Zu §5.12: Endliche Körper:

Satz: Für jeden endlichen Körper k gilt:

(a) $p := \mathrm{char}(k) > 0$.
(b) $|k| = p^n$ für $n := [k : \mathbb{F}_p] < \infty$.
(c) $k^\times$ ist zyklisch der Ordnung $p^n - 1$.
(d) $\forall a \in k: \; a^{p^n} = a$.
(e) k ist Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$.

Also ex. keine endl. Körper der Ord. 15.

– **Beweis:** (a) Da k endlich ist, ist auch der darin enthaltene Primkörper endlich. Also ist dieser $\mathbb{F}_p$ für eine Primzahl p.
– (b) k endlich $\Rightarrow n < \infty \Rightarrow k \cong \mathbb{F}_p^n$ als $\mathbb{F}_p$-Vektorraum.
– (c) $k^\times$ ist eine endliche abelsche Gruppe der Ordnung $p^n - 1$. Nach dem Strukturssatz ist also $k^\times \cong \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_r\mathbb{Z}$ mit Elementarteilern $1 < e_r | e_{r-1} | \ldots | e_1 \neq 0$. Dann ist $\exp(k^\times) = e_1$. Also gilt $\forall a \in k^\times, \; a^{e_1} = 1$. Aber das Polynom $X^{e_1} - 1$ hat höchstens e_1 verschiedene Nullstellen. Folglich gilt
$$p^n - 1 = |k^\times| \leq e_1 \leq e_1 \cdots e_r = |k^\times|.$$
Also ist $p^n - 1 = e_1$ und folglich $r = 1$ und $k^\times$ ist zyklisch.
– (d) Wegen $|k^\times| = p^n - 1$ und Lagrange — oder wegen (c) — gilt $\forall a \in k^\times: \; a^{p^n - 1} = 1 \Rightarrow a^{p^n} = a$.
Die letzte Gleichung gilt auch noch für $a = 0$.
– (e) Nach (b) und (d) hat das Polynom $X^{p^n} - X \in \mathbb{F}_p[X]$ die p^n verschiedenen Nullstellen $a \in k$. Folglich ist

(*) $$X^{p^n} - X = \prod_{a \in k} (X - a).$$

Ausserdem ist $k = \mathbb{F}_p(k)$. Also ist k der Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$.

zzd.

Satz: Für jedes $n \geq 1$ existiert ein endlicher Körper der Ordnung p^n. Dieser ist eindeutig bis auf nichteindeutige Isomorphie.

Beweis: Sei k ein Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$, also $k = \mathbb{F}_p(a_1, \dots, a_{p^n})$ mit $X^{p^n} - X = \prod_{i=1}^{p^n} (X - a_i)$.

Für alle i gilt dann $a_i^{p^n} - a_i = 0$, also $\mathrm{Frob}_{p^n}(a_i) = a_i^{p^n} = a_i$.

Da Frob_p ein Körperhomomorphismus $k \to k$ ist, folgt dann $\mathrm{Frob}_{p^n}(a) = a$ für alle $a \in k$. Also gilt $\forall a \in k : a^{p^n} - a = 0$.

Also ist $k = \{a_1, \dots, a_{p^n}\}$. Weiter ist $\frac{d}{dX}(X^{p^n} - X) = -1$ und folglich teilerfremd zu $X^{p^n} - X$. Also ist $X^{p^n} - X$ ein separabler Polynom. Daher sind $a_1, \dots, a_{p^n}$ alle verschieden, und es folgt $|k| = |\{a_1, \dots, a_{p^n}\}| = p^n$. Dies zeigt die Existenz.

Die Eindeutigkeit folgt aus der Eindeutigkeit des Zerfällungskörpers. qed.

Bem.: $\mathrm{Frob}_p : k \to k$ ist ein Automorphismus, der im Fall $n > 1$ zeigt, dass der Automorphismus nicht eindeutig ist.

Prop.: Für jeden endlichen Körper k mit $|k| = p^n$ ist

$$\mathrm{Aut}(k) = \mathrm{Aut}_{\mathbb{F}_p}(k) = \langle \mathrm{Frob}_p|_k \rangle \quad \text{zyklisch der Ordnung } n.$$

Beweis: Die Gleichheit folgt dem, dass jeder Körperhomomorphismus auf dem Primkörper die Identität ist.

Rückkehr mit $\sigma := \mathrm{Frob}_p|_k$. Dann gilt $\sigma^n = \mathrm{Frob}_{p^n}|_k = \mathrm{id}_k$.

Für alle $1 \leq i \leq n-1$ ist aber $|\{a \in k \mid \sigma^i(a) = a\}| =$
$= |\{a \in k \mid a^{p^i} - a = 0\}| \leq p^i < p^n = |k|$. Also ist $\sigma^i \neq \mathrm{id}$.
Daher ist $\langle \sigma \rangle$ zyklisch der Ordnung n.

Dass es nicht mehr Automorphismen gibt, folgt aus

$$|\mathrm{Aut}_{\mathbb{F}_p}(k)| = |\mathrm{Hom}_{\mathbb{F}_p}(k, k)| \leq [k : \mathbb{F}_p] = n.$$

§5.7

qed.

Baum-Natriel:

Anwendung: Quadrate:

Sei k ein endlicher Körper der Ordnung p^n.

Im Fall $p=2$ ist jedes Element in k ein Quadrat.

Prop.: Für $p>2$ ist jedes Element in k eine Summe von zwei Quadraten.

Beweis: $Q := \{a^2 \mid a \in k\} = \{0\} \cup \{a^2 \mid a \in k^\times\}$

$\Rightarrow |Q| = \quad 1 + \frac{p^n-1}{2} = \frac{p^n+1}{2}$

Für jedes $x \in k$ gilt mit $Q \cap \{x-a^2 \mid a \in k\} \neq \emptyset$

Ord $\frac{p^n+1}{2} + \frac{p^n+1}{2} > p^n$

Also $\exists a,b \in k : b^2 = x-a^2 \Rightarrow x = a^2+b^2$. qed.

Prop.: Für $p>2$ ist -1 ein Quadrat in k gdw. $p^n \equiv 1 \pmod 4$ ist.

Beweis: -1 hat Ordnung 2 in $k^\times \cong \mathbb{Z}/(p^n-1)\mathbb{Z}$.

Es ist ja genau dann wenn $\frac{p^n-1}{2} \in R(+,\cdot)$ ja Vielfaches von 2 ist.

Dies ist ja genau dann, wenn $\frac{p^n-1}{2}$ gerade ist. qed.

Bemerkung: Eine Verallgemeinerung davon ist das sogenannte quadratische Reziprozitätsgesetz.