A 8.1.1 Ww: $K := \{ \operatorname{diag}(x,x) \in \mathbb{R}^2 : x \in \mathbb{R} \} \cong \mathbb{R}$

Ges.: $I \in \mathbb{R}^{2\times 2} : I^2 = \operatorname{diag}(-1,-1)$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\Rightarrow \quad a^2 + bc = -1 \qquad (a+d)b = 0$$
$$(a+d)c = 0 \qquad bc + d^2 = -1$$

$a, d \in \mathbb{R} \Rightarrow b \neq 0 \neq c \Rightarrow a + d = 0 \Leftrightarrow a = -d$

$$b = -\frac{1+a^2}{c}$$

Wähle $a, c := 1 \Rightarrow b = -2,\ d = -1$ und

$$\begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ges.: $L: K \subset L \subset \mathbb{R}^{2\times 2}$, $\zeta : L \to \mathbb{C}$ Isomorphismus,

$L := \{ A + BI \in \mathbb{R}^{2\times 2} : A, B \in K \}$

$\zeta : Z = A + BI = aE_2 + b\cancel{E_2}I \mapsto a + bi = z$

A 8.1.7 Gg.: K Körper, I Menge;

(a) Zz: VR K^I mit $(x_i)_{i\in I} \cdot (y_j)_{j\in I} := (x_k y_k)_{k\in I}$ ist kommutative, assoziative K-Algebra mit Einselement

$\forall a,b,c \in K^I \ \forall x \in K$:

$a(b+c) = (a_i)_{i\in I}\,((b_i)_{i\in I} + (c_i)_{i\in I}) = (a_i)_{i\in I}\,(b_i + c_i)_{i\in I}$
$= (a_i\,(b_i + c_i))_{i\in I} = (a_i b_i + a_i c_i)_{i\in I} = (a_i b_i)_{i\in I} + (a_i c_i)_{i\in I}$
$= (a_i)_{i\in I}\,(b_i)_{i\in I} + (a_i)_{i\in I}\,(c_i)_{i\in I} = ab + ac$,

$(a+b)c = ac + bc$,

$x(ab) = (xa)b = a(xb)$,

$(ab)c = a(bc)$,

$ab = ba$;

$(1_K)_{i\in I}$ ist das Einselement.

(b) Zz: $K^{\langle I\rangle} \subset K^I$ mit obérem „$\cdot$" ist kommutative, assoziative K-Algebra mit (entweder) Einselement aus K^I oder keinem

$\forall a,b,c \in K^{\langle I\rangle}$: $I_a := \{i\in I : a_i \neq 0\}$, $\# I_a < \infty$, I_b, I_c;

$\Rightarrow \ I_{a+b} \subseteq I_a \cup I_b$, $\# I_{a+b} < \infty$,
$\quad I_{ab} = I_a \cap I_b$, $\# I_{ab} < \infty$;

Wenn $\# I < \infty$, so hat $K^{\langle I\rangle}$ ein Einselement.

(c) Gg: $I := \{1, 2\}$

Zz: K^2 hat ein Einselement, $U := \{(x_1, 0) \mid x_1 \in K\} \subset K^2$ ...

Einselemente gleich ?

A 8.1.9 Bsp: V, W K-Algebren, $f: V \to W$

K-Algebren-Antihomomorphismus, falls

$\forall a, b \in V: f(ab) = f(b) f(a)$

(Isomorphismus, Automorphismus)

(γ) $f: \begin{cases} D_2(K) \to D_2(K) \\ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mapsto \begin{pmatrix} z & y \\ 0 & x \end{pmatrix} \end{cases}$

Seien $A, B \in D_2(K)$ obere Δ-Matrizen.

$$f(AB) = f\left(\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}\begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}\right) = f\begin{pmatrix} a_1b_1 & a_1b_2 + a_2b_3 \\ 0 & a_3b_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_3b_3 & a_1b_2 + a_2b_3 \\ 0 & a_1b_1 \end{pmatrix} = \begin{pmatrix} b_3 & b_2 \\ 0 & b_1 \end{pmatrix}\begin{pmatrix} a_3 & a_2 \\ 0 & a_1 \end{pmatrix} = f(B)f(A).$$

$$\neq \begin{pmatrix} a_3 & a_2 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix} = f(A)f(B).$$

$\Rightarrow f$ involutorischer K-Algebren-Antiautomorphismus

$(f = (\cdot)^T)$

(δ) $f_k: \begin{cases} D_2(K) \to D_2(K) \\ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mapsto \begin{pmatrix} x & ky \\ 0 & z \end{pmatrix} \end{cases}$ mit $k \in K$

...

$$f_k(AB) = f_k\left(\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}\begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}\right) = f_k\begin{pmatrix} a_1b_1 & a_1b_2 + a_2b_3 \\ 0 & a_3b_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1b_1 & k(a_1b_2 + a_2b_3) \\ 0 & a_3b_3 \end{pmatrix} = \begin{pmatrix} a_1 & ka_2 \\ 0 & a_3 \end{pmatrix}\begin{pmatrix} b_1 & kb_2 \\ 0 & b_3 \end{pmatrix} = f_k(A)f_k(B).$$

$$\neq \begin{pmatrix} b_1 & kb_2 \\ 0 & b_3 \end{pmatrix}\begin{pmatrix} a_1 & ka_2 \\ 0 & a_3 \end{pmatrix} = f_k(B)f_k(A).$$

$\Rightarrow f$ K-Algebren-Homomorphismus

$k \neq 0_K \Rightarrow f_k^{-1} = f_{k^{-1}} \Rightarrow f$ bijektiv

$k = \pm 1_K \Rightarrow f$ involutorisch (ε) $f_k: \begin{cases} \mathbb{D}(K) \to \mathbb{D}(K) \\ xE_2 + y\varepsilon \mapsto xE_2 + ky\varepsilon \end{cases}$ mit $k \in K$

$\varepsilon := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in K^{2\times 2}$, $\mathbb{D}(K) := \{ xE_2 + y\varepsilon \mid x,y \in K \} \subset K^{2\times 2}$;

...

$$\begin{aligned} f_k(AB) &= f_k((x_a E_2 + y_a \varepsilon)(x_b E_2 + y_b \varepsilon)) \\ &= f_k(x_a x_b E_2 + (x_a y_b + x_b y_a)\varepsilon) \\ &= x_a x_b E_2 + k(x_a y_b + x_b y_a)\varepsilon \\ &= (x_a E_2 + k y_a \varepsilon)(x_b E_2 + k y_b \varepsilon) = f_k(A) f_k(B) \\ &= (x_b E_2 + k y_b \varepsilon)(x_a E_2 + k y_a \varepsilon) = f_k(B) f_k(A). \end{aligned}$$

$\Rightarrow$ wie (δ) nur auch mit „Anti"

A 8.2.1 Ges.: Nullstellen in K, Vielfachheit;

(β) Geg.: $X^3 - 2 \in \mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X]$.

$$= (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}\,X + \sqrt[3]{4})$$

$N_{\mathbb{Q}} = \emptyset$,

$N_{\mathbb{R}} = N_{\mathbb{Q}} \cup \{\sqrt[3]{2}\}$,

$N_{\mathbb{C}} = N_{\mathbb{R}} \cup \{-\sqrt[3]{2}/2 \pm i\sqrt{3}\,\sqrt[3]{2}/2\}$;

Mit dem Fundamentalsatz der Algebra sieht man, dass alle Vielfachheiten 1. sind.

(γ) $(X^4 - X)^2 \in GF(4)[X]$

$GF(4) := \{0, 1, a, b\}$

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$\Rightarrow$ $GF(4)$ hat involutorische Elemente bzgl. „+“.

$(X^4 - X)^2 = 0 \Leftrightarrow X^4 - X = 0 \Leftrightarrow X^4 = X \Rightarrow$

$N = GF(4)$

$\Rightarrow (X^4 - X^2)^2 = ((X-0)(X-1)(X-a)(X-b))^2$

$\Rightarrow$ Vielfachheiten sind 2.

(ε) $X^3 + X^2 + X + 1 \in \mathbb{Z}_2[X]$

$N = \{1\}$

Mit Vielfachheit 3.

A 8.2.3 Geg.: $m \in \mathbb{N}^{\times}$, $(\mathbb{Z}_m, +, \cdot)$ hat multiplikativ neutrales Element $\bar{1} = 1 + \mathbb{Z}m$ („Restklassenring modulo m"), $(\mathbb{Z}_m[X], +, \cdot)$ wie für Körper (Grad, Teiler, Vielfaches, Nullstelle);

(a) Ges.: $P(X) \in \mathbb{Z}_6[X]$: $\text{Grad}(P) = 2$, $N(P) = \mathbb{Z}_6$

A 8.2.7 Gg: K Körper, $\operatorname{Char} K \neq 2$, $P(X) = X^2 + a_0 \in K[X]$ hat keine Nullstelle in K;

(a) Zz: $L := \left\{ \begin{pmatrix} x & -a_0 y \\ y & x \end{pmatrix} \mid x, y \in K \right\}$ Körper

- abelsche „+"- Gruppe

  - Abgeschlossenheit: $\begin{pmatrix} x_1 & -a_0 y_1 \\ y_1 & x_1 \end{pmatrix} + \begin{pmatrix} x_2 & -a_0 y_2 \\ y_2 & x_2 \end{pmatrix}$

  $$= \begin{pmatrix} x_1 + x_2 & -a_0(y_1 + y_2) \\ y_1 + y_2 & x_1 + x_2 \end{pmatrix} \in L$$

  - ... ✓

- abelsche „·"- Gruppe

  - Abgeschlossenheit: $\begin{pmatrix} x_1 & -a_0 y_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & -a_0 y_2 \\ y_2 & x_2 \end{pmatrix}$

  $$= \underbrace{\begin{pmatrix} x_1 x_2 - a_0 y_1 y_2 & -a_0(x_1 y_2 + y_1 x_2) \\ y_1 x_2 + x_1 y_2 & x_1 x_2 - a_0 y_1 y_2 \end{pmatrix}}_{} \in L$$

  - ... ✓

  - Inverse: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \Big(\qquad \Big)$

$$\Rightarrow \begin{array}{l} 1 = x_1 x_2 - a_0 y_1 y_2 \\ 0 = y_1 x_2 + x_1 y_2 \end{array} \quad \text{oBdA. } y_1 \neq 0,\ a_0 \neq 0$$

$$\Rightarrow x_2 = \frac{x_1 y_2}{y_1} \Rightarrow 1 = x_1 \frac{x_1 y_2}{y_1} - a_0 y_1 y_2 = y_2 \left(\frac{x_1^2}{y_1} - a_0 y_1 \right)$$

$$\Leftrightarrow \frac{1}{\frac{x_1^2}{y_1} - a_0 y_1} = \frac{y_1}{x_1^2 - a_0 y_1^2} = y_2$$

$$\Rightarrow x_2 = \frac{x_1 \frac{y_1}{x_1^2 - a_0 y_1^2}}{y_1} = \frac{x_1}{x_1^2 - a_0 y_1^2}.$$

  - Kommutativität: $\begin{pmatrix} x_2 & -a_0 y_2 \\ y_2 & x_2 \end{pmatrix} \begin{pmatrix} x_1 & -a_0 y_1 \\ y_1 & x_1 \end{pmatrix}$

  $$= \begin{pmatrix} x_2 x_1 - a_0 y_2 y_1 & -a_0(x_2 y_1 + y_2 x_1) \\ y_2 x_1 + x_2 y_1 & -a_0 y_1 y_2 + x_2 x_1 \end{pmatrix}$$

- Distributivität ✓

(b) $\varphi : \begin{cases} K \to \tilde{L} := \{ A \in L : y = 0 \} \\ x \mapsto \operatorname{diag}(x, x) \end{cases}$ Körper - Isomorphismus

(c) Gg: $K \ni x \cong \operatorname{diag}(x, x)$, $i := \begin{pmatrix} 0 & -a_0 \\ 1 & 0 \end{pmatrix}$

Zz: $L = \{ x + yi \mid x, y \in K \}$

$$\underbrace{\begin{pmatrix} x & -a_0 y \\ y & x \end{pmatrix}}_{\in L} = \underbrace{\underbrace{\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}}_{\cong x} + y \underbrace{\begin{pmatrix} 0 & -a_0 \\ 1 & 0 \end{pmatrix}}_{i}}_{\in \{ x + yi \mid x, y \in K \}}$$

Ges.: $\dim L/K$

$= 2$, weil $\{ E_2, i \}$ eine Basis bildet

(d) Zz: Alle Nullstellen von $X^2 + a_0 \in L[X]$ sind $\pm i$

$$-a_0 = (x \pm iy)^2 = \left((x E_2)^2 \pm \begin{pmatrix} 0 & -a_0 \\ 1 & 0 \end{pmatrix} y \right)^2$$

$$= (x E_2)^2 \pm 2 \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 0 & -a_0 \\ 1 & 0 \end{pmatrix} y + \left(\begin{pmatrix} 0 & -a_0 \\ 1 & 0 \end{pmatrix} y \right)^2$$

$$= x^2 E_2 \pm 2xy \begin{pmatrix} 0 & -a_0 \\ 1 & 0 \end{pmatrix} + (-y^2 a_0) E_2$$

Für $x \neq 0$ oder $y \neq 1$, stimmt dies nicht.

Zz: $\exists! \zeta \in \operatorname{Aut}(L) : \begin{cases} \pm i \mapsto \mp i \\ x \mapsto x, \text{ falls } x \neq \pm i \end{cases}$

Fortsetzungssatz

(e) Zz: $\exists L$ Körper: $\# L = 9$

Betrachte: $X^2 + 1 \in \mathbb{Z}_3[X]$, hat keine Nullstellen

und L aus (a) mit $K = \mathbb{Z}_3$

A 8.2.9 Gg: V K-Algebra, $D \in L(V,V)$ mit

$$D(ab) = D(a)b + aD(b)$$

heißt „Derivation", „formale Ableitung" von $P(X) = \sum_{i \in \mathbb{N}} a_i X^i \in K[X]$

$$P'(X) := \sum_{i \in \mathbb{N}} (i+1) a_{i+1} X^i \in K[X].$$

(a) Zz: „formaler Ableitungsoperator" $D : \begin{cases} K[X] \to K[X] \\ P(X) \mapsto P'(X) \end{cases}$

Seien $\sum_{i \in \mathbb{N}} a_i X^i, \sum_{i \in \mathbb{N}} b_i X^i \in K[X]$,

$$\left(\sum_{i \in \mathbb{N}} (i+1) a_{i+1} X^i\right)\left(\sum_{i \in \mathbb{N}} b_i X^i\right) + \left(\sum_{i \in \mathbb{N}} a_i X^i\right)\left(\sum_{i \in \mathbb{N}} (i+1) b_{i+1} X^i\right) =$$

$$\underbrace{\sum_{k \in \mathbb{N}} \left(\sum_{i=0}^{k} (i+1) a_{i+1} b_{k-i}\right) X^k + \sum_{k \in \mathbb{N}} \left(\sum_{i=0}^{k} a_i (k-i+1) b_{k-i+1}\right) X^k}_{\sum_{k \in \mathbb{N}} \left(\sum_{i=0}^{k+1} i a_i b_{k+1-i}\right) X^k} =$$

$$= \sum_{k \in \mathbb{N}} \left((k+1) a_{k+1} b_0 + \sum_{i=0}^{k} (k+1) a_i b_{k+1-i}\right) X^k$$

$$= \sum_{k \in \mathbb{N}} (k+1) \left(\sum_{i=0}^{k+1} a_i b_{k+1-i}\right) X^k$$

(b) Gg: $t \in K$ Nullstelle von $P(X) \in K[X]$ mit Vielfachheit k

Zz: t ist $(k-1)$-fache Nullstelle von $P'(X)$

Ww: $\exists Q(X) \in K[X] : Q(X)(X-t)^k = P(X)$

$$\Leftrightarrow \quad Q'(X)(X-t)^k + \underbrace{Q(X)\, k\, (X-t)^{k-1}}_{\dots} = \dots$$

$$\dots = (Q(X)k + Q'(X)(X-t))(X-t)^{k-1}$$ ✓

$$\dots = \left(\sum_{0 \le i \le k}^{\infty} \binom{k}{i} (-t)^{k-i} X^i\right)' = \sum_{0 \le i \le k}^{\infty} (i+1) \underbrace{\binom{k}{i+1}}_{\frac{k!}{(i-1)!\,(k-i-1)!}} (-t)^{k-i-1} X^i =$$

$$k \sum_{0 \le i \le k}^{\infty} \frac{(k-1)!}{i!\,(k-1-i)!} (-t)^{k-1-i} X^i = k \sum_{i=0}^{\infty} \binom{k-1}{i} (-t)^{k-1-i} X^i.$$

A 8.2.10

Gg: $P(X) = X^n + a_{n-1} X^{n-1} + \dots + a_0 = \prod_{i=1}^{n} (X - t_i) \in K[X]$

(a) Zz: $\forall n \in \mathbb{N}_0 : a_0 = (-1)^n t_1 t_2 \cdots t_n$.

IA: $n = 0$. $a_0 = 1 = \prod_{i=1}^{0} \cdots$

IS: $\prod_{i=1}^{n+1} (X - t_i) = \prod_{i=1}^{n} (X - t_i)(X - t_{n+1})$

$= (X^n + a_{n-1} X^{n-1} + \dots + (-1)^n t_1 \cdots t_n)(X - t_{n+1})$

$= X^{n+1} + a_{n-1} X^n + \dots + a_0 X$

$\quad - t_{n+1} X^n - a_{n-1} t_{n+1} X^{n-1} - \dots + (-1) t_1 \cdots t_{n+1}$

(b) Zz: $\forall n \in \mathbb{N}^\times : a_{n-1} = -(t_1 + \dots + t_n)$

IA: $n = 1$. ✓

IS: $\prod_{i=1}^{n+1} (X - t_i) = \dots =$

$X^{n+1} - (t_1 + \dots + t_n) X^n + a_{n-2} X^{n-1} + \dots + a_0 X$

$- t_{n+1} X^n + (t_1 + \dots + t_n) t_{n+1} X^{n-1} - a_{n-2} t_{n+1} X^{n-2} - \dots - a_0 t_{n+1}$

$= X^{n+1} - (t_1 + \dots + t_{n+1}) X^n + \dots$

(c) Zz: $\forall n \in \mathbb{N}_{\geq 2} : a_{n-2} = \sum_{1 \leq i < j \leq n} t_i t_j$

IA: $n = 2$. ✓

IS: $\prod_{i=1}^{n+1} (X - t_i) = (X^n + a_{n-1} X^{n-1} + \sum_{1 \leq i < j \leq n} t_i t_j X^{n-2} + a_{n-3} X^{n-3}$

$+ \dots + a_0)(X - t_{n+1})$

$= \dots + \sum_{1 \leq i < j \leq n} t_i t_j X^{n-1} + \dots - \left(-\sum_{k=1}^{n} t_k\right) t_{n+1} X^{n-1} - \dots$