KAPITEL 8

Endliche Körper

Bemerkungen: Die folgenden Aussagen sind bereits bekannt:

(1) Ist K ein endlicher Körper, so gibt es eine Primzahl p mit

$$\sum_{i=1}^{k} 1 \neq 0 \text{ in } K \text{ für } k = 1, \ldots, p-1 \quad \text{und} \quad \sum_{i=1}^{p} 1 = 0 \text{ in } K.$$

Daher können wir $\mathbb{F}_p$ als Unterkörper von K auffassen:

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\} \subseteq K.$$

Man sagt, K hat Charakteristik p.

(2) K ist ein $\mathbb{F}_p$-Vektorraum, es gibt also eine $\mathbb{F}_p$-Basis $\omega_1, \ldots, \omega_n \in K$ von K über $\mathbb{F}_p$:

$$K = \{a_1\omega_1 + \cdots + a_n\omega_n : a_1, \ldots, a_n \in \mathbb{F}_p\}.$$

Dann gilt $[K : \mathbb{F}_p] = n$ und

$$|K| = p^n.$$

(3) Ist $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$, so gibt es einen Körperhomomorphismus $\sigma : K \to \overline{\mathbb{F}}_p$, das Bild $\sigma(K)$ ist ein zu K isomorpher Körper. Wir können also K als Teilmenge von $\overline{\mathbb{F}}_p$ auffassen:

$$\mathbb{F}_p \subseteq K \subseteq \overline{\mathbb{F}}_p.$$

(4) Die Abbildung $\pi : K \to K$ mit $\pi(\alpha) = \alpha^p$ erfüllt

$$(\alpha + \beta)^p = \alpha^p + \beta^p, \quad (\alpha\beta)^p = \alpha^p\beta^p, \quad 1^p = 1,$$

definiert daher einen Körperautomorphismus von K:

$$\pi \in \mathrm{Aut}(K|\mathbb{F}_p).$$

π wird **Frobenius-Automorphismus** genannt.

(5) Ist $\alpha \in K \setminus \{0\}$, so ist α ein Element der multiplikativen Gruppe K^*. Aus $\mathrm{ord}\,(\alpha) \mid |K^*|$ folgt dann $\alpha^{p^n-1} = 1$, also

$$\alpha^{p^n} = \alpha.$$

Die letzte Gleichung gilt natürlich auch für $\alpha = 0$. Daher gilt:

$$K \subseteq \{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} - \alpha = 0\}.$$

Da die rechte Seite die Nullstellenmenge des Polynoms $x^{p^n} - x$ (vom Grad p^n) ist, gilt sogar Gleichheit, da $x^{p^n} - x$ natürlich höchstens p^n Nullstellen hat:

$$K = \{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} = \alpha\}.$$

Von der letzten Aussage gilt auch die Umkehrung.

SATZ. *Sei p eine Primzahl und $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$. Für $n \in \mathbb{N}$ sei*

$$\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} = \alpha\}.$$

Dann gilt:

(1) *$\mathbb{F}_{p^n}$ ist ein Körper mit p^n Elementen. Elementen, nämlich $\mathbb{F}_{p^n}$.*

(2) *$\mathbb{F}_{p^n}$ ist normal und separabel über $\mathbb{F}_p$ vom Grad n, $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Insbesondere ist $\mathbb{F}_{p^n}$ galoissch über $\mathbb{F}_p$.*

Datei: kt_ek.tex. Version vom 1.7.2024

(3) *Für den Frobenius-Automorphismus*

$$\pi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \text{ mit } \pi(\alpha) = \alpha^p$$

gilt

$$\pi^k(\alpha) = \alpha^{p^k} \text{ für } k = 0, 1, 2, \ldots \quad \text{und} \quad \operatorname{ord}(\pi) = n.$$

(4) *Die Galoisgruppe von $\mathbb{F}_{p^n}$ über $\mathbb{F}_p$ ist zyklisch von der Ordnung n, erzeugt vom Frobenius-Automorphismus:*

$$\operatorname{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) = \langle \pi \rangle.$$

Beweis:

(1) (a) Wir zeigen zunächst mit dem Unterkörper-Kriterium, dass $\mathbb{F}_{p^n}$ ein Unterkörper von $\overline{\mathbb{F}}_p$, und damit ein Körper ist. Wir schauen uns die einzelnen Punkte des Unterkörper-Kriteriums an:

(i) $0 \in \mathbb{F}_{p^n}$: Klar.

(ii) $\alpha, \beta \in \mathbb{F}_{p^n} \Longrightarrow \alpha + \beta \in \mathbb{F}_{p^n}$: Aus $\alpha^{p^n} = \alpha$ und $\beta^{p^n} = \beta$ folgt mit der Additivität der p-Potenzierung in Charakteristik p

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta, \quad \text{also} \quad \alpha + \beta \in \mathbb{F}_{p^n}.$$

(iii) $\alpha \in \mathbb{F}_{p^n} \Longrightarrow -\alpha \in \mathbb{F}_{p^n}$: Gilt $\alpha^{p^n} = \alpha$, so folgt

$$(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n} = (-1)^{p^n}\alpha = \begin{cases} -\alpha & \text{für } p > 2, \\ \alpha = -\alpha & \text{für } p = 2, \end{cases}$$

also $-\alpha \in \mathbb{F}_{p^n}$.

(iv) $1 \in \mathbb{F}_{p^n}$: Klar.

(v) $\alpha, \beta \in \mathbb{F}_{p^n} \Longrightarrow \alpha\beta \in \mathbb{F}_{p^n}$: Aus $\alpha^{p^n} = \alpha$ und $\beta^{p^n} = \beta$ folgt natürlich

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta, \quad \text{also} \quad \alpha\beta \in \mathbb{F}_{p^n}.$$

(vi) $\alpha \in \mathbb{F}_{p^n} \setminus \{0\} \Longrightarrow \frac{1}{\alpha} \in \mathbb{F}_{p^n}$: Aus $\alpha^{p^n} = \alpha$ folgt

$$\frac{1}{\alpha} = \frac{\alpha}{\alpha^2} = \frac{\alpha^{p^n}}{\alpha^2} = \alpha^{p^n - 2} \in \mathbb{F}_{p^n}.$$

Daher ist $\mathbb{F}_{p^n}$ ein Körper.

(b) Für $f = x^{p^n} - x \in \mathbb{F}_p[x]$ gilt

$$\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}}_p : f(\alpha) = 0\}.$$

Nun ist aber $f' = -1$, also $\operatorname{ggT}(f, f') = 1$. Das Polynom f ist separabel, weswegen f genau $p^n = \operatorname{grad}(f)$ Nullstellen in $\overline{\mathbb{F}}_p$ hat. Also ist $|\mathbb{F}_{p^n}| = p^n$, d.h. $\mathbb{F}_{p^n}$ ist ein Körper mit p^n Elementen.

(2) $\mathbb{F}_{p^n}$ ist der Zerfällungskörper von $f = x^{p^n} - x$ über $\mathbb{F}_p$, also normal über $\mathbb{F}_p$. Da jedes Element von $\mathbb{F}_{p^n}$ Nullstelle des separablen Polynoms f ist, ist $\mathbb{F}_{p^n}$ über $\mathbb{F}_p$ auch separabel. (Dies wurde aber schon früher bewiesen.) Damit ist $\mathbb{F}_{p^n}|\mathbb{F}_p$ auch galoissch.

(3) Dass π ein Körperautomorphismus ist, haben wir bereits gesehen. Nun zeigen wir durch Induktion, dass $\pi^k(\alpha) = \alpha^{p^k}$ gilt. Für $k = 0$ und $k = 1$ ist die Formel klar. Sei nun die Formel bereits für k bewiesen. Dann folgt für $k + 1$

$$\pi^{k+1}(\alpha) = \pi^k(\pi(\alpha)) = \pi^k(\alpha^p) = (\alpha^p)^{p^k} = \alpha^{p^{k+1}},$$

was gezeigt werden sollte.
Für $\alpha \in \mathbb{F}_{p^n}$ gilt $\alpha^{p^n} = \alpha$, also

$$\pi^n(\alpha) = \alpha^{p^n} = \alpha = \mathrm{id}(\alpha), \quad \text{und damit} \quad \pi^n = \mathrm{id}.$$

Ist umgekehrt π^k die Identität, so gilt

$$\alpha^{p^k} = \alpha \text{ für alle } \alpha \in K_n.$$

Jedes α aus $\mathbb{F}_{p^n}$ ist also Nullstelle des Polynoms $x^{p^k}-x$. Da das Polynom höchstens p^k Nullstellen hat, folgt $|\mathbb{F}_{p^n}| \leq p^k$, also $k \geq n$. Dies zeigt, dass n minimal (in $\mathbb{N}$) ist mit $\pi^n = \mathrm{id}$. Daher folgt

$$\mathrm{ord}\,(\pi) = n.$$

(4) Aus $|\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p)| = n$ und $\mathrm{ord}\,(\pi) = n$ folgt, dass $\langle\pi\rangle$ schon die ganze Galoisgruppe ist. Dies zeigt die Behauptung. ■

Wir können nun alle endlichen Körper der Charakteristik p beschreiben:

SATZ. *Sei p eine Primzahl und $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$. Dann gilt:*

(1) *Für jedes $n \in \mathbb{N}$ gibt es genau einen endlichen Körper der Ordnung p^n in $\overline{\mathbb{F}}_p$, nämlich*

$$\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} = \alpha\}.$$

(2) *Die endlichen Unterkörper von $\overline{\mathbb{F}}_p$ sind genau die Körper $\mathbb{F}_{p^n}$ für $n \in \mathbb{N}$.*

(3) *Für $m, n \in \mathbb{N}$ gilt:*

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \quad \Longleftrightarrow \quad m \mid n.$$

(4) *Für $m, n \in \mathbb{N}$ gilt:*

$$\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^{\mathrm{ggT}(m,n)}} \quad \textit{und} \quad \mathbb{F}_{p^m}\mathbb{F}_{p^n} = \mathbb{F}_{p^{\mathrm{kgV}(m,n)}}.$$

(Dabei ist $\mathbb{F}_{p^m}\mathbb{F}_{p^n}$ das Kompositum der Körper $\mathbb{F}_{p^m}$ und $\mathbb{F}_{p^n}$, also der kleinste Teilkörper von $\overline{\mathbb{F}}_p$, der sowohl $\mathbb{F}_{p^m}$ als auch $\mathbb{F}_{p^n}$ enthält.)

Beweis:

(1) Dies folgt aus den einführenden Bemerkungen und dem letzten Satz.

(2) Ist $K \subseteq \overline{\mathbb{F}}_p$ ein endlicher Körper, so ist K ein endlicher $\mathbb{F}_p$-Vektorraum, also gibt es ein $n \in \mathbb{N}$ mit $|K| = p^n$. Die Behauptung folgt dann aus (1).

(3)
- $\Longrightarrow$ Gilt $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, so können wir $\mathbb{F}_{p^n}$ als Erweiterungskörper von $\mathbb{F}_{p^m}$ auffassen. Ist $d = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$, so ist $\mathbb{F}_{p^n}$ ein d-dimensionaler $\mathbb{F}_{p^m}$-Vektorraum. Daher folgt
$$p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d = (p^m)^d = p^{md}, \quad \text{also} \quad n = md,$$
und damit $m \mid n$, wie behauptet.
- $\Longleftarrow$ Es gelte $m \mid n$, d.h. es gibt ein $d \in \mathbb{N}$ mit $n = dm$. Damit erhalten wir:
$$\begin{aligned}
\alpha \in \mathbb{F}_{p^m} &\Longrightarrow \alpha^{p^m} = \alpha \Longrightarrow \\
&\Longrightarrow \alpha^{p^{2m}} = (\alpha^{p^m})^{p^m} = \alpha^{p^m} = \alpha \Longrightarrow \\
&\Longrightarrow \alpha^{p^{3m}} = (\alpha^{p^{2m}})^{p^m} = \alpha^{p^m} = \alpha \Longrightarrow \\
&\ \ \vdots \\
&\Longrightarrow \alpha^{p^n} = \alpha^{p^{dm}} = (\alpha^{p^{(d-1)m}})^{p^m} = \alpha^{p^m} = \alpha \Longrightarrow \\
&\Longrightarrow \alpha \in \mathbb{F}_{p^n}.
\end{aligned}$$
Dies beweist $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

(4) Für $d \in \mathbb{N}$ gilt:
$$\begin{aligned}
\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} &\Longleftrightarrow \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^m} \text{ und } \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n} \Longleftrightarrow \\
&\Longleftrightarrow d \mid m \text{ und } d \mid n \Longleftrightarrow d \mid \mathrm{ggT}(m,n).
\end{aligned}$$
Da der Durchschnitt $\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n}$ ein Körper ist, folgt die Behauptung aus der letzten Äquivalenz. $\mathbb{F}_{p^m}\mathbb{F}_{p^n}$ ist das Kompositum der beiden Körper. Für $d \in \mathbb{N}$ gilt:
$$\begin{aligned}
\mathbb{F}_{p^m}\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^d} &\Longleftrightarrow \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^d} \text{ und } \mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^d} \Longleftrightarrow \\
&\Longleftrightarrow m \mid d \text{ und } n \mid d \Longleftrightarrow \mathrm{kgV}(m,n) \mid d.
\end{aligned}$$
Wie eben folgt die Behauptung. ■

Wir betrachten nun einen Körper $\mathbb{F}_{p^n}$ und sammeln dafür obige Aussagen:

SATZ. *Sei p eine Primzahl und $n \in \mathbb{N}$. Dann ist*

$$\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) = \langle \pi \rangle \text{ mit } \mathrm{ord}\,(\pi) = n.$$

(1) *Die Unterkörper von $\mathbb{F}_{p^n}$ sind genau die Körper $\mathbb{F}_{p^d}$ mit $d \mid n$.*
(2) *Gilt $d \in \mathbb{N}$ und $d \mid n$, so ist*

$$\mathbb{F}_{p^d} = \mathbb{F}_{p^n}^{\langle \pi^d \rangle}, \quad [\mathbb{F}_{p^d} : \mathbb{F}_p] = d.$$

(3) *Sei $\beta \in \mathbb{F}_{p^n}$. Dazu sei $d \in \mathbb{N}$ minimal mit*

$$\pi^d(\beta) = \beta,$$

also sind die Elemente $\beta, \pi(\beta), \ldots, \pi^{d-1}(\beta)$ paarweise verschieden. Dann gilt

$$d \mid n, \quad \mathbb{F}_p(\beta) = \mathbb{F}_{p^n}^{\langle \pi^d \rangle} \quad \text{und} \quad [\mathbb{F}_p(\beta) : \mathbb{F}_p] = d.$$

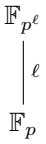
Definiert man

$$f = (x-\beta)(x-\pi(\beta))(x-\pi^2(\beta))\ldots(x-\pi^{d-1}(\beta)),$$

so hat f Koeffizienten in $\mathbb{F}_p$ und ist das Minimalpolynom von β über $\mathbb{F}_p$.

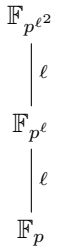
Beispiele: Wir betrachten ein paar Unterkörperdiagramme:

(1) Ist $n = \ell$ eine Primzahl, so hat n genau die Teiler $1, \ell$. Es gibt nur die Unterkörper $\mathbb{F}_p$ und $\mathbb{F}_{p^\ell}$:



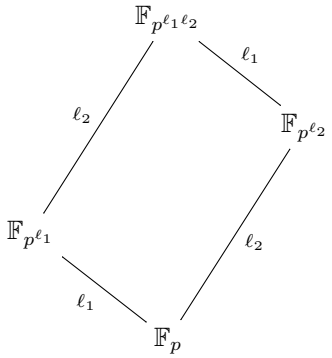
Beispiele sind $n = 2, 3, 5, 7, \ldots$

(2) Ist ℓ eine Primzahl und $n = \ell^2$, so hat n die Teiler $1, \ell, \ell^2$. Es gibt also die Unterkörper $\mathbb{F}_p$, $\mathbb{F}_{p^\ell}$ und $\mathbb{F}_{p^{\ell^2}}$:



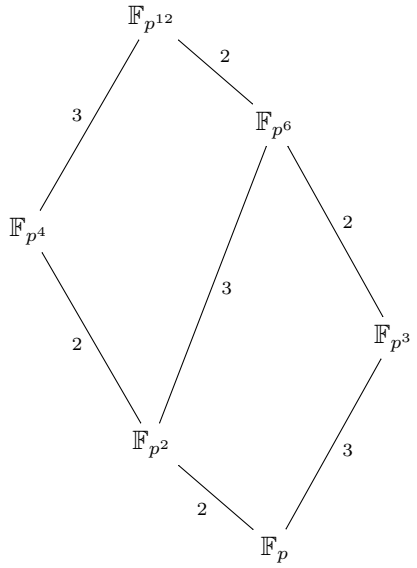
Beispiele sind $n = 4, 9, \ldots$

(3) Ist $n = \ell_1\ell_2$ mit zwei verschiedenen Primzahlen ℓ_1 und ℓ_2, so hat n genau die Teiler $1, \ell_1, \ell_2, \ell_1\ell_2$. Wir erhalten folgendes Unterkörperdiagramm:



Beispiele sind $n = 6, 10, 15, \ldots$

(4) $n = 12$. Die Teiler von 12 sind $1, 2, 3, 4, 6, 12$. Wir erhalten folgendes Unterkörperdiagramm:



Beispiel: Das Polynom $f = x^6 + x + 2 \in \mathbb{F}_5[x]$ ist irreduzibel, also ist $\mathbb{F}_{p^6} = \mathbb{F}_p(\alpha)$ mit $f(\alpha) = 0$. Es ist

$$\alpha^6 = 3 + 4\alpha.$$

- Wir betrachten $\beta = \alpha + \pi^2(\alpha) + \pi^4(\alpha)$. Es ist

$$\begin{aligned} \beta &= 3\alpha + 3\alpha^2 + 4\alpha^4 + 2\alpha^5, \\ \pi(\beta) &= 2\alpha + 2\alpha^2 + \alpha^4 + 3\alpha^5, \\ \pi^2(\beta) &= \beta. \end{aligned}$$

  Es ist

$$f = (x - \beta)(x - \pi(\beta)) = x^2 + 2 \in \mathbb{F}_5[x].$$

- Wir betrachten $\gamma = \alpha + \pi^3(\alpha)$. Es ist

$$\begin{aligned} \gamma &= \alpha + \alpha^{125} = 2\alpha + 3\alpha^2 + 4\alpha^3 + 2\alpha^4 + \alpha^5, \\ \pi(\gamma) &= \gamma^5 = \alpha + \alpha^2 + \alpha^3 + \alpha^4 + 2\alpha^5, \\ \pi^2(\gamma) &= 2\alpha + \alpha^2 + 2\alpha^4 + 2\alpha^5, \\ \pi^3(\gamma) &= \gamma. \end{aligned}$$

  Es ist

$$g = (x - \gamma)(x - \pi(\gamma))(x - \pi^2(\gamma)) = x^3 + x + 4 \in \mathbb{F}_5[x].$$

Die Teilkörper von $\mathbb{F}_{p^n}$ sind

$$\mathbb{F}_{p^d}, \text{ wo } d \text{ alle Teiler von } n \text{ durchläuft.}$$

Der folgende Satz gibt eine Formel für die Teileranzahl, wenn man die Primfaktorzerlegung von n kennt:

SATZ. *Ist $n \in \mathbb{N}$ mit der Primfaktorzerlegung*

$$n = q_1^{e_1} \dots q_r^{e_r}$$

(mit paarweise verschiedenen Primzahlen $q_1, \dots, q_r$ und $e_1, \dots, e_r \in \mathbb{N}$), so ist die Menge der Teiler von n genau

$$\{d \in \mathbb{N} : d \mid n\} = \{q_1^{d_1} \dots q_r^{d_r} : 0 \le d_i \le e_i \text{ für } i = 1, \dots, r\}.$$

Für die Anzahl der Teiler folgt

$$|\{d \in \mathbb{N} : d \mid n\}| = (e_1 + 1) \dots (e_r + 1).$$

Beispiel: $n = 12$ hat die Teiler $1, 2, 3, 4, 6, 12$, die Anzahl ist 6. Nun ist $12 = 2^2 \cdot 3$. Die Formel des Satzes liefert ebenfalls die Anzahl $(2 + 1) \cdot (1 + 1) = 6$.

SATZ. *Sei p eine Primzahl. Sei (bei festem p) a_n die Anzahl der irreduziblen normierten Polynome aus $\mathbb{F}_p[x]$ vom Grad n. Dann gilt:*

$$p^n = \sum_{d|n} d a_d.$$

Beweis: Sei I_d die Menge der normierten irreduziblen Polynome vom Grad d.

(1) Wir betrachten
$$Z = \bigcup_{d|n} \bigcup_{f \in I_d} \{\alpha \in \overline{\mathbb{F}}_p : f(\alpha) = 0\}.$$
Da verschiedene irreduzible normierte Polynome keine gemeinsamen Nullstellen haben, steht auf der rechten Seite eine disjunkte Vereinigung, sodass folgt
$$|Z| = \sum_{d|n} \sum_{f \in I_d} |\{\alpha \in \overline{\mathbb{F}}_p : f(\alpha) = 0\}| = \sum_{d|n} \sum_{f \in I_d} d = \sum_{d|n} d|I_d| = \sum_{d|n} d a_d.$$

(2) Wir wollen zeigen, dass gilt $Z = \mathbb{F}_{p^n}$.
- $\subseteq$: Sei $\alpha \in Z$. Dann gibt es einen Teiler $d \mid n$ und ein irreduzibles normiertes Polynom f aus $\mathbb{F}_p[x]$ vom Grad d mit $f(\alpha) = 0$. Dann ist $\mathbb{F}_p(\alpha)|\mathbb{F}_p$ eine Körpererweiterung vom Grad d, also $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. Aus $d \mid n$ folgt dann $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ und damit $\alpha \in \mathbb{F}_{p^n}$.
- $\supseteq$ Sei $\alpha \in \mathbb{F}_{p^n}$. Dann ist $\mathbb{F}_p(\alpha)$ ein Unterkörper, es gibt also einen Teiler $d \mid n$ mit $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. α hat also Grad d über $\mathbb{F}_p$. Das Minimalpolynom f von α hat Grad d und α als Nullstelle. Da es außerdem normiert und irreduzibel ist, folgt $\alpha \in Z$.

(3) Damit erhalten wir nun
$$p^n = |\mathbb{F}_{p^n}| = |Z| = \sum_{d|n} d a_d,$$
was wir zeigen wollten. ■

Beispiele:

(1) Die irreduziblen normierten Polynome vom Grad 1 sind $x + a$ mit $a \in \mathbb{F}_p$, es gibt also p Stück, d.h.
$$a_1 = p.$$

(2) Für $n = 2$ erhalten wir
$$p^2 = \sum_{d|2} d a_d = a_1 + 2a_2 = p + 2a_2,$$
also
$$a_2 = \frac{p^2 - p}{2}.$$

(3) Ist ℓ eine Primzahl, so gilt
$$p^\ell = \sum_{d|\ell} d a_d = a_1 + \ell a_\ell = p + \ell a_\ell,$$
woraus
$$a_\ell = \frac{p^\ell - p}{\ell}$$
folgt.

(4) Für $n = 4$ gilt
$$p^4 = \sum_{d|4} d a_d = a_1 + 2a_2 + 4a_4 = p + (p^2 - p) + 4a_4 = p^2 + 4a_4.$$
Also gilt
$$a_4 = \frac{p^4 - p^2}{4}.$$

Bemerkungen:

(1) Die Beispiele zeigen, dass man die Zahlen a_n rekursiv mit Hilfe der Formel

$$p^n = \sum_{d|n} d a_d$$

berechnen kann.

(2) Es gibt auch eine systematische Möglichkeit, die Zahlen a_n zu berechnen. Dazu benutzt man die **Möbius-Umkehrformeln**. Die **Möbius-Funktion** $\mu : \mathbb{N} \to \{0, 1, -1\}$ wird definiert durch

$$\mu(n) = \begin{cases} 0, & \text{falls } n \text{ durch das Quadrat einer Primzahl teilbar ist,} \\ (-1)^r, & \text{falls } n = p_1 \dots p_r \text{ mit verschiedenen Primzahlen } p_i. \end{cases}$$

Ist $f : \mathbb{N} \to \mathbb{C}$ eine Funktion und definiert man $g : \mathbb{N} \to \mathbb{C}$ durch

$$g(n) = \sum_{d|n} f(d),$$

so gilt

$$f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d),$$

man erhält also f wieder aus der Funktion g.
Als Anwendung wählen wir $f(n) = n a_n$. Dann ist

$$g(n) = \sum_{d|n} f(n) = \sum_{d|n} d a_d = p^n.$$

Die Möbius-Umkehrformeln liefern

$$n a_n = \sum_{d|n} \mu(\frac{n}{d}) p^d,$$

also

$$a_n = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d.$$

Beispielsweise ist

$$a_4 = \frac{1}{4} \sum_{d|4} \mu(\frac{4}{d}) p^d = \frac{1}{4} \left(\mu(4) p^0 + \mu(2) p^2 + \mu(1) p^4 \right) = \frac{1}{4} \left(-p^2 + p^4 \right) = \frac{p^4 - p^2}{4}.$$