12. Endliche Körper von Primzahlpotenzordnung

Irreduzible Polynome in $\mathbb{F}_p[X]$

Im Folgenden sei $\mathbb{F}_p[X]$ der Ring der Polynome über dem Körper $\mathbb{F}_p$ (p prim), d. h. $\mathbb{F}_p[X]$ ist die Menge der Polynome mit Koeffizienten in $\mathbb{F}_p$ mit der üblichen Addition und Multiplikation von Polynomen.

Für ein Polynom $f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{F}_p[X]$ ist der **Grad** von f definiert als $\deg(f) := \max\{k \in \mathbb{N} : a_k \neq 0\}$ falls solch eine Zahl existiert, sonst sei $\deg(f) := -\infty$ (d. h. $\deg(0) = -\infty$), wobei wir definieren $-\infty + -\infty = -\infty + n = -\infty$ für alle $n \in \mathbb{N}$.

Faktum 12.1. *Sind $f, g \in \mathbb{F}_p[X]$, so ist $\deg(f \cdot g) = \deg(f) + \deg(g)$.*

Beweis. Ist $f = 0$ oder $g = 0$, so ist $-\infty = \deg(f \cdot g) = \deg(f) + \deg(g)$. Andernfalls seien $f = a_0 + a_1X + \ldots + a_mX^m$ und $g = b_0 + b_1X + \ldots + b_nX^n$ mit $a_m \neq 0 \neq b_n$. Weil $\mathbb{F}_p$ ein Körper ist, gilt $a_mb_n \neq 0$ und aus $f \cdot g = a_0b_0 + (a_0b_1 + a_1b_0)X + \ldots + a_mb_nX^{m+n}$ folgt $\deg(f \cdot g) = \deg(f) + \deg(g)$. ⊣

Ein Polynom $f \in \mathbb{F}_p[X]$ mit $\deg(f) > 0$ heisst **irreduzibel** über $\mathbb{F}_p$, wenn aus $g \cdot h = f$ für $g, h \in \mathbb{F}_p[X]$ folgt $\deg(g) = 0$ oder $\deg(h) = 0$, sonst heisst f **reduzibel**. Wie für die Eindeutigkeit der Primfaktorzerlegung (Theorem 8.4) lässt sich zeigen, dass sich jedes Polynom $f \in \mathbb{F}_p[X]$ mit $f \neq 0$ bis auf Vertauschung der Faktoren und bis auf Faktoren aus $\mathbb{F}_p$ eindeutig als Produkt irreduzibler Polynome schreiben lässt.

Für $f \in \mathbb{F}_p[X]$ sei

$$(f) := \{g \cdot f : g \in \mathbb{F}_p[X]\}$$

das von f erzeugte Ideal in $\mathbb{F}_p[X]$. Dann ist mit Lemma 10.2 $\mathbb{F}_p[X]/(f)$ ein Ring.

Proposition 12.2. *Sei $f \in \mathbb{F}_p[X]$ mit $\deg(f) \geq 1$. Dann ist $\mathbb{F}_p[X]/(f)$ genau dann ein Körper wenn (f) irreduzibel über $\mathbb{F}_p$ ist.*

Beweis. ($\Leftarrow$) Sei $f \in \mathbb{F}_p[X]$ irreduzibel mit $\deg(f) \geq 1$. Für jedes $g \in \mathbb{F}_p[X] \setminus (f)$ finden wir mit dem vEA Polynome $h_1, h_2, d \in \mathbb{F}_p[X]$, sodass gilt $h_1f + h_2g = d$, wobei $d \mid f$ und $d \mid g$. Weil f irreduzibel ist, gilt entweder $d = f$ oder $d \in \mathbb{F}_p$ (also $\deg(d) = 0$). Im ersten Fall ist $d \in (f)$ und somit ist auch $g \in (f)$, was unserer Annahme widerspricht. Im zweiten Fall ist

$$h_1f + h_2g \equiv h_2g \equiv 1 \pmod{f}$$

(weil $\mathbb{F}_p$ ein Körper ist). Daraus folgt, dass $\bar{h}_2$ im Ring $\mathbb{F}_p[X]/(f)$ ein multiplikativ Inverses von $\bar{g} \neq \bar{0}$ ist, und weil g beliebig war, ist $\mathbb{F}_p[X]/(f)$ ein Körper.

($\Rightarrow$) Mit Kontraposition, d. h. wir nehmen an, dass (f) reduzibel ist. Mit Proposition 10.4 genügt es zu zeigen, dass (f) kein maximales Ideal ist. Ist f reduzibel, so existieren Polynome $g, h \in \mathbb{F}_p[X]$ mit $g \cdot h = f$ und $\deg(g), \deg(h) > 0$, d. h. weder g noch h ist in $\mathbb{F}_p$. Aus Faktum 12.1 folgt $\deg(f) = \deg(g) + \deg(h)$. Weil $\deg(h) > 0$, ist $\deg(g) < \deg(f)$, und mit $g \mid f$ folgt $(f) \subsetneq (g)$. Weiter erhalten wir mit $\deg(g) > 0$, dass $(g) \subsetneq \mathbb{F}_p[X]$. Also gilt $(f) \subsetneq (g) \subsetneq \mathbb{F}_p[X]$ und (f) ist kein maximales Ideal. ⊣

Korollar 12.3. *Ist $f \in \mathbb{F}_p[X]$ mit $\deg(f) = n \geq 1$ irreduzibel, so ist $\mathbb{F}_p[X]/(f)$ ein Körper der Ordnung p^n.*

Beweis. Mit Proposition 12.2 ist $\mathbb{F}_p[X]/(f)$ ein Körper und weil

$$\mathbb{F}_p[X]/(f) \cong \{g \in \mathbb{F}_p[X] : \deg(g) < n\}$$

und $|\mathbb{F}_p| = p$, hat der Körper $\mathbb{F}_p[X]/(f)$ die Ordnung p^n. ⊣

EXISTENZ VON KÖRPERN DER ORDNUNG p^n

Ein Polynom der Form $f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{F}_p[X]$ mit $a_n = 1$ heisst **normiert**. Ist $f = b_0 + b_1X + \ldots + b_nX^n \in \mathbb{F}_p[X]$ mit $b_n \neq 0$ ein irreduzibles Polynom, so ist auch $\frac{b_0}{b_n} + \frac{b_1}{b_n}X + \ldots + \frac{b_n}{b_n}X^n$ ein irreduzibles Polynom. Um die Existenz von Körpern der Ordnung p^n zu beweisen, genügt es also, die Existenz von normierten, irreduziblen Polynomen vom Grad n zu zeigen.

THEOREM 12.4. *Zu jeder positiven Zahl $n \in \mathbb{N}$ und zu jeder Primzahl p existiert ein Körper der Ordnung p^n.*

Beweis. Mit Korollar 12.3 genügt es zu zeigen, dass für jedes $n \geq 1$ und jede Primzahl p mindestens ein normiertes, irreduzibles Polynom $f \in \mathbb{F}_p[X]$ vom Grad n existiert.

Sei p prim beliebig, aber fest gewählt. Sei weiter I_n die Menge aller normierten, irreduziblen Polynome in $\mathbb{F}_p[X]$ vom Grad n, d. h.

$$I_n = \{f_{1,n}, \ldots, f_{r_n,n}\}$$

mit $f_{i,n}$ normiert, irreduzibel und $\deg(f_{i,n}) = n$. Ist $r_n = 0$, so ist $I_n = \emptyset$. Wir müssen also zeigen, dass für alle $n \geq 1$ gilt $r_n \geq 1$.

Für ein festes n betrachten wir zuerst die Menge F_n aller normierten (nicht notwendigerweise irreduziblen) Polynome beliebigen Grades, welche wir als Produkte von Polynomen $f_{i,n} \in I_n$ bilden können (beachte, dass Produkte normierter Polynome normiert sind). Der Menge F_n ordnen wir eine abzählende formale Potenzreihe zu: Mit dem Polynom $f_{i,n}$, für ein festes i $(1 \leq i \leq r_n)$, können wir die

Polynome	$f_{i,n}^0$	$f_{i,n}^1$	$f_{i,n}^2$	$\ldots$	$f_{i,n}^k$	$\ldots$	bilden, diese haben
Grad	0	n	$2n$	$\ldots$	kn	$\ldots$	und die abzählende
Potenzreihe ist	$1z^0$ +	$1z^n$ +	$1z^{2n}$ +	$\ldots$ +	$1z^{kn}$ +	$\ldots$	$= \mathrm{geo}(z^n)$.

Mit den beiden Polynomen $f_{i,n}$ und $f_{j,n}$ für $i \neq j$, können wir die

Polynome	$f_{i,n}^0 = f_{j,n}^0$	$f_{i,n}^1, f_{j,n}^1$	$f_{i,n}^2,\ f_{i,n}\cdot f_{j,n},\ f_{j,n}^2$	$\ldots$	bilden, mit
Grad	0	n	$2n$	$\ldots$	und abzählender
Potenzreihe	$1z^0$ +	$2z^n$ +	$3z^{2n}$ +	$\ldots$	$= \mathrm{geo}(z^n)^2$.

Allgemein erhalten wir für die r_n Polynome in I_n die abzählende Potenzreihe

$$\underbrace{a_0}_{=1} z^0 + a_1 z^n + a_2 z^{2n} + \ldots + a_k z^{kn} + \ldots = \mathrm{geo}(z^n)^{r_n}$$

wobei a_k die Anzahl der normierten Polynome vom Grad kn ist, welche als Produkt von Polynomen aus I_n geschrieben werden können.

Sei nun F die Menge *aller* normierten Polynome in $\mathbb{F}_p[X]$. Dann erhalten wir, mit dem vorigen Resultat, die zu F gehörende abzählende Potenzreihe

$$\psi(z) = \mathrm{geo}(z^1)^{r_1} \cdot \mathrm{geo}(z^2)^{r_2} \cdot \mathrm{geo}(z^3)^{r_3} \cdot \ldots = \prod_{n=1}^{\infty} \Big(\frac{1}{1-z^n}\Big)^{r_n}.$$

Andererseits gibt es in $\mathbb{F}_p[X]$ genau p^n normierte Polynome vom Grad n. Somit muss gelten

$$\psi(z) = 1z^0 + pz^1 + p^2z^2 + \ldots + p^nz^n + \ldots = \frac{1}{1-pz}.$$

Wir erhalten also

$$\prod_{n=1}^{\infty}\Big(\frac{1}{1-z^n}\Big)^{r_n}=\frac{1}{1-pz}\quad\text{bzw. für die reziproken Reihen}\quad\prod_{n=1}^{\infty}(1-z^n)^{r_n}=1-pz.$$

Mit logarithmischem Ableiten auf beiden Seiten erhalten wir

$$\sum_{n=1}^{\infty}\frac{D\big((1-z^n)^{r_n}\big)}{(1-z^n)^{r_n}}=\sum_{n=1}^{\infty}\frac{r_n(-nz^{n-1})(1-z^n)^{r_n-1}}{(1-z^n)^{r_n}}=\sum_{n=1}^{\infty}-\frac{r_n\cdot n}{1-z^n}z^{n-1}=$$

$$\frac{D(1-pz)}{1-pz}=\frac{-p}{1-pz}=-p\cdot\mathrm{geo}(pz)=\sum_{n=1}^{\infty}-p^nz^{n-1},$$

also

$$\sum_{n=1}^{\infty}\frac{r_n\cdot n}{1-z^n}z^{n-1}=\sum_{n=1}^{\infty}p^nz^{n-1}$$

Entwickeln wir die Summe auf der linke Seite, so erhalten wir:

$$\begin{array}{ccccccccccccccccccc}
r_1 & + & r_1z & + & r_1z^2 & + & r_1z^3 & + & r_1z^4 & + & r_1z^5 & + & r_1z^6 & + & r_1z^7 & + & r_1z^8 & + & \dots\\
 & & 2r_2z & + & & & 2r_2z^3 & + & & & 2r_2z^5 & + & & & 2r_2z^7 & + & & + & \dots\\
 & & & & 3r_3z^2 & + & & & & & 3r_3z^5 & + & & & & & 3r_3z^8 & + & \dots\\
 & & & & & & 4r_4z^3 & + & & & & & & & 4r_4z^7 & + & & & \dots\\
 & & & & & & & & 5r_5z^4 & + & & & & & & & & & \dots\\
 & & & & & & & & & & 6r_6z^5 & + & & & & & & & \dots\\
 & & & & & & & & & & & & 7r_7z^6 & + & & & & & \dots\\
 & & & & & & & & & & & & & & \dots & & & & \dots
\end{array}$$

Addieren wir spaltenweise, so erhalten wir

$$\sum_{n=1}^{\infty}\frac{r_n\cdot n}{1-z^n}z^{n-1}=\sum_{n=1}^{\infty}\Big(\sum_{d|n}d\cdot r_d\Big)\cdot z^{n-1}=\sum_{n=1}^{\infty}p^nz^{n-1}$$

und mit Koeffizientenvergleich erhalten wir:

$$\sum_{d|n}d\cdot r_d=p^n$$

Setzen wir $g(d):=d\cdot r_d$ und $f(n):=p^n$, so ist $\sum_{d|n}g(d)=f(n)$ und mit Aufgabe 49 gilt:

$$g(n)=\sum_{d|n}\mu(d)\cdot f(n/d),\quad\text{d. h.}\quad\underbrace{n\cdot r_n}_{=g(n)}=\sum_{d|n}\mu(d)\cdot\underbrace{p^{n/d}}_{=f(n/d)}\quad\text{also}\quad r_n=\frac{1}{n}\cdot\sum_{d|n}\mu(d)\cdot p^{n/d}.$$

Nach Definition ist $\mu(1)=1$ und allgemein $\mu(d)\in\{-1,0,1\}$, woraus folgt

$$n\cdot r_n=p^n+\ldots+\mu(n)p\geq p^n-\sum_{k=1}^{n-1}p^k\geq 2.$$

Insbesondere ist für alle $n\geq 1$, $n\cdot r_n\geq 2$, also $r_n\geq 1$, was zu zeigen war. ⊣

Beispiele:

- $r_1 = p$: Die p normierten, irreduziblen Polynome vom Grad 1 über $\mathbb{F}_p$ sind X, $X+1$, $\ldots$, $X+(p-1)$.
- $r_2 = \frac{1}{2}(p^2-p)$: $\frac{1}{2}\sum_{d|2}\mu(d)p^{2/d} = \frac{1}{2}(p^2+\mu(2)p) = \frac{1}{2}(p^2-p)$
- $r_3 = \frac{1}{3}(p^3-p)$: $\frac{1}{3}\sum_{d|3}\mu(d)p^{3/d} = \frac{1}{3}(p^3+\mu(3)p) = \frac{1}{4}(p^3-p)$
- $r_4 = \frac{1}{4}(p^4-p^2)$: $\frac{1}{4}\sum_{d|4}\mu(d)p^{4/d} = \frac{1}{4}(p^4+\mu(2)p^2+\mu(4)p) = \frac{1}{4}(p^4-p^2)$
- $r_5 = \frac{1}{5}(p^5-p)$: $\frac{1}{5}\sum_{d|5}\mu(d)p^{5/d} = \frac{1}{5}(p^5+\mu(5)p) = \frac{1}{5}(p^5-p)$
- $r_6 = \frac{1}{6}(p^6-p^3-p^2+p)$: $\frac{1}{6}\sum_{d|6}\mu(d)p^{6/d} = \frac{1}{6}(p^6+\underbrace{\mu(2)}_{=-1}p^3+\underbrace{\mu(3)}_{=-1}p^2+\underbrace{\mu(6)}_{=1}p)$
- Für $p=3$ erhalten wir
$$r_1 = 3, \quad r_2 = 3, \quad r_3 = 8, \quad r_4 = 18, \quad r_5 = 48, \quad r_6 = 116,$$
und für $p=7$ erhalten wir
$$r_1 = 7, \quad r_2 = 21, \quad r_3 = 112, \quad r_4 = 588.$$
- Die 21 normierten irreduziblen Polynome vom Grad 2 über $\mathbb{F}_7$ sind:
  0. X^2+1
  1. X^2+2
  2. X^2+4
  3. X^2+X+3
  4. X^2+X+4
  5. X^2+X+6
  6. X^2+2X+2
  7. X^2+2X+3
  8. X^2+2X+5
  9. X^2+3X+1
  10. X^2+3X+5
  11. X^2+3X+6
  12. X^2+4X+1
  13. X^2+4X+5
  14. X^2+4X+6
  15. X^2+5X+2
  16. X^2+5X+3
  17. X^2+5X+5
  18. X^2+6X+3
  19. X^2+6X+4
  20. X^2+6X+6
- Das Polynom $f = X^{100}+X^6+X^5+X^2+1$ ist irreduzibel über $\mathbb{F}_2$ und somit ist $\mathbb{F}_2[X]/(f)$ ein Körper der Ordnung $2^{100} = 1\,267\,650\,600\,228\,229\,401\,496\,703\,205\,376$.