§1 Signatur:

Definition: Sei $\sigma \in S_n$. Dann ist

$$\mathrm{sign}(\sigma) := \begin{cases} +1, & \text{die Anzahl der Fehlstände gerade,} \\ -1, & \text{— " — ungerade.} \end{cases}$$

Fehlstand von σ ist ein Paar (i,j) mit $i<j$ und $\sigma(i)>\sigma(j)$.

- $\mathrm{sign}(\sigma) = (-1)^{\#\text{Fehlstände von } \sigma}$.

$\#$: "Anzahl von"

Beh.: $\mathrm{sign}(\sigma) = \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j}$ für alle $\sigma \in S_n$.

Beweis:
$$\prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j} = \frac{\prod_{1\le i<j\le n} (\sigma(i)-\sigma(j))}{\prod_{1\le i<j\le n} (i-j)}$$

$$\sigma : \{1,\dots,n\} \xrightarrow{1:1} \{1,\dots,n\}$$

$$\{\sigma(1),\sigma(2),\dots,\sigma(n)\} = \{1,\dots,n\}$$

$$\{(i,j) \mid 1\le i<j\le n\} \xleftrightarrow{1:1} \{(\sigma(i),\sigma(j)) \mid 1\le i<j\le n\}$$

$\rightsquigarrow$ für $1\le i<j\le n$: $\sigma(i)-\sigma(j) = \begin{cases} \sigma(i)-\sigma(j), & \sigma(i)<\sigma(j) \text{ (d.h. kein Fehlst.)} \\ (-1)\cdot(\sigma(j)-\sigma(i)), & \sigma(j)<\sigma(i) \text{ (d.h. Fehlstand)} \end{cases}$

$$\rightsquigarrow \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j} = (-1)^{\#\text{Fehlst. von } \sigma} = \mathrm{sign}(\sigma). \qquad \square$$

Bsp.: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \in S_4$

Fehlst.: $(1,2), (1,4), (2,4), (3,4)$

$\mathrm{sign}(\sigma) = 1 = (-1)^4$

$1<2$, $\sigma(1) > \sigma(2)$
$\quad\;\; \|\qquad\quad \|$

$\mathrm{sign}(\sigma) = 1 = (-1)^4$

$1 < 2,\ \sigma(1) > \sigma(2)$
$\quad\ \ 3 \ > \ 2$

$\sigma(2) = 2 < 4 = \sigma(3)$
$\quad\ \ 2 < 3$

$$\prod_{1\le i<j\le 4} \frac{\sigma(i)-\sigma(j)}{i-j} = \underbrace{\frac{3-2}{1-2}}_{(1,2)} \cdot \underbrace{\frac{\cancel{3-4}}{1-3}}_{(1,3)} \cdot \underbrace{\frac{3-1}{1-4}}_{(1,4)} \cdot \underbrace{\frac{\cancel{2-4}}{2-3}}_{(2,3)} \cdot \underbrace{\frac{2-1}{\cancel{2-4}}}_{(2,4)} \cdot \underbrace{\frac{4-1}{\cancel{3-4}}}_{(3,4)}$$

$$= (-1)^{1+1+1+1} = (-1)^4 = 1 = \mathrm{sign}(\sigma).$$

$$\prod_{1\le i<j\le n} \frac{(-1)(\sigma(j)-\sigma(i))}{(-1)(j-i)} = \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j}.$$

Beh.: $\mathrm{sign}(\sigma\circ\tau) = \mathrm{sign}(\sigma)\cdot\mathrm{sign}(\tau)$ für alle $\sigma,\tau\in S_n$.

Bew.: Aus A.2.4.7 wissen wir:

$$\mathrm{sign}(\sigma\circ\tau) = \prod_{1\le i<j\le n} \frac{(\sigma\circ\tau)(j)-(\sigma\circ\tau)(i)}{j-i}$$

$$= \prod_{1\le i<j\le n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i}\cdot\frac{\tau(j)-\tau(i)}{\tau(j)-\tau(i)}$$

$$= \prod_{1\le i<j\le n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)}\cdot\frac{\tau(j)-\tau(i)}{j-i}$$

$$= \left(\prod_{1\le i<j\le n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)}\right)\cdot\underbrace{\prod_{1\le i<j\le n}\frac{\tau(j)-\tau(i)}{j-i}}_{\mathrm{sign}(\tau)}$$

$$= \left(\prod_{1\le i<j\le n} \frac{\sigma(j)-\sigma(i)}{j-i}\right)\cdot\mathrm{sign}(\tau)$$

$$= \mathrm{sign}(\sigma)\cdot\mathrm{sign}(\tau). \qquad (*) \qquad \square$$

Jede Permutation lässt sich schreiben als Verkettung von Transpositionen (nicht eindeutig!)

$\rightsquigarrow$ $\mathrm{sign}(\text{Transposition}) = -1$

$\rightsquigarrow$ Schreibe $\sigma \in S_n$ als Verkettung von Transp.

Formel (*) $\rightsquigarrow$ $\underline{\mathrm{sign}(\sigma)} = (-1)^{\#\text{Transpositionen}} = \begin{cases} 1, & \#\text{Transp. gerade} \\ -1, & \#\text{Transp. ungerade.} \end{cases}$

---

§2 Gruppen

- Wenn G endlich: $\mathrm{Ord}(G) :=$ Anzahl der Elemente von G

  Wenn $g \in G$:
  - $\mathrm{ord}(g) := \# \{ g^0, g^1, g^2, \dots \}$
  - $g^{\mathrm{Ord}(G)} = e$ $\underline{\text{für alle}}$ $g \in G$!

<u>Bsp.:</u> $G = \left((\mathbb{Z}/43\mathbb{Z})^*, \cdot \right)$. $\quad \left((\mathbb{Z}/43\mathbb{Z})^* := \mathbb{Z}/43\mathbb{Z} \setminus \{[0]\} \right)$

$\mathrm{Ord}(G) = 42$

gegeben: $[3]$ ist <u>Primitivwurzel</u> von G ist, d.h. $[3]$ ist ein Erzeuger von G, d.h.

$$G = \{ [3]^0, [3]^1, \dots, [3]^{41} \}.$$

$$[7]^3 = [7]^2 \cdot [7] = [49][7] = [6][7] = [-1] \Rightarrow [7]^6 = [-1]^2 = [1].$$

---

§3 Ringe

Seien R eine Menge, sowie zwei Verknüpfungen $+, \cdot : R \times R \to R$ mit ausgezeichneten Elemente $0, 1 \in R$ mit

(i) $(R, +)$ Gruppe mit neutralem Element 0

(ii) $(R, \cdot)$ Monoid mit neutralem Element 1

(iii) Distributivgesetze gelten:

$$(s+t) \cdot r = s \cdot r + t \cdot r$$
$$r \cdot (s+t) = r \cdot s + r \cdot t \quad \text{für alle } r, s, t \in R.$$

Dann heißt $(R, +, \cdot)$ "Ring".

Bsp.: $(\mathbb{Z}, +, \cdot)$

- ! es gibt auch nicht-nullteilerfreie Ringe

  Nullteiler: ein Element $r \in R$ mit $r \neq 0$, sodass ein $s \in R$, $s \neq 0$, $r \cdot s = 0$.

  Bsp.: $(\mathbb{Z}/6\mathbb{Z}, +, \cdot)$ $\rightsquigarrow$ $[2], [3] \neq [0]$

  Aber: $[2] \cdot [3] = [2 \cdot 3] = [6] = [0]$

  $\rightsquigarrow$ $[2], [3]$ Nullteiler in $\mathbb{Z}/6\mathbb{Z}$.

- Integritätsbereich $:=$ nullteilerfreier Ring

- Körper: $(K, +, \cdot)$ mit (i) $(K, +)$ Gruppe

Menge   2 Verknüpfungen $K \times K \to K$

(ii) $(K\setminus\{0\}, \cdot)$ Gruppe

(iii) Distributivgesetze gelten

$\Longleftrightarrow$ Körper = Ring, sodass zu jedem Element $\neq 0$ ein multiplikativ Inverses existiert.

$\to$ Jeder Körper ist ein nullteilerfreier Ring.

$\leadsto$ Umkehrung gilt nicht! (z.B. $(\mathbb{Z}, +, \cdot)$).

$\leadsto$ "Integritätsbereich" ist etwas zw. Ring und Körper".

$\{\text{Ringe}\} \supset \{\text{Integr.ber.}\} \supset \{\text{Körper}\}$

Bsp.: $(\mathbb{R}, +, \cdot)$ ist ein Körper.

$f(X) = 2X - 1, \quad g(X) = X^2 + 3$

$$(f+g)(X) = (2X-1) + (X^2+3) = X^2 + 2X + 2$$

$$(f \cdot g)(X) = (2X-1)\cdot(X^2+3) = 2X^3 - X^2 + 6X - 3$$

$$(f \circ g)(X) = f(g(X)) = 2 \cdot g(X) - 1 = 2\cdot(X^2+3) - 1 = 2X^2 + 5.$$

Sei $(R, +, \cdot)$ Ring & X eine formale Variable

$R[X] = \{$ Menge aller Polynome mit Koeff. in $R\}$.

$(R[X], +, \cdot)$ ist wieder ein Ring.