RUHR UNIVERSITÄT BOCHUM

RUB

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

Präsenzübungen zur Vorlesung

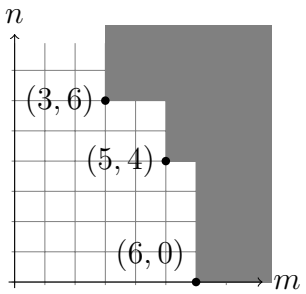
Kryptanalyse

WS 2011/2012

Blatt 13 / 25. Januar 2012

AUFGABE 1:

Sei $I \subset \mathbb{F}[x,y]$ das Monomideal $I =< x^3y^6, x^5y^4, x^6 >$. Man kann sich I wie in der folgenden Abbildung veranschaulicht durch die Vereinigung der drei Mengen $(3,6)+\mathbb{N}_0^2$, $(5,4)+\mathbb{N}_0^2$ und $(6,0)+\mathbb{N}_0^2$ vorstellen (wenn man Monome x^ny^m mit Punkten (n,m) identifiziert).



a) Führen Sie den konstruktiven Beweis zu Dicksons Lemma (Folie 88) bzgl. $>_{lex}$ durch, um eine Basis für I zu berechnen (dies mag sinnlos erscheinen, weil I schon durch eine endliche Menge von Monomen definiert ist, dient jedoch der Veranschaulichung des Beweises). Illustrieren Sie die erhaltene Basis auf ähnliche Weise wie oben beschrieben. Welche der Basismonome sind überflüssig?

b) Begründen Sie, wieso man nicht einfach die Monome $x^{\alpha^{(i)}}y^{t_i}$ als Basis für I wählen kann. Wie sähe eine entsprechende Basis für das obige Beispiel aus und welche Elemente aus I kann man dann nicht darstellen?

AUFGABE 2:

Sei $V_1 \supset V_2 \supset V_3 \supset \ldots$ eine absteigende Kette affiner Varietäten. Zeigen Sie: Es gibt ein $N \geq 1$, so dass $V_i = V_N$ für alle $i \geq N$.

Hinweis: Versuchen Sie, die *Ascending Chain Condition* (ACC) auf $I(V_j)$ anzuwenden.

AUFGABE 3:

Betrachten Sie $I :=< x - z^2, y - z^3 > \subset \mathbb{R}[x,y,z]$ und $>_{lex}$.

a) Beweisen Sie (ohne das Buchberger Kriterium zu benutzen), dass $\{x - z^2, y - z^3\}$ eine Gröbnerbasis für I ist.

b) Überprüfen Sie die Aussage mit dem Buchberger Kriterium.