37. *Vandermonde-Determinante.* Sei $R$ ein faktorieller Ring, $X_1, \ldots, X_n$ Unbestimmte über $R$. Beweisen Sie ohne Induktion:

$$\det\begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_n \\ X_1^2 & X_2^2 & \ldots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \ldots & X_n^{n-1} \end{pmatrix} = \prod_{1\le i<j\le n} (X_j - X_i).$$

*Hinweis.* Polynom, Nullstellen, Grade, 1 einfacher Koeffizientenvergleich.

38. Sei $L$ eine algebraische Körpererweiterung von $K$ und $\alpha$, $\beta \in L$ zwei Elemente, deren Grade $n$ bzw. $m$ über $K$ teilerfremd seien. Man beweise: $[K(\alpha, \beta) : K] = mn$.

39. Sei $K$ ein Körper und $\alpha$ ein Element, das eine Körpererweiterung von $K$ von Grad 5 erzeugt. Man beweise, dass $\alpha^2$ dieselbe Erweiterung erzeugt.

40. Man zerlege $X^9 - X$ und $X^{27} - X$ über $\mathbb{F}_3$ in irreduzible Faktoren.

41. Bestimmen Sie ein Polynom $p(X) \in \mathbb{F}_2[X]$, sodass $\mathbb{F}_{32} \cong \mathbb{F}_2[X]/(p(X))$, und ein primitives Element dieses Körpers.

42. Sei $F/K$ eine Körpererweiterung und $f \in K[x]$, dann bildet ein $\psi \in \mathrm{Aut}_K(F)$ Wurzeln von $f$ wiederum auf Wurzeln ab. Dabei ist

$$\mathrm{Aut}_K(F) := \{\psi : F \to F \text{ Automorphismus mit } \psi|_K = \mathrm{id}_K\}.$$

43. Sei $K$ ein Körper, $k \in \mathbb{N}$, $\ell \in \mathbb{N}_0$. Zeigen Sie, dass $X^k - X$ das Polynom $X^{k^\ell} - X$ in $K[X]$ teilt.

44. Sei $K$ ein Körper, $n \in \mathbb{N}$ mit $\chi(K) \nmid n$, $E_n(K)$ die Menge der $n$-ten Einheitswurzeln. Das Polynom $X^n - 1$ zerfalle in $K[X]$ in Linearfaktoren. Zeigen Sie, dass dann

$$\sum_{\zeta\in E_n(K)} \zeta = \begin{cases} 1, & \text{wenn } n = 1, \\ 0, & \text{sonst} \end{cases}$$

gilt.

45. Zeigen Sie, dass $\overline{\mathbb{Q}} := \{z \in \mathbb{C} : z \text{ algebraisch über } \mathbb{Q}\}$ ein algebraisch abgeschlossener Körper ist. (Ein Körper $K$ heißt algebraisch abgeschlossen, wenn jedes über $K$ algebraische Element bereits ein Element von $K$ ist.)

46. Zeigen Sie: Wenn es modulo $m$ eine Primitivwurzel gibt, so gibt es $\varphi(\varphi(m))$ Primitivwurzeln modulo $m$.

47. Geben Sie eine explizite Formel für $\cos(2\pi/5)$ an.

48. Es sei $f \in \mathbb{Z}[X]$ normiert mit Nullstellen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, sodass $\alpha_1 > 1$ und $0 < |\alpha_2|, \ldots, |\alpha_n| < 1$. Dann ist $f$ irreduzibel über $\mathbb{Q}$. (In diesem Fall nennt man $\alpha_1$ eine *Pisot-Zahl.*)