D-MATH Algebra II FS 2016
Prof. Richard Pink

Musterlösung Wiederholungsserie

Körpertheorie

1. Seien K_1 und K_2 Zwischenkörper einer endlichen Körpererweiterung L/K. Zeige, dass K_1 und K_2 genau dann linear disjunkt sind über K, wenn die natürliche Abbildung $K_1 \otimes_K K_2 \to K_1K_2$ ein K-Vektorraumisomorphismus ist.

   Lösung: Als Zwischenerweiterungen einer endlichen Erweiterung sind auch K_1/K und K_2/K endlich. Seien $a_1, \dots, a_n$ bzw. $b_1, \dots, b_m$ Basen von K_1 bzw. K_2 über K. Dann ist $\{a_i \otimes b_j : 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$ eine K-Basis von $K_1 \otimes_K K_2$. Die Abbildung $K_1 \times K_2 \to K_1K_2$, $(x, y) \mapsto xy$ ist K-bilinear und induziert eine natürliche K-lineare Abbildung $\varphi\colon K_1 \otimes_K K_2 \to K_1K_2$. Diese schickt das Basiselement $a_i \otimes b_j$ auf a_ib_j. Nach §5.2 der Vorlesung wird K_1K_2 von der Menge $\{a_ib_j : 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$ als K-Vektorraum erzeugt, also ist φ surjektiv. Folglich ist φ ein Isomorphismus genau dann, wenn $K_1 \otimes_K K_2$ und K_1K_2 dieselbe Dimension über K haben. Das Tensorprodukt $K_1 \otimes_K K_2$ hat aber die Dimension $mn = [K_1/K] \cdot [K_2/K]$, und nach Definition hat das Kompositum K_1K_2 diese Dimension genau dann, wenn K_1 und K_2 linear disjunkt über K sind. Fertig.

2. Sei L/K eine endliche Körpererweiterung und $f \in K[X]$ irreduzibel.

   (a) Zeige: Falls $\deg(f)$ und $[L/K]$ teilerfremd sind, ist f irreduzibel über L.

   (b) Gib Beispiele von irreduziblen Polynomen in $K[X]$ an, deren Grad nicht teilerfremd zu $[L/K]$ ist und die über L reduzibel sind.

   Lösung: (a) Sei a eine Nullstelle von f in einem algebraischen Abschluss von L. Multiplikativität der Körpergrade ergibt

   $$[L(a)/K] = [L(a)/L] \cdot [L/K] = [L(a)/K(a)] \cdot [K(a)/K].$$

   Also gilt

   $$[L(a)/L] = \frac{[L(a)/K(a)] \cdot [K(a)/K]}{[L/K]} = \frac{[L(a)/K(a)] \deg(f)}{[L/K]}.$$

   Da $[L/K]$ und $\deg(f)$ teilerfremd sind, ist also $[L/K]$ ein Teiler von $[L(a)/K(a)]$. Andererseits gilt immer $[L(a)/K(a)] \leqslant [L/K]$, und deshalb hier Gleichheit. Insgesamt folgt $[L(a)/L] = \deg(m_{a,L}) = \deg(f)$; somit ist f irreduzibel über L.

   (b) Sei zum Beispiel $a \in L \smallsetminus K$ und nimm $f = m_{a,K}$.

3. Finde für folgende Werte von x ein annullierendes Polynom von x über $\mathbb{Q}$ und folgere daraus eine einfachere Darstellung von x.

   (a) $x = \sqrt{4+\sqrt{7}} + \sqrt{4-\sqrt{7}}$.

   (b) $x = \sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$.

   Lösung: (a) Wir rechnen mit der binomischen Formel

   $$x^2 \;=\; (4+\sqrt{7}) + 2\sqrt{16-7} + (4-\sqrt{7}) \;=\; 4 + 2\cdot 3 + 4 \;=\; 14.$$

   Wegen $4 \pm \sqrt{7} > 0$ ist auch $x > 0$; somit folgt $x = \sqrt{14}$.

   (b) Wir rechnen

   $$x^3 = 2 + \sqrt{5} + 3\sqrt[3]{4-5}\left(\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}\right) + 2 - \sqrt{5}$$
   $$0 = x^3 + 3x - 4.$$

   Also ist $X^3 + 3X - 4$ ein annullierendes Polynom für x. Dieses hat Nullstelle 1 und $X^3 + 3X - 4 = (X-1)(X^2 + X + 4)$. Die weiteren Nullstellen sind nicht reell, aber x schon; also gilt $x = 1$.

4. Seien K ein Körper, $L = K(\alpha)$ eine endliche einfache Erweiterung und $F \subset L$ eine Zwischenerweiterung. Seien weiter $f \in K[X]$ und $f_F \in F[X]$ die Minimalpolynome von α über K, beziehungsweise über F.

   (a) Zeige, dass $f_F | f$ in $L[X]$ gilt.

   (b) Sei $f_F = X^n + \sum_{k=0}^{n-1} a_k X^k$. Zeige, dass $K(a_0, \ldots, a_{n-1}) = F$ ist.

   (c) Folgere, dass die Erweiterung L/K nur endlich viele Zwischenerweiterungen hat.

   Lösung: (a) Laut §5.3 gilt $\mathrm{Kern}(\mathrm{eval}_\alpha) = (f_F)$ in $F[X]$. Wegen $f \in \mathrm{Kern}(\mathrm{eval}_\alpha)$ folgt $f_F | f$ in $F[X]$, also auch in $L[X]$.

   (b) Aus $f_F \in F[X]$ folgt $F' := K(a_0, \ldots, a_{n-1}) \subset F$. Weiter gilt wegen $F \subset L$ die Körpergleichheit $F(\alpha) = L = F'(\alpha)$, und laut §5.3 gilt $[L/F] = \deg(f_F) = n$. Andererseits ist f_F auch ein annullierendes Polynom von α in $F'[X]$ und deshalb folgt $[L/F'] \leqslant n$. Mit der Multiplikativität der Körpergrade folgt

   $$[F/F'] = \frac{[L/F']}{[L/F]} \leqslant 1,$$

   also $F' = F$.

   (c) Sei $\overline{L}$ ein algebraischer Abschluss von L. Das Polynom f hat nur endlich viele Teiler in $\overline{L}[X]$. Aus (a) und (b) folgt, dass es höchstens so viel Zwischenkörper wie Teiler von f gibt.

5. Sind die folgenden Körper isomorph?

   (a) $\mathbb{Q}[X]/(X^2-2)$ und $\mathbb{Q}[X]/(X^2+2)$;

   (b) $\mathbb{Q}[X]/(X^2+1)$ und $\mathbb{Q}[X]/(X^2+2)$;

   (c) $\mathbb{R}[X]/(X^2+1)$ und $\mathbb{R}[X]/(X^2+2)$;

   (d) $\mathbb{Q}[X]/(X^3-2)$ und $\mathbb{Q}[X]/(X^3+2)$.

   Lösung: (a) Wir können beide Körper in $\mathbb{C}$ einbetten via $\mathbb{Q}[X]/(X^2-2) \cong \mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}[X]/(X^2+2) \cong \mathbb{Q}(\sqrt{2}i)$. Ein Isomorphismus $\mathbb{Q}[X]/(X^2+2) \to \mathbb{Q}[X]/(X^2-2)$ entspricht damit einem Isomorphismus $\sigma\colon \mathbb{Q}(\sqrt{2}i) \to \mathbb{Q}(\sqrt{2})$. Dieser ist auf dem Primkörper $\mathbb{Q}$ die Identität; also ist $-2 = \sigma(-2) = \sigma((\sqrt{2}i)^2) = \sigma(\sqrt{2}i)^2$ ein Quadrat in $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$; Widerspruch. Somit sind die beiden Körper nicht isomorph.

   (b) Wie in (*a*) bekommen wir $\sigma(\sqrt{2}i)^2 = -2$. Das ist in $\mathbb{Q}(i) \cong \mathbb{Q}[X]/(X^2+1)$ nicht möglich. Sei nämlich $(a+ib)^2 = -2$ mit $a, b \in \mathbb{Q}$. Dann ist $a^2-b^2+2abi = -2$, also $a^2 - b^2 = -2$ und $2ab = 0$. Die erste Gleichung impliziert $b \neq 0$, was mit der zweiten $a = 0$ impliziert. In die erste Gleichung eingesetzt folgt daraus $b^2 = 2$. Aber in $\mathbb{Q}$ gibt es keine Quadratwurzel aus 2, Widerspruch.

   Aliter: Wir können via $\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}(i)$ und $\mathbb{Q}[X]/(X^2+2) \cong \mathbb{Q}(\sqrt{2}i)$ beide Körper mit Unterkörpern von $\mathbb{C}$ identifizieren. Ihr Kompositum ist dann $\mathbb{Q}(\sqrt{2}, i)$ und hat Grad 4 über $\mathbb{Q}$; insbesondere sind sie verschieden. Nach Serie 24 Aufgabe 4 sind diese beiden Körper genau dann isomorph über $\mathbb{Q}$, wenn die Galoisgruppen $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(i))$ und $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(\sqrt{2}i))$ in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ konjugiert sind. Allerdings ist $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ isomorph zur Kleinschen Vierergruppe, also kommutativ, und hat keine verschiedenen zueinander konjugierten Untergruppen.

   (c) Wegen $\sqrt{2} \in \mathbb{R}$ induziert die Substitution $X \mapsto X/\sqrt{2}$ einen Isomorphismus.

   Aliter: Direkte Folge aus Aufgabe 21 (c) unten.

   (d) Ja, via der von $X \mapsto -X$ induzierten Abbildung.

   Aliter: $\mathbb{Q}[X]/(X^3-2) \cong \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(-\sqrt[3]{2}) \cong \mathbb{Q}[X]/(X^3+2)$.

6. Entscheide, ob sich der Winkel $\arccos(11/16)$ mit Zirkel und Lineal dritteln lässt.

   Lösung: Wir setzen $\alpha := \arccos\frac{11}{16}$ und $a := \cos\frac{\alpha}{3}$. Aus der Vorlesung wissen wir, dass ein Winkel genau dann konstruierbar ist, wenn sein Cosinus (oder äquivalenterweise sein Sinus) als Länge konstruierbar ist. Daher lässt sich der Winkel α genau dann dritteln, wenn a konstruierbar ist.

   Die allgemeine Formel $\cos x = 4\cos^3\frac{x}{3} - 3\cos\frac{x}{3}$ ergibt

$$\frac{11}{16} = \cos\alpha = 4a^3 - 3a.$$

   Folglich ist

$$f(X) = 64X^3 - 48X - 11$$

ein annullierendes Polynom von a. Die Substitution $Y = 4X$vereinfacht f zu dem Polynom $Y^3 - 12Y - 11$, für das man leicht sieht, dass es die Nullstelle -1 hat und daher in $\mathbb{Q}[X]$ in Faktoren vom Grad $\leqslant 2$ zerfällt. Die Nullstelle $a/4$ liegt somit in einer quadratischen Erweiterung von $\mathbb{Q}$ und ist konstruierbar, also gilt das auch für a. Somit lässt sich der Winkel α dritteln.

Genauer finden wir

$$Y^3 - 12Y - 11 = (Y + 1)(Y^2 - Y - 11).$$

Die Nullstellen dieses Polynoms sind $Y = -1, \frac{1\pm\sqrt{45}}{2}$. Folglich hat f die Nullstellen $-\frac{1}{4}, \frac{1\pm\sqrt{45}}{8}$. Wegen $0 < \frac{\alpha}{3} < \pi/2$ ist a positiv, daher gilt $a = \frac{1+\sqrt{45}}{8}$.

7. Zeige: Jede Körpererweiterung von $\mathbb{Q}$ vom Transzendenzgrad $\leqslant |\mathbb{R}|$ ist isomorph zu einem Unterkörper von $\mathbb{C}$.

   Lösung: Sei $K/\mathbb{Q}$ eine Körpererweiterung vom Transzendenzgrad $\leqslant |\mathbb{R}|$ mit Transzendenzbasis $\{X_i\}_{i\in I}$. Sei andererseits $\{y_j\}_{j\in J}$ eine Transzendenzbasis von $\mathbb{R}/\mathbb{Q}$. Nach §5.6 der Vorlesung ist dann $|J| = |\mathbb{R}|$; also existiert eine injektive Abbildung $\kappa\colon I \hookrightarrow J$. Aufgrund der universellen Eigenschaft des Polynomrings existiert ein eindeutiger Ringhomomorphismus $\varphi\colon \mathbb{Q}[\{X_i\}_{i\in I}] \to \mathbb{R}$ mit $X_i \mapsto y_{\kappa(i)}$ für alle $i \in I$. Da κ injektiv ist, sind die $y_{\kappa(i)}$ algebraisch unabhängig über $\mathbb{Q}$ und folglich ist φ injektiv. Es setzt sich somit fort zu einem eindeutigen Körperhomomorphismus $\varphi\colon \mathbb{Q}(\{X_i\}_{i\in I}) \to \mathbb{R}$. Da $K/\mathbb{Q}(\{X_i\}_{i\in I})$ algebraisch und $\mathbb{C}$ algebraisch abgeschlossen ist, lässt sich dieser nach §5.7 zu einem Homomorphismus $K \to \mathbb{C}$ fortsetzen. Dieser ist ein Isomorphismus von K auf einen Unterkörper von $\mathbb{C}$.

*8. Sei F/K eine (nicht notwendigerweise algebraische) Körpererweiterung mit Zwischenkörpern K_1 und K_2, sodass F algebraische Abschlüsse $\overline{K_1}$ von K_1 sowie $\overline{K_2}$ von K_2 enthält. Zeige oder widerlege:

   (*a) $\overline{K_1} \cap \overline{K_2}$ ist ein algebraischer Abschluss von $K_1 \cap K_2$.

   (**b) $\overline{K_1}\,\overline{K_2}$ ist ein algebraischer Abschluss von K_1K_2.

   Lösung: (a) Die Aussage stimmt im allgemeinen nicht. Für ein Gegenbeispiel sei X transzendent über K, und sei F ein algebraischer Abschluss von $K(X)$. Dann ist $\overline{K_1} := \overline{K_2} := F$ auch ein algebraischer Abschluss der Unterkörper $K_1 := K(X^2)$ und $K_2 := K(X^2 - X)$. Nach Aufgabe 17 unten gilt aber $K_1 \cap K_2 = K$. Da F/K nicht algebraisch ist, ist $\overline{K_1} \cap \overline{K_2} = F$ also kein algebraischer Abschluss von $K_1 \cap K_2$.

   (b) Siehe Shreeram Abhyankar, "On the Compositum of Algebraically Closed Subfields", `http://repository.ias.ac.in/191/1/405.pdf`

9. Finde alle Körperhomomorphismen $K = \mathbb{Q}(\sqrt[4]{2}, e^{\frac{\pi i}{4}}) \to \mathbb{C}$. Ist $K/\mathbb{Q}$ normal?

   Lösung: Wegen $e^{\frac{\pi i}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ gilt $\mathbb{Q}(\sqrt[4]{2}, e^{\frac{\pi i}{4}}) = \mathbb{Q}(\sqrt[4]{2}, i)$ und $[\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}] = 8 = |\operatorname{Hom}(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{C})|$.

   Die Körperhomomorphismen $\mathbb{Q}(i) \to \mathbb{C}$ sind die Identität und die komplexe Konjugation $\sigma\colon \mathbb{C} \to \mathbb{C}$ eingeschränkt auf $\mathbb{Q}(i)$.

   Das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(i)$ ist $X^4 - 2$ und hat die vier Nullstellen $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. Für jede Nullstelle α von $X^4 - 2$ gibt es einen Isomorphismus $\mathbb{Q}(i)[X]/(X^4 - 2) \to \mathbb{Q}(\alpha)$ über $\mathbb{Q}(i)$, der die Restklasse von X auf α abbildet. Daher gibt es für jedes α einen Homomorphismus $\tau_\alpha\colon \mathbb{Q}(i)(\sqrt[4]{2}) \to \mathbb{C}$ über $\mathbb{Q}(i)$, der $\sqrt[4]{2}$ auf α abbildet. Dieser ist eindeutig, da die Elemente in $\mathbb{Q}(i)(\sqrt[4]{2})$ als Polynome in $\sqrt[4]{2}$ mit Koeffizienten in $\mathbb{Q}(i)$ dargestellt werden können und der Homomorphismus auf $\mathbb{Q}(i)$ die Identität sein muss.

   Die acht Homomorphismen $\{\tau_\alpha, \tau_\alpha \circ \sigma : \alpha \in \mathbb{C}, \alpha^4 = 2\}$ sind die gesuchten acht Homomorphismen $K \to \mathbb{C}$.

   Die Erweiterung $K/\mathbb{Q}$ ist normal, da K der Zerfällungskörper des Polynoms $X^4 - 2$ ist.

10. Zeige: Für endliche Körper k und ℓ existiert ein Homomorphismus $k \to \ell$ genau dann, wenn $|\ell|$ eine Potenz von $|k|$ ist.

    Lösung: Wenn ein Homomorphismus $k \to \ell$ existiert, macht dieser ℓ zu einem endlich dimensionalen k-Vektorraum. Ist dessen Dimension n, so ist ℓ als k-Vektorraum isomorph zu k^n; also folgt $|\ell| = |k^n| = |k|^n$.

    Sei umgekehrt $|\ell| = |k|^n$, und sei $p := \operatorname{char}(k)$. Laut §5.12 der Vorlesung ist k ein Zerfällungskörper des Polynoms $X^{|k|} - X$ über $\mathbb{F}_p$. Analog ist ℓ ein Zerfällungskörper des Polynoms $X^{|\ell|} - X = X^{|k|^n} - X$ über $\mathbb{F}_p$. Aber

$$\frac{X^{|k|^n} - X}{X^{|k|} - X} = \frac{(X^{|k|-1})^{\frac{|k|^n - 1}{|k|-1}} - 1}{X^{|k|-1} - 1}$$

    ist eine endliche geometrische Summe, also ein Polynom; folglich ist $X^{|k|} - X$ ein Teiler von $X^{|k|^n} - X$. Damit enthält ℓ einen Zerfällungskörper von $X^{|k|} - X$ über $\mathbb{F}_p$, und da Zerfällungskörper eindeutig bis auf Isomorphie sind, ist dieser Unterkörper isomorph zu k. Dieser Isomorphismus liefert den gesuchten Homomorphismus.

    Aliter: Sei $\overline{\ell}$ ein algebraischer Abschluss von ℓ. Da k algebraisch über $\mathbb{F}_p$ ist, existiert eine Einbettung $k \hookrightarrow \overline{\ell}$; oBdA sei also $k \subset \overline{\ell}$. Da $|k|$ eine Potenz von p ist, ist $\operatorname{Frob}_{|k|}$ ein Körperautomorphismus von $\overline{\ell}$, und k sein Fixkörper. Aus dem gleichen Grund ist ℓ der Fixkörper von $\operatorname{Frob}_{|\ell|}$ in $\overline{\ell}$. Im Fall $|\ell| = |k|^n$ ist aber $\operatorname{Frob}_{|\ell|} = \operatorname{Frob}_{|k|}^n$; also wird jedes von $\operatorname{Frob}_{|k|}$ festgelassene Element von $\overline{\ell}$ auch von $\operatorname{Frob}_{|\ell|}$ festgelassen. Somit gilt $k \subset \ell$.

*11. Sei p eine Primzahl und sei $q = p^n$ für eine positive ganze Zahl n.

(a) Zeige: Ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ teilt $X^q - X$ in $\mathbb{F}_p[X]$ genau dann, wenn sein Grad ein Teiler von n ist.

(b) Sei I_d die Menge der normierten, irreduziblen Polynome vom Grad d in $\mathbb{F}_p[X]$. Beweise die Gleichung

$$X^q - X = \prod_{d|n} \prod_{f \in I_d} f.$$

(c) Folgere daraus, dass gilt $\sum_{d|n} d|I_d| = q$.

(d) Bestimme die Anzahl der irreduziblen Polynome vom Grad 6, 7, 8 in $\mathbb{F}_2[X]$.

Lösungsskizze: (a) Jedes irreduzible Polynom über einem endlichen Körper ist separabel. Also ist f ein Teiler von $X^q - X$ genau dann, wenn f und $X^q - X$ eine gemeinsame Nullstelle α in einem algebraischen Abschluss $\overline{\mathbb{F}_p}$ von $\mathbb{F}_p$ haben. Aber die Nullstellen von $X^q - X$ sind genau die Elemente des Unterkörpers $\mathbb{F}_q$ der Ordnung q. Für diese ist $[\mathbb{F}_p(\alpha)/\mathbb{F}_p]$ ein Teiler von $[\mathbb{F}_q/\mathbb{F}_p] = n$. Umgekehrt liegen nach Aufgabe 10 alle $\alpha \in \overline{\mathbb{F}_p}$ mit $[\mathbb{F}_p(\alpha)/\mathbb{F}_p] \mid n$ in $\mathbb{F}_q$.

(b) Wegen (a) teilt die rechte Seite die linke. Sei umgekehrt $a \in \overline{\mathbb{F}_p}$ eine Nullstelle von $X^q - X$. Dann gilt $m_{a,\mathbb{F}_p} | X^q - X$ und $\deg(m_{a,\mathbb{F}_p}) \leqslant [\mathbb{F}_q/\mathbb{F}_p] = n$, also ist das Polynom auf der rechten Seite ein annullierendes Polynom für a.

(c) Vergleiche den Grad auf der rechten und linken Seite in (b).

(d) Mit (c) gilt $2^6 = |I_1| + 2|I_2| + 3|I_3| + 6|I_6|$. Die irreduziblen Polynome von Grad 2 und 3 können wir schnell abzählen und wir finden $|I_6| = 9$.

Wieder gilt $2^7 = |I_1| + 7|I_7|$ und daher $|I_7| = \frac{128-2}{7} = 18$.

Es gilt $2^8 = |I_1| + 2|I_2| + 4|I_4| + 8|I_8|$, also $|I_8| = \frac{2+2+12}{8} = 2$.

12. Der *Satz von Wilson* besagt, dass für jede Primzahl p gilt $(p-1)! \equiv -1 \bmod (p)$. Beweise dies vermittels einer Rechnung in $\mathbb{F}_p^\times$.

Lösung: Für $p = 2$ ist die Aussage offensichtlich. Sei also p ungerade. Dann ist $\mathbb{F}_p^\times$ eine zyklische Gruppe gerader Ordnung $p - 1$. Darin sind 1 und -1 gleich ihrem Inversen, und alle übrigen Elemente tauchen als Paare mit ihren Inversen auf. Das Produkt über alle Elemente von $\mathbb{F}_p^\times$ ist folglich gleich $1 \cdot (-1)$ mal ein Produkt von gewissen $\alpha \cdot \alpha^{-1}$, also insgesamt gleich -1. Somit gilt $\prod_{i=1}^{p-1} i \equiv -1$ modulo (p).

13. Wann ist eine Körpererweiterung vom Grad 2 inseparabel?

Lösung: Eine Körpererweiterung L/K ist inseparabel genau dann, wenn ein Erzeuger inseparables Minimalpolynom hat. Ein irreduzibles Polynom $X^2 + bX + c$ vom Grad 2 in $K[X]$ ist inseparabel genau dann, wenn $\mathrm{Char}(K) = 2$ und $b = 0$ ist. Also ist eine Körpererweiterung vom Grad 2 genau dann inseparabel, wenn sie eine Radikalerweiterung vom Grad 2 eines Körpers der Charakteristik 2 ist.

14. Für welche Werte von k ist die Körpererweiterung $\mathbb{F}_7(X)/\mathbb{F}_7(X^k)$

    (a) separabel?

    (b) normal?

    (c) galoissch?

    Lösung: (a) Das Minimalpolynom von X über $\mathbb{F}_7(X^k)$ ist $T^k - X^k$, da X^k ein Primelement in $\mathbb{F}_7[X^k]$ ist und wir Eisenstein mit $p = X^k$ auf $T^k - X^k$ anwenden können. Dieses genau dann ist separabel, wenn seine Ableitung nicht verschwindet, also genau dann, wenn k nicht durch 7 teilbar ist.

    (b) Die Körpererweiterung ist normal genau dann, wenn alle Nullstellen von $T^k - X^k$ in einem algebraischen Abschluss L von $\mathbb{F}_7(X)$ schon in $\mathbb{F}_7(X)$ liegen. Das ist genau dann der Fall, wenn $\mathbb{F}_7(X)$ alle k-ten Einheitswurzeln von L enthält.

    Schreibe $k = \ell \cdot 7^n$ mit $7 \nmid \ell$. Dann gilt $X^k - 1 = (X^\ell - 1)^{7^n}$ über $\mathbb{F}_7$, also ist jede k-te Einheitswurzel in L schon eine ℓ-te Einheitswurzel. Dagegen ist $X^\ell - 1$ separabel über $\mathbb{F}_7$, also ist die Gruppe der ℓ-ten Einheitswurzeln von L zyklisch der Ordnung ℓ.

    Jede Einheitswurzel in $\mathbb{F}_7(X)$ ist algebraisch über $\mathbb{F}_7$. Nach Serie 16 Aufgabe 5a ist aber jedes Element von $\mathbb{F}_7(X) \smallsetminus \mathbb{F}_7$ transzendent. Somit sind die Einheitswurzeln von $\mathbb{F}_7(X)$ gleich denen in $\mathbb{F}_7$. Diese bilden die zyklische Gruppe $\mathbb{F}_7^\times$ der Ordnung 6.

    Insgesamt enthält also $\mathbb{F}_7(X)$ alle k-ten Einheitswurzeln von L genau dann, wenn $\mathbb{F}_7$ alle ℓ-ten Einheitswurzeln von L enthält. Dies ist genau dann der Fall, wenn ℓ ein Teiler von 6 ist, also für

    $$k \in \{7^n, 2 \cdot 7^n, 3 \cdot 7^n, 6 \cdot 7^n : n \geqslant 0\}.$$

    (c) Die Erweiterung ist genau dann normal und separabel, wenn $k \in \{1, 2, 3, 6\}$ ist.

15. Sei H die Gruppe aller Automorphismen von $\mathbb{C}(X)$ der Form $f(X) \mapsto f(X + a)$ für alle $a \in \mathbb{C}$. Bestimme den Fixkörper $\mathbb{C}(X)^H$.

    Lösung: Betrachte ein Element $f \in \mathbb{C}(X)^H \smallsetminus \{0\}$ und schreibe es in der Form $f = g/h$ für teilerfremde $g, h \in \mathbb{C}[X] \smallsetminus \{0\}$. Für jedes a gilt dann

    $$\frac{g(X)}{h(X)} = \frac{g(X + a)}{h(X + a)}.$$

    Da auch $g(X+a)$ und $h(X+a)$ teilerfremd sind, ist dies nur möglich mit $g(X+a) = \lambda g(X)$ für ein $\lambda \in \mathbb{C}^\times$. Vergleich der höchsten Koeffizienten impliziert dann $\lambda = 1$. Also gilt $g(X + a) = g(X)$. Für jede Nullstelle $z \in \mathbb{C}$ von g ist dann auch $z + a$ eine Nullstelle. Da a beliebig ist, aber g nur endlich viele Nullstellen haben kann, ist dies nur möglich, wenn g konstant ist. Dasselbe Argument für h zeigt, dass h

und folglich auch f konstant ist. Umgekehrt sind alle Konstanten in $\mathbb{C}$ offenbar invariant unter H. Folglich ist der Fixkörper $\mathbb{C}(X)^H = \mathbb{C}$.

Aliter: Wäre der Fixkörper nicht $\mathbb{C}$, so enthielte er ein transzendentes Element, und $\mathbb{C}(X)$ wäre endlich darüber. Dann wäre aber $|H| \leqslant |\operatorname{Aut}_{\mathbb{C}(X)^H}(\mathbb{C}(X))| \leqslant [\mathbb{C}(X)/\mathbb{C}(X)^H] < \infty$. Widerspruch.

16. Sei L/K eine endliche Galoiserweiterung mit Zwischenkörpern K_1 und K_2 und den entsprechenden Galoisgruppen $\Gamma_i := \operatorname{Gal}(L/K_i) \leqslant \Gamma := \operatorname{Gal}(L/K)$. Zeige:

    (a) $K_1K_2 = L^{\Gamma_1 \cap \Gamma_2}$,

    (b) $K_1 \cap K_2 = L^{\langle \Gamma_1, \Gamma_2 \rangle}$, wobei $\langle \Gamma_1, \Gamma_2 \rangle$ die von Γ_1 und Γ_2 erzeugte Untergruppe von Γ bezeichnet.

    (c) Nehme an, dass $K_1K_2 = L$ gilt, der Durchschnitt $K_1 \cap K_2 = K$ ist und dass ausserdem für $i = 1, 2$ die Erweiterung K_i/K galoissch ist. Dann ist $\operatorname{Gal}(L/K) \cong \Gamma_1 \times \Gamma_2$.

    Lösungsskizze: (a) Da sowohl K_1 als auch K_2 von $\Gamma_1 \cap \Gamma_2$ fixiert werden, folgt $K_1K_2 \subset L^{\Gamma_1 \cap \Gamma_2}$. Auf der anderen Seite gilt $\operatorname{Gal}(L/K_1K_2) \subset \Gamma_i$ für $i = 1, 2$, also folgt $K_1K_2 \supset L^{\Gamma_1 \cap \Gamma_2}$.

    (b) Da $K_1 \cap K_2$ von Γ_1 und Γ_2 fixiert wird, folgt $K_1 \cap K_2 \subset L^{\langle \Gamma_1, \Gamma_2 \rangle}$. Auf der anderen Seite gilt $L^{\langle \Gamma_1, \Gamma_2 \rangle} \subset L^{\Gamma_i}$ für $i = 1, 2$, also folgt $K_1 \cap K_2 \supset L^{\langle \Gamma_1, \Gamma_2 \rangle}$.

    (c) Wir müssen drei Bedingungen nachprüfen:

    i. $\langle \Gamma_1, \Gamma_2 \rangle = \operatorname{Gal}(L/K)$

    ii. $\Gamma_1 \cap \Gamma_2 = \{e\}$

    iii. $\Gamma_1, \Gamma_2 \lhd \operatorname{Gal}(L/K)$

    Bedingung i. folgt aus (b), Bedingung ii. folgt aus (a) und Bedingung iii. gilt, weil K_i/K galoissch ist.

*17. Sei K ein Körper der Charakteristik 0 und sei X transzendent über K. Zeige, dass $K(X^2) \cap K(X^2 - X) = K$ ist.

    Lösungsskizze: Die Erweiterungen $K(X)/K(X^2)$ und $K(X)/K(X^2 - X)$ haben Grad zwei und sind galoissch. Ihre nichttrivialen Galoisautomorphismen erfüllen $\sigma(X) = -X$ und $\tau(X) = -X + 1$. Wenn $K(X^2) \cap K(X^2 - X) \neq K$ gilt, dann enthält $K(X^2) \cap K(X^2 - X)$ ein transzendentes Element und die Erweiterung $K(X)/K(X^2) \cap K(X^2 - X)$ ist endlich. Das impliziert, dass die Gruppe

$$\langle \operatorname{Gal}(K(X)/K(X^2)), \operatorname{Gal}(K(X)/K(X^2 - X)) \rangle$$

    ebenfalls endlich sein muss. Wegen $(\sigma \circ \tau)^n(X) = X + n$ kann das aber nicht sein.

18. Zeige oder widerlege: Es existiert eine Körpererweiterung mit genau 50′000 echten Zwischenkörpern.

Lösung: Für jede natürliche Zahl n existiert eine zyklische Körpererweiterung vom Grad n, zum Beispiel eine Erweiterung $\mathbb{F}_{p^n}/\mathbb{F}_p$ vom Grad n für p prim, oder die Erweiterung $\mathbb{C}(X)/\mathbb{C}(X^n)$. Nach dem Hauptsatz der Galoistheorie ist die Anzahl der Zwischenkörper dann gleich der Anzahl der Untergruppen einer zyklischen Gruppe der Ordnung n, also gleich der Anzahl der Teiler von n. Für die echten Zwischenkörper sind die Teiler 1 und n wegzulassen, also suchen wir eine ganze Zahl $n > 1$ mit genau 50′002 Teilern. Ein Beispiel hierfür ist $n = r^{50'001}$ für eine Primzahl r, oder $k = r_1 r_2^{25'000}$ für Primzahlen r_1, r_2, oder $k = r_1 r_2^{22} r_3^{1086}$ für Primzahlen r_1, r_2, r_3.

19. Bestimme die Galoisgruppen der folgenden Polynome über $\mathbb{Q}$:

(a) $X^3 - 2X + 1$,

(b) $X^3 + X + 1$,

(c) $X^3 - 6X + 1$,

(d) $X^3 - 12X + 8$.

Lösungsskizze: (a) Das Polynom hat genau eine rationale Nullstelle, daher ist die Galoisgruppe zyklisch der Ordnung 2.

(b) Das Polynom ist irreduzibel, hat eine reelle und zwei nichtreelle Nullstellen, deshalb ist die Galoisgruppe S_3.

(c) Das Polynom ist irreduzibel, daher kann die Galoisgruppe nur gleich A_3 oder S_3 sein. Seine Diskriminante ist 837, also kein Quadrat in $\mathbb{Q}$, daher ist laut §6.5 die Galoisgruppe nicht in A_3 enthalten, muss also gleich S_3 sein.

(d) Das Polynom ist irreduzibel, daher kann die Galoisgruppe nur gleich A_3 oder S_3 sein. Seine Diskriminante ist $5184 = 72^2$, also ein Quadrat in $\mathbb{Q}$, daher ist laut §6.5 die Galoisgruppe in A_3 enthalten, ist also gleich A_3.

*20. Sei m ungerade, und sei K ein Körper der Charakteristik 0, der alle m-ten Einheitswurzeln enthält. Sei f ein irreduzibles Polynom der Form

$$f(X) = X^{2m} - 2aX^m + 1 \in K[X].$$

Zeige:

(a) Jeder Stammkörper L von f über K ist bereits ein Zerfällungskörper.

(b) Die Galoisgruppe $\mathrm{Gal}(L/K)$ ist isomorph zur Diedergruppe D_m.

(c) Bestimme alle Zwischenkörper von L/K.

Lösung: (a) Seien α eine Nullstelle von f in einem algebraischen Abschluss $\overline{K}$ von K und $\zeta_m \in K$ eine primitive m-te Einheitswurzel. Wegen $f(\zeta_m^i \alpha) = f(\alpha) = 0$ ist

$$A := \{\zeta_m^i \alpha \mid 0 \leqslant i \leqslant m-1\} \subset K(\alpha)$$

eine Teilmenge der Menge der Nullstellen von f. Wegen $f(0) = 1 \neq 0$ ist $\alpha \neq 0$, und weil ζ_m eine primitive m-te Einheitswurzel ist, folgt $|A| = m$. Weiter gilt $f(\alpha^{-1}) = \alpha^{-2m} - 2a\alpha^{-m} + 1 = \alpha^{-2m} f(\alpha) = 0$. Also ist auch α^{-1} eine Nullstelle von f, und daher genauso jedes Element von

$$A' := \{\zeta_m^i \alpha^{-1} \mid 0 \leqslant i \leqslant m-1\} \subset K(\alpha).$$

Diese Menge hat ebenfalls die Kardinalität $|A'| = m$. Ausserdem sind die Mengen A und A' disjunkt: Denn andernfalls existiert ein $0 \leqslant i \leqslant m-1$ mit $\alpha^{-1} = \zeta_m^i \alpha$. Daraus folgt $\alpha^2 = \zeta_m^{-i}$ und folglich $\alpha^{2m} = 1$, also ist α eine Nullstelle des Polynoms $X^{2m} - 1$. Nach Voraussetzung ist f das Minimalpolynom von α über K, also ist f dann ein Teiler von $X^{2m} - 1$. Aus Gradgründen muss somit $f(X) = X^{2m} - 1$ sein, was aber wegen der konstanten Koeffizienten nicht der Fall ist. Somit sind A und A' disjunkt.

Insgesamt folgt nun $|A \cup A'| = 2m$; also ist $A \cup A'$ genau die Nullstellenmenge von f. Wegen $A \cup A' \subset K(\alpha)$ ist der Stammkörper $K(\alpha)$ von f auch schon ein Zerfällungskörper. Damit ist die Aussage bewiesen.

(b) Die Diedergruppe D_m ist von einer Spiegelung s der Ordnung 2 und einer Drehung t der Ordnung m erzeugt mit der Relation $sts^{-1} = t^{-1}$. Wir zeigen, dass $\Gamma := \mathrm{Gal}(L/K)$ von zwei Elementen σ und τ mit den entsprechenden Eigenschaften erzeugt wird. Daraus folgt dann die gewünschte Isomorphie $\Gamma \cong D_m$.

Sei $L = K(\alpha)$ der oben gefundene Zerfällungskörper von f. Als Zerfällungskörper eines Polynoms ist L/K normal. Wegen $\mathrm{char}(K) = 0$ ist L/K separabel. Folglich ist L/K galoissch und es gilt

$$|\Gamma| = [L/K] = \deg(f) = 2m.$$

Da f irreduzibel ist, operiert Γ transitiv auf der Menge der Nullstellen $A \cup A'$. Wegen $L = K(\alpha)$ ist ausserdem jedes Element von Γ bereits durch seine Wirkung auf α bestimmt. Somit existieren eindeutige $\sigma, \tau \in \Gamma$ mit $\sigma(\alpha) = \alpha^{-1}$ und $\tau(\alpha) = \zeta_m \alpha$. Dann ist $\sigma^2(\alpha) = \alpha$ und somit $\sigma^2 = \mathrm{id}$; wegen $\sigma(\alpha) \neq \alpha$ hat σ daher die Ordnung 2. Weiter gilt $\tau^i(\alpha) = \zeta_m^i \alpha$ für jedes $i \in \mathbb{Z}$, und dieses ist gleich α genau dann, wenn $m|i$ ist. Somit ist $\tau^i = \mathrm{id}$ genau dann, wenn $m|i$ ist; also hat τ die Ordnung m. Ausserdem gilt

$$\tau\sigma\tau(\alpha) = \tau\sigma(\alpha^{-1}) = \tau(\zeta_m^{-1}\alpha^{-1}) = \zeta_m^{-1}\alpha = \sigma^{-1}(\alpha),$$

woraus $\tau\sigma\tau = \sigma^{-1}$ folgt. Damit erzeugen σ und τ eine zu D_m isomorphe Untergruppe $\langle \sigma, \tau \rangle < \Gamma$. Wegen $|D_m| = 2m = |\Gamma|$ folgt aus der Inklusion schliesslich die gewünschte Gleichheit.

(c) Jede Untergruppe ungerader Ordnung von Γ ist enthalten in der zyklischen Untergruppe $\langle\tau\rangle$ der Ordnung m, also gleich $\langle\tau^k\rangle$ für einen Teiler $k|m$. Wegen

$$\tau^k(\alpha^{m/k}) = \tau^k(\alpha)^{m/k} = (\zeta_m^k\alpha)^{m/k} = \zeta_m^m\alpha^{m/k} = \alpha^{m/k}$$

liegt $\alpha^{m/k}$ in dem zu $\langle\tau^k\rangle$ gehörenden Zwischenkörper $L^{\langle\tau^k\rangle}$. Also gilt $K(\alpha^{m/k}) \subset L^{\langle\tau^k\rangle}$. Betrachte andererseits das Polynom $X^{m/k} - \alpha^{m/k} \in K(\alpha^{m/k})[X]$. Da α eine Nullstelle dieses Polynoms ist, hat sein Minimalpolynom über $K(\alpha^{m/k})$ den Grad $\leqslant m/k$, und es folgt

$$[L/K(\alpha^{m/k})] = [K(\alpha^{m/k})(\alpha)/K(\alpha^{m/k})] \leqslant m/k = |\langle\tau^k\rangle| = [L/L^{\langle\tau^k\rangle}].$$

Wegen $K(\alpha^{m/k}) \subset L^{\langle\tau^k\rangle}$ folgt daraus

$$(*) \qquad L^{\langle\tau^k\rangle} = K(\alpha^{m/k}).$$

Jede Untergruppe gerader Ordnung $\Delta < \Gamma$ enthält ein Element der Ordnung 2. Da m ungerade ist, bilden die Elemente der Ordnung 2 von Γ genau die Konjugationsklasse der Spiegelung σ. Nach Konjugation von Δ betrachten wir daher zuerst den Fall $\sigma \in \Delta$. Dann ist weiter $\Delta \cap \langle\tau\rangle = \langle\tau^k\rangle$ für einen Teiler $k|m$, und folglich $\Delta = \langle\tau^k, \sigma\rangle$ der Ordnung $2k$.

Der zugehörige Fixkörper L^Δ ist dann in dem bereits bekannten Fixkörper $L^{\langle\tau^k\rangle} = K(\alpha^{m/k})$ enthalten, und es gilt $[L^{\langle\tau^k\rangle}/L^\Delta] = [\Delta : \langle\tau^k\rangle] = 2$. Um L^Δ zu bestimmen, suchen wir also ein Element von $K(\alpha^{m/k})$, das zusätzlich invariant unter $\sigma\colon \alpha \mapsto \alpha^{-1}$ ist und dabei möglichst nichttrivial ist. Dafür nehmen wir $\beta_k := \alpha^{m/k} + \alpha^{-m/k}$. Dieses Element ist offenbar invariant unter Δ, also gilt $K(\beta_k) \subset L^\Delta$. Da $\alpha^{m/k}$ eine Nullstelle des Polynoms $X^2 - \beta_k X + 1 \in K(\beta_k)[X]$ ist, folgt wie oben

$$[K(\alpha^{m/k})/K(\beta_k)] \leqslant 2 = [K(\alpha^{m/k})/L^\Delta].$$

Wegen $K(\beta_k) \subset L^\Delta$ folgt daraus $K(\beta_k) = L^\Delta$.

Schliesslich hat jede Untergruppe gerader Ordnung die Form ${}^\gamma\Delta$ für ein $\Delta = \langle\tau^k, \sigma\rangle$ wie oben und ein $\gamma \in \Gamma$. Wegen $\sigma \in \Delta$ gilt ${}^{\gamma\sigma}\Delta = {}^\gamma\Delta$; nach etwaigem Ersetzen von γ durch $\gamma\sigma$ können wir also oBdA $\gamma = \tau^i$ annehmen für ein $0 \leqslant i < m$. Nach Teil (c) des Hauptsatzes der Galoistheorie ist der entsprechende Fixkörper dann

$$(**) \quad L^{({}^{\tau^i}\Delta)} = \tau^i(L^\Delta) = \tau^i(K(\beta_k)) = K(\tau^i(\beta_k)) = K\big((\zeta_m^i\alpha)^{m/k} + (\zeta_m^i\alpha)^{-m/k}\big).$$

Mit $(*)$ und $(**)$ haben wir alle Zwischenkörper von L/K bestimmt.

*21. In dieser Aufgabe beweisen wir den Fundamentalsatz der Algebra mit Hilfe der Galoistheorie. Sei $K/\mathbb{R}$ eine endliche Körpererweiterung.

(a) Nimm an, $K/\mathbb{R}$ sei galoissch. Zeige, dass ein Körperturm $K = K_n/\ldots/K_0/\mathbb{R}$ existiert, sodass $[K_0/\mathbb{R}]$ ungerade ist und für jedes $0 \leqslant i \leqslant n-1$ die Erweiterung K_{i+1}/K_i den Grad 2 hat.

(b) Zeige, dass $\mathbb{R}$ keine nichttriviale Erweiterung von ungeradem Grad hat.

(c) Zeige, dass jede Erweiterung von $\mathbb{R}$ vom Grad 2 isomorph zu $\mathbb{C}$ ist.

(d) Zeige, dass $\mathbb{C}$ keine Erweiterung vom Grad 2 hat.

(e) Folgere, dass K entweder $\mathbb{R}$ oder $\mathbb{C}$ ist.

Lösung: (a) Set $G := \mathrm{Gal}(K/\mathbb{R})$. Write $|G| = 2^n m$, where m is an odd natural number. By Sylow, there exists a subgroup $G_0 < G$ of order $|G_0| = 2^n$. By the Galois correspondence, there is then an intermediate field K_0 such that

$$[K_0/\mathbb{R}] = [G : G_0] = m = \text{odd}.$$

Now repeat the process with the subgroup G_0. Since G_0 is a p-group for $p = 2$, there exists a chain of normal subgroups $1 = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0$ such that each G_l has order 2^{n-l}. By the Galois correspondence, it corresponds to a chain of intermediate fields $K = K_n \supset \ldots \supset K_0$ with $[K_{i+1} : K_i] = 2$.

(b) Suppose that $[K/\mathbb{R}]$ is odd. Take any element $\alpha \in K$ and let $f \in \mathbb{R}[X]$ be its minimal polynomial over $\mathbb{R}$. Then $\deg(f) = [\mathbb{R}(\alpha)/\mathbb{R}]$ divides $[K/\mathbb{R}]$ and is therefore also odd. By the Intermediate Value Theorem f then has a zero $\beta \in \mathbb{R}$. Thus $(X - \beta)$ divides f in $\mathbb{R}[X]$; but since f is already irreducible over $\mathbb{R}$ by assumption, we must have $f(X) = X - \beta$. Thus $\alpha = \beta \in \mathbb{R}$. This shows that every element of K already lies in $\mathbb{R}$; hence $K = \mathbb{R}$.

(c) If $[K/\mathbb{R}] = 2$, we have $K = \mathbb{R}(\alpha)$ for some element $\alpha \in K \smallsetminus \mathbb{R}$. After a linear substitution we may assume that $\alpha^2 \in \mathbb{R}$. The minimal polynomial of α over $\mathbb{R}$ is then $X^2 - \alpha^2$. As this is irreducible over $\mathbb{R}$, we must have $\alpha^2 < 0$, because otherwise it would have a real zero. Let β be the positive real square root of $|\alpha^2|$. Then $K = \mathbb{R}(\alpha) = \mathbb{R}(\frac{\alpha}{\beta})$ with $(\frac{\alpha}{\beta})^2 = \frac{\alpha^2}{\beta^2} = -1$. Thus $K \cong \mathbb{C}$ over $\mathbb{R}$ with $\frac{\alpha}{\beta} \leftrightsquigarrow i$.

(d) If $[K/\mathbb{C}] = 2$, we have $K = \mathbb{C}(\alpha)$ for some element $\alpha \in K \smallsetminus \mathbb{C}$. After a linear substitution we may assume that $\alpha^2 \in \mathbb{C}$. The minimal polynomial of α over $\mathbb{R}$ is then $X^2 - \alpha^2$. But every complex number has a square root in $\mathbb{C}$; so this polynomial is reducible over $\mathbb{C}$; contradiction.

(e) Suppose first that $K/\mathbb{R}$ is Galois, and let $K = K_n/\ldots/K_0/\mathbb{R}$ be as in (a). Then $K_0 = \mathbb{R}$ by (b). If $n = 0$, it follows that $K = \mathbb{R}$. Otherwise (c) implies that $K_1 \cong \mathbb{C}$, and (d) implies by induction that $K_i = K_1$ for all $1 \leqslant i \leqslant n$. Thus $K = K_n \cong \mathbb{C}$.

For general K let L be a Galois closure of $K/\mathbb{R}$. Then the preceding case shows that $L \cong \mathbb{R}$ or $\mathbb{C}$; hence the same follows for K.

22. Sei R ein Ring, und seien $f, g \in R[X]$ normierte Polynome. Zeige:

$$\mathrm{Disc}_{fg} = \mathrm{Disc}_f \cdot \mathrm{Disc}_g \cdot \mathrm{Res}_{f,g}^2 .$$

Lösung: Zuerst seien f und g in Linearfaktoren zerlegt, also $f(X) = \prod_{i=1}^{n}(X - \lambda_i)$ und $g(X) = \prod_{j=1}^{m}(X - \lambda'_j)$. Dann wissen wir

$$\begin{aligned}
\mathrm{Disc}_f &= \prod_{1 \leqslant i < j \leqslant n} (\lambda_i - \lambda_j)^2, \\
\mathrm{Disc}_g &= \prod_{1 \leqslant i < j \leqslant m} (\lambda'_i - \lambda'_j)^2, \\
\mathrm{Res}_{f,g} &= \prod_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} (\lambda_i - \lambda'_j).
\end{aligned}$$

Andererseits ist $fg(X) = \prod_{i=1}^{n+m}(X - \mu_i)$ mit $\mu_i := \lambda_i$ für $1 \leqslant i \leqslant n$ und $\mu_i := \lambda'_{i-n}$ für $n+1 \leqslant i \leqslant n+m$. Dadurch erhalten wir

$$\begin{aligned}
\mathrm{Disc}_{fg} &= \prod_{1 \leqslant i < j \leqslant n+m} (\mu_i - \mu_j)^2 \\
&= \prod_{1 \leqslant i < j \leqslant n} (\mu_i - \mu_j)^2 \prod_{n+1 \leqslant i < j \leqslant n+m} (\mu_i - \mu_j)^2 \prod_{\substack{1 \leqslant i \leqslant n \\ n+1 \leqslant j \leqslant n+m}} (\mu_i - \mu_j)^2 \\
&= \prod_{1 \leqslant i < j \leqslant n} (\lambda_i - \lambda_j)^2 \prod_{1 \leqslant i < j \leqslant m} (\lambda'_i - \lambda'_j)^2 \prod_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} (\lambda_i - \lambda'_j)^2 \\
&= \mathrm{Disc}_f \cdot \mathrm{Disc}_g \cdot \mathrm{Res}_{f,g}^2 .
\end{aligned}$$

Dadurch ist die Aussage für alle Polynome, die Produkte von Linearfaktoren sind, bewiesen.

Insbesondere gilt die Aussage dann, wenn die Nullstellen der Polynome unabhängige Variablen sind, also wenn $f(X) = \prod_{i=1}^{n}(X - Y_i)$ und $g(X) = \prod_{j=1}^{m}(X - Z_j)$ ist. In diesem Fall sind die Koeffizienten von f und g also $\pm$ die elementarsymmetrischen Polynome in den Y_i, bzw. in den Z_j. Nach dem Hauptsatz über symmetrische Polynome können die elementarsymmetrischen Polynome als unabhängige Variablne betrachtet werden und wir können sie durch beliebige Werte aus dem Ring R ersetzen. Dieses Verfahren liefert also das Resultat für alle normierten Polynome in $R[X]$.

23. Zeige: Für beliebige positive ganze Zahlen $q_1, \ldots, q_n$ gilt

$$L := \mathbb{Q}\big(\sqrt{q_1}, \ldots, \sqrt{q_n}\big) \;=\; \mathbb{Q}\big(\sqrt{q_1} + \ldots + \sqrt{q_n}\big).$$

Lösung: Als Zerfällungskörper des Polynoms $(X^2 - q_1) \cdots (X^2 - q_n)$ ist L endlich galoissch über $\mathbb{Q}$. Für jedes Element γ seiner Galoisgruppe und jedes i gilt $\gamma(\sqrt{q_i}) \in \{\pm\sqrt{q_i}\}$. Mit $a := \sqrt{q_1} + \ldots + \sqrt{q_n}$ gilt also $\gamma(a) = \pm\sqrt{q_1} \pm \ldots \pm \sqrt{q_n}$ mit gewissen voneinander unabhängigen Vorzeichen. Da alle $\sqrt{q_i} > 0$ sind, ist folglich $\gamma(a) = a$ nur dann, wenn alle diese Vorzeichen + sind. In diesem Fall gilt $\gamma(\sqrt{q_i}) = \sqrt{q_i}$ für jedes i, also ist γ schon die Identität auf ganz L. Somit ist der Stabilisator von a in $\mathrm{Gal}(L/\mathbb{Q})$ trivial. Dieser Stabilisator ist aber gleich $\mathrm{Gal}(L/\mathbb{Q}(a))$; darum ist $\mathbb{Q}(a) = L$, was zu zeigen war.

*24. Sei L/K eine endliche Körpererweiterung vom Grad m. Für jedes $\alpha \in L$ ist die *Spur* $\mathrm{Tr}_{L/K}(\alpha)$ definiert als Spur der K-linearen Abbildung $\mu_\alpha \colon L \to L$, $x \mapsto \alpha x$. Zeige:

(a) Ist $X^n + \sum_{k=0}^{n-1} a_k X^k$ das Minimalpolynom von $\alpha \in L$ über K, so gilt für die Spur $\mathrm{Tr}_{L/K}(\alpha) = -\frac{m}{n} a_{n-1}$.

(b) Die Spur induziert eine K-lineare Abbildung $\mathrm{Tr}_{L/K} \colon L \to K$.

(c) Ist L/K separabel und $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_m\}$ für einen algebraischen Abschluss $\overline{K}$ von K, so gilt $\mathrm{Tr}_{L/K}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_m(\alpha)$.

(d) Ist L/K separabel, so ist die Spurabbildung $\mathrm{Tr}_{L/K} \colon L \to K$ surjektiv.

(e) Benutze dies um den zur Untergruppe $\{1, 2, 4\} < \mathbb{F}_7^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_7)/\mathbb{Q})$ gehörenden Zwischenkörper explizit zu konstruieren.

(*f) Zeige allgemein: Für jede Primzahl p und jede Untergruppe $H < \mathbb{F}_p^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ und jede primitive p-te Einheitswurzel ζ gilt

$$\mathbb{Q}(\mu_p)^H = \; \mathbb{Q}\Big(\sum_{h \in H} \zeta^h\Big).$$

Beachte: Die Spur einer quadratischen Matrix ist definiert als die Summe ihrer Diagonaleinträge. Als minus der zweithöchste Koeffizient des charakteristischen Polynoms ist sie invariant unter Ähnlichkeit. (Vergleiche Lineare Algebra I Wiederholungsserie Aufgabe 9.) Für jeden Endomorphismus φ eines endlich dimensionalen K-Vektorraums mit Basis $\mathcal{B}$ ist die Spur der Darstellungsmatrx $M_{\mathcal{B}\mathcal{B}}(\varphi)$ folglich unabhängig von $\mathcal{B}$, hängt also nur von φ ab, und heisst die *Spur von* φ, englisch trace, geschrieben $\mathrm{Tr}(\varphi)$.

Lösungsskizze: (a) Da α den Grad n über K hat, ist $(1, \alpha, \ldots, \alpha^{n-1})$ eine Basis von $K(\alpha)$ über K. Sei ausserdem $(\beta_1, \ldots, \beta_{m/n})$ eine Basis von L über $K(\alpha)$. Wie im Beweis der Multiplikativität des Körpergrads ist dann

$$(\beta_1, \alpha\beta_1, \ldots, \alpha^{n-1}\beta_1, \beta_2, \ldots, \alpha^{n-1}\beta_{m/n})$$

eine Basis von L über K. Bezüglich dieser hat die Darstellungsmatrix von μ_α die Blockform

$$\begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & 0 \\ 0 & \cdots & 0 & B \end{pmatrix} \qquad \text{für} \qquad B := \begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & & & -a_1 \\ 0 & & & \vdots \\ & & 0 & -a_{n-2} \\ 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} \in M_{n\times n}(K).$$

Somit ist $\mathrm{Tr}_{L/K}(\alpha) = \frac{m}{n}\,\mathrm{Tr}(B) = -\frac{m}{n}a_{n-1}$.

(b) Sei $\mathrm{VHom}_K(L,L)$ die Menge der K-Vektorraumisomorphismen von L nach L. Dann gilt $\mathrm{VHom}_K(L,L) \cong \mathrm{Mat}_{m\times m}(K)$. Die Abbildungen $\mathrm{Tr}\colon \mathrm{Mat}_{m\times m}(K) \to K$ und $\mu\colon L \to \mathrm{VHom}_K(L,L)$ sind linear, also auch ihre Verknüpfung.

(c) Die Bilder von α unter den Einbettungen $\sigma_1,\dots,\sigma_m$ sind gerade die verschiedenen Nullstellen $\alpha_1,\dots,\alpha_n$ des Minimalpolynoms von α. Sei $\mathrm{Hom}_K(K(\alpha),\overline{L}) = \{\tau_1,\dots,\tau_n\}$. Jedes τ_i hat genau $[L/K(\alpha)] = m/n$ Fortsetzungen auf L. Das impliziert für jedes $1 \leqslant j \leqslant n$, dass $|\{1 \leqslant i \leqslant m : \sigma_i(\alpha) = \alpha_j\}| = m/n$ ist. Nach dem Satz von Vieta ist $\alpha_1 + \cdots + \alpha_n = -a_{n-1}$, und somit ist $\sigma_1(\alpha) + \cdots + \sigma_m(\alpha) = \frac{m}{n}(\alpha_1 + \cdots + \alpha_n) = -\frac{m}{n}a_{n-1} = \mathrm{Tr}_{L/K}(\alpha)$.

(d) Wegen (b) genügt es, zu zeigen, dass $\mathrm{Tr}_{L/K}$ ungleich null ist. Wir nehmen zuerst an, die Erweiterung L/K sei galoissch. Dann sind $\sigma_1,\dots,\sigma_m$ die Elemente der Galoisgruppe von L/K und somit linear unabhängig. Ist $\mathrm{Tr}_{L/K}$ ungleich null. Sei nun M die normale Hülle von L/K. Mit (c) können wir zeigen, dass $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$ gilt. Da $\mathrm{Tr}_{M/K} \neq 0$ ist, folgt $\mathrm{Tr}_{L/K} \neq 0$.

(e) Sei ζ eine primitive siebte Einheitswurzel. Dann ist $t := \zeta + \zeta^2 + \zeta^4$ die Summe aller Konjugierten von ζ unter der Untergruppe $\{1,2,4\}$ und liegt folglich im zugehörigen Fixkörper $\mathbb{Q}(\mu_7)^H$. Da die Untergruppe Index 2 hat, hat dieser Fixkörper Grad 2 über $\mathbb{Q}$. Wenn er also nicht schon von t erzeugt ist, so liegt t schon in $\mathbb{Q}$. In diesem Fall ist t gleich seinem Konjugierten unter einem der restlichen Elemente von $\mathbb{F}_7^\times$, also gleich $\zeta^3 + \zeta^5 + \zeta^6$. Es gibt $n+1$ Wege zu zeigen, dass dies nicht der Fall ist (elementare Trigonometrie, Analysis, Algebra, Zahlentheorie). Siehe (f).

(f) Als Summe aller Konjugierten von ζ unter H liegt $\sum_{h\in H}\zeta^h$ im Fixkörper $\mathbb{Q}(\mu_p)^H$. Genauer ist es nach (c) gleich der Spur von ζ unter der Körpererweiterung $\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p)^H$. Für die Gleichheit $\mathbb{Q}(\mu_p)^H = \mathbb{Q}(\sum_{h\in H}\zeta^h)$ bleibt daher nur noch zu zeigen, dass $\sum_{h\in H}\zeta^h$ nicht schon in einem kleineren Körper liegt. Dafür genügt es zu zeigen, dass es verschieden von seinen Konjugierten unter allen Elementen von $\mathbb{F}_p^\times \smallsetminus H$ ist.

Betrachte also ein $n \in \mathbb{F}_p^\times \smallsetminus H$. Das entsprechende Konjugierte von $\sum_{h\in H}\zeta^h$ ist dann $\sum_{h\in H}\zeta^{hn}$. Wäre es gleich $\sum_{h\in H}\zeta^h$, so hätten wir also die Gleichung $\sum_{h\in H}\zeta^{hn} - \sum_{h\in H}\zeta^h = 0$. Für jedes $i \in \mathbb{F}_p^\times$ sei $\overline{i}$ sein eindeutiger Repräsentant in $\{1,\dots,p-1\}$, und betrachte das Polynom

$$P(X) \;:=\; \sum_{h\in H} X^{\overline{hn}} - \sum_{h\in H} X^{\overline{h}} \;\in\; \mathbb{Z}[X].$$

Dann ist ζ eine Nullstelle von P. Andererseits ist ζ eine Nullstelle des p-ten Kreisteilungspolynoms

$$\Phi_p(X) \;:=\; X^{p-1} + \ldots + X + 1 \;\in\; \mathbb{Z}[X].$$

Letzteres ist irreduzibel und muss folglich P teilen. Aber P hat Grad $\leqslant p-1 = \deg(\Phi_p)$ und ist zusätzlich durch X teilbar. Folglich muss $P = 0$ sein. Aber da H und Hn nichtleer und disjunkt sind, ist $P \neq 0$, Widerspruch.

25. Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom, das in $\mathbb{C}$ sowohl reelle als auch nicht-reelle Nullstellen hat. Zeige, dass Gal_f nicht abelsch ist.

Lösung: Seien α eine reelle und β eine nicht-reelle komplexe Nullstelle von f. Da f irreduzibel ist, operiert Gal_f transitiv auf den Nullstellen von f; also existiert ein $\tau \in \mathrm{Gal}_f$ mit $\tau(\beta) = \alpha$. Sei weiter $\sigma \in \mathrm{Gal}_f$ die komplexe Konjugation. Dann gilt $\sigma(\tau(\beta)) = \sigma(\alpha) = \alpha$, aber $\tau(\sigma(\beta)) = \tau(\overline{\beta}) \neq \alpha$ wegen der Injektivität von τ. Also ist $\sigma \circ \tau \neq \tau \circ \sigma$ und somit Gal_f nicht-abelsch.

Aliter: Ist Gal_f abelsch, so wissen wir aus Serie 23 Aufgabe 4, dass der Zerfällungskörper von f bereits von jeder einzelnen Nullstelle über $\mathbb{Q}$ erzeugt wird. Insbesondere gilt dies für jede reelle Nullstelle, folglich liegt der Zerfällungskörper schon insgesamt in $\mathbb{R}$, im Widerspruch zur Annahme. Also kann Gal_f nicht abelsch sein.

**26. Konstruiere für jede natürliche Zahl $n \geqslant 1$

(a) ein Polynom vom Grad n über $\mathbb{Q}$ mit Galoisgruppe S_n.

(b) eine Erweiterung vom Grad n von $\mathbb{Q}$, die keine echten Zwischenkörper besitzt.

Lösung: Für (a) benutze Abschnitt 6.9 der Zusammenfassung; für (b) benutze (a).