RUHR UNIVERSITÄT BOCHUM

RUB

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

Hausübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 13 / 25. Januar 2012 / Abgabe bis spätestens 1. Februar 2012, 10 Uhr in dem Kasten auf NA 02

AUFGABE 1 (5 Punkte)**:**
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 den bereits bewiesenen Teil von Dicksons Lemma aus der Vorlesung benutzen (siehe Folie 88f).

AUFGABE 2 (5 Punkte)**:**

a) Zeigen Sie, dass die *Ascending Chain Condition* (ACC) den Hilbert'schen Basissatz impliziert, d.h. wenn jede aufsteigende Kette von Idealen $I_1 \subset I_2 \subset \ldots$ in $\mathbb{F}[x_1, \ldots, x_n]$ stationär wird (also $I_N = I_j$ für alle $j \geq N$ gilt), so ist jedes Ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$ endlich erzeugt (also $I =< g_1, \ldots, g_s >$ für $g_i \in I$).

b) Seien $f_1, f_2, \ldots \in \mathbb{F}[x_1, \ldots, x_n]$ und sei $\mathbf{V}(f_1, f_2, \ldots) \subset \mathbb{F}^n$ die Menge aller Lösungen des Gleichungssystem $f_1 = f_2 = \ldots = 0$ mit unendlich vielen Gleichungen. Zeigen Sie: Es gibt ein $N \geq 1$ mit $\mathbf{V}(f_1, f_2, \ldots) = \mathbf{V}(f_1, \ldots, f_N)$. (*Hinweis:* Die ACC ist hilfreich).

AUFGABE 3 (10 Punkte)**:**
Sei $G = \{x^2y - 1, xy^2 - x\}$ und betrachte $I := \langle G \rangle \subset \mathbb{R}[x, y]$. Führen Sie Teil a) bis c) sowohl für $>_{lex}$ als auch $>_{grlex}$ durch.

a) Formen Sie G mittels Buchberger Algorithmus in eine Gröbnerbasis für I um. (Geben Sie die wesentlichen Zwischenschritte mit an.)

b) Bilden Sie eine minimale Gröbnerbasis.

c) Bilden Sie die reduzierte Gröbnerbasis.

Nutzen Sie für die Beantwortung von d) und e) die reduzierte Gröbnerbasis für I bzgl. $>_{lex}$ (zur Kontrolle: Diese sollte $G = \{x^2 - y, y^2 - 1\}$ lauten). Beweisen oder widerlegen Sie durch anwenden des Divisionsalgorithmus die Aussage $f \in I$ für folgende Polynome f.

d) $f = -2x^3y^2 + 2xy^3 + xy^2 - x$

e) $f = x^4y - x^2y^2 + xy - y^2 + 1$