RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

Hausübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 13 / 19. Januar 2011 / Abgabe bis spätestens 26. Januar 2011, 10 Uhr (vor der Übung)

AUFGABE 1 (5 Punkte)**:**
Seien $f, g \in \mathbb{F}[x_1, \ldots, x_n] \backslash \{0\}$. Beweisen Sie folgende Aussagen.

i) $\text{multigrad}(f \cdot g) = \text{multigrad}(f) + \text{multigrad}(g)$,

ii) $\text{multigrad}(f + g) \leq \max\{\text{multigrad}(f), \text{multigrad}(g)\}$ für $f + g \neq 0$.

Geben Sie in ii) jeweils ein Beispiel an, für das der Ausdruck $=$ bzw. $<$ annimmt.

AUFGABE 2 (6 Punkte)**:**
Berechnen Sie den Rest, der bei der Division von $x^2y^2 + xy^2 - y + 1$ durch $F = \{xy^2 - x, x - y^3\}$ entsteht. Welcher Rest entsteht, wenn Sie die Reihenfolge der Quotienten vertauschen? Führen Sie die Berechnung jeweils für die Ordnungen lex und grlex mit $x > y$ durch.

AUFGABE 3 (4 Punkte)**:**
Beweisen oder widerlegen Sie, dass folgende Mengen eine Gröbnerbasis bilden (bzgl. lexikographischer Ordnung mit $x > y > z$).

a) $\{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$,

b) $\{x^2 + y, x - z\}$.