Hinweise zu den Übungsaufgaben in Algebra I

Übungsblatt 1

Aufgabe 4. Hier gibt es viele verschiedene Lösungswege. Eine Möglichkeit besteht darin, den Winkel α bei den unteren Ecken der Skizze als Innenwinkel von drei verschiedenen Teildreiecken zu erkennen und den Tangens von α dann jeweils über Gegen- und Ankathete auszudrücken. Zusammen mit dem Satz von Pythagoras erhält man dann drei Gleichungen für drei Unbekannte.

Übungsblatt 2

Aufgabe 5. Die Teilaufgaben a), c) und d) können unabhängig von b) bearbeitet werden.

Übungsblatt 3

Aufgabe 1. Für Teilaufgabe a) ist es nützlich zu wissen, dass der Realteil einer algebraischen Zahl wieder algebraisch ist (wieso stimmt das?). Für die Teilaufgaben b) und c) ist es nicht nötig, eine explizite Darstellung der Lösung α zu berechnen.

Aufgabe 2. Für Teilaufgabe a) ist es ebenfalls nicht nötig, explizite Darstellungen der Lösungen x bzw. y zu berechnen. Auch ohne deren Kenntnis kann man nämlich das Verfahren aus Proposition 1.3 bzw. Hilfssatz 1.4 des Skripts einsetzen. Zur Kontrolle hier eine der insgesamt sechs Teilrechnungen, bevor man zur Bestimmung der Determinante schreiten kann:

$$xy \cdot c_{20} = -c_{01} + c_{11}.$$

Aufgabe 5. Je nachdem, wie man Teilaufgabe b) angeht, ist folgende für ganze Zahlen a und n gültige Äquivalenz hilfreich:

$$[\exists m \in \mathbb{Z}\colon a\,m \equiv 1 \mod n] \quad \Longleftrightarrow \quad a \text{ und } n \text{ sind zueinander teilerfremd.}$$

Ausgeschrieben besagt die linke Aussage, dass es eine weitere ganze Zahl m gibt, sodass die Zahl $a\,m$ bei Division durch n den Rest 1 lässt.

Übungsblatt 4

Aufgabe 1. Bezeichne f die zugehörige Polynomfunktion. Zeige, dass für komplexe Zahlen $z \in \mathbb{C}$, die weiter als die angegebene Länge vom Ursprung entfernt sind, der Betrag $|f(z)|$ echt größer als Null ist. Unter anderem benötigt man dazu die für alle komplexen Zahlen $z_1, \ldots, z_n$ gültige Dreiecksungleichung

$$|z_1 + \cdots + z_n| \leq |z_1| + \cdots + |z_n|$$

und die für alle komplexen Zahlen x, y sog. umgekehrte Dreiecksungleichung

$$|x + y| \geq \Big||x| - |y|\Big| \geq |x| - |y|.$$

Aufgabe 2. Vorgehen kann man wie immer bei ϵ/δ-Aufgaben: Man gibt sich zunächst $R > 0$ und $\epsilon > 0$ beliebig vor. Dann lässt man schon an dieser Stelle Platz für die Definition von δ, da δ nicht von z und w abhängen darf – banalerweise ist die einfachste Möglichkeit, das sicherzustellen, δ vor z und w einzuführen. Danach gibt man sich beliebige $z, w \in \mathbb{C}$ mit $|z|, |w| \leq R$ und $|z - w| < \delta$ vor. In diesem Kontext versucht man schließlich (hierin steckt die Hauptarbeit), den Abstand $|f(z) - f(w)|$ nach oben durch ein Vielfaches von $|z - w|$ abzuschätzen; ist das gelungen, kann man nachträglich die Definition von δ ausfüllen. Für die Hauptarbeit ist neben der Dreiecksungleichung vielleicht die Identität

$$z^m - w^m = (z - w) \cdot (z^{m-1} + z^{m-2}w + z^{m-3}w^2 + \cdots + zw^{m-2} + w^{m-1})$$

hilfreich (wieso gilt sie?).

Aufgabe 5. Die Behauptung von Teilaufgabe b) ist nicht mit ihrer Umkehrung zu verwechseln (diese wird im Skript auf Seite 47 bewiesen).

Übungsblatt 5

Aufgabe 1. Zum Vergleich: Die dritte elementarsymmetrische Funktion in den Variablen X, Y, Z, W ist

$$e_3(X, Y, Z, W) = XYZ + XYW + XZW + YZW.$$

Die in Teilaufgabe d) auftretende Zahl $\binom{n}{k}$ ist die Anzahl der Möglichkeiten, aus der Menge $\{1, \ldots, n\}$ eine k-elementige Teilmenge auszuwählen.

Aufgabe 3. Teilaufgabe b) kann man durch eine längere, aber einfache, Rechnung lösen, wenn man direkt die Definition der Diskriminante benutzt und die durch den Vietaschen Satz gegebenen Relationen beachtet. Dazu ein Tipp: Als erstes die dritte Lösung über die anderen beiden Lösungen ausdrücken, dann Δ und $-4p^3 - 27q^2$ beide vollständig ausmultiplizieren und die Ergebnisse vergleichen. Man kann aber auch die Rechenarbeit gegen Denkarbeit tauschen, wenn man den Tipp von Seite 61 des Skripts befolgt und ausarbeitet.

Aufgabe 5. In der gesamten Aufgabe bezeichnet „$f^{(k)}$“ die k-te Ableitung eines Polynoms f. Teilaufgabe a) kann man etwa mit einem Induktionsbeweis und der für alle $k, i \geq 0$ gültigen Identität

$$\binom{k+1}{i} = \binom{k}{i-1} + \binom{k}{i}$$

in Angriff nehmen. Die Summenschreibweise in der Angabe bedeutet, dass über alle natürlichen Zahlen $i, j \geq 0$, die die Beziehung $i + j = k$ erfüllen, summiert wird. Eine sinnvolle Konvention ist $\binom{k}{-1} := 0$. Vor der unendlichen Summe in Teilaufgabe c) muss man keine Angst haben: Denn ab einem gewissen Summationsindex sind die auftretenden Ableitungen sowieso null, sodass die unendliche Summe tatsächlich eine endliche ist. Man hat schon viel gewonnen, wenn man die Behauptung für die Spezialfälle $f := X^n$, $n \geq 0$, bewiesen hat; dafür ist vielleicht der binomische Lehrsatz

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i \, b^{n-i}$$

und die Formel $\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$ hilfreich.

Übungsblatt 6

Aufgabe 2. Bei Teilaufgabe a) spart man sich viel Rechenaufwand, wenn man durch die Substitution $Y := X + \frac{a}{3}$ die gegebene Gleichung auf die reduzierte Form

$$Y^3 + pY + q = 0 \quad \text{mit} \quad p = b - \frac{a^2}{3}, q = \frac{2a^3 - 9ab + 27c}{27}$$

bringt. Die Diskriminante dieser Gleichung ist nämlich dieselbe wie die von der ursprünglichen Gleichung (wieso?) und dank Aufgabe 3b) von Übungsblatt 5 einfacher zu berechnen. Vielleicht findet ihr aber auch andere kreative Lösungswege. Nur zur Kontrolle: Das Ergebnis wird

$$\Delta = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$$

sein. Teilaufgabe b) ist unabhängig von a) bearbeitbar.

Aufgabe 4. Diese Aufgabe kann man durch eine Rechnung oder auch allein durch eine geometrische Konstruktion lösen.

Aufgabe 5. Die Definition von R in Teilaufgabe a) lautet etwas ausführlicher

$$R = \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j).$$

Für die Bearbeitung der Aufgabe ist Satz 2.12 von Seite 58 des Skripts hilfreich. Ohne Beweis kann verwendet werden, dass dieser nicht nur für Polynome mit ganzen, rationalen, reellen, komplexen und algebraischen Koeffizienten funktioniert, sondern auch für Polynome, deren Koeffizienten selbst aus einem Rechenbereich von Polynomen (oder einem Rechenbereich von symmetrischen Polynomen) stammen. Diesen Satz wird man dann insgesamt zweimal anwenden müssen. Teilaufgabe b) kann *unabhängig* von Teilaufgabe a) bearbeitet werden. Mit *verschwinden* ist *Null sein* gemeint. Ein Ansatz ist (wieso?), den Ausdruck

$$R := (x_1 - y_1) \cdot (x_1 - y_2) \cdot (x_2 - y_1) \cdot (x_2 - y_2)$$

zu verwenden, wobei x_1, x_2 die Lösungen der ersten und y_1, y_2 die Lösungen der zweiten Gleichung sind. Dann muss man diesen Ausdruck so umschreiben, dass nur noch die Gleichungskoeffizienten, aber nicht mehr die Lösungen, vorkommen. Das ist etwa mit den Beziehungen aus dem Vietaschen Satz oder der Mitternachtsformel möglich.

Übungsblatt 7

Aufgabe 1. Bei Teilaufgabe a) sollte man unbedingt den euklidischen Algorithmus verwenden, wenn man nicht stundenlang knobeln möchte. Für Teilaufgabe b) hier die Erinnerung an die relevante Definition:

> Ein Polynom d heißt genau dann *größter gemeinsamer Teiler* zweier Polynome f und g, falls
>
> 1. es ein Teiler von f und von g (also ein gemeinsamer Teiler) ist und
> 2. für jeden gemeinsamen Teiler $\widetilde{d}$ von f und g gilt, dass $\widetilde{d}$ seinerseits ein Teiler von d ist (kurz: $\widetilde{d} \mid d$).

Ohne eine Normiertheitsbedingung haben übrigens je zwei Polynome unendlich viele größte gemeinsame Teiler. Wenn man von *dem* größten gemeinsamer Teiler spricht, ist von diesen unendlich vielen immer der normierte gemeint. Den Eindeutigkeitsteil von Teilaufgabe b) kann man mit folgender Vorlage in Angriff nehmen:

Seien d und $\widetilde{d}$ beides normierte größte gemeinsame Teiler von f und g. Dann..., daher folgt $d = \widetilde{d}$.

In den Teilaufgaben c) und d) ist (wie immer, aber diesmal steht es nicht explizit in der Angabe) auch die Korrektheit des von euch angegebenen Konstruktionsverfahrens zu beweisen. Natürlich ist aber die reine Angabe eines Verfahrens auch schon viel Wert! Die Definition in Teilaufgabe d), die ihr finden sollt, sollte das kleinste gemeinsame Vielfache nicht durch eine explizite Konstruktion, sondern durch seine gewünschten Eigenschaften charakterisieren.

Aufgabe 2. Beispiel 3.5 auf Seite 75 des Skripts zeigt eine Möglichkeit, Teilaufgabe a) zu lösen. Andere Lösungswege sind aber auch möglich. Für Teilaufgabe c) mag es hilfreich sein, dass der relevante größte gemeinsame Teiler im Skript schon berechnet worden ist.

Aufgaben 3 und 4. Der Bequemlichkeit halber hier die nötigen Definitionen:

1. Eine *Zerlegung* eines normierten Polynoms f mit rationalen Koeffizienten ist eine Darstellung von f als Produkt $f = f_1 \cdots f_n$ aus $n \geq 1$ normierten, nichtkonstanten Polynomen mit rationalen Koeffizienten.
2. Ein normiertes Polynom f mit rationalen Koeffizienten heißt genau dann *irreduzibel (über den rationalen Zahlen)*, wenn es genau eine Zerlegung zulässt, und zwar die triviale: $f = f$. Sonst heißt es *reduzibel*.

Aus der präzisen Art und Weise, wie diese Definitionen formuliert sind, folgt insbesondere, dass das Einspolynom (das ist das konstante Polynom 1) nicht als irreduzibel gilt (wieso?). Das ist auch gut so, denn sonst wäre die Eindeutigkeit der Zerlegung in irreduzible Faktoren (Proposition 3.9 im Skript) nicht mehr gegeben (wieso?). Abschließend sei bemerkt, dass die *Umkehrung* von Teilaufgabe 4a) Gegenstand der Vorlesung war (Folgerung 3.11 im Skript).

Aufgabe 5. In der Vorlesung wurde die analoge Aussage für Polynome bewiesen (Proposition 3.1 im Skript). Man kann also versuchen, den dortigen Beweis auf die neue Situation der Aufgabe zu übertragen. Man kann auch versuchen, etwas expliziter ein Verfahren zu beschreiben, welches das geforderte d berechnet, und dann die Korrektheit des Verfahrens zu beweisen.

Übungsblatt 8

Aufgabe 1. Hier kann das Verfahren aus Beispiel 3.7 oder Beispiel 3.8 des Skripts verwendet werden. Näherungswerte für die Nullstellen erhält man etwa bei `http://www.wolframalpha.com/`.

Aufgabe 2. Dass $f(X)$ *nicht verschwindet* bedeutet, dass es nicht das konstante Nullpolynom 0 ist. Mit $\widetilde{f}$ ist wie in der Vorlesung das Polynom $c^{-1} \cdot f$ gemeint, wobei c der Inhalt von f ist.

Aufgabe 3. Für Teilaufgabe b) ist es hilfreich, mit einer Bézoutdarstellung des größten gemeinsamen Teilers von a und n zu arbeiten; eine solche existiert nach Aufgabe 5 von Übungsblatt 7. Alle Teilaufgaben können unabhängig voneinanander bearbeitet werden.

Aufgabe 5. Für Teilaufgabe a) kann ohne Beweis folgender Satz über die sogenannte Existenz und Eindeutigkeit der Polynominterpolation verwendet werden:

> Sei $n \geq 0$. Seien $x_0, \ldots, x_n$ paarweise verschiedene rationale Zahlen. Seien $y_0, \ldots, y_n$ beliebige rationale Zahlen. Dann gibt es genau ein Polynom f mit rationalen Koeffizienten und Grad $\leq n$, dessen Graph durch die Punkte (x_i, y_i) geht, also sodass
>
> $$f(x_i) = y_i$$
>
> für alle $i = 0, \ldots, n$ gilt.

Außerdem hilft es für Teilaufgabe a), sich folgende Frage zu stellen: Wie viele Teiler kann eine ganze Zahl ungleich Null haben? Teilaufgabe b) kann dann mit a) und c) kann mit b) gelöst werden.

Übungsblatt 9

Aufgabe 1. In Teilaufgabe b) soll die Linearkombination den Wert 0 haben (*verschwinden*) ohne, dass sie *trivial* wäre, d. h., dass alle Koeffizienten der Linearkombination jeweils 0 wären. Alle Teilaufgaben können unabhängig voneinander bearbeitet werden. Nur zur Kontrolle: Der Koeffizient vor x^2 in der in Teilaufgabe a) gesuchten Linearkombination ist (-20). Die kleinste Möglichkeit für n in Teilaufgabe b) ist 6 (aber größere Werte sind auch möglich).

Aufgabe 2. Alle Teilaufgaben können unabhängig voneinander bearbeitet werden. Nur zur Kontrolle: Die Ergebnisse von Teilaufgabe a) sind 4, 2 und 2. Eine Möglichkeit für das gesuchte Polynom in Teilaufgabe b) ist das Minimalpolynom der Zahl aus a) über $\mathbb{Q}$ (also $X^4 - 4\,X^2 + 16$). Für Teilaufgabe d) sind vielleicht die (zu begründenden) Beobachtungen hilfreich, dass α eine primitive zehnte und ζ eine primitive fünfte Einheitswurzel ist. Um dann die Basis anzugeben, kann die Beobachtung nützlich sein, dass $-\zeta$ ebenfalls eine primitive zehnte Einheitswurzel ist. Alternativ hilft vielleicht die Beobachtung, dass ζ und α beide vom Grad 4 über $\mathbb{Q}$ sind (das Minimalpolynom von α ist $X^4 - X^3 + X^2 - X + 1$, später werden wir diesen Umstand tiefer verstehen).

Aufgabe 3. Allgemein ist mit $\deg_{\mathbb{Q}(a)} b$ der Grad der Zahl b über $\mathbb{Q}(a)$ gemeint. Dessen Definition findet sich im Skript direkt nach Proposition 3.35.

Aufgabe 4. Für Teilaufgabe a) kann das Verfahren der Vorlesung (siehe etwa Beispiel 3.30) verwendet werden. Bei Teilaufgabe b) kann man ein wenig mit den Potenzen $(\sqrt{2} + \sqrt{3})^2$, $(\sqrt{2} + \sqrt{3})^3$ knobeln. Bei Teilaufgabe c) ist ein Induktionsbeweis möglich (denn was ist das Signalwort?). Für Teilaufgabe d) kann man das Ergebnis von Teilaufgabe c) verwenden (auch ohne einen Beweis von c) zu kennen).

Aufgabe 5. Der Titel der Aufgabe ist irreführend, vermutlich ist die schwierigste Aufgabe des Blatts Aufgabe 2d).

Übungsblatt 10

Aufgabe 1. Teilaufgabe b) ist sehr ähnlich, aber nicht völlig identisch, zu Aufgabe 3c) von Übungsblatt 9. Das Vorgehen dort lässt sich auf die Aufgabe hier übertragen. Vielleicht

helfen zwei allgemeine Erinnerungen: Für den Grad einer algebraischen Zahl w über einer anderen algebraischen Zahl u gilt die Formel

$$\deg_{\mathbb{Q}(u)} w = [\mathbb{Q}(u,w) : \mathbb{Q}(u)].$$

Falls $u \in \mathbb{Q}(w)$, gilt ferner $\mathbb{Q}(u,w) = \mathbb{Q}(w)$, sodass sich die Formel dann noch ein wenig vereinfacht.

Aufgabe 3. Zur Kontrolle: Eine der Nullstellen ist $\exp(2\pi\mathrm{i}/8)$. Das gegebene Polynom ist tatsächlich irreduzibel, wie man etwa mit dem Eisensteinverschiebungstrick sehen kann. Falls ihr euer primitives Element gegenchecken wollt, schaut einfach kurz im Büro 2031/L1 vorbei oder schreibt eine Mail.

Aufgabe 4. Eine der beiden Richtungen in Teilaufgabe a) wurde schon in der Vorlesung gezeigt, die andere aber noch nicht. Für Teilaufgabe b) mag es hilfreich sein, dass die Komposition $(g \circ f)(X) = g(f(X))$ zweier Polynome g und f wieder ein Polynom ist.

Aufgabe 5. Der Bequemlichkeit halber hier die beiden Aussagen des Skripts:

> **Hilfssatz 4.3.** Seien $x_1, \ldots, x_n$ die Lösungen (mit Vielfachheiten) einer Polynomgleichung mit rationalen Koeffizienten. Ist dann $V(X_1, \ldots, X_n)$ ein Polynom mit rationalen Koeffizienten, so sind die galoissch Konjugierten von $t = V(x_1, \ldots, x_n)$ alle von der Form $t' = V(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, wobei σ eine n-stellige Permutation ist.
>
> **Proposition 4.4.** Seien $x_1, \ldots, x_n$ die Lösungen (mit Vielfachheiten) einer Polynomgleichung mit rationalen Koeffizienten. Ist dann t ein primitives Element zu $x_1, \ldots, x_n$, so ist auch jedes galoissch Konjugierte t' von t ein primitives Element von $x_1, \ldots, x_n$.

Übungsblatt 11

Aufgabe 1. Für Teilaufgabe b) muss man sich daran erinnern, wie die Rechenoperation Symmetrie der Nullstellen · Zahl aus $\mathbb{Q}(x_1, \ldots, x_n)$ definiert war. Die Hinrichtung von Teilaufgabe c) ist einfacher als die Rückrichtung. Für die Rückrichtung lohnt es sich vielleicht, das Polynom

$$\prod_{\sigma \in \mathrm{Gal}_{\mathbb{Q}}(x_1,\ldots,x_n)} (X - \sigma \cdot x_1)$$

zu betrachten.

Aufgabe 2. Um Missverständnisse zu vermeiden: Die beiden Nullstellen x_1 und x_2 des Polynoms $f(X)$ aus Teilaufgabe a) können wegen der vorausgesetzten Separabilität also als verschieden angenommen werden.

Aufgabe 3. Die beiden Teilaufgaben können unabhängig voneinander bearbeitet werden.

Aufgabe 4. Eine Formel auf dem Merkblatt zu Rechenbereichserweiterungen könnte hilfreich sein.

Aufgabe 5. Teilaufgabe b) kann durch Probieren oder durch das in Teilaufgabe c) vorgestellte Verfahren gelöst werden. Um die Behauptung von Teilaufgabe c) zu beweisen, kann es hilfreich sein, für zwei verschiedene Permutationen $\sigma, \tau \in S_n$ die Zahl

$$|V(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) - V(x_{\tau(1)}, \ldots, x_{\tau(n)})|$$

zu betrachten und zu versuchen, sie nach unten abzuschätzen. Dafür wiederum mag es hilfreich sein, den größten Index $k \in \{1, \ldots, n\}$ mit $\sigma(k) \neq \tau(k)$ gesondert zu betrachten.

Übungsblatt 12

Aufgabe 1. Für Teilaufgabe a) muss man nur einen wichtigen Satz aus der Gruppentheorie kennen. Für Teilaufgabe b) ist dieser Satz dagegen überhaupt nicht zu gebrauchen, besser ist es da, sich an den Definitionen zu orientieren. Für Teilaufgabe c) sind angesichts der Definition

$$\sigma^i := \begin{cases} \sigma \circ \cdots \circ \sigma \text{ (i Faktoren)}, & \text{falls } i \geq 1, \\ \mathrm{id}, & \text{falls } i = 0, \\ \sigma^{-1} \circ \cdots \circ \sigma^{-1} \text{ ($-i$ Faktoren)}, & \text{falls } i \leq -1, \end{cases}$$

vielleicht Fallunterscheidungen sinnvoll.

Aufgabe 2. Wenn man Teilaufgabe a) rechnerisch löst, ist die Angelegenheit ein bisschen fiddelig. Einfacher ist es, wenn man die Teilaufgabe durch eine saubere Skizze und eine präzise Begründung (als Text) löst. Die Definition der für Teilaufgabe b) benötigten zyklischen Gruppe steht im Skript auf Seite 123 (oben):

$$\mathrm{C}_n := \{\sigma_0, \ldots, \sigma_{n-1}\} \subseteq \mathrm{S}_n.$$

Die σ_k sind dabei auf der Seite zuvor (ganz unten) definiert. In Kombination mit Teilaufgabe a) kann man schnell die gesuchten Ordnungen angeben, wenn man nur erkennt, dass sich alle Elemente von C_n als Potenzen eines bestimmten Grundelements ausdrücken lassen (welchem, und wieso?). Für Teilaufgabe c) mag die für alle endlichen Gruppen G gültige Äquivalenz

$$x \in G \text{ ist ein Erzeuger von } G \iff \text{die Ordnung von } x \text{ ist } |G|$$

hilfreich sein (wieso gilt sie?).

Aufgabe 3. Im Skript und auf der englischen Wikipedia ist ein Verfahren beschrieben, um die in Teilaufgabe a) verlangten Kreisteilungspolynome zu berechnen. Teilaufgabe b) kann man kurz und knapp mit Kreisteilungspolynomen oder auch etwas langsamer über das übliche Verfahren lösen.

Aufgabe 4. Welche Nullstellen hat das Polynom in Teilaufgabe a) modulo p? Für Teilaufgabe b) ist vielleicht die Formel

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n \cdot (n-1) \cdots (n-k+2) \cdot (n-k+1)}{k \cdot (k-1) \cdots 2 \cdot 1}$$

hilfreich. Die beiden Teilaufgaben haben nichts miteinander zu tun.

Aufgabe 5. Wenn man die Definition kennt, kann man Teilaufgabe a) einfach durch Probieren lösen. Teilaufgabe b) hat mit der ersten nichts zu tun; hier ein paar Stichworte: Eine *Bijektion* ist eine bijektive (d. h. injektive und surjektive) Abbildung. Hier allerdings folgt aus Injektivität schon Surjektivität und umgekehrt (wieso gelten diese Ausnahmeregeln?). Wenn ζ_0 eine primitive n-te Einheitswurzel ist, ist $(\zeta_0)^d$ genau dann ebenfalls eine primitive n-te Einheitswurzel, wenn d zu n teilerfremd ist (wieso?).

Übungsblatt 13

Aufgabe 2. Bei Teilaufgabe a) funktioniert Induktion. Erhellende Beweise, die ohne Induktion oder mit Auslassungszeichen umgeschriebene Induktionstechniken auskommen, geben Bonuspunkte. Teilaufgabe b) kann man mit a) lösen. Für Teilaufgaben c) und d) hilft vielleicht die wichtigste Formel der Analysis (die über die geometrische Reihe).

Aufgabe 3. Die Galoisgruppe haben wir schon in Aufgabe 3 von Blatt 10 berechnet: Wenn wir die Nullstellen in der Reihenfolge

$$x_1 = \xi, \quad x_2 = \xi^3, \quad x_3 = \xi^5, \quad x_4 = \xi^7,$$

notieren, wobei $\xi = \exp(2\pi\mathrm{i}/8)$ eine der primitiven achten Einheitswurzeln ist, ist $t := \xi$ ein primitives Element und es gilt

$$\begin{aligned}\mathrm{Gal}_{\mathbb{Q}}(x_1,x_2,x_3,x_4) &= \{\mathrm{id},\ (1,2)\circ(3,4),\ (1,3)\circ(2,4),\ (1,4)\circ(2,3)\}\\ &= \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}.\end{aligned}$$

Zur Kontrolle: Insgesamt gibt es fünf Untergruppen, eine von Ordnung 1, drei von Ordnung 2, keine von Ordnung 3 und eine von Ordnung 4. Die zugehörigen Zwischenerweiterungen kann man mit der Formel aus Proposition 5.9 (Seite 167) ausrechnen und mit den Rechenregeln für Rechenbereichserweiterungen vereinfachen. Etwa gehört zu der Untergruppe

$$H = \{\mathrm{id}, \sigma\}$$

mit $\sigma := (1,2)\circ(3,4)$ die Zwischenerweiterung

$$\begin{aligned}\mathbb{Q}(x_1,x_2,x_3,x_4)^H &= \mathbb{Q}(t)^H = \mathbb{Q}(e_1(\mathrm{id}\cdot t, \sigma\cdot t), e_2(\mathrm{id}\cdot t, \sigma\cdot t))\\ &= \mathbb{Q}(e_1(\xi,\xi^3), e_2(\xi,\xi^3)) = \mathbb{Q}(\xi+\xi^3, \xi\cdot\xi^3)\\ &= \mathbb{Q}(\xi+\xi^3, -1) = \mathbb{Q}(\xi+\xi^3) = \mathbb{Q}(\sqrt{2}\,\mathrm{i}).\end{aligned}$$

Aufgabe 6. Die Aufgabe soll dabei helfen, den Beweis von Proposition 4.34 genauer zu verstehen, denn hier geht es um eine Verallgemeinerung. Für Teilaufgabe a) kann man sich überlegen, wie viele Elemente die Galoisgruppe denn enthält und mit ein wenig Skriptwissen dann sofort die Behauptung folgern. Für Teilaufgabe b) sollte man sich erst ein wenig Ordnung schaffen: Die insgesamt p^n Zahlen x_i zerfallen in Blöcke von je p Zahlen, die von σ jeweils nur unter sich abgebildet werden (wieso?); die Zahlen $x_1, \sigma\cdot x_1, \ldots, \sigma^{p-1}\cdot x_1$ bilden einen dieser Blöcke. Dann kann man sich ein wenig vom Beweis von Proposition 4.34 inspirieren lassen.

Dann kann man $[\mathbb{Q}(y) : \mathbb{Q}] \leq p^{n-1}$ dadurch nachweisen, indem man ein geeignetes Polynom vom Grad p^{n-1} mit rationalen Koeffizienten und y als Nullstelle angibt. Ferner kann man ein Polynom vom Grad p mit Koeffizienten aus $\mathbb{Q}(y)$ und x als Nullstelle angeben, um nachzuweisen, dass $[\mathbb{Q}(x) : \mathbb{Q}(y)] \leq p$ gilt. Daraus folgt dann die Behauptung (wie?).