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 11 / 8. Januar 2013

AUFGABE 1:

Sei $r \in \mathbb{R}, r > 0$ eine feste Konstante. Skizzieren Sie die affinen Varietäten

$$V_1 = V(x^2 + y^2 - r^2) \subset \mathbb{R}^2$$
$$V_2 = V(xy) \subset \mathbb{R}^2$$
$$V_3 = V(x^2 + y^2 - r^2, xy)$$

und bestimmen Sie alle (endlich vielen) Punkte von V_3.

AUFGABE 2:

Sei $\mathbb{F}$ ein beliebiger Körper und $I \subset \mathbb{F}[X_1, \ldots, X_n]$ ein Ideal sowie $f_1, \ldots, f_s \in \mathbb{F}[X_1, \ldots, X_n]$. Zeigen Sie die Äquivalenz folgender Aussagen:

(i) $f_1, \ldots, f_s \in I$

(ii) $\langle f_1, \ldots, f_s \rangle \subset I$.

Zeigen Sie damit: $\langle X, Y \rangle = \langle X + Y, X - Y, XZ \rangle \subset \mathbb{F}[X, Y, Z]$, wobei $0 \neq 2 \in \mathbb{F}$.

AUFGABE 3:

Zeigen Sie:

(i) $M_1 = \{x \in \mathbb{R} \mid x > 0\}$ ist keine affine Varietät über $\mathbb{R}$.

(ii) $M_2 = \{x \in \mathbb{R} \mid x \geq 0\}$ ist keine affine Varietät über $\mathbb{R}$.

(iii) $M_3 = \mathbb{R} \subset \mathbb{C}$ ist keine affine Varietät über $\mathbb{C}$.

(iv) $M_4 = \{(x, 0) \mid x \in \mathbb{R}\} \subset \mathbb{R}^2$ ist eine affine Varietät über $\mathbb{R}$.

AUFGABE 4:

(a) Sei $\mathbb{F}$ zunächst ein beliebiger Körper, $n > 0$. Zeigen Sie, dass jede *endliche* Menge $M \subset \mathbb{F}^n$ eine affine Varietät über $\mathbb{F}$ ist.

(b) Sei $\mathbb{F}$ endlicher Körper und $\mathbb{F} \subset \mathbb{F}'$ für einen Körper $\mathbb{F}'$. Zeigen Sie, dass $\mathbb{F}$ eine affine Varietät über $\mathbb{F}'$ ist (vgl. Aufg. 3c). Wie sehen sie definierenden Gleichungen aus?