**Aufgabe 1** (Herbst 1996)**.** Man zeige für das Polynom $f = X^4 - X + 1 \in \mathbb{Z}[X]$:

(a) $f$ hat keine reelle Nullstelle.

(b) $f$ ist irreduzibel über $\mathbb{Q}$.

(c) Ist $u + iv$ (mit $u, v \in \mathbb{R}$ eine Nullstelle von $f$ in $\mathbb{C}$, so ist $g = X^3 - 4X - 1$ das Minimalpolynom von $4u^2$ über $\mathbb{Q}$.

(d) Die Galoisgruppe von $f$ über $\mathbb{Q}$ besitzt ein Element der Ordnung 3.

(e) Keine Nullstelle $a \in \mathbb{C}$ von $f$ ist, als Punkt der Zahlenebene, aus den Punkten 0 und 1 mit Zirkel und Lineal konstruierter.

*Lösung.* **Zu (a):** Für alle $a \in \mathbb{R}$ ist $f(a) > 0$. Dies sieht man folgendermaßen. Für $a \leqslant 0$ ist sowohl $a^4 \geqslant 0$, als auch $-a \geqslant 0$. Also

$$a^4 - a + 1 \geqslant 1.$$

Für $a \geqslant 1$ ist $a^4 \geqslant a$, also $a^4 - a \geqslant 0$, also

$$a^4 - a + 1 \geqslant 1.$$

Für $0 < a < 1$ ist sowohl $a^4 \geqslant 0$, also auch $1 - a \geqslant 0$. Also

$$a^4 - a + 1 \geqslant 0.$$

Also hat $f$ keine reellen Nullstellen.

**Zu (b):** Wir wenden das Reduktionskriterium modulo 2 an:

$$f \mod 2 = X^4 + X + 1 \in \mathbb{F}_2[X]$$

hat keine Nullstellen in $\mathbb{F}_2$, spaltet also keine Linearfaktoren ab. Angenommen $X^4 + X + 1$ zerfiele über $\mathbb{F}_2$ in quadratische Faktoren

$$X^4 + X + 1 = (X^2 + aX + b)(X^2 + cX + d) = X^4 + (a + c)X^3 + (d + ac + b)X^2 + (ad + bc)X + bd.$$

Wegen der Eindeutigkeit der Koeffizienten eines Polynoms ist also

$$\begin{aligned} 1 &= bd \quad \text{folglich } b = d = 1 \\ 0 &= d + ac + b = ac \quad \text{folglich} a = c = 0 \\ 1 &= ad + bc = 0 \quad \text{ein Widerspruch.} \end{aligned}$$

Also ist $X^4 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel. Nach dem Reduktionskriterium ist $f = X^4 - X + 1 \in \mathbb{Z}[X]$ irreduzibel, also ist es auch irreduzibel über $\mathbb{Q}$ (nach dem Satz von Gauß).

**Zu (c):** Die kubische Resolvente eines Polynoms $X^4 + pX^2 + qX + r$ ist gegeben durch $g = X^3 - pX^2 - 4rX + 4pr - q^2$. In unserem Fall ist $p = 0$, $q = -1$ und $r = 1$. Demnacht ist die kubische Resolvente des Polynoms $f = X^4 - X + 1$ gegeben durch

$$g = X^3 - 4X - 1.$$

Dies ist das Polynom aus der Angabe. Wir bestimmen nun eine Nullstelle davon. Seien $a_1, a_2, a_3, a_4$ die Nullstellen von $f$. Nach (a) sind diese echt komplex. Sie müssen paarweise konjugiert sein. Ohne Einschränkung nehmne wir an, daß $a_2 = \overline{a}_1$ und $a_4 = \overline{a}_3$. Mit ihnen kann man die Nullstellen von $g$ ausdrücken als

$$\begin{aligned} \alpha &= a_1 a_2 + a_3 a_4 \\ \beta &= a_1 a_3 + a_2 a_4 \\ \gamma &= a_1 a_4 + a_2 a_3 \end{aligned}$$

Es gilt

$$\begin{aligned} f = X^4 - X + 1 &= (X - a_1)(X - a_2)(X - a_3)(X - a_4) \\ &= X^4 - (a_1 + a_2 + a_3 + a_4)X^3 + (a_1a_2 + a_1a_3 + a_1a_4 + a_2a_3 + a_2a_4 + a_3a_4)X^2 + \\ &\quad - (a_1a_2a_3 + a_1a_2a_4 + a_1a_3a_4 + a_2a_3a_4)X + a_1a_2a_3a_4 \end{aligned}$$

Also muß

$$\begin{aligned} 1 &= a_1a_2a_3a_4 \\ 1 &= a_1a_2a_3 + a_1a_2a_4 + a_1a_3a_4 + a_2a_3a_4 \\ 0 &= a_1a_2 + a_1a_3 + a_1a_4 + a_2a_3 + a_2a_4 + a_3a_4 = \alpha + \beta + \gamma \\ 0 &= a_1 + a_2 + a_3 + a_4 \end{aligned}$$

Aus der letzten Gleichung folgt

$$0 = a_1 + \overline{a}_1 + a_3 + \overline{a}_3 = 2u_1 + 2u_3,$$

wobei $u_1$, $u_3$ jeweils die Realteile sind. Also $u_3 = -u_1$. Es ist nun

$$\begin{aligned} 4u_1^2 = 4u_3^2 &= (a_1 + \overline{a}_1)^2 \\ &= -(a_1 + \overline{a}_1)(a_3 + \overline{a}_3) \\ &= -(a_1 + a_2)(a_3 + a_4) \\ &= -(a_1a_3 + a_1a_4 + a_2a_3 + a_2a_4) \\ &= a_1a_2 + a_3a_4 = \alpha \end{aligned}$$

Es bleibt zu zeigen, daß $g$ irreduzibel ist. Wir wenden wieder das Reduktionskriterium modulo zwei and, und sehen, daß

$$g \mod 2 = X^3 + X + 1 \in \mathbb{F}_2[X]$$

keine NUllstelle hat, also irreduzibel über $\mathbb{F}_2$ und damit auch irreduzibel über $\mathbb{Z}$ und $\mathbb{Q}$ ist. Dies zeigt die Behauptung.

**Zu (d):** Sei $E = \mathbb{Q}(\alpha, \beta, \gamma)$ der Zerfällungskörper der kubischen Resolvente $g$. Dies ist eine Galoiserweiterung und es gilt $\mathrm{Gal}(g/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(f/\mathbb{Q})/N$, wobei $N \triangleleft \mathrm{Gal}(f/\mathbb{Q})$ das Urbild der Klein'schen VIerergruppe unter der Injektion $\varphi : \mathrm{Gal}(f/\mathbb{Q}) \hookrightarrow \mathfrak{S}_4$ ist. Es gilt $[E : \mathbb{Q}] = [\mathrm{Gal}(f/\mathbb{Q}) : N] = |\mathrm{Gal}(g/\mathbb{Q})|$. Da $g$ irreduzibel, normiert und separabel vom Grad 3 über $\mathbb{Q}$ ist, gilt

$$3 \big| \mathrm{Gal}(g/\mathbb{Q}) \big| 3! = 6.$$

Also ist $[\mathrm{Gal}(f/\mathbb{Q}) : N] \in \{3, \}6$. Es folgt, daß $3 \big| |\mathrm{Gal}(f/\mathbb{Q})|$. (Genauer $\mathrm{Gal}(f/\mathbb{Q}) \cong \mathfrak{S}_4$ oder $\mathrm{Gal}(f/\mathbb{Q}) \cong A_4$.) Da 3 prim ist, enthält $\mathrm{Gal}(f/\mathbb{Q})$ ein Element der Ordnung 3.

**Zu (e):** Sei $a \in \mathbb{C}$ eine Nullstelle des irreduziblen Polynoms $f \in \mathbb{Q}[X]$, also ist insbesondere $f$ das Minimalpolynom von $a$ über $\mathbb{Q}$. Wäre $a$ aus $\{0, 1\}$ mit Zirkel und Lineal konstruierbar, so wäre die Galoisgruppe $\mathrm{Gal}(f/\mathbb{Q})$ eine Zweigruppe, also $|\mathrm{Gal}(f/\mathbb{Q})| = 2^t$. Wir haben jedoch bereits in (d) gezeigt, daß $3 \big| |\mathrm{Gal}(f/\mathbb{Q})|$. Somit ist $a$ nicht konstruierbar.

**Aufgabe 2** (Frühjahr 1995)**.** Sei $F/K$ eine nichttriviale endliche Galoiserweiterung mit auflösbarer Galoisgruppe. Zeigen Sie, daß es einen Zwischenkörper $K \subset E \subset F$ gibt, so daß $E/K$ Galois'sch mit abelscher Galoisgruppe ist.

*Lösung.* Sei $G = \mathrm{Gal}(F/K)$. Nach Vorraussetzung ist $G$ auflösbar, sie besitzt also eine Normalreihe mit abelschen Faktoren, das heißt eine Folge von Untergruppen

$$G = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\},$$

$m \geqslant 0$, so daß $H_{i+1} \triangleleft H_i$ und $H_i/H_{i+1}$ abelsch ist für $0 \leqslant i < m$.

Insbesondere ist $H_1$ ein Normalteiler in $G$. Definiere nun $E := \mathrm{Fix}_F(H_1)$. Dies ist der nach dem Hauptsatz der Galoistheorie zu $H_1$ korrespondierende Zwischenkörper, $F/E$ ist Galois'sch und $\mathrm{Gal}(F/E) = H_1 \subset G$. Da aber $H_1$ Normalteiler von $G$ ist, ist nach dem zweiten Teil des Hauptsatzes der Galoistheorie auch $E/K$ Galois'sch mit Galoisgruppe $\mathrm{Gal}(E/K) \cong G/H_1$. Nach Voraussetzung ist $G = H_0$ und $H_0/H_1$ abelsch. Damit ist $\mathrm{Gal}(E/K)$ abelsch, und $E/K$ abelsche Galoiserweiterung, wie gewünscht

**Aufgabe 3** (Herbst 1999)**.** Die Antworten auf folgende Fragen sind mit einer kurzen Begründung zu versehen:

(a) Gibt es ein irreduzibles Polynom aus $\mathbb{Q}[X]$, das in $\mathbb{C}$ eine doppelte Nullstelle hat?

(b) Gibt es ein irreduzibles Polynom aus $K[X]$, das in einem Erweiterungskörper von $K$ eine doppelte Nullstelle besitzt, wenn $K$ ein endlicher Körper ist?

(c) Geben Sie einen Körper $K$ an und ein irreduzibles Polynom aus $K[X]$, das im algebraischen Abschluß von $K$ eine doppelte Nullstelle besitzt.

(d) Geben Sie einen Körper $K$ und ein Polynom fünften Grades aus $K[X]$ an, das nicht durch Radikale auflösbar ist.

*Lösung.* **Zu (a):** Nein: da der Körper $\mathbb{Q}$ Charakteristik 0 hat ist er vollkommen, also ist jedes irreduzible Polynom in $\mathbb{Q}[X]$ separabel, das heißt es hat in jedem Zerfällungskörper, und damit auch in $\mathbb{C}$ nur einfache Nullstellen.

**Zu (b):** Nein: endliche Körper sind vollkommen, also ist jedes Polynom über einem solchen separabel.

**Zu (c):** Sei $K = \mathbb{Z}/(2)(X)$, $f = Y^2 + X \in K[Y]$. Dann ist $f$ irreduzibel, denn $f$ ist irreduzibel in $\mathbb{Z}/(2)[X][Y]$ nach Eisenstein. Es gibt eine Erweiterung $K \subset L = K(y)$ vom Grad 2 mit $0 = f(y) = y^2 + X$, also $y^2 = X$ über $\mathbb{Z}/(2)$ und es gilt

$$(Y + y)^2 = Y^2 + 2Yy + y^2 = Y^2 + y^2 = Y^2 + X = f.$$

**Zu (d):** Sei $K$ ein Körper und $f \in K[X]$ ein separables Polynom. Wenn die Galoisgruppe $G(f)$ eine zu einer der Gruppen $A_n$, $n \geqslant 5$, isomorphen Untergruppe enthält, dann ist die Gleichung $f = 0$ nicht durch Radikale auflösbar. Der Grund: die $A_n$, $n \geqslant 5$, sind nicht auflösbar.
Ist insbesondere $F = X^n + U_1X^{n-1} + \ldots + U_{n-1}X + U_n \in K(U_1, \ldots, U_n)[X]$ das allgemeine Polynom $n^{\text{ten}}$ Grades, dann ist die Gleichung $F = 0$ für $n \geqslant 5$ nicht durch Radikale auflösbar, denn in diesem Fall ist $G(F) \cong \mathfrak{S}_n$.
Als Antwort auf die Frage können wir also als Grundkörper $K(U_1, \ldots, U_5)$ wählen, der transzendent über $K$ ist, wobei $K$ ein beliebiger Körper ist, und als Polynom $F = X^5 + U_1X^4 + \ldots + U_4X + U_5 \in K(U_1, \ldots, U_5)[X]$.

**Aufgabe 4** (Herbst 2016)**.** Finden Sie zwei Polynome $f, g \in \mathbb{Q}[X]$ gleichen Grades, so daß $\mathrm{Gal}(f)$ und $\mathrm{Gal}(g)$ gleich viele Elemente habe, aber $\mathrm{Gal}(f)$ abelsch und $\mathrm{Gal}(g)$ nicht abelsch ist.

*Lösung.* Die Ordnung der gesuchten Gruppen kann keine Primzahl sein. Die kleinste mögliche nichtabelsche Gruppe ist $\mathfrak{S}_3$ und hat Ordnung 6. Wir kennen bereits eine Galoiserweiterung mit dieser Galoisgruppe: Der Zerfällungskörper des Polynoms $X^3 - 2 \in \mathbb{Z}[X]$ ist $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ und hat Ordnung 6 über $\mathbb{Q}$. (Im Examen müsste man das zeigen, hier verweise ich auf die Vorlesungsnotizen.)

$$\mathrm{Gal}(X^3 - 2/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong \mathfrak{S}_3.$$

Jede abelsche Gruppe der Odrnung 6 ist isomorph zu $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Diese ist zyklisch und insbesondere isomorph zu $(\mathbb{Z}/7\mathbb{Z})^\times$. Wir wissen, daß dies die Galoisgruppe der Erweiterung $\mathbb{Q}^{(7)}/\mathbb{Q}$ ist, also des siebten Kreistielungskörpers $\mathbb{Q}(\zeta_7)$ über $\mathbb{Q}$. Das Minimalpolynom der primitiven siebten Einheitswurzel $\zeta_7$ ist das Kreisteilungspolynom $\phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$.

$$\mathrm{Gal}(\phi_7/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}.$$

Da nicht nach irreduziblen Polynomen gefragt war, können wir das Polynom $X^3-2$ mit linearen „trivialen“ Polynomen in $\mathbb{Z}[X]$ multiplizieren, um Polynome gleichen Grades zu erhalten. Etwa:

$$f = \phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$
$$g = (X^3 - 2)(X - 2)(X - 3)(X - 5)$$

Dann gilt

$$\mathrm{Gal}(f/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}/6\,\mathbb{Z}$$
$$\mathrm{Gal}(g/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong \mathfrak{S}_3$$

und $|\mathrm{Gal}(f/\mathbb{Q})| = |\mathrm{Gal}(g/\mathbb{Q})| = 6$.