16. Endliche Körper

Lemma 16.1 Ist K ein endlicher Körper mit m Elementen, so ist $m = p^n$ für $p, n \in \mathbb{N}$, $n \geq 1$ und p prim.

Beweis: Sei $p = \text{char}(K)$, dann ist p prim und $\mathbb{F}_p \subseteq K$, wobei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Primkörper von K ist.

- Somit ist K eine endl. Körpererweiterung von $\mathbb{F}_p$.
- Ist $[K : \mathbb{F}_p] = n$, dann ex. Basis $a_1, \ldots, a_n$ des Vektorraums K über $\mathbb{F}_p$, und jedes Element aus K lässt sich eindeutig schreiben als Linearkombination $k_1 \cdot a_1 + k_2 \cdot a_2 + \ldots + k_n \cdot a_n$ mit $k_i \in \mathbb{F}_p$ ($|\mathbb{F}_p| = p$).
- Es gibt p^n solche Lin.-Komb. und somit hat K p^n Elemente. ⊣

Lemma 16.2 Ist $f \in \mathbb{F}_p[X]$ irred. über $\mathbb{F}_p$ (p prim) mit $\text{grad}(f) = n \geq 1$, so ist $\mathbb{F}_p[X]/(f)$ ein Körper mit p^n Elementen.

Beweis: Mit Thm. 12.8 ist $\mathbb{F}_p[X]$ ein Hauptidealring und weil f irred. ist, ist (f) maximal, also ist mit Prp. 11.2 $\mathbb{F}_p[X]/(f)$ ein Körper.

- Die Elemente von $\mathbb{F}_p[X]/(f)$ sind die Nebenklassen $\bar{g}$ der Polynome $g \in \mathbb{F}_p[X]$ mit $\text{grad}(g) \leq n-1$; von diesen gibt es p^n. ⊣

Theorem 16.3 Zu jedem positiven $n \in \mathbb{N}$ und jeder Primzahl p existiert bis auf Isomorphie genau ein Körper mit p^n Elementen.

Beweis: Die Eindeutigkeit (bis auf Isomorphie) wird in Aufgabe 95 gezeigt. Mit Lem. 16.2 genügt es somit zu zeigen, dass für alle $n \geq 1$ und p prim immer ein irred. Polynom $f \in \mathbb{F}_p[X]$ mit $\operatorname{grad}(f) = n$ existiert.

[Beweis mit formalen Potenzreihen, generierenden Funktionen und Möbiusfunktion.]

- Sei p prim beliebig, aber fest gewählt.
- Sei I_n die Menge der normierten, irred. Polynome (in $\mathbb{F}_p[X]$) vom Grad n. D.h. $I_n = \{f_{1,n}, \dots, f_{r_n,n}\}$ mit $f_{i,n}$ norm., irred. Polynom vom Grad n. Ist $r_n = 0$, so ist $I_n = \emptyset$. Wir müssen also zeigen: $r_n \geq 1$ für alle $n \geq 1$.
- Für ein festes n betrachten wir die normierten Polynome beliebigen Grades, die wir mit Polynomen $f_{i,n} \in I_n$ bilden können, und ordnen dieser Menge eine abzählende formale Potenzreihe zu:

  Mit dem Polynom $f_{i,n}$ (für ein festes i) können wir die Polynome $f_{i,n}^0, f_{i,n}^1, f_{i,n}^2, \dots, f_{i,n}^k, \dots$ bilden, diese haben Grad: $0, n, 2n, \dots, kn, \dots$ und die abzählende Potenzreihe ist: $1 \cdot z^0 + 1 \cdot z^n + 1 \cdot z^{2n} + \dots + 1 \cdot z^{kn} + \dots = \frac{1}{1-z^n}$ (geom. Reihe)

  Mit den beiden Polynomen $f_{i,n}, f_{j,n}$ (für $i \neq j$) können wir die Polynome $f_{i,n}^0 = f_{j,n}^0$; $f_{i,n}^1, f_{j,n}^1$; $f_{i,n}^2, f_{i,n}^1 \cdot f_{j,n}^1, f_{j,n}^2$; ... bilden, diese haben Grad: $0, n, 2n, \dots$ und die abz. Potenreihe ist: $1 \cdot z^0 + 2z^n + 3z^{2n} + \dots = \left(\frac{1}{1-z^n}\right)^2$

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

$$\left(\frac{1}{1-z^n}\right)^{r_n} = \overbrace{1}^{=a_0} \cdot z^0 + a_1 \cdot z^n + a_2 z^{2n} + \dots + a_k \cdot z^{kn} + \dots$$

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

- Sei F die Menge der <u>normierten</u> Polynome in $\mathbb{F}_p[X]$. Dann erhalten wir, mit dem vorherigen Resultat, die zu F gehörende alsz. Potenzreihe

$$\varphi(z) = \left(\frac{1}{1-z^1}\right)^{r_1} \cdot \left(\frac{1}{1-z^2}\right)^{r_2} \cdot \ldots = \prod_{n=1}^{\infty} \left(\frac{1}{1-z^n}\right)^{r_n}$$

- Andererseits gibt es in $\mathbb{F}_p[X]$ genau p^n normierte Polynome vom Grad n, und somit muss gelten:

$$\varphi(z) = 1 \cdot z^0 + p z^1 + p^2 z^2 + \ldots = \frac{1}{1-pz}$$

- Wir erhalten also:

$$\prod_{n=1}^{\infty} \left(\frac{1}{1-z^n}\right)^{r_n} = \frac{1}{1-pz}$$

und für die Reziproken Reihen gilt:

$$\prod_{n=1}^{\infty} (1-z^n)^{r_n} = 1 - pz \quad \| \ln$$

$$\sum_{n=1}^{\infty} r_n \ln(1-z^n) = \ln(1-pz) \quad \| \frac{d}{dz}$$

$$\sum_{n=1}^{\infty} \frac{r_n \cdot n}{1-z^n} \cdot z^{n-1} = \underbrace{\frac{p}{1-pz}}_{= p \cdot (1 + pz + p^2 z^2 + \ldots)} = \sum_{n=1}^{\infty} p^n \cdot z^{n-1}$$

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

$$\begin{aligned}
&r_1 + r_1 z + r_1 z^2 + r_1 z^3 + r_1 z^4 + r_1 z^5 + r_1 z^6 + r_1 z^7 + r_1 z^8 + \ldots \\
&\quad 2r_2 z + \quad 2r_2 z^3 + \quad 2r_2 z^5 + \quad 2r_2 z^7 + \ldots \\
&\quad\quad 3r_3 z^2 + \quad\quad 3r_3 z^5 + \quad\quad 3r_3 z^8 + \ldots \\
&\quad\quad\quad 4r_4 z^3 + \quad\quad\quad 4r_4 z^7 + \ldots \\
&\quad\quad\quad\quad 5r_5 z^4 + \quad\quad\quad\quad \ldots \\
&\quad\quad\quad\quad\quad 6r_6 z^5 + \quad\quad\quad\quad \ldots \\
&\quad\quad\quad\quad\quad\quad 7r_7 z^6 + \quad\quad\quad\quad \ldots \\
&\quad\quad\quad\quad\quad\quad\quad 8r_8 z^7 + \quad\quad\quad\quad \ldots \\
&\quad\quad\quad\quad\quad\quad\quad\quad 9r_9 z^8 + \ldots \\
&\quad\quad\quad\quad\quad\quad\quad\quad\quad \ldots
\end{aligned}$$

Addieren wir kolonnenweise, so erhalten wir:

$$\sum_{n=1}^{\infty} \frac{r_n \cdot n}{1-z^n} \cdot z^{n-1} = \sum_{n=1}^{\infty} \underbrace{\left(\sum_{d|n} d \cdot r_d\right)}_{=} \cdot z^{n-1} \overset{!}{=} \sum_{n=1}^{\infty} \underbrace{p^n}_{=} \cdot z^{n-1}$$

Mit Koeffizientenvergleich erhalten wir die Gleichung:

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

Setzen wir $g(d) := r_d$ und $f(n) := p^n$

so ist $\sum_{d|n} d \cdot g(d) = f(n)$ und mit Aufgabe 94 gilt:

$$\underbrace{r_n}_{g(n)} = \sum_{d|n} \mu(d) \cdot \underbrace{p^{n/d}}_{f(n/d)}$$

Nach Def. von $\mu(d)$ ist

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

$\mu(d) \in \{-1, 0, 1\}$

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

<u>Beispiele</u>: • $r_1 = p$; irred. Polynome $X, X+1, \ldots, X+(p-1)$

$r_2 = \frac{1}{2}(p^2 - p)$

$r_3 = \frac{1}{3}(p^3 - p)$

$r_4 = \frac{1}{4}(p^4 - p^2)$

• Für $p = 7$ erhält man z.B. $r_1 = 7$, $r_2 = 21$, $r_3 = 112$, $r_4 = 588$.