Prof. Dr. Martin Henk

Algebra I – Klausur № 1

Name: _____

Vorname: _____

Matrikelnummer: _____

Aufgabe:	1	2	3	4	5	6	Σ	Note
Maximale Punktzahl:	10	5	6	6	6	7	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 12 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 (Multiple Choice, 10 Punkte). Es ist bei jeder Aussage mit einem Kreuz zu markieren, ob die Aussage richtig oder falsch ist.

- Keine Markierung liefert **0 Punkte**.
- Eine falsche Markierung liefert $-$**1 Punkt**.
- Eine richtige Markierung liefert **1 Punkt**.

Insgesamt erhalten Sie jedoch für diese Aufgabe mindestens 0 Punkte.

Jede endliche Körpererweiterung ist algebraisch. ☐ **richtig** ☐ **falsch**

Jede Gruppe ist auflösbar. ☐ **richtig** ☐ **falsch**

Euklidische Ringe sind Hauptidealbereiche. ☐ **richtig** ☐ **falsch**

Eine Gruppe $G = (G, \cdot)$ mit neutralem Element 1 ist genau dann abelsch, wenn

$Z(G) \trianglelefteq G$. ☐ **richtig** ☐ **falsch**

$[G, G] = \{1\}$. ☐ **richtig** ☐ **falsch**

Sei $\mathfrak{S}_n$ die symmetrische Gruppe.

Jedes $\sigma \in \mathfrak{S}_n$ lässt sich als Verknüpfung von Transpositionen schreiben. ☐ **richtig** ☐ **falsch**

Jedes $\sigma \in \mathfrak{S}_n$ lässt sich als Verknüpfung von Dreierzykeln schreiben. ☐ **richtig** ☐ **falsch**

Wir betrachten den Ring $R \coloneqq \mathbb{Z}/4\mathbb{Z}$. Dann gilt:

Die Gruppe $(R, +)$ ist zyklisch. ☐ **richtig** ☐ **falsch**

R ist ein Körper. ☐ **richtig** ☐ **falsch**

R ist ein lokaler Ring. ☐ **richtig** ☐ **falsch**

Antworten in dieser Reihenfolge: richtig, falsch, richtig, falsch, richtig, richtig, falsch, richtig, falsch, richtig.

Name: _____ Vorname: _____ Matrikelnummer: _____

Aufgabe 2 (5 Punkte). Seien $p, q \in \mathbb{N}$ Primzahlen mit $p < q$ und G eine Gruppe mit $|G| = p \cdot q$ Elementen. Zeige, dass es einen surjektiven Gruppenhomomorphismus $\pi\colon G \to \mathbb{Z}_p$ gibt, wobei $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ die zyklische Gruppe der Ordnung p bezeichnet.

Lösung zu Aufgabe 2:
Nach Vorlesung besitzt G einen Normalteiler N der Ordnung q, die eindeutige q-Sylow-Untergruppe von G. Damit ist die kanonische Projektion $\pi\colon G \to G/N =: H$ ein surjektiver Gruppenhomomorphismus und nach dem Satz von Lagrange gilt

$$|H| = \frac{|G|}{|N|} = \frac{pq}{q} = p.$$

Wir zeigen, dass H zyklisch ist: Wähle ein beliebiges Element $h \in H$, welches nicht das Neutralelement ist. Da die Ordnung von h ein Teiler der Gruppenordnung p ist und p eine Primzahl, muss h die Ordnung p haben. Damit ist $H = \langle h \rangle \cong \mathbb{Z}_p$.

Nur zur Vollständigkeit (dies war für die Lösung in der Klausur nicht erforderlich) hier der Beweis der Aussage, die aus der Vorlesung bekannt ist: Sei s_q die Anzahl der q-Sylow-Untergruppen von G. Dann ist nach den Sylow Sätzen $s_q \mid p$, also $s_q = 1$ oder $s_q = p$, aber außerdem gilt $s_q \equiv 1 \pmod{q}$ und $p < q$ impliziert somit $s_q = 1$. Damit gibt es eine eindeutige q-Sylow-Untergruppe von G, welche ebenfalls nach den Sylow-Sätzen ein Normalteiler ist.

Name: _____ Vorname: _____ Matrikelnummer: _____

Lösung zu Aufgabe 2 (Fortsetzung):

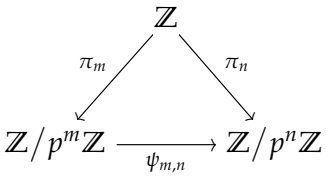
Name: _____ Vorname: _____ Matrikelnummer: _____

Aufgabe 3 (6 Punkte). Sei $p \in \mathbb{Z}$ eine Primzahl und $n, m \in \mathbb{N}$, $m \geq n \geq 1$. Bezeichne mit

$$\pi_m \colon \mathbb{Z} \longrightarrow \mathbb{Z}/p^m\mathbb{Z} \qquad \text{und} \qquad \pi_n \colon \mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

die kanonischen Projektionen. Zeige:

(a) Es existiert ein Ringhomomorphismus $\psi_{m,n} \colon \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ mit $\psi_{m,n} \circ \pi_m = \pi_n$. Mit anderen Worten, das Diagramm



kommutiert.

(b) Die Einschränkung von $\psi_{m,n}$ auf die Einheitengruppe von $\mathbb{Z}/p^m\mathbb{Z}$ liefert einen surjektiven Gruppenhomomorphismus $\eta_{m,n} \colon (\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times$.

(c) Der Kern $K \coloneqq \ker(\eta_{2,1})$ ist zyklisch. Gebe auch einen Erzeuger für K an.

Hinweis: Sie dürfen zum Beweis jedes Aufgabenteils die Aussagen der vorherigen Aufgabenteile verwenden, ohne diese bearbeitet zu haben.

Lösung zu Aufgabe 3:
Zu Aufgabenteil (a). Es ist $\ker(\pi_n) = p^n\mathbb{Z} \supseteq p^n(p^{m-n}\mathbb{Z}) = p^m\mathbb{Z}$, also folgt die Existenz von $\psi_{m,n}$ aus der universellen Eigenschaft des Quotienten.

Zu Aufgabenteil (b): Die Abbildung $\psi_{m,n}$ ist surjektiv, da π_n surjektiv ist. Es gilt zu zeigen, dass es zu jeder Einheit $u \in \mathbb{Z}/p^n\mathbb{Z}$ eine Einheit $v \in \mathbb{Z}/p^m\mathbb{Z}$ gibt mit $\psi_{m,n}(v) = u$. Sei $u = \pi_n(x)$, dann ist x teilerfremd zu p^n, also ist x teilefremd zu p und somit teilerfremd zu p^m. Damit ist $v \coloneqq \pi_m(x)$ eine Einheit, und wir haben $\psi_{m,n}(v) = \psi_{m,n}(\pi_m(x)) = \pi_n(x) = u$ wie gewünscht.

Zu Aufgabenteil (c): Sei $K \coloneqq \ker(\psi_{2,1})$ und bezeichne mit φ die Eulersche Phi-Funktion. Aus der Vorlesung ist bekannt, dass $\varphi(p^2) = p(p-1)$ und $\varphi(p) = p-1$. Damit ist

$$\begin{aligned} p(p-1) = \varphi(p^2) &= \left|(\mathbb{Z}/p^2\mathbb{Z})^\times\right| = |K| \cdot |\mathrm{im}(\eta_{2,1})| = |K| \cdot \left|(\mathbb{Z}/p\mathbb{Z})^\times\right| \\ &= |K| \cdot \varphi(p) = |K| \cdot (p-1), \end{aligned}$$

also ist $|K| = p$ und somit ist K zyklisch. Es ist

$$\psi_{m,n}(\pi_2(p+1)) = \pi_1(p+1) = 1,$$

also ist $\pi_2(p+1) \in K$ ein Erzeuger der zyklischen Gruppe K.

Name: _____ Vorname: _____ Matrikelnummer: _____

Lösung zu Aufgabe 3 (Fortsetzung):

Name: _____ Vorname: _____ Matrikelnummer: _____

Aufgabe 4 (6 Punkte). Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Definiere

$$I[X] := \left\{ \sum_{i=0}^{n} a_i X^i \;\middle|\; a_i \in I \text{ for } 0 \leq i \leq n \right\} \subseteq R[X],$$

die Menge aller Polynome mit Koeffizienten in I. Zeige:

(a) Die Menge $I[X]$ ist ein Ideal in $R[X]$.

(b) Es ist $R[X]/I[X] \cong (R/I)[X]$.

Lösung zu Aufgabe 4: Zu Aufgabenteil (a): Seien $f \in I[X]$ und $g \in R[X]$. Schreibe

$$f = \sum_{i=0}^{n} f_i X^i, \qquad\qquad g = \sum_{j=0}^{m} g_j X^j.$$

Wir dürfen $n = m$ annehmen und sonst mit Nullkoeffizienten ausgleichen. Falls $g \in I[X]$, so ist $f + g = \sum_{i=0}^{n} (f_i + g_i) X^i$ und für $0 \leq i \leq n$ gilt $f_i + g_i \in I$, da I ein Ideal ist.
Es ist $g \cdot f = \sum_{k=0}^{2n} \left(\sum_{i=0}^{k} f_i g_{k-i} \right) X^k$. Sei $0 \leq k \leq 2n$ beliebig. Wir zeigen, dass $\sum_{i=0}^{k} f_i g_{k-i} \in I$. Dazu genügt es zu zeigen, dass für alle $0 \leq i \leq k$ gilt: $f_i g_{k-i} \in I$. Da $f_i \in I$ und $g_{k-i} \in R$ folgt dies aus der Tatsache, dass I ein Ideal ist.

Zu Aufgabenteil (b). Betrachte die kanonische Projektion $\pi \colon R \to R/I$. Diese liefert einen Ringhomomorphismus

$$\begin{aligned} \bar{\pi} \colon R[X] &\longrightarrow (R/I)[X] \\ \sum_{i=0}^{n} a_i X^i &\longmapsto \sum_{i=0}^{n} \pi(a_i) X^i. \end{aligned}$$

Es genügt, nach universeller Eigenschaft des Quotienten, zu zeigen, dass $\ker(\bar{\pi}) = I[X]$. Es ist $\sum_{i=0}^{n} a_i X^i \in \ker(\bar{\pi})$ genau dann, wenn $\sum_{i=0}^{n} \pi(a_i) X^i = 0$. Dies ist der Fall genau dann, wenn $\pi(a_i) = 0$ für alle $0 \leq i \leq n$ ist. Dies wiederum ist genau dann der Fall, wenn $a_i \in \ker(\pi) = I$ für alle $0 \leq i \leq n$ ist. Dies zeigt, dass $\ker(\bar{\pi}) = I[X]$.

Name: _____ Vorname: _____ Matrikelnummer: _____

Lösung zu Aufgabe 4 (Fortsetzung):

Name: _____ Vorname: _____ Matrikelnummer: _____

Aufgabe 5 (6 Punkte). Sei $\mathbb{L} \supseteq \mathbb{K}$ eine Körpererweiterung. Man zeige:

(a) Ist $[\mathbb{L} : \mathbb{K}] = p$ eine Primzahl, dann gibt es ein $\xi \in \mathbb{L}$ mit $\mathbb{L} = \mathbb{K}(\xi)$.

(b) Seien $\alpha, \beta \in \mathbb{L}$ algebraisch über $\mathbb{K}$. Dann gilt

$$[\mathbb{K}(\alpha, \beta) : \mathbb{K}] \leq [\mathbb{K}(\alpha) : \mathbb{K}] \cdot [\mathbb{K}(\beta) : \mathbb{K}].$$

(c) $\mathbb{L}$ über $\mathbb{K}$ ist genau dann algebraisch, wenn jeder Ring R mit $\mathbb{K} \subseteq R \subseteq \mathbb{L}$ ein Körper ist.

(d) Ist $\mathbb{L}$ der Zerfällungskörper eines Polynoms $f \in \mathbb{K}[X]$ vom Grad $d = \deg(f)$, dann gilt $[\mathbb{L} : \mathbb{K}] \leq d!$.

Lösung zu Aufgabe 5:
Zu Aufgabenteil (a): Für ein beliebiges $\xi \in \mathbb{L} \setminus \mathbb{K}$ ist $\mathbb{K}(\xi)$ ein Zwischenkörper von $\mathbb{K} \subseteq \mathbb{L}$, welcher ungleich $\mathbb{K}$ ist. Weiterhin ist $p = [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(\xi)] \cdot [\mathbb{K}(\xi) : \mathbb{K}]$. Da p eine Primzahl ist und $[\mathbb{K}(\xi) : \mathbb{K}] \neq 1$ folgt $[\mathbb{L} : \mathbb{K}(\xi)] = 1$, also $\mathbb{L} = \mathbb{K}(\xi)$.

Zu Aufgabenteil (b): Wir wissen

$$[\mathbb{K}(\alpha, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta) : \mathbb{K}(\beta)] \cdot [\mathbb{K}(\beta) : \mathbb{K}].$$

Sei nun $\mu \in \mathbb{K}[X]$ das Minimalpolynom von α über $\mathbb{K}$. Dann ist auch $\mu \in \mathbb{K}(\beta)[X]$ ein Polynom, welches α als Nullstelle hat und somit ist das Minimalpolynom $\tilde{\mu}$ von α über $\mathbb{K}(\beta)$ ein Teiler von μ, insgesamt also $[\mathbb{K}(\alpha, \beta) : \mathbb{K}(\beta)] = \deg(\tilde{\mu}) \leq \deg(\mu) = [\mathbb{K}(\alpha) : \mathbb{K}]$.

Zu Aufgabenteil (c): Sei zunächst $\mathbb{K} \subseteq \mathbb{L}$ eine algebraische Körpererweiterung und R ein Ring mit $\mathbb{K} \subseteq R \subseteq \mathbb{L}$. Sei $a \in R \setminus \{0\}$ beliebig. Wir zeigen, dass $a^{-1} \in R$. Sei $\mu \in \mathbb{K}[X]$ das Minimalpolynom von a über $\mathbb{K}$. Dann ist $\mu(a) = 0$ und $\mu(0) \neq 0$. Sei $\nu \in \mathbb{K}[X]$ das Polynom mit $\mu - \mu(0) = \nu \cdot X$. Dann ist

$$\nu(a) \cdot a = \mu(a) - \mu(0) = -\mu(0),$$

insgesamt also $a^{-1} = -\mu(0)^{-1} \cdot \nu(a) \in \mathbb{K}[a] \subseteq R$. Andererseits angenommen, jeder Zwischenring der Körpererweiterung $\mathbb{K} \subseteq \mathbb{L}$ ist ein Körper. Sei $a \in \mathbb{L}$ beliebig – es genügt zu zeigen, dass a algebraisch über $\mathbb{K}$ ist. Nach Voraussetzung ist der Ring $R = \mathbb{K}[a]$ ein Körper, also ist $a^{-1} \in R$. Dann gibt es ein Polynom $\nu \in \mathbb{K}[X]$ mit $a^{-1} = \nu(a)$, somit ist $\mu := X \cdot \nu - 1 \in \mathbb{K}[X]$ ein Polynom mit $\mu(a) = a \cdot \nu(a) - 1 = 0$.

Zu Aufgabenteil (d): Wir nehmen f ohne Einschränkung als normiert an. Über einem algebraischen Abschluss $\overline{\mathbb{K}}$ von $\mathbb{K}$ zerfällt f vollständig in Linearfaktoren, $f = \prod_{i=1}^{d}(X - a_i)$ mit $a_i \in \overline{\mathbb{K}}$. Sei $f_i := \prod_{k=i+1}^{d}(X - a_k)$. Setze $\mathbb{K}_0 := \mathbb{K}$ und rekursiv $\mathbb{K}_{i+1} := \mathbb{K}_i(a_{i+1})$. Dann ist $\mathbb{L} = \mathbb{K}(a_1, \ldots, a_d) = \mathbb{K}_d$ der Zerfällungskörper von f. Wir haben jeweils $f_i \in \mathbb{K}_i[X]$ und $f_i(a_i) = 0$, somit folgt $[\mathbb{K}_{i+1} : \mathbb{K}_i] \leq \deg(f_i) = (d - i)$. Somit ist

$$[\mathbb{L} : \mathbb{K}] = \prod_{i=0}^{d-1}[\mathbb{K}_{i+1} : \mathbb{K}_i] \leq \prod_{i=0}^{d-1}(d - i) = \prod_{i=1}^{d} i = d!.$$

Name: _____ Vorname: _____ Matrikelnummer: _____

Lösung zu Aufgabe 5 (Fortsetzung):

Name: _____ Vorname: _____ Matrikelnummer: _____

Aufgabe 6 (7 Punkte). Sei R ein Integritätsbereich mit unendlich vielen Elementen. Sei weiterhin $f \in R[X_1, \ldots, X_n]$ ein Polynom, so dass für alle $(a_1, \ldots, a_n) \in R^n$ die Auswertung $f(a_1, \ldots, a_n) = 0$ ist. Zeige dann, dass $f = 0$ ist.

Hinweis: Verwende Induktion nach n.

Lösung zu Aufgabe 6:
Verwende Induktion nach n. Der Fall $n = 1$ bedeutet, dass ein Polynom in einer einzelnen Variablen $f \in R[X]$ unendlich viele Nullstellen hat. Da R ein Integritätsbereich ist, muss f das Nullpolynom sein.

Im Fall $n > 1$ fassen wir $f \in R[X_1, \ldots, X_{n-1}][X_n]$ als Polynom in der Variablen X_n über dem Polynomring in $n-1$ Variablen auf und schreiben $f = \sum_{k=0}^{d} f_k X_n^k$ für gewisse $f_i \in R[X_1, \ldots, X_{n-1}]$. Um zu zeigen, dass f das Nullpolynom ist, genügt es zu zeigen, dass alle f_k Nullpolynome sind. Dazu wenden wir die Induktionsvoraussetzung auf jedes f_k an: Wähle $(a_1, \ldots, a_{n-1}) \in R^{n-1}$ beliebig und setze $c_k \coloneqq f_k(a_1, \ldots, a_{n-1})$. Es genügt zu zeigen, dass $c_k = 0$ für alle $0 \leq k \leq d$.

Es ist $g(X_n) \coloneqq f(a_1, \ldots, a_{n-1}, X_n) = \sum_{k=0}^{d} c_k X_n^k \in R[X_n]$, ein univariates Polynom, welches für alle $a_n \in R$ die Gleichung $g(a_n) = f(a_1, \ldots, a_n) = 0$ erfüllt, also ist g das Nullpolynom nach Fall $n = 1$. Damit sind aber alle $c_k = 0$.

Name: _____ Vorname: _____ Matrikelnummer: _____

Lösung zu Aufgabe 6 (Fortsetzung):