Algebraische Körpererweiterung

1. Algebraische Körpererweiterung
2. $x^3 - x - 1 = 0$
3. Irreduzibles Polynom $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + x_0$
4. Irreduzibilitätsuntersuchung mit elementarsymm. Funktionen
5. Körper $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2 + x + 1)$
6. Körper $\mathbb{F}_8 = \mathbb{Z}_2[x]/(x^3 + x + 1)$
7. Lemma von Gauß
8. Eisenstein-Kriterium
9. Minimalpolynom
10. Endliche Körper
11. Beweisideen
12. Frobenius-Homomorphismus
13. Gradformel
14. Kreisteilungspolynome
15. Zerfällungskörper
16. Galois' Idee
17. Galois-Gruppe
18. Ordnung der Galois-Gruppe
19. Hauptsatz der Galois-Theorie, Radikalerweiterung
20. Zur Galois-Theorie
21. Minimalpolynome und Galois-Gruppe $\mathrm{Aut}(L\,|\,K)$
22. Galois-Gruppe $\mathrm{Gal}(L\,|\,\mathbb{Q})$
23. Galois-Gruppe von $f = x^4 + 1$
24. Zusammenhänge

↑ Algebraische Körpererweiterung $\mathbb{Q}^* = \mathbb{Q}(\alpha)$

In $\mathbb{Q}$ gibt es kein Element, dessen Quadrat 2 ist. Wir möchten in einem möglichst kleinen Zahlbereich $\mathbb{Q}^*$ mit $\mathbb{Q} \subset Q^*$ rechnen, in dem $x^2 - 2 = 0$ eine Lösung hat, sagen wir α, d. h. $\alpha^2 - 2 = 0$. Dass α die reelle Zahl $\alpha = \sqrt{2}$ ist, lassen wir mal außer acht, um das Allgemeine unserer Vorgehensweise zu erkennen. $\mathbb{Q}^*$ wird vermutlich aus den Elementen der Form $a + b\alpha$ mit $a, b \in \mathbb{Q}$ bestehen, da aus $\alpha^2 = 2 \quad \alpha^3 = 2\alpha$, $\alpha^4 = 4$, $\alpha^5 = 4\alpha$, usw. folgt. Die Potenzen von α liegen somit in $\mathbb{Q}^*$. Mit $\alpha^2 = 2$ sind auch die Verknüpfungen

$$\begin{aligned}(a + b\alpha) + (c + d\alpha) &= (a + c) + (b + d)\alpha \\ (a + b\alpha) \cdot (c + d\alpha) &= ac + ad\alpha + b\alpha c + bd\alpha^2 = (ac + 2bd) + (ad + bc)\alpha\end{aligned}$$

näher beschrieben, da in $\mathbb{Q}^*$ die uns vertrauten Rechenregeln (Assoziativ-, Kommutativ-, Distributivgesetz) gelten sollen.

$a + b\alpha$ erlaubt eine kürzere Schreibweise: $[a, b]$

Addition und Multiplikation nehmen dann die Form

$$\begin{aligned}[a, b] + [c, d] &= [a + c, b + d] \\ [a, b] \cdot [c, d] &= [ac + 2bd, ad + bc]\end{aligned}$$

an. Aus

$$\begin{aligned}[a, 0] + [c, 0] &= [a + c, 0] \\ [a, 0] \cdot [c, 0] &= [ac, 0]\end{aligned}$$

ist zu erkennen, dass mit den Paaren $[a, 0]$ genau so gerechnet werden kann wie in $\mathbb{Q}$.

Man kann daher das Paar $[a, 0]$ mit der rationalen Zahl a identifizieren. Demzufolge kann den Ausdrücken $a + [c, d]$ und $a \cdot [c, d]$ ein Sinn gegeben werden, nämlich

$$\begin{aligned}a + [c, d] &= [a, 0] + [c, d] = [a + c, d] \\ a \cdot [c, d] &= [a, 0] \cdot [c, d] = [ac, ad]\end{aligned}$$

Ein Element $[a, b]$ aus $\mathbb{Q}^*$ kann stets in der Form $[a, b] = [a, 0] + [0, b] = a \cdot [1, 0] + b \cdot [0, 1]$ geschrieben werden.
$[1, 0]$ ist mit der 1 zu identifizieren, $[0, 1]$ wegen $[0, 1]^2 = [2, 0] = 2$ mit α.
Mit $[a, b] = a + b\alpha$ schließt sich der Kreis.

$\mathbb{Q}^*$ ist somit auch ein 2-dimensionaler Vektorraum (das war allerdings schon eher zu sehen).

Werfen wir einen Blick auf die Division (die übrigen Körpergesetze können leicht verifiziert werden).

$$\frac{1}{a+b\alpha} = \frac{a-b\alpha}{(a+b\alpha)(a-b\alpha)} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\,\alpha \qquad \text{Nenner ungleich 0, da 2 irrational}$$

Alternativ kann das Gleichungssystem (a, b gegeben) $[a, b] \cdot [c, d] = [ac + 2bd, ad + bc] = [1, 0]$

$$\begin{aligned}ac + 2bd &= 1 \\ ad + bc &= 0 \quad \text{gelöst werden:} \qquad c = \frac{a}{a^2 - 2b^2},\ \ d = \frac{-b}{a^2 - 2b^2}\end{aligned}$$

$$\uparrow \quad x^3 - x - 1 = 0$$

Weiterführend ist der Euklidische Algorithmus.
Für z. B. $\frac{1}{1+\alpha}$ reicht eine Polynomdivision aus:

$$\begin{aligned} & \frac{\alpha^2-2}{\alpha+1} = \alpha - 1 - \frac{1}{1+\alpha} \\ \iff & (\alpha-1)(\alpha+1) - \underbrace{(\alpha^2-2)}_{0} = 1 \\ \iff & \frac{1}{1+\alpha} = \alpha - 1 \end{aligned}$$

Probe $\quad (\alpha-1)(\alpha+1) = \alpha^2 - 1 = 2 - 1 = 1$

Nun wagen wir uns etwas weiter vor. Wir möchten in einem möglichst kleinen Zahlbereich $\mathbb{Q}^\star$ mit $\mathbb{Q} \subset Q^\star$ rechnen, in dem $x^3 - x - 1 = 0$ eine Lösung hat, sagen wir β, d. h. $\beta^3 - \beta - 1 = 0$.
Dass β die reelle Zahl $\beta = \frac{\gamma^2+12}{6\gamma}$ mit $\gamma = (108+12\sqrt{69})^{1/3}$ ist, lassen wir außer acht.
Beim Rechnen ersetzen wir β^3 durch $\beta + 1$, β^4 durch $\beta^2 + \beta$, β^5 durch $\beta^3 + \beta^2$, also durch $\beta^2 + \beta + 1$, usw.
$\mathbb{Q}^\star$ wird vermutlich aus den Elementen der Form $a\beta^2 + b\beta + c$ mit $a, b, c \in \mathbb{Q}$ bestehen und ein 3-dimensionaler Vektorraum mit der Basis $\{1, \beta, \beta^2\}$ sein.

Aus algebraischer Sicht werden den Elementen des Polynomrings $\mathbb{Q}[\beta]$ Nullelemente $(\beta^3 - \beta - 1) \cdot p(\beta)$ mit $p(\beta) \in \mathbb{Q}[\beta]$ hinzugefügt. Es entsteht der Restklassenring $\mathbb{Q}(\beta) = \mathbb{Q}[\beta]/(\beta^3 - \beta - 1)$. Diese Sichtweise lassen wir hier außer Acht.

β^{-1} kann leicht ermittelt werden:

$$\begin{aligned} \beta^3 - \beta - 1 &= 0 \\ \beta^3 - \beta &= 1 \\ \underbrace{(\beta^2-1)}_{\beta^{-1}}\beta &= 1 \end{aligned}$$

$$\begin{aligned} \beta^n + \ldots + a_1\beta + a_0 &= 0 \qquad \text{allgemein} \\ (\beta^{n-1} + \ldots + a_1\beta)\beta &= -a_0 \\ \underbrace{\frac{1}{a_0}(-\beta^{n-1} - \ldots - a_1\beta)}_{\beta^{-1}}\beta &= 1 \end{aligned}$$

Wie erfolgt die Division, z. B. $\frac{1}{\beta^2+1}$?

$$\begin{aligned} \text{Der Euklidische Algorithmus liefert} \quad \beta^3 - \beta - 1 &= \beta(\beta^2+1) + (-2\beta - 1) \\ \beta^2 + 1 &= (-\tfrac{1}{2}\beta + \tfrac{1}{4})(-2\beta - 1) + \tfrac{5}{4} \end{aligned}$$

$$\begin{aligned} \tfrac{4}{5}(\beta^2+1) - \tfrac{4}{5}(-\tfrac{1}{2}\beta + \tfrac{1}{4})(-2\beta - 1) &= 1 \\ \tfrac{4}{5}(\beta^2+1) + (\tfrac{2}{5}\beta - \tfrac{1}{5})[(\beta^3 - \beta - 1) - \beta(\beta^2+1)] &= 1 \\ (-\tfrac{2}{5}\beta^2 + \tfrac{1}{5}\beta + \tfrac{4}{5})(\beta^2+1) + (\tfrac{2}{5}\beta - \tfrac{1}{5})\underbrace{[(\beta^3 - \beta - 1)]}_{0} &= 1 \\ \iff \quad \frac{1}{\beta^2+1} &= -\tfrac{2}{5}\beta^2 + \tfrac{1}{5}\beta + \tfrac{4}{5} \end{aligned}$$

Mit Maple gelangt man zum selben Ergebnis.

$p := x^3 - x - 1;$
$q := x^2 + 1;$
$gcdex(p, q, x, 'f', 'g');$
$'f' = f : 'g' = g :$
$f * p + g * q = 1;$
$expand(f * p + g * q);$

Mit

$$\begin{aligned}
(a + b\beta + c\beta^2) + (u + v\beta + w\beta^2) &= (a + d) + (b + e)\beta + (c + f)\beta^2 \\
(a + b\beta + c\beta^2) \cdot (u + v\beta + w\beta^2) &= au + bu\beta + av\beta + cu\beta^2 + bv\beta^2 + aw\beta^2 + cv\beta^3 + bw\beta^3 + cw\beta^4 \\
&\qquad\qquad \mid \beta^3 = \beta + 1,\ \ \beta^4 = \beta^2 + \beta \\
&= au + bw + cv + av\beta + bu\beta + bw\beta + cv\beta + cw\beta \\
&\qquad + aw\beta^2 + bv\beta^2 + cu\beta^2 + cw\beta^2
\end{aligned}$$

und der kürzeren Schreibweise $[a, b, c]$ für $a + b\beta + c\beta^2$

nehmen Addition und Multiplikation die folgende Form an:

$$\begin{aligned}
[a, b, c] + [u, v, w] &= [a + u, b + v, c + w] \\
[a, b, c] \cdot [u, v, w] &= [au + bw + cv, av + bu + bw + cv + cw, aw + bv + cu + cw]
\end{aligned}$$

z. B. gilt

$$\begin{aligned}
[0, 1, 0] \cdot [0, 1, 0] &= [0, 0, 1] \\
[0, 0, 1] \cdot [0, 0, 1] &= [0, 1, 1] \qquad \text{beachte } \beta^4 = \beta^2 + \beta
\end{aligned}$$

Die Division kann wieder mit Hilfe eines Gleichungssystems (a, b, c gegeben)

$$[a, b, c] \cdot [u, v, w] = [au + bw + cv, av + bu + bw + cv + cw, aw + bv + cu + cw] = [1, 0, 0]$$

$$\begin{aligned}
au + bw + cv &= 1 \\
av + bu + bw + cv + c &= 0 \\
aw + bv + cu + cw &= 0 \quad \text{erfolgen.}
\end{aligned}$$

Wir erhalten schon Bekanntes in anderer Darstellung.

$[1, 0, 1] \cdot \frac{1}{5}[4, 1, -2] = [1, 0, 0]$

↑ Irreduzibles Polynom $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + x_0$

Damit bei der Körpererweiterung die inversen Elemente mit dem Euklidischen Algorithmus bestimmt werden können, ist es hinreichend (und notwendig), dass das Polynom $f(x) = x^3 - x - 1$ irreduzibel ist, d. h. nicht in ein Produkt von Polynomen vom Grad ≥ 1 zerlegbar ist. Um die Irreduzibilität eines Polynoms $f(x)$ mit ganzzahligen Koeffizienten in $\mathbb{Q}$ nachzuweisen, reicht der Nachweis in $\mathbb{Z}$ aus (Lemma von Gauß). Jedes Polynom vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstelle in $\mathbb{Z}$ hat. Liegt die Nullstelle a vor, kann der Linearfaktor $(x - a)$ abgespalten werden. Für ein normiertes Polynom ($a_n = 1$) ist jede rationale Nullstelle eine ganze Zahl, die a_0 teilt. Für $f = x^3 - x - 1$ sind die Teiler ± 1 von a_0 keine Nullstellen, f ist irreduzibel.

Nullstellen-Kriterium.
Es sei $f(x) \in \mathbb{Q}[x]$ vom Grad 2 oder 3. Dann gilt:
$f(x)$ ist irreduzibel über $\mathbb{Q} \iff f(x)$ hat keine Nullstelle in $\mathbb{Q}$.

Beachte: Das Polynom $x^4 + 2x^2 + 1$ hat keine Nullstellen, zerfällt aber in $(x^2 + 1)(x^2 + 1)$.

Lemma von Gauß (2 Versionen)
Sei $f(x) \in \mathbb{Z}[x]$ ein irreduzibles Polynom über $\mathbb{Z}$. Dann ist $f(x)$ auch irreduzibel über $\mathbb{Q}$.

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

Um die Irreduzibilität eines Polynoms nachzuweisen, gibt es weitere Möglichkeiten.

Modulo-Kriterium
Seien $f \in \mathbb{Z}[x]$ mit $a_n \neq 0$ und eine Primzahl p gegeben mit $a_n \neq 0 \pmod p$. Es bezeichne $\overline{f}(x) = \overline{a}_n x^n + \ldots + \overline{a}_1 x + \overline{a}_0$ das Polynom über $\mathbb{Z}_p$ ($\overline{f}$ hat den gleichen Grad wie f).
Dann gilt: $\overline{f}(x)$ ist irreduzibel über $\mathbb{Z}_p \implies f(x)$ ist irreduzibel über $\mathbb{Z}$.

Koeffizientenvergleich
Eine Zerlegung $x^4 + 1 = (x^2 + ax \pm 1)(x^2 + bx \pm 1)$ in quadratische Faktoren für $a, b \in \mathbb{Z}$ ist nicht möglich. Dies zeigt ein Koeffizientenvergleich.

$$\begin{aligned} (x^2 + ax + 1)(x^2 + bx + 1) &= x^4 + (a+b)x^3 + (ab+2)x^2 + (a+b)x + 1 \implies b = -a \\ &= x^4 + (2 - a^2)x^2 + 1 \\ \implies \qquad a^2 &= 2 \end{aligned}$$

$$\begin{aligned} (x^2 + ax - 1)(x^2 + bx - 1) &= x^4 + (a+b)x^3 + (ab-2)x^2 - (a+b)x + 1 \implies b = -a \\ &= x^4 - (2 + a^2)x^2 + 1 \\ \implies \qquad a^2 &= -2 \end{aligned}$$

Irreduzibilitätskriterium von Eisenstein
$2x^3 + 15x^2 + 18x - 6$ ist irreduzibel nach diesem Kriterium mit der Primzahl $p = 3$.
p teilt alle Koeffizienten außer dem höchsten a_n. p^2 teilt nicht den konstanten Summanden a_0.

$f(x)$ ist irreduzibel $\iff f(x + a)$ ist irreduzibel.
In $f(x) = x^4 + 1$ setze man $x = y + 1$ und wähle $p = 2$.
Es ist nicht nötig, etwas aufzuschreiben.

↑ Irreduzibles Polynom $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + x_0$

Zum Modulo-Kriterium
Die Koeffizienten eines Polynoms f über $\mathbb{Z}$ werden modulo einer geeigneten Primzahl p reduziert, so dass der Grad erhalten bleibt (für normierte Polynome bleibt der Grad stets unverändert). Für $\overline{f}$ muss gezeigt werden, dass in $\mathbb{Z}_p$ keine Nullstelle und auch keine Zerlegung existiert.
$f(x) = x^3 - 3x^2 + 2x - 3$ ist irreduzibel, da seine Reduktion $x^3 + x^2 + 1$ modulo 2 irreduzibel über $\mathbb{Z}_2$ ist (keine Nullstelle, $\overline{f}(0) = 1$, $\overline{f}(1) = 1$).

Nullstellen-Kriterium.
Es sei $\overline{f}(x) \in \mathbb{Z}_p[x]$ vom Grad 2 oder 3. Dann gilt:
$\overline{f}(x)$ ist irreduzibel über $\mathbb{Z}_p \iff \overline{f}(x)$ hat keine Nullstelle in $\mathbb{Z}_p$.

Ein Polynom f vom Grad 4 kann in Produkte mit Polynomen vom Grad 1 (und 3) und vom Grad 2 (und 2) zerfallen.
Das einzige irreduzible Polynom vom Grad 2 in $\mathbb{Z}_2$ ist $x^2 + x + 1$. Bleibt bei der Polynomdivision in $\mathbb{Z}_2$ von $\overline{f}$ mit diesem Polynom ein Rest und hat $\overline{f}$ keine Nullstelle, so ist f irreduzibel.

Ein Polynom f vom Grad 5 kann in Produkte mit Polynomen vom Grad 1 (und 4) und vom Grad 2 (und 3) zerfallen.
Die irreduziblen Polynome vom Grad 2 in $\mathbb{Z}_3$ sind: $x^2 + 1$, $x^2 + x - 1$, $x^2 - x - 1$.
Bleibt bei den Polynomdivisionen in $\mathbb{Z}_3$ von $\overline{f}$ mit jeweils einem dieser Polynome stets ein Rest und hat $\overline{f}$ keine Nullstelle, so ist f irreduzibel.

Die Verwendung eines Computer-Algebra-Systems kann sehr nützlich sein.

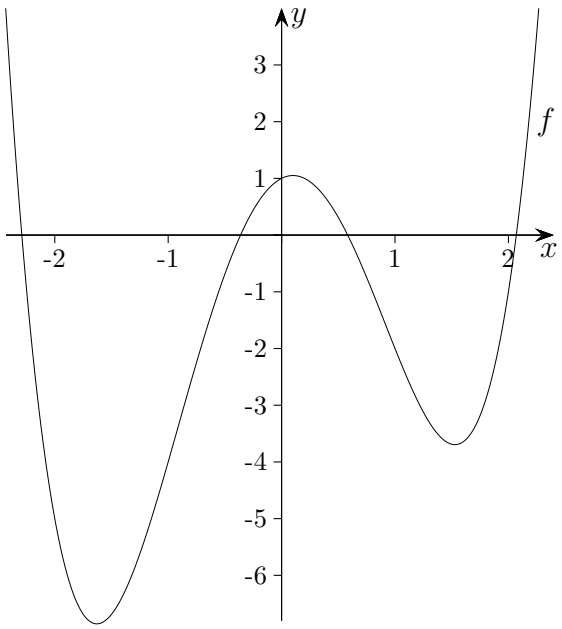
WolframAlpha erzeugt mit der Anweisung factor $x^2 + 2 \bmod 3$ $\quad (x + 2)(x + 1)$.

↑ Irreduzibilitätsuntersuchung mit elementarsymmetrischen Funktionen

Das Polynom $x^2 - 3x + 1$ hat die Nullstellen (genähert, CAS) $x_1 = 0{,}382$ und $x_2 = 2{,}618$.

$$x^2 - 3x + 1 = (x - x_1)(x - x_2)$$

Da x_1 (x_2) offensichtlich nicht aus $\mathbb{Z}$ ist, ist das Polynom irreduzibel.



$f = x^4 - 5x^2 + x + 1$ hat die Nullstellen (genähert) $x_1 = -2{,}290$, $x_2 = -0{,}362$, $x_3 = 0{,}583$, $x_4 = 2{,}070$.
Da diese offensichtlich nicht aus $\mathbb{Z}$ sind, lässt sich kein Linearfaktor abspalten.

$$\begin{aligned}
x^4 - 5x^2 + x + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\
(x^2 + px + q) &= (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2 \\
\text{oder} \quad (x^2 + px + q) &= (x - x_1)(x - x_3) = x^2 - (x_1 + x_3)x + x_1x_3 \\
\text{oder} \quad (x^2 + px + q) &= (x - x_1)(x - x_4) = x^2 - (x_1 + x_4)x + x_1x_4
\end{aligned}$$

Es reicht zu zeigen, dass diese Zerlegungen nicht möglich sind. Die Übrigen sind zu den Angegebenen komplementär.

$$\begin{aligned}
x_1 + x_2 &= -2{,}652 & x_1x_2 &= 0{,}829 \\
x_1 + x_3 &= -1{,}707 & x_1x_3 &= -1{,}335 \\
x_1 + x_4 &= -0{,}223 & x_1x_4 &= -4{,}733
\end{aligned}$$

Damit das Polynom f keinen Faktor vom Grade 2 über den rationalen Zahlen zulässt, ist es hinreichend, dass in jeder Zeile mindestens eine nichtganze Zahl auftaucht. Die Rechnung hätte also verkürzt werden können. f ist somit irreduzibel.

↑ Körper $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$

Das einzige irreduzible Polynom vom Grad 2 in $\mathbb{Z}_2$ ist x^2+x+1. Die Elemente der algebraischen Körpererweiterung für $\alpha^2+\alpha+1=0$ sind $a+b\alpha$ mit $a,b\in\{0,1\}$, somit sind die $2^2=4$ Elemente von $\mathbb{Z}_2(\alpha)$ $\{0,1,\alpha,\alpha+1\}$ ($\alpha^2+\alpha+1=0$, auf beiden Seiten $\alpha+1$ addieren: $\alpha^2=\alpha+1$). Basis des 2-dim. Vektorraums ist $\{1,\alpha\}$. Die Verknüpfungen lauten:

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Im allgemeinen muss man zwischen einem Polynom und der zugehörigen Polynomfunktion unterscheiden. Für die Polynome $f=x+1$ und $g=x^3+x^2+x+1$ über $\mathbb{F}_2$ gilt $f(0)=g(0)=1$ und $f(1)=g(1)=0$. Für die verschiedenen Polynome sind die Polynomfunktionen $f,g\colon \mathbb{F}_2\to\mathbb{F}_2$ also gleich. Polynome werden daher ohne Bezug auf Polynomfunktionen definiert. Es sei R ein Ring. Der Polynomring $R[x]$ besteht aus Ausdrücken der Form $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, $a_i\in R$, mit der Addition und Multiplikation …

↑ Körper $\mathbb{F}_8 = \mathbb{Z}_2[x]/(x^3+x+1)$

Die einzigen irreduziblen normierten Polynom vom Grad 3 in $\mathbb{Z}_2$ sind x^3+x+1 und x^3+x^2+1. Die Elemente der algebraischen Körpererweiterung für $\alpha^3+\alpha+1=0$ sind $a+b\alpha+c\alpha^2$ mit $a,b,c\in\{0,1\}$ $(\alpha^4=\alpha\cdot\alpha^3=\alpha(\alpha+1)=\alpha^2+\alpha)$.
Somit sind die $2^3=8$ Elemente von $\mathbb{Z}_2(\alpha)$ $\{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$.
Dies sind die möglichen Reste vom Grad $n<3$ bei Division eines Polynoms durch x^3+x+1.
Basis des 3-dim. Vektorraums ist $\{1,\alpha,\alpha^2\}$. Die Verknüpfungen lauten:

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

$$\alpha^2(\alpha^2+1) = \alpha^2+\alpha+\alpha^2=\alpha$$
$$\alpha^2(\alpha^2+\alpha) = \alpha^2+\alpha+\alpha+1=\alpha^2+1$$

↑ Lemma von Gauß

Sei $f(x) \in \mathbb{Z}[x]$ ein irreduzibles Polynom über $\mathbb{Z}$. Dann ist $f(x)$ auch irreduzibel über $\mathbb{Q}$.

Beweis
Sei $f(x) \in \mathbb{Z}[x]$ ein irreduzibles Polynom über $\mathbb{Z}$. Wir nehmen an, dass eine nicht-triviale Zerlegung $f = g \cdot h$ über $\mathbb{Q}$ existiert, d. h. $g, h \in \mathbb{Q}[x]$ sind nicht-konstante Polynome, und multiplizieren beide Seiten von $f = g \cdot h$ mit dem Produkt n der Nenner der Koeffizienten von g und h, Ergebnis $nf = g^\star \cdot h^\star$.
Sei p ein Primfaktor von n. Wir zeigen, dass p alle Koeffizienten von $g^\star$ oder von $h^\star$ teilt. Nach Kürzung des Faktors p wird n verkleinert. Das Argument wird wiederholt angewendet bis $n = 1$ ist. Damit liegt eine nicht-triviale Zerlegung von f über $\mathbb{Z}$ vor, im Widerspruch zur Irreduzibilität f über $\mathbb{Z}$.

$$\begin{aligned} g^\star &= g_0 + g_1x + g_2x^2 + g_3x^3 + \cdots + g_sx^s \\ h^\star &= h_0 + h_1x + h_2x^2 + h_3x^3 + \cdots + h_sx^t \end{aligned}$$

$$\begin{aligned} g^\star h^\star &= c_0 + c_1x + c_2x^2 + c_3x^3 + \cdots + c_{s+t}x^{s+t} \\ &= g_0h_0 + (g_0h_1 + g_1h_0)x + (g_0h_2 + g_1h_1 + g_2h_0)x^2 + (g_0h_3 + g_1h_2 + g_2h_1 + g_3h_0)x^3 + \cdots \end{aligned}$$

$p \,|\, g_0h_0 \quad \Longrightarrow \quad p \,|\, g_0$ oder $p \,|\, h_0$
$p \,|\, g_0h_1 + g_1h_0$ und $p \,|\, g_0 \quad \Longrightarrow \quad p \,|\, g_1$ oder $p \,|\, h_0$
$p \,|\, g_0h_1 + g_1h_0$ und $p \,|\, h_0 \quad \Longrightarrow \quad p \,|\, g_0$ oder $p \,|\, h_1$, usw.

Indirekte Annahme
Seien i und j minimal mit $p \nmid g_i$ und $p \nmid h_j$.

$$c_{i+j} = \sum_{k=0}^{i+j} g_k h_{i+j-k} = g_0h_{i+j} + g_1h_{i+j-1} + \cdots + g_ih_j + g_{i+1}h_{j-1} + \cdots + g_{i+j}h_0$$

p teilt jeden Summanden außer g_ih_j.
Dies liefert einen Widerspruch, da p außerdem c_{i+j} teilt.

Schlankere Argumentation
Sei p ein Primfaktor von n.
Wir betrachten die Gleichung $nf = g^\star \cdot h^\star$ in $\mathbb{Z}_p[x]$, d. h. alle Koeffizienten der Polynome werden modulo p reduziert. Das ergibt $\overline{0} = \overline{g^\star} \cdot \overline{h^\star}$.
Da $\mathbb{Z}_p[x]$ als Polynomring über einem Körper ein Integritätsring (nullteilerfrei) ist, ist dies nur möglich, wenn bereits einer der Faktoren gleich null ist. Dies bedeutet aber gerade, dass alle Koeffizienten von $g^\star$ oder $h^\star$ durch p teilbar sind.

↑ Eisenstein-Kriterium

Sei $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ und p eine Primzahl, sodass

a) $p \nmid a_n$
b) $p \mid a_i, \qquad i = 0, \ldots, a_{n-1}$
c) $p^2 \nmid a_0$

Dann ist f irreduzibel über $\mathbb{Q}$.

Beweis
Es reicht zu zeigen, dass f irreduzibel über $\mathbb{Z}$ ist. Wir nehmen an, dass $f = g \cdot h$,
$g = \sum_{i=0}^{s} g_i x^i \in \mathbb{Z}[x]$ und $h = \sum_{j=0}^{t} h_j x^j \in \mathbb{Z}[x]$ sind nicht-konstante Polynome.
Es gilt $a_0 = g_0 h_0$. Da $p \mid a_0$ und $p^2 \nmid a_0$, schließen wir, dass entweder $p \mid g_0$ oder $p \mid h_0$.
OBdA dürfen wir annehmen, dass $p \mid g_0$ und $p \nmid h_0$.
a) impliziert, dass p nicht alle Koeffizienten von g teilt. Sei i minimal mit $p \nmid g_i$.
Da $s = \mathrm{Grad}(g) < \mathrm{Grad}(f) = n$ ist, folgt $i < n$.
Nach b) ist p ein Teiler von a_i. Die Primzahl p teilt auch alle Terme der rechten Seite von

$$a_i = \sum_{k=0}^{i} g_k h_{i-k} = g_0 h_i + g_1 h_{i-1} + \cdots + g_i h_0 \text{ außer } g_i h_0.$$

Dies liefert einen Widerspruch. f ist somit irreduzibel über $\mathbb{Z}$.

Das Eisenstein-Kriterium mit $p = 2$ zeigt, dass $x^n - 2 \in \mathbb{Q}[x]$
für alle n irreduzibel ist.

Beweisidee veranschaulicht, $n = 5$:

$$\begin{aligned} g &= g_0 + g_1 x + g_2 x^2 \\ h &= h_0 + h_1 x + h_2 x^2 + h_3 x^3 \end{aligned}$$

$$\begin{aligned} gh &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 \\ &= g_0 h_0 + (g_0 h_1 + g_1 h_0) x + (g_0 h_2 + g_1 h_1 + g_2 h_0) x^2 + (g_0 h_3 + g_1 h_2 + g_2 h_1 + g_3 h_0) x^3 + \cdots + (\quad) x^5 \end{aligned}$$

Sei $i = 1$
$p \mid g_0 h_0 \overset{\text{OBdA}}{\Longrightarrow} p \mid g_0$ und $p \nmid h_0$,
$p \mid g_0 h_1 + g_1 h_0$ und $p \mid g_0 \implies p \mid g_1 \quad \lightning$

Sei $i = 2$
$p \mid g_0,\ p \mid g_1,\ p \mid g_0 h_2 + g_1 h_1 + g_2 h_0,\ p \nmid h_0 \implies p \mid g_2 \quad \lightning$
usw.

↑ Minimalpolynom

Sei L eine Körpererweiterung von K und $f \in K[x]$ ein normiertes Polynom kleinsten Grades mit der Nullstelle $\alpha \in L$. f heißt das Minimalpolynom $\mathrm{m}_{\alpha,K}$ von α bezüglich des Körpers K.

Ein Minimalpolynom muss irreduzibel über K sein, ansonsten wäre $\mathrm{m}_{\alpha,K}(x) = u(x)v(x)$ und $\mathrm{m}_{\alpha,K}(\alpha) = u(\alpha)v(\alpha) = 0$. Somit wäre $u(\alpha) = 0$ oder $v(\alpha) = 0$, im Widerspruch zur Annahme, dass $\mathrm{m}_{\alpha,K}$ minimal ist.

Für jedes Polynom $g \in K[x]$ mit $g(\alpha) = 0$ gilt: $\mathrm{m}_{\alpha,K} | g$

Indem wir das Polynom g durch $f = \mathrm{m}_{\alpha,K}$ teilen, erhalten wir $g(x) = f(x)q(x) + r(x)$ mit $\deg(r) < \deg(f)$. Dann gilt $r(\alpha) = g(\alpha) - f(\alpha)q(\alpha) = 0$. Wegen der Minimalität von $f(x)$ kann dies nur für $r(x) \equiv 0$ sein. Also ist $\mathrm{m}_{\alpha,K} | g$.

Falls ein Minimalpolynom von α existiert, ist es eindeutig bestimmt, und das Element α heißt algebraisches Element der Erweiterung L.

Ein irreduzibles, normiertes Polynom $h \in K[x]$ mit $h(\alpha) = 0$ ist das Minimalpolynom von α. Denn: h wird - wie wir gerade gesehen haben - von $\mathrm{m}_{\alpha,K}$ geteilt. h ist jedoch irreduzibel, beide Polynome sind normiert, nur $f = h$ verbleibt. Vielfach: $K = \mathbb{Q}$, $K = \mathbb{Q}(\beta)$

1. Sei $\sqrt{a} \notin \mathbb{Q}$, dann ist das zugehörige Minimalpolynom $x^2 - a$.

2. Minimalpolynom von $\alpha = \sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$

$$\begin{aligned} \alpha^2 &= 2 + 2\sqrt{6} + 3 \\ \alpha^2 - 5 &= 2\sqrt{6} \qquad\qquad |(\ )^2 \\ \alpha^4 - 10\alpha^2 + 25 &= 24 \\ \alpha^4 - 10\alpha^2 + 1 &= 0 \end{aligned}$$

Damit ist $\sqrt{2} + \sqrt{3}$ Nullstelle des normierten Polynoms $x^4 - 10x^2 + 1$. Dieses Polynom hat keine Nullstellen in $\mathbb{Q}$ (es wären die Teiler von 1) und ist auch nicht quadratisch zerlegbar, siehe Koeffizientenvergleich.

3. Minimalpolynom von $\alpha = \sqrt{2 + \sqrt{2}}$ über $\mathbb{Q}$

$$\begin{aligned} \alpha^2 &= 2 + \sqrt{2} \\ \alpha^2 - 2 &= \sqrt{2} \qquad |(\ )^2 \\ \alpha^4 - 4\alpha^2 + 4 &= 2 \\ \alpha^4 - 4\alpha^2 + 2 &= 0 \end{aligned}$$

Damit ist $\sqrt{2 + \sqrt{2}}$ Nullstelle des normierten Polynoms $f = x^4 - 4x^2 + 2$.
Dieses Polynom ist irreduzibel, Eisenstein, $p = 2$.

Nebenbei: In $\mathbb{Q}(\sqrt{2})$ ist f reduzibel, $f = (x^2 - 2 - \sqrt{2})(x^2 - 2 + \sqrt{2})$.

Die Basis von $\mathbb{Q}(\alpha)$ ist $\{1, \alpha, \alpha^2, \alpha^3\}$,

$$\begin{aligned} \alpha^{-1} &= ? \\ \alpha^4 - 4\alpha^2 &= -2 \\ -\alpha^4/2 + 2\alpha^2 &= 1 \\ -\alpha^3/2 + 2\alpha &= 1/\alpha \end{aligned}$$

↑ Endliche Körper

1. Satz von Lagrange

   1) Ist H eine Untergruppe von G, so ist $|H|$ ein Teiler von $|G|$.
   2) Insbesondere wird $|G|$ von der Ordnung von $a \in G$ geteilt.

2. Jeder endliche Körper enthält als kleinsten Teilkörper (Primkörper) $\mathbb{Z}_p$ für eine Primzahl p.

3. Ein endlicher Körper hat $q = p^n$ Elemente für eine Primzahl p und $n \in \mathbb{N}$.
   Die Anzahl ist also immer eine Primzahlpotenz. Seine Charakteristik ist p.

4. Jedes Element $a \in \mathbb{F}_q$ erfüllt die Gleichung $x^q - x = 0$.
   Dieses Polynom zerfällt in Linearfaktoren über $\mathbb{F}_q$.

5. Für ein Polynom $f = \sum_{k=0}^{n} a_k x^k \in K[x]$ über einem Körper K betrachten wir die formale Ableitung $f' = \sum_{k=1}^{n} k a_k x^{k-1}$. Für diese gilt:

   1) $(f+g)' = f' + g'$ und $(fg)' = f'g + fg'$.
   2) Sind f und f' teilerfremd, so hat f keine mehrfachen Nullstellen.
   3) Eine mehrfache Nullstelle von f ist auch Nullstelle von f'.
      $f = (x-a)^k h \quad \Longrightarrow \quad f' = k(x-a)^{k-1}h + (x-a)^k h'$

6. Für $a, b \in \mathbb{F}_q$ mit $q = p^n$ gilt $(a+b)^p = a^p + b^p$.

7. Für p Primzahl und $n \in \mathbb{N}$ existiert ein Körper mit $q = p^n$ Elementen.

8. Die multiplikative Gruppe $\mathbb{F}_q^*$ eines endlichen Körpers $\mathbb{F}_q$ ist eine zyklische Gruppe.

↑ Beweisideen

1. 1) Zwei Nebenklassen sind entweder disjunkt oder gleich und jedes Gruppenelement ist in einer Nebenklasse enthalten.
   2) $a \in G$ erzeugt die zyklische Untergruppe $\{a, a^2, a^3, \ldots, a^{\mathrm{ord}(a)} = 1\}$.

2. $\mathbb{Z}_p = \{0, 1, 1+1, 1+1+1, \ldots, p-1\}$.

3. Ein endlicher Körper K kann als $\mathbb{Z}_p$-Vektorraum aufgefasst werden. Mit z. B. 3 Basiselementen $\{1, a, b\}$ (Dimension $n = 3$) besteht K aus den p^n Elementen $\{z_1 + z_2 a + z_3 b\}$ mit $z_i \in \mathbb{Z}_p$.

4. Für die Elemente ungleich null gilt: $\mathrm{ord}(a)$ teilt $q-1$, $a^{q-1} = 1$, $a^q = a$
   Mit der Nullstelle a von $f_q = x^q - x$ kann der Linearfaktor $(x-a)$ abgespalten werden. 0 ist auch Nullstelle, $f_q = \prod_{a \in \mathbb{F}_q} (x-a)$.

5. 2) Annahme $f = (x-a)^2 h$, $f' = 2(x-a)h + (x-a)^2 h'$ ↯

6. Binomischer Lehrsatz, Binomialkoeffizienten sind aus $\mathbb{N}$ und durch p teilbar. $\mathbb{F}_q$ hat die Charakteristik p.

7. Sei L eine Körpererweiterung von $\mathbb{F}_p$ mit q Elementen, in dem $f_q = x^q - x$ in Linearfaktoren zerfällt (Zerfällungskörper). Sei $F \subset L$ die Menge der Nullstellen von f_q, $F = \{a \in L \mid a^q = a\}$. f_q besitzt wegen $f_q' = qx^{q-1} - 1 = -1 \in \mathbb{F}_p[x]$ keine mehrfachen Nullstellen. Also ist $|F| = q$.
   F ist ein Körper. Seien $a, b \in F$, es gilt $(ab)^q = a^q b^q = ab$, $(-a)^q = -a$, denn für $p = 2$ ist $-1 = 1$, sonst $(-1)^q = -1$, $(1/a) = 1/a^q = 1/a$ $(a \neq 0)$, $(a+b)^{p^2} = \big((a+b)^p\big)^p = (a^p + b^p)^p = a^{p^2} + b^{p^2}$, (mit $a := a^p$, $b := b^p$) usw, schließlich $(a+b)^q = a^q + b^q = a + b$.

8. $|F_q^*| = q - 1$, wir suchen ein $a \in F_q^*$ mit $\mathrm{ord}(a) = q-1$.
   Sei $m = \mathrm{ord}(a)$ maximal, Behauptung $\mathrm{ord}(a) = q-1$, andernfalls gäbe es ein $b \in F_q^* \backslash H$ mit der von a erzeugten Untergruppe H.
   Aus $b \notin H$ folgt $\mathrm{ord}(b) \nmid m = \mathrm{ord}(a)$, weil H gleich der Nullstellen von $x^m - 1$ ist, da es nur höchstens m Nullstellen geben kann und die m Elemente von H Nullstellen sind, somit $\mathrm{ord}(ab) = \mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b)) > \mathrm{ord}(a)$. ↯
   Konstruktiver: Sei $a \in F_q^*$ mit $m = \mathrm{ord}(a)$. Falls $m < q-1$, so gibt es nach obiger Überlegung ein c mit $\mathrm{ord}(a) < \mathrm{ord}(c)$. Nur endlich viele Wiederholungen sind möglich.

Die Vierergruppe ist kommutativ, aber nicht zyklisch.

$\cdot$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

z. B. $\mathrm{ord}(a) = 2$, $x^2 - 1 = 0$ wird von allen Elementen gelöst.

↑ Frobenius-Homomorphismus $\varphi(x)$

Die Abbildung $\varphi(x) = x^p$ ist injektiv, somit surjektiv, also ein Automorphismus auf $\mathbb{F}_q$.

$$\begin{aligned} \varphi(x \cdot y) &= (x \cdot y)^p = x^p \cdot y^p = \varphi(x) \cdot \varphi(y) \\ \varphi(x + y) &= (x + y)^p = x^p + y^p = \varphi(x) + \varphi(y) \\ \varphi(1) &= 1^p = 1 \end{aligned}$$

siehe vorige Seite 6.

$$\begin{aligned} \varphi(a) &= \varphi(b) && \text{z.z. } a = b \\ \varphi(a) - \varphi(b) &= \varphi(a - b) = 0 && \varphi(-b) = -\varphi(b) \iff \varphi(-b) + \varphi(b) = 0 \\ & && \iff \varphi(-b + b) = 0 \iff \varphi(0) = 0 \end{aligned}$$

für $a - b \neq 0$ gäbe es $(a - b)^{-1}$ mit

$$0 = \varphi((a - b)^{-1}) \cdot 0 = \varphi((a - b)^{-1})\varphi(a - b) = \varphi(1) = 1 \quad \lightning$$

allgemeiner
Der Gruppen-Homomorphismus $\varphi : G \longrightarrow G$ ist genau dann injektiv, wenn $\ker(\varphi) = \{0\}$ ist.
Für $\ker(\varphi) = \{0\}$ und $\varphi(a) = \varphi(b)$ folgt $\varphi(a + (-b)) = \varphi(a) + \varphi(-b) = 0$ und daher $a + (-b) = 0$, also $a = b$.
Ist umgekehrt die Injektivität gegeben und a aus $\ker(\varphi)$, so folgt $\varphi(a) = \varphi(0)$ und daraus bereits $a = 0$.

Für eine Abbildung $\varphi(x)$ auf einem Körper K mit

$$\begin{aligned} \varphi(x \cdot y) &= \varphi(x) \cdot \varphi(y) \\ \varphi(x + y) &= \varphi(x) + \varphi(y) \end{aligned}$$

ist $\ker(\varphi)$ entweder $\{0\}$ (φ ist dann injektiv) oder K (φ ist identisch null).

In der Definition vom Körperhomomorphismus ist $\varphi(1) = 1$ enthalten,
um den bedeutungslosen 2. Fall von vornherein auszuschließen.

↑ Gradformel

Für endliche Körpererweiterungen $K \subset L$ und $L \subset M$ ist $K \subset M$ eine endliche Körpererweiterung und es gilt $\operatorname{grad}_K M = \operatorname{grad}_L M \cdot \operatorname{grad}_K L$, alternative Schreibweise $[M{:}K] = [M{:}L][L{:}K]$.

Beweisidee

Sei $\{\boldsymbol{l}_1, \boldsymbol{l}_2, \boldsymbol{l}_3\}$ ein K-Basis von L und $\{\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4\}$ ein L-Basis von M.

Die 12 Produkte $\boldsymbol{l}_i\boldsymbol{m}_j$, $1 \le i \le 3$, $1 \le j \le 4$, erzeugen den Vektorraum M über K,
denn jedes Element $m = a_1\boldsymbol{m}_1 + a_2\boldsymbol{m}_2 + a_3\boldsymbol{m}_3 + a_4\boldsymbol{m}_4 \in M$ mit Koeffizienten $a_j \in L$ kann als K-Linearkombination $m = \sum_{i,j}(\ )\boldsymbol{l}_i\boldsymbol{m}_j$ dargestellt werden. Die a_j werden durch die K-Linearkombination der $\boldsymbol{l}_i$ ersetzt.

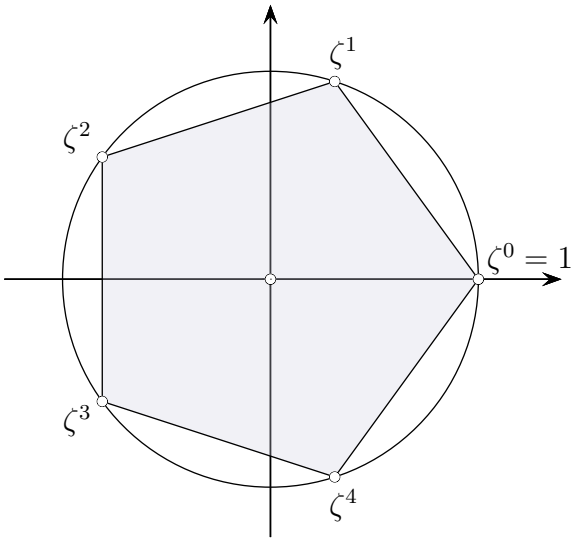
Diese Produkte sind linear unabhängig.

$$0 = \sum_{i,j} c_{i,j}\boldsymbol{l}_i\boldsymbol{m}_j = \sum_j \underbrace{\Big(\sum_i c_{i,j}\boldsymbol{l}_i\Big)}_{=0 \text{ für jedes } j, \text{ da die } \boldsymbol{m}_j \text{ linear unabhängig sind}} \boldsymbol{m}_j$$

Sämtliche $c_{i,j}$ sind null, da die $\boldsymbol{l}_i$ linear unabhängig sind.

$x^2 + 1$ ist irreduzibel in $\mathbb{R}$, $\mathbb{C} = \mathbb{R}/(x^2+1)$, $\mathrm{i}^2 + 1 = 0$,
$\mathbb{C}$ ist $\mathbb{R}$-Vektorraum mit der Basis $\{1, \mathrm{i}\}$.
Nach der Gradformel kann es keinen Zwischenkörper geben.

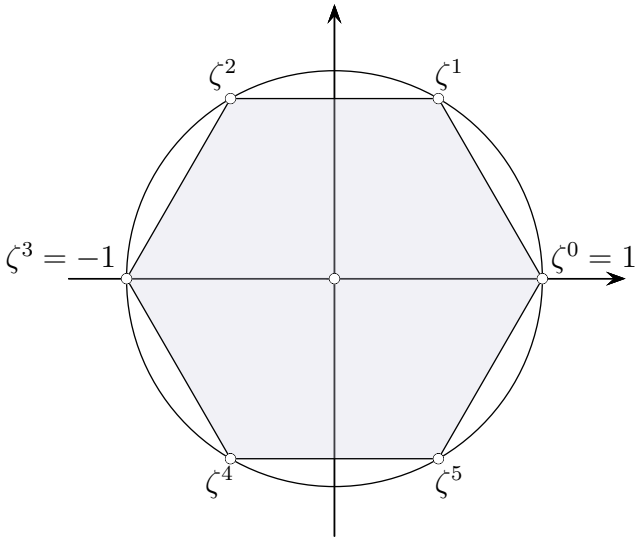
↑ Kreisteilungspolynome



Die Gleichung $x^n = 1$ hat in $\mathbb{C}$ genau n Lösungen
$E_n = \{1, \zeta^1, \zeta^2, \ldots, \zeta^{n-1}\} = \{e^{2\pi k/n} \mid k = 0, 1, \ldots, n-1\}$, die sogenannten n-ten Einheitswurzeln. Diese entsprechen den Ecken eines in den Einheitskreis einbeschriebenen regulären n-Ecks mit einer Ecke in 1. Die Untersuchung der Konstruierbarkeit des regulären n-Ecks mit Zirkel und Lineal ist historisch bedeutsam, da erstmals einige Fragen nur negativ entschieden werden konnten (das regelmäßige 17-Eck ist konstruierbar, Gauss 1796, das 7-Eck nicht).
Die Einheitswurzeln E_n bilden eine zyklische Gruppe, $\zeta^i\zeta^k = \zeta^{j+k \bmod n}$. Der Multiplikation entspricht geometrisch anschaulich einer Drehung. Einheitswurzeln ζ^d, die die Gruppe erzeugen (für die n die kleinste Potenz mit $\zeta^n = 1$ ist), heißen primitive Einheitswurzeln, für sie gilt $\mathrm{ggT}(n, d) = 1$. Die Konstruktion wird möglich, wenn eine primitive Einheitswurzel bekannt ist.

Von den 6-ten Einheitswurzeln sind genau ζ^1 und ζ^5 primitiv, wohingegen
$(\zeta^0)^1 = (\zeta^2)^3 = (\zeta^3)^2 = (\zeta^4)^3 = 1$ ist.

↑ Kreisteilungspolynome



Das Polynom $x^n - 1$ zerfällt in $\mathbb{C}$ in Linearfaktoren: $x^n - 1 = (x-1)(x-\zeta)(x-\zeta^2)\dots(x-\zeta^{n-1})$
Um in der Gaußschen Zahlenebene die Peripherie des Kreises mit dem Radius 1 in n gleiche Teile einzuteilen, muss eine primitive Einheitswurzel, also eine Nullstelle des Polynoms (n-tes Kreisteilungspolynom) $\Phi_n = \prod_{\substack{\zeta^n=1 \\ \zeta \text{ primitiv}}} (x-\zeta) = \prod_{\substack{1\le d\le n \\ \text{ggT}(n,d)=1}} (x-\zeta^d)$ bekannt sein.

$\Phi_6 = (x-\zeta^1)(x-\zeta^5) = \ldots = x^2 - t + 1 \in \mathbb{Z}[x]$, beachte $\zeta^1 + \zeta^5 = 1$.
$\Phi_1 = (x-1)$
$\Phi_2 = (x+1)$

Für die Kreisteilungspolynome gibt es viele Gesetzmäßigkeiten.

$$\begin{aligned}
\Phi_n &\in \mathbb{Z}[x] \text{ und irreduzibel} \\
\text{Grad } \Phi_n &= \varphi(n) \quad \text{Eulersche Funktion} \\
\Phi_p &= \frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1, \qquad p \text{ Primzahl} \\
x^n - 1 &= \prod_{m|n} \Phi_m
\end{aligned}$$

$$x^6 - 1 = \underbrace{(x-1)}_{\Phi_1}\underbrace{(x-\zeta^3)}_{\Phi_2}\underbrace{(x-\zeta^2)((x-\zeta^4))}_{\Phi_3}\underbrace{(x-\zeta^1)(x-\zeta^5)}_{\Phi_6}$$

Jede n-te Einheitswurzel ist eine primitive d-te Einheitswurzel für einen gewissen Teiler d von n und umgekehrt. Die Φ_i haben keine gemeinsamen Nullstellen.

Der Schnitt Kreis/Gerade bzw. zweier Kreise führt zur Hinzunahme einer neuen Wurzel α. $\mathbb{Q}(\alpha)$ ist eine Körpererweiterung von $\mathbb{Q}$ vom Grad 2. Der schrittweisen Konstruktion entspricht insgesamt eine Erweiterung vom Grad 2^k. $\sqrt[3]{a}$ kommt nur durch eine Körpererweiterung vom Grad 3 zustande und ist daher nicht konstruierbar.
Für $n \ge 3$ ist ein regelmäßiges n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.

↑ Zerfällungskörper

Der Zerfällungskörper eines gegebenen Polynoms f über K ist der kleinste (bis auf Isomorphie eindeutig bestimmte) Erweiterungskörper L von K, in dem f vollständig in Linearfaktoren zerfällt.

Sei $f = a(x-\alpha_1)(x-\alpha_2)(x-\alpha_3),\ a \in K.$

L wird durch Adjunktion der Nullstellen (Wurzeln) α_i ausgehend vom Körper K erhalten: $L = K(\alpha_1, \alpha_2, \alpha_3)$
α_1 ist algebraisch über K, α_2 ist algebraisch über $K(\alpha_1)$, α_3 ist algebraisch über $K(\alpha_1, \alpha_1)$.
$[L{:}K] = [K(\alpha_1, \alpha_2, \alpha_3){:}K(\alpha_1, \alpha_2)]\,[K(\alpha_1, \alpha_2){:}K(\alpha_1)]\,[K(\alpha_1){:}K]$

$x^2 - 2 \in \mathbb{Q}[x]$ zerfällt in $\mathbb{R}$ in Linearfaktoren: $f = (x-\sqrt{2})(x+\sqrt{2})$.
Der Zerfällungskörper von f ist also $L = \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$.
$L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Die Galois-Gruppe des Zerfällungskörpers L von f über K besteht aus allen Automorphismen, die die Elemente aus K unverändert (fix) lassen.
Diese K-Automorphismen permutieren die Nullstellen von f.
Voraussetzung: f besitzt keine mehrfache Nullstelle in L (f ist separabel).

$x^3 - 2 \in \mathbb{Q}[x]$ zerfällt in $\mathbb{C}$ in Linearfaktoren: $f = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta)(x - \sqrt[3]{2}\zeta^2)$
mit $\zeta = -\frac{1}{2} + \frac{\mathrm{i}\sqrt{3}}{2}$, einer dritten Einheitswurzel.
Der Zerfällungskörper von f ist also $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$, beachte: $\zeta^2 = -\zeta - 1$,
$x^3 - 1 = (x-1)(x^2+x+1)$
Basis des Vektorraums L über $\mathbb{Q}$ ist $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \zeta, \sqrt[3]{2}\zeta, \sqrt[3]{2}^2\zeta\}$.

alternativ: $L = \mathbb{Q}(\sqrt[3]{2}, \mathrm{i}\sqrt{3})$
Basis: $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \mathrm{i}\sqrt{3}, \sqrt[3]{2}\cdot\mathrm{i}\sqrt{3}, \sqrt[3]{2}^2\cdot\mathrm{i}\sqrt{3}\}$

Die $\mathbb{Q}$-Automorphismen sind durch die Bilder auf einer Basis festgelegt und hier bereits durch die Bilder von $\sqrt[3]{2}$ und $\mathrm{i}\sqrt{3}$. In Frage kommen nur die Nullstellen des eigenen Minimalpolynoms:
$\sqrt[3]{2} \to \sqrt[3]{2},\ \sqrt[3]{2} \to \sqrt[3]{2}\big(-\frac{1}{2} \pm \frac{\mathrm{i}\sqrt{3}}{2}\big),\ \mathrm{i}\sqrt{3} \to \pm\mathrm{i}\sqrt{3}.$
Die Vorzeichen können unabhängig voneinander gewählt werden.
Das müssen auch schon die 6 $\mathbb{Q}$-Automorphismen sein.

$x^4 - 2 \in \mathbb{Q}[x]$ zerfällt in $\mathbb{C}$ in Linearfaktoren (nach dem Eisensteinkriterium irreduzibel):
$x^4 - 2 = (x^2 + \sqrt{2})(x^2 - \sqrt{2}) = (x + \mathrm{i}\sqrt[4]{2})(x - \mathrm{i}\sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}).$
Der Zerfällungskörper ist $L = \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$.
$[L{:}\mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, \mathrm{i}){:}\mathbb{Q}(\sqrt[4]{2})]\,[\mathbb{Q}(\sqrt[4]{2}){:}\mathbb{Q}] = 2 \cdot 4 = 8$
$L = \{(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3) + (b_0 + a_1\alpha + b_2\alpha^2 + b_3\alpha^3)\mathrm{i} \mid a_i, b_i, \in \mathbb{Q},\ \alpha = \sqrt[4]{2}\}$

↑ Zerfällungskörper

Wie sieht der Zerfällungskörper $L = K(\alpha_1, \ldots, \alpha_n)$ (α_i seien paarweise verschieden) genauer aus? Zunächst enthält L die Elemente $t = m_1\alpha_1 + \ldots + m_n\alpha_n$ mit $m_i \in K$. Desweiteren Polynome in t: $T = k_0 + k_1 t + \ldots + k_m t^m$ mit $k_i \in K$. Die sukzessive Konstruktion von L ergibt, dass der höchste Exponent m begrenzt ist und das dies auch schon alle Elemente aus L sind.

Ein Automorphismus auf L, der die Elemente aus K unverändert lässt, permutiert die α_i, umgekehrt kann eine Permutation σ der α_i zu einem K-Automorphismus auf L erweitert werden: $\sigma(t) = m_1\sigma(\alpha_1) + \ldots + m_n\sigma(\alpha_n)$, $\sigma(T) = k_0 + k_1\sigma(t) + \ldots + k_m\sigma(t^m)$.

Galois untersuchte 1831 zu n komplexen Lösungen $\alpha_1, \ldots, \alpha_n$ einer Gleichung mit Koeffizienten aus $\mathbb{Q}$ die Permutationen der Lösungen, die jeweils alle polynomialen Beziehungen in $\alpha_1, \ldots, \alpha_n$, wie z.B. $\alpha_1^2 + \alpha_2^2 = 3$, erhalten. Diese Permutationen bilden die Galoisgruppe der Gleichung. Statt unendlich vieler Beziehungen des Zerfällungskörpers zu betrachten, entdeckte Galois für die Bestimmung der Gruppe einen Weg, bei dem er nur ein einziges, eigens dafür keiertes Polynom zu verwenden brauchte.

↑ Galois' Idee

Es geht um das Lösen von Gleichungen mit Wurzeltermen (durch Radikale, radix lat. Wurzel).
$x^4 - 6x^2 + 2 = 0, \quad x_{1/2} = \pm\sqrt{3+\sqrt{7}},\ x_{3/4} = \pm\sqrt{3-\sqrt{7}}$

Auch ohne Kenntnis der Lösungen gilt (Polynome in $\mathbb{C}[x]$ zerfallen in Linearfaktoren):

$$\begin{aligned} x^4 - 6x^2 + 2 &= (x-x_1)(x-x_2)(x-x_3)(x-x_4) \\ &= x^4 - (x_1+x_2+x_3+x_4)x^3 \\ &\quad + (x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3x_4)x^2 \\ &\quad - (x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)x \ + \ x_1x_2x_3x_4 \end{aligned}$$

Für die Gleichung bedeutet das:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0 \\ x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3x_4 &= -6 \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 &= 0 \\ x_1x_2x_3x_4 &= 2 \end{aligned}$$

In diesen vier Gleichungen sind die Lösungen nicht zu unterscheiden, mathematisch: es gibt 4!-Permutationen (Symmetrien), unter denen die Gleichungen invariant bleiben. In Beziehungen wie $x_1 + x_2 = 0$, $x_3 + x_4 = 0$, $x_1x_3 - x_2x_4 = 0$, $x_1x_4 - x_2x_3 = 0$, $x_1^2 \cdot x_3^2 = 2$, $x_1^2 \cdot x_4^2 = 2$ sind schon einige Eigenschaften der Lösungen enthalten. Die Gruppe der möglichen Permutationen reduziert sich auf die Galois-Gruppe
$D_4 = \{(1), (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$ (Symmetriegruppe des Quadrats unter Spiegelungen und Drehungen). Um die Lösungen weiter einzugrenzen, wird der Zahlbereich für die Lösungs-Beziehungen von $\mathbb{Q}$ auf $\mathbb{Q}(\sqrt{7})$ erweitert. Mit den Beziehungen
$x_1x_2 - 3 - \sqrt{7} = 0$, $x_3^2 - 3 + \sqrt{7} = 0$, $x_4^2 - 3 + \sqrt{7} = 0$ wird die Galois-Gruppe halbiert,
$V_4 = \{(1), (12), (34), (12)(34)\}$ (Kleinsche Vierergruppe). Die anschließenden Erweiterungen des Koeffizientenbereichs um $\sqrt{3+\sqrt{7}}$ und $\sqrt{3-\sqrt{7}}$ halbieren jeweils die Galois-Gruppe und führen zum Zerfällungskörper $L = \mathbb{Q}(x_{1/2}, x_{3/4})$. Aus $\mathbb{Z}_2 = \{(1), (34)\}$ wird $\{(1)\}$. Die schrittweisen Erweiterungen von $\mathbb{Q}$ bis zum Zerfällungskörper L spiegeln sich in einer mehrmaligen Untergruppenbildung der Galois-Gruppe wider.
Überdies findet man eine Eins-zu-eins-Beziehung zwischen allen Unterkörpern von L und allen Untergruppen der Galoisgruppe.

↑ Galois-Gruppe

Wir gehen von einem irreduziblen Polynom 2. Grades $x^2 + px + q \in \mathbb{Q}[x]$ aus, d. h. die Nullstellen sind nicht rational. Sei α eine Nullstelle und $\mathbb{Q}(\alpha)$ die algebraische Körpererweiterung $\{a + b\alpha \mid a, b \in \mathbb{Q}\}$. $\mathbb{Q}(\alpha)$ enthält auch die 2. Nullstelle $-p - \alpha$ und ist somit der Zerfällungskörper des Polynoms.

Es gilt:

$$\begin{aligned} \alpha + (-p - \alpha) &= -p \\ \alpha \cdot (-p - \alpha)) &= -p\alpha - \alpha^2 = q \end{aligned}$$

Ein $\mathbb{Q}$-Automorphismus (lässt die Elemente aus $\mathbb{Q}$ unverändert) permutiert die Nullstellen. Für ihn muss $\varphi(\alpha^2 + p\alpha + q) = \varphi(\alpha)^2 + p\varphi(\alpha) + q = \varphi(0) = 0,\ \varphi(\alpha) = -p - \alpha$ oder $\varphi(\alpha) = \alpha$ (=id) gelten.

Beispiele:

$x^2 + 4x + 1 \in \mathbb{Q}[x],\ x_1 = -2 + \sqrt{3},\ x_2 = -4 - x_1 = -2 - \sqrt{3}.$

$\varphi(a + b\sqrt{3}) = a - b\sqrt{3}$ ist der einzige nichttriviale $\mathbb{Q}$-Automorphismus von $\mathbb{Q}(x_1) = \mathbb{Q}(\sqrt{3})$.

Die Galois-Gruppe besteht aus φ und der Identität.

Betrachten wir nun das irreduzible Polynom (Eisenstein) $x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$ mit den Nullstellen (biquadratisch) $x_{1/2} = \pm\sqrt{1 + \sqrt{3}},\ x_{3/4} = \pm\mathrm{i}\sqrt{\sqrt{3} - 1}$ und dem Zerfällungskörper $\mathbb{Q}(x_1, x_3)$.

Er kann durch Adjunktion von x_3 zu $\mathbb{Q}(x_1)$ erhalten werden.

Das Minimalpolynom von x_1 über $\mathbb{Q}$ ist $x^4 - 2x^2 - 2$.

Für das Minimalpolynom von x_3 über $\mathbb{Q}(x_1)$ beachten wir $x_1^2 + x_3^2 = 2,\ x_1^2 - 2 + x_3^2 = 0,$

x_3 ist Nullstelle von $x_1^2 - 2 + x^2 = 0 \in \mathbb{Q}(x_1)$.

Der Grad des Minimalpolynoms kann nicht 1 sein, da $x_3 \notin \mathbb{Q}(x_1)$.

$[\mathbb{Q}(x_1, x_3):\mathbb{Q}] = [\mathbb{Q}(x_1, x_3):\mathbb{Q}(x_1)][\mathbb{Q}(x_1):\mathbb{Q}] = 2 \cdot 4 = 8.$

Es sind also 8 $\mathbb{Q}$-Automorphismen zu erwarten.

Für den Zerfällungskörper finden wir die explizite Darstellung

$\mathbb{Q}(x_1, x_3) = \{(a + bx_1 + cx_1^2 + dx_1^3) + (e + fx_1 + gx_1^2 + hx_1^3)x_3 \mid a, \ldots, h \in \mathbb{Q}\},$ beachte $x_3^2 = 2 - x_1^2$.

Es gibt vier $\mathbb{Q}$-Automorphismen, die durch $x_1 \to \pm x_1,\ x_3 \to \pm x_3$ charakterisiert sind, und vier weitere mit $x_1 \to \pm x_3,\ x_3 \to \pm x_1$. Die Vorzeichen können unabhängig voneinander gewählt werden.

Bezüglich der Galois-Gruppe invariante Beziehungen:

$$\begin{aligned} x_1^2 x_3^2 &= -2 \\ x_1^2 + x_3^2 &= 2 \\ x_1x_2 + x_3x_4 &= -2 \\ x_1x_3 - x_2x_4 &= 0 \\ x_1x_4 - x_2x_3 &= 0 \\ (x_1x_2 + 1)^2 &= 3 \\ (x_3x_4 + 1)^2 &= 3 \end{aligned}$$

↑ Ordnung der Galois-Gruppe $\mathrm{Gal}(L\,|\,K)$

Für einen Zerfällungskörper $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ existiert ein *primitives Element* α mit $L = K(\alpha)$ (die klassische Bezeichnung lautet Galois-Resolvente), siehe Galois-Theorie Anfänge. α erzeugt also bei alleiniger Adjunktion bereits den gesamten Körper L. Zu diesem Element α sucht man nun ein Polynom minimalen Grades n mit Koeffizienten im Körper K, das α als Nullstelle besitzt, das so genannte *Minimalpolynom*.
Die Elemente der Galois-Gruppe werden durch die Nullstellen des Minimalpolynoms repräsentiert:
Zu jeder Nullstelle α^* des Minimalpolynoms gibt es genau einen Automorphismus, der α auf α^* abbildet. Eine Basis von L ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, aber auch $\{1, \alpha^*, \alpha^{*2}, \ldots, \alpha^{*n-1}\}$.
Daraus ist zu erkennen, dass $K(\alpha)$ isomorph zu $K(\alpha^*)$ ist. Zusammengefasst:
Die Dimension von L stimmt mit der Ordnung der Galois-Gruppe überein,
$[L{:}K] = |\mathrm{Gal}(L\,|\,K)|$.

↑ Hauptsatz der Galois-Theorie

Sei K ein Unterkörper der komplexen Zahlen und L der Zerfällungskörper eines Polynoms mit Koeffizienten in K. Für die Galois-Gruppe $G = \mathrm{Gal}(L|K) = \mathrm{Aut}(L|K)$ und den Zwischenkörpern F, $K \subset F \subset L$, mit jeweils zugehörender Untergruppe $\mathrm{Aut}(L|F)$ von G (diese umfasst diejenigen Automorphismen von G, die jeden Wert von F unverändert lassen) bestehen folgende Zusammenhänge:

1. Der Grad der Körpererweiterung (Dimension) von L zu K stimmt mit der Ordnung der Galois-Gruppe überein, $[L{:}K] = |\mathrm{Gal}(L|K)|$.

2. Jedem Zwischenkörper F entspricht in umkehrbar eindeutiger Weise eine Untergruppe $\mathrm{Aut}(L|F)$ der Galois-Gruppe G. F ist der Fixkörper von $\mathrm{Aut}(L|F)$.

3. Entsteht ein Zwischenkörper F als Zerfällungskörper eines Polynoms mit Koeffizienten in K, so enthält die Galois-Gruppe $\mathrm{Aut}(F|K)$ insgesamt $|G|/|\mathrm{Aut}(L|F)|$ Automorphismen, die dadurch erhalten werden, dass man den Definitionsbereich der Automorphismen von G auf F einschränkt.

↑ Radikalerweiterung

$x^5 - 2 \in \mathbb{Q}[x]$ zerfällt in $\mathbb{C}$ in Linearfaktoren:
$f = (x - \sqrt[5]{2})(x - \sqrt[5]{2}\zeta)(x - \sqrt[5]{2}\zeta^2)(x - \sqrt[5]{2}\zeta^3)(x - \sqrt[5]{2}\zeta^4)$
mit einer primitiven fünften Einheitswurzel ζ, d. h. $\zeta^5 = 1$ und $\zeta^1,\ \zeta^2,\ \zeta^3,\ \zeta^4 \neq 1$
(außer $\zeta = 1$ sind alle 5-ten Einheitswurzeln primitiv).

Der Zerfällungskörper von f ist also $L = \mathbb{Q}(\sqrt[5]{2}, \zeta)$.

Basis des Vektorraums $\mathbb{Q}(\sqrt[5]{2})$ über $\mathbb{Q}$ ist $\{1,\ \sqrt[5]{2},\ \sqrt[5]{2}^2,\ \sqrt[5]{2}^3,\ \sqrt[5]{2}^4\}$.

Basis des Vektorraums L über $\mathbb{Q}(\sqrt[5]{2})$ ist $\{\zeta^1,\ \zeta^2,\ \zeta^3,\ \zeta^4\}$, beachte: $\zeta^1 + \zeta^2 + \zeta^3 + \zeta^4 = -1$
alternativ: $\{1,\ \zeta^1,\ \zeta^2,\ \zeta^3\}$, beachte: $(x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1$

$[L{:}\mathbb{Q}] = [L : \mathbb{Q}(\sqrt[5]{2})][\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 4 \cdot 5 = 20.$

Die Dimension von L stimmt mit der Ordnung der Galois-Gruppe überein,
$[L : \mathbb{Q}] = |\mathrm{Gal}(L|\mathbb{Q})| = 20$. Bei Adjunktion von $\sqrt[5]{2}$ schrumpft die Galois-Gruppe $\mathrm{Gal}(L|\mathbb{Q})$ auf ein Fünftel.

Allgemein:
Hat eine wiederholte Adjunktion von Wurzeln den Zerfällungskörper von f zum Ergebnis, so sind die Lösungen von f durch geschachtelte Wurzelausdrücke darstellbar. Die Galois-Gruppe reduziert sich schrittweise (löst sich auf) zu $\{\mathrm{id}\}$.

$f = x^4 - 4x^3 - 8x^2 + 4x + 11$

$x_{1/2} = 1 + \sqrt{5} \pm \sqrt{2 + \sqrt{5}},\ x_{3/4} = 1 - \sqrt{5} \pm \sqrt{2 - \sqrt{5}}$

Die Galois-Gruppe von $x^5 - x - 1 = 0$ kann nicht aufgelöst werden. Daher sind die Lösungen der Gleichung nicht durch geschachtelte Wurzelausdrücke darstellbar.

↑ Zur Galois-Theorie

Sei $L = \mathbb{Q}(\sqrt{2}, \mathrm{i})$ der Zerfällungskörper von $(x^2-2)(x^2+1)$ über $K = \mathbb{Q}$.

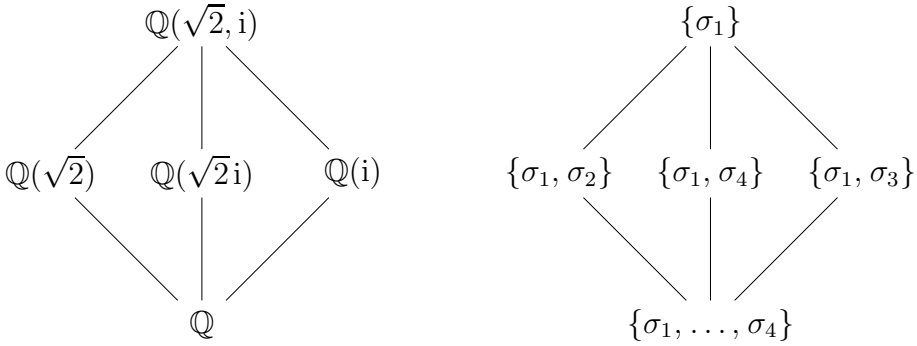
Die Galoisgruppe G besteht aus folgenden vier Elementen $\sigma_1, \ldots, \sigma_4$:

$$\begin{aligned}
\sigma_1 &: \sqrt{2} \to \sqrt{2},\ \mathrm{i} \to \mathrm{i} \\
\sigma_2 &: \sqrt{2} \to \sqrt{2},\ \mathrm{i} \to -\mathrm{i} \\
\sigma_3 &: \sqrt{2} \to -\sqrt{2},\ \mathrm{i} \to \mathrm{i} \\
\sigma_4 &: \sqrt{2} \to -\sqrt{2},\ \mathrm{i} \to -\mathrm{i}
\end{aligned}$$

Verknüpfungstafel:

$\circ$	σ_1	σ_2	σ_3	σ_4
σ_1	σ_1	σ_2	σ_3	σ_4
σ_2	σ_2	σ_1	σ_4	σ_3
σ_3	σ_3	σ_4	σ_1	σ_2
σ_4	σ_4	σ_3	σ_2	σ_1

Beachte: $\sigma_2 \circ \sigma_2 = \sigma_1$ und $\sigma_3 \circ \sigma_3 = \sigma_1$
In jeder Zeile und Spalte muss jedes Gruppenelement genau einmal vorkommen.



Die Diagramme enthalten die Untergruppen der Galois-Gruppe mit den dazu korrespondierenden Zwischenkörpern (Fixkörper).

Exemplarisch der Nachweis $L^{\{\sigma_1, \sigma_4\}} = \mathbb{Q}(\sqrt{2}\mathrm{i})$:

„$\supseteq$“ $\quad \sigma_4(\sqrt{2}\mathrm{i}) = \sigma_4(\sqrt{2})\sigma_4(\mathrm{i}) = (-\sqrt{2})(-\mathrm{i}) = \sigma_4(\sqrt{2}\mathrm{i})$

„$\subseteq$“ $\quad$ folgt aus Gradgründen:

$$\begin{aligned}
[L^{\{\sigma_1, \sigma_4\}} : \mathbb{Q}] &= |G| / |\{\sigma_1, \sigma_4\}| = 4/2 = 2 \\
[\mathbb{Q}(\sqrt{2}\mathrm{i}) : \mathbb{Q}] &= 2
\end{aligned}$$

↑ Minimalpolynome und Galois-Gruppe $\mathrm{Aut}(L\,|\,K)$

Sei L ein Zerfällungskörper über K, $\alpha \in L$
und $f := (x-\alpha_1)\dots(x-\alpha_r)$ mit $\{\varphi(\alpha)\,|\,\varphi \in \mathrm{Aut}(L|K)\} = \{\alpha_1,\dots,\alpha_r\}$, α_i paarweise verschieden.

$\Longrightarrow$ $f = a_0 + a_1x + \dots + a_{n-1}x^{r-1} + x^r \in K[x]$ ist das Minimalpolynom von α über K.

Ein Automorphismus φ auf L kann zu einem Automorphismus auf $L[x]$ fortgesetzt werden.
Da $\mathrm{Aut}(L|K)$ eine endl. Gruppe ist, ändert sich f nicht, $f = (x-\varphi(\alpha_1))\dots(x-\varphi(\alpha_r))$.
Daraus folgt $\varphi(a_i) = a_i$ für $i = 0,\dots,r-1$.
Da das für jeden Automorphismus aus $\mathrm{Aut}(L|K)\}$ gilt, liegen die Koeffizienten von f im Fixkörper der Galois-Gruppe, also in K.
Alternative Begründung:
Jedes $\varphi \in \mathrm{Aut}(L|K)$ permutiert die α_i, lässt symmetrische Ausdrücke der $\alpha_1,\dots,\alpha_r$ fest.
Die Koeffizienten von f sind aber die sogenannten elementarsymmetrischen Funktionen der α_i.
Sie liegen also in K.
f ist irreduzibel in $K[x]$.
Mit $g(\alpha) = 0$ und $g(\varphi(\alpha)) = \varphi(g(\alpha)) = 0$ für $\varphi \in \mathrm{Aut}(L|K)$ existieren r Nullstellen.
Es gilt $f(x)\,|\,g(x)$.

↑ Galois-Gruppe $\mathrm{Gal}(L|\mathbb{Q})$

Die Nullstellen des Polynoms $f = x^4 - 10x^2 + 1$ lauten $x_1 = \sqrt{2} + \sqrt{3}$, $x_2 = \sqrt{2} - \sqrt{3}$, $x_3 = -\sqrt{2} + \sqrt{3}$ und $x_4 = -\sqrt{2} - \sqrt{3}$. Der Zerfällungskörper von f ist $L = \mathbb{Q}(x_1, x_2, x_3, x_4)$.
Wir werden die Galois-Gruppe $\mathrm{Gal}(L|\mathbb{Q})$ ermitteln, also alle Permutationen (Symmetrien) der Nullstellen, die alle polynomialen Relationen in $\mathbb{Q}$ zwischen den Nullstellen erhalten.
Die Permutation σ ist in $\mathrm{Gal}(L|\mathbb{Q})$, wenn für jede Relation $g(x_1, x_2, x_3, x_4) = 0$
$g(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}) = 0$ folgt.

Für L existiert ein primitives Element $t = \sqrt{2} + \sqrt{3}$ und
zu t das Minimalpolynom $x^4 - 10x^2 + 1$ (stimmt hier zufällig mit f überein) mit den Nullstellen $t_1 = t = \sqrt{2} + \sqrt{3}$, $t_2 = \sqrt{2} - \sqrt{3}$, $t_3 = -\sqrt{2} + \sqrt{3}$ und $t_4 = -\sqrt{2} - \sqrt{3}$.

Die x_i können durch t ausgedrückt werden, beachte $L = \mathbb{Q}(t)$, Basis $\{1, t, t^2, t^3\}$.

$$\begin{aligned} \sqrt{2} + \sqrt{3} &= t \\ \sqrt{2} - \sqrt{3} &= t^3 - 10t \\ -\sqrt{2} + \sqrt{3} &= -t^3 + 10t \\ -\sqrt{2} - \sqrt{3} &= -t \end{aligned}$$

Z. B. führt der Ansatz $\sqrt{2} - \sqrt{3} = at^3 + bt^2 + ct$ auf $11a + c = 1$ und $9a + c = -1$ mit $a = 1$, $b = 0$, $c = -10$. Mit der Schreibweise

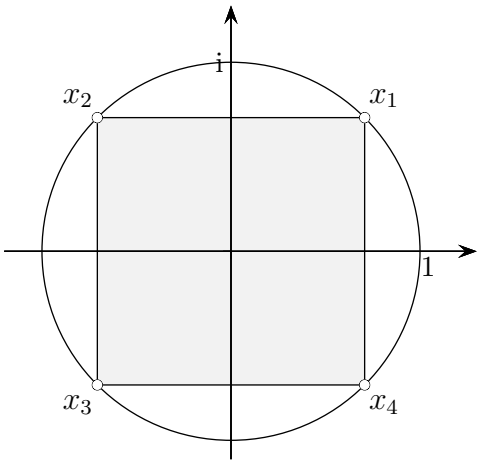
$$\begin{aligned} x_1 &= h_1(t) \\ x_2 &= h_2(t) \\ x_3 &= h_3(t) \\ x_4 &= h_4(t) \end{aligned}$$

und den folgenden Einsetzungen sind die vier Symmetrien zu erkennen.
Die Idee geht auf Galois zurück.

$x_1 = h_1(t_1)$	$x_2 = h_1(t_2)$	$x_3 = h_1(t_3)$	$x_4 = h_1(t_4)$
$x_2 = h_2(t_1)$	$x_1 = h_2(t_2)$	$x_4 = h_2(t_3)$	$x_3 = h_2(t_4)$
$x_3 = h_3(t_1)$	$x_4 = h_3(t_2)$	$x_1 = h_3(t_3)$	$x_2 = h_3(t_4)$
$x_4 = h_4(t_1)$	$x_3 = h_4(t_2)$	$x_2 = h_4(t_3)$	$x_1 = h_4(t_4)$
id	(12)(34)	(13)(24)	(14)(23)

Aus der Kenntnis der Nullstellen t_i des Minimalpolynoms eines primitiven Elements t können wir die Galois-Gruppe bestimmen. Die Nullstellen x_i werden mit t polynomial dargestellt und die t_i in die Polynome für t eingesetzt. Die Anzahl der Nullstellen stimmt mit der Anzahl der Symmetrien überein.

↑ Galois-Gruppe von $f = x^4 + 1$



$f = x^4 + 1 \in \mathbb{Q}[x]$, f ist irreduzibel, siehe Irreduzibles Polynom.

Sei x_1 die Nullstelle von f in $\mathbb{C}$ im 1. Quadrant. $x_1 = \frac{\sqrt{2}}{2} + \frac{\mathrm{i}\sqrt{2}}{2}$ wird nicht benötigt.
Die weiteren Nullstellen sind dann $x_2 = \mathrm{i}x_1$, $x_3 = -x_1$, $x_4 = -\mathrm{i}x_1$.
Es ist $x_1^2 = \mathrm{i}$, x_1 primitives Element, Zerfällungskörper $L = \mathbb{Q}(x_1)$.
Wegen $[L : \mathbb{Q}] = |G(f)|$ sind 4 Symmetrien zu ermitteln.
Es gibt keine große Auswahl. x_1 kann nur auf eine Nullstelle abgebildet werden.
$\sigma(x_1) = -x_1$, $\tau(x_1) = x_1^3$
σ und τ sind die Permutationen, die (x_1, x_2, x_3, x_4) in (x_2, x_1, x_4, x_3) bzw. (x_4, x_3, x_2, x_1) überführen. $\sigma^2 = \tau^2 = \mathrm{id}$, $\sigma\tau = \tau\sigma$, $G = \{\mathrm{id}, (13)(24), (12)(34), (14)(23)\}$

↑ Zusammenhänge

1. Die Nullstellen $t_1, \ldots, t_n$ des Minimalpolynoms eines primitiven Elements t von L sind primitive Elemente.

   Das Minimalpolynom hat den Grad n, somit hat die Basis einer Nullstelle t' n Elemente. t' ist dann ein primitives Element, $L = \mathbb{Q}(t')$.

2. Für die Nullstellen des Minimalpolynoms eines primitiven Elements t von $L = \mathbb{Q}(x_1, \ldots, x_n)$ gilt: $t = v(x_1, \ldots, x_n)$ und alle weiteren Nullstellen sind von der Form $t' = v(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, wobei σ eine n-stellige Permutation ist, $\sigma = \mathrm{id}$ ergibt t.

   Das primitive Element t kann durch ein Polynom v mit rationalen Koeffizienten in der angegebenen Weise dargestellt werden.
   Sei $V(x) = \prod_{\sigma \in S_n} \big(x - v(x_{\sigma(1)}, \ldots, x_{\sigma(n)})\big)$, wobei das Produkt über alle n-stelligen Permutationen läuft. $V(x)$ ist symmetrisch, somit auch seine Koeffizienten. Diese lassen sich als Linearkombination von Produkten elementarsymmetrischer Funktionen der x_i darstellen. Die Koeffizienten von $V(x)$ sind daher rationale Zahlen.

   $V(x)$ enthält den Faktor $(x - t)$ für $\sigma = \mathrm{id}$. Zum Minimalpolynom von t (es teilt $V(x)$) gehören weitere Faktoren mit Nullstellen, die von der angegebenen Form sind.
   Es wird sich zeigen, dass die zugehörigen Permutationen die Galois-Gruppe bilden.

3. Für den Nachweis wird häufiger benutzt:
   Ein Polynom $f(x)$ mit rationalen Koeffizienten und der Nullstelle t hat auch jede Nullstelle t' des Minimalpolynoms von t als Nullstelle.

   Hierbei ist lediglich zu beachten, dass $f(x)$ ein Vielfaches des Minimalpolynoms von t ist.

4. Für ein primitives Element t existieren Polynome mit $x_1 = h_1(t), \ldots, x_n = h_n(t)$.
   Für jede Nullstelle t' des Minimalpolynoms von t stellt $x_{\sigma(1)} = h_1(t'), \ldots, x_{\sigma(n)} = h_n(t')$ eine Permutation von $x_1, \ldots, x_n$ dar.

   L ist Zerfällungskörper von f.
   Die Polynome $f(h_1(x)), \ldots, f(h_n(x))$ haben t als Nullstelle und damit nach 3. auch t'.
   $h_i(t')$ ist eine Nullstelle von $f(x)$, muss also mit einem x_i übereinstimmen.
   Aus $h_i(t') = h_j(t')$ folgt $h_i(t') - h_j(t') = 0$ und nach 3. $h_i(t) - h_j(t) = 0$, $x_i - x_j = 0$, $x_i = x_j$.
   Da $x_1, \ldots, x_n$ paarweise verschieden sind, folgt $i = j$. Die x_i werden somit permutiert.

5. Von besonderer Bedeutung ist nun:
   Die unter 4. definierte Permutation σ ist eine Symmetrie der Nullstellen.
   Dazu betrachten wir eine algebraische Relation $g(x_1, \ldots, x_n) = g(h_1(t), \ldots, h_n(t)) = 0$.
   Nach 3. und 4. gilt $g(h_1(t'), \ldots, h_n(t')) = g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = 0$, d. h., σ erhält die algebraische Relation $g(x_1, \ldots, x_n) = 0$.

   Umgekehrt gilt:
   Zur n-stelligen Symmetrie σ gibt es eine Nullstelle t' des Minimalpolynoms von t mit
   $$x_{\sigma(1)} = h_1(t'), \ldots, x_{\sigma(n)} = h_n(t').$$
   Sei $m(x) = \prod_{\tau \in B} \big(x - v(x_{\tau(1)}, \ldots, x_{\tau(n)})\big)$ das Minimalpolynom von t mit $B \subsetneqq S_n$,
   $$t = v(x_1, \ldots, x_n).$$

Aus der Gleichheit der Koeffizienten beider Seiten ergeben sich algebraische Relationen, die von σ erhalten bleiben. Daher folgt $m(x) = \prod_{\tau\in B}\big(x - v(x_{\sigma(\tau(1))}, \ldots, x_{\sigma(\tau(n))})\big)$.
Für $\tau = \mathrm{id}$ ergibt das die Nullstelle $t' = v(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.
Durch $x_i = h_i(t) = h_i(v(x_1, \ldots, x_n))$ für $i = 1, \ldots, n$ ist eine algebraische Relation zwischen den x_i gegeben. Diese wird durch σ erhalten, also haben wir schließlich
$x_{\sigma(i)} = h_i(v(x_{\sigma(1)}, \ldots, x_{\sigma(n)})) = h_i(t')$.

6. Die Anzahl der Nullstellen des Minimalpolynoms eines primitiven Elements von L entspricht der Anzahl der Symmetrien von $x_1, \ldots, x_n$.
Mit den Nullstellen des Minimalpolynoms kann die Galois-Gruppe bestimmt werden.
Die folgende Methode, ein primitives Element zu finden, geht auf Lagrange zurück.

7. Nimmt für ein Polynom V mit n Variablen der Term $V(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ für jede n-stellige Permutation σ (deren Anzahl beträgt $N = n!$) einen unterschiedlichen Wert an, so ist die *galoissche Resolvente* $t = V(x_1, \ldots, x_n)$ ein primitives Element von L, z. B. $t = m_1x_1 + \ldots + m_nx_n$ mit geeigneten ganzen Zahlen m_i.

Zu zeigen ist, dass sich die x_i polynomial mit rationalen Koeffizienten durch t darstellen lassen. Hierzu nummerieren wir die N Permutationen ($\sigma_1 = \mathrm{id}$) und die zugehörigen t-Werte ($t_1 = t$) und konstruieren ein Gleichungssystem.

$$\begin{aligned}
x_{\sigma_1(1)} &+ \ldots + & x_{\sigma_N(1)} &= b_0 && x_{\sigma_1(1)} = x_1\\
t_1x_{\sigma_1(1)} &+ \ldots + & t_nx_{\sigma_N(1)} &= b_1\\
t_1^2x_{\sigma_1(1)} &+ \ldots + & t_n^2x_{\sigma_N(1)} &= b_2\\
& & \vdots\\
t_1^{N-1}x_{\sigma_1(1)} &+ \ldots + & t_n^{N-1}x_{\sigma_N(1)} &= b_{N-1}
\end{aligned}$$

Wird eine Permutation auf die symmetrische Gruppe $\{\sigma_1, \ldots, \sigma_N\}$ angewandt, so geht die Gruppe in sich über. Die Zahlen b_0, …, b_{N-1} sind somit jeweils symmetrische Ausdrücke in den $x_1, \ldots, x_n$ und damit Polynome mit rationalen Koeffizienten.
Wir können dieses System als inhomogenes lineares Gleichungssystem mit den Unbestimmten $x_{\sigma_1(1)}$, …, $x_{\sigma_N(1)}$ lesen. Die Determinante

$$D = \begin{vmatrix} 1 & \ldots & 1\\ t_1 & \ldots & t_n\\ t_1^2 & \ldots & t_n^2\\ \vdots & & \vdots\\ t_1^{N-1} & \ldots & t_n^{N-1} \end{vmatrix}$$ der Koeffizientenmatrix

ist durch $D = \prod_{1\le i<j\le N}(t_j - t_i)$ gegeben (Vandermonde).

Es ist $D \neq 0$, da nach Voraussetzung $t_1, \ldots, t_N$ paarweise verschieden sind. Sei weiter

$$D_1 = \begin{vmatrix} b_0 & 1 & \ldots & 1 \\ b_1 & t_2 & \ldots & t_n \\ b_2 & t_2^2 & \ldots & t_n^2 \\ \vdots & \vdots & & \vdots \\ b_{N-1} & t_2^{N-1} & \ldots & t_n^{N-1} \end{vmatrix}$$

Nach der cramerschen Regel für die Lösung eines inhomogenen Gleichungssystems ist

$$x_1 = \frac{D_1}{D} = \frac{D_1 \cdot D}{D^2}$$

Der Nenner D^2 ist symmetrisch in $t_1, \ldots, t_N$ und damit auch in $x_1, \ldots, x_n$, ist also eine rationale Zahl.

Die Vorzeichen von D und D_1 wechseln jeweils bei Vertauschung zweier Elemente aus $t_2, \ldots, t_N$ (für D_1 bedeutet das eine Vertauschung zweier Spalten), das Produkt ist invariant, also symmetrisch in $t_2, \ldots, t_N$ und lässt sich daher durch elementarsymmetrische Funktionen in $t_2, \ldots, t_N$ polynomial darstellen.
Jede elementarsymmetrische Funktion in $t_2, \ldots, t_N$ ist ein Polynom mit ganzzahligen Koeffizienten in den elementarsymmetrischen Funktionen in $t_1, \ldots, t_N$ und in t_1, z. B.
$t_2t_3 + t_2t_4 + t_3t_4 = t_1t_2 + t_1t_3 + t_2t_3 + t_1t_4 + t_2t_4 + t_3t_4 - t_1(t_1 + t_2 + t_3 + t_4) + t_1^2$,
somit auch $D_1 \cdot D$, siehe 8.
Analog folgt, dass ebenfalls x_2 ($\sigma_2 = \mathrm{id}$) Polynom in $t = V(x_1, ..., x_n)$ mit rationalen Koeffizienten ist, usw.

8. Die elementarsymmetrischen Funktionen $e_1(x_2, \ldots, x_n)$, $e_2(x_2, \ldots, x_n)$, $\ldots$, $e_{n-1}(x_2, \ldots, x_n)$ sind ganzzahlige Polynome in x_1 und den elementarsymmetrischen Funktionen

$$\begin{aligned} e_1(x_1, x_2, \ldots, x_n) &= x_1 + x_2 + \ldots + x_n \\ e_2(x_1, x_2, \ldots, x_n) &= x_1x_2 + x_1x_3 + x_2x_3 + \ldots + x_{n-1}x_n \\ e_3(x_1, x_2, \ldots, x_n) &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + \ldots + x_{n-2}x_{n-1}x_n \\ &\vdots \\ e_n(x_1, x_2, \ldots, x_n) &= x_1x_2x_3 \ldots x_n \end{aligned}$$

$$e_k(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i_1 \leq i_2 \leq \ldots \leq i_k \leq n} x_{i_1}x_{i_2} \ldots x_{i_k}, \qquad 1 \leq k \leq n.$$

Begründung
Ein Vergleich der beiden Seiten von

$$(x-x_1)(x-x_2)(x-x_3)\cdot\ldots\cdot(x-x_n)$$
$$= x(x-x_2)(x-x_3)\cdot\ldots\cdot(x-x_n) - x_1(x-x_2)(x-x_3)\cdot\ldots\cdot(x-x_n)$$

führt zu den Relationen:

$$\begin{aligned}
e_1(x_2,\ldots,x_n) &= e_1(x_1,x_2,\ldots,x_n) - x_1\\
e_2(x_2,\ldots,x_n) &= e_2(x_1,x_2,\ldots,x_n) - x_1\cdot e_1(x_2,\ldots,x_n)\\
e_3(x_2,\ldots,x_n) &= e_3(x_1,x_2,\ldots,x_n) - x_1\cdot e_2(x_2,\ldots,x_n)\\
&\vdots\\
e_{n-1}(x_2,\ldots,x_n) &= e_{n-1}(x_1,x_2,\ldots,x_n) - x_1\cdot e_{n-2}(x_2,\ldots,x_n)
\end{aligned}$$

Damit lassen sich die $e_k(x_2,\ldots,x_n)$ als Polynome in den $e_k(x_1,x_2,\ldots,x_n)$ und x_1 darstellen (rekursiv, von unten nach oben).

9. Sei f ein irreduzibles normiertes Polynom über $\mathbb{Q}$, in L daher ein Minimalpolynom m zu α. Dann hat f in L keine mehrfachen Nullstellen.

   Eine mehrfache Nullstelle von f wäre auch eine Nullstelle von $\frac{1}{n}f'$, mit $\operatorname{grad} f = n$.

   $$f = (x-a)^k h \quad\Longrightarrow\quad f' = k(x-a)^{k-1}h + (x-a)^k h'$$

   Dann wäre $\frac{1}{n}f'$ ein Vielfaches von m. Das ist nicht möglich, da $\operatorname{grad} f' = n-1$ ist.

10. Seien $x_1,\ldots,x_n$ die verschiedenen Nullstellen eines irreduziblen normierten Polynoms f über $\mathbb{Q}$. Die galoissche Gruppe G operiert transitiv auf diesen Nullstellen, d. h., für jedes Paar (x_i, x_j) existiert (mindestens) eine Symmetrie σ mit $x_{\sigma(i)} = x_j$.

    Die Koeffizienten von $g = \prod_{\sigma\in G}(x - x_{\sigma(i)})$ $\qquad i$ fest

    sind invariant unter den Symmetrien, $\sigma \in G \iff \tau\circ\sigma \in G$.
    g ist daher ein normiertes Polynom mit rationalen Koeffizienten, siehe Polynomring 13.
    f ist das Minimalpolynom von x_i. Mit $\sigma = \mathrm{id}$ ist x_i Nullstelle von $g(x)$ und damit sind alle weiteren x_k Nullstellen von g, insbesondere auch x_j, siehe 3. Somit existiert eine Symmetrie mit $x_{\sigma(i)} = x_j$.

↑ Zusammengefasst

11. Sei L Zerfällungskörper von f mit rationalen Koeffizienten, den verschiedenen Nullstellen $x_1, \ldots, x_n$ und $t = V(x_1, \ldots, x_n)$ eine galoissche Resolvente. Die Symmetrien der Nullstellen (Elemente der Galois-Gruppe) sind dann genau diejenigen n-stelligen Permutationen $\sigma_1, \ldots, \sigma_m$, so dass $g = (x - t_1)(x - t_2)\ldots(x - t_m)$ das Minimalpolynom zu t ist mit:

$$\begin{aligned} t_1 &= V(x_{\sigma_1(1)}, \ldots, x_{\sigma_1(n)}) \qquad\qquad \sigma_1 = \mathrm{id}, \quad t_1 = t \\ t_2 &= V(x_{\sigma_2(1)}, \ldots, x_{\sigma_2(n)}) \\ &\vdots \\ t_m &= V(x_{\sigma_m(1)}, \ldots, x_{\sigma_m(n)}) \end{aligned}$$

Sei L Zerfällungskörper von $f = x^3 + x^2 + x + 1$.
Die Nullstellen lauten $x_1 = -1$, $x_2 = \mathrm{i}$, $x_3 = -\mathrm{i}$.
$t = V(x_1, x_2, x_3) = x_2 - x_1$ ist eine galoissche Resolvente,
denn für die 6 Permutationen erhalten wir 6 verschiedene Werte:

$$\begin{aligned} V(x_1, x_2, x_3) &= 1 + \mathrm{i} = t \\ V(x_1, x_3, x_2) &= 1 - \mathrm{i} \\ V(x_2, x_1, x_3) &= -1 - \mathrm{i} \\ V(x_2, x_3, x_1) &= -2\mathrm{i} \\ V(x_3, x_1, x_2) &= -1 + \mathrm{i} \\ V(x_3, x_2, x_1) &= 2\mathrm{i} \end{aligned}$$

$$\begin{aligned} G &= \big(x - (1+\mathrm{i})\big)\big(x - (1-\mathrm{i})\big)\big(x - (-1-\mathrm{i})\big)\big(x - (-2\mathrm{i})\big)\big(x - (-1+\mathrm{i})\big)\big(x - 2\mathrm{i}\big) \\ &= x^6 + 4x^4 + 4x^2 + 16 \\ &= (x^2 + 4)(x^2 - 2x + 2)(x^2 + 2x + 2) \end{aligned}$$

Das Minimalpolynom ist der irreduzible Faktor $g = x^2 - 2x + 2$ von G, der die Nullstelle t enthält.

$$x^2 - 2x + 2 = (x - (1+\mathrm{i}))(x - (1-\mathrm{i}))$$

Die Galois-Gruppe besteht aus den beiden Permutationen, die (x_1, x_2, x_3) in (x_1, x_2, x_3) bzw. (x_1, x_3, x_2) überführen, also den Abbildungen id und $\mathrm{i} \to -\mathrm{i}$.

Das Beispiel soll den Sachverhalt lediglich veranschaulichen, das Ergebnis ist wegen $(x^4 - 1)/(x - 1) = x^3 + x^2 + x + 1$, $x^4 - 1 = (x^2 + 1)(x^2 - 1)$ und $L = \mathbb{C}$ offensichtlich.

Noch einmal:

↑ Galois-Gruppe von f

Die verschiedenen Nullstellen eines Polynoms f (separabel) lauten $x_1, \ldots, x_n$.
(f ist irreduzibel oder ein separables Produkt von irreduziblen Faktoren.)
Der Zerfällungskörper sei L.

1. Ein primitives Element t, d. h. $L = L(t)$ ist zu eruieren.
   Weiter sind das Minimalpolynom m von t und seine Nullstellen t_i zu ermitteln.

   In einfachen Fällen gelingt das durch genaues Hinschauen.
   Die Nullstellen von m sind primitive Elemente von L.
   Ein Automorphismus, der $\mathbb{Q}$ festlässt, bildet ein primitives Element auf ein solches ab.
   $\{1, t, t^2, \ldots, t^k\}$, grad $m = k$, ist eine Basis des $\mathbb{Q}$-Vektorraums L.
   Die Nullstellen x_i werden durch t polynomial dargestellt: $x_1 = h_1(t)$, … , $x_n = h_n(t)$
   Ein Wechsel von t nach t' bewirkt eine Permutation der x_i:
   $x_{\sigma(1)} = h_1(t')$, … , $x_{\sigma(n)} = h_n(t')$.
   Jede Nullstelle von m ergibt eine Symmetrie der Galois-Gruppe.

2. Ein primitives Element wird mit einem Term $t = v(x_1, \ldots, x_n)$ (*galoissche Resolvente*) ermittelt, der für jede n-stellige Permutation einen unterschiedlichen Wert $t' = v(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ annimmt, möglich ist der Ansatz $t = m_1 x_1 + \ldots + m_n x_n$.

   Das Minimalpolynom m ist der irreduzible Faktor von
   $V(x) = \prod_{\sigma \in S_n} \big(x - v(x_{\sigma(1)}, \ldots, x_{\sigma(n)})\big)$, der $\big(x - v(x_1, \ldots, x_n)\big)$ enthält.
   Dieser Linearfaktor ergibt die Identität, die weiteren Linearfaktoren des irreduziblen Faktors liefern die restlichen Symmetrien der Galois-Gruppe.

Ein Zwischenkörper K von $\mathbb{Q}$ und einem Zerfällungskörper L ist eine endlich erzeugte Erweiterung $K = \mathbb{Q}(t_1, \ldots, t_k)$ von $\mathbb{Q}$ mit algebraischen Elementen t_i. Die Koeffizienten von Polynomen sind Elemente eines Körpers, z. B. K. Algebraische Relationen von Nullstellen und die galoissche Gruppe G sind hinsichtlich eines Körpers K definiert. Die aufgeführten Aussagen bleiben auch für K statt $\mathbb{Q}$ gültig, z. B.

Ein Polynom $f(x)$ über K mit der Nullstelle t hat auch jede Nullstelle t' des Minimalpolynoms von t über K als Nullstelle.

Statt von $\mathbb{Q}$ kann von K ausgegangen werden, namentlich bei der Festlegung eines primitiven Elements $t = V(x_1, \ldots, x_n)$ und des Minimalpolynoms von t. Seine Nullstellen sind primitive Elemente von der Form $t' = V(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, wobei σ eine n-stellige Permutation ist. Die Koeffizienten der polynomialen Darstellung von t' sind aus K.

Für einen Zwischenkörper K von $\mathbb{Q}$ und L ist jede Symmetrie über L auch eine Symmetrie über K, $K \subset L$, $\mathrm{Gal}(L|\mathbb{Q}) \subset \mathrm{Gal}(L|K)$.
Zwischen den Untergruppen von G und den Zwischenkörpern gibt es eine Eins-zu-Eins-Entsprechung (inklusionsumkehrende Bijektion). Zu jeder Untergruppe gehört ein Fixkörper.

12. Sei $f \in K[x]$ ein Polynom über einem Körper K mit dem Grad n.
    Ist f irreduzibel, so ist die Ordnung $|G(f)|$ der Galoisgruppe von f ein Vielfaches von n.

    Sei α eine Nullstelle von f, L der Zerfällungskörper von f.
    $K(\alpha) \subset L$, $[K(\alpha) : K] = n$, $[L : K] = |G(f)|$, beachte die Gradformel.

↑ Galois-Gruppe von $f = x^3 + px + q$

Sei $f = x^3 + px + q$, $p, q \in \mathbb{Q}$, ein irreduzibles Polynom mit den verschiedenen Nullstellen x_1, x_2, x_3.

Die Diskriminante lautet (siehe hier): $D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = -4p^3 - 27q^2$

1. Fall $\sqrt{D} \in \mathbb{Q}$ $\quad G = A_3$
Falls D ein Quadrat in $\mathbb{Q}$ ist, existiert eine rationale Zahl $\alpha \neq 0$ mit
$\alpha = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ (beachte: die Nullstellen sind verschieden).

Diese algebraische Relation muss von jedem Element der galoisschen Gruppe G erhalten bleiben. Damit kann G nur gerade Permutationen enthalten (sie bestehen aus einer geraden Anzahl von Transpositionen). G muss daher eine Untergruppe der alternierenden Gruppe A_3 sein (das Produkt von zwei geraden Permutationen ist wieder gerade). Keine echte Teilmenge von A_3 operiert transitiv auf den x_i (siehe Zusammenhänge 10.), somit folgt $G = A_3$. A_n enthält genau die Hälfte der Elemente der symmetrischen Gruppe S_n (Anzahl $n!$), da die Multiplikation mit einer Transposition alle ungeraden Permutationen ergibt. Die identische Permutation $\mathrm{id} = (1) = (12)(12)$ ist gerade.

2. Fall $\sqrt{D} \notin \mathbb{Q}$ $\quad G = S_3$
α ist kein Quadrat in den rationalen Zahlen. Es muss eine Symmetrie geben, welche D nicht invariant lässt (siehe Polynomring 13.). Das bedeutet, dass mindestens eine ungerade Permutation in G liegt. Da G transitiv auf x_1, x_2, x_3 operiert, muss G mindestens ein weiteres Element enthalten.

Ein genauerer Blick auf die 6-elementige Gruppe S_3 ergibt, dass wegen der Abgeschlossenheit der Verknüpfung von G $G = S_3$ ist.

$\circ$	(1)	(123)	(132)	(12)	(23)	(13)
(1)	(1)	(123)	(132)	(12)	(23)	(13)
(123)	(123)	(132)	(1)	(13)	(12)	(23)
(132)	(132)	(1)	(123)	(23)	(13)	(12)
(12)	(12)	(23)	(13)	(1)	(132)	(123)
(23)	(23)	(13)	(12)	(123)	(1)	(132)
(13)	(13)	(12)	(23)	(132)	(123)	(1)

$A_3 \subset S_3, \quad \sigma \circ \tau(i) = \sigma(\tau(i))$

$f = x^3 - 3x + 1$ ist irreduzibel ($f(x-1) = x^3 - 3x^2 + 3$ Eisenstein-Kriterium) und separabel über $\mathbb{Q}$ (siehe Zusammenhänge 9.), $D = -4(-3)^3 - 27(1)^2 = 81$. Die Galoisgruppe von f ist A_3.

↑ Permutationen und Galois-Gruppe von $f = x^5 - 5x + 1$

1. $(a_1 a_2 \dots a_k) = (a_1 a_k) \circ \dots \circ (a_1 a_3) \circ (a_1 a_2)$
   Jeder Zykel der Länge k lässt sich als Produkt von $k-1$ Transpositionen schreiben.

2. Schreibt man eine Permutation $\sigma \in S_n$ auf verschiedene Weise als Produkt von Transpositionen, so ist deren Anzahl entweder stets gerade oder stets ungerade.

   Betrachte für das n-Tupel (a, b, c, d, e) das Produkt

   $$\begin{aligned} P \;=\; & (a-b)(a-c)(a-d)(a-e) \\ & (b-c)(b-d)(b-e) \\ & (c-d)(c-e) \\ & (d-e) \end{aligned}$$

   P ist die Vandermonde-Determinante

   Die Vertauschung zweier benachbarter Elemente ändert das Vorzeichen von P, z. B. ergibt sich für das n-Tupel (a, c, b, d, e) :

   $$\begin{aligned} -P \;=\; & (a-c)(a-b)(a-d)(a-e) \\ & (c-b)(c-d)(c-e) \\ & (b-d)(b-e) \\ & (d-e) \end{aligned}$$

   □

3. $(a_1 a_2 \dots a_k)$ wird mit σ konjugiert.

   Für jede Permutation σ gilt $\quad \sigma \circ (a_1 a_2 \dots a_k) \circ \sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k))$.

   $\sigma \circ (a_1 a_2 \dots a_k) \circ \sigma^{-1}$ angewandt auf $\sigma(a_i)$ ergibt

   $$\sigma \circ (a_1 a_2 \dots a_k) \circ \sigma^{-1}(\sigma(a_i)) \;=\; \sigma \circ (a_1 a_2 \dots a_k)(a_i)) \;=\; \sigma(a_{i+1})$$ □

4. S_n wird von $\sigma = (12 \dots k)$ der Länge n (n-Zykel) und $\tau = (12)$ erzeugt, d. h. für eine Untergruppe $H \subset S_n$, die σ und τ enthält, gilt $H = S_n$.

   Für eine Transposition benachbarter Elemente gilt: $(i \;\; i+1) = \sigma^{i-1} \circ \tau \circ \sigma^{-(i-1)}$.
   Eine beliebige Transposition kann als Produkt von Transpositionen benachbarter Elemente geschrieben werden. □

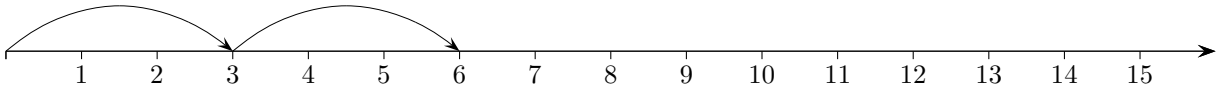
5. Sei $f \in \mathbb{Q}[x]$ irreduzibel vom Grad p, p Primzahl, mit genau zwei nicht-reellen Nullstellen in $\mathbb{C}$. Die Galois-Gruppe G ist S_p.

   Mit der komplexen Konjugation liegt ein Element (i, j) aus G vor, o.B.d.A. sei dies $(1, 2)$. Da f irreduzibel ist, ist p ein Teiler von $|G|$. Nach dem Satz von Cauchy hat G ein Element der Ordnung p. Stellt man dieses als Produkt disjunkter Zykel dar, so ist p das kgV der Längen. Mithin muss das Element ein p-Zykel $(1\, i \dots k)$ sein, beachte: die Schreibweise erlaubt eine zyklische Vertauschung der Elemente. Dann gibt es ein m mit $(12\dots) = (1\, i \dots k)^m$. Wegen $\mathrm{ggT}(m, p) = 1$ hat $(12\dots)$ ebenfalls die Ordnung p, ist also ein p-Zykel, z. B. $(13425)^3 = (12354)$. Mit 4. folgt die Behauptung. □

   Für $f = x^5 - 5x + 1$ ist $G = S_5$.
   3 reelle Nullstellen, siehe Graph von f, $f(x-1) = x^5 - 5x^4 + 10x^3 - 10x^2 + 5$ ist irreduzibel.

↑ Euklidischer Algorithmus

1. Welche Zahlen sind durch 3 teilbar?



Lösung: Alle Zahlen, die mit 3er-Schritten erreichbar sind, d. h. alle Vielfachen von 3, nämlich: 3, 6, 9, 12, 15, ...

2. Ist 7063 durch 7 teilbar?

Lösung: 7063 = 7000 + 63
Mit 1000 und anschließend 9 7er-Schritten ist die Zahl erreichbar.

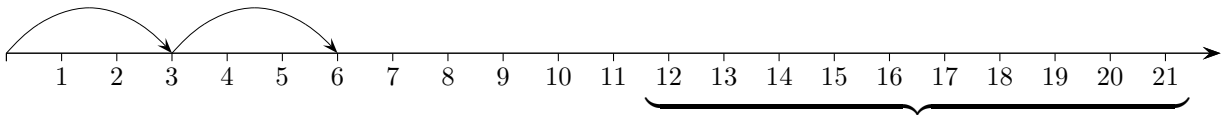
3. Ist 582 durch 3 teilbar?

Lösung: Um dies zu erkennen, gibt es eine einfache Regel. Hierzu zerlegen wir 582 geschickt:
$582 = 100 \cdot 5 + 10 \cdot 8 + 2$
$582 = 99 \cdot 5 + 1 \cdot \underline{5} + 9 \cdot 8 + 1 \cdot \underline{8} + \underline{2}$
Da 99 und 9 durch 3 teilbar sind, muss lediglich untersucht werden, ob dies auch für $\underbrace{5 + 8 + 2}$ *zutrifft.*
Dies ist die Quersumme von 582.

Eine Zahl ist durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

Die Zerlegung liefert auch eine Begründung für:
Eine Zahl ist durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

4. Wie lauten alle gemeinsamen Teiler von 12 und 21?



Wenn 12 mit einer bestimmten Schrittweite erreichbar ist und auch 21 mit dieser Schrittweite,
dann trifft dies auch für die Differenz $21 - 12 = 9$ zu (beachte die Schritte von 12 bis 21).
Statt die Teiler von 12 und 21 zu suchen, können daher auch die Teiler von 12 und 9 ermittelt werden. Offensichtlich gibt es nur den gemeinsamen Teiler 3. Die Bildung der Differenz kann wiederholt werden. Mit diesem Verfahren kann der größte gemeinsame Teiler (ggT) gefunden werden.

$\text{ggT}(52, 30) = 2$ Von unten nach oben gelesen erhält man daraus die Darstellung:

$$\begin{aligned} 52 &= 1 \cdot 30 + 22 \\ 30 &= 1 \cdot 22 + 8 \\ 22 &= 2 \cdot 8 + 6 \\ 8 &= 1 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

$$\begin{aligned} 2 &= 3 \cdot 30 - 4 \cdot (52 - 30) = 7 \cdot 30 - 4 \cdot 52 \\ &= 3 \cdot (30 - 22) - 22 \quad = 3 \cdot 30 - 4 \cdot 22 \\ &= 8 - (22 - 2 \cdot 8) \quad = 3 \cdot 8 - 22 \\ 2 &= 8 - 6 \end{aligned}$$

Mit der vorletzten Zeile beginnen.

$\text{ggT}(48, 5) = 1$ Von unten nach oben gelesen erhält man daraus die Darstellung:

$$\begin{aligned} 48 &= 9 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 2 \cdot (48 - 9 \cdot 5) - 5 = 2 \cdot 48 - 19 \cdot 5 \\ &= 3 - (5 - 3) \quad = 2 \cdot 3 - 5 \\ 1 &= 3 - 2 \end{aligned}$$

Damit ist gezeigt, dass

$$1 = 2 \cdot 48 - 19 \cdot 5$$

gilt, woraus

$$-19 \cdot 5 \mod 48 = 1$$

folgt.

Addieren wir auf der linken Seite noch $48 \cdot 5$ (was auf der rechten Seite nichts ändert, da wir modulo 48 rechnen) erhalten wir

$$29 \cdot 5 \mod 48 = 1$$

Satz von Bézout
Seien $a, b \in \mathbb{N}_0$. Der größte gemeinsame Teiler $\text{ggT}(a, b)$ lässt sich als ganzzahlige Linearkombination von a und b darstellen:

$$\text{ggT}(a, b) = u \cdot a + v \cdot b \quad \text{mit } u, v \in \mathbb{Z}.$$

Die Darstellung ist nicht eindeutig,
die Gleichung wird durch verschiedene Zahlenpaare u, v erfüllt.

$$\begin{aligned} \text{ggT}(16, 6) = 2 &= -1 \cdot 16 + 3 \cdot 6 \\ &= \quad 2 \cdot 16 - 5 \cdot 6 \end{aligned}$$

↑ Polynomring

Der Polynomring $\mathbb{Q}[x]$ hat viele Eigenschaften, die man von den ganzen Zahlen $\mathbb{Z}$ kennt.

1. Eine Division mit Rest erfolgt mit der Polynomdivision.
   Seien $f(x)$ und $g(x)$ Polynome, $g(x)$ normiert. Dann existieren eindeutig bestimmte Polynome $q(x)$ und $r(x)$ mit $f(x) = q(x) \cdot g(x) + r(x)$ und grad $r(x) <$ grad $g(x)$.

2. Je zwei Polynome besitzen einen größten gemeinsamen Teiler.

3. Der größte gemeinsame Teiler von zwei Polynomen $f(x)$ und $g(x)$ besitzt eine Darstellung $\mathrm{ggT}(f(x), g(x)) = u(x)f(x) + v(x)g(x)$ mit geeignet gewählten Polynomen $u(x)$ und $v(x)$. Die Berechnung kann mit dem Euklidischen Algorithmus erfolgen.
   Aus $\mathrm{ggT}(f(x), g(x)) = 1$ folgt $1 = u(\alpha)f(\alpha)$ für $g(\alpha) = 0$, also $f^{-1}(\alpha) = u(\alpha)$.

4. Seien $f(x)$ und $g(x)$ zwei normierte Polynome aus $\mathbb{Q}[x]$ mit einer gemeinsamen Nullstelle. Ist dann $f(x)$ irreduzibel (prim, $f(x)$ lässt sich nicht als Produkt von Polynomen kleineren Grades schreiben), so teilt $f(x)$ das Polynom $g(x)$.

   Zwei irreduzible normierte Polynome aus $\mathbb{Q}[x]$ sind somit schon gleich, wenn sie eine gemeinsame Nullstelle besitzen.

5. Jedes Polynom besitzt über den rationalen Zahlen eine bis auf die Reihenfolge eindeutige Zerlegung in irreduzible Faktoren.

6. Ist das normierte irreduzible Polynom $f(x)$ Teiler von $g(x) \cdot h(x)$, so teilt $f(x)$ (mindestens) einen der beiden Faktoren.
   In diesem Sinne verhält sich ein normiertes irreduzibles Polynom wie eine Primzahl in $\mathbb{Z}$.

7. Jede algebraische Zahl x ist Nullstelle genau eines normierten irreduziblen Polynoms mit rationalen Koeffizienten. Dieses Polynom heißt das Minimalpolynom von x.

8. Die Zerlegung eines Polynoms in irreduzible Faktoren ist, abgesehen von der Reihenfolge und Konstanten, eindeutig.
   Beachte: Im Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$ ist dies nicht so, $20 = 4 \cdot 5$,
   $20 = (2 + 6\mathrm{i})(1 - 3\mathrm{i})$.

9. Ein irreduzibles normiertes Polynom über den rationalen Zahlen hat keine doppelten Nullstellen (ist separabel).

10. Zu jedem normierten Polynom gibt es genau eine normiertes Polynom, das die gleichen Nullstellen besitzt, diese aber jeweils mit der Vielfachheit 1.

11. Fundamentalsatz der Algebra
    Jedes Polynom mit komplexen Koeffizienten $f(x)$ vom Grad n besitzt genau n, möglicherweise mehrfach zu zählende, komplexe Nullstellen und zerfällt daher vollständig in Linearfaktoren, $f(x) = (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n)$ mit $x_i \in \mathbb{C}$.

12. Ein Polynom in n Variablen heißt symmetrisch, wenn es sich unter Vertauschen der Variablen nicht ändert.
Die Koeffizienten einer normierten Polynomgleichung sind bis auf Vorzeichen die elementarsymmetrischen Funktionen in den Lösungen x_i.
$x^2 - (x_1 + x_2)x + x_1x_2 = 0,$ $\qquad (x - x_1)(x - x_2) = 0$
$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3 = 0,$ $\qquad (x - x_1)(x - x_2)(x - x_3) = 0$

13. Jedes in $x_1, \ldots, x_n$ symmetrische Polynom lässt sich als Polynom in den elementarsymmetrischen Polynomen darstellen, siehe hier, z. B.
$$x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2(x_1x_2)$$
$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3)$$
$$x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 = (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) - 3x_1x_2x_3$$

Vielfache Argumentation ($n = 4$, a, b, c, d rational):

$$\begin{aligned} f = x^4 + ax^3 + bx^2 + cx + d &= (x - x_1)(x - x_2)(x - x_3)(x - x_4) \\ &= x^4 - (x_1 + x_2 + x_3 + x_4)x^3 \\ &\quad + (x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3x_4)x^2 \\ &\quad - (x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)x \; + \; x_1x_2x_3x_4 \end{aligned}$$

Für das Polynom f bedeutet das:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= -a \\ x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3x_4 &= b \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 &= -c \\ x_1x_2x_3x_4 &= d \end{aligned}$$

Ein in $x_1, \ldots, x_4$ symmetrisches Polynom mit rationalen Koeffizienten ist eine rationale Zahl.

Es gilt auch die schwächere Bedingung:
Ist ein Polynom in $x_1, \ldots, x_n$ invariant bezüglich der Symmetrien der Galois-Gruppe, dann ist es eine rationale Zahl ($\mathbb{Q}$ ist der Fixkörper).

Beweis
$z = g(x_1, \ldots, x_n) = g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = g(h_1(t_\sigma), \ldots, h_n(t_\sigma)),$ siehe Zusammenhänge 4.
Summiert man die verschiedenen Darstellungen des Wertes z über die Permutationen der Galois-Gruppe G, ergibt das:
$$|G| \cdot z = \sum_{\sigma \in G} g(h_1(t_\sigma), \ldots, h_n(t_\sigma))$$
Die t_σ, $\sigma \in G$, sind die Nullstellen des Minimalpolynoms, der Summenterm ist symmetrisch in den Werten t_σ und kann daher polynomial durch die elementarsymmetrischen Polynome der t_σ, also durch die rationalen Koeffizienten des Minimalpolynoms ausgedrückt werden.
z ist rational.

Hier befindet sich die Nahtstelle zur modernen Galois-Theorie nach Dedekind und Artin, die von einer endlichen Körpererweiterung L von K und der Gruppe aller Automorphismen von L ausgeht, die K elementweise fest lassen (K ist der Fixkörper).
↑

$$x^8 - 8x^7 + 24x^6 - 32x^5 + 18x^4 - 8x^3 + 8x^2 - 1 = 0$$

$$x_i = 1 \pm \sqrt{1 \pm \sqrt{-1 \pm \sqrt{2}}}$$

Galois 1811-1832 wurde von Fragestellungen um Polynomgleichungen und deren Lösungen durch Wurzelterme gefesselt. Er fand heraus, dass die Nullstellen eines Polynoms f genau dann durch Wurzelterme ausgedrückt werden können, wenn die Symmetriegruppe von f bestimmte Untersymmetriegruppen enthält ...

↑

Äquivalenzrelation, Restklassen, Kleiner Satz von Fermat, Satz von Euler

Galois-Theorie Anfänge

Hauptsatz über elementarsymmetrische Polynome

Startseite