# Inhaltsverzeichnis

## Lösungsvorschlag zu Blatt 3, Aufgabe 5

Seien $a_0, \dots, a_{n-1} \in \mathbb{Q}$.

Sei $z \in \mathbb{C}$ mit $z$ transzendent. $\quad =: c$

Beh.: $z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$ ist transzendent.

Bew.: Angenommen, diese Zahl wäre algebraisch.
Dann gäbe es eine Polynomgleichung mit rationalen Koeffizienten, die normiert ist und $c$ als Lösung besitzt:

$$c^m + b_{m-1} c^{m-1} + \dots + b_1 c + b_0 = 0.$$

Ausgeschrieben:

$$\left(z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0\right)^m + b_{m-1} \left(z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0\right)^{m-1} + \dots + b_0 = 0.$$

Multipliziert man die Klammern aus, erkennt man, dass diese Gleichung auch eine normierte Polynomgleichung mit rationalen Koeffizienten ist, die $z$ als Lösung besitzt.
Aber das ist ein Widerspruch zur Transzendenz von $z$.

### Alternativbeweis:

Angenommen, $c$ wäre algebraisch.
Dann betrachte folgende Gleichung:

$$X^n + a_{n-1} X^{n-1} + \dots + a_1 X + (a_0 - c) = 0$$

Dies ist eine normierte Polynomgleichung mit Koeffizienten

$$a_{n-1}, a_{n-2}, \dots, a_2, a_1, a_0 - c;$$

diese sind alle algebraisch.
Weiter ist $z$ eine Lösung dieser Gleichung:

$$z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 - \left(z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0\right) = 0$$

Nach einem Satz der Vorlesung ist daher $z$ algebraisch.
Aber das ist ein Widerspruch zur Transzendenz von $z$.

Lösungsvorschlag zu Blatt 3, Aufgabe 6

(a) Sei $\zeta$ eine vierte Einheitswurzel, d.h. $\zeta \in \mathbb{C}$ mit $\zeta^4 = 1$.
Sei $\Theta$ eine sechste Einheitswurzel, d.h. $\Theta \in \mathbb{C}$ mit $\Theta^6 = 1$.

Beh.: $\zeta\Theta$ ist eine zwölfte Einheitswurzel.

Bew.: Zu zeigen ist: $(\zeta\Theta)^{12} = 1$.
Also: $(\zeta\Theta)^{12} = \zeta^{12}\Theta^{12} = (\zeta^4)^3(\Theta^6)^2 = 1^3 \cdot 1^2 = 1$. ✓

(b) Seien $m, n \geq 1$ mit $ggT(m,n)$.
Sei $\zeta$ eine $m$-te Einheitswurzel und $\Theta$ eine $n$-te Einheitswurzel.

Beh.: $\zeta\Theta$ ist eine $k$-te Einheitswurzel, wobei $k := mn/(m,n)$.

Bew.: Wir schreiben zunächst $m$ und $n$ als Vielfache ihres ggT:

$$m = (m,n)\,\tilde{m}$$
$$n = (m,n)\,\tilde{n}.$$

Dann gilt:

$$(\zeta\Theta)^k = (\zeta\Theta)^{mn/(m,n)} = (\zeta\Theta)^{\tilde{m}\tilde{n}(m,n)}$$
$$= \left(\zeta^{\tilde{m}(m,n)}\right)^{\tilde{n}} \left(\Theta^{\tilde{n}(m,n)}\right)^{\tilde{m}}$$
$$= (\zeta^m)^{\tilde{n}} (\Theta^n)^{\tilde{m}} = 1^{\tilde{n}} 1^{\tilde{m}} = 1.$$ ✓

Warnung: Komplexe Zahlen kann man nicht ohne Weiteres mit rationalen Exponenten potenzieren. Insbesondere sind Wurzeln (Exponent $1/2$ für die Quadratwurzel, Exponent $1/n$ für die $n$-te Wurzel) nicht wohldefiniert.
Mit „wohldefiniert" ist hier gemeint: Es gibt i.A. mehrere Zahlen, die alle gleiches Recht haben, sich zu einer gegebenen Zahl „Wurzel" zu nennen. (So gibt es beispielsweise $n$ verschiedene $n$-te Einheitswurzeln.)

Warnung: Folgende Rechnung ist nicht zulässig:

$$-1 = i^2 = i \cdot i = \sqrt{-1} \cdot \sqrt{-1} = \sqrt{(-1)(-1)} = \sqrt{1} = 1.$$

Blatt 4, Aufgabe 7

Sei $f$ ein Polynom mit $\deg f \leq n$, also

$$f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0,$$

wobei einige der $a_i$, auch die ersten, vielleicht null sind, da die Voraussetzung nicht $\deg f = n$, sondern nur $\deg f \leq n$ lautet.

Sei weiter $g$ ein Polynom mit $\deg g \leq m$, also

$$g = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0.$$

Beh.: $\deg(f+g) \leq \max\{n, m\}$.

Beweis: $f + g = a_n X^n + \dots + a_0 + b_m X^m + \dots + b_0$

dann sieht man, dass die höchste Potenz, die vorkommen kann, $\max\{n,m\}$ ist.

Bem.: Wegen Auslöschungseffekten gilt i. A. nicht $\deg(f+g) = \max\{\deg f, \deg g\}$.
Ein mögliches Gegenbeispiel ist:

$$(X^3 + 5X^2 - 9) + (-X^3 + 11X) = 5X^2 + 11X - 9$$

hat kleineren Grad als die Summanden!

Beh.: $\deg(fg) \leq n+m$.

Beweis: $fg = (a_n X^n + \dots + a_0)(b_m X^m + \dots + b_0) = a_n b_m X^{n+m} + a_n b_{m-1} X^{n+m-1} + \dots + a_0 b_0$,

ausmultiplizieren

daran sieht man,
dass die höchste Potenz,
die vorkommen kann, $n+m$ ist.

Lösungsvorschlag zu Aufgabe 8, Blatt 3

Sei: $z = r e^{i\phi}$ mit $r \in \mathbb{R}$, $r > 0$ und $\phi \in \mathbb{R}$ gegeben.

Sei $z$ algebraisch.

Behauptung: $|z| = r$ ist algebraisch.

Beweis: Zunächst zeigen wir ganz allgemein:

Behauptung: Ist $u$ algebraisch, dann auch $\bar{u}$.

Beweis: Da $u$ algebraisch ist, gibt es eine normierte Polynomgleichung mit rationalen Koeffizienten, die $u$ als Nullstelle besitzt:

$$u^n + a_{n-1} u^{n-1} + \dots + a_1 u + a_0 = 0.$$

Wir behaupten nun: $\bar{u}$ ist auch eine Lösung der Gleichung

$$X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 = 0.$$

Denn:

$$\begin{aligned}
&\bar{u}^n + a_{n-1} \bar{u}^{n-1} + \dots + a_1 \bar{u} + a_0 \\
&= \overline{u^n} + a_{n-1} \overline{u^{n-1}} + \dots + a_1 \bar{u} + a_0 \\
&= \overline{u^n} + \overline{a_{n-1}}\, \overline{u^{n-1}} + \dots + \overline{a_1}\, \bar{u} + \overline{a_0} \\
&\overset{a_i \in \mathbb{Q} \subseteq \mathbb{R}}{=} \overline{u^n + a_{n-1} u^{n-1} + \dots + a_1 u + a_0} = \bar{0} = 0. \quad \checkmark
\end{aligned}$$

Zurück zur eigentlichen Aufgabe. Wir wollen $z\bar{z}$ ausrechnen.

$$z\bar{z} = r e^{i\phi} \cdot e^{-i\phi} = r^2 e^{i\phi - i\phi} = r^2 e^0 = r^2 \cdot 1 = r^2.$$

Da $z$ und nach der Vorüberlegung auch $\bar{z}$ algebraisch ist, ist somit $r^2$ algebraisch. Aus der Vorlesung ist bekannt, dass Wurzeln algebraischer Zahlen wieder algebraisch sind. Somit ist auch $r$ wieder algebraisch.

Alternativbeweis: (benötigt auch die Vorüberlegung)

Wir wissen, dass $\operatorname{Re} z = \frac{1}{2}(z + \bar{z})$. Somit ist, da $z$, $\bar{z}$ und $\frac{1}{2}$ algebraisch sind, auch $\operatorname{Re} z$ algebraisch.

Ferner können wir wegen $\operatorname{Im} z = \frac{1}{2i}(z - \bar{z})$ folgern, dass auch $\operatorname{Im} z$ algebraisch ist.

Es folgt, dass

$$r = |z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}$$

als Wurzel der Summe der Quadrate algebraischer Zahlen algebraisch ist.

Blatt 3, Aufgabe 9

Gesucht: Alle Lösungen von $x^6 + 1 = 0$.

Über Formel aus Skript:

$x^6 + 1 = 0 \iff x^6 = -1 = e^{i\pi}$.

$\rightsquigarrow$ die Lösungen sind $z_1, \dots, z_6$ mit

$$z_k = e^{(2\pi i k + \pi i)/6}, \quad k = 1, \dots, 6.$$

Über eigene Rechnung:

Sei: $z \in \mathbb{C}$ beliebig. Dann gilt:

$z^6 + 1 = 0$

$\iff z^6 + 1 = 0$ und $z \neq 0$

$\iff (re^{i\varphi})^6 + 1 = 0$

↖ da $z \neq 0$, lässt sich $z$ schreiben als $z = re^{i\varphi}$ für ein $r \in \mathbb{R}$, $\varphi \in \mathbb{R}$, $r > 0$.

$\iff r^6 e^{6i\varphi} = -1 = e^{i\pi}$

$\iff r^6 \cdot e^{6i\varphi} = 1 \cdot e^{i\pi}$

$\iff r^6 = 1$ und $6\varphi - \pi$ Vielfaches von $2\pi$

↖ Vergleich der Radien und Winkel

$\iff r = 1$ und $6\varphi - \pi = 2\pi k$ für ein $k \in \mathbb{Z}$

$\iff r = 1$ und $\varphi = (2\pi k + \pi)/6$ — " —

Also sind die Lösungen alle Zahlen der Form

$1 \cdot e^{i(2\pi k + \pi)/6}$, $k \in \mathbb{Z}$. ($k = 0, \dots, 5$ genügt, da sich danach die Lösungen wiederholen.)

In beiden Fällen war dann noch die Darstellung in kartesischer Scheibweise verlangt.

Das geht so:

$$z_k = e^{i(2\pi k + \pi)/6} = \cos((2\pi k + \pi)/6) + i \sin((2\pi k + \pi)/6),$$

Lösungsvorschlag zu Blatt 3, Aufgabe 10

Gesucht: Eine normierte Polynomgleichung (mit komplexen Koeffizienten), die die sieben Ecken des regelmäßigen 7-Ecks mit Zentrum = Ursprung und einer Ecke = $1+\frac{1}{2}i$ als Nullstellen besitzt.

Betrachte

$$X^7 - \left(1+\tfrac{1}{2}i\right)^7 = 0.$$

Das ist eine normierte Polynomgleichung, die zumindest $1+\frac{1}{2}i$ als Lösung besitzt. Die anderen sechs Ecken müssen auch Nullstellen sein; vgl. Anschauung der Einheitswurzeln.

Lösungsvorschlag zu Blatt 3, Aufgabe 11(b)

Sei $p(X) := X^{n-1} + X^{n-2} + \dots + X + 1 = 0$.

Beh.: Die Gleichung $p(X) = 0$ besitzt als Lösungen genau die $n$-ten Einheitswurzeln mit Ausnahme der 1.

↑ nicht mehr, nicht weniger

Beweis: Sei $z \in \mathbb{C}$ beliebig. Dann gilt:

$p(z) = 0$

$\overset{(*)}{\iff}$ $p(z) = 0$ und $z \neq 1$

$\overset{(\#)}{\iff}$ $p(z)(z-1) = 0$ und $z \neq 1$

$= (z^{n-1} + z^{n-2} + \dots + z + 1)(z-1) =$

$= z^n + z^{n-1} + \dots + z^2 + z$

$\quad - z^{n-1} - \dots - z^2 - z - 1$

$= z^n - 1$

$\iff$ $z^n - 1 = 0$ und $z \neq 1$

$\iff$ $z^n = 1$ und $z \neq 1$

$\iff$ $z$ ist eine $n$-te Einheitswurzel, aber nicht 1.

Zu (*): „$\Rightarrow$": Sei $p(z) = 0$, zu zeigen: $p(z) = 0$ und $z \neq 1$.

Angenommen nicht, also $z = 1$.
Dann $p(z) = 0 = z^{n-1} + \dots + z + 1$
$= 1 + \dots + 1 + 1$
$= n$, ↯

„$\Leftarrow$": Sei $p(z) = 0$ und $z \neq 1$, zu zeigen: $p(z) = 0$.

klar.

Zu (#): „$\Rightarrow$": Sei $p(z) = 0$ und $z \neq 1$, zu zeigen:
$p(z)(z-1) = 0$ und $z \neq 1$

$= 0 \cdot (z-1) = 0$ ✓ klar

„$\Leftarrow$": Sei $p(z)(z-1) = 0$ und $z \neq 1$, zu zeigen:
$p(z) = 0$ und $z \neq 1$.

klar

klar, da Produkt genau dann null, wenn (mindestens einer der Faktoren null)

Blatt 3, Aufgabe 12

Beh.: Die Additionstheoreme für Sinus und Kosinus.

Beweis: $\exp((x+y)i) = \cos(x+y) + i\sin(x+y)$

$\exp(xi)\exp(yi) = (\cos(x) + i\sin(x)) \cdot (\cos(y) + i\sin(y))$

$= \underbrace{(\cos(x)\cos(y) - \sin(x)\sin(y))}_{\Leftarrow \cos(x+y) =} + i\underbrace{(\cos(x)\sin(y) + \sin(x)\cos(y))}_{\Leftarrow \sin(x+y) =}$

$\Rightarrow$ Vergleich der Real- und Imaginärteile

Blatt 4, Aufgabe 12

Seien $p, q, f, g \in \bar{\mathbb{Q}}[X]$ („Polynome mit algebraischen Koeffizienten").
Sei $d$ ein weiteres Polynom mit
$d \mid f$ und $d \mid g$.

Beh.: $d \mid pf + qg$.

Bew.: Wegen $d \mid f$ gibt es ein $\tilde{f}$ mit $f = d\tilde{f}$.
Wegen $d \mid g$ gibt es ein $\tilde{g}$ mit $g = d\tilde{g}$.
Es folgt
$$pf + qg = dp\tilde{f} + dq\tilde{g} = d(p\tilde{f} + q\tilde{g}),$$
also ist $pf + qg$ ein Vielfaches von $d$, also ist $d$ ein Teiler von $pf + qg$.

## Blatt 4, Aufgabe 16

Sei $t \in \mathbb{C}$. Es gelte $\mathbb{Q}[t] = \mathbb{Q}(t)$.

Beh.: $t$ ist algebraisch.

Zur Erinnerung:

$$\mathbb{Q}[X] = \left\{ \sum_{k=0}^{N} a_k X^k \mid N \geq 0,\ a_0, \dots, a_N \in \mathbb{Q} \right\}$$

(Menge der Polynome in der Variablen $X$ mit rationalen Koeffizienten)

$$\mathbb{Q}[t] = \left\{ \sum_{k=0}^{N} a_k t^k \mid \text{---}''\text{---} \right\} \subseteq \mathbb{C}$$

(Menge der polynomiellen Ausdrücke (mit rationalen Koeffizienten) in $t$)

Elemente von $\mathbb{Q}[X]$ sind also Polynome, während Elemente von $\mathbb{Q}[t]$ Zahlen sind.

Ferner:

$$\mathbb{Q}(t) = \left\{ \frac{x}{y} \mid x \in \mathbb{Q}[t],\ y \in \mathbb{Q}[t],\ y \neq 0 \right\} \subseteq \mathbb{C}.$$

Nun zum Beweis.

Bew.: 1. Fall: $t = 0$. Dann ist $t$ auch algebraisch.

2. Fall: $t \neq 0$. Dann gilt sicherlich $\frac{1}{t} \in \mathbb{Q}(t)$, da Zähler und Nenner trivialerweise polynomielle Ausdrücke in $t$ sind.

Wegen $\mathbb{Q}(t) = \mathbb{Q}[t]$ folgt, dass $\frac{1}{t}$ auch ein in $t$ polynomieller Ausdruck ist.

Es gibt also ein Polynom $p \in \mathbb{Q}[X]$ mit:

$$\frac{1}{t} = p(t).$$

Dieses Polynom ist nicht das Nullpolynom, da sonst $\frac{1}{t} = 0$ wäre, was nicht gelt.

Es folgt

$$0 = p(t)\,t - 1,$$

also löst $t$ die Polynomgleichung

$$0 = p(X)X - 1.$$

Das Polynom dieser ~~Gleichung~~ ist vielleicht noch nicht normiert, aber da es nicht das Nullpolynom ist, können wir es normieren.

Folglich ist $t$ Nullstelle eines normierten Polynoms mit rationalen Koeffizienten, das war zu zeigen.

Blatt 4, Aufgabe 5

Sei $X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 = 0$ eine normierte Polynomgleichung mit komplexen Koeffizienten.

Beh.: Jede Lösung $z$ dieser Gleichung erfüllt die Ungleichung

$$|z| \leq 1 + m,$$

wobei $m := \max\{|a_0|, \dots, |a_{n-1}|\}$.

Bew.: Wir zeigen umgekehrt: Ist $z$ eine beliebige komplexe Zahl mit $|z| > 1+m$, so kann sie keine Lösung der Gleichung sein.
Um wiederum das zu zeigen, beweisen wir, dass $|f(z)| > 0$ für solche $z$ mit $|z| > 1+m$.

Also:

$$|f(z)| = |z^n - (-a_{n-1}z^{n-1} - \dots - a_1 z - a_0)|$$

$$\geq |z^n| - |-a_{n-1}z^{n-1} - \dots - a_1 z - a_0|$$

(umgekehrte Dreiecksungleichung; Dreiecksungleichung)

$$= |a_{n-1}z^{n-1} + \dots + a_1 z + a_0| \leq |a_{n-1}z^{n-1}| + \dots + |a_1 z| + |a_0|$$

$$\leq |a_{n-1}|\,|z|^{n-1} + \dots + |a_1|\,|z| + |a_0|$$

$$\leq m|z|^{n-1} + \dots + m|z| + m$$

$$= m(|z|^{n-1} + \dots + |z|^0)$$

$$= m\,\frac{|z|^n - 1}{|z| - 1} \leq m\,\frac{|z|^n - 1}{1+m-1} = |z|^n - 1$$

($\leq$: $|z| > 1+m \Rightarrow |z| - 1 > 1 + m - 1$; Zähler $> 0$: $\frac{|z|^n - 1}{|z|-1} \leq \frac{|z|^n - 1}{1+m-1}$)

$$\geq |z|^n - (|z|^n - 1) = 1 > 0.$$

Lösungsvorschlag zu Blatt 5, Aufgabe 3

Seien $g, h$ Polynome.

Beh.: $(gh)^{(k)} = \sum_{\substack{i+j=k \\ i,j\geq 0}} \binom{k}{i} g^{(i)} h^{(j)}$ für alle $k \geq 0$ (oder $k \geq 1$),

wobei wir die Konvention $\binom{k}{i} = 0$ für $i < 0$ und für $i > k$ vereinbaren; damit ist die Summe auf jeden Fall endlich.

Bew.: Induktion über $k$:

- $\underline{k=0}$: $(gh)^{(0)} = gh = \binom{0}{0} g^{(0)} h^{(0)} = \sum_{\substack{i+j=0 \\ i,j\geq 0}} \binom{k}{i} g^{(i)} h^{(j)}$ ✓

(Oder, wenn man bei $k=1$ beginnen möchte:

- $\underline{k=1}$: $(gh)^{(1)} = (gh)' \overset{\text{Def}}{=} g'h + gh' = \binom{1}{1} g^{(1)} h^{(1-1)} + \binom{1}{0} g^{(0)} h^{(1-0)}$

$= \sum_{\substack{i+j=1 \\ i,j\geq 0}} \binom{1}{i} g^{(i)} h^{(j)}$ ✓

- $\underline{k \to k+1}$: $(gh)^{(k+1)} = ((gh)')^{(k)} \overset{\text{Def}}{=} (g'h + gh')^{(k)} = (g'h)^{(k)} + (gh')^{(k)}$

$\overset{\text{IV}}{=} \sum_{\substack{i+j=k \\ i,j\geq 0}} \binom{k}{i} (g')^{(i)} h^{(j)} + \sum_{\substack{i+j=k \\ i,j\geq 0}} \binom{k}{i} g^{(i)} (h')^{(j)}$

$= \sum_{\substack{i+j=k \\ i,j\geq 0}} \binom{k}{i} g^{(i+1)} h^{(j)} + \sum_{\substack{i+j=k \\ i,j\geq 0}} \binom{k}{i} g^{(i)} h^{(j+1)}$

$= \sum_{\substack{\hat{i}+j=k+1 \\ \hat{i}\geq 1,\ j\geq 0}} \binom{k}{\hat{i}-1} g^{(\hat{i})} h^{(j)}$ (Indexverschiebung: $\hat{i} := i+1$, $\hat{j} := j$)

$= \sum_{\substack{i+\hat{j}=k+1 \\ i\geq 0,\ \hat{j}\geq 1}} \binom{k}{i} g^{(i)} h^{(\hat{j})}$ (Indexverschiebung: $\hat{i} := i$, $\hat{j} := j+1$)

$= \sum_{\substack{\hat{i}+j=k+1 \\ \hat{i}\geq 1,\ j\geq 0}} \binom{k}{\hat{i}-1} g^{(\hat{i})} h^{(j)} + \sum_{\substack{\hat{i}+j=k+1 \\ \hat{i}\geq 0,\ \hat{j}\geq 1}} \binom{k}{\hat{i}} g^{(\hat{i})} h^{(\hat{j})} = \sum_{\substack{\hat{i}+\hat{j}=k+1 \\ \hat{i},\hat{j}\geq 0}} \binom{k+1}{\hat{i}} g^{(\hat{i})} h^{(\hat{j})}$ ✓

($\binom{k}{\hat{i}-1} = 0$ für $\hat{i} = 0$, $\binom{k}{\hat{i}} = 0$ für $\hat{i} = k+1$)

($\binom{k}{\hat{i}-1} + \binom{k}{\hat{i}} = \binom{k+1}{\hat{i}}$)

Lösungsvorschlag zu Blatt 6, Aufgabe 6

Sei $f = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \in \overline{\mathbb{Q}}[X]$ mit Lösungen $x_1, \dots, x_n \in \overline{\mathbb{Q}}$.

Sei $g = Y^m + b_{m-1}Y^{m-1} + \dots + b_1 Y + b_0 \in \overline{\mathbb{Q}}[Y]$ mit Lösungen $y_1, \dots, y_m \in \overline{\mathbb{Q}}$.

Beh. Der Ausdruck $R = \prod_{\substack{1 \le i \le n \\ 1 \le j \le m}} (x_i - y_j) \in \overline{\mathbb{Q}}$ lässt sich als Polynom in den Koeffizienten $a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1}$ der beiden Polynome schreiben.

Bew: Schritt 1: Wir definieren ein Polynom

$$P = \prod_{i,j} (X_i - Y_j). \qquad \text{(Großbuchstaben!)}$$

Dieses ist eigentlich ein Polynom aus $\overline{\mathbb{Q}}[X_1, \dots, X_n, Y_1, \dots, Y_m]$, wir können es aber auch als Polynom aus $(\overline{\mathbb{Q}}[Y_1, \dots, Y_m])[X_1, \dots, X_n]$ auffassen. Für uns sind also die $X_i$ die Unbestimmten des Polynoms, und die Koeffizienten des Polynoms sind wiederum Polynome, in den Unbestimmten $Y_1, \dots, Y_m$.

So aufgefasst, ist $P$ symmetrisch (in den $X_i$). Nach Vorlesung folgt daher:

$$\prod_{i,j} (x_i - Y_j) = H(a_0, \dots a_{n-1}), \qquad (*)$$

für ein Polynom $H$ mit Koeffizienten aus derselben Menge, wie auch $P$ nach unserer Auffassung hat, also $\overline{\mathbb{Q}}[Y_1, \dots, Y_m]$.

linke Seite: $P$, wobei man die Lösungen $x_i$ für die Variablen $X_i$ eingesetzt hat.

rechte Seite: $H$ ist ein Polynom mit Koeffizienten aus $\overline{\mathbb{Q}}[Y_1, \dots, Y_m]$, also ist die rechte Seite ein Element von $\overline{\mathbb{Q}}[Y_1, \dots, Y_m]$.

↓

Schritt 2: Die rechte Seite von (*),

$H(a_0, \dots, a_{n-1})$,

ist eigentlich ein Element aus $\bar{\mathbb{Q}}[Y_1, \dots, Y_m]$.
Jetzt können wir das auch sagen, dass es ein Element von

$(\bar{\mathbb{Q}}[a_0, \dots, a_{n-1}])[Y_1, \dots, Y_m]$

ist.

So aufgefasst, ist es als Polynom in den $Y_j$ symmetrisch.
Nach Vorlesung folgt daher:

$H(a_0, \dots, a_{n-1})$, wobei man $y_j$ für $Y_j$ einsetzt $= L(b_0, \dots, b_{m-1})$

für ein Polynom $L$. Die Koeffizienten von $L$ stammen aus derselben Menge, aus denen auch die Koeffizienten von $\bullet$ stammen, also

$\bar{\mathbb{Q}}[a_0, \dots, a_{n-1}]$.

Fazit: Die rechte Seite, $L(b_0, \dots, b_{m-1})$ ist ein polynomieller Ausdruck in

$a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1}$.

Die linke Seite ergibt sich als:

$LS = H(a_0, \dots, a_{n-1})$, wobei man $y_j$ für $Y_j$ einsetzt

$\overset{(*)}{=} \prod_{i,j} (x_i - Y_j)$, ——— " ———

$= \prod_{i,j} (x_i - y_j) = R$.

Damit ist die Behauptung gezeigt.

Bem.: Zweimal haben wir einen Satz der Vorlesung verwendet. Dieser wurde da eigentlich nur für Polynome mit algebraischen Koeffizienten, und nicht für Polynome mit Koeffizienten, die wiederum Polynome sind, bewiesen. Der Beweis lässt sich aber ohne Änderungen auf die allgemeinere Situation übertragen.

Aufgabe 7 zeigt eine Anwendung dieser Aufgabe.

Lösungsvorschlag zu Blatt 6, Aufgabe 7

Gegeben: Gleichungen $X^2 + aX + b = 0$, $Y^2 + cX + d = 0$.

Gesucht: Ein in $a, b, c, d$ polynomieller Ausdruck, der genau dann 0 ist, wenn die beiden Gleichungen eine (mind.) eine gemeinsame Lösung besitzen.

Idee: Der Ausdruck

$$R = (x_1 - y_1)(x_1 - y_2)(x_2 - y_1)(x_2 - y_2),$$

wobei $x_1, x_2$ die Lösungen der ersten und $y_1, y_2$ die Lösungen der zweiten Gleichung sind, erfüllt zumindest diese genau-dann-0-wenn-gemeinsame-Lösungen-Bedingung.

Zu zeigen ist nur noch, dass er sich als Polynom in $a, b, c, d$ schreiben lässt. Durch Aufgabe 6 wissen wir, dass das auf jeden Fall möglich ist; wir müssen nur noch die Rechnung ausführen.

Also: $R = (x_1 - y_1)(x_1 - y_2)(x_2 - y_1)(x_2 - y_2)$

$= x_1^2 x_2^2 - x_1^2 x_2 y_2 - x_1^2 x_2 y_1 + x_1^2 y_1 y_2$

$- x_1 x_2^2 y_2 + x_1 x_2 y_2^2 + x_1 x_2 y_1 y_2 - x_1 y_1 y_2^2$

$= (x_1^2 - x_1 y_2 - x_1 y_1 + y_1 y_2)(x_2^2 - x_2 y_2 - x_2 y_1 + y_1 y_2)$

Zu (*): Nach Vieta:

$b = x_1 x_2$

$a = -x_1 - x_2$

$d = y_1 y_2$

$c = -y_1 - y_2$

$\overset{(*)}{=} (x_1^2 + cx_1 + d)(x_2^2 + cx_2 + d)$

$= x_1^2 x_2^2 + c x_1^2 x_2 + d x_1^2 + c x_1 x_2^2 + c^2 x_1 x_2 + cd x_1 + d x_2^2 + cd x_2 + d^2$

$\overset{(*)}{=} b^2 + bc x_1 + d x_1^2 + bc x_2 + c^2 b + cd x_1 + d x_2^2 + cd x_2 + d^2$

$\overset{(*)}{=} b^2 - abc + d\underbrace{(x_1^2 + x_2^2 + 2x_1 x_2)}_{= (x_1 + x_2)^2 = a^2} - \underbrace{2x_1 x_2 d}_{= b} - acd + c^2 b + d^2$

$= a^2 d - abc - acd + b^2 + bc^2 - 2bd + d^2.$

Bsp: Die Gleichungen $X^2 \underbrace{- 3}_{= a} X + \underbrace{2}_{= b} = 0$, $Y^2 \underbrace{- 4}_{= c} X + \underbrace{3}_{= d} = 0$ besitzen eine gemeinsame (Nicht-)Lösung, da

$$R = 9 \cdot 3 - 24 - 36 + 4 + 32 - 12 + 9 = 0.$$

Nutzen: Mithilfe dieser Aufgabe ist es also möglich, herauszufinden, ob zwei Polynomgleichungen eine gemeinsame Lösung besitzen, ohne, dass man die Lösungen selbst kennen muss!

Lösungsvorschlag zu Blatt 7, Aufgabe 7

Sei $a \in \overline{\mathbb{Q}}$.

Betrachte $f_a = X^3 + 2a^2X - a + 5$.

Gesucht: Normierte Polynomgleichung mit rationalen Koeffizienten, die genau dann von a erfüllt wird, wenn $f_a$ nicht separabel ist.

Dazu: $f_a$ nicht separabel $\overset{\text{Vorlesung}}{\Longleftrightarrow}$ $\Delta_{f_a} = 0$ (Diskriminante von $f_a$)

Somit ist schonmal klar: $\Delta_{f_a} = 0$ ist eine Gleichung, die von a genau dann erfüllt wird, wenn $f_a$ nicht separabel ist.

Wir müssen aber noch zeigen, dass es sich bei dieser Gleichung um eine Polynomgleichung mit rationalen Koeffizienten handelt.

Dazu: $\Delta_{f_a} = -4(2a^2)^3 - 27(-a+5)^2 = \ldots = -32a^6 - 27a^2 + 270a - 25 \cdot 27$

(Formel für die Diskriminante eines reduzierten kubischen Polynoms)

Fazit: $f_a$ ist genau dann nicht separabel, wenn a folgende Polynomgleichung mit rationalen Koeffizienten erfüllt:

$$-32A^6 - 27A^2 + 270A - 25 \cdot 27 = 0 \qquad (*)$$

Rem.: Die Gleichung (*) hat höchstens sechs verschiedene Lösungen.
Somit ist $f_a$ für alle bis auf sechs bestimmte algebraische Zahlen a separabel.

## Lösungsvorschlag zu Blatt 7, Aufgabe 8

**Beh.:** Das Polynom
$$f = X^3 - \tfrac{3}{2}X^2 + X - \tfrac{6}{5} \in \mathbb{Q}[X]$$
besitzt keine rationale Nullstelle.

**Bew.:** Seien $x_1, x_2, x_3 \in \bar{\mathbb{Q}}$ die Nullstellen von $f$ über den algebraischen Zahlen (mit Vielfachheiten), dann gilt
$$f = (X - x_1)(X - x_2)(X - x_3).$$

Näherungsweise ergibt sich:
$$x_1 \approx 1{,}3985, \quad x_2 \approx 0{,}0507 + i\,0{,}9249, \quad x_3 \approx 0{,}0507 + i\,0{,}9249. \qquad (*)$$

Der Inhalt von $f$ ist $1/10$, $\tilde{f} = (1/10)^{-1} f$ ist ein primitives ganzzahliges Polynom:
$$10f = 10X^3 - 15X^2 + 10X - 12 \qquad (\mathrm{ggT}(10, -15, 10, -12) = 1)$$
$$= 10(X - x_1)(X - x_2)(X - x_3)$$

Nun ist $10f$ irreduzibel über $\mathbb{Z}$, denn:
Wenn $10f = gh$ eine nicht-triviale Zerlegung von $10f$ über $\mathbb{Z}$ wäre (d.h. $g, h \in \mathbb{Z}[X]$ mit $\deg g, \deg h \geq 1$), wäre, da $\deg(10f) = 3$, $g$ oder $h$ vom Grad 1.
OBdA sei $g$ vom Grad 1.
Dann folgt $g = (X - x_i)$ oder $g = 10(X - x_i)$ für ein $i \in \{1,2,3\}$
Aber da
$$x_1, x_2, x_3, \quad 10x_1, 10x_2, 10x_3 \qquad (\#)$$
allesamt nicht ganze Zahlen sind, ist das nicht möglich!

Da $10f$ primitiv ist, folgt nach dem fünften Lemma, dass $10f$ auch über $\mathbb{Q}$ irreduzibel ist. Somit besitzt $10f$ insbesondere keine Nullstelle über $\mathbb{Q}$. Da aber natürlich die Nullstellen von $10f$ dieselben wie die von $f$ sind, folgt die Behauptung.

**Bem.:** Man kann nun nicht direkt nach der näherungsweisen Berechnung der Nullstellen, $(*)$, aufhören. Denn es ist nicht klar, ob die exakten Lösungen rational sind oder nicht — das kann man einer festen Anzahl von gegebenen Nachkommaziffern nicht entscheiden. (Bsp.: $\sqrt{2}$ ist nicht rational, $\sqrt{2} \approx 1{,}41$; die Dezimalbruchweise gibt aber keinen Hinweis auf Rationalität oder Irrationalität.)

Man kann aber sehr wohl anhand weniger Nachkommaziffern entscheiden, ob eine Zahl ganzzahlig ist oder nicht! Das nutzen wir oben auch aus, bei $(\#)$.

## Lösungsvorschlag zu Blatt 7, Aufgabe 10 a

Seien $f, g \in \mathbb{Q}[X]$.

Seien $p_1, \dots, p_m$ all diejenigen irreduziblen Faktoren, die in $f$ oder $g$ auftauchen.

Schreibe $f = \prod_{i=1}^{m} p_i^{r_i}$, für $g = \prod_{i=1}^{m} p_i^{s_i}$ mit $r_i, s_i \in \mathbb{N}_0$. ($r_i = 0$ bedeutet, dass $p_i$ in $f$ nicht vorkommt)

Definiere $d := \prod_{i=1}^{m} p_i^{t_i}$ mit $t_i := \min\{r_i, s_i\}$.

Beh.: $d$ ist der ggT von $f$ und $g$.

Bew.: Zu zeigen ist:

1) $d \mid f$, $d \mid g$.
2) Für alle $\tilde{d}$ mit $\tilde{d} \mid f$, $\tilde{d} \mid g$ gilt: $\tilde{d} \mid d$.

Zu 1): klar, da $t_i \le r_i$ und $t_i \le s_i$ für alle $i = 1, \dots, m$.

Zu 2): Sei $\tilde{d}$ mit $\tilde{d} \mid f$, $\tilde{d} \mid g$ beliebig gegeben.
Es folgt, dass die irreduziblen Faktoren von $\tilde{d}$ nur die von $f$ und $g$ sein können — sonst könnte $\tilde{d} \mid f$ und $\tilde{d} \mid g$ nicht gelten.

Somit kann man $\tilde{d}$ wie folgt schreiben:

$$\tilde{d} = \prod_{i=1}^{m} p_i^{u_i} \quad \text{für gewisse } u_i \in \mathbb{N}_0.$$

Wegen $\tilde{d} \mid f$ folgt außerdem: $u_i \le r_i$.
Analog folgt wegen $\tilde{d} \mid g$: $u_i \le s_i$.
Zusammengenommen folgt: $u_i \le \min\{r_i, s_i\} = t_i$.

Damit ist klar, dass $\tilde{d}$ ein Teiler von $d$ ist.

Damit folgt die Behauptung.

Bem.: Ersetzt man „min" durch „max", erhält man ein Verfahren für das kleinste gemeinsame Vielfache.

Bsp.: Sei $f = (X^2+1)^3 (X-5)^7 (X+2)$, $g = (X^2+1)^{11} (X-5)^6 (X+3)^2$.
Dann gilt:

$$\mathrm{ggT}(f, g) = (X^2+1)^3 (X-5)^6$$

$$\mathrm{kgV}(f, g) = (X^2+1)^{11} (X-5)^7 (X+2)(X+3).$$

Lösungsvorschlag zu Blatt 7, Aufgabe 10

Sei: $f \in \mathbb{Q}[X]$ normiert.

Beh.: $f$ prim $\Rightarrow$ $f$ irreduzibel.

Bem.: Die Umkehrung „$\subseteq$" wurde in der Vorlesung gezeigt, es gilt daher:
$f$ prim $\Leftrightarrow$ $f$ irreduzibel.

Bew. d. Beh.:

Sei: $f = gh$, z.z.: $f = g$ oder $f = h$.
Wegen $f = gh$ folgt insbesondere $f \mid gh$.
Da $f$ prim ist, folgt somit: $f \mid g$ oder $f \mid h$.
Außerdem gilt wegen $f = gh$, dass $g \mid f$ und $g \mid h$.

Somit folgt:
1) Sollte $f \mid g$ sein, gilt sogar $f = g$.
2) Sollte $f \mid h$ sein, gilt sogar $f = h$.
In beiden Fällen sind wir fertig.

Lösungsvorschlag zu Blatt 7, Aufgabe 11

Sei: $f \in \mathbb{Q}[X]$ normiert und irreduzibel.

Beh.: Für alle $n \geq 1$ und Polynome $g_1, \dots, g_n \in \mathbb{Q}[X]$ gilt:

$$f \mid g_1 \cdots g_n \Rightarrow f \mid g_1 \text{ oder } \cdots \text{ oder } f \mid g_n$$

Bew.: Durch Induktion über $n$:

$n = 1$: klar.

$n \to n+1$: $f \mid g_1 \cdots g_n g_{n+1} \Rightarrow f \mid (g_1 \cdots g_n) g_{n+1} \overset{f \text{ prim}}{\Rightarrow} f \mid g_1 \cdots g_n$ oder $f \mid g_{n+1}$

($f$ prim, da $f$ irreduzibel)

$f \mid g_1 \cdots g_n$ oder $f \mid g_{n+1}$ $\overset{IV}{\Rightarrow}$ $f \mid g_1$ oder $\cdots$ oder $f \mid g_n$

Bem.: Eine analoge Aussage gilt für Primzahlen:

Für alle $n \geq 1$ und ganze Zahlen $g_1, \dots, g_n \in \mathbb{Z}$ gilt:

$$p \mid g_1 \cdots g_n \Rightarrow p \mid g_1 \text{ oder } \cdots \text{ oder } p \mid g_n,$$

falls $p \in \mathbb{Z}$ eine Primzahl ist.

Lösungsvorschlag zu Blatt 9, Aufgabe 2

$a \in \mathbb{Z}$, $d > 1$, $d \in \mathbb{Z}$.

Beh.: $a + \sqrt{d}$ ist eine ganz-algebraische Zahl.

Beweis: Setze $x := a + \sqrt{d}$. Dann folgt:

$$x - a = \sqrt{d} \quad \Rightarrow \quad (x-a)^2 = x^2 - 2ax + a^2 = d \quad \Rightarrow \quad x^2 - 2ax + a^2 - d = 0.$$

Somit löst $x$ die Gleichung

$$X^2 - 2aX + a^2 - d = 0. \qquad (*)$$

Diese ist eine Polynomgleichung, normiert und hat nur ganzzahlige Koeffizienten (nämlich $1$, $-2a$ und $a^2 - d$). Damit folgt die Behauptung.

Gesucht: $[\mathbb{Q}(x) : \mathbb{Q}]$.

Beweis: Die Gleichung $(*)$ besitzt die Lösungen $a + \sqrt{d}$ und $a - \sqrt{d}$ (nachrechnen!).

Somit gilt:

$$f(x) = 0 \text{ mit } f = X^2 - 2aX + a^2 - d = (X - (a+\sqrt{d}))(X - (a-\sqrt{d})).$$

1. Fall: $\sqrt{d} \notin \mathbb{Q}$, d.h. $d$ ist keine Quadratzahl.

Dann liegen auch die Nullstellen von $f$ nicht in $\mathbb{Q}$.

Somit ist, da $\deg f = 2$, $f$ über $\mathbb{Q}$ irreduzibel, und, da $f$ bekanntlich die Zahl $x$ als Nullstelle besitzt, das Minimalpolynom von $x$.

Somit folgt $[\mathbb{Q}(x) : \mathbb{Q}] = \deg f = 2$.

2. Fall: $\sqrt{d} \in \mathbb{Q}$, d.h. $d$ ist eine Quadratzahl.

~~Dann liegt $\sqrt{d}$ sogar in $\mathbb{Z}$ (Übungsaufgabe auf einem der ersten Blätter).~~

Dann liegt auch $a + \sqrt{d}$ in $\mathbb{Q}$.

Somit ist $X - (a+\sqrt{d}) \in \mathbb{Q}[X]$ das Minimalpolynom von $a + \sqrt{d}$, und der Grad von $a + \sqrt{d}$ über $\mathbb{Q}$ ist $1$.

## Lösungsvorschlag zu Blatt 5, Aufgabe 3

Sei $x = \sqrt{2} + \sqrt[3]{2}$.

Gesucht: Natürliche Zahl $n$ und nicht-triviale verschwindende Linearkombination von $1, x, x^2, \dots, x^n$ mit rationalen Koeffizienten.

Dazu: ~~$x^2 = (\sqrt{2} + \sqrt[3]{2})^2 = 2 + 2\sqrt{2}\sqrt[3]{2} + \sqrt[3]{2}\sqrt[3]{4}$~~

$$(x - \sqrt{2})^3 = x^3 - 3x^2\sqrt{2} + 6x - 2\sqrt{2} = 2.$$

$$\Rightarrow x^3 + 6x - 2 = \sqrt{2}(3x^2 + 2)$$

$$\Rightarrow (x^3 + 6x - 2)^2 = (\sqrt{2}(3x^2 + 2))^2$$

$$\| \qquad\qquad \|$$

$$x^6 + 6x^4 - 2x^3 \qquad 2(9x^4 + 12x^2 + 4)$$

$$+ 6x^4 + 36x^2 - 12x$$

$$- 2x^3 - 12x + 4$$

$$\Rightarrow x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4 = 0.$$

↑ das ist eine gesuchte nicht-triviale, trotzdem verschwindende Linearkombination von $1, x, x^2, \dots, x^6$. (Setze also $n = 6$.)

Bem.: Ohne die Einschränkung „mit rationalen Koeffizienten" wäre die Aufgabe trivial, beispielsweise ist

~~$(-1) \cdot 1 + 1 \cdot x$~~

$(-x) \cdot 1 + 1 \cdot x$

eine nicht-triviale verschwindende Linearkombination von $1, x$ über $\overline{\mathbb{Q}}$.

Lösungsvorschlag zu Blatt 9, Aufgabe 4

Sei $x \in \overline{\mathbb{Q}}$ mit Minimalpolynom $f = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$ über $\mathbb{Q}$.
Dann ist $\mathbb{Q}(x)$ ein Rechenbereich, aber auch ein $\mathbb{Q}$-Vektorraum der Dimension $n$, wobei eine mögliche Basis

$$(1, x, x^2, \dots, x^{n-1}) =: B$$

ist.

Man kann die Abbildung

$$\phi : \mathbb{Q}(x) \to \mathbb{Q}(x), \quad y \mapsto xy$$

definieren; da diese eine ($\mathbb{Q}$-)lineare Abbildung ist, kann man die Matrix von $\phi$ bzgl. $B$ im Quell- und Zielraum angeben:

$$\phi(1) = x = 0 \cdot 1 + 1 \cdot x + 0 \cdot x^2 + \dots + 0 \cdot x^{n-1}$$
$$\phi(x) = x^2 = 0 \cdot 1 + 1 \cdot x + 1 \cdot x^2 + \dots + 0 \cdot x^{n-1}$$
$$\phi(x^2) = x^3 = \dots$$
$$\vdots$$
$$\phi(x^{n-1}) = x^n = -a_{n-1}x^{n-1} - \dots - a_1 x - a_0 = (-a_0)1 + (-a_1)x + (-a_2)x^2 + \dots + (-a_{n-1})x^{n-1}$$

$$\Rightarrow M(\phi; B, B) = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & \ddots & & & -a_1 \\ & \ddots & \ddots & & \vdots \\ & & \ddots & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix} \in \mathbb{Q}^{n \times n}.$$

Diese Matrix hat auch den Namen „Begleitmatrix zu $f$" und von Wikipedia, NWs LA II oder vestedt auch KHs LA II weiß man, dass das Minimalpolynom dieser Matrix gleich $f$ ist.

## Lösungsvorschlag zu Blatt 9, Aufgabe 5

**Gesucht:** Ein primitives Element zu $i$ und $\sqrt[3]{2}$,
d.h. eine algebraische Zahl $z$ mit folgenden Eigenschaften:

1) $z$ ist rational in $i$, $\sqrt[3]{2}$ (d.h. $z \in \mathbb{Q}(i, \sqrt[3]{2})$)
2) $i$ ist rational in $z$ (d.h. $i \in \mathbb{Q}(z)$)
3) $\sqrt[3]{2}$ ist rational in $z$ (d.h. $\sqrt[3]{2} \in \mathbb{Q}(z)$).

**Variante 1:** Durch Raten kommt man auf die Idee,

$$z := i\sqrt[3]{2}$$

zu setzen. Dann ist 1) sicherlich erfüllt.

Zu 2): $z^3/(-2) = i^3 \cdot 2/(-2) = -i^2 i = i$ ✓

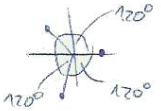
Zu 1): $z^4/2 = i^4 \cdot 2 \cdot \sqrt[3]{2}/2 = (i^2)^2 \sqrt[3]{2} = (-1)^2 \sqrt[3]{2} = \sqrt[3]{2}$ ✓

**Variante 2:** Man folgt dem Beweis der Vorlesung.

Dazu: Minimalpolynom von $i$: $X^2 + 1$, hat Nullstellen $i, -i$.
Minimalpolynom von $\sqrt[3]{2}$: $X^3 - 2$, hat Nullstellen $\sqrt[3]{2}$, $e^{2\pi i/3}\sqrt[3]{2}$, $e^{4\pi i/3}\sqrt[3]{2}$

Die Menge $S$ der Vorlesung ist damit:

$$S = \left\{ \frac{x' - i}{\sqrt[3]{2} - y'} \;\middle|\; x' \in \{i, -i\},\ y' \in \{e^{2\pi i/3}\sqrt[3]{2}, e^{4\pi i/3}\sqrt[3]{2}\} \right\}$$




$$\cap \mathbb{Q}$$

$$= \left\{ \frac{i-i}{\dots}, \frac{i-i}{\dots}, \frac{-i-i}{\sqrt[3]{2} - e^{2\pi i/3}\sqrt[3]{2}}, \frac{-i-i}{\sqrt[3]{2} - e^{4\pi i/3}\sqrt[3]{2}} \right\} \cap \mathbb{Q}$$

$$= \{0, \underbrace{-\frac{2i}{\sqrt[3]{2}}(1 - e^{2\pi i/3})^{-1}}_{\approx 0{,}5 - 0{,}8i,\ \notin \mathbb{Q}}, \underbrace{-\frac{2i}{\sqrt[3]{2}}(1 - e^{4\pi i/3})}_{\approx -0{,}5 - 0{,}8i,\ \notin \mathbb{Q}}\} \cap \mathbb{Q} = \{0\}.$$

Damit sind beispielsweise $i + 1 \cdot \sqrt[3]{2}$, oder $i + 17 \cdot \sqrt[3]{2}$, oder allgemeiner $i + \lambda\sqrt[3]{2}$ mit $\lambda \neq 0, \lambda \in \mathbb{Q}$, primitive Elemente zu $i, \sqrt[3]{2}$.
(Die geforderten Eigenschaften 1), 2), 3) wurden schon allgemein in der Vorlesung bewiesen.)

Lösungsvorschlag zu Blatt 9, Aufgabe 6

Aufgabe: Schreibe $\sqrt{2}$ und $\sqrt{3}$ als Polynome in $\sqrt{2}+\sqrt{3}$ mit rationalen Koeffizienten.

Variante 1: Setze $z := \sqrt{2}+\sqrt{3}$.

Dann gilt $z^2 = 2+3+2\sqrt{6}$, also $\sqrt{6} = (z^2-5)/2$.

Ferner gilt $z\sqrt{6} = (z^3-5z)/2 = \sqrt{2}\sqrt{2}\sqrt{3}+\sqrt{3}\sqrt{2}\sqrt{3} = 2\sqrt{3}+3\sqrt{2}$.

Somit folgt:

$$\sqrt{2} = z\sqrt{6} - 2z = \frac{1}{2}(z^3-5z-4z) = \frac{1}{2}(z^3-9z).$$

$$\sqrt{3} = 3z - z\sqrt{6} = \frac{1}{2}(6z-z^3+5z) = \frac{1}{2}(-z^3+11z).$$

Variante 2: Wegen ~~$(\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3}) =$~~ $(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2}) = 3-2 = 1$ gilt $1/z = \sqrt{3}-\sqrt{2}$.

Somit folgt: $\sqrt{2} = \frac{1}{2}(z-\frac{1}{z})$, $\sqrt{3} = \frac{1}{2}(z+\frac{1}{z})$.

Das sind aber nur rationale, nicht polynomielle Ausdrücke in $z$;
wir müssen also $1/z$ noch als Polynom in $z$ schreiben.
(Da $z$ algebraisch ist, wissen wir wegen $\mathbb{Q}(z) = \mathbb{Q}[z]$, dass das gehen muss.)

Dazu suchen wir eine Polynomgleichung, die $z$ als Lösung besitzt:

$$z^2 = 5+2\sqrt{6} \quad \Rightarrow \quad (z^2-5)^2 = z^4-10z^2+25 = 24$$

$$\Rightarrow z^4-10z^2+1 = 0$$

Jetzt stellen wir diese Gleichung um:

$$z^4-10z^2 = -1$$

$$\Rightarrow z(z^3-10z) = -1$$

$$\Rightarrow z^3-10z = -1/z \quad \Rightarrow \quad -z^3+10z = 1/z.$$

Somit erhalten wir:

$$\sqrt{2} = \frac{1}{2}(z-1/z) = \frac{1}{2}(z+z^3-10z) = \frac{1}{2}(z^3-9z).$$

$$\sqrt{3} = \frac{1}{2}(z+1/z) = \frac{1}{2}(z-z^3+10z) = \frac{1}{2}(-z^3+11z).$$

Lösungsvorschlag zu Blatt 9, Aufgabe 7

Beh.: $\sqrt{2}$ ist nicht in $\sqrt{3}$ rational, d.h. $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$.

Bew.: Da das Minimalpolynom von $\sqrt{3}$

$$x^2 - 3$$

ist und somit der Grad von $\sqrt{3}$ über $\mathbb{Q}$ zwei ist, ist eine mögliche Basis vom $\mathbb{Q}$-Vektorraum $\mathbb{Q}(\sqrt{3})$

$$B = (1, \sqrt{3}) = (\sqrt{3}^0, \sqrt{3}^1).$$

Somit gilt $\mathbb{Q}(\sqrt{3}) = \{a \cdot 1 + b \cdot \sqrt{3} \mid a, b \in \mathbb{Q}\}$.

Ann., $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. Dann folgt also $\sqrt{2} = a + b\sqrt{3}$ für gewisse $a, b \in \mathbb{Q}$.
Wir treffen nun eine Fallunterscheidung:

1. Fall: $a = 0, b = 0$: $\Rightarrow \sqrt{2} = 0$, ↯.

2. Fall: $a \neq 0, b = 0$: $\Rightarrow \sqrt{2} = a$, ↯ zu $\sqrt{2} \notin \mathbb{Q}$.

3. Fall: $a = 0, b \neq 0$: $\Rightarrow \sqrt{2} = b\sqrt{3}$

$\Rightarrow 2 = 3b^2$

hier taucht der Primfaktor 2 eine gerade Anzahl von Malen auf

hier auch

aber hier taucht der Primfaktor 2 nur einmal, insbesondere eine ungerade Anzahl von Malen, auf. ↯

4. Fall: $a \neq 0, b \neq 0$: $\Rightarrow 2 = a^2 + 3b^2 + 2ab\sqrt{3}$

$\Rightarrow \sqrt{3} = (2 - a^2 - 3b^2) / \underbrace{(2ab)}_{\neq 0} \in \mathbb{Q}$, ↯ zu $\sqrt{3} \notin \mathbb{Q}$.

Somit liegt in jedem der Fälle ein Widerspruch vor, fertig.

## Lösungsvorschlag zu Blatt 9, Aufgabe 8

**Beh.:** Für alle $n \geq 1$ und alg. Zahlen $x_1, \dots, x_n$ existiert eine alg. Zahl $z$ mit

$$\mathbb{Q}(z) = \mathbb{Q}(x_1, \dots, x_n).$$

**Bew.:** Induktion über $n$:

**$n = 1$:** Wähle $z := x_1$. Dann gilt offensichtlich $\mathbb{Q}(z) = \mathbb{Q}(x_1)$.

**$n \to n+1$:** $\mathbb{Q}(x_1, \dots, x_n, x_{n+1}) = \underbrace{\mathbb{Q}(x_1, \dots, x_n)}_{\text{IV}}(x_{n+1}) = \mathbb{Q}(\tilde{z})(x_{n+1}) = \mathbb{Q}(\tilde{z}, x_{n+1}) = \mathbb{Q}(z)$

$= \mathbb{Q}(\tilde{z})$ für ein $\tilde{z}$

nach Satz über primitives Element existiert ein $z$ mit $\mathbb{Q}(z) = \mathbb{Q}(\tilde{z}, x_{n+1})$.

Lösungsvorschlag zu Blatt 9, Aufgabe 11

Gesucht: Ein Polynom, welches über rationale Koeffizienten besitzt und
1) über $\mathbb{Q}$ irreduzibel ist,
2) über $\mathbb{Q}(\sqrt{2})$ in (genau) zwei irreduzible Polynome zerfällt und
3) über $\mathbb{Q}(\sqrt{2}+i)$ in (genau) vier irreduzible Polynome zerfällt.

Dazu: Setze $f := X^4 - 2X^2 + 9$.
(Auf dieses Polynom kommt man beispielsweise, wenn man in Aufgabe 10 versucht, ein Polynom mit rationalen Koeffizienten zu finden, das $\sqrt{2}+i$ als Nullstelle besitzt:

$$x := \sqrt{2}+i \Rightarrow (x-i)^2 - 2 = x^2 - 2ix - 1 - 2 = 0$$
$$\Rightarrow (x^2-3)^2 + 4x^2 = 0)$$
$$\| $$
$$x^4 - 2x^2 + 9$$

Auf jeden Fall gilt: $x := \sqrt{2}+i$ ist eine Nullstelle von $f$.
Außerdem gilt $\deg f = 4 = [\mathbb{Q}(\sqrt{2}+1) : \mathbb{Q}]$.
$\uparrow$ Ü10
Damit folgt schon, dass
$f$ das Minimalpolynom von $x$ über $\mathbb{Q}$ ist! Insbesondere ist $f$ über $\mathbb{Q}$ irreduzibel, damit ist 1) gezeigt.

Lösungsvorschlag zu Blatt 9, Aufgabe 11 (Tutorium)

Zu 2): $f$ besitzt neben $\sqrt{2}+i$ noch die Nullstellen $\sqrt{2}-i$, $-\sqrt{2}+i$ und $-\sqrt{2}-i$. (Nachrechnen!)

Somit folgt:

$$f = \underbrace{(X-(\sqrt{2}+i))(X-(\sqrt{2}-i))}_{=X^2-2\sqrt{2}X+3 \in \mathbb{Q}(\sqrt{2})[X]} \underbrace{(X-(-\sqrt{2}+i))(X-(-\sqrt{2}-i))}_{=X^2+2\sqrt{2}X+3 \in \mathbb{Q}(\sqrt{2})[X]} \quad (*)$$

$X^2-2\sqrt{2}X+3$ irreduzibel über $\mathbb{Q}(\sqrt{2})$, da Grad zwei und die beiden Nullstellen nicht in $\mathbb{Q}(\sqrt{2})$ liegen

Also zerfällt $f$ über $\mathbb{Q}(\sqrt{2})$ in zwei Polynome, die über $\mathbb{Q}(\sqrt{2})$ jeweils irreduzibel sind.

Ann., $\sqrt{2}+i \in \mathbb{Q}(\sqrt{2})$.

$\Rightarrow \underbrace{(\sqrt{2}+i)}_{\in \mathbb{Q}(\sqrt{2})} + \underbrace{(-\sqrt{2})}_{\in \mathbb{Q}(\sqrt{2})} = i \in \mathbb{Q}(\sqrt{2})$, ↯

Zu 3): (*) zeigt eine Zerlegung von $f$ in vier Polynome, die jeweils sicherlich irreduzibel sind (da Grad = 1). Wir müssen aber noch zeigen, dass die vier Faktoren auch in $\mathbb{Q}(\sqrt{2}+i)[X]$ liegen.

Das ist klar, wenn man weiß, dass $\mathbb{Q}(\sqrt{2}+i) = \mathbb{Q}(\sqrt{2}, i)$, dies gilt, da $\sqrt{2}+i$ ein primitives Element zu $\sqrt{2}, i$ ist.

„bekannt aus Vorlesung", oder explizit:

i) $\mathbb{Q}(\sqrt{2}+i) \subseteq \mathbb{Q}(\sqrt{2}, i)$ ist klar.

ii) Setzt man $u := \sqrt{2}+i$, so gilt:

$(u^3+u)/6 = (2\sqrt{2}+6i-3\sqrt{2}i+\sqrt{2}+i)/6 = i.$

$(-u^3+5u)/6 = (-2\sqrt{2}-6i+3\sqrt{2}+i+5\sqrt{2}+5i)/6 = \sqrt{2}.$

## Lösungsvorschlag zu Blatt 9, Aufgabe 12

Sei $\zeta$ eine beliebige Lösung von $f(X) = 0$ mit $f = X^4 + X^3 + X^2 + X + 1$.
Sei $\alpha := e^{\pi i/5}$.

**Beh.:** $\zeta$ ist in $\alpha$ rational, d.h. $\zeta \in \mathbb{Q}(\alpha)$.

**Bew.:** Nach Blatt 3, Aufgabe 11 wissen wir:
$\zeta$ ist eine der fünf 5-ten Einheitswurzeln, aber nicht die 1.
Also gilt $\zeta = e^{2\pi i k/5}$ für ein $k \in \{1, 2, 3, 4\}$.
Somit folgt $\zeta = e^{2\pi i k/5} = (e^{\pi i/5})^{2k} = \alpha^{2k}$, also ist $\zeta$ in $\alpha$ rational.

**Bem.:** Es folgt $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\alpha)$.
Damit können wir den Rechenbereich $\mathbb{Q}(\alpha)$ auch als $\mathbb{Q}(\zeta)$-Vektorraum ansehen, wobei $\dim_{\mathbb{Q}(\zeta)} \mathbb{Q}(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}(\zeta)]$ gilt.
(Ganz unabhängig von der Aufgabe können wir $\mathbb{Q}(\alpha)$ auch als $\mathbb{Q}$-Vektorraum ansehen, wobei dann $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ gilt.)

**Gesucht:** Eine mögliche Basis vom $\mathbb{Q}(\zeta)$-Vektorraum $\mathbb{Q}(\alpha)$.
**Dazu:** Wir berechnen zunächst $\dim_{\mathbb{Q}(\zeta)} \mathbb{Q}(\alpha)$, um zu wissen, wie lang die Basis sein muss.

Nach der Gradformel gilt: $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\alpha) : \mathbb{Q}(\zeta)]}_{= \dim_{\mathbb{Q}(\zeta)} \mathbb{Q}(\alpha),\ \text{gesucht}} [\mathbb{Q}(\zeta) : \mathbb{Q}]$ über $\mathbb{Q}$.

**Zu $[\mathbb{Q}(\zeta) : \mathbb{Q}]$:** Wir behaupten, dass $f$ das Minimalpolynom von $\zeta$ ist. Wenn wir das gezeigt haben, folgt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg f = 4$.
Da nach Voraussetzung klar ist, dass $f$ die Zahl $\zeta$ als Nullstelle besitzt, müssen wir nur noch zeigen, dass $f$ irreduzibel ist.
Das geht leicht mit dem Eisensteinschen Kriterium:
$f(X+1) = X^4 + 5X^3 + 10X^2 + 10X + 5$, $p = 5$.
(Vgl. Bsp. fürs Eisensteinsche Kriterium im Skript.)

**Zu $[\mathbb{Q}(\alpha) : \mathbb{Q}]$:** $\alpha$ ist Lösung der Gleichung $g(X) = 0$, wobei $g = X^5 + 1$.
~~g ist aber reduzibel~~ ($g$ ist nicht das Minimalpolynom von $\alpha$, da $g$ reduzibel ist, da $g$ bspw. $(-1) \in \mathbb{Q}$ als Nullstelle besitzt.)
Somit folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 5$.

Lösungsvorschlag zu Blatt 9, Aufgabe 12 (Forts.)

Es gibt wegen der Gradformel von oben also nur noch eine Möglichkeit:

$[\mathbb{Q}(\alpha):\mathbb{Q}(\gamma)] = 1$, und $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4 \cdot 1 = 4$.

Denn $[\mathbb{Q}(\alpha):\mathbb{Q}(\gamma)] = 2$ oder höher ist ausgeschlossen,
und $[\mathbb{Q}(\alpha):\mathbb{Q}(\gamma)] = 0$ ist sowieso ausgeschlossen.

(Denn sonst $\dim_{\mathbb{Q}(\gamma)} \mathbb{Q}(\alpha) = 0$,
also $\mathbb{Q}(\alpha) = \{0\}$ (Nullvektorraum)
im Widerspruch zu $\mathbb{Q}_1 \subset \mathbb{Q}(\alpha)$.)

Somit gilt:

$$\left.\begin{array}{l} \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha) \\ \dim_{\mathbb{Q}_1} \mathbb{Q}(\gamma) = 4 = \dim_{\mathbb{Q}_1} \mathbb{Q}(\alpha) \end{array}\right\} \Rightarrow \mathbb{Q}(\gamma) = \mathbb{Q}_1(\alpha).$$

Eine mögliche $\mathbb{Q}(\gamma)$-Basis von $\mathbb{Q}_1(\alpha)$ ist also

$B = (1)$,

oder

$B = (17)$,

oder $B = (\gamma)$, $B = (\alpha)$, $B = (\gamma + \alpha)$, oder allgemein $B = (u)$ mit $u \neq 0$, $u \in \mathbb{Q}(\gamma) = \mathbb{Q}(\alpha)$.

Bem.: Eine mögliche $\mathbb{Q}$-Basis von $\mathbb{Q}(\alpha)$, also eine mögliche Basis von $\mathbb{Q}(\alpha)$ aufgefasst als $\mathbb{Q}$-Vektorraum, ist:

$(1, \alpha, \alpha^2, \alpha^3)$.

Lösungsvorschlag zu Blatt 10, Aufgaben 1 und 2

$x \in \mathbb{Q}$, $y \in \mathbb{Q}(x)$, $z \in \mathbb{Q}(y)$.

Frage: Wie lässt sich $[\mathbb{Q}(x) : \mathbb{Q}(z)]$ aus $[\mathbb{Q}(x) : \mathbb{Q}(y)]$ und $[\mathbb{Q}(y) : \mathbb{Q}(z)]$ berechnen?

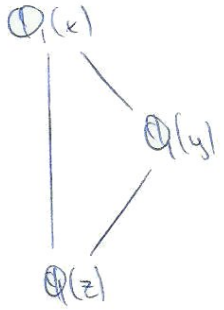
Antwort: Nach Gradformel gilt:

$$[\mathbb{Q}(x) : \mathbb{Q}(z)] = [\mathbb{Q}(x) : \mathbb{Q}(y)]\,[\mathbb{Q}(y) : \mathbb{Q}(z)]$$

Beh: $[\mathbb{Q}(y) : \mathbb{Q}(z)]$ teilt $[\mathbb{Q}(x) : \mathbb{Q}(z)]$.

Bew: Klar, $[\mathbb{Q}(x) : \mathbb{Q}(z)]$ ist ein $[\mathbb{Q}(x) : \mathbb{Q}(y)]$-Vielfaches von $[\mathbb{Q}(y) : \mathbb{Q}(z)]$.

Skizze:



Lösungsvorschlag zu Blatt 10, Aufgabe 3

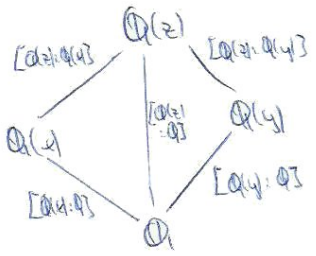
$x, y, z \in \overline{\mathbb{Q}}$, $x, y \in \mathbb{Q}(z)$.

Beh.: $[\mathbb{Q}(z) : \mathbb{Q}(x)]\,[\mathbb{Q}(x) : \mathbb{Q}] = [\mathbb{Q}(z) : \mathbb{Q}(y)]\,[\mathbb{Q}(y) : \mathbb{Q}]$.

Bew.: Linke Seite $= [\mathbb{Q}(z) : \mathbb{Q}(x)]\,[\mathbb{Q}(x) : \mathbb{Q}] \overset{\text{Grad-formel}}{=} [\mathbb{Q}(z) : \mathbb{Q}]$ ✓

rechte Seite $= [\mathbb{Q}(z) : \mathbb{Q}(y)]\,[\mathbb{Q}(y) : \mathbb{Q}] \overset{\text{Grad-formel}}{=} [\mathbb{Q}(z) : \mathbb{Q}]$

Skizze:



Lösungsvorschlag zu Blatt 10, Aufgabe 7

Gesucht: Zwei algebraische Zahlen, die nicht zueinander gal. konjugiert sind.

Dazu: Beispielsweise $x_1 = 17$ und $x_2 = \sqrt[3]{17}$, denn:

$x_1$ hat als Minimalpolynom

$$X - 17,$$

aber $x_2$ ist keine Nullstelle davon.

Oder: $x_1 = 1, \quad x_2 = 0$

Oder: $x_1 = \sqrt{2}, \quad x_2 = \sqrt{3}, \quad \ldots$

Lösungsvorschlag zu Blatt 10, Aufgabe 8

Sei $t \in \overline{\mathbb{Q}}$.

Bdh.: $t_1 \cdot t_2 \cdot \dots \cdot t_n \in \mathbb{Q}$, $t_1 + \dots + t_n \in \mathbb{Q}$,
wobei die $t_i$ die gal. Konjugierten von $t$ sind, $t$ selbst inklusive.

Bew.: Sei $f = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$ das gemeinsame Minimalpolynom der $t_i$.
Nach Satz von Vieta gilt:

~~$f = \prod_{k=0}^{n} (X - t_k)$~~

$$a_k = (-1)^{n-k} e_{n-k}(t_1, \dots, t_n) \in \mathbb{Q}, \quad k = 0, \dots, n-1 \qquad (a_n = 1)$$

Insbesondere gilt somit:

$$a_0 = (-1)^n t_1 \cdot t_2 \cdot \dots \cdot t_n \in \mathbb{Q} \quad \Rightarrow \quad t_1 \cdots t_n \in \mathbb{Q}$$

$$a_{n-1} = -(t_1 + \dots + t_n) \in \mathbb{Q} \quad \Rightarrow \quad t_1 + \dots + t_n \in \mathbb{Q}$$

Bem.: Analog gilt beispielsweise, dass
$t_1 t_2 + t_1 t_3 + \dots + t_1 t_n + t_2 t_3 + t_2 t_4 + \dots + t_2 t_n + \dots + t_{n-1,n} \in \mathbb{Q}$.
(Nämlich für $k = n-2$.)

Bem.: Alternativ kann man wie folgt argumentieren:
$t_1 \cdots t_n$ ist invariant unter der Wirkung der Galoisgruppe von $t_1, \dots, t_n$,
~~denn $t_1 \cdots t_n$ ist sogar invariant unter~~
denn:
$$\sigma \cdot (t_1 \cdots t_n) \overset{\text{Bild. A7}}{=} (\sigma \cdot t_1) \cdots (\sigma \cdot t_n) = t_{\sigma(1)} \cdots t_{\sigma(n)} = t_1 \cdots t_n.$$
Nach Proposition 4.10 folgt damit, dass $t_1 \cdots t_n$ rational ist.
Für $t_1 + \dots + t_n$ geht das genauso.

Lösungsvorschlag zu Blatt 10, Aufgabe 9

$x, y, z \in \overline{\mathbb{Q}}$, $x, y$ gal. konj., $y, z$ gal. konj.

Beh.: $x, z$ gal. konj.

Bew.: Wegen $x$ gal. konj. zu $y$ ist $m_x = m_y$.

($m_x$: Minimalpolynom von $x$; $m_y$: Minimalpolynom von $y$)

Wegen $y$ gal. konj. zu $z$ ist $m_y = m_z$.

($m_y$: Minimalpolynom von $y$; $m_z$: Minimalpolynom von $z$)

$\Rightarrow m_x = m_y = m_z$

$\Rightarrow m_x = m_z$, also: $x$ und $z$ sind zueinander gal. konjugiert.

Lösungsvorschlag zu Blatt 10, Aufgabe 11

$p, q \in \mathbb{Z}$, $p, q$ prim, $p \neq q$.

Gesucht: Alle gal. konjugierten von $\sqrt{p}+\sqrt{q}$.

Dazu: Wir finden zunächst das Minimalpolynom von $x := \sqrt{p}+\sqrt{q}$.

$$x = \sqrt{p}+\sqrt{q} \Rightarrow x^2 = p + 2\sqrt{p}\sqrt{q} + q$$
$$\Rightarrow (x^2-(p+q))^2 = 4pq \quad \Rightarrow \quad x^4 - 2x^2(p+q) + (p^2+2pq+q^2) = 4pq$$
$$\Rightarrow x \text{ löst die Gleichung}$$
$$f(X) = 0,$$
$$\text{wobei } f(X) = X^4 - 2X^2(p+q) + (p-q)^2.$$

Da $f$ normiert ist, nur rationale Koeffizienten besitzt und $x$ als Nullstelle besitzt, gilt somit auf jeden Fall: $[\mathbb{Q}(x):\mathbb{Q}] \leq \deg f = 4$, es gibt also ($x$ selbst eingeschlossen), höchstens vier gal. konjugierte.

Die Nullstellen von $f$ sind: $\pm_1\sqrt{p} \pm_2 \sqrt{q}$. (vier Stück)

Denn: $\hat{x} = \pm\sqrt{p} \pm \sqrt{q} \Rightarrow \hat{x}^2 = p \pm 2\sqrt{pq} + q \Rightarrow \hat{x}^2 - (p+q) = \pm 2\sqrt{p}\sqrt{q}$

$$\Rightarrow (\hat{x}^2-(p+q))^2 = 4pq \quad \Rightarrow \quad f(\hat{x}) = 0.$$

Jetzt zeigen wir noch, dass $f$ irreduzibel ist. Sobald wir das gezeigt haben, ist insgesamt klar: Die gal. konjugierten von $\sqrt{p}+\sqrt{q}$ sind die vier Nullstellen von $f$, also $\pm_1\sqrt{p}\pm_2\sqrt{q}$.

Zur Irreduzibilität: Sei $x_1 = \sqrt{p}+\sqrt{q}$, $x_2 = \sqrt{p}-\sqrt{q}$, $x_3 = -\sqrt{p}+\sqrt{q}$, $x_4 = -\sqrt{p}-\sqrt{q}$.

$e_1(x_1,x_2) = x_1+x_2 = 2\sqrt{p} \notin \mathbb{Q}$

$e_1(x_1,x_3) = x_1+x_3 = 2\sqrt{q} \notin \mathbb{Q}$

$e_1(x_1,x_4) = x_1+x_4 = 0 \in \mathbb{Q}$, aber zum Glück $e_2(x_1,x_4) = x_1x_4 = -(p+q+2\sqrt{p}\sqrt{q}) \notin \mathbb{Q}$

$e_1(x_2,x_3) = x_2+x_3 = 0 \in \mathbb{Q}$, aber zum Glück $e_2(x_2,x_3) = x_2x_3 = -(p+q+2\sqrt{p}\sqrt{q}) \notin \mathbb{Q}$

$e_1(x_2,x_4) = x_2+x_4 = -2\sqrt{q} \notin \mathbb{Q}$

$e_1(x_3,x_4) = x_3+x_4 = -2\sqrt{p} \notin \mathbb{Q}$.

Damit ist gezeigt: Von $f$ können keine quadratischen Faktoren abspalten.
Von $f$ können auch keine linearen Faktoren abspalten, da die Nullstellen nicht in $\mathbb{Q}$ liegen.
Schließlich können auch keine kubische Faktoren abspalten, da sonst ja auch ein zugehöriger linearer Faktor abspalten würde.

Lösungsvorschlag zu Blatt 10, Aufgabe 12

$t, t' \in \overline{\mathbb{Q}}$.

Beh.: $t, t'$ gal. konjugiert $\Leftrightarrow \left[\forall f \in \mathbb{Q}[X]: f(t)=0 \Rightarrow f(t')=0\right]$

Bew.: „$\Rightarrow$": s. Prop. 4.2

„$\Leftarrow$": Sei $m$ das Minimalpolynom von $t$.
Somit gilt sicherlich $m(t)=0$.
Nach Voraussetzung folgt $m(t')=0$, somit sind $t, t'$ gal. konjugiert.

Lösungsvorschlag zu Blatt 11, Aufgabe 1

Beh.: $A_n \subseteq S_n$ ist eine Untergruppe.

Bew.: $A_n = \{\sigma \in S_n \mid \operatorname{sgn} \sigma = +1\}$.

Zu zeigen ist:

1) $\mathrm{id} \in A_n$
2) $\sigma, \tau \in A_n \Rightarrow \sigma \circ \tau \in A_n$
3) $\sigma \in A_n \Rightarrow \sigma^{-1} \in A_n$

Zu 1): $\operatorname{sgn} \mathrm{id} = +1$ ✓

Zu 2): $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau) = (+1) \cdot (+1) = 1$. ✓

Zu 3): $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)^{-1} = (+1)^{-1} = \frac{1}{+1} = 1$. ✓

Bem.: Hier haben wir die Rechenregeln

$$\operatorname{sgn}(\mathrm{id}) = 1, \quad \operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau), \quad \operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)^{-1} \quad (*)$$

benutzt.

Bem.: Wer weiß, was ein Gruppenhomomorphismus und was der Kern eines Gruppenhomomorphismus ist, kann auch wie folgt argumentieren:

$\operatorname{sgn}: S_n \longrightarrow \{-1, +1\}$ ist ein Gruppenhomomorphismus, wegen $(*)$.
Somit ist $\ker(\operatorname{sgn})$ eine Untergruppe von $S_n$.
Es gilt $\ker(\operatorname{sgn}) = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\} = A_n$.

## Ergänzung zu Blatt 11, Aufgabe 3

Seien $x_1, \dots, x_n$ die (alle) Nullstellen eines normierten irreduziblen Polynoms $f$ über den rationalen Zahlen.
Die Aufgabe hatte behauptet:

$x_2 = \sigma x_1 \Rightarrow x_1, x_2$ gal. konj.

Der Beweis ging so:
Sei $m$ das Minimalpolynom von $x_1$ über $\mathbb{Q}$.
Definiere $H(X_1, \dots, X_n) := m(X_1)$.
Dann ist $H$ eine alg. Relation, denn $H \in \mathbb{Q}[X_1, \dots, X_n]$ und $H(x_1, \dots, x_n) = m(x_1) = 0$.

$\Rightarrow H(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = H(x_2, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = m(x_2) = 0$

$\Rightarrow x_1, x_2$ gal. konj.

Es kann die Frage auf, ob die Rückrichtung gilt. Das ist in der Tat der Fall!
Beweis:

Definiere $V(X) := \prod_{\sigma \in \mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_n)} (X - \sigma \cdot x_1)$.

Obwohl es zunächst nicht so scheint, hat $V$ ausschließlich rationale Koeffizienten, denn die Koeffizienten sind invariant unter beliebigen Symmetrien $\tau \in \mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_n)$, da je über alle Symmetrien multipliziert wird.

Außerdem gilt $V(x_1) = 0$, denn unter all den $\sigma$'s des Produkts muss auch die Identitätspermutation vorkommen.

Da nun nach Voraussetzung $x_1, x_2$ über $\mathbb{Q}$ gal. konj. sind, $V$ rationale Koeffizienten hat und $V(x_1) = 0$ gilt, folgt $V(x_2) = 0$.

$\Rightarrow \prod_{\sigma \in \mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_n)} (x_2 - \sigma x_1) = 0 \Rightarrow x_2 - \sigma x_1 = 0$ für ein $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_n) \Rightarrow$ Beh.

Zusammenfassend gilt also:

$x_1, x_2$ gal. konj. über $\mathbb{Q} \iff \exists \sigma \in \mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_n): x_2 = \sigma x_1$

Lösungsvorschlag zu Blatt 11, Aufgabe 9

Sei $f \in \mathbb{Q}[X_1, \dots, X_n] \neq 0$ (d.h. $f$ soll nicht das Nullpolynom sein).

Beh.: $\exists m_1, \dots, m_n \in \mathbb{Z}: \; f(m_1, \dots, m_n) \neq 0$.

Bew.: Folgende Argumentation funktioniert nicht:

„$f$ ist ein Polynom, und hat daher nur endlich viele Nullstellen.
Folglich müssen wir als $(m_1, \dots, m_n)$ nur irgendein Tupel ganze Zahlen wählen, welches keine der endlich vielen Nullstellen ist."

Die Argumentation funktioniert deswegen nicht, weil ein Polynom in mehreren Variablen durchaus unendlich viele Nullstellen besitzen kann, Beispiel:
$X^2 + Y^2 - 1$ besitzt als Nullstellen genau alle Punkte des Einheitskreis.

Bew. d. Beh.:

Induktion über $n$:

$n = 1$: Finde die endlich vielen Nullstellen von $f$, und wähle dann irgendeine ganze Zahl $m_1$, die keine der endlich vielen Nullstellen ist.

Alternativ: Rechne die Zahlen $f(1), f(2), \dots, f(\deg f + 1)$ aus.
Da $f$ nicht mehr als $\deg f$ viele Nullstellen besitzen kann, diese Aufzählung aber [mit Vielfachheiten] $(\deg f + 1)$ Zahlen enthält, muss sich unter diesen Zahlen mindestens eine befinden, die nicht 0 ist.

Alternativ: Rate irgendwelche $(\deg f + 1)$ viele ganze Zahlen $z_1, \dots, z_{\deg f + 1}$. Dann muss mindestens eine dieser Zahlen keine Nullstelle von $f$ sein, Begründung wie oben.

$n \to n+1$: Es gelte also $f \in \mathbb{Q}[X_1, \dots, X_{n+1}]$, $f \neq 0$.
Wir sortieren nach der Variablen $X_{n+1}$:

$$f = \sum_{i=0}^{z} g_i(X_1, \dots, X_n) \cdot X_{n+1}^i$$

(d.h. wir fassen $f$ als Polynom aus $(\mathbb{Q}[X_1, \dots, X_n])[X_{n+1}]$ auf)

Da $f \neq 0$, muss irgendein $g_j$ ungleich 0 sein. Nach IV existieren somit ganze Zahlen $m_1, \dots, m_n$ mit $g_j(m_1, \dots, m_n) \neq 0$.
Nun betrachten wir das Polynom $f(m_1, \dots, m_n, X) = \sum_{i=0}^{z} g_i(m_1, \dots, m_n) X^i$.
Der Koeffizient $g_j(m_1, \dots, m_n) \in \mathbb{Q}$ dieses Polynoms ist nicht null, also ist auch dieses Polynom insgesamt nicht das Nullpolynom. Da dieses Polynom nur noch von einer Variablen abhängt, nämlich $X$, können wir ein $m_{n+1} \in \mathbb{Z}$ wie im Induktionsanfang beschrieben, sodass $f(m_1, \dots, m_n, m_{n+1}) \neq 0$ gilt.

Lösungsvorschlag zu Blatt 11, Aufgabe 9 (Fortsetzung)

Bsp: Wir wollen den Beweis noch veranschaulichen, indem wir ihn speziell auf das Polynom

$$f(X_1, X_2, X_3) = X_1^2 + 2X_2X_3 - X_3^5 + X_1X_2X_3 - 13$$

anwenden.

Sortierung nach $X_3$:

$$(X_1^2 - 13) + (2X_2 + X_1X_2)X_3 \cdot - 1 \cdot X_3^5$$

Wähle $g_j = 1$.

Als Nebenrechnung: Finde ganze Zahlen $m_1, m_2$ mit $1(m_1, m_2) \neq 0$.
Das ist aber einfach, $1(m_1, m_2)$ ist ja eh, für alle $m_1, m_2$, gleich 1.
Wähle also bspw.

$$m_1 = 0, \quad m_2 = 0.$$

Nach Einsetzen:

$$-13 - X_3^5$$

Rate $m_3 = 0$, denn $-13 - 0^5 = -13 \neq 0$.

Fazit: $f(m_1, m_2, m_3) = 0$ für $(m_1, m_2, m_3) = (0, 0, 0)$.

Lösungsvorschlag zu Blatt 11, Aufgabe 10

Gesucht: Eine gal. Resolvente zu den Nullstellen von $X^2+X+1$.

Dazu: Die Nullstellen von $X^2+X+1$ sind:

$$x_{1,2} = \frac{1}{2}\left(-1 \pm \sqrt{1-4}\right) = \frac{1}{2}(-1 \pm 3i).$$

Eine gal. Resolvente $V(X_1, X_2)$ muss folgende Bedingung erfüllen:
Für alle Permutationen (nicht nur die Symmetrien der Nullstellen, sondern wirklich alle) $\sigma$ muss gelten:

$$V(x_{\sigma(1)}, x_{\sigma(2)})$$

Fertigt man eine Liste aller

$$V(x_{\sigma(1)}, \dots, x_{\sigma(n)}),$$

hier also $V(x_{\sigma(1)}, x_{\sigma(2)})$

an, wobei $\sigma$ alle Permutationen aus $S_n$ durchläuft, so darf auf dieser Liste keine Zahl doppelt vorkommen.

Hier gibt es nur zwei mögliche Permutationen,

$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ und $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

Wir setzen nun: $V(X_1, X_2) := X_1$.

Dann gilt:

$$\left.\begin{aligned} V(x_1, x_2) &= x_1 \\ V(x_2, x_1) &= x_2 \end{aligned}\right) \neq \checkmark$$

Somit ist $V$ eine gal. Resolvente zu $x_1, x_2$.

Bem: Auch möglich wäre

$V(X_1, X_2) = X_1 - X_2$,

oder $V(X_1, X_2) = X_1 + 2X_2$

oder viele weitere.

Bem: Siehe Bem. bei Lösungsvorschlag zu A12.

Lösungsvorschlag zu Blatt 11, Aufgabe 11

Frage: Warum wurde der Begriff der gal. Resolvente nur für separable Polynome definiert?

Antwort: Von einer gal. Resolvente $V$ fordert man, dass

~~$V(x_{\sigma(1)}, \dots, x_{\sigma(n)})$~~ $V(x_{\sigma(1)}, \dots, x_{\sigma(n)})$

für $\sigma \in S_n$ paarweise verschieden ist, wobei $x_1, \dots, x_n$ die Nullstellen des gegebenen Polynoms sind.

Ist nun das gegebene Polynom nicht separabel, so hätte es mindestens eine doppelte Nullstelle, bspw. $x_1 = x_2$.

Dann ist aber die Forderung oben überhaupt nicht erfüllbar!
(Denn $V(x_1, x_2, \dots) = V(x_2, x_1, \dots)$)

Fazit: Für nicht separable Polynome ist der Begriff uninteressant, da es überhaupt keine gal. Resolventen gäbe.

## Lösungsvorschlag zu Blatt 11, Aufgabe 12

Seien $x_1, \dots, x_n$ (alle) Nullstellen von $f$, wobei $f \in \mathbb{Q}[X]$ normiert und separabel.
Sei $C$ irgendeine natürliche Zahl, die die Forderungen

$$n \cdot \frac{|x_i - x_j|}{|x_k - x_\ell|} \leq C$$

für alle $i, j, k, \ell = 1, \dots, n$ mit $k \neq \ell$ erfüllt.
↑ um Division durch Null zu vermeiden!

**Behauptung:** $V(X_1, \dots, X_n) := X_1 + CX_2 + C^2X_3 + \dots + C^{n-1}X_n = \sum_{i=1}^{n} C^{i-1}X_i$
ist eine gal. Resolvente zu den Nullstellen von $f$.

**Bem:** Die Aussage dieser Aufgabe ist enorm hilfreich, um gal. Resolventen zu finden.
Beispiel:
Sei $x_1 = \sqrt{2}$, $x_2 = \sqrt{3}$. Wir wollen mithilfe dieser Aufgabe eine gal. Resolvente zu $x_1, x_2$ finden.

Dazu müssen wir lediglich eine Zahl $C$ finden, für die gilt:

$$C \geq 2 \cdot \frac{|x_1 - x_1|}{|x_1 - x_2|}, \quad C \geq 2 \cdot \frac{|x_1 - x_2|}{|x_1 - x_2|}, \quad C \geq 2 \cdot \frac{|x_2 - x_1|}{|x_1 - x_2|}, \quad C \geq 2 \cdot \frac{|x_2 - x_2|}{|x_1 - x_2|},$$

und dasselbe nochmal mit $|x_2 - x_1|$ statt $|x_1 - x_2|$ im Nenner, aber das macht ja nichts.

Es muss also gelten:

$$C \geq 2 \cdot 0, \quad C \geq 2 \cdot 1, \quad C \geq 2 \cdot 1, \quad C \geq 2 \cdot 0.$$

Das wird erfüllt, wenn man beispielsweise $C = 2$ definiert.
Fazit: $V(X_1, X_2) = X_1 + 2X_2$ ist eine gal. Resolvente zu $x_1, x_2$.
Folgerung: $V(x_1, x_2) = x_1 + 2x_2$ ist ein primitives Element zu $x_1, x_2$.

**Beweis d. Behauptung:**
Wir müssen also zeigen: $V(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \neq V(x_{\tau(1)}, \dots, x_{\tau(n)})$ für alle Permutationen $\sigma, \tau$ mit $\sigma \neq \tau$.
Umformuliert müssen wir zeigen:

$$|V(x_{\sigma(1)}, \dots, x_{\sigma(n)}) - V(x_{\tau(1)}, \dots, x_{\tau(n)})| = \left| \sum_{i=1}^{n} (x_{\sigma(i)} - x_{\tau(i)}) C^{i-1} \right| > 0.$$

Die Idee ist nun folgende: $C$ ist so groß, dass die höchste vorkommende Potenz von $C$ in der Summe alle weiteren, vielleicht negativen, Summanden ausgleichen kann.

Im Folgenden setzen wir diese Idee um.

## Lösungsvorschlag zu Blatt 11, Aufgabe 12 (Forts.)

Sei $k \in \{1, \dots, n\}$ der größte Index mit

$$x_{\sigma(k)} \neq x_{\tau(k)}.$$

(In Spezialfällen ist vielleicht $k=1$ oder $k=n$, das ist okay.)

Damit können wir die Summe vereinfachen: (statt vorhin $n$)

$$|V(x_{\sigma(1)}, \dots, x_{\sigma(n)}) - V(x_{\tau(1)}, \dots, x_{\tau(n)})| = \left| \sum_{i=1}^{k} (x_{\sigma(i)} - x_{\tau(i)})\, C^{i-1} \right|$$

$$\geq \left| (x_{\sigma(k)} - x_{\tau(k)})\, C^{k-1} + \sum_{i=1}^{k-1} (x_{\sigma(i)} - x_{\tau(i)})\, C^{i-1} \right|$$

$$\geq |x_{\sigma(k)} - x_{\tau(k)}|\, C^{k-1} - \sum_{i=1}^{k-1} |x_{\sigma(i)} - x_{\tau(i)}|\, C^{i-1}$$

umgekehrte Dreiecksungleichung

$|x_{\sigma(k)} - x_{\tau(k)}| \neq 0$, da $\sigma(k) \neq \tau(k)$ und alle $x_\ell$ verschieden

$|x_{\sigma(i)} - x_{\tau(i)}| \leq \frac{1}{n} C\, |x_{\tau(k)} - x_{\tau(k)}|$

$\frac{|x_{\sigma(i)} - x_{\tau(i)}|}{n\, |x_{\tau(k)} - x_{\tau(k)}|} \leq C$

$$\geq |x_{\sigma(k)} - x_{\tau(k)}| \left( C^{k-1} - \sum_{i=1}^{k-1} \frac{1}{n} C^{i} \right)$$

$\leq C^{k-1}$, da $C \geq 1$, da $C$ natürliche Zahl

$$\geq |x_{\sigma(k)} - x_{\tau(k)}| \left( C^{k-1} - \sum_{i=1}^{k-1} \frac{1}{n} C^{k-1} \right) = \underbrace{C^{k-1}}_{>0}\, \underbrace{|x_{\sigma(k)} - x_{\tau(k)}|}_{>0} \left(1 - \underbrace{\frac{k-1}{n}}_{<1,\ \text{da } k-1<n}\right) > 0.$$

$= (k-1)\frac{1}{n} C^{k-1}$

Lösungsvorschlag zu Blatt 11, Aufgabe 14

$H \in \bar{\mathbb{Q}}[X_1, \dots, X_n]$ symmetrisch in $X_3, \dots, X_n$.

Beh.: $H$ lässt sich als Polynom in
$X_1$, $X_2$ und den elementarsymm. Pol. von $X_1, \dots, X_n$
schreiben.

Bew.: Wir wollen $H$ als ein Polynom $\tilde{H} \in (\bar{\mathbb{Q}}[X_1, X_2])[X_3, \dots, X_n]$ auffassen.
$\tilde{H}$ ist dann in all seinen Variablen $(X_3, \dots, X_n)$ symmetrisch.
Nach dem Hauptsatz über elementarsymm. Pol. folgt:

$$\tilde{H}(X_3, \dots, X_n) = g(e_1(X_3, \dots, X_n), \dots, e_{n-2}(X_3, \dots, X_n)) \quad (*)$$

für ein $g \in (\bar{\mathbb{Q}}[X_1, X_2])[Y_1, \dots, Y_{n-2}]$.

Nach Hilfssatz 4.14 (zweimal angewendet) sind die $e_i(X_3, \dots, X_n)$ selbst wiederum Polynome in $X_1, X_2$ und den $e_j(X_1, \dots, X_n)$.

Insgesamt folgt damit die Behauptung.

Beh.: Diese Darstellung ist eindeutig.

Bew.: Angenommen, irgendjemand schreibt $H$ als Polynom in $X_1, X_2$ und den $e_j(X_1, \dots, X_n)$.
Dann können wir zunächst (auf genau eine Weise) statt gewisser $X_1^i, X_2^j$'s und $e_j(X_1, \dots, X_n)$'s gemäß Hilfssatz 4.14 die Darstellung auch gewisse $X_1^i$'s, $X_2^j$'s und $e_i(X_3, \dots, X_n)$ schreiben.
Wir erhalten also eine Darstellung wie in $(*)$.
Aber der Hauptsatz über elementarsymm. Pol. sagt dann, dass es nur ein solches $g$ gibt.
Insgesamt folgt damit die Eindeutigkeit.

Lösungsvorschlag zu Blatt 12, Aufgabe 6

Resultat: Vollständige Faktorisierung von $X^3+X^2+X+1$ in irreduzible Polynome (über $\mathbb{Q}$).

Dazu: Man sieht durch Raten, dass $(-1)$ eine Nullstelle ist:

$$(-1)^3+(-1)^2+(-1)+1 = (-1)+1+(-1)+1 = 0.$$

Polynomdivision:

$$(X^3+X^2+X+1):(X-(-1)) = X^2+1,$$
$$-(X^3+X^2)$$
$$X+1$$

also $X^3+X^2+X+1 = \underbrace{(X+1)}_{\text{irred. über } \mathbb{Q}}\underbrace{(X^2+1)}_{\text{irred. über } \mathbb{Q}}$

↑ (da keine Nullstellen über $\mathbb{Q}$ und Grad $\leq 3$)

Alternativ über Kreisteilungspolynome:

Idee: Betrachte $(X-1)\cdot(X^3+X^2+X+1)$.

Also: $(X-1)(X^3+X^2+X+1) = \dots = X^4-1 = \Phi_1(X)\,\Phi_2(X)\,\Phi_4(X)$

$$= \underbrace{(X-1)}_{=\Phi_1(X),\ \text{irred.}}\underbrace{(X+1)}_{=\Phi_2(X),\ \text{irred.}}\underbrace{(X^2+1)}_{=\Phi_4(X),\ \text{irred.}},$$

$\Rightarrow X^3+X^2+X+1 = (X+1)(X^2+1)$.

Zur Berechnung von $\Phi_4$ siehe Lösungsvorschlag zu Aufgabe 7.

Lösungsvorschlag zu Blatt 12 Aufgabe 7

(x) Gesucht: $\Phi_3$

Dazu: Über Polynomformel aus Skript:

$$\Phi_3 = \frac{x^3-1}{\Phi_1} = \frac{x^3-1}{(x-1)(x+1)} =$$

$$\Phi_3 = \frac{x^3-1}{\Phi_1} = \frac{x^3-1}{x-1} = \dots = x^2+x+1.$$

Polynomdivision

Die allgemeine Formel lautet: $\Phi_n = \prod_{0<d<n,\ d\mid n} \Phi_d$.

(y) Gesucht: $\Phi_6$

Dazu: $\Phi_6 = \frac{x^6-1}{\Phi_1 \Phi_2 \Phi_3} = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = \frac{(x^3-1)(x^3+1)}{(x-1)(x+1)(x^2+x+1)}$

dritte binomische Formel

$$= \frac{(x^3+1)\cdot\Phi_3}{(x+1)\cdot\Phi_3} = \frac{x^3+1}{x+1} = x^2-x+1$$

Polynomdivision

(z) Gesucht: $\Phi_9$

Dazu: $\Phi_9 = \frac{x^9-1}{\Phi_1 \Phi_3} = \frac{x^9-1}{(x-1)(x^2+x+1)} = \frac{(x^3-1)(x^6+x^3+1)}{(x-1)(x^2+x+1)} = \Phi_3 \cdot (x^6+x^3+1)$

dritte binomische Formel

$$= \frac{x^8+x^7+x^6+\dots+x+1}{x^2+x+1} = \dots \text{(Polynomdivision)} \dots = x^6+x^3+1.$$

Noch zu Aufgabe 6: $\Phi_4 = \frac{x^4-1}{\Phi_1 \Phi_2} = \frac{(x^2-1)(x^2+1)}{(x-1)(x+1)} = \frac{(x^2-1)(x^2+1)}{(x^2-1)} = x^2+1.$

Lösungsvorschlag zu Blatt 12, Aufgabe 8

Sei $p$ eine Primzahl.

Beh.: $\binom{p^2}{p}$ ist durch $p$, aber nicht durch $p^2$ teilbar.

Beweis: $\binom{p^2}{p} = \frac{(p^2)!}{p!\,(p^2-p)!} = \frac{p^2\,(p^2-1)(p^2-2)\cdots(p^2-p+1)}{p\,(p-1)(p-2)\cdots 3\cdot 2\cdot 1} = p \cdot \underbrace{\frac{(p^2-1)(p^2-2)\cdots(p^2-p+1)}{(p-1)(p-2)\cdots 3\cdot 2\cdot 1}}_{= \binom{p^2-1}{p-1} \in \mathbb{Z}}$

$\Rightarrow$ $p$ ist ein Teiler von $\binom{p^2}{p}$,
denn $\binom{p^2}{p}$ ist das $\binom{p^2-1}{p-1}$-fache von $p$.

Jetzt müssen wir noch zeigen, dass $\binom{p^2}{p}$ nicht durch $p^2$ teilbar ist.
Dazu zeigen wir, dass der zweite Faktor, $\binom{p^2-1}{p-1}$, nicht durch $p$ teilbar ist.

Dazu: Der Zähler $(p^2-1)(p^2-2)\cdots(p^2-p+1)$ ist nicht durch $p$ teilbar, da
keiner der Faktoren durch $p$ teilbar ist, da jeweils die „Reste" $-1, -2, \ldots, -p+1$
übrig bleiben, und da $p$ prim ist.
Damit folgt schon die Behauptung.

Lösungsvorschlag zu Blatt 13, Aufgabe 8

Beh.: $\sqrt{2}+\sqrt{7}$ und $-\sqrt{2}-\sqrt{7}$ sind über $\mathbb{Q}$ gel. konjugiert.

Bew.: In Aufgabe 11 von Blatt 11 haben wir schon gesehen:
$\pm_1\sqrt{2}$ $\pm_2\sqrt{7}$ sind über $\mathbb{Q}$ jeweils zueinander gel. konjugiert.

Beh.: $\sqrt{2}+\sqrt{7}$ und $-\sqrt{2}-\sqrt{7}$ sind nicht über $\mathbb{Q}(\sqrt{7})$ gel. konjugiert.

Bew.: Wir bestimmen das Minimalpolynom von $\sqrt{2}+\sqrt{7}$ über $\mathbb{Q}(\sqrt{7})$.

$x := \sqrt{2}+\sqrt{7} \Rightarrow (x-\sqrt{7})^2 - 2 = x^2 - 2x\sqrt{7} + 7 - 2 = x^2 - 2x\sqrt{7} + 5 = 0.$

Also: $x$ ist Nullstelle des Polynoms

$X^2 - 2X\sqrt{7} + 5$,

welches normiert ist und Koeffizienten aus $\mathbb{Q}(\sqrt{7})$ hat.

Ferner ist es irreduzibel, da seine beiden Nullstellen $\sqrt{2}+\sqrt{7}$ und $-\sqrt{2}+\sqrt{7}$ beide nicht in $\mathbb{Q}(\sqrt{7})$ liegen (sonst wäre auch $\sqrt{2} \in \mathbb{Q}(\sqrt{7})$ und es hat 2 hat.

Folglich ist es Minimalpolynom von $x$. Da es $-\sqrt{2}-\sqrt{7}$ nicht als Nullstelle besitzt, folgt die Behauptung.

Lösungsvorschlag zu Blatt 13, Aufgabe 10

$K \subseteq L$, $x \in \overline{\mathbb{Q}}$.

Beh.: $x'$ zu $x$ über $L$ gal. konj. $\Rightarrow$ $x'$ zu $x$ über $K$ gal. konj.

Bew.: Seien $m_L$, $m_K$ die Minimalpolynome von $x$ über $L$ bzw. $K$.

Da $m_K(x) = m_L(x) = 0$ und $m_L$ über $L$ irreduzibel ist, folgt mit dem obigen Irreduzibilitätssatz (angewendet auf $m_L, m_K \in L[X]$), dass $m_L$ ein Teiler von $m_K$ ist.

Damit folgt schon die Behauptung:

Sei $x'$ zu $x$ über $L$ gal. konj. $\Rightarrow m_L(x') = 0 \Rightarrow m_K(x') = 0 \Rightarrow x'$ zu $x$ über $K$ gal. konj.

## Lösungsvorschlag zu Blatt 14, Aufgabe 3

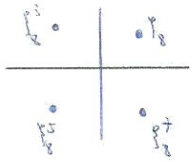
**Gesucht:** $\mathrm{Gal}_{\mathbb{Q}}(x_1, x_2, x_3, x_4)$, wobei die $x_i$ die Nullstellen von $f = X^4 + 1$ sind.

**Dazu:** **1. Schritt:** Nullstellen finden

$$x^4 + 1 = 0 \iff x^4 = -1 = e^{i\pi} \overset{1.7}{\iff} x \in \left\{ \zeta_8^1, \zeta_8^3, \zeta_8^5, \zeta_8^7 \right\},$$

wobei $\zeta_8 = e^{2\pi i/8}$ die „erste" 8-te Einheitswurzel ist.

In der Zahlenebene:




**2. Schritt:** Ein primitives Element zu den Nullstellen finden

Hier funktioniert $t := \zeta_8$, denn:

- $t$ ist in $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7$ rational (klar)
- Die vier Nullstellen sind in $t$ rational:

$$x_i = h_i(t) \quad \text{mit} \quad h_1 = X, \; h_2 = X^3, \; h_3 = X^5, \; h_4 = X^7$$

**3. Schritt:** Alle galoisschen Konjugierten des primitiven Elements finden

Das Polynom $f$ ist bereits irreduzibel: Das kann man sehen, wenn man wie immer die elementarsymmetrischen Funktionen in den Nullstellen ausrechnet, oder wenn man weiß, dass $f = \Phi_8$ gilt und das Kreisteilungspolynom damit irreduzibel sein muss.

Folglich ist $f$ das Minimalpolynom von $t$ über $\mathbb{Q}$, und die gal. Konjugierten von $t = \zeta_8 = x_1$ sind:

$$\begin{array}{cccc} \zeta_8, & \zeta_8^3, & \zeta_8^5, & \zeta_8^7. \\ \| & \| & \| & \| \\ t_1 & t_2 & t_3 & t_4 \end{array}$$

**4. Schritt:** Die Elemente der Galoisgruppe auflisten

1) $(h_1(t_1), h_2(t_1), h_3(t_1), h_4(t_1)) = (x_1, x_2, x_3, x_4)$
2) $(h_1(t_2), h_2(t_2), h_3(t_2), h_4(t_2)) = (x_2, x_1, x_4, x_3)$
3) $(h_1(t_3), h_2(t_3), h_3(t_3), h_4(t_3)) = (x_3, x_4, x_1, x_2)$
4) $(h_1(t_4), h_2(t_4), h_3(t_4), h_4(t_4)) = (x_4, x_3, x_2, x_1)$

**Fazit:**

$$\mathrm{Gal}_{\mathbb{Q}}(x_1, x_2, x_3, x_4) = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}}_{=:\sigma}, \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}}_{=:\tau}, \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}}_{=:\mu} \right\}.$$

Lösungsvorschlag zu Blatt 14, Aufgabe 3 (Forts.)

Gesucht: Alle Untergruppen von $G := Sal_4(x_1, \dots, x_4)$.

Dazu: Untergruppen der Ordnung 1:

$U_1 = \{ id \}$

Untergruppen der Ordnung 2:

$U_2 = \{ id, \sigma \}$ (denn $\sigma^2 = id$)

$U_3 = \{ id, \tau \}$ (denn $\tau^2 = id$)

$U_4 = \{ id, \mu \}$ (denn $\mu^2 = id$)

Untergruppen der Ordnung 3:

Kann es nicht geben, da 3 kein Teiler von $|G| = 4$ ist.

Untergruppen der Ordnung 4:

$U_5 = G = \{ id, \sigma, \tau, \mu \}$.

Gesucht: Zwischenerweiterungen von $\mathbb{Q}(x_1, \dots, x_4)$ über $\mathbb{Q}$, die diesen Untergruppen im Sinne des Hauptsatzes entsprechen.

Dazu: $\mathbb{Q}(x_1, \dots, x_4)^{U_1} = \mathbb{Q}(x_1, \dots, x_4)^{\{id\}} = \mathbb{Q}(e_1(id(t))) = \mathbb{Q}(t) = \mathbb{Q}(x_1, \dots, x_4) = \mathbb{Q}(t) = \mathbb{Q}(x_1)$

$\mathbb{Q}(x_1, \dots, x_4)^{U_2} = \mathbb{Q}(x_1, \dots, x_4)^{\{id, \sigma\}} = \mathbb{Q}(e_1(id(t), \sigma(t)),\ e_2(id(t), \sigma(t))) = \mathbb{Q}(e_1(x_1, x_2),\ e_2(x_1, x_2))$

$= \mathbb{Q}(x_1 + x_2,\ x_1 x_2) = \mathbb{Q}(\sqrt{2}\, i,\ \underbrace{-1}_{\in \mathbb{Q}}) = \mathbb{Q}(\sqrt{2}\, i)$

$\mathbb{Q}(x_1, \dots, x_4)^{U_3} = \mathbb{Q}(x_1, \dots, x_4)^{\{id, \tau\}} = \mathbb{Q}(e_1(id(t), \tau(t)),\ e_2(id(t), \tau(t))) = \mathbb{Q}(e_1(x_1, x_3),\ e_2(x_1, x_3))$

$= \mathbb{Q}(x_1 + x_3,\ x_1 x_3) = \mathbb{Q}(0, -i) = \mathbb{Q}(-i) = \mathbb{Q}(i)$

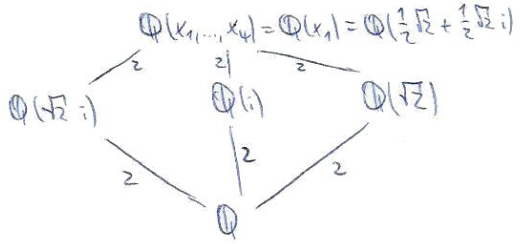
$\mathbb{Q}(x_1, \dots, x_4)^{U_4} = \mathbb{Q}(x_1, \dots, x_4)^{\{id, \mu\}} = \mathbb{Q}(e_1(id(t), \mu(t)),\ e_2(id(t), \mu(t))) = \mathbb{Q}(e_1(x_1, x_4),\ e_2(x_1, x_4))$

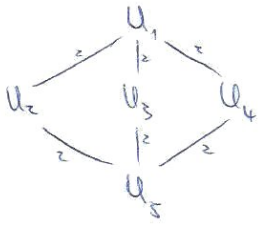
$= \mathbb{Q}(x_1 + x_4,\ x_1 x_4) = \mathbb{Q}(-\sqrt{2},\ 1) = \mathbb{Q}(\sqrt{2})$

$\mathbb{Q}(x_1, \dots, x_4)^{U_5} = \mathbb{Q}(x_1, \dots, x_4)^{G} = \mathbb{Q}$

Lösungsvorschlag zu Blatt 14, Aufgabe 3 (Fr. Lu)

Graphik:



Lösungsvorschlag zu Blatt 14 Aufgabe 4

Seien $m$ Variablensätze $\underline{X}_1, \dots, \underline{X}_m$ gegeben, mit $\underline{X}_i$ Abkürzung für $X_{i1}, \dots, X_{in}$.

Die rechte Seite von Gleichung (1),

$$\prod_{j=1}^{m} (1 + X_{1j} T_1 + \dots + X_{nj} T_n) =: F(T_1, \dots, T_n)$$

ist (u.a.) ein Polynom in den Variablen $T_1, \dots, T_n$.

Den Koeffizient von $T_1^{k_1} \cdots T_n^{k_n}$ in diesem Polynom bezeichnen wir mit $e_{(k_1, \dots, k_n)}$.

Bem: Sei $n = 1$. Dann lautet die rechte Seite von Gleichung (1):

$$\prod_{j=1}^{m} (1 + X_{1j} T_1), \qquad (\#)$$

und sei noch spezieller $m = 3$, dann hat man

$$\begin{aligned}
\prod_{j=1}^{3} (1 + X_{1j} T_1) &= (1 + X_{11} T_1)(1 + X_{12} T_1)(1 + X_{13} T_1) \\
&= 1 + X_{13} T_1 + X_{12} T_1 + X_{11} T_1 + X_{11} X_{12} T_1^2 + X_{11} X_{13} T_1^2 + X_{12} X_{13} T_1^2 \\
&\quad + X_{11} X_{12} X_{13} T_1^3 \\
&= 1 + (X_{11} + X_{12} + X_{13}) T_1 + (X_{11} X_{12} + X_{11} X_{13} + X_{12} X_{13}) T_1^2 + X_{11} X_{12} X_{13} T_1^3.
\end{aligned}$$

Wir sehen: Der Koeffizient von $T_1$ ist gerade $e_1(X_{11}, X_{12}, X_{13})$, der von $T_1^2$ ist $e_2(X_{11}, X_{12}, X_{13})$ und der von $T_1^3$ ist $e_3(X_{11}, X_{12}, X_{13})$.

Man kann also die üblichen elementarsymmetrischen Funktionen als Koeffizienten des Polynoms $(\#)$ wiederfinden.

(1) Ges: $e_{(l,0,\dots,0)}(\underline{X}_1, \dots, \underline{X}_m)$.

Dazu: $e_{(l,0,\dots,0)}$ = der Koeffizient von $T_1^l T_2^0 \cdots T_n^0$ in $F(T_1, \dots, T_n)$

= der Koeffizient von $T_1^l$ in $F(T_1, 0, \dots, 0)$

$\overset{\text{Bem.}}{=} e_l(X_{11}, X_{12}, \dots, X_{1m})$.

↑ übliche elementarsymmetrische Funktion

Bem: Analog gilt $e_{(0,\dots,0,\underset{\uparrow}{l},0,\dots,0)} = e_l(X_{i1}, X_{i2}, \dots, X_{im})$.

↑ $i$-te Stelle

Lösungsvorschlag zu Blatt 14, Aufgabe 4 (Forts.)

(2) Beh.: $e_\lambda$ ist symmetrisch in $\underline{X}_1, \dots, \underline{X}_m$ im Sinne der Definition der Aufgabe.

Bew.: Sei $\sigma \in S_m$ beliebig, dann gilt:

$$\begin{aligned}
\sigma \cdot e_\lambda &= \sigma \cdot (\text{der Koeffizient von } „T^{\lambda}“ \text{ in } F) \\
&= \text{der Koeffizient von } „T^{\lambda}“ \text{ in } \underbrace{\sigma \cdot F}_{= \prod_{j=1}^{m} (1 + X_{1,\sigma(j)} T_1 + \dots + X_{n,\sigma(j)} T_n) = F} \\
&\vdots \\
&= \text{der Koeffizient von } „T^{\lambda}“ \text{ in } F \\
&= e_\lambda.
\end{aligned}$$

(Dabei meint $„T^{\lambda}“$ folgendes: $\lambda$ ist ja ein Multiindex, $\lambda = (\lambda_1, \dots, \lambda_n)$. $„T^{\lambda}“$ meint dann: $T_1^{\lambda_1} \cdots T_n^{\lambda_n}$.)

(Kurz: Die rechte Seite von Gleichung (1), $F$, ist symmetrisch in den $\underline{X}_i$. Daher muss auch jeder der Koeffizienten in den $\underline{X}_i$ symmetrisch sein. Die Koeffizienten sind aber gerade die $e_\lambda$.)

Lösungsvorschlag zu Blatt 14, Aufgabe 4 (Tuts)

(4) $K$ Koeffizientenbereich, $x_1, \dots, x_n$ Null die Nullstellen eines sep. Polynoms $f \in K[X]$.
$H = \{\sigma_1, \dots, \sigma_m\} \subseteq \mathrm{Gal}_Q(x_1, \dots, x_n)$ Untergruppe

Beh: $K(x_1, \dots, x_n)^H = K(e_\lambda(\sigma_1 \cdot \underline{x}, \dots, \sigma_m \cdot \underline{x}))$,
wobei $\lambda$ über alle Tupel $(k_1, \dots, k_n)$ mit $k_1 + \dots + k_n \leq m$ läuft
und $\sigma_i \cdot \underline{x}$ Kurzschreibweise für $(\sigma_i x_1, \dots, \sigma_i x_n)$ ist.

Bew: „$\supseteq$": Klar, denn:
Sei $y \in K(e_\lambda(\sigma_1 \underline{x}, \dots, \sigma_m \underline{x}))$ beliebig.
Dann lässt sich $y$ schreiben als $y = \tilde{H}(e_\lambda(\sigma_1 \underline{x}, \dots, \sigma_m \underline{x}))$,
wobei $\tilde{H}$ ein Polynom mit Koeffizienten aus $K$ in so vielen
Variablen ist, wie es $e_\lambda$'s gibt.

Sei nun $\sigma \in H$ beliebig, z.Z.: $\sigma \cdot y = y$.
Dazu: $\sigma \cdot y = \sigma \cdot \tilde{H}(e_\lambda(\sigma_1 \underline{x}, \dots, \sigma_m \underline{x})) = \tilde{H}(e_\lambda(\sigma\sigma_1 \underline{x}, \dots, \sigma\sigma_m \underline{x})) = y$. ✓

$\tilde{H}$ und $e_\lambda$ haben nur Koeffizienten aus $K$

$= e_\lambda(\sigma_1 \underline{x}, \dots, \sigma_m \underline{x})$

$e_\lambda$ im richtigen Sinn symmetrisch

„$\subseteq$": Sei $y \in K(x_1, \dots, x_n)^H$ beliebig.
Dann lässt sich $y$ schreiben als $y = p(x_1, \dots, x_n)$ für ein Polynom $p \in K[X_1, \dots, X_n]$.
Dabei gilt:
$\sigma_i \cdot y = y = p(\sigma_i x_1, \dots, \sigma_i x_n) = p(\sigma_i \cdot \underline{x})$ für alle $i \in \{1, \dots, m\}$.
Definiere nun folgendes Polynom:
$g(\underline{z}_1, \dots, \underline{z}_m) := \frac{1}{m}\left(p(\underline{z}_1) + \dots + p(\underline{z}_m)\right)$.
Da $g$ offensichtlich symmetrisch in den $\underline{z}_i$ ist, existiert nach (3)
ein Polynom $\hat{H} \in K[U_1, U_2, \dots, U_r]$ in so vielen Variablen, wie es $e_\lambda$'s gibt,
so dass gilt:
$g(\underline{z}_1, \dots, \underline{z}_m) = \hat{H}(e_\lambda(\underline{z}_1, \dots, \underline{z}_m))$.
Setzen wir nun für $\underline{z}_i$ konkret $(\sigma_i x_1, \dots, \sigma_i x_n)$ ein, erhalten wir:

$$g(\sigma_1 \underline{x}, \dots, \sigma_m \underline{x}) = \hat{H}(e_\lambda(\sigma_1 \underline{x}, \dots, \sigma_m \underline{x}))$$
$$\| $$
$$\frac{1}{m}\left(f(\sigma_1 \underline{x}) + \dots + f(\sigma_m \underline{x})\right)$$
$$\| $$
$$\frac{1}{m} \cdot m \cdot y = y$$

Fertig!

Lösungsvorschlag zu Blatt 14, Aufgabe 5

$f = X^6 - 2X^3 - 1 \in \mathbb{Q}[X]$.

(α) Beh.: $f$ ist irreduzibel.

Bew.: Nach Blatt 10, Aufgabe 10 ist das toll, denn dort haben wir gesehen, dass $f$ das Minimalpolynom von $x := \sqrt[3]{1+\sqrt{2}}$ über $\mathbb{Q}$ ist.

Bez.: Die Nullstellen von $f$.

Dazu: Sei $x := \sqrt[3]{1+\sqrt{2}}$, $\omega := \zeta_3$ (die „erste" dritte Einheitswurzel).

Dann gilt:

$z := \omega^i \sqrt[3]{1 \pm \sqrt{2}}$, $i \in \{0,1,2\}$ (also sechs mögliche Werte für $z$)

$\Rightarrow z^3 = 1 \pm \sqrt{2} \Rightarrow (z^3 - 1)^2 - 2 = z^6 - 2z^3 - 1 = 0$

Folglich besitzt $f$ folgende Nullstellen:

$x, \omega x, \omega^2 x, \tilde{x}, \omega\tilde{x}, \omega^2\tilde{x}$,

mit $\tilde{x} = \sqrt[3]{1-\sqrt{2}} \in \mathbb{R}$.

Es gilt: $-\frac{1}{x} = -\frac{1}{\sqrt[3]{1+\sqrt{2}}} = -\sqrt[3]{\frac{1}{1+\sqrt{2}}} = -\sqrt[3]{\frac{1-\sqrt{2}}{1^2-(\sqrt{2})^2}} = \sqrt[3]{1-\sqrt{2}} = \tilde{x}$.

Somit können wir die Nullstellen von $f$ auch so schreiben:

| | | | | | |
|---|---|---|---|---|---|
| $x_1$ | $\omega x_1$ | $\omega^2 x_1$ | $-1/x_1$ | $-\omega/x_1$ | $-\omega^2/x$ |
| ‖ | ‖ | ‖ | ‖ | ‖ | ‖ |
| $y_1$ | $y_2$ | $y_3$ | $y_4$ | $y_5$ | $y_6$ |

(β) Beh.: $[\mathbb{Q}(x,\omega) : \mathbb{Q}] = 12$.

Bew.: $[\mathbb{Q}(x,\omega) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(x,\omega) : \mathbb{Q}(x)]}_{\overset{(*)}{=} 2} \underbrace{[\mathbb{Q}(x) : \mathbb{Q}]}_{= \deg f = 6} = 12$.

Zu (*): Der Grad $[\mathbb{Q}(x,\omega) : \mathbb{Q}(x)]$ kann nicht 1 sein, denn $\omega$ liegt nicht in $\mathbb{Q}(x)$, denn $\omega \in \mathbb{C} \setminus \mathbb{R}$, aber $\mathbb{Q}(x) \subseteq \mathbb{R}$ wegen $x \in \mathbb{R}$.

Andererseits kann der Grad höchstens nur 2 sein, denn $\omega$ erfüllt folgende normierte Polynomgleichung mit ~~konkreten Koeffizienten~~ Koeffizienten aus $\mathbb{Q}(x)$ (sogar aus $\mathbb{Q}$):

$X^2 + X + 1 = 0$. $\quad (\Phi_3 = X^2 + X + 1)$

Lösungsvorschlag zu Blatt 14, Aufgabe 5 (Fortsetzung)

Behauptung: $|\mathrm{Gal}_{\mathbb{Q}}(\underline{y})| = 12$, wobei $\mathrm{Gal}_{\mathbb{Q}}(\underline{y}) := \mathrm{Gal}_{\mathbb{Q}}(y_1, \dots, y_6)$.

Beweis: $|\mathrm{Gal}_{\mathbb{Q}}(\underline{y})| = [\mathbb{Q}(y_1, \dots, y_6) : \mathbb{Q}] = [\mathbb{Q}(x_1, \omega) : \mathbb{Q}] = 12$.

$\mathbb{Q}(y_1, \dots, y_6) = \mathbb{Q}(x_1, \omega x_1, \omega^2 x_1, -\frac{1}{x_1}, -\frac{\omega}{x_1}, -\frac{\omega^2}{x_1}) \overset{\text{II}' := \text{II} \cdot \text{IV}}{=} \mathbb{Q}(x_1, -\omega, \omega^2 x_1, -\frac{1}{x_1}, -\frac{\omega}{x_1}, -\frac{\omega^2}{x_1})$

$= \mathbb{Q}(x_1, -\omega) = \mathbb{Q}(x_1, \omega)$

$\omega^2 x_1, -\frac{1}{x_1}, -\frac{\omega}{x_1}, -\frac{\omega^2}{x_1}$ rational in $x_1, -\omega$

## Lösungsvorschlag zu Blatt 14, Aufgabe 5 (Forts.)

(4) **Beh.** Es gibt Permutationen $s$ und $d$ mit

$$s\cdot x = x^6,\quad s\cdot\omega = \omega^2,$$
$$d\cdot x = -\omega^2/x,\quad d\cdot\omega = \omega^2,$$

welche beide Elemente der Galoisgruppe $\mathrm{Gal}_{\mathbb{Q}}(\underline{y})$ sind.

**Bew.:** Zunächst eine Vorüberlegung:

1) Es gilt $x^6 - 2x^3 - 1 = 0$. (kleines „x"!)
Somit folgt für jede Symmetrie $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(\underline{y})$:
$$0 = \sigma\cdot 0 = \sigma\cdot(x^6 - 2x^3 - 1) = (\sigma\cdot x)^6 - 2(\sigma\cdot x)^3 - 1,$$
also ist $\sigma\cdot x$ eine Lösung der Gleichung
$$X^6 - 2X^3 - 1 = 0$$
und somit (nach (*)) gleich eine der Zahlen
$$x,\ \omega x,\ \omega^2 x,\ -1/x,\ -\omega/x,\ -\omega^2/x.$$

2) Es gilt $\omega^2 + \omega + 1 = 0$.
Somit folgt für jede Symmetrie $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(\underline{y})$:
$$0 = \sigma\cdot 0 = \sigma\cdot(\omega^2 + \omega + 1) = (\sigma\cdot\omega)^2 + (\sigma\cdot\omega) + 1,$$
also ist $\sigma\cdot\omega$ eine Lösung der Gleichung
$$Z^2 + Z + 1 = 0,$$
also ist $\sigma\cdot\omega$ gleich $\omega$ oder gleich $\omega^2$.

Wir definieren nun: $M := \{(a,b) \mid a\in A,\ b\in B\}$, wobei $A = \{x, \omega x, \omega^2 x, -1/x, -\omega/x, -\omega^2/x\}$ und $B := \{\omega, \omega^2\}$.
Nach dem Zählprinzip enthält die Menge $M$ zwölf Elemente — also genau so viele, wie die gesuchte Galoisgruppe.

Ferner definieren wir eine Abbildung:
$$\varphi: \mathrm{Gal}_{\mathbb{Q}}(\underline{y}) \longrightarrow M,\quad \sigma \longmapsto (\sigma\cdot x,\ \sigma\cdot\omega).$$

Nach der Vorüberlegung ist diese wohldefiniert, d.h. $(\sigma\cdot x, \sigma\cdot\omega)\in M$ für $\sigma\in\mathrm{Gal}_{\mathbb{Q}}(\underline{y})$.
Außerdem ist sie injektiv, denn da $\Phi(y_1,\dots,y_6) = \Phi_1(x,\omega)$ ist eine Symmetrie $\sigma$ durch die Angabe von $\sigma\cdot x$ und $\sigma\cdot\omega$ schon eindeutig bestimmt.
Da Quell- und Zielmenge gleich viele und endlich viele Elemente besitzen, folgt, dass $\varphi$ surjektiv und somit bijektiv ist.

Lösungsvorschlag zu ~~Blatt~~ Blatt 14, Aufgabe 5 (Forts.)

Damit haben wir gezeigt:

Zu jeder Vorgabe $(a,b) \in M$ gibt es eine Symmetrie $\sigma \in \mathrm{Sol}_{\mathbb{Q}}(\underline{4})$ mit

$$\sigma \cdot x = a, \quad \sigma \cdot \omega = b.$$

Insbesondere können wir $(a,b) := (x, \omega^2)$ wählen und somit $s$ als Element der Galoisgruppe nachweisen; und analog erhalten wir $d$, wenn wir $(a,b) := (-\omega^2/x, \omega^2)$ setzen.

Lösungsvorschlag zu Blatt 14, Aufgabe 5 (Forts.)

Ges.: Alle Elemente von $\mathrm{Gal}_{\mathbb{Q}}(\underline{y})$.

Bew.: 1) id.

2) $\delta: x \longmapsto -\omega^3/x, \quad \omega \longmapsto \omega^2$

3) $\delta^2: x \longmapsto \omega^2 x, \quad \omega \longmapsto \omega^4 = \omega^3\,\omega = 1\cdot\omega = \omega$

denn: $\delta^2 \cdot x = \delta\cdot(\delta\cdot x) = \delta\cdot\left(-\frac{\omega^2}{x}\right) = -\frac{\delta\cdot\omega^2}{\delta\cdot x} = -\frac{(\delta\cdot\omega)(\delta\cdot\omega)}{\delta\cdot x} = -\frac{\omega^4}{-\omega^2/x}$

4) $\delta^3: x \longmapsto -\frac{1}{x}, \quad \omega \longmapsto \omega^2$

5) $\delta^4: x \longmapsto x/\omega^2, \quad \omega \longmapsto \omega^4 = \omega$

6) $\delta^5: x \longmapsto -\omega/x, \quad \omega \longmapsto \omega^2$

($\delta^6 \cdot x = x, \ \delta^6\cdot\omega = \omega$, also $\delta^6 = \mathrm{id}$, schon unter 1) aufgeführt)

7) $s\delta: x \longmapsto -\omega/x, \quad \omega \longmapsto \omega$

($s^2\delta: x \longmapsto -\omega^2/x, \quad \omega \longmapsto \omega^2$, schon unter 2) aufgeführt)

8) $\delta s: x \longmapsto -\omega^2/x, \quad \omega \longmapsto \omega$

9) $s: x \longmapsto x, \quad \omega \longmapsto \omega^2$

10) $\delta^2 s: x \longmapsto \omega^2 x, \quad \omega \longmapsto \omega^2$

11) $\delta^3 s: x \longmapsto -1/x \quad \omega \longmapsto \omega$

12) $\delta^4 s: x \longmapsto x/\omega^2, \quad \omega \longmapsto \omega^2$

Das sind jetzt zwölf verschiedene Elemente, wir können aufhören.

Beispielhaft die Wirkung von $\delta^3 s$ genauer:

$\delta^3 s \cdot y_1 = y_4, \quad \delta^3 s \cdot y_2 = y_5, \quad \delta^3 s \cdot y_3 = y_6, \quad \delta^4 s \cdot y_4 = y_1, \quad \delta^4 s \cdot y_5 = y_2, \quad \delta^4 s \cdot y_6 = y_3,$

$$\delta^3 s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

(d) Beh.: $\mathbb{Q}(x,\omega) = \mathbb{Q}(x+\omega)$

Bew.: „$\supseteq$" ist klar, „$=$" folgt aus Freiheit: $[\mathbb{Q}(x+\omega):\mathbb{Q}] = [\underbrace{\mathbb{Q}(x+\omega,x)}_{=\mathbb{Q}(x,\omega)}:\mathbb{Q}(x)]\,[\mathbb{Q}(x):\mathbb{Q}] = 2\cdot 6$

$= [\mathbb{Q}(x,\omega):\mathbb{Q}]$

(e) Ges.: Übliche Namen von $\mathrm{Gal}_{\mathbb{Q}}(\underline{y})$.

Bew.: Schreibt man die Verknüpfungstafeln von $\mathrm{Gal}_{\mathbb{Q}}(\underline{y})$ und $D_6$ hin, so sieht man, dass bis auf Umbenennung der Elemente das gleiche dasteht.

Folglich: „$\mathrm{Gal}_{\mathbb{Q}}(\underline{y})$ ist isomorph zu $D_6$."

# Aufgabe 9 von Blatt 15

Sei $f \in \mathbb{Q}[X]$ normiert, separabel, $x_1, \dots, x_n$ seien die (alle) Nullstellen von $f$. Mindestens eine der Nullstellen sei nicht-reell.

**Behauptung.** *Es gibt eine Permutation $\sigma \in S_n$ mit folgenden zwei Eigenschaften:*

1. $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_n)$.
2. *$\sigma$ hat Ordnung 2, d. h. $\sigma \neq \mathrm{id}$ und $\sigma^2 = \mathrm{id}$.*

*Beweis (danke an Martin!).* Man weiß: Hat ein Polynom mit reellen Koeffizienten eine nicht-reelle Nullstelle, so ist auch das komplex Konjugierte der Nullstelle eine Nullstelle des Polynoms.

[Denn: Gelte ganz allgemein $p(x) = 0$, wobei $p$ nur reelle Koeffizienten hat und $x \in \mathbb{C}$ eine beliebige Nullstelle ist. Dann gilt: $0 = \overline{0} = \overline{p(x)} = p(\overline{x})$, wobei somit auch $\overline{x}$ eine Nullstelle von $p$ ist. Der letzte Schritt der Rechnung folgt daraus, dass $p$ nur reelle Koeffizienten besitzt.]

Wir ordnen nun die Nullstellen von $f$ so an, dass die reellen Nullstellen hinten stehen $(x_{r+1}, \dots, x_n)$, und dass die komplex-konjugierten Paare vorne nebeneinander stehen, also dass gilt:

$$x_2 = \overline{x_1}, \quad x_4 = \overline{x_3} \quad \dots \quad x_r = \overline{x_{r-1}}.$$

Wir definieren nun folgende Permutation:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & r-1 & r & r+1 & \cdots & n \\ 2 & 1 & 4 & 3 & \cdots & r & r-1 & r+1 & \cdots & n \end{pmatrix}$$

Dann ist zumindest klar, dass die Ordnung von $\sigma$ zwei ist. Es ist aber noch nicht klar, dass $\sigma$ ein Element der Galoisgruppe ist.

Um das zu zeigen, gehen wir direkt nach Definition vor: Sei $H \in \mathbb{Q}[X_1, \dots, X_n]$ eine beliebige algebraische Relation der Nullstellen, d. h. es gilt $H(x_1, \dots, x_n) = 0$.

Zu zeigen ist, dass auch gilt:

$$H(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = H(x_2, x_1, x_4, x_3, \dots, x_r, x_{r-1}, x_{r+1}, \dots, x_n) = 0$$

Dazu folgende Rechnung:

$$\begin{aligned} 0 &= H(x_1, \dots, x_n) \\ &= \overline{H(x_1, \dots, x_n)} \\ &= H(\overline{x_1}, \dots, \overline{x_n}) \\ &= H(x_2, x_1, x_4, x_3, \dots, x_r, x_{r-1}, x_{r+1}, \dots, x_n) \end{aligned}$$

Der Schritt von der zweiten in die dritte Zeile ist deswegen erlaubt, weil $H$ nur reelle Koeffizienten besitzt. Damit ist der Beweis abgeschlossen. □

# Aufgabe 9 der Probeklausur

Sei $f \in \mathbb{Q}[X]$ normiert und separabel, seien $x_1, \dots, x_n$ die (alle) Nullstellen von $f$. Sei $\mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_4)$ zyklisch von Ordnung 4.

**Behauptung.** *Die Gleichung*

$$X^2 + 1 = 0$$

*besitzt keine Lösung in* $K := \mathbb{Q}(x_1, \dots, x_4)$.

*Beweis (Ausarbeitung der Lehrstuhllösung).* Zunächst eine Vorüberlegung: Das Polynom $f$ ist nicht nur separabel, sondern auch irreduzibel. Denn da die Galoisgruppe der Nullstellen von $f$ nach Voraussetzung zyklisch ist, gilt insbesondere, dass die Wirkung der Galoisgruppe transitiv auf den Nullstellen ist (d. h., dass es für alle $1 \leq i, j \leq 4$ eine Symmetrie $\sigma$ der Galoisgruppe mit $\sigma(i) = j$ gibt). Somit sind aber alle vier Nullstellen zueinander galoisch konjugiert. (Denn: Zwei Zahlen aus $K$ sind genau dann zueinander galoisch konjugiert, wenn es eine Symmetrie der Galoisgruppe gibt, die bei Multiplikation mit ihr die eine Zahl auf die andere abbildet.) Das geht nur, wenn $f$ irreduzibel ist.

Insbesondere ist somit klar, dass $f$ das gemeinsame Minimalpolynom der $x_i$ ist, und dass die $x_i$ jeweils vom Grad 4 über $\mathbb{Q}$ sind. Außerdem ist klar, dass $x_1$ ein primitives Element der $x_i$ ist, denn es gilt:

$$\left.\begin{aligned} &\mathbb{Q}(x_1) \subseteq \mathbb{Q}(x_1, \dots, x_4) \\ &[\mathbb{Q}(x_1) : \mathbb{Q}] = [\mathbb{Q}(x_1, \dots, x_4) : \mathbb{Q}] = 4 \end{aligned}\right\} \quad \Rightarrow \quad \mathbb{Q}(x_1) = \mathbb{Q}(x_1, \dots, x_4)$$

Die beiden Lösungen der Gleichung sind $i$ und $-i$. Würde $K$ eine dieser beiden Zahlen enthalten, dann auch die andere, da $K$ als Körper unter Negativenbildung abgeschlossen ist.

Eine weitere Vorüberlegung: Eine der Nullstellen $x_i$ muss nicht-reell sein. Denn wären alle Nullstellen reell, so wäre $K$ eine Teilmenge von $\mathbb{R}$ und würde somit sicher nicht $i$ enthalten. Ohne Beschränkung der Allgemeinheit sei $x_1$ eine der nicht-reellen Nullstellen.

Nun zum Hauptteil des Beweises, wir nehmen die Widerspruchsannahme an, dass $i$ ein Element von $K$ ist. Wir müssen irgendwie die spezielle Voraussetzung an die Galoisgruppe ausnutzen; unser Plan dazu, ist, den Hauptsatz der Galoistheorie zu verwenden!

Es ist nämlich klar, dass (unter der Widerspruchsannahme) $\mathbb{Q}(i)$ eine Zwischenerweiterung von $K$ ist,

$$\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq K,$$

wobei natürlich $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ gilt.

Somit ist $\mathrm{Gal}_{\mathbb{Q}(i)}(x_1, \dots, x_4)$ eine Untergruppe von $\mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_4)$ vom Index 2. Man weiß nun, dass, die Gruppe $\mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_4)$ genau eine Untergruppe vom Index 2 besitzt, da sie zyklisch ist.

[Denn: Wir können $\mathrm{Gal}_{\mathbb{Q}}(x_1, \ldots, x_4)$ schreiben als $\mathrm{Gal}_{\mathbb{Q}}(x_1, \ldots, x_4) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$, wobei $\sigma$ ein (nach Voraussetzung existenter) Erzeuger von $\mathrm{Gal}_{\mathbb{Q}}(x_1, \ldots, x_4)$ ist. Die einzige Untergruppe von Ordnung 2 ist dann $\{\mathrm{id}, \sigma^2\}$.]

Nach dem Hauptsatz der Galoistheorie gibt es somit auch nur eine Zwischenerweiterung von $\mathbb{Q}(x_1, \ldots, x_4)$ vom Grad 2.

Wir werden nun folgende Strategie verfolgen: Etwas unmotiviert werden wir eine weitere Zwischenerweiterung $L$ vom Grad 2 konstruieren. Da es nur eine solche Zwischenerweiterung gibt, muss dann $L = \mathbb{Q}(i)$ gelten; von $L$ wird aber klar sein, dass $L$ die Zahl $i$ nicht enthält, womit dann der Widerspruch erreicht ist.

Dazu betrachten wir nun zunächst das Minimalpolynom $g \in \mathbb{Q}(i)[X]$ von $x_1$ über $\mathbb{Q}(i)$. Nach der Vorüberlegung ist klar, dass $g$ Grad 2 hat, denn es gilt mit der Gradformel

$$4 = [\mathbb{Q}(x_1, \ldots, x_4) : \mathbb{Q}] = [\mathbb{Q}(x_1, \ldots, x_4) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(x_1) : \mathbb{Q}(i)].$$

Damit können wir auch das Polynom $f$ in einer anderen Form angeben, es gilt nämlich:

$$f(X) = g(X) \cdot \overline{g(X)}$$

Das hat folgenden Grund: Das Produkt $g\overline{g}$ ist normiert, hat nur rationale Koeffizienten, besitzt $x_1$ als Nullstelle und hat denselben Grad (nämlich 4) wie das Minimalpolynom von $x_1$ über $\mathbb{Q}$ (also $f$). Daraus folgt schon, dass $g\overline{g}$ das Minimalpolynom von $x_1$ ist.

Somit ist klar, dass die Zahl $\overline{x_1}$ eine weitere Nullstelle von $f$ ist. (Sie ist nämlich eine Nullstelle vom Faktor $\overline{g}$.)

Wir definieren nun

$$L := \mathbb{Q}(x_1 + \overline{x_1}, x_1\overline{x_1})$$

und zeigen:

a) $L$ ist eine Zwischenerweiterung von $K$.

b) $L$ hat Index 2 in $K$.

c) $L$ enthält nicht $i$.

Damit ist der Beweis dann abgeschlossen, denn wegen der oben angesprochenen Eindeutigkeit muss $L$ gleich $\mathbb{Q}(i)$ sein, da es nur eine Zwischenerweiterung vom Grad 2 gibt. Somit gilt $i \in \mathbb{Q}(i) = L$ im Widerspruch zu c).

a) Da $\overline{x_1}$ auch eine der vier Nullstellen von $f$ ist, sind die Zahlen $x_1 + \overline{x_1}$ und $x_1\overline{x_1}$ Elemente von $L$.

c) Klar, denn da $x_1 + \overline{x_1}$ und $x_1\overline{x_1}$ beides reelle Zahlen sind (die erste ist einfach der doppelte Realteil von $x_1$, die zweite das Quadrat des Betrags von $x_1$), gilt $L \subseteq \mathbb{R}$.

b) Es ist $(X - x_1)(X - \overline{x_1}) = X^2 - (x_1 + \overline{x_1}) + x_1\overline{x_1}$ das Minimalpolynom von $x_1$ über $L$. Denn es ist normiert, hat Koeffizienten nur aus $L$ und ist irreduzibel. Irreduzibel ist es deswegen, da es keine Nullstellen in $L$ besitzt (da es ein Polynom vom Grad 2 ist, ist diese Schlussweise ja zulässig): Denn $x_1 \in \mathbb{C} \setminus \mathbb{R}$, während $L \subseteq \mathbb{R}$.

Somit folgt mit der Gradformel aus

$$4 = [\mathbb{Q}(x_1, \ldots, x_4) : \mathbb{Q}] = [\mathbb{Q}(x_1) : \mathbb{Q}] = [\mathbb{Q}(x_1) : L] \cdot [L : \mathbb{Q}] = 2 \cdot [L : \mathbb{Q}]$$

in der Tat, dass $[L : \mathbb{Q}] = 2$ gilt. □

## Beispiel für den euklidischen Algorithmus

Für ganze Zahlen:

$x = 129, \quad y = 93.$

$$129 = 1 \cdot 93 + 36$$
$$93 = 2 \cdot 36 + 21$$
$$36 = 1 \cdot 21 + 15$$
$$21 = 1 \cdot 15 + 6$$
$$15 = 2 \cdot 6 + 3$$
$$6 = 2 \cdot 3 + 0$$

$\Rightarrow ggT(129, 93) = 3.$

Darstellung des ggT als $a \cdot 129 + b \cdot 93$:

$$3 = 15 - 2 \cdot 6 = 15 - 2 \cdot (21 - 1 \cdot 15) = 3 \cdot 15 - 2 \cdot 21 = 3 \cdot (36 - 1 \cdot 21) - 2 \cdot 21 = 3 \cdot 36 - 5 \cdot 21 = 13 \cdot 36 - 5 \cdot 93 = 13 \cdot 129 - 18 \cdot 93$$

mit $6 = 21 - 1 \cdot 15$, $15 = 36 - 1 \cdot 21$, $21 = 93 - 2 \cdot 36$, $36 = 129 - 1 \cdot 93$.

also $3 = \underline{13} \cdot 129 + \underline{(-18)} \cdot 93.$

## Beispiel für den euklidischen Algorithmus (Forts.)

Für Polynome:

$$f = x^7 - 5x^6 + 6x^5 + 5x^4 - 17x^3 + 15x^2 - 3x - 2$$
$$g = x^5 - 5x^4 + 8x^3 - 6x^2 + x + 1$$

$$f = (x^2 - 2)g + \underbrace{(x^4 - 2x^3 + 2x^2 - x)}_{=:p}$$
$$g = (x - 3)p + \underbrace{(x^2 - 2x + 1)}_{=:q}$$
$$p = (x^2 + 1)q + (x - 1)$$
$$q = (x - 1)(x - 1) + 0$$

$$\Rightarrow \operatorname{ggT}(f, g) = x - 1.$$

Darstellung des ggT als $af + bg$ für gewisse Polynome $a, b \in \mathbb{Q}[x]$:

$$\begin{aligned} x - 1 &= p - (x^2 + 1)q = p - (x^2 + 1)(g - (x - 3)p) \\ &= (1 + (x - 3)(x^2 + 1))p - (x^2 + 1)g \\ &= (1 + (x - 3)(x^2 + 1))(f - (x^2 - 2)g) - (x^2 + 1)g \\ &= (1 + (x - 3)(x^2 + 1))f + (-(x^2 - 2)(1 + (x - 3)(x^2 + 1)) - (x^2 + 1))g \\ &= \underbrace{(x^3 - 3x^2 + x - 2)}_{=:a} f + \underbrace{(-x^5 + 3x^4 + x^3 - 5x^2 + 2x - 5)}_{=:b} g \end{aligned}$$

## Beispiel zur Abgeschlossenheit der algebraischen Zahlen unter Multiplikation

Sei $x = 1+\sqrt{2}$. Sei $y = \sqrt{3}+5$.

Dann sind $x$ und $y$ algebraisch, denn sie sind Nullstellen normierter Polynomgleichungen mit rationalen Koeffizienten:

$$x^2 - 2x - 1 = (1+\sqrt{2})^2 - 2(1+\sqrt{2}) - 1 = 1 + 2\sqrt{2} + 2 - 2 - 2\sqrt{2} - 1 = 0.$$

$$y^2 - 10y + 22 = 3 + 10\sqrt{3} + 25 - 10\sqrt{3} - 50 + 22 = 0.$$

Nach Vorlesung ist daher auch das Produkt $x \cdot y$ algebraisch.

Mit folgendem Verfahren kann man ganz allgemein eine normierte Polynomgleichung mit rationalen Koeffizienten finden, die $x \cdot y$ als Nullstelle hat, und somit die Algebraizität von $x \cdot y$ beweist.

Dazu definieren wir Zahlen $c_{ij}$:

$$c_{ij} := x^i y^j \quad \text{für } i = 0, \dots, m-1 \quad j = 0, \dots, n-1,$$

wobei $m$ der Grad des Polynoms zu $x$ (hier also 2) und $n$ der Grad des Polynoms zu $y$ (hier also wieder 2) ist.

Nun schreibt man $x \cdot y \cdot c_{ij}$ für alle $c_{ij}$ als rationale Linearkombinationen der $c_{ij}$:

$$xy\,c_{00} = xy\,x^0y^0 = xy = c_{11}$$

$$xy\,c_{01} = xy\,x^0y^1 = xy^2 = x(10y - 22) = 10xy - 22x = 10c_{11} - 22c_{10}$$

$$xy\,c_{10} = xy\,x^1y^0 = x^2y = (2x+1)y = 2xy + y = 2c_{11} + c_{01}$$

$$xy\,c_{11} = xy\,x^1y^1 = x^2y^2 = (2x+1)(10y-22) = 20xy - 44x + 10y - 22$$
$$= -22c_{00} + 10c_{01} - 44c_{10} + 20c_{11}$$

In Matrixform:

$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{pmatrix} & & & 1 \\ & & -22 & 10 \\ & 1 & & 2 \\ -22 & 10 & -44 & 20 \end{pmatrix} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} = xy \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix}$$

$\qquad\qquad 00 \quad 01 \quad 10 \quad 11$

Also ist $xy$ ein Eigenwert dieser Matrix, und somit eine Nullstelle des charakteristischen Polynoms dieser Matrix,

$$p = \det \begin{pmatrix} -\lambda & 0 & 0 & 1 \\ 0 & -\lambda & -22 & 10 \\ 0 & 1 & -\lambda & 2 \\ -22 & 10 & -44 & 20-\lambda \end{pmatrix} = -\lambda \det \begin{pmatrix} -\lambda & -22 & 10 \\ 1 & -\lambda & 2 \\ 10 & -44 & 20-\lambda \end{pmatrix} - \det \begin{pmatrix} 0 & -\lambda & -22 \\ 0 & 1 & -\lambda \\ -22 & 10 & -44 \end{pmatrix}$$

$$= -\lambda\left(\lambda^2(20-\lambda) - 440 - 440 + 100\lambda - 88\lambda + \frac{110}{22}(20-\lambda)\right)$$

$$+ 22\left(\lambda^2 + 22\right) = \dots =$$

$$= \lambda^4 - 20\lambda^3 + \frac{100}{32}\lambda^2 + \frac{660}{1080}\lambda + 484$$

Wir sehen: Dieses Polynom ist normiert, hat nur rationale Koeffizienten, und hat $xy$ als Nullstelle. Damit haben wir unser Ziel erreicht.

Bemerkungen:

- Der Grad des gefundenen Polynoms war hier 4.
  Was ist er im Allgemeinen, in Abhängigkeit von $n$ und $m$, den Graden der Polynome zu $x$ und $y$?
- Zu jeder algebraischen Zahl gibt es unendlich viele normierte Polynomgleichungen mit rationalen Koeffizienten, die sie als Nullstelle haben, z.B. für $x$:
  $x^2 - 2x - 1$
  $(x^2-2x-1)^2$
  $(x^2-2x-1)(x^2+1)$
  $(x^2-2x-1)(x-17)$
  $\vdots$
- In der Praxis kann man vielleicht schneller auf direktem Weg (durch Gleichung umstellen/potenzieren) eine Gleichung für $xy$ (oder auch $x+y$, ...) finden.
  Das hier beschriebene Verfahren funktioniert aber auch, wenn man keine geschlossenen Formeln für $x$ und $y$ kennt. Damit ist gemeint:
  Sei $x$ eine Lösung von $x^{11} - 3x^2 + 5x - 12 = 0$,
  sei $y$ eine Lösung von $y^{100} + 10y^{10} + y + 1 = 0$.
  Dann lässt sich eine normierte Polynomgleichung mit rationalen Koeffizienten, die $xy$ als Nullstelle besitzt, mit diesem Verfahren bestimmen, ohne $x$ und $y$ selbst zu kennen!
- Je nach LA-Konvention ist das charakteristische Polynom vielleicht nicht normiert, sondern hat $-1$ als Koeffizient der höchsten Potenz. In diesem Fall die Gleichung einfach noch mit $-1$ durchmultiplizieren.
- Für $x+y$ statt $xy$ ändert sich nur das Aufstellen der rationalen Linearkombinationen, es muss dann heißen:
  $(x+y)\, c_{00} = \cdots$
  $(x+y)\, c_{01} = \cdots$
  $\vdots$
  $(x+y)\, c_{n-1,m-1} = \cdots$

**Das Newton-Verfahren** zur Bestimmung von Näherungslösungen von Gleichungen für normale, nicht-programmierbare Taschenrechner

Sei $f(X)=0$ eine Gleichung.
Aus der Numerik weiß man, dass die Iteration

$x_0$ beliebig
$x_1 = x_0 - f(x_0)/f'(x_0)$
$x_2 = x_1 - f(x_1)/f'(x_1)$
$x_3 = x_2 - f(x_2)/f'(x_2)$
$\vdots$
$x_{n+1} = x_n - f(x_n)/f'(x_n)$
$\vdots$

unter guten Bedingungen gegen eine Nullstelle von $f$ konvergiert.
Man kann dieses Verfahren auf normalen, nicht-programmierbaren Taschenrechnern umsetzen, sofern sie nur eine Taste wie „Ans", die das letzte Ergebnis zurückliefern, besitzen.

**Bsp:** Wir wollen näherungsweise eine Nullstelle von
$f = X^3 - 3X^2 + 5$
finden. Dazu tippen wir in einen Taschenrechner eine beliebige Startlösung, beispielsweise

17,

ein. Dann tippen wir ein:

Ans − (Ans³ − 3 Ans² + 5) / (3 Ans² − 6 Ans)

und drücken wiederholt (10 bis 20 Mal) die =-Taste.
Unter guten Bedingungen, d.h. mit ein wenig Glück, stabilisieren sich die ausgegebenen Näherungen zu einer Nullstelle von $f$.

**Bem:** Das Verfahren funktioniert nicht nur für Polynome, sondern auch für beliebige (genügend glatte) Funktionen, bspw. $f$ mit $f(x) = 17\sin^2 x + \sqrt{2x}$.

**Bem:** Oder man nimmt http://www.wolframalpha.com/. ☺