Algebra, Prüfung am 28.4.2016, Winkler

Name, Matrikelnummer (bitte ausfüllen):

Die **mündlichen Prüfungen** werden möglichst bald nach Korrektur der schriftlichen stattfinden. Zwecks persönlicher Terminvereinbarung finden Sie sich bitte unmittelbar nach Ende der schriftlichen Prüfung im Bereich vor dem Eingang zu diesem Hörsaal ein.

Hinweise bevor Sie beginnen:
Die einzelnen Teilfragen haben ungefähr gleiches Gewicht.
Ihre Arbeitszeit beträgt 100 Minuten.
Vergessen Sie nicht auf die Rückseite der Angabe.

1. Wir betrachten die Varietät $\mathcal{A}$ aller abelschen Gruppen. Bekanntlich lässt sich jedes $A \in \mathcal{A}$ auch als unitärer $\mathbb{Z}$-Modul auffassen, indem man, so wie das generell bei additiver Schreibweise üblich ist, ka für $k \in \mathbb{Z}$ und $a \in A \in \mathcal{A}$ als k-fache additive Potenz von a interpretiert.

   Die Varietät $\mathcal{A}$ enthält als Untervarietäten alle $\mathcal{A}_n$, die entstehen, wenn man zu den Gesetzen, die in allen abelschen Gruppen gelten, auch noch das Gesetz $na = 0$, $n \in \mathbb{N}$, hinzufügt. Eine prominente Rolle spielen in dieser Aufgabe außerdem die kommutativen Restklassenringe $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ mit Einselement.

   (a) Für welche Paare $(n_1, n_2) \in \mathbb{N}^2$ gilt $\mathcal{A}_{n_1} \subseteq \mathcal{A}_{n_2}$?

   (b) Geben Sie ein Beispiel für $n_1, n_2 \in \mathbb{N}$ und $A \in \mathcal{A}_{n_2} \setminus \mathcal{A}_{n_1}$ an.

   (c) Gegeben sei $m \in \mathbb{N}$. Für welche $n \in \mathbb{N}$ gibt es zu jedem $A \in \mathcal{A}_n$ eine Abbildung $\cdot : \mathbb{Z}_m \times A \to A$ derart, dass A bezüglich $\cdot$ ein unitärer $\mathbb{Z}_m$-Modul ist?

   (d) Für $m = n = 3$ gibt es stets eine Abbildung $\cdot$ wie in (c). Gibt es zu jedem $A \in \mathcal{A}_3$ genau ein solches $\cdot$ oder in manchen Fällen auch mehrere? Im ersten Fall ist dieses eindeutige $\cdot$ anzugeben, im zweiten Fall zu einem geeigneten $A \in \mathcal{A}_3$ zwei verschiedene Abbildungen $\cdot_1$ und $\cdot_2$ mit der geforderten Eigenschaft.

   (e) Für welche Paare (m, n) ist jedes $A \in \mathcal{A}_n$ ein Vektorraum über $\mathbb{Z}_m$? (In diesem Fall sind die Gruppenhomomorphismen genau die linearen Abbildungen.)

   (f) Sei $\mathcal{V}$ irgendeine Varietät, $F \in \mathcal{V}$ und X eine Teilmenge (der Trägermenge) von F. Was bedeutet es definitionsgemäß, dass F in $\mathcal{V}$ frei über X ist?

   (g) Aus der Linearen Algebra ist bekannt, dass jeder Vektorraum eine Basis hat. Zeigen Sie damit und mit einem weiteren wohlbekannten Satz aus der Linearen Algebra, dass jedes $F \in \mathcal{A}_3$ frei über einer geeigneten Teilmenge $X \subseteq A$ ist.

   (h) Sei $n \in \mathbb{N}$ und $A, B \in \mathcal{A}_n$. Weil $\mathcal{A}_n$ eine Varietät ist, gibt es ein $A \coprod B \in \mathcal{A}_n$, das zusammen mit Homomorphismen (in diesem Fall isomorphe Einbettungen) $\iota_A : A \to A \coprod B$ und $\iota_B : B \to A \coprod B$ ein Koprodukt von A und B in $\mathcal{A}_n$ bildet. Beschreiben Sie $A \coprod B$, ι_A und ι_B.

2. Ist K ein kommutativer Ring mit Einselement (später werden wir uns auf den Fall eines Körpers beschränken), so bilden bekanntlich die formalen Potenzreihen über R wieder einen kommutativen Ring $R := K[[x]]$ mit Einselement. Die Elemente $r \in R$ lassen sich auffassen als Folgen $r = (a_n)_{n\in\mathbb{N}}$ mit $a_n \in R$, die man gern auch als formale Ausdrücke $r = \sum_{n=0}^{\infty} a_n x^n$ anschreibt. Die Addition erfolgt gliedweise, die konstante Folge mit $a_n = 0$ für alle $n \in \mathbb{N}$ ist das Nullelement in R, und die additiven Inversen werden ebenfalls gliedweise gebildet. Die Multiplikation in R ist durch das Cauchyprodukt gegeben, bezüglich dessen die Folge $(1, 0, 0, \ldots)$ ($a_0 = 1$ und $a_n = 0$ für alle $n \geq 1$) Einselement ist.

   Wir unterscheiden die Teilmengen $R^+ := R \setminus \{0\}$ und R^*, die Menge (sogar Gruppe) der (multiplikativen) Einheiten in R. Für $r = (a_n)_{n\in\mathbb{N}} \in R^+$ sei n_0 das kleinste n mit $a_n \neq 0$. Dann heißt n_0 auch die Ordnung von r, und wir schreiben $n_0 = o(r)$. Außerdem vereinbaren wir $o(0) := \infty$ (mit den üblichen Regeln für ∞: $n < \infty$ und $\infty + n = n + \infty = \infty + \infty = \infty$ für alle $n \in \mathbb{N}$). Dann ist $o : R \mapsto \mathbb{N} \cup \{\infty\}$ auf ganz R definiert. Offenbar gilt (diese Aussagen dürfen in der Folge verwendet werden):

   - $o(r + s) \geq \min\{o(r), o(s)\}$
   - $o(rs) \geq o(r) + o(s)$
   - $o(rs) = o(r) + o(s)$, falls K sogar ein Integritätsbereich ist.

   Außerdem seien die Mengen I_n für alle $n \in \mathbb{N}$ definiert durch

   $$I_n := \{r \in R : \ o(r) \geq n\}.$$

   Für die nun folgenden Aufgaben sei K ein Körper.

   (a) Ist $e = (a_n)_{n\in\mathbb{N}} \in R^*$, so gibt es ein $e' \in R$ mit $ee' = 1$. Es gilt $o(e) + o(e') = o(ee') = o(1) = 0$, was wegen $o(e), o(e') \geq 0$ nur für $o(e) = 0$ möglich ist. Zeigen Sie, dass umgekehrt jedes $e = (a_n)_{n\in\mathbb{N}} \in R$ mit $o(e) = 0$ (d.h. mit $a_0 \neq 0$) eine Einheit ist. Tun sie das, indem Sie für das gesuchte Inverse $e' = (b_n)_{n\in\mathbb{N}}$ mit $ee' = 1$ das erste Glied b_0 sowie eine Rekursionsformel für alle b_n mit $n \geq 1$ angeben.

   Damit ist bewiesen und darf in der Folge verwendet werden:
   $R^* = \{r = (a_n)_{n\in\mathbb{N}} \in R : \ a_0 \neq 0\} = \{r \in R : o(r) = 0\}$

   (b) Gilt für $r, s \in R$ die Teilbarkeitsrelation $r|s$, also $s = rq$ mit $q \in R$, so folgt $o(r) \leq o(r) + o(q) = o(rq) = o(s)$. Zeigen Sie umgekehrt: Aus $o(r) \leq o(s)$ folgt $r|s$. Hinweis: Für $r \neq 0$ ist in Potenzreihenschreibweise $r = x^n e$ mit $n = o(r)$ und $e \in R^*$ sowie $s = x^n s'$ mit einem geeigneten $s' \in R$.

   Beachtet man noch die entsprechenden trivialen Beziehungen für $r = 0$ oder $s = 0$, so ist damit bewiesen, dass für $r, s \in R$ die Teilbarkeitsrelation $r|s$ genau dann gilt, wenn $o(r) \leq o(s)$.

   (c) Zeigen Sie, dass die formale Potenzreihe x (entspricht der Folge $(0, 1, 0, 0, \ldots)$, d.h. $a_1 = 1$ und $a_n = 0$ für alle $n \neq 1$) ein Primelement von R ist. (Hinweis: Verwenden Sie (b).)

   (d) Zeigen Sie, dass R ein faktorieller Ring ist. (Hinweis: Verwenden Sie (a) und (c).)

   (e) Begründen Sie, warum alle I_n, $n \in \mathbb{N}$, Ideale von R sind.

   (f) Sei I ein Ideal in R mit $I \neq \{0\}$ und $n = \min\{o(r) : \ r \in I \setminus \{0\}\}$. Zeigen Sie, dass dann $I = I_n$ gilt. (Hinweis: Verwenden Sie (b).)

   (g) Ist R ein Hauptidealring? Begründen Sie Ihre Antwort, möglichst unter Zuhilfenahme vorangegangener Aufgabenteile.

   (h) Ist R sogar ein euklidischer Ring? Wenn ja, geben Sie eine euklidische Bewertung an; wenn nein, begründen Sie Ihre Antwort.