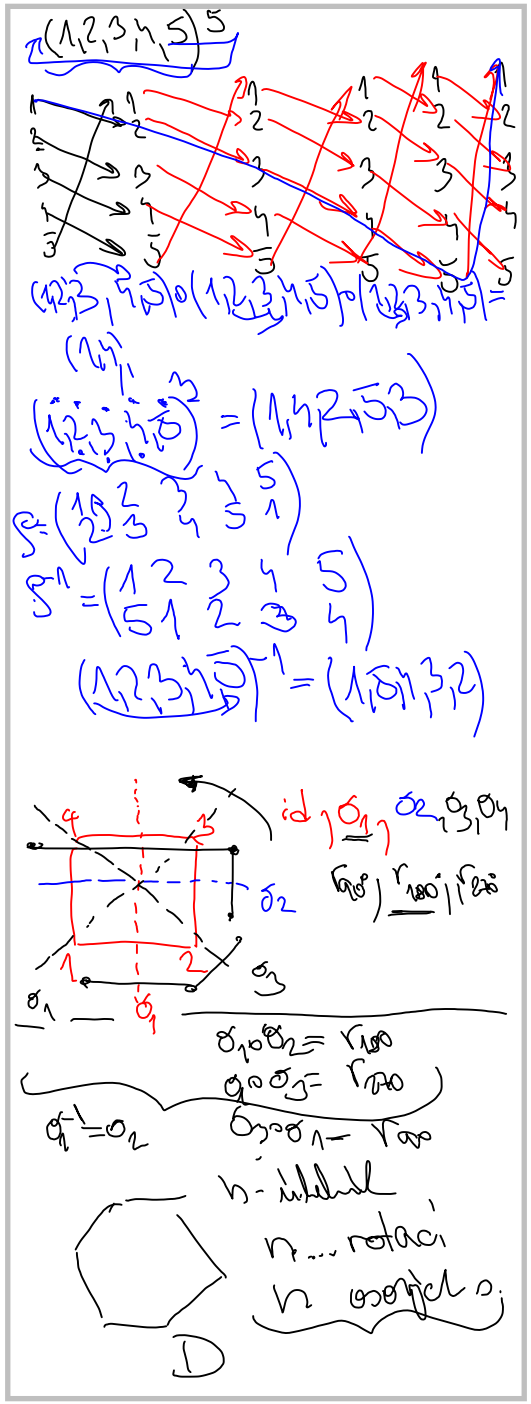
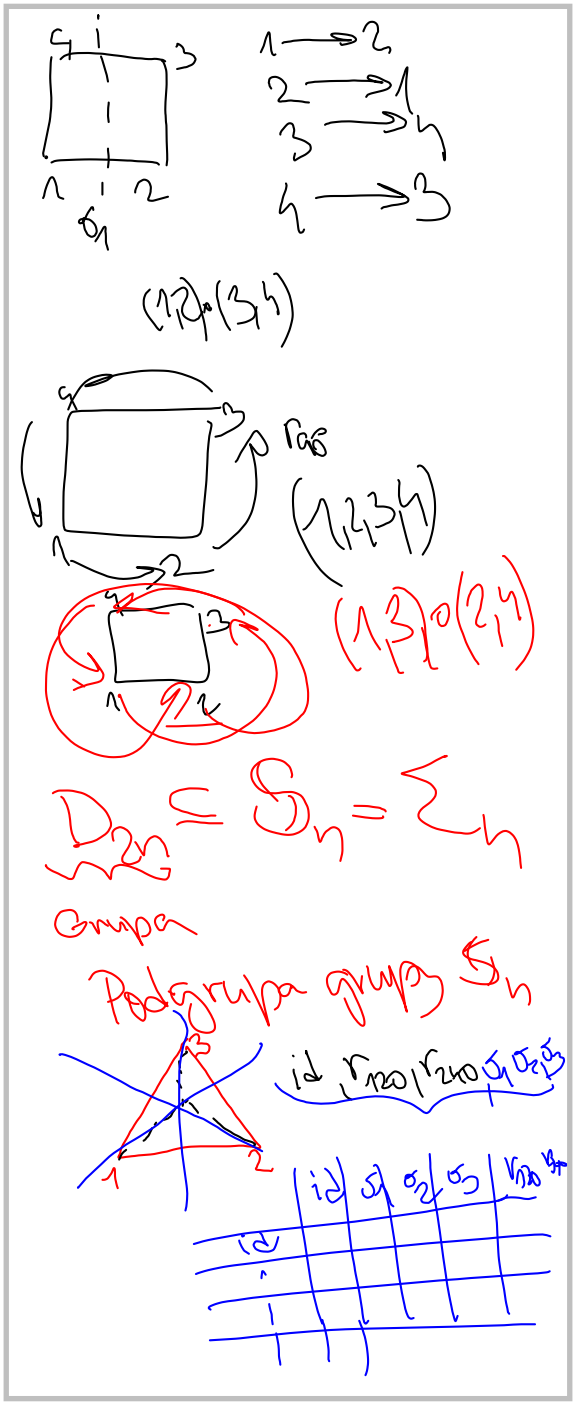
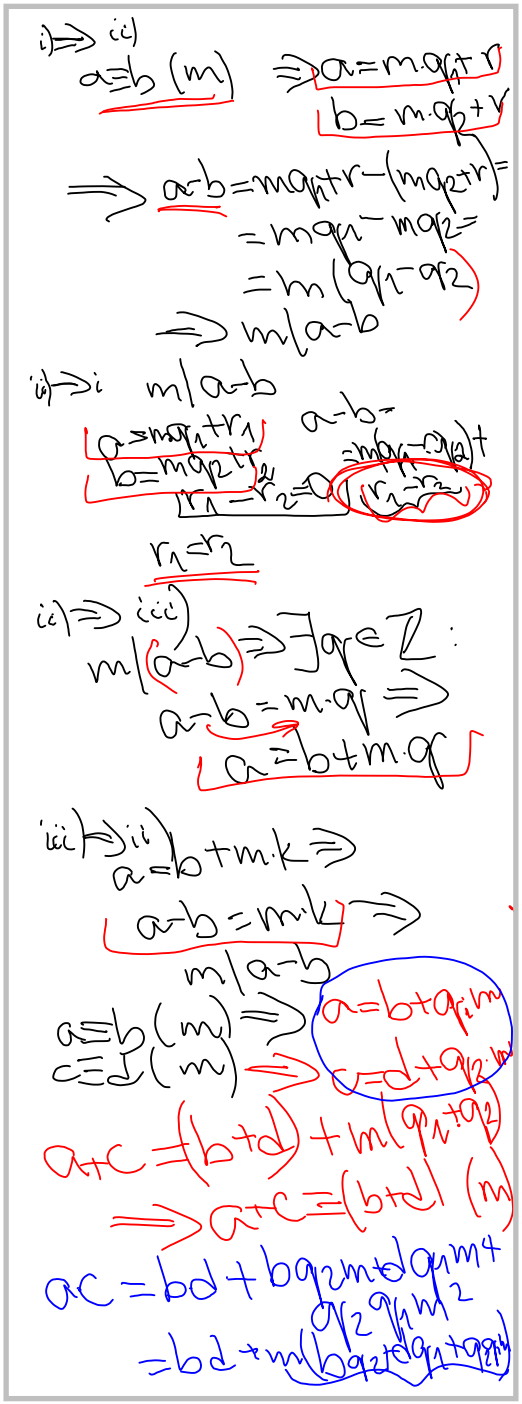

(1,2,3,4,5)
id, σ1, σ2, σ3, σ4
r0, r180, r240
σ1 ∘ σ2 = r180
σ4 ∘ σ3 = r240
σ3 ∘ σ1 = r240
σ4⁻¹ = σ2
n - počet
n ... rotací
n osových os
D


1 → 2
2 → 1
3 → 4
4 → 3
(1,2)∘(3,4)
r_{90}
(1,2,3,4)
(1,3)∘(2,4)
$D_{2n} \subseteq S_n = \Sigma_n$
Grupa
Podgrupa grupy S_n
id r_{120} r_{240} σ_1 σ_2 σ_3
id
1


i) ⇒ ii)
a ≡ b (m) ⇒ a = m·q1 + r
b = m·q2 + r
⇒ a − b = mq1 + r − (mq2 + r) =
= mq1 − mq2 =
= m(q1 − q2)
⇒ m | a − b
ii) ⇒ i
m | a − b
a = mq1 + r1
b = mq2 + r2
r1 − r2 = 0
a − b = m(q1 − q2) + (r1 − r2)
r1 = r2
ii) ⇒ iii)
m | (a − b) ⇒ ∃q ∈ ℤ :
a − b = m·q ⇒
a = b + m·q
iii) ⇒ ii)
a = b + m·k ⇒
a − b = m·k ⇒
m | a − b
a ≡ b (m) ⇒
c ≡ d (m) ⇒
a = b + q1·m
c = d + q2·m
a + c = (b + d) + m(q1 + q2)
⇒ a + c ≡ (b + d) (m)
ac = bd + bq2m + dq1m + q1q2m²
= bd + m(bq2 + dq1 + q1q2m)

$a^{p-1} \equiv 1 \ (p)$ $\quad (a,p)=1$

$a^p \equiv a \ (p)$

$x_1, \dots, x_a$ R

M = p-znaká slova

$|M| = a^p$

$\sigma(\text{pes}) = \text{esp}$

$\sigma: M \to M$

$\sigma(x_{i1} \dots x_{ip}) = (x_{i2} \dots x_{ip} x_{i1})$

$\sigma^k(s) = s$

$k = p$

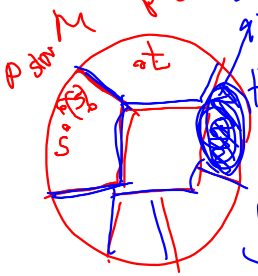
$k = 1 \dots$ pro slova $\left.\begin{matrix}(x_1 \dots x_1) \\ \vdots \\ (x_a \dots x_a)\end{matrix}\right\} N$

p slov $\quad x_1 \dots x_1, \ \dots, \ x_a \dots x_a$

$s, \sigma(s), \sigma^2(s), \dots$

$s \notin N$

$t, \sigma(t), \sigma^2(t), \dots$



$|H| = a$

$|M| = a^p$

$|M| - |H| = a^p - a$

$p \mid a^p - a$

$a^p - a \equiv 0 \ (p)$

$a^p \equiv a \ (p)$ MFV

$[a]_m \cdot [a^{-1}]_m = [1]_m$

$a \cdot a^{-1} \equiv 1 \ (m)$

$a \cdot x \equiv 1 \ (m)$

$(a,m) \mid 1 \Rightarrow (a,m) = 1$

$\varphi(m)$

$\varphi(24) = \varphi(2^3 \cdot 3) =$

$(2-1) \cdot 2^{3-1} \cdot (3-1) \cdot 3^0 =$

$4 \cdot 2 = \boxed{8}$

$|\mathbb{Z}_{24}^{\times}| = 8$

$[5]_{17}$ $\boxed{(5,17) = 1}$

$[5]_{17} \cdot [x]_{17} = [1]_{17}$

$5x \equiv 1 \ (17)$

$5x = 1 + 17y$

$5x - 17y = 1$

$(3,17) = 1$

$3x + 17y = 1$