Strassen-Matrix-Multiplication

multiplication of $(n\times n)$-matrices

with $0(n^{\log 7}) = O(n^{2,8\ldots})$ arithmetic operations

rings

Here

$$\mathbb{N} = \{1, 2, \ldots\}$$

Ring $R = (S, +, *, 0, 1)$

- S: set
- $+, * : S \times S \to S$ operations
- $+$ associative and commutative, $*$ associative

$$(a+b)+c = (a+(b+c)) \quad , \quad a+b = b+a \quad , \quad (a*b)*c = a*(b*c)$$

- distributivity laws from both sides

$$a*(b+c) = a*b+a*c \quad , \quad (b+c)*a = b*a+c*a$$

- 0 and 1 are neutral elements of $+$ and $*$

$$r+0 = 0+r = r \quad , \quad r*1 = 1*r = r$$

- elements $r \in S$ have inverse elements $(-r)$ with respec t to $+$

$$r+(-r) = 0$$

define

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

rings

Here

$$\mathbb{N} = \{1, 2, \dots\}$$

Ring $R = (S, +, *, 0, 1)$

- S: set
- $+, * : S \times S \to S$ operations
- $+$ associative and commutative, $*$ associative

$$(a+b)+c = (a+(b+c)) \quad , \quad a+b = b+a \quad , \quad (a*b)*c = a*(b*c)$$

- distributivity laws from both sides

$$a*(b+c) = a*b+a*c \quad , \quad (b+c)*a = b*a+c*a$$

- 0 and 1 are neutral elements of $+$ and $*$

$$r+0 = 0+r = r \quad , \quad r*1 = 1*r = r$$

- elements $r \in S$ have inverse elements $(-r)$ with respec t to $+$

$$r+(-r) = 0$$

define

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

examples

- integers

$$(\mathbb{Z}, +, -, 0, 1)$$

- integers mod m

$$\mathbb{Z}_m = ([0:m-1], + \quad \mathrm{mod}\ m, \cdot \quad \mathrm{mod}\ m,\ 0,\ 1)$$

ring homomorphisms

rings

$$\begin{aligned} R &= (S, +, *, 0, 1) \\ R' &= (S', +', *', 0', 1') \end{aligned}$$

def:

$$h : S \to S'$$

with

$$\begin{aligned} h(a+b) &= h(a) +' h(b) \\ h(a*b) &= h(a) *' h(b) \end{aligned}$$

is called *ring homomorphism*

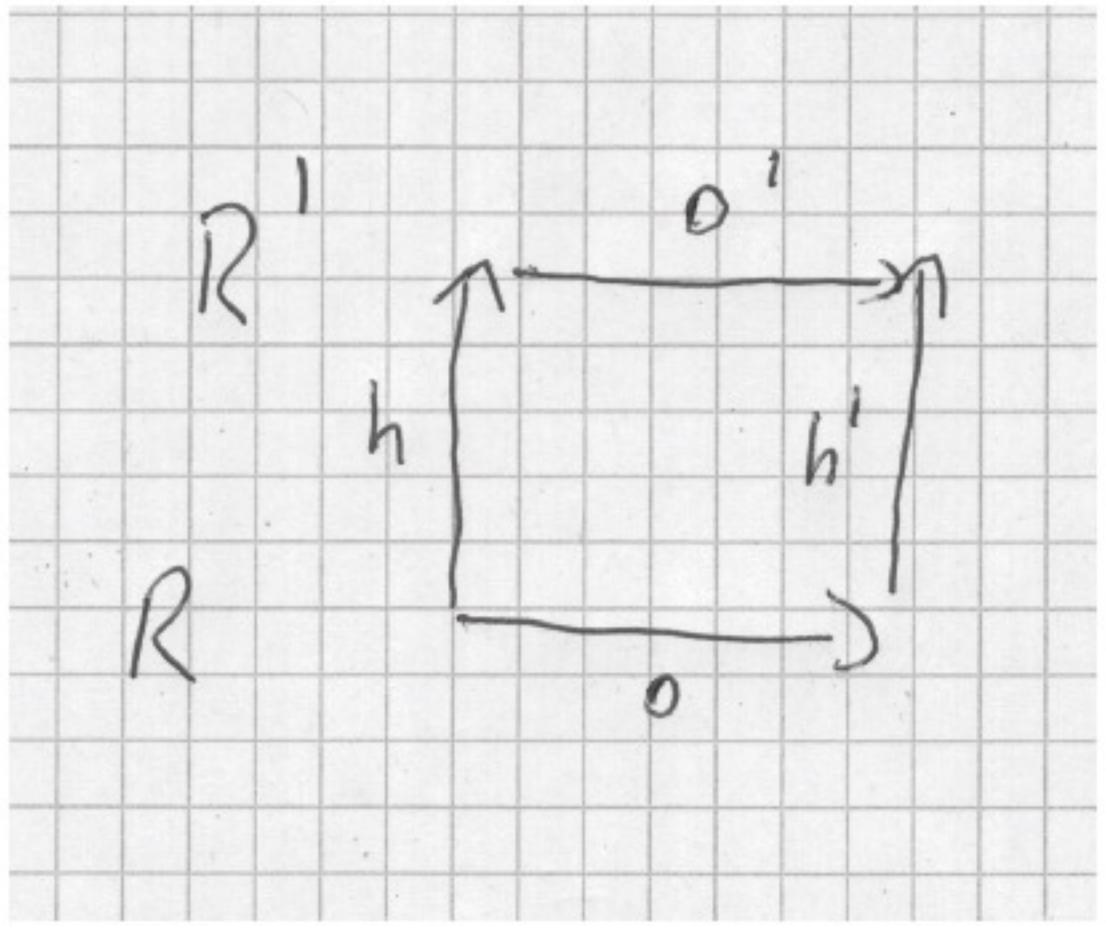

Figure 1: commutative diagram illustrating ring homomorphism h with $\circ \in \{+, *\}$

ring homomorphisms

rings

$$\begin{aligned} R &= (S, +, *, 0, 1) \\ R' &= (S', +', *', 0', 1') \end{aligned}$$

def:

$$h : S \to S'$$

with

$$\begin{aligned} h(a+b) &= h(a) +' h(b) \\ h(a*b) &= h(a) *' h(b) \end{aligned}$$

is called *ring homomorphism*

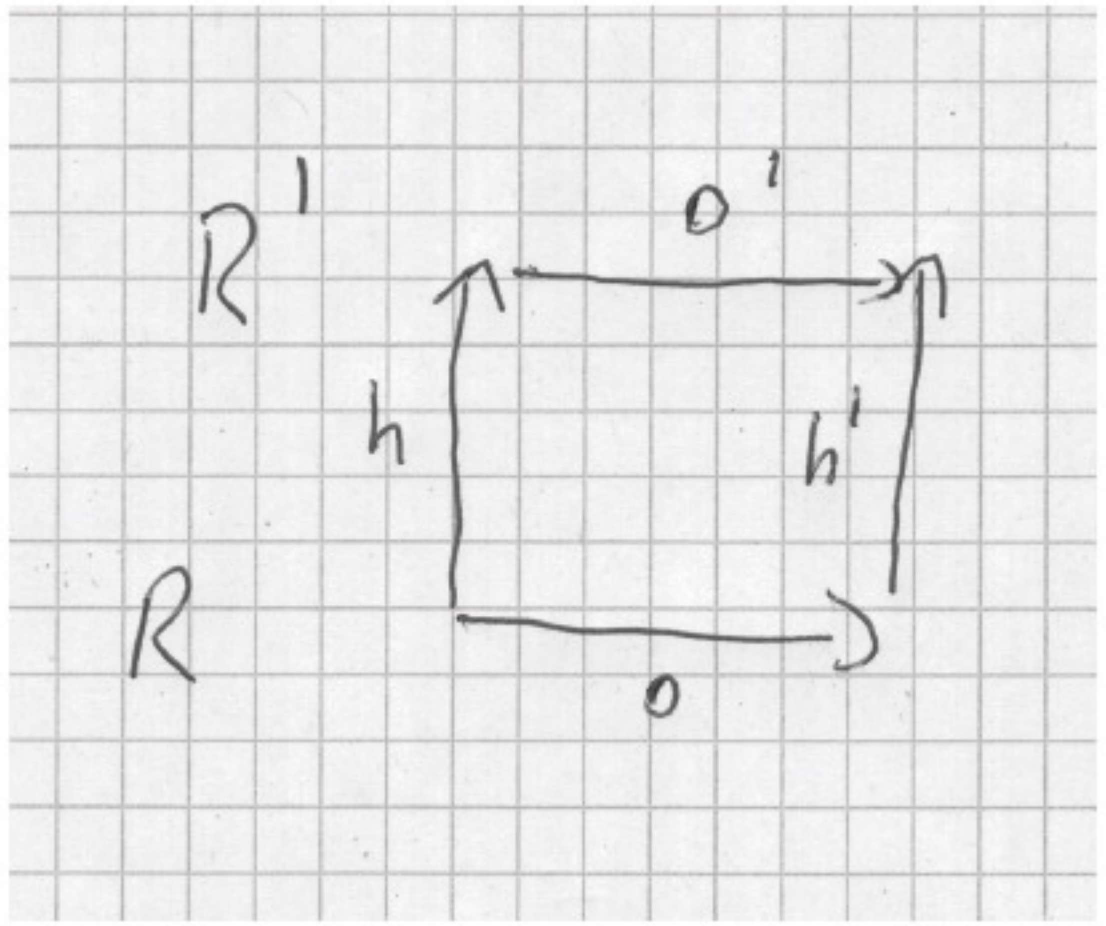

Figure 1: commutative diagram illustrating ring homomorphism h with $\circ \in \{+, *\}$

Example

$$\begin{aligned} R &= (\mathbb{Z}, +, *, 0, 1) \\ R' &= (\mathbb{B}, \oplus, \wedge, 0, 1) \\ h(a) &= (a \bmod 2) \end{aligned}$$

rings of matrices

$$R = (S, +, -, 0, 1) \quad \text{Ring}$$

def: $n \times n$ Matrices with elements in S

$$S_n = \{a : [1:n]^2 \to S \mid a(i,j) \in S \text{ for all } i, j\}$$

def: zero and indentity matrix

$$0_n(i,j) = 0 \text{ for all } i, j$$

$$I_n(i,j) = \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}$$

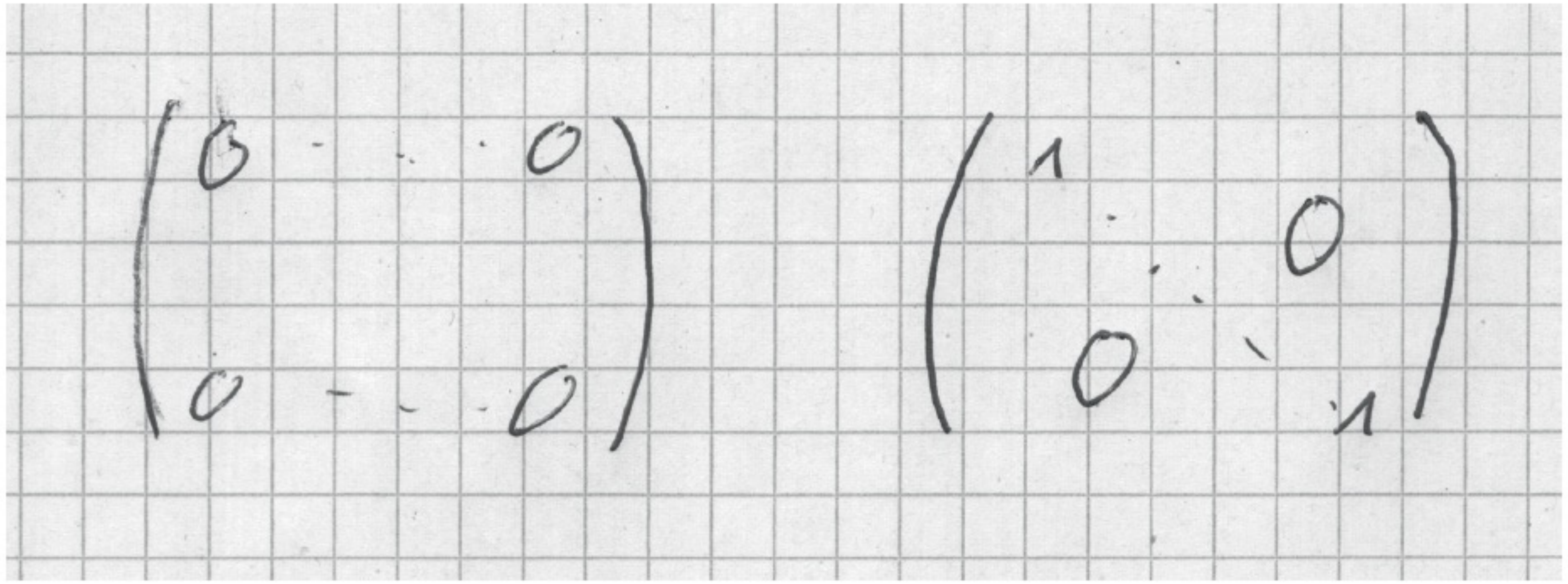

Figure 2: zero matrix (left) and identity matrix (right)

rings of matrices

$$R = (S, +, -, 0, 1) \quad \text{Ring}$$

def: $n \times n$ Matrices with elements in S

$$S_n = \{a : [1:n]^2 \to S \mid a(i,j) \in S \text{ for all } i,j\}$$

def: zero and indentity matrix

$$0_n(i,j) = 0 \text{ for all } i,j$$

$$I_n(i,j) = \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}$$

def: matrix addition and multiplication for $a, b \in S_n$

$$\begin{aligned} (a +_n b)(i,j) &= a(i,j) + b(i,j) \quad \text{(add component wise)} \\ (a *_n b)(i,j) &= \sum_{k=1}^{n} a(i,k) * b(k,j) \quad \text{(scalar product)} \end{aligned}$$

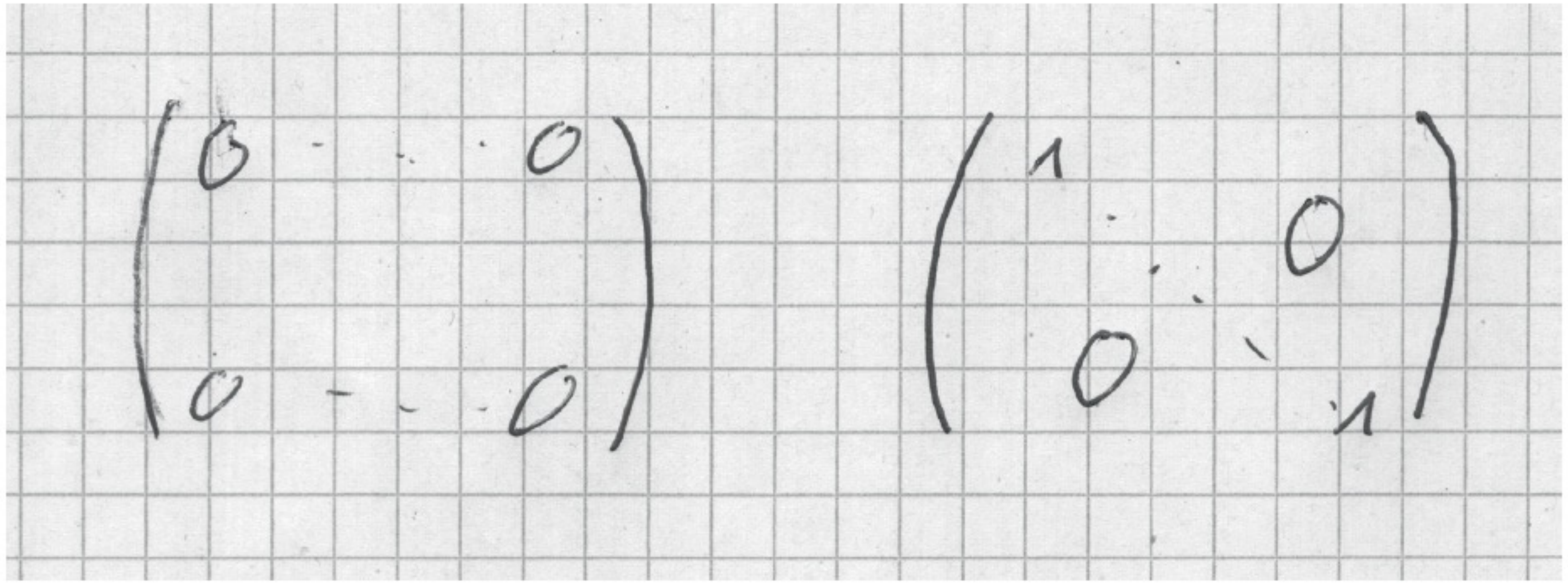

Figure 2: zero matrix (left) and identity matrix (right)

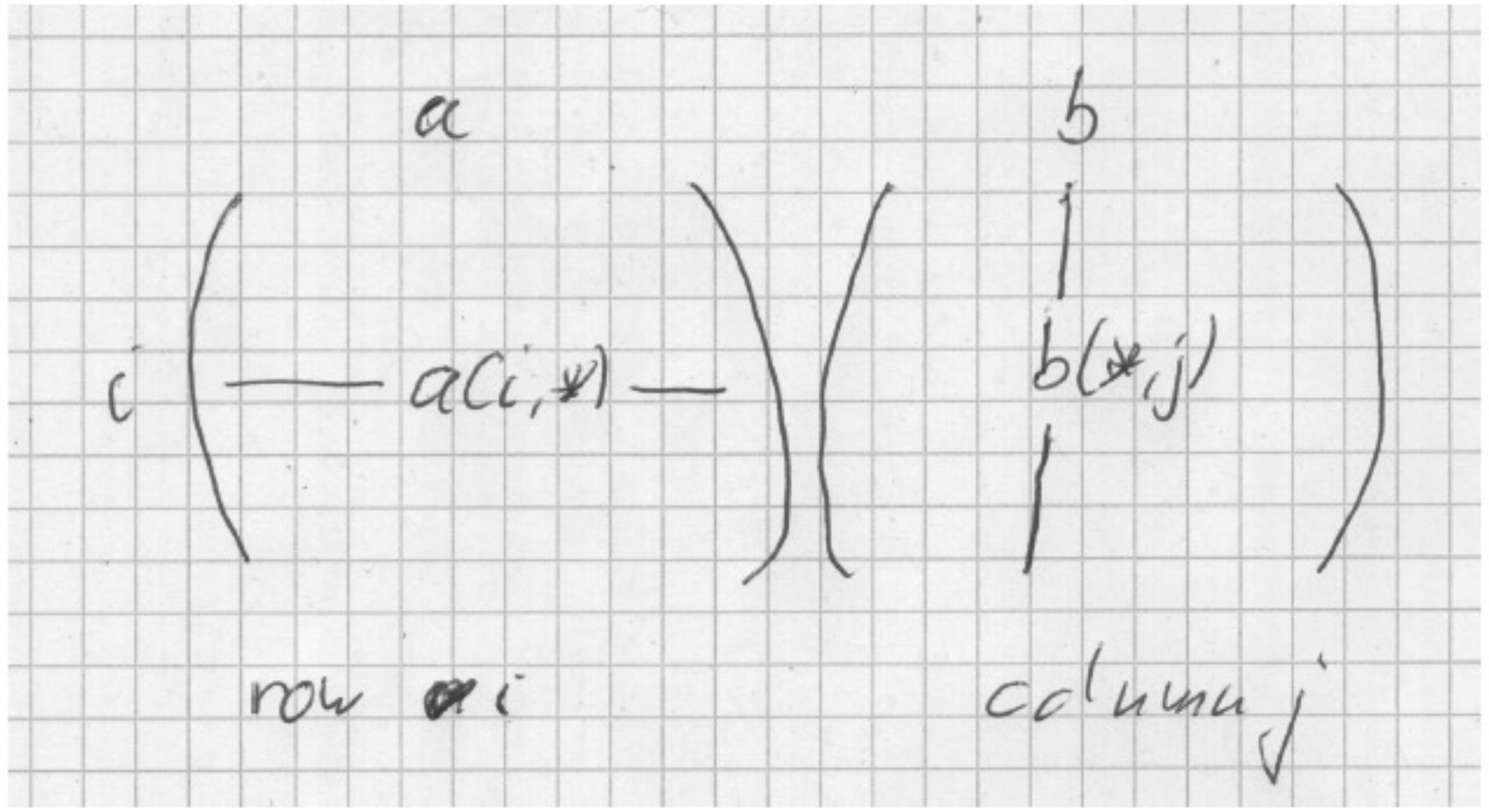

Figure 3: $(a*b)(i,j)$ is computed as scalar product of row i of a with column j of b

rings of matrices

$$R = (S, +, -, 0, 1) \quad \text{Ring}$$

def: $n \times n$ Matrices with elements in S

$$S_n = \{a : [1:n]^2 \to S \mid a(i,j) \in S \text{ for all } i,j\}$$

def: zero and indentity matrix

$$0_n(i,j) = 0 \text{ for all } i,j$$

$$I_n(i,j) = \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}$$

def: matrix addition and multiplication for $a, b \in S_n$

$$\begin{aligned} (a +_n b)(i,j) &= a(i,j) + b(i,j) \quad \text{(add component wise)} \\ (a *_n b)(i,j) &= \sum_{k=1}^{n} a(i,k) * b(k,j) \quad \text{(scalar product)} \end{aligned}$$

Lemma 1. $R_n = (S_n, +_n, *_n, 0_n, I_n)$ *is a ring*

Proof. exercise □

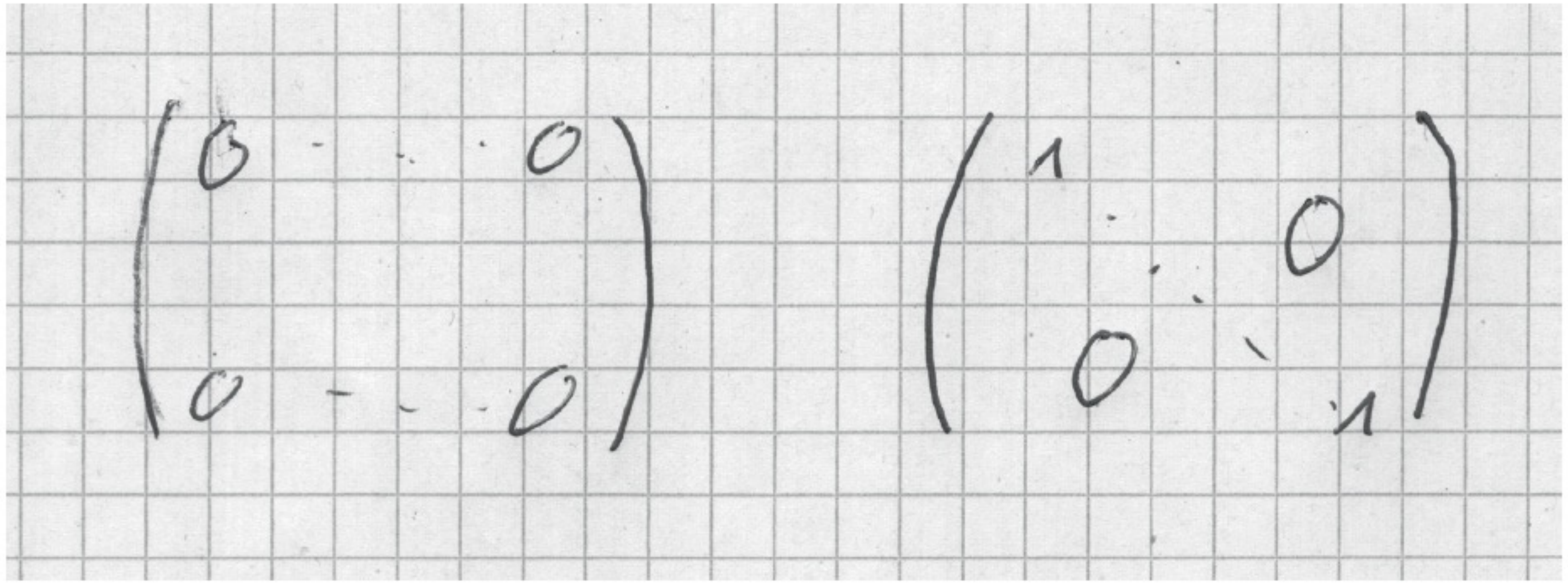

Figure 2: zero matrix (left) and identity matrix (right)

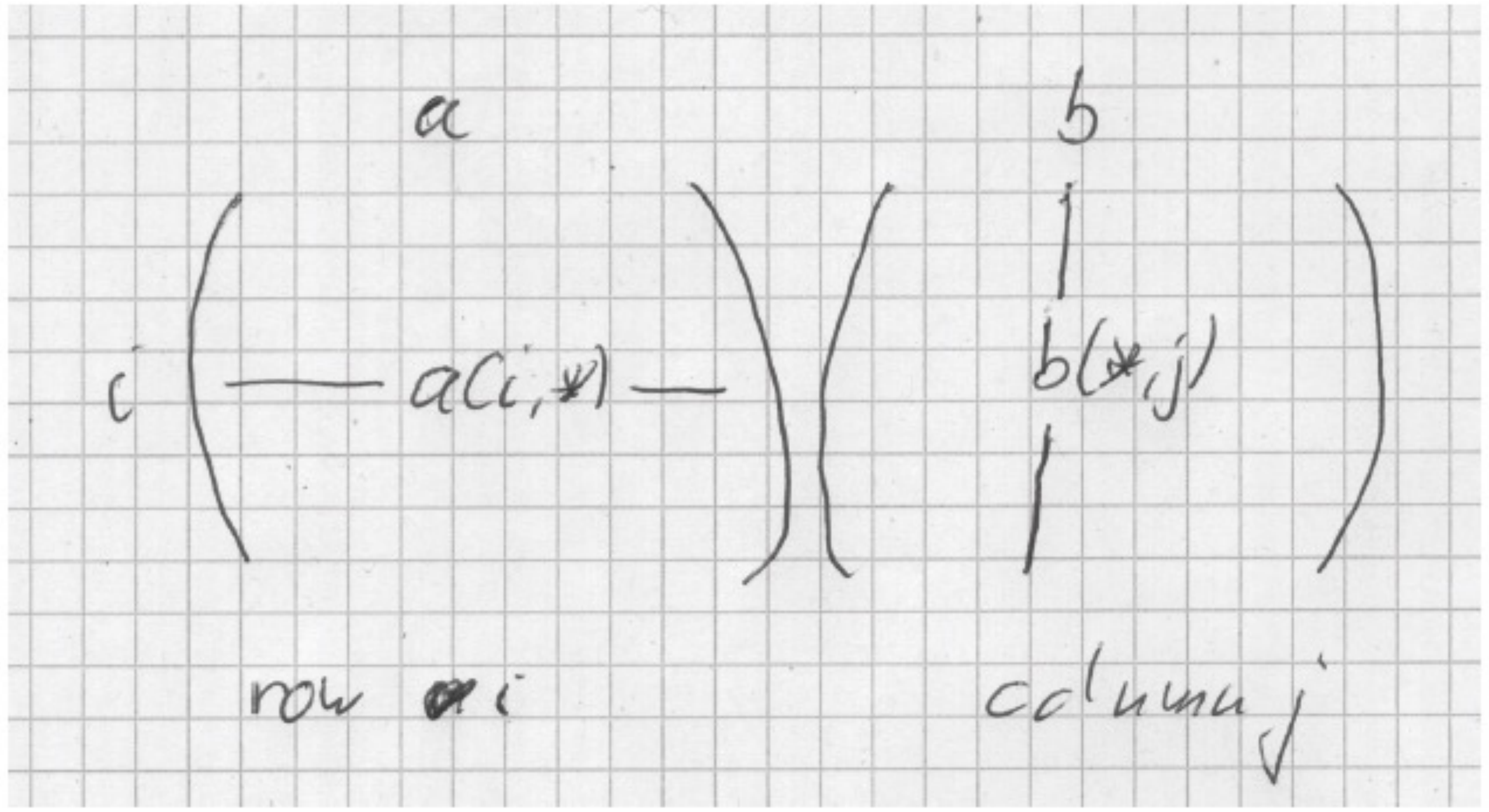

Figure 3: $(a * b)(i,j)$ is computed as scalar product of row i of a with column j of b

divide and conquer for matrix addition and multiplication

$$n = 2^k$$

consider 4 rings

- matrix elements

$$R = (S, +, *, 0, 1)$$

- $(n \times n)$-matrices with elements in R

$$R_n = (S_n, +_n, *_n, 0_n, I_n)$$

- $(n/2 \times n/2)$-matrices with elements in R where $n/2$ is reduced problem size.

$$R_{n/2} = (S_{n/2}, +_{n/2}, *_{n/2}, 0_{n/2}, I_{n/2})$$

- (2×2)-matrices with elements in $S_{n/2}$

$$R_{n/2,2} = (S_{n/2,2}, +_{n/2,2}, *_{n/2,2}, 0_{n/2,2}, I_{n/,2})$$

divide and conquer for matrix addition and multiplication

$$n = 2^k$$

consider 4 rings

- matrix elements

$$R = (S, +, *, 0, 1)$$

- $(n \times n)$-matrices with elements in R

$$R_n = (S_n, +_n, *_n, 0_n, I_n)$$

- $(n/2 \times n/2)$-matrices with elements in R where $n/2$ is reduced problem size.

$$R_{n/2} = (S_{n/2}, +_{n/2}, *_{n/2}, 0_{n/2}, I_{n/2})$$

- (2×2)-matrices with elements in $S_{n/2}$

$$R_{n/2,2} = (S_{n/2,2}, +_{n/2,2}, *_{n/2,2}, 0_{n/2,2}, I_{n/,2})$$

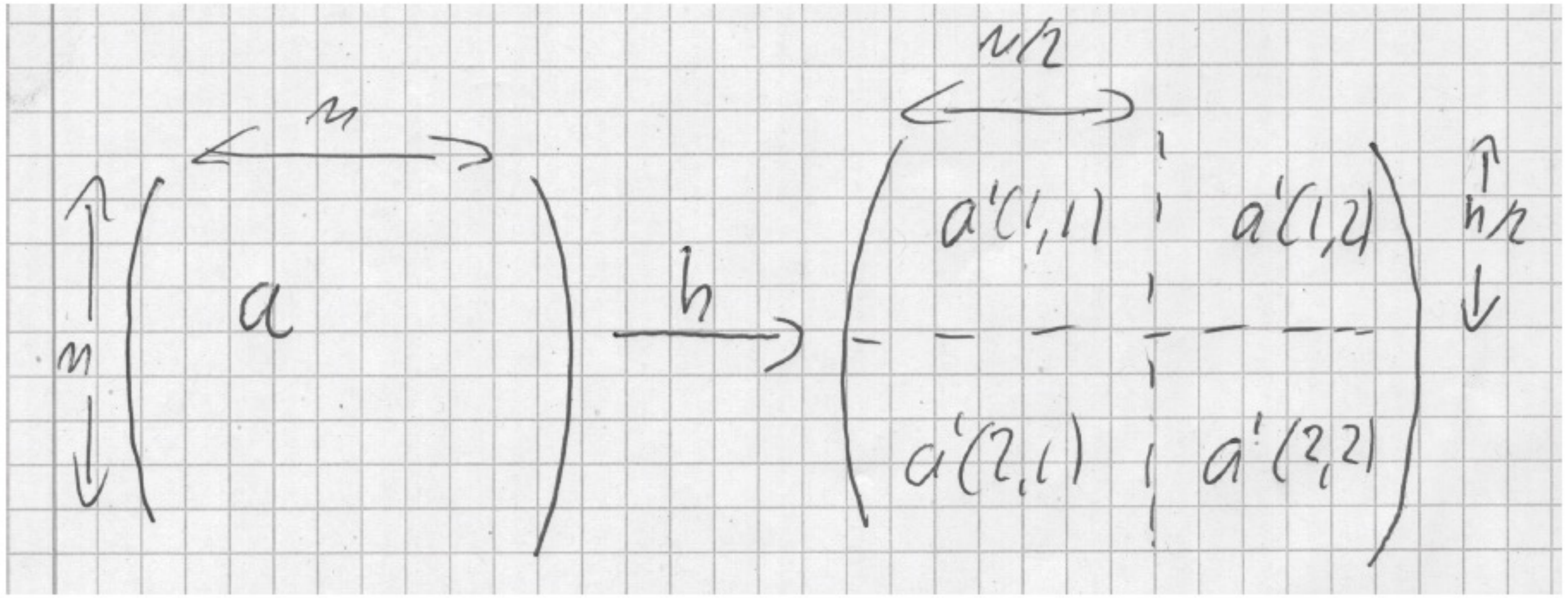

Figure 4: Interpreting $(n \times n)$-matrices as (2×2)-matrices of $(n/2 \times n/2)$-matrices

divide and conquer for matrix addition and multiplication

$$n = 2^k$$

consider 4 rings

- matrix elements

$$R = (S, +, *, 0, 1)$$

- $(n \times n)$-matrices with elements in R

$$R_n = (S_n, +_n, *_n, 0_n, I_n)$$

- $(n/2 \times n/2)$-matrices with elements in R where $n/2$ is reduced problem size.

$$R_{n/2} = (S_{n/2}, +_{n/2}, *_{n/2}, 0_{n/2}, I_{n/2})$$

- (2×2)-matrices with elements in $S_{n/2}$

$$R_{n/2,2} = (S_{n/2,2}, +_{n/2,2}, *_{n/2,2}, 0_{n/2,2}, I_{n/,2})$$

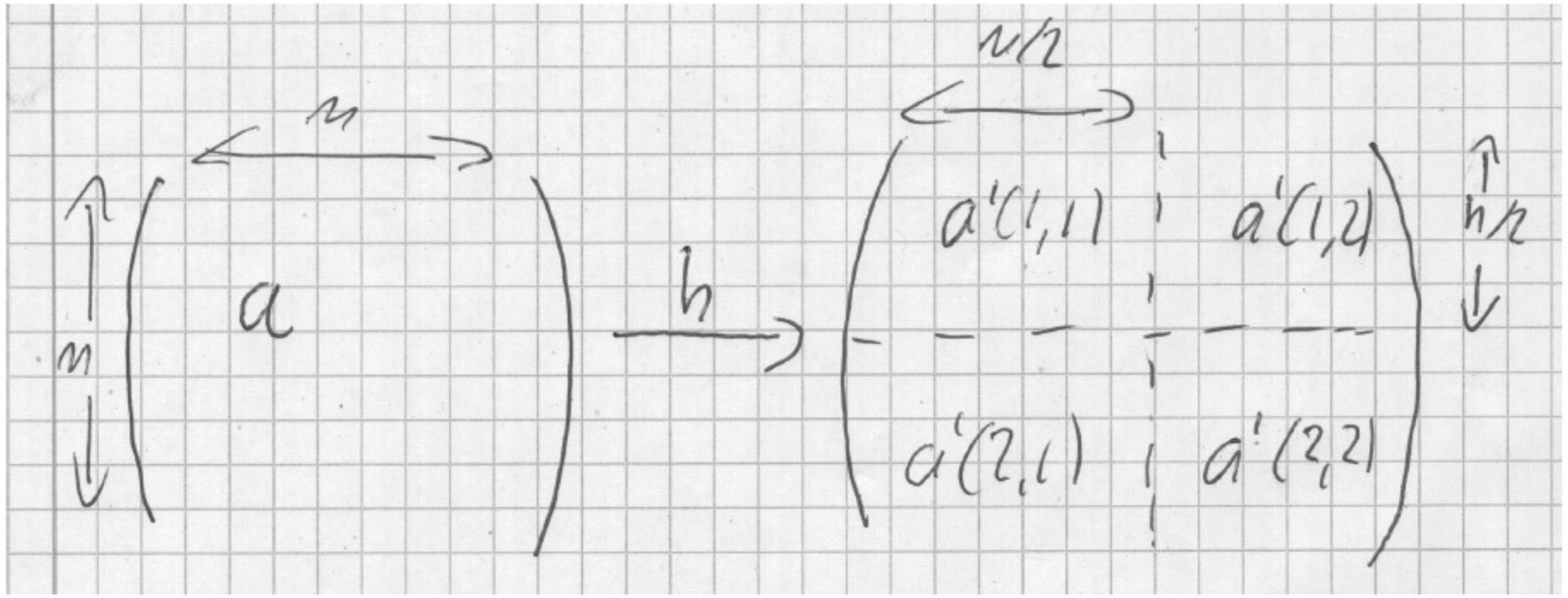

Figure 4: Interpreting $(n \times n)$-matrices as (2×2)-matrices of $(n/2 \times n/2)$-matrices

$$\begin{aligned}
h : S_n &\rightarrow (S_{n/2})_2 \\
h(a) &= \begin{pmatrix} a'(1,1) & a'(1,2) \\ a'(2,1) & a'(2,2) \end{pmatrix} \\
a'(1,1)(i,j) &= a(i,j) \\
a'(1,2)(i,j) &= a(i, n/2 + j) \\
a'(2,1)(i,j) &= a(i + n/2, j) \\
a'(2,2)(i,j) &= (a(i + n/2, j + n/2)
\end{aligned}$$

divide and conquer for matrix addition and multiplication

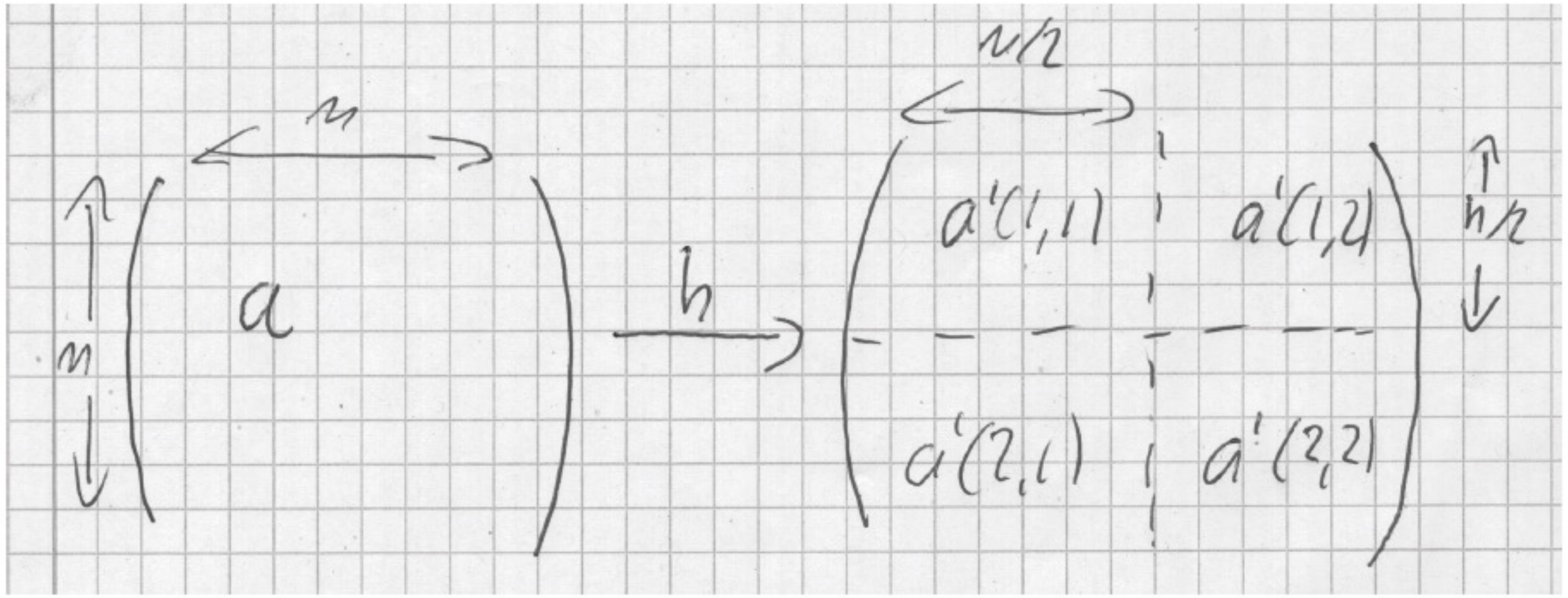

Figure 4: Interpreting $(n \times n)$-matrices as (2×2)-matrices of $(n/2 \times n/2)$-matrices

$$
\begin{aligned}
h : S_n &\rightarrow (S_{n/2})_2 \\
h(a) &= \begin{pmatrix} a'(1,1) & a'(1,2) \\ a'(2,1) & a'(2,2) \end{pmatrix} \\
a'(1,1)(i,j) &= a(i,j) \\
a'(1,2)(i,j) &= a(i,n/2+j) \\
a'(2,1)(i,j) &= a(i+n/2,j) \\
a'(2,2)(i,j) &= (a(i+n/2,j+n/2)
\end{aligned}
$$

Lemma 2. *h is bijective.*

Proof. trivial

divide and conquer for matrix addition and multiplication

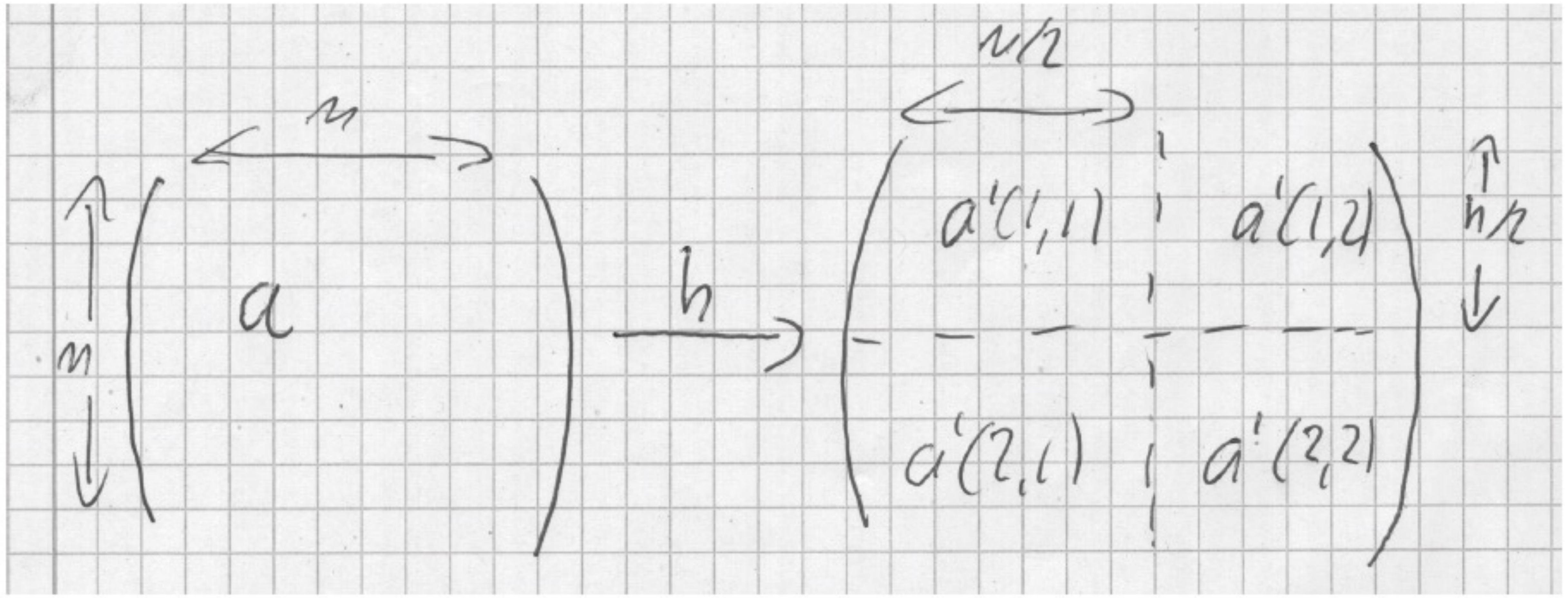

Figure 4: Interpreting $(n \times n)$-matrices as (2×2)-matrices of $(n/2 \times n/2)$-matrices

$$
\begin{aligned}
h : S_n &\rightarrow (S_{n/2})_2 \\
h(a) &= \begin{pmatrix} a'(1,1) & a'(1,2) \\ a'(2,1) & a'(2,2) \end{pmatrix} \\
a'(1,1)(i,j) &= a(i,j) \\
a'(1,2)(i,j) &= a(i,n/2+j) \\
a'(2,1)(i,j) &= a(i+n/2,j) \\
a'(2,2)(i,j) &= (a(i+n/2,j+n/2)
\end{aligned}
$$

Lemma 2. *h is bijective.*

Proof. trivial

Lemma 3. *h is ring homomorphism*

Proof. exercise

$$
\begin{aligned}
a,b \in S_n &\rightarrow \\
h(a *_n b) &= h(a) *_{n/2,2} h(b) \\
\end{aligned}
$$

$$
\boxed{a *_n b = h^{-1}(h(a) *_{n/2,2} h(b))}
$$

Lemma 4. *For arbitrary rings R we can compute the product of (2×2)-matrices $\in R_2$ with 7 multiplications and $O(1)$ additions and subtractions in R*

divide and conquer for matrix addition and multiplication

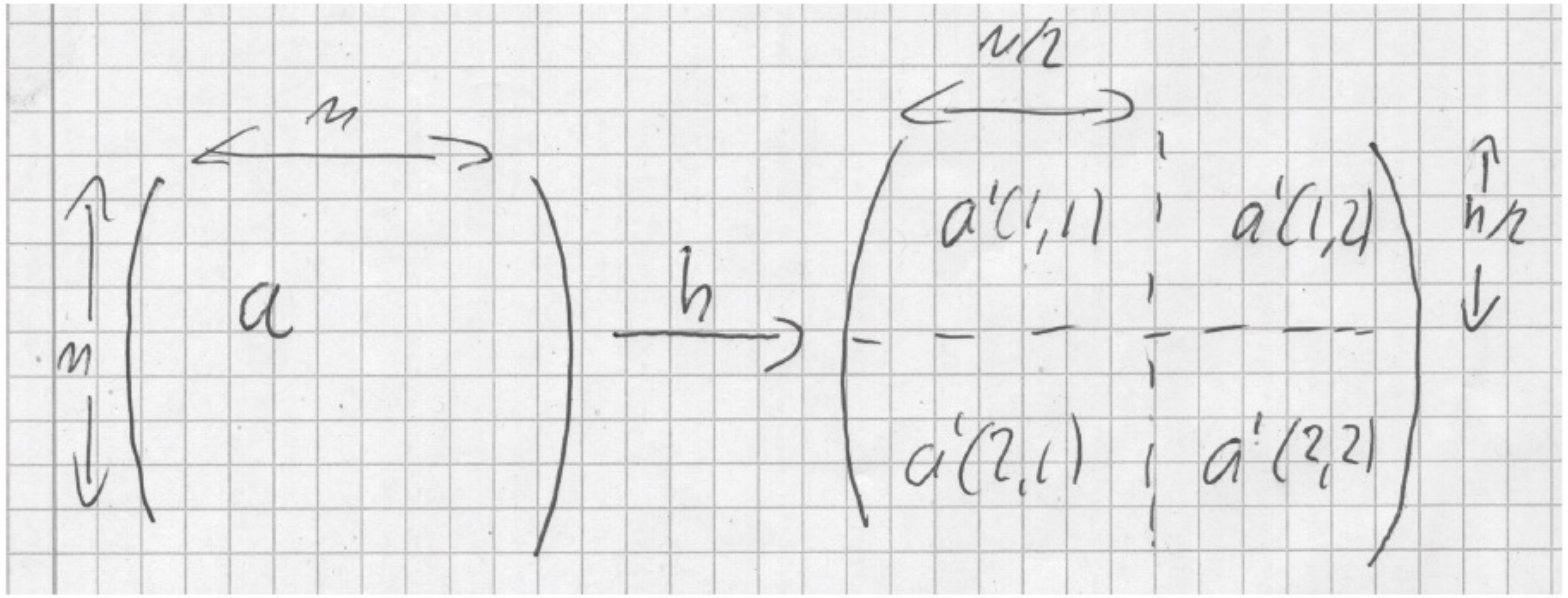

Figure 4: Interpreting $(n \times n)$-matrices as (2×2)-matrices of $(n/2 \times n/2)$-matrices

$$
\begin{aligned}
h : S_n &\rightarrow (S_{n/2})_2 \\
h(a) &= \begin{pmatrix} a'(1,1) & a'(1,2) \\ a'(2,1) & a'(2,2) \end{pmatrix} \\
a'(1,1)(i,j) &= a(i,j) \\
a'(1,2)(i,j) &= a(i,n/2+j) \\
a'(2,1)(i,j) &= a(i+n/2,j) \\
a'(2,2)(i,j) &= (a(i+n/2,j+n/2)
\end{aligned}
$$

Lemma 2. *h is bijective.*

Proof. trivial

Lemma 3. *h is ring homomorphism*

Proof. exercise

$$
\begin{aligned}
a,b \in S_n &\rightarrow \\
h(a *_n b) &= h(a) *_{n/2,2} h(b) \\
\boxed{a *_n b = h^{-1}(h(a) *_{n/2,2} h(b))}
\end{aligned}
$$

multiplication of $(2{\times}2)$-matrices with 7 multiplications

Lemma 4. *For arbitrary rings R we can compute the product of (2×2)-matrices $\in R_2$ with 7 multiplications and $O(1)$ additions and subtractions in R*

multiplication of (2×2)-matrices with 7 multiplications

Lemma 4. *For arbitrary rings R we can compute the product of (2×2)-matrices $\in R_2$ with 7 multiplications and $O(1)$ additions and subtractions in R*

$$
\begin{aligned}
M_1 &:= (A_{1,1} + A_{2,2}) \cdot (B_{1,1} + B_{2,2}) \\
M_2 &:= (A_{2,1} + A_{2,2}) \cdot B_{1,1} \\
M_3 &:= A_{1,1} \cdot (B_{1,2} - B_{2,2}) \\
M_4 &:= A_{2,2} \cdot (B_{2,1} - B_{1,1}) \\
M_5 &:= (A_{1,1} + A_{1,2}) \cdot B_{2,2} \\
M_6 &:= (A_{2,1} - A_{1,1}) \cdot (B_{1,1} + B_{1,2}) \\
M_7 &:= (A_{1,2} - A_{2,2}) \cdot (B_{2,1} + B_{2,2})
\end{aligned}
$$

$$
\begin{aligned}
C_{1,1} &= M_1 + M_4 - M_5 + M_7 \\
C_{1,2} &= M_3 + M_5 \\
C_{2,1} &= M_2 + M_4 \\
C_{2,2} &= M_1 - M_2 + M_3 + M_6
\end{aligned}
$$

multiplication of $(2{\times}2)$-matrices with 7 multiplications

Lemma 4. *For arbitrary rings R we can compute the product of (2×2)-matrices $\in R_2$ with 7 multiplications and $O(1)$ additions and subtractions in R*

Showing that $C_{i,j}$ form matrix product: exercise

$$
\begin{aligned}
M_1 &:= (A_{1,1} + A_{2,2}) \cdot (B_{1,1} + B_{2,2})\\
M_2 &:= (A_{2,1} + A_{2,2}) \cdot B_{1,1}\\
M_3 &:= A_{1,1} \cdot (B_{1,2} - B_{2,2})\\
M_4 &:= A_{2,2} \cdot (B_{2,1} - B_{1,1})\\
M_5 &:= (A_{1,1} + A_{1,2}) \cdot B_{2,2}\\
M_6 &:= (A_{2,1} - A_{1,1}) \cdot (B_{1,1} + B_{1,2})\\
M_7 &:= (A_{1,2} - A_{2,2}) \cdot (B_{2,1} + B_{2,2})
\end{aligned}
$$

$$
\begin{aligned}
C_{1,1} &= M_1 + M_4 - M_5 + M_7\\
C_{1,2} &= M_3 + M_5\\
C_{2,1} &= M_2 + M_4\\
C_{2,2} &= M_1 - M_2 + M_3 + M_6
\end{aligned}
$$

counting arithmetic operations

Lemma 4. *For arbitrary rings R we can compute the product of (2×2)-matrices $\in R_2$ with 7 multiplications and $O(1)$ additions and subtractions in R*

$$
\begin{aligned}
M_1 &:= (A_{1,1} + A_{2,2}) \cdot (B_{1,1} + B_{2,2}) \\
M_2 &:= (A_{2,1} + A_{2,2}) \cdot B_{1,1} \\
M_3 &:= A_{1,1} \cdot (B_{1,2} - B_{2,2}) \\
M_4 &:= A_{2,2} \cdot (B_{2,1} - B_{1,1}) \\
M_5 &:= (A_{1,1} + A_{1,2}) \cdot B_{2,2} \\
M_6 &:= (A_{2,1} - A_{1,1}) \cdot (B_{1,1} + B_{1,2}) \\
M_7 &:= (A_{1,2} - A_{2,2}) \cdot (B_{2,1} + B_{2,2})
\end{aligned}
$$

$$
\begin{aligned}
C_{1,1} &= M_1 + M_4 - M_5 + M_7 \\
C_{1,2} &= M_3 + M_5 \\
C_{2,1} &= M_2 + M_4 \\
C_{2,2} &= M_1 - M_2 + M_3 + M_6
\end{aligned}
$$

Showing that $C_{i,j}$ form matrix product: exercise

counting basic ring operations $*, +, -$

$$
\begin{aligned}
M(1) &= 1 \\
M(n) &= 7 \cdot M(n/2) + 18 \cdot (n/2)^2
\end{aligned}
$$

counting arithmetic operations

Lemma 4. *For arbitrary rings R we can compute the product of (2×2)-matrices $\in R_2$ with 7 multiplications and $O(1)$ additions and subtractions in R*

$$
\begin{aligned}
M_1 &:= (A_{1,1} + A_{2,2}) \cdot (B_{1,1} + B_{2,2}) \\
M_2 &:= (A_{2,1} + A_{2,2}) \cdot B_{1,1} \\
M_3 &:= A_{1,1} \cdot (B_{1,2} - B_{2,2}) \\
M_4 &:= A_{2,2} \cdot (B_{2,1} - B_{1,1}) \\
M_5 &:= (A_{1,1} + A_{1,2}) \cdot B_{2,2} \\
M_6 &:= (A_{2,1} - A_{1,1}) \cdot (B_{1,1} + B_{1,2}) \\
M_7 &:= (A_{1,2} - A_{2,2}) \cdot (B_{2,1} + B_{2,2})
\end{aligned}
$$

$$
\begin{aligned}
C_{1,1} &= M_1 + M_4 - M_5 + M_7 \\
C_{1,2} &= M_3 + M_5 \\
C_{2,1} &= M_2 + M_4 \\
C_{2,2} &= M_1 - M_2 + M_3 + M_6
\end{aligned}
$$

Showing that $C_{i,j}$ form matrix product: exercise

counting basic ring operations $*, +, -$

$$
\begin{aligned}
M(1) &= 1 \\
M(n) &= 7 \cdot M(n/2) + 18 \cdot (n/2)^2
\end{aligned}
$$

(our) master theorem does not quite apply. Showing

$$\boxed{M(n) = O(n^{\log 7}) = O(n^{2.8\ldots})}$$

exercise