RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 12 / 18. Januar 2012

AUFGABE 1:
Sei $>$ eine beliebige Monomordnung. Zeigen Sie:

a) $\alpha \geq 0$ für alle $\alpha \in \mathbb{N}_0^n$.

b) Wenn x^α das Monom x^β teilt, so gilt $\alpha \leq \beta$. Gilt die Umkehrung im Allgemeinen?

c) Sei $\alpha + \mathbb{N}_0^n := \{\alpha + x : x \in \mathbb{N}_0^n\}$. Dann gilt $\alpha \leq \beta$ für alle $\beta \in \alpha + \mathbb{N}_n^0$.

AUFGABE 2:
Führen Sie den Divisionsalgorithmus über $\mathbb{R}[x, y]$ durch für $f = x^2y^2 + x^2y - y + 1$ und $F = (xy^2 + x, xy - y^3)$ und verwenden Sie als Monomordnung $>_{lex}$.