Alg '18, Blatt 13

A1 | $a_i \in L$ algebraisch $/K$, alle $i \in I$

Beh: $L_0 := K((a_i)_{i \in I})$ ist eine algebraische KE über K.

Bew: Nach Def. $\overset{(3.2.1)}{}$ ist L_0 der kleinste UK von L, der K und alle a_i enthält. Also ist L_0 ein Körper.

Nach Satz 3.4.2 ist

$$A_K := \{a \in L \mid a \text{ alg } /K\} \text{ ein UK von } L.$$

Es gilt A_K enthält K und alle a_i.

Also $A_K \supseteq L_0$. D.h. jedes Element von L_0 ist algebraisch $\Rightarrow$ L_0/K algebraisch.

Alg'18, Blatt 13

A2| a) $f(X) := X^3 + X + 3$ mit Nullstellen $a_1, a_2, a_3 \in \mathbb{C}$.

Nach Hinweis ist $f'(X) = 3X^2 + 1$.

[Wenn f als Funktion $\mathbb{R} \to \mathbb{R}$ betrachtet, die ist stetig].

So ist $\left.\begin{array}{l} f(-2) = -8-2+3 = -7 \\ f(-1) = -1-1+3 = 1 \end{array}\right\} \xRightarrow{\text{Zwstz}} \exists a_1 \in (-2,-1) \subseteq \mathbb{R}$ mit $f(a_1) = 0$.

Außerdem, da $f'(a) \geq 1 > 0$ für alle $a \in \mathbb{R}$, ist

$f(b) < 0$, $\forall b < a_1$ und $f(c) > 0$, $\forall c > a_1$.

(b) $K := \mathbb{Q}(a_1)$, L der Zerfällungskörper von f.

Beh: $[L:K] = 2$

Bew.

$L \leq \mathbb{C}$ und $f(X) = (X-a_1)(X-a_2)(X-a_3)$ über L. Nach (a) ist

$a_1 \in K$ und $a_2, a_3 \in \mathbb{C} \setminus K$, da $K \subseteq \mathbb{R}$.

Also $\deg(\mathrm{MiPo}_{a_j/K}) \gneq 1$ für $j \in \{2,3\}$.

$\Rightarrow [L:K] \geq 2$.

Aber $L \geq K \geq \mathbb{Q} \Rightarrow [L:\mathbb{Q}] = \underbrace{[L:K]}_{\geq 2} \cdot \underbrace{[K:\mathbb{Q}]}_{=3} \geq 6$.

da $f = \mathrm{MiPo}_{a_1/\mathbb{Q}}$ hat Grad 3.

Umgekehrt,
Satz 3.5.2 $\Rightarrow [L:\mathbb{Q}] \leq 3! = 6$ $\boxed{(*)\ f \text{ irr}/\mathbb{Q}}$

Also $[L:\mathbb{Q}] = 6 \Rightarrow [L:K] = 2$.

Alg '18, Blatt 13

A2 (b) (*): Beh: $f(x) = X^3 + X + 3$ ist irreduzibel über $\mathbb{Q}$.

⌈Bew: Da $\deg f \leq 3$, genügt um zu zeigen, dass f keine Nst in $\mathbb{Q}$ hat.

Angenommen (zum $\lightning$) $a \in \mathbb{Q}$ mit $f(a) = 0$.
Offensichtlich $a \neq 0$. Also $a =: \frac{P}{Q}$ mit $P, Q \in \mathbb{Z} \setminus \{0\}$ und $ggT(P, Q) = 1$.

$$\Rightarrow f(a) = f(P/Q) = \frac{P^3}{Q^3} + \frac{P}{Q} + 3 = 0$$

$$\Rightarrow P^3 + P.Q^2 + 3.Q^3 = 0$$

$$\Rightarrow P^3 = -Q^2(P + 3Q)$$

$$\Rightarrow Q^2 \mid P^3$$

$$\Rightarrow ggT(P, Q) \neq 1 \quad \lightning$$

⌟

Also mit (a), $a_1 \in \mathbb{R} \setminus \mathbb{Q}$.

Alg '18, B13

A2 (c) Beh (i): $\mathrm{Aut}(\mathbb{Q})$ ist trivial.

Bew. Sei $\sigma \in \mathrm{Aut}(\mathbb{Q})$. Es gilt $\sigma(1)=1$, $\sigma(0)=0$.

Für jedes $n \in \mathbb{N}^{>0}$ ist $n = \underbrace{1+\cdots+1}_{n\text{-mal}}$. Also $\sigma(n) = \underbrace{\sigma(1)+\cdots+\sigma(1)}_{n\text{-mal}}$

$\Rightarrow \sigma(n) = n$

Auch für alle $m \in \mathbb{Z}$, $\sigma(m)=m$. Für $q \in \mathbb{Q}$ ist $q = \frac{n}{m}$, $m \neq 0$.

weil $\sigma(-x) = -\sigma(x)$

Es gilt $\sigma(q) = \frac{\sigma(n)}{\sigma(m)} = \frac{n}{m} = q$, $\forall q \in \mathbb{Q}$

$\Rightarrow \mathrm{Aut}(\mathbb{Q}) = \{id\}$.

Beh (ii) $\mathrm{Aut}(K) = \mathrm{Aut}(\mathbb{Q}(a_1))$ ist trivial.

Bew: Wie in B11, A2 / Beispiel 2.2.8, für jedes $b \in \mathbb{Q}(a_1)$

(*) ist $b = b_0 + b_1 a_1 + b_2 a_1^2$ für geeignete $b_0, b_1, b_2 \in \mathbb{Q}$.

Sei $\sigma \in \mathrm{Aut}(K)$.

Für jedes $c \in \mathbb{Q}$ ist $\sigma(c) = c$, wie oben in (i).

Also $\mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{Q})$.

(mit Hinweis) Nach Hinweis (Satz 3.4.15) ist die Bahn $\mathrm{Aut}(\mathbb{Q}^{alg}/\mathbb{Q}).a_1 \subseteq \{a_1, a_2, a_3\}$. [Bem: $\mathbb{Q}^{alg} \subsetneq \mathbb{C}$]

(oder Alternativ): [Muss $\sigma(a_1)$ eine Nullstelle von f sein, also $\sigma(a_1) \in \{a_1, a_2, a_3\}$]

Aber $\sigma(a_1) \neq a_2, a_3$, da $a_2, a_3 \notin K$ (nach (a)).

Also $\sigma(a_1) = a_1$, $\forall \sigma \in \mathrm{Aut}(K)$.

Mit (*), für jedes $b \in \mathbb{Q}(a_1)$ ist dann

$\sigma(b) = \sigma(b_0) + \sigma(b_1)\sigma(a_1) + \sigma(b_2)\cdot\sigma(a_1)^2 = b$.

Alg '18, B 13

A2| d) Beh: $\exists\, \sigma \in Aut(L/K)$ mit $\sigma(a_2) = a_3$ und $\sigma(a_3) = a_2$.

Bew:

Nach 3.4.15 b(ii) ist $Aut(K^{alg}/K).a_2 = Aut(K^{alg}/K).a_3 = \{a_2, a_3\}$

weil $MiPo_{a_2/K} = MiPo_{a_3/K} = f/(X-a_1) \in K[X]$.

Also gibt es $\hat{\sigma} \in Aut(K^{alg}/K)$ mit $\hat{\sigma}(a_2) = a_3$. Nach 3.5.3 (c), so ist $\sigma := \hat{\sigma}_{|L} \in Aut(L/K)$. σ ist bijektiv, so muss $\sigma(a_3) = a_2$ sein.

(e) Bem. dass $L = \mathbb{Q}(a_1, a_2) = \mathbb{Q}(a_2, a_1) = \mathbb{Q}(a_2, a_1, a_3)$

Wie in (c) ist $Aut(L) = Aut(L/\mathbb{Q})$.

Nach 3.4.15 ist die Bahn

$Aut(\mathbb{Q}^{alg}/\mathbb{Q}).a_1 = Aut(\mathbb{Q}^{alg}/\mathbb{Q}).a_2 = \{a_1, a_2, a_3\}$,

weil $MiPo_{a_1/\mathbb{Q}} = MiPo_{a_2/\mathbb{Q}} = MiPo_{a_3/\mathbb{Q}} = f \in \mathbb{Q}[X]$.

D.h.: $\exists\, \hat{\sigma} \in Aut(\mathbb{Q}^{alg}/\mathbb{Q})$ mit $\hat{\sigma}(a_1) = a_2$.

Außerdem, es gilt $\underbrace{\hat{\sigma}(\mathbb{Q}(a_1, a_2, a_3))}_{=\,\hat{\sigma}(L)} = \underbrace{\mathbb{Q}(\hat{\sigma}(a_1), \hat{\sigma}(a_2), \hat{\sigma}(a_3))}_{=\,L}$

Also $\hat{\sigma}_{|L} = \sigma' \in Aut(L)$ mit $\sigma'(a_1) = a_2$.

Zusätzlich hat σ' Ordnung ≤ 3 und $\sigma'(a_2) = a_3$.

Alg'18, B13

A2| 8) Wie in 3.5.2 ist $\mathrm{Aut}(L) = \mathrm{Aut}(L/\mathbb{Q}) \overset{\varphi}{\cong} H \leq \mathrm{Sym}\{a_1, a_2, a_3\}$

wobei $\varphi(\sigma) = (2\,3) \in S_3$ und $\varphi(\sigma') = (1\,2)$ [Fall 1]

oder $\varphi(\sigma') = (1\,2\,3)$ [Fall 2].

Also ist $\mathrm{Aut}(L) \cong \langle (2\,3), (1\,2) \rangle = S_3$ [Fall 1],

oder $\mathrm{Aut}(L) \cong \langle (2\,3), (1\,2\,3) \rangle = S_3$ [Fall 2].

Alg '18, B13 $\quad \sigma \in \mathrm{Aut}(K)$

A3 a) $\hat{\sigma}: K[X] \longrightarrow K[X]$

$$\sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} \sigma(a_i) . X^i$$

Beh: $\hat{\sigma}$ ein Aut. des Rings $K[X]$.

[Bew: (i) $1 \longmapsto \sigma(1) . X^0 = 1$

(ii) $\underbrace{\sum_{i=0}^{n} a_i X^i}_{= f} + \underbrace{\sum_{i=0}^{m} b_i X^i}_{= g} = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i \longmapsto \sum \sigma(a_i + b_i) X^i = \hat{\sigma}(f) + \hat{\sigma}(g)$

(iii) $\sigma(f \cdot g) = \sum_{i=0}^{n+m} \sigma(c_i) X^i \overset{\text{nur Rechnung}}{=} \sigma(f) . \sigma(g)$

wobei c_i die Cauchy koeffizienten, $\left[c_i = \sum_{k=0}^{i} a_k b_{i-k} \right]$.

(iv) $\hat{\sigma}$ ist offensichtlich bijektiv, da σ bijektiv ist]

(b) Also $f = (X - a_1)^{n_1} \cdots (X - a_k)^{n_k} . g$ (*), wobei $g \in K[X]$ keine Nullstellen in K hat.

Beh: $\{\sigma(a_1), \ldots, \sigma(a_k)\}$ ist die Menge der Nullstellen von $\hat{\sigma}(f)$ in K.

[Bew: (*) & (a) $\Rightarrow \hat{\sigma}(f) = (X - \sigma(a_1))^{n_1} . (X - \sigma(a_2))^{n_2} \cdots (X - \sigma(a_k))^{n_k} . \hat{\sigma}(g)$

wobei $\hat{\sigma}(g)$ keine Nullstellen in K hat.

]

Alg' 18, B13

A4 | $K = \mathbb{F}_5(T) = \mathrm{Quot}(\mathbb{F}_5[T])$.

(a) $f = X^5 - T \in K[X]$ ist irreduzibel in $K[X]$ nach Eisenstein (2.7.7) mit $R = \mathbb{F}_5[T]$, weil $f \in R[X]$, ($\deg(f) \geq 1$), $K = \mathrm{Quot}(R)$ und T irreduzibel in R.

(b) $a \in K^{alg}$, $f(a) = 0$.

Beh: $f = (X - a)^5$

Überprüfung: $f(a) = 0 \Rightarrow a^5 = T$.

$(X-a)^5 = X^5 - a^5 + \sum_{k=1}^{4} \binom{5}{k} X^k a^{5-k}$ wie B12, A3 es gilt $5 \mid \binom{5}{k}$.

Also über $\mathbb{F}_5(T)^{alg}$ ist $(X-a)^5 = X^5 - a^5 = X^5 - T$ wie gefordert. ⌟

(c) Also ist $a \in K^{alg}$ das einzige Element (in K^{alg}) mit $\mathrm{MiPo}_{\cdot/K} = X^5 - T$.
Nach Satz 3.4.15 gilt

$$\sigma(a) = a, \quad \forall \sigma \in \mathrm{Aut}(K^{alg}/K).$$

Insbesondere ist $\rho(a) = a, \ \forall \rho \in \mathrm{Aut}(K(a)/K)$

$\rightarrow \mathrm{Aut}(K(a)/K) = \{id\}$, da ρ von a festgelegt ist.