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 Möbius-funktion.]

- 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. Potenzreihe 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 zugeh. 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:

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

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

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

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

Potenzen von z: z^0 z^1 z^2 z^3

$$r_1 + r_1 z + r_1 z^2 + r_1 z^3 + r_1 z^4 + r_1 z^5 + r_1 z^6 + r_1 z^7 + r_1 z^8 + \ldots$$

ohne Potenzen von z, nur Koeff. von r_n:

Spalte: 1 2 3 4 5 6 7 8

1	1	1	1	1	1	.	.
	2		2		2	.	.
		3			3		
			4				4
			.	.			

$$2r_2 z + 2r_2 z^3 + 2r_2 z^5 + 2r_2 z^7 + \ldots$$

$$3r_3 z^2 + 3r_3 z^5 + 3r_3 z^8 + \ldots$$

$$4r_4 z^3 + 4r_4 z^7 + \ldots$$

$$5r_5 z^4 + \ldots$$

$$6r_6 z^5 + \ldots$$

$$7r_7 z^6 + \ldots$$

$$8r_8 z^7 + \ldots$$

$$9r_9 z^8 + \ldots$$

$$\ldots$$

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 $g(d) := r_d \cdot d$ und $f(n) := p^n$

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

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

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

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

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

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

also $r_n \geq 1$

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

$r_2 = \frac{1}{2}(p^2-p) = \frac{1}{2} \cdot \sum_{d|2} \mu(d) \cdot p^{2/d} = \frac{1}{2} \cdot (p^2 + \mu(2) \cdot p) = \frac{1}{2}(p^2-p)$

$r_3 = \frac{1}{3}(p^3-p) = \frac{1}{3} \cdot \sum_{d|3} \mu(d) \cdot p^{3/d} = \frac{1}{3} \cdot (p^3 + \mu(3) \cdot p) = \frac{1}{3} \cdot (p^3-p)$

$r_4 = \frac{1}{4}(p^4-p^2) = \frac{1}{4} \cdot \sum_{d|4} \mu(d) \cdot p^{4/d} = \frac{1}{4} \cdot (p^4 + \mu(2) \cdot p^2 + \underbrace{\mu(4)}_{=0} \cdot p) = \frac{1}{4} \cdot (p^4-p^2)$

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

Proposition 16.4 Ist $a \in L$ ($L \supseteq \mathbb{F}_p$) eine Nullstelle des Polynoms $h \in \mathbb{F}_p[X]$, so ist auch $a^p \in L$ eine Nullstelle von h.

Beweis: Es gilt $0 = h(a) = h(a)^p = (\overbrace{b_0 + b_1 a + \ldots + b_n a^n}^{h(a)})^p$ $(b_i \in \mathbb{F}_p)$

$$\overset{\text{Aufg. 98.(a)}}{=} b_0^p + b_1^p a^p + \ldots + b_n (a^p)^n$$

$$\overset{\text{Aufg. 98.(b)}}{=} b_0 + b_1 a^p + \ldots + b_n (a^p)^n = 0$$

und somit ist a^p eine Nullstelle von h. ⊣

Satz 16.5 Sei p prim und $h \in \mathbb{F}_p[X]$ ein irred. Polynom über $\mathbb{F}_p$ mit $\operatorname{grad}(h) = m \geq 2$.

(a) Ist a eine Nullstelle von h in $L \supseteq \mathbb{F}_p$, so sind $a^{p^0}, a^{p^1}, \ldots, a^{p^{m-1}}$ die m paarweise verschiedenen Nullstellen von h in L, d.h. h zerfällt in L in Linearfaktoren.

(b) Ist $a \in \mathbb{F}_{p^n}$, so gilt $m \mid n$.

Beweis: (a) Mit Prp. 16.4 sind $a^{p^0}, \ldots, a^{p^{m-1}}$ Nullstellen von h.

Wir zeigen zuerst, dass die Nullstellen paarweise versch. sind.

- Sei $1 \leq k \leq m$ die kl. Zahl mit $a = a^{p^k}$. Dann sind $a, a^p, \ldots, a^{p^{k-1}}$ paarweise versch.
- Zu zeigen: $m = k$

  In L definieren wir $g := \prod_{i=0}^{k-1} (X - a^{p^i})$.

  Dann folgt einerseits $(g)^p = (b_0 + b_1 X + \ldots + \overbrace{b_{k-1}}^{=1} X^{k-1})^p$ $(b_i \in L)$

  $$= b_0^p + b_1^p \underbrace{X^p}_{=:Y} + \ldots + \underbrace{b_{k-1}^p}_{=1} \underbrace{(X^{k-1})^p}_{=Y^{k-1}}$$

  weil $\operatorname{char}(L) = p$.

  Setzen wir $Y := X^p$, so entspricht $(g)^p$ dem Polynom $\tilde{g} \in L[Y]$ mit $\operatorname{grad}(g) = \operatorname{grad}(\tilde{g}) = k-1$.

Andererseits werden die Nullstellen von g durch das Potenzieren nur zyklisch permutiert. D.h. g und $\tilde{g}$ haben dieselben Nullstellen, und weil g und $\tilde{g}$ über L in Linearfaktoren zerfallen, gilt für alle $0 \leq i < k$, $b_i^p = b_i$ und mit Aufg. 98.(b) erhalten wir $b_i \in \mathbb{F}_p$.

Somit ist $g \in \mathbb{F}_p[X]$ und nach Konstruktion von g gilt $g \mid h$, und weil h irred. über $\mathbb{F}_p$ ist, ist $g = h$ und $k = m$.

(b) Ist $a \in \mathbb{F}_{p^n}$, so ist mit Aufg. 95.(a) sowohl a wie auch $a^p, \dots, a^{p^{m-1}}$ Nullstellen von $X^{p^n} - X$. Wir nehmen an, h sei normiert (damit ändert sich der Grad von h nicht).
Dann gilt $h \mid X^{p^n} - X$. Sei $K_h := \mathbb{F}_p(a) \cong \mathbb{F}_p[X]/(h)$.
Dann ist $|K_h| = p^m$ und es gilt, weil $K_h \subseteq \mathbb{F}_{p^n}$,

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : K_h] \cdot \underbrace{[K_h : \mathbb{F}_p]}_{= m}, \quad \text{also } m \mid n.$$

Korollar 16.6 Das Polynom $X^{p^n} - X$ ist über $\mathbb{F}_p$ das Produkt aller normierten irred. Polynome vom Grad m mit $m \mid n$. Insbesondere ist die Summe der Grade dieser irred. Polynome gleich p^n.

[Beweis in den Übungen]

Proposition 16.7 Für jeden endlichen Körper K ist die Abbildung

$$\begin{aligned} K &\longrightarrow K \\ a &\longmapsto a^p \end{aligned}$$

mit $p = \mathrm{char}(K)$ ein Automorphismus; die Abbildung $a \mapsto a^p$ heißt Frobeniushomomorphismus.

[Beweis in den Übungen]