H24T1A5

(c) Geben Sie für jedes $n \in \mathbb{N}$ mit $n \geq 3$ eine Erweiterung $K_n | \mathbb{Q}$ vom Grad n an, die <u>nicht</u> galoissch ist. Bestimmen Sie jeweils die Ordnung $|\mathrm{Aut}_{\mathbb{Q}}(K_n)|$.

(Erinnerung: Ist $L | K$ eine endliche Körper-erweiterung, dann gilt immer $|\mathrm{Aut}_K(L)| \leq [L:K]$, und $|\mathrm{Aut}_K(L)| = [L:K]$ genau dann, wenn $L | K$ galoissch ist.)

Sei $n \in \mathbb{N}$, $n \geq 3$ und $K_n = \mathbb{Q}(\sqrt[n]{2})$.

Es ist $\mu_{\sqrt[n]{2}, \mathbb{Q}} = x^n - 2$, denn: Das Polynom $f_n = x^n - 2 \in \mathbb{Q}[x]$ ist normiert, erfüllt $f_n(\sqrt[n]{2}) = 0$, und ist irreduzibel über $\mathbb{Q}$ auf Grund des Eisenstein-Kriteriums. Daraus folgt

$$[K_n : \mathbb{Q}] = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = \text{grad}(f_n) = n.$$

<u>Beh.</u>: $K_n | \mathbb{Q}$ ist nicht normal (und somit auch nicht galois'sch)

Wäre $K_n | \mathbb{Q}$ normal, dann müsste jedes irreduzible Polynom aus $\mathbb{Q}[x]$, das in K_n eine

E

B

B

mi

(2

Dara

Nullstelle besitzt, über K_n in Linearfaktoren zerfallen. Jede komplexe Nullstelle eines solchen Polynoms müsste also schon in K_n liegen. aber: $f_n \in \mathbb{Q}[x]$ ist irreduzibel und hat in K_n die Nullstelle $\sqrt[n]{2}$ (s.o.) Sei $\zeta_n = e^{2\pi i/n}$ (dies ist eine primitive n-te Einheitswurzel). Auch $\zeta_n \sqrt[n]{2} \in \mathbb{C}$ ist eine Nullstelle von f_n, da

$$f_n(\zeta_n \sqrt[n]{2}) = (\zeta_n \sqrt[n]{2})^n - 2 = \zeta_n^n \cdot (\sqrt[n]{2})^n - 2 = 1 \cdot 2 - 2 = 0$$

Laut der Annahme von oben müsste $\zeta_n \sqrt[n]{2}$ also in $\mathbb{Q}(\sqrt[n]{2})$ liegen, erst recht in $\mathbb{R}$.

Es gilt aber $\zeta_n \sqrt[n]{2} = \sqrt[n]{2} \cdot \left(\cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right) \right)$

$\in \mathbb{R}$ wegen $0 < \frac{2\pi}{n} < \pi \Rightarrow \sin\left(\frac{2\pi}{n}\right) \neq 0$. $\lightning$

Daraus folgt die Behauptung.

Bestimmung der Ordnung von $\mathrm{Aut}_{\mathbb{Q}}(K_n)$:

<u>Beh.</u>: (1) Die Ordnung $|\mathrm{Aut}_{\mathbb{Q}}(K_n)|$ stimmt überein mit der Anzahl der Nullstellen von f_n in K_n.

(2) Diese Anzahl ist gleich 1, falls n ungerade ist, und gleich 2, wenn n gerade ist.

Daraus folgt also insg. $|\mathrm{Aut}_{\mathbb{Q}}(K_n)| = \begin{cases} 1 & \text{falls } n \text{ ungerade} \\ 2 & \text{falls } n \text{ gerade} \end{cases}$

zu (1) Aus dem Fortsetzungssatz wurde in der Vorlesung hergeleitet, dass für bel. Erweiterungskörper K, L von $\mathbb{Q}$ die Anzahl der $\mathbb{Q}$-Hom. $K \to L$ übereinstimmt mit der Anzahl der Nullstellen von $\mu_{\alpha,\mathbb{Q}}$ in L, falls $K = \mathbb{Q}(\alpha)$ für ein $\alpha \in K$ gilt. Anwendung hier: Die Anzahl der $\mathbb{Q}$-Hom. $\mathbb{Q}(\sqrt[n]{2}) \to \mathbb{Q}(\sqrt[n]{2})$ stimmt überein mit der Anzahl der Nullstellen von $\mu_{\sqrt[n]{2},\mathbb{Q}} = f_n$ in $\mathbb{Q}(\sqrt[n]{2})$. Da $\mathbb{Q}(\sqrt[n]{2})|\mathbb{Q}$ eine algebraische Erwei-

Im Fall
Also sei
$= e^{\pi i} \sqrt[n]{\ldots}$
im Körper

F14T1

$L = \mathbb{F}_p($
über $\mathbb{F}_p$

(a) Das
$K[x]$

(b) Die Er
normal

... der Anzahl der

torung ist, stimmt die Menge der $\mathbb{Q}$-Hom. $\mathbb{Q}(\sqrt[n]{2}) \to \mathbb{Q}(\sqrt[n]{2})$ mit $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[n]{2}))$ überein.

__zu (2)__ Die Menge der Nullstellen von $\mathbb{Q}(\sqrt[n]{2})$ in $\mathbb{C}$ ist geg. durch $N = \{\zeta_n^k \sqrt[n]{2} \mid 0 \le k \le n-1\}$.
Denn .... (Begründung als Übung).

__1. Fall__: n ungerade

Für $0 < k \le n-1$ ist $\frac{2\pi k}{n}$ jeweils kein ganzzahliges Vielfaches von $\frac{2\pi k}{n}$,
denn: Ang. $\exists\, l \in \mathbb{Z}$ mit $\frac{2\pi k}{n} = l\pi \Rightarrow$

$$\frac{2k}{n} = l \Rightarrow 2k = nl \Rightarrow n \mid (2k)$$

$$\overset{n \text{ ungerade}}{\Longrightarrow} n \mid k \ \lightning \text{ da } 0 < k < n.$$

Hom.

) iterein.

$\mathbb{Q}(\sqrt[n]{2})$

$0 \le k \le n-1\}$.

).

eils

von $\frac{2\pi k}{n}$,

$= l\pi \Rightarrow$

$n \mid (2k)$

$k < n$.

$\Rightarrow \sin\left(\frac{2\pi k}{n}\right) \neq 0 \Rightarrow$

$\rho_n^k = e^{\frac{2\pi i k}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right) \notin \mathbb{R}$.

$\Rightarrow \rho_n^k \sqrt[n]{2} \notin \mathbb{R} \Rightarrow \rho_n^k \sqrt[n]{2} \notin \mathbb{Q}(\sqrt[n]{2})$.

Also ist $\sqrt[n]{2}$ die einzige Nullstelle von f_n in K_n.

2. <u>Fall</u>: n gerade

Sei $k \in \{0, \dots, n-1\}$ mit $\rho_n^k \sqrt[n]{2} \in K_n$.

$\Rightarrow \rho_n^k \sqrt[n]{2} \in \mathbb{R} \Rightarrow \rho_n^k \in \mathbb{R} \Rightarrow$

$e^{2\pi i k/n} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right) \in \mathbb{R} \Rightarrow$

$\sin\left(\frac{2\pi k}{n}\right) = 0 \Rightarrow \exists\, l \in \mathbb{Z}$ mit $\frac{2\pi k}{n} = l\pi$

$\Rightarrow 2k = ln \quad k \ge 0 \Rightarrow l \ge 0 \quad k < n \Rightarrow l \le 1$

also: $l \in \{0, 1\}$

...te wurde
...ss für
...von $\mathbb{Q}$ die
...übereinstimmt
...len von
...(α) für ein
...ner: Die
...$) \to \mathbb{Q}(\sqrt[n]{2})$
...zahl der
...n in $\mathbb{Q}(\sqrt[n]{2})$.
...aische Erwei-

Im Fall $l = 0$ ist $k = 0$, im Fall $l = 1$ ist $k = \frac{1}{2} n$. Also sind $\sqrt[n]{2}$ und $\zeta_n^{n/2} \cdot \sqrt[n]{2} = (e^{\frac{2\pi i \frac{n}{2}}{n}}) \sqrt[n]{2} = e^{\pi i} \sqrt[n]{2} = -\sqrt[n]{2}$ die einzigen Nullstellen von f_n im Körper K_n. $\square$

<u>F14T1A5</u> Sei p eine Primzahl, $L = \mathbb{F}_p(t)$ der rationale Funktionenkörper über $\mathbb{F}_p$ und $K = \mathbb{F}_p(t^p)$. Zeigen Sie:

(a) Das Polynom $f = x^p - t^p$ ist in $K[x]$ irreduzibel.

(b) Die Erweiterung $L|K$ ist endlich und normal, aber nicht separabel.

<u>zu (a)</u> Wegen char $\mathbb{F}_p(t)[x] = p$ gilt $f = x^p - t^p = (x-t)^p$. Ang. f ist über $k = \mathbb{F}_p(t^p)$ reduzibel $\Rightarrow \exists$ Polynome $g, h \in k[x] \setminus k$ mit $f = g h$. Dabei können g und h so gewählt werden, dass sie normiert sind.

(denn: Ist $c = lt(g)$ der Leitkoeff. von g, $d = lt(h)$ der von h, dann gilt $cd = lt(g)\, lt(h) = lt(f) = \bar{1}$. Ist $c \neq \bar{1}$, dann ersetze g, h durch die normierten Pol. $\tilde{g} = c^{-1} g$, $\check{h} = c h$.)

Sei $m = \mathrm{grad}(g)$, $n = \mathrm{grad}(h)$. Dann gilt $1 \leq m, n \leq p-1$, und aus $gh = f = (x-t)^p$ folgt $g = (x-t)^m$ und $h = (x-t)^n$. Die konstanten Terme von g und h sind also $(-t)^m$ bzw. $(-t)^n$. Aber diese Elemente liegen nicht in K. Denn jedes Element aus K hat die Form $\frac{u(t^p)}{v(t^p)}$ mit $u, v \in \mathbb{F}_p[t]$, also:

Ang. $(-t)^m \in K \Rightarrow \exists u, v \in \mathbb{F}_p[t]$ mit $(-t)^m = \frac{u(t^p)}{v(t^p)}$

$\Rightarrow (-t)^m \cdot v(t^p) = u(t^p)$ ↯ denn der Grad von $u(t^p)$ ist durch p teilbar, ebenso der Grad von $v(t^p)$

)

.

e

aus

also:

$= \frac{u(t^p)}{v(t^p)}$

von

von $v(t^p)$

aber nicht $\operatorname{grad}((-t)^m) = m$. Genauso zeigt man $(-t)^n \notin K$. Aber $(-t)^m \cdot (-t)^n \notin K$ steht im Widerspruch zu $g, h \in K[x]$.

<u>zu (b)</u> z.zg.: (1) $L|K$ ist endlich

(2) $L|K$ ist normal

(3) $L|K$ ist nicht separabel

<u>zu (1)</u> Das Polynom $f \in K[x]$ ist normiert, nach Teil (a) in $K[x]$ irreduzibel, und es gilt $f(t) = t^p - t^p = \bar{0}$.

$\Rightarrow f = \mu_{t,K} \Rightarrow [L:K] = [\mathbb{F}_p(t) : \mathbb{F}_p(t^p)] = [\mathbb{F}_p(t^p)(t) : \mathbb{F}_p(t^p)] = [K(t) : K] = \operatorname{grad}(f) = p$

Insbesondere ist $L|K$ also endlich.

<u>zu (2)</u> Es genügt z.zg., dass L Zerfällungskörper des Polynoms f über K ist. $f = (x-t)^p \Rightarrow f$ zerfällt (wegen $t \in L$) über L in Linearfaktoren. Die Gleichung $L = K(t)$ zeigt, dass L über K durch die Nullstellen von f erzeugt wird. Also ist L tatsächlich Zerf.körp. von f über K.

<u>zu (3)</u> Ang. $L|K$ ist separabel. Dann wäre $t \in L$ separabel über K, und $f = \mu_{t,K}$ wäre ein separables Polynom. Aber wegen $f' = px^{p-1} = \bar{0}$ und $ggT(f, f') = ggT(f, \bar{0}) = f \neq \bar{1}$ ist $f \in K[x]$ kein separables Polynom. $\square$

<u>H24T2A5</u> Sei $f = x^6 - 6 \in \mathbb{Q}[x]$.

in Teil (a) gezeigt: $L = \mathbb{Q}(\sqrt[6]{6}, \sqrt{-3})$ ist Zerfällungskörper von f über $\mathbb{Q}$, und es ist $[L : \mathbb{Q}] = 12$

(b) Zeigen Sie, dass $L|\mathbb{Q}$ eine Galois-Erweiterung ist, und dass $G = \mathrm{Gal}(L|\mathbb{Q})$ einen Normalteiler der Ordnung 6 besitzt.

Als Zerfällungskörper von f über $\mathbb{Q}$ ist L normal über $\mathbb{Q}$, damit ist $L|\mathbb{Q}$ auch eine algebraische Erweiterung. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ folgt daraus wiederum, dass $L|\mathbb{Q}$ auch separabel ist. Insgesamt ist über $\mathbb{F}_p$ und $K = \mathbb{F}_p(t)$ zeigen Sie:

$\in \mathbb{Q}[x]$.

$, \sqrt{-3})$

$\mathbb{Q}$, und

Galois-

$\mathrm{Gal}(L|\mathbb{Q})$

besitzt.

$\mathbb{Q}$ ist

$|\mathbb{Q}$ auch

Wegen

...mm, dass

...samt ist

$L|\mathbb{Q}$ damit eine Galois-Erweiterung.

Da $L|\mathbb{Q}$ galoissch ist, gilt

$|G| = |\mathrm{Aut}_{\mathbb{Q}}(L)| = [L : \mathbb{Q}] = 12$.