Matematika IV – 1. přednáška
Základy teorie grup

Michal Bulant

Masarykova univerzita
Fakulta informatiky

22. 2. 2010

Obsah přednášky

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- *Předmětové záložky v IS MU*

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- *Předmětové záložky v IS MU*
- Jiří Rosický, *Algebra*, PřF MU, 2002.
- Peter J. Cameron. *Introduction to algebra*, Oxford University Press, 2001, 295 s. (Dostupné v knihovně PřF).
- P. Horák, Základy matematiky, `http://www.math.muni.cz/~horak/09p_zm_skripta.pdf`

Plán přednášky

Chceme abstraktně pracovat s objekty a se situacemi, ve kterých je možné rovnice

$$a \cdot x = b$$

vždy jednoznačně řešit (tak jako u lineárních rovnic jsou objekty a a b jsou dány, zatímco x hledáme).
Jde o tzv. **teorii grup**. Všimněme si, že zatím nic nevíme o povaze objektů, ani co znamená ta "tečka" v rovnici.

Plán přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi
- **komutativní grupa** (grupoid, pologrupa, monoid apod.), je taková grupa (grupoid, ...), že operace $\cdot$ je komutativní. Často se v případě komutativních grup setkáte rovněž s pojmem **abelovská grupa**.

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi
- **komutativní grupa** (grupoid, pologrupa, monoid apod.), je taková grupa (grupoid, ...), že operace $\cdot$ je komutativní. Často se v případě komutativních grup setkáte rovněž s pojmem **abelovská grupa**.

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi
- **komutativní grupa** (grupoid, pologrupa, monoid apod.), je taková grupa (grupoid, ...), že operace $\cdot$ je komutativní. Často se v případě komutativních grup setkáte rovněž s pojmem **abelovská grupa**.

Poznámka k nejednoznačnosti terminologie (multiplikativní vs. aditivní)

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií).

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií). Pro informatiky, kteří mají za sebou funkcionální programování (příp. prácí s objekty, metodami, šablonami apod.), by to možná mohl být přirozený postup, my však na to bohužel nemáme dostatek času.

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií).
Pro informatiky, kteří mají za sebou funkcionální programování (příp. prácí s objekty, metodami, šablonami apod.), by to možná mohl být přirozený postup, my však na to bohužel nemáme dostatek času.
Pro všechny *struktury* (pologrupy, grupy, okruhy, tělesa, svazy, atd.) lze definovat několik základních pojmů analogickým způsobem:

- **pod**struktury

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií).
Pro informatiky, kteří mají za sebou funkcionální programování (příp. prácí s objekty, metodami, šablonami apod.), by to možná mohl být přirozený postup, my však na to bohužel nemáme dostatek času.
Pro všechny *struktury* (pologrupy, grupy, okruhy, tělesa, svazy, atd.) lze definovat několik základních pojmů analogickým způsobem:

- **pod**struktury
- **homomorfismy** mezi strukturami stejného typu

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií).

Pro informatiky, kteří mají za sebou funkcionální programování (příp. prácí s objekty, metodami, šablonami apod.), by to možná mohl být přirozený postup, my však na to bohužel nemáme dostatek času.

Pro všechny *struktury* (pologrupy, grupy, okruhy, tělesa, svazy, atd.) lze definovat několik základních pojmů analogickým způsobem:

- **pod**struktury
- **homomorfismy** mezi strukturami stejného typu
- **součiny** struktur téhož typu

Příklad

1. Přirozená čísla (s nulou) $\mathbb{N}_0 = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkovým prvkem, neexistují v ní ale inverzní prvky.

Příklad

1. Přirozená čísla (s nulou) $\mathbb{N}_0 = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkovým prvkem, neexistují v ní ale inverzní prvky.

Příklad

1. Přirozená čísla (s nulou) $\mathbb{N}_0 = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkovým prvkem, neexistují v ní ale inverzní prvky.
2. Celá čísla $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ tvoří grupoid vůči kterékoliv z operací sčítání, odčítání, násobení. Jsou dokonce komutativní grupou vzhledem ke sčítání, jsou však jen komutativní pologrupou vůči násobení (neexistují inverze k prvkům $a \neq \pm 1$). Operace odčítání není ani asociativní (např. $(5-3)-2 = 0 \neq 5-(3-2) = 4$). Všimněte si také, že pro odečítání je nula pravý neutrální prvek, ne však levý. Dokonce v tomto případě levý neutrální prvek neexistuje.

Příklad

1. Přirozená čísla (s nulou) $\mathbb{N}_0 = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkovým prvkem, neexistují v ní ale inverzní prvky.
2. Celá čísla $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ tvoří grupoid vůči kterékoliv z operací sčítání, odčítání, násobení. Jsou dokonce komutativní grupou vzhledem ke sčítání, jsou však jen komutativní pologrupou vůči násobení (neexistují inverze k prvkům $a \neq \pm 1$). Operace odčítání není ani asociativní (např. $(5-3)-2 = 0 \neq 5-(3-2) = 4$). Všimněte si také, že pro odečítání je nula pravý neutrální prvek, ne však levý. Dokonce v tomto případě levý neutrální prvek neexistuje.

Příklad

1. Přirozená čísla (s nulou) $\mathbb{N}_0 = \{0, 1, 2, \dots\}$, spolu s kteroukoliv z operací sčítání a násobení jsou asociativní a komutativní pologrupa s jednotkovým prvkem, neexistují v ní ale inverzní prvky.
2. Celá čísla $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ tvoří grupoid vůči kterékoliv z operací sčítání, odčítání, násobení. Jsou dokonce komutativní grupou vzhledem ke sčítání, jsou však jen komutativní pologrupou vůči násobení (neexistují inverze k prvkům $a \neq \pm 1$). Operace odčítání není ani asociativní (např. $(5-3)-2 = 0 \neq 5-(3-2) = 4$). Všimněte si také, že pro odečítání je nula pravý neutrální prvek, ne však levý. Dokonce v tomto případě levý neutrální prvek neexistuje.
3. Racionální čísla $\mathbb{Q}$ jsou komutativní grupou vzhledem ke sčítání (celá čísla spolu se sčítáním jsou jejich podgrupou) a nenulová racionální čísla jsou grupou vůči násobení.

Příklad (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.

Příklad (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.

Příklad (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.

Příklad (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.

Příklad (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.
3. Množina všech lineárních zobrazení $\mathrm{Hom}(V, V)$ na vektorovém prostoru je pologrupa vzhledem ke skládání zobrazení a komutativní grupa vzhledem ke sčítání zobrazení.

Příklad (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.
3. Množina všech lineárních zobrazení $\mathrm{Hom}(V, V)$ na vektorovém prostoru je pologrupa vzhledem ke skládání zobrazení a komutativní grupa vzhledem ke sčítání zobrazení.

Příklad (pokračování)

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.
3. Množina všech lineárních zobrazení $\mathrm{Hom}(V, V)$ na vektorovém prostoru je pologrupa vzhledem ke skládání zobrazení a komutativní grupa vzhledem ke sčítání zobrazení.
4. V obou předchozích příkladech, podmnožina invertibilních objektů uvažované (multiplikativní) pologrupy tvoří grupu. V případě matic jde o tzv. grupu invertibilních (tj. regulárních) matic, ve druhém o grupu lineárních transformací vektorového prostoru (tj. invertibilních lineárních zobrazení).

Příklad

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.

Příklad

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.

Příklad

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.
3. Množina všech lineárních zobrazení $\mathrm{Hom}(V, V)$ na vektorovém prostoru je pologrupa vzhledem ke skládání zobrazení a komutativní grupa vzhledem ke sčítání zobrazení.

Příklad

1. Pro $k \in \mathbb{N}$, množina všech k-tých odmocnin z jedničky, tj. množina $\{z \in \mathbb{C};\ z^k = 1\}$ je konečná grupa vůči násobení komplexních čísel. Např. pro $k = 2$ dostaneme grupu $\{-1, 1\}$ se dvěma prvky, které jsou oba samy sobě inverzí, zatímco pro $k = 4$ dostáváme grupu $G = \{1, i, -1, -i\}$.
2. Množina Mat_n všech čtvercových matic je (nekomutativní) pologrupa vzhledem k násobení matic a komutativní grupa vzhledem ke sčítání matic.
3. Množina všech lineárních zobrazení $\mathrm{Hom}(V, V)$ na vektorovém prostoru je pologrupa vzhledem ke skládání zobrazení a komutativní grupa vzhledem ke sčítání zobrazení.
4. V obou předchozích příkladech, podmnožina invertibilních objektů uvažované pologrupy tvoří grupu. V případě matic jde o tzv. grupu invertibilních matic, ve druhém o grupu lineárních transformací vektorového prostoru (tj. invertibilních lineárních zobrazení).

Plán přednášky

Grupy permutací

Zpravidla grupy a pologrupy potkáváme jako množiny zobrazení na pevně dané množině M, které jsou uzavřeny vůči skládání zobrazení. Často si ale tuto skutečnost přímo neuvědomujeme. Na každé konečné množině M, s $m = |M| \in \mathbb{N}$ prvky máme k dispozici m^m možných definic zobrazení (každý z m prvků můžeme zobrazit na kterýkoliv v M) a všechna taková zobrazení umíme skládat.

Grupy permutací

Zpravidla grupy a pologrupy potkáváme jako množiny zobrazení na pevně dané množině M, které jsou uzavřeny vůči skládání zobrazení. Často si ale tuto skutečnost přímo neuvědomujeme. Na každé konečné množině M, s $m = |M| \in \mathbb{N}$ prvky máme k dispozici m^m možných definic zobrazení (každý z m prvků můžeme zobrazit na kterýkoliv v M) a všechna taková zobrazení umíme skládat.

Pokud chceme, aby existovala k zobrazení $\alpha : M \to M$ jeho inverze α^{-1}, musí být α bijekcí. Složením dvou bijekcí vznikne opět bijekce a proto podmnožina Σ_m všech bijekcí na množině M o m prvcích je grupa. Říkáme jí **grupa permutací** na m prvcích.

Název **grupa permutací** přitom uvádí jinou souvislost, kdy místo bijekcí na konečné množině vnímáme permutace jako přerovnání rozlišitelných prvků. Potkávali jsme se s ní např. při studiu determinantů.

Název **grupa permutací** přitom uvádí jinou souvislost, kdy místo bijekcí na konečné množině vnímáme permutace jako přerovnání rozlišitelných prvků. Potkávali jsme se s ní např. při studiu determinantů.

V grupě permutací Σ_3 na číslech $\{1, 2, 3\}$ si třeba označíme jednotlivá pořadí

$$a = (1, 2, 3),\ b = (2, 3, 1),\ c = (3, 1, 2),$$
$$d = (1, 3, 2),\ e = (3, 2, 1),\ f = (2, 1, 3).$$

Skládání našich permutací je pak zadáno tabulkou

$\cdot$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

Všimněme si podstatného rozdílu mezi permutacemi a, b a c a dalšími třemi. Ty první tři tvoří tzv. **cyklus** generovaný prvkem b nebo prvkem c:

$$b^2 = c,\ \ b^3 = a,\ \ c^2 = b,\ \ c^3 = a$$

a samy o sobě jsou tyto tři prvky komutativní podgrupou. V ní a je jednotka, a b s c jsou vzájemně inverzní. Je tedy tato podgrupa stejná jako je grupa $\mathbb{Z}_3$ zbytkových tříd celých čísel modulo 3, resp. jako grupa třetích odmocnin z jedničky z jednoho z předchozích příkladů.

Všimněme si podstatného rozdílu mezi permutacemi a, b a c a dalšími třemi. Ty první tři tvoří tzv. **cyklus** generovaný prvkem b nebo prvkem c:

$$b^2 = c,\ b^3 = a,\ c^2 = b,\ c^3 = a$$

a samy o sobě jsou tyto tři prvky komutativní podgrupou. V ní a je jednotka, a b s c jsou vzájemně inverzní. Je tedy tato podgrupa stejná jako je grupa $\mathbb{Z}_3$ zbytkových tříd celých čísel modulo 3, resp. jako grupa třetích odmocnin z jedničky z jednoho z předchozích příkladů.
Další tři prvky jsou samy sobě inverzí a každý z nich je tedy společně s jednotkou a podgrupou stejnou jako je $\mathbb{Z}_2$. Říkáme, že b a c jsou **prvky řádu** 3, zatímco prvky d, e a f jsou řádu 2.

Obdobně se chovají všechny grupy permutací Σ_m.
Každá permutace σ rozkládá množinu M na disjunktní sjednocení maximálních invariantních podmnožin M_x, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu M_x přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \dots,$ dokud není $\sigma^k(x) = x$.

Obdobně se chovají všechny grupy permutací Σ_m.
Každá permutace σ rozkládá množinu M na disjunktní sjednocení maximálních invariantních podmnožin M_x, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu M_x přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \dots,$ dokud není $\sigma^k(x) = x$.

Každou permutaci tak dostáváme jako složení jednodušších permutací, tzv. cyklů, které se chovají jako identická permutace vně M_x a tak jako σ na M_x.

Obdobně se chovají všechny grupy permutací Σ_m.
Každá permutace σ rozkládá množinu M na disjunktní sjednocení maximálních invariantních podmnožin M_x, které dostaneme tak, že postupně vybíráme dosud nezpracované prvky $x \in M$ a do třídy rozkladu M_x přidáváme všechny akce iterací $\sigma^k(x)$, $k = 1, 2, \dots,$ dokud není $\sigma^k(x) = x$.

Každou permutaci tak dostáváme jako složení jednodušších permutací, tzv. cyklů, které se chovají jako identická permutace vně M_x a tak jako σ na M_x.

Pokud přitom očíslujeme prvky v M_x jako pořadí $(1, 2, \dots, |M_x|)$ tak aby i odpovídalo $\sigma^i(x)$, pak je naše permutace prostým posunutím o jednu pozici v cyklu (tj. poslední prvek je zobrazen zpátky na první). Odtud název **cyklus**. Zjevně přitom tyto cykly komutují, takže je jedno, v jakém pořadí z nich permutaci σ složíme.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ. Dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$ se nazývají **transpozice**.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ. Dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$ se nazývají **transpozice**.

Každý cyklus zjevně můžeme poskládat z permutací sousedních prvků (necháme *probublat* první prvek nakonec) $\Rightarrow$ každou permutaci napsat jako složení transpozic sousedních prvků. Skutečnost, jestli potřebujeme sudý nebo lichý počet permutací je na našich volbách nezávislá.

Nejjednodušší cykly jsou jednoprvkové pevné body permutace σ. Dvouprvkové $(x, \sigma(x))$, kde $\sigma(\sigma(x)) = x$ se nazývají **transpozice**.

Každý cyklus zjevně můžeme poskládat z permutací sousedních prvků (necháme *probublat* první prvek nakonec) $\Rightarrow$ každou permutaci napsat jako složení transpozic sousedních prvků. Skutečnost, jestli potřebujeme sudý nebo lichý počet permutací je na našich volbách nezávislá.

Máme proto definováno dobře zobrazení $\operatorname{sgn} : \Sigma_m \to \mathbb{Z}_2 = \{\pm 1\}$, tzv. **paritu** permutace. Dokázali jsme si znovu tvrzení, která jsme již využívali při studiu determinantů:

Věta

Každá permutace konečné množiny je složením cyklů. Cyklus délky ℓ *lze vyjádřit jako složení* $\ell - 1$ *transpozic. Parita cyklu délky* ℓ *je* $(-1)^{\ell-1}$. *Parita složení permutací je součinem parit jednotlivých z nich, tzn. že zobrazení* sgn *převádí složení permutací* $\sigma \circ \tau$ *na součin* $\operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$ *v komutativní grupě* $\mathbb{Z}_2$.