Aufgabe 1 (Frühjahr 2014)**.** Sei L/K eine endliche Galoiserweiterung. Zeigen Sie, daß für $\alpha \in L$ folgende Aussagen äquivalent sind.

(a) Es gilt $L = K(\alpha)$.

(b) Für alle $g \in \mathrm{Gal}(L/K)$ mit $g \neq \mathrm{id}$ gilt $g(\alpha) \neq \alpha$.

Lösung. **„(a) ⇒ (b)“:** Nach (a) nehmen wir an, daß α ein primitives Element von L über K ist. Da L eine K-Algebra ist und genauer als K-Algebra von α erzeugt, ist jeder K-Automorphismus von L, das heißt jedes Element $g \in \mathrm{Gal}(L/K)$ eindeutig durch das Bild von α bestimmt. Es ist also $g = \mathrm{id}_L$ genau dann, wenn $g(\alpha) = \alpha$. Dies zeigt (b).

„(b) ⇒ (a)“: Wir nehmen (b) an, das heißt es gilt $g(\alpha) \neq \alpha$ für alle $\mathrm{id}_L \neq g \in \mathrm{Gal}(L/K)$. Es ist $K \subset K(\alpha) \subset L$ ein Zwischenkörper, also ist $L/K(\alpha)$ Galois'sch und hat Galoisgruppe $\mathrm{Gal}(L/K(\alpha)) \subset \mathrm{Gal}(L/K)$. Nach Definition gilt für $g \in \mathrm{Gal}(L/K(\alpha))$ daß $g\big|_{K(\alpha)} = \mathrm{id}_{K(\alpha)}$, also insbesondere $g(\alpha) = \alpha$. Nach der Voraussetzung ist dann $g = \mathrm{id}_L$, also $\mathrm{Gal}(L/K(\alpha)) = \{\mathrm{id}_L\}$. Nach dem Hauptsatz der Galoistheorie ist der dazu korrespondierende Zwischenkörper L und es folgt $K(\alpha) = L$.

Aufgabe 2 (Herbst 2003)**.** Gegeben sei das Element $z = X^2 + X^{-2}$ des rationalen Funktionenkorpers $\mathbb{Q}(X)$.

(a) Zeigen Sie, daß $\mathbb{Q}(X)$ über $\mathbb{Q}(z)$ endlich vom Grad $\leqslant 4$ ist.

(b) Bestimmen Sie die Gruppe der Automorphismen von $\mathbb{Q}(X)$ die z festlassen.

(c) Zeigen Sie, daß $\mathbb{Q}(X)$ über $\mathbb{Q}(z)$ Galois'sch ist und geben Sie alle Körper zwischen $\mathbb{Q}(X)$ und $\mathbb{Q}(z)$ an.

Lösung. **Zu (a):** Wir zeigen, daß X Nullstelle eines Polynoms über $\mathbb{Q}(z)$ ist. Nach Umstellen der Gleichung $z = X^2 + X^{-2}$ gilt

$$zX^2 = X^4 + 1$$

Also $X^4 - zX^2 + 1 = 0$, das heißt X ist Nullstelle des Polynoms $Y^4 - zY^2 + 1 \in \mathbb{Q}(z)[Y]$. Das Element X ist also algebraisch über $\mathbb{Q}(z)$ und das Minimalpolynom von X über $\mathbb{Q}(z)$ teilt $Y^4 - zY^2 + 1$. Damit hat die Erweiterung $\mathbb{Q}(X)/\mathbb{Q}(z)$ maximal den Grad 4.

Zu (b): Die sind genau die Elemente in $\mathrm{Gal}(\mathbb{Q}(X)/\mathbb{Q}(z))$ und nach (a) ist $|\mathrm{Gal}(\mathbb{Q}(X)/\mathbb{Q}(z))| \leqslant [\mathbb{Q}(X) : \mathbb{Q}(z)] \leqslant 4$. Jedes Element in $\sigma \in \mathrm{Gal}(\mathbb{Q}(X)/\mathbb{Q}(z))$ ist eindeutig bestimmt durch den Wert $\sigma(X)$.
Sei $\sigma(X) = \frac{f}{g}$ mit teilerfremden Polynomen $f, g \in \mathbb{Q}[X]$ und $g \neq 0$. Nach Definition gilt

$$\begin{aligned}
\sigma(z) &= z \\
\sigma(X^2 + X^{-2}) &= X^2 + X^{-2} = \frac{X^4 + 1}{X^2} && \big| \text{ mit } z = X^2 + X^{-2} \\
\sigma(X^2 + X^{-2}) &= \sigma(X)^2 + \sigma(X)^{-2} = \frac{f^2}{g^2} + \frac{g^2}{f^2} = \frac{f^4 + g^4}{f^2 g^2} && \big| \text{ denn } \sigma \text{ ist Körperhomomorphismus}
\end{aligned}$$

Also

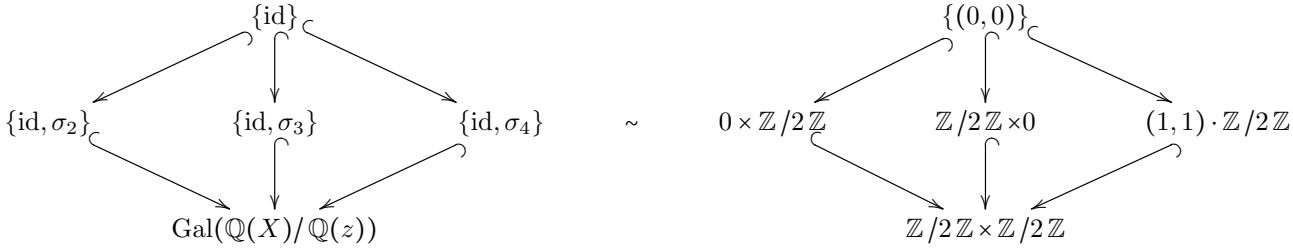
$$\frac{X^4 + 1}{X^2} = \frac{f^4 + g^4}{f^2 g^2}$$

und beide Brüche sind vollständig gekürzt, damit $f^2 g^2 = X^2$ und $f^4 + g^4 = X^4 + 1$. Also ist $f = \pm X$ und $g = \pm 1$ oder umgekehrt. $\sigma(X)$ kann also die Werte X, $-X$, X^{-1}, und $-X^{-1}$ annehmen. Damit gibt es vier Elemente in $\mathrm{Gal}(\mathbb{Q}(X)/\mathbb{Q}(z))$ gegeben durch

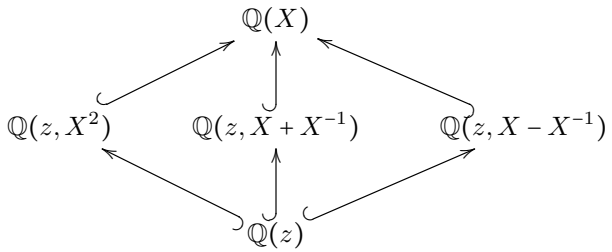
$$\begin{aligned}
\sigma_1(X) &= X && \text{also } \sigma_1 = \mathrm{id}_{\mathbb{Q}(X)} \\
\sigma_2(X) &= -X && \text{also } \sigma_2^2 = \mathrm{id}_{\mathbb{Q}(X)} \\
\sigma_3(X) &= X^{-1} && \text{also } \sigma_3^2 = \mathrm{id}_{\mathbb{Q}(X)} \\
\sigma_4(X) &= -X^{-1} && \text{also } \sigma_4^2 = \mathrm{id}_{\mathbb{Q}(X)}
\end{aligned}$$

Damit ist $\mathrm{Gal}(\mathbb{Q}(X)/\mathbb{Q}(z))$ isomorph zu $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Zu (c): Nach (b) gilt $4 = |\mathrm{Gal}(\mathbb{Q}(X)/\mathbb{Q}(z))| \leqslant [\mathbb{Q}(X):\mathbb{Q}(z)] \leqslant 4$ also hat die Erweiterung $\mathbb{Q}(X)/\mathbb{Q}(z)$ den Grad 4, und $Y^4 - zY^2 + 1 \in \mathbb{Q}(z)[Y]$ ist das Minimalpolynom von X über $\mathbb{Q}(z)$. Es hat genau die Nullstellen X, X^{-1}, $-X$ und $-X^{-1}$, die alle in $\mathbb{Q}(X)$ enthalten sind. Also ist $\mathbb{Q}(X)$ Zerfällungskörper von $Y^4 - zY^2 + 1 \in \mathbb{Q}(z)[Y]$ über $\mathbb{Q}(z)$, und damit ist die Erweiterung $\mathbb{Q}(X)/\mathbb{Q}(z)$ normal und separabel, also Galois'sch.
Nach dem Hauptsatz der Galoistheorie sind die Zwischenkörper von $\mathbb{Q}(X)/\mathbb{Q}(z)$ genau die Fixkörper der Untergruppen von $\mathrm{Gal}(\mathbb{Q}(X)/\mathbb{Q}(z)) = \{\mathrm{id}, \sigma_2, \sigma_3, \sigma_4\}$.



σ_2 hat den Fixpunkt X^2. Wir haben einen Turm $\mathbb{Q}(z) \subset \mathbb{Q}(z, X^2) \subset \mathbb{Q}(X)$. Da $X \notin \mathbb{Q}(z, X^2)$ ist die zweite Inklusion echt. Außerden ist X^2 kein Fixpunkt von σ_3 oder σ_4, liegt damit nicht im Grundkörper. Also ist $\mathbb{Q}(z, X^2)$ der Fixkörper von $\langle\sigma_2\rangle$.
σ_3 hat den Fixpunkt $X + X^{-1}$, und wieder haben wir echte Erweiterungen $\mathbb{Q}(z) \subsetneq \mathbb{Q}(z, X + X^{-1}) \subsetneq \mathbb{Q}(X)$, denn $X \notin \mathbb{Q}(z, X + X^{-1})$ und $X + X^{-1} \notin \mathbb{Q}(z)$, da $X + X^{-1}$ ist kein Fixpunkt von σ_2 oder σ_4. Also ist $\mathbb{Q}(z, X + X^{-1})$ der Fixkörper von $\langle\sigma_3\rangle$.
σ_4 hat den Fixpunkt $X - X^{-1}$, und wieder haben wir echte Erweiterungen $\mathbb{Q}(z) \subsetneq \mathbb{Q}(z, X - X^{-1}) \subsetneq \mathbb{Q}(X)$, denn $X - X^{-1} \notin \mathbb{Q}(z)$ und $X \notin \mathbb{Q}(z, X - X^{-1})$. Also ist $\mathbb{Q}(z, X - X^{-1})$ der Fixkörper von $\langle\sigma_4\rangle$.



Aufgabe 3 (Frühjahr 2004)**.** Es sei K/k eine Galoiserweiterung, deren Galoisgruppe isomorph zur symmetrischen Gruppe S_n ist. Zeigen Sie:

(a) K enthält n zueinander konjugierte Zwischenkörper vom Grad n über k, die zusammen K über k erzeugen.

(b) K ist der Zerfällungskörper eines Polynoms vom Grad n aus $k[X]$ über k

Lösung. **Zu (a):** Nach dem Hauptsatz der Galoistheorie gibt es zu jedem Zwischenkörper $k \subset E_i \subset K$ vom Grad n über k korrespondiert eine Untergruppe $U_i \subset \mathrm{Gal}(K/k) \cong S_n$ vom Index n, also Untergruppen der Ordnung $(n-1)!$. Dies sind die n Gruppen, die jeweils ein Element i festlassen

$$\mathrm{Stab}_{S_n}(i) = \{\sigma \in S_n \mid \sigma(i) = i\}.$$

Die zugehörigen n Zwischenkörper sind die gesuchten $k \subset E_i \subset K$ und es gilt

$$\mathrm{Gal}(K/E_i) \cong \mathrm{Stab}_{S_n}(i).$$

Das Kompositum $E_1 \cdots E_n$ ist ein Zwischenkörper $k \subset E_i \subset E_1 \cdots E_n \subset K$ und hat Galoisgruppe

$$\mathrm{Gal}(K/E_1 \cdots E_n) \cong \mathrm{Gal}(K/E_1) \cap \cdots \cap \mathrm{Gal}(K/E_n) \cong \mathrm{Stab}_{S_n}(1) \cap \cdots \cap \mathrm{Stab}_{S_n}(n) = \{\mathrm{id}\}.$$

Es folgt $K = E_1 \cdots E_n$.
Die Gruppen $\mathrm{Stab}_{S_n}(i)$ sind paarweise konjugiert zueinander: für $\sigma = (ij)$ gilt

$$\mathrm{Stab}_{S_n}(i) = \sigma \,\mathrm{Stab}_{S_n}(j)\sigma^{-1},$$

also $\mathrm{Gal}(K/E_i) = \sigma \,\mathrm{Gal}(K/E_j)\sigma^{-1}$ Für die zugehÃ¶rigen Körper gilt $E_i = \sigma(E_j)$, das heißt sie sind konjugiert.

Zu (b): Die Körper E_i aus (a) sind also separabel über k, und für einen davon, ohne Einschränkung E_1/k wählen wir ein primitives Element $E_1 = k(a)$. Sei $m_{k,a} \in k[X]$ das Minimalpolynom von $a$über k. Es hat Grad $\deg(m_{k,a}) = [E_1 : k] = n$.
Da K/k normal ist, und das ireduzible Polynome $m_{k,a} \in k[X]$ eine Nullstelle in K hat, muß $m_{k,a}$ über K in Linearfaktorne zerfallen. Wir behaupten, daß K der Zerfällungskörper von $m_{k,a}$ ist.
D E_1 zu jedem E_i konjugiert ist, gibt es zu jedem i ein $\sigma_i \in Gal(K/k) \cong S_n$ (nämlich $\sigma_i = (1i)$) mit $\sigma_i(E_1) = E_i$, insbesondere gilt $\sigma_i(a) \in E_i$. Da σ_i ein k-Automorphismus von K ist, ist $\sigma_i(a)$ ein primitives Element von E_i und ebenfalls eine Wurzel von $m_{k,a}$, denn es gilt $\sigma_i(m_{k,a}) = m_{k,a}$ und $0 = \sigma_i(0) = \sigma(m_{k,a}(a)) = m_{k,a}(\sigma_i(a))$.
Setzten wir $a_i = \sigma_i(a)$, so gilt $K = E_1 \cdots E_n = k(a_1, \ldots, a_n)$ wobei die a_i genau die n Nullstellen von $m_{k,a}$ sind.

Aufgabe 4 (Herbst 2004)**.** Es sei $K = \mathbb{F}_{3^3}$ der Körper mit 27 Elementen. Was ist die Ordnung der Galoisgruppe $G = \mathrm{Gal}(K/\mathbb{F}_3)$? In wieviele und wie lange Bahnen zerfällt K unter der Operation von G?

Lösung. Wie jede endliche Erweiterung eines endlichen Körpers ist $K/\mathbb{F}_3$ Galois'sch mit zyklischer Galoisgruppe die vom Frobenius $\sigma : K \to K, a \mapsto a^3$ erzeugt wird. Die Ordnung der Galoisgruppe ist der Grad der Körpererweiterung

$$|\mathrm{Gal}(K/\mathbb{F}_3)| = [K : \mathbb{F}_3] = 3.$$

Die Galoisgruppe enthält die Elemente

$$\mathrm{id} = \sigma^0 : a \mapsto a$$
$$\sigma : a \mapsto a^3$$
$$\sigma^2 : a \mapsto a^9$$

Wir untersuchen die Operation

$$\cdot : G \times K \to K, (g, a) \mapsto g(a).$$

Ist $a \in \mathbb{F}_3$, so git $a = a^3 = a^9$, also für die Bahn

$$G \cdot a = \{a\},$$

das heißt $|G \cdot a| = 1$, und es gibt drei solcher Bahnen der Länge 1.
Ist $a \in K \setminus \mathbb{F}_3$, so ist $a \neq a^3$, $a \neq a^9$ und $a^3 \neq a^9$, also

$$G \cdot a = \{a, a^3, a^9\},$$

das heißt $|G \cdot a| = 3$. Da $|K \setminus \mathbb{F}_3 = 27 - 3 = 24$ gibt es $\frac{24}{3} = 8$ solcher Bahnen.