Algebra 1
SoSe 2004
Schmale **24. 5. 2004**

Aufgabenblatt 6

(20) **Hauptideale und Teilbarkeit:** Beweisen Sie Satz 9.5 (b), (d), (e) und (g). Dabei sollen nur die vorangehenden Definitionen und Eigenschaften benutzt werden.
Anleitung zu (d): wegen (c) ist $1 = ar + bs$ mit geeigneten $r, s \in R$. Multiplikation mit c.

(21) **Zur Berechnung multiplikativer Inverser in R/I und dazu isomorphen Ringen.** Zeigen Sie:

(a) Zu $a + I \in R/I$ existiert ein multiplikatives Inverses in R/I genau dann, wenn $aR + I = R$.

(b) Wenn $I = dR$ ein Hauptideal ist, dann lautet die Bedingung in (a): $\exists r, s \in R : ar + ds = 1$.

(c) Berechnen Sie $b \in \mathbb{Z}_{1001}$ mit $225 \odot b = 1$, ($b = a^{\textcircled{-1}}$).

(22) **Ganz schön verwickelt ?**
Sei $K = \mathbb{Z}_2[x]_{2,x^2+x+1}$

(a) Bestimmen Sie die Menge Π der Primpolynome von Grad 2 in $K[y]$ und zeigen Sie insbesondere damit: $y^2 + y + x \in \Pi$.

(b) Sei $L = K[y]_{2,y^2+y+x}$. Berechnen Sie y^{-1} in L

(c) Sei $g = x^2 + x + 1$ in $\mathbb{Z}[x]$. Zeigen Sie im geeigneten Kontext: $\varrho_2 \circ \varrho_g = \varrho_g \circ \varrho_2$

(d) **Zusatz:** Wir erweitern den Ausgangsring zu $\mathbb{Z}_2[x, y]$ und betrachten zusätzlich noch das Polynom $f = y^2 + y + x$. Gilt nun $\varrho_f \circ \varrho_g = \varrho_g \circ \varrho_f$?

(23) **Unzerlegbar aber nicht prim !**
Sei $R = \left\{ \sum_{k=0}^{n} a_k x^k : n \in \mathbb{N},\, a_0, \ldots, a_n \in \mathbb{Q},\, a_1 = 0 \right\}$. Zeigen Sie:

(a) R ist Unterring des Ringes $\mathbb{Q}[x]$ aller Polynome mit rationalen Koeffizienten und es gilt: $G(R) = G(\mathbb{Q}[x])$.

(b) x^2 und x^3 sind unzerlegbar, aber nicht prim in R.

(24) **Elementeordnungen.**

Seien M ein Monoid und $a, b \in G(M)$ Elemente endlicher Ordnung, für die gilt: $ab = ba$. Seien m, n die Ordnungen von a und b und T die Menge der positiven Teiler von m.
Zeigen Sie:

(a) $\forall r \in \mathbb{Z} : \mathrm{ord}(a^r) \in T$

(b) $\forall d \in T : \mathrm{ord}(a^d) = \frac{m}{d}$

(c) $\forall d \in T \;\; \forall r \in \mathbb{Z} : \mathrm{ord}(a^r) = d \Leftrightarrow \exists s \in \mathbb{Z} : r = s\frac{m}{d}$ und $ggT(s, d) = 1$.
Anleitung: $r = s\frac{m}{d} + t$ mit $0 \leq td < m$. Es geht auch anders.

(d) $\forall d \in T : \;\; |\{r \in \mathbb{Z}_m : \mathrm{ord}(a^r) = d\}| = |G(\mathbb{Z}_d)|$

(e) Wenn ggT$(m, n) = 1$, dann ist $\mathrm{ord}(ab) = mn$.

(f) Es gibt ein $c \in < a, b >$ derart, dass $\mathrm{ord}(c) =$kgV(m, n)

Ich empfehle zumindest (20), (22) und (23).