6.2 Die Arithmetik des Grundkörpers

Für den AES-Algorithmus wird der 8-dimensionale $\mathbb{F}_2$-Vektorraum $\mathbb{F}_2^8$ mit dem Körper $\mathbb{F}_{256}$ gleichgesetzt. Dies bedarf einer Erläuterung.

Algebraische Darstellung des Grundkörpers

Endliche Körper werden über dem jeweiligen Primkörper $\mathbb{F}_p$ am einfachsten als Restklassenringe des Polynomrings $\mathbb{F}_p[X]$ nach einem Hauptideal konstruiert, das von einem irreduziblen Polynom $h \in \mathbb{F}_p[X]$ erzeugt wird. Dann ist $h\mathbb{F}_p[X]$ Primideal, also

$$K := \mathbb{F}_p[X]/h\mathbb{F}_p[X]$$

ein endlicher Körper, der über $\mathbb{F}_p$ den Grad (= die Dimension) $n = \operatorname{Grad} h$ hat. Für die Identifikation von K mit dem Vektorraum $\mathbb{F}_p^n$ werden die Restklassen der Potenzen von X mit den n Einheitsvektoren gleichgesetzt, also für $x = X \bmod h$:

$$x^0 = 1 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \quad x^1 = x = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, \quad \ldots, \quad x^{n-1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}.$$

Ist $h = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ (o. B. d. A. normiert), so folgt aus $h \bmod h = 0$, dass

$$x^n = -a_1x^{n-1} - \cdots - a_{n-1}x - a_n$$

in K. Darüber hinaus zeigt diese Gleichung, wie die Restklasse eines jeden Polynoms f durch $1, x, \ldots, x^{n-1}$, also durch die kanonische Basis ausgedrückt werden kann. Algorithmisch läuft das auf den Rest der Polynom-Division „f geteilt durch h“ hinaus.

Für AES wird das Polynom

$$h = X^8 + X^4 + X^3 + X + 1 \in \mathbb{F}_2[X]$$

verwendet.

Multiplikationstafel

Die Multiplikationstafel für die Basis $(1, x, \ldots, x^{n-1})$ ergibt sich aus der durch h gegebenen Relation. Für AES ist etwa

$$x^2 \cdot x^7 = x^9 = x \cdot x^8 = x \cdot (x^4 + x^3 + x + 1) = x^5 + x^4 + x^2 + x.$$

Effiziente Inversion

Bei AES wird eine vollständige Wertetabelle für S-Box verwendet; das ist effizient implementierbar, da es sich ja nur um 256 Werte handelt.