Algebra I – Klausur № 2

Name: ______________________

Vorname: ______________________

Matrikelnummer: ______________________

Aufgabe:	1	2	3	4	5	6	Σ	Note
Maximale Punktzahl:	10	6	7	6	6	5	40	
Erreichte Punktzahl:								

Ich gestatte die Veröffentlichung meines Klausurergebnisses unter Angabe meiner Matrikelnummer im Internet:

☐ Einverstanden ☐ Nicht Einverstanden ______________________

(**Unterschrift**)

Wichtige Hinweise zur Klausur:

- Sollten Sie sich aus gesundheitlichen Gründen nicht in der Lage fühlen, an der Klausur teilzunehmen, melden Sie sich **noch vor Beginn** bei der Klausuraufsicht.
- Kontrollieren Sie diese Klausur auf Vollständigkeit: Sie sollte genau 13 Seiten haben.
- Tragen Sie Ihren **Namen**, **Vornamen** und Ihre **Matrikelnummer** auf allen Seiten ein.
- Bitte **nicht mit Bleistift oder in Rot schreiben**.
- Bitte die Klammerung der Klausur nicht lösen.
- Die Dauer der Klausur beträgt **120 Minuten**.
- Lösungswege und Lösungen sind in die Klausurvorlage einzutragen. Bei Platzmangel stellt die Klausuraufsicht zusätzliches Papier zur Verfügung.
- Alle Aussagen sind zu beweisen, wenn sie nicht aus der Vorlesung bekannt sind.
- Bitte schreiben Sie in Ihrem eigenen Interesse leserlich. Einen nicht lesbaren Lösungsansatz müssen wir als ungenügend bewerten.
- Während der Klausur sind Kommunikationsgeräte jeder Art (Mobiltelefone, Computer, etc.) auszuschalten und außer Griffreichweite zu verstauen.

Hilfsmittel. Ausschließlich die folgenden Hilfsmittel sind zur Klausur zugelassen:

- Ein nicht programmierbarer Taschenrechner.
- Stifte und Lineal.
- Nahrung und Getränke in angemessenem Umfang.

Remark. You may use a dictionary of your choice and answer in English.

Name: ______________ Vorname: ______________ Matrikelnummer: ______________

Aufgabe 1 (10 Punkte). Zeige oder widerlege:

(a) Für jeden Integritätsbereich R und jedes Ideal $I \subseteq R$ ist R/I wieder ein Integritätsbereich.

(b) Sei G eine endliche Gruppe. Es gibt einen Primfaktor p von $|G|$, so dass G eine normale p-Sylow Untergruppe besitzt.

(c) Das Zentrum einer Gruppe ist ein Normalteiler.

(d) Es gibt einen Isomorphismus von Ringen $\mathbb{Q}[X]/\langle X^2 - 1 \rangle \cong \mathbb{Q} \times \mathbb{Q}$.

(e) Der Faktorring $\mathbb{Z}[i]/\langle 2 \rangle$ ist ein Körper, wobei $i \in \mathbb{C}$ die imaginäre Einheit ist.

Lösung zu Aufgabe 1: Zu Aufgabenteil (a). Nein. Betrachte den Integritätsbereich $\mathbb{Z}$, der Quotient $\mathbb{Z}/4\mathbb{Z}$ ist nicht nullteilerfrei.

Zu Aufgabenteil (b). Nein. Betrachte eine einfache Gruppe, etwa $\mathfrak{A}_n$ für $n \geq 5$. Diese Gruppe hat eine p-Sylow-Untergruppe für jeden Primfaktor p von $|\mathfrak{A}_n|$, aber sie enthält keine einzige normale Untergruppe.

Zu Aufgabenteil (c). Ja. Sei G eine Gruppe und $h \in Z(G)$. Dann ist $ghg^{-1} = gg^{-1}h = h \in Z(G)$ für alle $g \in G$, insbesondere $gZ(G)g^{-1} = Z(G)$.

Zu Aufgabenteil (d): Ja. Es gilt $X^2 - 1 = (X+1)(X-1)$ und da $X+1$ und $X-1$ beide prim sind, sind sie insbesondere teilerfremd. Ihr kleinstes gemeinsames Vielfaches ist damit $X^2 - 1$ und somit ist $\langle X+1 \rangle \cap \langle X-1 \rangle = \langle X^2 - 1 \rangle$. Damit folgt aus dem Chinesischen Restsatz, dass

$$\mathbb{Q}[X]/\langle X^2 - 1 \rangle \cong \mathbb{Q}/\langle X+1 \rangle \times \mathbb{Q}[X]/\langle X-1 \rangle = \mathbb{Q} \times \mathbb{Q}.$$

Zu Aufgabenteil (e). Nein. Es ist $(1+i)^2 = 1 + 2i + i^2 = 2i \in \langle 2 \rangle$, aber $1 + i \notin \langle 2 \rangle$. Demnach ist $\langle 2 \rangle$ kein Primideal, insbesondere nicht maximal, also kann der Quotient kein Körper sein.

Name: ____________ Vorname: ____________ Matrikelnummer: ____________

Lösung zu Aufgabe 1 (Fortsetzung):

Name: ______________ Vorname: ______________ Matrikelnummer: ______________

Aufgabe 2 (6 Punkte). Sei G eine endliche Gruppe, und für $x \in G$ sei $G.x = \{gxg^{-1} \mid g \in G\}$ die Bahn von x bzgl. Konjugation.

(a) Angenommen, es gibt genau eine Bahn $G.x$ mit $|G.x| > 1$. Zeige, dass dann

$$|G| = |Z(G)| + [G : Z_G(x)].$$

Hier bezeichnet $Z(G)$ das Zentrum von G und $Z_G(x)$ den Zentralisator von x in G.

(b) Zeige, dass die Situtation von Aufgabenteil (a) nicht eintreten kann, d.h. es kann nicht genau eine Bahn mit mehr als einem Element enthalten.

Hinweis: Zeige, dass unter den Annahmen von Aufgabenteil (a) stets $|Z_G(x)| = 2$ gilt.

Lösung zu Aufgabe 2:

(a) Wir lassen G auf sich selbst durch Konjugation wirken. Nach der Klassengleichung gilt

$$|G| = |Z(G)| + \sum_{x \in R} |G.x|,$$

wobei R ein Vertretersystem der Bahnen ist, welche mehr als ein Element besitzen. Nach Voraussetzung ist $R = \{x\}$. Da $Z_G(x)$ der Stabilisator von x unter der Konjugationswirkung ist, folgt aus der Bahnformel $|G.x| = [G : Z_G(x)]$ und somit die Aussage.

(b) Angenommen es gibt genau eine Bahn $G.x$ mit mehr als einem Element. Sei $n := |G|$. Nach Voraussetzung ist $Z(G) \neq G$, also ist $Z(G)$ eine echte Untergruppe von G und somit $|Z(G)| \leq \frac{n}{2}$; beachte $|Z(G)|$ ist Teiler der Gruppenordung. Weiterhin ist $Z_G(x)$ eine nicht-triviale Untergruppe von G, da $x \in Z_G(x)$ und x nicht das neutrale Element ist, andernfalls wäre $x \in Z(G)$. Daraus folgt auch $[G : Z_G(x)] \leq \frac{n}{2}$. Nach Teil a) wissen wir aber auch $n = |Z(G)| + [G : Z_G(x)]$, so dass wir folgern können

$$|Z(G)| = [G : Z_G(x)] = \frac{n}{2}.$$

Damit ist $|Z_G(x)| = 2$. Es ist $Z(G) \subsetneq Z_G(x)$ da $x \notin Z(G)$, also ist $|Z(G)| \leq 1$ und da $Z(G)$ das neutrale Element enthält gilt $|Z(G)| = 1$. Es folgt nun $n = 2$, doch damit ist $G = Z(G)$, ein Widerspruch.

Name: ________________ Vorname: ________________ Matrikelnummer: ________________

Lösung zu Aufgabe 2 (Fortsetzung):

Name: ______________ Vorname: ______________ Matrikelnummer: ______________

Aufgabe 3 (7 Punkte). Sei $n \geq 1$, $\mathbb{K}$ ein Körper und $a = (a_1, \ldots, a_n) \in \mathbb{K}^n$. Definiere die Teilmenge

$$M_a := \{f \in \mathbb{K}[X_1, \ldots, X_n] \mid f(a_1, \ldots, a_n) = 0\} \subseteq \mathbb{K}[X_1, \ldots, X_n].$$

(a) Zeige, dass M_a ein maximales Ideal in $\mathbb{K}[X_1, \ldots, X_n]$ ist.

(b) Verwende Induktion nach n um zu zeigen, dass $M_a = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

(c) Betrachte den Fall $n = 1$. Angenommen, für jedes maximale Ideal $M \subseteq \mathbb{K}[X]$ existiert ein $a \in \mathbb{K}$, so dass $M = M_a$. Zeige, dass $\mathbb{K}$ dann algebraisch abgeschlossen ist.

Lösung zu Aufgabe 3: Zu Aufgabenteil (a): Der Auswertungshomomorphismus

$$\begin{aligned} \phi_a \colon \mathbb{K}[X_1, \ldots, X_n] &\longrightarrow \mathbb{K} \\ f &\longmapsto f(a) \end{aligned}$$

erfüllt $\ker(\phi_a) = M_a$ nach Definition. Damit ist $\mathbb{K}[X_1, \ldots, X_n]/M_a \cong \mathbb{K}$ nach den Isomorphiesätzen ein Körper, und somit muss M_a ein maximales Ideal sein.

Wir zeigen Aufgabenteil (b) per Induktion nach n, wobei $n = 1$ aus der Vorlesung bekannt ist. Sei $\tilde{a} := (a_2, \ldots, a_n)$ und betrachte $\phi_{\tilde{a}} \colon \mathbb{K}[X_2, \ldots, X_n] \to \mathbb{K}$, den Auswertungshomomorphismus $\phi_{\tilde{a}}(f) = f(\tilde{a})$. Nach Induktionsvoraussetzung ist $\ker(\phi_{\tilde{a}}) = M_{\tilde{a}} = \langle X_2 - a_2, \ldots, X_n - a_n \rangle$. Betrachte außerdem die Auswertungsabbildung

$$\begin{aligned} \psi \colon \mathbb{K}[X_2, \ldots, X_n][X_1] &\longrightarrow \mathbb{K}[X_2, \ldots, X_n] \\ f &\longmapsto f(a_1). \end{aligned}$$

Es ist $\ker(\psi) = \langle X_1 - a_1 \rangle$. Außerdem $\phi_a = \phi_{\tilde{a}} \circ \psi$ und somit

$$M_a = \ker(\phi_a) = \ker(\phi_{\tilde{a}} \circ \psi) = \psi^{-1}(\ker(\phi_{\tilde{a}})) = \psi^{-1}(\langle X_2 - a_2, \ldots, X_n - a_n \rangle).$$

Für $f \in M_a$ gibt es also gewisse $g_i \in \mathbb{K}[X_2, \ldots, X_n]$ mit $\psi(f) = \sum_{i=2}^n g_i(X_i - a_i)$. Wir führen Polynomdivision von f nach $X_1 - a_1$ durch und erhalten $f = g_1(X_1 - a_1) + r$ für ein "konstantes" Polynom $r \in \mathbb{K}[X_2, \ldots, X_n]$ und ein $g_1 \in \mathbb{K}[X_1, \ldots, X_n]$. Dann ist

$$\begin{aligned} & & r = \psi(r) = \psi(f) &= \sum_{i=2}^n g_i(X_i - a_i), \\ &\Longrightarrow & f = g_1(X_1 - a_1) + r &= \sum_{i=1}^n g_i(X_i - a_i) \in \langle X_1 - a_1, \ldots, X_n - a_n \rangle. \end{aligned}$$

Somit ist $M_a \subseteq \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Die andere Inklusion ist klar.

Zu Aufgabenteil (c). Sei $\overline{\mathbb{K}}$ ein algebraischer Abschluss von $\mathbb{K}$ und $t \in \overline{\mathbb{K}}$. Wir setzen $\mathbb{L} := \mathbb{K}(t)$. Da t algebraisch über $\mathbb{K}$ ist, gibt es ein Polynom $f \in \mathbb{K}[X]$ mit $\mathbb{L} \cong \mathbb{K}[X]/\langle f \rangle$. Wir definieren das Ideal $M := \langle f \rangle$, dann ist M maximal und somit gibt es ein $a \in \mathbb{K}$ mit $M = M_a$. Damit ist $t = \phi_a(X) = a \in \mathbb{K}$. Da t beliebig war, folgt $\mathbb{K} = \overline{\mathbb{K}}$.

Name: ________________ Vorname: _______________ Matrikelnummer: _________________

Lösung zu Aufgabe 3 (Fortsetzung):

Name: ______________ Vorname: ______________ Matrikelnummer: ______________

Aufgabe 4 (6 Punkte). Sei G eine Gruppe der Ordnung 33.

(a) Zeige, dass G jeweils einen Normalteiler der Ordnung 3 und der Ordnung 11 enthält.

(b) Zeige, dass G eine zyklische Gruppe sein muss.

Hinweis: Argumentiere dazu, dass es ein Element der Ordnung 33 geben muss.

Lösung zu Aufgabe 4: Es ist $33 = 3 \cdot 11$ und für die Anzahl s_3 der 3-Sylow Untergruppen von G gilt nach den Sylow-Sätzen $s_3 \mid 11$. Insbesondere ist also $s_3 \leq 11$ und weiterhin besagen die Sylow-Sätze, dass $s_3 \in \{1, 4, 7, 10\}$. Damit muss $s_3 = 1$ gelten. Die Anzahl s_{11} der 11-Sylow Untergruppen muss $s_{11} \mid 3$ erfüllen, also folgt auch $s_{11} = 1$. Demnach sind also diese p-Sylow Untergruppen für $p \in \{3, 11\}$ von G beides Normalteiler und wir haben Aufgabenteil (a) gezeigt.

Zu Aufgabenteil (b). Die Ordnung eines Elements $g \in G$ muss ein Teiler von 33 sein, allerdings hat 33 nur die Teiler 1, 3, 11 und 33. Ein Element der Ordnung 3 erzeugt eine Untergruppe der Ordnung 3, äquivalent für 11. Da es aber jeweils nur eine Untergruppe der Ordnung 3 und 11 gibt, existieren höchstens $3 + 11 = 14 < 33$ Element in G, deren Ordnung kleiner als 33 ist. Damit muss es ein Element der Ordnung 33 in G geben.

Name: ________________ Vorname: _______________ Matrikelnummer: _________________

Lösung zu Aufgabe 4 (Fortsetzung):

Name: ______________ Vorname: ______________ Matrikelnummer: ______________

Aufgabe 5 (6 Punkte).

(a) Man bestimme alle algebraischen Körpererweiterungen von $\mathbb{R}$ und $\mathbb{C}$.

(b) Seien $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ Körpererweiterungen, so dass $\mathbb{L}$ eine algebraische Erweiterung von $\mathbb{K}$ ist und $x \in \mathbb{M}$ transzendent über $\mathbb{K}$. Zeige, das x dann auch transzendent über $\mathbb{L}$ ist.

(c) Sei $\alpha := \sqrt[4]{2}$ die positive vierte reelle Wurzel aus $2 \in \mathbb{Q}$ und $i \in \mathbb{C}$ die imaginäre Einheit. Zeige, dass $\mathbb{K} := \mathbb{Q}(\alpha, i)$ der Zerfällungskörper des Polynoms $X^4 + 2 \in \mathbb{Q}[X]$ ist.

Hinweis: Man stelle sich eine primitive 8-te Einheitswurzel in der komplexen Ebene vor und ermittle, wie sich diese berechnen lässt.

Lösung zu Aufgabe 5:

(a) Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen, also ist $\mathbb{C}$ die einzige algebraische Erweiterung. Es ist $\mathbb{R} \subseteq \mathbb{C}$ und da $\mathbb{C}$ algebraisch abgeschlossen ist, ist jede algebraische Körpererweiterung von $\mathbb{R}$ in $\mathbb{C}$ enthalten. Sei also $\mathbb{R} \subseteq \mathbb{K}$ eine Körpererweiterung. Wenn $\mathbb{R} \neq \mathbb{K}$, so gibt es ein $a + bi \in \mathbb{K}$ mit $b \neq 0$ und daraus folgt sofort $i = b^{-1} \cdot ((a + bi) - a) \in \mathbb{K}$. Damit ist $\mathbb{K} = \mathbb{C}$. Also sind die einzigen algebraischen Körpererweiterungen von $\mathbb{R}$ der Körper $\mathbb{R}$ selbst und $\mathbb{C}$.

(b) Angenommen, x ist nicht transzendent über $\mathbb{L}$. Dann ist $\mathbb{L}(x)$ eine endliche Körpererweiterung von $\mathbb{L}$. Sei $\mu = a_0 + a_1 X + \cdots + X^n \in \mathbb{L}[X]$ das Minimalpolynom von x über $\mathbb{L}$. Damit ist der Körper $\mathbb{L}' := \mathbb{K}(a_0, \ldots, a_{n-1}) \subseteq \mathbb{L}$ eine endliche algebraische Erweiterung von $\mathbb{K}$, so dass x algebraisch über $\mathbb{L}'$ ist. Wir ersetzen $\mathbb{L}$ durch $\mathbb{L}'$ und dürfen nun davon ausgehen, dass die Erweiterung $\mathbb{K} \subseteq \mathbb{L}$ sogar endlich ist.

Damit ist auch $[\mathbb{L}(x) : \mathbb{K}] = [\mathbb{L}(x) : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}] < \infty$ und somit $\mathbb{L}(x)$ eine endliche, somit algebraische Erweiterung von $\mathbb{K}$. Dann ist aber x algebraisch über $\mathbb{K}$.

(c) Sei $\omega \in \mathbb{C}$ eine primitive 8-te Einheitswurzel. Wir stellen fest, dass $\omega\alpha$ eine Nullstelle von $f := X^4 + 2$ ist, denn ω^4 ist eine primitive zweite Einheitswurzel, also $\omega^4 = -1$. Wir erhalten nun die weiteren Nullstellen des Polynoms durch multiplikation mit der primitiven vierten Einheitswurzel i:

$$\omega\alpha \qquad i\omega\alpha \qquad -\omega\alpha \qquad -i\omega\alpha$$

Im Zerfällungskörper von f sind also die Elemente $i = \frac{i\omega\alpha}{\omega\alpha}$ und $\omega\alpha$ sicherlich enthalten. Es bleibt zu zeigen, dass $\mathbb{Q}(i, \omega\alpha) = \mathbb{Q}(i, \alpha)$ ist. Dies folgt jedoch, da $\omega = \frac{1}{\sqrt{2}}(1 + i)$, also $\alpha^2\omega = 1 + i$. Damit ist

$$\alpha = \frac{1+i}{\alpha\omega} \in \mathbb{Q}(i, \alpha\omega) \qquad \alpha\omega = \frac{1+i}{\alpha} \in \mathbb{Q}(i, \alpha).$$

Andererseits sind auch alle Nullstellen von f in $\mathbb{Q}(\omega\alpha, i)$ enthalten, somit muss dies der Zerfällungskörper von f sein.

Name: ____________ Vorname: ____________ Matrikelnummer: ____________

Lösung zu Aufgabe 5 (Fortsetzung):

Name: ________________ Vorname: _______________ Matrikelnummer: __________________

Aufgabe 6 (5 Punkte). Betrachte den Ring $R := \mathbb{Z}/12\mathbb{Z}$.

(a) Gebe ohne Mehrfachnennung alle Ideale von R an.

(b) Zeige, dass R genau zwei maximale Ideale hat und geben Sie diese an.

(c) Gebe alle Körper an, die von der Form R/M für ein maximales Ideal $M \subseteq R$ sind.

(d) Welcher der Körper aus Aufgabenteil (c) lässt sich in $\mathbb{C}$ einbetten?

Lösung zu Aufgabe 6:

(a) Jedes Ideal in R ist von einem Element erzeugt, da $\mathbb{Z}$ ein Hauptidealbereich ist. Die Ideale von R sind somit $0R$, $R = 5R = 7R = 11R$, $2R = 10R$, $3R = 9R$, $4R = 8R$ und $6R$. Zusammenfassend haben wir die Erzeuger

$$0 \qquad 1 \qquad 2 \qquad 3 \qquad 4 \qquad 6$$

welche gerade den Teilern von 12 entsprechen.

(b) Die Ideale $2R$ und $3R$ sind maximal, da $4R \subseteq 2R$ und $6R \subseteq 3R$.

(c) Wir erhalten die Körper $R/2R = \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ und $R/3R = \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$.

(d) Keiner dieser Körper lässt sich in $\mathbb{C}$ einbetten, da die Charakteristik beider Körper ungleich 0 ist.

Name: ________________ Vorname: ________________ Matrikelnummer: ________________

Lösung zu Aufgabe 6 (Fortsetzung):