

F26T1A2

geg. $f = x^4 - 6x^2 - 3 \in \mathbb{Q}[x]$

(a) gezeigt: f ist irreduzibel und hat die vier komplexen Nullstellen $\pm \alpha, \pm \beta$ wobei $\alpha = \sqrt{3+2\sqrt{3}}$, $\beta = \sqrt{3-2\sqrt{3}}$

(b) Zeigen Sie: $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ und $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{3})$

Es gilt $3+2\sqrt{3} > 0$ und somit $\alpha \in \mathbb{R}$, andererseits $\sqrt{3} > \frac{3}{2} \Rightarrow 3-2\sqrt{3} < 0 \Rightarrow \beta \in \mathbb{C} \setminus \mathbb{R}$ also: $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$

$$\text{und } \mathbb{Q}(\beta) \not\subseteq \mathbb{R} \Rightarrow \mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$$

$$" \Rightarrow " \quad \frac{1}{2}(\alpha^2 - 3) = \sqrt{3} \in \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$$

$$(-\frac{1}{2})(\beta^2 - 3) = \sqrt{3} \in \mathbb{Q}(\beta) \Rightarrow \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\beta)$$

Insgesamt gilt also $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$

$$f \text{ irred., normiert, } f(\beta) = 0 \Rightarrow f = \mu_{\beta, \mathbb{Q}} \\ \Rightarrow [\mathbb{Q}(\beta) : \mathbb{Q}] = \text{grad}(f) = 4$$

$\sqrt{3} \in \mathbb{Q}(\beta) \Rightarrow \mathbb{Q}(\sqrt{3})$ ist Zwischenk.p. von

$$\mathbb{Q}(\beta) / \mathbb{Q} \quad \text{Gradformel} \Rightarrow$$

$$4 = [\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{3})] [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

$3 \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei $\Rightarrow$ lt. VL

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \Rightarrow [\mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{3})] = 2$$

$$\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta)$$

$$\text{Gradf.} \Rightarrow 2 = [\mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{3})] \stackrel{(*)}{=}$$

$$[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{3})]$$

Wegen $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) \subseteq \mathbb{R}$, $\mathbb{Q}(\beta) \not\subseteq \mathbb{R}$ gilt

$$[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)] > 1 \stackrel{(*)}{\Rightarrow}$$

$$[\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{3})] = 1 \Rightarrow \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{3})$$

F26T3A4 Sei $\zeta = e^{2\pi i/5}$

(a) Zeigen Sie, dass $x^2 + x - 1$ das Minimalpolynom von $\alpha = \zeta + \zeta^4$ über $\mathbb{Q}$ ist.

bekannt: $\mu_{5, \mathbb{Q}} = \Phi_5 = x^4 + x^3 + x^2 + x + 1$

(5-tes Kreisteilungspolynom)

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$$

→ $[\mathbb{Q}(S) : \mathbb{Q}] = \text{grad } \Phi_5 = 4$, und

$\{1, S, S^2, S^3\}$ ist Basis von $\mathbb{Q}(S)$ als $\mathbb{Q}$ -Vektorraum ($\Rightarrow$ jedes $x \in \mathbb{Q}(S)$ hat eindeutige Darstellung $x = a + bS + cS^2 + dS^3$ mit $a, b, c, d \in \mathbb{Q}$.)

Überprüfe: α ist Nullstelle von $f = x^2 + x - 1$

Es gilt $S^5 = 1$ und $S^4 = -1 - S - S^2 - S^3$ wegen

$$\Phi_5(S) = 0. \quad f(x) = x^2 + x - 1 = (S + S^4)^2$$

$$+ S + S^4 - 1 = S^2 + 2S^5 + S^8 + S + S^4 - 1$$

$$= S^2 + 2 \cdot 1 + S^3 + S - (1 + S + S^2 + S^3) - 1 = 0$$

Wäre f reduzibel, dann hätte f wg. $\text{grad}(f) = 2$

eine rationale Nullst. r . $f \in \mathbb{Z}[x]$, normiert

$\Rightarrow r \in \mathbb{Z}$, r teilt den konstanten Term -1 von f

$\Rightarrow$

$\Rightarrow r \in \{\pm 1\}$ aber: $f(1) = 1 \neq 0$, $f(-1) = -1 \neq 0$ $\nmid$ Somit ist f irreduzibel, außerdem normiert, und $f(\alpha) = 0 \Rightarrow f$ ist das Min. pol. von α über $\mathbb{Q}$. $\square$

D_K
insbesondere
 R ein Körper

$\alpha^{-1} \in R$
 $[\alpha]$ hat
also

$g(\alpha)$
Nullstelle
 $([\alpha] \setminus \{0\})^\times$
 $\square$

Übung: F23T3A4 (c)

H22T1A4 (a), (b)

H24T3A4 (a), (b)

F26T3A3 Übung: F21T1A3

Sei $L|K$ eine Körpererweiterung. Zeigen Sie, dass die folgenden beiden Aussagen äquivalent sind:

(i) Die Erweiterung $L|K$ ist algebraisch.

iii) Jeder Ring R mit $K \subseteq R \subseteq L$ ist ein Körper.

"ii) $\Rightarrow$ iii)" Sei R ein Ring wie angegeben und $x \in R \setminus \{0\}$. Da x dann auch in $L \setminus \{0\}$ liegt und L ein Körper ist, existiert für x ein multiplikatives Inverses x^{-1} . Wenn wir zeigen können, dass x^{-1} in R liegt, dann ist damit gezeigt, dass jedes $x \in R \setminus \{0\}$ invertierbar und R somit ein Körper ist.

Auf Grund der Vor. (i) ist x algebraisch über K .

Sei $f = \mu_{x,K} = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$

mit $n \in \mathbb{N}$, $a_0, a_1, \dots, a_{n-1} \in K$. $\Rightarrow$

$$0 = f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

$a_n)$
 $\dots + a_n)$
ungerade -
 $+ a_n) \in R$

$+ a_n) \times$

$0 \downarrow$

algebraisch
 R ist Ring

$$\Rightarrow -a_0 = x(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1)$$

1. Fall: $a_0 \neq 0$

$$\Rightarrow 1 = x \cdot \left(-\frac{1}{a_0}\right)(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1)$$

$$\Rightarrow x^{-1} = \left(-\frac{1}{a_0}\right)(x^{n-1} + \dots + a_{n-1}x^{n-2} + \dots + a_1)$$

Aus $K \subseteq R$ und $x \in R$ (und der Ringeigenschaft von R) folgt $\left(-\frac{1}{a_0}\right)(x^{n-1} + \dots + a_1) \in R$ und $x^{-1} \in R$.

2. Fall: $a_0 = 0 \Rightarrow f = (x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1)x$

f irreduz. $n=1$, $f=x \Rightarrow x=f(x)=0 \downarrow$

"iii) $\Rightarrow$ i)" Sei $\alpha \in L$ z.zg. α ist algebraisch über K . Sei $R = K[\alpha]$. $\xrightarrow{\alpha \in L}$ R ist Ring

mit $K \subseteq R \subseteq L$ Voraussetzung (ii) $\Rightarrow$

R ist ein Körper 1. Fall: $\alpha = 0_L = 0_K$

In diesem Fall liegt α in K , ist also insbesondere algebraisch über K . 2. Fall: $\alpha \neq 0_L$ Da R ein Körper

ist und α in $R \setminus \{0_L\}$ liegt, gilt $\alpha^{-1} \in R$ bekannt: Jedes Element in $R = K[\alpha]$ hat die Form $g(\alpha)$ für ein $g \in K[x]$ also:

Es gibt ein $g \in K[x]$ mit $\alpha^{-1} = g(\alpha)$

$\Rightarrow \alpha g(\alpha) - 1_K = 0_K \Rightarrow \alpha$ ist Nullstelle

des Polynoms $h = xg - 1_K \in K[x] \setminus \{0_K\}$

$\Rightarrow \alpha$ ist algebraisch über K . $\square$

$\Rightarrow$

$= -$

außer

P ist

über

H22

H24

F26T

Sei L

Sei, da

Äquiva

(i) Die

Endliche Körper

Hauptsatz

- (i) Ist K ein endlicher Körper, dann ist $|K|$ eine Primzahlpotenz > 1 . (Grund: Ist P der Primkörper von K und $p = \text{char}(P) = \text{char}(K)$, dann ist p eine Primzahl, und $P \cong \mathbb{Z}/p\mathbb{Z}$. Der Grad $d = [K:P]$ ist endlich. $\Rightarrow K$ ist d -dim. P -Vektorraum $\Rightarrow |K| = |P|^d = p^d$.)
- (ii) Ist $K/\mathbb{F}_p$ eine endliche Erweiterung und $\alpha \in K$ mit $K = \mathbb{F}_p(\alpha)$, $d = [K:\mathbb{F}_p]$.

dann gilt $|K| = p^d$, $K = \{a_0 + a_1\alpha + \dots + a_{d-1}\alpha^{d-1} \mid$

$a_0, a_1, \dots, a_{d-1} \in \mathbb{F}_p\}$.

Bsp. $\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{0, 1, \alpha, 1+\alpha\}$, wobei α
Nullstelle von $f = x^2 + x + 1 \in \mathbb{F}_2[x]$.

iii) Für jeden endlichen Körper K ist $K^\times$
eine endliche zyklische Gruppe.

iv) Ist q eine Primzahlpotenz größer als 1,
dann gibt es bis auf Isomorphie genau
einen Körper K mit $|K| = q$.

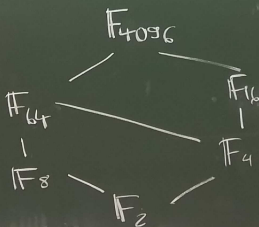
(Ein solcher Körper kommt zu Stande als
Zerfällungskörper des Polynoms $f = x^q - x$
 $\in \mathbb{F}_p[x]$ über $\mathbb{F}_p$, wobei p Primzahl,
 q Potenz von p .)

(iv) Ist p eine Primzahl und $\mathbb{F}_p^{\text{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_p$, dann existiert für jedes $n \in \mathbb{N}$ genau ein Zwischenkörper von $\mathbb{F}_p^{\text{alg}} / \mathbb{F}_p$ mit p^n Elementen, der mit $\mathbb{F}_{p^n}$ bezeichnet wird.

Es gilt $\mathbb{F}_p^{\text{alg}} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$ sowie die

Äquivalenz $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n \quad \forall m, n \in \mathbb{N}$

$$4096 = 2^{12}$$



F22T2A4 Sei p eine Primzahl.

(a) Zeigen Sie: $\mathbb{F}_p(x) = \mathbb{F}_{p^2} \quad \forall x \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$

Sei $x \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Gradformel $\Rightarrow$

$$2 = [\mathbb{F}_{p^2} : \mathbb{F}_p] = [\mathbb{F}_{p^2} : \mathbb{F}_p(x)] \cdot [\mathbb{F}_p(x) : \mathbb{F}_p]^{(*)}$$

$$x \notin \mathbb{F}_p \Rightarrow \mathbb{F}_p(x) \neq \mathbb{F}_p \Rightarrow [\mathbb{F}_p(x) : \mathbb{F}_p] > 1$$

$$\text{Aus } (*) \text{ folgt damit } [\mathbb{F}_{p^2} : \mathbb{F}_p(x)] = 1.$$

$$\Rightarrow \mathbb{F}_{p^2} = \mathbb{F}_p(x)$$

(b) Bestimmen Sie die Anzahl der Elemente $x \in \mathbb{F}_{p^2}$

$$\text{mit } \mathbb{F}_{p^2} = \mathbb{F}_p(x)$$

Die Menge der Elemente mit dieser Eigenschaft ist nach Teil (a) gleich $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$, und die Mächtigkeit dieser Menge ist $|\mathbb{F}_{p^2}| - |\mathbb{F}_p| = p^2 - p$.