Gruppe: Verknüpfung $*$ auf Menge M

- neutrales Element $e * a = a * e = a \quad \forall a \in M$
- Assoziativität: $(a * b) * c = a * (b * c)$
- inverses Element: für jedes $a \in M$ gibt es ein $b \in M$ s.d.
  $a * b = b * a = e$
  ($b =$ "$-a$")

M ist **kommutativ** wenn $a * b = b * a \quad \forall a, b \in M$.

Ellipt. Kurve: $P \in E$

$A \in \mathbb{N}$

$$A \cdot P = \begin{cases} \text{1. Methode: } \underbrace{(\overbrace{(\underbrace{P \oplus P}_{=2 \cdot P}) \oplus P}^{=3 \cdot P}) \oplus P \oplus \ldots}_{A-1 \text{ Rechenschritte}} \\ \text{2. Methode:} \end{cases}$$

Binärdarstellung $A = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \ldots, \quad \leftarrow a_0, a_1, \ldots \in \{0, 1\}$

$P \oplus P = 2P \quad \leftarrow$ 1 Rechenschritt

$(2P) \oplus (2P) = 4P$

$(4P) \oplus (4P) = 8P$

$(8P) \oplus (8P) = 16P$ usw.

$$A \cdot P = a_0 \cdot P \oplus a_1 \cdot (2P) \oplus a_2 \cdot (4P) \oplus \ldots$$ $\leftarrow$ weniger Rechenschritte!

Bsp: $135 \cdot P$

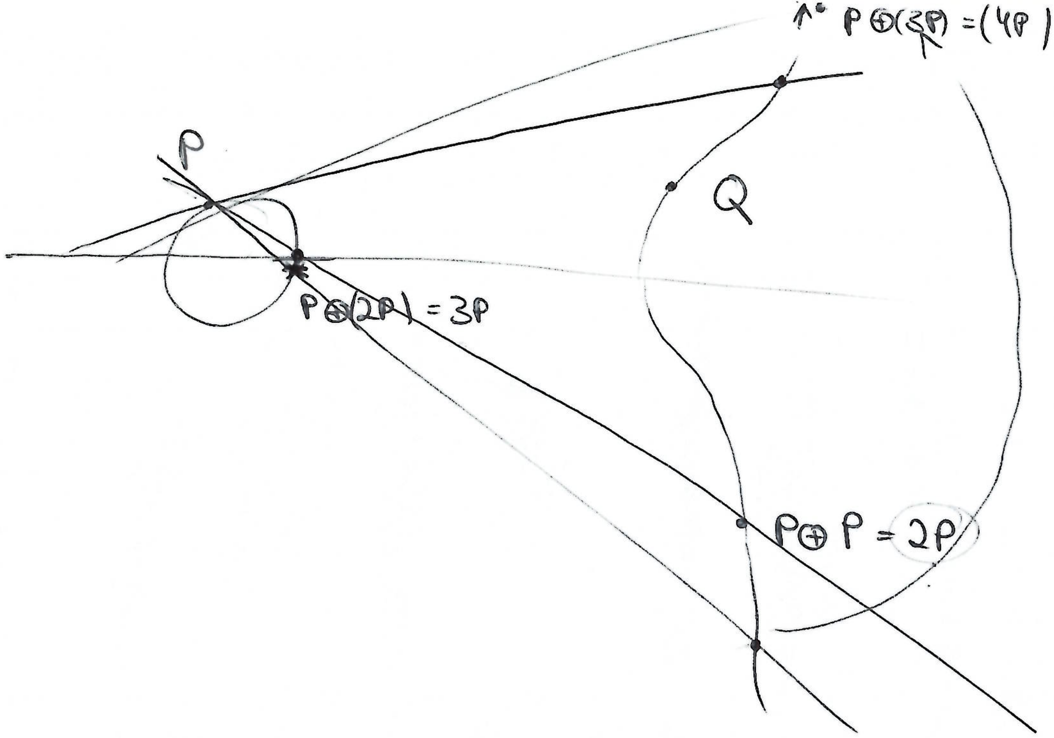
Methode 1: 134 Additionen

Methode 2: $135 = 128 + 4 + 2 + 1$
$= 2^7 + 2^2 + 2^1 + 2^0$

10 Additionen:

$\rightarrow$ Berechne $\underbrace{2 \cdot P,\ 2^2 \cdot P,\ 2^3 \cdot P,\ 2^4 \cdot P,\ 2^5 \cdot P,\ 2^6 \cdot P,\ 2^7 \cdot P}_{7 \text{ Additionen}}$

und $135 \cdot P = \underbrace{(2^7 \cdot P) \oplus (2^2 \cdot P) \oplus (2 \cdot P) \oplus P}_{3 \text{ Additionen}}$

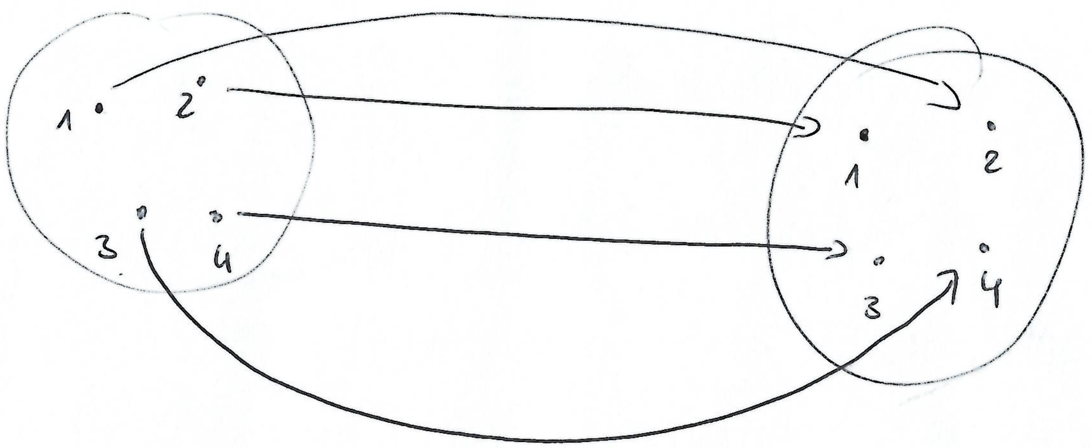


Abbildungsgruppen:

$M = \{1, \dots, 4\}$

bijektive Abb

$f: M \to M$



1	2	3	4
2	1	4	3

$f(2) = 1$

1-4 durchgetausch / permutiert

$\Downarrow$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

"Permutation von 4 Elementen"

- $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\qquad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id$$

$$f \circ g = id.$$

- $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ $\qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

$$f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\cancel{1 \quad 2 \quad 3 \quad 4}$$

$$\begin{array}{|c|c|c|c|} 4 & 3 & 1 & 2 \\ \hline 1 & 2 & 3 & 4 \end{array}$$

$$\cancel{\begin{array}{|c|c|c|c|} 4 & 3 & 1 & 2 \\ \hline 1 & 2 & 3 & 4 \end{array}}$$

$$\begin{array}{|c|c|c|c|} 2 & 1 & 4 & 3 \\ \hline 1 & 2 & 3 & 4 \end{array}$$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Verknüpfung. $\qquad$ neutrales Element: $id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

nicht kommutativ

inverses Element zu $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \text{ allgemein } \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}^{-1} = \begin{cases} a \longmapsto 1 \\ b \longmapsto 2 \\ c \longmapsto 3 \end{cases} \quad d \to 4$$

+ Assoziativität: $(f \circ g) \circ h(x) = f(g(h(x))) = f \circ (g \circ h(x))$

Ringe:

- $(\mathbb{Z}, +, \cdot)$: Ring, weil

  $(\mathbb{Z}, +)$: kommutative Gruppe

  $\cdot$ und $+$ erfüllen Assoziativ- und Distributivgesetz.

- $(m\mathbb{Z}, +, \cdot)$ ist ein Unterring.

  $m\mathbb{Z} = \{m \cdot x \mid x \in \mathbb{Z}\}$.

  - Abgeschlossenheit bzgl $+$: $m \cdot x + m \cdot y = m \cdot (x+y) \in m\mathbb{Z}$ ✓
  - Abgeschlossenheit bzgl $\cdot$: $(m \cdot x) \cdot (m \cdot y) = m(m\,xy) \in m\mathbb{Z}$ ✓
  - Abgeschlossenheit bzgl Inversenbildung (bzgl $+$): das Inverse von $m \cdot x$ ist $-mx$ bzw. $m \cdot (-x) \in m\mathbb{Z}$ ✓

- $(\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$: Ring = "Restklassenring"

  $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{(m-1)}\}$

  $\bar{0}$ neutrales Element

  $-\bar{a} = \overline{m-a}$ inverse

  z. B. $\mathbb{Z}/5\mathbb{Z}$: $\bar{2} \oplus \bar{3} = \bar{0}$

  Assoziativgesetz für $\odot$: $(\bar{a} \odot \bar{b}) \odot \bar{c} =$

  $\overline{a \cdot b} \odot \bar{c} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot (b \cdot c)} = \bar{a} \odot \overline{b \cdot c}$

  $= \bar{a} \odot (\bar{b} \odot \bar{c})$.

  alle anderen Assoz. / Distributivgesetze folgen aus denen in $\mathbb{Z}$.

- **Polynomringe:**

  z. B. $\mathbb{Q}[x]$ = alle Polynome mit rationalen Koeffizienten

  $\mathbb{Z}[x]$ = alle Polynome mit ganzzahligen Koeffizienten.

~~R R~~ $(R, +, \cdot)$ Ring $\Rightarrow$ $(R, +)$ Gruppe

$(K, +, \cdot)$ $\Rightarrow$ $(K, +, \cdot)$ auch Ring $\Rightarrow$ $(K, +)$ Gruppe
Körper $\Rightarrow$ $(K \setminus 0, \cdot)$ auch Gruppe

Polynomring $\mathbb{Z}[x]$: Nullpolynom $= 0$ neutrale Element
$5x^3 + 2x^2 - 10$ inverses El. bzgl $+$: z.B.

$f(x) = 1 + 2x + x^3$: $-f(x) = -1 - 2x - x^3 \in \mathbb{Z}[x]$

$g(x) = 4 + 3x$

$f \cdot g = (1 + 2x + x^3)(4 + 3x) =$
$= 4 + 3x + 8x + 6x^2 + 4x^3 + 3x^4$
$= 3x^4 + 4x^3 + 6x^2 + 11x + 4.$