Erinnerung:

6.4.3 Definition: Ein Oberkörper von K, welcher algebraisch über K und selbst algebraisch abgeschlossen ist, heisst ein *algebraischer Abschluss von* K. Ein solcher wird oft bezeichnet mit $\overline{K}$.

6.4.6 Satz: Je zwei algebraische Abschlüsse von K sind isomorph über K.

6.4.8 Satz: Jeder Körper besitzt einen algebraischen Abschluss.

Beweis: Setze $S_K := K[X]\setminus K$.

Lemma 1: $\forall f_1,\dots,f_n \in S_K \ \exists L/K$ endlich so dass jedes f_i eine Nullstelle in L hat.

Beweis: Zerfällungskörper von $f_1\cdots f_n$ hat's. qed

$\boxed{\text{Lemma 2: } \exists K'/K \text{ algebraisch so dass jedes } f\in S_K \text{ in } K' \text{ eine Nullstelle hat.}}$

Beweis: Für jedes $f\in S_K$ wähle Variable X_f. Setze $R := K[X_f \mid f\in S_K]$.

Betrachte das Ideal $I = (\{f(X_f) \mid f\in S_K\}) \subset R$.

Beh.: $I \neq R$. Beweis: Wenn $I=R$, wähle $f_1,\dots,f_m\in S_K$ und $g_1,\dots,g_m\in R$ mit $\boxed{\sum g_i\cdot f_i(X_{f_i})=1}$. Dann existieren $f_{m+1},\dots,f_n\in S_K$ so dass jedes $g_i\in K[X_{f_1},\dots,X_{f_n}] =: R'$ und $(f_1(X_{f_1}),\dots,f_n(X_{f_n}))_{R'} = R'$.

Sei L/K wie in Lemma 1, mit $a_i \in L$ eine Nullstelle von f_i.

$R' \xrightarrow{\varphi} L$, $X_{f_i} \mapsto a_i$. Homo, id auf K.

$\Rightarrow \varphi(f_i(X_{f_i})) = f_i(\varphi(X_{f_i})) = f_i(a_i) = 0$

$\Rightarrow 1 = \varphi(1) = \sum \varphi(g_i) \cdot \varphi(f_i(X_{f_i})) = 0 \Rightarrow$ Widerspruch! qed (Beh.)

Krull $\Rightarrow \exists$ max. Ideal $m \subset R$ mit $I \subset m$.

$\Rightarrow K' := R/m$ Körper. Sei $R \xrightarrow{\pi} R/m = K'$

$\Rightarrow \forall f \in S_K: f(\underbrace{\pi(X_f)}_{\in K'}) = \pi(\underbrace{f(X_f)}_{\in I < m}) = 0$. Insbesondere ist $\pi(X_f)$ algebraisch über K.

Da K' als K-Algebra von den $\pi(X_f)$ für alle $f \in S_K$ erzeugt

$\Longrightarrow K'/K$ algebraisch. qed (Lemma 2)

Setze $K_0 := K$, $K_1 := K'$, usw. ... Konstruiere K_{n+1} aus K_n wie in Lemma 2.

$K_0 \subset K_1 \subset \dots \subset K_\infty := \bigcup_{n \geq 0} K_n$ = Körper

Induktion $\Rightarrow$ jedes K_n/K algebraisch $\Rightarrow K_\infty/K$ algebraisch.

Sei $f \in K_\infty[X] \setminus K_\infty \Rightarrow \exists n: f \in K_n[X] \setminus K_n \Rightarrow f$ hat eine Nullstelle in K_{n+1}.

$\Rightarrow f$ hat Nullstelle in K_∞. $\Rightarrow K_\infty$ alg. abg. qed.

6.5 Separable und irreduzible Polynome

Betrachte einen algebraischen Abschluss $\overline{K}$ von K. Aufgrund der Eindeutigkeit von $\overline{K}$ bis auf Isomorphie ist der folgende Begriff unabhängig von der Wahl von $\overline{K}$.

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

6.5.2 Vorsicht: Manche Autoren verwenden diese Definition nur für irreduzible Polynome und eine *dazu nicht äquivalente* für reduzible Polynome. Die hier benutzte Definition hat den folgenden Vorteil:

6.5.3 Proposition: Für jede Körpererweiterung L/K gilt: Ein Polynom $f \in K[X] \smallsetminus \{0\}$ ist separabel über K genau dann, wenn es separabel als Polynom über L ist.

Bew: Sei $\overline{L}$ ein alg. Abschluss von L.

Wähle $\overline{K}$:

$$\begin{array}{ccc} & & \overline{L} \\ \overline{K} & \overset{\exists}{\hookrightarrow} & | \\ & & L \\ & K & \end{array}$$

$\Rightarrow$ Fasse $\overline{L}$ als Erweiterung von $\overline{K}$ auf.

f separabel über $K \Leftrightarrow$ keine mehrfachen Nullstellen in $\overline{K}$
$\qquad\qquad\;\; \ldots\; L \;\ldots \qquad\qquad \longrightarrow \overline{L}$

f zerfällt über $\overline{K}$ in Linearfaktoren $\Rightarrow$ alle Nullstellen von f in $\overline{L}$ liegen schon in $\overline{K}$. qed.

6.5.4 Proposition: Für jede Körpererweiterung L/K gilt: Zwei Polynome $f, g \in K[X] \smallsetminus \{0\}$ sind teilerfremd in $K[X]$ genau dann, wenn sie teilerfremd in $L[X]$ sind.

Bew: "$\Leftarrow$" leicht.

"$\Rightarrow$": f, g teilerfremd in $K[X] \Longrightarrow \exists\, u, v \in K[X]$: $f \cdot u + g \cdot v = 1$

gilt auch in $L[X]$

$\Longrightarrow f, g$ teilerfremd in $L[X]$. qed.

6.5.5 Definition: Die *formale Ableitung* eines Polynoms $f(X) = \sum_k' a_k X^k$ ist das Polynom

$$f'(X) \;:=\; \tfrac{df}{dX}(X) \;:=\; \sum_k' a_k k X^{k-1}.$$

6.5.6 Proposition: Die formale Ableitung erfüllt die üblichen Regeln:

$$\boxed{\begin{aligned} \forall f,g \in K[X]:&\quad (f \pm g)' \;=\; f' \pm g' \\ \forall a \in K\ \forall f \in K[X]:&\quad (af)' \;=\; af' \\ \forall f,g \in K[X]:&\quad (fg)' \;=\; f'g + fg' \quad \text{(Leibniz-Regel)} \end{aligned}}$$

Genügt auf Basis! $(X^k X^l)' = (X^{k+l})' = (k+l)\cdot X^{k+l-1} = k\cdot X^{k-1}\cdot X^l + X^k\cdot l X^{l-1}$
$= (X^k)'\cdot X^l + X^k \cdot (X^l)'$.

6.5.7 Proposition: Ein Polynom $f \in K[X] \smallsetminus \{0\}$ ist separabel genau dann, wenn f und f' teilerfremd in $K[X]$ sind.

Beweis: Sei $a \in \bar{K}$ eine Nullstelle der Vielfachheit $\nu \geq 1$ von f.
Schreibe $f(X) = (X-a)^\nu \cdot g(X)$ für $g \in \bar{K}[X]$ und $g(a) \neq 0$.
$\Rightarrow\; f'(X) = \nu (X-a)^{\nu-1}\cdot g(X) + (X-a)^\nu \cdot g'(X)$
Ist $\nu \geq 2$, dann ist $(X-a)$ teilt f' in $\bar{K}[X]$. $\Rightarrow f, f'$ nicht teilerfremd in $\bar{K}[X]$
$\overset{6.5.4}{\Rightarrow}$ nicht teilerfremd in $K[X]$.
D.h.: f nicht separabel $\Rightarrow f, f'$ nicht teilerfremd.
Sei f separabel $\Rightarrow \nu = 1 \Rightarrow f'(a) = g(a) + 0 \neq 0 \Rightarrow (X-a) \nmid f'$ in $\bar{K}[X]$.

$\Rightarrow f, f'$ haben keine gemeinsamen Nullstellen in $\bar{K}$ $\Rightarrow$ teilerfremd in $\bar{K}[X] \Leftrightarrow$ auch in $K[X]$ z.z.

6.5.8 Proposition: Ein irreduzibles Polynom $f \in K[X]$ ist separabel genau dann, wenn $f' \neq 0$ ist.

Beweis: $f' = 0 \Rightarrow f \mid f' \Rightarrow f, f'$ nicht teilerfremd $\overset{6.5.7}{\Rightarrow} f$ nicht separabel

$f' \neq 0 \Rightarrow \left.\begin{array}{l} \deg(f') < \deg(f), \\ f \text{ irred.} \end{array}\right\} \Rightarrow f, f'$ teilerfremd $\overset{6.5.7}{\Rightarrow} f$ separabel. qed.

Erinnerung:

3.1.3 Proposition: Jeder Körper K besitzt einen eindeutigen kleinsten Unterkörper. Dieser ist entweder isomorph zu $\mathbb{Q}$ oder zu $\mathbb{F}_p$ für eine eindeutige Primzahl p.

3.1.4 Definition: Dieser Unterkörper heisst der *Primkörper von* K, und die Zahl

$$\mathrm{char}(K) := \begin{cases} 0 & \text{falls der Primkörper } \mathbb{Q} \text{ ist,} \\ p & \text{falls der Primkörper } \mathbb{F}_p \text{ ist,} \end{cases}$$

heisst die *Charakteristik von* K.

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

(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.

Bew.: (a) $\mathrm{Char}(K) = 0 \Rightarrow \forall f \in K[X] \setminus K$: $\deg(f') = \deg(f) - 1$.

da $f(X) = aX^n +$ kleinere Terme mit $a \neq 0$ und $n > 0$.

$\Rightarrow f'(X) = n \cdot a \cdot X^{n-1} +$ kleinere Terme mit $na \neq 0$.

Also f irred. $\Rightarrow f' \neq 0 \overset{6.5.8}{\Longrightarrow} f$ separabel.

(b) Falls $f' \neq 0$ genauso: f sep, also $r = 0$, $g = f$. ✓

Sei also $f' = 0$. Schreibe $f(X) = \sum_{i \geq 0}' a_i X^i \Rightarrow f'(X) = \sum_{i \geq 0}' i \cdot a_i \cdot X^{i-1}$

$\Rightarrow \forall i \geq 0$: $i a_i = 0$.

D.h.: $\forall i \geq 0$: $p \nmid i \Rightarrow i \cdot 1_K \in \mathbb{F}_p^\times$ $\Big\} \Rightarrow a_i = 0$.

$\Rightarrow f(X) = \sum_{j \geq 0}' a_{pj} X^{pj} = g(X^p)$ für $g(X) := \sum_{j \geq 0}' a_{pj} \cdot X^j$.

f irred. $\Rightarrow g$ irred.

Fertig mit Induktion über $\deg(f)$. qed.

6.5.10 Beispiel: Betrachte den rationalen Funktionenkörper $K := \mathbb{F}_p(Y)$ und das Polynom $g(X) := X - Y \in K[X]$. Für jedes $r \geqslant 1$ ist dann $g(X^{p^r}) = X^{p^r} - Y$ irreduzibel über K, aber nicht separabel.

$\shortparallel$

$f(X)$ $\mathbb{F}_p[X, Y]$.

$\Rightarrow f'(X) = p^r \cdot X^{p^r - 1} = 0$ falls $r \geq 1$.

Sei $L = K(Z)$ ein Stammkörper von f

$\Rightarrow 0 = f(Z) = Z^{p^r} - Y \Rightarrow Y = Z^{p^r}$

$\Rightarrow f(X) = X^{p^r} - Z^{p^r} = (X - Z)^{p^r}$

6.6.3.

$\Rightarrow f$ hat genau 1 Nullstelle in $\overline{K}$.

6.6 Perfekte Körper

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

6.6.2 Proposition: Jeder Körper der Charakteristik 0 ist perfekt.

6.6.3 Proposition-Definition: 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

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

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

Bem.: Genügt für $r = 1$, da durch Iteration.

$\Longrightarrow (xy)^p = x^p y^p$

$1^p = 1$

$$(x+y)^p = \sum_{k=0}^{p} \underbrace{\binom{p}{k}}_{= \frac{p!}{k!(p-k)!}} \cdot x^k \cdot y^{p-k}$$

$\in \mathbb{Z}$

$= x^p + y^p$

$\binom{p}{0} = \binom{p}{p} = 1.$

Für $0 < k < p$ teilt p den Zähler, aber nicht den Nenner.

$\Longrightarrow \binom{p}{k} \equiv 0 \mod p.$

qed.