Klausur zur Algebra für Lehramt

Beachten Sie die folgenden **Hinweise:**

- **Bearbeitungszeit:** 120 Minuten.
- **Erlaubte Hilfsmittel:** Vier eigenhändig handbeschriebene Seiten DIN A4.
- Wer den Klausurraum vor Ende der Bearbeitungszeit endgültig verlässt, hat damit zu rechnen, dass seine Klausur als nicht bestanden gewertet wird.
- Eintragungen mit Bleistift oder Rotstift sind unerwünscht.
- **Antworten sind zu begründen.** Nachvollziehbare Rechnungen zählen als Begründungen.
- Es sind insgesamt 40 Punkte erreichbar.
- Die Prüfungsergebnisse werden voraussichtlich ab dem **01.10.2022** im Campus-System bekanntgegeben.

Viel Erfolg!

Hinweise für Wiederholer:

Wer diese Prüfung als Wiederholungsprüfung schreibt, wird darauf hingewiesen, dass zu dieser Wiederholungsprüfung unter bestimmten Umständen eine mündliche Nachprüfung gehört, es sei denn, die schriftliche Prüfung ergibt die Note 4,0 oder besser.

Wiederholer, bei denen eine mündliche Nachprüfung erforderlich ist, müssen dafür mit dem Prüfer bis zum **15.10.2022** einen Termin vereinbaren. Sie sind verpflichtet, sich rechtzeitig über das Ergebnis der schriftlichen Prüfung zu informieren und sich zum vereinbarten Zeitpunkt für die mündliche Nachprüfung bereitzuhalten.

Mit Ihrer Teilnahme an dieser Prüfung erkennen Sie diese Verpflichtungen an.

Aufgabe 1 (2+1+2 Punkte)

(1) Untersuchen Sie unter Verwendung des Satzes von Descartes, ob das Polynom $X^3+X+3 \in \mathbb{Z}[X]$ eine Nullstelle in $\mathbb{Q}$ hat.

(2) Folgern Sie aus (1): Es ist $X^3 + X + 3$ irreduzibel in $\mathbb{Q}[X]$.

(3) Zeigen Sie: Es ist $X^9 + 6X + 3$ irreduzibel in $\mathbb{Q}[X]$.

Lösung.

Zu (1). Die Nullstellen in $\mathbb{Q}$ des Polynoms $f(X) := X^3 + X + 3$ sind enthalten in der Menge $\{-1, 1, -3, 3\}$ der Teiler des Koeffizienten 3 von X^0.

Es ist $f(-1) = (-1)^3 + (-1) + 3 = 1$.

Es ist $f(1) > 0$.

Es ist $f(-3) = (-3)^3 + (-3) + 3 = -27$.

Es ist $f(3) > 0$.

Also hat $f(X) = X^3 + X + 3$ keine Nullstelle in $\mathbb{Q}$.

Zu (2). Da $\deg(X^3 + X + 3) = 3 \in \{2, 3\}$ liegt und da gemäß (1) dieses Polynom keine Nullstelle in $\mathbb{Q}$ hat, folgt, daß $X^3 + X + 3 \in \mathbb{Q}[X]$ irreduzibel ist.

Zu (3). Wir wenden das Eisenstein-Kriterium an für die Primzahl $p = 3$.

Außer dem Leitkoeffizient sind alle Koeffizienten von $X^9 + 6X + 3$ durch 3 teilbar.

Der Koeffizient 3 von X^0 ist nicht durch 3^2 teilbar.

Gemäß Eisenstein-Kriterium ist also $X^9 + 6X + 3 \in \mathbb{Q}[X]$ irreduzibel.

Aufgabe 2 (1+2+1 Punkte)

(1) Man bestimme einen Ringisomorphismus φ von $\mathbb{Z}/(15)$ nach $\mathbb{Z}/(3) \times \mathbb{Z}/(5)$.

(2) Man bestimme zu φ aus (1) eine Abbildungsvorschrift für $\varphi^{-1} : \mathbb{Z}/(3) \times \mathbb{Z}/(5) \xrightarrow{\sim} \mathbb{Z}/(15)$.

(3) Man finde Elemente $e,\ f \in (\mathbb{Z}/(15))^\times$ mit $e + f = 1$ und $e^2 = e$ und $f^2 = f$.

Lösung.

Zu (1). Es ist $(3)+(5) = (\mathrm{ggT}(3,5)) = (1) = \mathbb{Z}$. Es ist $(3)\cap(5) = (\mathrm{kgV}(3,5)) = (15)$. Der chinesische Restsatz gibt also folgenden Ringisomorphismus.

$$\begin{array}{ccccc} \mathbb{Z}/(15) & \xrightarrow[\sim]{\varphi} & \mathbb{Z}/(3) & \times & \mathbb{Z}/(5) \\ z + (15) & \mapsto & (z + (3) & , & z + (5)) \end{array}$$

Zu (2). Es ist

$$\begin{array}{rcl} -5 + (15) & \overset{\varphi}{\mapsto} & (1 + (3), 0 + (5)) \\ 6 + (15) & \overset{\varphi}{\mapsto} & (0 + (3), 1 + (5)) \end{array}$$

Also ist

$$-5a + 6b + (15) \ \overset{\varphi}{\mapsto}\ (a + (3), b + (5))$$

für $a,\ b \in \mathbb{Z}$. Folglich ist

$$\varphi^{-1}\big((a + (3), b + (5))\big) \ = \ -5a + 6b + (15)\ ,$$

wobei $a,\ b \in \mathbb{Z}$.

Zu (3). In $(\mathbb{Z}/(3) \times \mathbb{Z}/(5))^\times$ können wir $\tilde{e} := (1 + (3),\ 0 + (5))$ und $\tilde{f} := (0 + (3),\ 1 + (5))$ wählen und erhalten $\tilde{e} + \tilde{f} = 1$, $\tilde{e}^2 = \tilde{e}$ und $\tilde{f}^2 = \tilde{f}$.

Also ist mit

$$\begin{array}{rcccl} e & := & \varphi^{-1}(\tilde{e}) & = & -5 + (15) \\ f & := & \varphi^{-1}(\tilde{f}) & = & 6 + (15) \end{array}$$

auch $e + f = 1$ und $e^2 = e$ und $f^2 = f$.

Aufgabe 3 (2 Punkte)

Man bestimme x, $y \in \mathbb{Z}$ mit

$$\mathrm{v}_5(x+y) \ > \ \min\{\mathrm{v}_5(x), \mathrm{v}_5(y)\} \ > \ 0 \ .$$

Lösung.

Sei $x := 5$ und $y := 20$.

Dann ist $\mathrm{v}_5(x+y) = \mathrm{v}_5(25) = 2$.

Ferner ist $\min\{\mathrm{v}_5(x), \mathrm{v}_5(y)\} = \min\{\mathrm{v}_5(5), \mathrm{v}_5(20)\} = \min\{1, 1\} = 1$.

Also ist in der Tat $\mathrm{v}_5(x+y) > \min\{\mathrm{v}_5(x), \mathrm{v}_5(y)\} > 0$.

Aufgabe 4 (2+1+1 Punkte)

Wir betrachten S_4 als S_4-Menge via Konjugation.

(1) Man bestimme $\mathrm{Stab}_{\mathrm{S}_4}\big((1,2,4)\big) = \mathrm{C}_{\mathrm{S}_4}\big((1,2,4)\big)$.

(2) Man bestimme $|\,{}^{\mathrm{S}_4}(1,2,4)|$ unter Verwendung des Bahnenlemmas.

(3) Man bestimme $\{\, f \in {}^{\mathrm{S}_4}(1,2,4) \,:\, f(1) = 3 \,\}$.

Lösung.

Zu (1). Für $f \in \mathrm{S}_4$ ist ${}^{f}(1,2,4) = (1,2,4) = (2,4,1) = (4,1,2)$ genau dann, wenn einer der folgenden drei Fälle eintritt.

Fall 1. Es ist $f(1) = 1$, $f(2) = 2$ und $f(4) = 4$. Dann ist $f(3) = 3$. Es folgt $f = \mathrm{id}$.

Fall 2. Es ist $f(1) = 2$, $f(2) = 4$ und $f(4) = 1$. Dann ist $f(3) = 3$. Es folgt $f = (1,2,4)$.

Fall 3. Es ist $f(1) = 4$, $f(2) = 1$ und $f(4) = 2$. Dann ist $f(3) = 3$. Es folgt $f = (1,4,2)$.

Also ist $\mathrm{Stab}_{\mathrm{S}_4}\big((1,2,4)\big) = \mathrm{C}_{\mathrm{S}_4}\big((1,2,4)\big) = \{\mathrm{id}, (1,2,4), (1,4,2)\} = \langle (1,2,4) \rangle$.

Zu (2). Dank Bahnenlemma wird $|\,{}^{\mathrm{S}_4}(1,2,4)| = \dfrac{|\mathrm{S}_4|}{|\,\mathrm{Stab}_{\mathrm{S}_4}\big((1,2,4)\big)|} = \dfrac{24}{3} = 8$.

Zu (3). In der Konjugationsklasse ${}^{\mathrm{S}_4}(1,2,4)$ liegen alle Elemente f der Form (a,b,c) mit $a,\ b,\ c \in \{1,2,3,4\}$ und mit $|\{a,b,c\}| = 3$.

Die Bedingung $f(1) = 3$ verlangt nun, daß $1 \in \{a,b,c\}$ liegt, da das Element in $\{1,2,3,4\} \smallsetminus \{a,b,c\}$ von f festgelassen wird.

O.E. ist $a = 1$. Dann muß $b = 3$ sein. Folglich wird

$$\{\, f \in {}^{\mathrm{S}_4}(1,2,4) \,:\, f(1) = 3 \,\} \;=\; \{(1,3,2), (1,3,4)\}\ .$$

Aufgabe 5 (2+2+2 Punkte)

Man zeige oder widerlege.

(1) Jede Gruppe G mit $|G| = 45$ besitzt einen Normalteiler der Ordnung 5 und einen Normalteiler der Ordnung 9.

(2) Jede Gruppe G mit $|G| = 45$ ist abelsch.

(3) Jede Gruppe G mit $|G| = 45$ enthält ein Element der Ordnung 9.

Lösung.

Zu (1). Die Aussage ist richtig.

Es ist $|\operatorname{Syl}_5(G)| \equiv_5 1$. Es ist $|\operatorname{Syl}_5(G)|$ ein Teiler von $\frac{45}{5} = 9$. Also ist $|\operatorname{Syl}_5(G)| = 1$. Also ist das einzige Element von $\operatorname{Syl}_5(G)$ ein Normalteiler $N \trianglelefteq G$ der Ordnung $|N| = 5$.

Es ist $|\operatorname{Syl}_5(G)| \equiv_3 1$. Es ist $|\operatorname{Syl}_5(G)|$ ein Teiler von $\frac{45}{9} = 5$. Also ist $|\operatorname{Syl}_3(G)| = 1$. Also ist das einzige Element von $\operatorname{Syl}_3(G)$ ein Normalteiler $M \trianglelefteq G$ der Ordnung $|M| = 9$.

Zu (2). Die Aussage ist richtig.

Wir verwenden die Normalteiler M und N aus (1).

Es ist $|M \cap N| = 1$, da $|M \cap N|$ ein Teiler von $|M| = 9$ und von $|N| = 5$ ist. Also ist $M \cap N = 1$.

Es ist $|M| \cdot |N| = 9 \cdot 5 = 45 = |G|$.

Also ist $G \simeq M \times N$. Es ist $|N|$ prim, also ist N abelsch. Es ist M das Quadrat einer Primzahl, also ist M abelsch. Somit ist $M \times N$ abelsch. Also ist G abelsch.

Zu (3). Die Aussage ist falsch. Z.B. enthält $G := \mathrm{C}_5 \times \mathrm{C}_3 \times \mathrm{C}_3$ kein Element der Ordnung 9.

Denn für jedes Element $(x, y, z) \in \mathrm{C}_5 \times \mathrm{C}_3 \times \mathrm{C}_3$ ist $x^5 = 1$, $y^3 = 1$ und $z^3 = 1$. Folglich ist auch $(x, y, z)^{15} = 1$. Gäbe es ein Element der Ordnung 9 in G, dann würde hieraus folgen, daß 9 ein Teiler von 15 ist, was nicht zutrifft.

Aufgabe 6 (2 Punkte)

Sei $A = \begin{pmatrix} 1 & 3 \\ 5 & 7 \\ 9 & 11 \end{pmatrix} \in \mathbb{Z}^{3\times 2}$.

Man bestimme eine Matrix $D \in \mathbb{Z}^{3\times 2}$ in Elementarteilerform, für welche es $S \in \mathrm{GL}_3(\mathbb{Z})$ und $T \in \mathrm{GL}_2(\mathbb{Z})$ gibt mit $SAT = D$.

Die Matrizen S und T brauchen nicht ausgerechnet zu werden.

Lösung.

Wir formen mit Zeilen und Spaltenoperationen.

$$\begin{pmatrix} 1 & 3 \\ 5 & 7 \\ 9 & 11 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 3 \\ 0 & -8 \\ 0 & -16 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & -8 \\ 0 & -16 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & -8 \\ 0 & 0 \end{pmatrix} =: D$$

Aufgabe 7 (1+2+3+1+1+2 Punkte)

(1) Man bestimme alle irreduziblen Polynome von Grad 2 in $\mathbb{F}_2[X]$.

(2) Man zeige: Es ist $X^5 + X^2 + 1 \in \mathbb{F}_2[X]$ irreduzibel.

(3) Man konstruiere einen Körper $\mathbb{F}_{32}$ mit 32 Elementen.
Man gebe eine $\mathbb{F}_2$-lineare Basis von $\mathbb{F}_{32}$ an.

Sind die Ringe $\mathbb{F}_{32}$ und $\mathbb{Z}/(32)$ zueinander isomorph?

(4) Sei $u \in \mathrm{U}(\mathbb{F}_{32})$ mit $u \neq 1$ gegeben. Man bestimme die Ordnung von u.

Wieso müssen dazu die Potenzen von u nicht berechnet werden?

(5) Sei $y \in \mathbb{F}_{32}$ mit $y \notin \{0, 1\}$ gegeben. Man bestimme $\deg(\mu_{y,\mathbb{F}_2}(X))$.

(6) Sei $\mathrm{Aut}(\mathbb{F}_{32}|\mathbb{F}_2)$ die Gruppe der Automorphismen von $\mathbb{F}_{32}$ über $\mathbb{F}_2$.

Man gebe einen Automorphismus $\varphi \in \mathrm{Aut}(\mathbb{F}_{32}|\mathbb{F}_2)$ an mit $\varphi \neq \mathrm{id}_{\mathbb{F}_{32}}$.

Man bestimme die Ordnung von φ in $\mathrm{Aut}(\mathbb{F}_{32}|\mathbb{F}_2)$.

Lösung.

Zu (1). Da 0 keine Nullstelle sein darf, sollte der Koeffizient von X^0 gleich 1 sein. Da 1 keine Nullstelle sein darf, ist $X^2 + X + 1 \in \mathbb{F}_2[X]$ das einzige irreduzible Polynom von Grad 2.

Zu (2). Es sind weder 0 noch 1 Nullstellen von $X^5 + X^2 + 1$. Also hat dieses Polynom keinen irreduziblen Teiler von Grad 1.

Um zu zeigen, daß es irreduzibel ist, genügt es nun, zu zeigen, daß es keinen irreduziblen Teiler von Grad 2 hat. Dank (1) genügt es zu zeigen, daß es nicht durch $X^2 + X + 1$ teilbar ist. Wir führen hierzu eine Polynomdivision durch.

$$
\begin{array}{lll}
X^5 + X^2 + 1 & = & (X^2 + X + 1) \cdot (X^3 + X^2) + 1 \\
-(X^5 + X^4 + X^3) & & \\
\hline
\quad X^4 + X^3 + X^2 + 1 & & \\
\quad -(X^4 + X^3 + X^2) & & \\
\hline
\qquad\qquad 1 & &
\end{array}
$$

In der Tat ist der Rest ungleich 0.

Zu (3). Sei $\mathbb{F}_{32} := \mathbb{F}_2[X]/(X^5 + X^2 + 1)$.

Sei $\kappa := X + (X^5 + X^2 + 1) \in \mathbb{F}_{32}$. Dann ist $(\kappa^0, \kappa^1, \kappa^2, \kappa^3, \kappa^4)$ eine $\mathbb{F}_2$-lineare Basis von $\mathbb{F}_{32}$. Insbesondere ist in der Tat $|\mathbb{F}_{32}| = 2^5 = 32$.

Es sind die Ringe $\mathbb{F}_{32}$ und $\mathbb{Z}/(32)$ nicht isomorph, da $\mathbb{F}_{32}$ ein Körper ist, $\mathbb{Z}/(32)$ jedoch nicht. In der Tat ist wegen $(2+(32))\cdot(16+(32)) = 0+(32)$ das Element $2+(32) \in (\mathbb{Z}/(32))^\times$ nicht invertierbar.

Zu (4). Es ist $|\mathrm{U}(\mathbb{F}_{32})| = 31$. Also ist die Ordnung von u ein Teiler von 31. Da $u \neq 1$ ist, ist die Ordnung von u ungleich 1. Also hat u die Ordnung 31.

Da 31 prim ist, mußten keine Potenzen von u betrachtet werden, um zu dieser Aussage zu kommen.

Zu (5). Es ist $\mathbb{F}_{32}|\mathbb{F}_2(y)|\mathbb{F}_2$. Da $y \notin \mathbb{F}_2$, ist $\mathbb{F}_2 \neq \mathbb{F}_2(y)$ und also $[\mathbb{F}_2(y) : \mathbb{F}_2] > 1$.

Somit folgt aus

$$5 \;=\; [\mathbb{F}_{32} : \mathbb{F}_2] \;=\; [\mathbb{F}_{32} : \mathbb{F}_2(y)] \cdot [\mathbb{F}_2(y) : \mathbb{F}_2]\ ,$$

daß $[\mathbb{F}_2(y) : \mathbb{F}_2] = 5$ ist.

Somit ist auch $\deg(\mu_{y,\mathbb{F}_2}(X)) = [\mathbb{F}_2(y) : \mathbb{F}_2] = 5$.

Zu (6). Wir schreiben kurz $\mathrm{id} := \mathrm{id}_{\mathbb{F}_{32}}$.

Sei $\varphi := \mathrm{Fr}_{\mathbb{F}_{32}} : \mathbb{F}_{32} \to \mathbb{F}_{32} : x \mapsto x^2$. Es ist $\varphi \in \mathrm{Aut}(\mathbb{F}_{32}|\mathbb{F}_2)$. Da z.B. $\varphi(\kappa) = \kappa^2 \neq \kappa$, ist $\varphi \neq \mathrm{id}$.

Wegen $|\mathrm{U}(\mathbb{F}_{32})| = 31$ ist $x^{31} = 1$ für $x \in \mathrm{U}(\mathbb{F}_{32}) = \mathbb{F}_{32}^\times$. Also ist $\varphi^5(x) = x^{32} = x$ für $x \in \mathbb{F}_{32}$.

Somit ist $\varphi^5 = \mathrm{id}$, aber $\varphi \neq \mathrm{id}$. Also hat φ die Ordnung 5 in $\mathrm{Aut}(\mathbb{F}_{32}|\mathbb{F}_2)$.

Aufgabe 8 (1+3+1+2 Punkte)

(1) Man bestimme $\Phi_1(X) \cdot \Phi_5(X)$ und $\Phi_1(X) \cdot \Phi_5(X) \cdot \Phi_{25}(X)$.

(2) Man bestimme das Kreisteilungspolynom $\Phi_{25}(X)$.

(3) Man bestimme den Körpergrad $[\mathbb{Q}(\zeta_{25}) : \mathbb{Q}]$.

(4) Gibt es einen Zwischenkörper Z mit $\mathbb{Q}(\zeta_{25}) \,|\, Z \,|\, \mathbb{Q}$ und mit $[Z : \mathbb{Q}] = 8$?

Lösung.

Zu (1).

Es ist $\Phi_1(X) \cdot \Phi_5(X) = X^5 - 1$, da 1 und 5 die Teiler von 5 sind, die in $[1, 5]$ liegen.

Es ist $\Phi_1(X) \cdot \Phi_5(X) \cdot \Phi_{25}(X) = X^{25} - 1$, da 1, 5 und 25 die Teiler von 25 sind, die in $[1, 25]$ liegen.

Zu (2). Dank (1) ist $\Phi_{25}(X) = \dfrac{X^{25} - 1}{X^5 - 1}$.
Es ist $(X^{20} + X^{15} + X^{10} + X^5 + X^0) \cdot (X^5 - 1) = X^{25} - 1$ und infolgedessen

$$\Phi_{25}(X) \;=\; X^{20} + X^{15} + X^{10} + X^5 + X^0 \;=\; X^{20} + X^{15} + X^{10} + X^5 + 1\,.$$

Alternativ kann dies mit einer Polynomdivision berechnet werden.

Zu (3). Es ist $[\mathbb{Q}(\zeta_{25}) : \mathbb{Q}] = \deg(\mu_{\zeta_{25},\mathbb{Q}}(X)) = \deg(\Phi_{25}(X)) \overset{(2)}{=} 20$.

Zu (4). Nein, einen solchen Zwischenkörper gibt es nicht.
Annahme, doch. Dann ist

$$20 \overset{(3)}{=} [\mathbb{Q}(\zeta_{25}) : \mathbb{Q}] \;=\; [\mathbb{Q}(\zeta_{25}) : Z] \cdot [Z : \mathbb{Q}] \;=\; [\mathbb{Q}(\zeta_{25}) : Z] \cdot 8\,.$$

Aber 8 ist kein Teiler von 20. Wir haben einen *Widerspruch.*