

## 1.9 Matrixgeneratoren über endlichen Körpern

Ein Matrix-Generator über einem Körper  $K$  wird durch eine  $r \times r$ -Matrix

$$A \in M_r(K)$$

vollständig beschrieben (bis auf die Wahl des Startvektors  $x_0 \in K^r$ ). Das Ziel dieses Abschnitts ist die Charakterisierung der Folgen mit maximaler Periodenlänge.

Im Polynomring  $K[T]$  in einer Unbestimmten  $T$  bildet die Menge

$$\{\rho \in k[T] \mid \rho(A) = 0\}$$

ein Ideal. Da  $k[T]$  Hauptidealring ist (sogar euklidischer Ring), wird dieses Ideal von einem eindeutig bestimmten normierten Polynom  $\mu$  erzeugt; dieses heißt das **Minimalpolynom** von  $A$ . Da  $A$  auch Nullstelle seines charakteristischen Polynoms  $\chi$  ist, gilt also  $\mu \mid \chi$ . Ist  $A$  invertierbar, so ist das absolute Glied von  $\mu$  nicht 0; denn sonst hätte  $\mu$  die Nullstelle 0 und  $A$  den Eigenwert 0.

**Hilfssatz 2** Sei  $K$  ein Körper,  $A \in GL_r(K)$  von endlicher Ordnung  $t$ ,  $\mu$  das Minimalpolynom von  $A$ ,  $s = \text{Grad } \mu$ ,  $R := K[T]/\mu K[T]$  und  $a \in R$  die Restklasse von  $T$ . Dann gilt:

$$a^k = 1 \iff \mu \mid T^k - 1 \iff A^k = \mathbf{1}.$$

Insbesondere ist  $a \in R^\times$ ,  $t$  auch die Ordnung von  $a$  und  $\mu \mid T^t - 1$ .

*Beweis.*  $R$  ist eine  $K$ -Algebra der Dimension  $s$ . Ist  $\mu = b_s T^s + \dots + b_0$ , so

$$\mu - b_0 = T \cdot (b_s T^{s-1} + \dots + b_1);$$

da  $b_0 \neq 0$ , ist also  $T \bmod \mu$  invertierbar, also  $a \in R^\times$ . Da  $a^k$  die Restklasse von  $T^k$  ist, folgt die behauptete Äquivalenzkette.  $\diamond$

**Korollar 1** Ist  $K$  ein endlicher Körper mit  $q$  Elementen, so ist

$$t \leq \#R^\times \leq q^s - 1 \leq q^r - 1.$$

Sei von jetzt an  $K$  ein endlicher Körper mit  $q$  Elementen. Dann ist auch die Gruppe  $GL_r(K)$  der invertierbaren  $r \times r$ -Matrizen endlich. Der Vektorraum  $K^r$  besteht aus  $q^r$  Vektoren. Wir wissen bereits, dass jede Folge, die von dem Matrixgenerator zu  $A$  erzeugt wird, rein-periodisch ist. Eine volle Periode wird immer vom Nullvektor  $0 \in K^r$  alleine gebildet. Alle übrigen Vektoren werden im allgemeinen auf mehrere Perioden aufgeteilt sein. Ist  $s$  die Länge einer solchen Periode und  $x_0$  der entsprechende Startvektor, so

ist  $x_0 = x_s = A^s x_0$ . Also hat  $A^s$  den Eigenwert 1 und folglich  $A$  eine  $s$ -te Einheitswurzel als Eigenwert.

Denkbar ist aber auch, dass alle Vektoren  $\neq 0$  zusammen eine Periode der maximal möglichen Länge  $q^r - 1$  bilden. In diesem Fall gilt  $A^s x = x$  für alle Vektoren  $x \in K^r$  mit  $s = q^r - 1$ , aber für keinen kleineren Exponenten  $> 0$ . Also ist  $t = q^r - 1$  die Ordnung von  $A$ . Damit ist gezeigt:

**Korollar 2** *Ist  $K$  endlich mit  $q$  Elementen, so gilt:*

- (i) *Erzeugt der Matrixgenerator zu  $A$  für einen Startvektor  $\neq 0$  eine Folge der Periode  $s$ , so hat  $A$  eine  $s$ -te Einheitswurzel als Eigenwert.*
- (ii) *Gibt es eine Periode der Länge  $q^r - 1$ , so ist  $t = q^r - 1$  die Ordnung von  $A$ .*

**Hilfssatz 3** *Sei  $K$  ein endlicher Körper mit  $q$  Elementen und  $\varphi \in K[T]$  ein irreduzibles Polynom vom Grad  $d$ . Dann gilt  $\varphi | T^{q^d - 1} - 1$ .*

*Beweis.* Der Restklassenring  $R = k[T]/\varphi K[T]$  ist ein Erweiterungskörper vom Grad  $d = \dim_K R$ , hat also  $h := q^d$  Elemente und enthält mindestens eine Nullstelle  $a$  von  $\varphi$ , nämlich die Restklasse von  $T$ . Da jedes  $x \in R^\times$  die Gleichung  $x^{h-1} = 1$  erfüllt, ist insbesondere  $a$  auch Nullstelle von  $T^{h-1} - 1$ . Also ist  $\text{ggT}(\varphi, T^{h-1} - 1)$  nicht konstant. Da  $\varphi$  irreduzibel ist, folgt  $\varphi | T^{h-1} - 1$ .  $\diamond$

**Definition.** Ein Polynom  $\varphi \in K[T]$  vom Grad  $d$  über dem endlichen Körper  $K$  mit  $q$  Elementen heißt **primitiv**, wenn  $\varphi$  irreduzibel und kein Teiler von  $T^k - 1$  ist für  $1 \leq k < q^d - 1$ .

**Hauptsatz 1** *Sei  $K$  ein endlicher Körper mit  $q$  Elementen und  $A \in GL_r(K)$ . Dann sind folgende Aussagen äquivalent:*

- (i) *Der Matrixgenerator zu  $A$  erzeugt eine Folge der Periode  $q^r - 1$ .*
- (ii)  *$A$  hat die Ordnung  $q^r - 1$ .*
- (iii) *Das charakteristische Polynom  $\chi$  von  $A$  ist primitiv.*

*Beweis.* „(i)  $\implies$  (ii)“: Siehe Korollar 2 (ii).

„(ii)  $\implies$  (iii)“: In Korollar 1 ist  $t = q^r - 1$ . Also ist  $\#R^\times = q^s - 1$ , also  $R$  ein Körper und daher  $\mu$  irreduzibel. Ferner ist  $s = r$ , also  $\mu = \chi$ , und  $\mu$  nach Hilfssatz 2 kein Teiler von  $T^k - 1$  für  $1 \leq k < q^r - 1$ , also  $\mu$  primitiv.

„(iii)  $\implies$  (i)“: Da  $\chi$  irreduzibel ist, ist  $\chi = \mu$ . Die Restklasse  $a$  von  $T$  ist Nullstelle von  $\mu$  und hat nach der Definition von „primitiv“ die multiplikative Ordnung  $q^r - 1$ . Da das Potenzieren mit  $q$  ein Automorphismus des Körpers  $R$  ist, der  $K$  elementweise festlässt, sind auch die  $r$  Potenzen  $a^{q^k}$  für  $0 \leq k <$

$r$  Nullstellen von  $\mu$ , und zwar alle verschieden. Dies müssen daher sämtliche Nullstellen sein, und alle haben die multiplikative Ordnung  $q^r - 1$ . Daher hat  $A$  keinen Eigenwert von geringerer Ordnung und daher gibt es nach Korollar 2 (i) auch keine kürzere Periode.  $\diamond$

Für ein lineares Schieberegister ist  $A$  die Begleitmatrix wie in 1.7. Das charakteristische Polynom ist also  $T^l - a_1T^{l-1} - \dots - a_l$ .

**Korollar 1** *Ein lineares Schieberegister der Länge  $l$  erzeugt genau dann eine Folge der maximal möglichen Periode  $2^l - 1$ , wenn sein charakteristisches Polynom primitiv und der Startwert  $\neq 0$  ist.*

Die Konstruktion von linearen Schieberegistern, die Folgen maximaler Periode erzeugen, ist also auf die Konstruktion primitiver Polynome über dem Körper  $\mathbb{F}_2$  zurückgeführt.

Im eindimensionalen Fall  $r = 1$  erhalten wir speziell den multiplikativen Generator mit der Rekursionsvorschrift  $x_n = ax_{n-1}$  über dem endlichen Körper  $K$  mit  $q$  Elementen. Die zugehörige Matrix  $A = (a)$  bewirkt die Multiplikation mit  $a$ , also ist  $a$  der einzige Eigenwert und  $\chi = T - a \in K[T]$  das charakteristische Polynom. Dieses ist, da linear, in jedem Fall irreduzibel. Da

$$\chi|T^k - 1 \iff a \text{ Nullstelle von } T^k - 1 \iff a^k = 1,$$

ist  $\chi$  also genau dann primitiv, wenn  $a$  erzeugendes Element der multiplikativen Gruppe  $K^\times$ , also primitives Element ist. Damit ist die folgende leichte Verallgemeinerung des Korollars zu Satz 2 gezeigt:

**Korollar 2** *Ein multiplikativer Generator über  $K$  mit Multiplikator  $a$  erzeugt genau dann eine Folge der Periode  $q - 1$ , wenn  $a$  primitives Element und der Startwert  $x_0 \neq 0$  ist.*