14. Permutace

V příští části se budeme zabývat determinanty matic. Determinant je zobrazení, které přiřazuje každé čtvercové matici M s prvky z tělesa $\mathbf{T}$ nějaký prvek tohoto tělesa nazývaný *determinant* M. Abychom mohli definovat determinant čtvercové matice M řádu n, potřebujeme umět všemi možnými způsoby vybrat z matice n prvků tak, abychom vzali z každého sloupce a každého řádku jeden prvek.

Je-li i jedno z čísel $1, 2, \dots, n$, pak z i-tého řádku vybereme prvek, který leží v j-tém sloupci, kde j je rovněž jedno z čísel $1, 2, \dots, n$. Označme si prvek j symbolem $p(i)$. Tento symbol $p(i)$ tedy označuje nějaké z čísel $1, 2, \dots, n$. Protože z každého řádku vybíráme jeden prvek, symbol $p(i)$ je dobře definován pro každé $i = 1, \dots, n$. Náš výběr je ale takový, že vybíráme také z každého sloupce jeden prvek. Proto se každé z čísel $1, 2, \dots, n$ rovná právě jednomu $p(i)$. Symbol p tedy označuje vzájemně jednoznačné zobrazení množiny $\{1, 2, \dots, n\}$ prvních n kladných přirozených čísel do sebe. Vzájemně jednoznačným zobrazením nějaké množiny říkáme permutace.

Definice 14.39. *Permutace* na množině X je vzájemně jednoznačné zobrazení $p : X \to X$. Je-li p permutace na množině X, pak inverzní zobrazení $p^{-1} : X \to X$ je rovněž permutace na množině X, které říkáme *inverzní permutace* k permutaci p. Jsou-li p, q dvě permutace na množině X, pak složené zobrazení $q \circ p$, které přiřazuje každému prvku $i \in X$ prvek $q(p(i))$, je také permutace na množině X. Nazýváme ji *složení* permutací p a q.

Dříve, než se budeme zabývat permutacemi podrobněji, uvedeme si několik technických pojmů.

Definice 14.40. *Relace* na množině X je libovolná množina $R \subseteq X \times X$ uspořádaných dvojic prvků množiny X. Relace R je *reflexivní*, jestliže platí $(x, x) \in R$ pro každý prvek $x \in X$. Relace R je *symetrická*, jestliže z $(x, y) \in R$ plyne $(y, x) \in R$. Relace R se nazývá *tranzitivní*, jestliže pro každé tři prvky $x, y, z \in X$ z předpokladu $(x, y), (y, z) \in R$ plyne rovněž $(x, z) \in R$. Relace R se nazývá antisymetrická, jestliže pro každé dva prvky $x, y \in X$ z předpokladu $(x, y), (y, x) \in R$ plyne $x = y$.

Relace R na množině X se nazývá *ekvivalence* na X, je-li reflexivní, symetrická a tranzitivní. Relace R se nazývá *kvaziuspořádání,* je-li reflexivní a tranzitivní. Nazývá se *uspořádání,* je-li reflexivní, antisymetrická a tranzitivní.

Věta 14.72. Buď R ekvivalence na množině X. Pro každý prvek $x \in X$ definujeme množinu

$$R[x] = \{z \in X : (x, z) \in R\}.$$

Potom platí

a) Je-li pro nějaké dva prvky $x, y \in X$ $R[x] \cap R[y] \neq \emptyset$, pak $R[x] = R[y]$,

Typeset by $\mathcal{AMS}$-TeX

b) $X = \bigcup_{x \in X} R[x]$.

Důkaz. Důkaz je velmi jednoduchý. Je-li průnik $R[x] \cap R[y]$ neprázdný, vezměme libovolný prvek $z \in R[x] \cap R[y]$. Potom platí $(y, z) \in R$ a protože R je symetrická relace, dostáváme rovněž $(z, y) \in R$. Protože také $(x, z) \in R$, z tranzitivity R plyne, že také $(x, y) \in R$ a protože R je symetrická, také $(y, x) \in R$. Je-li nyní $u \in R[x]$ libovolný prvek, platí $(x, u) \in R$. Protože také $(y, x) \in R$, opět z tranzitivity R dostáváme $(y, u) \in R$, tj. $u \in R[y]$. Proto $R[x] \subseteq R[y]$. Opačná inkluze se dokáže zcela stejně. Tolik k důkazu tvrzení a).

Tvrzení b) plyne okamžitě z toho, že R je reflexivní relace. Platí proto pro každé $x \in X$, že $(x, x) \in R$, neboli $x \in R[x]$. $\square$

Definice 14.41. Rozklad množiny X na dizjunktní podmnožiny $R[x]$ podle předchozí věty nazýváme *rozklad určený ekvivalencí R*. Množiny $R[x]$ se nazývají *třídy (bloky)* ekvivalence R.

Věta 14.73. Buď $X = \bigcup_{i \in I} X_i$ rozklad množiny X na dizjunktní sjednocení podmnožin X. Definujme relaci R na množině X předpisem

$$(x, y) \in R \text{ právě když existuje } i \in I \text{ tak, že } x, y \in X_i.$$

Takto definovaná relace R je ekvivalence na množině X.

Důkaz. Důkaz reflexivity a symetrie relace R je snadný. Platí-li $(x, y) \in R$ a $(y, z) \in R$, existují prvky $i, j \in I$ takové, že $x, y \in X_i$ a $y, z \in X_j$. Množiny X_i, $i \in I$, jsou ale vzájemně dizjunktní a $y \in X_i \cap X_j$, proto $i = j$ a $x, z \in X_i = X_j$, tj. $(x, z) \in R$. Relace R je tedy také tranzitivní. $\square$

Snadno si ověříte, že vyjdeme-li od ekvivalence R na množině X, sestrojíme rozklad množiny X určený R podle Věty 14.72 a z tohoto rozkladu ekvivalenci podle Věty 14.73, dostaneme původní ekvivalenci R (rozmyslete si, co je třeba dokázat). Stejně tak vyjdeme-li z nějakého rozkladu množiny X na dizjunktní sjednocení podmnožin, přiřadíme mu ekvivalenci R podle Věty 14.73 a této ekvivalenci R přiřadíme rozklad X podle Věty 14.72, dostaneme původní rozklad množiny X. Ekvivalence na množině X a jí určený rozklad množiny X jsou jenom dva různé pohledy na stejný matematický objekt.

Nyní se vrátíme zpět k permutacím na množině X. Napřed si zavedeme označení. Je-li p permutace na množině X a n kladné přirozené číslo, pak symbolem p^n označujeme permutaci

$$\underbrace{p \circ p \circ \cdots \circ p}_{n},$$

tj. n-násobné složení permutace p. Podobně symbolem p^{-n} označujeme permutaci

$$\underbrace{p^{-1} \circ p^{-1} \circ \cdots \circ p^{-1}}_{n},$$

tj. n-násobné složení inverzní permutace k permutaci p. Dále ještě definujeme p^0 jako identickou permutaci na množině X, tj. platí $p^0(x) = x$ pro každý prvek $x \in X$. Tím jsme dali význam označení p^k pro každé celé číslo k a platí $p^k \circ p^l = p^{k+l}$ pro libovolná dvě celá čísla k, l, a platí $p^k \circ p^l = p^{k+l}$ pro libovolná dvě celá čísla k, l.

Věta 14.74. Buď p permutace na množině X. Definujme relaci R_p na množině X předpisem

$$(x, y) \in R_p \quad \text{právě když existuje celé číslo } n \text{ takové, že } x = p^n(y).$$

Potom R_p je ekvivalence na množině X.

Důkaz. Protože platí $p^0(x) = x$ pro každé $x \in X$, je relace R_p reflexivní. Je-li $(x, y) \in R_p$, platí $x = p^n(y)$ pro nějaké celé číslo n. Potom také platí $y = p^{-n}(x)$, proto $(y, x) \in R_p$, relace R_p je tedy také symetrická. A nakonec, platí-li $(x, y) \in R_p$ a $(y, z) \in R_p$, existují celá čísla n, m taková, že $x = p^n(y)$ a $y = p^m(z)$. Potom $x = p^{n+m}(z)$, což znamená, že R_p je také tranzitivní relace. $\square$

Bloky ekvivalence R nazýváme *cykly (orbity)* permutace p. Jestliže pro nějaká dvě přirozená čísla $i > j$ platí $p^i(x) = p^j(x)$, pak také platí $p^{i-j}(x) = x$ a $i - j > 0$. Označme k nejmenší kladné přirozené číslo takové, že $p^k(x) = x$. Potom pro libovolná dvě přirozená čísla $0 \leq j < i < k$ platí, že prvky $p^j(x)$ a $p^i(x)$ jsou různé. Orbita permutace p obsahující prvek x tedy sestává z prvků $\{x = p^0(x), p^1(x), \ldots, p^{k-1}(x)\}$.

Dále budeme předpokládat, že permutace p je definována na **konečné** množině X. Označme $X_1, X_2, \ldots, X_r$ všechny orbity permutace p. V každé orbitě X_i zvolíme nějaký prvek a_{i1}. Je-li k_i počet prvků orbity X_i, označme $a_{i2} = p(a_{i1})$, $a_{i3} = p(a_{i2})$, $\ldots$, $a_{ik_i} = p(a_{i(k_i-1)}) = p^{k-1}(a_{i1})$ všechny prvky orbity X_i. Platí tedy také $a_{i1} = p(a_{ik_i})$. Permutaci p můžeme tedy zapsat v tvaru

$$(a_{11}, a_{12}, \ldots, a_{1k_1})(a_{21}, a_{22}, \ldots, a_{2k_2}) \ldots (a_{r1}, a_{r2}, \ldots, a_{rk_r}).$$

Tomuto zápisu říkáme *cyklický zápis* permutace p. Cyklický zápis permutace není určený jednoznačně, závisí na pořadí orbit a volbě prvků a_{i1}. Přesto můžeme z cyklického zápisu permutace zjistit hodnotu v každém prvku množiny X. Není-li prvek $x \in X$ posledním prvkem v závorce, ve které se nachází, je hodnota permutace p v bodě x rovna prvku, který následuje prvek x v cyklickém zápisu p. Pokud je prvek x poslední v příslušné závorce, zobrazí se permutací p do prvního prvku v téže závorce. Obvykle z cyklického zápisu vynecháváme všechny cykly (orbity) délky 1. Takovému zápisu se také říká *redukovaný cyklický zápis* permutace p. *Transpozice* na množině X je permutace, která má jeden cyklus délky 2 a ostatní cykly délky 1. Je-li redukovaný cyklický zápis transpozice t roven (a, b), znamená to, že $t(a) = b$, $t(b) = a$ a $t(c) = c$ pro všechny ostatní prvky $c \neq a, b$ množiny X.

Věta 14.75. Každou permutaci na konečné množině X lze složit z transpozic.

Důkaz. Buď $(a_{11}, a_{12}, \ldots, a_{1k_1})(a_{21}, a_{22}, \ldots, a_{2k_2}) \ldots (a_{r1}, a_{r2}, \ldots, a_{rk_r})$ redukovaný cyklický zápis permutace p na množině X. Snadno se přesvědčíme, že platí

$$(a_{i1}, a_{i2}, \ldots, a_{ik_i}) = (a_{i(k_i-1)}, a_{ik_i}) \circ (a_{i(k_i-2)}, a_{i(k_i-1)}) \circ \cdots \circ (a_{i1}, a_{i2})$$

pro každé $i = 1, \dots, r$. Podobně vyjádříme všechny ostatní cykly z redukovaného cyklického zápisu permutace p jako složení transpozic a dostaneme tak vyjádření celé permutace p jako složení transpozic. □

Přímým výpočtem si sami můžete dokázat následující lemma.

Lemma 14.76. Jsou-li r, s dvě přirozená čísla, pak platí

$$(a,b) \circ (a, c_1, \dots, c_r, b, d_1, \dots, d_s) = (a, c_1, \dots, c_r)(b, d_1, \dots, d_s),$$

$$(a,b) \circ (a, c_1, \dots, c_r)(b, d_1, \dots, d_s) = (a, c_1, \dots, c_r, b, d_1, \dots, d_s),$$

$$(a, c_1, \dots, c_r, b, d_1, \dots, d_s) \circ (a,b) = (a, d_1, \dots, d_s)(b, c_1, \dots, c_r),$$

a

$$(a, c_1, \dots, c_r)(b, d_1, \dots, d_s) \circ (a,b) = (a, d_1, \dots, d_s, b, c_1, \dots, c_r).$$

□

Definice 14.42. Je-li p permutace na konečné množině X, pak *znaménkem* permutace p rozumíme číslo

$$\operatorname{sgn}(p) = (-1)^{n-r},$$

kde n je počet prvků množiny X a r je počet orbit permutace p. Permutace se znaménkem 1 nazýváme *sudé,* permutace se znaménkem -1 nazýváme *liché.*

Snadno si ověříte, že $\operatorname{sgn}(t) = -1$ pro každou transpozici t a je-li p identická permutace, pak $\operatorname{sgn}(p) = 1$.

Věta 14.77. a) Buď t transpozice a p permutace na množině X. Potom platí

$$\operatorname{sgn}(t \circ p) = -\operatorname{sgn}(p), \quad \operatorname{sgn}(p \circ t) = -\operatorname{sgn}(p),$$

b) permutace p je sudá právě když ji lze složit ze sudého počtu transpozic a je lichá právě když ji lze složit z lichého počtu transpozic,

c) složení dvou sudých nebo dvou lichých permutací je sudá permutace, složení liché permutace se sudou (v libovolném pořadí) je lichá permutace.

Důkaz. a) Toto tvrzení plyne z Lemma 14.76, které ukazuje, že složením nějaké permutace p s transpozicí t se změní počet cyklů o jeden. Počet cyklů v permutaci $t \circ p$ je o jedna větší než počet cyklů v permutaci p, jestliže transpozice t prohazuje dva prvky z téhož cyklu permutace p. Podobně je počet cyklů v permutaci $t \circ p$ o jedna menší než počet cyklů v permutaci p, pokud t přehazuje dva prvky z různých cyklů permutace p. Stejně tak, skládáme-li p a t v opačném pořadí.

b) Je-li $p = t_k \circ t_{k-1} \circ \cdots \circ t_1$ vyjádření nějaké permutace p jako složení transpozic, pak podle předchozí věty platí $\operatorname{sgn}(p) = (-1)^k$. Odtud plyne, že permutace p je sudá, pokud ji lze složit ze sudého počtu transpozic, a je lichá, pokud ji lze složit z lichého počtu transpozic. Protože je každá permutace buď sudá nebo lichá, platí v obou případech ekvivalence.

c) Toto tvrzení plyne bezprostředně z předchozí části. Jsou-li totiž $p = t_k \circ \cdots \circ t_1$ a $q = u_l \circ \cdots \circ u_1$ vyjádření permutací p, q pomocí transpozic, pak

$$q \circ p = u_l \circ \cdots \circ u_1 \circ t_k \circ \cdots \circ t_1.$$

Permutace $q \circ p$ je tedy složením $l + k$ transpozic. Toto číslo je sudé právě když jsou obě čísla l, k sudá nebo když jsou obě lichá. Je liché, pokud je jedno z čísel l, k sudé a druhé liché. $\square$

Závěrem dokážeme ještě jedno tvrzení, které budeme potřebovat v příští kapitole.

Věta 14.78. Buď t libovolná transpozice na množině $\{1, 2, \ldots, n\}$. Definujeme relaci R_t na množině všech permutací na $\{1, 2, \ldots, n\}$ předpisem

$$pR_tq \text{ právě když buď } p = q \text{ nebo } p = qt.$$

Relace R_t je ekvivalence na množině všech permutací na množině $\{1, 2, \ldots, n\}$. Dvě permutace p, q leží v téže třídě rozkladu podle R_t právě když buď $p = q$ nebo $p = qt$. Každá třída rozkladu podle R_t tak obsahuje právě dvě permutace.

Důkaz. Snadno si sami ověříte, že R_t je ekvivalence. Zbytek plyne z konstrukce rozkladu podle R_t. $\square$