Algebra, Prüfung am 20.6.2018, Winkler

Name, Matrikelnummer (bitte gleich ausfüllen):

Vereinbarter **Termin der mündlichen Prüfung** (nicht vorzeitig ausfüllen!):

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

1. Wir beschäftigen uns mit der Erweiterung von $\mathbb{N}$ zu $\mathbb{Z}$ und den Möglichkeiten zur Verallgemeinerung.

   (a) Die Gruppe $(\mathbb{Z}, +, 0, -)$ lässt sich aus der Struktur $(\mathbb{N}, +, 0)$ mit einer Standardmethode konstruieren. Welche Eigenschaften einer Algebra $(M, \cdot_M, e_M)$ vom Typ $(2, 0)$ reichen aus, um zu garantieren, dass mit Hilfe dieser Methode stets eine Gruppe $(G, \cdot_G, e_G, .^{-1})$ entsteht, in die $(M, \cdot_M, e_M)$ isomorph eingebettet werden kann?

   (b) Die Methode aus Teil (a) ist nun etwas genauer zu beschreiben. Sei dazu $(M, \cdot_M, e_M)$ mit den Eigenschaften aus (a) gegeben. Wie ist davon ausgehend die resultierende Trägermenge G definiert, wie die binäre Operation $\cdot_G$, wie das neutrale Element e_G, wie die Inversenbildung $.^{-1}$ und wie die zugehörige Einbettung $\iota : M \to G$?

   (c) Was versteht man unter einem initialen Objekt I in einer Kategorie $\mathcal{C}$?

   (d) Bekanntlich ist $(\mathbb{Z}, +, 0, -)$ in einem gewissen Sinn die kleinste Gruppe, die das Monoid $(\mathbb{N}, +, 0)$ enthält. Diese etwas ungenaue Aussage lässt sich mit Hilfe des Begriffs des initialen Objektes aus (c) präzisieren. Und zwar geschieht das in einer Weise, die auch für die allgemeinere Situation in (b) zutrifft. Für gegebenes $(M, \cdot_M, e_M)$ sei also $\mathcal{C} = \mathcal{C}(M, \cdot_M, e_M)$ die entsprechende Kategorie derart, dass ein $(G, \cdot_G, e_G, .^{-1})$ insofern eine minimale Gruppenerweiterung von $(M, \cdot_M, e_M)$ ist, als es sich dabei – zusammen mit ι wie in (a) und (b) – um ein initiales Objekt in $\mathcal{C}$ handelt. Was sind die Objekte, was die Morphismen dieser Kategorie $\mathcal{C}$?

   (e) Sei nun speziell M die Menge aller reellen 2×2-Matrizen, aufgefasst als multiplikatives Monoid $(M, \cdot_M, \mathrm{id})$ mit der Matrizenmultiplikation $\cdot_M$ und der Einheitsmatrix id. Weiters werde die Teilmenge $M_0 \subseteq M$ als Untermonoid erzeugt von der Streckung $m_1 := 2\,\mathrm{id}$ und der Drehung m_2 mit der Matrixdarstellung

   $$m_2 := \frac{1}{2} \begin{pmatrix} \sqrt{3} & -1 \\ 1 & \sqrt{3} \end{pmatrix}$$

   bezüglich der kanonischen Basis des $\mathbb{R}^2$. Welche der beiden Strukturen $(M, \cdot_M, \mathrm{id})$ und $(M_0, \cdot_M, \mathrm{id})$ hat alle Eigenschaften aus (a), und welche dieser Eigenschaften gehen der anderen Struktur ab?

   (f) Bestimmen Sie für jene der beiden Strukturen $(M, \cdot_M, \mathrm{id})$ oder $(M_0, \cdot_M, \mathrm{id})$ aus (e), die die Voraussetzungen aus (a) erfüllt, zwei Ihnen vertraute nichttriviale Gruppen G_1 und G_2 (für die wir Standardbezeichnungen haben), so dass die entsprechende Gruppe $(G, \cdot_G, e_G, .^{-1})$ aus (a) isomorph ist zum direkten Produkt $G_1 \times G_2$.

2. Sei $R = \mathbb{Z}[\sqrt{-2}]$ jene Ringerweiterung von $\mathbb{Z}$ innerhalb $\mathbb{C}$, die vom Element $i\sqrt{2}$ ($i^2 = -1$) erzeugt wird. Wie üblich bezeichne $N : R \to \mathbb{N}$, $z \mapsto |z|^2$, die Normfunktion auf R.

   (a) Beschreiben Sie die Trägermenge von R sowohl formal als Menge komplexer Zahlen $z = a + ib$ mit gewissen Real- und Imaginärteilen a bzw. b, als auch geometrisch als Punktmenge in der Ebene anhand einer Skizze.

   (b) Begründen Sie: Aus der Teilbarkeit $x|y$ zweier Elemente $x, y \in R$ folgt die Teilbarkeit $N(x)|N(y)$ ihrer Normen in $\mathbb{Z}$.

   (c) Folgern Sie aus (b), dass $N(e) = 1$ für jede Einheit $e \in R$ gilt, und ermitteln Sie sämtliche Einheiten in R.

   (d) Geben Sie ein irreduzibles Element in R an und begründen Sie, warum es sich um ein solches handelt.

   (e) Sei $x \in R$ gegeben, $x \neq 0$. Wegen Teil (a) und der geometrischen Deutung der Multiplikation mit einer komplexen Zahlen (in unserem Fall mit x) als Drehstreckung ist die Menge $Rx = \{qx : \ q \in R\}$ ein Gitter in der Ebene mit Rechtecken als Zellen. Die Seitenlängen jeder dieser Zellen sind $|x|$ und $\sqrt{2}|x|$. Jede komplexe Zahl z, insbesondere also jedes $y \in R \subseteq \mathbb{C}$ liegt in einer solchen Zelle. Der Abstand $|y - qx|$ zwischen y und dem nächstgelegenen Eckpunkt der Zelle (= zum nächsten Punkt qx aus Rx) ist höchstens so groß wie der Abstand des Mittelpunktes der Zelle zu einem Eckpunkt. Das ist die halbe Diagonale eines Rechtecks mit den Seitenlängen $|x|$ und $\sqrt{2}|x|$. Verwenden Sie den Satz von Pythagoras, um ein möglichst kleines $\lambda > 0$ zu finden, so dass stets $|y - qx| \leq \lambda|x|$ garantiert werden kann.

   (f) Finden Sie ein primes Element in R und begründen Sie, warum es sich tatsächlich um ein solches handelt. Hinweis: Vorangegangene Teile können helfen.

3. Das Polynom $f(x) := x^8 - 1 \in \mathbb{Q}[x]$ zerfällt in $\mathbb{C}$ in Linearfaktoren: $f(x) = \prod_{j=0}^{7}(x - \zeta^j)$. Dabei ist $\zeta := \exp(\frac{\pi}{4}i) = \frac{\sqrt{2}}{2}(1 + i)$ (also eine der primitiven 8-ten Einheitswurzeln) und $i \in \mathbb{C}$ die imaginäre Einheit mit $i^2 = -1$. Wir befassen uns mit den Körpererweiterungen $K_j := \mathbb{Q}(\zeta^j)$ von $\mathbb{Q}$ durch Adjunktion jeweils einer der Nullstellen $\zeta^j \in \mathbb{C}$, $j = 0, \ldots, 7$, von f. (Eine Skizze könnte hilfreich sein.)

   (a) Die Nullstellen von f bilden eine multiplikative Gruppe G von $\mathbb{C}$. Geben Sie den Untergruppenverband $(\mathrm{Sub}(G), \subseteq)$ durch sein Hassediagramm an.

   (b) Finden Sie die Zerlegung des Polynoms $f(x) := x^8 - 1 \in \mathbb{Q}[x]$ in irreduzible Faktoren über $\mathbb{R}$.

   (c) Finden Sie die Zerlegung des Polynoms $f(x) := x^8 - 1 \in \mathbb{Q}[x]$ in irreduzible Faktoren über $\mathbb{Q}$.

   (d) Unter den K_j herrschen einige Teilmengenbeziehungen und auch Gleichheiten. Zeichnen Sie das Hassediagramm aller (verschiedenen) K_j, $j = 0, \ldots, 7$, bezüglich $\subseteq$.

   (e) Geben Sie die Erweiterungsgrade $g_j := [K_j : \mathbb{Q}]$ für $j = 0, \ldots, 7$ an.

   (f) Wieviele Automorphismen hat der Körper $K_1 = \mathbb{Q}(\zeta)$? (Hinweis: Jede Nullstelle eines Polynoms über dem Primkörper $\mathbb{Q}$ muss auf eine Nullstelle desselben Polynoms abgebildet werden, und Automorphismen sind durch ihre Werte auf einer Erzeugendenmenge eindeutig bestimmt.)