Algebra, Prüfung am 25.1.2019, Winkler

Name, Matrikelnummer (bitte gleich ausfüllen):

Terminvereinbarung für die mündliche Prüfung persönlich im Anschluss an die schriftliche unmittelbar vor dem Hörsaal.

Hinweise bevor Sie beginnen:
Die einzelnen Teilfragen haben ungefähr gleiches Gewicht.
Verwenden Sie für jede der beiden Aufgaben ein eigenes Blatt.
Bei Bedarf erhalten Sie zusätzliche Blätter.
Ihre Arbeitszeit beträgt 100 Minuten.
Vergessen Sie nicht auf die Rückseite der Angabe.

1. In dieser Aufgabe geht es um Körper K_n mit n Elementen, wobei $n = 2^k$ mit positivem $k \in \mathbb{N}$. Dabei spielen Polynome über $K_2 = \{0, 1\}$ (aufgefasst als zweielementiger Restklassenkörper) eine wichtige Rolle.

   (a) Geben Sie die Operationstafel für die Addition auf K_4 an. Bezeichnen Sie dabei Null- und Einselement wie üblich mit 0 und 1, die anderen beiden Elemente mit a und b.

   (b) Wie (a), nur mit der Multiplikation statt der Addition.

   (c) Sei $K_{16} = K_2(\alpha)$. Welche multiplikativen Ordnungen sind für α möglich?

   (d) Wie viele α wie in (c) gibt es?

   (e) Angenommen ein α wie in (c) ist gegeben. Wie lassen sich aus diesem α mit Hilfe der Körperoperationen sämtliche Elemente von K_{16} eindeutig darstellen?

   (f) Geben Sie für die Grade $n = 0, 1, 2, 3$ sämtliche Polynome vom Grad n über K_2 an, für $n \geq 1$ samt Zerlegung in irreduzible Faktoren.

   (g) Bestimmen Sie zwei Tripel $(a_2, a_1, a_0) \neq (b_2, b_1, b_0) \in K_2^3$, für die es ein $\alpha \in K_8$ gibt mit $K_8 = K_2(\alpha)$ und $\alpha^3 = \sum_{k=0}^{2} a_k \alpha^k$ oder $\alpha^3 = \sum_{k=0}^{2} b_k \alpha^k$.

   (h) Geben Sie ein Polynom vom Grad 4 über K_2 an, das reduzibel ist, aber keine Nullstelle in K_2 hat.

2. In dieser Aufgabe geht es allgemein um Gruppen G, Endomorphismen etc. Speziell tritt die zyklische Gruppe $C_{100} := \mathbb{Z}/100\mathbb{Z}$ der Ordnung 100 aus. Als Trägermenge fungiere in üblicher Weise die Menge $\{k + 100\mathbb{Z} : \ k \in \mathbb{N}, 0 \leq k < 100\}$ aller Restklassen modulo 100. Da C_{100} kommutativ ist, empfiehlt sich additive Notation.

   (a) Definieren Sie, was ein Homomorphismus φ zwischen zwei Gruppen G und H ist. Wann heißt φ sogar Endo-, wann Automorphismus?

   (b) Die Menge $\mathrm{End}(G)$ aller Endomorphismen einer abelschen Gruppe G bilden, wenn man die fünf fundamentalen Operationen geeignet definiert, eine Algebra vom Typ $(2, 0, 1, 2, 0)$, die sogar ein Ring mit Einselement ist. Dieser Ring sei kurz auch mit R bezeichnet, die Operationen mit $+_R, 0_R, -_R, \cdot_R, 1_R$. Wie lautet eine geeignete Definition dieser Operationen?

   (c) Was versteht man unter einem Erzeugendensystem E einer Gruppe G? (Sie dürfen als Definition eine Charakterisierung verwenden, die Ihnen die Arbeit in Teilaufgabe (d) erleichtert.)

   (d) Begründen Sie: Seien $E \subseteq G$ ein Erzeugendensystem der Gruppe G und φ_1 und φ_2 Homomorphismen von G nach H, die auf E übereinstimmen. Dann folgt $\varphi_1 = \varphi_2$.

   (e) Für welche $i \in \{0, 1, 2, 3\}$ gibt es (mindestens) ein Erzeugendensystem E_i von C_{100} mit i Elementen, das bezüglich $\subseteq$ minimal ist, d.h. für das keine echte Teilmenge ein Erzeugendensystem ist? In jenen Fällen, wo ein derartiges E_i existiert, ist ein solches auch explizit anzugeben. In jenen Fällen, wo keines existiert, genügt es das zu vermerken, ein Beweis für die Nichtexistenz ist nicht erforderlich.

   (f) Zu jedem $k \in \{0, 1, \ldots, 99\}$ gibt es einen eindeutigen Endomorphismus φ_k von C_{100} mit $\varphi_k(1 + 100\mathbb{Z}) = k + 100\mathbb{Z}$. Begründen Sie die Eindeutigkeitsaussage möglichst unter Verwendung bisheriger Teilaufgaben.

   (g) Umgekehrt gibt es offenbar zu jedem Endomorphismus φ von C_{100} ein eindeutiges $k \in \{0, 1, \ldots, 99\}$ mit $\varphi = \varphi_k$ wie in (f). Folglich sind die in (b) erwähnten binären Operationen auf $\mathrm{End}(C_{100})$ von der Gestalt $\varphi_{k_1} + \varphi_{k_2} = \varphi_{\omega_+(k_1,k_2)}$ und $\varphi_{k_1} \circ \varphi_{k_2} = \varphi_{\omega_\cdot(k_1,k_2)}$ mit binären Operationen $\omega_+, \omega_\cdot : N_{100}^2 \to N_{100}$ auf $N_{100} := \{0, 1, \ldots, 99\}$. Beschreiben Sie diese beiden Operationen ω_+ und $\omega_\cdot$ und schließen Sie daraus, ob der Endomorphismenring R von C_{100} kommutativ ist.

   (h) Bekanntlich besteht die Einheitengruppe eines beliebigen Rings mit Einselement aus den multiplikativ invertierbaren Elementen. Wie viele davon gibt es in $R := \mathrm{End}(C_{100})$?