Spezielle Matrizen aus $K^{n \times n}$

E_{ij} : Eintrag 1 an Stelle (i,j), sonst 0.

$$D_j(\lambda) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \lambda & & \\ & & & & 1 & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \leftarrow j\text{-te Zeile}$$

$T_{ij} = E + E_{ij}$ für $i \neq j$.

<u>Notiz</u> $A = (\underline{a}_1 \ldots \underline{a}_n)$

Dann $$A \cdot D_j(\lambda) = (\underline{a}_1 \ldots \underline{a}_j \ldots \underline{a}_n) \cdot \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \lambda & \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

$$= (\underline{a}_1 \ldots \underline{a}_{j-1} \; \lambda \underline{a}_j \; \underline{a}_{j+1} \ldots \underline{a}_n)$$

und $$A \cdot T_{ij} = (\underline{a}_1 \ldots \underline{a}_i \ldots \underline{a}_j \ldots \underline{a}_n) \cdot \begin{array}{c} \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & 1 & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \begin{array}{l} \\ \\ \leftarrow i \\ \\ \leftarrow j \\ \\ \\ \end{array} \\ \begin{array}{cc} \uparrow & \uparrow \\ i & j \end{array} \end{array}$$

$$= (\underline{a}_1 \ldots \underline{a}_{j-1} \; \underline{a}_j + \underline{a}_i \; \underline{a}_{j+1} \ldots \underline{a}_n)$$

für $i \neq j$

<u>Folgt</u> $\det(A \cdot T_{ij}) = \det(A)$

$\det(A \cdot D_j(\lambda)) = \lambda \det(A)$

6.12 Satz Vorgelegt ist eine Funktion $f: K^{n\times n} \to K$
mit
- $f(A \cdot T_{ij}) = f(A)$ für alle $A \in K^{n\times n}$, $i \neq j$
- $f(A \cdot D_j(\lambda)) = \lambda \cdot f(A)$ für alle $A \in K^{n\times n}$, j, $\lambda \in K$.

Dann gibt es ein $r_0 \in K$, nämlich $r_0 = f(E)$,
so dass $f(A) = r_0 \cdot \det(A)$ für alle $A \in K^{n\times n}$ gilt.

6.13 Satz Für $A, B \in K^{n\times n}$ gilt $\det(A \cdot B) = \det(A) \cdot \det(B)$

Beweis (6.13) Setze $f(B) := \det(A \cdot B)$ für $B \in K^{n\times n}$.
Erhalte: $f: K^{n\times n} \to K$ mit
- $f(B \cdot T_{ij}) = \det(A \cdot B \cdot T_{ij}) = \det(A \cdot B) = f(B)$
- $f(B \cdot D_j(\lambda)) = \det(A \cdot B \cdot D_j(\lambda)) = \lambda \cdot \det(AB) = \lambda \cdot f(B)$

Mit (6.12) erhalte

$$\det(A \cdot B) = f(B) = f(E) \cdot \det(B) = \det(A \cdot E) \cdot \det(B) = \det(A) \cdot \det(B)$$

$\blacksquare$

6.12 Satz Vorgelegt ist eine Funktion $f: K^{n\times n} \to K$

mit
- $f(A \cdot T_{ij}) = f(A)$ für alle $A \in K^{n\times n}$, $i \neq j$
- $f(A \cdot D_j(\lambda)) = \lambda \cdot f(A)$ für alle $A \in K^{n\times n}$, j, $\lambda \in K$.

Dann gibt es ein $r_0 \in K$, nämlich $r_0 = f(E)$,

so dass $f(A) = r_0 \cdot \det(A)$ für alle $A \in K^{n\times n}$ gilt.

Beweis (6.12): Zeige, dass f eine alternierende Multilinearform auf K^n ist, also $f \in \mathrm{Alt}_n(K^n)$, also $f = r_0 \cdot \det$ für passendes $r_0 \in K$.

Dabei $f(E) = r_0 \cdot \det E = r_0$; alles gezeigt!

Vorbereitung: $\lambda \neq 0$, $i \neq j \Rightarrow f(\ldots, \underline{a}_i, \ldots, \underline{a}_j, \ldots)$

$= \frac{1}{\lambda} f(\ldots \lambda \underline{a}_i \ldots \underline{a}_j \ldots) = \frac{1}{\lambda} f(\ldots \lambda \underline{a}_i \ldots \underline{a}_j + \lambda \underline{a}_i \ldots)$

$= f(\ldots \underline{a}_i \ldots \underline{a}_j + \lambda \underline{a}_i \ldots)$

Schritt 1: $\underline{a}_1, \ldots, \underline{a}_n$ lin. abh. $\overset{!}{\Longrightarrow} f(\underline{a}_1, \ldots, \underline{a}_n) = 0$

Dazu sei z.B. $\underline{a}_1 = \sum_{k=2}^{n} \lambda_k \underline{a}_k$.

Dann gilt $f(\underline{a}_1, \ldots) = f(\underline{a}_1 - \sum_{k=2}^{n} \lambda_k \underline{a}_k, \text{—})$

$= f(\underline{0}, \ldots) = f((\underline{0}\ \underline{a}_2 \ldots \underline{a}_n) D_1(0)) =$

$= 0 \cdot f(\underline{0}\ \underline{a}_2 \ldots \underline{a}_n) = 0$ ✓

Schritt 2 f ist multilinear (dann fertig)

- $f(\ldots \lambda \underline{a}_j \ldots) = f((\ldots \underline{a}_j \ldots) \cdot D_j(\lambda)) = \lambda \cdot f(\ldots \underline{a}_j \ldots)$
- Fehlt: $f(\ldots, \underline{a}_i + \underline{\tilde{a}}_i, \ldots) = f(\ldots, \underline{a}_i, \ldots) + f(\ldots, \underline{\tilde{a}}_i, \ldots)$

Sind $\underline{a}_1, \ldots, \underline{a}_{i-1}, \underline{a}_{i+1}, \ldots, \underline{a}_n$ linear abhängig,
so stimmt die Gleichung: $0 = 0 + 0$

Sonst: Ergänze zu einer Basis $\underline{a}_1, \ldots, \underline{a}_{i-1}, \underline{w}, \underline{a}_{i+1}, \ldots, \underline{a}_n$
von K^n und schreibe $\underline{a}_i = \sum_{i \neq j} \alpha_j \underline{a}_j + \lambda \cdot \underline{w}$

und $\underline{\tilde{a}}_i = \sum_{i \neq j} \tilde{\alpha}_j \underline{a}_j + \tilde{\lambda} \cdot \underline{w}$

Dann $f(\ldots, \underline{a}_i, \ldots) = f(\ldots, \underline{a}_i - \sum_{i \neq j} \alpha_j \underline{a}_j, \ldots)$

$= f(\ldots, \lambda \underline{w}, \ldots) = \lambda \cdot f(\ldots \underline{w} \ldots)$

Analog: $f(\ldots \underline{\tilde{a}}_i \ldots) = \tilde{\lambda} \cdot f(\ldots \underline{w} \ldots)$

$f(\ldots \underline{a}_i + \underline{\tilde{a}}_i \ldots) = (\lambda + \tilde{\lambda}) \cdot f(\ldots \underline{w} \ldots)$

$\blacksquare$

Einschub: Polynome

Vorgelegt ist ein Körper K.

Wir studieren den Polynomring $K[x]$.

- Ist $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x]$ mit $a_n \neq 0$, so heißt die Zahl $n = \operatorname{grad} p(x)$ der Grad von $p(x)$.
- $p(x), q(x) \in K[x]$. Dann heißt $p(x)$ ein Teiler von $q(x)$, wenn es ein $a(x) \in K[x]$ mit $q(x) = a(x) \cdot p(x)$ gibt. "$p(x)$ teilt $q(x)$".
  Schreibe dann $p(x) \mid q(x)$

Beispiel: $x^2+x+1 \mid 2x^4 - x^3 - 2x + 1$, denn:

$$(2x^4 - x^3 - 2x + 1) : (x^2+x+1) = 2x^2 - 3x + 1$$

$$\begin{array}{l}
(2x^4 - x^3 - 2x + 1) \\
-(2x^4 + 2x^3 + 2x^2) \quad \leftarrow \quad 2x^2 \cdot (x^2+x+1) \\
\hline
 -3x^3 - 2x^2 - 2x + 1 \\
 -(-3x^3 - 3x^2 - 3x) \\
\hline
 x^2 + x + 1 \\
 -(x^2 + x + 1) \\
\hline
 0
\end{array}$$

Also: $2x^4 - x^3 - 2x + 1$

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

✓

Division mit Rest:

Zu zwei Polynomen $p(x)$, $q(x)$ gibt $a(x)$, $r(x)$ mit

- $q(x) = a(x) \cdot p(x) + r(x)$
- $\operatorname{grad} r(x) < \operatorname{grad} p(x)$

Der Grad des Nullpolynoms ist $-\infty$

Bsp: $q(x) = 3x^4 + x^3 + 5x^2 + x + 6$

$p(x) = x^2 + x + 1$

$$(3x^4 + x^3 + 5x^2 + x + 6) : (x^2 + x + 1) = 3x^2 - 2x + 4$$

$$\begin{array}{l}
(3x^4 + x^3 + 5x^2 + x + 6) \\
\underline{-(3x^4 + 3x^3 + 3x^2)} \\
\qquad -2x^3 + 2x^2 + x + 6 \\
\qquad \underline{-(-2x^3 - 2x^2 - 2x)} \\
\qquad\qquad 4x^2 + 3x + 6 \\
\qquad\qquad \underline{-(4x^2 + 4x + 4)} \\
\qquad\qquad\qquad -x + 2
\end{array}$$

$$3x^4 + x^3 + 5x^2 + x + 6 = (3x^2 - 2x + 4) \cdot (x^2 + x + 1) + \overbrace{(-x + 2)}^{\text{Rest}}$$

Übung. Dividiere mit Rest:

(a) $(x^5 + 3x^4 - 2x^3 + x^2 + 1) : (x^2 + 2x - 3)$

(b) $(x^6 + 1) : (x^4 - 1)$

(a) $(x^5 + 3x^4 - 2x^3 + x^2 + 1) : (x^2 + 2x - 3) = x^3 + x^2 - x + 6$

$$
\begin{array}{l}
x^5 + 3x^4 - 2x^3 + x^2 + 1 \\
-(x^5 + 2x^4 - 3x^3) \\
\hline
\phantom{-(x^5 +{}} x^4 + x^3 + x^2 + 1 \\
\phantom{-(x^5 +{}} -(x^4 + 2x^3 - 3x^2) \\
\hline
\phantom{-(x^5 + x^4 +{}} -x^3 + 4x^2 + 1 \\
\phantom{-(x^5 + x^4 +{}} -(-x^3 - 2x^2 + 3x) \\
\hline
\phantom{-(x^5 + x^4 + x^3 +{}} 6x^2 - 3x + 1 \\
\phantom{-(x^5 + x^4 + x^3 +{}} -(6x^2 + 12x - 18) \\
\hline
\phantom{-(x^5 + x^4 + x^3 + 6x^2 {}} -15x + 19
\end{array}
$$

$$x^5 + 3x^4 - 2x^3 + x^2 + 1 = (x^3 + x^2 - x + 6) \cdot (x^2 + 2x - 3) - 15x + 19.$$

Übung: Dividiere mit Rest:

(b) $(x^6+1):(x^4-1)$

$$
\begin{array}{l}
(x^6+1):(x^4-1) = x^2 \\
-\underline{(x^6-x^2)} \\
x^2+1
\end{array}
$$

$$x^6+1 = x^2\cdot(x^4-1) + x^2+1$$

Größter gemeinsamer Teiler:

$0 \neq p(x), q(x) \in K[x]$ vorgelegt.

Ein Polynom $d(x) \in K[x]$ heißt **größter gemeinsamer Teiler (ggT)** von $p(x), q(x)$, falls

(1.) $d(x) \mid p(x), q(x)$

(2.) $g(x) \mid p(x), q(x) \implies g(x) \mid d(x)$

Satz Es gibt einen größten gemeinsamen Teiler $d(x)$ von $p(x), q(x)$, und dieser lässt sich schreiben als

$$d(x) = s(x) \cdot p(x) + t(x) \cdot q(x)$$

für passende Polynome $s(x), t(x)$.

Der erweiterte Euklidische Algorithmus:

Eingabe: $p(x), q(x) \in K[x] \setminus \{0\}$

Initialisierung: $k = 0$, $r_0(x) = p(x)$, $r_1(x) = q(x)$
$s_0(x) = 1$, $s_1(x) = 0$
$t_0(x) = 0$, $t_1(x) = 1$

Schleife:

- Erhöhe k um 1
- Division mit Rest: $r_{k-1}(x) = a(x) \cdot r_k(x) + r(x)$ mit $\operatorname{grad} r(x) < \operatorname{grad} r_k(x)$
- Setze $r_{k+1}(x) = r(x) = r_{k-1}(x) - a(x) \cdot r_k(x)$
  und $s_{k+1}(x) = s_{k-1}(x) - a(x) \cdot s_k(x)$
  und $t_{k+1}(x) = t_{k-1}(x) - a(x) \cdot t_k(x)$

bis $r_{k+1}(x) = 0$ gilt.

Rückgabe: $d(x) = r_k(x)$, $s(x) = s_k(x)$, $t(x) = t_k(x)$

Dann ist $d(x)$ ein ggT von $p(x), q(x)$
und es gilt $d(x) = s(x) \cdot p(x) + t(x) \cdot q(x)$

Beweis Initialisierung: $k=0$, $r_0(x) = p(x)$, $r_1(x) = q(x)$

$s_0(x) = 1$, $s_1(x) = 0$

$t_0(x) = 0$, $t_1(x) = 1$

Setze $r_{k+1}(x) = r(x) = r_{k-1}(x) - a(x)\cdot r_k(x)$

und $s_{k+1}(x) = s_{k-1}(x) - a(x)\cdot s_k(x)$

und $t_{k+1}(x) = t_{k-1}(x) - a(x)\cdot t_k(x)$

① Der Algorithmus terminiert, denn

$\operatorname{grad} r_1(x) > \operatorname{grad} r_2(x) > \operatorname{grad} r_3(x) > \ldots$

② Beh.: $r_j(x) = s_j(x)\cdot p(x) + t_j(x)\cdot q(x)$ für jedes j

Dann nach Schleife: $d(x) = r_k(x) = s_k(x)\cdot p(x) + t_k(x)\cdot q(x)$

$= s(x)\cdot p(x) + t(x)\cdot q(x)$.

$j=0$: $p(x) = 1\cdot p(x) + 0\cdot q(x)$ ✓

$j=1$: $q(x) = 0\cdot p(x) + 1\cdot q(x)$ ✓

$j \geq 1$: $s_{j+1}(x)\cdot p(x) + t_{j+1}(x)\cdot q(x)$

$= (s_{j-1}(x) - a(x)\cdot s_j(x))\cdot p(x) + (t_{j-1}(x) - a(x)\cdot t_j(x))\cdot q(x)$

$= (s_{j-1}(x)\, p(x) + t_{j-1}(x)\, q(x)) - a(x)\,(s_j(x)\, p(x) + t_j(x)\, q(x))$

$= r_{j-1}(x) - a\cdot r_j(x) = r_{j+1}(x)$ ✓

(3) $r_0(x) = p(x), \quad r_1(x) = q(x)$

$$r_0(x) = a_1(x)\cdot r_1(x) + r_2(x)$$
$$r_1(x) = a_2(x)\cdot r_2(x) + r_3(x)$$
$$r_2(x) = a_3(x)\cdot r_3(x) + r_4(x)$$
$$\vdots$$
$$r_{k-3}(x) = a_{k-2}(x)\, r_{k-2}(x) + r_{k-1}(x)$$
$$r_{k-2}(x) = a_{k-1}(x)\, r_{k-1}(x) + r_k(x)$$
$$r_{k-1}(x) = a_k(x)\cdot r_k(x) + \underline{\underline{0}}$$
$$= a_k(x)\cdot d(x)$$

$d(x) \mid r_0(x), r_1(x)$

$d(x) \mid r_1(x), r_2(x)$

$\vdots$

$d(x) \mid r_{k-2}(x), r_{k-3}(x)$

$d(x) \mid r_{k-1}(x), r_{k-2}(x)$

$d(x) \mid r_k(x), r_{k-1}(x)$

$d(x)$ teilt $r_0(x) = p(x)$ und $r_1(x) = q(x)$

(4) Teilt $g(x)$ sowohl $p(x)$ als auch $q(x)$, so ist $g(x)$ ein Teiler von $d(x) = s(x)\,p(x) + t(x)\,q(x)$

Also ist $d(x)$ ein ggT von $p(x), q(x)$ $\blacksquare$

Beispiel Der ggT von 22 und 122

	$k=0$	$k=1$	$k=2$				
r	122	22	12	10	2	0	STOP
s	1	0	1	-1	2		
t	0	1	-5	6	-11		
a	–	5 ↑	1	1			

$$122 = 5 \cdot 22 + 12$$
$$12 = 122 - 5 \cdot 22$$
$$1 = 1 - 5 \cdot 0$$
$$-5 = 0 - 5 \cdot 1$$

$$22 = 1 \cdot 12 + 10$$
$$10 = 22 - 1 \cdot 12$$

$$12 = 1 \cdot 10 + 2$$

$$10 = 5 \cdot 2 + 0$$

$$2 = \mathrm{ggT}(122; 22) = 2 \cdot 122 - 11 \cdot 22$$
$$(= 244 - 242)$$

<u>Beispiel</u> Berechne den ggT von x^7-1 und x^2-1

r	x^7-1	x^2-1	$x-1$	0 STOP
s	1	0	1	
t	0	1	$-x^5-x^3-x$	
a		x^5+x^3+x	$x+1$	

$$
\begin{array}{l}
(x^7-1):(x^2-1) = x^5+x^3+x \\
\underline{(x^7-x^5)} \\
\quad x^5-1 \\
\underline{-(x^5-x^3)} \\
\quad x^3-1 \\
\underline{-(x^3-x)} \\
\quad x-1
\end{array}
$$

$$x-1 = \operatorname{ggT}(x^7-1, x^2-1)$$

$$= 1\cdot(x^7-1) - (x^5+x^3+x)\cdot(x^2-1)$$

Hausaufgabe LA13 A

Bestimme einen größten gemeinsamen Teiler $d(x)$ von

$$p(x) = x^3 - 2x^2 - x + 2$$

$$q(x) = x^3 - 4x^2 + 3x$$

und stelle ihn in der Form $d(x) = s(x)\,p(x) + t(x)\,q(x)$

mit Polynomen $s(x), t(x) \in \mathbb{R}[x]$ dar

Einschub: Der Körper GF(p), p Primzahl.

$(\mathbb{Z},+,\cdot)$ ist ein Ring, d.h.

- $(\mathbb{Z},+)$ ist eine abelsche Gruppe, also
  - $(a+b)+c = a+(b+c)$
  - es gibt ein neutrales Element 0, also $a+0=a$
  - zu jedem a gibt es ein a' (nämlich $a'=-a$) mit $a+a'=0$
  - $a+b = b+a$.
- $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
- $a\cdot(b+c) = a\cdot b + a\cdot c$
  $(a+b)\cdot c = a\cdot c + b\cdot c$

$(\mathbb{Z},+,\cdot)$ ist ein kommutative Ring mit Eins, d.h.

zusätzlich gilt:
- $a\cdot b = b\cdot a$
- $1\cdot a = a$

Vorgelegt ist eine natürliche Zahl $n \geq 2$.

Dann ist die Menge $J = n \cdot \mathbb{Z}$ ein Ideal von $\mathbb{Z}$, d.h.

- $0 \in J$
- $a, b \in J \Rightarrow a - b \in J$

$\Big\}$ J Untergruppe von $(\mathbb{Z}, +)$

$a + b = a - (0 - b)$

- $a \in J,\ b \in \mathbb{Z} \Rightarrow a \cdot b \in J$

Für $z \in \mathbb{Z}$ setze $\boxed{\overline{z} = [z]_n = \{ z + j \mid j \in J \}}$

z.B.
$$
\begin{aligned}
[3]_5 &= \{ 3 + j \mid j \in 5 \cdot \mathbb{Z} \} \\
&= \{ 3 + 5 \cdot k \mid k \in \mathbb{Z} \} \\
&= \text{Menge der Zahlen mit Rest } 3 \text{ bei Division durch } 5 \\
&= [18]_5
\end{aligned}
$$

$$(3 + 5 \cdot k) + (4 + 5 \cdot j) = 7 + 5 \cdot (k + j) = 2 + 5(k + j + 1)$$

$$\overline{3} + \overline{4} = \overline{2}$$

Für das Ideal $\mathcal{J} = n \cdot \mathbb{Z}$ setze

$$\mathbb{Z}/\mathcal{J} = \{ [z]_n \mid z \in \mathbb{Z} \}$$

Restklasse

Faktorring;
lies " $\mathbb{Z}$ nach $\mathcal{J}$ "

z.B. $\mathbb{Z}/5\cdot\mathbb{Z} = \{ [0]_5, [1]_5, [2]_5, [3]_5, [4]_5 \}$

Beh.: $\mathbb{Z}/\mathcal{J}$ wird mit

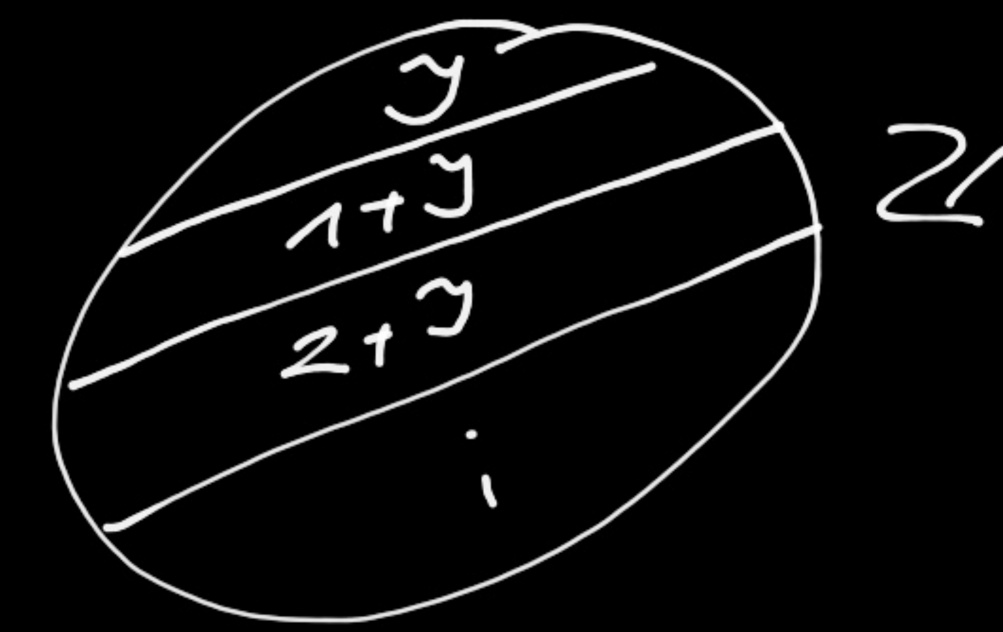
$$\bar{x} + \bar{y} = \overline{x+y}$$
$$\bar{x} \cdot \bar{y} = \overline{x \cdot y}$$

ein kommutativer Ring mit 1.

"+", "·" sind wohldefiniert, d.h.

$$\bar{x} = \bar{x'} \text{ und } \bar{y} = \bar{y'} \implies \overline{x+y} = \overline{x'+y'}$$
$$\text{und } \overline{x \cdot y} = \overline{x' \cdot y'}$$

$\mathbb{Z}/\mathcal{J} = \{\bar{x} \mid x \in \mathbb{Z}\}$



- $x = x+0 \in \bar{x}$,

  d.h. die Restklassen $\bar{x}$

  "überdecken" $\mathbb{Z}$, also $\mathbb{Z} = \bigcup_{x \in \mathbb{Z}} \bar{x}$

- $\bar{x} \neq \bar{y} \overset{!}{\Longrightarrow} \bar{x} \cap \bar{y} = \emptyset$

  bzw. $\bar{x} \cap \bar{y} \neq 0$, $\quad z \in \bar{x} \cap \bar{y} \overset{!}{\Longrightarrow} \bar{x} = \bar{y}$

  $z \in \bar{x} \cap \bar{y} \Longrightarrow z = x + j_1 = y + j_2$ mit $j_1, j_2 \in \mathcal{J}$

  $\Longrightarrow x = y + (j_2 - j_1)$

Also: $\bar{x} = \{x + j \mid j \in \mathcal{J}\} = \{y + \underbrace{(j_2 - j_1) + j}_{\in \mathcal{J}} \mid j \in \mathcal{J}\}$

$\subseteq \{y + j' \mid j' \in \mathcal{J}\} = \bar{y}$,

analog $\bar{y} \subseteq \bar{x}$, also $\bar{x} = \bar{y}$

Folgt: $\bar{x} = \bar{y} \iff \exists j \in \mathcal{J} : y = x + j$ bzw. $y - x \in \mathcal{J}$

$(\in \bar{x} \cap \bar{y})$

"+" und "·" sind wohldefiniert:

$\overline{x'} = \overline{x}$ bzw. $x' = x + i$, $i \in \mathcal{J}$

$\overline{y'} = \overline{y}$ bzw. $y' = y + j$, $j \in \mathcal{J}$

- $x' + y' = x + i + y + j = x + y + \underbrace{(i+j)}_{\in \mathcal{J}} \in \overline{x+y}$

  Also $\overline{x' + y'} = \overline{x+y}$

- $x' \cdot y' = (x+i)\cdot(y+j) = x \cdot y + \underbrace{\underbrace{x \cdot j}_{\in \mathcal{J}} + \underbrace{y \cdot i}_{\in \mathcal{J}} + \underbrace{i \cdot j}_{\in \mathcal{J}}}_{\in \mathcal{J}} \in \overline{x \cdot y}$

  Also $\overline{x \cdot y} = \overline{x' \cdot y'}$

$\mathbb{Z}/\mathcal{J}$ ist ein kommutativ mit Eins:

Assoziativität von $+$:

$$(\overline{x} + \overline{y}) + \overline{z} = \overline{x+y} + \overline{z} = \overline{(x+y)+z}$$

$$= \overline{x+(y+z)} = \overline{x} + \overline{y+z} = \overline{x} + (\overline{y} + \overline{z})$$

Rest ähnlich, neut. Element $\overline{0}$, Eins $\overline{1}$.

Ist n keine Primzahl, so ist $\mathbb{Z}/n\mathbb{Z}$ kein Körper.

<u>Bsp</u> $n = 6 = 2 \cdot 3$

$[2]_6 \neq [0]_6 \neq [3]_6$ $\qquad (\overline{2}, \overline{3} \neq \overline{0})$

Aber $\overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = [6]_6 = [0]_6 = \overline{0}$

Wäre $\overline{z} \cdot \overline{2} = 1$, so wäre $\left.\begin{aligned} \overline{z} \cdot \overline{2} \cdot \overline{3} &= \overline{0} \\ = 1\,\overline{3} &= \overline{3} \end{aligned}\right\}$ ↯

Folgt $\overline{2}$ lässt sich in $\mathbb{Z}/6\mathbb{Z}$ nicht invertieren.

Satz: Ist p eine Primzahl, so ist

$$GF(p) = \mathbb{Z}/p\cdot\mathbb{Z}$$ ein Körper.

Beweis: Zum Körper fehlt lediglich die Existenz inverser Elemente.

Dazu: $[m]_p \neq [0]_p$, d.h. p ist kein Teiler von m.

p Primzahl $\Rightarrow 1 = ggT(p, m) = s\cdot p + t\cdot m$

für passende $s, t \in \mathbb{Z}$

Also: $1 \in [t\cdot m]_p \Rightarrow [1]_p = [t\cdot m]_p = [t]_p \cdot [m]_p$

bzw. $[t]_p$ ist ein multiplikatives Inverses von $[m]_p$. ∎

Beispiele

GF(2):

$+$	$\bar 0$	$\bar 1$
$\bar 0$	$\bar 0$	$\bar 1$
$\bar 1$	$\bar 1$	$\bar 0$

$\cdot$	$\bar 0$	$\bar 1$
$\bar 0$	$\bar 0$	$\bar 0$
$\bar 1$	$\bar 0$	$\bar 1$

GF(5)

$+$	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$
$\bar 0$	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$
$\bar 1$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 0$
$\bar 2$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 0$	$\bar 1$
$\bar 3$	$\bar 3$	$\bar 4$	$\bar 0$	$\bar 1$	$\bar 2$
$\bar 4$	$\bar 4$	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$

$\cdot$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$
$\bar 1$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$
$\bar 2$	$\bar 2$	$\bar 4$	$\bar 1$	$\bar 3$
$\bar 3$	$\bar 3$	$\bar 1$	$\bar 4$	$\bar 2$
$\bar 4$	$\bar 4$	$\bar 3$	$\bar 2$	$\bar 1$

GF(127) : $\overline{20}^{-1} = ?$

r	127	20	7	6	1	0	STOP
s	1	0	1	-2	3		
t	0	1	-6	13	-19		
a		6	2	1	6		

$$\bar 1 = \bar 3 \cdot \underbrace{\overline{127}}_{}{}^{=\bar 0} - \overline{19} \cdot \overline{20}$$

$$381 - 380$$

$$-19 + 127 = 108$$

$$\bar 1 = \overline{-19} \cdot \overline{20}$$
$$= \overline{108} \cdot \overline{20}$$

$$\rightsquigarrow \overline{20}^{-1} = \overline{108}$$

Exkurs: $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ ↖ 4-dim.

E, M, M^2, M^3, M^4 linear abhängig

Man findet $r_0, \dots, r_4 \in \mathbb{R}$ mit

$$p(M) = r_4 M^4 + r_3 M^3 + r_2 \cdot M^2 + r_1 M + r_0 \cdot E = 0$$

$$p(x) = r_4 x^4 + r_3 x^3 + r_2 x^2 + r_1 x + r_0 \in \mathbb{R}[x]$$

$$\varphi : \mathbb{R}[x] \longrightarrow \mathbb{R}^{2\times 2}, \quad p(x) \longmapsto p(M)$$

$$\mathcal{I} = \text{"}\ker \varphi\text{"} = \{ p(x) \in \mathbb{R}[x] \mid p(M) = 0 \}$$ <u>Ideal</u>

Es ist $\mathcal{I} = \mathbb{R}[x] \cdot \mu(x)$

Hier: $\mu(x) = (x-2)\cdot(x-3) = x^2 - 5x + 6$

$$M^2 - 5M + 6E = \begin{pmatrix} 4 & 0 \\ 0 & 9 \end{pmatrix} - 5 \cdot \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} + 6 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 4 - 10 + 6 & 0 \\ 0 & 9 - 15 + 6 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$