Rozhledy matematicko-fyzikální

Vojtěch David

Burnsideovo lemma aneb proč se starat o teorii grup

Rozhledy matematicko-fyzikální, Vol. 98 (2023), No. 4, 1–11

Persistent URL: `http://dml.cz/dmlcz/151998`

Terms of use:

© Jednota českých matematiků a fyziků, 2023

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

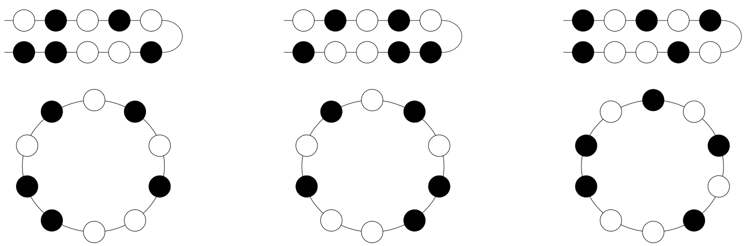
This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* `http://dml.cz`

Burnsideovo lemma aneb proč se starat o teorii grup

Vojtěch David, student MFF UK, Praha

Úvod a motivace

Uvažme následující situaci. Máme 5 černých a 5 bílých korálků, které navlékáme na provázek a chceme si vyrobit náramek. Kolik takových náramků můžeme vytvořit? Již při prvotním zamyšlení tato otázka není úplně snadná, při počítání možností nemůžeme uvažovat jen pořadí, v jakém korálky navlékáme, neboť můžou různá pořadí jejich navlečení vést ke stejným náramkům jako na obr. 1.

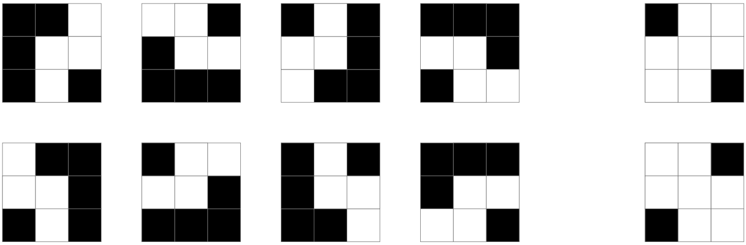


Obr. 1:

Tento problém má zřejmě jakousi symetrii, která nám jeho řešení komplikuje. Než se pustíme do snažení o práci s touto symetrií, uvedeme ještě jeden příklad.

Máme tabulku 3×3. Kolik různých obarvení políček černou nebo bílou barvou existuje? Při takto prvoplánovém dotazu můžeme odpovědět téměř okamžitě – pro každé z devíti políček máme právě 2 možnosti obarvení, proto je zjevně celkový počet možností $2^9 = 512$. Co když do hry ale opět přidáme symetrie problému? Co když budeme chtít jen obarvení, která jsou různá, i když tabulku budeme libovolně otáčet nebo překlápět? V tomto případě nám zřejmě zbyde méně možností, ale není jisté, kolik jich bude, protože některé tabulky získáme z jiného počtu původních možností než jiné, jak ukazuje obr. 2.

Je tedy zřejmé, že budeme předvedené problémy muset zkoumat nepřímo – přes přímočaré počítání „objektů“ se k výsledku dostaneme jen s velkými obtížemi.[1] Pojďme tedy zabřednout do teorie grup, která nabízí naprosto přirozený způsob, jak nahlížet na symetrie různých matematických objektů.



Obr. 2:

Grupy

Nejprve uvedeme formální definici.

Definice 1. Grupa je množina G vybavená binární operací, řekněme $\cdot\colon G \times G \to G$, pro kterou platí následující.

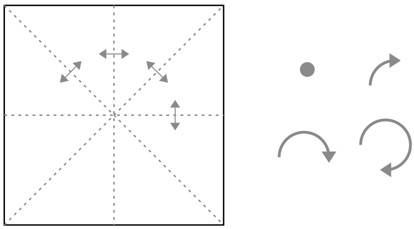
- **Operace je asociativní**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ pro všechna $a, b, c \in G$.
- **Grupa obsahuje neutrální prvek**: existuje prvek $1 \in G$ takový, že $a \cdot 1 = a = 1 \cdot a$ pro všechna $a \in G$.
- **Ke každému prvku existuje inverzní prvek**: pro všechna $a \in G$ existuje prvek $a^{-1} \in G$ takový, že $a \cdot a^{-1} = 1 = a^{-1} \cdot a$.

Nakolik abstraktní se může tato definice zpočátku zdát, tvrdí vlastně něco poměrně přirozeného a očekávaného.

Jako jednoduchý příklad grupy můžeme uvést celá čísla s operací sčítání. Sčítání je zřejmě asociativní, existuje číslo, které když přičteme k libovolnému jinému číslu, nic se nezmění (mluvíme o nule) a ke každému celému číslu existuje jiné celé číslo, jejichž součet dává nulu (např. k 5 je to -5) – jedná se tedy skutečně o grupu. Dále můžeme uvést třeba racionální čísla bez nuly spolu s násobením nebo reálná čísla se sčítáním – že se jedná o grupy, ověříme úplně stejně.

[1] Tato myšlenka je dokonce klíčová při důkazu Burnsideova lemmatu, který bude uvedený později.

Také ale existují další příklady grup – pro nás budou užitečné tzv. dihedrální grupy. Vezměme si například čtverec a uvažme množinu všech zobrazení, která jej převedou na sebe sama – chceme-li, jeho symetrie. Co vše bude tato množina obsahovat? Zjevně identické zobrazení, tedy zobrazení, které se čtvercem „neudělá nic“, dále rotace o 90°, 180° a 270° a nakonec osové symetrie – dvě podle os stran a dvě podle úhlopříček. Můžeme si rozmyslet, že žádné další symetrie čtverec nemá.[2)]



Obr. 3: Grupa symetrií čtverce

Máme tedy množinu a ještě potřebujeme operaci. Touto operací pro nás bude poměrně přirozeně skládání zobrazení. Všimněme si, že když například nejprve čtverec otočíme o 90° a následně překlopíme podle osy „horní strany“ čtverce, bude to mít stejný efekt, jako kdybychom čtverec rovnou překlopili podle úhlopříčky. Budeme-li tuto operaci značit $\circ$ a doprava umístíme zobrazení, které provádíme jako první, můžeme pak neformálně psát

$$\leftrightarrow \circ \curvearrowright = \swarrow\!\!\!\!\nearrow .$$

Vidíme tedy, že složením dvou symetrií čtverce je opět symetrie čtverce. Můžeme také ověřit, že je tato operace asociativní, že existuje neutrální prvek (je jím zobrazení „neudělej nic“) a že ke každému zobrazení existuje inverzní zobrazení, které jej „vyruší“. Tato množina bude tedy skutečně grupou.

Podobnou grupu můžeme zavést pro libovolný pravidelný n-úhelník. Budeme ji nazývat dihedrální grupou (nebo prostě grupou symetrií n-úhelníku) a dá se ukázat, že bude mít pokaždé $2n$ prvků (identitu, $n-1$ netriviálních rotací a n osových symetrií).

[2)] Též to můžeme precizněji dokázat, očíslujeme-li si vrcholy čtverce a budeme-li uvažovat všechny možnosti, jak čtverec přečíslovat, abychom zachovali sousednost, tj. abychom jej nijak nedeformovali.

Nyní si uvědomme dvě věci. Zaprvé poukažme na sílu definice grupy – ukázali jsme, že jak např. celá čísla, tak množina „věcí, co můžeme dělat se čtvercem“ mají strukturu grupy, existuje mezi nimi tedy nějaká vnitřní podobnost. Pokud tedy dokážeme nějaké tvrzení obecně pro grupu, bude toto tvrzení platit pro všechny její „realizace“ – a takových tvrzení není vůbec málo! Grupami se zabývá celý obor matematiky, který v tomto článku nelze pomalu ani přiblížit.

Zadruhé se vraťme k původním motivačním příkladům. Nyní jsme totiž popsali docela dobře symetrie, které obtěžkávají naše situace. Hledáme počet různých náramků až na *působení* grupy symetrií desetiúhelníku nebo (poněkud intuitivněji) počet různých čtverců až na *působení* grupy symetrií čtverce (kterou jsme si dokonce popsali explicitně). Co je to ale ono působení grupy?

Působení grupy na množinu a Burnsideovo lemma

Na dvou motivačních příkladech jsme poměrně intuitivně přiblížili, co to znamená, že grupa působí na nějakou množinu, tento koncept nyní můžeme trochu formalizovat.

Definice 2. Grupa G působí na množinu X, pokud pro každé $g \in G$ a každé $x \in X$ existuje prvek $gx \in X$ a platí

1. $h(gx) = (hg)x$ pro všechna g, $h \in G$, $x \in X$ (tedy nezáleží, jestli nejprve působím prvkem g a pak až h nebo jestli působím rovnou prvkem hg),
2. $1 \cdot x = x$ pro všechna $x \in X$ (působení neutrálního prvku nic nedělá).

Vybaveni touto definicí můžeme s působením grupy pracovat trochu abstraktněji. Zlatým grálem našeho snažení bude Burnsideovo lemma – tvrzení, které nám umožní pouhým dosazením vyřešit prezentované problémy. Ještě předtím ale musíme definovat pár pojmů a odvodit pro ně nějaká snadná tvrzení.

Definice 3. Nechť grupa G působí na množinu X. Orbitou prvku x budeme rozumět množinu

$$G_x = \{gx \mid g \in G\}.$$

Pro daný prvek $x \in X$ budeme tedy orbitou rozumět množinu všech možných prvků, které můžeme dostat působením grupy G. V našem příkladu se čtvercem, kdy množinou X rozumíme všechna vybarvení čtverce a grupou G grupu symetrií čtverce, tedy budeme moct s trochou nadsázky psát:

Je tedy vidět, že nás v tomto problému zajímá pouze počet různých orbit. Za tímto účelem uveďme ještě jednu definici.

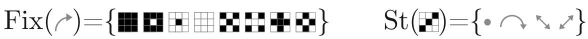
Definice 4. X/G značí množinu všech orbit při působení grupy G na množinu X, tedy
$$X/G = \{G_x \mid x \in X\}.$$

V tuto chvíli jsme již celé zadání úlohy převedli do abstraktního jazyka, protože nás zřejmě bude zajímat velikost této množiny, tedy $|X/G|$. Máme před sebou ale ještě poněkud zdlouhavou cestu, než budeme umět tento počet přímo určit. Zavedeme nyní dva v jistém smyslu podobné pojmy.

Definice 5. Množinou fixních bodů pro $g \in G$ budeme nazývat
$$\operatorname{Fix} g = \{x \in X \mid gx = x\}.$$

Definice 6. Stabilizátorem prvku $x \in X$ při působení grupy G na množinu X budeme rozumět
$$\operatorname{St} x = \{g \in G \mid gx = x\}.$$

Zatímco množina fixních bodů obsahuje takové prvky množiny X, které jsou zachované působením specifického prvku grupy g, stabilizátor prvku x obsahuje právě ty prvky grupy G, jejichž působením je zachován. Znovu to ilustrujeme na zkoumaném příkladu:



Tyto koncepty nám stále ještě o hodnotě $|X/G|$ nic neřeknou, můžeme ale učinit velmi důležité pozorování o jejich velikostech.

Pozorování 1.
$$\sum_{x \in X} |\operatorname{St} x| = \sum_{g \in G} |\operatorname{Fix} g|\,.$$

Důkaz. Označíme $S = \{[x, g] \mid gx = x\}$, tedy množinu všech dvojic $[x, g]$, které splňují $gx = x$. Počet takovýchto dvojic pak můžeme spočítat dvojím způsobem.

- Nejprve pro každé x spočteme, kolik prvků g je zachovává, a následně tuto hodnotu sečteme pro každé x, tedy

$$|S| = \sum_{x \in X} |\mathrm{St}\, x| \,.$$

- Nejprve pro každé g spočteme, kolik prvků množiny x toto g nezmění, následně tuto hodnotu sečteme pro všechna g.

$$|S| = \sum_{g \in G} |\mathrm{Fix}\, g| \,.$$

Odsud triviálně plyne chtěná rovnost

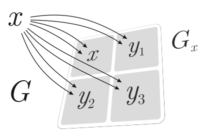
$$\sum_{x \in X} |\mathrm{St}\, x| = |S| = \sum_{g \in G} |\mathrm{Fix}\, g| \,.$$

Toto pozorování nám umožňuje místo počítání velikostí stabilizátorů, počítat velikosti množin fixních bodů – to je snazší, protože symetrií máme zpravidla méně a kladou nám jasný požadavek na to, jak musí prvek množiny X vypadat, aby byl danou symetrií zachován. Nyní už jsme téměř připraveni, jen potřebujeme učinit ještě jedno pozorování.

Pozorování 2.

$$|\mathrm{St}\, x| \cdot |G_x| = |G| \,.$$

Důkaz. Standardně by důkaz tvrzení vyplynul z Lagrangeovy věty. Ta ale není předmětem tohoto článku, proto nastíníme důkaz trochu jiný, o něco intuitivnější.



Obr. 4: Znázornění Pozorování 2; šipky reprezentují působení unikátními prvky grupy G

Zvolme pevně nějaký prvek $x \in X$. Budeme-li na něj působit postupně všemi prvky grupy G, získáme postupně z definice všechny prvky orbity G_x. Klíčovým pozorováním (které dále dokážeme) bude, že se z x na libovolný prvek $y \in G_x$ dostaneme pomocí právě $|\mathrm{St}\, x|$ prvků grupy G. Pak totiž tímto způsobem rozdělíme prvky G do $|G_x|$ množin po $|\mathrm{St}\, x|$ prvcích, čímž dokážeme požadované tvrzení.

Nechť tedy $y = gx$ pro nějaké pevně zvolené $g \in G$ a $y \in G_x$. Chceme ukázat

$$|\{g' \in G \mid g'x = y = gx\}| = |\mathrm{St}\, x|\,.$$

Všimněme si, že existuje jednoznačná korespondence mezi prvky stabilizátoru a prvky množiny $M = \{g' \in G \mid g'x = y = gx\}$. Totiž platí

$$g' \in M \iff gx = y = g'x = (gg^{-1})g'x = ghx \iff g^{-1}g' = h \in \mathrm{St}\, x.$$

Z každého prvku stabilizátoru h tedy vyrobíme prvek $g' \in M$ tak, že položíme $g' = gh$. Naopak, z každého $g' \in M$ dostaneme $h \in \mathrm{St}\, x$ jako $h = g^{-1}g'$, což skutečně náleží stabilizátoru, neboť

$$gx = g'x \iff g^{-1}g'x = x.$$

Nakonec pozorujme, že $g'_1 = g'_2 \in M$, právě když $h_1 = h_2 \in \mathrm{St}\, x$, tedy ze dvou různých prvků M vyrobíme dva různé prvky $\mathrm{St}\, x$ a naopak. To je ale snadné, protože platí

$$g'_1 = g'_2 \iff g^{-1}g'_1 = g^{-1}g'_2 \iff h_1 = h_2.$$

Tímto jsme tedy skutečně vytvořili jednoznačné párování mezi prvky stabilizátoru a prvky grupy, kterými se z x dostaneme na y. Ukázali jsme tedy, co jsme chtěli, a požadované tvrzení

$$|\mathrm{St}\, x| \cdot |G_x| = |G|$$

je tímto dokázáno.

Po tomto techničtějším důkazu se již konečně dostáváme k Burnsideovu lemmatu.

Lemma 1 (Burnsideovo lemma)**.**

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}\, g|\,.$$

Důkaz. Nejprve provedeme pár zdánlivě zbytečných a triviálních kroků.

$$|X/G| = |\{G_x \mid x \in X\}| = \sum_{G_x \in X/G} 1 = \sum_{G_x \in X/G} \sum_{y \in G_x} \frac{1}{|G_x|} = \sum_{x \in X} \frac{1}{|G_x|}.$$

Zpočátku jsme po rozepsání definice za každou orbitu v množině X/G přičetli 1. To jsme dále pro každou orbitu rozepsali jako součet převrácených hodnot velikosti orbity za každý její prvek. Nakonec jsme si všimli, že tímto způsobem vlastně sčítáme přes všechny prvky množiny x.

Tyto úpravy si můžeme poměrně jednoduše představit – mějme před sebou několik krabiček, každou s několika kuličkami. Počet těchto krabiček pak (zdánlivě zbytečně složitě) určíme tak, že se budeme dívat na jednotlivé kuličky a pro každou z nich přičteme převrácenou hodnotu počtu kuliček v krabičce, v níž se nachází.

Nyní již stačí vytknout z celého součtu $1/|G|$, použít učiněná pozorování a dojdeme k požadovanému výsledku.

$$|X/G| = \sum_{x \in X} \frac{1}{|G_x|} = \frac{1}{|G|} \sum_{x \in X} \frac{|G|}{|G_x|} \overset{2}{=} \frac{1}{|G|} \sum_{x \in X} |\mathrm{St}\, x| \overset{1}{=} \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}\, g|\,.$$

Užití

Nyní jsme se vybavili Burnsideovým lemmatem a můžeme se konečně vrátit zpět k původním příkladům; začněme tím se čtvercem.

Burnsideovo lemma říká, že pro spočtení množství všech orbit při působení grupy na množinu, stačí spočíst velikost grupy a pro každý její prvek velikost množiny fixních bodů. To je – jak nyní ukážeme – velmi snadné. V příkladu nám figuruje grupa symetrií čtverce, ta má, jak jsme odvodili, 8 prvků. Nyní pro každý z nich určíme, kolik konfigurací zachovává – tedy která vybarvení budou vypadat stejně, když provedeme danou symetrii.

- **Identita**: při identickém zobrazení jsou všechny prvky fixní, proto má množina fixních bodů velikost $2^9 = 512$.
- **Rotace o** $90°$: dříve jsme všechny konfigurace zachované rotací o $90°$ dokonce vypsali, víme tedy, že jich je 8. Kdybychom na to ale chtěli jít systematicky, můžeme si uvědomit, že vybarvení políčka v levém horním rohu určuje nutně vybarvení políčka v pravém horním rohu, to zase jednoznačně určuje vybarvení políčka v pravém dolním rohu, což

nakonec zase určuje vybarvení políčka vlevo dole. Obdobné můžeme říci pro políčka ve středech stran, dostaneme tedy, že máme 2 možnosti pro vybarvení rohů, 2 možnosti pro vybarvení středů stran a nakonec 2 možnosti vybarvení středu čtverce, celkem tedy skutečně $2^3 = 8$ možností.

- **Rotace o** $180°$: nyní každé políčko jednoznačně určuje vybarvení toho přesně „naproti" němu, obdobně jako výše je tedy vybarvení celého čtverce určeno vybarvením 4 políček na okraji a jednoho uprostřed. Celkem tedy máme $2^5 = 32$ možností.
- **Rotace o** $270°$: stejně jako u rotace o $90°$, máme 8 možností.
- **Překlopení podle svislé osy**: políčka vlevo určují, jak budou vypadat políčka vpravo, políčka uprostřed můžeme obarvit libovolně. Celkem tedy máme 6 stupňů volnosti, což nám dává $2^6 = 64$ možností.
- **Překlopení podle vodorovné osy**: totéž co svislá osa, 64 možností.
- **Překlopení podle hlavní diagonály**: totéž co svislá osa, 64 možností.
- **Překlopení podle vedlejší diagonály**: totéž co svislá osa, 64 možností.

Nyní již stačí dosadit a získáme, že odpovědí na úlohu je číslo

$$\frac{1}{8}(512 + 8 + 32 + 8 + 64 + 64 + 64 + 64) = 102.$$

Obdobně můžeme přistupovat k náramkům, nebudeme počítat každou symetrii zvlášť, ale rovnou si například rozmyslíme, že symetrické rotace (tedy například rotace o $36°$ a $324°$) budou dávat stejný výsledek, stejně tak všech 5 symetrií podle os stran dá stejný výsledek a všech 5 symetrií podle os úhlů dá stejný výsledek. Počítejme tedy po těchto skupinách.

- **Identita**: Máme celkem $\binom{10}{5} = 252$ možností, jak vybrat pozice pro černé korálky, zbylé pozice zaplníme bílými.
- **Rotace o** $36°$ **a** $324°$: každý korálek musí mít stejnou barvu jako korálek následující, to ale nejde. Tyto rotace tedy nezachovávají žádnou možnost.
- **Rotace o** $72°$ **a** $288°$: každý druhý korálek musí mít stejnou barvu, to nám dává pouze dvě možnosti (pokud bude jedna takto vzniklá pětice černá, druhá musí být nutně bílá).

- **Rotace o** 108° **a** 252°: každý třetí korálek musí mít stejnou barvu – to ale znamená (po „oběhnutí pár koleček“), že musí mít stejnou barvu všechny korálky, nula možností.
- **Rotace o** 144° **a** 216°: každý čtvrtý korálek musí mít stejnou barvu – to ale znamená (znovu „po oběhnutí kolečka“), že každý druhý korálek musí mít stejnou barvu, což nás znovu nechává s dvěma možnostmi.
- **Rotace o** 180°: každý korálek musí mít stejnou barvu jako korálek naproti – to by ale znamenalo, že korálky tvoří páry podle své barevnosti, museli bychom tedy mít sudý počet černých i sudý počet bílých korálků. To ale nejde, proto zde máme znovu nula možností.
- **Symetrie podle os stran**: každý korálek musí mít stejnou barvu jako korálek, který je s ním souměrně sdružený podle osy zvolené strany – to ale dle stejného argumentu jako výše nejde, proto tady nemáme žádnou validní možnost.
- **Symetrie podle os úhlů**: na každé straně od osy máme 4 korálky, které musí mít stejnou barvu jako jejich protějšky. Abychom se vyvarovali předchozím situacím, musí mít korálky ležící na ose nutně každý jinou barvu, což můžeme provést dvěma možnostmi, a ke každé z těchto dvou možností máme $\binom{4}{2} = 6$ možností, jak zvolit barvu korálků ležících mimo osu (na každé straně od osy musí být právě dva černé korálky, máme čtyři možnosti, kam je umístit). Celkem nám tyto osové symetrie dávají 12 možností.

Dohromady tedy dosazením do vzorce dostáváme překvapivě malý počet

$$\frac{1}{20}(252 + 2 \cdot 2 + 2 \cdot 2 + 5 \cdot 12) = 16.$$

Všechny tyto možnosti jsou znázorněny na konci textu (obr.5).

Dodatky

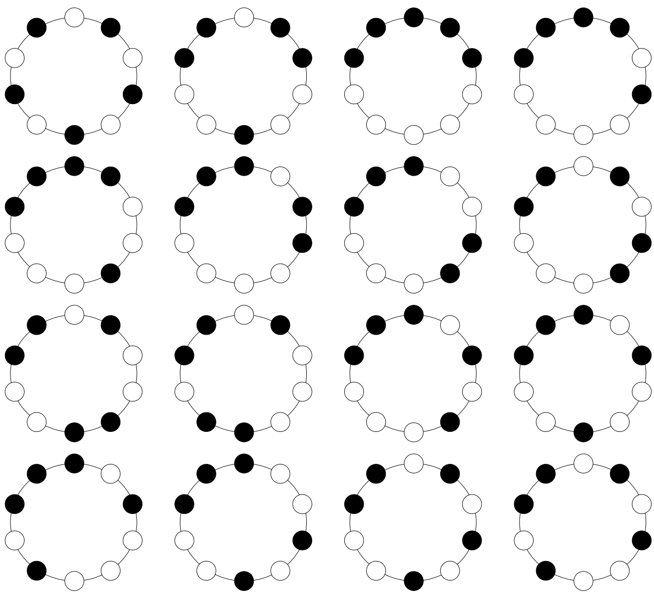
Burnsideovo lemma nachází využití nejen v elementární kombinatorice, umožňuje ale nalézt odpovědi na zajímavější problémy z různých oblastí matematiky. Uvedeme třeba (jen pro ilustraci!) jeden příklad z univerzální algebry, který můžeme užitím Burnsideova lemmatu vyřešit poměrně efektivně.

Nalezněte počet čtyřprvkových množin vybavených jednou 3-nární operací (zobrazením $X \times X \times X \to X$) až na isomorfismus.[3)]

Poznámka 1. Množiny X a X' vybavené operacemi f a f' jsou izomorfní, existuje-li bijekce $g\colon X \to X'$ taková, že pro každá $x_1, x_2, x_3 \in X$ platí $g(f(x_1, x_2, x_3)) = f'(g(x_1), g(x_2), g(x_3))$.

Toto využití také více zdůrazňuje sílu teorie grup. Všimněme si, že jsme v jistém kroku všechna tvrzení odvodili plně abstraktně, kdykoliv proto v našem problému vystupuje objekt mající grupovou strukturu, můžeme na něj aplikovat všechna obecně dokázaná tvrzení – nezáleží na problému jako takovém, pouze na jeho struktuře.

Tyto myšlenky jsou ale jen malými střípky ukazujícími pár myšlenek abstraktní algebry. Ta sama o sobě nabízí plno krásných tvrzení, a je-li o tom v této fázi čtenář alespoň trochu přesvědčen, splnil tento text svůj účel.



Obr. 5: Řešení motivační úlohy s náramky

3) Výsledek: 14178431955039102651224805804387336192, viz posloupnost A091510 na `oeis.org`