Matematické hlavolamy a základy teorie grup

3. kapitola. Polohy prvků

In: Jiří Tůma (author): Matematické hlavolamy a základy teorie grup. (Czech). Praha: Mladá fronta, 1988. pp. 44–116.

Persistent URL: http://dml.cz/dmlcz/404170

Třetí kapitola

POLOHY PRVKŮ

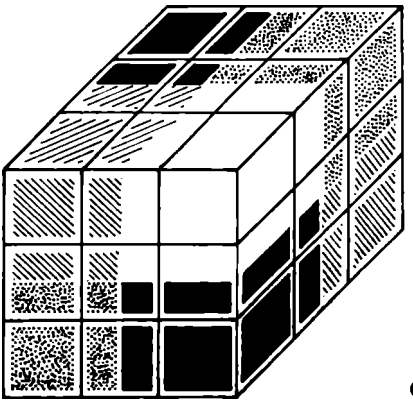
3.1. Poloha a orientace. Umíme už kreslit grafy pozic u patnáctky, víme, co jsou cykly a jak jejich počet ovlivňuje řešitelnost nebo neřešitelnost pozice. Nyní se vrátíme zpět k Rubikově krychli a dalším hlavolamům. Ty jsou podstatně složitější, než je celkem jednoduchá patnáctka.

Obtížnost Rubikovy krychle má dvě hlavní příčiny. Na krychli jsou složitější tahy. U patnáctky mění každý tah polohu pouhých dvou prvků hry — posunovaného čísla a prázdného místa. Všechno ostatní zůstává na původním místě. Zato u krychle mění každý tah polohu hned osmi prvků — čtyř rohových a čtyř hranových kostiček. Jsou to dvě pětiny všech pohyblivých prvků. Uděláme-li v základní pozici patnáctky čtyři tahy, pozice se příliš nerozhází, a snadno ji zase vrátíme zpět. Po čtyřech tazích na Rubikově krychli obvykle nezůstane nic na původních místech, a vrátit čtyři tahy zpět je dost obtížné. Vrátit sedm nebo osm tahů pak skoro nemožné.

Rubikovu krychli navíc komplikuje skutečnost, že stejná malá kostička může být na jednom místě různě pootočená, s různou orientací. Na obrázku 1.14. jsou špatně orientované kostičky na správných místech. Nic takového se u patnáctky stát nemůže. Hrám, u kterých záleží nejenom na poloze prvků (kostiček, kuliček, čísel, apod.), ale také na jejich orientaci, říkáme *hry s orientací*. U jiných her se o orientaci starat nemusíme, jsou to *hry*

bez orientace. Mezi ně patří patnáctka, babylónská věž, uši nebo domino.

Význam orientace můžeme ovlivnit obarvením. Na Rubikově krychli s normálním obarvením záleží na orientaci rohových a hranových kostiček, a nezáleží vůbec na orientacích stěnových. Při netradičním obarvení podle obrázku 3.1 naopak nezáleží na orientacích rohových kostiček — všechny tři plošky mají vždy stejnou barvu — zato orientace hranových a stěnových je důležitá.



Obr. 3.1

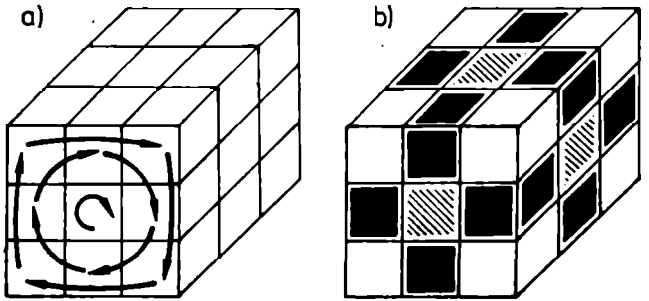
Cvičení 3.1. a) Navrhněte obarvení Rubikovy krychle, při kterém záleží na orientacích rohových a stěnových kostiček, a nezáleží na orientacích hranových.

b) Navrhněte označení, při kterém záleží na orientacích všech kostiček — rohových, hranových i stěnových.

Rubikova krychle je hra s orientací. Při jejím skládání musíme nejenom dostat všechny prvky na správná místa, ale navíc také se správnou orientací. V této

a následující kapitole se budeme zabývat pouze polohami prvků, naučíme se, jak dostat všechny na správná místa, případně poznat, kdy to nejde. Orientace si zatím všímat nebudeme, podrobně ji prozkoumáme až v páté kapitole. Znamená to, že ve třetí a čtvrté kapitole se naučíme řešit hry bez orientace, a pouze částečně hry s orientací.

3.2. Orbity. Pouze na první pohled vypadá Rubikova krychle jakoby složená ze samých stejných malých kostiček. Ve skutečnosti jsou mezi nimi rozdíly. Na obrázku 3.2.a vidíme, jak se kostičky přesunou při otočení jednou vrstvou.



Obr. 3.2

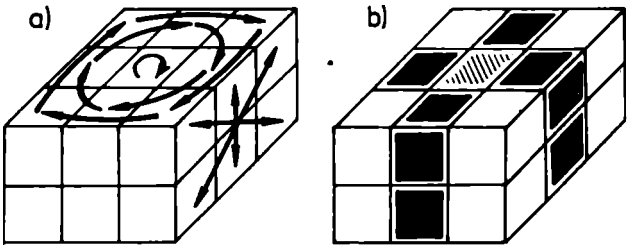
Každý prvek, který byl původně v rohu, je po nějakém tahu opět v rohu. Každý postup proto přemístí *rohové kostičky* na místa jiných rohových kostiček. Mezi těmito kostičkami už žádné rozdíly nejsou, každá z nich může být na místě kterékoliv jiné. Je jich celkem osm a na krychli obíhají z rohu do rohu, budeme říkat, že tvoří *rohovou orbitu*.

Další orbitu tvoří *hranové kostičky*. Ty jsou obarvené černě na obrázku 3.2.b. Každá z nich přejde po libovolném tahu, a tím i postupu, na místo nějaké jiné hranové kostičky. Mezi nimi opět žádné rozdíly nejsou, každá z nich může být na místě libovolné jiné hranové kostičky. Těchto dvanáct prvků obíhá na krychli z hrany na hranu a tvoří tak *hranovou orbitu*.

Stěnové kostičky jsou jiné. Můžeme je pouze pootáčet, nikoliv prohazovat. Každá zůstává při každém tahu na místě, nepřesunuje se na místo jiné (otáčíme pouze krajními vrstvami!). Stěnové kostičky mají vůči sobě stále stejnou polohu a tvoří tak *souřadný systém* na Rubikově krychli, určují jediné správné místo a orientaci pro všechny pohyblivé prvky. Na obrázku 3.2.b jsou rozlišeny všechny tři možné typy kostiček. Rohová orbita je bílá, hranová černá, a pevné stěnové kostičky jsou označené šrafami.

Podobně můžeme rozdělit pohyblivé prvky do orbit i na dalších hračkách.

Domino. Na obrázku 3.3.a jsou vyznačené přesuny prvků při obou možných typech tahů. Také tady pohyblivé prvky z rohů přecházejí při každém tahu do rohů a hranové prvky na místa jiných hranových.



Obr. 3.3

Domino má dvě osmiprvkové orbity — rohovou a hranovou. Dva stěnové prvky můžeme vůči sobě pootáčet, ne však prohazovat.

Uši. Tady je to jednoduché, každou kuličku můžeme přesunout na místo libovolné jiné, uši mají pouze jednu orbitu, kterou tvoří všech dvaadvacet kuliček.

Podobně každý ze šestnácti pohyblivých prvků (patnácti čísel a prázdného místa) u patnáctky můžeme přesunout na místo libovolného jiného, patnáctka má jen jednu orbitu. Jenom jednu orbitu má také babylónská věž.

Obecně můžeme říct, že dva pohyblivé prvky na nějaké hře leží ve stejné orbitě, jestliže existuje postup, který jeden z těchto prvků převede na místo druhého. Udělejte si následující cvičení.

Cvičení 3.2. Rozdělte do orbit pohyblivé prvky na čtyřstěnu a dvanáctistěnu.

Cvičení 3.3. Jaké orbity jsou na krychli $2 \times 2 \times 2$ a $4 \times 4 \times 4$?

Cvičení 3.4. Proč netvoří všechny rohové a hranové kostičky na Rubikově krychli společně jednu orbitu?

Hry, které mají jenom jednu orbitu, jsou *souvislé*, mají-li aspoň dvě orbity, jsou *nesouvislé*. Uši, krychle $2 \times 2 \times 2$, babylónská věž, patnáctka a koule jsou souvislé, Rubikova krychle, čtyřstěn, dvanáctistěn, kosá krychle, domino a krychle $4 \times 4 \times 4$ jsou nesouvislé.

3.3. Základní pozice. V tomto odstavci vhodně označíme pohyblivé prvky na Rubikově krychli, abychom mohli polohu prvků v pozicích zapisovat stejně, jako jsme to dělali u patnáctky. Pokud to bude nutné, upra-

víme označení prvků na některých dalších hlavolamech tak, aby v základní pozici bylo pro každý pohyblivý prvek jediné správné místo.

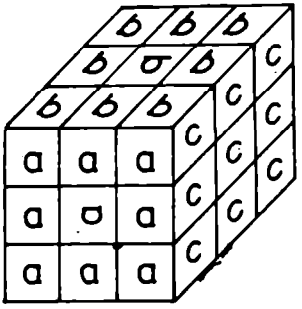
Na obrázku 1.1. jsme si jednotlivé stěny Rubikovy krychle označili písmeny *a*, *b*, *c*, *d*, *e* a *f*. Každou kostičku můžeme nyní popsat seznamem písmen, jimiž je označena. Tak třeba stěnová kostička ve stěně *a* je označena také *a*. Ostatní stěnové kostičky jsou *b*, *c*, *d*, *e* a *f*. Hranový prvek mezi stěnami *a* a *b* má dvě plošky označené stejnými písmeny, budeme jej proto zapisovat jako *ab*. Tady je seznam všech prvků hranové orbity: *ab*, *ac*, *ae*, *af*, *bc*, *bd*, *bf*, *cd*, *ce*, *de*, *df*, *ef*. Ze šesti barev *a*, *b*, *c*, *d*, *e*, *f* můžeme udělat celkem 15 různých dvojic. Pouze *ad*, *be* a *cf* neodpovídají žádným hranovým kostičkám, protože žádný prvek nemůže ležet současně ve dvou protilehlých stěnách.

Rohová kostička ležící ve stěnách *a*, *b*, *c* má tři plošky označené těmito písmeny, budeme ji proto zapisovat jako *abc*.

Cvičení 3.5. Napište seznam všech prvků patřících do rohové orbity Proč symbol *ade* neoznačuje žádnou rohovou kostičku ?

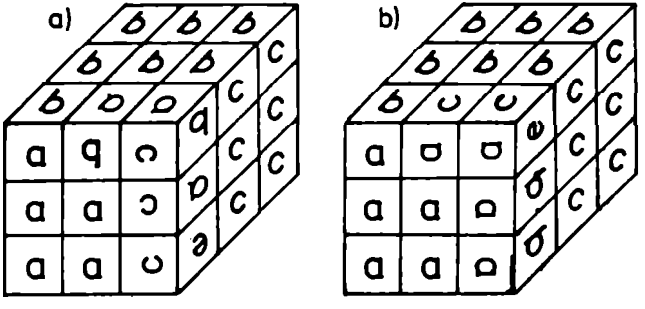
Poznamenejme ještě, že díky označení malých kostiček písmeny máme nyní možnost rozlišit různé orientace stěnových kostiček, což při normálním obarvení nemůžeme. Jedna z mnoha nejrůznějších odpovědí na cvičení 3.1.b je proto už na obrázku 1.1.b. My si různých orientací stěnových prvků nebudeme všímat a pozice jako na obrázku 3.4. budeme považovat také za základní. Liší se od pozice 1.1.b pouze v orientacích některých stěnových prvků.

Souřadný systém stěnových kostiček určuje pro každý pohyblivý prvek jediné správné místo v základní pozici.



Obr. 3.4

Tak třeba hranový prvek *ab* musí ležet ve stěnách *a* a *b*, mezi stěnovými prvky *a*, *b*. Na obrázcích 1.1.b a 3.4. je *ab* na správném místě. Také na obrázku 3.5.a je na správném místě, ale se špatnou orientací.



Obr. 3.5

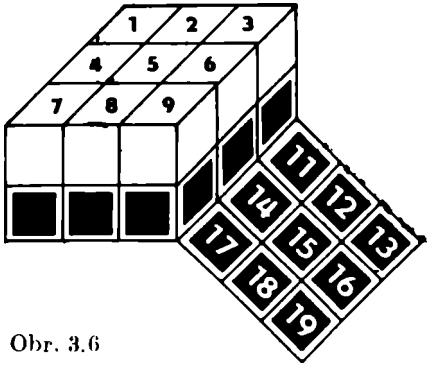
Na obrázku 3.5.b na správném místě není. Je na místě, kde má být v základní pozici prvek *ac*, zatímco kostička *ac* je na místě *ab*.

Podobně je tomu i s rohovými prvky. Kostička *abc* musí být v základní pozici ve stěnách *a*, *b* a *c*, musí proto

ležet v jediném společném rohu stěn, v jejichž středech jsou stěnové kostičky *a*, *b*, *c*. Na obrázcích 1.1.b a 3.4. je prvek *abc* na správném místě. Také na obrázku 3.5.a je na správném místě, ale se špatnou orientací. Na obrázku 3.5.b na správném místě není. Je tam, kde má být v základní pozici prvek *ace* — vpravo dole. Prvek *ace* je naopak na místě *abc*.

Také na dalších hračkách můžeme jednoznačně určit správné místo v základní pozici pro každý pohyblivý prvek.

Domino. Změníme označení jednotlivých prvků a místo dominových symbolů budeme používat čísla. V horní bílé stěně čísla 1, 2, 3, ..., 9 a v dolní černé stěně 11, 12, ..., 19. Základní pozice takto očíslovaného domina je na obrázku 3.6. Proti kostičce 1 je v dolní stěně 13, proti 2 pak 12, atd.

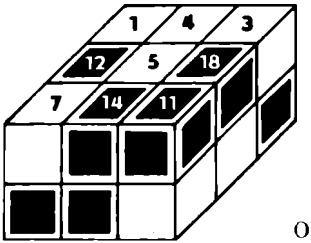


Obr. 3.6

Rohovou orbitu tvoří kostičky 1, 3, 7, 9, 11, 13, 17 a 19, hranovou 2, 4, 6, 8, 12, 14, 16 a 18. Dvě stěnové kostičky jsou označené 5 a 15. Oproti původnímu označení máme

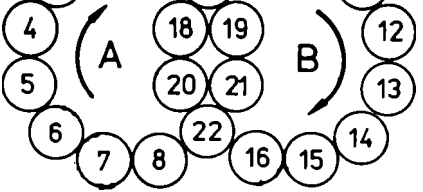
opět možnost rozlišit různá pootočení dolní černé kostičky 15 vůči horní bílé 5. Tak jako na Rubikově krychli si toho nebudeme všímat.

Každý prvek má nyní jediné správné místo. Vlevo nahoře nad 5 musí být 1, přímo nad 5 pak 2 atd. V pozici na obrázku 3.7. je kostička 4 na místě kostičky 2, kostička 12 na místě 4, 18 na místě 6 atd. Kostičky 1 a 3 jsou na správném místě.

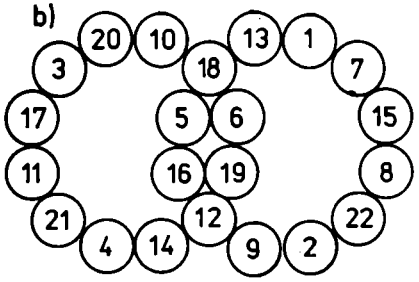


Obr. 3.7

Uši. Na uších označíme kuličky čísly 1, 2, 3, ..., 22 a za základní budeme považovat pozici na obrázku 3.8.a. Tím je opět jednoznačně určené správné místo pro každou kuličku. Na obrázku 3.8.b je rozházená



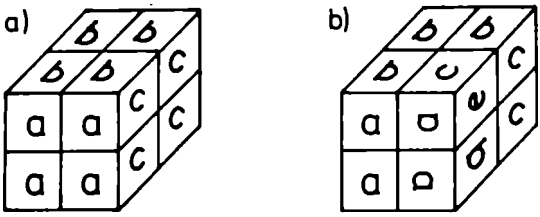
Obr. 3.8



Obr. 3.8

pozice, kulička 1 je na místě, kde má být 10, kulička 2 je na místě 15, atd.

Krychle $2 \times 2 \times 2$. Tato hračka nemá žádné pevné vnější části, při určování správného místa pro malé kostičky musíme proto postupovat trochu rafinovaněji. Správná pozice je většinou určená stejně jako na Rubikově krychli — jednobarevnými stěnami. My opět použijeme písmena *a*, *b*, *c*, *d*, e a *f*. Základní pozice je na obrázku 3.9.a.



Obr. 3.9

Dvojice protilehlých stěn jsou opět *a*, *d*, další *b*, e a poslední *c*, *f*. Každá malá kostička má potom tři písmena a jejich seznam bude označení této kostičky. Tady

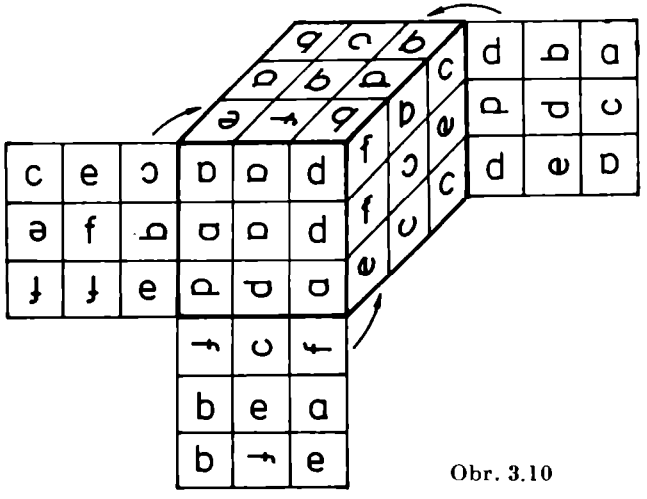
jsou všechny prvky na krychli $2 \times 2 \times 2$: *abc*, *abf*, *ace*, *aef*, *bcd*, *bdf*, *cde*, *def*.

Libovolně rozházenou krychli $2 \times 2 \times 2$ můžeme vždy uchopit tak, aby prvek *abf* byl v čelní stěně vlevo nahoře, ploškou *b* v horní stěně, stejně jako na obrázku 3.9. Vzhledem k tomuto prvku mají všechny ostatní jednoznačně určené správné místo v základní pozici 3.9.a. Prvek *abc* musí být vpravo od *abf*, pod *abc* musí být *ace*, atd. V pozici 3.9.b je prvek *ace* na místě, kde má být *abc*, zatímco prvek *abc* je na místě *ace*, vpravo dole v čelní stěně.

Prvek *abf* takto určuje souřadný systém na krychli $2 \times 2 \times 2$. Otočení nějakou vrstvou vpravo udělá v pozici stejnou změnu jako otočení rovnoběžnou vrstvou také vpravo. Z každé dvojice rovnoběžných vrstev můžeme vybrat jednu vrstvu a každé otočení považovat za otočení jednou z těchto vybraných vrstev. Vybereme-li *c*, *d*, *e*, pak všechny možné posloupnosti tahů C, D, E, C^{-1}, D^{-1}, E^{-1} odpovídají všem možným postupům na krychli $2 \times 2 \times 2$. Tím jsme získali „pevné místo", vůči kterému posuzujeme polohu všech ostatních pohyblivých prvků.

3.4. Tabulka a graf pozice. Pokud si nevšímáme orientací prvků, jsme s Rubikovou krychlí ve stejné situaci jako s patnáctkou na počátku druhé kapitoly. Umíme pro každou kostičku určit její správné místo v základní pozici a umíme také v rozházené pozici poznat, na místě které kostičky se ta která nachází. Ve druhé kapitole jsme různé pozice u patnáctky zapisovali pomocí tabulek a grafů. Stejným způsobem teď budeme zaznamenávat polohy pohyblivých prvků i na dalších hračkách.

Jak sestavíme tabulku pozice na obrázku 3.10.?



Obr. 3.10

Zcela stejně jako u patnáctky. Pro každý pohyblivý prvek zapíšeme místo, kde se nachází. Začneme třeba hranovými. Kostička *ab* je na místě *af*, kostička *ac* je na místě *ce* atd. Tabulka poloh hranových prvků vypadá takto:

$$\begin{pmatrix} ab, ac, ae, af, bc, bd, bf, cd, ce, de, df, ef \\ af, ce, bf, ab, bd, bc, ef, ae, df, cd, ac, de \end{pmatrix}$$

Připomeňme si ještě jednou význam řádek v tabulce: prvek *xy* je na místě prvku *uv*, právě když pod symbolem *xy* v první řádce je symbol *uv* v řádce druhé. Tak kostička *bc* je na místě *bd*, kostička *de* je na místě *cd* atd.

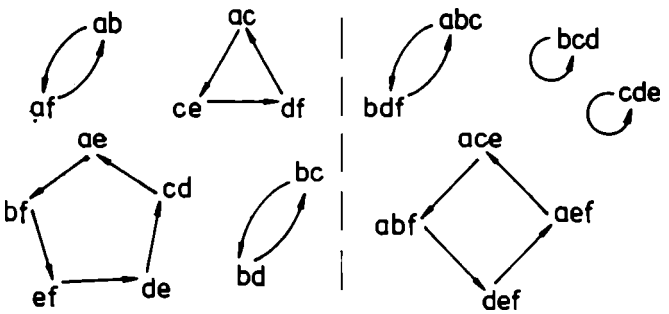
Rohová část tabulky pozice 3.10. vypadá následovně:

$$\begin{pmatrix} abc, abf, ace, aef, bdf, bcd, cde, def \\ bdf, def, abf, ace, abc, bcd, cde, aef \end{pmatrix}.$$

Kostička *abc* je na místě *bdf*, kostička *aef* je na místě *ace* atd.

Obě uvedené tabulky — hranová a rohová — tvoří společně celou tabulku pozice 3.10. Sestrojili jsme ji stejně jako tabulky pozic u patnáctky, přesto je mezi nimi podstatný rozdíl. Zatímco pozice u patnáctky zrekonstruujeme zpět z jejich tabulek, pozici 3.10. z její tabulky rekonstruovat nemůžeme. Důvod je zřejmý — *orientace*. Tabulka neobsahuje žádnou informaci o orientacích jednotlivých prvků. Podle tabulky můžeme dát každý prvek zpět na stejné místo, nevíme ale, jak ho orientovat.

Vlastnosti pozic budeme zkoumat opět především pomocí grafů. Na obrázku 3.11. je graf pozice 3.10.



Obr. 3.11

Graf jsme sestrojili z tabulky pozice stejně jako u patnáctky. Pro každý pohyblivý prvek jsme zvolili jeden bod a každému sloupci v tabulce odpovídá jedna šipka. Z bodu *ab* vede šipka do bodu *af*, protože pod *ab* je v tabulce *af*. Ze stejného důvodu vede šipka z *abf* do bodu *def*. Z každého bodu vede právě jedna šipka, která určuje, kde se daný prvek nachází, a do každého

bodu vede také jedna šipka, která určuje, jaký prvek je na daném místě.

Cvičení 3.6. Může vést v grafu nějaké pozice šipka z *ab* do bodu *abf*? Nebo z bodu *bcd* do bodu *ae*?

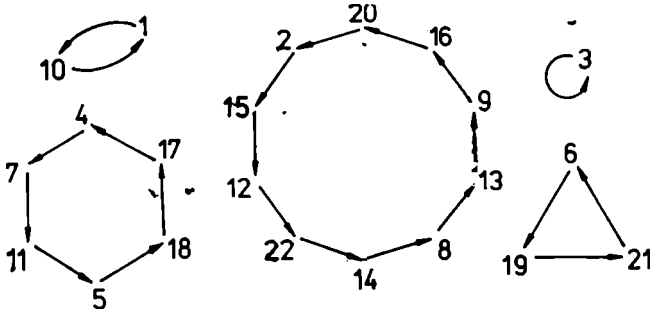
Odpověď na cvičení je jednoznačná — NE. Žádný hranový prvek nemůže být na místě rohového a naopak. Z hranových bodů vedou šipky jen do hranových a z rohových jen do rohových. Každý graf se proto rozpadá na hranovou a rohovou část, obě části jsme oddělili svislou čárkovanou čarou na obrázku 3.11.

Stejně jako tabulka, ani graf pozice neobsahuje žádnou informaci o orientacích prvků. A tak, zatímco z tabulky sestrojíme graf a z grafu zpětně tabulku, ani tabulka, ani graf nestačí k úplné rekonstrukci pozice. Jiná je situace u her bez orientace. Tady tabulka i graf obsahují úplnou informaci o dané pozici.

Uši. Vezměme si pozici na obrázku 3.8.b. Srovnáním se základní pozicí 3.8.a snadno určíme, kde se každá kulička nachází. Tabulka pozice 3.8.b vypadá následovně:

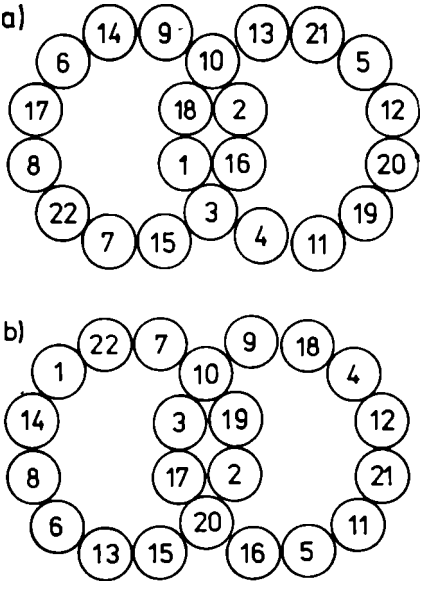
$$\begin{pmatrix} 1, & 2, 3, 4, & 5, & 6, & 7, & 8, & 9, 10, 11, 12, 13, 14, \\ 10, 15, 3, 7, 18, 19, 11, 13, 16, & & 1, & 5, 22, & 9, & 8, & \\ & & & & & & 15, 16, 17, 18, 19, 20, 21, 22 \\ & & & & & & 12, 20, 4, 17, 21, 2, 6, 14 \end{pmatrix}.$$

Graf pozice je na obrázku 3.12. Z tohoto grafu můžeme zpět zrekonstruovat tabulku a z tabulky pozici 3.8.b. Kuličku 1 dáme na místo, kde je v základní pozici kulička 10, kuličku 2 dáme na místo 15 atd.



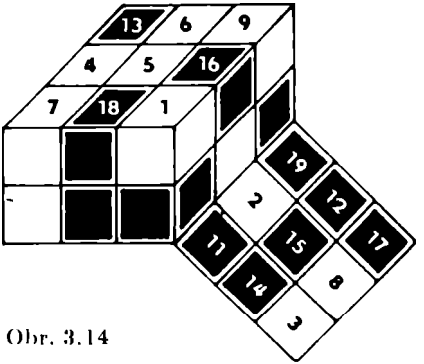
Obr. 3.12

Cvičení 3.7. Napište tabulky a nakreslete grafy pozic na uších, které jsou na obrázku 3.13.



Obr. 3.13

Cvičení 3.8. Napište tabulku a nakreslete graf pozice na dominu na obrázku 3.14.



Obr. 3.14

3.5. Permutace. V předchozích odstavcích jsme stále připomínali podobnost Rubikovy krychle s Loydovou patnáctkou a s dalšími hlavolamy. Ukázali jsme, jak polohu pohyblivých prvků u patnáctky, uší, Rubikovy krychle a dalších her zapisovat pomocí tabulek a grafů. V tomto odstavci shrneme dosavadní poznatky a uvedeme matematický pojem, který zachycuje dosud zjištěné podobnosti mezi jednotlivými hračkami. Pojem *permutace* je klíčový pojem celé teorie hlavolamů uvedené v této knížce a bude v dalším textu stále používán.

Na každém hlavolamu je skupina pohyblivých prvků — osm rohových a dvanáct hranových kostiček na Rubikově krychli, patnáct čtverečků s čísly a prázdné místo u patnáctky, dvaadvacet kuliček u uší, třicet šest kuliček a dvě prázdná místa na babylónské věži apod. Skupinu (nebo, chcete-li, množinu) všech pohyblivých prvků budeme vždy označovat I. Tyto *pohyblivé prvky* mohou měnit polohu vůči pevným částem hlavolamu

a také vzájemně mezi sebou. Pro každý pohyblivý prvek existuje přesně jedno správné místo v základní pozici. V jiných pozicích jsou prvky na nesprávných místech. Polohu všech pohyblivých prvků v nějaké pozici p můžeme snadno popsat. Je-li prvek i na místě, kde má být v základní pozici prvek j, řekneme, že prvek i je v pozici p na místě j. Tím jsme každému prvku i přiřadili nějaký prvek j, prvek, na jehož místě se i nachází. Toto přiřazení má dvě důležité vlastnosti:

a) Každému prvku i je přiřazen právě jeden prvek j, protože každý prvek je na jednom místě,

b) každý prvek j je přiřazen přesně jednomu prvku i, protože na každém místě je přesně jeden prvek.

Přiřazení, které má tyto dvě vlastnosti, se nazývá *vzájemně jednoznačné* přiřazení mezi prvky množiny I, a místo slova přiřazení je v matematice více vžitý název *zobrazení*.

Permutace na množině I je vzájemně jednoznačné zobrazení $p : I \to I$, které každému prvku $i \in I$ přiřazuje jednoznačně určený prvek $ip \in I$.

Poloha pohyblivýoh prvků v nějaké pozici na nějakém hlavolamu je tedy matematicky popsána permutací na množině I všech pohyblivých prvků tohoto hlavolamu. Proto je permutace nejdůležitější pojem celé knížky.

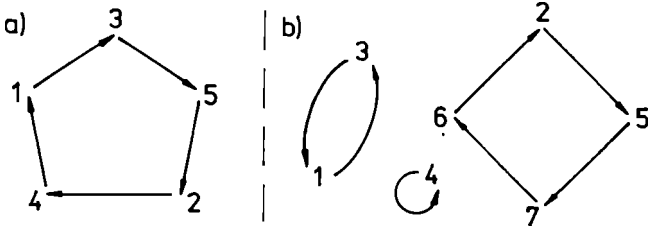
Tabulka permutace. Permutace můžeme zapisovat pomocí tabulek, stejně jako jsme zapisovali polohy pohyblivých prvků na hlavolamech. Vždy můžeme prvky množiny I očíslovat přirozenými čísly 1, 2, 3, ..., ..., k. (U Rubikovy krychle to neděláme proto, aby lépe vyniklo, co je správné místo pro každou kostičku.) Tato čísla napíšeme do prvního řádku tabulky a pod každé z nich pak napíšeme jemu přiřazené číslo do druhého řádku. Tak třeba

$$p = \begin{pmatrix} 1, & 2, & 3, & 4, & 5 \\ 3, & 4, & 5, & 1, & 2 \end{pmatrix}$$

je tabulka permutace na množině $I = \{1, 2, 3, 4, 5\}$.

Graf permutace. Pro každý prvek I nakreslíme v rovině jeden bod a z každého bodu i uděláme šipku do bodu ip. Graf permutace p je na obrázku 3.15.a. Na obrázku 3.15.b je graf permutace

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



Obr. 3.15

Protože permutace je vzájemně jednoznačné zobrazení, z každého bodu vychází právě jedna šipka a do každého bodu vede také právě jedna šipka.

Cykly v permutaci. Z grafu permutace ihned zjistíme, kolik má cyklů a jaké jsou jejich délky. Tak například permutace r, jejíž graf je na obrázku 3.15.b, má tři cykly, jeden má délku 1, druhý 2 a třetí 4. Permutace p má jediný cyklus délky 5.

Cvičení 3.9. Nakreslete grafy následujících permutací, určete, kolik mají cyklů, a jejich délky

$$p = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 2, 3, 1, 5, 6, 4 \end{pmatrix} \quad q = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 1, 3, 2, 4, 6, 7, 8, 5 \end{pmatrix}$$

$$r = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 \\ 2, 5, 7, 3, 12, 6, 1, 10, 8, 9, 4, 11 \end{pmatrix}.$$

Cvičení 3.10. Napište tabulky a nakreslete grafy všech šesti možných permutací na množině $I = \{1, 2, 3\}$.

Cvičení 3.11. Kolik různých permutací existuje na množině, která má 4 prvky? Kolik na množině, která má k prvků?

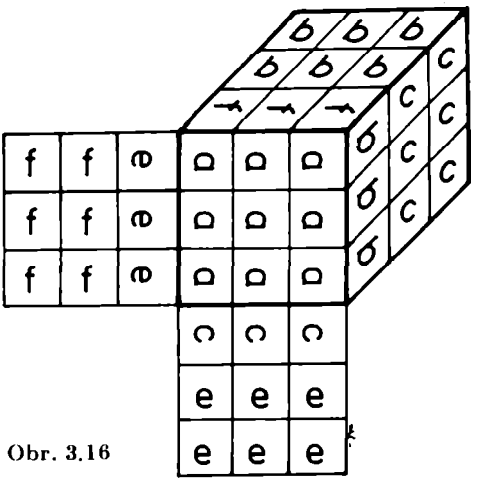
Identická permutace na množině I je permutace n, pro kterou platí $in = i$ pro všechny prvky i množiny I. V základní pozici **n** na každé hračce jsou všechny prvky na správných místech. Poloha prvků v základní pozici je proto vždy popsána identickou permutací n na množině I všech pohyblivých prvků.

3.6. Jaké permutace dělají tahy a postupy. Vzájemnou polohu pohyblivých prvků můžeme měnit pomocí tahů a z nich složených postupů. Vztah mezi postupy a pozicemi jsme si stručně vysvětlili už v první kapitole. Každý postup **P** převede hračku ze základní pozice **n** do nějaké jiné pozice **p**. Zapisujeme to **PU** = **p** — postup **P** udělá pozici **p**. Polohu prvků v pozici **p** zapisujeme permutací p na množině I všech pohyblivých prvků. Zatímco v pozici **p** je důležitá jak poloha, tak orientace všech prvků, permutace p zachycuje pouze jejich polohu. Postup **P** polohu prvků změní, říkáme, že udělá permutaci p. Protože jsme tak zapomněli na orientace, budeme to zapisovat $PV = p$. U her bez orientace není mezi pozicí **p** = **PU** a permutací p = **PV** žádný podstatný rozdíl, pozici **p** můžeme s permutací p ztotožnit. Je-li

hra s orientací, permutace p nepopisuje pozici $\mathbf{p}$ úplně, chybí informace o orientacích. V tomto případě nemůžeme pozici $\mathbf{p}$ s permutací p ztotožnit, $\mathbf{PU} \neq \mathbf{PV}$. Budeme říkat, že p je *polohová permutace* pozice $\mathbf{p}$.

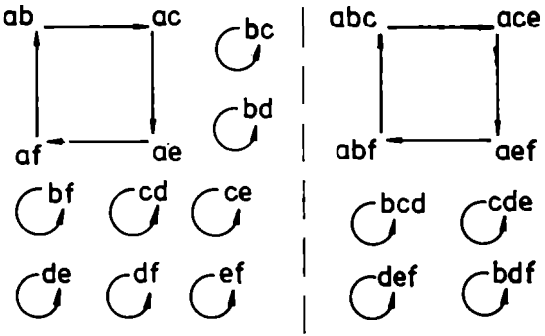
Každý postup $\mathbf{P}$ tedy udělá na množině I všech pohyblivých prvků nějakou permutaci $p = \mathbf{PV}$, polohovou permutaci pozice $\mathbf{p} = \mathbf{PU}$. Teoreticky můžeme napsat tabulku a nakreslit graf této permutace. Hlavolamy jsou ale zajímavé především proto, že vztah mezi postupy a pozicemi je složitý. Pochopit, jak nějaký postup přehazuje a pootáčí jednotlivé prvky, není vůbec snadné. Pouze u těch nejjednodušších postupů je to zcela jasné.

Nejjednodušší postupy, které základní pozici nějak změní, jsou tahy. Jakou permutaci udělá tah A — otočení vrstvou a o 90° vpravo — na Rubikově krychli? Ze základní pozice $\mathbf{n}$ dostaneme pozici na obrázku 3.16.



Obr. 3.16

Kostička *ab* přejde na místo *ac*, *ac* na místo *ae*, *ae* na místo *af* a *af* na místo *ab*. Ostatní hranové prvky se nepohybují, zůstanou na původních místech. Podobně se posunou rohové kostičky: *abc* přejde na místo *ace*, *ace* na místo *aef*, *aef* na místo *abf* a *abf* na místo *abc*. Zbývající rohové prvky opět zůstávají na původních místech. Tahem A uděláme permutaci $a = AV$, jejíž graf je na obrázku 3.17.



Obr. 3.17

Graf permutace a má dva cykly délky 4, jeden na rohových a druhý na hranových kostičkách, ostatní cykly mají délku 1. Všechny ostatní tahy na Rubikově krychli udělají permutace, které mají také jeden cyklus délky 4 na rohových prvcích, druhý cyklus délky 4 na hranových kostičkách a ostatní cykly délky 1.

Cvičení 3.12. Nakreslete grafy permutací, které udělají tahy A^{-1}, B, D na Rubikově krychli.

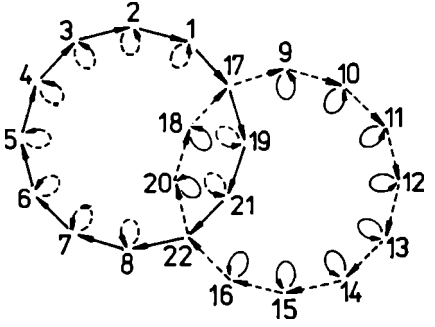
A jaké permutace dělají tahy na jiných hlavolamech?

Uši. Základní pozice je na obrázku 3.8.a. Tahem

A přejde kulička 1 na místo 17, kulička 2 na místo 1, atd. Permutace — pozice $AU = a$ má tabulku

$$\begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, \\ 17, 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad 15, 16, 17, 18, 19, 20, 21, 22 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad 15, 16, 19, 18, 21, 20, 22, \ 8 \end{pmatrix}$$

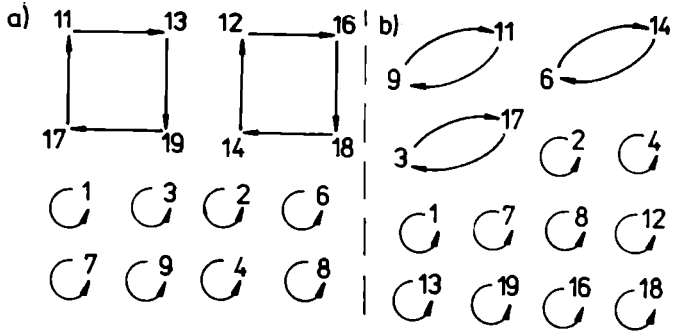
a její graf je na obrázku 3.18. plnými čarami. Čárkovaně je tam graf permutace $b = BU$. Obě permutace mají jeden cyklus délky 12 a ostatní cykly délky 1.



Obr. 3.18

Domino. Tah A otáčí spodní stěnou o 90° vpravo, kostička 11 přejde na místo 13, 13 na místo 19, 12 na místo 16 atd. Graf permutace $a = AU$ je na obrázku 3.19.a. Permutace má dva cykly délky 4, jeden na rohových a druhý na hranových kostičkách, zbývající cykly mají délku 1.

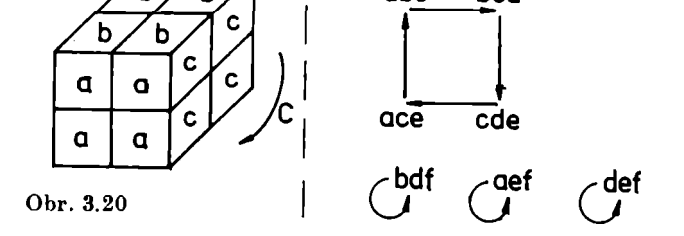
Na obrázku 3.19.b je graf permutace $c = CU$, kterou udělá otočení pravou boční vrstvou. Tato permutace má tři cykly délky 2, jeden na hranových a dva na rohových



Obr. 3.19

prvcích. Ostatní cykly mají opět délku 1. Všechny další tahy B, D, E udělají permutace, které mají rovněž dva cykly délky 2 na rohových kostičkách, jeden cyklus délky 2 na hranových a všechny ostatní cykly délky 1.

Krychle $2 \times 2 \times 2$. Připomeňme si, že polohu prvků posuzujeme vzhledem ke kostičce *abf*, kterou považujeme za pevnou. Množinu I všech pohyblivých prvků tvoří sedm zbývajících kostiček. Na obrázku 3.20.a je naznačený tah C a na obrázku 3.20.b je graf permutace $c = CV$, kterou tah C udělá. Má jeden cyklus délky 4 a tři cykly délky 1.



Obr. 3.20

Všechny ostatní tahy udělají také jeden čtyřcyklus a tři cykly délky 1.

Cvičení 3.13. Napište tabulku a nakreslete graf permutace $e = EV$, kterou udělá tah E na krychli $2 \times 2 \times 2$.

3.7. Co udělá složení dvou postupů a inverzní postup?

Nějaký postup P udělá na Rubikově krychli permutaci $p = PV$, třeba tu, jejíž graf je na obrázku 3.11. a tabulka podrobně vysvětlena v odstavci 3.4. Jiný postup Q udělá permutaci $q = QV$. Permutace q je polohová permutace pozice, kterou dostaneme postupem Q z pozice základní. Jakou permutaci uděláme složeným postupem PQ, jak vypadá permutace $(PQ)\,V$?

Děláme-li postup PQ ze základní pozice, začínáme postupem P. Po jeho skončení dostáváme jako částečný mezivýsledek pozici $p = PU$. Z této pozice pokračujeme postupem Q a chceme určit, na jakých místech budou pohyblivé prvky po skončení celého postupu PQ. Na jakém místě bude třeba rohová kostička *bdf*? Po postupu P — v pozici p — bude na místě *abc*, platí $(bdf)\,p = abc$. Chceme vědět, kam se *bdf* přemístí, pokračujeme-li dále postupem Q. Představme si, že máme kromě krychle v pozici p (obrázek 3.10) ještě jednu krychli v pozici základní, a postup Q děláme na obou krychlích současně. Prvek *bdf* je na první krychli na místě *abc* a posunuje se po stejné dráze jako prvek *abc* na druhé krychli — na obou děláme stejné tahy. Po skončení postupu budou oba prvky na stejném místě. Toto místo známe na druhé krychli — prvek *abc* bude na místě $(abc)\,q$. Prvek *bdf* bude proto na první krychli po skončení celého postupu PQ na stejném místě $(abc)\,q$. A protože $abc = (bdf)\,p$, můžeme toto místo zapsat také jako $((bdf)\,p)\,q$. Stejně určíme polohu všech ostatních prvků

po postupu PQ: hranová kostička af bude na místě $((af)\,p)\,q$, rohová abc bude na místě $((abc)\,p)\,q$, atd.

Obecně můžeme polohu pohyblivých prvků na nějakém hlavolamu po postupu PQ ze základní pozice určit následovně. Postupem P jsme udělali permutaci $p = PV$. Prvek i je v pozici $p = PU$ na místě $j = ip$. Pokračujeme-li nyní postupem Q, přejde prvek i na stejné místo, na jaké dostaneme prvek j postupem Q ze základní pozice, tj. na místo jq. Postupem PQ proto přemístíme prvek i ze základní pozice na místo $jq = (ip)\,q$.

Slovní popis permutace, kterou udělá postup PQ, doplníme ještě tabulkou a grafem. Jak najdeme tabulku a graf permutace $(PQ)\,V$, známe-li tabulky a grafy permutací $p = PV$ a $q = QV$, které udělají postupy P a Q? Vrátíme se opět ke konkrétnímu příkladu na Rubikově krychli z počátku odstavce. Tabulka permutace $p = PV$ je v odstavci 3.4., rohová část je

$$\begin{pmatrix} abc, & abf, & ace, & aef, & bdf, & bcd, & cde, & def \\ bdf, & def, & abf, & ace, & abc, & bcd, & cde, & aef \end{pmatrix}.$$

Postupem Q uděláme na rohových prvcích třeba tuto permutaci

$$\begin{pmatrix} abc, & abf, & ace, & aef, & bdf, & bcd, & cde, & def \\ ace, & bdf, & abc, & aef, & bcd, & abf, & def, & cde \end{pmatrix}.$$

Jak dostaneme tabulku permutace, kterou uděláme na rohových kostičkách postupem PQ? Kostička abc bude po postupu P na místě bdf. Postupem Q ji dále posuneme na stejné místo, na jaké přejde prvek bdf, uděláme-li Q ze základní pozice. Toto místo najdeme ve druhé řádce tabulky permutace q pod bdf, je to bcd. Kostička abc přejde postupem PQ na místo bcd. Podobně zjistíme polohu jakékoliv jiné kostičky. Můžeme si to zjednodu-

šit tak, že napíšeme obě tabulky permutací p a q pod sebe, přičemž druhý řádek tabulky p považujeme za první řádek tabulky q:

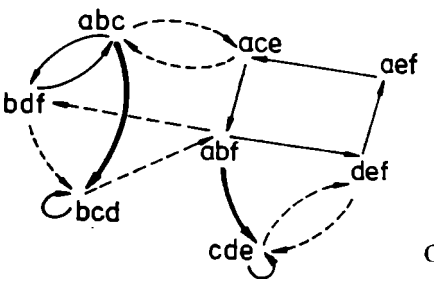
$$\begin{pmatrix} abc, abf, ace, aef, bdf, bcd, cde, def \\ bdf, def, abf, ace, abc, bcd, cde, aef \\ bcd, cde, bdf, abc, ace, abf, def, aef \end{pmatrix},$$

a potom vynecháme „průběžný stav" po postupu P, zachycený ve druhé řádce. Zůstane tabulka permutace (PQ) V, kterou udělá postup PQ na rohových prvcích:

$$\begin{pmatrix} abc, abf, ace, aef, bdf, bcd, cde, def \\ bcd, cde, bdf, abc, ace, abf, def, aef \end{pmatrix}.$$

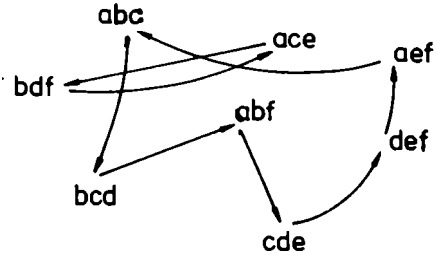
Stejně dostaneme i hranovou část tabulky permutace (PQ) V.

Vzpomeneme-li si na vztah mezi tabulkou a grafem permutace, snadno sestrojíme také graf permutace (PQ) V. Nejdříve si nakreslíme graf permutace $p = PV$ — obrázek 3.11. Potom do stejného obrázku překreslíme čárkovaně graf permutace $q = QV$. Na obrázku 3.21. vidíme rohovou část obou grafů. Kam povede v grafu permutace (PQ) V šipka z bodu abc? Kostička abc přejde postupem P na místo bdf — plná šipka —



Obr. 3.21

a z tohoto místa postupem Q na místo *bcd* — čárkovaná šipka. V grafu $(PQ)\,V$ tedy povede šipka z *abc* do *bcd* — silná šipka. Kostička *abf* přejde podél plné šipky do bodu *def* a dále podle čárkované šipky do bodu *cde*. Celá rohová část grafu permutace $(PQ)\,V$ je na obrázku 3.22.



Obr. 3.22

Cvičení 3.14. Hranová část tabulky permutace QV je

$$\begin{pmatrix} ab, ac, ae, af, bc, bd, bf, cd, ce, de, df, ef \\ af, bf, ac, bc, ce, ef, bd, df, cd, ae, ab, de \end{pmatrix}.$$

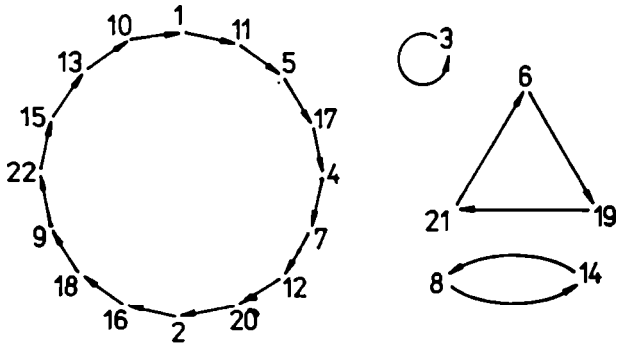
Sestrojte hranovou část tabulky a grafu permutace, kterou udělá postup PQ. Sestrojte tabulku a graf permutace, kterou udělá postup QP — napřed Q, potom P. Sestrojte tabulku a graf permutace $(PP)\,V$ — postup P opakujeme dvakrát po sobě.

Cvičení 3.15. Nakreslete graf permutace, kterou uděláme, jestliže v pozici na obrázku 3.10. pokračujeme tahem B.

Zcela stejně můžeme uvažovat i o všech ostatních hlavolamech. Ukážeme si to stručně na uších.

Uši. Vezměme si třeba pozici p na obrázku 3.8.b, dostali jsme ji nějakým postupem P. Jak se pozice změní,

uděláme-li teď tah B? Graf pozice $\boldsymbol{b} = \boldsymbol{BU}$ je čárkovaně na obrázku 3.18. Kulička 1 je v pozici $\boldsymbol{p}$ na místě 10, tahem B se posune na místo 11. Kulička 2 přejde z místa 15 na místo 16 atd. Graf nové pozice je na obrázku 3.23.



Obr. 3.23

Cvičení 3.16. a) Použijte obrázek 3.18. a nakreslete grafy permutací, které uděláme na uších postupy AB a BA.

b) Použijte část a) tohoto cvičení a nakreslete graf permutace, kterou dostaneme, jestliže v pozici na obrázku 3.12.b uděláme postup $Q = AB$.

Na závěr skládání postupů ještě důležitá poznámka. Při řešení hlavolamů začínáme v nějaké rozházené pozici $\boldsymbol{p}$, kterou jsme dostali neznámým postupem $\boldsymbol{P}$. Na tento případ se také hodí dosavadní výsledky tohoto odstavce. V pozici $\boldsymbol{p}$, jejíž polohová permutace je p, uděláme nějaký postup Q. Známe-li permutaci $q = \boldsymbol{QV}$, kterou postup Q udělá, můžeme určit polohy prvků v nové pozici — prvek i bude na místě $(ip)\,q$. Pokud je

permutace q dostatečně jednoduchá, umíme si změnu pozice $\boldsymbol{p}$ po postupu Q představit. Postupným pozměňováním dostaneme nakonec pozici základní. Naše strategie řešení hlavolamů spočívá proto v hledání postupů, které v pozicích udělají co nejjednodušší změny. Metodám vyhledávání takových postupů bude věnována čtvrtá kapitola.

A jakou permutaci uděláme postupem P^{-1}, inverzním k postupu P? Použijeme už známé výsledky. Složeným postupem PP^{-1} základní pozici nezměníme, na konci bude stejná jako na počátku. Uprostřed tohoto postupu, po P, bude krychle v pozici $\boldsymbol{p}$, její polohová permutace je p. Jestliže nějaký prvek i přejde postupem P na místo $j = ip$, pak postup P^{-1} jej zase vrátí zpět z místa j na místo i. Permutace $(P^{-1})\ \boldsymbol{V}$ proto zobrazuje prvek j do i, právě když permutace $p = P\boldsymbol{V}$ zobrazuje i do j. Graf $(P^{-1})\ \boldsymbol{V}$ dostaneme tak, že v grafu permutace p obrátíme směry všech šipek a její tabulku tak, že v tabulce p prohodíme oba řádky.

3.8. Skládání permutací. V pátém odstavci této kapitoly jsme ukázali, jak matematický pojem permutace popisuje polohy pohyblivých prvků na nejrůznějších hlavolamech. Nyní uvedeme další matematický pojem, který vystihuje, jak se poloha prvků mění, děláme-li nějaké postupy.

Zopakujme si stručně, co jsme zjistili v minulém odstavci. Je-li poloha prvků v nějaké pozici $\boldsymbol{p}$ popsána permutací p a uděláme-li postupem Q permutaci $q = Q\boldsymbol{V}$, pak poloha prvků v pozici, kterou dostaneme postupem Q z pozice $\boldsymbol{p}$, je popsána permutací na množině I všech pohyblivých prvků, která každému prvku i přiřazuje prvek $(ip)\,q$. Z permutací p a q jsme tak dostali jakousi novou permutaci. Můžeme to udělat s libovol-

nými dvěma permutacemi, nejenom s polohovými permutacemi na hlavolamech.

Jsou-li p a q permutace na nějaké množině I, pak *složení permutací* $p \circ q$ je permutace na množině I, která každému prvku i přiřazuje prvek $i(p \circ q) = (ip)\,q$.

Složeným postupem PQ tedy uděláme permutaci, která je složením permutací $p = PV$ a $q = QV$.

Permutaci jsme definovali jako vzájemně jednoznačné zobrazení na množině I. Aby mělo složení permutací smysl, musíme ukázat, že $p \circ q$ je opravdu permutace — vzájemně jednoznačné zobrazení. To je jasné v případě polohových permutací na hlavolamech, a obecný případ není o nic obtížnější. Zobrazení $p \circ q$ přiřazuje každému prvku $i \in I$ jednoznačně určený prvek $(ip)\,q$. A je-li naopak k nějaký prvek I, existuje přesně jeden prvek $j \in I$ takový, že $jq = k$, protože q je permutace. Existuje také přesně jeden prvek $i \in I$ takový, že $ip = j$, protože také p je permutace. Tento prvek i je jediný, pro který platí $(ip)\,q = i(p \circ q) = k$. Zobrazení $p \circ q$ je tedy opravdu vzájemně jednoznačné, je to permutace.

Tabulku a graf složení permutací umíme najít už z minulého odstavce, takže jenom stručné opakování.

Tabulka složené permutace. Napíšeme si napřed tabulku permutace p a pod ní tabulku q, přičemž dolní řádek tabulky p považujeme za horní řádek tabulky q — na pořadí prvků v tabulce nezáleží. Dostaneme tak tabulku o třech řádcích. Vynecháním „průběžného" druhého řádku dostaneme tabulku permutace $p \circ q$. Pod prvkem i v prvním řádku je ve druhém řádku ip a ve třetím $(ip)\,q = i(p \circ q)$:

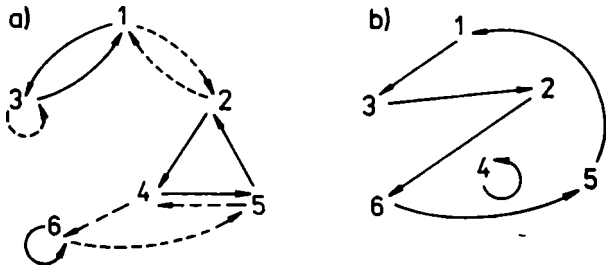
$$\begin{pmatrix} \ldots\ldots, & i, & \ldots\ldots \\ \ldots\ldots, & ip, & \ldots\ldots \\ \ldots\ldots, & (ip)\,q, & \ldots\ldots \end{pmatrix}.$$

Cvičení 3.17. Napište tabulky permutací $p \circ q$, $q \circ p$ a $p \circ p$, je-li

$$p = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 3, 4, 1, 5, 2, 6 \end{pmatrix} \quad , \quad q = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 2, 1, 3, 6, 4, 5 \end{pmatrix}$$

Důležité upozornění. Výsledek předchozího cvičení ukazuje, že složením dvou permutací v různém pořadí můžeme dostat různé výsledky. Permutace $p \circ q$ a $q \circ p$ mohou být, a většinou také jsou, různé.

Graf složení permutací. Nakreslíme do jednoho obrázku grafy obou permutací p a q. Na obrázku 3.24.a jsou grafy permutací p (plnou čarou) a q (čárkovaně) ze cvičení 3.17. Šipka v grafu $p \circ q$ z bodu i povede do bodu $(ip)q$. Tento bod najdeme tak, že se vydáme z bodu i po šipce grafu p do bodu ip, a dále po šipce grafu q dojdeme do bodu $(ip)q$. Graf $p \circ q$ je na obrázku 3.24.b.



Obr. 3.24

Cvičení 3.18. Nakreslete grafy permutací $q \circ p$ a $q \circ q$, p, q stejné jako ve cvičení 3.17. — obrázek 3.24.a.

Závěrem ještě několik jednoduchých vlastností skládání permutací.

Asociativita. Máme-li složit tři permutace p, q, r na množině I v tomto pořadí, můžeme to udělat dvěma způsoby. Buď napřed složíme p s q a výsledek $p \circ q$ složíme s r, nebo složíme p s permutací $q \circ r$. Obě možnosti $(p \circ q) \circ r$ a $p \circ (q \circ r)$ vedou ke stejnému výsledku. V prvém případě zobrazíme prvek i napřed do prvku $i(p \circ q) = (ip)\, q$ a tento pak do prvku $((ip)\, q)\, r$. Ve druhém případě zobrazíme napřed i do ip a potom do $(ip)\,(q \circ r) = ((ip)\, q)\, r$. Obě permutace $(p \circ q) \circ r$ a $p \circ (q \circ r)$ zobrazují libovolný prvek $i \in I$ do jednoho a téhož prvku $((ip)\, q)\, r$. Znamená to, že se rovnají, $(p \circ q) \circ r = p \circ (q \circ r)$ pro každé tři permutace p, q, r na množině I. Říkáme, že *skládání permutací je asociativní.*

Asociativita skládání permutací má jeden důležitý důsledek. Máme-li složit k permutací $p_1, p_2, \ldots, p_k$ v tomto pořadí, můžeme to udělat mnoha způsoby. Vybereme nějakou sousední dvojici p_i a p_{i+1}, složíme ji, a místo obou permutací napíšeme v seznamu jedinou permutaci $p_i \circ p_{i+1}$. V novém seznamu opět vybereme dvě sousední permutace a celý postup opakujeme. Děláme to tak dlouho, až dostaneme jedinou permutaci. Z asociativity skládání permutací plyne, že všechny způsoby vedou ke stejnému výsledku, který označíme $p_1 \circ p_2 \circ \ldots \circ p_k$. Nebudeme to dokazovat teď, dokážeme to až v hvězdičkovaném odstavci 3.13., používat to ale budeme i dříve.

Identická permutace je neutrální. Pro každou permutaci p platí $p \circ n = n \circ p = p$. Jinými slovy, identická permutace je neutrální vzhledem ke skládání permutací, složíme-li ji s nějakou permutací p, dostaneme opět p.

Cvičení 3.19. Dokažte rovnosti $p \circ n = n \circ p = p$.

Inverzní permutace. Nějakým postupem P uděláme permutaci $p = PV$ a inverzním postupem P^{-1} uděláme permutaci, která zobrazuje prvek j do i, právě když $ip = j$. Permutaci $(P^{-1})\,V$ budeme říkat *inverzní permutace* k $p = PV$ a značit ji p^{-1}. Stejně můžeme definovat inverzní permutaci p^{-1} k libovolné permutaci p na množině I. Pro permutaci p^{-1} platí $jp^{-1} = i$, právě když $ip = j$. Tabulku p^{-1} dostaneme tak, že v tabulce p zaměníme oba řádky. Tak třeba

$$\begin{pmatrix} 2, & 1, & 3, & 6, & 4, & 5 \\ 1, & 2, & 3, & 4, & 5, & 6 \end{pmatrix}$$

je tabulka permutace q^{-1} inverzní k permutaci q ze cvičení 3.17. Graf inverzní permutace p^{-1} dostaneme tak, že v grafu p obrátíme směry všech šipek. Snadno se také ověří, že k permutaci p^{-1} je inverzní zase permutace p, tj. platí $(p^{-1})^{-1} = p$.

Z vlastnosti inverze hlavolamů plyne, že umíme-li udělat nějakou permutaci p, pak umíme udělat také permutaci inverzní p^{-1}. Ukázali jsme to na konci minulého odstavce. A nakonec lehká, ale důležitá vlastnost inverzních permutací.

Cvičení 3.20. Dokažte rovnosti $p \circ p^{-1} = p^{-1} \circ p = n$.

Tato vlastnost je pro inverzní permutaci p^{-1} charakteristická. Pokud $p \circ q = n$ nebo $q \circ p = n$ pro nějakou permutaci q, pak $q = p^{-1}$. Opravdu, je-li $ip = j$, pak z každé z těchto rovností ihned plyne $jq = i$.

3.9. Matematický model úplných hlavolamů. Víme toho už o hračkách dost, abychom mohli sestavit jejich matematický model. Na každém hlavolamu je nějaká

skupina pohyblivých prvků, kterou označujeme I. Polohu těchto prvků popisujeme permutacemi na množině I. Na počátku je hra v základní pozici, poloha prvků je popsána identickou permutací. Polohu prvků měníme pomocí tahů, každý tah udělá nějakou permutaci. Permutace, které uděláme jednotlivými tahy, budeme nazývat *generátory*. Postupným prováděním tahů děláme další pozice. Jejich polohové permutace dostaneme složením odpovídajících generátorů. Známe-li generátory, známe vlastně celou hru. Všechna možná složení generátorů odpovídají polohovým permutacím všech pozic, které můžeme dostat nějakým postupem z pozice základní, a tedy všem řešitelným pozicím. Generátory tak určují všechny vlastnosti polohy prvků na hlavolamu.

Matematický model úplného hlavolamu vypadá takto. Máme nějakou množinu I a několik permutací-generátorů na I. Umět řešit hlavolam znamená umět popsat všechny permutace na I, které jsou složením generátorů, a pro každou takovou permutaci najít nějaké její vyjádření jako složení generátorů.

Množinu I jsme vždy interpretovali jako množinu všech pohyblivých prvků. Náš model tak přesně popisuje hry bez orientace a částečně hry s orientací, ztrácí se v něm právě ta orientace. Pokud nemáme domino nebo uši, můžeme si hrát aspoň na papíře s jejich matematickým modelem. A co víc, můžeme hrát i hry, které neexistují, nebyly vyrobeny. V příštím odstavci tak budeme zkoumat model hry, ve které jsou obzvlášť jednoduché tahy. Tato hra bude velice snadná, a přesto se při ní naučíme mnoho užitečného i pro další hlavolamy. Složitost hlavolamů totiž zcela závisí na složitosti vzájemné polohy generátorů a vlastnosti, které budou očividné v naší jednoduché hře, by bylo mnohem obtížnější odhalit na Rubikově krychli nebo čtyřstěnu.

Poznámka, kterou je možné přeskočit. Při vhodné interpretaci množiny I můžeme náš matematický model použít i ke studiu orientací. Ukážeme si stručně jak na Rubikově krychli. Množinu I budeme tentokrát interpretovat jako množinu malých plošek — čtverečků na krychli, a ne jako množinu pohyblivých prvků. Každý tah udělá dva čtyřcykly na hranových ploškách a tři čtyřcykly na rohových ploškách. Pozice pak chápeme ne jako permutace na kostičkách, ale jako permutace na ploškách. V tomto modelu se dají studovat i orientace, není k tomu ale příliš vhodný. Lepší matematický model her s orientací sestavíme v páté kapitole.

A nakonec ještě pár slov o významu modelů vůbec. Matematické modely jsou běžně používány v nejrůznějších oblastech vědy a techniky. Rozsah jejich aplikací nesmírně vzrostl použitím výkonných počítačů. Ty umožňují zpracovávat složité modely, jejichž studium by jinak bylo zcela nemyslitelné. Nákladné experimentování při stavbě lodí, letadel, automobilů nebo raketoplánů lze nahradit mnohem lacinějším experimentováním na počítači. Místo zkoušení různých profilů křídel v aerodynamických tunelech stačí často sestavit a zpracovat správné rovnice obtékání těles. A v případě stavby přehrady, mostu nebo jaderné elektrárny si ani nějaké experimentování nejde dost dobře představit, všechno musí být propočítané předem. Matematické modely se používají v genetice, v teorii přenosu informace, fyziologii, psychologii nebo ve fyzice elementárních částic. Teoretická práce v mnoha oborech spočívá převážně ve studiu matematických modelů. V tom je zcela určitě nejdále fyzika. První složitější modely přírodních jevů vytvořili patrně astronomové, pravidelný pohyb planet a hvězd na nebeské klenbě je k tomu jako stvořený. Rozvíjení a zkoumání stále složitějších modelů dalo vznik celým matematickým disciplínám. Určitě

není náhodou, že zákony klasické mechaniky a objev infinitezimálního počtu jsou spojeny s jedním člověkem, Isaacem Newtonem.

Mnohem častěji je ale při sestavování modelů používána matematika již vytvořená. A tak vlastnosti modelů závisí hodně na matematických znalostech těch, kdo je sestavují. Vždyť ani my nepoužíváme při zkoumání a řešení hlavolamů v této knize pojmy a metody, které by nebyly matematikům známé aspoň sto padesát let.

3.10. Nezajímavé hračky. Nezajímavé jsou takové hlavolamy, které každý snadno vyřeší. Nikdo by je nekupoval, a proto je také nikdo nevyrábí. Přesto se jimi budeme trochu zabývat. Nemusíme si ani představovat, jak by asi vypadaly, stačí nám jejich matematický model.

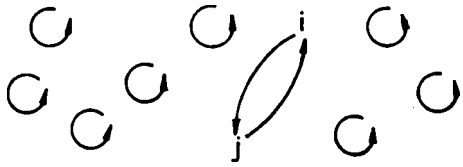
Tento model spočívá ve výběru nějaké množiny permutací-generátorů na množině $I = \{1, 2, \ldots, k\}$. Nejjednodušší by bylo řešit hlavolam, na kterém bychom mohli prohodit každé dva prvky na libovolných dvou místech, a žádné jiné by polohu nezměnily. Znamená to, že pro každé dva různé prvky $i, j \in I$ bychom měli k dispozici tah, který by udělal permutaci

$$t = \begin{pmatrix} 1, 2, \ldots i, \ldots j, \ldots, k-1, k \\ 1, 2, \ldots j, \ldots i, \ldots, k-1, k \end{pmatrix}.$$

Graf této permutace je na obrázku 3.25., má jeden cyklus délky 2 a ostatní s délkou 1.

Takovým permutacím se v matematice říká *transpozice*. Každá transpozice je jednoznačně popsána dvojicí prvků, které tvoří cyklus délky 2. Právě uvedená transpozice t je popsána dvojicí (i, j). Pro snazší orientaci budeme transpozice označovat dvojicemi prohazova-

ných prvků, (i, j) je tedy nové označení pro transpozici t na obrázku 3.25.



Obr. 3.25

Cvičení 3.21. Nechť i, j, k, l jsou čtyři různé prvky množiny I. Nakreslete grafy složení transpozic $(i, j) \circ (i, j), (i, j) \circ (j, k), (i, j) \circ (k, l), (i, j) \circ (j, k) \circ (i, j)$.

Naše snadná hra má pro každou dvojici různých prvků $i, j \in I$ jeden tah, který udělá transpozici (i, j). Velká zásoba jednoduchých tahů umožňuje snadno složit každou pozici-permutaci. Začneme konkrétním příkladem. Množina I má osm prvků 1, 2, 3, 4, 5, 6, 7, 8 a jejich poloha je popsána permutací

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

Permutace p není identická, až na jeden jsou všechny prvky na nesprávných místech. Vezmeme si jeden z nich, třeba 1. Ten je na místě 2, abychom ho dostali na správné místo, uděláme transpozici (1, 2). Dostaneme novou permutaci

$$p \circ (1, 2) = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 1, 5, 3, 6, 7, 8, 2, 4 \end{pmatrix}.$$

Dále dáme na správné místo prvek 2. Ten je na místě 5, uděláme proto transpozici (2, 5). Dostaneme permutaci

$$p \circ (1, 2) \circ (2,5) = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 1, 2, 3, 6, 7, 8, 5, 4 \end{pmatrix}.$$

Stále ještě není všechno na správném místě, třeba 6 je na místě 8, uděláme tedy transpozici (6, 8). Každý snadno ověří, že složením transpozic (1, 2) ∘ (2, 5) ∘ ∘ (6, 8) ∘ (5, 7) ∘ (4, 8) dostaneme hru z pozice p do pozice základní, tj. že platí $p \circ (1, 2) \circ (2, 5) \circ (6, 8) \circ \circ (5, 7) \circ (4, 8) = n$. Permutaci p jsme složili z transpozic.

Zcela stejně se přesvědčíme, že každou permutaci q na množině $I = \{1, 2, \ldots, k\}$ lze složit z transpozic. Pokud je q identická permutace, není třeba dělat nic. Pokud není, existuje prvek i takový, že $iq \neq i$, tj. i není na správném místě. Složíme q s transpozicí (i, iq). Protože $iq \neq i$ a q je vzájemně jednoznačné zobrazení, existuje jiný prvek $j \in I$, pro který platí $jq = i$ (na každém místě je nějaký prvek!). Ani prvek j není na správném místě:

$$q = \begin{pmatrix} 1, \ldots, & i, \ldots, & j, \ldots, k \\ 1q, \ldots, & iq, \ldots, & i = jq, \ldots, kq \end{pmatrix}.$$

V nové pozici $q \circ (i, iq)$ budou s výjimkou prvků i a j všechny ostatní na stejných místech jako v pozici q. Všechny, které byly na správných místech v q, budou proto na správných místech také v $q \circ (i, iq)$. Navíc bude správně také i. Tahem (i, iq) jsme tak zvětšili počet prvků na správných místech aspoň o jeden. Pokud je permutace $q \circ (i, iq)$ identická, jsme u cíle. Pokud není, vybereme nějaký prvek, který ještě na správném místě není, a opakujeme celou úvahu znovu. Tak postupně zvětšujeme počet prvků na správných místech, až po nejvýše $k - 1$ krocích dostaneme identickou permutaci n. Platí proto, že

(I) ke každé permutaci q existují transpozice $t_1, t_2, \ldots, t_l$ takové, že $q \circ (t_1 \circ t_2 \circ \ldots \circ t_l) = n$.

Z poslední věty odstavce 3.8. plyne, že $t_1 \circ t_2 \circ \ldots \circ t_l$ musí být inverzní permutace q^{-1} k permutaci q, tj. $q^{-1} = t_1 \circ t_2 \circ \ldots \circ t_l$. Každou permutaci inverzní k nějaké permutaci q na množině I tedy můžeme vyjádřit jako složení nějakých transpozic. A protože každá permutace je inverzní k nějaké jiné, q je inverzní ke q^{-1}, dostáváme

(II) pro každou permutaci q existují transpozice $u_1, u_2, \ldots, u_m$ tak, že $q = u_1 \circ u_2 \circ \ldots \circ u_m$.

Dokázali jsme tak, že z vlastnosti (I) plyne vlastnost (II). Platí to i naopak, z (II) plyne (I). Vyjádříme q^{-1} jako složení transpozic: $q^{-1} = u_1 \circ u_2 \circ \ldots \circ u_m$. Potom platí $q \circ (u_1 \circ u_2 \circ \ldots \circ u_m) = q \circ q^{-1} = n$, neboli platí vlastnost (I). Obě vlastnosti (I) a (II) jsou proto ekvivalentní. Budeme říkat, že

každou permutaci lze složit z transpozic.

Formulace (I) je výhodnější při řešení hlavolamů, formulace (II) je zase vhodnější pro teoretické zkoumání permutací. Uvidíme to v příštím odstavci.

Po těchto poněkud teoretičtějších úvahách se vrátíme zpět k naší nezajímavé hře. Její řešení je opravdu snadné. Každou permutaci lze složit, máme-li k dispozici všechny transpozice. Nalezení posloupnosti transpozic, kterými z nějaké permutace p dostaneme permutaci identickou, také není nijak obtížné. Vezmeme vždy nějaký prvek, který není na správném místě, a uděláme transpozici, která ho na správné místo převede. Tím

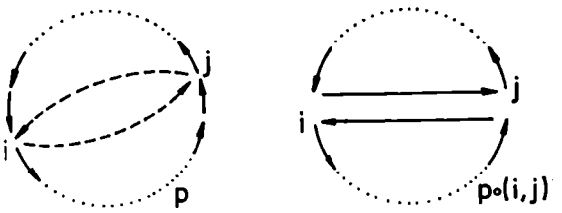
postupně zvyšujeme počet prvků na správných místech, až dostaneme všechny tam, kde mají být.

Jakkoliv je hra, ve které můžeme dělat všechny transpozice, snadná, můžeme se z ní hodně poučit. Zjistili jsme, že každou permutaci lze složit z transpozic. Kdybychom uměli na každé Rubikově kostce najít postupy, které udělají libovolnou transpozici, bylo by snadné dostat všechny prvky na správná místa. Tím bychom uměli řešit všechny hry bez orientace a také trochu hry s orientací. Brzy si ale ukážeme, že tak jednoduché to zase není. V mnoha případech postupy, které by udělaly nějakou transpozici, vůbec neexistují, zrovna Rubikova krychle je takový případ. Nebo sice existují, jsou ale příliš dlouhé a jejich nalezení obtížné. Tak je tomu třeba na uších.

Přesto se touto myšlenkou budeme ještě zabývat. Její upravená verze nám už umožní vyřešit všechny hlavolamy bez orientace a dostat všechny prvky na správné místo u her s orientací. Napřed ale zopakujeme a zobecníme poznatky druhé kapitoly.

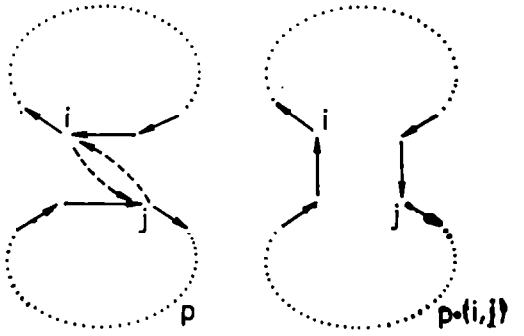
3.11. Sudé a liché permutace. V tomto odstavci ukážeme, že všechny permutace na množině $I = \{1, 2, \ldots, k\}$ můžeme přirozeným způsobem rozdělit na sudé a liché podobně jako celá čísla. V podstatě jsme to udělali už ve druhé kapitole při zkoumání pozic u patnáctky. Tam měla množina I šestnáct prvků.

Vezmeme nějakou permutaci p na množině I a transpozici (i, j). Jak se liší grafy permutací p a $p \circ (i, j)$? Jsou-li i a j ve stejném cyklu permutace p — obrázek 3.26. — rozpadne se tento cyklus do dvou menších cyklů v grafu $p \circ (i, j)$. Ostatní cykly se nezmění, jejich celkový počet se tak zvětší o jeden.



Obr. 3.26

Jsou-li prvky i, j naopak v různých cyklech v grafu p, propojí se tyto dva cykly do jednoho velkého v grafu $p \circ (i, j)$.



Obr. 3.27

I v tomto případě se tak počet cyklů změní, tentokrát zvětší, o jeden. V každém případě se proto počty cyklů v permutacích p a $p \circ (i, j)$ liší o jeden. Přidáme-li k p sudý počet transpozic, musí se lišit počty cyklů v p a v $p \circ t_1 \circ t_2 \circ \ldots \circ t_{2m}$ o sudé číslo. Přidáme-li lichý počet transpozic, je rozdíl mezi počtem cyklů v p a v $p \circ t_1 \circ t_2 \circ \ldots \circ t_{2m+1}$ vždy lichý.

Rozdíl mezi počtem cyklů v identické permutaci n

a v permutaci $n \circ t_1 \circ t_2 \circ \ldots \circ t_{2m}$ (složení sudého počtu transpozic) je proto vždy sudý, rozdíl mezi počtem cyklů v n a v $n \circ t_1 \circ t_2 \circ \ldots \circ t_{2m+1} = t_1 \circ t_2 \circ \ldots \circ t_{2m+1}$ (složení lichého počtu transpozic) je vždycky lichý. Z minulého odstavce víme, že každou permutaci p můžeme složit z transpozic, $p = t_1 \circ t_2 \circ \ldots \circ t_l$. Je-li rozdíl mezi počtem cyklů v identické permutaci (ten se rovná k, každý cyklus má délku 1) a v permutaci p sudý, musíme použít sudý počet transpozic, je-li rozdíl lichý, pak musí být číslo l liché. Tyto úvahy vedou k následující definici.

Permutace p na množině I je *sudá*, je-li rozdíl mezi počtem prvků I a počtem cyklů v p sudý, a je *lichá*, je-li tento rozdíl lichý.

Cvičení 3.22. Které z následujících permutací jsou sudé a které liché?

$$p = \begin{pmatrix} 1, 2, 3, 4, 5 \\ 2, 3, 5, 4, 1 \end{pmatrix} \quad q = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 3, 1, 2, 5, 6, 4 \end{pmatrix} \quad r = \begin{pmatrix} 1, 2 \\ 2, 1 \end{pmatrix}$$

$$s = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, & 8, 9, 10, 11, 12 \\ 7, 4, 6, 1, 9, 2, 8, 10, 3, & 5, 11, 12 \end{pmatrix} \quad n = \begin{pmatrix} 1, 2, 3, 4 \\ 1, 2, 3, 4 \end{pmatrix}.$$

Cvičení 3.23. Kterých permutací na množině I je více, sudých, nebo lichých?

Permutace p a inverzní permutace p^{-1} mají stejný počet cyklů stejných délek, jejich grafy se liší jen ve směru šipek. Obě jsou současně buď liché, nebo sudé.

Už před definicí sudých a lichých permutací jsme ukázali následující *pravidlo o počtu transpozic*.

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.

S tímto pravidlem snadno zjistíme, kdy je složení dvou permutací sudé a kdy liché. Vezměme si dvě permutace p a q na množině I a jejich libovolná vyjádření $p = t_1 \circ t_2 \circ \ldots \circ t_l$ a $q = u_1 \circ u_2 \circ \ldots \circ u_m$ jako složení transpozic. Složenou permutaci $p \circ q$ pak můžeme vyjádřit jako $p \circ q = t_1 \circ t_2 \circ \ldots \circ t_l \circ u_1 \circ \ldots \circ u_m$. K rozhodnutí, je-li $p \circ q$ sudá nebo lichá, stačí zjistit, je-li číslo $l + m$ sudé nebo liché. Je sudé, jestliže jsou obě čísla l a m současně sudá nebo současně lichá, a je liché v opačném případě. Permutace $p \circ q$ je tedy sudá, právě když jsou obě permutace p a q sudé nebo obě liché, a je lichá, právě když je jedna z nich sudá a druhá lichá. Skládání permutací má stejné vlastnosti jako sčítání celých čísel.

Složení dvou sudých nebo dvou lichých permutací je sudá permutace, složení sudé s lichou je permutace lichá.

Toto pravidlo budeme nazývat *pravidlo o paritě složení permutací*. Je to pravidlo velmi důležité, s jeho pomocí už budeme v příštím odstavci schopni dokázat neřešitelnost nejrůznějších pozic na mnoha hlavolamech. Všimněte si ještě, jak byl při jeho odvození užitečný ekvivalentní popis sudých a lichých permutací pomocí počtu transpozic potřebných k jejich složení. Kdybychom měli používat pouze definici, museli bychom počítat počet cyklů v $p \circ q$ v závislosti na počtech cyklů

v permutacích p a q, což by bylo podstatně složitější. Různé pohledy na stejnou věc jsou vždy užitečné. Ukážeme si ještě jeden pohled na sudé a liché permutace.

Tentokrát budeme počítat počet sudých cyklů v permutacích p a $p \circ (i, j)$. Jsou-li prvky i, j v témže cyklu permutace p, rozpadne se tento cyklus na dva menší v $p \circ (i, j)$. Má-li původní cyklus lichou délku, musí být jeden z menších cyklů sudý a druhý lichý, sudých cyklů v permutaci $p \circ (i, j)$ je tedy o jeden více než v permutaci p. Je-li původní velký cyklus sudý, musí být oba menší buď sudé, nebo liché. Ve všech třech případech se tak počet sudých cyklů v p a $p \circ (i, j)$ liší o jeden.

Zcela stejně se ukáže, že také v případě, kdy jsou i, j v různých cyklech grafu p, je rozdíl mezi počtem sudých cyklů v p a $p \circ (i, j)$ rovný jedné (v absolutní hodnotě).

Identická permutace n má pouze liché cykly délky 1, žádný sudý. Jestliže tedy nějakou permutaci p složíme ze sudého počtu transpozic, musí mít sudý počet sudých cyklů, a složíme-li ji z lichého počtu transpozic, musí mít lichý počet sudých cyklů. Tím jsme ukázali *pravidlo o počtu sudých cyklů.*

> Permutace je sudá, právě když má sudý počet cyklů sudé délky, a je lichá, právě když má lichý počet cyklů sudé délky.

Cvičení 3.24. Každá transpozice je lichá permutace.

V odstavcích 3.4. a 3.5. jsme se naučili zaznamenávat polohu pohyblivých prvků v pozicích na hlavolamech pomocí permutací. Nyní už umíme mezi permutacemi

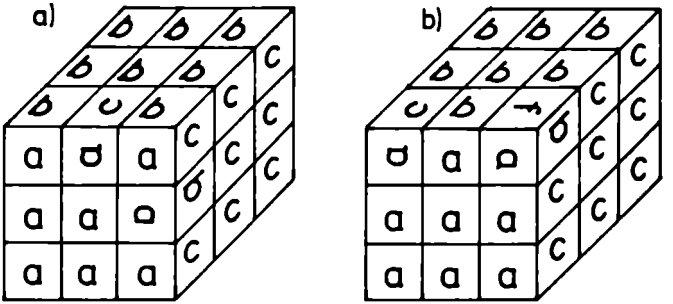
rozlišovat sudé a liché, můžeme tedy rozlišovat také mezi pozicemi.

Pozice na nějakém hlavolamu je *sudá*, je-li její polohová permutace sudá, a je *lichá*, je-li její polohová permutace lichá.

Cvičení 3.25. Které z následujících pozic na uších jsou sudé a které liché: pozice na obrázku 3.8.b, 3.13.a, 3.13.b.

Cvičení 3.26. Je pozice na Rubikově krychli na obrázku 3.10. sudá, nebo lichá? Její graf je na obrázku 3.11.

3.12. Některé neřešitelné pozice. Konečně se můžeme přesvědčit o neřešitelnosti mnoha pozic na hlavolamech. Začneme opět Rubikovou krychlí. Na obrázku 3.28. jsou dvě pozice. Všechny kostičky s výjimkou dvou jsou vždy na správných místech.



Obr. 3.28

V pozici a) jsou přehozené pouze hranové kostičky *ab* a *ac*, v pozici b) jsou špatně jenom rohové kostičky *abc* a *abf*. Polohové permutace obou pozic jsou transpozice,

mají jeden cyklus délky 2 a ostatní s délkou 1. Obě pozice jsou proto liché.

Dříve než dokážeme neřešitelnost těchto pozic, naučíme se ještě rozlišovat sudé a liché tahy na hračkách. Každému tahu jsme přiřadili nějakou permutaci — polohovou permutaci pozice, kterou tímto tahem dostaneme z pozice základní.

Budeme říkat, že nějaký *tah* je *sudý*, jestliže tímto tahem uděláme sudou permutaci, a že je *lichý*, jestliže jím uděláme permutaci lichou.

Každý tah na Rubikově krychli udělá permutaci, která má dva cykly délky 4 a ostatní cykly délky 1. Tato permutace je sudá, má dva sudé cykly.

Každý tah na Rubikově krychli je sudý.

Z tahů skládáme postupy. Jakou permutaci uděláme nějakým postupem $P = X_1 X_2 \ldots X_m$? V odstavci 3.7. jsme si vysvětlili, že permutaci, kterou udělá postup P, dostaneme složením permutací, které udělají jednotlivé tahy. Symbolicky to zapisujeme $PV = (X_1 V) \circ (X_2 V) \circ \circ \ldots \circ (X_m V)$. Právě jsme si ukázali, že každý tah na Rubikově krychli je sudý, udělá sudou permutaci. Všechny permutace $X_i V$ jsou proto sudé. Podle pravidla o paritě složení permutací musí být sudé i jejich složení, permutace PV.

Každý postup na Rubikově krychli udělá sudou permutaci.

Už z první kapitoly, z odstavce 1.9., víme, že řešitelné jsou jenom ty pozice, které můžeme dostat ze základní nějakým postupem. Každý postup ale udělá sudou per-

mutaci, nikdy lichou. Liché pozice jsou proto neřešitelné.

> Všechny liché pozice na Rubikově krychli jsou neřešitelné.

A tak obě liché pozice na obrázku 3.28. jsou neřešitelné. Na Rubikově krychli neexistuje žádný postup, který by prohodil pouze dva prvky, a ostatní nechal na původních místech. Transpozice nejdou udělat.

Jiná varianta důkazu neřešitelnosti lichých pozic je v následujícím cvičení.

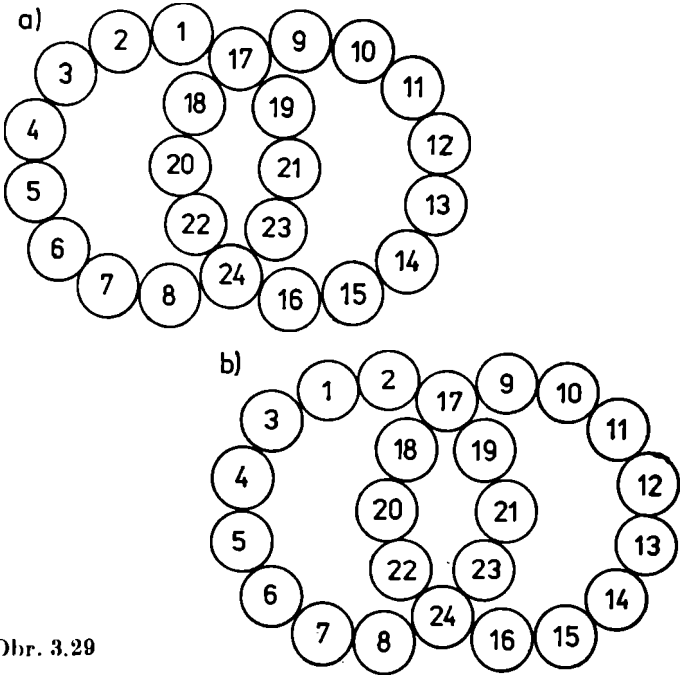
Cvičení 3.27. Jaká je polohová permutace pozice, kterou dostaneme z liché pozice nějakým postupem? Můžeme někdy dostat pozici, ve které jsou všechny prvky na správných místech?

V příští kapitole ukážeme, jak každou sudou pozici srovnat do pozice, ve které jsou všechny prvky na správných místech. Každá sudá pozice je srovnatelná. Neznamená to ještě, že je řešitelná. I mezi sudými pozicemi je mnoho neřešitelných. Příčina jejich neřešitelnosti je ale v orientacích, nikoliv už v polohách jednotlivých prvků.

A teď na další hračky!

Uši. Každý tah udělá jeden cyklus délky 12 a zbývající cykly jsou jednoprvkové. Na uších jsou tahy liché, mají jeden sudý cyklus. Pomocí pravidla o paritě složení permutací zjistíme, že sudým počtem tahů uděláme sudou pozici a lichým počtem lichou. Řešitelné pozice na uších mohou být proto jak sudé, tak liché. V příští kapitole ukážeme, že ve skutečnosti jsou všechny pozice řešitelné.

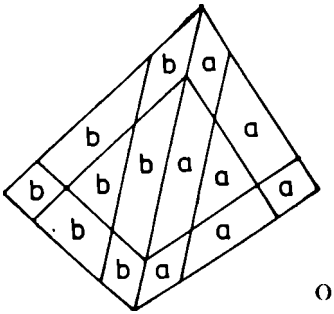
Jiné je to u varianty s lichým počtem kuliček v jednom uchu. Na obrázku 3.29. je jich třináct.



Obr. 3.29

Na obrázku a) je základní pozice, pozice na obrázku b) je lichá, její polohová permutace je transpozice. Každý tah udělá jeden cyklus délky 13 a ostatní cykly jsou délky 1. Tentokrát je každý tah sudý a pravidlo o paritě složení permutací pak dává, že každý postup udělá sudou permutaci. Liché pozice jsou proto neřešitelné. Sudé řešitelné jsou, jak uvidíme v příští kapitole.

Čtyřstěn. Touto hrou jsme se dosud příliš nezabývali, a tak ji nyní probereme podrobněji. Čtyřstěn má čtyři pohyblivé vrstvy, tvoří je vždy sedm prvků ležících v jedné stěně. Každou vrstvou lze otočit o 120° vpravo nebo vlevo. Stěny a vrstvy v základní pozici označíme podle obrázku 3.30. písmeny *a*, *b*, *c*, *d*, zadní stěna je *c* a dolní *d*. Příslušná otočení vpravo pak budeme značit *A*, *B*, *C*, *D*.



Obr. 3.30

Poloha a orientace prvků v základní pozici je jednoznačně určená čtyřmi stěnovými trojúhelníky, které tvoří souřadný systém na čtyřstěnu. Můžeme jimi pootáčet, nelze je ale prohazovat. Jednotlivé prvky budeme označovat tak jako na Rubikově krychli, seznamem písmen, kterými jsou označené. Stěnové trojúhelníky budou *a*, *b*, *c*, *d*, hranové prvky *ab*, *ac*, *ad*, *bc*, *bd* a *cd* a rohové *abc*, *abd*, *acd* a *bcd*. Čtyřstěn je hra nesouvislá, má dvě orbity, šestiprvkovou hranovou a čtyřprvkovou rohovou. Je to hra úplná, každý tah lze udělat kdykoliv, a s orientací.

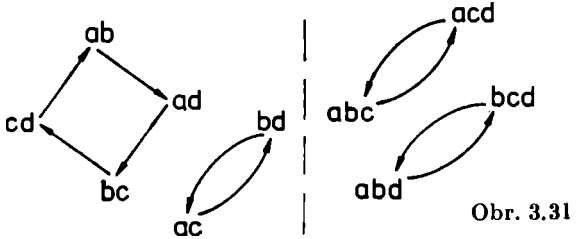
Souřadný systém stěnových trojúhelníků určuje jediné správné místo v základní pozici pro každý pohyblivý prvek. Hranový prvek *ab* musí ležet mezi trojúhelníky

a a b, rohový abc pak ve společném vrcholu stěn, v jejichž středech jsou trojúhelníky a, b a c.

Polohu pohyblivých prvků zapisujeme pomocí tabulek a grafu. Tak třeba

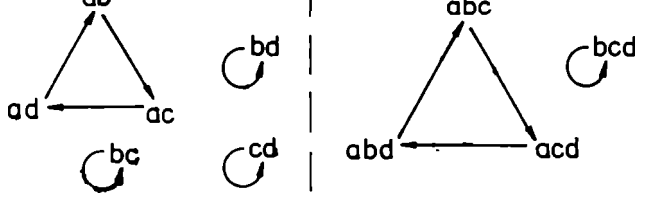
$$p = \begin{pmatrix} ab, ac, ad, bc, bd, cd, abc, abd, acd, bcd \\ ad, bd, bc, cd, ac, ab, acd, bcd, abc, abd \end{pmatrix}$$

je tabulka polohové permutace nějaké pozice na čtyřstěnu, její graf je na obrázku 3.31.



Obr. 3.31

Jaké permutace udělají jednotlivé tahy? Třeba tah A? Prvek ab přejde na místo ac, ac na místo ad a ad zpět na místo ab. Jiné hranové prvky se nepohybují. Z rohových přejde abc na místo acd, acd na místo abd a abd zpět na místo abc. Prvek bcd se nepohybuje. Graf permutace, kterou udělá tah A, je na obrázku 3.32.



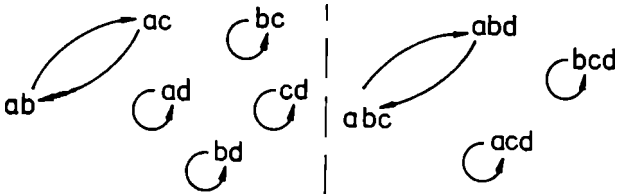
Obr. 3.32

Má dva cykly délky 3 a čtyři cykly délky 1. Tah A je sudý, nemá žádný cyklus sudé délky. Také všechny ostatní tahy jsou sudé.

Každý tah na čtyřstěnu je sudý.

Složením sudých permutací dostaneme jenom sudé permutace, každý postup na čtyřstěnu proto udělá sudou permutaci. Liché pozice jsou neřešitelné.

O Rubikově krychli jsme si řekli, a v příští kapitole to dokážeme, že všechny sudé pozice jsou srovnatelné, lze je převést do pozice, ve které jsou všechny prvky na správných místech. Na čtyřstěnu to ale neplatí. Na obrázku 3.33. je graf pozice, kterou nejde srovnat. Je neřešitelná, protože ji nikdy nedostaneme do pozice, ve které by byly všechny prvky na správných místech.



Obr. 3.33

Proč to nejde? Podívejme se ještě jednou na obrázek 3.32., na graf permutace, kterou udělá tah A. Soustředíme-li se jenom na hranovou část, vidíme, že na hranových prvcích udělá tah A také sudou permutaci, má jeden trojcyklus a tři cykly délky 1. A protože to platí pro každý tah, jsou všechny tahy sudé na hranových prvcích. Každý postup proto udělá na hranových kostič-

kách sudou permutaci, nikdy lichou. Všechny pozice, jejichž polohové permutace jsou liché na hranových prvcích, jsou proto neřešitelné.

Také na rohových prvcích dělají všechny tahy, a tedy také všechny postupy, sudé permutace. Tím jsme podstatně zvětšili počet pozic, o kterých umíme dokázat, že jsou neřešitelné.

> Každá pozice na čtyřstěnu, jejíž polohová permutace na hranových nebo na rohových prvcích je lichá, je neřešitelná.

Polohová permutace žádné řešitelné pozice proto nemůže mít graf jako na obrázku 3.33.

Jako obvykle slíbíme, že v příští kapitole najdeme postupy, které všechny ostatní pozice srovnají, převedou do pozice, ve které jsou všechny prvky na správných místech.

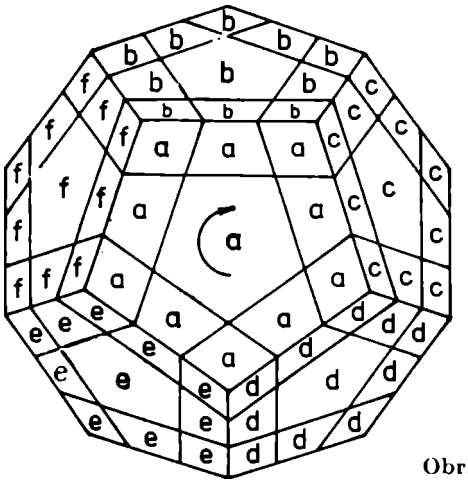
Dvanáctistěn. Tato hračka má, aspoň pokud jde o polohy prvků, podobné vlastnosti jako čtyřstěn. Na obrázku 3.34. vidíme dvanáctistěn v základní pozici a s naznačeným tahem A. Libovolnou z dvanácti vrstev můžeme otáčet vpravo nebo vlevo o 72°. Také tady tvoří prvky ve středech stěn souřadný systém, určující správné místo a orientaci pro každý pohyblivý prvek. Dvanáctistěn je hra nesouvislá, jednu orbitu tvoří třicet hranových prvků, druhou dvacet rohových. Je to hra úplná a s orientací.

Tahem A uděláme permutaci, která má jeden cyklus délky 5 na hranových kostičkách, druhý cyklus délky 5 na rohových kostičkách, a zbývající cykly mají délku 1. Stejné délky cyklů mají také všechny ostatní permuta-

ce, které uděláme všemi možnými tahy. Každý tah, a tedy také každý postup, udělá jak na hranových, tak na rohových prvcích pouze sudé permutace.

> Každá pozice na dvanáctistěnu, jejíž polohová permutace na hranových nebo na rohových prvcích je lichá, je neřešitelná.

Všechny ostatní pozice jsou srovnatelné, lze je dostat do pozice, ve které jsou všechny prvky na správných místech. Kvůli orientacím je mezi nimi stále ještě dost neřešitelných.



Obr. 3.34

Domino. Na dominu jsou dva různé typy tahů — otočení čtvercovou vrstvou a otočení některou ze čtyř

obdélníkových vrstev. Grafy permutací, které tyto tahy udělají, jsou na obrázku 3.19. Otočení čtvercovou vrstvou, část a), udělá sudou permutaci, která má dva cykly délky 4 a ostatní jednoprvkové. Otočení boční obdélníkovou vrstvou, část b), udělá permutaci lichou — má tři cykly délky 2. Na dominu tedy existují jak sudé, tak liché tahy, řešitelné pozice mohou být proto sudé i liché. Ve skutečnosti jsou řešitelné všechny pozice, ukážeme to rovněž v příští kapitole.

Krychle $2 \times 2 \times 2$. Na této krychli jsou liché tahy, každý udělá jeden čtyřcyklus — obrázek 3.20. Různými postupy můžeme proto udělat sudé i liché permutace a v příští kapitole ukážeme, že každá pozice na krychli $2 \times 2 \times 2$ je srovnatelná. Neřešitelné pozice ale existují, je to kvůli orientacím.

A nakonec ještě naposledy o neřešitelných pozicích na patnáctce.

Patnáctka. Na patnáctce jsou všechny tahy liché. Mění polohu pouhých dvou prvků, dělají transpozice. Chceme-li převést reklamní pozici 2.1. do základní pozice 1.11., musíme udělat nějaký speciální postup — začínáme a končíme prázdným místem v pravém dolním rohu. Trik se šachovnicí ukazuje, že každý speciální postup musí mít sudý počet tahů, začíná a končí prázdným místem stejné barvy. Každý speciální postup tak udělá permutaci, která je složením sudého počtu transpozic, a tedy sudá.

Uděláme-li nějaký speciální postup v liché reklamní pozici, dostaneme pozici, jejíž polohová permutace je složením liché (reklamní) a sudé (speciálním postupem udělané) permutace. Výsledek je proto zase lichá pozice, nikdy sudá základní. Reklamní pozice 2.1. je opravdu neřešitelná.

3.13. Pojem grupy. Symetrická a alternativní grupa. Zopakujme si vlastnosti skládání permutací na množině I, které jsme zjistili v odstavci 3.8.

a) **Asociativita.** Pro každé tři permutace p, q, r na množině I platí $(p \circ q) \circ r = p \circ (q \circ r)$.

b) **Existence neutrálního prvku.** Identická permutace n je neutrální vzhledem ke skládání permutací, složíme-li ji s nějakou permutací, tato permutace se nezmění. Platí $p \circ n = n \circ p = p$ pro každou permutaci p na I.

c) **Existence inverzního prvku.** Pro každou permutaci p existuje permutace p^{-1} taková, že $p \circ p^{-1} = p^{-1} \circ p = n$. Permutace p^{-1} se nazývá *inverzní permutace* k permutaci p.

Podobné vlastnosti má operace sčítání na množině všech celých čísel.

a) **Asociativita.** Pro každá tři celá čísla platí $(x + y) + z = x + (y + z)$.

b) **Existence neutrálního prvku.** Pro každé celé číslo x platí $x + 0 = 0 + x = x$, 0 je neutrální vzhledem ke sčítání.

c) **Existence inverzního prvku.** Pro každé celé číslo x platí $x + (-x) = (-x) + x = 0$, $-x$ je inverzní číslo k x.

Snadno ověříme, že také operace násobení na množině nenulových racionálních čísel má vlastnosti a), b) a c). Asociativita je známá, neutrální prvek je 1 a inverzní prvek k x je x^{-1}.

Jak vidět, operace, které každé dvojici prvků x, y nějaké množiny G přiřazují jednoznačně určený prvek

$x \circ y \in G$ a které mají vlastnosti a), b) a c), jsou v matematice časté a důležité. Byly proto pojmenovány zvláštním jménem.

Operaci, která každým dvěma prvkům nějaké množiny G přiřazuje jiný prvek této množiny, budeme obecně říkat *skládání* na množině G a její výsledek $x \circ y$ bude *složení* prvků x, $y \in G$. V konkrétním případě může být operací sčítání, násobení, nebo třeba skládání permutací.

Množina G spolu s operací skládání na G se nazývá *grupa*, jestliže splňuje tyto podmínky:

a) $(x \circ y) \circ z = x \circ (y \circ z)$ pro každé tři prvky x, y, $z \in G$,

b) existuje prvek $n \in G$ takový, že $x \circ n = n \circ x = x$ pro každý prvek $x \in G$, prvek n se nazývá *neutrální prvek* grupy G,

c) ke každému prvku $x \in G$ existuje prvek $x^{-1} \in G$ takový, že $x \circ x^{-1} = x^{-1} \circ x = n$, prvek x^{-1} se nazývá *inverzní prvek* k x.

Jinak řečeno, operace je asociativní, existuje neutrální prvek a ke každému prvku existuje prvek inverzní. Podmínkám a), b), c) se také říká *axiómy grupy*.

Známe už tři příklady grup. Množina S_I všech permutací na I spolu s operací skládání permutací je grupa. Budeme ji značit $\mathbf{S}_I$ a nazývat *symetrická grupa* na množině I. Také množina všech celých čísel spolu s operací sčítání je grupa — *aditivní grupa celých čísel*. Značit ji budeme $\mathbf{Z}$. Také množina nenulových racionálních čísel spolu s operací násobení je grupa. Je to *multiplikativní grupa racionálních čísel* a obvykle se označuje $\mathbf{Q}_0$.

Musíme zdůraznit, že grupa je vždy množina spolu s nějakou operací, není to ani jenom množina, ani jenom operace. Zatímco množina celých čísel s operací sčítání je grupa, stejná množina s operací násobení grupa není. Násobení je sice asociativní, neexistuje ale neutrální

prvek, kazí to 0. Množina nenulových celých čísel s operací násobení také není grupa. Násobení je asociativní a existuje i neutrální prvek 1, k číslu 2 však neexistuje prvek inverzní (1/2 není celé číslo, a nepatří tedy do Z). Jiné příklady jsou ve cvičení.

Cvičení 3.28. Které z následujících množin s příslušnými operacemi jsou grupy?

a) množina racionálních čísel s operací sčítání,

b) množina nenulových racionálních čísel s operací sčítání,

c) množina reálných čísel s operací násobení,

d) množina nenulových reálných čísel s operací násobení,

e) množina celých čísel s operací násobení,

f) množina komplexních čísel s operací násobení,

g) množina nenulových komplexních čísel s operací násobení,

h) množina komplexních čísel s operací sčítání.

Další příklad vysvětlíme podrobněji. Podle pravidla o paritě složení permutací je složení libovolných dvou sudých permutací zase sudá permutace. Pro každé tři sudé permutace p, q, r platí $(p \circ q) \circ r = p \circ (q \circ r)$, protože to platí pro libovolné tři permutace. Skládání permutací je proto asociativní operace na množině všech sudých permutací na I. Tuto množinu budeme značit A_I. Neutrální prvek také existuje, identická permutace je sudá, nemá žádný sudý cyklus. A protože inverzní permutace k sudé je také sudá — má cykly stejných délek — existuje ke každé permutaci z A_I inverzní prvek v A_I. Množina A_I všech sudých permutací spolu s operací skládání permutací tedy tvoří grupu. Tato grupa se nazývá *alternativní grupa* na množině I. Označovat ji budeme $\boldsymbol{A}_I$.

Význam asociativity. Skládání v grupě je definováno pouze pro dvojice prvků. Máme-li složit tři prvky x, y, z v tomto pořadí, musíme pomocí závorek určit, jaké dvojice postupně skládat. Můžeme to udělat dvěma způsoby: $(x \circ y) \circ z$ a $x \circ (y \circ z)$. Asociativita říká, že oba způsoby vedou ke stejnému výsledku, který označíme $x \circ y \circ z$. V případě čtyř prvků už je možností více.

Cvičení 3.29. Pomocí závorek určete všechny možné způsoby, jak složit v nějaké grupě čtyři prvky u, v, x, y v tomto pořadí. Vede to vždy ke stejnému výsledku?

Máme-li složit v nějaké grupě G m prvků $a_1, a_2, \ldots, \ldots, a_m$ v tomto pořadí, je možností ještě více. Z asociativity ale plyne, že všechny vedou ke stejnému výsledku. Dokážeme to teď indukcí podle počtu prvků, tj. podle m.

*Je-li $m = 3$, skládáme tři prvky, a rovnost $(a_1 \circ a_2) \circ a_3 = a_1 \circ (a_2 \circ a_3)$ plyne přímo z definice grupy, skládání je asociativní.

Předpokládejme nyní, že $m > 3$ a že všechny způsoby, jak spočítat složení méně než m prvků v daném pořadí, vedou ke stejnému výsledku. Znamená to, že každý výpočet složení libovolných prvků $b_1, b_2, \ldots, b_l$ v tomto pořadí dává stejný výsledek, který označíme $b_1 \circ b_2 \circ \ldots \circ b_l$. Počítáme-li nějak složení $a_1, a_2, \ldots, a_m$, v posledním kroku děláme výpočet $(a_1 \circ a_2 \circ \ldots \circ a_l) \circ (a_{l+1} \circ \ldots \circ a_m)$. V obou závorkách je složení méně než m prvků, můžeme proto použít indukční předpoklad, všechny možné výpočty vedou ke stejnému výsledku. Při jiném výpočtu složení všech m prvků počítáme v posledním kroku $(a_1 \circ a_2 \circ \ldots \circ a_k) \circ (a_{k+1} \circ \ldots \circ a_m)$. Pro výpočty v závorkách opět používáme indukční předpoklad. Pokud je $k = l$, oba výpočty vedou samozřejmě ke stejnému výsledku. Budeme předpokládat,

že třeba $k < l$. První závorku v prvním výpočtu ještě rozdělíme na $a_1 \circ a_2 \circ \ldots \circ a_l = (a_1 \circ a_2 \circ \ldots \circ a_k) \circ \circ (a_{k+1} \circ \ldots \circ a_l)$.

Prvním způsobem tak dostáváme výsledek

$$(a_1 \circ a_2 \circ \ldots \circ a_l) \circ (a_{l+1} \circ \ldots \circ a_m) = \\ = ((a_1 \circ a_2 \circ \ldots \circ a_k) \circ (a_{k+1} \circ \ldots \circ a_l)) \circ \\ \circ (a_{l+1} \circ \ldots \circ a_m).$$

Nyní použijeme-li asociativitu, rovná se to dále

$$(a_1 \circ a_2 \circ \ldots \circ a_k) \circ ((a_{k+1} \circ \ldots \circ a_l) \circ (a_{l+1} \circ \\ \circ \ldots \circ a_m)) = (a_1 \circ a_2 \circ \ldots \circ a_k) \circ (a_{k+1} \circ \ldots \circ \\ \circ a_m).$$

Na poslední řádce je ale poslední krok při výpočtu druhým způsobem. Oba výsledky se tak rovnají. Všechny možné způsoby výpočtu složení $a_1, a_2, \ldots a_m$ proto vedou ke stejnému výsledku, který označíme $a_1 \circ a_2 \circ \circ \ldots \circ a_m$.

Matematickou indukcí jsme tak dokázali, že při výpočtu složení libovolně mnoha prvků nějaké grupy v daném pořadí dostaneme všemi možnými způsoby vždy jeden a tentýž výsledek.

Zpětně jsme tím dokázali také vlastnost skládání permutací, kterou jsme uvedli v odstavci 3.8. a používali v odstavcích 3.10., 3.11. a 3.12. Nic než jednoduché vlastnosti skládání, dokázané už v odstavci 3.8., jsme k tomu nepotřebovali.

Vrátíme se ještě jednou k základním příkladům grup z počátku tohoto odstavce. Symetrická a alternativní grupa se od číselných grup $\boldsymbol{Z}$ a $\boldsymbol{Q}_0$ liší v jednom podstatném rysu. Existují dvojice sudých permutací p, q takové, že $p \circ q \neq q \circ p$. Každý snadno najde dvě takové permutace, pokud má I aspoň čtyři prvky. Na-

proti tomu $x + y = y + x$ pro libovolná dvě celá čísla a $xy = yx$ pro každá dvě nenulová racionální čísla. Budeme říkat, že grupa $\mathbf{G}$ na množině G je *komutativní*, jestliže $g \circ h = h \circ g$ pro každé dva prvky $g, h \in G$. Grupy $\mathbf{Z}$ a $\mathbf{Q}_0$ jsou komutativní, symetrická a alternativní grupa komutativní nejsou, pokud má množina I aspoň čtyři prvky.

A kolik je vlastně sudých permutací? Pro ty, kdo nezvládli cvičení 3.22., a zajímá je výsledek, teď dokážeme, že na každé množině I, která je konečná a má aspoň dva prvky, je sudých permutací přesně tolik, kolik je lichých.

Vybereme libovolné dva různé prvky $i, j \in I$ a transpozici $t = (i, j)$. Je-li p nějaká sudá permutace na I, pak $p \circ t$ je podle pravidla o paritě složení permutací lichá. Každé sudé permutaci p jsme tak přiřadili lichou permutaci $p \circ t$. Jsou-li p, q sudé permutace a $p \circ t = q \circ t$, pak také

$$(p \circ t) \circ t = (q \circ t) \circ t,$$

a tedy také

$$p \circ (t \circ t) = q \circ (t \circ t),$$

tj.

$$p = q.$$

Různým sudým permutacím proto odpovídají různé liché. Lichých permutací je tedy aspoň tolik, kolik je sudých. Abychom dokázali, že je jich stejně, musíme se přesvědčit o tom, že každá lichá permutace je přiřazena nějaké sudé. To je ale snadné. Je-li r lichá, pak $p = r \circ t$ je sudá, a této permutaci je přiřazena lichá permutace $p \circ t = (r \circ t) \circ t = r \circ (t \circ t) = r$. Sudých permutací je proto přesně tolik co lichých. A protože všech permutací na k-prvkové množině je $k!$ (cvičení 3.11.), je sudých permutací na k-prvkové množině $(1/2)\, k!$.

***3.14. Podgrupy. Lagrangeova věta.** Stejnou metodou teď dokážeme Lagrangeovu větu. Jako jeden z prvních výsledků rodící se teorie grup ji dokázal ještě v 18. století francouzský matematik J. L. Lagrange (1736 až 1813).

Dříve než ji zformulujeme a dokážeme, vysvětlíme si pořádně, co je to podgrupa. Každá grupa $\boldsymbol{G}$ je určena nějakou množinou G a operací, která každým dvěma prvkům $x, y \in G$ přiřazuje jejich složení $x \circ y \in G$. Je-li nyní H nějaká podmnožina G, je pro každé dva prvky $x, y \in H$ definované jejich složení (v grupě $\boldsymbol{G}$) $x \circ y$. Toto složení nemusí být samozřejmě prvkem H. Pokud ale je $x \circ y \in H$ pro libovolné dva prvky $x, y \in H$, můžeme se ptát, je-li H spolu s operací skládání indukovanou takto z grupy $\boldsymbol{G}$ také grupa. Jaké podmínky musí množina H splňovat? Jednu jsme si už řekli. Je-li $x, y \in H$, musí být také $x \circ y \in H$. Operace skládání na množině H je potom asociativní, rovnost $(x \circ y) \circ z = x \circ (y \circ z)$ platí pro každé tři prvky $x, y, z \in H$, protože platí také v grupě $\boldsymbol{G}$. Je-li navíc neutrální prvek n grupy $\boldsymbol{G}$ v množině H a pro každý prvek $x \in H$ je také inverzní prvek x^{-1} v H, splňuje množina H spolu s operací skládání indukovanou z grupy $\boldsymbol{G}$ všechny axiómy grupy, a je to tedy také grupa. Říkáme, že je to *podgrupa* grupy G.

Několik příkladů. Aditivní grupa celých čísel $\boldsymbol{Z}$ je podgrupou aditivní grupy racionálních čísel (tj. grupy všech racionálních čísel s operací sčítání).

Množina $\{1, -1\}$ spolu s operací násobení je grupa (ověřte to!) a je to podgrupa multiplikativní grupy nenulových racionálních čísel $\boldsymbol{Q}_0$.

Multiplikativní grupa racionálních čísel $\boldsymbol{Q}_0$ je grupa, není to ale podgrupa aditivní grupy racionálních čísel. Nenulová racionální čísla sice tvoří podmnožinu množi-

ny všech racionálních čísel, operace jsou ale definovány různě; 2.3 (v grupě $\mathbf{Q}_0$) se nerovná 2 + 3 (v aditivní grupě racionálních čísel).

Alternativní grupa $\boldsymbol{A}_I$ je podgrupou symetrické grupy $\boldsymbol{S}_I$.

A teď k Langrangeově větě.

Lagrangeova věta. *Je-li* $\boldsymbol{G}$ *konečná grupa a* $\boldsymbol{H}$ *její podgrupa, pak počet prvků grupy* $\boldsymbol{H}$ *je dělitelem počtu prvků grupy* $\boldsymbol{G}$.

Důkaz. Označíme G množinu, na které je definována grupa $\boldsymbol{G}$, a H množinu, na které je definována grupa $\boldsymbol{H}$. Protože je $\boldsymbol{H}$ podgrupa $\boldsymbol{G}$, platí $H \subseteq G$. Můžeme předpokládat, že množina H má k prvků, a označíme je $h_1, h_2, \ldots, h_k$.

Je-li $H = G$, mají obě grupy stejný počet prvků. Jestliže $H \neq G$, existuje nějaký prvek $x_2 \in G$, který neleží v podmnožině H. Symbolem Hx_2 označíme množinu všech prvků tvaru $h \circ x_2$, kde $h \in H$. Všechny prvky $h \circ x_2$ leží v G. Ukážeme, že množiny H a Hx_2 mají stejný počet prvků.

Jsou-li h_i a h_j dva prvky H a $h_i \circ x_2 = h_j \circ x_2$, pak také $(h_i \circ x_2) \circ x_2^{-1} = (h_j \circ x_2) \circ x_2^{-1}$. Z asociativity pak plyne $h_i \circ (x_2 \circ x_2^{-1}) = h_j \circ (x_2 \circ x_2^{-1})$. Protože $x_2 \circ x_2^{-1} = n$, platí $h_i \circ n = h_j \circ n$, tj. $h_i = h_j$.

Všechny prvky $h_1 \circ x_2$, $h_2 \circ x_2$, $\ldots$, $h_k \circ x_2$ množiny Hx_2 jsou proto různé. A protože žádný jiný prvek v Hx_2 ležet nemůže, má Hx_2 stejný počet prvků jako H, tj. k.

Množiny H a Hx_2 jsou navíc disjunktní. Kdyby totiž existoval prvek $g \in H \cap Hx_2$, bylo by $g \in H$ a současně $g = h \circ x_2$ pro nějaký prvek $h \in H$. Potom ale $h^{-1} \circ g = x_2$. Protože $g, h \in H$, je také $h^{-1} \in H$ a $h^{-1} \circ g \in H$. Prvek $x_2 = h^{-1} \circ g$ by musel ležet v množině H, což je ve sporu s tím, jak jsme ho vybrali.

Množiny H a Hx_2 jsou proto opravdu disjunktní. Obě obsahují k prvků a jsou podmnožinami G. Množina G tak obsahuje aspoň $2k$ různých prvků:

$$H: \quad h_1, h_2, h_3, \ldots, h_k,$$
$$Hx_2: h_1 \circ x_2, h_2 \circ x_2, \ldots, h_k \circ x_2.$$

Je-li $G = H \cup Hx_2$, obsahuje G přesně $2k$ prvků. Je-li $G \neq H \cup Hx_2$, existuje prvek $x_3 \in G$, který v $H \cup Hx_2$ neleží. Symbolem Hx_3 označíme množinu všech prvků tvaru $h \circ x_3$, kde $h \in H$. Všechny tyto prvky opět leží v G. Stejně jako v případě množiny Hx_2 ukážeme, že Hx_3 obsahuje přesně k prvků a je disjunktní s H. Navíc je Hx_3 také disjunktní s Hx_2. Kdyby totiž existoval prvek $g \in Hx_3 \cap Hx_2$, platilo by $g = h_i \circ x_3$ a $g = h_j \circ x_2$ pro nějaké prvky $h_i, h_j \in H$. Z rovnosti $h_i \circ x_3 = h_j \circ x_2$ plyne $x_3 = h_i^{-1} \circ (h_j \circ x_2) = (h_i^{-1} \circ h_j) \circ x_2$. $\mathbf{H}$ je ale podgrupa $\mathbf{G}$, proto $h_i^{-1} \circ h_j \in H$, a tedy $x_3 \in Hx_2$, což je opět ve sporu s naším výběrem $x_3 \notin H \cup Hx_2$. Proto je Hx_2 disjunktní s Hx_3. Grupa $\mathbf{G}$ tak obsahuje aspoň $3k$ různých prvků

$$H: \quad h_1, h_2, h_3, \ldots, h_k,$$
$$Hx_2: h_1 \circ x_2, h_2 \circ x_2, \ldots, h_k \circ x_2,$$
$$Hx_3: h_1 \circ x_3, h_2 \circ x_3, \ldots, h_k \circ x_3.$$

Jestliže je nyní $G = H \cup Hx_2 \cup Hx_3$, má $\mathbf{G}$ přesně $3k$ prvků. Je-li $G \neq H \cup Hx_2 \cup Hx_3$, vybereme libovolný prvek x_4, který v $H \cup Hx_2 \cup Hx_3$ neleží, a celý postup znovu opakujeme. Označíme Hx_4 množinu všech prvků tvaru $h \circ x_4$, kde $h \in H$. Množina Hx_4 obsahuje přesně k prvků a je disjunktní s $H \cup Hx_2 \cup Hx_3$. Množina G tak má aspoň $4k$ prvků. Takto pokračujeme dále, až nakonec po nějakých l krocích dostaneme úplný seznam všech prvků grupy $\mathbf{G}$:

$$
\begin{aligned}
&H\colon\ h_1, h_2, h_3, \ldots, h_k,\\
&Hx_2\colon h_1 \circ x_2, h_2 \circ x_2, \ldots, h_k \circ x_2,\\
&Hx_3\colon h_1 \circ x_3, h_2 \circ x_3, \ldots, h_k \circ x_3,\\
&\vdots\\
&Hx_l\colon h_1 \circ x_l, h_2 \circ x_l, \ldots, h_k \circ x_l.
\end{aligned}
$$

Celkový počet prvků množiny G je tedy kl. Lagrangeova věta je tím dokázána.

Počet prvků grupy $\boldsymbol{G}$ se nazývá *řád grupy* $\boldsymbol{G}$ a značí se $|\boldsymbol{G}|$. Řád symetrické grupy na k-prvkové množině je tedy $k!$, alternativní grupy na stejné množině pak $(1/2)k!$. Lagrangeovu větu můžeme formulovat také takto:

Je-li $\boldsymbol{G}$ *konečná grupa a* $\boldsymbol{H}$ *její podgrupa, pak číslo* $|\boldsymbol{G}|/|\boldsymbol{H}|$ *je celé.*

Toto číslo se nazývá index podgrupy $\boldsymbol{H}$ v grupě $\boldsymbol{G}$. Index alternativní grupy $\boldsymbol{A}_l$ v symetrické grupě $\boldsymbol{S}_l$ je tedy 2.

***3.15. Grupy na hračkách.** Na každém úplném hlavolamu můžeme objevit řadu různých grup. V tomto odstavci si ukážeme dvě, grupu polohových permutací a grupu redukovaných postupů. V páté kapitole ukážeme další dvě, grupu řešitelných pozic a grupu všech možných pozic.

Grupa polohových permutací. Přesněji bychom ji měli nazývat grupa všech permutací, které můžeme udělat nějakými postupy. V této grupě leží všechny permutace p na množině I pohyblivých prvků, které můžeme vyjádřit ve tvaru $p = \boldsymbol{PV}$. Operací bude opět skládání

permutací. Grupa polohových permutací na nějakém hlavolamu je proto podgrupa grupy všech permutací na množině I všech pohyblivých prvků.

Musíme ověřit, že to opravdu podgrupa symetrické grupy je. Jestliže permutaci p uděláme postupem P a permutaci q postupem Q, pak jejich složení $p \circ q$ uděláme složeným postupem PQ — odstavec 3.7. Inverzní permutaci p^{-1} uděláme inverzním postupem P^{-1}, také podle výsledků z odstavce 3.7. Zbývá nějak udělat identickou permutaci n. To je ale jednoduché, nemusíme dělat vůbec nic, stačí na to neutrální postup N.

Grupa redukovaných postupů. Redukované postupy a jejich skládání jsme definovali už v první kapitole. Nyní dokážeme, že množina všech redukovaných postupů spolu s operací redukovaného skládání tvoří grupu — grupu redukovaných postupů na nějakém úplném hlavolamu. Musíme ověřit axiómy grupy.

a) Jsou-li P, Q, R tři redukované postupy, pak oba postupy $(P \circ Q) \circ R$ a $P \circ (Q \circ R)$ dostaneme redukováním téhož postupu PQR. V prvém případě redukujeme napřed začátek PQ a potom připojíme R, ve druhém případě naopak začínáme od konce redukcí QR a pak přidáme P. Z jednoznačnosti redukce postupů dokázané v odstavci 1.10. plyne, že oběma způsoby dostaneme stejný výsledek, $(P \circ Q) \circ R = P \circ (Q \circ R)$.

b) Neutrální prvek existuje, je jím neutrální postup N, $P \circ N = N \circ P = P$ pro každý redukovaný postup P.

c) Inverzní postup P^{-1} k redukovanému postupu P je rovněž redukovaný. Je-li $P = X_1 X_2 \ldots X_k$, pak $P^{-1} = X_k^{-1} X_{k-1}^{-1} \ldots X_1^{-1}$. Při redukci postupu $PP^{-1} = X_1 X_2 \ldots X_k X_k^{-1} X_{k-1}^{-1} \ldots X_1^{-1}$ můžeme vynechávat dva prostřední tahy tak dlouho, až nic nezbyde, tj. až zbyde neutrální postup N. Proto $P \circ P^{-1} = N$. Ze stejného důvodu také platí $P^{-1} \circ P = N$.

Našli jsme tak dvě různé grupy na každém hlavolamu. První z nich je konečná grupa permutací, druhá pak nekonečná grupa postupů. Mezi oběma je úzký vztah, který si vysvětlíme v příštím odstavci.

***3.16. Homomorfismus a izomorfismus grup.** V odstavci 3.11. jsme dokázali pravidlo o paritě složení permutací. Toto pravidlo lze také vyjádřit způsobem na první pohled zcela odlišným.

Setkali jsme se už s grupou $\boldsymbol{T}$, kterou tvoří množina $\{1, -1\}$ spolu s operací násobení. Každé permutaci na množině I teď přiřadíme jedno z čísel 1 a -1:

je-li p sudá permutace, pak $p\boldsymbol{W} = 1$,

je-li p lichá permutace, pak $p\boldsymbol{W} = -1$.

Definovali jsme tak jakési zobrazení z množiny S_I všech permutací na I do množiny $\{1, -1\}$. Zobrazení $\boldsymbol{W}$ vystihuje jistou souvislost mezi symetrickou grupou $\boldsymbol{S}_I$ a grupou $\boldsymbol{T}$. Má následující vlastnosti:

a) $(p \circ q)\,\boldsymbol{W} = (p\boldsymbol{W})\,(q\boldsymbol{W})$,

to je vlastně pravidlo o paritě složení permutací. Složení dvou sudých nebo dvou lichých permutací je permutace sudá, složení sudé s lichou je permutace lichá.

b) $n\boldsymbol{W} = 1$,

identická permutace je sudá.

c) Inverzní permutace k sudé je sudá a k liché lichá, platí proto

$$(p\boldsymbol{W})\,(p^{-1}\boldsymbol{W}) = 1.$$

Můžeme to vyjádřit také jinak, inverzní prvek k $p\boldsymbol{W}$

v grupě $\boldsymbol{T}$, to je $(p\boldsymbol{W})^{-1}$, se rovná $(p^{-1})\,\boldsymbol{W}$, neboli

$$(p\boldsymbol{W})^{-1} = (p^{-1})\,\boldsymbol{W}$$

pro každou permutaci p.

Podmínky a), b) a c) ukazují, že zobrazení $\boldsymbol{W}$ těsně souvisí se strukturou grup $\boldsymbol{S}_I$ a $\boldsymbol{T}$. Podmínka a) říká, že $\boldsymbol{W}$ zachovává operace skládání. Součin $p\boldsymbol{W}.q\boldsymbol{W}$ můžeme spočítat také tak, že napřed složíme p s q v grupě $\boldsymbol{S}_I$, a výsledek $p \circ q$ pak zobrazíme do grupy $\boldsymbol{T}$, $(p \circ q)\,\boldsymbol{W} = p\boldsymbol{W}.q\boldsymbol{W}$. Podmínka b) říká, že $\boldsymbol{W}$ zachovává také neutrální prvek, obraz $n\boldsymbol{W}$ neutrálního prvku grupy $\boldsymbol{S}_I$ je neutrální prvek grupy $\boldsymbol{T}$. A podmínka c) je o zachovávání inverzního prvku, obraz $p^{-1}\boldsymbol{W}$ inverzního prvku k p je inverzní k prvku $p\boldsymbol{W}$ v grupě $\boldsymbol{T}$, $p^{-1}\boldsymbol{W} = (p\boldsymbol{W})^{-1}$.

Struktura dvouprvkové grupy $\boldsymbol{T}$ se prostřednictvím zobrazení $\boldsymbol{W}$ odráží v symetrické grupě $\boldsymbol{S}_I$, a proto platí pravidlo o paritě složení permutací.

Zobrazení mezi grupami s vlastnostmi a), b) a c) tak umožňují porovnávat různé grupy, nakolik jsou podobné nebo odlišné.

Jsou-li $\boldsymbol{G}$ a $\boldsymbol{H}$ dvě grupy definované na množinách G a H, pak zobrazení $\boldsymbol{W}$: $G \to H$ se nazývá *homomorfismus grup* $\boldsymbol{G}$ a $\boldsymbol{H}$, jestliže splňuje podmínky

a) $(g \circ h)\,\boldsymbol{W} = (g\boldsymbol{W}) \circ (h\boldsymbol{W})$ pro každé dva prvky $g, h \in G$,

b) je-li n neutrální prvek grupy $\boldsymbol{G}$, pak $n\boldsymbol{W}$ je neutrální prvek grupy $\boldsymbol{H}$,

c) $g^{-1}\boldsymbol{W} = (g\boldsymbol{W})^{-1}$ pro všechny prvky g grupy $\boldsymbol{G}$.

To, že $\boldsymbol{W}$ je homomorfismus grup $\boldsymbol{G}$ a $\boldsymbol{H}$, zapisujeme $\boldsymbol{W} : \boldsymbol{G} \to \boldsymbol{H}$. Je-li zobrazení $\boldsymbol{W}$ navíc vzájemně jednoznačné, říkáme, že $\boldsymbol{W}$ je *izomorfismus grup* $\boldsymbol{G}$ a $\boldsymbol{H}$, a zapisujeme to $\boldsymbol{W} : \boldsymbol{G} \leftrightarrow \boldsymbol{H}$. Grupy $\boldsymbol{G}$ a $\boldsymbol{H}$ jsou v tom případě *izomorfní*.

Izomorfní grupy jsou v podstatě stejné, liší se pouze ve jménech prvků množin G a H. V odstavci 3.18. uká-

žeme, že každá grupa je izomorfní nějaké grupě permutací, každou grupu si můžeme představit jako grupu permutací.

Nyní jeden příklad homomorfismu na hlavolamech. V minulém odstavci jsme si ukázali dvě grupy na každém úplném hlavolamu, grupu redukovaných postupů a grupu polohových permutací. V předchozím textu jsme často používali zobrazení V, jež každému redukovanému postupu P přiřazuje permutaci $p = PV$, kterou postup P udělá na množině I pohyblivých prvků. Ukážeme, že zobrazení V je homomorfismus grup. Musíme ověřit, že má vlastnosti a), b) a c).

a) V odstavci 3.7. jsme ukázali, že složeným postupem PQ uděláme permutaci, která je složením permutací PV a QV, tj. $(PQ)V = PV \circ QV$. Postup PQ ale nemusí být redukovaný, nerovná se vždy redukovanému složení $P \circ Q$. Jestliže ale v nějakém postupu vynecháme dvojici sousedních inverzních tahů, výsledná pozice se nezmění. Nezmění se proto ani její polohová permutace. Redukcí $P \circ Q$ postupu PQ proto udělám stejnou permutaci jako postupem PQ. A tak $(P \circ Q)V = (PQ)V = (PV) \circ (QV)$.

b) Neutrálním postupem N nic nezměníme, hračka zůstane v základní pozici n, proto $NV = n$.

c) Inverzním postupem P^{-1} uděláme permutaci inverzní k $p = PV$, dokázali jsme to také v odstavci 3.7. Platí proto

$$P^{-1}V = (PV)^{-1}.$$

Zobrazení V je tedy homomorfismus grup, který ukazuje, jak spolu souvisí postupy na hlavolamu a permutace, které jimi uděláme.

3.17. Sylowovy věty. Každá grupa G má určitě aspoň dvě podgrupy. Jednu tvoří grupa G samotná

a druhou jednoprvková množina $\{n\}$, obsahující neutrální prvek G spolu s operací $n \circ n = n$. Tyto podgrupy nejsou příliš zajímavé, říká se jim *nevlastní podgrupy grupy* G. Všem ostatním podgrupám říkáme *vlastní*. Jaké další podgrupy G obsahuje? Část odpovědi známe už z odstavce 3.14. Lagrangeova věta říká, že řád každé podgrupy H grupy G musí dělit řád grupy G. Pokud je řád $|G|$ prvočíslo, nemůže G žádné další podgrupy kromě nevlastních obsahovat. Pokud ale řád G není prvočíslo, Lagrangeova věta o existenci dalších podgrup nic neříká, a vyvolává tak řadu dalších otázek:

1. Existuje pro každého dělitele k řádu grupy G podgrupa, která má přesně k prvků?
2. Pokud ne, pro které dělitele k čísla $|G|$ určitě existují podgrupy řádu k?
3. Pokud existují podgrupy řádu k, kolik takových podgrup G obsahuje?

Tyto otázky byly podrobně zkoumány v 19. století a výzkum vyvrcholil v práci německého matematika L. Sylowa v roce 1872. Sylow dokázal řadu hlubokých tvrzení o existenci, počtu a vzájemné poloze podgrup v konečných grupách. Tyto výsledky patří v současné době mezi základní poznatky teorie konečných grup a jsou shrnovány pod společný název Sylowovy věty. Pro zajímavost uvedeme nejjednodušší z nich.

Sylowova věta. *Je-li G konečná grupa, p prvočíslo a i přirozené číslo takové, že p^i dělí řád grupy G, pak existuje podgrupa H grupy G, která obsahuje přesně p^i prvků.*

Z této věty plyne, že každá konečná grupa G, jejíž řád není prvočíslo, obsahuje vlastní podgrupu. Existuje totiž prvočíslo p, které dělí $|G|$, a G musí obsahovat podgrupu řádu p.

3.18. Cayleyho reprezentace. Jako poněkud pokročilejší ukázku práce s axiómy grupy teď dokážeme, že každá grupa je izomorfní nějaké grupě permutací. Nebo jinak řečeno, každou grupu si lze představit (reprezentovat) jako nějakou grupu permutací. Autorem tohoto klasického výsledku teorie grup je anglický matematik A. C. Cayley (1821—1895), a reprezentace grupy jako grupy permutací, kterou ukážeme, se nazývá *Cayleyho reprezentace.*

Vezmeme si tedy nějakou grupu $\boldsymbol{G}$. Množinu jejích prvků budeme označovat jako vždy G a operaci skládání $\circ$. Na množině G sestrojíme jakousi permutační grupu a ukážeme, že je izomorfní grupě $\boldsymbol{G}$.

Každému prvku $a \in G$ musíme přiřadit nějakou permutaci p_a. Tuto permutaci definujeme na množině G předpisem

$$xp_a = x \circ a \text{ pro každý prvek } x \in G.$$

Nejdříve musíme dokázat, že zobrazení p_a je skutečně permutace, vzájemně jednoznačné zobrazení, na množině G. Každému prvku $x \in G$ je přiřazený přesně jeden prvek $xp_a = x \circ a$. Jsou-li x, y dva prvky G a $xp_a = yp_a$, pak podle definice zobrazení p_a platí $x \circ a = y \circ a$. Poslední rovnost složíme s prvkem a^{-1} zprava a použijeme asociativitu. Dostáváme tak postupně

$$\begin{aligned}(x \circ a) \circ a^{-1} &= (y \circ a) \circ a^{-1},\\ x \circ (a \circ a^{-1}) &= y \circ (a \circ a^{-1}),\\ x \circ n &= y \circ n,\\ x &= y.\end{aligned}$$

Různé prvky G se proto zobrazují do různých prvků. Je-li $z \in G$ libovolný prvek, pak $(z \circ a^{-1})\, p_a = (z \circ a^{-1}) \circ a = z \circ (a^{-1} \circ a) = z$. Tím je dokázáno, že každý

prvek $z \in G$ je přiřazen právě jednomu prvku G, p_a je opravdu permutace.

Teď dokážeme několik vlastností permutací p_a.

a) Jsou-li a, b prvky G, pak složení permutací $p_a \circ p_b$ má tuto vlastnost: pro každé $x \in G$ platí

$$x(p_a \circ p_b) = (xp_a)\, p_b = (x \circ a)\, p_b = (x \circ a) \circ b = \\ = x \circ (a \circ b) = xp_{a \circ b}.$$

To znamená, že $p_a \circ p_b = p_{a \circ b}$. Označíme-li symbolem H množinu všech permutací tvaru p_a pro nějaké $a \in G$, pak složení $p_a \circ p_b$ libovolných dvou permutací p_a, $p_b \in H$ patří také do H, rovná se $p_{a \circ b}$. Můžeme se proto ptát, tvoří-li H spolu s operací skládání permutací grupu, podgrupu symetrické grupy $\boldsymbol{S}_G$. K tomu potřebujeme zjistit, zda H obsahuje identickou permutaci na G a inverzní permutace.

Jak vypadá permutace p_n, určená neutrálním prvkem n grupy $\boldsymbol{G}$? Pro každé $x \in G$ platí $xp_n = x \circ n = x$. To znamená, že p_n je identická permutace na G.

A je-li $p_a \in H$, pak pro permutaci $p_{a^{-1}}$ platí $x(p_a \circ p_{a^{-1}}) = xp_{a \circ a^{-1}} = xp_n = x$ a také $x(p_{a^{-1}} \circ p_a) = xp_{a^{-1} \circ a} = xp_n = x$ pro každé $x \in G$. Permutace $p_{a^{-1}}$ je proto inverzní k p_a. Množina H spolu s operací skládání permutací je tedy grupa, budeme ji dále označovat $\boldsymbol{H}$.

Grupa permutací $\boldsymbol{H}$ je těsně spjata s grupou $\boldsymbol{G}$, a dokážeme teď, že je s ní izomorfní. Definujeme zobrazení $\boldsymbol{W} : G \to H$ předpisem

$$a\boldsymbol{W} = p_a.$$

Víme, že

a) $(a \circ b)\, \boldsymbol{W} = p_{a \circ b} = p_a \circ p_b = (a\boldsymbol{W}) \circ (b\boldsymbol{W})$,

b) $n\boldsymbol{W} = p_n$ — identická permutace na G a neutrální prvek grupy $\boldsymbol{H}$,

c) $a^{-1}\boldsymbol{W} = p_{a^{-1}} = (p_a)^{-1} = (a\boldsymbol{W})^{-1}$.

Ověřili jsme tak vlastnosti z definice homomorfismu grup, grupy G a H jsou homomorfní. Abychom ukázali, že jsou izomorfní, musíme ověřit, že zobrazení W je vzájemně jednoznačné. Každá permutace $p_a \in H$ je přiřazena prvku $a \in G$, zbývá dokázat, že různým prvkům b, c nemůže být přiřazena stejná permutace z H. Platí ale $np_b = b \neq c = np_c$, permutace p_b a p_c jsou tedy různé. Zobrazení $W : G \to H$ je proto opravdu izomorfismus grup.

3.19. Volné grupy. V první kapitole jsme se podrobně zabývali postupy a skládáním postupů na úplných hrách s vlastností inverze. Názvy tah, postup, složení postupů jsme volili tak, aby bezprostředně souvisely s řešením hlavolamů. V odstavci 3.15. jsme ukázali, že množina všech redukovaných postupů spolu s operací redukovaného skládání tvoří grupu — grupu redukovaných postupů. Tato grupa je speciální případ důležité teoretické konstrukce používané v teorii grup. Pro úplnost nyní uvedeme tuto konstrukci s matematickou terminologií. Následující úvahy jsou analogické úvahám, které jsme dělali o postupech a redukovaných postupech v první kapitole a v odstavci 3.15, a jejich důkazy jsou proto ponechány jako poslední cvičení ke třetí kapitole.

a) Uvažujme nějakou množinu A, její prvky jsou $a_1, a_2, \ldots, a_k$. Budeme si představovat, že A je jakási abeceda a že z jejích prvků můžeme sestavovat nějaká slova. První pravidlo říká, že ke každému prvku a_i můžeme udělat inverzní prvek a_i^{-1} a že všechny prvky $a_1, a_2, \ldots, a_k$ a prvky inverzní $a_1^{-1}, a_2^{-1}, \ldots, a_k^{-1}$ jsou navzájem různé.

b) Libovolná posloupnost z prvků $a_1, a_2, \ldots, a_k, a_1^{-1}, \ldots, a_k^{-1}$ se nazývá *slovo nad abecedou* A. Tak třeba

$a_2a_1a_3a_1^{-1}a_2a_2$ je slovo nad A. Speciální slovo je posloupnost neobsahující žádný prvek, ta se nazývá *prázdné slovo*.

c) Slovo, ve kterém se nevyskytuje žádná dvojice sousedních inverzních prvků $a_ia_i^{-1}$ nebo $a_i^{-1}a_i$, se nazývá *redukované slovo*. Každé slovo můžeme redukovat postupným vynecháváním sousedních dvojic tvaru $a_ia_i^{-1}$ nebo $a_i^{-1}a_i$, až dostaneme redukované slovo. Stejně jako v odstavci 1.10. můžeme dokázat, že libovolnou redukcí nějakého slova dostaneme vždy stejné redukované slovo.

d) Z každých dvou slov můžeme vytvořit slovo nové tak, že příslušné posloupnosti napíšeme po sobě. Takto vytvořené slovo se nazývá *složení* původních slov. Redukce složení dvou slov se nazývá *redukované složení*, nebo také *součin* těchto slov.

e) Množina všech redukovaných slov s operací redukovaného složení (součinu) slov je grupa. Tato grupa se nazývá *volná grupa* nad abecedou A.

f) Vrátíme-li se zpět ke grupám redukovaných postupů na úplných hlavolamech s vlastností inverze, vidíme, že jde vždy o volné grupy nad nějakou abecedou. Touto abecedou je vždy nějaká množina tahů. Tak třeba u Rubikovy krychle je to množina všech otočení krajními vrstvami *vpravo* o 90°. Tato otočení jsme označovali stejným písmenem jako příslušnou stěnu, můžeme proto také říct, že grupa redukovaných postupů na Rubikově krychli je volná grupa nad abecedou stěn. Abeceda má v tomto případě šest prvků. Podobně grupa redukovaných postupů na dvanáctistěnu je volná grupa nad dvanáctiprvkovou abecedou všech stěn, na čtyřstěnu má abeceda čtyři prvky. Také na kosé krychli je grupa redukovaných postupů volná grupa nad čtyřprvkovou abecedou, na uších má abeceda dva prvky.