RUHR UNIVERSITÄT BOCHUM

RUB

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

**Präsenzübungen zur Vorlesung**

# Kryptanalyse

**WS 2010/2011**

Blatt 13 / 19. Januar 2011

**AUFGABE 1:**
Beweisen Sie, dass die lexikographische Ordnung $>_{lex}$ eine Monomordnung ist.

*Hinweis: Um zu zeigen, dass $>_{lex}$ eine Ordnung ist, müssen Sie Reflexivität, Antisymmetrie und Transitivität der Relation zeigen.*

**AUFGABE 2:**
Schreiben Sie die folgenden Polynome um, indem Sie die Terme mit lex, grlex und grevlex ordnen. Geben Sie jeweils LM, LT und multideg an. Benutzen Sie die Ordnung $x > y > z$ auf den Variablen.

i) $f(x, y, z) = 2x + 3y + z + x^2 - z^2 + x^3$,

ii) $f(x, y, z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$.

**AUFGABE 3:**
Beweisen Sie: Jedes Monomideal $I = \langle x^\alpha \mid \alpha \in A \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$ besitzt eine endliche Basis $I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(m)} \right\rangle$ mit $\alpha^{(i)} \in A$.

*Hinweis: Sie dürfen Dicksons Lemma Teil I benutzen.*