Algebra - druhý díl

Lenka Zalabová

Ústav matematiky a biomatematiky, Přírodovědecká fakulta, Jihočeská univerzita v Českých Budějovicích

zima 2012

Obsah

Co o tom víte ze střední

Permutace n prvků ... pořadí těchto n prvků, případně jejich počet.

Example

Kolik různých pěticiferných přirozených čísel lze vytvořit pomocí číslic $1, 2, 3, 4, 5$, pokud každá číslice se použije jen jednou?

Co o tom víte ze střední

Permutace n prvků ... pořadí těchto n prvků, případně jejich počet.

Example

Kolik různých pěticiferných přirozených čísel lze vytvořit pomocí číslic $1, 2, 3, 4, 5$, pokud každá číslice se použije jen jednou?

- Počet hledaných pěticiferných čísel...permutace množiny $\{1,2,3,4,5\}$, t.j. permutace pětiprvkové množiny:

Co o tom víte ze střední

Permutace n prvků ... pořadí těchto n prvků, případně jejich počet.

Example

Kolik různých pěticiferných přirozených čísel lze vytvořit pomocí číslic $1, 2, 3, 4, 5$, pokud každá číslice se použije jen jednou?

- Počet hledaných pěticiferných čísel...permutace množiny $\{1,2,3,4,5\}$, t.j. permutace pětiprvkové množiny:

$$P(5) = 5! = 120.$$

A teď pořádně

Definition

Označme množinu $X = \{1, 2, \ldots, n\}$. *Permutace* množiny X je vzájemně jednoznačné zobrazení (bijekce) množiny X na sebe.

Neboli:
Každému prvku množiny X (vzoru) přiřadíme prvek množiny X (obraz) tak, aby každý prvek množiny X měl právě jeden obraz a právě jeden vzor.

Example

Buď $X = \{1, 2, 3, 4\}$. Rozhodněte, zda následující předpis zadává permutaci množiny X:

- Zobrazení $\sigma : X \to X$, kde

$$\sigma(1) = 3,\ \sigma(2) = 1,$$
$$\sigma(3) = 4,\ \sigma(4) = 2.$$

Example

Buď $X = \{1, 2, 3, 4\}$. Rozhodněte, zda následující předpis zadává permutaci množiny X:

- Zobrazení $\sigma : X \to X$, kde

$$\sigma(1) = 3,\ \sigma(2) = 1,$$
$$\sigma(3) = 4,\ \sigma(4) = 2.$$

...ano

Example

Buď $X = \{1, 2, 3, 4\}$. Rozhodněte, zda následující předpis zadává permutaci množiny X:

- Zobrazení $\sigma : X \to X$, kde

$$\sigma(1) = 3,\ \sigma(2) = 1,$$
$$\sigma(3) = 4,\ \sigma(4) = 2.$$

  ...ano
- Zobrazení $\pi : X \to X$, kde

$$\pi(1) = 2,\ \pi(2) = 4,$$
$$\pi(3) = 3,\ \pi(4) = 2.$$

Example

Buď $X = \{1, 2, 3, 4\}$. Rozhodněte, zda následující předpis zadává permutaci množiny X:

- Zobrazení $\sigma : X \to X$, kde

$$\sigma(1) = 3, \ \sigma(2) = 1,$$
$$\sigma(3) = 4, \ \sigma(4) = 2.$$

  ...ano

- Zobrazení $\pi : X \to X$, kde

$$\pi(1) = 2, \ \pi(2) = 4,$$
$$\pi(3) = 3, \ \pi(4) = 2.$$

  ...ne

Obvyklý zápis

Mějme $X = \{1, 2, 3, \dots, n\}$. Permutaci σ množiny X píšeme do tabulky tvaru

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Druhý řádek (obrazy) tvoří nějaké pořadí prvků množiny X, první řádek (vzory) říkají pozici prvku (obrazu) v daném pořadí.

Example

Mějme $X = \{1, 2, 3, 4\}$. Permutaci $\sigma : X \to X$ z předchozího příkladu, která je dána předpisem

$$\begin{aligned}\sigma(1) &= 3\\ \sigma(2) &= 1\\ \sigma(3) &= 4\\ \sigma(4) &= 2,\end{aligned}$$

zapíšeme ve tvaru

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

Nějaký další příklad

Mějme množinu $X = \{1, 2, 3\}$.

- Najděte všechny permutace tříprvkové množiny X.
- Určete počet permutací množiny X a zdůvodněte teoreticky váš výsledek.

Množina všech permutací

Mějme množinu $X = \{1, 2, 3, \ldots, n\}$. Pak množinu všech permutací budeme značit S_n.

Theorem

Počet prvků množiny S_n je $n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$.

Proof: ...

Skládání permutací

- Z matematické analýzy víte, co to je složené zobrazení (složená funkce) a za jakých podmínek lze zobrazení skládat.
- Mějme dva prvky $\sigma, \pi \in S_n$. Protože se jedná o bijektivní zobrazení $X \to X$, máme korektně definováno jejich složení $\sigma \circ \pi$. To je opět bijektivní zobrazení a tedy $\sigma \circ \pi \in S_n$.
- Zdůrazněme, že je nutné dávat pozor na pořadí skládání: $(\sigma \circ \pi)(x) = \sigma(\pi(x))$ pro každé $x \in X$.

Skládání permutací

Jsou-li permutace σ a π tvaru

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix},$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix},$$

pak jejich složení $\sigma \circ \pi$ je permutace tvaru

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(\pi(1)) & \sigma(\pi(2)) & \sigma(\pi(3)) & \dots & \sigma(\pi(n)) \end{pmatrix}.$$

Zdůrazněme, že $\pi \circ \sigma$ je obecně úplně jiná permutace!

Example

Na S_4 najděte permutaci $\sigma \circ \pi$, kde permutace $\sigma, \pi \in S_4$ jsou tvaru

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Example

Na S_4 najděte permutaci $\sigma \circ \pi$, kde permutace $\sigma, \pi \in S_4$ jsou tvaru

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

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

Example

Na S_4 najděte permutaci $\sigma \circ \pi$, kde permutace $\sigma, \pi \in S_4$ jsou tvaru

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Ještě jeden příklad

Mějme permutace $\sigma, \pi \in S_8$ tvaru

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 4 & 1 & 2 & 8 & 3 & 5 \end{pmatrix},$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 8 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

- Najděte permutaci $\sigma \circ \pi$,
- najděte permutaci $\pi \circ \sigma$.

Grupa permutací

Theorem

- *Množina S_n společně s operací skládání permutací tvoří konečnou grupu (pro libovolné $n \in \mathbb{N}$).*
- *Tato grupa není komutativní, pokud $n > 2$.*

Proof: ...

Grupa permutací

Theorem

- *Množina S_n společně s operací skládání permutací tvoří konečnou grupu (pro libovolné $n \in \mathbb{N}$).*
- *Tato grupa není komutativní, pokud $n > 2$.*

Proof: ...

Definition

- Grupa $(S_n, \circ)$ se nazývá *symetrická grupa stupně n*.
- Operaci $\circ$ se často říká *součin*.

1. Permutace
2. Grupa permutací
3. Více o permutacích
4. Použití permutací
   - Symetrie ohraničených rovinných útvarů
   - Substituční šifry

Nějaké další pojmy

Definition

Permutace tvaru

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

se nazývá *identita*.

Nějaké další pojmy

Definition

Permutace tvaru
$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$
se nazývá *identita*.

Definition

Permutace tvaru
$$\begin{pmatrix} 1 & 2 & 3 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & 3 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$
se nazývá *transpozice*.

Jedná se o permutaci, při které se prohodí i a j, ostatní zůstane na místě.

Nějaké další pojmy

Definition

Permutace tvaru

$$\begin{pmatrix} 1 & \dots & i_1 & \dots & i_2 & \dots & i_k & \dots & n \\ 1 & \dots & i_2 & \dots & i_3 & \dots & i_1 & \dots & n \end{pmatrix}$$

se nazývá *cyklus délky k*.

Jedná se o permutaci, při které k prvků vytvoří ‘kolečko’ tvaru

$$\begin{tikzcd} i_1 \arrow[r] & i_2 \arrow[r] & i_3 \arrow[r] & \cdots \arrow[r] & i_{k-1} \arrow[r] & i_k \arrow[lllll, bend left] \end{tikzcd},$$

ostatní zůstane na místě. Transpozice je cyklus délky 2.

Jiný zápis cyklů

Místo psaní celé permutace

$$\begin{pmatrix} 1 & \dots & i_1 & \dots & i_2 & \dots & i_k & \dots & n \\ 1 & \dots & i_2 & \dots & i_3 & \dots & i_1 & \dots & n \end{pmatrix}$$

bývá efektivnější zapsat pouze příslušné ‘kolečko’

$$(i_1, i_2, i_3, \dots, i_{k-1}, i_k).$$

Toto jednoznačně určuje, který prvek se kam zobrazí. Prvky, které se v něm nevyskytují, zůstávají na místě.

Jiný zápis permutací

Definition

Dva cykly $(i_1, i_2, \ldots, i_{k-1}, i_k)$ a $(j_1, j_2, \ldots, j_{l-1}, j_l)$ se nazývají *nezávislé*, jestliže

$$\{i_1, i_2, \ldots, i_{k-1}, i_k\} \cap \{j_1, j_2, \ldots, j_{l-1}, j_l\} = \emptyset.$$

Neboli: ‘Kolečka’ se nepotkají.

Jiný zápis permutací

Definition

Dva cykly $(i_1, i_2, \dots, i_{k-1}, i_k)$ a $(j_1, j_2, \dots, j_{l-1}, j_l)$ se nazývají *nezávislé*, jestliže

$$\{i_1, i_2, \dots, i_{k-1}, i_k\} \cap \{j_1, j_2, \dots, j_{l-1}, j_l\} = \emptyset.$$

Neboli: 'Kolečka' se nepotkají.

Example

Rozhodněte, zda cykly $(1, 2, 5)$ a $(3, 6)$ jsou nezávislé?

Jiný zápis permutací

Definition

Dva cykly $(i_1, i_2, \dots, i_{k-1}, i_k)$ a $(j_1, j_2, \dots, j_{l-1}, j_l)$ se nazývají *nezávislé*, jestliže

$$\{i_1, i_2, \dots, i_{k-1}, i_k\} \cap \{j_1, j_2, \dots, j_{l-1}, j_l\} = \emptyset.$$

Neboli: ‘Kolečka’ se nepotkají.

Example

Rozhodněte, zda cykly $(1, 2, 5)$ a $(3, 6)$ jsou nezávislé?
... ano

Zejména, jsou-li dva cykly nezávislé, jejich složení je nezávislé na pořadí!

Jiný zápis permutací

Theorem

Každou neidentickou permutaci množiny $X = \{1, 2, \ldots, n\}$ lze rozložit na složení navzájem nezávislých cyklů. Tento rozklad je dán jednoznačně až na pořadí cyklů.

Proof: ...

Example

Rozložte permutaci $\sigma \in S_{10}$ na složení nezávislých cyklů, kde

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 1 & 8 & 5 & 7 & 9 & 4 & 3 & 2 \end{pmatrix}.$$

Example

Rozložte permutaci $\sigma \in S_{10}$ na složení nezávislých cyklů, kde

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 1 & 8 & 5 & 7 & 9 & 4 & 3 & 2 \end{pmatrix}.$$

- Dostaneme

$$\sigma = (1, 6, 7, 9, 3) \circ (2, 10) \circ (4, 8).$$

Jiný zápis permutací

Theorem

Každá permutace množiny $X = \{1, 2, \ldots, n\}$ pro $n > 1$ je složení transpozic.

Proof:

- $id = (i, j) \circ (j, i)$
- $(i_1, i_2, \ldots, i_k) = (i_1, i_k) \circ (i_1, i_3) \circ (i_1, i_2)$

Jiný zápis permutací

Theorem

Každá permutace množiny $X = \{1, 2, \ldots, n\}$ pro $n > 1$ je složení transpozic.

Proof:

- $id = (i, j) \circ (j, i)$
- $(i_1, i_2, \ldots, i_k) = (i_1, i_k) \circ (i_1, i_3) \circ (i_1, i_2)$

Example

$$\begin{aligned}\sigma &= (1, 6, 7, 9, 3) \circ (2, 10) \circ (4, 8)\\ &= (1, 3) \circ (1, 9) \circ (1, 7) \circ (1, 6) \circ (2, 10) \circ (4, 8)\end{aligned}$$

Inverze v permutaci

Definition

- *Inverze* v permutaci σ je dvojice prvků taková, že $i < j$ a $\sigma(i) > \sigma(j)$.

Example

V permutaci $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 1 & 8 & 5 & 7 & 9 & 4 & 3 & 2 \end{pmatrix}$:

- dvojice $1 < 3$ tvoří inverzi,
- dvojice $1 < 2$ netvoří inverzi.

Parita permutace

Definition

- *Parita* permutace σ se definuje jako

$$sgn(\sigma) = (-1)^p,$$

kde p je počet inverzí v permutaci σ.

- Permutace σ se nazývá *sudá*, jestliže $sgn(\sigma) = 1$, permutace σ se nazývá *lichá*, jestliže $sgn(\sigma) = -1$.

Theorem

1. *Permutace, která je složením k transpozic, je sudá právě tehdy, když k je sudé.*

Theorem

1. *Permutace, která je složením k transpozic, je sudá právě tehdy, když k je sudé.*
2. *Buďte $\sigma, \pi \in S_n$ permutace. Pak platí*

$$sgn(\sigma \circ \pi) = sgn(\sigma) \cdot sgn(\pi).$$

Theorem

1. *Permutace, která je složením k transpozic, je sudá právě tehdy, když k je sudé.*
2. *Buďte $\sigma, \pi \in S_n$ permutace. Pak platí*
$$sgn(\sigma \circ \pi) = sgn(\sigma) \cdot sgn(\pi).$$
3. *Složení dvou sudých permutací je sudá permutace.*
4. *Množina všech sudých permutací A_n společně s operací $\circ$ tvoří grupu. Ta má $\frac{n!}{2}$ prvků.*

Proof: ...

Theorem

1. *Permutace, která je složením k transpozic, je sudá právě tehdy, když k je sudé.*
2. *Buďte $\sigma, \pi \in S_n$ permutace. Pak platí*

$$sgn(\sigma \circ \pi) = sgn(\sigma) \cdot sgn(\pi).$$

3. *Složení dvou sudých permutací je sudá permutace.*
4. *Množina všech sudých permutací A_n společně s operací $\circ$ tvoří grupu. Ta má $\frac{n!}{2}$ prvků.*

Proof: ...

Definition

Grupa $(A_n, \circ)$ se nazývá *alternující grupa řádu n.*

Nějaký další příklad

Mějme permutaci $\sigma \in S_{10}$ tvaru

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 1 & 10 & 7 & 2 & 8 & 3 & 9 & 4 \end{pmatrix}.$$

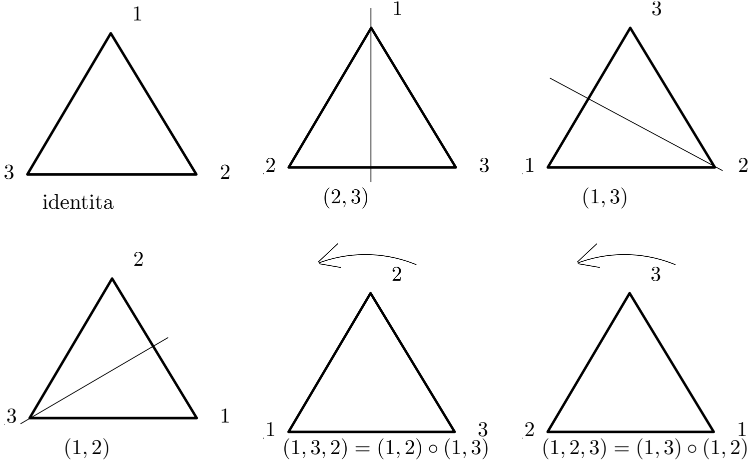
- Napište permutaci jako složení transpozic.
- Určete její paritu, t.j. rozhodněte, zda je sudá nebo lichá.
- Určete paritu permutace $\sigma^3 = \sigma \circ \sigma \circ \sigma$.

1. Permutace
2. Grupa permutací
3. Více o permutacích
4. Použití permutací
   - Symetrie ohraničených rovinných útvarů
   - Substituční šifry

Základní pojmy

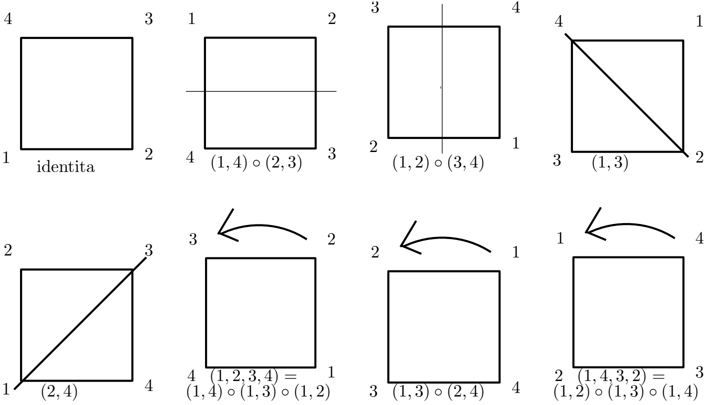
- Ohraničený rovinný útvar ... úsečka, trojúhelník, čtverec, obdélník a pod. umístěné v rovině.
- Symetrie takového útvaru ... transformace roviny, která útvar zobrazí na sebe.

Symetrie rovnostranného trojúhelníku

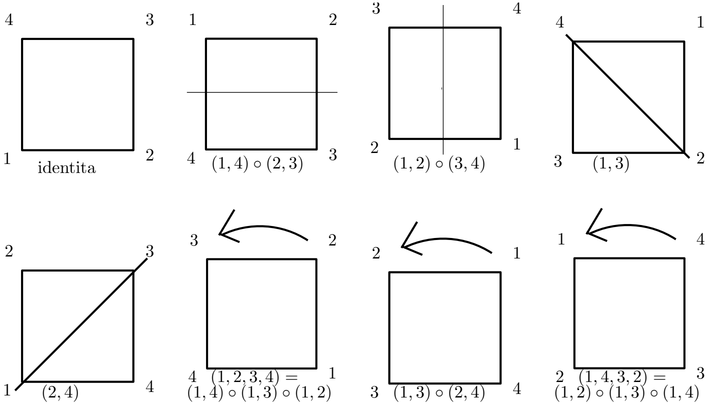


- Všechny symetrie rovnostranného trojúhelníka tvoří grupu, která je shodná se symetrickou grupou S_3. Tato grupa se nazývá *dihedrální grupa stupně* 3 a značí D_3. Tvoří ji 3 reflexe a 3 otočení.
- Symetrie každého pravidelného n-úhelníku tvoří grupu. Tato grupa se nazývá *dihedrální grupa stupně* n a značí D_n. Tvoří ji n reflexí a n otočení. Pro $n > 3$ ovšem neplatí $D_n = S_n$!
- Očíslujme vrcholy pravidelného n–úhelníku $\{1, 2, \ldots, n\}$. Pak každý prvek D_n lze realizovat vhodnou permutací z S_n, a tedy $D_n \subset S_n$ se stejnou operací skládání.
- Uvědomme si, že S_n má $n!$ prvků, zatímco D_n má $2n$ prvků.

Symetrie čtverce



Symetrie čtverce



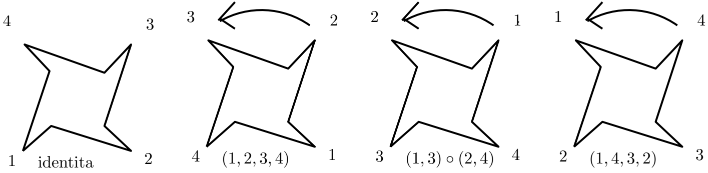
Například permutace $(1, 2) \in S_4$ není symetrií čtverce.

Symetrie méně pravidelných útvarů

Pro některé ohraničené rovinné útvary platí, že jejich grupa symetrií sestává pouze z otočení. Taková grupa se nazývá *cyklická* a v chemii se značí C_n. Je vždy komutativní.

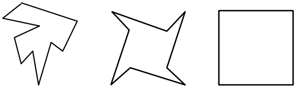
Symetrie méně pravidelných útvarů

Pro některé ohraničené rovinné útvary platí, že jejich grupa symetrií sestává pouze z otočení. Taková grupa se nazývá *cyklická* a v chemii se značí C_n. Je vždy komutativní.



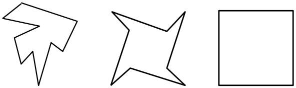
Theorem

Mějme ohraničený útvar v rovině, jehož grupa symetrií je konečná. Pak tato grupa je buď triviální (neexistuje žádná symetrie kromě identity) nebo je rovna jedné z grup C_n, D_n pro vhodné $n > 1$.

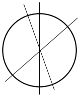


Theorem

Mějme ohraničený útvar v rovině, jehož grupa symetrií je konečná. Pak tato grupa je buď triviální (neexistuje žádná symetrie kromě identity) nebo je rovna jedné z grup C_n, D_n pro vhodné $n > 1$.



Předpoklady věty jsou důležité! Například grupa symetrií kružnice se nerovná ani jedné z výše uvedených, je nekonečná. (Například reflexe podle libovolného průměru je symetie kružnice.)



Pro přehlednost

Místo čísel budeme zapisovat písmena abecedy v obvyklém smyslu, t.j. máme $a \leftrightarrow 1$, $b \leftrightarrow 2$, ... , $z \leftrightarrow 26$.

Idea

Substituční šifra ... záměna množiny symbolů (abecedy) za jinou množinu symbolů.

Monoalfabetická šifra

- Každé písmeno zaměníme vzájemně jednoznačně za jiné písmeno.
- Každá permutace zadává jeden klíč k zašifrování, inverzní permutace pak zadává dešifrování.
- Máme 26! klíčů ... nelze řešit hrubou silou. Jde snadno řešit statisticky.

Example

$$\sigma = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ m & o & i & u & s & z & c & f & h & n & t & j & g & e & l & q & d & x & b & p & k & y & r & w & v & a \end{pmatrix}$$

- algebrajejednoducha $\leftrightarrow$

Monoalfabetická šifra

- Každé písmeno zaměníme vzájemně jednoznačně za jiné písmeno.
- Každá permutace zadává jeden klíč k zašifrování, inverzní permutace pak zadává dešifrování.
- Máme 26! klíčů ... nelze řešit hrubou silou. Jde snadno řešit statisticky.

Example

$$\sigma = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ m & o & i & u & s & z & c & f & h & n & t & j & g & e & l & q & d & x & b & p & k & y & r & w & v & a \end{pmatrix}$$

- algebrajejednoducha $\leftrightarrow$ mjcsoxmnsnsuelukifm

Polyalfabetická šifra

- Každé písmeno šifrujeme pomocí jiné permutace.

Polyalfabetická šifra

- Každé písmeno šifrujeme pomocí jiné permutace.

Example

$$\sigma_1 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ m & o & i & u & s & z & c & f & h & n & t & j & g & e & l & q & d & x & b & p & k & y & r & w & v & a \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ m & o & i & y & r & w & v & a & j & g & e & l & q & d & x & b & u & s & z & c & f & h & n & t & p & k \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ l & q & d & x & b & p & k & y & r & f & h & n & t & j & g & e & w & v & a & m & o & i & u & s & z & c \end{pmatrix}$$

- algebrajejednoducha $\leftrightarrow$

Polyalfabetická šifra

- Každé písmeno šifrujeme pomocí jiné permutace.

Example

$$\sigma_1 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ m & o & i & u & s & z & c & f & h & n & t & j & g & e & l & q & d & x & b & p & k & y & r & w & v & a \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ m & o & i & y & r & w & v & a & j & g & e & l & q & d & x & b & u & s & z & c & f & h & n & t & p & k \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ l & q & d & x & b & p & k & y & r & f & h & n & t & j & g & e & w & v & a & m & o & i & u & s & z & c \end{pmatrix}$$

- algebrajejednoducha $\leftrightarrow$ mlksovmgbnrxexxkiym

Šifrovací stroje

- Používaly se zejména v první polovině dvacátého století.
- Mechanizovaly používání polyalfabetických šifer.
- Nejznámější z nich byla Enigma.

(Obrázek: www.security-portal.cz)

Enigma

Šifrování odpovídá skládání permutací. Chod přístroje je dán:

- třemi rotory ... permutace ρ_1, ρ_2, ρ_3
- reflektorem ... složení nezávislých transpozic ρ
- propojovací deskou ... složení nezávislých transpozic τ

Pak j-té písmeno zprávy je šifrováno permutací

$$\tau \circ (\sigma^{i_1} \circ \rho_1 \circ \sigma^{-i_1}) \circ (\sigma^{i_2} \circ \rho_2 \circ \sigma^{-i_2}) \circ (\sigma^{i_3} \circ \rho_3 \circ \sigma^{-i_3}) \circ \rho$$

$$\circ(\sigma^{-i_3} \circ \rho_3^{-1} \circ \sigma^{i_3}) \circ (\sigma^{-i_2} \circ \rho_2^{-1} \circ \sigma^{i_2}) \circ (\sigma^{-i_1} \circ \rho_1^{-1} \circ \sigma^{i_1}) \circ \tau,$$

kde $\sigma = (ab \dots z)$ a i_1, i_2, i_3 závisí na j a nastavení rotorů.