1. Zeige, dass $\mathbb{Q}(\sqrt{2}, i)$ Zerfällungskörper von $X^4 + 1 \in \mathbb{Q}[X]$ ist.

   *Lösung:* Die vier Nullstellen von $X^4 + 1$ über $\overline{\mathbb{Q}}$ sind

$$x_1 = \frac{1}{\sqrt{2}}(+1 + i), \qquad x_2 = \frac{1}{\sqrt{2}}(+1 - i),$$
$$x_3 = \frac{1}{\sqrt{2}}(-1 + i), \qquad x_4 = \frac{1}{\sqrt{2}}(-1 - i).$$

   Damit ist ein Zerfällungskörper des Polynoms durch den Unterkörper von $\mathbb{Q}(x_1, \ldots, x_4)$ von $\overline{\mathbb{Q}}$ gegeben. Diese Darstellung kann man vereinfachen:

$$\begin{aligned}\mathbb{Q}(x_1, \ldots, x_4) &= \mathbb{Q}(x_1, x_2) = \mathbb{Q}(x_1, x_2, x_1 + x_2) \\ &= \mathbb{Q}(x_1, x_2, \sqrt{2}) = \mathbb{Q}(1 + i, 1 - i, \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})\end{aligned}$$

2. Betrachte das Polynom $f = X^3 + X + 2$. Ist es über $\mathbb{Q}$, $\mathbb{Q}(i)$ oder $\mathbb{F}_2$ separabel? (Rep. d. Alg., 5.9.1)

   *Erste Lösungsmöglichkeit:* Das Polynom $f$ besitzt über jedem der Körper $-1$ als Nullstelle. Durch Polynomdivision findet man die Zerlegung

$$f = (X + 1)(X^2 - X + 2).$$

   Im Körper $\mathbb{F}_2$ gilt $2 = 0$, daher schreibt sich über $\mathbb{F}_2$ das Polynom somit als $f = (X+1)(X^2 - X) = X(X-1)^2$ und ist daher nicht separabel. Über den anderen beiden Körpern zeigt die Berechnung der Diskriminante des zweiten Faktors, $(-1)^2 - 4 \cdot 1 \cdot 2 = -7 \neq 0$ („$b^2 - 4ac$“), dass der zweite Faktor keine doppelte Nullstellen in $\overline{\mathbb{Q}}$ besitzt. Ferner hat er keine Nullstelle mit dem ersten Faktor, $X+1$, gemeinsam. Damit ist gezeigt, dass $f$ über $\mathbb{Q}$ und $\mathbb{Q}(i)$ separabel ist.

   *Zweite Lösungsmöglichkeit:* Die formale Ableitung von $f$ ist $f' = 3X^2 + 1$. Über $\mathbb{Q}$ und $\mathbb{Q}(i)$ zeigt der euklidische Algorithmus in einer Nebenrechnung (hier nicht aufgeführt), dass der größte gemeinsame Teiler von $f$ und $f'$ das konstante Polynom 1 ist. Damit ist also $f$ über $\mathbb{Q}$ und $\mathbb{Q}(i)$ separabel.

   Über dem Körper $\mathbb{F}_2$ verläuft die Rechnung des euklidischen Algorithmus anders, man erhält als größten gemeinsamen Teiler von $f$ und $f'$ das Polynom $X^2 + 1$. Also ist $f$ über $\mathbb{F}_2$ nicht separabel.

3. Sei $K$ ein algebraisch abgeschlossener Körper. Zeige, dass $K$ vollkommen ist. (Rep. d. Alg., 5.9.5)

   *Lösung:* Nach einem Satz der Vorlesung müssen wir für jede Primzahl $p$ zeigen, dass $p \cdot 1 \neq 0$ in $K$ oder dass jedes Element in $K$ eine $p$-te Wurzel besitzt.

   Sei also eine beliebige Primzahl $p$ gegeben. Da $K$ ein Körper ist, können wir folgende Fallunterscheidung treffen:

a) $p \cdot 1 = 0$. Sei dann ein beliebiges Element $x \in K$ gegeben, wir müssen zeigen, dass es eine $p$-te Wurzel besitzt. Dazu betrachten wir das Polynom $X^p - x$. Dieses muss, da $K$ algebraisch abgeschlossen ist, in Linearfaktoren zerfallen und somit insbesondere eine Nullstelle $y$ besitzen. Diese erfüllt dann $y^p - x = 0$, also ist mit $y$ eine $p$-te Wurzel von $x$ gefunden.

b) $p \cdot 1$ ist invertierbar und somit insbesondere nicht gleich null. Dann ist nichts weiter zu zeigen.

4. Konstruiere einen Körper mit 16 Elementen.

   *Tipp:* Einziges irreduzibles Polynom vom Grad 2 über $\mathbb{F}_2$ ist $X^2 + X + 1$.

   *Lösung:* Nach unseren Überlegungen im Ferienkurs benötigen wir also ein irreduzibles Polynom vom Grad 4 über $\mathbb{F}_2$. Ein solches ist $f = X^4 + X + 1$. Denn es besitzt keine Nullstellen, womit kein Linearfaktor und kein kubischer Faktor abspalten kann; es ist auch nicht ein Vielfaches des einzigen irreduziblen Polynoms vom Grad 2, $X^2+X+1$ (eine Nebenrechnung zeigt, dass $f$ bei Division durch $X^2+X+1$ den Rest 1 lässt). Damit kann auch kein quadratischer Faktor abspalten.

   Somit ist $\mathbb{F}_2[X]/(X^4 + X + 1)$ ein Körper mit 16 Elementen.

5. Konstruiere einen Zerfällungskörper des Polynoms $f = X^5 + X + 1$ über $\mathbb{F}_2$. Was ist sein Grad über $\mathbb{F}_2$?

   *Tipp:* $f = (X^3+X^2+1)(X^2+X+1)$, und diese beiden Faktoren sind über $\mathbb{F}_2$ irreduzibel (wieso?).

   *Lösung:* Beide angegebenen Faktoren sind irreduzibel, da sie vom Grad 2 oder 3 sind und keine Nullstellen über $\mathbb{F}_2$ besitzen. Unser Verfahren zur Konstruktion eines Zerfällungskörpers sieht nun vor, dass wir beispielsweise

$$K_1 := \mathbb{F}_2[T]/(T^3 + T^2 + 1)$$

   setzen. Über $K_1$ besitzt der erste Faktor eine Nullstelle, nämlich $T$; er zerfällt aber sogar in Linearfaktoren, denn $T^2$ ist eine weitere Nullstelle:

$$(T^2)^3 + (T^2)^2 + 1 = (T^3)^2 + T^4 + 1 = (T^2 + 1)^2 + T^4 + 1 = 0.$$

   Damit muss der erste Faktor auch eine dritte Nullstelle besitzen (das haben wir im Ferienkurs gesehen – man kann aber auch direkt nachrechnen, dass $T^3$ die letzte Nullstelle ist).

   Bleibt der zweite Faktor. Indem man alle acht Elemente von $K_1$ einsetzt, sieht man, dass der zweite Faktor auch über $K_1$ noch irreduzibel ist. Somit setzen wir

$$K_2 := K_1[S]/(S^2 + S + 1).$$

   Über diesem besitzt der zweite Faktor die Nullstelle $S$ und muss somit, da er vom Grad 2 ist, auch schon in Linearfaktoren zerfallen. Es ist also $K_2$ der gesuchte Zerfällungskörper.

   Zum Grad: $[K_2 : \mathbb{F}_2] = [K_2 : K_1] \cdot [K_1 : \mathbb{F}_2] = 2 \cdot 3 = 6$.

6. Sei $x \in \overline{\mathbb{Q}}$ mit $x^3 + 5x^2 - x + 1 = 0$. Finde eine normierte Polynomgleichung über $\overline{\mathbb{Q}}$, die $1/x = x^{-1}$ als Nullstelle besitzt.

   *Lösung:* Trivialerweise gilt

   $$(x^{-1})^{-3} + 5(x^{-1})^{-2} - (x^{-1})^{-1} + 1 = 0.$$

   Aus dieser Gleichung für $x^{-1}$ können wir durch Durchmultiplizieren mit $(x^{-1})^3$ eine Polynomgleichung für $x^{-1}$ bauen:

   $$1 + 5x^{-1} - (x^{-1})^2 + (x^{-1})^3 = 0.$$

   Diese ist sogar schon normiert.

7. Sei $f \in \mathbb{Q}[X]$ ein separables Polynom über $\mathbb{Q}$, welches über $\overline{\mathbb{Q}}$ mindestens eine nicht-reelle Nullstelle besitzt. Gib ein Element der Ordnung 2 in der Galoisgruppe von $f$ (also der Galoisgruppe der Körpererweiterung $L := \mathbb{Q}(x_1, \ldots, x_n)$ über $\mathbb{Q}$, wobei die $x_i$ die Nullstellen von $f$ in $\overline{\mathbb{Q}}$ sind) an.

   *Tipp:* Komplexe Konjugation...

   *Lösung:* Wir betrachten die Abbildung der komplexen Konjugation:

   $$\sigma\colon \begin{array}{ccc} \overline{\mathbb{Q}} & \longrightarrow & \overline{\mathbb{Q}} \\ x & \longmapsto & \overline{x} \end{array}$$

   Wir behaupten als Erstes, dass die Einschränkung $\tilde{\sigma}$ dieser Abbildung auf $L$,

   $$\tilde{\sigma}\colon \begin{array}{ccc} L & \longrightarrow & L \\ x & \longmapsto & \overline{x}, \end{array}$$

   ein Element der Galoisgruppe ist. Dazu müssen wir uns zunächst klarmachen, dass $\tilde{\sigma}$ wohldefiniert ist, dass also $\tilde{\sigma}(x)$ für alle $x \in L$ wieder in $L$ liegt. Ein beliebiges $x \in L$ ist nach Definition ein rationaler Ausdruck in den Nullstellen $x_1, \ldots, x_n$ von $f$. Somit ist $\overline{x}$ ein rationaler Ausdruck in $\overline{x_1}, \ldots, \overline{x_n}$. Da die Koeffizienten von $f$ als reell vorausgesetzt sind, sind diese auch Nullstellen von $f$ und somit Elemente von $L$.

   Als nächstes ist zu zeigen, dass $\tilde{\sigma}$ ein Ringhomomorphismus ist. Das ist klar. Und schließlich müssen wir nachweisen, dass $\tilde{\sigma}$ ein $\mathbb{Q}$-Algebrenhomomorphismus ist. Das ist ebenfalls klar, denn die komplexe Konjugation lässt reelle Zahlen unverändert.

   Damit ist bewiesen, dass $\tilde{\sigma}$ ein Element der Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$ ist. Es steht noch der Nachweis aus, dass dieses Element Ordnung 2 hat.

   Bisher haben wir aber auch noch nicht benutzt, dass mindestens eine der Nullstellen von $f$, sagen wir $x_i$, nicht reell ist. Daher gilt $\tilde{\sigma} \neq \mathrm{id}_L$, denn $\tilde{\sigma}(x_i) = \overline{x_i} \neq x_i$. Andererseits gilt $\tilde{\sigma}^2 = \mathrm{id}_L$; also hat $\tilde{\sigma}$ in der Tat Ordnung 2.

8. Zeige: $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}\}$.

   *Lösung:* Da $X^3 - 2$ das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist, ist $\mathbb{Q}(\sqrt[3]{2})$ als $\mathbb{Q}$-Algebra isomorph zu $\mathbb{Q}[T]/(T^3 - 2)$. Daher können wir die Aufgabe auch für $\mathbb{Q}[T]/(T^3 - 2)$ statt $\mathbb{Q}(\sqrt[3]{2})$ lösen.

   Nach Aufgabe 10 stehen die $\mathbb{Q}$-Algebrenhomomorphismen von $\mathbb{Q}[T]/(T^3 - 2)$ nach $L := \mathbb{Q}[T]/(T^3-2)$ in Bijektion mit den Nullstellen des Polynoms $X^3-2$ in $L$.

   Im Ferienkurs hatten wir gesehen, dass dieses Polynom in $L$ nur eine Nullstelle besitzt, nämlich $[T]$. Somit gibt es genau einen $\mathbb{Q}$-Algebrenhomomorphismus von $L$ nach $L$, insbesondere gibt es daher auch nur genau einen $\mathbb{Q}$-Algebrenisomorphismus von $L$ nach $L$, nämlich die Identitätsabbildung, die es ja immer gibt.

9. Sei $L \supseteq K$ eine Körpererweiterung. Sei $f \in K[X]$ ein normiertes Polynom. Finde eine Bijektion zwischen den Mengen

   $$M := \{\varphi\colon K[X]/(f) \longrightarrow L \mid \varphi \text{ ist ein } K\text{-Algebrenhomomorphismus}\}$$

   und

   $$N := \{x \in L \mid x \text{ ist eine Nullstelle von } f\}.$$

   *Zur Erinnerung:* Eine Abbildung $\varphi$ wie oben heißt genau dann *$K$-Algebrenhomomorphismus*, wenn sie ein Ringhomomorphismus ist und $\varphi(k) = k$ für alle $k \in K$ gilt.

   *Lösung:* Wir definieren die Abbildung

   $$\begin{array}{rccl} A\colon & M & \longrightarrow & N \\ & \varphi & \longmapsto & \varphi([X]). \end{array}$$

   Dann gilt:

   a) $A$ ist wohldefiniert, d. h. $A(\varphi) = \varphi([X])$ liegt für $\varphi \in M$ tatsächlich in $N$:

      $$f(\varphi([X])) = \varphi(f([X])) = \varphi([f(X)]) = \varphi(0) = 0.$$

      Dabei gilt die erste Gleichheit deswegen, weil die Koeffizienten von $f$ aus $K$ stammen und $\varphi$ die Elemente aus $K$ fix lässt.

   b) $A$ ist surjektiv:
      Sei $x \in N$ eine Nullstelle von $f$ in $L$. Wir definieren folgende Abbildung $\varphi$:

      $$\begin{array}{rrcl} \varphi\colon & K[X]/(f) & \longrightarrow & L \\ & [p] & \longmapsto & p(x) \end{array}$$

      Dann ist $\varphi$ wohldefiniert (aus $[p] = [\tilde{p}]$ folgt $p - \tilde{p} \in (f)$, also $p(x) - \tilde{p}(x) = 0$, da $f(x) = 0$), offensichtlich ein Ringhomomorphismus und außerdem ein $K$-Algebrenhomomorphismus (denn $\varphi(k) = \varphi([k]) = k$ für alle $k \in K$, die wir in $K[X]/(f)$ mit ihren zugehörigen konstanten Polynomen identifizieren). Somit liegt $\varphi$ in $M$.
      Ferner gilt in der Tat $A(\varphi) = \varphi([X]) = X(x) = x$.

c) $A$ ist injektiv:
Sei $\varphi([X]) = \tilde{\varphi}([X])$, wir müssen zeigen, dass $\varphi = \tilde{\varphi}$. Sei dazu $p \in K[X]$ beliebig. Dann gilt:

$$\varphi([p]) = p(\varphi([X])) = p(\tilde{\varphi}([X])) = \tilde{\varphi}([p]).$$

Damit ist alles gezeigt.