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

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 11 / 11. Januar 2012

AUFGABE 1:
Sei $r > 0, r \in \mathbb{R}$ fix. Skizzieren Sie die affine Varietät

$$\mathbf{V}(x^2 + y^2 - r^2, xy) \subset \mathbb{R}^2$$

und bestimmen Sie alle Punkte von $\mathbf{V}$.

AUFGABE 2:

a) Sei $I \subset \mathbb{F}[x_1, \ldots, x_n]$ ein Ideal. Zeigen Sie die Äquivalenz folgender Aussagen

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

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

b) Zeigen Sie $\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathbf{V}(x^2 - 4, y^2 - 1)$ über $\mathbb{Q}$.

AUFGABE 3:
Sei $H = \{(x, y) \in \mathbb{R}^2 \mid y > 0\}$. Zeigen Sie, dass H *keine* affine Varietät ist.

Hinweis: Betrachten Sie $f(x, x)$ und zeigen Sie, dass $f(0, 0) = 0$.