6.6 Perfekte Körper

Erinnerung: Ein Polynom in $K[X] \setminus \{0\}$, das keine mehrfachen Nullstellen in $\overline{K}$ besitzt, heisst *separabel*.

6.6.1 Definition: Ein Körper K heisst *vollkommen* oder *perfekt*, wenn jedes irreduzible Polynom über K separabel ist.

Erinnerung: Satz 6.5.9 (a): Ist $\mathrm{char}(K) = 0$, so ist jedes irreduzible Polynom über K separabel.

6.6.2 Proposition: Jeder Körper der Charakteristik 0 ist perfekt.

Erinnerung: Proposition-Definition 6.6.3: Sei R ein Ring, und sei p eine Primzahl mit $p \cdot 1_R = 0_R$. Dann ist für jedes $r \geqslant 1$ die Abbildung

$$\mathrm{Frob}_{p^r} : R \to R, \ x \mapsto x^{p^r}$$

ein Ringhomomorphismus, genannt der *Frobenius-Endomorphismus vom Grad p^r*.

Insbesondere besitzt jeder Körper K der Charakteristik $p > 0$ den Endomorphismus $\mathrm{Frob}_{p^r} : K \to K$. Als Körperhomomorphismus ist dieser injektiv.

Erinnerung: Satz 6.5.9 (b): Ist $p := \mathrm{char}(K) > 0$, so hat jedes irreduzible Polynom über K die Form $f(X) = g(X^{p^r})$ für ein eindeutiges $r \geqslant 0$ und ein separables irreduzibles Polynom g über K.

6.6.4 Proposition: Ein Körper K der Charakteristik $p > 0$ ist perfekt genau dann, wenn der Frobenius-Endomorphismus $\mathrm{Frob}_p \colon K \to K$ bijektiv ist.

Beweis: "$\Rightarrow$" Sei K perfekt. Sei $a \in K$ und sei $b \in \overline{K}$ eine Nullstelle von $f(X) := X^p - a$.
In $\overline{K}[X]$ gilt dann $(X-b)^p = X^p - b^p = X^p - a = f$. Also ist b die einzige Nullstelle von f.
Sei g das Min.Pol. von b über K. $\Rightarrow g \mid f$. K perfekt $\Rightarrow g$ separabel. $\Rightarrow g = X - b$. $\Rightarrow b \in K$.
$\Rightarrow \mathrm{Frob}_p(b) = a$ ✓
"$\Leftarrow$" Sei $\mathrm{Frob}_p : K \to K$ bijektiv. Sei $f \in K[X]$ irred., nicht separabel. Dann $\exists g \in K[X] : f(X) = g(X^p)$.
Schreibe $g(X) = \sum a_i X^i$ mit $a_i \in K$. Nach Vor. ist $a_i = b_i^p$ für ein $b_i \in K$. Setze $h(X) := \sum b_i X^i$
$\Rightarrow h(X)^p = \left(\sum_i b_i X^i\right)^p = \sum_i b_i^p X^{ip} = \sum a_i X^{ip} = f(X)$ $\Rightarrow$ Widspr. zu irred. qed.

6.6.5 Proposition: Jeder endliche Körper ist perfekt.

Beweis: $\mathrm{Frob}_p : K \to K$ injektiv. $\Rightarrow$ bijektiv. qed.

6.6.6 Beispiel: Der rationale Funktionenkörper $\mathbb{F}_p(Y)$ ist nicht perfekt.

Beweis: $X^p - Y \in \mathbb{F}_p(Y)[X]$ irred., nicht separabel.
$\mathrm{Frob}_p : \mathbb{F}_p(Y) \to \mathbb{F}_p(Y)$, $f(Y) \mapsto f(Y^p)$

6.7 Endliche Körper

6.7.1 Satz: Für jeden endlichen Körper k gilt:

(a) $p := \mathrm{char}(k) > 0$.

(b) $|k| = p^n$ für $n := [k/\mathbb{F}_p]$.

(c) Die multiplikative Gruppe $k^\times$ ist zyklisch der Ordnung $p^n - 1$.

(d) $a^{p^n} = a$ für alle $a \in k$. *(Kleiner Satz von Fermat)*

(e) k ist ein Zerfällungskörper des Polynoms $X^{p^n} - X$ über $\mathbb{F}_p$.

Bew.: (a) k endlich $\Rightarrow \mathbb{Q} \not\subset k \Rightarrow$ Primkörper $\mathbb{F}_p \subset k$.

(b) k ist endlicher $\mathbb{F}_p$-Vektorraum $\Rightarrow [\mathbb{F}_p/k] = \dim_{\mathbb{F}_p}(k) =: n < \infty$ und $|k| = p^n$.

(c) $k^\times$ endliche abelsche Gruppe $\Rightarrow k^\times \cong \mathbb{Z}/e_1\mathbb{Z} \times \ldots \times \mathbb{Z}/e_r\mathbb{Z}$ für $e_1, \ldots, e_r \in \mathbb{Z}^{>1}$ und $e_1 | e_2 | \ldots | e_r$.

$\Rightarrow$ Exponent von $k^\times$ ist e_r. Also $\forall a \in k^\times: a^{e_r} = 1$. Das heißt a ist Nullstelle von $X^{e_r} - 1$.

$\Rightarrow |k^\times| \leq e_r \leq e_1 \cdots e_r = |k^\times| \Rightarrow$ Gleichheit $\Rightarrow e_1 = \ldots = e_{r-1} = 1 \Rightarrow r = 1$ und $k^\times$ zyklisch.

(d) Für alle $a \in k^\times$ ist $a^{p^n - 1} = 1$ nach Lagrange. $\Rightarrow a^{p^n} = a$. Auch $0^{p^n} = 0$.

(e) Jedes $a \in k$ ist Nullstelle von $X^{p^n} - X$ nach (d).

$\Rightarrow X^{p^n} - X = \prod_{a \in k} (X - a)$ $\in \mathbb{F}_p[X]$.

Da k über $\mathbb{F}_p$ von k erzeugt wird, folgt (e).

q.e.d.

$\rightsquigarrow$ Insbesondere: $\forall a \in \mathbb{Z}: a^p \equiv a \bmod (p)$

6.7.2 Satz: Für jede Primpotenz p^n existiert ein endlicher Körper der Ordnung p^n. Dieser ist bis auf Isomorphie bestimmt; der Isomorphismus ist aber im allgemeinen nicht eindeutig. Eine häufige Bezeichnung dafür ist $\mathbb{F}_{p^n}$.

Bem.: Sei k ein Zerfällungskörper von $X^{p^n}-X$ über $\mathbb{F}_p$. Zu zeigen: $|k| = p^n$.
$\Rightarrow k$ bis auf Isomorphie eindeutig.
Schreibe: $X^{p^n}-X = \prod_{i=1}^{p^n}(X-a_i)$ mit $a_i \in k$. Wegen $\frac{d}{dX}(X^{p^n}-X) = p^n \cdot X^{p^n-1} - 1 = -1$ ist dies teilerfremd zu $f \Rightarrow f$ separabel $\Rightarrow a_i$ paarweise verschieden $\Rightarrow |k| \geq p^n$. Betrachte $\sigma := \mathrm{Frob}_p^n : k \to k$.
$\Rightarrow \sigma$ Homomorphismus mit $\sigma(a_i) = a_i$ für alle i, $\Rightarrow \sigma$ auf $k = \mathbb{F}_p(a_1, \ldots)$ die Identität, $\Rightarrow$ Jedes $a \in k$ ist Nullstelle von f. $\Rightarrow |k| \leq p^n$. qed

6.7.3 Proposition: Für jeden endlichen Körper k der Ordnung p^n ist

$$\mathrm{Aut}(k) = \mathrm{Aut}_{\mathbb{F}_p}(k) = \langle \mathrm{Frob}_p | k \rangle$$

zyklisch der Ordnung n.

Bem.: Jeder Automorphismus ist die Identität auf $\mathbb{F}_p$.
Sei $\sigma := \mathrm{Frob}_p | k$. Dann ist $\sigma^n = \mathrm{Frob}_p^n | k = \mathrm{id}_k$.
Für jedes $1 \leq i < n$ ist $X^{p^i}-X$ von Grad $p^i < p^n = |k| \Rightarrow$ ist nicht identische Null auf k.
$\Rightarrow \sigma^i \neq \mathrm{id}$. $\Rightarrow \sigma$ hat die genaue Ordnung n.

$|\mathrm{Aut}_{\mathbb{F}_p}(k)| \leq |\mathrm{Hom}_{\mathbb{F}_p}(k,k)| \leq [k:\mathbb{F}_p] = n$
nach Prop. 6.2. $\Rightarrow$
$\Rightarrow \mathrm{Aut}_{\mathbb{F}_p}(k) = \langle \sigma \rangle$. qed

$k \hookrightarrow l$, k_0

6.7.4 Bemerkung: Einen algebraischen Abschluss von $\mathbb{F}_p$ kann man konstruieren als Vereinigung aller $\mathbb{F}_{p^{n!}}$ für $n \geqslant 0$ via irgendwie gewählten Einbettungen $\mathbb{F}_{p^{n!}} \hookrightarrow \mathbb{F}_{p^{(n+1)!}}$.

Bem.: $k, l / \mathbb{F}_p \Rightarrow \exists$ Homom. $k \to l$ g.d.w. $|l|$ eine Potenz von $|k|$ ist.
$X^{p^n}-X \mid X^{p^m}-X$ g.d.w. $n \mid m$.

6.7.5 Definition: Ein Ring, der alle Körperaxiome ausser vielleicht die Kommutativität der Multiplikation erfüllt, heisst eine *Divisionsalgebra* oder ein *Schiefkörper*.

6.7.6 Satz: *(Wedderburn)* Jeder endliche Schiefkörper ist kommutativ. (ohne Beweis)

6.8 Separable Körpererweiterungen

6.8.1 Definition: Betrachte eine algebraische Körpererweiterung L/K.

(a) Ein Element von L, dessen Minimalpolynom über K separabel ist, heisst *separabel über K*.

(b) Ist jedes Element von L separabel über K, so heisst L/K *separabel*.

6.8.2 Proposition: Ein Körper K ist perfekt genau dann, wenn jede algebraische Erweiterung von K separabel ist.

6.8.3 Folge: Im Fall $\mathrm{char}(K) = 0$ oder $|K| < \infty$ ist jede algebraische Erweiterung von K separabel.

Bew.: "$\Rightarrow$" K perfekt, L/K algebraisch, $a \in L$ mit Min.Pol. $f \in K[X]$.
$\Rightarrow f$ irred. $\Rightarrow f$ separabel $\Rightarrow a$ separabel über K.

"$\Leftarrow$" Jede alg. Erw. von K separabel $\Rightarrow$ bes. $a \in K$.
$\mathrm{char}(K) = 0$ fertig. $K(b)$
$\mathrm{char}(K) = p > 0$ $\rightsquigarrow$ L Zerfällungskörper von $X^p - a$ über K, mit $b^p = a$.
$\Rightarrow L/K$ separabel, $\Rightarrow$ Min.pol. von b ist Teiler von $X^p - a$
separable $= (X-b)^p$
$\Rightarrow = X - b \Rightarrow b \in K$.

qed.

6.8.4 Proposition: Sei $L = K(a_1, \ldots, a_n)/K$ endlich, und sei $\overline{K}$ ein algebraischer Abschluss von K. Dann sind äquivalent:

(a) L/K ist separabel.

(b) Jedes a_i ist separabel über K.

(c) $|\mathrm{Hom}_K(L, \overline{K})| = [L/K]$.

"$\leq$" nach Prop. 6.2.7.

Lemma: $L/K'/K$, $a \in L$ separabel über K $\Rightarrow$ a separabel über K'.

Beweis: Sei f das Min.Pol. von a über K: $f \in K[X]$
g . . . . . K': $g \in K'[X]$
$f(a) = 0 \Rightarrow g \mid f$ in $K'[X]$.
f separabel $\Rightarrow$ g separabel. qed

Beweis: (a) $\Rightarrow$ (b) ✓

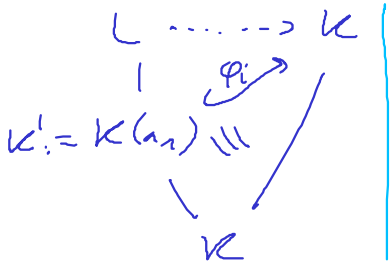
(b) $\Rightarrow$ (c) Induktion über n.

Fall $n = 0$: $L = K \Rightarrow |\mathrm{Hom}_K(K, \overline{K})| = 1 = [L/K]$.

Fall $n > 0$: Sei $f \in K[X]$ das Min.Pol. von a_1 über K.

$\Rightarrow f(X) = \prod_{i=1}^{d} (X - b_i)$ für $b_i \in \overline{K}$ paarweise verschieden.

Jedes b_i entspricht einem Homo $K(a_1) \xrightarrow{\varphi_i} \overline{K}$ über K, $a_1 \mapsto b_i$



Die $a_2, \ldots, a_n$ sind separabel über K'.

$L = K'(a_2, \ldots, a_n)$

$\Rightarrow$ Jedes φ_i besitzt genau $[L/K']$ Fortsetzungen in $\mathrm{Hom}_K(L, \overline{K})$.

$[K'/K] = d$

$\Rightarrow |\mathrm{Hom}_K(L, \overline{K})| = [L/K'] \cdot [K'/K]$
$= [L/K]$.

Bleibt zu zeigen: (c) $\Rightarrow$ (a).