Aufgabe 62:
Sei L der Zerfällungskörper von $x^4 - 3 \in \mathbb{Q}[x]$ über $\mathbb{Q}$. Bestimme alle Zwischenkörper der Körpererweiterung $L/\mathbb{Q}$ und alle Untergruppen der Galoisgruppe $G(L/K)$.

Die Nullstellen des Polynoms f in L sind $\sqrt[4]{3}$, $-\sqrt[4]{3}$, $i\sqrt[4]{3}$ und $-i\sqrt[4]{3}$. Damit ist f separabel über $\mathbb{Q}$ und $L = \mathbb{Q}(i, \sqrt[4]{3})$ der Zerfällungskörper eines separablen Polynoms. Also ist die Körpererweiterung $L/\mathbb{Q}$ Galoissch und nach 12.32 gilt

$$|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[4]{3})] \cdot [\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Offensichtlich sind die Abbildungen τ und σ mit $\tau(i) = -i$, $\tau|_{\mathbb{Q}(\sqrt[4]{3})} = id|_{\mathbb{Q}(\sqrt[4]{3})}$ bzw. $\sigma(i) = i$, $\sigma(\sqrt[4]{3}) = i\sqrt[4]{3}$ Elemente von $\mathrm{Gal}(L/\mathbb{Q})$ und es ergibt sich

$$\mathrm{Gal}(L/\mathbb{Q}) = \{id, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \cong D_4.$$

Als Untergruppen der D_4 erhalten wir

$U_0 = \{id\}$	$U_1 = \{id, \sigma^2\}$	$U_2 = \{id, \tau\}$	$U_3 = \{id, \sigma\tau\}$
$U_4 = \{id, \sigma^2\tau\}$	$U_5 = \{id, \sigma^3\tau\}$	$U_6 = \langle\sigma\rangle$	$U_7 = \{id, \tau, \sigma^2, \sigma^2\tau\}$
$U_8 = \{id, \sigma^2, \sigma\tau, \sigma^3\tau\}$		$U_9 = \mathrm{Gal}(L/\mathbb{Q})$	

und die zugehörigen Fixkörper $L_i = \mathrm{Fix}_{U_i}(L)$ mit

$L_0 = L$	$L_1 = \mathbb{Q}(i, \sqrt{3})$	$L_2 = \mathbb{Q}(\sqrt[4]{3})$	$L_3 = \mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3})$
$L_4 = \mathbb{Q}(i\sqrt[4]{3})$	$L_5 = \mathbb{Q}((1-i)\sqrt[4]{3})$	$L_6 = \mathbb{Q}(i)$	$L_7 = \mathbb{Q}(\sqrt{3})$
$L_8 = \mathbb{Q}(i\sqrt{3})$	$L_9 = \mathbb{Q}$		

Aufgabe 63:
Sei K ein Körper und $f \in K[x]\backslash K$ ein Polynom. Ist L der Zerfällungskörper von f über K, so heißt $\mathrm{Gal}(f : K) = \mathrm{Gal}(L/K)$ die *Galoisgruppe* von f über K. Sei nun f irreduzibel über K. Zeigen Sie:

a) Enthält K alle n-ten Einheitswurzeln für $n \geq 2$ und ist $f(x) = x^n - a$ für ein $a \in K$, so gilt $\mathrm{Gal}(f : K) \cong \mathbb{Z}/n\mathbb{Z}$.
b) Ist $p = \deg(f)$ eine Primzahl und enthält $G(f : K)$ ein Element der Ordnung p sowie eine Transposition, so gilt $\mathrm{Gal}(f : K) \cong S_p$.
c) Sei p prim und $f \in \mathbb{Q}[x]$ mit $\deg(f) = p$. Hat f genau zwei nicht-reelle Nullstellen in $\mathbb{C}$, so gilt $\mathrm{Gal}(f : \mathbb{Q}) \cong S_p$.
d) Ist $f \in \mathbb{Q}[x]$ mit abelscher Galoisgruppe $\mathrm{Gal}(f : \mathbb{Q})$, so ist $\mathrm{Gal}(f : \mathbb{Q})$ eine Gruppe der Ordnung $\deg(f)$.

Beweis. Für den Beweis von a) sei b eine Nullstelle von $f(x) = x^n - a$ und ξ eine primitive n-te Einheitswurzel. Dann sind durch $b, \xi b, \ldots, \xi^{n-1}b$ alle Nullstellen von f gegeben, d.h. wegen $\xi \in K$ ist $K(b)$ der Zerfällungskörper von f über K. Nun ist jeder Automorphismus $\sigma \in \mathrm{Gal}(f : K)$ eindeutig durch $\sigma(b) = \xi^k b$ bestimmt mit $k \in \{0, \ldots, n-1\}$. Die Behauptung folgt nun aus der Tatsache, dass die Abbildung $\varphi : \mathrm{Gal}(f : K) \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $\sigma \mapsto k + n\mathbb{Z}$ ein Automnorphismus ist (leicht nachzuprüfen).

Da jedes Element von $\mathrm{Gal}(f : K)$ die p Nullstellen von f permutiert, ist $\mathrm{Gal}(f : K)$ eine Untergruppe der S_p. Weiter enthält $\mathrm{Gal}(f : K)$ einen p-Zyklus σ, da wegen p prim diese die einzigen Elemente in S_p der Ordnung p sind. Nach Voraussetzung enthält $\mathrm{Gal}(f : K)$ auch eine Transposition τ. Da σ und τ die S_p erzeugen, folgt b).

Für den Beweis von c) besitze nun $f \in \mathbb{Q}[x]$ genau zwei nicht-reelle Nullstellen. Dann ist der Automorphismus $\tau : L \longrightarrow L, z \mapsto \overline{z}$ offensichtlich ein Element von $\mathrm{Gal}(f : \mathbb{Q})$. Also enthält $\mathrm{Gal}(f : \mathbb{Q})$ eine Transposition. Die Galoisgruppe besitzt auch ein Element der Ordnung p, denn ist a eine Nullstelle von f, so gilt

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}] = [L : \mathbb{Q}(a)] \cdot p.$$

Da $L/\mathbb{Q}$ nach 12.20 Galoissch ist, ist p demnach ein Teiler von $|\mathrm{Gal}(f : \mathbb{Q})|$. Nach dem Satz von Cauchy existiert in $\mathrm{Gal}(f : \mathbb{Q})$ also ein Element der Ordnung p. Mit b) folgt dann die Behauptung.

Um d) zu zeigen, sei n der Grad von f. Die Galoisgruppe $\mathrm{Gal}(f : \mathbb{Q})$ operiert transitiv auf der Menge der Nullstellen $\{a_1, \ldots, a_n\}$ von f, d.h. zu jedem $i \in \{1, \ldots, n\}$ existiert ein $\sigma_i \in \mathrm{Gal}(f : \mathbb{Q})$ mit $\sigma_i(a_1) = a_i$. Also gilt $\{\sigma_1, \ldots, \sigma_n\} \subseteq \mathrm{Gal}(f : \mathbb{Q})$ und somit $|\mathrm{Gal}(f : \mathbb{Q})| \geq n$. Andererseits ist auch $|\mathrm{Gal}(f : \mathbb{Q})| \leq n$ erfüllt, denn jedes $\sigma \in \mathrm{Gal}(f : \mathbb{Q})$ bildet a_1 auf eine Nullstelle a_j von f ab. Es ist daher

$$\sigma(a_1) = a_j = \sigma_j(a_1),$$

d.h.

$$\sigma(a_i) = \sigma\sigma_i^{-1}(a_1) = \sigma_i^{-1}\sigma(a_1) = \sigma_i^{-1}\sigma_j(a_1) = \sigma_j(a_i).$$

Also ergibt sich $\sigma = \sigma_j$. □

Aufgabe 64:
Bestimmen Sie die Galoisgruppe der folgenden Polynome:

a) $f(x) = x^3 - 10 \in \mathbb{Q}[x]$,
b) $f(x) = x^p - a \in K[x]$ mit $a \in K$ und $\mathrm{char}(K) = p > 0$,
c) $f(x) = x^n - a \in \mathbb{C}(a)[x]$ mit $n \in \mathbb{N}$ und a transzendent über $\mathbb{C}$.

Das Polynom $f(x) = x^3 - 10$ ist irreduzibel (Eisenstein) und hat in $\mathbb{C}$ die Nullstellen $\sqrt[3]{10}$, $\xi\sqrt[3]{10}$, $\xi^2\sqrt[3]{10}$, wobei ξ eine primitive dritte Einheitswurzel sei. Damit besitzt f genau zwei nicht-reelle Nullstellen und mit Aufgabe 63 b) folgt $\mathrm{Gal}(f : \mathbb{Q}) = S_3$.

Sei b eine Nullstelle des Polynoms $f(x) = x^p - a \in K[x]$. Dann ist $b^p = a$ und $x^p - a = (x - b)^p$ in $K(b)[x]$. Jeder Automorphismus $\sigma \in \mathrm{Gal}(K(b) : K) = \mathrm{Gal}(f : K)$ ist durch $\sigma(b)$ eindeutig bestimmt. Da das Bild von b wieder eine Nullstelle von f ist, muss $\sigma(b) = b$ und somit $\sigma = id$ gelten. Also erhalten wir $\mathrm{Gal}(f : K) = \{id\}$.

Auch das Polynom $f(x) = x^n - a \in \mathbb{C}(a)[x]$ ist irreduzibel, da a in $C[a]$ prim ist. Mit Aufgabe 63 a) folgt schließlich $\mathrm{Gal}(f : \mathbb{C}(a)) \cong \mathbb{Z}/n\mathbb{Z}$.

Aufgabe 65:
Sei K ein Körper und $L = K(x_1, \ldots, x_n)$ der Körper der rationalen Funktionen in den Unbestimmten $x_1, \ldots, x_n$ über K. Zeigen Sie:

a) Sind $s_0, \ldots, s_n$ die elementarsymmetrischen Polynome in $x_1, \ldots, x_n$ über K und ist $M = K(s_0, \ldots, s_n)$, so ist die Körpererweiterung L/M Galoissch vom Grad $n!$.
b) Das *allgemeine Polynom n-ten Grades* $f(x) = x^n + y_1x^{n-1} + \cdots + y_{n-1}x + y_n \in K(y_1, \ldots, y_n)[x]$ ist über $K(y_1, \ldots, y_n)$ für $n \geq 5$ nicht durch Radikale auflösbar.

Beweis. Das Polynom $f(x) = (x-x_1)\cdots(x-x_n) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n \in M[x]$ ist offensichtlich separabel mit Nullstellen $x_1, \ldots, x_n$, d.h. L ist der Zerfällungskörper von f über M. Nach Satz 12.20 ist L/M Galoissch. Ferner ist $\mathrm{Gal}(f : M)$ eine Untergruppe der S_n und, da s_i für $i = 0, \ldots, n$ symmetrisch ist, auch $\sigma(s_i) = s_i$ für alle $\sigma \in S_n$, d.h. $S_n \subseteq \mathrm{Gal}(f : M)$. Insgesamt folgt also $[L : M] = |\mathrm{Gal}(f : M)| = |S_n| = n!$.

Für den Beweis von b) sei L' der Zerfällungskörper von f über $K(y_1, \ldots, y_n)$. Betrachte den Homomorphismus $\varphi : K(y_1, \ldots, y_n) \longrightarrow K(s_1, \ldots, s_n)$, $y_i \mapsto (-1)^i s_i$. Dieser ist wegen der algebraischen Unabhängigkeit von $s_1, \ldots, s_n$ bijektiv und besitzt eine Fortsetzung $\Phi : L' \longrightarrow L$. Wir erhalten nun mit $\sigma \mapsto \Phi^{-1}\sigma\Phi$ einen Isomorphismus der Galoisgruppen $\mathrm{Gal}(f : K(y_1, \ldots, y_n))$ und $\mathrm{Gal}(g : M)$ mit $g(x) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$. Da letztere isomorph zur S_n ist und diese für $n \geq 5$ nicht auflösbar ist, ist auch f für $n \geq 5$ nicht auflösbar. $\square$