4.13 Ausblick / Schlussbemerkung:

Für irreduzible Polynome höheren Grades über $\mathbb{Q}$ kann man immer mit Hilfe des Diskriminantenkriteriums (1.16) und Satz 1.17 die Galoisgruppe von unten abschätzen. Im Allgemeinen ist es sehr schwierig, die Galoisgruppe eines Polynoms vom Grad $n \geq 5$ über $\mathbb{Q}$, exakt zu bestimmen.
Für irreduzible Polynome 6.Grades über $\mathbb{Q}$ ist es allein deshalb so schwierig die Galoisgruppe zu ermitteln, weil es sehr viele transitiven Untergruppen in der symmetrischen Gruppe S_7 gibt. Allein S_3, S_4 und S_5 können schon als transitive Untergruppen interpretiert werden.
Betrachtet man sich die symmetrische Gruppe S_7, so stellt man fest, dass S_7 bis auf Konjugation nur sieben transitive Untergruppen besitzt.
Sei $\sigma = (1234567)$ und $\tau = (243756)$. Dann sind
S_7, A_7, $D_7 =< \sigma, \tau^3 >$, $F_{21} =< \sigma, \tau^2 >$, $F_{42} =< \sigma, \tau >$, $C_7 =< \sigma >$ und $PSL(2,7)$, die projektive spezielle linearen Gruppe der 2×2 Matrizen über $\mathbb{F}_7$, die transitiven Untergruppen von S_7. Das Gruppendiagramm sieht wie folgt aus:



Zur Abschätzung der Galoisgruppe eines irreduziblen Polynoms f mit Grad 7 über $\mathbb{Q}$ verwendet man zuerst das Diskriminantenkriterium. Man erhält

- $Gal(f) \cong A_7$, $PSL(2,7)$, F_{21} oder C_7, falls $D(f) \in (\mathbb{Q}^*)^2$;
- $Gal(f) \cong S_7$ oder F_{42} oder D_7, falls $D(f) \notin (\mathbb{Q}^*)^2$.

Nun verwendet man den Aspekt, dass C_7, , D_7, , F_{21} und F_{42} auflösbar sind. Dadurch erhält man eine weitere Abschätzung der Galoisgruppe:

- Falls f auflösbar durch Radikale ist und $D(f) \notin (\mathbb{Q}^*)^2$, dann ist $Gal(f) \cong F_{42}$ oder D_7;
- Falls f auflösbar durch Radikale ist und $D(f) \in (\mathbb{Q}^*)^2$, dann ist $Gal(f) \cong F_{21}$ oder C_7;
- Falls f nicht auflösbar durch Radikale ist und $D(f) \in (\mathbb{Q}^*)^2$, dann ist $Gal(f) \cong A_7$ oder $PSL(2,7)$;
- Falls f nicht auflösbar durch Radikale ist und $D(f) \notin (\mathbb{Q}^*)^2$, dann ist $Gal(f) \cong S_7$.

Wenn $Gal(f) \cong S_7$ ist, dann kann man dies durch diese Vorgehensweise exakt bestimmen. Für die anderen Möglichkeiten kann man Satz 1.17, den Satz von Cebotarev und den χ^2- Anpassungstest verwenden, um zumindest mit einer gewissen Wahrscheinlichkeit sagen zu können, welche Galoisgruppe f besitzt. Diese Methode sieht auf den ersten Blick nicht so schwierig aus, aber im Allgemeinen ist es sehr schwierig, zu entscheiden, ob ein Polynom 7.Grades auflösbar ist.
Abschließend möchte ich noch erwähnen, dass es einige Computeralgebra-Programme (z.B. PARI) gibt, mit denen man die Galoisgruppe eines Polynoms über $\mathbb{Q}$ bis zu einem bestimmten Grad berechnen kann.

Literaturverzeichnis

[GenPol]: C.U. Jensen, A. Ledet, N. Yui, Generic Polynomials: Constructive Aspects of the Inverse Galois Problem, Cambridge University Press, Mathematical Sciences Research Institute, 2002

[KaWa]: L.C. Kappe und B. Warren, An Elementary Test for the Galois Group of a Quartic Polynomial, The American Mathematical Monthly Vol 96, Nr. 2, Feb., 1989

[Krengel]: U. Krengel, Einführung in die Wahrscheinlichkeitstheorie und Statistik, vieweg-studium, 8. Auflage, 2005

[Lang]: S. Lang, Algebra, Revised Third Edition, Graduate Texts in Mathematics 211, Springer Verlag, 2002

[Lorenz]: F. Lorenz, F. Lemmermeyer, Algebra 1: Körper und Galoistheorie, HochschulTaschenbuch, Elsevier Spektrum Akademischer Verlag, 4. Auflage, 2007

[Matzat]: B. Heinrich Matzat, Konstruktive Galoistheorie, Lecture Notes in Mathematics 1284, Springer Verlag, 1987

[Neuk]: J. Neukirch, Algebraische Zahlentheorie, Springer Verlag, 2007

[PaFa]: G. Roland, N. Yui und D. Zagier, A Parametric Family of Quintic Polynomials with Galois Group D_5, Journal of Number Theory 15, 137-142 (1982)

[Pillot]: Rainer Schulze-Pillot, Einführung in die Algebra und Zahlentheorie, Springer-Verlag, 2008