Norbert Klingen

Algebra II

Übungen zur Vorlesung
(mit Lösungen)

Universität zu Köln SS 1985

Inhaltsverzeichnis

Algebra II

Übung 1

Aufgabe 1. (m)
Wiederholen Sie die Grundbegriffe der Galoistheorie und berichten Sie kurz über

a) Polynomringe, euklidischen Algorithmus, Hauptideal- und faktorielle Ringe.

b) Algebraische Elemente und Körpererweiterungen, Minimalpolynom, Stammkörper.

c) Algebraisch abgeschlossene Körper und algebraischer Abschluss.

d) Körpermonomorphismen, separable Polynome, Elemente und Körpererweiterungen.

e) Körperautomorphismen, normale Körpererweiterungen, Zerfällungskörper.

f) galoissche Körpererweiterungen und ihre verschiedenen Charakterisierungen.

g) Hauptsatz der Galoistheorie.

Überprüfen – und vertiefen Sie ggf. – ihre Kenntnisse aus der Algebra I an folgenden Übungen.

Aufgabe 2. (m)
Es bezeichne für $n \in \mathbb{N}$ ζ_n jeweils eine primitive n-te Einheitswurzel in $\mathbb{C}$ bzw. einer algebraisch abgeschlossenen Hülle $\tilde{\mathbb{Q}}$ von $\mathbb{Q}$. Zeigen Sie:

a) $\mathbb{Q}(\sqrt{3}, \sqrt{3} + \sqrt[3]{9}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$.

b) $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$.

c) $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$.

d) $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ ist der Zerfällungkörper von $X^3 - 2$ über $\mathbb{Q}$.

Lösung:
a) $\subseteq$ wegen $\sqrt[3]{9} = (\sqrt[3]{3})^2$. $\supseteq$ wegen $\sqrt[3]{3} = \frac{3}{\sqrt[3]{9}}$.
b) $\subseteq$ wegen $\zeta_6 = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + \frac{1}{2}i\sqrt{3}$ und $\zeta_3 = -\frac{1}{2} + \frac{1}{2}i\sqrt{3} = \zeta_6 - 1$.
$\supseteq$ wegen $\sqrt{-3} = 2\zeta_3 + 1 = 2\zeta_6 - 1$.
c) $\subseteq$ wegen $\zeta_8 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{1}{2}\sqrt{2}(1+i)$. $\supseteq$ wegen $i = \zeta_4 = \zeta_8^2$ und $\sqrt{2} = \frac{2\zeta_8}{1+\zeta_8^2}$.
d) Körpergleichheit ist klar. $X^3 - 2$ hat die reelle Wurzel $\alpha = \sqrt[3]{2}$ und jede Wurzel β von $X^3 - 2$ hat als Quotient $\zeta = \frac{\beta}{\alpha}$ mit $\zeta^3 = \frac{\beta^3}{\alpha^3} = 1$, also $\beta = \zeta\alpha = \zeta_3^j\alpha$, $j = 0, 1, 2$. Damit zerfällt $X^3 - 2$ über dem gegebenen Körper in die drei Linearfaktoren $X - \zeta_3^j\sqrt[3]{2}$ $(j = 0, 1, 2)$.

Aufgabe 3. (m)
Welche Erweiterungen sind galoissch?

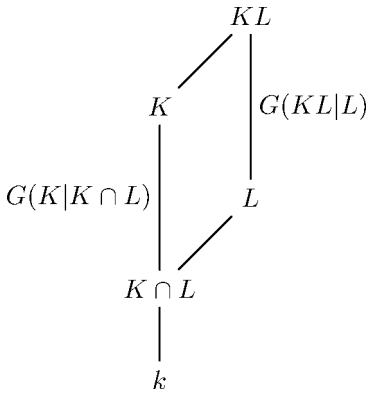
a) $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{2}, i)|\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2})|\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$.

b) $\mathbb{Q}(\zeta_n)|\mathbb{Q}$

c) $\mathbb{F}_p(\alpha)|\mathbb{F}_p$ mit einem über $\mathbb{F}_p$ algebraischen Element α.

Lösung:
a/b) In Charakteristik 0 sind alle algebraischen Erweiterungen separabel und daher ist *galoissch* gleichbedeutend mit *normal.*
a) $\mathbb{Q}(\sqrt{2})$ ist Zerfällungskörper von $X^2-2=(X-\sqrt{2})(X+\sqrt{2})$, also normal und galoissch über $\mathbb{Q}$. $\mathbb{Q}(\sqrt[4]{2},i)$ ist Zerfällungskörper von $X^4-2=(X^2-2)(X^2+2)=(X-\sqrt{2})(X+\sqrt{2})(X-i\sqrt{2})(X+i\sqrt{2})$, also normal und galoissch über $\mathbb{Q}$.
$\mathbb{Q}(\sqrt[3]{2},\zeta_3)$ ist Zerfällungskörper von $X^3-2=\prod_{j=0}^{2}(X-\zeta_3^j\sqrt[3]{2})$, also galoissch über $\mathbb{Q}$.
Als 2-Eisensteinpolynom ist X^4-2 irreduzibel, es hat zwei Wurzeln im reellen Körper $\mathbb{Q}(\sqrt[4]{2})$, zerfällt dort aber nicht in Linearfaktoren, die Erweiterung ist daher nicht normal und nicht galoissch über $\mathbb{Q}$.
b) ζ_n ist eine primitive Einheitswurzel, d. h. $\operatorname{ord}\zeta_n = n$ und daher erzeugt ζ_n die Gruppe $\mu_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}$ aller n-ten Einheitsurzeln. Diese sind aber gerade die Wurzeln des Polynoms X^n-1, so dass $\mathbb{Q}(\zeta_n)$ Zerfällungskörper von $X^n-1 \in \mathbb{Q}[X]$ und daher normal über $\mathbb{Q}$ ist.
c) Über endlichen Körpern sind alle algebraischen Erweiterungen galoissch (siehe Vorlesung Algebra I, Satz III.2.15). Zur Erinnerung: Jeder endliche Körper k der Mächtigkeit $q=p^s$ ist galoissch über dem Primkörper $\mathbb{F}_p$, da dieser genau der Fixkörper des Automorphismus $\alpha \mapsto \alpha^p$, $p = \operatorname{char} k$ ist. k ist der Zerfällungskörper des Polynoms $f = X^q - X$, welches separabel ist ($f' = qX^{q-1} - 1 = -1$ hat keine Nullstellen).

Aufgabe 4. (s)
K, L seien endliche Erweiterungen eines Körpers k, die in einem gemeinsamen Erweiterungskörper Ω von k liegen. KL sei das Kompositum (Erzeugnis) von K und L, d. h. der kleinste K und L umfassende Teilkörper von Ω.
Es sei $K|k$ ist galoissch! Folgern Sie daraus:



a) $KL|L$ ist galoissch.

b) $G(KL|L) \xrightarrow{\sim} G(K|K\cap L) \subseteq G(K|k)$, $\sigma \mapsto \sigma|_K$, ist ein Gruppenisomorphismus.

c) $(KL\colon L) = (K\colon K\cap L)$ und folglich
$(KL : K\cap L) = (K : K\cap L)(L : K\cap L)$.

d) Zeigen Sie durch ein Gegenbeispiel, dass c) ohne die Voraussetzung '$K|k$ galoissch' falsch ist.

Lösung:
a) Als galoissche Erweiterung ist $K|k$ Zerfällungskörper eines separablen Polynoms $f \in k[X]$, also sind $K|K\cap L$ bzw. $KL|L$ Zerfällungskörper desselben Polynoms über $K\cap L$ bzw. L und damit galoissch.
b) Die Restriktionsabbildung Φ ist natürlich ein Homomorphismus und die Werte liegen in der angegebenen Gruppe. Φ ist injektiv, denn für $\sigma \in G(KL|L)$ gilt:

$$\sigma|_K = \mathrm{id}_K \implies \mathrm{Fix}(\sigma) \supset K \cup L \implies \sigma = \mathrm{id}_{KL}\,.$$

Weiter gilt

$$\mathrm{Fix}_K(\operatorname{Im}\Phi) = K \cap \mathrm{Fix}_{KL}(G(KL|L)) = K\cap L = \mathrm{Fix}_K(G(K|K\cap L))$$

und daher nach dem Hauptsatz der Galoistheorie $\operatorname{Im}\Phi = G(K|K\cap L)$. Φ ist also auch surjektiv.
c) Die erste Gradgleichheit folgt dann aus der Isomorphie und dem Hauptsatz, die zweite aus der Multiplikativität der Körpergrade in Körpertürmen.

d) Wegen der Symmetrie in c) kann man ein Gegenbeispiel nur dann finden, wenn $K|k$ *und* $L|k$ *beide* nicht galoissch sind. Sei $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ und $L = \mathbb{Q}(\zeta_3\sqrt[3]{2})$. K und L sind verschiedene kubische Zahlkörper ($K \subset \mathbb{R}$, $L \not\subset \mathbb{R}$) und ihr Durchschnitt aus Gradgründen daher $K \cap L = k = \mathbb{Q}$. Weiter ist $KL = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = K(\zeta_3) = K(\sqrt{-3})$ (vgl. Aufgabe 2.b)) und die Behauptung von c) gilt für diese Körper nicht:

$$(KL : K) = (K(\sqrt{-3}) : K) \leq 2 < 3 = (L : K \cap L)\,.$$

Aufgabe 5. (s)
Zusätzlich zu den Voraussetzungen von Aufgabe 4 gelte:

$$K \text{ und } L \text{ sind galoissch über } k\,.$$

Zeigen Sie:

a) KL und $K \cap L$ sind galoissch über k.

b) $G(KL|k) \hookrightarrow G(K|k) \times G(L|k)$, $\sigma \mapsto (\sigma\,|_K, \sigma\,|_L)$ ist ein Gruppenmonomorphismus.

c*) Bestimmen Sie das Bild.

d) $K \cap L = k \implies G(KL|k) \simeq G(K|k) \times G(L|k)$.

Lösung:
a) $K = k(W_f)$ und $L = k(W_g)$ sind Zerfällungskörper separabler Polynome $f, g \in k[X]$. Dann ist $KL = k(W_f \cup W_g) = W_{fg}$ Zerfällungskörper von fg. Aber Vorsicht: fg ist nicht separabel, wenn f, g gemeinsame Primteiler haben. Deshalb wählt man statt fg das Polynom $h = \mathrm{kgV}(f, g)$, welches alle Primteiler von f und g jeweils nur einmal enthält, also separabel ist und dieselben Nullstellen wir fg hat. Also ist $KL = k(W_h)$ galoissch.
b) Der Homomorphismus $\Phi : G(KL|k) \to G(K|k) \times G(L|k)$, $\sigma \mapsto (\sigma\,|_K, \sigma\,|_L)$ ist injektiv, da KL über k von K und L erzeugt wird, also $\sigma\,|_K = \mathrm{id}_K\,,\ \sigma\,|_L = \mathrm{id}_L \implies \sigma = \mathrm{id}_{KL}$ gilt.
d) Ist $K \cap L = k$, so sind gemäß Aufgabe 4.c) die Gruppen in b) gleichmächtig:

$$\#G(KL|k) = (KL : k) = (KL : L)(L : k) = (K : k)(L : k) = \#(G(K|k) \times G(L|k))\,,$$

so dass aus der Injektivität die Surjektivität folgt.
c∗) Offenbar liegt das Bild von Φ in

$$F := \{(\sigma, \tau) \in G(K|k) \times G(L|k) \mid \sigma\,|_{K\cap L} = \tau\,|_{K\cap L}\}\,.$$

Behauptung: $F = \operatorname{Im}\Phi$.
Sei dazu $(\sigma, \tau) \in F$. Setze τ fort zu $\tilde{\tau} \in G(KL|k)$ (Fortsetzungssatz) und schränke auf K ein: $\tilde{\tau}\,|_K$. Dann ist $\rho = (\tilde{\tau}\,|_K)^{-1} \circ \sigma \in G(K|K \cap L)$ wegen $\sigma\,|_{K\cap L} = \tilde{\tau}\,|_{K\cap L} = \tau\,|_{K\cap L}$. Gemäß Aufgabe 4.b) besitzt ρ eine Fortsetzung $\tilde{\rho} \in G(KL|L)$. Dann ist $\tilde{\tau} \circ \tilde{\rho} \in G(KL|k)$ das gesuchte Urbild:

$$(\tilde{\tau} \circ \tilde{\rho})\,|_K = \tilde{\tau} \circ \rho = \tilde{\tau} \circ (\tilde{\tau}\,|_K)^{-1} \circ \sigma = \sigma\,, \quad (\tilde{\tau} \circ \tilde{\rho})\,|_L \underset{\tilde{\rho}\,|_L = \mathrm{id}}{=} \tilde{\tau}\,|_L = \tau\,.$$

Algebra II

Übung 2

Aufgabe 6. (m)

a) Wiederholen Sie die Grundbegriffe über Permutationsgruppen und berichten Sie kurz über Zyklenzerlegung (siehe Algebra I, I.2.5), Erzeugungen von $\mathcal{A}_n$ (I.2.7) und $\mathcal{S}_n$ (Übungen zur Algebra I, Aufgabe 20).

b) Sei $G \leq \mathcal{S}_p$ eine Permutationsgruppe von Primzahlgrad p. Enthält G ein Element σ der Ordnung p und eine Transposition τ, so ist $G = \mathcal{S}_p$.

Lösung:
b) Ganz allgemein ist die Ordnung einer Permutation der kgV der Zyklenlängen in seiner Zyklenzerlegung (siehe a)), also hat eine Permutation genau dann die Ordnung p, wenn sie Produkt elementfremder Zyklen der Länge p (oder ein einzelner solcher Zyklus) ist. In $\mathcal{S}_p$ gibt es keine zwei elementfremden p-Zyklen, also haben in $\mathcal{S}_p$ nur die p-Zyklen die Ordnung p.
Nach Voraussetzung enthält also G einen p-Zyklus und eine Transposition $(a_1\, a_2)$. Durch die Potenzen eines p-Zykluses σ kann jedes Element auf jedes andere in $\{1, \ldots, p\}$ abgebildet werden, also auch $\sigma^j(a_1) = a_2$ für ein j. Mit σ ist auch jede Potenz $\sigma^j \neq \mathrm{id}$ ein p-Zyklus. Damit enthält G die Transposition $\tau = (a_1\, a_2)$ und einen p-Zyklus $\rho = (a_1, a_2, \ldots, a_p)$. Wegen $\langle \rho, \tau \rangle = \mathcal{S}\{a_1, \ldots, a_p\} = \mathcal{S}_p$ (siehe a)) ist $G = \mathcal{S}_p$.

Aufgabe 7. (s)

a) Sei k ein Teilkörper von $\mathbb{R}$ und $f \in k[X]$ ein irreduzibles Polynom von Primzahlgrad p mit genau zwei nicht-reellen Nullstellen. Zeigen Sie: Die Galoisgruppe von f ist $\mathcal{S}_p$.

b) $f = X^5 - 5X^4 + 5$ hat über $\mathbb{Q}$ als Galoisgruppe die volle symmetrische Gruppe $\mathcal{S}_5$.

Lösung:
a) Als irreduzibles Polynom ist f separabel (Charakteristik 0) und der Zerfällungskörper N von f über k wird von den p verschiedenen Wurzeln von f erzeugt. Da f genau zwei nicht-reelle Wurzeln hat, werden diese von der komplexen Konjugation vertauscht und die übrigen Wurzeln bleiben fest, also operiert die komplexe Konjugation als Transposition auf den Wurzeln von f.
N enthält einen Stammkörper $K = k(\alpha)$ von f über k und daher ist $p = \deg f = (k(\alpha) : k)$ ein Teiler von $(N : k) = \#G(N|k) = \#G(f)$. Damit enthält $G(f)$ ein Element der Ordnung p (Sylowsätze) und nach Aufgabe 6.b) ist $G(f) = \mathcal{S}_p$.
b) Als Eisensteinpolynom für $p = 5$ ist f irreduzibel und daher separabel. Eine schulbekannte Kurvendiskussion zeigt: Die reelle Polynomfunktion $f(x) = x^5 - 5x^4 + 5$ hat ein nur 2 Extrema, ein lokales Minimum bei 2 mit Wert $f(2) < 0$ und ein Maximum bei 0 mit Wert $f(0) = 5 > 0$. Wegen $\lim_{x \to \pm\infty} f(x) = \pm\infty$ hat f genau drei einfache reelle Nullstellen, also zwei nicht-reelle Nullstellen in $\mathbb{C}$, so dass b) aus a) folgt.

Aufgabe 8. (s)
Geben Sie für folgende Körpererweiterungen sämtliche Zwischenkörper mit erzeugenden Elementen an:
a) $\mathbb{Q}(\zeta_6)\mathbb{Q}$ b) $\mathbb{Q}(\zeta_8)|\mathbb{Q}$ c) $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ d) $\mathbb{Q}(\sqrt{3}, \sqrt{3} + \sqrt[3]{9})|\mathbb{Q}$
e) $\mathbb{F}_p(\alpha)|\mathbb{F}_p$ mit einem algebraischen Element vom Grade s über $\mathbb{F}_p$, p eine Primzahl.

Lösung:
a) $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$ ist quadratische Erweiterung von $\mathbb{Q}$, hat also keine echten Zwischenkörper.
b) $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ (siehe Aufgabe 2.c)) ist *biquadratisch;* die Galoisgruppe ist $G \simeq G(\mathbb{Q}(i)|\mathbb{Q}) \times G(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \simeq \mathcal{V}_4$ (vgl. Aufgabe 5.d)). Es gibt also genau 3 quadratische Zwischenkörper $\mathbb{Q}(i)$,

$\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{-2})$.
c) $\mathbb{Q}(\sqrt[4]{2})$ enthält nur $\mathbb{Q}(\sqrt{2})$ als echten Zwischenkörper, wie man aus dem bekannten Zwischenkörperverband der galoisschen Hülle $\mathbb{Q}(i, \sqrt[4]{2})|\mathbb{Q}$ abliest, siehe Vorlesung, Beispiel IV.1.7.
d) $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$ ist ein Körper vom Grade 6, da $(\mathbb{Q}(\sqrt{3}) : \mathbb{Q}) = 2$, $\mathbb{Q}(\sqrt[3]{3})|\mathbb{Q}) = 3$ und $2, 3$ teilerfremd sind.
Sei L ein quadratischer Zwischenkörper. Angenommen $\sqrt{3} \notin L$. Dann ist $(L(\sqrt{3}) : \mathbb{Q}) = 4$ ein Teiler von $(K : \mathbb{Q}) = 6$, Wid. Also $\sqrt{3} \in L$ und damit $\mathbb{Q}(\sqrt{3}) = L$.
Sei nun L ein kubischer Zwischenkörper. Wäre $L \neq \mathbb{Q}(\sqrt[3]{3})$, so folgte $1 < (L(\sqrt[3]{3}) : L) \mid (K : L) = 2$. Dann wäre aber $X^3 - 3$ über L reduzibel und hätte in L eine Wurzel $\alpha \neq \sqrt[3]{3}$. $\alpha = \zeta\sqrt[3]{3} \in L \subset K$ ist nicht reell, aber $K \subset \mathbb{R}$. Wid.
Die einzigen Zwischenkörper sind also nur die beiden offensichtlichen Körper $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt[3]{3})$.
Anmerkung: Ersetzt man $\sqrt{3}$ durch $\sqrt{-3}$, so ergibt sich ein anderes Resultat, nämlich 2 weitere kubische Teilkörper.
e) $K = \mathbb{F}_p(\theta)|\mathbb{F}_p$ ist galoissch vom Grade s mit Galoisgruppe $G = \langle\sigma\rangle$ zyklisch von der Ordnung s, erzeugt von $\sigma : K \to K\,,\ \alpha \mapsto \alpha^p$ (siehe Vorlesung Algebra I, Satz III.2.15). Damit existiert zu jedem $t \mid s$ genau ein Zwischenkörper L_t vom Grade t über $\mathbb{F}_p$. Es ist $G(K|L_t) = \langle\sigma^t\rangle$, denn $\#\langle\sigma^t\rangle = \operatorname{ord}\sigma^t = \frac{s}{t} = (K : L_t)$. K hat die $\mathbb{F}_p$-Basis $1, \theta, \theta^2, \ldots, \theta^{s-1}$; daher wird $L_t = \operatorname{Fix}(U_t) = \operatorname{Fix}\langle\sigma^t\rangle$ erzeugt von (siehe Bem. IV.1.6)

$$S_{U_t}(\theta^\nu) = \sum_{i=0}^{s/t} \sigma^{ti}(\theta^\nu) = \sum_{i=0}^{s/t} \theta^{\nu p^{ti}} \quad (0 \leq \nu < s)\,.$$

In diesem Fall, in dem die Zwischenkörper als die eindeutig bestimmten Körper $L_t = \mathbb{F}_{p^t}$ von p^t Elementen unabhängig von θ festliegen, kann man auch eine von θ unabhängige Erzeugung angeben:

$$\mathbb{F}_{p^t} = \mathbb{F}_p(\zeta_{p^t-1}) \text{ mit einer primitiven } (p^t-1)\text{-ten Einheitswurzel}$$

denn $\mathbb{F}_{p^t}^\times = \langle\zeta_{p^t-1}\rangle$ (siehe Algebra I, Satz III.2.15).

Aufgabe 9. (s)
Sei $\zeta_n \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Die komplexe Konjugation eingeschränkt auf $K_n := \mathbb{Q}(\zeta_n)$ ist ein $\mathbb{Q}$-Automorphismus $c \in G(K_n|\mathbb{Q})$. Der Fixkörper K_n^+ heißt *maximal-reeller* Teilkörper von K_n.

a) Bestimmen Sie erzeugende Elemente für $K_n^+|\mathbb{Q}$.

b) Berechnen Sie das Minimalpolynom f_{ζ_n, K_n^+} von ζ_n über K_n^+.

c) Bestimmen Sie ein primitives Element für $K_n^+|\mathbb{Q}$.

Lösung:
a) $G := G(K_n|K_n^+) = \langle c\rangle = \{\mathrm{id}, c\}$. ζ_n^ν $(0 \leq \nu < \varphi(n))$ bildet eine $\mathbb{Q}$,-Basis von K_n, also bilden die G-Spuren $S_G(\zeta_n^\nu) = \zeta_n^\nu + c(\zeta_n^\nu) = \zeta_n^\nu + \bar{\zeta}_n^\nu$ $(0 \leq \nu < \varphi(n))$ ein $\mathbb{Q}$-Erzeugendensystem von K_n^+.
b) $K_n = K_n^+(\zeta_n)$ und $(K : K_n^+) = \#G(K_n|K_n^+) = 2$, also ist f_{ζ_n, K_n^+} quadratisch und daher

$$f_{\zeta_n, K_n^+} = X^2 - \mathcal{S}_{K_n|K_n^+}(\zeta_n)X + \mathcal{N}_{K_n|K_n^+}(\zeta_n) = X^2 - (\zeta_n + \bar{\zeta}_n)X + \zeta_n\bar{\zeta}_n = X^2 - 2\mathrm{Re}\,\zeta_n \cdot X + 1\,.$$

c) $f_{\zeta_n, K_n^+} \in \mathbb{Q}(\mathrm{Re}\,\zeta_n))[X]$, also gilt $(K_n : \mathbb{Q}(\mathrm{Re}\,\zeta_n)) \leq 2 = (K_n : K_n^+)$, und wegen $\mathbb{Q}(\mathrm{Re}\,\zeta_n) = \mathbb{Q}(\zeta_n + \bar{\zeta}_n) \subset K_n^+$ daher die Gleichheit $\mathbb{Q}(\zeta_n + \bar{\zeta}_n) = K_n^+$.

Aufgabe 10. (s)
Sei $n \in \mathbb{N}_+$, $\zeta_n \in \mathbb{C}$ eine primitive n-te Einheitswurzel und $\Phi_n = f_{\zeta_n,\mathbb{Q}}$ das n-te *Kreisteilungspolynom.* Zeigen Sie:

a) $\Phi_{2m}(X) = \Phi_m(-X)$ für ungerades $m \in \mathbb{N}$, $m > 1$.

b) $\Phi_n = \mathrm{ggT}\{1 + X^{n/p} + X^{2n/p} + \ldots + X^{(p-1)n/p} \mid p \text{ Primteiler von } n\}$.
[Tipp: $\frac{X^n-1}{X^{n/p}-1} \in \mathbb{Q}[X]$.]

c) Berechnen Sie Φ_{p^ν} (p Primzahl), Φ_6 und Φ_{30}.

Lösung:
a) $2, m$ teilerfremd $\implies -\zeta_m$ ist primitive $2m$-te Einheitswurzel. $-\zeta_m$ ist Wurzel von $\Phi_m(-X)$ und mit Φ_m ist auch $\Phi_m(-X)$ irreduzibel, also ist $\Phi_m(-X)$ das Minimalpolynom von $-\zeta_m$ – falls es normiert ist. Dies ist für $m > 1$ richtig, denn dann ist $\deg \Phi_m = \varphi(m)$ gerade und $\Phi_m(-X)$ normiert, also $\Phi_m(-X) = \Phi_{2m}(X)$. (Für $m = 1$ ist dies falsch: $\Phi_2(X) = X+1 \neq X-1 = \Phi_1(X)$.)
b) $\Psi_n := \mathrm{ggT}\{1+X^{n/p}+X^{2n/p}+\ldots+X^{(p-1)n/p} \mid p \text{ Primteiler von } n\}$ ist ein normiertes Polynom aus $\mathbb{Q}[X]$. Also ist $\Psi_n = f_{\zeta_n,\mathbb{Q}} = \prod_{\mathrm{ord}\,\zeta=n}(X-\zeta)$, wenn gezeigt ist:
1) Ψ_n ist separabel, hat keine mehrfachen Wurzeln.
2) Die Wurzeln von Ψ_n sind genau die primitiven n-ten Einheitswurzeln.
ad 1) Es ist $\frac{X^p-1}{X-1} = 1 + X + X^2 + \ldots + X^{p-1}$, also nach Einsetzung von $X^{n/p}$

$$\frac{X^n-1}{X^{n/p}-1} = 1 + X^{n/p} + X^{2n/p} + \ldots + X^{(p-1)n/p} =: \Psi_{n,p}\,.$$

Also ist $\Psi_n = \mathrm{ggT}\{\Psi_{n,p} \mid p \text{ teilt } n\}$. Ist $n > 1$ und p irgendein Primteiler, so folgt $\Psi_n \mid \Psi_{n,p} \mid X^n - 1$. Da $X^n - 1$ separabel ist, muss es auch Ψ_n sein.
ad 2) Da $X^n - 1$ separabel ist, sind die Nullstellen von $\Psi_{n,p} = \frac{X^n-1}{X^{n/p}-1}$ genau die Nullstellen von $X^n - 1$, die keine Nullstellen von $X^{n/p} - 1$ sind:

$$\Psi_{n,p}(\zeta) = 0 \iff \zeta^n = 1 \ \wedge\ \zeta^{n/p} \neq 1\,,$$

und folglich

$$\bigwedge_{p|n} \Psi_{n,p}(\zeta) = 0 \iff \zeta^n = 1 \ \wedge\ \bigwedge_{p|n} \zeta^{n/p} \neq 1 \iff \mathrm{ord}\,\zeta = n\,.$$

Nun sind die gemeinsamen Nullstellen der $\Psi_{n,p}$ genau die Nullstellen des ggT (Primzerlegung über dem algebraischen Abschluss $\tilde{\mathbb{Q}}$ betrachten), und daher sind die Nullstellen von Ψ_n genau die primitiven n-ten Einheitswurzeln.
c) Nach b) ist

$$\Phi_{p^\nu} = \Psi_{p^\nu,p} = 1 + X^{p^{\nu-1}} + X^{2p^{\nu-1}} + \ldots + X^{(p-1)p^{\nu-1}}\,.$$

Als wichtigen Spezialfall halten wir fest

$$\Phi_p = 1 + X + X^2 + \ldots + X^{p-1}\,.$$

Daraus ergibt sich $\Psi_{n,p} = \Phi_p(X^{n/p})$ und b) nimmt folgende Form an:

$$\Phi_n = \mathrm{ggT}\{\Phi_p(X^{n/p}) \mid p \text{ teilt } n\}\,.$$

Nun zu den konkreten Beispielen: $\Phi_6(X) = \Phi_3(-X) = X^2 - X + 1$. $\Phi_{30} = \Phi_{15}(-X)$ mit

$$\Phi_{15} = \mathrm{ggT}\{\Phi_5(X^3), \Phi_3(X^5)\} = \mathrm{ggT}(1 + X^5 + X^{10}, 1 + X^3 + X^6 + X^9 + X^{12})\,.$$

Die Berechnung des ggT mit dem euklidischen Algorithmus ergibt

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1\,,\ \Phi_{30} = \Phi_{15}(-X) = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1\,.$$

Algebra II
Übung 3

Aufgabe 11. (m)
Sei p eine Primzahl $p \neq 2$ und $s \in \mathbb{N}_+$. Zeigen Sie:

a) Die kanonische Projektion $\mathbb{Z}/p^s\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$, $a + p^s\mathbb{Z} \mapsto a + p\mathbb{Z}$, induziert einen Gruppenepimorphismus $\mathcal{P}(p^s) \twoheadrightarrow \mathcal{P}(p) = \mathbb{F}_p^\times$.

b) Ist $a + p\mathbb{Z}$ ein erzeugendes Element von $\mathbb{F}_p^\times$ (eine sog. *Primitivwurzel* modulo p), so hat $a + p^s\mathbb{Z}$ in $\mathcal{P}(p^s)$ eine Ordnung d mit $p - 1 \mid d \mid (p-1)p^{s-1}$.

c) In $\mathcal{P}(p^s)$ gibt es ein Element der Ordnung $p - 1$.

Lösung:
a) $a + p\mathbb{Z} \in \mathcal{P}(p) \iff p \nmid a \iff a + p^s\mathbb{Z} \in \mathcal{P}(p^s)$.
Aber Vorsicht: $R \twoheadrightarrow S$ unitärer Ringepimorphismus impliziert *nicht* $R^\times \twoheadrightarrow S^\times$ surjektiv. Gegenbeispiel: $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$ für $p > 3$.
b) Nach Voraussetzung hat $a + p\mathbb{Z} \in \mathbb{F}_p^\times$ die Ordnung $\#\mathbb{F}_p^\times = p - 1$. Sei nun d die Ordnung von $a + p^s\mathbb{Z}$. Dann gilt $p \mid p^s \mid a^d - 1 \implies p - 1 = \operatorname{ord}(a + p\mathbb{Z}) \mid d$, und nach dem Satz von Lagrange gilt natürlich $d \mid \#\mathcal{P}(p^s) = (p-1)p^{s-1}$.
c) Da $\mathbb{F}_p^\times$ zyklisch ist, gibt es ein a wie in b) und es gilt dann $\operatorname{ord}(a + p^s\mathbb{Z}) = (p-1)p^\mu$ mit $0 \leq \mu < s$. Dann hat $a^{p^\mu} + p^s\mathbb{Z}$ die Ordnung $p - 1$.

Aufgabe 12. (s)

a) Beweisen Sie induktiv für Primzahlen $p \neq 2$:

$$(1+p)^{p^r} = 1 + ap^{r+1} \quad \text{mit } a \in \mathbb{Z}\,,\ p \nmid a\,.$$

b) Beweisen Sie induktiv $5^{2^r} = 1 + a \cdot 2^{r+2}$ mit $a \in \mathbb{Z}$, $2 \nmid a$.

c) Folgern Sie für Primzahlen p: In $\mathcal{P}(p^s)$ hat $1 + p + p^s\mathbb{Z}$ die Ordnung p^{s-1} $(p \neq 2)$ und $5 + 2^s\mathbb{Z}$ die Ordnung 2^{s-2} $(p = 2)$.

Lösung:
a) $r = 0$ ist klar. $r \to r + 1$:

$$\begin{aligned}
(1+p)^{p^{r+1}} &= (1 + ap^{r+1})^p = \sum_{i=0}^{p} \binom{p}{i} (a + p^{r+1})^i \\
&= 1 + p \cdot ap^{r+1} + \underbrace{\frac{p(p-1)}{2} \cdot a^2 p^{2r+2}}_{\equiv 0 \bmod p^{2r+3}\ (p \neq 2)} + \underbrace{\sum_{i=3}^{p} \binom{p}{i} a^i p^{ir+i}}_{\equiv 0 \bmod p^{r+3}} \\
&= 1 + ap^{r+2} + bp^{r+3} = 1 + (a + bp)p^{r+2} \text{ mit } a + bp \in \mathbb{Z}\,,\ a + bp \equiv a \not\equiv 0 \bmod p\,.
\end{aligned}$$

b) Genauso.
c) Nach a) gilt für $1 + \bar{p} = 1 + p + p^s\mathbb{Z} \in \mathcal{P}(p^s)$:

$$\begin{aligned}
(1+p)^{p^{s-1}} &= 1 + ap^s \equiv 1 \bmod p^s &&\implies \operatorname{ord}(1+\bar{p}) \mid p^{s-1}\,, \\
(1+p)^{p^{s-2}} &= 1 + a'p^{s-1} \not\equiv 1 \bmod p^s &&\implies \operatorname{ord}(1+\bar{p}) \nmid p^{s-2}\,,
\end{aligned}$$

also $\operatorname{ord}(1 + \bar{p}) = p^{s-1}$ für $p \neq 2$. Analog schließt man für $p = 2$.

Aufgabe 13. (s)
Zeigen Sie:

a) Für Primzahlen $p \neq 2$ ist $\mathcal{P}(p^s)$ zyklisch.

b) Für $s \geq 3$ ist $\mathcal{P}(2^s) = \langle -\bar{1} \rangle \times \langle \bar{5} \rangle$ direktes Produkt zweier zyklischer Gruppen der Ordnung 2 und 2^{s-2}.

Lösung:
a) Nach den vorangehenden Aufgaben gibt es in $\mathcal{P}(p^s)$ ein Element w der Ordnung $p-1$ und $v = 1 + \bar{p}$ der Ordnung p^{s-1} ($p \neq 2$). Da $p-1$ und p^{s-1} teilerfremd sind, hat vw die Ordnung $(p-1)p^{s-1} = \#\mathcal{P}(p^s)$.
b) $\mathcal{P}(2) = \{1\}$, $\mathcal{P}(4) = \langle -\bar{1} \rangle$. Sei nun $s \geq 3$. Dann hat $\bar{5} \in \mathcal{P}(2^s)$ die Ordnung 2^{s-2} und $-\bar{1}$ die Ordnung 2. Bleibt nur zu zeigen, dass $-\bar{1} \notin \langle \bar{5} \rangle$ gilt.
Annahme: $-1 \equiv 5^\nu \bmod 2^s$ für ein $0 \leq \nu < 2^{s-2}$. Dann folgt

$$1 \equiv 5^{2\nu} \bmod 2^s \implies \operatorname{ord}(\bar{5}) = 2^{s-2} \mid 2\nu \implies \nu = 2^{s-3}\,.$$

Also $-1 \equiv 5^{2^{s-3}} \bmod 2^s$. Andererseits wissen wir $5^{2^{s-3}} = 1 + a \cdot 2^{s-1}$ für ein $a \in \mathbb{Z}$ und daher $-1 \equiv 1 \bmod 2^{s-1}$, Wid. für $s - 1 \geq 2$.

Algebra II
Übung 4

Aufgabe 14. (m)
Sei $p \neq 2$ eine Primzahl und $s \in \mathbb{N}_+$.

a) Zeigen Sie, dass $\mathbb{Q}(\mu_{p^s})|\mathbb{Q}$ genau einen quadratischen Teilkörper L enthält. L ist unabhängig von s.

b) Zu welcher Untergruppe U von $G(\mathbb{Q}(\mu_{p^s})|\mathbb{Q})$ gehört L im Sinne der Galoistheorie?

c) Bestimmen Sie erzeugende Elemente für $L|\mathbb{Q}$.

d) Beschreiben Sie den nicht-trivialen Automorphismus σ von L.

Lösung:
a) $G := G(\mathbb{Q}(\mu_{p^s})|\mathbb{Q}) \simeq \mathcal{P}(p^s)$ ist für $p \neq 2$ zyklisch (nach Aufgabe 13.a)). Also besitzt $\mathbb{Q}(\mu_{p^s}|\mathbb{Q})$ für jeden Teiler von $(\mathbb{Q}(\mu_{p^s}) : \mathbb{Q}) = \varphi(p^s) = (p-1)p^{s-1}$ genau einen Zwischenkörper L_d vom Grade d über $\mathbb{Q}$. Da $p-1$ gerade ist, ist $d = 2$ ein Teiler und es gibt einen genau quadratischen Teilkörper L in $\mathbb{Q}(\mu_p) \subset \mathbb{Q}(\mu_{p^s})$ für alle s.
b) Zum quadratischen Teilkörper $L \in \mathbb{Q}(\mu_p)$ gehört die Untergruppe $U \leq G$ vom Index 2: $U = \{\sigma^2 \mid \sigma \in G\} \simeq \mathbb{F}_p^{\times 2}$.
c) Bestimmung von L als Teilkörper in $\mathbb{Q}(\mu_p)$. L wird erzeugt von den U-Spuren der $\mathbb{Q}$-Basis $1, \zeta_p, \ldots, \zeta_p^{p-2}$ von $\mathbb{Q}(\mu_p)$:

$$s_j := S_U(\zeta_p^j) = \sum_{\tau \in U} \tau \zeta_p^j \qquad (0 \leq j < p-1)\,.$$

Da L quadratisch ist, wird L bereits von einer dieser Spuren erzeugt, und zwar von jeder, die nicht in $\mathbb{Q}$ liegt. $s_0 = \#U = \frac{p-1}{2} \in \mathbb{Q}$, aber alle anderen Spuren s_j $(1 \leq j \leq p-2)$ liegen nicht in $\mathbb{Q}$. Begründung: Alle $\zeta_p^j \neq 1$ sind primitive p-te Einheitswurzeln, also untereinander konjugiert: $\zeta_p^j = \rho\zeta_p$ für ein $\rho \in G(\mathbb{Q}(\mu_p)|\mathbb{Q})$ und daher auch $\rho s_1 = \sum_{\tau \in U} \rho\tau\zeta_p \underset{U \lhd G}{=} \sum_{\tau \in U} \tau\rho\zeta_p = s_j$. Also $s_1 \in \mathbb{Q} \iff s_j \in \mathbb{Q}$. L wird daher erzeugt von

$$s_1 = \mathcal{S}_U(\zeta_p) = \sum_{\tau \in U} \tau\zeta_p = \sum_{\bar{\alpha} \in \mathbb{F}_p^{\times 2}} \zeta_p^{\alpha} = \sum_{0 \leq i < \frac{p-1}{2}} \zeta_p^{a^{2i}}\,,$$

wobei a eine Primitivwurzel modulo p sei, also $\langle a \rangle = \mathbb{F}_p^{\times} \simeq G(\mathbb{Q}(\mu_p)|\mathbb{Q})$ und $\langle a^2 \rangle = \mathbb{F}_p^{\times 2} \simeq U$.
d) $G(\mathbb{Q}(\mu_p)|\mathbb{Q}) \simeq \mathbb{F}_p^{\times}$ wird erzeugt von $\sigma : \zeta \mapsto \zeta_p^a$ $(\zeta \in \mu_p)$, also ist $\sigma\,|_L$ Erzeugendes von $G(L|\mathbb{Q})$. $\sigma\,|_L$ wirkt auf das Erzeugende $\mathcal{S}_U(\zeta_p)$ durch

$$\mathcal{S}_U(\zeta_p) = \sum_{0 \leq i < \frac{p-1}{2}} \zeta_p^{a^{2i}} \mapsto \sigma(\mathcal{S}_U(\zeta_p)) = \mathcal{S}_U(\zeta_p^a) = \sum_{0 \leq i < \frac{p-1}{2}} \zeta_p^{a^{2i+1}}\,.$$

Aufgabe 15. (s)
Bestimmen Sie in $\mathbb{Q}(\mu_p)$ für $p = 5, 7, 11, 13$ den quadratischen Teilkörper L in der Form $\mathbb{Q}(\sqrt{d})$. Was fällt Ihnen auf?

Lösung:
Nach Aufgabe 14 wird L erzeugt von $w := S_U(\zeta_p)$. Da L quadratisch ist, genügt w einer quadratischen Gleichung, und zwar

$$f_{w,\mathbb{Q}} = X^2 - \mathcal{S}(w)X + \mathcal{N}(w) \text{ mit } \mathcal{S} = \mathcal{S}_{L|\mathbb{Q}}\,,\ \mathcal{N} = \mathcal{N}_{L|\mathbb{Q}}\,.$$

Man löst die quadratische Gleichung $0 = f_{w,\mathbb{Q}}(w)$ nach w auf

$$w = \frac{1}{2}\mathcal{S}(w) \pm \sqrt{\frac{1}{4}\mathcal{S}(w)^2 - \mathcal{N}(w)}$$

und findet

$$L = \mathbb{Q}(\sqrt{\mathcal{S}(w)^2 - 4\mathcal{N}(w)})\,.$$

Damit ist das Problem auf die Berechnung von Spur und Norm von w reduziert.
1. Spur: $\mathcal{S}_{L|\mathbb{Q}}(w) = \mathcal{S}_{L|\mathbb{Q}}(\mathcal{S}_U(\zeta_p)) = \mathcal{S}_{L|\mathbb{Q}} \circ \mathcal{S}_{\mathbb{Q}(\mu_p)|L}(\zeta_p) = \mathcal{S}_{\mathbb{Q}(\mu_p)|\mathbb{Q}}(\zeta_p) = -1$, denn $f_{\zeta_p,\mathbb{Q}} = \Phi_p(X) = 1 + X + \ldots + X^{p-2} + X^{p-1}$ hat den zweithöchsten Koeffizienten $+1$.
2. Bereits in Aufgabe 14.d) haben wir Vorarbeit geleistet. Für eine Primitivwurzel a modulo p und $\zeta := \zeta_p$ gilt:

$$w = \mathcal{S}_U(\zeta_p) = \sum_{0\le i<\frac{p-1}{2}} \zeta^{a^{2i}}\,, \quad \sigma(w) = \sigma(\mathcal{S}_U(\zeta_p)) = \sum_{0\le i<\frac{p-1}{2}} \zeta^{a^{2i+1}}\,.$$

Unter Beachtung von 1. gilt $w + \sigma(w) = \mathcal{S}_{\mathbb{Q}(\mu_p)|\mathbb{Q}}(w) = -1 \iff \sigma(w) = -1 - w$ und daher $\mathcal{N}(w) = w(-1-w)$.
Wir behandeln nun die konkreten Fälle:
$\underline{p = 5}$: $a = 2$ ist Primitivwurzel modulo 5: $p - 1 = 4$, $2^2 = 4 \equiv -1$. Also

$$\begin{aligned} &w = \zeta + \zeta^4\,,\ \sigma(w) = \zeta^2 + \zeta^8 = \zeta^2 + \zeta^3\,,\\ &\mathcal{N}(w) = (\zeta + \zeta^4)(\zeta^2 + \zeta^3) = \zeta^3 + \zeta^4 + \zeta + \zeta^2 = \mathcal{S}_{\mathbb{Q}(\mu_5)|\mathbb{Q}}(\zeta) = -1\,,\\ &L = \mathbb{Q}(\sqrt{\mathcal{S}(w)^2 - 4\mathcal{N}(w)}) = \mathbb{Q}(\sqrt{1+4}) = \mathbb{Q}(\sqrt{5})\,. \end{aligned}$$

$\underline{p = 7}$: $a = 3$ ist Primitivwurzel modulo 7: $p - 1 = 6$, $3^2 \equiv 2$, $3^3 \equiv -1$. Also

$$\begin{aligned} w &= \zeta + \zeta^2 + \zeta^4\,,\ \sigma(w) = \zeta^3 + \zeta^6 + \zeta^5\,,\\ \mathcal{N}(w) &= (\zeta + \zeta^2 + \zeta^4)(\zeta^3 + \zeta^6 + \zeta^5)\\ &= \zeta^4 + \zeta^6 + 1 \ + \ \zeta^5 + 1 + \zeta \ + \ 1 + \zeta^2 + \zeta^3 = 3 + \mathcal{S}_{\mathbb{Q}(\mu_7)|\mathbb{Q}}(\zeta) = 3 - 1 = 2\,,\\ L &= \mathbb{Q}(\sqrt{\mathcal{S}(w)^2 - 4\mathcal{N}(w)}) = \mathbb{Q}(\sqrt{1-8}) = \mathbb{Q}(\sqrt{-7})\,. \end{aligned}$$

$\underline{p = 11}$: $a = 2$ ist Primitivwurzel modulo 11: $p - 1 = 10$, $2^2 = 4$, $2^5 \equiv -1$. Also

$$\begin{aligned} w &= \zeta + \zeta^4 + \zeta^5 + \zeta^9 + \zeta^3\,,\ \sigma(w) = \zeta^2 + \zeta^8 + \zeta^{10} + \zeta^7 + \zeta^6\,,\\ \mathcal{N}(w) &= (\zeta + \zeta^4 + \zeta^5 + \zeta^9 + \zeta^3)(\zeta^2 + \zeta^8 + \zeta^{10} + \zeta^7 + \zeta^6)\\ &= \ldots = 5 + 2\mathcal{S}_{\mathbb{Q}(\mu_{11})|\mathbb{Q}}(\zeta) = 3\,,\\ L &= \mathbb{Q}(\sqrt{\mathcal{S}(w)^2 - 4\mathcal{N}(w)}) = \mathbb{Q}(\sqrt{1-12}) = \mathbb{Q}(\sqrt{-11})\,. \end{aligned}$$

$\underline{p = 13}$: $a = 2$ ist Primitivwurzel modulo 13: $p - 1 = 12$, $2^4 \equiv 3$, $2^6 \equiv -1$. Also

$$\begin{aligned} w &= \zeta + \zeta^4 + \zeta^3 + \zeta^{12} + \zeta^9 + \zeta^{10}\,,\ \sigma(w) = \zeta^2 + \zeta^8 + \zeta^6 + \zeta^{11} + \zeta^5 + \zeta^7\,,\\ \mathcal{N}(w) &= w\sigma(w) = \ldots = 3\mathcal{S}_{\mathbb{Q}(\mu_{13})|\mathbb{Q}}(\zeta) = -3\,,\\ L &= \mathbb{Q}(\sqrt{\mathcal{S}(w)^2 - 4\mathcal{N}(w)}) = \mathbb{Q}(\sqrt{1+12}) = \mathbb{Q}(\sqrt{13})\,. \end{aligned}$$

Es ist unübersehbar, dass in diesen 4 Fällen der quadratische Teilkörper von $\mathbb{Q}(\mu_p)$ von der Form $\mathbb{Q}(\sqrt{\pm p})$ ist. Kein Zufall! Siehe Aufgabe 21.

Aufgabe 16. (m)
Sei k ein Körper. zeigen Sie:

a) Ist $f \in k[X]$ irreduzibel und inseparabel, so ist $\operatorname{char} k = p$ eine Primzah und $f = g(X^p)$ mit $g \in k[X]$ irreduzibel.

b) Sei $K|k$ eine endliche Körpererweiterung, $\alpha \in K$ und $f_{\alpha,k}$ inseparabel. Dann ist $\operatorname{char} k = p$ eine Primzahl und es gibt ein $\nu \in \mathbb{N}_+$ mit

$$f_{\alpha,k} = f_{\alpha^{p^\nu},k}(X^{p^\nu}) \quad \text{und} \quad f_{\alpha p^\nu,k} \text{ separabel.}$$

c) $K_s := \{\alpha \in K \mid \alpha \text{ separabel über } k\}$ ist ein Teil*körper* von K.

Lösung:
a) Wiederholung (Algebra I, Prop. III.2.4 d)). Wäre g reduzibel, so auch $g(X^p) = f$.
b) $f := f_{\alpha,k}$ ist irreduzibel. Ist also f inseparabel, so exisitiert nach a) ein irreduzibles $f_1 \in k[X]$ mit $f = f_1(X^p)$. Ist f_1 wiederum inseparabel, so kann man dies wiederholen und erhält $f_1 = f_2(X^p)$, bzw. $f = f_1(X^p) = f_2(X^{p^2})$ mit irreduziblem f_2. Induktiv folgt die Existenz von irreduziblen Polynomen $f_\nu \in k[X]$ mit $f = f_\nu(X^{p^\nu})$. Dieser Prozess endet, wenn erstmalig f_ν *separabel* ist. Dieser Fall muss eintreten, da f endlichen Grad hat und die Grade der f_ν abnehmen.
Das so gefundene f_ν ist normiert und irreduzibel und es gilt $0 = f(\alpha) = f_\nu(\alpha^{p^\nu})$, also ist f_ν das Minimalpolynom von α^{p^ν} über k.
c) beruht auf der Charakterisierung der Separabiliät durch die Invariante $\mu(K|k)$, die Anzahl der k-Monomorphismen von $K \to \tilde{k}$, und deren Multiplikativität in Körpertürmen (siehe Algebra I, Prop. III.2.2). Dies hatte zur Folge α, β separabel $\iff k[\alpha,\beta]|k$ separabel (siehe Algebra I, Prop. III.2.5). Sind also $\alpha, \beta \in K_s$, so folgt $k[\alpha,\beta] \subset K_s$ und K_s ist abgeschlossen gegenüber den Körperoperationen.

Aufgabe 17. (s)
Sei $K|k$ eine endliche Erweiterung und $\alpha \in K$. Zeigen Sie:

a) Für $\alpha \notin k$ sind äquivalent:

   i) $\mu(k(\alpha)|k) = 1$.
   ii) $f_{\alpha,k} = (X-\alpha)^n$ für ein $n \in \mathbb{N}_+$.
   iii) $\operatorname{char} k = p$ Primzahl und $f_{\alpha,k} = (X-\alpha)^{p^\nu}$ für ein $\nu \in \mathbb{N}_+$.
   iv) $\operatorname{char} k = p$ Primzahl und $\alpha^{p^\nu} \in k$ für ein $\nu \in \mathbb{N}_+$

b) Für $K \neq k$ sind äquivalent:

   i) $\mu(K|k) = 1$
   ii) $\operatorname{char} k = p$ Primzahl und für jedes $\alpha \in K$ existiert ein $\nu \in \mathbb{N}$ mit $\alpha^{p^\nu} \in k$.
   iii) $K_s = k$, d. h. $\alpha \in K$ separabel über $k \implies \alpha \in k$.

   [Eine derartige echte Erweiterung $K|k$ heißt *rein inseparabel.]*

c) Sei $K|k$ rein inseparabel. Dann gilt:
   1) $\operatorname{char} k = p$ Primzahl.
   2) $(K:k) = p^m$ für ein $m \in \mathbb{N}_+$.
   3) $\alpha^{(K:k)} \in k$ für alle $\alpha \in K$.

d) Sei $K|k$ eine beliebige endliche Erweiterung. Dann gilt:

$K = K_s|k$ separabel oder

$K|K_s$ rein inseparabel, $(K : K_s) = p^m$ mit $p = \operatorname{char} k$ Primzahl und $(K_s : k) = \mu(K|k)$.

Lösung:
a) i) $\Leftrightarrow$ ii): $\mu(k(\alpha)|k)$ ist die Zahl der verschiedenen Wurzeln von $f_{\alpha,k}$ in $\tilde{k}$ (siehe Algebra I, Prop. III.2.2 c)).
ii) $\Rightarrow$ iii): $f_{\alpha,k}$ ist inseparabel (wegen $\alpha \notin k$ und folglich $n = (k(\alpha) : k) \geq 2$), also $\operatorname{char} k = p$ und daher gilt für $n = p^\nu m$ mit $p \nmid m$

$$f_{\alpha,k} = (X - \alpha)^{p^\nu m} = (X^{p^\nu} - \alpha^{p^\nu})^m .$$

Dann muss $g(X) := (X - \alpha^{p^\nu})^m$ auch irreduzibel sein über k. Wegen $p \nmid m = \deg g$, muss g dann separabel sein (siehe 16.a)) und daher $m = 1$: $f_{\alpha,k} = (X - \alpha)^{p^\nu}$.
iii) $\Rightarrow$ iv): $(X - \alpha)^{p^\nu} = X^{p^\nu} - \alpha^{p^\nu} \in k[X]$.
iv) $\Rightarrow$ ii): α Wurzel von $X^{p^\nu} - \alpha^{p^\nu} \implies f_{\alpha,k} \mid (X - \alpha)^{p^\nu} \implies$ ii).
b) i) $\Leftrightarrow$ ii): Wegen $K \neq k$ und der Multiplikativität von μ folgt aus a): $\mu(K|k) = 1 \iff \bigwedge_{\alpha \in K} \mu(k(\alpha)|k) = 1 \underset{K \neq k}{\iff}$ ii).
ii) $\Rightarrow$ iii): $\alpha \in K \setminus k \implies \alpha^{p^\nu} \in k \underset{a)}{\implies} \mu(k(\alpha)|k) = 1 \implies k(\alpha)|k$ inseparabel $\implies \alpha \notin K_s$.
iii) $\Rightarrow$ ii): Wegen $K \neq k$ existiert ein $\alpha \in K \setminus k \underset{iii)}{\implies} \alpha \notin K_s \implies \alpha$ inseparabel über $k \underset{\text{a)}}{\implies} \operatorname{char} k = p$ Primzahl und $f_{\alpha,k} = f_{\alpha^{p^\nu},k}(X^{p^\nu})$ mit separablem $f_{\alpha^{p^\nu},k}$. Dann ist aber $\alpha^{p^\nu} \in K_s = k$.
c) 1) bereits bewiesen.
ad 2): $K|k$ endlich, also $K = k[\alpha_1, \ldots, \alpha_r]$ endlich erzeugt algebraisch. $K|k$ rein inseparabel $\implies k_i := k[\alpha_1, \ldots, \alpha_i]|k_{i-1}$ rein inseparabel $\implies (k_i : k_{i-1}) = \deg f_{\alpha_i,k_{i-1}} \underset{a)}{=} p^{\nu_i} \implies (K : k)$ p-Potenz.
ad 3): Für alle $\alpha \in K$ gibt es ein $\nu \in \mathbb{N}$ mit $f_{\alpha,k} = (X - \alpha)^{p^\nu}$, also $\alpha^{p^\nu} \in k$ und $p^\nu = (k(\alpha) : k) \mid (K : k) = p^m \implies \alpha^{p^m} \in k$.
d) Sei $K \neq K_s$, dann ist $K|K_s$ rein inseparabel, denn:

$$\begin{aligned}
&\alpha \in K \text{ separabel über } K_s(!)\\
&\implies \alpha \text{ separabel über } L := k[\alpha_1, \ldots, \alpha_r]\,,\ \alpha_i \in K_s \text{ separabel über } k\\
&\implies \mu(k[\alpha]|k) = \mu(k[\alpha]|L)\mu(L|k) = (k[\alpha] : L)(L : k) = (k[\alpha] : k)\\
&\implies \alpha \text{ separabel über } k \iff \alpha \in K_s
\end{aligned}$$

Der Rest ist dann klar, denn nach b) ist $(K : K_s) = p^m$ mit $\operatorname{char} k = p$ und

$$(K_s : k) = \mu(K_s|k) = \underbrace{\mu(K|K_s)}_{=1} \cdot \mu(K_s|k) = \mu(K|k)\,.$$

Algebra II
Übung 5

Aufgabe 18. (s)
Berechnen Sie – unter Verwendung der Ergebnisse von Aufgabe 15 – eine primitive 5-te Einheitswurzel ζ_5 durch sukzessive Quadratwurzeln.

Lösung:
Sei ζ eine primitive 5-te Einheitswurzel. Dann ist $\mathbb{Q}(\zeta)|\mathbb{Q}$ zyklisch vom Grad $\varphi(5) = 4$. Der einzige (quadratische) Zwischenkörper ist nach Aufgabe 15 $L = \mathbb{Q}(w)$ mit $w = \zeta + \zeta^{-1}$ und w ist Wurzel von $X^2 - \mathcal{S}_{L|\mathbb{Q}}(w)X + \mathcal{N}_{L|\mathbb{Q}}(w) \underset{15.}{=} X^2 + X - 1$. Also $w = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$.
Eine Darstellung von ζ der gewünschten Art findet man, indem man das Minimalpolynom $f_{\zeta,L}$ berechnet. Wegen $(\mathbb{Q}(\zeta) : L) = 2$ ist dies $f_{\zeta,L} = X^2 - \mathcal{S}_{\mathbb{Q}(\zeta)|L}(\zeta)X + \mathcal{N}_{\mathbb{Q}(\zeta)|L}(\zeta)$. Es gilt:

$$\mathcal{S}_{\mathbb{Q}(\zeta)|L}(\zeta) = \zeta + \zeta^{-1} = w\,, \quad \mathcal{N}_{\mathbb{Q}(\zeta)|L}(\zeta) = \zeta\zeta^{-1} = 1 \implies \zeta \text{ Wurzel von } X^2 - wX + 1\,.$$

Dies ergibt

$$\zeta = \frac{w}{2} \pm \sqrt{\frac{w^2}{4} - 1} = \frac{w}{2} \pm \sqrt{\frac{-w+1}{4} - 1} = \frac{1}{2}(w \pm i\sqrt{w+3})$$

Durch die 4 Vorzeichenkombinationen in den Formeln für w und ζ erhält man (alle) vier primitiven 5-ten Einheitswurzeln:

$$\zeta^5 = 1 \ \wedge\ \zeta \neq 1 \iff \zeta = \begin{cases} \frac{1}{4}\Big(-1 + \sqrt{5} \pm i\sqrt{10 + 2\sqrt{5}}\Big) \\ \frac{1}{4}\Big(-1 - \sqrt{5} \pm i\sqrt{10 - 2\sqrt{5}}\Big) \end{cases}$$

$$\begin{aligned} \zeta &= \frac{1}{4}\Big(-1 + \sqrt{5} + i\sqrt{10 + 2\sqrt{5}}\Big) \\ \zeta^2 &= \frac{1}{4}\Big(-1 - \sqrt{5} + i\sqrt{10 - 2\sqrt{5}}\Big) \\ \zeta^{-2} &= \frac{1}{4}\Big(-1 - \sqrt{5} - i\sqrt{10 - 2\sqrt{5}}\Big) \\ \zeta^{-1} &= \frac{1}{4}\Big(-1 + \sqrt{5} - i\sqrt{10 + 2\sqrt{5}}\Big) \end{aligned}$$

Aufgabe 19. (m)
Sei $p \neq 2$ eine Primzahl. Zeigen Sie:

a) $p \equiv -1 \bmod 4 \iff \mathbb{F}_p^\times$ enthält eine primitive 4-te Einheitswurzel $\iff -1 \in \mathbb{F}_p^{\times 2}$.

b) $\mathbb{F}_p^\times = \langle a \rangle \implies \mathbb{F}_p^{\times 2} = \langle a^2 \rangle$ und $\#\mathbb{F}_p^{\times 2} = \frac{p-1}{2}$.

c) $\mathbb{F}_p^\times = \mathbb{F}_p^{\times 2} \dot\cup\, b\mathbb{F}_p^{\times 2} = \mathbb{F}_p^{\times 2} \dot\cup\, a\mathbb{F}_p^{\times 2}$ mit a wie in b) und $b \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$ beliebig.
$b = -1$ wählbar $\iff p \equiv 3 \bmod 4$

Lösung:
a) $p \equiv 1 \bmod 4 \iff 4 \mid p-1 \iff$ in der zyklischen Gruppe $\mathbb{F}_p^\times$ der Ordnung $p-1$ gibt es ein Element der Ordnung 4. Dessen Quadrat hat die Ordnung 2 und ist daher -1, also $-1 \in \mathbb{F}_p^{\times 2}$.
Umgekehrt: $-1 = a^2 \in \mathbb{F}_p^{\times 2} \underset{p\neq 2}{\Longrightarrow} \operatorname{ord} a = 4 \implies a = \zeta_4 \in \mathbb{F}_p^\times$.
b) $\mathbb{F}_p^\times = \langle a \rangle \implies \mathbb{F}_p^{\times 2} = \langle a^2 \rangle$ und $\#\mathbb{F}_p^{\times 2} = \operatorname{ord} a^2 = \frac{p-1}{2}$.
c) $(\mathbb{F}_p^\times : \mathbb{F}_p^{\times 2}) = 2$. Außerdem $\mathbb{F}_p^\times = \langle a \rangle \implies a \notin \mathbb{F}_p^{\times 2}$.
Schließlich gilt: $b = -1$ wählbar $\iff -1 \notin \mathbb{F}_p^{\times 2} \iff p \equiv 3 \bmod 4$.

Aufgabe 20. (s)
Sei $p \neq 2$ eine Primzahl, $Q := \mathbb{F}_p^{\times 2}$ die Menge der Quadrate sowie $N := \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2} = b \cdot Q$, $b \notin Q$ beliebig, die Menge der Nichtquadrate in $\mathbb{F}_p^\times$. Studieren Sie die Abbildung $+ : Q \times N \to \mathbb{F}_p$, $(\alpha, \beta) \mapsto \alpha + \beta$ und beweisen Sie:

a) $0 \in \mathbb{F}_p$ liegt im Bild der Abbildung $\iff p \equiv 3 \bmod 4$.

Genauer: Die Anzahl der Urbilder der 0 ist

$$n_0 = \begin{cases} 0 & p \equiv 1 \bmod 4 \\ \frac{p-1}{2} & p \equiv 3 \bmod 4 \end{cases}.$$

b) Alle $\gamma \in \mathbb{F}_p^\times$ haben gleich viele Urbilder.

c) Die Anzahl der Urbilder der $1 \in \mathbb{F}_p$ ist

$$n_1 = \begin{cases} \dfrac{(\frac{p-1}{2})^2}{p-1} = \dfrac{p-1}{4} & \text{für } p \equiv 1 \bmod 4. \\ \dfrac{(\frac{p-1}{2})^2 - \frac{p-1}{2}}{p-1} = \dfrac{p-3}{4} & \text{für } p \equiv 3 \bmod 4, \end{cases}$$

Lösung:
a) $0 \in$ Bild $\iff 0 = \alpha + \beta$ mit $\alpha \in Q, \beta = -\alpha \in N \implies -1 = \frac{\beta}{\alpha} \notin Q = \mathbb{F}_p^{\times 2} \iff p \equiv 3 \bmod 4$. Umgekehrt: $-1 \in N \implies 0$ hat die Urbilder $(\alpha, -\alpha)$, $\alpha \in Q$ beliebig. Also $n_0 = \#Q = \frac{p-1}{2}$.
b) Die Zerlegung $\mathbb{F}_p^\times = Q \,\dot\cup\, N$ wird bei Multiplikation mit $\delta \neq 0$ in sich überführt, wobei $\delta Q = Q, \delta N = N$ ist (wenn $\delta \in Q$) oder $\delta Q = N, \delta N = Q$ ist (wenn $\delta \in N$). Daher werden die Urbilder von γ_1 durch Multiplikation mit $\delta = \frac{\gamma_2}{\gamma_1}$ bijektiv auf die Urbilder von γ_2 abgebildet.
c) Es ist n_0 die Anzahl der Urbilder von 0 und n_1 die Anzahl der Urbilder eines jeden $\gamma \in \mathbb{F}_p^\times$. Also ist

$$n_0 + n_1 \cdot \#\mathbb{F}_p^\times = n_0 + n_1(p-1) = \#(Q \times N) = (\frac{p-1}{2})^2.$$

Mit dem in a) bestimmten n_0 errechnet man daraus das in c) angegebenen n_1.

Aufgabe 21. (s*)
Bearbeiten Sie Aufgabe 15 für beliebige Primzahlen $p \neq 2$ und beweisen Sie dadurch die dort aufgestellte Vermutung. [Tipp: Aufgabe 20.c) nutzen.]

Lösung:
Für einen allgemeinen Beweis analysiert man den Beweisgang in den Spezialfällen (Aufgabe 15): Sei $p \neq 2$ Primzahl, $\zeta := \zeta_p$ eine primitive p-te Einheitswurzel und a eine Primitivwurzel mod p, also $\langle \bar a \rangle = \mathbb{F}_p^\times \xrightarrow{\sim} G(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ und $\sigma = (\zeta_p \mapsto \zeta_p^a)$ der zugehörige erzeugende Automorphismus der Galoisgruppe. Seien Q bzw. N die Mengen der Quadrate bzw. Nichtquadrate in $\mathbb{F}_p^\times$. Dann ist der quadratische Teilkörper in $\mathbb{Q}(\zeta)$ gegeben durch $L = \mathbb{Q}(w)$ mit

$$\begin{aligned} w &= \sum_{0 \le i < \frac{p-1}{2}} \zeta^{a^{2i}} = \sum_{\alpha \in Q} \zeta^\alpha \text{ (siehe Aufgabe 14.c)}, \\ \sigma(w) &= \sum_{0 \le i < \frac{p-1}{2}} \zeta^{a^{2i+1}} = \sum_{\beta \in N} \zeta^\beta \text{ das Konjugierte über } \mathbb{Q}. \end{aligned}$$

Ebenfalls aus Aufgabe 14 ist bekannt: w ist Wurzel von $X^2 - \mathcal{S}_{L|\mathbb{Q}}(w) \cdot X + \mathcal{N}_{L|\mathbb{Q}}(w) = X^2 + X + w\sigma(w)$ und zur Bestimmung von w muss man $\mathcal{N}_{L|\mathbb{Q}}(w) = w \cdot \sigma(w)$ berechnen. Dies ist in

Aufgabe 15 für $p = 5, 7, 11, 13$ geschehen. Man erhielt für $w\sigma(w)$ eine Darstellung als Summe von Einheitswurzeln. Mit den hier benutzten Bezeichnungen gilt

$$w\sigma(w) = (\sum_{\alpha\in Q} \zeta^\alpha) \cdot (\sum_{\beta\in N} \zeta^\beta) = \sum_{(\alpha,\beta)\in Q\times N} \zeta^{\alpha+\beta} = \sum_{\gamma\in\mathbb{F}_p} n_\gamma \zeta^\gamma$$

mit $n_\gamma = \#\{(\alpha, \beta) \in Q \times N \mid \alpha + \beta = \gamma\}$. Dies sind die in Aufgabe 20 bestimmten Anzahlen.

Bevor wir die Berechnung jetzt auf der Basis von Aufgabe 20 für beliebiges $p \neq 2$ durchführen, hier ein paar Bemerkungen, wie man zu den Behauptungen von Aufgabe 20 kommt: Bei den Berechnungen von $w \cdot \sigma(w)$ in Aufgabe 15 zeigte sich, dass in den genannten Summen von Einheitswurzeln alle *primitiven* p-ten Einheitswurzeln ζ^γ gleich oft vorkamen: $n_1 = n_2 = \ldots = n_{p-1}$. Ist dies der Fall, so ist

$$w \cdot \sigma(w) = n_0 + n_1(\zeta + \zeta^2 + \ldots + \zeta^{p-1}) = n_0 + n_1 \mathcal{S}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\zeta) = n_0 - n_1\,.$$

Damit ist $\mathcal{N}_{L|\mathbb{Q}}(w) = w \cdot \sigma(w) \in \mathbb{Q}$ – wie es ja auch sein muss.
Umgekehrt ist aber aus der Tatsache $\mathcal{N}_{L|\mathbb{Q}}(w) \in \mathbb{Q}$ auch die in 20.b) behauptete Gleichheit $n_1 = \ldots = n_{p-1}$ *herleitbar:*

$$\begin{aligned}
&\mathbb{Q} \ni n_0 + n_1\zeta + n_2\zeta^2 + \ldots + n_{p-1}\zeta^{p-1} \iff \\
&\mathbb{Q} \ni n_1\zeta + n_2\zeta^2 + \ldots + n_{p-1}(-1 - \zeta - \ldots - \zeta^{p-2}) \quad \text{wegen } f_{\zeta,\mathbb{Q}} = 1 + X + X^2 + \ldots + X^{p-1} \\
&\quad = -n_{p-1} + (n_1 - n_{p-1})\zeta + (n_2 - n_{p-1})\zeta^2 + \ldots + (n_{p-2} - n_{p-1})\zeta^{p-2}
\end{aligned}$$

Da $1, \zeta, \ldots, \zeta^{p-2}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\zeta)$ ist, folgt

$$n_1 - n_{p-1} = n_2 - n_{p-1} = \ldots = n_{p-2} - n_{p-1} = 0\,, \text{ also } n_1 = n_2 = \ldots = n_{p-1}.$$

Nach diesen Zwischenbemerkungen berechnen wir nun

$$\begin{aligned}
w \cdot \sigma(w) &\underset{20.b)}{=} n_0 + n_1(\zeta + \zeta^2 + \ldots + \zeta^{p-1}) = n_0 + n_1 \mathcal{S}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\zeta) \\
&= n_0 - n_1 \underset{20.c)}{=} \begin{cases} -\frac{p-1}{4} = \frac{1-p}{4} & \text{für } p \equiv 1 \bmod 4, \\ \frac{p-1}{2} - \frac{p-3}{4} = \frac{1+p}{4} & \text{für } p \equiv 3 \bmod 4\,. \end{cases}
\end{aligned}$$

Als Wurzel von $X^2 + X + \mathcal{N}_{L|\mathbb{Q}}(w)$ erhalten wir für w (vgl. Aufgabe 15) $w = -\frac{1}{2} \pm \frac{1}{2}\sqrt{D}$ mit

$$D = 1 - 4\mathcal{N}_{L|\mathbb{Q}}(w) = 1 - 4w\sigma(w) = \begin{cases} p & \text{für } p \equiv 1 \bmod 4, \\ -p & \text{für } p \equiv 3 \bmod 4 \end{cases},$$

so dass für alle $p \neq 2$ gilt:

$$L = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{für } p \equiv 1 \bmod 4, \\ \mathbb{Q}(\sqrt{-p}) & \text{für } p \equiv 3 \bmod 4. \end{cases}$$

Aufgabe 22. (s)
Seien G, G' endliche abelsche Gruppen und $\langle \ldots, \ldots \rangle : G \times G' \to \mu$ eine nicht-ausgeartete Paarung zwischen ihnen. Man setzt dann für Untergruppen $H \leq G$

$$H^\perp := \{g' \in G' \mid \langle h, g' \rangle = 1 \text{ für alle } h \in H\}\,.$$

Zeigen Sie:

a) Es existieren nicht-ausgeartete Paarungen

$$H \times G'/H^\perp \to \mu \quad \text{und} \quad G/H \times H^\perp \to \mu\,.$$

b) Die Restriktion $\mathrm{res} : \hat{G} \to \hat{H}$, $\chi \mapsto \chi\,|_H$ hat den Kern $H^\perp$ und ist surjektiv, also

$$\hat{G}/H^\perp \xrightarrow{\sim} \hat{H}\,.$$

c) Jeder Charakter von H ist auf G fortsetzbar.

d) Es gilt $\widehat{G/H} \simeq H^\perp$.

Lösung:
a) Entsprechend der Definition von $H^\perp$ gilt $\langle h, h'\rangle = 1$ für $h \in H$, $h' \in H^\perp$ und daher sind die folgenden Paarungen wohldefiniert:

$$\begin{array}{rcl} H \times G'/H^\perp & \to & \mu\,, \\ (h, g'H^\perp) & \mapsto & \langle h, g'\rangle \end{array} \quad \text{und} \quad \begin{array}{rcl} G/H \times H^\perp & \to & \mu\,, \\ (gH, h') & \mapsto & \langle g, h'\rangle\,. \end{array}$$

Die Homomorphie in beiden Argumenten ist klar. Beide Paarungen sind nicht ausgeartet:

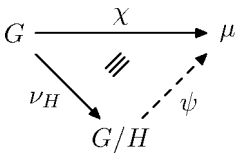
$$\bigwedge_{h\in H} \langle h, g'H^\perp\rangle = 1 \iff \bigwedge_{h\in H} \langle h, g'\rangle = 1 \iff g' \in H^\perp \iff g'H^\perp = 1_{G'/H^\perp}$$

$$\bigwedge_{g'H^\perp \in G'/H^\perp} \langle h, g'H^\perp\rangle = 1 \iff \bigwedge_{g'\in G'} \langle h, g'\rangle = 1 \iff h = 1_G \quad (\text{da } \langle \ldots, \ldots\rangle \text{ n. a.})$$

Genauso argumentiert man für die zweite Paarung:
b) In den folgenden Aufgabenteilen benutzen wir a) für die Standardpaarung $G \times \hat{G} \to \mu$, $\langle \sigma, \chi\rangle = \chi(\sigma)$. Für diese ist dann

$$H^\perp = \{\chi \in \hat{G} \mid \chi\,|_H = 1\}\,.$$

$H^\perp$ ist also der Kern der Restriktionsabbildung $\mathrm{res} : \hat{G} \to \hat{H}$. Also gilt $\hat{G}/H^\perp \hookrightarrow \hat{H}$. Gemäß a) ist $\hat{G}/H^\perp$ dual zu H, also gilt $\#(\hat{G}/H^\perp) = \#H = \#\hat{H}$ und die Injektion $\hat{G}/H^\perp \hookrightarrow \hat{H}$ muss auch surjektiv sein.
c) Damit ist dann auch $\mathrm{res} : \hat{G} \twoheadrightarrow \hat{G}/H^\perp \twoheadrightarrow \hat{H}$ surjektiv, d. h. jeder Charakter von H besitzt eine Fortsetzung auf G.
d) Jeder Charakter ψ von G/H induziert einen Charakter $\psi \circ \nu_H$ von H ($\nu_H : G \twoheadrightarrow G/H$ natürlicher Epimorphismus) und es gilt $\psi \circ \nu_H\,|_H = 1$, also $\psi \circ \nu_H \in H^\perp$.
Der so definierte Homomorphismus $\widehat{G/H} \to H^\perp$, $\psi \mapsto \psi \circ \nu_H$ ist surjektiv, wie der Homomorphiesatz zeigt:



$$\chi \in H^\perp \iff \chi\,|_H = 1 \iff H \subseteq \mathrm{Ke}\,\chi \implies \bigvee_{\psi : G/H \to \mu} \psi \circ \nu_H = \chi$$

Da nach a) $\#\widehat{G/H} = \#H^\perp$ ist, folgt aus der Surjektivität auch die Injektivität und damit d).

Algebra II
Übung 6

Aufgabe 23. (m)
Beweisen Sie Satz (2.13) über die Kummer-Paarung.

Lösung:
1) Rechtfertigungen für die Definition der Paarung:
1a) $b \in \langle a_1, \ldots, a_r\rangle k^{\times n}/k^{\times n} \implies b = a_1^{i_1} \cdot \ldots \cdot a_r^{i_r} \cdot c^n$ für ein $c \in k^\times \implies b$ besitzt eine n-te Wurzel $\beta \in K \implies \frac{\sigma\beta}{\beta} \in \mu_n$ ist definiert und wegen $\zeta_n \in k$ unabhängig von der gewählten Wurzel β:

$$\beta'^n = b \implies \zeta = \frac{\beta'}{\beta} \in \mu_n \subset k \implies \zeta = \sigma\zeta \implies \frac{\beta'}{\beta} = \frac{\sigma\beta'}{\sigma\beta} \implies \frac{\sigma\beta'}{\beta'} = \frac{\sigma\beta}{\beta}$$

1b) Die Paarung ist nur von der Restklasse $bk^{\times n}$ abhängig:
Ist $b' = bc^n$ mit $c \in k^\times$, so ist $\beta' = \beta c$ eine n-te Wurzel von b' und

$$\frac{\sigma\beta'}{\beta'} = \frac{\sigma(\beta c)}{\beta c} \underset{c\in k}{=} \frac{\sigma\beta}{\beta}\,.$$

2) Homomorphie im ersten Argument: Sind $\sigma, \tau \in G(K|k)$, so gilt

$$\frac{\sigma\circ\tau(\beta)}{\beta} = \frac{\sigma(\tau(\beta))}{\tau(\beta)} \cdot \frac{\tau(\beta)}{\beta} = \frac{\sigma(\beta')}{\beta'} \cdot \frac{\tau(\beta)}{\beta} \underset{1a)}{=} \frac{\sigma(\beta)}{\beta} \cdot \frac{\tau(\beta)}{\beta}\,.$$

3) Homomorphie im zweiten Argument:

$$\beta^n = b\,,\ \gamma^n = c \implies (beta\gamma)^n = bc \underset{1a)}{\implies} \langle\sigma, bck^{\times n}\rangle = \frac{\sigma(\beta\gamma)}{\beta\gamma} = \frac{\sigma\beta}{\beta} \cdot \frac{\sigma\gamma}{\gamma}\,.$$

4) „Linker“ Kern: Sei $\sigma \in G(K|k)$. Dann gilt

$$\bigwedge_b \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}} = 1 \iff \bigwedge_i \sigma(\sqrt[n]{a_i}) = \sqrt[n]{a_i} \iff \sigma = \mathrm{id}_K\,.$$

5) „Rechter“ Kern: Sei $b \in \langle a_1, \ldots, a_r\rangle k^{\times n}$. Dann gilt

$$\bigwedge_\sigma \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}} = 1 \underset{K|k \text{ gal.}}{\iff} \sqrt[n]{b} \in K \iff b \in k^{\times n} \iff \bar{b} = \bar{1}\,.$$

Man beachte, dass $K|k$ Zerfällungskörper des Polynoms $\prod_{i=1}^r (X^n - a_i)$ vom Grade n^r ist und dieses separabel ist, weil wegen $\operatorname{ord}\zeta_n = n$ $\operatorname{char} k$ kein Teiler von n^r ist.

Aufgabe 24. (s)
Sei G eine abelsche Gruppe der Ordnung n. Zeigen Sie:

a) $\chi \in \hat{G} \implies \sum_{g\in G} \chi(g) = \begin{cases} \#G & \text{für } \chi = 1_{\hat{G}} \\ 0 & \text{für } \chi \neq 1_{\hat{G}} \end{cases}$.

b) $g \in G \implies \sum_{\chi\in\hat{G}} \chi(g) = \begin{cases} \#G & \text{für } g = 1_G, \\ 0 & \text{für } g \neq 1_G. \end{cases}$

c) Die aus den Charakterwerten für $g \in G$ gebildeten Vektoren $e_g := (\chi(g) \mid \chi \in \hat{G})$ bilden eine Orthogonalbasis des $\mathbb{C}^G = \mathbb{C}^n$.

Lösung:
a) $\chi = 1_{\hat{G}} \implies \sum_{g\in G}\chi(g) = \#G$. Sei nun $\chi \neq 1_{\hat{G}}$, also $\chi(g_0) \neq 1$ für ein $g_0 \in G$. Dann gilt

$$\chi(g_0)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(g_0 g) = \sum_{g'\in G}\chi(g') \implies (\chi(g_0)-1)\sum_{g\in G}\chi(g) = 0 \underset{\chi(g_0)\neq 1}{\implies} \sum_{g\in G}\chi(g) = 0\,.$$

b) Mit dem Ansatz von a) folgt allgemein

$$\sum_{g\in G}\langle g,h\rangle = \begin{cases} \#G & \text{für } h = 1_H, \\ 0 & \text{für } h \neq 1_H \end{cases} \quad \text{für } \textit{jede} \text{ n. a. Paarung } G\times H \to \mu\,.$$

Angewendet auf die $\hat{G}\times G \to \mu$ folgt b).
[Ein zu a) analoger Beweis ist natürlich auch möglich.]
c) Sei $(\ldots,\ldots)$ das Standardskalarprodukt auf $\mathbb{C}^n$. Dann gilt

$$(e_g, e_{g'}) = \sum_{\chi\in\hat{G}}\chi(g)\bar{\chi}(g') \underset{\chi(g')\in\mu_n}{=} \sum_{\chi\in\hat{G}}\chi(g)\chi(g')^{-1} = \sum_{\chi\in\hat{G}}\chi(gg'^{-1}) = 0 \text{ für } gg'^{-1} \neq 1_G\,.$$

Damit bilden die e_g ein Orthogonalsystem von n Vektoren im $\mathbb{C}^n$. Die Länge der Vektoren ist $\sqrt{\sum_{\chi\in\hat{G}}\chi(gg^{-1})} = \sqrt{n} \neq 0$, also liegt eine Orthogonal*basis* des $\mathbb{C}^n$ vor.

Aufgabe 25. (m)

a) Wiederholen Sie die grundlegenden Fakten über auflösbare Gruppen. Entscheiden Sie für die symmetrischen Gruppen $\mathcal{S}_n$ und die Gruppen kleiner Ordnung (etwa ≤ 10) über die Auflösbarkeit.

Zeigen Sie:

b) Sind $K_1, K_2|k$ auflösbare Körperweiterungen, so ist auch $K_1K_2|k$ auflösbar.

c) Sind $K|L$ und $L|k$ auflösbar, so ist die galoissche Hülle N von $K|k$ auflösbar über k.

d) In c) kann i. a. *nicht* geschlossen wwerden, dass $K|k$ auflösbar ist.

Lösung:
a) 1) G auflösbar $\iff$ es gibt eine Untergruppen-Kette $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_r = \{e\}$ mit G_i/G_{i+1} abelsch (bzw. zyklisch bzw. primzyklisch) für alle $0 \leq i < r$.
2) $H \leq G \ \wedge\ G$ auflösbar $\implies H$ auflösbar.
3) $H \triangleleft G$: G auflösbar $\iff H$ und G/H auflösbar.
4) Satz von Feit-Thompson: $\#G$ ungerade $\implies G$ auflösbar.
Auflösbarkeit:
5) $\mathcal{A}_n$ einfach für $n \geq 5$, also nicht auflösbar.
6) $\mathcal{S}_n$ nicht auflösbar für $n \geq 5$ (wegen 5) und 3)).
7) $\mathcal{S}_4$ auflösbar: $\mathcal{S}_4 \triangleright \mathcal{A}_4 \triangleright \mathcal{V}_4 \triangleright \mathbb{Z}/2\mathbb{Z} \triangleright \{e\}$ ist eine Kompositionsreihe; die Kompositionsfaktoren sind die primzyklischen Gruppen C_2, C_3, C_2, C_2.
8) $\mathcal{S}_3$ ist auflösbar nach 7) und 2).
9) Alle Gruppen der Ordnung $< 60 = \#\mathcal{A}_5$ sind auflösbar.
b) K_1, K_2 auflösbar $\implies K_1K_2|k$ galoissch und $G(K_1K_2|k)$ ist Untergruppe der auflösbaren Gruppe $G(K_1|k)\times G(K_2|k)$ (siehe Aufgabe 5), also selbst auflösbar.
c) Mit $K|L$ und $L|k$ ist auch $K|k$ separabel, also ist die normale Hülle von $K|k$ $N = \prod_{\sigma\in\mathcal{M}(K|k)}\sigma K$ Kompositum separabler Erweiterungen und damit normal und separabel, also galoissch über k. Da $L|k$ galoissch ist, gilt $L = \sigma L \subset \sigma K$ für alle σ und $G(\sigma K|L) = G(\sigma K|\sigma L) \xrightarrow{\sim} G(K|L)$ ist auflösbar. Nach b) ist dann $N|L$ auflösbar und folglich

$$G(N|L) \simeq G(N|k)/G(L|k) \text{ auflösbar und } G(L|k) \text{ auflösbar } \underset{a)3)}{\implies} G(N|k) \text{ auflösbar}\,.$$

d) Das Problem ist wohlbekannt: $K|L$ und $L|k$ galoissch $\not\Rightarrow$ $K|k$ galoissch. Gegenbeispiel etwa: $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ zyklisch vom Grade 2, aber $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ ist nicht galoissch, denn $\zeta_4 = i \notin \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$.

Aufgabe 26. (s)
Sei k ein Körper der Charakteristik $p \neq 0$ und $f(X) = X^p - X - a \in k[X]$ ein sog. Artin-Schreier-Polynom. Sei $\alpha \in \tilde{k}$ eine Wurzel von f.

a) Bestimmen sie die übrigen Wurzeln von f und folgern Sie: f ist separabel und

$$f \text{ zerfällt über } k \text{ in Linearfaktoren} \quad \text{oder} \quad f \text{ ist irreduzibel über } k\,.$$

b) Ist f irreduzibel über k, so ist $k(\alpha)|k$ zyklisch vom Grad p; die Galoisgruppe wird erzeugt vom k-Automorphismus σ mit $\sigma(\alpha) = \alpha + 1$.

c) Ist $K|k$ zyklisch vom Grad p und σ Erzeugendes der Galoigruppe $G(K|k)$, so wird K erzeugt von $\alpha := \sum_{i=1}^{p-1} i\sigma^i(\xi)$ für ein geeignetes $\xi \in K$.

d) Ist $K|k$ zyklisch vom Grad p, so ist K Stammkörper eines geeigneten Artin-Schreier-Polynoms $f = X^p - X - a \in k[X]$.

Lösung:
a) Seien α, β Wurzeln von f, also $\alpha^p - \alpha - a = \beta^p - \beta - a = 0 \iff (\alpha - \beta)^p = \alpha - \beta \iff \alpha - \beta \in \mathbb{F}_p$, denn der Primkörper $\mathbb{F}_p$ besteht genau aus den Wurzeln von $X^p - X$. Damit ist die Wurzelmenge von f genau $W_f = \{\alpha + c \mid c \in \mathbb{F}_p\}$. Dies sind p verschiedene Wurzeln von f, also hat f wegen $\deg f = p$ nur einfache Wurzeln, f ist separabel.
Ist f reduzibel, also $f = g \cdot h$ mit $g, h \in k[X]$, $1 \leq d := \deg g < p$, so ist $g = \prod_{i=1}^{d}(X - \alpha - n_i)$ mit $n_i \in \mathbb{F}_p$. Dann hat g als Koeffizienten von X^{d-1} $c_{d-1} = -d\alpha + N$ mit $N \in \mathbb{F}_p \subset k$, also $d\alpha \in k$. Wegen $d < p$ ist $d \cdot 1_k \neq 0$ und daher $\alpha \in k$. Dies bedeutet, dass k alle Wurzeln von f enthält, f zerfällt über k in Linearfaktoren.
b) Nach a) enthält $k(\alpha)$ alle Wurzeln von f, ist also Zerfällungskörper des separablen Polynoms f und daher galoissch über k. Da f irreduzibel ist, gibt es zu jeder Wurzel von f, also auch zu $\alpha + 1$ einen k-Monomorphismus $\sigma \in \mathcal{M}(k(\alpha)|k) = G(k(\alpha)|k$ mit $\sigma\alpha = \alpha + 1$ und folglich $\sigma^i(\alpha) = \alpha + \bar{i} \cdot 1_k$ für alle $i \in \mathbb{Z}$. Wegen $i \cdot 1_k = 0_k \iff p = \operatorname{char} k \mid i$ hat σ die Ordnung $p = (k(\alpha) : k)$ und erzeugt daher die Galoisgruppe $G(k(\alpha)|k)$.
c) Für $\xi \in K$ setzen wir α wie angegeben, dann gilt

$$\begin{aligned}
\sigma\alpha &= \sum_{i=0}^{p-1} i\sigma^{i+1}(\xi) = \sum_{j=1}^{p}(j-1)\sigma^j(\xi) \\
&= \sum_{j=0}^{p-1}(j-1)\sigma^j(\xi) \qquad\qquad (\text{wegen } (p-1)\sigma^p(\xi) = -\sigma^0(\xi)) \\
&= \alpha - \sum_{j=0}^{p-1}\sigma^j(\xi) = \alpha - \mathcal{S}_{K|k}(\xi)\,.
\end{aligned}$$

Da $K|k$ separabel ist, ist $\mathcal{S}_{K|k} : K \twoheadrightarrow k$ ein Epimorphismus (Prop. (1.5)), also gibt es ein $\xi \in K$ mit $\mathcal{S}_{K|k}(\xi) = 1$. Für das dadurch definierte α gilt dann $\sigma\alpha = \alpha + 1 \neq \alpha$, also $\alpha \notin k$ und daher $k(\alpha) = K$, denn $(K : k) = p$ ist prim.
d) Wegen $\sigma\alpha = \alpha + 1$ ist α Wurzel eines Artin-Schreier-Polynoms $f = X^p - X - a \in k[X]$.
Begründung: $f(\alpha) = 0 \iff a = \alpha^p - \alpha$ zeigt wie man a zu wählen hat. Man muss lediglich zeigen, dass a in k liegt:

$$a := \alpha^p - \alpha \implies \sigma a = \sigma\alpha^p - \sigma\alpha = (\alpha+1)^p - (\alpha+1) \underset{\operatorname{char} k = p}{=} \alpha^p + 1 - \alpha - 1 = a\,.$$

α ist also Wurzel des Artin-Schreier-Polynoms $X^p - X - a \in k[X]$, das wegen $\alpha \notin k$ irreduzibel sein muss (siehe a)).

Aufgabe 27. (s*)

a) Bestimmen Sie für $\mathbb{Q}(\mu_7)$ – und ggf. unter Benutzung eines Computers für $\mathbb{Q}(\mu_{11})$ – Auflösungen durch Radikale.

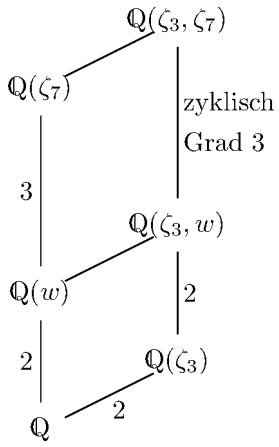
b) Entwerfen Sie einen Algorithmus, der dieses Problem für beliebige Kreiskörper $\mathbb{Q}(\mu_n)$ löst.

c) Berechnen Sie die primitiven 7-ten Einheitswurzeln durch Radikale.

Lösung:
a) Gesucht ist eine Radikalerweiterung $R|\mathbb{Q}$, die $K := \mathbb{Q}(\mu_7) = \mathbb{Q}(\zeta_7)$ enthält. $\mathbb{Q}(\mu_7)|\mathbb{Q}$ ist galoissch mit zyklischer Galoisgruppe $G(\mathbb{Q}(\mu_7)|\mathbb{Q}) \simeq \mathbb{F}_7^\times$ der Ordnung 6. Es ist 3 mod 7 eine Primitivwurzel modulo 7 und daher $G(\mathbb{Q}(\mu_7)|\mathbb{Q}) = \langle\sigma\rangle$ mit $\sigma(\zeta_7) = \zeta_7^3$.
Wir gehen aus von Aufgabe 15 (bzw. 21), in der wir den quadratischen Teilkörper $L \subset \mathbb{Q}(\mu_7)$ bestimmt haben. Es gilt

$$L = \mathbb{Q}(w) = \mathbb{Q}(\sqrt{-7}) \text{ mit } w = \mathcal{S}_{\langle\sigma^2\rangle}(\zeta_7) = \zeta_7 + \zeta_7^2 + \zeta_7^4\,,\ f_{w,\mathbb{Q}} = X^2 + X + 2\,.$$

$\mathbb{Q}(\zeta_7)|\mathbb{Q}(w)$ ist kubisch mit zyklischer Galoisgruppe, man erweitert also den Grundkörper um die dritten Einheitswurzeln, um den Hauptsatz der Kummertheorie anwenden zu können. Wir bekommen so das nebenstehende Körperdiagramm: $\mathbb{Q}(\zeta_7)$ und $\mathbb{Q}(\zeta_3)$ sind zyklische Erweiterungen mit Durchschnitt $\mathbb{Q}$ (siehe Prop. (2.2)) und daher



$$G(\mathbb{Q}(\zeta_7,\zeta_3)|\mathbb{Q}) \xrightarrow{\sim} G(\mathbb{Q}(\zeta_7)|\mathbb{Q}) \times G(\mathbb{Q}(\zeta_3)|\mathbb{Q})\,.$$

Deshalb haben die Erweiterungen die im Diagramm angegebenen Körpergrade und es gilt $f_{w,\mathbb{Q}(\zeta_3)} = f_{w,\mathbb{Q}} = X^2 + X + 2$. $\mathbb{Q}(w,\zeta_3) = \mathbb{Q}(\sqrt{-7},\sqrt{-3})$ ist eine Radikalerweiterung und $Q(\zeta_7,\zeta_3)|\mathbb{Q}(w,\zeta_3)$ als zyklische kubische Erweiterung gemäß Kummertheorie (Satz (2.8)) ebenfalls. Ein erzeugendes Radikal erhalten wir durch die Lagrangesche Resolvente. Es ist

$$G(\mathbb{Q}(\zeta_7,\zeta_3)|\mathbb{Q}(w,\zeta_3)) \xrightarrow{\sim} G(\mathbb{Q}(\zeta_7)|\mathbb{Q}(w)) = \langle\sigma^2\rangle \text{ mit } \sigma^2(\zeta_7) = \zeta_7^{3^2} = \zeta_7^2\,.$$

Damit erhalten wir als Radikal die Lagrangesche Resolvente

$$\alpha = \sum_{i=0}^{2} \zeta_3^i \zeta_7^{2^i} = \zeta_7 + \zeta_3\zeta_7^2 + \zeta_3^2\zeta_7^4\,.$$

Wir berechnen den Radikanden $\alpha^3 \in \mathbb{Q}(w,\zeta_3)$. Es gilt also dreigliedrige Summen in die dritte Potenz zu erheben, eine etwas mühselige Rechnung, aber noch „per Hand“ durchführbar. Wir gehen aus von

$$\begin{aligned}(\sum_{i=0}^{2} A_i)^3 &= \sum_{i,j,k} A_iA_jA_k \\ &= A_0^3 + A_1^3 + A_2^3 + 3(A_0A_1^2 + A_0A_2^2 + A_1A_0^2 + A_1A_2^2 + A_2A_0^2 + A_2A_1^2) + 6A_0A_1A_2\end{aligned}$$

und erhalten mit $A_iA_jA_k = \zeta_3^{i+j+k}\zeta_7^{2^i+2^j+2^k}$

$$\begin{aligned}\alpha^3 &= (\zeta_7^3 + \zeta_7^6 + \zeta_7^5) + 3(\zeta_3\zeta_7^4 + \zeta_3^2\zeta_7^6 + \zeta_3\zeta_7 + \zeta_3^2\zeta_7^5 + \zeta_3\zeta_7^2 + \zeta_3^2\zeta_7^3) + 6 \\ &= (\zeta_7^3 + \zeta_7^6 + \zeta_7^5) + 3\zeta_3(\zeta_7^4 + \zeta_7 + \zeta_7^2) + 3\zeta_3^2(\zeta_7^6 + \zeta_7^5 + \zeta_7^3) + 6\,.\end{aligned}$$

Dies reduzieren wir mittels $w = \zeta_7 + \zeta_7^2 + \zeta_7^4$, $\sigma w = \zeta_7^3 + \zeta_7^6 + \zeta_7^5$, $w + \sigma w = \mathcal{S}_{K|\mathbb{Q}}(\zeta_7) = -1$ und schließlich $f_{\zeta_3,\mathbb{Q}} = X^2 + X + 1$, also $\zeta_3^2 = -\zeta_3 - 1$:

$$\begin{aligned}\alpha^3 &= \sigma w + 3\zeta_3 w + 3\zeta_3^2 \sigma w + 6 = -1 - w + 3\zeta_3 w + 3(-\zeta_3 - 1)(-1 - w) + 6 \\ &= 3\zeta_3 + 8 + w(6\zeta_3 + 2) \in \mathbb{Q}(w, \zeta_3)\end{aligned}$$

Mit $w = -\frac{1}{2} + \frac{1}{2}\sqrt{-7}$ und $\zeta_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ erhält man daraus den Radikanden in der Form

$$a = \frac{1}{2}(14 - \sqrt{-7} + 3\sqrt{-3}\sqrt{-7})$$

und damit explizit die Radikalerweiterung

$$\mathbb{Q}(\zeta_7) \subset \mathbb{Q}(w, \zeta_3, \alpha) = \mathbb{Q}\Big(\sqrt{-7}, \sqrt{-3}, \sqrt[3]{\frac{14 - \sqrt{-7} + 3\sqrt{-3}\sqrt{-7}}{2}}\Big)\,.$$

Ergebnisse für $\mathbb{Q}(\mu_{11})$:
$(\mathbb{Q}(\mu_{11}) : \mathbb{Q}) = 10$, $-\zeta_5$ ist eine primitive 10-te Einheitswurzel. Nach Aufgabe 18 ist

$$\zeta_5 = \frac{1}{4}\Big(-1 + \sqrt{5} + \sqrt{-10 - 2\sqrt{5}})\Big)\,, \quad \mathbb{Q}(\mu_{10}) = \mathbb{Q}(\mu_5) = \mathbb{Q}\Big(\sqrt{5}, \sqrt{-10 - 2\sqrt{5}})\Big)\,.$$

Für $\mathbb{Q}(\zeta_{10}, \zeta_{11})|\mathbb{Q}(\zeta_{10})$ setzen wir als Radikal die Lagrangesche Resolvente an

$$\alpha := \sum_{j=0}^{9} \zeta_{10}^j \zeta_{11}^{2^j} = \sum_{j=0}^{9} (-\zeta_5)^j \zeta_{11}^{2^j}$$

und berechnen mit Computerunterstützung den Radikanden[1)]

$$\begin{aligned}a = \alpha^{10} &= 11(8664 - 6840\zeta_5 - 1965\zeta_5^2 - 7600\zeta_5^3) \\ &= \tfrac{11}{4}(51061 + 2725\sqrt{5}) - \tfrac{55}{8}\sqrt{-125662120 + 44525192\sqrt{5}}\end{aligned}$$

Dann ist $\mathbb{Q}(\mu_{11})$ Teilkörper der Radikalerweiterung

$$\mathbb{Q}\Big(\sqrt{5}, \sqrt{-10 - 2\sqrt{5}}, \sqrt[10]{a}\Big)$$

vom Grade $2 \cdot 2 \cdot 10 = 40$. Diese Radikalerweiterung ist $\mathbb{Q}(\mu_{10 \cdot 11})$.

b) Algorithmus zur Bestimmung einer Radikalauflösung für Kreiskörper $\mathbb{Q}(\mu_n)$.
Input: $n \in \mathbb{N}_+$
Output: $r \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_r \in \tilde{\mathbb{Q}}$, $K_i := \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ für $0 \le i \le r$ mit

$$K_i|\mathbb{Q} \text{ galoissch}\,,\ (K_i : K_{i-1}) = p_i \text{ Primzahl}\,, \quad \alpha_i^{p_i} \in K_{i-1}\,, \quad \mu_n \subset K_r\,.$$

Gegeben $n \in \mathbb{N}_+$. Der Algorithmus verzweigt in die folgenden 4 Fälle:
(1) $n = 1, 2$.
(2) $n = p$ ungerade Primzahl.
(3) $n = p \cdot m$ mit p Primzahl, $p \nmid m$, $m > 1$.
(4) $n = p \cdot m$ mit p Primzahl, $p \mid m$.
(1) Output $r = 0$. Die Bedingungen sind erfüllt: $\mu_1 \subset \mu_2 \subset K_0 = \mathbb{Q}$.
(2) Rekursiver Aufruf des Algorithmus für $p - 1 < p$ liefert den Output r, α_i, K_i, p_i mit den genannten Bedingungen für $p - 1$. Wegen $G(K_r(\zeta_p)|K_r) \hookrightarrow G(\mathbb{Q}(\zeta_p)|\mathbb{Q}) \simeq \mathbb{F}_p^\times$ ist $K_r(\zeta_p)|K_r$

[1)] Hinweis: Für die beiden Darstellungen des Radikanden a gibt es jeweils 4 unterschiedliche (algebraisch nicht unterscheidbare) Möglichkeiten, in der ersten Form abhängig von den 4 Möglichkeiten für ζ_5, in der zweiten Form von den 4 Vorzeichenkombinationen für die beiden auftretenden Quadratwurzeln, vgl. Aufgabe 18.

zyklisch vom Grade $d \mid p-1$ und $\mu_d \subset \mu_{p-1} \subset K_r$. Im Falle $d = 1$ ist nichts zu tun, andernfalls ist nach Satz (2.8) $K_r(\zeta_p)$ eine reine Radikalerweiterung über K_r vom Grade d. Als Radikal kann man jede Lagrangesche Resolvente $\alpha := \alpha_\zeta$, $\zeta \in \mu_d$, wählen, die $\neq 0$ ist (siehe Satz (3.5)). Die Radikalerweiterung $K_r(\alpha)|K_r$ ist entsprechend der Primzerlegung $d = \prod_{j=1}^{s} q_j$ ein Turm von reinen Radikalerweiterungen $K_r(\alpha) \supset K_r(\alpha^{q_1}) \supset K_r(\alpha^{q_1 q_2}) \supset \ldots \supset K_r(\alpha^d) = K_r$ von Primzahlgraden $q_1, q_2, \ldots, q_s$. Damit erhält man dann für $n = p$ den gewünschten Output $r + s$, $\alpha_{r+j} = \alpha^{q_1 \ldots q_{s-j}}$ mit den geforderten Eigenschaften für $n = p$, insbesondere $\mu_p \subset K_{r+s} = K_r(\alpha)$.
(3) Dann gilt $p < n$, $m < n$ und der Algorithmus liefert zu m den Output r, α_i, K_i, p_i mit den genannten Bedingungen für m und zu $p < n$ den Output s, β_j, L_j, q_j mit den entsprechenden Eigenschaften für p. Man erweitert nun den Output für m um den Output für p

$$\alpha_{r+j} := \beta_j \ (j = 1, \ldots s)\,, \quad K_{r+j} := K_r\ (\beta_1, \ldots, \beta_j)\ (j = 1, \ldots, s)\,.$$

Da alle K_i und L_j über $\mathbb{Q}$ galoissch sind, ist auch $K_{r+j} = K_r L_j|\mathbb{Q}$ galoissch. Also gilt

$$G(K_{r+j}|K_{r+j-1}) = G(K_r L_j|K_r L_{j-1}) \hookrightarrow G(L_j|L_{j-1}) \implies (K_{r+j} : K_{r+j-1}) \mid (L_j : L_{j-1}) = q_j\,.$$

Damit ist $(K_{r+j} : K_{r+j-1}) = q_j$ eine Primzahl – es sei denn $K_{r+j} = K_{r+j-1}$, in welchem Falle K_{r+j} überflüssig ist und nicht in den Output aufgenommen wird. Weiter gilt $\alpha_{r+j}^{p_{r+j}} = \beta_j^{q_j} \in L_j \subset K_{r+j}$. Und wegen $p \nmid m$ gilt schließlich $\mu_n = \mu_m \mu_p \subset K_r L_s = K_{r+s}$, so dass alle Forderungen für $n = pm$ erfüllt sind.
(4) Dann gilt $m < n$ und der Algorithmus liefert zu m den Output r, α_i, K_i, p_i mit den genannten Bedingungen für m. Sei $p^\nu \cdot l = m$ mit $\nu \geq 1$, $p \nmid l$ und folglich $n = p^{\nu+1} \cdot l$. Es ist $\zeta_{p^\nu} := \zeta_m^l \in K_r$ eine primitive p^ν-te Einheitswurzel und $\zeta_{p^{\nu+1}} := \sqrt[p]{\zeta_{p^\nu}}$ erzeugt eine Radikalerweiterung von K_r vom Grad p (oder 1, falls $\zeta_{p^{\nu+1}} \in K_r$), denn für $\nu \geq 1$ gilt $\mathbb{Q}(\zeta_{p^{\nu+1}}) : \mathbb{Q}(\zeta_{p^\nu}) = \frac{\varphi(p^{\nu+1})}{\varphi(p^\nu)} = p$. Man erweitert also im erstgenannten Fall den Output für m um $\alpha_{r+1} := \sqrt[p]{\zeta_{p^\nu}}$ und der Körper $K_{r+1} = K_r(\alpha_{r+1})$ enthält dann die primitive n-te Einheitswurzel $\zeta_n = \zeta_l \cdot \zeta_{p^{\nu+1}}$.
c) Eine Radikaldarstellung für ζ_7 gewinnen wir aufbauend auf Teil a) mittels IV. Satz (3.5):

$$\alpha_{\zeta_3^i} = \sum_{j=0}^{2} \zeta_3^{ij} \sigma^j(\zeta_7) = \sum_{j=0}^{2} \zeta_3^{ij} \zeta_7^{2^j} = \zeta_7 + \zeta_3^i \zeta_7^2 + \zeta_3^{2i} \zeta_7^4\,,$$

$$b_i := b(\zeta_3^i) = \alpha_{\zeta_3^i} \alpha^{3-i}\,, \quad a_i := a(\zeta_3^i) = \frac{b_i}{a} \in \mathbb{Q}(w, \zeta_3) = \mathbb{Q}(\sqrt{-7}, \sqrt{-3})$$

$$\begin{aligned}
i = 0 :\ & b_0 = (\zeta_7 + \zeta_7^2 + \zeta_7^4)\alpha^3 = \mathcal{S}_{\mathbb{Q}(\zeta_7)|L}(\zeta_7) \cdot a = w \cdot a, \quad a_0 = \tfrac{b_0}{a} = w = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-7} \\
i = 1 :\ & b_0 = \alpha_{\zeta_3} \alpha^2 = \alpha^3 = a, \quad a_0 = \tfrac{b_0}{a} = 1. \\
i = 2 :\ & b_2 = \alpha_{\zeta_3^2} \alpha = (\zeta_7 + \zeta_3^2 \zeta_7^2 + \zeta_3 \zeta_7^4)(\zeta_7 + \zeta_3 \zeta_7^2 + \zeta_3^2 \zeta_7^4) \\
& \quad = \zeta_7^2 + \zeta_3 \zeta_7^3 + \zeta_3^2 \zeta_7^5 + \zeta_3^2 \zeta_7^3 + \zeta_7^4 + \zeta_3 \zeta_7^6 + \zeta_3 \zeta_7^5 + \zeta_3^2 \zeta_7^6 + \zeta_7 \\
& \quad = \zeta_7^2 + \zeta_7^4 + \zeta_7 \ + \ \zeta_3(\zeta_7^3 + \zeta_7^5 + \zeta_7^6) \ + \ \zeta_3^2(\zeta_7^3 + \zeta_7^6 + \zeta_7^5) \\
& \quad = w + \sigma(w) \cdot (\zeta_3 + \zeta_3^2) = w - \sigma(w) = 2w + 1 = \sqrt{-7}\,. \\
& a_2 = \frac{b_2}{a} = \frac{2\sqrt{-7}}{14 - \sqrt{-7} + 3\sqrt{-3}\sqrt{-7}} = \frac{-14 + \sqrt{-7} + 3\sqrt{-3}\sqrt{-7}}{14}
\end{aligned}$$

Schließlich

$$3\zeta_7 = -\frac{1}{2} + \frac{1}{2}\sqrt{-7} + \alpha + \frac{\sqrt{-7}}{\alpha} = -\frac{1}{2} + \frac{1}{2}\sqrt{-7} + \alpha + \frac{1}{14}\Big(-14 + \sqrt{-7} + 3\sqrt{-3}\sqrt{-7}\Big) \cdot \alpha^2$$

mit dem kubischen Radikal

$$\alpha = \sqrt[3]{\frac{14 - \sqrt{-7} + 3\sqrt{-3}\sqrt{-7}}{2}}\,.$$

Algebra II
Übung 7

Aufgabe 28. (m)
Seien $K = k(T_1, \ldots, T_n)$ der rationale Funktionenkörper in n Unbestimmten, L der Körper der symmetrischen Funktionen in K und $s_j \in K$ die elementarsymmetrischen Polynome

a) Zeigen Sie für $L_i := L(T_1, \ldots, T_i)$ $(i = 0, 1, \ldots, n)$

$$(L_{i+1} : L_i) = n - i\,, \qquad f_{T_j, L_i} = \begin{cases} X - T_j & \text{für } 1 \le j \le i, \\ f_i := \prod_{\nu=i+1}^{n}(X - T_\nu) & \text{für } i < j \le n. \end{cases}$$

b) Geben Sie eine Basis für $K|L$ an.

c) Zeigen Sie: Jede rationale Funktion $f \in K$ hat eine Darstellung

$$f = \sum_{\substack{(\nu_1, \ldots, \nu_n) \in \mathbb{N}^n \\ 0 \le \nu_i \le n-i}} g_{\underline{\nu}}(s_1, \ldots, s_n) T_1^{\nu_1} \cdot \ldots \cdot T_n^{\nu_n}$$

mit eindeutig bestimmten rationalen Funktionen $g_{\underline{\nu}} \in k(Y_1, \ldots, Y_n)$.

Lösung:
Die symmetrische Gruppe $\mathcal{S}_n$ operiert durch Permutation der T_i auf K und der Fixkörper ist definitionsgemäß der Körper L der symmetrischen Funktionen. Also ist $K|L$ galoissch mit Galoisgruppe $\mathcal{S}_n$ und Körpergrad $(K : L) = n!$.
a) $f_0 := \prod_{\nu=1}^{n}(X - T_\nu)$ ist ein symmetrisches Polynom, also $f_0 \in L[X]$. Sei nun $0 \le i \le n$. Wegen $f_0 \in L[X]$ und $g_i := \prod_{\nu=1}^{i}(X - T_\nu) \in L_i[X]$ folgt $f_i = \frac{f_0}{g_i} \in L_i[X]$ mit Wurzel T_{i+1}. Also ist $(L_{i+1} : L_i) = (L_i(T_{i+1}) : L_i) \le \deg f_i = n - i$. Wir erhalten so

$$n! = (K : L) = \prod_{i=0}^{n-1}(L_{i+1} : L_i) = \prod_{i=0}^{n-1}(L_i(T_{i+1}) : L_i) \le \prod_{i=0}^{n-1}(n - i) = n!\,.$$

Es muss in der Abschätzung also an allen Stellen Gleichheit gelten:

$$(L_{i+1} : L_i) = n - i = \deg f_i \quad \text{und daher} \quad f_i = f_{T_{i+1}, L_i}\,.$$

Damit ist a) bewiesen, denn für $j \le i$ ist $T_j \in L_i$ und daher $f_{T_j, L_i} = X - T_j$, während für $j > i$ T_j Wurzel des irreduziblen Polynoms $f_i \in L_i[X]$ ist, also $f_i = f_{T_j, L_i}$.
b) Für alle $1 \le i \le n$ ist $(L_{i-1}(T_i) : L_{i-1}) = n - i + 1$, also

$$\{T_i^\nu \mid 0 \le \nu \le n - i\} \text{ Basis für } L_i|L_{i-1}$$

und daher

$$\{T_1^{\nu_1} \cdot \ldots \cdot T_n^{\nu_n} \mid 0 \le \nu_i \le n - i \text{ für } 1 \le i \le n\} \text{ Basis für } K = L_n|L_0 = L\,.$$

c) ist eine explizite Formulierung von b) unter Benutzung von $L_0 = k(s_1, \ldots, s_n)$ und der algebraischen Unabhängigkeit der s_i über k.

Aufgabe 29. (m)
a) Bestimmen Sie für die folgenden symmetrischen Polynome

$\alpha)$ $f = X_1^2X_2 + X_1^2X_3 + X_2^2X_3 + X_1X_2^2 + X_1X_3^2 + X_2X_3^2$

$\beta)$ $g = (A^2B+B^2C+C^2A)^2+(AB^2+BC^2+CA^2)^2+(A^2B+B^2C+C^2A)(AB^2+BC^2+CA^2)$

ihre Darstellungen durch die elementarsymmetrischen Polynome.
b) Unter der Voraussetzung $s_1(A,B,C,D) = A+B+C+D = 0$ sind

$\alpha)$ $h = (A+B)^2(B+C)^2 + (A+B)^2(C+A)^2 + (B+C)^2(C+A)^2$

$\beta)$ $p = (A+B)(B+C)(C+A)$

symmetrisch in $A, B, C, \underline{D}$. Berechnen Sie die entsprechenden Darstellungen für h und p durch die elementarsymmetrischen Polynome $s_j(A,B,C,D)$.

Lösung:
a) α): $f \in \mathbb{Z}[X_1,X_2,X_3]$ ist homogen vom Grade 3 und symmetrisch, also existieren nach Satz IV.3.11 $\alpha,\beta,\gamma \in \mathbb{Z}$ mit

$$f = \alpha s_3+\beta s_2s_1+\gamma s_1^3 = \alpha X_1X_2X_3+\beta(X_1X_2+X_1X_3+X_2X_3)(X_1+X_2+X_3)+\gamma(X_1+X_2+X_3)\,.$$

Bestimmung der Koeffizienten durch Einsetzen:

$$\begin{array}{lll} X_1=1\,,X_2=X_3=0 & \Longrightarrow & 0=\alpha\cdot 0+\beta\cdot 0+\gamma \;\Longrightarrow\; \gamma=0 \\ X_1=X_2=1\,,X_3=0 & \Longrightarrow & 2=\alpha\cdot 0+\beta\cdot 1\cdot 2 \;\Longrightarrow\; \beta=1 \\ X_1=X_2=X_3=1 & \Longrightarrow & 6=\alpha+1\cdot 3\cdot 3 \;\Longrightarrow\; \alpha=-3 \end{array}$$

Also $f = -3sS_3 + s_1s_2 = -3X_1X_2X_3 + (X_1X_2+X_1X_3+X_2X_3)(X_1+X_2+X_3)$.
a) β): $\mathcal{S}_3 = \mathcal{S}(A,B,C)$ wird erzeugt von $(A\,B)$ und $(A\,B\,C)$ (siehe Algebra I, Übung 4, Aufgabe 20). g ist invariant gegenüber der Transposition $(A\,B)$ (die ersten beiden Summanden werden vertauscht, ebenso die Faktoren im dritten Summanden). Außerdem ist g invariant gegenüber der zyklischen Vertauschung $(A\,B\,C)$ (offensichtlich durch den formalen Aufbau der Terme). Damit ist g symmetrisch und homogen vom Grade 6, besitzt also eine Darstellung

$$g = \alpha s_3^2 + \beta s_3s_2s_1 + \gamma s_3s_1^3 + \delta s_2^3 + \epsilon s_2^2s_1^2 + \eta s_2s_1^4 + \vartheta s_1^6\,.$$

Koeffizientenbestimmung durch Einsetzen:

$$\begin{array}{llll} A=1\,,B=C=0 & \Longrightarrow & 0 = \vartheta\cdot 1 & \Longrightarrow\; \vartheta=0 \\ A=1\,,B=-1\,,C=0 & \Longrightarrow & 1 = \delta\cdot(-1)^3 & \Longrightarrow\; \delta=-1 \\ A=B=1\,,C=-2 & \Longrightarrow & 3\cdot 3^2 = \alpha(-2)^2-(-3)^3 & \Longrightarrow\; \alpha=0 \\ A=B=1\,,C=0 & \Longrightarrow & 3 = -1+4\epsilon+16\eta & \Longleftrightarrow\; \epsilon=1-4\eta \\ A=1\,,B=2\,,C=0 & \Longrightarrow & 12 = -(-2)^3+4(1-4\eta)-2\eta & \Longrightarrow\; \eta=0\,,\epsilon=1 \\ A=B=C=1 & \Longrightarrow & 3\cdot 3^2 = 3\cdot 3\cdot\beta+3^2\gamma-3^3+3^2\cdot 3^2 & \Longleftrightarrow\; \beta=-3-3\gamma \\ A=1\,,B=C=-1 & \Longrightarrow & 3 = (-1)^2\beta+(-1)^3\gamma-(-1)^3+1 & \Longrightarrow\; \gamma=-1\,,\beta=0 \end{array}$$

Also $g = (AB+AC+BC)^2(A+B+C)^2 - (AB+AC+BC)^3 - ABC(A+B+C)^3$.
b): h ist offenbar invariant unter der Transposition $(A\,B)$. Wegen $A+B+C+D=0$ gilt $(A+B)^2=(C+D)^2$, $(A+C)^2=(B+D)^2$ etc. und daher ist h auch invariant unter dem Zyklus $(A\,B\,C\,D)$. Genauso argumentiert man für p. Die gesuchten Darstellungen für h und p gewinnt man wie unter a). Wegen $s_1(A,B,C,D)=0$ sind die Darstellungen kürzer:

$$h = \alpha s_4 + \beta s_2^2\,, \qquad p = \gamma s_3\,.$$

Aber beim Einsetzen muss man diese Bedingung $A+B+C+D=0$ beachten.

α). $A=B=1\,,C=0\,,D=-2 \implies 9=\beta(-3)^2 \implies \beta=1$

$A=B=1\,,C=D=-1 \implies 0=\alpha+\beta(-2)^2 \implies \alpha=-4$

$$h=(AB+AC+AD+BC+BD+CD)^2-4ABCD\,.$$

β): $A=B=1\,,C=0\,,D=-2 \implies 2=\gamma(-2) \implies \gamma=-1$.

$$p=(A+B)(B+C)(C+D)=-(ABC+ABD+ACD+BCD) \qquad (A+B+C+D=0!)$$

Aufgabe 30. (s)
Sei $f=X^n+\sum_{i=0}^{n-1}a_iX^i\in k[X]$ ein normiertes Polynom n-ten Grades über einem Körper k mit den Nullstellen $\alpha_1,\ldots,\alpha_n$ im algebraischen Abschluss $\tilde{k}$: $f=\prod_{i=1}^n(X-\alpha_i)$.

a) Die sog. *Diskriminante* $D(f)=\prod\limits_{i<j}(\alpha_i-\alpha_j)^2$ besitzt eine Darstellung als Polynom

$$D(f)=\sum_{(\nu_0,\ldots,\nu_{n-1})\in\mathbb{N}^n}\alpha_{\underline{\nu}}\cdot a_0^{\nu_0}\cdot\ldots\cdot a_{n-1}^{\nu_{n-1}}$$

in den Koeffizienten $a_0,\ldots,a_{n-1}$ von f.

Dabei treten nur Monome mit $n\nu_0+(n-1)\nu_1+\ldots+2\nu_{n-2}+\nu_{n-1}=n(n-1)$ auf.

b) Berechnen Sie für $n=2,3$ diese Darstellung von $D(f)$.

Lösung:
Es gilt $a_i=(-1)^{n-i}s_{n-i}(\alpha_1,\ldots,\alpha_n)$. Also muss man $D(f)$ als Polynom in den $s_j(\alpha_1,\ldots,\alpha_n)$ ausdrücken. Dies ist genau dann möglich, wenn $D(f)$ als Polynom in den α_i symmetrisch ist, was offensichtlich der Fall ist. Also existieren β_μ mit

$$D(f)=\sum_{\underline{\mu}\in\mathbb{N}^n}\beta_{\underline{\mu}}s_1^{\mu_1}(\underline{\alpha})\cdot\ldots\cdot s_n^{\mu_n}(\underline{\alpha})\,.$$

Da $D(f)$ als Polynom in den α_i homogen vom Grad $2\cdot\binom{n}{2}=n(n-1)$ ist, treten in der obigen Darstellung von $D(f)$ nur Summanden mit

$$\mu_1+2\mu_2+\ldots+n\mu_n=n(n-1)$$

auf. Setzt man nun $s_j(\alpha_1,\ldots,\alpha_n)=(-1)^ja_{n-j}$ ein, so erhält man die Behauptung von 30. a. (beachte $\mu_j=\nu_{n-j}$).
b) $n=2$: $D(f)=(\alpha_1-\alpha_2)^2=\alpha_1^2-2\alpha_1\alpha_2+\alpha_2^2=(\alpha_1+\alpha_2)^2-4\alpha_1\alpha_2=(-a_1)^2-4a_0$, also

$$D(f)=a_1^2-4a_0\,.$$

$n=3$: $D(f)$ ist symmetrisch in den α_i und homogen vom Grade 6, also

$$D(f)=\alpha s_3^2+\beta s_3s_2s_1+\gamma s_3s_1^3+\delta s_2^3+\epsilon s_2^2s_1^2+\eta s_2s_1^4+\vartheta s_1^6\,.$$

Man bestimmt die Koeffizienten wie unter 29. a) β). Dabei benutzt man dieselben Einsetzungen, so dass sich nur die linke Seite der Gleichung (die Auswertung von $D(f)$) ändert.
Ergebnis: $\vartheta=0\,,\delta=-4\,,\alpha=-27\,,\eta=0,\epsilon=1\,,\gamma=-4,\beta=18$ und daher

$$D(f)=-27a_0^2+18a_0a_1a_2-4a_0a_2^3-4a_1^3+a_1a_2^2\,.$$

Aufgabe 31. (s)
Zeigen Sie mit den Bezeichnungen von Aufgabe 30:

a) Ist $\hat{\sigma} \in G(k(\alpha_1, \ldots, \alpha_n)|k)$ und $\sigma := \hat{\sigma}\,|_{\{\alpha_1,\ldots,\alpha_n\}}$ die induzierte Permutation der Wurzeln, so gilt
$$\hat{\sigma}(\sqrt{D(f)}\,) = \operatorname{sign}\sigma \cdot \sqrt{D(f)}\,.$$

b) Ist $D(f) \neq 0$, so ist f separabel und es gilt für die Galoisgruppe $G(f)$ von f:
$$G(f) \subset \mathcal{A}_n \iff D(f) \in k^2\,.$$

c) Bestimmen Sie für kubische Polynome die Galoisgruppe explizit.

Lösung:
a) Gemäß der Definition besitzt $D(f)$ in $K := k(\alpha_1, \ldots, \alpha_n)$ die Quadratwurzel $\prod_{i<j}(\alpha_i - \alpha_j)$ und es gilt (o. E. für $D(f) \neq 0$)
$$\hat{\sigma}(\sqrt{D(f)}\,) = \prod_{i<j}(\sigma\alpha_i - \sigma\alpha_j) = \prod_{i<j}\frac{\sigma\alpha_i - \sigma\alpha_j}{\alpha_i - \alpha_j} \cdot \prod_{i<j}(\alpha_i - \alpha_j) = \operatorname{sign}\sigma \cdot \sqrt{D(f)}\,.$$

b) f separabel $\iff$ alle α_i sind verschieden $\iff$ $D(f) \neq 0$. Dann gilt
$$D(f) \in k^2 \iff \bigwedge_{\hat{\sigma}\in G(K|k)} \hat{\sigma}(\sqrt{D(f)}) = \sqrt{D(f)} \underset{a)}{\iff} \bigwedge_{\sigma\in G(f)} \operatorname{sign}\sigma = +1 \iff G(f) \subset \mathcal{A}_n\,.$$

c) Ist f kubisch, separabel und reduzibel, so hat f genau eine oder drei Wurzeln in k. Dementsprechend ist $G(f) = \mathcal{S}_2 \subset \mathcal{S}_3$ oder $G(f)$ trivial.
Ist f irreduzibel, so ist $G(f) \subset \mathcal{S}_3$ transitiv (siehe Prop. (1.2)) und es gibt daher nur die beiden Möglichkeiten $\mathcal{A}_3$ oder $\mathcal{S}_3$ für $G(f)$:
$$G(f) \simeq \begin{cases} \mathcal{A}_3 & \text{falls } D(f) \in k^2, \\ \mathcal{S}_3 & \text{falls } D(f) \notin k^2. \end{cases}$$

Aufgabe 32. (s)
Sei R ein Integritätsbereich und $R[X_1, \ldots, X_n]$ der Polynomring in n Unbestimmten über R. Wir betrachten die *lexikographische* Ordnung auf $\mathbb{N}^n$:
$$\mu = (\mu_1, \ldots, \mu_n) > \nu = (\nu_1, \ldots, \nu_n) \iff \bigvee_{1\le k\le n} \mu_k > \nu_k \ \wedge \bigwedge_{j<k} \mu_j = \nu_j\,.$$

Diese übertragen wir auf die in einem Polynom vorkommenden Monome $aX^\nu = a \cdot X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n}$ ($a \neq 0$) und definieren so das führende Monom $\mathrm{FM}(f)$, als das in f vorkommende Monom mit lexikographisch größtem Index ν. (Existenz?, Eindeutigkeit?). Zeigen Sie:

a) $\mathrm{FM}(fg) = \mathrm{FM}(f) \cdot \mathrm{FM}(g)$ für alle $0 \neq f, g \in R[X_1, \ldots, X_n]$.

b) Ist f symmetrisch und $\mathrm{FM}(f) = aX^\nu$, so gilt $\nu_1 \geq \nu_2 \geq \ldots \geq \nu_n$.

c) $\nu_1 \geq \nu_2 \geq \ldots \geq \nu_n \implies \mathrm{FM}(s_1^{\nu_1-\nu_2} s_2^{\nu_2-\nu_3} \cdot \ldots \cdot s_{n-1}^{\nu_{n-1}-\nu_n} s_n^{\nu_n}) = X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n}$.

d) Beschreiben Sie einen Algorithmus, der zu gegebenem symmetrischem Polynom f eine Darstellung $f = \sum_\mu \alpha_\mu s_1^{\mu_1} \cdot \ldots \cdot s_n^{\mu_n}$ ($\alpha_\mu \in R$) liefert.

e) Führen Sie diesen Algorithmus für das Beispiel aus Aufgabe 29.a) α) durch.

Lösung:
a) Die lexikographische Ordnung ist eine Totalordnung, also hat jedes Polynom $f \neq 0$ genau ein lexikographisch größtes Monom $\mathrm{FM}(f)$ und der Beweis von a) verläuft völlig analog zum Fall einer Unbestimmten:

$$f = \sum_{\mu\in\mathbb{N}^n} a_\mu X^\mu\,, \quad g = \sum_{\nu\in\mathbb{N}^n} b_\nu X^\nu \implies f\cdot g = \sum_{\rho\in\mathbb{N}^n} c_\rho X^\rho \quad \text{mit} \quad c_\rho = \sum_{\mu+\nu=\rho} a_\mu b_\nu$$

Es gilt

$$\begin{aligned}\mathrm{FM}(f) = a_{\tilde\mu}X^{\tilde\mu} &\implies a_\mu = 0 \text{ für } \mu > \tilde\mu\\ \mathrm{FM}(g) = b_{\tilde\nu}X^{\tilde\nu} &\implies b_\nu = 0 \text{ für } \nu > \tilde\nu\end{aligned}$$

und daher

$$\mu+\nu > \tilde\mu+\tilde\nu \implies \mu > \tilde\mu \ \vee\ \nu > \tilde\nu \implies c_\rho = \sum_{\mu+\nu=\rho} a_\mu b_\nu = 0 \quad \text{für } \rho > \tilde\rho := \tilde\mu+\tilde\nu.$$

Genauso folgt

$$c_{\tilde\rho} = \sum_{\mu+\nu=\tilde\mu+\tilde\nu} a_\mu b_\nu = a_{\tilde\mu}b_{\tilde\nu} \neq 0\,.$$

Also $\mathrm{FM}(fg) = c_{\tilde\rho}X^{\tilde\rho} = a_{\tilde\mu}b_{\tilde\nu}X^{\tilde\mu+\tilde\nu} = \mathrm{FM}(f)\cdot\mathrm{FM}(g)$.
b) Ist $\mathrm{FM}(f) = aX^\nu = aX_1^{\nu_1}\cdot\ldots\cdot X_n^{\nu_n}$ und f symmetrisch, so muss auch $aX_1^{\nu_2}X_2^{\nu_1}X_3^{\nu_3}\cdot\ldots\cdot X_n^{\nu_n}$ (mit $a\neq 0$) in f vorkommen, also gilt nach Definition von $\mathrm{FM}(f)$

$$(\nu_1,\nu_2,\ldots,\nu_n) \geq (\nu_2,\nu_1,\nu_3,\ldots,\nu_n) \implies \nu_1 \geq \nu_2\,.$$

Genauso folgt $\nu_2 \geq \nu_3$ durch Vertauschung $X_2 \leftrightarrow X_3$ etc.
c) Nach a) gilt

$$\begin{aligned}&\mathrm{FM}(s_1^{\nu_1-\nu_2}s_2^{\nu_2-\nu_3}\ldots) = \mathrm{FM}(s_1)^{\nu_1-\nu_2}\cdot\mathrm{FM}(s_2)^{\nu_2-\nu_3}\cdot\ldots\cdot\\ &= X_1^{\nu_1-\nu_2}\cdot(X_1X_2)^{\nu_2-\nu_3}\cdot(X_1X_2X_3)^{\nu_3-\nu_4}\ldots\\ &= X_1^{\nu_1-\nu_2+\nu_2-\nu_3+\cdots}\cdot X_2^{\nu_2-\nu_3+\cdots}\cdot\ldots = X_1^{\nu_1}X_2^{\nu_2}\cdot\ldots\cdot X_n^{\nu_n}\end{aligned}$$

d) Grundidee: Subtrahiere vom symmetrischen Polynom f ein Potenzprodukt der s_i mit gleichem führenden Monom (siehe b), c)) und iteriere dies. Explizit:
Wir definieren rekursiv zwei Polynomfolgen f_j, g_j mit folgenden Eigenschaften:

$$f_j \text{ symmetrisch}\,, \quad g_j \in k(s_1,\ldots,s_n)\,, \quad f_j+g_j = f\,, \quad \mathrm{FM}(f_j) < \mathrm{FM}(f_{j-1}) \text{ für } f_j \neq 0\,.$$

Wir starten mit $f_0 := f$ und $g_0 := 0$. Ist $f_j = 0$, so endet das Verfahren. Ist $f_j \neq 0$, gilt nach b),c)

$$\mathrm{FM}(f_j) = a\cdot X_1^{\nu_1}\cdot\ldots\cdot X_n^{\nu_n} \implies \mathrm{FM}(f_j) = \mathrm{FM}(h) \text{ für } h = a\cdot s_1^{\nu_1-\nu_2}\cdot\ldots\cdot s_{n-1}^{\nu_{n-1}-\nu_n}\cdot s_n^{\nu_n}\,.$$

Setze dann $f_{j+1} = f_j - h$ und $g_{j+1} = g_j + h$, also gilt unverändert $f_{j+1}+g_{j+1} = f_j+g_j = f$. Nach Konstruktion ist (im Falle $f_{j+1}\neq 0$) $\mathrm{FM}(f_{j+1}) < \mathrm{FM}(f_j)$, $g_{j+1} = g_j + h \in k(s_1,\ldots,s_n)$ und mit h ist auch f_{j+1} wieder symmetrisch.
Da die führenden Monome der f_j lexikographisch echt absteigen, muss das Verfahren nach endlich vielen Schritten bei $f_j = 0$ enden. Dann gilt $f = 0 + g_j \in k(s_1,\ldots,s_n)$, wie behauptet.
e) $f = X_1^2X_2 + X_1^2X_3 + X_2^2X_3 + X_1X_2^2 + X_1X_3^2 + X_2X_3^2$ ist symmetrisch mit $\mathrm{FM}(f) = X_1^2X_2$. Setze also $h = s_1^{2-1}s_2^{1-0}s_3^0 = s_1s_2$ und damit

$$\begin{aligned}h &= (X_1+X_2+X_3)(X_1X_2+X_1X_3+X_2X_3)\\ &= X_1^2X_2 + X_1^2X_3 + X_1X_2X_3 + X_1X_2^2 + X_1X_2X_3 + X_2^2X_3 + X_1X_2X_3 + X_1X_3^2 + X_2X_3^2\\ f_1 &= f - h = -3X_1X_2X_3 = -3s_3\,, \qquad g_1 = h = s_1s_2\\ f_2 &= f_1 + 3s_3 = 0\,, \qquad g_2 = g_1 - 3s_3 = s_1s_2 - 3s_3\end{aligned}$$

und damit $f = g_2 = s_1s_2 - 3s_3$ (vgl. 29. a) α)).

Algebra II
Übung 8

Aufgabe 33. (s)
Berechnen Sie eine primitive 17-te Einheitswurzel durch Radikale.

Lösung:
Für eine Primzahl p und eine primitive p-te Einheitswurzel ζ_p ist die Galoisgruppe $G(\mathbb{Q}(\zeta_p)|\mathbb{Q}) = \langle\sigma\rangle$ zyklisch von der Ordnung $p-1$. Also existiert zu jedem Teiler $d \mid p-1$ eindeutig ein Zwischenkörper L_d vom Grad d über $\mathbb{Q}$. Die Galoisgruppe $G(\mathbb{Q}(\zeta_p)|L_d)$ ist die eindeutig bestimmte Untergruppe $U_d = \langle\sigma^d\rangle$ vom Index d. Es ist $\#U_d =: f$ mit $f \cdot d = p-1$. Die U_d-Spuren von $1 \neq \zeta \in \mu_p$

$$\mathcal{S}_{U_d}(\zeta) = \sum_{j=0}^{f-1} \sigma^{dj}(\zeta) =: P_f \in L_d$$

sind die sog. f-gliedrigen *Gaußschen Perioden.* Es gilt

$$L_d = \mathbb{Q}(P_f) \quad \text{für jedes } 1 \neq \zeta \in \mu_p\,.$$

Denn da $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ abelsch ist, ist jeder Zwischenkörper über $\mathbb{Q}$ galoissch, also

$$\bigwedge_i \mathcal{S}_{U_d}(\sigma^i\zeta) = \sigma^i P_f \in \mathbb{Q}(P_f) \iff \bigwedge_{1\neq\zeta\in\mu_p} \mathcal{S}_{U_d}(\zeta) \in \mathbb{Q}(P_f) \subset L_d\,.$$

Also folgt mit Bemerkung IV.1.6

$$L_d = \mathbb{Q}(\mathcal{S}_{U_d}(\zeta) \mid 1 \neq \zeta \in \mu_p) \subset \mathbb{Q}(P_f) \subset L_d$$

und damit die behauptete Gleichheit $L_d = \mathbb{Q}(P_f)$ für jede f-gliedrige Periode, $fd = p-1$.

Im Fall $p = 17$ ist $p - 1 = 2^4$ eine 2-Potenz, also hat man eine Kette quadratischer Erweiterungen in $\mathbb{Q}(\mu_{17})$:

$$\mathbb{Q}(\mu_{17}) = L_{16} = \mathbb{Q}(P_1) \supset L_8 = \mathbb{Q}(P_2) \supset L_4 = \mathbb{Q}(P_4) \supset L_2 = \mathbb{Q}(P_8) \supset L_1 = \mathbb{Q}\,.$$

Jede Periode genügt also einer quadratischen Gleichung über dem nächst kleineren Körper, um also $\zeta = P_1$ durch Quadratwurzeln zu beschreiben, muss man dies sukzessive für die f-gliedrigen Perioden tun.

In jedem quadratischen Schritt $L_{2d}|L_d$ genügt $P_{f/2} \in L_{2d}$ der quadratischen Gleichung $X^2 - s_d X + n_d = 0$ mit

$$\begin{aligned} s_d &= \mathcal{S}_{L_{2d}|L_d}(P_{f/2}) = P_{f/2} + \sigma^d P_{f/2} = P_f\,,\\ n_d &= \mathcal{N}_{L_{2d}|L_d}(P_{f/2}) = P_{f/2} \cdot \sigma^d P_{f/2}\,, \end{aligned}$$

und daher gilt

$$P_{f/2} = -\frac{1}{2}P_f \pm \frac{1}{2}\sqrt{P_f^2 - 4n_d}\,.$$

Modulo 17 ist 3 eine Primitivwurzel, also wird $G(\mathbb{Q}(\zeta_{17})|\mathbb{Q})$ erzeugt von σ mit $\sigma\zeta = \zeta^3$ für $\zeta \in \mu_{17}$ und es gilt

$$P_f = \sum_{j=0}^{f-1} \sigma^{dj}\zeta = \sum_{j=0}^{f-1} \zeta^{3^{dj}} \quad (f \cdot d = 16)\,.$$

Wir erhalten so

$$\begin{aligned}
P_1=\zeta\in L_{16}:\quad s_8 &= P_2=P_1+\sigma^8P_1=\zeta+\zeta^{-1}\,,\\
n_8 &= \zeta\zeta^{-1}=1\,,\\
P_1 &= \tfrac{1}{2}P_2\pm\tfrac{1}{2}\sqrt{P_2^2-4}\,,\\
P_2\in L_8:\qquad s_4 &= P_4=P_2+\sigma^4P_2=\zeta+\zeta^{-1}+\zeta^{-4}+\zeta^4\,.\\
n_4 &= P_2\cdot\sigma^4P_2=(\zeta+\zeta^{-1})(\zeta^{-4}+\zeta^4)=\zeta^{-3}+\zeta^5+\zeta^{-5}+\zeta^3=\sigma P_4\\
P_2 &= \tfrac{1}{2}P_4\pm\tfrac{1}{2}\sqrt{P_4^2-4\sigma P_4}\\
P_4,\sigma P_4\in L_4:\quad s_8 &= P_8\,,\\
n_8 &= P_4\cdot\sigma^2P_4=(\zeta+\zeta^{-1}+\zeta^4+\zeta^{-4})(\zeta^9+\zeta^{-9}+\zeta^2+\zeta^{-2})=\ldots=-1\\
P_4 &= \tfrac{1}{2}P_8\pm\tfrac{1}{2}\sqrt{P_8^2+4}\,,\\
\sigma P_4 &= \tfrac{1}{2}\sigma P_8\pm\tfrac{1}{2}\sqrt{(\sigma P_8)^2+4}\,.
\end{aligned}$$

P_8 schließlich erzeugt den quadratischen Teilkörper von $\mathbb{Q}(\mu_{17})$ und wurde in Aufgabe 21 bestimmt:

$$P_8=w=-\frac{1}{2}+\frac{1}{2}\sqrt{17}\,,\ \sigma P_8=-\frac{1}{2}-\frac{1}{2}\sqrt{17}\,.$$

Davon ausgehend erhalten wir dann

$$\begin{aligned}
P_4 &= \tfrac{1}{2}P_8+\tfrac{1}{2}\sqrt{P_8^2+4}\,,\qquad \sigma P_4=\tfrac{1}{2}\sigma P_8+\tfrac{1}{2}\sqrt{(\sigma P_8)^2+4}\,,\\
P_2 &= \tfrac{1}{2}P_4+\tfrac{1}{2}\sqrt{P_4^2-4\sigma P_4}\\
\zeta=P_1 &= \tfrac{1}{2}P_2+\tfrac{1}{2}\sqrt{P_2^2-4}
\end{aligned}$$

Explizit ausmultipliziert (mit DERIVE):

$$\begin{aligned}
P_4 &= -\tfrac{1}{4}+\tfrac{1}{4}\sqrt{17}+\sqrt{\tfrac{17}{8}-\tfrac{1}{8}\sqrt{17}}\,,\\
\sigma P_4 &= -\tfrac{1}{4}-\tfrac{1}{4}\sqrt{17}+\sqrt{\tfrac{17}{8}+\tfrac{1}{8}\sqrt{17}}\,,\\
P_2 &= -\tfrac{1}{8}+\tfrac{1}{8}\sqrt{17}+\sqrt{\tfrac{17}{32}-\tfrac{1}{32}\sqrt{17}}+\sqrt{\tfrac{17}{16}+\tfrac{3}{16}\sqrt{17}-\sqrt{\tfrac{85}{128}+\tfrac{19}{128}\sqrt{17}}}\,,\\
\zeta=P_1 &= \tfrac{1}{2}P_2+\tfrac{1}{2}\sqrt{P_2^2-4}
\end{aligned}$$

```
SQRT(-SQRT(19*SQRT(17)/2048+85/2048)+3*SQRT(17)/64+17/64)
+SQRT(17/128-SQRT(17)/128)
+SQRT(17)/16
-1/16
+i*SQRT(
     -SQRT(
           -SQRT(5491*SQRT(17)/8388608+24565/8388608)
           +51*SQRT(17)/4096
           +289/4096
          )
      +SQRT( -SQRT(19*SQRT(17)/8388608+85/8388608) + 3*SQRT(17)/4096 +17/4096 )
      -SQRT( -SQRT(731*SQRT(17)/524288+3757/524288)
             +17*SQRT(17)/1024
             +119/1024
           )
       +SQRT(17/512-SQRT(17)/512)
```

```
-SQRT(17)/32
+17/32
)
```

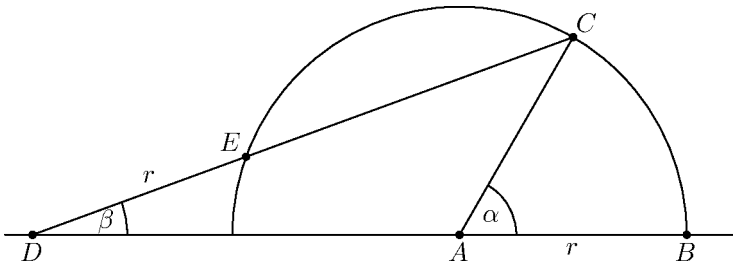
Aufgabe 34. (s)
Bestimmen Sie alle natürlichen Zahlen n, für die $\varphi(n)$ eine 2-Potenz ist (φ Eulersche Phi-Funktion).

Lösung:
Sei $n = 2^s \cdot p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ ($r, s \in \mathbb{N}$, $\nu_i \geq 1$, $p_i \neq 2$ verschiedene Primzahlen) die Primzerlegung von n. Dann gilt

$$\varphi(n) = 2^{s-1} \cdot \prod_{i=1}^{r} (p_i - 1) p_i^{\nu_i - 1} \text{ 2-Potenz } \iff \nu_i = 1 \ \wedge \ p_i - 1 \text{ 2-Potenz für alle } i.$$

Es gilt: $p = 2^t + 1$ Primzahl $\implies$ t ist eine 2-Potenz.
Annahme: t hat einen ungeraden Teiler $1 < u < t$. Dann ist $p = 2^t + 1 = 2^{uv} + 1 = (2^v)^u - (-1)^u$ teilbar durch $2^v - (-1) = 2^u + 1$ und damit nicht prim. Wid.
Also kommen in der Primzerlegung von n alle ungeraden Primteiler nur in erster Potenz vor und sind Fermatzahlen $2^{2^j} + 1$ sein.

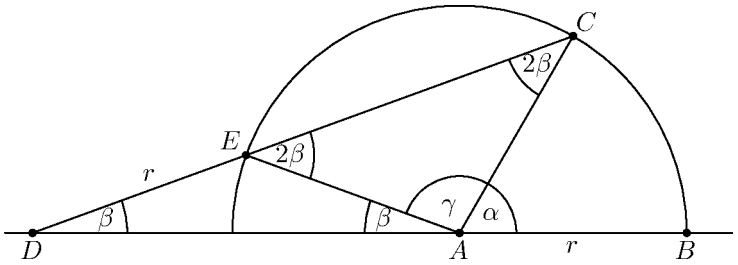
Aufgabe 35. (m)



a) Zeigen Sie: Ist der Abstand $d(D, E)$ gleich dem Kreisradius r, so ist $3\beta = \alpha$.

b) Diskutieren Sie die Problematik der Winkeldreiteilung nach dieser Methode.

Lösung:



a) Das Dreieck DEA ist gleichschenklig, also $\angle(DAE) = \beta$ und der Außenwinkel $\angle(AEC)$ bei E dann gleich 2β. Das Dreieck EAC ist ebenfalls gleichschenklig, also auch $\angle(ACE) = 2\beta$. Damit gilt $\gamma + 4\beta = 180 = \beta + \gamma + \alpha$ und folglich $\alpha = 3\beta$.
b) Zwar ist die Abtragung des Abstandes zweier (bereits konstruierter) Punkte auf einer beliebigen anderen Geraden keine der Grundkonstruktionen, aber doch mit Zirkel und Lineal möglich (siehe Aufgabe 37). Dafür muss aber die Gerade, auf der der vorgegebene Abstand abgetragen werden soll, gegeben sein. Jedoch ist keiner der beiden Punkte D, E für sich alleine konstruierbar. Keiner der Punkte ist Schnittpunkt zweier zuvor konstruierter Figuren.

Aufgabe 36. (m)

a) Konstruieren Sie zu einem gegebenen Quadrat ein Quadrat mit doppeltem Flächeninhalt.

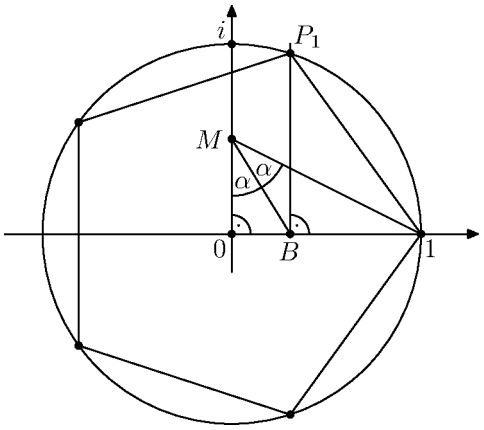
b) Dritteln Sie die Winkel 360^0, 180^0 und 90^0 mit Zirkel und Lineal.

Lösung:
a) Gegeben ein Quadrat $ABCD$. Das Quadrat über der Diagonale AC hat den doppelten Flächeninhalt: Man konstruiert also $E \in l(A, g(A, C)) \cap K(A; C)$, und dann $F \in p(E, g(A, C)) \cap l(C, g(A, C))$. Das so konstruierte Quadrat ist aus 4 zum 'Halbquadrat' ABC kongruenten Dreiecken mit gemeinsamer Spitze C zusammengesetzt, hat also den doppelten Flächeninhalt wie das Ausgangsquadrat.
b) Zwei sich schneidende Geraden bilden 4 Winkel, um einen Winkel eindeutig festzulegen, benutzen wir daher Dreiecke ABC und bezeichnen den Winkel bei A mit $\angle(BAC)$. Zur Lösung der Aufgabe genügt es den Winkel von 60^0, also ein gleichschenkliges Dreieck zu konstruieren: Ist $A \in K(0; 1) \cap K(1; 0)$, so ist $0 \neq A \neq 1$ und $01A$ ein gleichseitiges Dreieck mit dem Winkel $\angle(A01)$ von 60^0
Die beiden anderen geforderten Winkel von 120^0 bzw. 30^0 erhält man durch Verdopplung bzw. Halbierung. Verdopplung und Halbierung von Winkeln ist mit Zirkel und Lineal möglich.
Gegeben der Winkel $\angle(BAC)$. Halbierung:
1. $C' \in g(A, B) \cap K(A; C)$.
2. $D \in K(C; C') \cap K(C'; C)$, $A \neq D$.
3. $E \in g(B, C) \cap g(A, D)$.
Dann ist $\angle(CAE)$ halb so groß wie der gegebene.
Verdopplung: 1. wie oben
2. $D \in K(A; C) \cap K(C'; C)$, $D \neq C$
Dann ist der Winkel $\angle(CAD)$ doppelt so groß wie der gegebene.

Aufgabe 37. (s)
Zeigen Sie, dass das fragwürdige Abtragen von Radien eine unnötige Grundoperation ist, d. h.: Konstruieren Sie mit Zirkel und Lineal zu zwei Punkten A, B, einer Geraden g und einem Punkt $C \in g$ einen Punkt $D \in g$ mit $d(A, B) = d(C, D)$.

Lösung:
Ergänze im Falle $C \notin g(A, B)$ ABC zu einem Parallelogramm: $D' \in p(C, g(A, B)) \cap p(B, g(A, C))$ ist konstruierbar und es gilt $d(A, B) = d(C, D')$. Schlage dann den Kreis um C durch D' und finde D: $D \in K(C; D') \cap g$. Nach Konstruktion $d(C, D) = d(C, D') = d(A, B)$.
Sind A, B, C kollinear, so konstruiert man zunächst auf der Senkrechten $l(A, g(A, B))$ einen Punkt B' mit $d(A, B) = d(A, B')$: $B' \in K(A; B) \cap l(A, g(A, B))$. Wegen $B' \notin g(A, B)$ sind dann A, B', C nicht kollinear. Wie oben konstruiert man dann $D \in g$ mit $d(C, D) = d(A, B') = d(A, B)$.

Aufgabe 38. (s)
Konstruieren Sie mit Zirkel und Lineal ein regelmäßiges Fünfeck. Begründen Sie Ihre Konstruktion.
[Tip: Nachstehende Skizze und Additionstheorem des Tangens.]



Lösung:
Konstruiere $\mathbb{R} = g(0,1)$, $i\mathbb{R} = l(0,\mathbb{R})$, Einheitskreis $EK = K(0;1)$, $i \in i\mathbb{R} \cap EK$, M Mittelpunkt zwischen 0 und i, Winkelhalbierende w des Winkels $\angle(0M1)$, $B \in w \cap \mathbb{R}$, $P_1 \in EK \cap l(B,\mathbb{R})$. Dann ist der Winkel $\angle(1\,0\,P_1)$ ein Fünftel des Vollwinkels und $P_1 = e^{2\pi i/5} = \zeta_5$. Die übrigen Eckpunkte des Fünfecks erhält man durch Winkelverdopplung.
Begründung: Sei $b = \operatorname{Re} B = d(0,B)$. Dann gilt nach Konstruktion

$$\tan(\alpha) = \frac{b}{1/2} = 2b\,, \quad \tan(2\alpha) = \frac{1}{1/2} = 2\,.$$

Wegen $\tan(2\alpha) = \frac{2\tan\alpha}{1-\tan^2\alpha}$ folgt

$$2(1-4b^2) = 4b \iff b^2 + \frac{1}{2}b - \frac{1}{4} = 0 \iff b = -\frac{1}{4} + \frac{1}{4}\sqrt{5}\,.$$

Nach Übung 5, Aufgabe 18 ist $b = \operatorname{Re}\zeta_5$ und folglich der Punkt P_1 auf dem Einheitskreis gleich ζ_5.

Algebra II
Übung 9

Aufgabe 39. (m)

a) Wiederholen Sie aus Algebra I die grundlegenden Begriffsbildungen und Fakten über Operationen von Gruppen auf Mengen (Bahnen, Fixgruppen, Bahnenzerlegung, Bahnengleichung)

und zeigen Sie für $G \leq \mathcal{S}(\Omega)$, $\#\Omega = n$:

b) G transitiv auf $\Omega \implies n \mid \#G$.

c) G k-fach transitiv auf $\Omega \iff G$ transitiv und G_α $(k-1)$-fach transitiv auf $\Omega \setminus \{\alpha\}$ für ein/alle $\alpha \in \Omega$.

d) G k-fach transitiv $\implies n(n-1)\dots(n-k+1) \mid \#G$.

Ist G scharf k-fach transitiv, so gilt $n(n-1)\dots(n-k+1) = \#G$.

e) $G \leq \mathcal{S}_n$ $\begin{Bmatrix} n-2 \\ n-1 \end{Bmatrix}$-fach transitiv $\iff G = \begin{cases} \supseteq \mathcal{A}_n \\ = \mathcal{S}_n \end{cases}$.

$\begin{Bmatrix} \mathcal{A}_n \\ \mathcal{S}_n \end{Bmatrix}$ ist scharf $\begin{Bmatrix} n-2 \\ n \end{Bmatrix}$-fach transitiv.

Lösung:
b) Gemäß Bahnengleichung gilt für transitives G: $n = \#\Omega = \#G\alpha = (G : G_\alpha) \mid \#G$.
c) $\Rightarrow$: G k-fach transitiv und $k \geq 1 \implies G$ transitiv. Seien $\alpha_2, \dots, \alpha_k \in \Omega \setminus \{\alpha\}$ verschieden und $\beta_2, \dots, \beta_k \in \Omega \setminus \{\alpha\}$ verschieden. Dann existiert zu $\alpha, \alpha_2, \dots, \alpha_k$ und $\alpha, \beta_2, \dots, \beta_k$ ein $\sigma \in G$ mit $\sigma\alpha = \alpha$, also $\sigma \in G_\alpha$, und $\sigma\alpha_i = \beta_i$ für $i \geq 2$. G_α ist somit $k-1$-fach transitiv auf $\Omega \setminus \{\alpha\}$.
$\Leftarrow$: Seien α_i bzw. β_i $(1 \leq i \leq k)$ jeweils paarweise verschieden in Ω gegeben. Sei $\alpha \in \Omega$ mit G_α $(k-1)$-fach transitiv. Da G transitiv ist, existieren $\sigma, \tau \in G$ mit $\sigma\alpha_1 = \alpha = \tau\beta_1$. Setze für $i \geq 2$ $\alpha_i' = \sigma\alpha_i$ bzw. $\beta_i' = \tau\beta_i$. Dann sind auch diese jeweils paarweise verschieden und $\alpha_i', \beta_i' \in \Omega \setminus \{\alpha\}$. Also gibt es nach Voraussetzung ein $\rho \in G_\alpha$ mit $\rho\alpha_i' = \beta_i'$, also $\rho\sigma\alpha_i = \tau\beta_i$ für $i \geq 2$. Außerdem gilt $\rho\sigma\alpha_1 = \rho\alpha = \alpha = \tau\beta_1$. Daher erfüllt $\tilde{\rho} := \tau^{-1}\rho\sigma \in G$ die Forderung $\tilde{\rho}\alpha_i = \beta_i$ für alle $1 \leq i \leq k$.
d) Sei $k \leq n$ und $\alpha_1, \dots \alpha_k \in \Omega$ verschieden. Da G k-fach transitiv ist, folgt für $1 \leq j < k$ nach c) rekursiv $G_{\alpha_1,\dots,\alpha_j}$ ist $k-j$-transitiv auf $\Omega \setminus \{\alpha_1, \dots, \alpha_j\}$. Daher gilt nach b)

$$\begin{aligned} k - j \geq 1 &\implies n - j = \#\Omega \setminus \{\alpha_1, \dots, \alpha_j\} = (G_{\alpha_1,\dots,\alpha_j} : G_{\alpha_1,\dots,\alpha_{j+1}}) \\ &\implies n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = (G : G_{\alpha_1,\dots,\alpha_k}) \mid \#G \end{aligned}$$

Ist G scharf k-transitiv, so existiert genau ein $\sigma \in G$ mit $\sigma\alpha_i = \alpha_i$ für $1 \leq i \leq k$, nämlich $\sigma = \mathrm{id}$. Dies bedeutet $\#G_{\alpha_1,\dots,\alpha_k} = 1$ und es gilt die behauptete Gleichheit.
e) $\Rightarrow$: Ist G $(n-1)$-fach transitiv, so folgt $n(n-1)\dots\cdot 2 = n! \mid \#G$ und $G = \mathcal{S}_n$. Sei nun G $(n-2)$-fach transitiv, also $n(n-1)\cdot\ldots\cdot 3 = \frac{n!}{2} \mid \#G$ und somit $(\mathcal{S}_n : G) \leq 2$. Wir zeigen:

$$G \leq \mathcal{S}_n \ \wedge \ (\mathcal{S}_n : G) = 2 \implies \mathcal{A}_n \subset G \implies G = \mathcal{A}_n\,.$$

Beweis: Als Untergruppe vom Index 2 ist G Normalteiler in $\mathcal{S}_n$.
$n \geq 5$: Wäre $\mathcal{A}_n \not\subset G$, so wäre $G \cap \mathcal{A}_n \trianglelefteq \mathcal{A}_n$ ein echter Normalteiler in $\mathcal{A}_n$, wegen der Einfachheit von $\mathcal{A}_n$ also $G \cap \mathcal{A}_n = \{e\}$. Dies kann nicht sein, da dann $\#\mathcal{A}_n = (\mathcal{A}_n : \mathcal{A}_n \cap G) \leq (\mathcal{S}_n : G) = 2$ wäre.
$n = 4$: $6 \mid \#G \implies G$ enthält ein Element ρ der Ordnung 3. Wegen $n = 4$ kann ρ nur ein

3-Zyklus sein. Also enthält der Normalteiler G *alle* 3-Zyklen, $\mathcal{A}_4 \subseteq G$.
$n = 3$: $\mathcal{A}_3$ ist die einzige Untergruppe der Ordnung 3 bzw. vom Index 2.
$n = 2$: $\#G = 1 = \#\mathcal{S}_2$.
ad $\Leftarrow$: Offenbar ist $\mathcal{S}_n$ scharf n-transitiv.
Seien nun $a_1, \ldots, a_{n-2}$ bzw. $b_1, \ldots, b_{n-2}$ verschiedene Elemente in $\Omega = \{1, \ldots, n\}$ und a_{n-1}, a_n bzw. b_{n-1}, b_n die jeweils verbleibenden zwei Elemente in Ω. Dann existiert $\sigma \in \mathcal{S}_n$ mit $\sigma a_i = b_i$ für alle i. Ist nun $\sigma \in \mathcal{A}_n$, so ist man fertig. Andernfalls ist $\tilde{\sigma} := (b_{n-1}\, b_n) \circ \sigma \in \mathcal{A}_n$ und es gilt $\tilde{\sigma} a_i = (b_{n-1}, b_n)(b_i) = b_i$ für $1 \leq i \leq n-2$. Da σ und $\tilde{\sigma}$ die einzigen Elemente $\rho \in \mathcal{S}_n$ sind mit $\rho a_i = b_i$ für $1 \leq i \leq n-2$, aber nur eines davon in $\mathcal{A}_n$ liegt, ist $\mathcal{A}_n$ scharf $(n-2)$-transitiv.

Aufgabe 40. (m)
Sei $G \leq \mathcal{S}(\Omega)$ eine transitive Permutationsgruppe. Zeigen Sie:

a) Ist $\emptyset \neq B \subset \Omega$ ein Block für G, so besteht $\mathcal{B} := \{\sigma B \mid \sigma \in G\}$ aus lauter G-Blöcken, die Ω disjunkt überdecken.

b) Die Mächtigkeit $\#B$ eine Blockes B teilt die Mächtigkeit $\#\Omega$.

c) Ist $\#\Omega = p$ eine Primzahl, so ist operiert G primitiv auf Ω.

d) Ist die Operation von G auf Ω 2-fach transitiv, so ist sie auch primitiv.

Lösung:
a) Sei B ein G-Block und $\sigma \in G$. Dann gilt für alle $\tau \in G$

$$\tau\sigma B \cap \sigma B \neq \emptyset \implies \sigma^{-1}\tau\sigma B \cap B \neq \emptyset \underset{B \text{ Block}}{\Longrightarrow} \sigma^{-1}\tau\sigma B = B \implies \tau\sigma B = \sigma B\,.$$

Da G transitiv operiert und B nicht leer ist, überdecken die σB ganz Ω. Da B ein Block ist, sind die *verschiedenen* σB disjunkt.
b) Nach a) ist $\Omega = \dot{\bigcup}_{B' \in \mathcal{B}}$ und $\#B' = \#\sigma B = \#B$, also $\#\Omega = \#\mathcal{B} \cdot \#B$.
c) $\Omega = p$ hat nur die Teiler 1 und p, also sind nach b) nur die trivialen Blöcke möglich: G ist primitiv.
d) Indirekt: Sei B ein Block mit $2 \leq \#B < \#\Omega$ (ein *Imprimitivitätsgebiet* für G). Wähle $b_1 \neq b_2$ in B und $a_2 \notin B$. Da G 2-fach transitiv ist, existiert ein $\sigma \in G$ mit $\sigma b_1 = b_1$ und $\sigma b_2 = a_2$. Also gilt $b_1 \in \sigma B \cap B \neq \emptyset$ und daher $\sigma B = B$, im Widerspruch zu $\sigma b_2 = a_2 \notin B$.

Aufgabe 41. (s)
Sei $G \leq \mathcal{S}(\Omega)$ eine Permutationsgruppe. Zeigen Sie:

a) Ist G primitiv, so ist jeder Normalteiler $1 \neq N \lhd G$ transitiv.

b) Sei $N \neq 1$ ein minimaler Normalteiler in G. Ist N abelsch und transitiv auf Ω, so ist G primitiv.

Lösung:
a) Ist B eine N-Bahn in Ω, so ist B ein Block für G. Denn: $\sigma B \cap B \neq \emptyset \implies \sigma\alpha = \beta$ mit $\alpha, \beta \in B$. Da B eine Bahn unter N ist, ist $N\alpha = N\beta = B$ und daher $\sigma B = \sigma N\alpha \underset{N \lhd G}{=} N\sigma\alpha = N\beta = B$.
Wegen $N \neq 1$ gibt es eine Bahn $N\alpha = B$ mit $\#B \geq 2$. Da G primitiv und B ein Block ist, folgt $N\alpha = B = \Omega$, N operiert transitiv.
b) N transitiv $\implies$ $N\alpha = \Omega$ und alle Fixgruppen N_α, N_β sind in N konjugiert. Da N abelsch ist, folgt $N_\alpha = N_\beta$ für alle $\alpha, \beta \in \Omega$ und daher $N_\alpha = \bigcap_\beta N_\beta = \{\mathrm{id}\}$. Damit ist $N \to \Omega$, $\rho \mapsto \rho\alpha$ bijektiv!
Sei nun B ein G-Block, also auch ein N-Block und damit $B = Hb$ für eine Untergruppe $H \leq N$ (vgl. Beweis von Prop. V.1.5 b)).
Wir zeigen: $(*)$ $\quad H \lhd G$.

Daraus folgt dann wegen der Minimalität von N: $H = 1$, $B = \{b\}$ oder $H = N$, $B = Nb = \Omega$. Also sind alle G-Blöcke trivial und G ist primitiv.
Beweis von $(*)$: Sei $\sigma \in G$. Wähle $\rho \in N$ mit $\rho b = \sigma b$, also $\sigma^{-1}\rho b = b$. Dann gilt $\sigma^{-1}\rho B \cap B \neq \emptyset$ und folglich $\sigma^{-1}\rho B = B$, also wegen $H \leq N \lhd G$

$$Hb = B = \sigma^{-1}\rho H b = \sigma^{-1}\rho H \cdot \rho^{-1}\sigma b\,.$$

Wegen der Bijektivität von $N \to Nb = \Omega$ gilt daher $H = \sigma^{-1}\rho H \rho^{-1}\sigma$. Wegen $\rho \in N$, $H \leq N$ und der Kommutativität von N folgt dann $H = \sigma^{-1} H \sigma$ und $(*)$ ist bewiesen.

Aufgabe 42. (s)
Sei $K = \mathbb{F}_q$ der endliche Körper mit $q = p^f$ Elemente, $p = \operatorname{char} K$, $f \in \mathbb{N}$. Es sei $\Omega = K \cup \{\infty\}$ die projektive Gerade über K. Wir betrachten die Gruppe der gebrochen linearen Funktion

$$G := \mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{PGL}(2,q) = \{\frac{ax+b}{cx+d} \mid a,b,c,d \in \mathbb{F}_q\,,\ ad - bc \neq 0\}$$

als Permutationsgruppe auf Ω vermöge $x \mapsto \frac{ax+b}{cx+d}$ mit den üblichen Konventionen für ∞:

$$\frac{a}{0} = \infty \text{ für } a \neq 0\,, \quad \frac{a\infty + b}{c\infty + d} = \frac{a}{c} \text{ für } c \neq 0\,.$$

a) Bestimmen Sie die Fixgruppen G_∞ und $G_{\infty,0}$.

b) Zeigen Sie: G operiert scharf 3-fach transitiv auf Ω.

c) $\#G = (q+1)q(q-1)$.

Lösung:
a) $\sigma = \frac{ax+b}{cx+d} \in G_\infty \iff \infty = \sigma\infty = \frac{a}{c} \iff c = 0 \iff \sigma = a'x + b' \in A(1,q)$. Daraus folgt dann $\sigma \in G_{\infty,0} = A(1,q)_0 \iff \sigma = ax$ $(a \in K^\times)$.
b) $a \in K^\times \implies ax$ bildet 1 auf a ab, also ist $G_{\infty,0}$ transitiv auf $\Omega \setminus \{\infty, 0\} = K^\times$,
$x - 1 \in G_\infty$ bildet 1 auf 0 ab, also ist G_∞ transitiv auf K,
$\frac{1}{x-1}$ bildet 1 auf ∞ ab, also ist G transitiv auf Ω.
Insgesamt ist damit G 3-fach transitiv auf Ω (siehe Aufgabe 39.c)). G ist sogar scharf 3-fach transitiv, denn hat $\sigma \in G$ drei Fixpunkte, so ist $\sigma = \mathrm{id}$:

$$\sigma \in G_{\infty,0,1} \iff \sigma = ax \ \wedge\ \sigma 1 = 1 \iff a = 1\,,\ \sigma = \mathrm{id}\,.$$

c) folgt aus Aufgabe 39.d), denn $\#\Omega = q + 1$.

Aufgabe 43. (s)
Sei $K = \mathbb{F}_q$, $q = p^f$ wie in Aufgabe 42 und

$$\Gamma(q) := \{a\sigma + b \mid \sigma \in \mathrm{Aut}(K)\,, a,b \in K\,, a \neq 0\}$$

die Gruppe ser *semilinearen* Abbildungen von K. Zeigen Sie:

a) $A(1,q)$ ist Normalteiler in $\Gamma(q)$ mit zyklischer Faktorgruppe der Ordnung f.

b) $\Gamma(q)$ ist auflösbar von der Ordnung $q(q-1)\cdot f$.

c) $\Gamma(q)$ ist 2-fach transitiv auf K;
$\Gamma(q)$ 3-fach transitiv $\iff q = 3 \ \vee\ q = 4$. Es ist $\Gamma(3) \simeq \mathcal{S}_3$ und $\Gamma(4) \simeq \mathcal{S}_4$.

Lösung:
a) $\rho \in \Gamma(q) \implies \rho = a\sigma + b = (ax+b) \circ \sigma$ mit $ax+b \in A(1,q)$ und $\sigma \in \mathrm{Aut}(K)$. Also ist

$$A(1,q) \lhd \Gamma(q) \iff \bigwedge_{\tau \in \mathrm{Aut}(K)} \tau A(1,q) = A(1,q)\tau\,.$$

Es gilt in der Tat $\tau \circ (ax+b) = \tau(a)\tau(x) + \tau(b) = (\tau(a)x + \tau(b)) \circ \tau \in A(1,q)\tau$.
Damit ist Surjektivität von $\mathrm{Aut}(K) \to \Gamma(q)/A(1,q)$, $\sigma \mapsto \sigma A(1,q)$ gezeigt. Zur Injektivität: $\sigma \in A(1,q) \iff \sigma = ax+b \implies 0 = b \implies 1 = a \implies \sigma = \mathrm{id}$.
Damit ist $\Gamma(q)/A(1,g) \simeq \mathrm{Aut}(\mathbb{F}_{p^f}) = G(\mathbb{F}_{p^f}|\mathbb{F}_p)$ zyklisch von der Ordnung $(\mathbb{F}_{p^f} : \mathbb{F}_p) = f$.
b) $A(1,q) = \{ax+b \mid a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q\}$ hat den Normalteiler $T = \{x+b \mid b \in \mathbb{F}_q\}$ mit Faktorgruppe $A(1,q) \simeq \{ax \mid a \in \mathbb{F}_q^\times\}$. Damit erhalten wir folgende Normalreihe

$$\Gamma(q) \rhd A(1,q) \rhd T \rhd \{id\}$$

mit den abelschen Faktoren

$\Gamma(q)/A(1,q) \simeq G(\mathbb{F}_q|\mathbb{F}_p)$ zyklisch von der Ordnung f,

$A(1,q)/T \simeq \mathbb{F}_q^\times$ zyklisch von der Ordnung $q-1$,

$T \simeq (\mathbb{F}_q, +)$ elementarabelsch von der Ordnung $p^f = q$.

Somit ist $\Gamma(q)$ auflösbar von der Ordnung $q(q-1)\cdot f$.
c) Bereits $A(1,q)$ ist 2-fach transitiv auf $\mathbb{F}_q$ (siehe Aufgabe 42.a)). Ist $\Gamma(q)$ 3-fach transitiv, so gilt

$$q(q-1)(q-2) \mid q(q-1)f \implies p^f - 2 \mid f \implies p^f = 4 \ \vee \ p^f = 3\,,$$

denn: $p^f - 2 - f$ ist bei festem p als Funktion von $f \in \mathbb{R}$ streng monoton steigend und es gilt

$$\begin{aligned}
p > 3 &\implies p^f - 2 - f \geq p^1 - 2 - 1 > 0 \implies p^f - 2 \not| f \text{ für alle } f \geq 1\,,\\
p = 3 &\implies p^f - 2 - f > p - 2 - 1 = 0 \implies p^f - 2 \not| f \text{ für alle } f \geq 2\,,\\
p = 2 &\implies p^f - 2 - f > p^2 - 2 - 2 = 0 \implies p^f - 2 \not| f \text{ für alle } f \geq 3\,.
\end{aligned}$$

Umgekehrt: $\Gamma(q) \leq \mathcal{S}_q$ und es gilt $\#\Gamma(2^2) = 4 \cdot 3 \cdot 2 = 4!$ bzw. $\#\Gamma(3) = 3 \cdot 2 = 3!$, also ist für $q = 3, 4$ $\Gamma(q) = \mathcal{S}_q$) und damit 3-transitiv.

Aufgabe 44. (s)
Beweisen Sie den *Satz von Galois*: Für ein irreduzibles Polynom von Primzahlgrad über einem Körper k der Charakteristik 0 sind äquivalent:

(i) f ist durch Radikale auflösbar.

(ii) Der Zerfällungskörper von f wird bereits von zwei beliebigen Wurzeln von f erzeugt.

(iii) $G(f)$ ist als Permutationsgruppe (isomorph zu einer) Untergruppe von $A(1,p)$.

(iv) Der Zerfällungskörper $K|k$ von f enthält einen galoisschen Teilkörper $L|k$ mit $(K : L) = p$.

Lösung:
Dieser Satz ist eine Umformulierung von Satz V.1.8: Sei $K = k(W_f)$ der Zerfällungskörper des (wegen der Irreduzibilität und $\mathrm{char}\, K = 0$) separablen Polynoms f. Dann ist $G := G(K|k) \simeq$

$G(f)$ und $G(f)$ transitiv von Primzahlgrad p. Nun gilt

(i) $\underset{\text{IV.3.3}}{\iff}$ G auflösbar $\iff$ Satz V.1.8 (i),

(ii) $\iff$ $K = k(\alpha, \beta)$ für $\alpha, \beta \in W_f, \alpha \neq \beta$,

$\iff$ $\mathrm{Fix}_G K = \mathrm{Fix}_G\{\alpha, \beta\}$ $\iff$ $\{\mathrm{id}\} = G(f)_{\alpha,\beta}$

$\iff$ Satz V.1.8 (iii).

(iii) $\iff$ Satz V.1.8 (ii)

(iv) $\iff$ $G(f)$ enthält einen Normalteiler der Ordnung p

$\iff$ $G(f)$ hat genau eine p-Sylowgruppe (Sylowsätze, $p^2 \nmid \#\mathcal{S}_p$)

$\iff$ V.1.8 (iv)

Algebra II
Übung 10

Aufgabe 45. (m)
Sei K ein Körper der Charakteristik 0 und $b = (b_i)_{i\in\mathbb{Z}} \in K^{\mathbb{Z}}$ eine Funktion $\mathbb{Z} \to K$, als $\mathbb{Z}$-indizierte Folge notiert.Dann definiert man die Folgen $\Delta^k b \in K^{\mathbb{Z}}$ durch

$$\Delta^0 b := b\,, \quad \Delta^k b := \Delta(\Delta^{k-1} b)\ (k \in \mathbb{N}_+)\,, \qquad (\Delta b)_\nu := b_{\nu+1} - b_\nu\ (\nu \in \mathbb{Z})\,.$$

[Man schreibt oft ungenau $\Delta b_\nu := (\Delta b)_\nu$.] Zeigen Sie:

a) $(\Delta^k b)_\nu = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} b_{\nu+j}$, also ist $(\Delta^k b)_\nu$ bereits durch $b_\nu, b_{\nu+1}, \ldots, b_{\nu+k}$ festgelegt.
Rechenschema:

$$\begin{array}{ccccccccccc}
\ldots & b_0 & & b_1 & & b_2 & & b_3 & & b_4 & & b_5 & \ldots \\
& \ldots & \Delta b_0 & & \Delta b_1 & & \Delta b_2 & & \Delta b_3 & & \Delta b_4 & \ldots & \\
& & \ldots & \ldots & \Delta^2 b_0 & & \Delta^2 b_1 & & \Delta^2 b_2 & & \Delta^2 b_3 & \ldots & \\
\end{array}$$

b) (Interpolationsformel von Newton)
Sind $a_i = a_0 + ih$ äquidistante Punkte in K ($h \in K^\times$) und $b_i \in K$ beliebig, so ist

$$f_s(X) := \sum_{k=0}^{s} \frac{\Delta^k b_0}{k! h^k} (X - a_0) \ldots (X - a_{k-1})$$

das (eindeutig bestimmte) Polynom in $K[X]$ mit $\deg f \le s$ und $f(a_i) = b_i$ für $0 \le i \le s$.

c) Unter welcher Bedingung an $\Delta^k b$ gibt es ein Polynom f mit $f(a_i) = b_i$ für alle $i \in \mathbb{N}$?

d) Interpolieren Sie in $\mathbb{Q}$ die Werte

a_i	-4	-3	-2	-1	0	1	2	3	4
b_i	-59	-23	-5	1	1	1	7	25	61

durch ein Polynom kleinstmöglichen Grades.

e) Vergleichen Sie die Interpolationsformeln von Lagrange und Newton (Vor-/Nachteile).

Lösung:
a) $k = 0$ ist klar. $k \to k+1$:

$$\begin{aligned}
&(\Delta^{k+1} b)_\nu = (\Delta^k b)_{\nu+1} - (\Delta^k b)_\nu \\
&= \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} b_{\nu+1+j} - \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} b_{\nu+j} \\
&= b_{\nu+1+k} + \sum_{j=1}^{k} (-1)^{k-j+1} \binom{k}{j-1} b_{\nu+j} - \sum_{j=1}^{k} (-1)^{k-j} \binom{k}{j} b_{\nu+j} - (-1)^k b_\nu \\
&= b_{\nu+1+k} + \sum_{j=1}^{k} (-1)^{k+1-j} \Big[\binom{k}{j-1} + \binom{k}{j} \Big] b_{\nu+j} - (-1)^k b_\nu \\
&= \sum_{j=0}^{k+1} (-1)^{k+1-j} \binom{k+1}{j} b_{\nu+j}
\end{aligned}$$

b) $s = 0$ ist klar. $s - 1 \to s$: Es ist

$$f_s(X) = f_{s-1}(X) + \frac{\Delta^s b_0}{s!h^s}(X - a_0)\dots(X - a_{s-1})\,.$$

und daher $f_s(a_i) = f_{s-1}(a_i) = b_i$ für $0 \le i \le s-1$.

$$\begin{aligned}
f_s(a_s) &= \sum_{k=0}^{s} \tfrac{\Delta^k b_0}{k!h^k}(a_s - a_0)\dots(a_s - a_{k-1}) \\
&= \sum_{k=0}^{s}\sum_{j=0}^{k}(-1)^{k-j}\tbinom{k}{j}\tfrac{1}{k!h^k}b_j \cdot sh\cdot(s-1)h\dots(s-k+1)h \\
&= \sum_{0\le j\le k\le s}(-1)^{k-j}\tbinom{k}{j}\tfrac{s(s-1)\dots(s-k+1)}{k!}\cdot b_j \\
&= \sum_{j=0}^{s}\Big[\sum_{k=j}^{s}(-1)^{k-j}\tbinom{k}{j}\tfrac{s(s-1)\dots(s-k+1)}{k!}\Big]\cdot b_j \\
[\dots] &= \sum_{k=j}^{s}(-1)^{k-j}\tfrac{k!}{j!(k-j)!}\tfrac{s!}{k!(s-k)!} = \sum_{l=0}^{s-j}(-1)^l\tfrac{s!}{j!l!(s-l-j)!} \\
&= \sum_{l=0}^{s-j}(-1)^l\tfrac{s!}{j!(s-j)!}\tfrac{(s-j)!}{l!(s-l-j)!} \\
&= \tbinom{s}{j}\sum_{l=0}^{s-j}(-1)^l\tbinom{s-j}{l} = \tbinom{s}{j}(1-1)^{s-j} = \begin{cases}0 & \text{für } j<s\\ 1 & \text{für } j=s\end{cases} \\
f(a_s) &= b_s
\end{aligned}$$

c) Gibt es ein solches Polynom f und ist d sein Grad, so muss für alle $s \ge d$ $f = f_s$ sein, denn f erfüllt die für f_s geforderten Bedingungen ($\deg f \le s$ und $f(a_i) = b_i$ für $0 \le i \le s$) und f_s ist eindeutig. Ein solches f existiert also genau dann, wenn für ein d und alle $s > d$ $f_s = f_d$ bzw. $f_s = f_{s-1}$ ist. Nun gilt

$$\begin{aligned}
&\bigwedge_{s>d} 0 = f_s - f_{s-1} = \frac{\Delta^s b_0}{s!h^s}(X - a_0)\dots(X - a_{s-1}) \\
&\iff \bigwedge_{s\ge d+1}\Delta^s b_0 = 0 \iff \bigwedge_{\nu\ge 0}\Delta^{d+1}b_\nu = 0
\end{aligned}$$

Zur letzten Äqivalenz: $\Leftarrow$ ist klar. ad $\Rightarrow$: Induktiv. $\nu = 0$ klar. $\nu \to \nu + 1$:

$$\Delta^{d+1}b_{\nu+1} = \Delta^{d+1}b_{\nu+1} - \underbrace{\Delta^{d+1}b_\nu}_{=0 \text{ Ind.Vor.}} = \Delta^{d+2}b_\nu = 0\,.$$

Fazit: Es gibt ein Polynom f mit $f(a_i) = b_i$ für alle $i \in \mathbb{N}$, wenn ein d existiert mit $\Delta^{d+1}b_\nu = 0$ für alle $\nu \ge 0$. Es ist dann $f = f_d$ und das minimale derartige d ist der Grad von f.

d/e) An diesem Beispiel zeigt sich der Vorteil der Newtonschen Formel. Der Theorie gemäß gibt es genau ein Polynom f höchstens vom Grade 8 mit $f(a_i) = b_i$ $(0 \le i \le 8)$ wie gefordert. Dieses ist aber nur vom Grade 3, weil $\Delta^4 b_i = 0$ $(0 \le i \le 4)$ und damit $\Delta^s b_0 = 0$ ist für $4 \le s \le 8$, wie man leicht berechnet.

a_i	-4	-3	-2	-1	0	1	2	3	4
b_i	-59	-23	-5	1	1	1	7	25	61
Δ^1	36	18	6	0	0	6	18	36	
Δ^2	-18	-12	-6	0	6	12	18		
Δ^3	6	6	6	6	6	6			
Δ^4	0	0	0	0	0				

Interpoliert man die 4 Werte $1, 1, 1, 7$ bei $-1, 0, 1, 2$, so erhält man aus dem entsprechenden Teil des obigen Differenzenschemas (der Spalte bei -1) gemäß b)

$$f(X) = 1 + 0\cdot(x+1) + 0\cdot(x+1)x + \frac{6}{3!}(x+1)x(x-1) = (x+1)x(x-1) + 1$$

Bei Benutzung der Lagrangeschen Form ergäbe sich natürlich dasselbe Ergebnis, jedoch nach ungleich längerer Rechnung. Der entscheidende Vorteil der Newtonschen Form liegt darin, dass bei Erweiterung der Stützstellen, die bisher berechneten Interpolationen nur durch einen Zusatzterm ergänzt werden.

Aufgabe 46. (s)
Sei $K|\mathbb{Q}$ eine endliche Erweiterung und $\alpha \in K$. Zeigen Sie:

a) $f_{\alpha,\mathbb{Q}} \in \mathbb{Z}[X] \iff$ es gibt ein *normiertes* Polynom $g \in \mathbb{Z}[X]$ mit $g(\alpha) = 0$
($\iff$: α ist *ganz über* $\mathbb{Z}$)

b) $\alpha \in K$ ganz über $\mathbb{Z} \iff$ es gibt einen endlich erzeugten $\mathbb{Z}$-Untermodul $M \subset K$ mit $\mathbb{Z}[\alpha] \subseteq M$.
[Tip zu $\Leftarrow$: $\alpha\alpha_j = \sum_{i=1}^{r} a_{ij}\alpha_i$ für $\mathbb{Z}[\alpha] \subseteq M = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_r$.]

c) $R_K := \{\alpha \in K \mid \alpha \text{ ganz über } \mathbb{Z}\}$ ist ein unitärer Unterring von K.

d) K ist der Quotientenkörper von R_K; genauer:

$$\text{Für jedes } \alpha \in K \text{ gibt es ein } 0 \neq d \in \mathbb{Z} \text{ mit } d\alpha \in R_K.$$

Lösung:
a) $\Rightarrow$ ist klar. $\Leftarrow$: Sei $g \in \mathbb{Z}[X]$ normiert mit $g(\alpha) = 0$. Zerlege g im faktoriellen Ringe $\mathbb{Z}[X]$ in Primfaktoren $g = g_1 \cdot \ldots \cdot g_r$; da g normiert ist, sind die führenden Koeffizienten der g_i Einheiten in $\mathbb{Z}$, also können die g_i normiert gewählt werden. Nach dem Lemma von Gauß sind die g_i irreduzibel über $\mathbb{Q}$. α ist Nullstelle eines der irreduziblen normierten g_i, also folgt $f_{\alpha,\mathbb{Q}} = g_i \in \mathbb{Z}[X]$.
b) $\Rightarrow$: Analog zum Körperfall zeigt man $\mathbb{Z}[\alpha]$ selbst ist endlich erzeugter $\mathbb{Z}$-Modul:

$$f_{\alpha,\mathbb{Q}} \in \mathbb{Z}[X] \implies \alpha^n = \sum_{i=0}^{n-1} a_i\alpha^i \in \sum_{i=0}^{n-1} \mathbb{Z}\alpha^i$$

$$\underset{\text{induktiv}}{\Longrightarrow} \alpha^\nu \in \sum_{i=0}^{n-1} \mathbb{Z}\alpha^i \text{ für alle } \nu \implies \mathbb{Z}[\alpha] = \sum_{i=0}^{n-1} \mathbb{Z}\alpha^i \text{ endlich erzeugt.}$$

$\Leftarrow$: Sei $\mathbb{Z}[\alpha] \subset M = \sum_{i=1}^{r} \mathbb{Z}\alpha_i$ und $\alpha_i \neq 0$, also

$$\bigwedge_{j=1}^{r} \alpha\alpha_j = \sum_{i=1}^{r} a_{ij}\alpha_i \quad \text{mit } a_{ij} \in \mathbb{Z}\,.$$

Dies bedeutet: Das homogene lineare Gleichungssystem $\sum_{i=1}^{r} (\alpha\delta_{ij} - a_{ij})x_i = 0$ $(j = 1, \ldots, r)$ hat die (nicht-triviale) Lösung $(\alpha_1, \ldots, \alpha_r)$ in K. Also gilt $\det(\alpha\delta_{ij} - a_{ij}) = 0$ und α ist Nullstelle des charakteristischen Polynoms $\det(X\delta_{ij} - a_{ij})$, einem normierten Polynom vom Grade r mit Koeffizienten in $\mathbb{Z}$, d. h. α ist ganz über $\mathbb{Z}$.
c) Für beliebige $\alpha, \beta \in R_K$ gilt:

$$\alpha, \beta \in R_K \underset{\text{b)}}{\Longrightarrow} \mathbb{Z}[\alpha] \subseteq \sum_{i=1}^{r} \mathbb{Z}\alpha_i\,,\ \mathbb{Z}[\beta] \subseteq \sum_{j=1}^{s} \mathbb{Z}\beta_j$$

$$\implies \mathbb{Z}[\alpha, \beta] \subset \sum_{i=1}^{r}\sum_{j=1}^{s} \mathbb{Z}\alpha_i\beta_j \quad \text{endlich erzeugt}$$

$$\underset{\text{b)}}{\Longrightarrow} \mathbb{Z}[\alpha, \beta] \subset R_K$$

Also ist R_K ein Unterring von K.

d) Ist $\alpha \in K$, so ist α Nullstelle eines (i. a. nicht normierten) Polynoms $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ mit $a_n \neq 0$. Dann gilt

$$0 = a_n^{n-1} f(\alpha) = (a_n\alpha)^n + \sum_{i=0}^{n-1} a_i a_n^{n-1-i}(a_n^i \alpha^i)\,.$$

Also ist $a_n\alpha$ Wurzel des normierten ganzzahligen Polynoms $g(X) = X^n + \sum_{i=1}^{n-1} a_i a_n^{n-1-i} X^i$ und daher $a_n\alpha \in R_K$ mit $a_n \in \mathbb{Z}$.

Aufgabe 47. (s)
Sei S ein kommutativer Ring mit Eins, $T \subseteq S$ *multiplikativ,* d. h. $0 \notin T$, $1 \in T$ und T multiplikativ abgeschlossen.

a) Das Ideal $\mathfrak{a} \lhd S$ sei maximal mit der Eigenschaft $\mathfrak{a} \cap T = \emptyset$. Zeigen Sie, dass $\mathfrak{a}$ ein Primideal ist.

b) Formulieren und begründen Sie eine Umkehrung für a).

Lösung:
a) Indirekt: Sei $bc \in \mathfrak{a}$, aber $b \notin \mathfrak{a}, c \notin \mathfrak{a}$. Wegen der Maximalität von $\mathfrak{a}$ gilt dann $\mathfrak{a} + bS \cap T \neq \emptyset$, $\mathfrak{a} + cS \cap T \neq \emptyset$, also existieren $a_1 + bs_1, a_2 + cs_2 \in T$mit $a_i \in \mathfrak{a}, s_i \in S$. Dann gilt auch

$$T \ni (a_1 + bs_1)(a_2 + cs_2) = \underbrace{a_1a_2 + bs_1a_2 + cs_2a_1}_{\in \mathfrak{a} \lhd S} + \underbrace{bcs_1s_2}_{\in \mathfrak{a}} \in \mathfrak{a}\,,$$

im Widerspruch zu $\mathfrak{a} \cap T = \emptyset$.
b) Es sind äquivalent:

(i) $\mathfrak{a} \subsetneq S$ echtes Primideal.

(ii) Es gibt eine multiplikative Menge $T \subset S$, so dass $\mathfrak{a} \lhd S$ maximal ist mit $\mathfrak{a} \cap T = \emptyset$.

(ii)$\Rightarrow$ (i) ist in a) gezeigt. (i)$\Rightarrow$ (ii) ist aber einfach, denn wenn $\mathfrak{a}$ ein echtes Primideal ist, so ist $T = S \setminus \mathfrak{a}$ multiplikativ abgeschlossen und natürlich $1 \in T$, $0 \notin T$. Und $\mathfrak{a}$ ist maximal, ja sogar das größte Ideal mit $\mathfrak{a} \cap (S \setminus \mathfrak{a}) = \emptyset$.

Aufgabe 48. (s)
Sei $S|R$ eine kommutative unitäre Ringerweiterung, $\mathfrak{p} \lhd R$ ein Primideal in R.

a) Konstruieren Sie ein Primideal $\mathfrak{P} \lhd S$ mit $\mathfrak{P} \cap R \subset \mathfrak{p}$.

b)* Ist $S|R$ ganz (was heißt das?), so kann $\mathfrak{p} \subset \mathfrak{P}$ (und damit $\mathfrak{p} = \mathfrak{P} \cap R$) gezeigt werden.

Lösung:
a) Sei $\mathfrak{p} \subsetneq R$ ein echtes Primideal, also $T := R \setminus \mathfrak{p}$ multiplikative Teilmenge in S. Nach dem Lemma von Zorn existiert ein Ideal $\mathfrak{P} \lhd S$ maximal mit $\mathfrak{P} \cap T = \emptyset$. Dann ist $\mathfrak{P}$ Primideal in S und $\mathfrak{P} \cap R \subset R \setminus T = \mathfrak{p}$.
b)* Wie im Körperfall mit dem Begriff „algebraisch“ definiert man „$S|R$“ ist ganz, wenn jedes Element $s \in S$ einer *ganzen Gleichung* genügt:

$$s^n + \sum_{i=0}^{n-1} a_i s^i = 0 \quad \text{mit } a_i \in R\,.$$

Sei nun $p \in \mathfrak{p}$ und angenommen $p \notin \mathfrak{P}$. Nach Wahl von $\mathfrak{P}$ enthält dann $\mathfrak{P} + pS$ ein Element $P + ps = t \in T = R \setminus \mathfrak{p}$, also $t - ps = P \in \mathfrak{P} \iff t \equiv ps \bmod \mathfrak{P}$. s erfüllt eine ganze Gleichung

wie oben, also

$$0 = (ps)^n + \sum_{i=0}^{n-1} p^{n-i} a_i (ps)^i \equiv \underbrace{t^n + \sum_{i=0}^{n-1} p^{n-i} a_i t^i}_{\in R} \bmod \mathfrak{P}$$

$$\implies t^n + \sum_{i=0}^{n-1} p^{n-i} a_i t^i \in R \cap \mathfrak{P} \subset \mathfrak{p} \underset{p \in \mathfrak{p}}{\implies} t^n \in \mathfrak{p} \implies t \in \mathfrak{p} \quad \text{Wid.}$$

Aufgabe 49. (m)
Sei $f \in \mathbb{Z}[X]$ normiert vom Grade n, $W_f = \{\alpha_1, \ldots, \alpha_n\}$ die Wurzelmenge und K der Zerfällungskörper von f. Es sei $N = \{1, \ldots, n\}$ und für $I \subseteq N$ $\alpha_I := \sum_{i \in I} \alpha_i$. Zeigen Sie:

a) Für alle $1 \leq r \leq n-1$ gilt $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\alpha_I \mid I \subset N\,,\ \#I = r)$.

[Tip: $r \geq 2 \implies \sum\limits_{\substack{\#I=r \\ i \in I \subset N}} \alpha_I = \binom{n-1}{r-1}\alpha_i + \binom{n-2}{r-2} \sum\limits_{j \neq i} \alpha_j = \binom{n-2}{r-1}\alpha_i + \binom{n-2}{r-2} \sum\limits_{j=1}^{n} \alpha_j$.]

b) Sei $f_r := \Big[\prod\limits_{\#I=r} (X - \alpha_I) \Big]_{\text{sep}}$ = Produkt der *verschiedenen* Linearfaktoren. Dann gilt:

$$f_r \text{ irreduzibel} \iff G(f) \subseteq \mathcal{S}(N) \text{ operiert transitiv auf } \mathcal{P}_r(N) := \{I \subset N \mid \#I = r\}\,.$$

c) Ist für ein $1 \leq r \leq n-1$ $f_r \in \mathbb{Z}[X]$ reduzibel, so gilt $G(f) \not\supseteq \mathcal{A}_n$.

d) Setzen Sie die Polynome f_r in Beziehung zu Satz V.2.1 der Vorlesung.

Lösung:
a) $\supseteq$ ist klar, ebenso der Fall $r = 1$. Sei nun $r \geq 2$ und $i \in N$:

$$c_i := \sum_{\substack{\#I=r \\ i \in I}} \alpha_I = \sum_{\substack{I' \subset N \setminus \{i\} \\ \#I' = r-1}} (\alpha_i + \alpha_{I'}) = \#\{I' \subset N \setminus \{i\} \mid \#I' = r-1\} \cdot \alpha_i + \sum_{\substack{I' \subset N \setminus \{i\} \\ \#I' = r-1}} \alpha_{I'}$$

$$= \binom{n-1}{r-1} \cdot \alpha_i + \sum_{j \neq i} \#\{I' \subset N \setminus \{i\} \mid \#I' = r-1\,, j \in I'\} \cdot \alpha_j$$

$$= \binom{n-1}{r-1} \cdot \alpha_i + \sum_{j \neq i} \#\{I'' \subset N \setminus \{i,j\} \mid \#I'' = r-2\} \cdot \alpha_j = \binom{n-1}{r-1} \cdot \alpha_i + \binom{n-2}{r-2} \sum_{j \neq i} \alpha_j$$

$$= \left[\binom{n-1}{r-1} - \binom{n-2}{r-2} \right] \cdot \alpha_i + \binom{n-2}{r-2} \sum_{j=1}^{n} \alpha_j = \underbrace{\binom{n-2}{r-1}}_{\neq 0\,(r<n)} \cdot \alpha_i + \binom{n-2}{r-2} \cdot \mathcal{S}_{K|\mathbb{Q}}(\alpha_1)\,,$$

also folgt $\alpha_i \in \mathbb{Q}(c_i) \subset \mathbb{Q}(\alpha_I \mid \ldots)$ und damit die Inklusion $\subseteq$ von a).
b) f_r ist separabel und nach a) ist $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ der Zerfällungskörper von f_r. Also gilt

$$\begin{aligned} &f_r \text{ irreduzibel über } \mathbb{Q} \\ &\iff G(f_r) = G(K|\mathbb{Q}) \text{ transitiv auf } W_{f_r} = \{\alpha_I \mid \#I = r\} \\ &\iff G(f) = G(K|\mathbb{Q}) \text{ transitiv auf } W_{f_r} = \{\alpha_I \mid \#I = r\} \end{aligned}$$

Sei $\sigma \in G(f)$ und $\hat{\sigma}$ seine Fortsetzung auf K. Dann gilt

$$\hat{\sigma}\alpha_I = \sum_{i \in I} \hat{\sigma}\alpha_i = \sum_{i \in I} \alpha_{\sigma i} = \alpha_{\sigma I}\,.$$

Also operiert $G(K|\mathbb{Q})$ transitiv auf $\{\alpha_I \mid \#I = r\} \iff G(f) \subset \mathcal{S}_n = \mathcal{S}(N)$ operiert transitiv auf $\{I \subset N \mid \#I = r\} = \mathcal{P}_r(N)$.
c) Z. z. Die alternierende Gruppe $\mathcal{A}_n$ operiert transitiv auf $\mathcal{P}_r(N)$ für alle $1 \leq r \leq n-1$.
Ist $r \leq n-2$, so ist $\mathcal{A}_n$ r-transitiv, also erst recht transitiv auf $\mathcal{P}_r(N)$.
$r = n-1$: $\mathcal{P}_{n-1}(N)$ besteht aus den Komplementen einelementiger Mengen, auf denen $\mathcal{A}_n$ natürlich transitiv operiert.
d) In Satz V.2.1 wurde das Polynom

$$F = F(U_1, \ldots, U_n; X) = \prod_{\sigma \in \mathcal{S}_n} (X - \sum_{i=1}^{n} U_i \alpha_{\sigma i})$$

betrachtet. f_r ist eine ‚Spezialisierung' von F, nämlich

$$f_r = F(\underbrace{1, \ldots 1}_{r\text{-mal}}, \underbrace{0, \ldots, 0}_{n-r\text{-mal}}; X)_{\text{sep}}\,.$$

Algebra II

Übung 11

Aufgabe 50. (s)
Bestimmen Sie die Galoisgruppen der nachfolgenden Polynome über $\mathbb{Q}$ – oder schränken Sie $G(f)$ möglichst weitgehend ein.

a) $f(X) = X^5 - 14X + 7$

b) $f(X) = X^4 + 8X^2 - 8X + 4$

c) $f(X) = X^4 - 8X^2 + 17$

d) $f(X) = X^5 + 20X + 16$

e)* $f(X) = X^7 - 7X + 3$.

Tipp: Zyklenhäufigkeiten transitiver Permutationsgruppen (McKay-Tabelle[2)])

Grad 3:

G	$\#G$	1^3	1.2	3^1
A_3	3	1		2
S_3	6	1	3	2

Grad 4:

G	$\#G$	1^4	$1^2.2$	2^2	1.3	4
C_4	4	1		1		2
V_4	4	1		3		
D_8	8	1	2	3		2
A_4	12	1		3	8	
S_4	24	1	6	3	8	6

Grad 5:

G	$\#G$	1^5	$1^3.2$	1.2^2	2.3	$1^2.3$	1.4	5
C_5	5	1						4
$C_5 \rtimes C_2$	10	1		5				4
$C_5 \rtimes C_4$	20	1		5			10	4
A_5	60	1		15		20		24
S_5	120	1	10	15	20	20	30	24

Grad 7:

G	$\#G$	1^7	$1^5.2$	$1^3.2^2$	1.2^3	$1^4.3$	$1^2.2.3$	$2^2.3$	1.3^2	$1^3.4$	$1.2.4$	3.4	$1^2.5$	2.5	1.6	7
C_7	7	1														6
D_{14}	14	1			7											6
$C_7 \rtimes C_3$	21	1							14							6
$C_7 \rtimes C_6$	42	1			7				14						14	6
$\mathrm{GL}_3(2)$	168	1		21					56		42					48
A_7	2520	1		105		70		210	280		630		504			720
S_7	5040	1	21	105	105	70	420	210	280	210	630	420	504	504	840	720

Die Tabellen enthalten für die Grade $n = 3, 4, 5, 7$ alle transitiven Untergruppen von S_n, ihre Ordnung sowie die absoluten Häufigkeiten der auftretenden Zyklentypen. Dabei steht $1^2.2^3.3^1$ abkürzend für den Zyklentyp $(1, 1, 2, 2, 2, 3)$, die Basis gibt also die Länge, der Exponent die Zahl der auftretenden Zyklenfaktoren an, die Fixpunkte sind mit erfasst.

Lösung:
Ergebnisse:

[2)] John McKay: *Some remarks on computing Galois groups.* SIAM J. Comput. **8** (1979) 344–347.
Zum dort zu lesenden Lemma 3 und Proposition siehe Aufgabe 49.

a) $G(X^5 - 14X + 7) = \mathcal{S}_5$.

b) $G(X^4 + 8X^2 - 8X + 4) = \mathcal{A}_4$.

c) $G(X^4 - 8X^2 + 17) = D_8$.

d) $G(X^5 + 20X + 16) = \mathcal{A}_r$.

e)* $G(X^7 - 7X + 3) = \mathrm{PSL}_3(2)$.

$\mathrm{PSL}_(2) = \mathrm{GL}_3(2)$ ist *die* einfache Gruppe der Ordnung 168.

$\mathrm{GL}_3(2)$ operiert in natürlicher Weise auf $\mathbb{F}_2^3$ und $\mathbb{F}_2^3 \setminus \{(0,0,0)\} = \Omega$ mit $\#\Omega = 7$.

Begründungen:
a) Wie Übung 2, Aufgabe 7.b): f ist eisensteinsch für $p = 7$ und hat genau drei reelle Nullstellen.
b) Wir untersuchen $\bar{f} = f \bmod p$ modulo diverser Primzahlen.
mod2: $\bar{f} = X^4$, also ist $\bar{f}$ inseparabel und $2 \mid D(f)$.
Wir berechnen (sukzessive nach Erfordernis) die Primzerlegung von Polynomwerten $f(x)$ für betraglich wachsende Argumente $x \in \mathbb{Z}$:

x	-3	-2	-1	0	1	2	3
$f(x)$	181	68	21	4	5	36	133
	181	$2^2 \cdot 17$	$3 \cdot 7$	2^2	5	$2^2 \cdot 3^2$	$7 \cdot 19$

Hieraus liest man ab:
mod 5: $\bar{f} = f \bmod 5$ hat genau eine Nullstelle $x = 1$, sie ist einfach ($f'(1) = 12 \not\equiv 0 \bmod 5$). Also gilt $\bar{f} = (X-1)\bar{g}$ mit $\deg \bar{g} = 3$, $\bar{g}$ irreduzibel, weil ohne Nullstelle. Also ist $\bar{f}$ separabel und nach dem speziellen Reduktionssatz V.3.1 enthält $G(f)$ einen 3-Zyklus.
mod7: $\bar{f}$ hat genau 2 Nullstellen ($x = -1, 3$), aber beide sind doppelt: $7 \mid D(f)$.
Über $\mathbb{Q}$: f hat in $\mathbb{Q}$ keine Nullstelle, weil dafür nur die Teiler von 4 in $\mathbb{Z}$, also $\pm 1, \pm 2, \pm 4$ in Frage kämen. Wäre f reduzibel, so wäre $f = g_1 \cdot g_2$ mit quadratischen irreduziblen Faktoren. Dann könnte aber $G(f) = \mathcal{S}_2 \times \mathcal{S}_2$ keinen 3-Zyklus enthalten.
Also ist f irreduzibel, $G(f) \subset \mathcal{S}_4$ transitiv und $G(f)$ enthält einen 3-Zyklus. Daher $G(f) \supset \mathcal{A}_4$ (Tabelle McKay). Also entscheidet die Berechnung der Diskriminante:

$$D(f) = 200704 = 2^{12} \cdot 7^2 \text{ Quadrat } \implies G(f) = \mathcal{A}_4\,.$$

Berechnung von $D(f)$ mit allgemeiner Formel für Polynome vom Grade 4 (Fortführung von Aufgabe 30.b) oder mittels der Resultanten $D(f) = (-1)^{n(n-1)/2} R(f, f')$ (nicht in der Vorlesung behandelt).)
c) Bei diesem Polynom $f = X^4 - 8X^2 + 17$ kann man die Wurzeln berechnen und so mit rein körpertheoretischen Methoden die Galoisgruppe bestimmen (wie in Algebra I).
Alternativ mit der Reduktionsmethode: f ist gerade.
Wertetabelle

x	0	± 1	± 2	± 3
$f(x)$	17	$2 \cdot 5$	1	$2 \cdot 13$

.
mod2: $\bar{f} = X^4 + 1 = (X+1)^4$, $2^2 \not| f(1) = 10$, also ist $f(x-1)$ eisensteinsch für 2 und f daher irreduzibel.
mod5: $\bar{f}$ hat genau zwei Nullstellen $\pm 1 \bmod 5$, beide sind einfach ($f'(\pm 1) \equiv \pm 3 \bmod 5$), also enthält $G(f)$ nach dem Reduktionssatz eine Transposition.
Damit kommen für $G(f)$ nur D_8 oder $\mathcal{S}_4$ in Frage (Tabelle McKay). Wäre $G(f) = \mathcal{S}_4$, so gäbe es in $G(f)$ eine Permutation mit *genau* einem Fixpunkt. Da f gerade ist, ist mit jedem Fixpunkt $\alpha \in W_f$ auch $-\alpha \in W_f$ fix, es müsste also $\alpha = 0$ sein, Wid.
d) $f(X) = X^5 + 20X + 16$.
$D(f) = 80^4 \cdot 5^2 = 2^{16} \cdot 5^4$ ist ein Quadrat, also $G(f) \subset \mathcal{A}_5$. $D(f)$ mittels der Resultanten leicht berechenbar, da f und somit auch die zu berechnende Determinante spärlich besetzt ist.

Eine Wertetabelle ergibt wie oben:
mod11: $\bar{f}$ ist separabel und hat genau zwei Nullstellen $2, 3$, also enthält $G(f)$ einen 3-Zyklus.
mod 3: $\bar{f}$ hat keine Nullstellen. Wäre $\bar{f}$ reduzibel, so wäre $\bar{f} = \bar{f}_2\bar{f}_3$ mit $\deg \bar{f}_i = i$, $\bar{f}_i$ irreduzibel. Dann aber enthält $G(f)$ eine Permutation vom Typ (2,3) im Widerspruch zu $G(f) \subset \mathcal{A}_5$. Also ist $\bar{f}$ und damit f irreduzibel. Dann folgt aber $G(f) = \mathcal{A}_5$, denn $G(f)$ enthält einen 3-Zyklus und ist primitiv, weil transitiv von Primzahlgrad.
e)* Auch hier lässt sich die Diskriminante problemlos über die Resultante berechnen: $D(f) = -R(f, f') = 3^6 \cdot 7^8$. Außerdem sind alle Restklassenpolynome $f \bmod p$ separabel für $p \neq 3, 7$.
Aus einer geeigneten Wertetabelle entnimmt man:
mod7: 4 ist einzige Nullstelle von $\bar{f}$. Wegen $7 \mid D(f)$ könnte $f(X+4)$ 7-eisensteinsch sein, und in der Tat

$$f(X+4) \equiv (X+4)^7 + 3 \equiv X^7 + \underbrace{4^7}_{\equiv 4} + 3 \equiv X^7 \bmod 7 \quad \text{und} \quad f(4) \not\equiv 0 \bmod 7^2 .$$

Also ist f irreduzibel und $G(f)$ transitiv.
Man untersucht nun die Primzerlegung von $f \bmod p$ und vergleicht die auftretenden Grade mit den Zyklentypen in den noch möglichen vier Galoisgruppen (Tabelle McKay). Ein erster Schritt ist die Auswertung einer Wertetabelle und Bestimmung aller Nullstellen von $f \bmod p$. Deren Anzahl vergleicht man mit der Anzahl der Fixpunkte in den Zyklentypen der 4 relevanten Gruppen. Mit Unterstützung durch Taschenrechner (mühselig, aber möglich) oder Computer berechnet man für $|a| \leq 36$ die Werte $f(a)$ und ihre Primzerlegungen. Daraus entnimmt man, dass im Bereich $p \leq 73$, $p \neq 3, 7$, $f \bmod p$ entweder *keine* oder *genau eine* Nullstelle besitzt:

p	2	5	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73
Nullstellen				2	7	4	−4			−2	4	−17	−8	−	24	27	7	20	−27

Das Auftreten von nur einer Nullstelle (konkret: $f \bmod 13$ hat nur die Nullstelle 2 in $\mathbb{F}_{13}$) schließt die zyklische Galoisgruppe Z_7 aus, da sie keinen Zyklentyp mit genau einem Fixpunkt enthält. Wertet man nun auch die Häufigkeit der Primzahlen p mit einer festen Anzahl von Nullstellen für $f \bmod p$ aus und vergleicht mit der Häufigkeit von Zyklentypen mit gleicher Fixpunktzahl (Tabelle McKay), so erhält man folgende Tabelle:

#Fixpunkte	Z_7	F_{21}	$\mathrm{PSL}_3(2)$	$\mathcal{A}_7$	$*$
0	86%	29%	29%	37%	32%
1	—	67%	58%	36%	68%
2 . . . 6	—	—	13%	27%	—
7	14%	5%	1%	< 0,1%	—

Die Ergebnisse in Spalte $*$ geben die Häufigkeit der Primzahlen (bezogen auf den Bereich $p \leq 73$) an, für die $f \bmod p$ die entsprechende Anzahl Nullstellen hat. Diese Ergebnisse lassen $G(f) = F_{21}$ vermuten (siehe Čebotarevscher Dichtigkeitssatz IV.3.5), aber für die nächste Primzahl $p = 79$ findet man genau *drei* Nullstellen für $f \bmod 79$, (nämlich -4, 6 und 28), so dass auch F_{21} ausgeschlossen ist und nur noch zwei Möglichkeiten für $G(f)$ verbleiben: $\mathrm{PSL}_3(2)$ oder $\mathcal{A}_7$. Die Häufigkeitsverteilung in Spalte $*$ legt dann sehr stark die *Vermutung* nahe: $G(f) = \mathrm{PSL}_3(2)$.
Um nun eine der beiden Gruppen ausschließen zu können, könnte man die Untersuchung verfeinern und nicht nur Linearfaktoren, sondern weitere Informationen über die Primzerlegung von $f \bmod p$ ermitteln und mit den möglichen Zyklentypen in $\mathrm{PSL}_3(2)$ und $\mathcal{A}_7$ vergleichen. Im vorliegenden Fall ist dies allerdings nicht hilfreich, da in beiden Gruppen genau dieselben Zyklentypen auftreten (wenn auch mit unterschiedlicher Häufigkeit) und somit auf diesem Wege keine definitive Entscheidung möglich ist.
Den Nachweis, dass $G(f) \neq \mathcal{A}_7$ ist, kann man jedoch mit Aufgabe 49.c) erreichen. Man muss ein $r \in \{1, \ldots 6\}$ finden, für das das dort definierte Polynom f_r *reduzibel* ist. Da die Grade der f_r recht groß werden, ist dies mit erheblichem Rechenaufwand verbunden – wenn auch (über $\mathbb{Z}$) zumindest im Prinzip durchführbar (siehe Satz V.2.2). Auf dem hier skizzierten Weg wird in

Erbach, Fischer, McKay:
Polynomomials with $\mathrm{PSL}_2(7)$ *as Galois groups.*
J. Number Theory **11** (1979) 69–75

$G(f) = \mathrm{PSL}_3(2)$ bewiesen. Das Polynom in e) und ein ähnlicher Beweis stammen von W. Trinks (1969, unveröffentlichte Diplomarbeit, U Karlsruhe bei Prof. Dr. H.-W. Leopoldt).

Die oben genannten Autoren zeigen, dass f_r für $r = 3$ reduzibel ist. Der Wert $r = 3$ ist wie folgt erklärbar: Die Gruppe $\mathrm{GL}_3(2)$ operiert transitiv auf $\Omega = \mathbb{F}_2^3 \setminus \{(0,0,0)\}$, $\#\Omega = 7$. Da die Operation linear ist, wird eine Ebene E $(= \{0, a, b, c = a + b\})$ in $\mathbb{F}_2^3$ wieder in eine Ebene E' abgebildet. Also kann G auf den 3-elementigen Teilmengen von Ω *nicht transitiv* sein, wenn $G(f) = \mathrm{GL}_3(2)$ ist.