

Deitmar Algebra 2026:

- 1) a) wann heißt eine Körpererw. normal, wann separabel?
b) Was ist ein algebraischer Abschluss und inwiefern ist er eindeutig?
c) Welche endlichen Körper gibt es und welche Inklusionsbeziehung besteht zwischen ihnen?
d) Was ist ein Normalteiler, eine Quotientengruppe und was die universelle Eigenschaft der Quotientengruppe?
- 2) Für eine abelsche Gruppe G ist $\phi: G \rightarrow G, x \mapsto x^2$ ein Gruppenhomomorphismus. Die Bilder nennt man Quadrate. Betrachte nun $G = \mathbb{F}_q^\times$, wobei $\mathbb{F}_q$ der Körper mit q Elementen. Wie viele Quadrate hat $\mathbb{F}_q^\times$?
- 3) Betrachte das Polynom $x^4 - 25 \in \mathbb{Q}[x]$.
a) Bestimme den Zerfällungskörper L und $[L:\mathbb{Q}]$. (Hinweis: Ist $x^4 - 25$ irred.?)
b) Bestimme $\text{Gal}(L/\mathbb{Q})$.
c) Bestimme alle Zwischenkörper von $L/\mathbb{Q}$.
- 4) a) Zeige: $x^4 + x + 1 = f(x) \in \mathbb{F}_2[x]$ ist irreduzibel.
(Hinweis: Angenommen, $f = gh$. Was kann man über g, h sagen?)
b) Aus a) folgt: $K = \mathbb{F}_2[x]/(f)$ ist ein Körper.
Eine $\mathbb{F}_2$ -Basis ist $1, \bar{x}, \bar{x}^2, \bar{x}^3$.
Bestimme die Ordnung von $\bar{x}$ in $K^\times$.
- 5) Sei $\varepsilon = e^{\frac{2\pi i}{5}}$. Zeige: $\mathbb{Q}(\sqrt[5]{5}, \varepsilon)$ ist galoissch. Bestimme $[\mathbb{Q}(\sqrt[5]{5}, \varepsilon) : \mathbb{Q}]$.
(Hinweis: $(x^5 - 5) \cdot (x^5 - 1)$)

$$2) \phi: \mathbb{F}_q^{\times} \rightarrow \mathbb{F}_q^{\times}, \quad \phi(x) = x^2$$

Berechne $|\text{Im } \phi|$. Wegen Homomorphism ist $\text{Im } \phi = \mathbb{F}_q^{\times} / \ker \phi$
 $\Rightarrow |\text{Im } \phi| = \frac{|\mathbb{F}_q^{\times}|}{|\ker \phi|} = \frac{q-1}{2}$

$$\ker \phi = \{x \in \mathbb{F}_q^{\times} \mid x^2 = 1\} = \{x \mid x^2 - 1 = 0\} = \{\pm 1\}$$

1. Fall: $q = 2^n$, d.h. char $\mathbb{F}_q = 2 \Rightarrow q = 2^n$ für ein $n \in \mathbb{N}$
 $\Rightarrow |\ker \phi| = 1 \Rightarrow |\text{Im } \phi| = \frac{q-1}{2} = \frac{2^n-1}{2}$

2. Fall: $q \neq 2^n$, d.h. char $\mathbb{F}_q = p > 2 \Rightarrow q = p^n$ für ein $n \in \mathbb{N}$
 $\Rightarrow |\ker \phi| = 2 \Rightarrow |\text{Im } \phi| = \frac{q-1}{2}$ (Bem.: q ungerade, da p ungerade, $\Rightarrow q-1$ gerade)

$$3) f(x) = x^4 - 25 = (x^2 - 5)(x^2 + 5) = (x - \sqrt{5})(x + \sqrt{5})(x - \sqrt{5}i)(x + \sqrt{5}i)$$

$$a) \Rightarrow \mathbb{K}_{\mathbb{Q}}(f) = \mathbb{Q}(\sqrt{5}, \sqrt{5}i) = \mathbb{Q}(\sqrt{5}, i) =: L$$

Es ist $m_{\sqrt{5}/\mathbb{Q}} = x^2 - 5$, da Irr. / Eisenstein oder keine NST in $\mathbb{Q}$
mit NST $\pm \sqrt{5}$ (D)

$m_{i/\mathbb{Q}(\sqrt{5})} = x^2 + 1$, da keine NST in $\mathbb{Q}(\sqrt{5})$
mit NST $\pm i$ (DD) ($i \in \mathbb{C} \setminus \mathbb{Q}(\sqrt{5})$)

$$\begin{aligned} \Rightarrow [L:\mathbb{Q}] &= [\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}(\sqrt{5})] \cdot [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] \\ &= \deg m_{i/\mathbb{Q}(\sqrt{5})} \cdot \deg m_{\sqrt{5}/\mathbb{Q}} \\ &= 2 \cdot 2 = 4 \end{aligned}$$

b) $w \in \text{Gal}(L/\mathbb{Q})$: $L/\mathbb{Q}$ galoisch, da normal, endlich, separabel (hier, da char $\mathbb{Q}$)

$$\Rightarrow \text{Gal}(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\} \text{ mit}$$

$$\sigma_1: \sqrt{5} \mapsto \sqrt{5}, \quad \sigma_2: \sqrt{5} \mapsto -\sqrt{5}$$

$$i \mapsto i, \quad i \mapsto i$$

$$\sigma_3: \sqrt{5} \mapsto \sqrt{5}, \quad \sigma_4: \sqrt{5} \mapsto -\sqrt{5}$$

$$i \mapsto -i, \quad i \mapsto -i$$

alle selbstinvers, $\sigma_4 = \sigma_1 \circ \sigma_3 = \sigma_3 \circ \sigma_2$

$$\Rightarrow \text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

c) Unterkörper von L :

~~hat~~ $\text{Gal}(L/\mathbb{Q})$ hat 3 nichttriviale Untergruppen

$$(\mathbb{Z}/22 \times \mathbb{Z}/3, \mathbb{Z}/3 \times \mathbb{Z}/12, \{1, 0\}, \{7, 7\})$$

HS

$\Rightarrow L/\mathbb{Q}$ hat 3 nichttriviale Zwischenkörper
Gal. Theorie

$\mathbb{Q}(\sqrt{5}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{5}i)$ sind damit alle

(alle versch., da $\sqrt{5} \notin \mathbb{Q}(i), i \notin \mathbb{Q}(\sqrt{5}), \sqrt{5}i \notin \mathbb{Q}(i)$
 $\notin \mathbb{Q}(\sqrt{5}), \notin \mathbb{Q}(\sqrt{5}i), \notin \mathbb{Q}(\sqrt{5})$)

4) a) $f = x^4 + x + 1 \in \mathbb{F}_2[x]$ irred., denn

ang. $f = g \cdot h$ für $g, h \in \mathbb{F}_2[x] \setminus \mathbb{F}_2$

1. Fall: $\deg g = 1, \deg h = 3$ oder umgekehrt

$\Rightarrow f$ hat NST, da g Linearfaktor

aber $0^4 + 0 + 1 \neq 0, 1^4 + 1 + 1 = 1 \neq 0$

2. Fall: $\deg g = \deg h = 2$

Sei $g = x^2 + ax + b$ (Koeff. nur 0 oder 1)

$h = x^2 + cx + d$

$$\Rightarrow x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (d+b+ac)x^2 + (ad+bc)x + bd$$

$$\Rightarrow bd = 1 \Rightarrow b = d = 1$$

$$1 = ad + bc = a + c \Rightarrow \begin{matrix} a=0 & \text{oder} & c=0 \\ c=1 & & a=1 \end{matrix}$$

$$0 = a + c = 1$$

b) wegen a) ist $K = \mathbb{F}_2[x]/(f)$ Körper $\mathbb{F}_{2^4}$ mit $\bar{1}, \bar{x}, \bar{x}^2, \bar{x}^3, \dots, \bar{x}^{15}$
 $\text{ord } \bar{x} \mid |K^*| = |K| - 1 = 2^4 - 1 = 15$
da (x)

$$\Rightarrow \text{ord } \bar{x} \in \{1, 3, 5, 15\}$$

$\text{ord } \bar{x} \notin \{1, 3\}$, da $\bar{x} \neq \bar{1}, \bar{x}^3 \neq \bar{1}, \bar{x}^5 = \bar{x}^4 \cdot \bar{x} = (\bar{x} + \bar{1}) \cdot \bar{x} = \bar{x}^2 + \bar{x} \neq \bar{1}$

$$\Rightarrow \text{ord } \bar{x} = 15$$

5) $L = \mathbb{Q}(\sqrt[5]{5}, \varepsilon), \varepsilon = e^{\frac{2\pi i}{5}}$ (Hinweis: $(x^5-5)(x^5-1) = f$)

$L/\mathbb{Q}$ galois.

• separabel klar, da $K/\mathbb{Q}$ über $\mathbb{Q}$.

• normal: $L = \mathbb{Z}K_{\mathbb{Q}}(f)$, denn: NSP von f :

$x^5-5=0 \Leftrightarrow x^5=5$

$\Leftrightarrow x^5 = \sqrt[5]{5} \cdot \varepsilon^k$

$k=0, \dots, 4$

$x^5-1=0 \Leftrightarrow x^5=1$

$\Leftrightarrow x = \varepsilon^k, k=0, \dots, 4$

$\Rightarrow \mathbb{Z}K = \mathbb{Q}(\sqrt[5]{5} \cdot \varepsilon^k | k=0, \dots, 4) \cup \{\varepsilon^k | k=0, \dots, 4\}$

$= \mathbb{Q}(\sqrt[5]{5}, \varepsilon) = L$

$\supseteq$: klar

$\subseteq$: klar, da Erzeuger drin liegen

alternativ: $L = \mathbb{Z}K(x^5-5, x^5-1)$

• endlich: $[L:\mathbb{Q}] = 5 \cdot 4 = 20 < \infty$, dann:

$([L:\mathbb{Q}(\sqrt[5]{5})] \cdot [\mathbb{Q}(\sqrt[5]{5}):\mathbb{Q}])$

$m_{\mathbb{Q}(\sqrt[5]{5})/\mathbb{Q}}(x) = x^5-5$

$m_{\mathbb{Q}(\varepsilon)/\mathbb{Q}}(x) = x^4+x^3+x^2+x+1$

$m_{\mathbb{Q}(\varepsilon)/\mathbb{Q}}(x) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$

$(5, VL)$

5-tes Kreisteilungspolynom

5 Primzahl

nicht so
einfach zu
begründen
daher anders:

da $\mathbb{Q}(\varepsilon), \mathbb{Q}(\sqrt[5]{5}) \subseteq L$, muss

$[\mathbb{Q}(\varepsilon):\mathbb{Q}] = 4$ ($m_{\mathbb{Q}(\varepsilon)/\mathbb{Q}} = x^4+x^3+x^2+x+1$, 5-tes Kreisteilungspol.)

$[\mathbb{Q}(\sqrt[5]{5}):\mathbb{Q}] = 5$ ($m_{\mathbb{Q}(\sqrt[5]{5})/\mathbb{Q}} = x^5-5$, da irred. nach Eisenstein)

Teiler von $[L:\mathbb{Q}]$ sein,

also ist 20 Teiler von $[L:\mathbb{Q}]$ sein, insb. $20 \leq [L:\mathbb{Q}]$

Andererseits ist $[L:\mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{5}, \varepsilon):\mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{5}):\mathbb{Q}] \cdot [\mathbb{Q}(\varepsilon):\mathbb{Q}] \leq 20$ (**)

≤ 4 , 5-tes
da Kreisteilungspol.
 $x^4+x^3+x^2+x+1$ als
NSP hat, also über
 $\mathbb{Q}(\sqrt[5]{5})$ entf. radikal
geworden ist,
womit sich der Grad verringert hätte

$(*)$, $(**)$
 $\Rightarrow [L:\mathbb{Q}] = 20$