

Weiter zu A19: (Zerfällungskörper)

19.7. Def: Sei $f \in K[T]$, $n := \deg f > 0$.

$L|K$ heißt ZK von f über K

$\Leftrightarrow \exists x_1, \dots, x_n \in L \exists a \in K:$

$$f(T) = a \prod_{i=1}^n (T - x_i) \text{ und } L = K(x_1, \dots, x_n).$$

19.8. Bsp.: Sei $p \in \mathbb{N}$ prim, $f = T^p - 1 \in \mathbb{Q}[T]$.

Gesucht: ZK von $f|Q$?

Die Wurzeln von f in $\mathbb{C}$ sind die p.w.

Komplexen Zahlen ζ^k , $0 \leq k < p$,

mit $\zeta := e^{2\pi i/p}$, die man p-te

Einheitswurzeln nennt.

$$f(T) = (T-1) \cdot (T^{p-1} + T^{p-2} + \dots + T + 1)$$

Somit:

$\Phi_p(T) \in \mathbb{Q}[T]$ ist irred. (nach Bsp. A15.17, Eisenstein)

$$f = \prod_{a=0}^{p-1} (T - \zeta^a) \in \mathbb{C}[T] \Rightarrow \Phi_p(T) = \prod_{a=1}^{p-1} (T - \zeta^a) \in \mathbb{C}[T]$$

↑
ist Kup von ζ

$$\Rightarrow \mathbb{Q}(\zeta, \zeta^2, \dots, \zeta^{p-1}) = \mathbb{Q}(\zeta) \text{ ist ZK von } f|Q, \text{ ferner: } [\mathbb{Q}(\zeta):Q] = p-1.$$

$$\text{Bsp.: } p=3 \leadsto T^3 - 1 = (T-1)(T^2 + T + 1)$$

$$\uparrow (T-\zeta)(T-\zeta^2), \quad \zeta = e^{2\pi i/3}$$

$$\zeta \text{ bzw } \zeta^2 \text{ ist } = -\frac{1}{2} \pm \sqrt{\frac{1}{4} - 1} = -\frac{1}{2} \pm \frac{i}{2}\sqrt{3}$$

(Vgl. A22)

19.9. Bsp.: Sei $p \in \mathbb{N}$ prim, $g(T) = T^p - 2 \in \mathbb{Q}[T]$. Gesucht: ZK von $g|Q$?

Sei $x \in \mathbb{C}$ mit $x^p = 2$ (z.B. $x = \sqrt[p]{2}$). Die Wurzeln von g sind also

$$x, \zeta x, \zeta^2 x, \dots, \zeta^{p-1} x, \text{ wobei } \zeta = e^{2\pi i/p}.$$

Motivation:

$$K(x_1, \dots, x_n) \leftarrow \underline{\underline{ZK!}}$$

$$K(x_1, x_2)$$

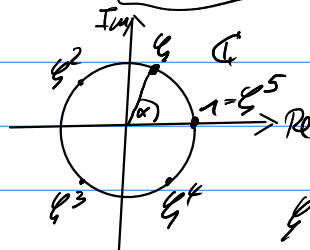
$$K(x_1) \cong K[T]/(f)$$

$$K$$

$$f \in K[T]$$

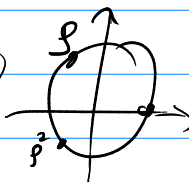
$$\deg(f) = n$$

$$f = (T-x_1) \cdot f_1 \cdot \dots \cdot f_{n-1}$$



$$\zeta = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$$

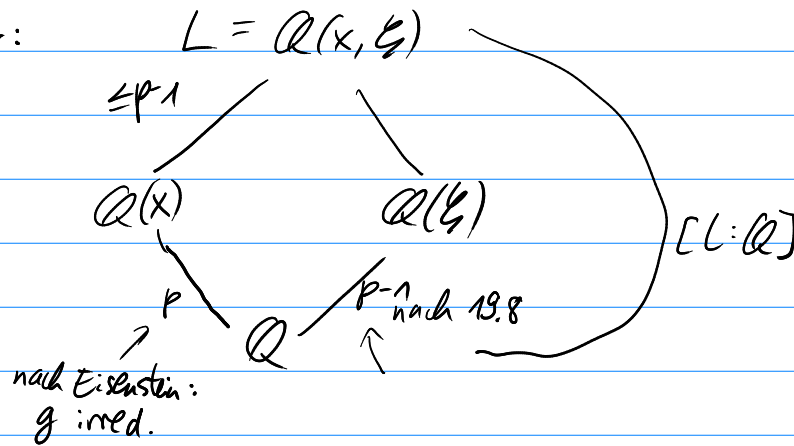
$$\zeta = e^{2\pi i/5}$$



-2-

Setze $L := \mathbb{Q}(x, \xi, \dots, \xi^{p-1}x) = \mathbb{Q}(\xi, x)$ ist $\mathbb{Z}K$ von $g \mid \mathbb{Q}$

Ferner:



Bsp. $\mathbb{Z}K$ von $T^5 - 2$
ist $\mathbb{Q}(e^{2\pi i/5}, \sqrt[5]{2})$

$$[L : \mathbb{Q}(x)] = [\mathbb{Q}(x, \xi) : \mathbb{Q}(x)] \leq p-1.$$

das Mipo von $\xi/\mathbb{Q}$
hat auch Koeff. in $\mathbb{Q}(x)$

Somit: $[L : \mathbb{Q}] \leq p \cdot (p-1)$.

Da p und $p-1$ Teiler von $[L : \mathbb{Q}]$ sind, folgt: $[L : \mathbb{Q}] = p(p-1)$.

19.10. Lemma: Sei L/K $\mathbb{Z}K$ eines $f \in K[T]$, $\deg(f) = d \Rightarrow [L : K] \leq d!$.

Bew.: VI nach d ...

□

Eigenschaften des $\mathbb{Z}K$:

19.11. Satz: Sei K Körper, $f \in K[T]$, $\deg f = d > 0$. Dann:

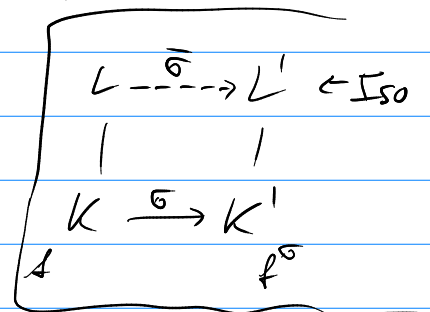
(1) $\exists \mathbb{Z}K$ von $f \mid K$,

(2) $\sigma : K \rightarrow K'$ Iso, $L|K$, $L'|K'$ seien $\mathbb{Z}K$ von $f \mid K$ bzw. $f^\sigma \mid K'$
 $\Rightarrow \sigma$ forts'ber zu Iso $\bar{\sigma} : L \rightarrow L'$.

Bew.: (1): VI nach d ... (s. Motivation)

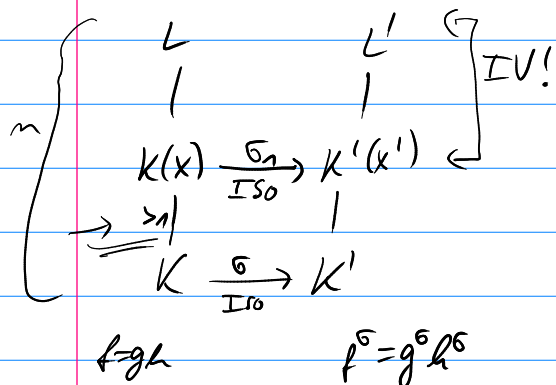
(2): VI nach $m = [L : K]$. ($\leq d!$)

$m=1$: $L=K$, $\bar{\sigma}=\sigma$.



-3-

$n > 1$: Sei $f = g \cdot h$, $g \in K[T]$ irred. mit $\deg(g) \geq 1$, $g(x) = 0$.

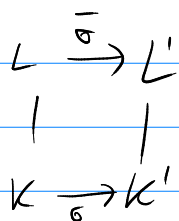


Nach 19.2(2): $\exists$ Forts. $\sigma_n: K(x) \rightarrow K'(x')$,
wenn x' Wurzel von f^σ .

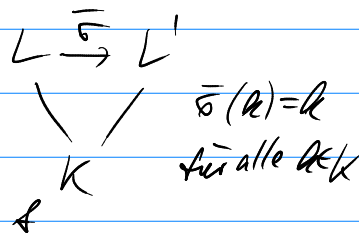
Nun: $L \not\subset K$ von $f \mid K(x)$
 $L' \not\subset K$ von $f^\sigma \mid K'(x')$

daher $[L:K(x)] < n$.

IV auf $\sigma_n: K(x) \rightarrow K'(x')$, f, f', L, L'
 liefert Forts. $\bar{\sigma}: L \rightarrow L'$ (Iso) von σ_n
 bzw. von σ . $\square$



Spezialfall: $\sigma = \text{id}$, $K = K' \rightarrow$



19.12 Satz: Sei L/K endl. Dann sind äquiv.:

(1) L ist $\mathbb{Z}K$ eines $f \in K[T]$ über K

$E \rightarrow E$ || (2) Für jeden Auto $\sigma: E \rightarrow E$, $E \mid L$, mit $\sigma|_K = \text{id}_K$, gilt: $\sigma(L) = L$.

(3) Für jedes irred. $g \in K[T]$ mit $(\exists x \in L: g(x) = 0)$ gilt:
 g zerfällt über L in Linearfaktoren.

19.13 Def.: Eine endl. Erw. L/K heißt normal, wenn eine der Bed. (1), (2) oder (3)
 aus 19.12 erfüllt ist. $\hookrightarrow$ (d.h. ist $\mathbb{Z}K$ eines $f \mid K$)

Bew. von 19.12: (1) $\Rightarrow$ (2): Sei $L = K(x_1, \dots, x_n)$, $x_1, \dots, x_n$ die Wurzeln von $f \in K[T]$.
 Sei $f = \sum_{i=0}^n a_i T^i$ und $\sigma: E \rightarrow E$ Auto, $E \mid L$,
 $\sigma|_K = \text{id}_K$. (nicht notw. p.w.v.)

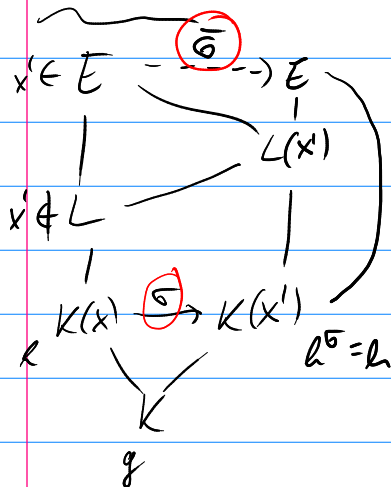
Dann: $0 = \sigma(f(x_j)) = \sum_{i=0}^n \underbrace{(\sigma a_i)}_{=a_i} (\sigma x_j)^i = f(\underbrace{\sigma x_j}_{\uparrow})$.

- 4 -

$$\text{Also: } \{\sigma x_1, \dots, \sigma x_m\} = \{x_1, \dots, x_m\} \Rightarrow \sigma L = \sigma K(x_1, \dots, x_m) = \underbrace{K(x_1, \dots, x_m)}_{\substack{\text{werden mit } \sigma \\ \text{permuriert!}}} = L$$

vgl. Notation: $\sigma \in S_m$

(2) $\Rightarrow$ (3): Sei $L = K(x_1, \dots, x_m)$, $g_i \in K[T]$ seien die Mipo von x_i , $1 \leq i \leq m$.



Sei $g \in K[T]$ irred. mit $x \in L$,

sei E/L ein $\mathbb{Z}K$ von $g \cdot g_1 \dots g_m = h \cdot k$.

Ann.: $\exists$ Wurzel $x' \in E$ von g , $x' \notin L$.

Nach Lemma 19.6 ex. Iso $\sigma: K(x) \rightarrow K(x')$,
 $\sigma|_K = \text{id}_K$.

E ist $\mathbb{Z}K$ von $L/K(x)$, E ist $\mathbb{Z}K$ von $L^\sigma = L/K(x')$

Nach Satz 19.11 ex. Forts. $\bar{\sigma}: E \rightarrow E$,

Auto mit $\bar{\sigma}(x) = x' \notin L \Rightarrow x \notin L$ (2) $\Rightarrow$ (3).

(3) $\Rightarrow$ (1): Sei $L = K(x_1, \dots, x_m)$, und $g_i \in K[T]$ die Mipo von x_i $\mid K$,
 $1 \leq i \leq m$, sei $g := g_1 \dots g_m$.

Da die g_i in L in Lin.faktoren zerfallen, also ist L ein $\mathbb{Z}K$ von g/K . $\square$

$\hookrightarrow$ galsis = normal & separabel

A 20: Separabilität

20.1. Einführung: Polynom, das nur p.w.v. Wurzeln in einem $\mathbb{Z}K$ hat, heißt separabel.

20.2. Def.: $f \in K[T]$ separabel $\Leftrightarrow$ f hat in einem $\mathbb{Z}K$ lauter verschiedene Wurzeln, d.h. $f = a \prod_{i=1}^m (T - x_i)$, die $x_i \in L$ sind pwv.

20.3. Def.: formale Ableitung von $f = \sum_{i=0}^m a_i T^i \in K[T]$ ist $f' := \sum_{i=1}^m i a_i T^{i-1}$.

20.4. Lemma: $\forall f, g \in K[T] \forall a \in K: (f+g)' = f' + g', (af)' = af',$
 $(f \cdot g)' = f'g + fg'.$ [✓]

20.5. Satz: $f \in K[T]$ separabel $\Leftrightarrow \gcd(f, f') = 1$ (= das Konst.-1-Polynom).

Bew.: Seien $x_1, \dots, x_m$ die Wurzeln von f in $\mathbb{Z}K L$ von $f|K$.

Dann $\gcd(f, f') = 1 \Leftrightarrow \forall i: (T - x_i) \nmid f'$ in $L[T]$ [vgl. 20.6]

$\Leftrightarrow \forall i: f'(x_i) \neq 0.$

x_i sei Wurzel der Vielfachheit μ_i , d.h. $f = (T - x_i)^{\mu_i} f_1, f_1(x_i) \neq 0$.

Dann: $f' = \mu_i (T - x_i)^{\mu_i - 1} f_1 + (T - x_i)^{\mu_i} f_1'$

also: $f'(x_i) = 0 \Leftrightarrow \mu_i - 1 \geq 1 \Leftrightarrow \mu_i \geq 2.$

Also: $\forall i: f'(x_i) \neq 0 \Leftrightarrow \forall i: \mu_i = 1 \Leftrightarrow f$ separabel. □

20.6. Bem.: Sei $L|K$, h sei ein ggT von $f, g \in K[T]$ in $K[T]$,
dann h auch ggT von f, g in $L[T]$.

Bew.: $L[T], K[T]$ sind HIB.

$$\exists x, y \in K[T]: h = xf + yg,$$

$$\text{sei } t \in L[T]: \exists u, v \in L[T] \text{ mit } f = ut, g = vt.$$

$$\text{Dann: } xut = xf = h - yg = h - yvt \Rightarrow (xu + yv)t = h \Rightarrow t|h.$$

$$\text{Also: } h \text{ ein ggT}(f, g) \text{ in } L[T]. \quad \square$$

20.7. Kor.: Sei $f \in K[T]$ ired. Dann: f separabel $(\Leftrightarrow) f' \neq 0$.

Bew.: Es ist $\text{ggT}(f, f') = \begin{cases} f, & f' = 0, \text{ weiter Satz 20.5} \\ 1, & f' \neq 0 \end{cases}$ denn: $q|f, q|f'$

$$\stackrel{f \text{ ired.}}{\Rightarrow} q=1 \text{ oder } q=f \quad f|f', \quad \begin{matrix} \text{in } \deg f' \\ = \deg f \end{matrix}$$

20.8. Kor.: $\text{Char } K = 0 \Rightarrow$ jedes $f \in K[T]$
das ired. ist, ist separabel.

Bew.: $\text{Char } K = 0 \Rightarrow \deg f' = \deg f - 1$, also $f' \neq 0$. $\square$

20.9. Def.: Sei $L|K$, $x \in L$ alg. $|K$.

x heit separabel $|K$, falls $\exists$ sep. $f \in K[T]: f(x) = 0$

$(\Leftrightarrow)$ Minp. von $x|K$ ist separabel.

20.10. Def.: $L|K$ heit separable (algebraische) Erw. von K

$\Leftrightarrow \forall x \in L: x \text{ ist sep. } |K$.