Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil III: KÖRPER

A21: Endliche Körper

Stichworte: endl. UGen der mult. Gr. eines Körpers sind zyklisch, Frobenius-Endomorphismus, Konstruktion des endlichen Körpers mit p^n Elementen (bis auf Isomorphie), endliche Körper sind perfekt

---

21.1. Einleitung: Wir zeigen zunächst als Hilfsmittel den fundamentalen Satz, dass die endl. UGen der multiplikativen Gruppe eines bel. Körpers stets zyklisch sind. Dieser Hilfssatz wird benutzt, um zu zeigen, dass jeder endliche Körper perfekt ist. Wir geben darüberhinaus eine Konstruktionsmöglichkeit an, wie jeder endliche Körper (bis auf Isomorphie) konstruiert werden kann. Dabei spielt der Frobenius-Endomorphismus eine zentrale Rolle.

21.2. Satz: Endliche UGen der mult. Gr. eines (nicht notw. endl.) Körpers K sind stets zyklisch.

Bew.: Sei $U \subseteq K^\times$ endl. der Ordnung $n > 1$, schreibe $U = U_1 \times \dots \times U_m$, die U_i p_i-Gruppen $\neq e$ mit $p_1, \dots, p_m \in \mathbb{N}$ prim, pwv.
Zeige jetzt: Alle U_i sind zyklisch (dann U zyklisch).

* Sei $\{e\} \subsetneq U$ eine p-Gruppe, d.h. $\exists e > 1 : \#U = p^e$ [U zyklisch für $e = 1$].
Ann.: U nicht zyklisch.
[Dann: $U = C_1 \times C_2 \times \dots \times C_r$, die C_i zykl. p-Gr. ($r \geq 2$), laut Hauptsatz, und $p^e = p^{e_1} \cdot p^{e_2} \cdot \dots \cdot p^{e_r}$, die $e_i < e$, da U nicht zykl.
Sei $e' := \max\{e_i ; 1 \leq i \leq r\} \Rightarrow \forall x \in U : x^{p^{e'}} = 1$ [Glg. in jeder Komponente]
$\Rightarrow \forall x \in U : x^{p^{e-1}} = 1$.
Somit: $f = T^{p^{e-1}} - 1$ hat p^e ($> \deg f = p^{e-1}$) viele versch. Wurzeln in K, ↯ zu Satz 14.13.]

* Seien $\#U_i = p_i^{e_i}$, $U_i = \langle a_i \rangle$, $\operatorname{ord}(a_i) = p_i^{e_i}$. Sei $0 \neq a = a_1 \cdot \dots \cdot a_m \in U$.
Dann: $\operatorname{ord}(a) = \operatorname{kgV}(\operatorname{ord}(a_1), \dots, \operatorname{ord}(a_m)) = p_1^{e_1} \cdot \dots \cdot p_m^{e_m} = \#U$,
also $U = \langle a \rangle$, d.h. U ist zyklisch. □

21.3. **Lemma**: Sei K Körper, $\mathrm{Char}\, K = p > 0$ prim. Dann:

$\sigma: K \to K,\ a \mapsto a^p$ ist inj. Endomorphismus.

K endlich $\Rightarrow \sigma$ Automorphismus.

Bew.: Endo: $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$,

$\sigma(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$,

da für $0 < i < p$ gilt: $p \mid \binom{p}{i}$.

Inj.: $\ker \sigma = 0$, da $0, K$ einzige Ideale in K. □

21.4. **Def.**: Der inj. Endo σ aus 21.3 heißt Frobenius-Endomorphismus.

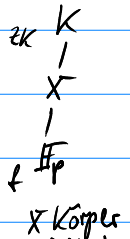
21.5. **Satz**: (1) $\forall p$ prim $\forall n \geq 1$ $\exists$ bis auf Iso genau ein endl. Körper $\mathbb{F}_{p^n}$, $\#\mathbb{F}_{p^n} = p^n$,

nämlich: $\mathbb{F}_{p^n} = $ ZK von $f := T^{p^n} - T \in \mathbb{F}_p[T]$ (sep.),

(2) $a \in \mathbb{F}_{p^n} \Leftrightarrow f(a) = 0$,

(3) K endl. Körper $\Rightarrow \exists p$ prim $\exists n \geq 1$: $K \cong \mathbb{F}_{p^n}$.

Bew.: (1): Ex.: Sei $p \in \mathbb{N}$ prim, $n \geq 1$. Sei $\mathbb{F}_p[T] \ni f(T) := T^{p^n} - T$.



f ist separabel, da $f' = p^n T^{p^n - 1} - 1 = -1$ teilerfremd zu f.

Sei K der ZK von f über $\mathbb{F}_p$, und

sei $X := \{x \in K;\ f(x) = 0\}$, $\#X = p^n$, da f separabel.

Sei σ der Frobenius-Endo von K, d.h. $\sigma: K \to K$, $x \mapsto x^p$ (inj.).

Somit: $X = \{x \in K;\ \sigma^n(x) = x^{p^n} = x\} =: \mathrm{Fix}(\sigma^n)$.

Für jeden Körperendo τ ist $\mathrm{Fix}(\tau)$ ein Körper,

also ist $X = K$ (da also X ZK von f über $\mathbb{F}_p$).

Da f separabel, ist $\#K = p^n$. Bez.: $\mathbb{F}_{p^n} := K$.

Eind.: Sei K nun ein endl. Körper, $\#K = p^n$.

Es ist $\#K^\times = p^n - 1$, d.h. $\forall x \in K^\times$: $x^{p^n - 1} = 1$, vgl. Satz 21.2: $K^\times$ zyklisch!

$\Rightarrow$ Jedes $x \in K$ ist Wurzel von $T^{p^n} - T \in \mathbb{F}_p[T]$,

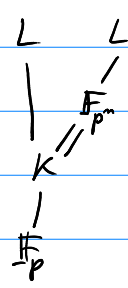
d.h. K ist ZK von $T^{p^n} - T \in \mathbb{F}_p[T]$ über $\mathbb{F}_p$, also eind. best.

(2): $a \in \mathbb{F}_{p^n} \Leftrightarrow a \in X = \{x \in \mathbb{F}_{p^n} ; f(x)=0\} \Leftrightarrow f(a)=0$.

(3): Sei K endl. Körper, $p := \mathrm{Char}(K)$, d.h.
PrimKörper $\mathrm{Prim}(K) \cong \mathbb{F}_p$, sei also $\mathbb{O} \cong \mathbb{F}_p \subseteq K$.
Sei $x_1, \dots, x_m$ eine $\mathbb{F}_p$-Basis von K, dann:
$K \underset{\text{VR-Iso}}{\cong} \underbrace{\mathbb{F}_p \oplus \dots \oplus \mathbb{F}_p}_{n} \cong \mathbb{F}_p^n$, d.h. $\#K = p^n$. Also: $K \cong \mathbb{F}_{p^n}$. □

21.6. **Satz:** $\forall$ endl. Körper K $\forall m \geq 1$ $\exists$ (bis auf Iso über K genau ein) $L|K$: $[L:K]=m$.
Dann: L normal, separabel, einfach (vgl. Satz A20.16 vom primitiven El.).
Also: K perfekt.

Bew.: Geg.: K, $m \geq 1$. Sei $q := \#K = p^n$, $L' := \mathbb{F}_{p^{nm}} = \mathbb{F}_{q^m}$.
Dann: $\#L'^{\times} = q^m - 1 = (q-1)(q^{m-1} + \dots + q + 1)$,



$L'^{\times}$ zyklisch nach Satz 21.2.
Somit enthält $L'^{\times}$ eine UG der Ordnung $q-1$.
$\Rightarrow$ L' enthält zu K K' von $T^q - T \in \mathbb{F}_p[T]$ über $\mathbb{F}_p$,
also $K' = \mathbb{F}_{p^n} \cong K$.
Sei daher $\mathbb{O} \cong K \subseteq L'$.

* Eind., normal, separabel:
Jede Erw. $L|K$, $[L:K]=m$ hat Grad nm über $\mathbb{F}_p$,
ist also zu K des separablen $T^{p^{nm}} - T \in \mathbb{F}_p[T]$.
Also: L eind., normal, separabel über $\mathbb{F}_p$, bzw. über K.
* Sei x ein erz. El. der Gruppe $L^{\times}$, also: $L = K(x)$. □