Zadania

1. (1 bod) Každá konečná pologrupa $(P, *)$ obsahuje idempotentný prvok. (Teda prvok s vlastnosťou $x * x = x$.)

2. ($4\times 0{,}5$bodu) Nech G je grupa. Pre podmnožiny $A, B \subseteq G$ označíme $AB = \{ab; a \in A, b \in B\}$.
   a) Nech A a B sú podgrupy G. Dokážte, že AB je podgrupa G práve vtedy, keď $AB = BA$.
   b) Nájdite príklad grupy G a jej podgrúp A a B takých, že AB nie je podgrupa G.
   c) Ak A, B sú konečné podgrupy G, tak $|AB|.|A \cap B| = |A|.|B|$.
   d) Nech A, B, C sú podgrupy také, že $A \subseteq C \subseteq AB$. Dokážte $C = (AB) \cap (AC) = A(B \cap C)$.

3. (1bod) Dokážte, že grupa A_4 párnych permutácií 4-prvkovej množiny nemá žiadnu 6-prvkovú podgrupu. (Kontrapríklad ukazujúci, že neplatí obrátenie Lagrangeovej vety.)

4. (1 bod, ak určíte aspoň počet prvkov tejto grupy, je to 1/4 bodu.) Dokážte, že grupa všetkých symetrií kocky, ktoré zachovávajú orientáciu,[1] je izomorfná grupe S_4.

5. (2 body. Určenie počtu prvkov = 1/2 bodu.) Je grupa všetkých symetrií dvadsaťstena (ikosaédra), ktoré zachovávajú orientáciu, izomorfná niektorej z grúp S_5, A_5, A_6? [2]

6. (1 bod) Nech p je prvočíslo. Dokážte, že až na izomorfizmus existujú práve 2 grupy, ktoré majú p^2 prvkov a že obe tieto grupy sú komutatívne.[3]

7. (1 bod) Dokážte, že alternujúca grupa A_n je jedinou podgrupou S_n indexu 2. Nájdite príklad grupy, ktorá má viac než jednu podgrupu indexu 2.

Riešenia

1. (M. Adamčík, V. Bachratá, J. Nižňanský, D. Švec) Najprv ukážme, že v P existuje konečný počet prvkov $a_1, \dots, a_n$ tak, že

$$a_1a_1 = a_2, a_2a_2 = a_3, \dots, a_{n-1}a_{n-1} = a_n \text{ a } a_na_n = a_1.$$

Ak totiž zoberieme ľubovoľný prvok za x_1 a indukciou definujeme $x_{n+1} = x_nx_n$, raz sa nejaký prvok musí zopakovať (pretože máme len konečne veľa prvkov). Prvý prvok, ktorý sa zopakuje, môžeme zobrať za a_1.

Ak máme prvky $a_1, \dots, a_n$ s vlastnosťami uvedenými hore, tak $x = a_1 \dots a_n$ je idempotent. Stačí si uvedomiť, že tieto prvky komutujú – všetky sú totiž mocniny a_1 – a

$$(a_1 \dots a_n)(a_1 \dots a_n) = (a_1a_1)(a_2a_2)\dots(a_na_n) = a_2 \dots a_na_1 = a_1a_2 \dots a_n,$$

[1] `http://en.wikipedia.org/wiki/Rigid_motion` – lepšie to do Slovenčiny preložiť neviem

[2] Ak sami vymyslíte a dokážete ďalšiu vetu typu: (niektoré) symetrie pravidelného m-stena tvoria grupu izomorfnú s S_k (alebo A_k), uznám to ako prémiu za 1 bod.

[3] Táto úloha je podstatne ťažšia než som si myslel, keď som ju zadával.

čiže skutočne platí $x = xx$.

Iné riešenie: Zvoľme si ľubovoľné $x \in P$. Uvažujme prvky $x, x^2, x^4, \dots, x^{2^k}, \dots$ Keďže pologrupa P je konečná, určite sa raz začnú opakovať, pre nejaké k a $l > 0$ máme teda:

$$x^{2^k} = x^{2^{k+l}}.$$

a) $l = 1 \Rightarrow x^{2^k}$ je idempotent.
b) $l > 1 \Rightarrow$ máme $x^a = x^b$, pričom $b > 2a$. Prenásobíme túto rovnosť x^{b-2a} a dostaneme $x^{b-a} = x^{2b-2a}$, čiže x^{b-a} je idempotent. (Tu je dôležité, že $b - 2a$ je kladné číslo – v pologrupe nemáme definované mocninu daného prvku pre záporné exponenty.)

2. (J. Nižňanský, čiastočné riešenie: J. Székely)

a) AB je podgrupa $\Leftrightarrow AB = BA$

$\boxed{\Rightarrow}$ Najprv ukážeme $BA \subseteq AB$. Nech $x = ba$, kde $b \in B$ a $a \in A$. Potom $(ba)^{-1} = a^{-1}b^{-1} \in AB$ a pretože AB je grupa aj $((ba)^{-1})^{-1} = ba \in AB$.

Ešte treba dokázať $AB \subseteq BA$. Nech $x \in AB$. Pretože AB je grupa, aj $x^{-1} = \in AB$, čiže $x^{-1} = ab$ pre nejaké $a \in A$, $b \in B$. To znamená, že $x = ab^{-1} = b^{-1}a^{-1} \in BA$.

$\boxed{\Leftarrow}$ Nech $AB = BA$. Chceme ukázať, že je to podgrupa G. Zrejme $e = e.e \in AB$. Ak $x, y \in AB$, tak $x = ab$ a $y = a'b'$ pre nejaké $a, a' \in A$ a $b, b' \in B$. To znamená, že $xy = a(ba')b'$. Pretože $ba' \in BA = AB$, aj prvok ba' vieme dostať ako $ba' = a''b''$ pre nejaké $a'' \in A$, $b'' \in B$, čiže

$$xy = (aa'')(bb'') \in AB.$$

Ak $x \in AB$, tak $x = ab$ pre nejaké $a \in A$, $b \in B$, ale potom aj $x^{-1} = b^{-1}a^{-1} \in BA = AB$.

b) Zoberme podgrupy $A = \{id, (12)\}$ a $B = \{id, (23)\}$ grupy S_3. Potom $AB = \{id, (12), (23), (123)\}$, ale $(23)(13) = (132) \notin AB$, teda AB nie je grupa.

c) Stačí ukázať, že všetky vyjadrenie toho istého prvku $ab \in AB$ ako súčinu $a'b'$, kde $a' \in A$, $b' \in B$ sú tvaru $axx^{-1}b$, kde $x \in A \cap B$. (Potom počet možných dvojíc $(a, b) \in A \times B$) treba vydeliť práve počtom prvkov $A \cap B$, aby sme dostali počet prvkov množiny $A.B$.) Lenže ak $ab = a'b'$, tak $x = a^{-1}a' = bb'^{-1} \in A \cap B$ a máme $ax = a'$ a $x^{-1}b = b'$.

Iný spôsob: $\frac{|A|}{|A \cap B|}$ je počet prvkov rozkladu A podľa podgrupy $A \cap B$. Chceme dokázať $|AB| = \frac{|A|}{|A \cap B|}|B|$. Na to stačí ukázať, že $ab = a'b'$ práve vtedy, keď a a a' padnú do tej istej triedy rozkladu A podľa $A \cap B$. To môžeme urobiť podobným postupom, ako sme použili v predchádzajúcom odseku.

d) Je vcelku ľahké si všimnúť, že platí (pre ľubovoľné $A, B, C \subseteq G$)

$$A(B \cap C) \subseteq AB \cap AC.$$

Z toho, že $A \subseteq C$ máme $AC = C$, a teda

$$AB \cap AC = AB \cap C = C.$$

Ďalej vieme, že $C \subseteq AB$. Teda každý prvok $c \in C$ môžeme napísať v tvare $c = ab$ pre $a \in A$ a $b \in B$. Pretože $A \subseteq C$, máme $a \in C$ a $b = a^{-1}c \in C$. Teda $b \in B \cap C$, z čoho vyplýva $ab \in A(B \cap C)$. Ukázali sme

$$C \subseteq A(B \cap C).$$

Spojením týchto inklúzií a rovnosti dostaneme

$$C = AB \cap AC = A(B \cap C).$$

3. (V. Bachratá, D. Švec) Využijeme nasledujúce tvrdenie: Ak H je podgrupa G také, že $[G : H] = 2$, tak H je normálna a pre všetky $x \in G$ platí $x^2 \in H$. (Bolo to síce na cviku a asi to mala niektorá skupina aj na písomke, ale asi sa nezaškodí pripomenúť dôkaz. Ak $[G : H] = 2$, znamená to, že rozklad G podľa H má dve triedy. Pretože jedna z tried je H, druhá z nich musí byť $G \setminus H$. Teda existuje jediný taký rozklad, čo znamená, že ľavý a pravý rozklad sa rovnajú a H je normálna. Ak $x \in G$ tak rád prvku xH v dvojprvkovej grupe G/H je deliteľom 2, preto $x^2H = (xH)(xH) = H$, čiže $x^2 \in H$.)

V našom prípade má grupa S_4 24 prvkov a A_4 má 12 prvkov. (Párne permutácie sú práve identita, cykly dĺžky 3 a permutácie pozostávajúce z 2 disjunktných transpozícií. Cyklov dĺžky 3 je $\binom{4}{3}.2 = 6$ – pretože 3 prvky môžeme vybrať $\binom{4}{3}$ spôsobmi a rotovať ich môžeme 2 smermi. Ak permutácia pozostáva z 2 disjunktných transpozícií, tak je jednoznačne určená prvkom, ktorý je v transpozícii spolu s prvkom 1, a na výber tohto prvku máme 3 možnosti.)

Ak by H bola 6-prvková podgrupa S_4, tak podľa tvrdenia, ktoré sme uviedli pred chvíľou, by platilo $\varphi^2 \in H$ pre všetky permutácie z A_4. Špeciálne tak dostaneme, že H obsahuje všetky trojprvkové cykly (pretože $(abc) = (acb)^2$), a teda H má aspoň 8 prvkov, čo je spor.

Iné riešenie: (Základná myšlienka je podobná – ukážeme, že by H obsahovala viac než 6 prvkov, trochu iným postupom.) Predpokladajme, že by A_4 obsahovala 6-prvkovú podgrupu H. Potom H obsahuje permutáciu φ rádu 2. (Každá grupa s párnym počtom prvkov obsahuje prvok rádu 2.)

Párna permutácia 4-prvkovej množiny musí byť súčin 2 disjunktných cyklov dĺžky 2. Bez ujmy na všeobecnosti môžeme predpokladať, že sme prvky preusporiadali tak, že $\varphi = (12)(34)$.

Ďalej si uvedomme, že H musí obsahovať aj nejaký prvok rádu 3. Prvok rádu 1 je totiž jedine identita a prvky rádu 2 máme v A_4 iba 3: $(12)(34)$, $(13)(24)$ a $(14)(23)$. V A_4 sú len prvky rádov 1,2,3 (cyklus dĺžky 4 je totiž nepárna permutácia).

Vidíme teda, že existuje prvok $\tau \in H$, ktorý má rád 3. Zrejme τ je cyklus dĺžky 3. Vhodným prečíslovaním opäť môžeme dosiahnuť, že $\tau = (123)$.

(Prvky skutočne môžeme prečíslovať tak ako sme uviedli. Máme totiž permutáciu τ, ktorá je cyklom dĺžky 3 a φ, ktorá pozostáva z dvoch cyklov dĺžky 2. Z troch prvkov vystupujúcich v cykle τ budú práve 2 v rovnakom cykle dĺžky 2 vo φ. Tieto označíme ako 1 a 2, zvyšný prvok z tohoto cyklu označíme 3 a máme ich očíslované tak, ako sme chceli.)

Dostali sme sa teda do situácie, keď vieme, že H obsahuje permutácie $(12)(34)$ a (123). Ďalší postup je jednoduchý: skladaním týchto permutácií sa nám podarí vytvoriť viac ako 6 permutácií, čo je spor s tým, že H má 6 prvkov.
$(12)(34)(123) = (134) \in H$
$(123)(134) = (124) \in H$
$(123)^2 = (132) \in H$, $(134)^2 = (143) \in H$, $(124)^2 = (142) \in H$
Našli sme teda celkove 8 rôznych prvkov, ktoré musia patriť do každej podgrupy obsahujúcej $(12)(34)$ a (123) – sú to permutácie id, $(12)(34)$, (123), (132), (134), (143), (124), (142).

Ďalšie riešenie môžete nájsť v [G] (začiatok 2. kapitoly).

4. (M. Širáň; čiastočné riešenie L. Kovalčinová) Návod (z [FS], resp. [P]): Kocka má 4 telesové uhlopriečky. Treba si ozrejmiť, že každá symetria kocky, ktorá nemení orientáciu zodpovedá jednoznačne nejakej permutácii týchto telesových uhlopriečok (a takisto, že toto priradenie zachováva skladanie zobrazení).

Pretože je to prvý príklad zo série úloh týkajúcich sa symetrií pravidelných telies, nezaškodí spomenúť pár vecí, ktoré je dobre si uvedomiť.

Úlohu by sme mohli riešiť tak, že vezmeme graf telesa (hrany a vrcholy) a symetrie telesa sú potom práve automorfizmy grafu (t.j. také zobrazenia množiny vrcholov do seba, ktoré zachovávajú susednosť).

Niektoré dvojice telies sú duálne: kocka a osemsten; dvanásťsten a dvadsaťsten. Duálne teleso znamená, že vezmeme za vrcholy nového telesa stredy stien pôvodného telesa. (Takto dostaneme z kocky osemsten a z osemstenu kocku). Duálne telesá musia mať rovnaké grupy symetrií. (Ak by sme urobili podobný postup pre rovinné grafy, dostaneme tzv. duálny graf.)

Vďaka tomu, že ide vlastne o úlohu nájsť všetky zobrazenia daného grafu, dá sa úloha vyriešiť mechanicky – vyskúšaním všetkých možností. Samozrejme, ručne by to trvalo pridlho – ale dá sa to naprogramovať. V [M] sa môžete dozvedieť ako sa to dá urobiť pomocou programu Maple. Program asi najčastejšie využívaný na tento typ výpočtov je GAP.

Snáď by ešte stálo za zmienku, že kocka sa dá chápať ako Cayleyho graf (budete mať – alebo už ste mali – na teórii grafov).

Spomeňme si ešte jednu možnosť, ktorá by sa dala použiť v úlohách tohoto typu. Uvažujme permutácie $s = (12)$ a $r = (123)$. Pre ne platí

$$sr = r^2 s, s^2 = id, r^3 = id.$$

Tiež si všimnime, že z predchádzajúcich vzťahov môžeme už jednoznačne určiť súčin ľubovoľných 2 prvkov z grupy $\{id, r, r^2, s, sr, sr^2\}$ (môžete skúsiť vyplniť tabuľku grupovej operácie). Získame tak vlastne grupu S_3.

Grupa S_3 je teda určená množinou prvkov uvedenou hore a vzťahmi $sr = r^2 s$, $s^2 = id$, $r^3 = id$. Inak povedané, je to grupa s generátormi r a s, ktorá spĺňa dané vzťahy a neplatia v nej už žiadne rovnosti, ktoré nemožno odvodiť z týchto vzťahov (aj keď toto nie je asi až také jednoduché dokázať). Ak máme grupu zadanú pomocou generátorov a vzťahov, ktoré pre ne platia, hovoríme o *konečnej reprezentácii* grupy.

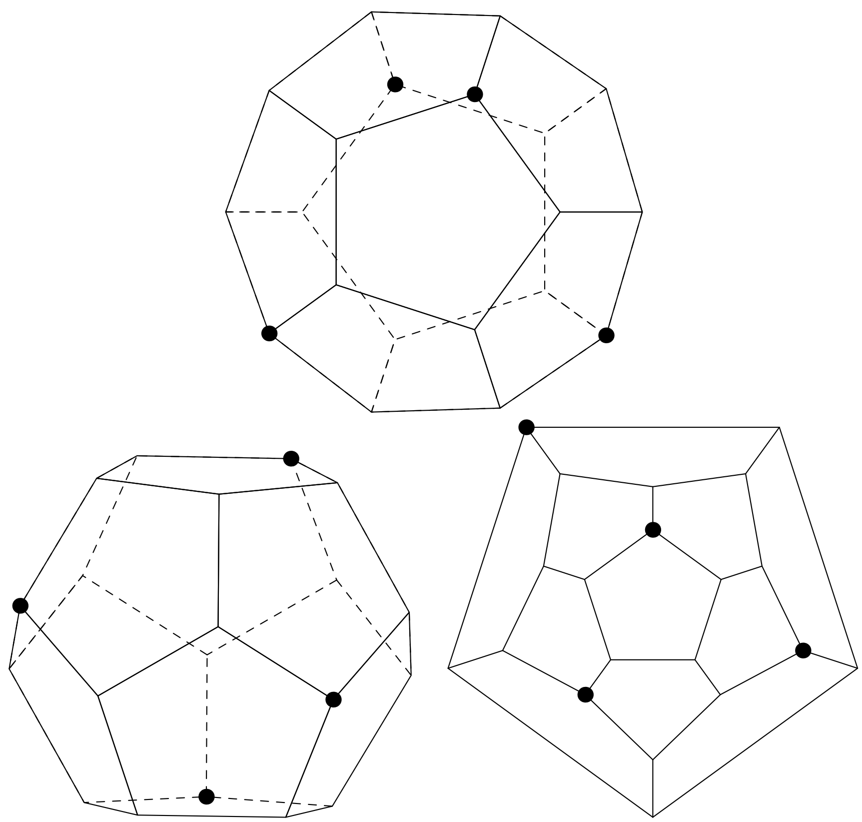
V našom príklade by sme mohli použiť nejaké generátory S_4, nájsť vzťahy, ktoré jednoznačne určia grupu S_4, týmto generátorom priradiť nejaké symetrie kocky a ukázať, že spĺňajú tie isté vzťahy. Ak okrem toho ešte ukážeme, že grupy majú rovnaký počet prvkov, tak už musia byť izomorfné.

5. (M. Širáň – skoro kompletné riešenie) Dvadsaťsten:

Moje riešenie (t.j. berte ho s rezervou – môže tam byť chyba). Niektoré zdôvodnenia možno nie sú až tak detailné ako by mali byť – ale s trochou geometrickej predstavivosti sa to snáď bude dať pochopiť. Možno pomôžu aj obrázky. (Jeden z obrázkov predstavuje dvanásťsten ako rovinný graf – t.j. jednu stenu sme roztiahli tak, aby sa všetky vrcholy dali umiestniť do jednej roviny. Ďalšie 2 sú pohľad zhora a spredu.)

Najprv spočítajme, koľko symetrií vlastne obsahuje naša grupa. Pri troche geometrickej predstavivosti si ľahko uvedomíme, že zobrazením 2 susedných vrcholov je už celá symetria jednoznačne určená. Máme teda celkove $20 \times 3 = 60$ symetrii (20 možných vrcholov, každý má 3 susedov). Zo zadaných grúp má takýto počet prvkov len A_5; pokúsime sa teda ukázať, že grupa symetrií dvanásťstena je izomorfná s alternujúcou grupou A_5.

Skúsme sa inšpirovať príkladom kocky. Tam sme mali 4 uhlopriečky, ktoré nám pomohli ukázať, že ide o grupu S_4. Fajn, tak teraz by sa nám hodilo mať nejakých 5 útvarov. Keby sme všetkých 20 vrcholov 12-stenu rozdelili na 5 častí, v každej musia byť 4 vrcholy. Vedeli by sme rozdeliť vrcholy 12-stenu na 5 pravidelných štvorstenov?



Zoberme si 1 vrchol 12-stenu. (Skúste si 12-sten predstaviť tak, že je jednou stenou položený na vodorovnej podložke. Potom máme hornú a spodnú stenu a 2 „vrstvy“ pozostávajúce z 5 stien. Občas použijem termín „horná“ alebo „dolná stena“ – z tohto by malo byť jasné, čo sa tým myslí. Prvý obrázok v takomto prípade predstavuje pohľad zhora.) Tento vrchol patrí 3 stenám. Ostatné vrcholy vyberieme z protiľahlých stien.

Zoberme si najprv jednu protiľahlú stenu. V nej sú 2 vrcholy s minimálnou možnou vzdialenosťou od vrcholu ktorý sme si zvolili ako prvý. (Na našom obrázku sú horná a spodná stena o kúsok pootočené 5-uholníky. K danému vrcholu z horného 5-uholníku máme 2 najbližšie vrcholy v spodnom.)

Teraz budeme rovnako pokračovať pre ostatné steny. Teraz však chcem nájsť vrchol, ktorý je rovnako vzdialený od oboch (všetkých 3) doteraz zvolených vrcholov. Preto bude už teraz voľba jednoznačná. (Jeden štvorsten, ktorý takto získame, je znázornený na obrázku.)

Tým sme našli jeden štvorsten, jeho pootočením dostaneme ďalšie 4 a tak rozdelíme všetky vrcholy medzi 5 pravidelných štvorstenov. (Ak si stále predstavujete 12-sten položený jednou stenou na vodorovnej podložke, tak sú všetky vrcholy rozdelené do 4 pätíc, ktoré sú v rovnakej výške. Práve popísaným postupom sme vybrali 1 vrchol z každej úrovne – teda sme rozdelili skutočne všetky.)

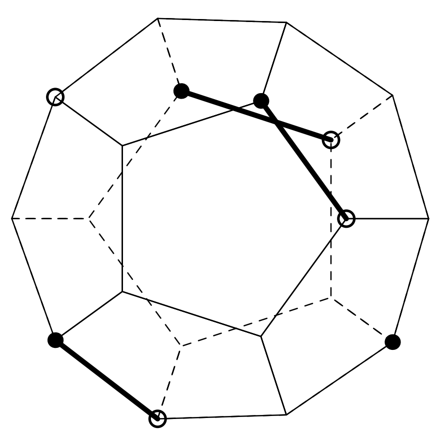
Fajn, takže máme 5 štvorstenov - a každá symetria musí zobraziť niektorý štvorsten na iný (pretože zachováva vzdialenosti, teda štvorica rovnako vzdialených bodov sa musí zobraziť na štvoricu rovnako vzdialených bodov), čiže každej symetrii sme priradili prvok z S_5 (permutáciu štvorstenov, ktoré sme práve popísali).

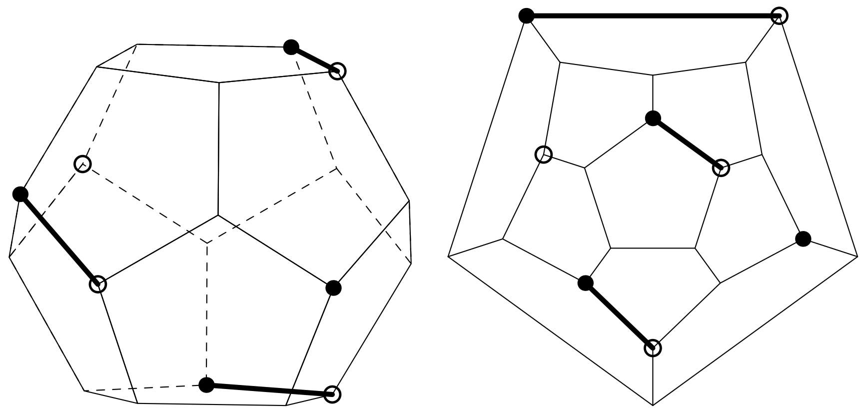
POZOR! Predchádzajúca úvaha má drobnú trhlinu (ktorú ale našťastie vieme zaplátať). V skutočnosti štvorstenov, ktorých hrany majú takúto vzdialenosť je 10 – v prvom kroku našej konštrukcie sme si mohli vybrať niektorý z dvojice najbližších vrcholov, ďalšie 2 vrcholy štvorstenu boli už jednoznačne určené. Lenže dvojice štvorstenov, ktoré takto dostaneme sú zrkadlovými obrazmi (podľa vhodnej roviny súmernosti; ak máte stále pred očami náš obrázok, bude to zvislá rovina, ktorá prechádza vrcholom z hornej podstavy, ktorý sme si zvolili a k nemu protiľahlým vrcholom 12-stena). Rovinná súmernosť mení orientáciu – preto takýto štvorsten nemôžeme dostať pomocou symetrie z grupy G. Teda nám zostáva naozaj len 5 štvorstenov.

Máme teda zobrazenie $\varphi\colon G \to S_5$, kde G je grupa permutácií, ktoré skúmame a S_5 sú permutácie piatich štvorstenov. Je to tiež homomorfizmus (ak zložíme 2 symetrie, aj permutácia našich štvorstenov je zloženie príslušných permutácií). Najprv by sme chceli ukázať, že φ je injekcia.

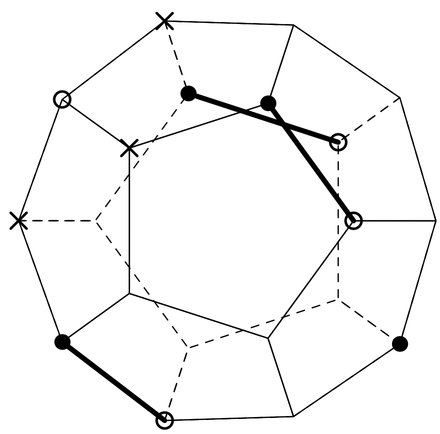
Nech f je symetria dvanásťstena, ktorej zodpovedá identická permutácia štvorstenov. Teda každý vrchol sa môže zobraziť iba na niektorý vrchol z jemu prislúchajúceho štvorstenu. Samozrejme musí byť pritom zachovaná susednosť vrcholov.

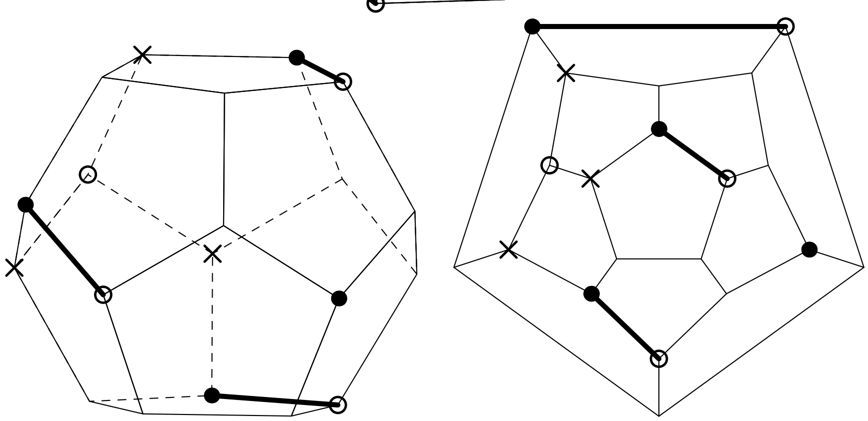
Predpokladajme, že $f \neq id$. Potom sa niektorý bod musí zobraziť na iný bod. Bez ujmy na všeobecnosti nech je to bod štvorstenu, ktorý sme si nakreslili ako prvý. Ak teraz vezmeme „susedný“ štvorsten, zistíme, že máme iba tri dvojice vrcholov, ktoré sú susedné. (Susedné štvorsteny - jeden vznikol pootočením druhého o $\frac{2\pi}{5}$ okolo zvislej osi prechádzajúcej stredmi protiľahlých stien.) Sú znázornené na obrázkoch.





Ako sme už spomínali, zobrazením dvojice vrcholov je symetria jednoznačne určená (keď vieme, že nemení orientáciu). Ak si vezmeme ďalšieho suseda (nazvime ho X) prvého vrcholu v hornej stene, tak pre každú z týchto dvoch symetrií vieme určiť kam sa zobrazí (na obrázku je to vyznačené krížikom). Ale ani 1 z týchto dvoch možných pozícií po zobrazení nie je v tom istom štvorstene ako X.





Pretože $\varphi\colon G \to S_5$ je injekcia, grupa G je izomorfná s podgrupou $\varphi[G]$ grupy S_5 (kde $\varphi[G]$ označuje obraz G v zobrazení φ.) Pretože táto grupa má 60 prvkov, teda polovicu z počtu prvkov S_5, podľa prémiovej úlohy 7 to musí byť A_5.

Iné riešenie sa dá nájsť v [FS] alebo [P].

Ďalšia možnosť riešenia je ukázať, že S_5 je generovaná permutáciami $r = (12345)$ a $s = 142$ a je určená vzťahmi $(sr)2 = s^3 = r^5 = ud$. Tieto vzťahy spĺňajú aj symetrie $r =$ rotácia okolo niektorej osi prechádzajúcej vrcholom a $s =$rotácia okolo osi prechádzajúca stredom steny (pričom vrchol volíme na tejto stene). Treba okrem toho ešte ukázať, že každá symetria sa dá dostať z s a r.

Takto sa zhruba dá preformulovať riešenie M. Širáňa. (Ja som bol však príliš lenivý skontrolovať to úplne detailne.)

Štvorsten: Celkom ľahko sa dá zistiť, že každá permutácia vrcholov zodpovedá nejakej symetrii a orientáciu zachovávajú práve párne permutácie.

Teleso	Bez zmeny orientácie	Všetky symetrie
Štvorsten	A_4	S_4
Kocka	S_4	$S_4 \times \mathbb{Z}_2$
Osemsten	S_4	$S_4 \times \mathbb{Z}_2$
Dvanásťsten	A_5	$A_5 \times \mathbb{Z}_2$
Dvadsaťsten	A_5	$A_5 \times \mathbb{Z}_2$

6. (čiastočné riešenie: M. Adamčík) Táto úloha je podstatne ťažšia než som si myslel, keď som ju zadával. Za to sa ospravedlňujem – keď som ju zadával, predpokladal som, že až taká zložitá nebude. Ale súvisí to s tým, že sa zdáte dosť šikovní, preto som Vám chcel zadať veľa prémiových úloh – aby ste sa cez semester nenudili. Pretože som ich chcel zadať veľa, nestihol som si poriadne rozmyslieť riešenia všetkých úloh :-(

Nepodarilo sa mi nájsť riešenie, ktoré by vystačilo s vedomosťami z druhého ročníka. Riešenie, ktoré Vám viem povedať sa opiera o dôsledok 3, ktorý hovorí, že a G má p^2 prvkov, tak existuje nejaký prvok tejto grupy (rôzny od neutrálneho), ktorý komutuje so všetkými prvkami grupy G. Ak ste ochotný tomuto uveriť, tak riešenie už bude pomerne jednoduché. Stručný dôkaz tohoto faktu som sa pokúsil spísať dole – najprv uvediem spomínané riešenie. (Ak predsa len niekto prídete na oveľa jednoduchšie riešenie, dajte mi vedieť – ja som na nič jednoduchšie neprišiel).

Nech G je p^2-prvková grupa a nech $a \neq e$ je prvok, ktorý komutuje so všetkými prvkami z G. Podľa Lagrangeovej vety je rád tohoto prvku buď p^2 alebo p.

Ak je rád prvku a rovný p^2, tak ide o cyklickú grupu a teda G je izomorfná so $\mathbb{Z}_{p^2}$.

Nech teraz rád a je rovný p. Ukážeme, že existuje izomorfizmus medzi G a $\mathbb{Z}_p \times \mathbb{Z}_p$. Zoberme si ľubovoľný prvok $b \notin [a]$. Ak je rád prvku b rovný p^2, ide opäť o cyklickú grupu. Bez ujmy na všeobecnosti môžeme teda predpokladať, že rád prvku b je tiež p. Grupa G určite obsahuje prvky tvaru $a^k b^l$, kde $k, l \in \{0, 1, \ldots, p-1\}$. Zo zákonov o krátení vyplýva, že sú to rôzne prvky. Tvrdíme, že zobrazenie $\varphi \colon G \to \mathbb{Z}_p \times \mathbb{Z}_p$ definované ako $\varphi : a^k b^l \mapsto (k, l)$ je izomorfizmus. To, že φ je bijekcia, je zrejmé. Jediné, čo si treba uvedomiť, aby sme videli, že je to aj homomorfizmus, stačí si všimnúť rovnosť

$$a^k b^l a^m b^n = a^{k+m} b^{l+n},$$

ktorá vyplýva z toho, že prvok a komutuje s prvkom b.

Zvyšok je venovaný dôkazu dôsledku 3.

Ak a je prvok grupy G, tak ako $C(a)$ označíme množinu $Z(a) = \{g \in G; ag = ga\}$ všetkých prvkov, ktoré komutujú s a. (Množina $Z(a)$ sa zvykne nazývať centralizátor prvku a.) Pre ľubovoľný prvok $a \in G$ je jeho centralizátor $Z(a)$ podgrupa G.

Dva prvky a, b grupy G nazveme *konjugované,* ak $a = gbg^{-1}$ pre nejaké $g \in G$. Budeme používať označenie $a \sim b$. Dá sa pomerne ľahko overiť, že $\sim$ je relácia ekvivalencie. Triedy tejto ekvivalencie budeme nazývať *triedy konjugácie* a triedu prvku a označíme $C(a)$. Čiže

$$C(a) = \{gag^{-1}; g \in G\}$$

Lema 1. *Pre triedy konjugácie platí*

$$|C(a)| = [G : Z(a)].$$

Dôkaz. Nech $x, y \in C(a)$. To znamená, že existujú $g, h \in G$ také, že $x = gag^{-1}$ a $y = hah^{-1}$. Potom

$$x = y \Leftrightarrow gag^{-1} = hah^{-1} \Leftrightarrow h^{-1}ga = ahg^{-1} = a(h^{-1}g)^{-1},$$

teda prvky x a y sa rovnajú práve vtedy, keď $h^{-1}g \in Z(a)$, čiže h a g patria do tej istej triedy rozkladu G podľa $Z(a)$.

Preto každá trieda rozkladu G podľa $Z(a)$ určuje práve jeden prvok z $C(a)$, teda prvkov v $C(a)$ je toľko isto ako tried rozkladu. □

Dôsledok 1. *Počet prvkov každej triedy konjugácie delí počet prvkov grupy G.*

Centrom grupy nazývame množinu $\{a \in G; (\forall g \in G) ag = ga\}$ tých prvkov, ktoré komutujú s každým prvkom z G.

Dôsledok 2.

$$|C(a)| = 1 \qquad \Leftrightarrow a \in Z(G)$$

Dôkaz. Podľa predchádzajúcej vety $|C(a)| = 1$ znamená $Z(a) = G$, teda a komutuje s každým prvkom grupy G a $a \in Z(G)$. □

Pre nás sú dôležité tieto fakty: Počet prvkov každej triedy konjugácie delí počet prvkov G a triedy konjugácie tvoria rozklad G (pretože konjugácia je relácia ekvivalencie). Preto počet prvkov G je súčtom počtov prvkov jednotlivých tried konjugácie.

V našom prípade máme $|C(a)| \mid p^2$ pre všetky $a \in G$. Pritom $|C(e)| = 1$ (pretože e je v centre grupy G). Ostatné triedy konjugácie môžu mať teda veľkosť 1 alebo p. Keby všetky mali počet prvkov p, tak by platilo $p^2 = kp + 1$, kde k je počet tried konjugácie, čo je spor (číslo na ľavej strane rovnosti je deliteľné p, číslo napravo nie). Teda musí existovať aspoň jeden prvok rôzny od e, ktorý leží v centre grupy G.

Dôsledok 3. *Každá p^2-prvková grupa má netriviálne centrum (t.j. $Z(G) \neq \{e\}$).* {DOSCEN}

Viac o veciach, ktoré súvisia s predchádzajúcimi tvrdeniami, sa môžete dozvedieť v 2. kapitole v [G].

Literatúra

[FS] D. K. Faddeev and I. C. Sominskii. *Zadači po vysšej algebre*. St. Peterburg, 1999.

[G] J. Guričan. Vybrané kapitoly z algebry. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?clen=gurican`.

[M] P. J. Morandi. Computing the symmetry groups of the platonic solids with the help of Maple. available at `http://sierra.nmsu.edu/morandi/notes/PlatonicSolids.pdf`.

[P] I. V. Proskurjakov. *Sbornik zadač po lineinoi algebre*. Moskva, 1966.