2* (Endliche Körper). Wir klassifizieren bis auf Isomorphie alle endlichen Körper. Zeigen Sie dazu:

(i) Ist K ein endlicher Körper, so ist $\mathrm{char}(K) = p$ eine Primzahl und $|K| = p^n$ für ein $n \in \mathbb{N}$.

(ii) Es sei p eine Primzahl, $n \in \mathbb{N}$, und K ein Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{Z}_p$. Dann ist $|K| = p^n$.

(iii) Sind K_1 und K_2 endliche Körper mit $|K_1| = |K_2|$, so gilt $K_1 \cong K_2$. (*Hinweis:* Charakterisieren Sie K_i als Zerfällungskörper eines geeigneten Polynoms über dem Primkörper von K_i.)

Für den, bis auf Isomorphie eindeutig bestimmten, Körper mit p^n Elementen schreibt man oft $\mathbb{F}_{p^n}$.

Beweis: (i) Es existiert ein Ringhomomorphisms $\varphi\colon \mathbb{Z} \to K$, $a \mapsto a1_K$, und es ist $\ker(\varphi) = m\mathbb{Z}$ für ein $m \in \mathbb{N}$. Es ist $m = \mathrm{char}(K)$ (nach Definition der Charakteristik). Damit induziert φ aber einen injektiven Homomorphismus $\mathbb{Z}/m\mathbb{Z} \to K$, d.h. $\mathbb{Z}/m\mathbb{Z}$ ist ein isomorph zu einem Teilring von K und muss demnach ein Bereich sein. Das bedeutet aber $m \in \mathbb{P}$ oder $m = 0$, wobei $m = 0$ unmöglich ist, weil K endlich ist. Somit ist $m = p \in \mathbb{P}$.

Das Bild von $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ unter ϕ ist isomorph zum Körper $\mathbb{Z}_p$. Damit ist K ein endlich-dimensionaler $\mathbb{Z}_p$-Vektorraum, also notwendigerweise $|K| = p^n$ für ein $n \in \mathbb{N}$.

(ii) Es sei $f = X^{p^n} - X \in \mathbb{Z}_p[X]$, und es sei K ein Zerfällungskörper von f (Anm.: Die Existenz eines solchen folgt aus Satz 11.2.). Es ist $f' = p^n X^{p^n-1} - 1 = -1$, und damit sind f und f' teilerfremd. Also ist f separabel und besitzt demnach p^n paarweise verschiedene Nullstellen in K. Damit ist $|K| \geq p^n$.

Die Menge

$$A = \{a \in K \mid f(a) = 0\} = \{a \in K \mid a^{p^n} = a\}$$

bildet einen Teilring von K (vgl. Blatt 10, Übung 1(ii)), und weil f höchstens p^n Nullstellen besitzt, ist $|A| \leq p^n$. Als Teilring eines Körpers ist A ein Bereich, und natürlich ist A endlich. Also ist A ein Körper. (Man kann alternativ auch Blatt 9, Übung 5 anwenden.) Es ist $\mathbb{Z}_p \subset A$, weil $a^p = a$ für alle $a \in \mathbb{Z}_p$ gilt. Somit ist A bereits ein Zerfällungskörper von f, d.h. also $A = K$, und es folgt $|K| \leq p^n$.

(iii) Nach (i) ist $|K_1| = |K_2| = p^n$ für ein $p \in \mathbb{P}$ und $n \in \mathbb{N}$. Sei k_i jeweils der Primkörper von K_i. Dann ist $k_1 \cong \mathbb{Z}_p \cong k_2$. Sei $\varphi\colon k_1 \to k_2$ ein Isomorphismus.

Wir zeigen zuerst: Für $i \in \{1, 2\}$ ist K_i ein Zerfällungskörper von $f_i = X^{p^n} - X \in k_i[X]$ über k_i. Es ist $|K_i^\times| = p^n - 1$. Ist $a \in K_i^\times$, so ist also

$\mathrm{ord}_{K_i^\times}(a) \mid p^n - 1$, und deshalb

$$a^{p^n} = a(a^{p^n-1}) = a.$$

Natürlich ist auch $0^{p^n} = 0$. Damit hat aber f in K_i insgesamt p^n paarweise verschiedene Nullstellen, wegen $\deg(f) = p^n$ zerfällt es also in Linearfaktoren. Da jedes $a \in K_i$ Nullstelle von f ist, ist natürlich $K_i = \mathbb{Z}_p(\{a \in K_i \mid f_i(a) = 0\})$. Damit ist K_i ein Zerfällungskörper von f_i.

Nun wenden wir Satz 11.3, um zu zeigen $K_1 \cong K_2$: Wir setzen $\varphi\colon k_1 \to k_2$ fort zu einem Isomorphismus $\varphi\colon k_1[X] \to k_2[X]$. Dann ist $\varphi(f_1) = f_2$. Nachdem K_1 ein Zerfällungskörper von f_1 über k_1 ist, und K_2 ein Zerfällungskörper von f_2 über k_2 ist, folgt $K_1 \cong K_2$ nach Satz 11.3. □