Satz 18.5 Sei $L:K$ eine separable Körpererweiterung und sei M ein Zwischenkörper, also $K \subseteq M \subseteq L$.
Dann sind die Körpererweiterungen $M:K$ und $L:M$ separabel.

Beweis: Es ist klar, dass mit $L:K$ auch $L:M$ und $M:K$ algebraisch sind, und dass $M:K$ separabel ist.

- Sei $\alpha \in L$ mit Minimalpolynom $h \in K[X]$ über K und $\bar{h} \in M[X]$ über M. Dann ist $h = \bar{h} \cdot g$ für ein $g \in M[X]$.
- Da nun h separabel ist (nur einfache Nullstellen besitzt) ist auch $\bar{h}$ separabel, d.h. α ist separabel über M. $L:K$ sep. ⊣

Korollar 18.6 Jeder endliche Körper ist perfekt.

Beweis: Folgt aus Prp. 18.3 ($\mathbb{F}_p$ ist perfekt), Satz 18.5 und Satz 16.5. $\left[K = \mathbb{F}_p,\ M = \mathbb{F}_p[X]/(g),\ L = M[X]/(g) \cong \mathbb{F}_p[X]/(h) \right]$ ⊣

Bem. In Aufgabe 108 wird ein Kriterium für irred. inseparable Polynome $f \in K[X]$ (mit $\mathrm{char}(K) = p$) gegeben.

19. Die Galoisgruppe

Def. Es sei $L:K$ eine Körpererweiterung.

- Ein Isomorphismus $\sigma: L \xrightarrow{\sim} L$ mit $\sigma|_K = id.$ heißt K-Automorphismus von L (oder Autom. über K).
- Die K-Automorphismen von L bilden unter der Komposition als Verknüpfung eine Gruppe, die sogenannte Galoisgruppe $Gal(L:K)$ von L über K.

Bsp. $\mathbb{Q}(i):\mathbb{Q}$; $\mathbb{Q}$-Basis ist $\{1, i\}$; $\sigma \in \mathbb{Q}(i) \xrightarrow{\sim} \mathbb{Q}(i)$, $\sigma|_{\mathbb{Q}} = id.$

Dann gilt $(\sigma(i))^2 = \sigma(i)\cdot\sigma(i) = \sigma(i\cdot i) = \sigma(-1) = -1.$

Somit gilt $\sigma(i) = i$ (d.h. $\sigma = id.$) oder $\sigma(i) = -i$, [andere Nullst. von X^2+1]

also $\sigma(a+ib) = a - ib$ mit $\sigma^2 = id.$

D.h. $Gal(\mathbb{Q}(i):\mathbb{Q}) \cong C_2$.

Satz 19.1 Es sei $L:K$ eine Körpererweiterung mit $G = Gal(L:K)$.

Weiter sei $H \leq G$ eine Untergruppe von G. Dann ist

$$L^H := \{a \in L : \forall \sigma \in H\ (\sigma(a) = a)\} \subseteq L$$

ein Unterkörper von L mit $K \subseteq L^H \subseteq L$,

Weiter gilt $H \leq Gal(L:L^H)$.

Beweis: Mit $a, b \in L^H$ ist auch $a-b$ und ab^{-1} [$b \neq 0$] in L^H.

Weiter gilt $K \subseteq L^H$, und weil jeder L^H-Autom. von L auch ein K-Autom. von L ist, ist $H \leq Gal(L:L^H)$. ⊣

Def. Der Körper $L^H \subseteq L$, der von den Autom. aus $H \leq Gal(L:K)$ (punktweise) fixiert wird, heißt Fixkörper zur Untergruppe H.

Satz 19.2 Sei $L:K$ eine Körpererweiterung mit $G=\mathrm{Gal}(L:K)$. Weiter sei M ein Zwischenkörper, also $K\subseteq M\subseteq L$. Dann ist

$$G_M := \{\sigma\in G : \forall b\in M\,(\sigma(b)=b)\} = \mathrm{Gal}(L:M).$$

Insbesondere ist $G_M \leq \mathrm{Gal}(L:K)$.

Beweis: Mit $\sigma,\tau\in G_M$ ist auch $\sigma\circ\tau^{-1}\in G_M$, damit ist $G_M\leq \mathrm{Gal}(L:K)$. Weil jedes $\sigma\in G_M$ ein M-Autom. von L ist, und umgekehrt jeder M-Autom. von L in G_M ist, gilt $G_M=\mathrm{Gal}(L:M)$. ⊣

Zur Galoisgruppe einer Körpererweiterung:
Sei $L:K$ eine alg. Körpererweiterung und sei $f\in K[X]$ mit $\mathrm{grad}(f)=n$ das Min.-Poly. von einem $\alpha\in L$. Weiter sei $\sigma\in\mathrm{Gal}(L:K)$, dann gilt:

$$0=\sigma(0)=\sigma(f(\alpha))=\sigma(a_0+a_1\alpha+\ldots+a_n\alpha^n) \qquad [\sigma|_K=\mathrm{id}.]$$
$$=a_0+a_1\sigma(\alpha)+\ldots+a_n\sigma(\alpha)^n=f(\sigma(\alpha))$$

Mit α ist also auch $\sigma(\alpha)$ eine Nullstelle von f.

Def. Sei $L:K$ eine Körpererweiterung, sei $\alpha\in L$ alg. über K und sei $f\in K[X]$ das Min.-Poly. von α über K. Die Nullstellen in L des Polynoms $f\in K[X]$ heissen die in L zu α konjugierten Elemente.

Bsp. $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$; $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$

Aus der Definition und den obigen Ausführungen folgt direkt

Korollar 19.3 Ist $L:K$ alg., $\alpha\in L$, $\sigma\in\mathrm{Gal}(L:K)$, so ist $\sigma(\alpha)$ in L zu α konjugiert.

Sei $L_f \supseteq K$ der Zerfällungskörper eines Polynoms $f \in K[X]$.
D.h. $L_f = K(\alpha_1, \dots, \alpha_n)$ wobei $\alpha_1, \dots, \alpha_n$ die Nullstellen des Polynoms f sind. Mit Kor. 19.3 können wir jedem $\sigma \in \mathrm{Gal}(L_f : K)$ eine Permutation $\pi_\sigma \in S_n$ zuordnen, sodass die Abbildung

$$\mathrm{Gal}(L_f : K) \longrightarrow S_n$$
$$\sigma \longmapsto \pi_\sigma$$

ein Homomorphismus ist. Weil nun L_f durch K und $\alpha_1, \dots, \alpha_n$ erzeugt wird, ist dieser Homom. injektiv. Damit ist $\mathrm{Gal}(L_f : K)$ isomorph zu einer Untergruppe von S_n, wobei die n Elemente die permutiert werden die Nullstellen von f sind.

Es gilt somit folgender Satz:

Satz 19.4 Ist L_f der Zerfällungskörper von $f \in K[X]$, dann ist $\mathrm{Gal}(L_f : K)$ isomorph zu einer Untergruppe der Permutationsgruppe der Nullstellen von f.

Def. Ist L_f der Zerfällungskörper von $f \in K[X]$, so heisst $\mathrm{Gal}(L_f : K)$ die Galoisgruppe von f, bezeichnet mit $\mathrm{Gal}(f)$.

Korollar 19.5 Ist $f \in K[X]$ mit $\mathrm{grad}(f) = n$, so gilt
[Bew. Aufg. III]
$$|\mathrm{Gal}(f)| \mid n!$$

Proposition 19.6 Sei $L : K$ eine endl. Körpererweiterung.
Dann gilt $|\mathrm{Gal}(L : K)| \leq [L : K]$.

Dies folgt direkt aus

Satz 19.7 Sei $L : K$ eine endl. Körpererw. und $\varphi : K \to L'$ ein Körperhomom. Dann gibt es höchstens $[L : K]$ verschiedene Körperhomom. $\tilde{\varphi} : L \to L'$ mit $\tilde{\varphi}|_K = \varphi$.

Bem. Setzen wir $L' = L$ und $\varphi = \mathrm{id}$., so ex. höchstens $[L : K]$ versch. Körperhomom. $L \to L'$, also höchstens $[L : K]$ versch. K-Autom. von L.