Prüfungsteilnehmer	Prüfungstermin	Einzelprüfungsnummer
Kennzahl: ____________	Frühjahr 2024	63912
Kennwort: ____________		
Arbeitsplatz-Nr.: ________		

Erste Staatsprüfung für ein Lehramt an öffentlichen Schulen

— Prüfungsaufgaben —

Fach: **Mathematik (vertieft studiert)**

Einzelprüfung: **Algebra**

Anzahl der gestellten Themen (Aufgaben): 3

Anzahl der Druckseiten dieser Vorlage: 7

Bitte wenden!

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Sei $n > 0$ und $M_n = (m_{ij})$ die reelle $n \times n$-Matrix mit $m_{ij} = 0$, falls $j < i - 1$ oder $j > i + 1$, $m_{ij} = 1$, falls $j = i - 1$, $m_{ij} = 3$, falls $j = i$ und $m_{ij} = 2$, falls $j = i + 1$. Also ist beispielsweise

$$M_5 = \begin{pmatrix} 3 & 2 & 0 & 0 & 0 \\ 1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & 0 & 1 & 3 \end{pmatrix}.$$

Sei d_n die Determinante von M_n.

(a) Berechnen Sie d_1 und d_2.

(b) Zeigen Sie, dass für alle $n \geq 3$ gilt $d_n = 3d_{n-1} - 2d_{n-2}$.

(c) Zeigen Sie, dass $d_n = 2^{n+1} - 1$ gilt.

Aufgabe 2 (12 Punkte)

(a) Bestimmen Sie alle $n \in \{1, 2, 3, \ldots\}$, für die die Gruppe $\mathbb{Z}/n\mathbb{Z}$ außer der Identität keinen weiteren Gruppenautomorphismus besitzt.

Sei G eine endliche Gruppe der Ordnung ≥ 2 mit der Eigenschaft, dass die Identität der einzige Gruppenautomorphismus ist.

(b) Zeigen Sie, dass G eine abelsche Gruppe ist.

(c) Zeigen Sie, dass $G \cong \mathbb{Z}/2\mathbb{Z}$ ist.

Aufgabe 3 (12 Punkte)

(a) Sei R ein kommutativer Ring. Ein Element $x \in R$ heißt *nilpotent*, falls es ein $k \in \{1, 2, 3, ...\}$ gibt mit $x^k = 0$. Sei $I \subset R$ ein Primideal und $x \in R$ nilpotent. Zeigen Sie $x \in I$.

(b) Sei $I = (1 + i)$ das von $1 + i$ erzeugte Ideal im Ring $\mathbb{Z}[i]$. Zeigen Sie, dass der Ring $\mathbb{Z}[i]/I$ genau zwei Elemente hat.

(c) Seien R ein Integritätsbereich und $a, b, c \in R$. Zeigen Sie: Erzeugen a und b in R das Einsideal und ist a ein Teiler von bc, so ist a ein Teiler von c.

Aufgabe 4 (12 Punkte)

Sei p eine Primzahl mit der Eigenschaft, dass $p-1 = p_1 \cdot \ldots \cdot p_n$ Produkt der paarweise verschiedenen Primzahlen $p_1, \ldots, p_n$ ist.

(a) Zeigen Sie, dass es genau 2^n verschiedene Untergruppen in $G = (\mathbb{Z}/p\mathbb{Z})^\times$ gibt.

(b) Sei $\zeta_p \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Bestimmen Sie die Anzahl der Zwischenkörper in der Körpererweiterung $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

Aufgabe 5 (12 Punkte)

Sei $\alpha = \sqrt{10 - 5\sqrt{2}} \in \mathbb{R}$.

(a) Bestimmen Sie das Minimalpolynom von α über $\mathbb{Q}$.

(b) Zeigen Sie, dass $\mathbb{Q}(\alpha)/\mathbb{Q}$ eine Galoiserweiterung ist.

(c) Zeigen Sie, dass die Galoisgruppe von $\mathbb{Q}(\alpha)/\mathbb{Q}$ zu $\mathbb{Z}/4\mathbb{Z}$ isomorph ist.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

(a) Bestimmen Sie eine Zerlegung des Elements $z = 29 \in \mathbb{Z}[i]$ in Primelemente.

(b) Es sei $p > 3$ eine Primzahl. Zeigen Sie, dass es in der multiplikativen Gruppe $\mathbb{F}_{p^2}^{\times}$ ein Element a der Ordnung 12 gibt.

(c) Entscheiden Sie, ob $\overline{437} \in \mathbb{Z}/911\mathbb{Z}$ invertierbar ist. Bestimmen Sie gegebenenfalls das Inverse.

(d) Entscheiden Sie begründet, ob $\mathbb{R}$ eine algebraische Erweiterung von Grad 4 hat.

Aufgabe 2 (12 Punkte)

Es sei $N = a_{n-1}a_{n-2}\ldots a_1a_0$ mit $a_i \in \{0,\ldots,9\}, a_{n-1} \neq 0$ die dezimale Zifferndarstellung einer natürlichen Zahl N.

(a) Die *Wechselsumme* von N ist durch

$$W(N) = \sum_{i=0}^{n-1}(-1)^i a_i$$

gegeben. (Beispiel: $W(123456) = 6 - 5 + 4 - 3 + 2 - 1$)

Zeigen Sie: Es ist N genau dann durch 11 teilbar, wenn $W(N)$ durch 11 teilbar ist.

(b) Wir nennen N *palindromisch*, wenn die Ziffernanzahl n gerade ist und

$$a_{n-1}a_{n-2}\ldots a_1a_0 = N = a_0a_1\ldots a_{n-2}a_{n-1}$$

gilt. (Beispiel: 493394 ist palindromisch.)

Bestimmen Sie alle palindromischen Primzahlen.

(c) Sei die Folge (U_n) mit $U_1 = 1, U_2 = 11, U_3 = 111, U_4 = 1111, \ldots$ gegeben.

Zeigen Sie:

(i) Im Fall $k \mid n$ gilt $U_k \mid U_n$.

(ii) Ist $n = k \cdot \ell$ mit $k, \ell \in \{2, 3, 4, \ldots\}$, so ist U_n keine Primzahl.

Aufgabe 3 (12 Punkte)

(a) Entscheiden und begründen Sie, ob es eine Gruppe gibt, die außer dem neutralen Element vier Elemente der Ordnung 5, sechs Elemente der Ordnung 2 und keine weiteren Elemente enthält.

(b) Entscheiden und begründen Sie, ob es eine abelsche Gruppe gibt, die nur Elemente mit den Ordnungen 1, 2 und 4 enthält, wobei die Anzahl der Elemente durch

Ordnung	1	2	4
Anzahl	1	3	12

gegeben ist. Entscheiden Sie begründet, ob die abelsche Gruppe durch diese Angabe bis auf Isomorphie eindeutig bestimmt ist.

(c) Beweisen oder widerlegen Sie die folgende Aussage: Ist G eine endliche Gruppe und d ein Teiler der Gruppenordnung $\#G$, so hat G eine Untergruppe U mit $\#U = d$.

Aufgabe 4 (12 Punkte)

(a) Entscheiden Sie begründet, ob ein Ring R existiert, der unendlich viele Einheiten $u \in R^\times$ endlicher multiplikativer Ordnung hat. (D. h. $\mathrm{ord}_{R^\times}(u) < \infty$.)

(b) Entscheiden Sie begründet, ob ein Ring R existiert, der unendlich viele Einheiten $u \in R^\times$ endlicher additiver Ordnung hat. (D. h. $\mathrm{ord}_{(R,+)}(u) < \infty$.)

(c) Entscheiden Sie begründet, ob ein Ring R existiert, der nur endlich viele Einheiten hat und in dem die multiplikative Ordnung einer Einheit $u \in R^\times$ unendlich ist.
(D. h. $\mathrm{ord}_{R^\times}(u) = \infty$.)

Aufgabe 5 (12 Punkte)

Es seien $a_1, \ldots, a_n \in \mathbb{Q}$ und das Polynom $f \in \mathbb{Q}[X]$ von Grad $2n$ durch

$$f := X^{2n} + a_1X^{2n-1} + \cdots + a_{n-1}X^{n+1} + a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + 1$$

gegeben. Sei K der Zerfällungskörper von f über $\mathbb{Q}$. Zeigen Sie:

(a) Ist r eine Nullstelle von f, so ist auch $\frac{1}{r}$ eine Nullstelle von f.

(b) Es ist $\#\mathrm{Gal}(K/\mathbb{Q}) \leq 2^n \cdot n!$.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

(a) Es sei $\mathbb{F}_3$ der endliche Körper mit drei Elementen. Bestimmen Sie die Anzahl der Elemente des Kerns U der linearen Abbildung $\varphi : \mathbb{F}_3^3 \to \mathbb{F}_3^2$, $\varphi(v) = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix} v.$

(b) Bestimmen Sie eine Zerlegung des Polynoms $f = 2X^3 + 4X^2 - 2X \in \mathbb{Z}[X]$ in über $\mathbb{Z}$ irreduzible Faktoren.

(c) Bestimmen Sie ein $f \in \mathbb{R}[X]$ mit $(f) = (X^2 - 1, X^3 - 1)$ und begründen Sie, warum Ihre Wahl diese Gleichheit erfüllt.

(d) Zeigen Sie, dass das Element $2 \in \mathbb{Z}[\sqrt{-13}]$ irreduzibel ist.

Aufgabe 2 (12 Punkte)

(a) Ermitteln Sie die Anzahl der Lösungen der folgenden Gleichungen in $\mathbb{Z}/8\mathbb{Z}$.

$$x^5 = 0\,, \qquad x^5 = 1\,, \qquad x^5 = 2\,, \qquad x^5 = 3$$

(b) Ermitteln Sie die Anzahl der Lösungen der folgenden Gleichungen in $\mathbb{Z}/2024\mathbb{Z}$. ($2024 = 8 \cdot 11 \cdot 23$)

$$x^5 = 0\,, \qquad x^5 = 1\,, \qquad x^5 = 2\,, \qquad x^5 = 3$$

(c) Bestimmen Sie, wie viele fünfte Potenzen es in $\mathbb{Z}/2024\mathbb{Z}$ gibt.

Aufgabe 3 (12 Punkte)

Für eine Primzahl p sei $\mathbb{F}_p$ der endliche Körper mit $|\mathbb{F}_p| = p$; weiter sei $R := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \, a, b \in \mathbb{F}_p \right\}$.

(a) Zeigen Sie, dass R ein Teilring des Ringes der 2×2-Matrizen über $\mathbb{F}_p$ ist.

(b) Zeigen Sie, dass die Einheitengruppe $R^\times$ im Fall $p \neq 2$ nicht einfach ist.

(c) Nun sei $p = 257$. Entscheiden Sie begründet, ob die Einheitengruppe $R^\times$ in diesem Fall auflösbar ist.

Aufgabe 4 (12 Punkte)

(a) Seien K ein Körper und $f \in K[X]$ ein irreduzibles separables Polynom über K. Begründen Sie, warum die Ordnung der Galoisgruppe von f über K durch den Grad von f teilbar ist.

(b) Geben Sie ein Beispiel an, wieso die Aussage in (a) im Allgemeinen falsch wird, wenn f nicht mehr als irreduzibel vorausgesetzt wird.

(c) Begründen Sie, warum es zu jeder natürlichen Zahl $n \geq 1$ eine Galoiserweiterung E/F von Körpern E, F gibt, deren Galoisgruppe die Ordnung n hat.

(d) Zeigen Sie, dass die Aussage in (c) im Allgemeinen falsch wird, wenn der Körper F fest vorgegeben wird.

Aufgabe 5 (12 Punkte)

(a) Geben Sie eine explizite Darstellung der primitiven fünften Einheitswurzeln mithilfe von Quadratwurzeln an.

(Tipp: Wenn $X^4+X^3+X^2+X+1 = 0$, welche Polynomgleichung erfüllt dann $Y := X+X^{-1}$?)

(b) Folgern Sie aus Ihrer Lösung der Teilaufgabe (a) eine Konstruktionsvorschrift eines regelmäßigen Fünfecks mit Zirkel und Lineal.

(c) Geben Sie eine Konstruktionsvorschrift eines regelmäßigen Zwanzigecks mit Zirkel und Lineal an.

Prüfungsteilnehmer	Prüfungstermin	Einzelprüfungsnummer
Kennzahl: ______ Kennwort: ______ Arbeitsplatz-Nr.: ______	**Herbst 2024**	**63912**

Erste Staatsprüfung für ein Lehramt an öffentlichen Schulen

— Prüfungsaufgaben —

Fach: **Mathematik (vertieft studiert)**

Einzelprüfung: **Algebra**

Anzahl der gestellten Themen (Aufgaben): 3

Anzahl der Druckseiten dieser Vorlage: 7

Bitte wenden!

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Sei H die Menge aller reellen 2×2 - Matrizen der Form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

mit $a^2 + b^2 \neq 0$.

(a) Zeigen Sie, dass H eine Untergruppe der Gruppe $\mathrm{GL}(2, \mathbb{R})$ der invertierbaren reellen 2×2 - Matrizen ist.

(b) Seien $A, B, C \in H$. Zeigen Sie, dass die Gleichung $AYB = C$ eine eindeutige Lösung Y in H hat.

(c) Lösen Sie die Gleichung

$$\begin{pmatrix} 4 & 3 \\ -3 & 4 \end{pmatrix} Y \begin{pmatrix} 6 & 2 \\ -2 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix}.$$

Aufgabe 2 (12 Punkte)

Sei G eine Gruppe der Ordnung 2024 $(= 2^3 \cdot 11 \cdot 23)$. Zeigen Sie:

(a) G hat einen Normalteiler H der Ordnung 23.

(b) H operiert transitiv durch Konjugation auf den Untergruppen der Ordnung 11.

(c) G hat einen Normalteiler N der Ordnung 253.

(d) G ist auflösbar.

Aufgabe 3 (12 Punkte)

Sei K ein Körper und sei

$$R := \left\{ \sum_{i=0}^{n} a_i X^i \in K[X] \,\middle|\, a_1 = 0 \right\}.$$

(a) Zeigen Sie, dass R ein Teilring (mit Eins) des Polynomrings $K[X]$ über K ist.

(b) Entscheiden Sie begründet, ob $f = X^3 \in R$ irreduzibel ist und ob $f = X^3 \in R$ prim ist.

(c) Entscheiden Sie begründet, ob R ein faktorieller Ring ist.

(d) Geben Sie ein $a \in R$ an, sodass das Ideal (X^3, a) von R kein Hauptideal ist, und begründen Sie Ihre Wahl.

Aufgabe 4 (12 Punkte)

(a) Sei $K/\mathbb{Q}$ eine Körpererweiterung. Zeigen Sie, dass jeder Körperautomorphismus von K ein $\mathbb{Q}$-Automorphismus ist.

(b) Sei K eine endliche Körpererweiterung von $\mathbb{Q}$ und sei $\varphi : K \to K$ ein Körperhomomorphismus. Zeigen Sie, dass φ bijektiv ist.

(c) Geben Sie eine Körpererweiterung K von $\mathbb{Q}$ und einen Körperhomomorphismus $\varphi : K \to K$ an, der nicht bijektiv ist. Begründen Sie dabei Ihre Aussagen.

Aufgabe 5 (12 Punkte)

(a) Zeigen Sie: Ist L/K eine Körpererweiterung vom Grad 2 und ist $\operatorname{char}(K) \neq 2$, so ist L/K eine Galoiserweiterung.

(b) Geben Sie begründet eine Körpererweiterung L/K vom Grad 2 an, die nicht galoissch ist.

(c) Geben Sie für jedes $n \in \mathbb{N}$ mit $n \geq 3$ eine Körpererweiterung $K/\mathbb{Q}$ vom Grad n an, die nicht galoissch ist, und geben Sie für Ihre Beispiele die Anzahl der Körperautomorphismen von K an. Begründen Sie dabei Ihre Aussagen.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Sei R ein Ring und eine Folge $(a_n)_{n\geq 0}$ von Elementen von R rekursiv definiert wie folgt:

$$a_0 = a_1 = 1\,, \qquad a_{n+2} = 2a_{n+1} + a_n\,.$$

(a) Sei $\alpha \in R$ mit $\alpha^2 = 2$. Zeigen Sie, dass dann für alle $n \geq 0$ gilt

$$2a_n = (1+\alpha)^n + (1-\alpha)^n\,.$$

(b) Sei p eine ungerade Primzahl, sodass es ein $\alpha \in R = \mathbb{F}_p$ (der Körper mit p Elementen) gibt mit $\alpha^2 = 2$.

Zeigen Sie, dass die Folge (a_n) periodisch ist mit einer minimalen Periode, die $p-1$ teilt.

(c) Bestimmen Sie die kleinste ganze Zahl $k > 0$, sodass für $R = \mathbb{F}_7$ gilt $a_{n+k} = a_n$ für alle $n \geq 0$.

(d) Zeigen Sie, dass es für $R = \mathbb{Z}$ keine ganzen Zahlen $m, n \geq 0$ mit der Eigenschaft $a_n = m^6 + 4$ gibt.

Aufgabe 2 (12 Punkte)

(a) Bestimmen Sie die ganze Zahl $a \in \{0, \ldots, 82\}$ mit $50^{247} \equiv a \pmod{83}$.

(b) Der Satz von Wilson besagt, dass $(p-1)! \equiv -1 \,(\operatorname{mod} p)$ für jede Primzahl p gilt. Bestimmen Sie hiermit die ganze Zahl $a \in \{0, \ldots, 100\}$ mit $98! \equiv a \pmod{101}$.

Hinweis: Sie dürfen den Satz von Wilson ohne Beweis benutzen.

(c) Im Folgenden bezeichne φ die Eulersche φ-Funktion. Beweisen oder widerlegen Sie:

(i) für alle $m, n \in \mathbb{N}$ mit $n > m$ gilt $\varphi(n) \geq \varphi(m)$;

(ii) für alle $n \in \mathbb{N}$ gilt $\varphi(2n) \geq \varphi(n)$;

(iii) für alle $n \in \mathbb{N}$ gilt $\varphi(n) \mid \varphi(n^2)$.

Aufgabe 3 (12 Punkte)

(a) Es sei $n \in \mathbb{N}$ und es sei G eine einfache Untergruppe der symmetrischen Gruppe S_n mit $|G| > 2$. Zeigen Sie, dass G bereits eine Untergruppe der alternierenden Gruppe A_n ist.

(b) Es sei G eine einfache Gruppe der Ordnung 90. Zeigen Sie, dass G zu einer Untergruppe der alternierenden Gruppe A_6 isomorph ist.

(c) Zeigen Sie, dass es keine einfache Gruppe der Ordnung 90 gibt.

Aufgabe 4 (12 Punkte)

Im Folgenden sei $R := \mathbb{Z} + i\mathbb{Z}$ der Ring der ganzen Gauß'schen Zahlen. Ohne Beweis darf benutzt werden, dass dies ein euklidischer Ring bezüglich der Normabbildung

$$N : R\backslash\{0\} \to \mathbb{N}, x + iy \mapsto x^2 + y^2$$

und somit insbesondere ein Hauptidealring und ein faktorieller Ring ist.

(a) Bestimmen Sie alle $a \in R$ mit $N(a) \leq 5$.

(b) Schreiben Sie mithilfe der Teilaufgabe (a) jede der ganzen Zahlen aus $\{2, \ldots, 6\}$ als Produkt irreduzibler Elemente in R.

(c) Bestimmen Sie ein $d \in R$ mit $(d) = (5 + 10i, 1 + 3i)$. Zeigen Sie, dass $R/(d)$ ein Körper ist.

Aufgabe 5 (12 Punkte)

Gegeben sei das Polynom $f := X^6 - 6 \in \mathbb{Q}[X]$.

(a) Es sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von f über $\mathbb{Q}$. Bestimmen Sie den Grad $[L : \mathbb{Q}]$.

(b) Zeigen Sie, dass $L/\mathbb{Q}$ eine Galoiserweiterung ist. Zeigen Sie weiter, dass die Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$ einen Normalteiler der Ordnung 6 enthält.

(c) Entscheiden Sie begründet, ob die Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$ abelsch ist.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Für einen Körper K sei $G(K) := \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle|\ a, b \in K \right\}$.

(a) Zeigen Sie, dass $G(K)$ eine abelsche Untergruppe von $\mathrm{GL}(3, K)$ ist.

(b) Für eine Primzahl p sei $\mathbb{F}_p$ der endliche Körper mit $|\mathbb{F}_p| = p$. Entscheiden Sie begründet, zu welchem direkten Produkt zyklischer Gruppen $G(\mathbb{F}_p)$ isomorph ist. (Hauptsatz für endliche abelsche Gruppen)

(c) Für eine Primzahl p sei $\mathbb{F}_{p^2}$ der endliche Körper mit $|\mathbb{F}_{p^2}| = p^2$. Entscheiden Sie begründet, zu welchem direkten Produkt zyklischer Gruppen $G(\mathbb{F}_{p^2})$ isomorph ist. (Hauptsatz für endliche abelsche Gruppen)

Aufgabe 2 (12 Punkte)

Sei R der Restklassenring $\mathbb{Z}[X]/(X^3 + X)$.

(a) Zeigen Sie, dass R zum Produktring $\mathbb{Z} \times \mathbb{Z}[i]$ isomorph ist.

(b) Geben Sie sämtliche Einheiten des Ringes $\mathbb{Z} \times \mathbb{Z}[i]$ an.

(c) Bestimmen Sie alle Elemente $a, b \in \mathbb{Z}$, sodass die Restklasse von $X^2 + aX + b$ in R eine Einheit ist.

Aufgabe 3 (12 Punkte)

Sei $f = X^{2024} + 2024 \in \mathbb{Z}[X]$. Wir definieren die Iterierten von f als $f_0 = X$ und $f_{n+1} = f(f_n) = f_n^{2024} + 2024$ für $n \geq 0$. Zeigen Sie:

(a) f ist irreduzibel.

(b) Für alle $n \geq 1$ gilt $f_n(0) \equiv 2024 \bmod 2024^2$.

(c) f_n ist irreduzibel für alle $n \geq 0$.

Aufgabe 4 (12 Punkte)

Sei $f(X) = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$ und sei $a \in \mathbb{C}$ eine beliebige Nullstelle von f.

(a) Zeigen Sie durch Polynomdivision, dass $f(X^2 - 2)$ durch $f(X)$ teilbar ist.

(b) Zeigen Sie, dass a und $a^2 - 2$ verschiedene Nullstellen von f sind.

(c) Zeigen Sie, dass $\mathbb{Q}(a)/\mathbb{Q}$ eine Galoiserweiterung ist, deren Galoisgruppe zu $\mathbb{Z}/3\mathbb{Z}$ isomorph ist.

Aufgabe 5 (12 Punkte)

Sei $\zeta_{16} = e^{\frac{2\pi i}{16}} \in \mathbb{C}$.

(a) Zeigen Sie, dass $\mathbb{Q}(\zeta_{16})/\mathbb{Q}(i)$ eine Galoiserweiterung vom Grad 4 ist.

(b) Bestimmen Sie das Minimalpolynom von ζ_{16} über $\mathbb{Q}(i)$.

(c) Entscheiden Sie begründet, ob die Galoisgruppe von $\mathbb{Q}(\zeta_{16})/\mathbb{Q}(i)$ zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ isomorph ist.