Die folgenden Lösungsansätze stellen weder den Anspruch auf Vollständigkeit, noch auf formale Korrektheit und sollen lediglich dem Lesenden eine Idee geben, wie er oder sie an die Aufgabe hätte herangehen können.

Zur Formalisierung von $\overline{\mathbb{F}_p} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$

Es sei $\mathcal{F}$ eine Menge von Körpern und $\leq$ eine partielle Ordnung auf $\mathcal{F}$, sodass für alle $F_1, F_2 \in \mathcal{F}$ ein $F_3 \in \mathcal{F}$ existiert mit $F_1 \leq F_3$ und $F_2 \leq F_3$. Zudem sei für alle $E, F \in \mathcal{F}$ mit $E \leq F$ ein Körperhomomorphismus $\varphi_{E,F} : E \to F$ gegeben, sodass $\varphi_{E,E} = \mathrm{id}_E$ und $\varphi_{L,F} = \varphi_{E,F} \circ \varphi_{L,E}$ für alle $L, F, E \in \mathcal{F}$ mit $L \leq E \leq F$ gelte.

Wir betrachten auf der Vereinigung $V(\mathcal{F}) = \bigcup_{L\in\mathcal{F}} \{L\} \times L$ die Äquivalenzrelation $\sim$, für die $(E, a) \sim (F, b)$ genau dann gilt, wenn es ein $(L, c) \in V(\mathcal{F})$ gibt mit $E \leq L$ und $F \leq L$ sowie $\varphi_{E,L}(a) = c = \varphi_{F,L}(b)$. Die Äquivalenzklasse von (E, a) bezeichnen wir mit $[E, a]$ und mit $K(\mathcal{F}) = V(\mathcal{F})/\sim$ die Menge der Äquivalenzklassen.

Auf $K(\mathcal{F})$ definieren wir nun

$$[E, a] + [F, b] = [L, c]$$

genau dann wenn ein $(L', c') \in [F, c]$ existiert mit $E \leq L'$ und $F \leq L'$ und $c' = \varphi_{E,L'}(a) + \varphi_{F,L'}(b)$.

Analog schreiben wir

$$[E, a] \cdot [F, b] = [L, c]$$

genau dann wenn ein $(L', c') \in [F, c]$ existiert mit $E \leq L'$ und $F \leq L'$ und $c' = \varphi_{E,L'}(a)\varphi_{F,L'}(b)$.

Zeigen Sie:

1. Die Relation $\sim$ ist tatsächlich eine Äquivalenzrelation.

2. Die soeben definierte Addition und Multiplikation $+, \cdot : K \times K \to K$ sind wohldefinierte Abbildungen.

3. Zusammen mit $+$ und $\cdot$ wird K zu einem Körper.

4. Für jedes $F \in \mathcal{F}$ ist $\varphi_F : F \to K, a \mapsto [F, a]$ ein Körperhomomorphismus.

5. Es ist $\varphi_F = \varphi_E \circ \varphi_{F,E}$ für alle $E, F \in \mathcal{F}$ mit $F \leq E$ und es gilt $K(\mathcal{F}) = \bigcup_{F\in\mathcal{F}} \mathrm{Bild}(\varphi_F)$.

6. Definiert man $\mathbb{F}_{p^n} \leq \mathbb{F}_{p^m}$ genau dann, wenn m ein Vielfaches von n ist, so definiert $\leq$ auf $\mathcal{F}_p := \{\mathbb{F}_{p^n} \mid n \in \mathbb{N}\}$ eine partielle Ordnung wie oben und es gibt Körperhomomorphismen $\varphi_{\mathbb{F}_{p^n},\mathbb{F}_{p^m}}$, die bezüglich $\leq$ die obigen Voraussetzungen erfüllen. Es gilt $\overline{\mathbb{F}_p} \cong K(\mathcal{F}_p)$.

Lösungsansatz

1. Die Relation $\sim$ ist reflexiv, denn für $(E, a) \in V(\mathcal{F})$ ist $E \leq E$ und $a = \varphi_{E,E}(a)$. Die Relation ist per Definition symmetrisch. Sie ist zudem transitiv, denn falls $(E, a) \sim (F, b)$ und $(F, b) \sim (L, c)$ gilt, so existiert ein $(E', a') \in V(\mathcal{F})$ mit $E \leq E'$ und $F \leq E'$ sowie $\varphi_{E,E'}(a) = a' = \varphi_{F,E'}(b)$ und ein $(L', c') \in V(\mathcal{F})$ mit $E \leq L'$ und $F \leq L'$ sowie $\varphi_{F,L'}(b) = c' = \varphi_{L,L'}(c)$. Ist nun $F' \in \mathcal{F}$ mit $E', L' \leq F'$ so gilt

$$\begin{aligned}\varphi_{E,F'}(a) &= \varphi_{E',F'}(\varphi_{E,E'}(a)) \\ &= \varphi_{E',F'}(\varphi_{F,E'}(b)) \\ &= \varphi_{F,F'}(b) \\ &= \varphi_{L',F'}(\varphi_{F,L'}(b)) \\ &= \varphi_{L',F'}(\varphi_{L,L'}(c)) \\ &= \varphi_{L,F'}(c)\end{aligned}$$

   und damit gilt $(E, a) \sim (L, c)$.

2. Es seien $(E, a) \sim (E', a')$ und $(F, b) \sim (F', b')$ und $(L, c) \in V(\mathcal{F})$ mit $E, F \leq L$ und $c = \varphi_{E,L}(a)_{F,L}(b)$ sowie $(L', c) \in V(\mathcal{F})$ mit $E', F' \leq L'$ und $c' = \varphi_{E',L'}(a')_{F',L'}(b')$ Es gibt ein $F'' \in \mathcal{F}$ mit $E, E', F, F', L, L' \leq F'$ und $\varphi_{E,F''}(a) = \varphi_{E',F''}(a')$ sowie $\varphi_{F,F''}(b) = \varphi_{E',F''}(b')$.

   Dann ist für $\square \in \{\cdot, +\}$

$$\begin{aligned}\varphi_{L,F''}(c) &= \varphi_{E,F''}(a) \square \varphi_{F,F''}(b) \\ &= \varphi_{E,F''}(a') \square \varphi_{F,F''}(b') \\ &= \varphi_{L',F''}(c')\end{aligned}$$

   und damit $(L, c) \sim (L', c')$.

3. Es seien $[E, a], [F, b], [L, c] \in K(\mathcal{F})$. Durch Wahl geeigneter Vertreter können wir $E = F = L$ annehmen. Dann gilt mit $\square \in \{+, \cdot\}$ sowohl

   $$([E, a] \square [F, b]) \square [L, c] = [E, (a \square b) \square c] = [E, a \square (b \square c)] = [E, a] \square ([F, b] \square [L, c])$$

   als auch

   $$[E, a] \square [F, b] = [E, a \square b] = [E, b \square a] = [F, b] \square [E, a]$$

   und

   $$([E, a] + [F, b]) \cdot [L, c] = [E, (a+b) \cdot c] = [E, ac + bc] = ([E, a] \cdot [L, c]) + ([F, b] \cdot [L, c])$$

sowie

$$[E,a]+[F,0]=[E,a]=[F,0]+[E,a]$$

und

$$[E,a]\cdot[F,1]=[E,a]=[F,1]\cdot[E,a].$$

Man beachte dabei, dass $(E,a)\sim(E',a)$ für $a\in\{0,1\}$ und alle $E,E'\in\mathcal{F}$ gilt. Ist zudem $(E,a)\sim(F,0)$, so ist $a=0$ und ist $(E,a)\sim(F,1)$, so ist $a=1$. Ist nun $[E,a]\in K(\mathcal{F})$, dann ist $[E,a]+[E,-a]=[E,0]$ und falls $[E,a]\neq[E,0]$ ist, so ist $[E,a^{-1}]\cdot[E,a]=[E,1]$.

Folglich ist $K(\mathcal{F})$ ein Körper.

4. Es ist $[F,a]+[F,b]=[F,a+b]$ und $[F,a][F,b]=[F,ab]$ für alle $a,b\in F$. Zudem ist $[F,1]\neq[F,0]$, also $\varphi_F:F\to K(\mathcal{F})$ ein Körperhomomorphismus.

5. Es sei $E\leq F$ und $a\in E$. Dann ist $\varphi_E(a)=[E,a]=[F,\varphi_{E,F}(a)]=\varphi_F\circ\varphi_{E,f}(a)$ und da a beliebig ist, ist $\varphi_E=\varphi_F\circ\varphi_{E,F}$.

   Es ist

$$\bigcup_{F\in\mathcal{F}}\mathrm{Bild}(\varphi_F)=\bigcup_{F\in\mathcal{F}}\{[F,a]\mid a\in F\}=K(\mathcal{F})$$

6. Für jedes $n\in\mathbb{N}$ und jede Primzahl r wählen wir einen Körperautomorphismus

$$\varphi_{n,rn}:\mathbb{F}_{p^n}\to\mathbb{F}_{p^{rn}}.$$

   Ist nun $m\in\mathbb{N}$ ein Vielfaches von n so ist $m/n=\prod_{i=1}^{l}r_i$ für Primzahlen $r_1\geq r_2\geq\cdots\geq r_n$.

   Wir definieren dann

$$\varphi_{n,m}=\varphi_{m,n\prod_{i=1}^{l-1}r_i}\circ\cdots\circ\varphi_{r_1n,n}$$

   Dann ist per Definition $\varphi_{n,m}=\varphi_{s,m}\varphi_{n,s}$ für alle $n\mid s\mid m$. Folglich sind die Voraussetzungen erfüllt. Der Körper $K(\mathcal{F}_p)$ enthält damit für jedes $n\in\mathbb{N}$ einen Teilkörper isomorph zu $\mathbb{F}_{p^n}$, nämlich das Bild von $\mathbb{F}_{p^n}$ unter dem Körperhomomorphismus $\varphi_{\mathbb{F}_{p^n}}:\mathbb{F}_{p^n}\to K(\mathcal{F}_p)$ und es gilt $K(\mathcal{F}_p)=\bigcup_n\mathrm{Bild}(\varphi_{\mathbb{F}_{p^n}})$.

   Insbesondere ist $K(\mathcal{F}_p)/\mathrm{Bild}(\varphi_{\mathbb{F}_p})$ algebraisch, da jedes Element in $K(\mathcal{F}_p)$ bereits in einem $\mathrm{Bild}(\varphi_{\mathbb{F}_{p^n}})$ liegt und $\mathbb{F}_{p^n}/\mathbb{F}_p$ algebraisch ist. Ist nun $f\in\mathbb{F}_p[X]$, so existiert ein $n\in\mathbb{N}$, sodass f in $\mathbb{F}_{p^n}[X]$ in Linearfaktoren zerfällt. Folglich zerfällt auch f in $K(\mathcal{F}_p)[X]$ in Linearfaktoren. Mit einer alten Übungsaufgabe folgt $K(\mathcal{F}_p)\cong\overline{\mathbb{F}_p}$.

Elementarsymmetrische Polynome und rationale Funktionenkörper
Es sei K ein Körper.

1. Für $n \in \mathbb{N}$ und $1 \leq k \leq n$ bezeichne

$$\sigma_{n,k} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k} \in K[X_1, X_2, \ldots, X_n]$$

das $k$te *elementarsymmetrische Polynom* in n Variablen.

Zeigen Sie:

a) Es gilt $\sigma_{n+1,n+1} = X_{n+1}\sigma_{n,n}$, $\sigma_{n+1,1} = X_{n+1} + \sigma_{n,1}$ und $\sigma_{n+1,k} = \sigma_{n,k} + X_{n+1}\sigma_{n,k-1}$ für alle $n \in \mathbb{N}$ und $1 < k \leq n$.

b) In $K[X_1, X_2, \ldots, X_n][T]$ ist $\prod_{i=1}^{n}(T + X_i) = T^n + \sum_{k=1}^{n} \sigma_{n,k} T^{n-k}$.

c) Die symmetrische Gruppe S_n operiert auf $K(X_1, X_2, \ldots, X_n)$ durch Automorphismen via

$$X_i^\sigma = X_{i^\sigma}$$

für alle $1 \leq i \leq n$ und es gilt

$$K(X_1, X_2, \ldots, X_n)^{S_n} = K(\sigma_{n,1}, \sigma_{n,2}, \ldots, \sigma_{n,n}).$$

2. Es sei $E = K(X_n | n \in \mathbb{N})$ der Körper der rationalen Funktionen in abzählbar vielen Variablen über einem Körper K. Zeigen Sie, dass

$$G = \{\sigma \in \mathrm{Aut}_K(E) \mid |\{n \in \mathbb{N} \mid \sigma(X_n) \neq X_n\}| < \infty\}$$

eine echte Untegruppe von $\mathrm{Aut}_K(E)$ ist und $E^G = K$ gilt.

Lösungsansatz

1. Es ist

$$\sigma_{n+1,n+1} = \prod_{i=1}^{n+1} X_i = X_{n+1} \prod_{i=1}^{n} X_i = X_{n+1}\sigma_{n,n}$$

und

$$\sigma_{n+1,1} = \sum_{i=1}^{n+1} X_i = X_{n+1} + \sum_{i=1}^{n} X_i = X_{n+1} + \sigma_{n,1}$$

für alle $n \geq 1$.

Es ist

$$\begin{aligned}\sigma_{n+1,k} &= \sum_{1\le i_1<i_2<\cdots<i_k\le n+1} X_{i_1}X_{i_2}\cdots X_{i_k}\\ &= \sum_{1\le i_1<i_2<\cdots<i_k\le n} X_{i_1}X_{i_2}\cdots X_{i_k}\\ &\quad + \sum_{1\le i_1<i_2<\cdots<i_{k-1}<n+1} X_{i_1}X_{i_2}\cdots X_{i_{k-1}}X_{n+1}\\ &= \sigma_{n,k} + X_{n+1}\sigma_{n,k-1}\end{aligned}$$

für alle $1 < k \le n$.

Es ist

$$\prod_{i=1}^{n}(T+X_i) = T^n + \sum_{k=1}^{n}\sigma_{n,k}T^{n-k}$$

für $n = 1$. Ist

$$\prod_{i=1}^{n}(T+X_i) = T^n + \sum_{k=1}^{n}\sigma_{n,k}T^{n-k}$$

für ein $n \in \mathbb{N}$ dann ist

$$\begin{aligned}\prod_{i=1}^{n+1}(T+X_i) &= (T+X_{n+1})(T^n + \sum_{k=1}^{n}\sigma_{n,k}T^{n-k})\\ &= T^{n+1} + X_{n+1}\sigma_{n,n} + \sum_{k=1}^{n}(\sigma_{n,k} + X_{n+1}\sigma_{n,k-1})T^{n+1-k}\\ &= T^{n+1} + \sum_{k=1}^{n+1}\sigma_{n+1,k}T^{n+1-k}\end{aligned}$$

und per Induktion folgt die Behauptung.

Es ist $E = K(X_1, X_2, \ldots, X_n)$ der Zerfällungskörper des separablen Polynoms $\prod_{i=1}^{n}(T-X_i) = T^n + \sum_{k=1}^{n}(-1)^k\sigma_{n,k}T^{n-k}$ über $L = K(\sigma_{n,1}, \sigma_{n,2}, \ldots, \sigma_{n,n})$ und damit insbesondere Galoisch.

Ist $\sigma \in S_n$ so gibt es einen eindeutigen K-Algebrenhomomorphismus

$$\varphi_\sigma : K[X_1, X_2, \ldots, X_n]$$

mit $\varphi_\sigma(X_i) = X_{i^{\sigma^{-1}}}$ für alle $1 \le i \le n$. Insbesondere ist $\varphi_{\mathrm{id}} = \mathrm{id}$.

Sind $\sigma, \tau \in S_n$ so ist

$$(\varphi_\sigma \circ \varphi_\tau)(X_i) = \varphi_\sigma(X_{i^{\tau^{-1}}}) = X_{(i^{\tau^{-1}})^{\sigma^{-1}}} = X_{i^{(\sigma\tau)^{-1}}} = (\varphi_{\sigma\tau})(X_i)$$

für alle $1 \leq i \leq n$ und damit

$$\varphi_\sigma \circ \varphi_\tau = \varphi_{\sigma\tau}.$$

Es folgt, dass φ_σ für jedes $\sigma \in S_n$ invertierbar ist. Entsprechend lässt sich φ_σ auf $E = \mathrm{Quot}(K(X_1, X_2, \ldots, X_n))$ fortsetzen, definiert einen Automorphismus $\varphi_\sigma : E \to E$ und es gilt

$$\varphi_\sigma \circ \varphi_\tau = \varphi_{\sigma\tau}$$

und

$$\varphi_{\mathrm{id}} = \mathrm{id}$$

für diese Fortsetzungen.

Es gilt $\varphi_\sigma(\sigma_{n,k}) = \sigma_{n,k}$ für alle $1 \leq k \leq n$ und $\varphi_\sigma = \mathrm{id}$ genau dann, wenn $\sigma = \mathrm{id}$ gilt.

Entsprechend erhalten wir einen Monomorphismus

$$S_n \to \mathrm{Aut}_L(E), \sigma \mapsto \varphi_\sigma$$

Gleichzeitig operiert $\mathrm{Aut}_L(E)$ treu auf $\{X_1, \ldots, X_n\}$, den Nullstellen von $T^n + \sum_{k=1}^{n} (-1)^k \sigma_{n,k} T^{n-k}$, was einen Monomorphismus

$$\mathrm{Aut}_L(E) \to S_n$$

definiert. Ein Vergleich der Ordnungen erlaubt uns zu folgern, dass $\mathrm{Aut}_L(E) \cong S_n$ gilt. Nach dem Hauptsatz der Galoistheorie ist $L = \mathrm{Fix}_{S_n}(E)$.

2. Für jede Bijektion $\sigma : \mathbb{N} \to \mathbb{N}$ gibt es einen eindeutigen K-Algebrenhomomorphismus

$$\varphi_\sigma : K[X_n | n \in \mathbb{N}] \to K[X_n | n \in \mathbb{N}]$$

mit $\varphi_\sigma(X_n) = X_{\sigma(n)}$ für alle $n \in \mathbb{N}$. Es ist $\varphi_{\mathrm{id}} = \mathrm{id}$ und $\varphi_{\sigma\tau} = \varphi_\sigma \varphi_\tau$ für alle Bijektionen $\sigma, \tau : \mathbb{N} \to \mathbb{N}$ analog zum ersten Teil der Aufgabe.

Insbesondere ist φ_σ invertierbar mit $\varphi_\sigma^{-1} = \varphi_{\sigma^{-1}}$.

Entsprechend setzen diese Automorphismen fort zu Körperautomorphismen $E \to E$.

Ist $\sigma : \mathbb{N} \to \mathbb{N}$ derart, dass $\{i \mid \sigma(i) \neq i\}$ endlich ist, so ist $\varphi_\sigma \in G$.

Es sei nun $f \in E \backslash K$, dann gibt es ein minimales $N \in \mathbb{N}$ mit $f \in K(X_1, X_2, \ldots, X_N)$. Ist nun $\sigma : \mathbb{N} \to \mathbb{N}$ definiert durch $\sigma(n) = n$ für $n \neq N, N+1$ und $\sigma(N) = N+1$ und $\sigma(N+1) = N$. Dann ist $\sigma^2 = \mathrm{id}_N$, also σ eine Bijektion und $\varphi_\sigma(f) \notin K(X_1, X_2, \ldots, X_N)$.

folglich ist $f \notin E^G$. Es ist $K \subseteq E^G$ und damit $E^G = K$.