Musterlösung Serie 25

GALOISERWEITERUNGEN, TRANSZENDENTE ERWEITERUNGEN, SYMMETRISCHE FUNKTIONEN

1. Betrachte $K := \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{R}$.

   (a) Zeige, dass $K/\mathbb{Q}$ galoissch ist mit Galoisgruppe $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   (b) Sei $L := K\left(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right) \subset \mathbb{R}$. Zeige, dass $L/\mathbb{Q}$ galoissch ist.

   (*c) Bestimme $[L/\mathbb{Q}]$.

   (*d) Bestimme $\mathrm{Gal}(L/\mathbb{Q})$ bis auf Isomorphie.

Lösung: (a) Als Zerfällungskörper des Polynoms $(X^2-2)(X^2-3)$ ist $K/\mathbb{Q}$ normal. Wegen $\mathrm{char}(K) = 0$ ist die Erweiterung ausserdem separabel; folglich ist sie galoissch.

Wir wissen bereits, dass $[\mathbb{Q}(\sqrt{2})/\mathbb{Q}] = 2$ gilt. Weiter behaupten wir $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Daraus folgt dann mit Aufgabe 1 von Serie 10

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})(\sqrt{3})/\mathbb{Q}(\sqrt{2})] = 2,$$

und mit der Multiplikativität der Körpergrade daher

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2})/\mathbb{Q}] = 2 \cdot 2 = 4.$$

Für die Behauptung $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ nehmen wir an, es sei $\sqrt{3} = \alpha + \beta\sqrt{2}$ mit $\alpha, \beta \in \mathbb{Q}$. Wegen $\sqrt{3} \notin \mathbb{Q}$ gilt $\beta \neq 0$. Wir quadrieren und erhalten $3 = \alpha^2 + 2\beta\sqrt{2} + \beta^2 2$, was ein Widerspruch ist zu $\sqrt{2} \notin \mathbb{Q}$.

Also ist $\Gamma := \mathrm{Gal}(K/\mathbb{Q})$ eine Gruppe der Ordnung 4. Diese operiert treu auf der Menge der Nullstellen $\{\pm\sqrt{2}, \pm\sqrt{3}\}$. Dabei kann $\pm\sqrt{2}$ nur auf eine Nullstelle von dessen Minimalpolynom $X^2 - 2$ abgebildet werden, also nur auf $\pm\sqrt{2}$. Genauso kann auch $\pm\sqrt{3}$ nur auf $\pm\sqrt{3}$ abgebildet werden. Die Gruppe der Permutationen von $\{\pm\sqrt{2}, \pm\sqrt{3}\}$ mit diesen Eigenschaften ist aber isomorph zu $S_2 \times S_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) Jeder Homomorphismus $\varphi\colon L \to \mathbb{C}$ entsteht, indem wir zuerst einen Homomorphismus $K \to \mathbb{C}$ betrachten und diesen auf L fortsetzen durch eine geeignete Wahl einer Quadratwurzel aus $\varphi((2+\sqrt{2})(3+\sqrt{3}))$. Da $K/\mathbb{Q}$ normal ist, gilt schon $\varphi(K) = K$ und $\varphi|_K \in \mathrm{Gal}(K/\mathbb{Q})$. Die Möglichkeiten für $\varphi((2+\sqrt{2})(3+\sqrt{3}))$ sind also nach (a) genau die vier reellen Zahlen $(2 \pm \sqrt{2})(3 \pm \sqrt{3})$. Diese sind positiv und besitzen daher die positiven reellen Quadratwurzeln

$$\begin{aligned}
x_1 &:= \sqrt{(2+\sqrt{2})(3+\sqrt{3})},\\
x_2 &:= \sqrt{(2-\sqrt{2})(3+\sqrt{3})},\\
x_3 &:= \sqrt{(2+\sqrt{2})(3-\sqrt{3})},\\
x_4 &:= \sqrt{(2-\sqrt{2})(3-\sqrt{3})}.
\end{aligned}$$

Dann ist $\varphi(x_1) = \varepsilon x_i$ für ein $\varepsilon \in \{\pm 1\}$ und $1 \leqslant i \leqslant 4$. Direkte Rechnung zeigt nun

$$(*)\qquad \begin{array}{rclclcl}
x_1x_2 & := & \sqrt{(2^2-2)(3+\sqrt{3})^2} & = & \sqrt{2}\cdot(3+\sqrt{3}) & \in & K^\times,\\
x_1x_3 & := & \sqrt{(2+\sqrt{2})^2(3^2-3)} & = & (2+\sqrt{2})\cdot\sqrt{2}\cdot\sqrt{3} & \in & K^\times,\\
x_1x_4 & := & \sqrt{(2^2-2)(3^2-3)} & = & 2\cdot\sqrt{3} & \in & K^\times.
\end{array}$$

In jedem Fall gilt also $\varphi(L) = \varphi(K(x_1)) = \varphi(K)(\varphi(x_1)) = K(\varepsilon x_i) = K(x_1) = L$. Da dies für jedes φ gilt, ist somit L/K normal, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ dann auch galoissch.

(c) Betrachte die Automorphismen $\sigma,\ \tau \in \mathrm{Gal}(K/\mathbb{Q})$ mit $\sigma(\sqrt{2}) = -\sqrt{2}$ und $\sigma(\sqrt{3}) = \sqrt{3}$ beziehungsweise $\tau(\sqrt{2}) = \sqrt{2}$ und $\tau(\sqrt{3}) = -\sqrt{3}$.

Nehmen wir an, es sei $L = K$. Dann sind insbesondere $x_1, x_2 \in K$, und nach Konstruktion von x_1 und x_2 gilt $\sigma(x_1)^2 = \sigma(x_1^2) = x_2^2$ und folglich $\sigma(x_1) = \varepsilon x_2$ für ein gewisses $\varepsilon \in \{\pm 1\}$. Setze $y := x_1 \cdot \sigma(x_1)$. Da σ die Ordnung 2 hat, gilt $\sigma(y) = \sigma(x_1)\cdot\sigma^2(x_1) = y$; deshalb liegt y im Fixkörper der Untergruppe $\langle\sigma\rangle < \Gamma$, das heisst in $\mathbb{Q}(\sqrt{3})$. Nach der obigen Rechnung $(*)$ ist andererseits $y = \varepsilon x_1 x_2 = \pm\sqrt{2}\cdot(3+\sqrt{3})$. Somit ist auch $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. Dies widerspricht aber der bereits etablierten Tatsache, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \neq \mathbb{Q}(\sqrt{3})$ ist. Daher ist $L \neq K$.

Wegen $L = K(x_1)$ mit $x_1^2 \in K$ ist $[L/K] = 2$. Daraus folgt schliesslich $[L/\mathbb{Q}] = [L/K]\cdot[K/\mathbb{Q}] = 2 \cdot 4 = 8$.

(d) Setze $\tilde{\Gamma} := \mathrm{Gal}(L/\mathbb{Q})$. Dann ist $\mathrm{Gal}(L/K) < \tilde{\Gamma}$ eine Untergruppe der Ordnung 2; sei ρ ihr nichttriviales Element. Wegen $L = K(x_i)$ mit $x_i^2 \in K$ gilt dann $\rho(x_i) = -x_i$ für jedes $1 \leqslant i \leqslant 4$. Da $K/\mathbb{Q}$ selbst galoissch ist, folgt aus Teil (e) des Hauptsatzes der Galoistheorie, dass die Untergruppe $\langle\rho\rangle$ normal in $\tilde{\Gamma}$ und die Faktorgruppe natürlich isomorph zu Γ ist.

Insbesondere existieren Elemente $\tilde{\sigma},\ \tilde{\tau} \in \tilde{\Gamma}$ mit $\tilde{\sigma}|_K = \sigma$ und $\tilde{\tau}|_K = \tau$. Nach Konstruktion von x_1 und x_2 gilt dann $\tilde{\sigma}(x_1)^2 = \tilde{\sigma}(x_1^2) = \sigma(x_1^2) = x_2^2$ und folglich $\tilde{\sigma}(x_1) = \pm x_2$. Nach etwaigem Ersetzen von $\tilde{\sigma}$ durch $\rho\tilde{\sigma}$ können wir also $\tilde{\sigma}(x_1) = x_2$ annehmen. Analog gilt $\tilde{\tau}(x_3) = \pm x_4$, und nach etwaigem Ersetzen von $\tilde{\tau}$ durch $\rho\tilde{\tau}$ können wir $\tilde{\tau}(x_3) = x_4$ annehmen. Damit haben wir aber unsere Wahlmöglichkeiten erschöpft und müssen nun berechnen, wie $\tilde{\sigma}$ und $\tilde{\tau}$ miteinander interagieren.

Die Werte $\tilde\sigma(x_i)$ für die übrigen i bestimmen wir mittels der Rechnung $(*)$ und der analogen Rechnung

$$(**)\qquad \begin{array}{rcl} x_2x_3 &:=& \sqrt{(2^2-2)(3^2-3)} &=& 2\cdot\sqrt{3} &\in& K^\times, \\ x_2x_4 &:=& \sqrt{(2-\sqrt{2})^2(3^2-3)} &=& (2-\sqrt{2})\cdot\sqrt{2}\cdot\sqrt{3} &\in& K^\times, \\ x_3x_4 &:=& \sqrt{(2^2-2)(3-\sqrt{3})^2} &=& \sqrt{2}\cdot(3-\sqrt{3}) &\in& K^\times. \end{array}$$

Unter Benutzung der bereits bekannten Operation von $\tilde\sigma$ auf K erhalten wir

$$\begin{array}{rclclclcl} \tilde\sigma(x_1)\tilde\sigma(x_2) &=& \tilde\sigma(x_1x_2) &=& \tilde\sigma\big(\sqrt{2}\cdot(3+\sqrt{3})\big) &=& -\sqrt{2}\cdot(3+\sqrt{3}) &=& -x_1x_2, \\ \tilde\sigma(x_1)\tilde\sigma(x_3) &=& \tilde\sigma(x_1x_3) &=& \tilde\sigma\big((2+\sqrt{2})\cdot\sqrt{2}\cdot\sqrt{3})\big) &=& -(2-\sqrt{2})\cdot\sqrt{2}\cdot\sqrt{3} &=& -x_2x_4, \\ \tilde\sigma(x_1)\tilde\sigma(x_4) &=& \tilde\sigma(x_1x_4) &=& \tilde\sigma\big(2\cdot\sqrt{3}\big) &=& 2\cdot\sqrt{3} &=& +x_2x_3, \end{array}$$

was wegen $\tilde\sigma(x_1)=x_2$ die Werte $\tilde\sigma(x_2)=-x_1$ und $\tilde\sigma(x_3)=-x_4$ und $\tilde\sigma(x_4)=+x_3$ impliziert. Die entsprechende Rechnung liefert uns die Werte $\tilde\tau(x_2)=+x_4$ und $\tilde\tau(x_3)=-x_1$ und $\tilde\tau(x_4)=-x_2$. Insgesamt erhalten wir so die Werte

	σ	$\tilde\sigma$	$\tilde\tau$	$\tilde\sigma^2$	$\tilde\tau^2$	$\tilde\sigma\tilde\tau$	$(\tilde\sigma\tilde\tau)^2$
x_1	$-x_1$	$+x_2$	$+x_3$	$-x_1$	$-x_1$	$-x_4$	$-x_1$
x_2	$-x_2$	$-x_1$	$+x_4$	$-x_2$	$-x_2$	$+x_3$	$-x_2$
x_3	$-x_3$	$-x_4$	$-x_1$	$-x_3$	$-x_3$	$-x_2$	$-x_3$
x_4	$-x_4$	$+x_3$	$-x_2$	$-x_4$	$-x_4$	$+x_1$	$-x_4$

Diese Tabelle impliziert $\tilde\sigma^2=\tilde\tau^2=(\tilde\sigma\tilde\tau)^2=\rho$; insbesondere haben $\tilde\sigma$ und $\tilde\tau$ und $\tilde\sigma\tilde\tau$ alle die Ordnung 4. Weiter gilt $\tilde\sigma\tilde\tau(x_1)=-x_4=-\tilde\tau\tilde\sigma(x_1)$. Somit ist die Gruppe Γ nichtabelsch. Da sie mit $\tilde\sigma^{\pm1}$ und $\tilde\tau^{\pm1}$ und $(\tilde\sigma\tilde\tau)^{\pm1}$ schon 6 verschiedene Elemente der Ordnung 4 besitzt, und selbst die Ordnung 8 hat, kann sie nur eine Quaternionengruppe sein.

2. Betrachte einen Körper der Form $K=\mathbb{C}(t,u)$ mit t, u algebraisch unabhängig über $\mathbb{C}$. Betrachte die Körpererweiterung $L=K(\alpha,\beta)$, wobei α eine Nullstelle des Polynoms X^n-t und β eine Nullstelle von X^m-u ist. Finde ein primitives Element von L/K.

   Lösung: Die Polynome $f(X):=X^n-t$ und $g(X):=X^m-u$ sind irreduzibel in $\mathbb{C}[t,u,X]$, da sie bis auf das Vorzeichen normiert vom Grad 1 in t beziehungsweise u sind. Somit sind sie auch irreduzibel in $K[X]$. Da sie ausserdem normiert in X sind mit $f(\alpha)=g(\beta)=0$, sind sie die Minimalpolynome von α beziehungsweise β über K. Seien ζ_n, $\zeta_m\in\mathbb{C}$, eine primitive n-te, bzw. m-te, Einheitswurzel. Dann sind $\alpha,\zeta_n\alpha,\ldots,\zeta_n^{n-1}\alpha\in L$ die Nullstellen von f und $\beta,\zeta_m\beta,\ldots,\zeta_m^{m-1}\beta\in L$ die Nullstellen von g. Die in dem Beweis des Satzes vom primitiven Element verwendete Teilmenge (vergleiche Aufgabe 1 von Serie 23) ist also

$$\left\{ \frac{(\zeta_n^j-1)\alpha}{(1-\zeta_m^k)\beta} \;\middle|\; j=0,\ldots,n-1;\ k=1,\ldots,m-1 \right\}.$$

Wegen $\alpha^n = t$ und $\beta^m = u$ ist nun aber $\left(\frac{\alpha}{\beta}\right)^{nm} = \frac{t^m}{u^n}$. Da dieses transzendent über K ist, ist auch $\frac{\alpha}{\beta}$ transzendent über K. Daher besteht die obige Menge nur aus 0 und gewissen über $\mathbb{C}$ transzendenten Elementen der Form $d\cdot\frac{\alpha}{\beta}$ mit $d \in \mathbb{C}^\times$, enthält also 1 nicht. Demnach ist $\alpha+\beta$ ein primitives Element von L.

Aliter: Die Erweiterung L/K ist ein Zerfällungskörper des Polynoms $f\cdot g$ und daher normal. Als Erweiterung von Körpern der Charakteristik Null ist sie daher galoissch. Nach Proposition 7.2.5 der Vorlesung entsprechen die Bahnen von $\mathrm{Gal}(L/K)$ auf den Nullstellen den irreduziblen Faktoren von $f\cdot g$. Die Operation bildet daher die Nullstellen von f bzw. von g auf ebensolche ab. Für jedes $\sigma \in \mathrm{Gal}(L/K)$ gilt also $\sigma(\alpha) = \zeta_n^i\alpha$ und $\sigma(\beta) = \zeta_m^j\beta$ für eindeutige $0 \leqslant i < n$ und $0 \leqslant j < m$.

Behauptung: Für nichttriviale $\sigma \in \mathrm{Gal}(L/K)$ ist $\sigma(\alpha+\beta) \neq \alpha+\beta$.

Beweis: Ist $\sigma(\alpha+\beta) = \alpha+\beta$, so folgt $\zeta_n^i\alpha + \zeta_m^j\beta = \alpha+\beta$ und damit $(1-\zeta_n^i)\alpha = (\zeta_m^j - 1)\beta$. Da σ nichttrivial ist, ist dabei $i > 0$ oder $j > 0$, und entsprechend $1-\zeta_n^i \neq 0$ oder $\zeta_m^j - 1 \neq 0$. Daraus folgt nun $\frac{\beta}{\alpha} \in \mathbb{C}$ oder $\frac{\alpha}{\beta} \in \mathbb{C}$. Beides widerspricht aber dem oben erklärten Umstand, dass $\frac{\alpha}{\beta}$ transzendent über $\mathbb{C}$ ist. □

Als Zwischenkörper einer Galoiserweiterung ist nun auch $L/K(\alpha+\beta)$ galoissch und ihre Galoisgruppe ist eine Untergruppe von $\mathrm{Gal}(L/K)$. Nach der Behauptung enthält diese Untergruppe aber kein nicht-triviales Element. Nach der Galoiskorrespondenz folgt also $L = K(\alpha+\beta)$, wie gewünscht.

*3. Zeige, dass alle Transzendenzbasen einer Körpererweiterung L/K dieselbe Kardinalität haben, auch wenn sie unendlich sind.

Lösungsskizze: Betrachte zwei Transzendenzbasen B, B'. Die Aussage ist bekannt, falls B oder B' endlich sind. Wir nehmen also an, dass B und B' unendlich sind. Jedes $b' \in B'$ ist algebraisch über $K(B)$. Da Polynome nur endlich viele Koeffizienten haben, können wir $n \geqslant 0$ und $b_1, \ldots, b_n \in B$ so wählen, dass b' schon algebraisch über $K(b_1, \ldots, b_n)$ ist. Mit dem Auswahlaxiom (!) können wir dies gleichzeitig für alle $b' \in B'$ tun und erhalten eine Funktion

$$t\colon B' \to \bigcup_{n\geqslant 0} B^n, \quad b' \mapsto (b_1, \ldots, b_n).$$

Dabei kann jedes Tupel $(b_1, \ldots, b_n)$ nur höchstens n mal als Bild $t(b')$ auftreten, weil $K(b_1, \ldots, b_n)/K$ den Transzendenzgrad n hat. Durch Numerieren der entsprechenden b' erhalten wir also eine Einbettung $B' \hookrightarrow \bigcup_{n\geqslant 0} n \times B^n$. Da B unendlich ist, gilt nun aber

$$|n \times B^n| \leqslant |B \times B^n| = |B|^{n+1} = |B|.$$

Die entsprechenden Einbettungen $n \times B^n \hookrightarrow B$ liefern also zusammen eine Einbettung $B' \hookrightarrow \omega \times B$. Daraus folgt

$$|B'| \leqslant |\omega \times B| = \omega \cdot |B| = |B|.$$

Analog zeigen wir $|B| \leqslant |B'|$ und folgern zusammen $|B| = |B'|$.

4. Zeige für jeden Körperturm $M/L/K$ die Formel

$$\operatorname{trdeg}(M/K) = \operatorname{trdeg}(M/L) + \operatorname{trdeg}(L/K).$$

Lösung: Sei S eine Transzendenzbasis von L/K, und T eine von M/L. Dann ist $S \subset L \smallsetminus K$ und $T \subset M \smallsetminus L$, also $S \cap T = \varnothing$ und daher $|S \cup T| = |S| + |T|$. Es genügt daher zu zeigen, dass $S \cup T$ eine Transzendenzbasis von M/K ist.

Nach der Wahl von S ist $L/K(S)$ eine algebraische Körpererweiterung. Da die Körpererweiterung $L(T) = L(S \cup T)/K(S \cup T)$ von den Elementen von L erzeugt wird, die algebraisch über $K(S \cup T)$ sind, ist auch dies eine algebraische Körpererweiterung. Nach der Wahl von T ist aber auch $M/L(T)$ eine algebraische Erweiterung. Also ist auch $M/K(S \cup T)$ eine algebraische Erweiterung.

Nun betrachte ein ein von 0 verschiedenes Polynom $f \in K[X_1, \ldots, X_k, Y_1, \ldots, Y_\ell]$ und paarweise verschiedene Elemente $s_1, \ldots, s_k \in S$ und $t_1, \ldots, t_\ell \in T$ mit der Eigenschaft $f(s_1, \ldots, s_k, t_1, \ldots, t_\ell) = 0$. Schreibe f als Polynom in $Y_1, \ldots, Y_\ell$ mit Koeffizienten in $K[X_1, \ldots, X_k]$. Dann ist mindestens einer dieser Koeffizienten ungleich Null. Da $s_1, \ldots, s_k$ bereits algebraisch unabhängig über K sind, bleibt dieser Koeffizient auch nach Einsetzen dieser Werte ungleich Null. Somit ist auch das Polynom

$$g(Y_1, \ldots, Y_\ell) := f(s_1, \ldots, s_k, Y_1, \ldots, Y_\ell) \in L[Y_1, \ldots, Y_\ell]$$

von 0 verschieden. Nach Konstruktion gilt nun aber $g(t_1, \ldots, t_\ell) = 0$. Also sind $t_1, \ldots, t_\ell$ algebraisch abhängig über L, im Widerspruch zur Annahme an T. Zusammen zeigt dies, dass die Menge $S \cup T$ algebraisch unabhängig über K ist.

5. Zeige: Eine Körpererweiterung L/K ist genau dann rein transzendent, wenn L isomorph über K zum Quotientenkörper eines Polynomrings über K ist.

Lösung: Wir zeigen zuerst, dass der Quotientenkörper eines beliebigen Polynomrings rein transzendent ist. Sei also $K((X_\nu)_{\nu \in N})$ ein solcher Quotientenkörper. Wir müssen zeigen, dass kein nichtverschwindendes Polynom $f \in K[(X_\nu)_{\nu \in N}]$ existiert mit $f((X_\nu)_{\nu \in N}) = 0$. Das gilt offensichtlich nach Definition.

Sei nun $L = K((a_\nu)_{\nu \in N})$ eine rein transzendente Körpererweiterung mit Transzendenzbasis $\{a_\nu : \nu \in N\}$. Betrachte die Auswertungsabbildung

$$\operatorname{eval}\colon K[(X_\nu)_{\nu \in N}] \to K[(a_\nu)_{\nu \in N}] : f \mapsto f((a_\nu)_{\nu \in N}).$$

Sie ist offensichtlich ein surjektiver Ringhomomorphismus, der auf K die Identität ist. Wir zeigen Injektivität und betrachten dazu ein $f \in \operatorname{Ker}(\operatorname{eval})$, das heisst

$f((a_\nu)_{\nu\in N}) = 0$. Da $\{a_\nu : \nu \in N\}$ algebraisch unabhängig ist, folgt, dass f das Nullpolynom ist und somit ist die Auswertungsabbildung injektiv. Folglich lässt sich eval zu einem surjektiven Körperhomorphismus, also einem Körperisomorphismus, der Quotientenkörper $K((X_\nu)_{\nu\in N}) \to K((a_\nu)_{\nu\in N})$ fortsetzen, der auf K die Identität ist.

*6. Zeige: Der *elliptische Funktionenkörper* $\mathbb{C}(x,y)$ für über $\mathbb{C}$ transzendente Elemente x und y mit $y^2 = x^3 - x$ ist nicht rein transzendent über $\mathbb{C}$.

Hinweis: Ist $\mathbb{C}(x,y) = \mathbb{C}(t)$, so schreibe $x = f/g$ mit teilerfremden Polynomen $f, g \in \mathbb{C}[t]$. Zeige dann, dass $f, g, f \pm g$ paarweise teilerfremde Quadrate in $\mathbb{C}[t]$ sind und folglich $x = s^2$ für ein über $\mathbb{C}$ transzendentes Element $s \in \mathbb{C}(t)$. Folgere aus $[\mathbb{C}(x,y)/\mathbb{C}(x)] = 2$, dass $\mathbb{C}(t) = \mathbb{C}(s)$ sein muss. Eine direkte Rechnung in dem Polynomring $\mathbb{C}[s]$ liefert jetzt schnell einen Widerspruch.

Lösung: Da x transzendent über $\mathbb{C}$ und y algebraisch über $\mathbb{C}(x)$ ist, hat die Erweiterung $\mathbb{C}(x,y)/\mathbb{C}$ den Transzendenzgrad 1. Wenn sie rein transzendent ist, muss sie also gleich $\mathbb{C}(t)$ sein für ein über $\mathbb{C}$ transzendentes Element t. Mit diesem können wir rechnen wie mit einer Variablen, und dann werden x und y rationale Funktionen in t.

Schreibe also $x = f/g$ mit teilerfremden Polynomen $f, g \in \mathbb{C}[t] \setminus \{0\}$. Dann ist

$$g^4 \cdot y^2 \;=\; g^4 \cdot (x^3 - x) \;=\; g^4 \cdot \left(\tfrac{f^3}{g^3} - \tfrac{f}{g}\right) \;=\; f^3 g - f g^3 \;=\; f \cdot g \cdot (f+g) \cdot (f-g).$$

Da f und g teilerfremd sind, sind auch alle Faktoren auf der rechten Seite paarweise teilerfremd. Da die rechte Seite ein Polynom in t ist, gilt das auch für die linke Seite. Diese ist aber ein Quadrat in $\mathbb{C}(t)$ und somit auch ein Quadrat in $\mathbb{C}[t]$. Aufgrund der Teilerfremdheit ist daher jeder Faktor auf der rechten Seite ein Quadrat. Insbesondere ist $x = f/g = s^2$ für ein $s \in \mathbb{C}(t)$.

Da nun x transzendent über $\mathbb{C}$ ist, gilt dies auch für s. Daher ist $[\mathbb{C}(s)/\mathbb{C}(x)] = [\mathbb{C}(s)/\mathbb{C}(s^2)] = 2$. Andererseits haben wir schon $[\mathbb{C}(x,y)/\mathbb{C}(x)] = 2$. Wegen $\mathbb{C}(x) \subset \mathbb{C}(s) \subset \mathbb{C}(t) = \mathbb{C}(x,y)$ und der Multiplikativität der Körpergrade muss daher $[\mathbb{C}(t)/\mathbb{C}(s)] = 1$ und somit $\mathbb{C}(t) = \mathbb{C}(s)$ sein.

Wir können deshalb t vergessen und x und y als rationale Funktionen in der Variablen s auffassen. Wegen $x = s^2$ ist dann

$$y^2 \;=\; x^3 - x \;=\; s^6 - s^2 \;=\; s^2 \cdot (s^4 - 1).$$

Hier hat die rechte Seite aber eine einfache Nullstelle bei $s = 1$ und ist folglich kein Quadrat in $\mathbb{C}(s)$. Damit haben wir einen Widerspruch, und die gewünschte Aussage ist gezeigt.

7. Schreibe die folgenden Ausdrücke in Termen der elementarsymmetrischen Polynome in $X_1, \ldots, X_n$:

(a) $\sum_{i \neq j} X_i^3 X_j$.

(b) $\sum_i X_i^4$.

(c) $\sum_{i \neq j \neq k \neq i} X_i^2 X_j^2 X_k^2$.

(d) $\sum_{i \neq j} X_i / X_j$.

Lösung: (a) $\sum_{i \neq j} X_i^3 X_j = S_1^2 S_2 - S_1 S_3 - 2S_2^2 + 4S_4$.

(b) $\sum_i X_i^4 = S_1^4 - 4S_1^2 S_2 + 2S_2^2 + 4S_1 S_3 - 4S_4$.

(c) $\sum_{i \neq j \neq k \neq i} X_i^2 X_j^2 X_k^2 = 6(S_3^2 + 2S_1 S_5 - 2S_2 S_4 - 2S_6)$.

(d) $\sum_{i \neq j} X_i / X_j = \frac{S_1 S_{n-1}}{S_n} - n$.