RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 12 / 15. Januar 2013

AUFGABE 1:

(a) Wiederholen Sie die Definition einer Monomordnung.

(b) Zeigen Sie, dass $>_{\texttt{lex}}$ eine Monomordnung auf $\mathbb{N}^n$ für $n \in \mathbb{N}$ ist.

AUFGABE 2:

Seien $f, g \in \mathbb{F}[X_1, \ldots, X_n] \backslash \{0\}$. Beweisen Sie folgende Aussagen.

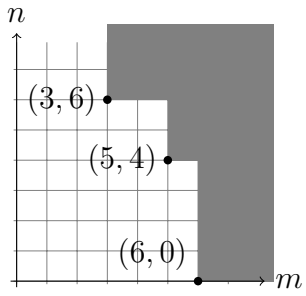
i) $\text{multigrad}(f \cdot g) = \text{multigrad}(f) + \text{multigrad}(g)$,

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, in dem $=$ bzw. $<$ angenommen wird.

AUFGABE 3:

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 88f) 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 4:
Beweisen Sie den 2. Teil von Dicksons Lemma (auf Hausübung verlegt):
Sei $I = \langle x^\alpha \mid \alpha \in A \rangle \subset \mathbb{F}[X_1, \ldots, X_n]$ ein Monomideal für eine beliebige (potenziell unendliche) Erzeugermenge A. Zeigen Sie, dass I stets eine endliche Basis *aus Elementen der gegebenen Erzeugermenge* A besitzt, d.h. $A' \subset A$ existiert mit $I = \langle x^\alpha \mid \alpha \in A' \rangle$, $|A'|$ endlich.

AUFGABE 5:
Sei $f = X^4Y^2 + XY^3 + Y^4, g = XY - 1$ in $\mathbb{Q}[X, Y]$. Berechnen Sie die Polynomdivision mit Rest von f durch $\{g\}$ bzgl. der Mononomordnung $>_{\texttt{lex}}$ (wobei $X >_{\texttt{lex}} Y$).