**Algebra, Prüfung am 25.11.2013, Winkler**

Name, Matrikelnummer (bitte ausfüllen):

Mündliche Prüfung: Die Termineinteilung für die mündliche Prüfung werde ich an der Tür zu meinem Dienstzimmer aushängen. Kreuzen Sie bitte an, welcher der folgenden Halbtage für Sie in Frage kommt (Doppelmeldung möglich, sogar erwünscht). Ist keiner der beiden Termine möglich, bitte ich um persönliche Terminbesprechung unmittelbar nach der schriftlichen Prüfung.
∘ Mo, 2.12., nachmittags
∘ Fr, 6.12., vormittags
Ort: Prüfungs- und Besprechungsraum (Freihaus, grüner Bereich, 5.Stock, gegenüber dem Lift)

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. Sei $(K, +, 0, -, *, 1)$ ein Körper mit 25 Elementen. Sei $K_+$ die additive Gruppe von $K$, und $K_*$ die multiplikative Gruppe von $K$. Sei $P$ der Primkörper von $K$.

   (a) Finden Sie ein Produkt $G_1$ von zyklischen Gruppen, das zu $K_+$ isomorph ist.

   (b) Finden Sie ein Produkt $G_2$ von zyklischen Gruppen, das zu $K_*$ isomorph ist.

   (c) Geben Sie explizit einen nichttrivialen Gruppenautomorphismus $f : G_1 \to G_1$ an (d.h. ein $f \neq \mathrm{Id}_{G_1}$).

   (d) Geben Sie explizit einen nichttrivialen Gruppenautomorphismus $g : G_2 \to G_2$ an.

   (e) Zeigen Sie, dass das Polynom $r(x) := x^2 + x + 1 \in P[x]$ irreduzibel ist.

   (f) Sei $I$ das von $r(x)$ erzeugte Ideal in $P[x]$. Was für eine algebraische Struktur trägt die Menge $P[x]/I$, wie viele Elemente hat sie?

   (g) Das Polynom $y^2 + y + 1 \in K[y]$ hat in $K$ zwei Nullstellen $\alpha_1 \neq \alpha_2$. Beschreiben Sie alle Isomorphismen $\varphi : K \to P[x]/I$, indem Sie für jedes $\varphi$ die Werte $\varphi(\alpha_1)$ und $\varphi(\alpha_2)$ angeben.

   (h) Zeigen Sie, dass es mindestens einen nichttrivialen Körperautomorphismus von $K$ gibt. Hinweis: Verwenden Sie (g).

   (i) Zeigen Sie, dass es höchstens einen nichttrivialen Körperautomorphismus von $K$ gibt. Hinweis: Verwenden Sie (g).

2. Sei $R := \{\frac{k}{2^n} :\ k \in \mathbb{Z},\ n \in \mathbb{N}\} \subseteq \mathbb{Q}$.

(a) Offenbar ist $R$ ein Unterring von $\mathbb{Q}$ (bezüglich der üblichen Operationen $+$ und $\cdot$) mit $\mathbb{Z} \subseteq R$ und $\frac{1}{2} \in R$. Begründen Sie, warum jeder weitere Unterring $R'$ von $\mathbb{Q}$ mit diesen beiden Eigenschaften $R$ umfassen muss.

(b) Die additive Gruppe von $R$ ist nicht endlich erzeugt. Begründen Sie dies.

(c) Jedes Element der Form $\pm 2^k \in R$ hat ein multiplikatives Inverses $\pm 2^{-k} \in R$, liegt also in der Einheitengruppe $R^*$. Begründen Sie, warum $R^*$ außer diesen keine weiteren Einheiten enthält.

(d) Die multiplikative Gruppe $R^*$ ist isomorph zur additiven Gruppe $\mathbb{Z} \times (\mathbb{Z}/(2\mathbb{Z}))$. Geben Sie einen Isomorphismus $\varphi : \mathbb{Z} \times (\mathbb{Z}/(2\mathbb{Z})) \to R^*$ an.

(e) Sei $S$ ein Integritätsbereich, $S^\times = S \setminus \{0\}$, $E(S)$ die Einheitengruppe von $S$ und $J$ eine beliebige Indexmenge. Angenommen es gibt einen Halbgruppenisomorphismus $\psi : S^\times/E(S) \to \bigoplus_{j\in J} \mathbb{N}$. Dabei bezeichne $S^\times/E(S)$ das multiplikative Monoid modulo Einheiten und $\mathbb{N}$ das additive Monoid. Außerdem steht $\bigoplus_{j\in J} \mathbb{N}$ für die direkte Summe, bestehend aus jenen $(n_j)_{j\in J} \in \prod_{j\in J} \mathbb{N}$, wo $n_j \neq 0$ nur für endlich viele $j \in J$ gilt. Dann ist $S$ ein faktorieller Ring. Charakterisieren Sie die irreduziblen = primen Elemente $p \in S$ durch ihre Bilder $\psi(p)$.

(f) Umgekehrt gibt es zu jedem faktoriellen Ring $S$ einen Isomorphismus $\psi$ wie in (e). Geben Sie einen solchen an. (Hinweis: Nehmen Sie als Indexmenge $J = J(S)$ die Menge der Assoziiertenklassen primer Elemente.)

(g) Der Ring $R$ ist faktoriell. Nach (f) gibt es daher ein $\psi$ wie in (e). Geben Sie $J(R)$ und die $n_j$ in $\psi(\frac{k}{2^n}) = (n_j)_{j\in J}$ explizit an.

(h) Sei $I$ ein Ideal von $R$. Dann ist offensichtlich $I_{\mathbb{Z}} := I \cap \mathbb{Z}$ ein Ideal in $\mathbb{Z}$.

- Weil $\mathbb{Z}$ ein Hauptidealring ist, gibt es ein $m \in \mathbb{Z}$ mit $I_{\mathbb{Z}} = \{\ell m :\ \ell \in \mathbb{Z}\}$. Wegen der Idealeigenschaft von $I$ ist $RI_{\mathbb{Z}} = \{\frac{\ell m}{2^n} :\ \ell \in \mathbb{Z},\ n \in \mathbb{N}\} \subseteq I$.
- Sei umgekehrt $r = \frac{k}{2^n} \in I$ mit $k \in \mathbb{Z}$ und $n \in \mathbb{N}$. Wieder weil $I$ ein Ideal ist, folgt $k = 2^n r \in I \cap \mathbb{Z} = I_{\mathbb{Z}}$. Folglich ist $k = \ell m$ mit einem $\ell \in \mathbb{Z}$. Also ist $r = \frac{\ell m}{2^n} \in RI_{\mathbb{Z}}$.

Ist $R$ ein Hauptidealring? (Begründung)

(i) Seien $k_a, k_b \in \mathbb{Z}$ und $n_a, n_b \in \mathbb{N}$ vorgegeben, $k_a \neq 0$. Division mit Rest in $\mathbb{Z}$ liefert ein $q \in \mathbb{Z}$ und ein $r \in \{0, 1, \ldots, |k_a| - 1\}$ mit $k_b = qk_a + r$. Nach Division durch $2^{n_b}$ erhalten wir die Gleichung $\frac{k_b}{2^{n_b}} = \frac{q}{2^{n_b - n_a}} \frac{k_a}{2^{n_a}} + \frac{r}{2^{n_b}}$. Ist $R$ ein Euklidischer Ring? Wenn ja, geben Sie eine Euklidische Bewertung explizit an; wenn nein, begründen Sie dies.