Jak číst seriál

Ahoj,

vítáme vás u letošního seriálu zaměřeného na teorii grup, který pro vás letos píší Filip Bialas a Kuba Löwit. Pokud nevíte, co to vůbec taková grupa je, ale rádi byste to zjistili, tak jste tady správně. I když se jedná o vysokoškolské téma, měl by být text při pozorném čtení srozumitelný a pochopitelný i pro běžného středoškoláka se zájmem o matematiku. V průběhu celého roku vás ve třech dílech provedeme zajímavými partiemi matematiky s grupami souvisejícími.

Vypracovanou teorii se budeme snažit i aplikovat na specifické případy – v prvním díle se bude jednat o jednoduchá tvrzení z teorie čísel, která se nám s použitím grup povede dokázat velmi elegantně, o geometrická zobrazení a o Pellovu rovnici. Grupy původně vznikly při zkoumání permutací v souvislosti s důkazem, že neexistuje obecný vzorec pro řešení polynomiálních rovnic pátého a vyššího stupně. Na tento důkaz bude seriál bohužel moc krátký, ale k důkladnému zkoumání permutací se dostaneme v druhém díle.

V seriálu se budou vyskytovat úlohy označené jako „Cvičení“. Doporučujeme zkusit si takové úlohy vyřešit nejdřív samostatně. Pokud se vám to ale nepovede, nezoufejte a přečtěte si řešení, které se bude nacházet na konci daného dílu. Zajímavější cvičení budeme občas nazývat vzletně slovem „Úloha“. Úlohy mohou být těžší a znalost jejich řešení nebude nutná k dalšímu čtení seriálu. Proto si můžete nechat na řešení volný čas až po přečtení seriálu. U cvičení bychom ale byli rádi, kdybyste si po chvíli přemýšlení přečetli řešení, a až potom pokračovali ve čtení textu. Na konci každého dílu každopádně naleznete řešení jak cvičení, tak i úloh.

Určité části mohou být těžší na pochopení, některé z nich ale nebudou třeba pro porozumění zbytku. Pokud se tedy v nějakém odstavci zaseknete, můžete ho zkusit přeskočit.

I když nepřečtete vše, určitě si zkuste vyřešit tři seriálové úlohy. Tyto úlohy by se měly týkat různých částí daného dílu a pro některé z nich by mělo stačit rozumět několika základním pojmům.

V případě jakýchkoliv nejasností v seriálu se nás nebojte kontaktovat na mailech *f.bialas26@gmail.com* nebo *jakub.lowit@gmail.com*.

Teorie grup I – Moc abstrakce

The theory of groups is a branch of mathematics in which one does something to something and then compares the results with the result of doing the same thing to something else, or something else to the same thing.

James R. Newman

Prolog I

Po dlouhé středověké odmlce se v Evropě v 16. století znovu probouzí matematika. S Eulerem, Gaussem a mnoha dalšími dochází na přelomu 18. a 19. století k obrovskému skoku kupředu. Rozvíjejí se úplně nové směry v geometrii, teorii čísel i algebře. Sám Euler už vlastně ve svých pracích o modulární teorii čísel dokazuje různá tvrzení o grupách – jen o tom neví. Podobně Gauss po něm.

Ve stejné době Lagrange při studiu algebraických rovnic nalézá souvislost jejich řešitelnosti s jakýmsi „prohazováním“ jejich kořenů. O pár let později přichází mladý norský matematik Abel. Navzdory chudobě se s využitím vládního grantu dostává do Paříže, kde se snaží prosadit. Přitom se mu daří vyřešit jednu z palčivých otázek tehdejší matematiky – dokazuje totiž obecnou neřešitelnost rovnic pátého (a vyššího) stupně. Jeho práce je ale založena a nedoceněna, a tak se smutně vrací zpět domů, kde posléze před očima své snoubenky umírá na tuberkulózu. Je trochu ironické, že dva dny po jeho smrti je v Paříži jeho práce znovu nalezena, bouřlivě oceněna, a posléze je mu uděleno místo na univerzitě v Berlíně.

Nikdo zatím slovo grupa nezná – její silueta už se ale rýsuje za pokrokovými pracemi mnohých matematiků. K její abstraktní definici sice ještě povede dlouhá cesta, první krůčky už ale byly vykonány.

Konkrétní versus abstraktní

Než si definujeme, co to grupa je, rádi bychom zdůraznili rozdíl mezi konkrétními a abstraktními objekty v matematice. Samozřejmě že celá matematika je v jistém smyslu abstraktní – nejde ji pěstovat na zahrádce nebo si ji schovat do šuplíku. To zde ale nemáme na mysli.

Když mluvíme o konkrétním matematickém objektu, myslíme tím něco, jako jsou třeba reálná čísla. To je hromádka prvků nějaké množiny, které navíc umíme sčítat, násobit, porovnávat a podobně. Když si pak o takovém objektu položíme nějakou otázku, v principu na ni existuje jednoznačná odpověď. Naproti tomu odpovídajícím abstraktním objektem by byla jakási sada pravd (axiomů), které o reálných číslech platí. Když budeme takovou abstraktní teorii zkoumat, jistě tím zjistíme cenné informace o reálných číslech, možná ale i o dalších konkrétních objektech, které tyto axiomy splňují.

Abstraktní přístup má mnoho výhod – zejména tu, že se nám několika pojmy daří vystihnout nepřeberné množství odlišných věcí, díky čemuž pak můžeme nacházet nečekané souvislosti. Přitom ale musíme být velmi ostražití – pokud mluvíme o nějakém abstraktním objektu (jako budeme za chvíli), typicky vlastně ani nevíme, co zkoumáme (respektive **co všechno** zkoumáme). Pokud to

však budeme mít na paměti, není se čeho obávat.

Zobrazení

Po celou dobu seriálu budeme pracovat s různými zobrazeními[1], připomeňme si tedy, oč jde.

Definice. *Zobrazením* f množiny A do množiny B rozumíme cokoli, co každému prvku $a \in A$ přiřadí právě jeden prvek z B. Ten pak značíme $f(a)$.

Fakt, že f zobrazuje množinu A do množiny B, někdy zkráceně zapisujeme jako $f : A \to B$. Podobně někdy píšeme $f : a \mapsto b$, když chceme říct, že obrazem prvku a je b.

Když na sebe dvě zobrazení „navazují“ (tedy první z nich vede tam, kde druhé začíná), lze je složit, čímž získáme opět zobrazení. Složením zobrazení f, g myslíme zobrazení, které vznikne provedením nejprve f a následně g. To značíme $g \circ f$, neboli zobrazení skládáme v pořadí zprava doleva.[2]

Skládání zobrazení má zajímavou vlastnost. Pokud na sebe postupně tři zobrazení f, g, h navazují, pro jejich složení platí rovnost $f \circ (g \circ h) = (f \circ g) \circ h$. Slovy, kdykoli něco zobrazujme pomocí této složeniny, je jedno, jestli nejprve provedeme $(g \circ h)$ a potom f, nebo nejprve h a potom $(f \circ g)$. Zjednodušeně proto můžeme vzniklou funkci zapisovat bez závorek jako $f \circ g \circ h$ a představovat si ho tak, že nejdřív provedeme h, pak g a nakonec f. Právě popsaná vlastnost se nazývá *asociativita* a bude nás provázet celým seriálem. Lidově: asociativita říká, že závorky si můžeme strčit za klobouk.

Definice. Zobrazení $f : A \to B$ nazveme:

(1) *prosté*, jestliže se každé dva různé prvky z A zobrazí na různé prvky z B;
(2) *na*, jestliže se na každý prvek z B zobrazí alespoň jeden prvek z A;
(3) *bijekce*, jestliže je zároveň prosté i na.

Bijekce jsou tedy ta zobrazení, které „spárují“ prvky A s prvky B. Ke každé bijekci f z A do B přitom existuje inverzní bijekce f^{-1} vedoucí z B do A, která vznikne „převrácením“ f. Je dobré si uvědomit, že složením dvou funkcí, které jsou prosté, dostaneme opět prostou funkci. Podobně složením dvou funkcí, které jsou na, dostaneme opět funkci s toutéž vlastností. Dohromady tedy složením dvou bijekcí dostaneme opět bijekci (což je také v podstatě zřejmé).

Se zobrazeními úzce souvisí pojem *operace*. Operací budeme myslet něco, co nám z nějakého pevného počtu seřazených prvků z určité množiny vyrobí jednu jinou věc. Klasickým příkladem operace je třeba násobení dvou čísel na množině reálných čísel. Jedná se o operaci *binární*, neboť jsme do ní vložili dvě čísla. Funkce lze chápat jako operace *unární*, tj. s jedním vstupem. Můžeme dokonce uvažovat i operace, která nemají žádný vstup, a vždy nám tedy musí vrátit stejnou věc. Uvažování těchto divných operací nám později ušetří trochu práce.

Definice. O operaci $\star$ řekneme, že je *uzavřená* na množině M, pokud výsledek této operace s libovolnými dvěma prvky z této množiny leží také v M.

Jako operaci, která není uzavřená na nějaké množině, můžeme uvést třeba sčítání na lichých číslech, například protože výsledkem $1 + 1$ není liché číslo. Zato na sudých číslech sčítání uzavřené je.

Použití binární operace $\star$ na uspořádanou dvojici prvků $a, b \in M$ budeme psát jako $a \star b$, tedy stejným způsobem, jakým běžně používáme $+$, $\cdot$ a podobně.

Definice. Binární operace $\star$ na množině M je *asociativní*, pokud pro libovolné tři prvky $a, b, c \in M$ platí $(a \star b) \star c = a \star (b \star c)$.

[1] Pojmy *zobrazení* a *funkce* znamenají to samé, pouze se používají při jiných příležitostech – podobně jako se při různých příležitosti pijí různé čaje.

[2] To má historické důvody. Přestože je to na první pohled kontraintuitivní, je to tak běžné a většinou přehlednější.

Jak už jsme komentovali dříve, asociativita hlásá „Zapomeňte na závorky!“. Definice nám sice dovoluje zapomenout pouze na jednu závorku, induktivně si ale lze rozmyslet, že pak už můžeme zapomenout na všechny závorky napsané v libovolném výrazu.

Povídání o funkcích a operacích uzavřeme jednou těžší úlohou.

Úloha 1. Mějme konečnou množinu X a nějakou binární asociativní operaci $\star$, která je na X uzavřená. Dokažte, že pak existuje prvek $a \in X$, který splňuje $a \star a = a$.

Grupa

Nyní už nám nic nebrání definovat, co to ta grupa vlastně je.

Definice. *Grupou* nazýváme množinu G spolu s binární operací $\cdot$, která je na množině G uzavřená a navíc má následující vlastnosti:

(1) Existuje prvek $e \in G$ takový, že pro každé $g \in G$ platí $e \cdot g = g \cdot e = g$. Tomuto prvku se říká *neutrální*.
(2) Pro každý prvek $g \in G$ existuje prvek $h \in G$ takový, že $g \cdot h = e = h \cdot g$. Prvek h poté nazýváme prvkem *inverzním* k g a značíme ho g^{-1}.
(3) Binární operace $\cdot$ je asociativní, tedy pro každé tři prvky $a, b, c \in G$ platí $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

V definici jsme psali binární operaci pomocí násobicí tečky, což ale vůbec neznamená, že tato operace opravdu musí být nám známé násobení čísel. Mohli bychom ji klidně označovat pomocí znaménka plus[3] nebo úplně jiného symbolu. Použité *multiplikativní* značení je ale asi nejpoužívanější a postupem času budeme stejně jako u násobení tečku vynechávat. Z praktických důvodů budeme o grupové binární operaci často mluvit jako o *násobení*, i když to vlastně násobení v běžném smyslu vůbec nemusí být. Když budeme jeden prvek násobit několikrát sám sebou, budeme to značit jako umocňování. Nebude-li hrozit nedorozumění, budeme grupu i její nosnou množinu označovat jedním stejným velkým písmenem (nejčastěji G, H, K); prvky grupy budeme značit malými písmeny (nejčastěji g, h, a, b).

Opusťme nyní na chvíli abstraktní přemýšlení a uveďme si pár příkladů toho, co je grupa, a co naopak není.

Příklad. Celá čísla s binární operací sčítání grupu tvoří – neutrálním prvkem je 0, inverzním prvkem k a je číslo $-a$. Tuto grupu budeme značit $\mathbb{Z}$.

Příklad. Pro každé přirozené číslo n tvoří zbytky po dělení číslem n grupu (s binární operací sčítání). Přesněji tuto grupu tvoří množina $\{0, 1, \ldots, n-1\}$ a výsledkem operace provedené s prvky a, b je zbytek $a + b$ po dělení n. Popsanou grupu budeme označovat $\mathbb{Z}_n$.

Příklad. Kladná reálná čísla s binární operací násobení tvoří grupu – neutrálním prvkem je 1, inverzním prvkem k a je číslo $\frac{1}{a}$.

Příklad. Přirozená čísla $\mathbb{N}$ grupou nejsou, třeba protože v ní není žádný neutrální prvek.

Co nám vlastnosti binární operace z definice vlastně říkají? První nám zaručuje existenci něčeho, co při násobení nic nemění – tedy jakési „jedničky“. Samotná tato vlastnost nám o struktuře grupy vlastně moc neříká, ale je důležitá kvůli dobrému popsání druhé vlastnosti – existence inverzního prvku. Existence inverzního prvku nám umožňuje jakési „dělení“. Třetí vlastnost je asociativita, o které jsme se bavili už dříve. V praxi z ní dostáváme to, že nemusíme používat závorky a zápisy přesto budou jednoznačné. Např. výraz $a \cdot b \cdot b^{-1} \cdot a^{-1}$ můžeme postupně upravovat následovně: $a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = (a \cdot e) \cdot a^{-1} = a \cdot a^{-1} = e$ (závorky jsme zde použili, jen aby bylo jasné, jakou operaci zrovna provádíme; výsledek nijak neovlivnily).

Operaci tedy můžeme závorkovat, jak se nám zlíbí, žádná vlastnost nám ale nezaručuje, že je tato operace *komutativní*. Komutativní operací je taková, kde pro všechna a, b platí $a \cdot b = b \cdot a$. Brzy si ukážeme, že opravdu existují i grupy, jejichž binární operace komutativní není. Třeba výraz

[3] Toto značení se v některých souvislostech i používá.

$a \cdot b \cdot a^{-1}$ nemůžeme bez znalosti struktury grupy nijak obecně upravit, neboť nemůžeme přehazovat pořadí členů a obecně nevíme, co je výsledkem $a \cdot b$ nebo $b \cdot a^{-1}$.

Stejně tak musíme být opatrní, když budeme pracovat s rovnicemi. Můžeme podobně jako při řešení klasických rovnic vzít další prvek a provést s ním binární operaci na obou stranách rovnice. Je ale třeba si dát pozor, abychom tuto operaci prováděli, že tuto operaci provádíme vždy ze stejné strany (z $a = b$ plyne $g \cdot a = g \cdot b$ nebo také $a \cdot g = b \cdot g$, ale obecně ne $a \cdot g = g \cdot b$). Toto vynásobení je v grupě ekvivalentní úpravou rovnice:

Tvrzení. *Nechť $a, b, g \in G$, pak $a = b \Leftrightarrow g \cdot a = g \cdot b$ (a obdobně $a = b \Leftrightarrow a \cdot g = b \cdot g$).*

Důkaz. Dokážeme dvě implikace. Pokud $a = b$, pak už také $g \cdot a = g \cdot b$, protože naše operace musí dávat na stejných uspořádaných dvojicích prvků stejný výsledek. K důkazu druhé implikace $g \cdot a = g \cdot b \Rightarrow a = b$ nám stačí vynásobit obě strany předpokladu zleva prvkem g^{-1} a dostaneme $g^{-1} \cdot g \cdot a = g^{-1} \cdot g \cdot b$, což upravíme jako $(g^{-1} \cdot g) \cdot a = (g^{-1} \cdot g) \cdot b$, a po zkrácení dostaneme $e \cdot a = e \cdot b$, tedy $a = b$, jak jsme chtěli dokázat.

Příklady grup

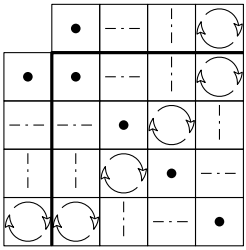
V minulé části jsme si zadefinovali grupu a bavili jsme se o tom, jak s ní zhruba můžeme pracovat. Pár konkrétních příkladů jsme již viděli, ale teď si ukážeme, že grupy mohou nabývat ještě mnohem rozmanitějších podob. A to je fajn – kdyby nebylo grupou hodně různých konkrétních objektů v matematice, nemělo by moc smysl ji definovat a přemýšlet o ní abstraktně.

Nejdříve se zamyslíme, jak můžeme vůbec popsat, jak grupa vypadá. Nejjednodušším způsobem u grup, jejichž množina G má málo prvků, je asi vypsat výsledky binární operace pro všechny možné dvojice prvků do ní vložené. Tedy vypsat jakousi multiplikativní tabulku. Podobnou tabulku si vytváříme třeba pro malou násobilku; zde nám bude ale navíc záležet na pořadí prvků v binární operaci, protože tato operace nemusí být komutativní – domluvíme se na tom, že jako první budeme brát prvek odpovídající řádku tabulky.

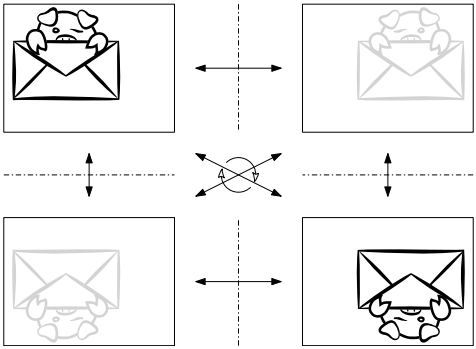
Příklad. Nejhloupějším a nejtriviálnějším příkladem grupy je grupa obsahující pouze jeden prvek, který musí být nutně neutrální (tento prvek musí v každé grupě existovat).

Příklad. Kleinova grupa V je grupa mající čtyři prvky e, a, b, c a následující multiplikativní tabulku:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



Kleinovu grupu si můžeme přiblížit i geometricky. Představme si obdélníkový list papíru položený na stole. Máme nyní čtyři způsoby, jak tento list poobracet tak, aby jeho obrys na stole zůstal pořád stejný (můžeme ho otočit o 180° přímo na stole, převrátit ho podle svislé osy, převrátit ho podle vodorovné osy nebo ho nechat ležet na místě). Těmto čtyřem způsobům můžeme přiřadit prvky Kleinovy grupy, přičemž výsledek binární operace nám bude říkat, jakým způsobem jsme mohli otočit papír rovnou místo toho, abychom ho otáčeli dvakrát za sebou. Rovnost $a^2 = b^2 = c^2 = e$ například vyjadřuje skutečnost, že pokud papír dvakrát otočíme stejným způsobem, ocitne se opět v původní pozici.



Příklad. Při představě Kleinovy grupy jsme si hráli s obracením a otáčením obdélníka. Podobně můžeme definovat grupu, která bude odpovídat otáčení a obracení pravidelného n-úhelníka, tak aby byl jeho obrys pořád stejný. Tato grupa má $2n$ prvků – identitu, která nechává ležet n-úhelník na místě; $n-1$ neidentických otočení; a n osových souměrností. Právě popsaná grupa se nazývá *dihedrální* a značí se D_{2n}[4]. Všimněte si, že binární operace v této grupě není komutativní – například při skládání libovolné osové souměrnosti a otočení o $\frac{360^\circ}{n}$ záleží na pořadí.

Sami si můžete ověřit, že popsané grupy opravdu splňují definici.

Celou multiplikativní tabulku ale nemůžeme vypsat vždy. Pro grupy s velkým počtem prvků by to bylo časově velmi náročné, a co teprve pro grupy, jejichž množina má nekonečnou velikost? Už třeba grupa $\mathbb{Z}$ celých čísel se sčítáním má nekonečně prvků. Z multiplikativní tabulky se navíc těžko poznává, jestli je binární operace vůbec asociativní. Pokud tedy chceme nějakou novou grupu vyrobit, multiplikativní tabulky nám pomohou jen stěží. Grupy si proto musíme představovat jinak, často je to tak ale i přirozenější. Protože se často budeme bavit o velikosti grupy, zavedeme následující pojem:

Definice. *Řádem grupy* nazveme velikost množiny G. Pokud je řád grupy nekonečný, pak o této grupě budeme říkat, že je *nekonečná*, a ostatním budeme říkat *konečné*. Řád grupy budeme označovat pomocí $|G|$.

Mohli jste si všimnout, že všechny dosud zmíněné grupy (kromě dihedrální) měly komutativní binární operaci. Takové grupy budeme dále nazývat *abelovské*[5]. Nyní si ukážeme další případ neabelovské grupy. Začneme tou možná nejdůležitější skupinou grup vůbec, a sice *symetrickými grupami*.

Symetrické grupy poprvé

Definice. *Symetrická grupa* na množině X je grupa všech permutací této množiny vybavená binární operací skládání. Budeme ji značit S_X.

Permutacemi ale nemyslíme jednotlivá seřazení prvků množiny X, nýbrž zobrazení, které nám říká, jak tyto prvky máme zamíchat. Binární operace skládání nejdříve provede jedno zamíchání a poté na už zamíchaných prvcích druhé. Jedná se ale skutečně o grupu? Musíme ověřit všechny axiomy. Složením dvou zamíchání dostaneme znovu zamíchání množiny, takže operace skládání je na S_X uzavřená. Neutrálním prvkem bude zamíchání, která nedělá nic. Inverzní prvek vždy existuje, prostě zamícháme prvky tak, jak byly předtím. Asociativita se dá také lehce rozmyslet.

[4]Do dolního indexu nepíšeme počet vrcholů mnohoúhelníka, nýbrž počet prvků této grupy

[5]Na počest zmíněného norského matematika Nielse Henrika Abela.

Jak jste si mohli všimnout, permutace množiny X jsou formálně právě bijekce z množiny X do X a skládání permutací je to samé jako skládání těchto bijekcí. Invertování bijekcí jako zobrazení přesně odpovídá jejich invertování v S_X.

Je jasné, že pokud máme dvě množiny se stejným počtem prvků, pak bude jejich symetrická grupa „vypadat“ úplně stejně. Pro konečné množiny X budeme častěji používat značení S_n, kde n je počet prvků X. Řád této grupy bude $n! = n(n-1)(n-2)\cdots 2\cdot 1$ (pro první prvek máme n možností, kam ho přesunout; pro druhý $n-1$ atd.). Všimněme si, že pro $n > 2$ není grupa S_n abelovská. Uvažujme např. následující dvě permutace: p – prohození prvního a druhého prvku; q – prohození prvního a třetího prvku. Pokud nejdříve provedeme permutaci p a poté q (protože permutace je jen určitým typem zobrazení, zapisujeme toto skládání jako qp – permutace provádíme postupně zprava), tak nám výsledné přerovnání přesune první prvek na druhý prvek, druhý na třetí a třetí na první. Permutace pq nám ale přesune první na třetí, druhý na první a třetí na druhý, takže $pq \neq qp$.

Grafické znázornění permutace a jejího rozkladu na cykly

Každou permutaci na konečné množině (tedy prvek grupy S_n) můžeme rozložit do takzvaných *cyklů*. Uvažujme permutaci p a vezměme si nějaký prvek i množiny X. Zaveďme nyní následující posloupnost: $a_0 = i$, $a_n = p(a_{n-1})$ pro přirozená n. Jelikož je v množině X pouze konečně mnoho prvků, musejí se v posloupnosti nějaké dva členy rovnat. Jaké číslo se jako první zopakuje? Ukážeme, že to musí být nutně i. Jelikož je p bijekce, tak se na žádné číslo nezobrazí dvě různá. Žádné jiné číslo než i se ale nemůže poprvé zopakovat, protože pak by byl nutně v posloupnosti zopakovaný již jeho předchůdce. Označíme-li j nejmenší index větší než 0 takový, že $a_j = a_0$, pak říkáme, že j je *délka* cyklu a že i patří do cyklu $(i\ p(i)\ p(p(i))\cdots p^{j-1}(i))$. Z tohoto cyklu vidíme, kam se zobrazí všechna čísla, která se v něm nacházejí (poslední na to první, ostatní na to o jedno dál vpravo). Tuto konstrukci můžeme opakovat pro čísla, která se zatím ještě v žádném cyklu nevyskytla. Nakonec budeme mít každé číslo právě v jednom cyklu.

Permutace z předchozího odstavce p, q v grupě S_4 bychom mohli tímto způsobem zapsat jako $p = (12)(3)(4), q = (13)(2)(4)$. Cykly délky 1 zřejmě nejsou pro jednoznačnost zápisu nutné, takže je budeme vynechávat – můžeme tedy psát $p = (12), q = (13)$.

Nyní už můžete tušit, jakých mnoha různých podob může grupa v konkrétních případech nabývat (struktura celých čísel a struktura permutační grupy opravdu není moc podobná). Síla abstraktního přístupu ale spočívá v tom, že můžeme dokazovat věty přímo o obecných grupách – tedy věty, které poté budou platit ve všech těchto konkrétních případech.

Jak to v grupách funguje?

Už jsme se přesvědčili o tom, že se pod pojmem grupy opravdu něco konkrétního schovává, pojďme tedy dokázat některé základní vlastnosti grup abstraktně. Při tom si můžeme všimnout, jak dobře tyto vlastnosti vystihují symetrické grupy – ještě aby ne, když z nich historicky naše abstraktní definice vznikla.

Cvičení 1. Dokažte, že v každé grupě existuje právě jeden neutrální prvek.

Cvičení 2. Nechť g je prvek grupy G. Pak existuje právě jeden prvek k němu inverzní. Navíc pokud platí $gh = e$, pak už nutně $hg = e$ (a stejně tak z $hg = e$ plyne $gh = e$).

Cvičení 3. Nechť g je prvek v G a g^{-1} je prvek k němu inverzní. Pak g je inverzní k g^{-1}.

Cvičení 4. Nechť g je prvek v G a n přirozené číslo. Dokažte, že $(g^n)^{-1} = (g^{-1})^n$. S využitím tohoto cvičení můžeme definovat i g^k, kde k je záporné celé číslo, pomocí vztahu $g^k = (g^{-1})^{-k}$.

Toto bylo pár jednoduchých příkladů, co můžeme zvládnout dokázat obecně o všech grupách. První dva výsledky nám umožňují formulaci, která bude dále velmi příjemná. Díky jednoznačnosti inverzního a neutrálního prvku můžeme mluvit o dalších dvou operacích v grupách. Jedné unární, která vezme prvek a přiřadí prvek k němu inverzní, a jedné, která nebere jako vstup nic a vrátí nám neutrální prvek. Když budeme dále mluvit o *grupových operacích*, tak budeme myslet právě binární operaci $\cdot$ a tyto dvě.

Když už víme, že je inverzní prvek jednoznačný, tak ho snadno najdeme:

Cvičení 5. Najděte inverzní prvek k součinu ab.

Nyní se ale přesuneme dále a začneme zkoumat, jaké „menší“ grupy mohou grupy obsahovat.

Podgrupy

Definice. Mějme grupu G s binární operací $\cdot$. Je-li H podmnožina G uzavřená na všechny grupové operace, pak H nazveme *podgrupou* G (značíme $H \leq G$)[6].

Uzavřeností na všechny grupové operace myslíme, že pro libovolné dva prvky $g, h \in H$ je $gh \in H$, inverzní prvek ke g leží v H a neutrální prvek e je v H. Každá grupa G má dvě *triviální* podgrupy – celou grupu G a triviální grupu obsahující pouze neutrální prvek. Další podgrupy G mít může, ale nemusí. Později si ukážeme, že třeba $\mathbb{Z}_p$, kde p je prvočíslo, žádné netriviální podgrupy nemá. Naopak třeba $\mathbb{Z}$ má hned nekonečně mnoho podgrup. Pro každé přirozené n totiž můžeme sestrojit grupu celých čísel dělitelných číslem n se sčítáním. Tato grupa je pro libovolné přirozené n zřejmě podgrupou $\mathbb{Z}$ (a pro $n \neq 1$ netriviální podgrupou).

Jak popsat nějakou konkrétní podgrupu? Často to můžeme udělat tak, že uvedeme jen několik prvků, které ji potom celou „vytvoří“. Budeme chtít vlastně najít „nejmenší“ grupu, která obsahuje všechny tyto prvky.

Definice. O n-tici prvků $\{a_1, a_2, \ldots, a_n\}$ podgrupy H grupy G budeme říkat, že ji *generují*, pokud je H nejmenší podgrupa G, která všechny tyto prvky obsahuje. Potom značíme $H = \langle a_1, a_2, \ldots, a_n \rangle$.

Není jasné, že taková nejmenší podgrupa vůbec existuje a že je jednoznačně určena. Je ale vidět, že grupa, která danou n-tici prvků obsahuje, musí obsahovat i všechny součiny několika prvků z dané n-tice nebo jejich inverzů. Co víc, množina všech takovýchto součinů již je grupa, protože součin dvou součinů nám vytvoří jiný součin; identita mezi naše prvky patří (to ukážeme pomocí součinu $a_1 \cdot a_1^{-1} = e$); a konečně inverzní prvek k $a_{\alpha_1}^{\beta_1} \cdot a_{\alpha_2}^{\beta_2} \cdots a_{\alpha_k}^{\beta_k}$ je zřejmě $a_{\alpha_k}^{-\beta_k} \cdot a_{\alpha_{k-1}}^{-\beta_{k-1}} \cdots a_{\alpha_1}^{-\beta_1}$. Takto popsaná grupa obsahuje jen prvky, které nutně obsahovat musí, takže je nejmenší možná.

Jako příklad si vezměme $G = S_n$, kde $n \geq 3$. Pak podgrupa $\langle (1,2) \rangle$ obsahuje právě transpozici $(1,2)$ a identitu, protože jakýmkoliv kombinováním skládání permutace, která přehazuje první dva prvky (a je sama sobě inverzí), nedostaneme jistě žádnou jinou permutaci než identitu a ji samotnou. Jiným příkladem může být podgrupa $\langle (1,2), (2,3) \rangle$ – tato podgrupa jistě nebude obsahovat žádné permutace, které pohybují s jinými než prvními třemi prvky. Můžete si ale sami rozmyslet, že všech šest permutací, které nepohybují žádnými jinými než prvními třemi prvky, již vytvořit umíme.

Cvičení 6. Nechť H, K jsou dvě podgrupy grupy G. Pak $H \cap K$ je také podgrupa G.

Toto cvičení se dá zobecnit i na libovolný počet podgrup (klidně i nekonečný). Podgrupu G generovanou nějakou množinou díky tomu můžeme definovat jako průnik všech podgrup G, které tuto množinu obsahují.

Definice. Grupu nazveme *cyklickou*, pokud v ní existuje prvek, který ji celou generuje.

[6] Ano, používáme tu značení, které znáte ve významu porovnávání čísel – ale toto značení je dost výstižné; navíc už jsme si zvykli, že tečka nemusí znamenat násobení, tak nás to nemůže vyvést z rovnováhy.

Příkladem konečných cyklických grup jsou grupy $\mathbb{Z}_n$. Nekonečnou cyklickou grupou jsou celá čísla $\mathbb{Z}$.

Ukážeme si nyní, že všechny prvky cyklické grupy můžeme vlastně popsat hrozně jednoduše. Mějme grupu generovanou prvkem a. Potom všechny prvky této grupy získáme jako konečný součin prvků a nebo a^{-1}. Pokud ale narazíme vedle sebe na tyto dva různé prvky, můžeme je zkrátit. Všechny výrazy tedy můžeme krátit až do té doby, kdy se zde vyskytují buď jen a, nebo jen a^{-1}, nebo nám vyjde identita. Každý prvek cyklické grupy můžeme tedy napsat jako a^k, kde k je celé číslo.

Lehce si všimneme, že každá taková grupa je abelovská, neboť z asociativity pro libovolné dva prvky a^n, a^m je jejich součin $a^n a^m = a^{n+m} = a^m a^n$.

Definice. *Řádem prvku* a grupy G budeme rozumět řád cyklické podgrupy $\langle a \rangle$.

Pokud je řád prvku a konečný, tak je roven nejmenšímu přirozenému n takovému, že $a^n = e$. Předpokládejme pro spor, že by byl jiný. Pokud by byl počet prvků grupy $\langle a \rangle$ menší než n, pak by musely mezi prvky $a^0 = e, a^1 = a, a^2, \ldots, a^{n-1}$ být dva stejné – tedy $a^i = a^j$, kde $i < j$. Vynásobením a^{-i} ale dostaneme $e = a^{j-i}$, kde $j - i$ je přirozené číslo menší než n, což není možné. Aby tedy mohl být řád jiný než n, musel by být větší. Ale $\langle a \rangle$ nemůže obsahovat více než n prvků, neboť každý exponent x můžeme napsat ve tvaru $x = kn + r$, kde k je celé a $0 \leq r < n$, a proto $a^x = a^{kn+r} = a^{kn} a^r = (a^n)^k a^r = e^k a^r = a^r$, což je spor. Například každý prvek $\mathbb{Z}$ kromě nuly má řád nekonečný; v grupě S_n má cyklus o k prvcích řád k; všechny prvky Kleinovy grupy kromě identity mají řád dva.

Shodnosti roviny

Vraťme se na chvíli do „reality“ a předveďme si jednu konkrétní grupu, která nám ukáže některá geometrická tvrzení z nového úhlu.

Definice. *Shodným zobrazením v rovině* nazveme každé zobrazení $\mathbb{R}^2 \to \mathbb{R}^2$, které zachovává vzdálenosti.

Souslovím „zachovává vzdálenosti“ myslíme fakt, že pro libovolné body $X, Y \in \mathbb{R}^2$ je jejich vzdálenost stejná jako vzdálenost jejich obrazů $f(X)$, $f(Y)$. Na první pohled je proto kupříkladu zřejmé, že taková funkce f je prostá, neboť různé body v rovině mezi sebou mají kladnou vzdálenost. Přitom samozřejmě známe různá shodná zobrazení jako otočení (rotace), posunutí (translace), osové symetrie (reflexe), středové symetrie a podobně. Jak ale vypadají všechna shodná zobrazení?

Uvažme nyní libovolné shodné zobrazení f a nějaký (nedegenerovaný) trojúhelník ABC v rovině. Obrazy bodů A, B, C budou opět tvořit trojúhelník. Protože je f shodné zobrazení, délky stran trojúhelníku $f(A)f(B)f(C)$ zůstanou nezměněny, tyto trojúhelníky tedy budou nutně shodné.

Rozmysleme si nyní, že obrazem bodů A, B, C už je f jednoznačně určeno. Vezměme tedy nějaký další bod X. Protože $|AX| = |f(A)f(X)|$ a $|BX = f(B)f(X)|$, máme pouze dvě možnosti, kam X zobrazit. Pomocí bodu C, který leží mimo přímku AB, pak umíme jednoznačně určit, ve které polorovině $f(X)$ leží. Přitom je jasné, že pokud takovým způsobem najdeme obrazy všech bodů roviny, dostaneme vskutku její shodné zobrazení.

Z uvedené konstrukce je navíc zřejmé, že každé shodné zobrazení f je dokonce bijekce. Identické zobrazení je očividně shodné zobrazení, shodná zobrazení můžeme jako bijekce invertovat, dokonce i skládat. Složení dvou shodných zobrazení také zachovává vzdálenosti bodů, dohromady tedy dostáváme, že shodná zobrazení v rovině spolu se skládáním tvoří grupu.[7]

Všechna shodná zobrazení v rovině lze navíc popsat velmi elegantně.

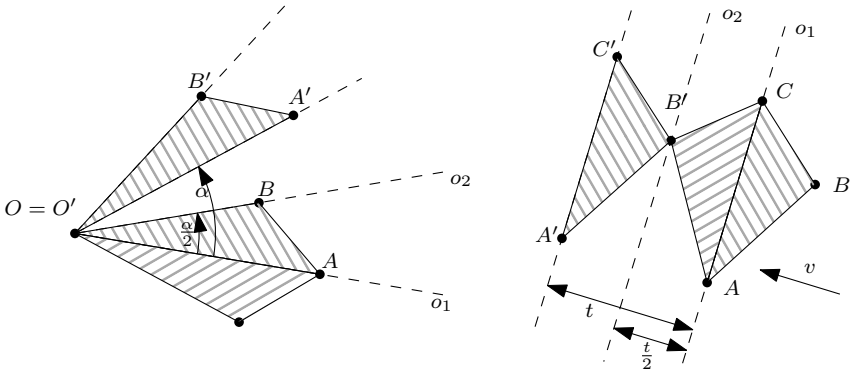
Tvrzení. *Grupa shodných zobrazení v rovině je generována osovými souměrnostmi.*

Důkaz. Už jsme si všimli, že shodná zobrazení odpovídají funkcím, které na sebe zobrazují dva shodné trojúhelníky ABC, $A'B'C'$. Takovou dvojicí trojúhelníků je už dané shodné zobrazení

[7] Na kterou se klidně můžeme dívat jako na podgrupu symetrické grupy $S_{\mathbb{R}^2}$.

f jednoznačně určena. Budeme tedy chtít ukázat, že každé dva shodné trojúhelníky na sebe lze zobrazit postupným použitím konečně mnoha osových symetrií, čímž budeme hotovi.

Nejprve si ale rozmysleme, jak pomocí osových symetrií získat otočení podle středu O o úhel α proti směru hodinových ručiček. K tomu stačí vzít libovolné dvě osy o_1, o_2, které prochází bodem O a svírají úhel $\frac{\alpha}{2}$, a složit příslušné souměrnosti v pořadí proti směru hodinových ručiček. Snadno nahlédneme, že vrcholy trojúhelníku OAB, kde $A \in o_1$, $B \in o_2$, se tak opravdu otočí o α proti směru hodinových ručiček. Popsané zobrazení je ale shodné, takže poloha ostatních bodů je již jednoznačně určena a musí odpovídat našemu otočení. Podobně, posunutí ve směru šipky v o vzdálenost t získáme složením osových souměrností podle os o_1, o_2, které jsou kolmé na směr v a vzdálené $\frac{t}{2}$.



Mějme tedy dva libovolné shodné trojúhelníky ABC, $A'B'C'$ a zkusme je na sebe zobrazit pouze pomocí osových symetrií. Nejprve označme v směr polopřímky AA', $t = |AA'|$ a proveďme odpovídající posunutí, které již umíme zapsat jako složení dvou osových symetrií. Nyní proto body A, A' splývají. Následně se podíváme, jestli jsou oba trojúhelníky stejně natočené. Přesněji, označme úhel mezi přímkami AB, $A'B'$ jako α. Posléze použijme na trojúhelník ABC otočení o úhel α se středem A, které opět umíme napsat jako složení dvou osových symetrií. Po jeho provedení už úsečky AB, $A'B'$ v tomto pořadí vrcholů splývají. Nakonec se podíváme, jestli jsou oba trojúhelníky stejně orientovány, to jest jestli C splývá s C'. Pokud ano (trojúhelníky jsou *přímo shodné*), neuděláme nic. Pokud ne (když jsou *nepřímo shodné*), vezmeme osu AB trojúhelník ABC podle ní zobrazíme, čímž splynou i poslední dva vrcholy.

Předešlé tvrzení není užitečné jen samo o sobě, vyplatí se také vědět, jak shodná zobrazení skutečně rozložit. Stejně by se ale mohlo zdát, že takový přístup ve skutečných geometrických úlohách využijeme jen stěží. Tento omyl zkusíme vyvrátit hravou úlohou.

Úloha 2. (Žabí porisma) V rybníce jsou kameny očíslované čísly $1, 2, \ldots, 2n$ a na břehu sedí žába. Ta postupně přeskočila všechny kameny v pořadí od 1 do $2n$, čímž se dostala zpět na místo, kde začínala.[8] Další den znovu přišla k rybníku, stoupla si na libovolné místo a opět postupně přeskákala všechny kameny. Dokažte, že zase skončila tam, kde tento den začínala.

Na závěr si ještě všimněme, že jakmile rozložíme nějaké shodné zobrazení na osové souměrnosti, okamžitě poznáme, jestli je přímá, nebo nepřímá. To totiž odpovídá tomu, zda je v jejím libovolném

[8]Přeskočením kamene rozumíme takový skok, že střed kamene leží přesně ve středu úsečky mezi počáteční a koncovou polohou žáby.

rozkladu sudý, nebo lichý počet souměrností. Speciálně platí, že přímá shodná zobrazení tvoří podgrupu grupy všech shodných zobrazení. Podobné situace ještě v budoucnu potkáme.

Lagrangeova věta

Nyní se přesuneme k důležité větě, která nám ukazuje základní vztah mezi grupou a jejími podgrupami.

Věta. *(Lagrangeova věta)*
Mějme konečnou grupu G a její podgrupu H. Potom $|H|$ dělí $|G|$.

Před samotným důkazem si nejdříve definujme následující pojem.

Definice. Levým *kosetem*[9] podgrupy H a prvku $g \in G$ nazveme množinu $gH = \{gh \mid h \in H\}$. Podobně můžeme definovat pravý koset.

V předchozí definici jsme použili značení gH pro množinu, která obsahuje všechny prvky vzniklé použitím libovolného prvku množiny H ve výrazu místo H. Podobné značení budeme dále používat již bez vysvětlení. Pokud nebudeme mít ve výrazu pouze jednu množinu, ale hned více, pak tím budeme myslet zkoušení všech kombinací. Např. AB, kde A, B jsou podmnožiny G, by byla množina všech prvků ve tvaru ab, kde $a \in A, b \in B$. Dále si můžeme všimnout, že takovéto násobení množin je asociativní, což plyne z asociativity násobení jednotlivých prvků.

Cvičení 7. Nechť H je podgrupa grupy G. Pak $HH = H$.

Proč jsou kosety užitečné k důkazu Lagrangeovy věty? Můžeme si všimnout, že všechny kosety budou mít $|H|$ prvků. Žádné dva různé prvky H totiž nemohou po vynásobení g zleva dát stejný výsledek, jak již víme z úplně prvního tvrzení. Dále si můžeme všimnout, že každý prvek g grupy G je alespoň v jednom kosetu obsažen – třeba v kosetu gH (pokud $e \in H$, pak $g \in gH$).

Dokážeme nyní odvážné tvrzení, a to, že když mají dva kosety neprázdný průnik, pak už jsou nutně stejné. (To by znamenalo, že každý prvek se nachází v právě jednom kosetu, který ale můžeme zapsat více způsoby – jako gH pro libovolný prvek g z daného kosetu). Uvažme dva kosety g_1H, g_2H s neprázdným průnikem – tj. existují $h_1, h_2 \in H$ taková, že $g_1h_1 = g_2h_2$. Vezmeme nyní libovolný prvek x BÚNO z g_1H a ukážeme, že leží i v g_2H. Jelikož x leží v g_1H, můžeme ho napsat jako $x = g_1h$ pro nějaké $h \in H$ a tento výraz můžeme upravovat:

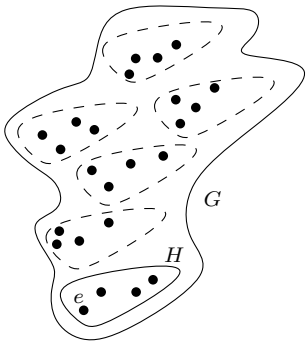
$$x = g_1h = g_1eh = g_1(h_1h_1^{-1})h = (g_1h_1)h_1^{-1}h = g_2h_2h_1^{-1}h = g_2(h_2h_1^{-1}h);$$

$h_2h_1^{-1}h$ leží jistě v H, neboť je to výsledek několika operací uvnitř H, na které je H uzavřená. Z toho ale plyne $x \in g_2H$. Každý prvek kosetu g_1H tedy leží i v g_2H a stejný postup můžeme použít i na dokázání, že všechny prvky z g_2H leží v g_1H. Kosety g_1H, g_2H proto musí být stejné.

Tím máme již důkaz Lagrangeovy věty hotov, neboť nám kosety rozdělí všechny prvky G do disjunktních množin s velikostí $|H|$. Tedy pokud je k počet kosetů, pak $k|H| = |G|$, takže $|H|$ dělí $|G|$.

Definice. Počet kosetů podgrupy H grupy G budeme nazývat *indexem* H v G a značit $|G : H|$. Pro konečné grupy máme tedy podle předchozí věty $|G| = |G : H||H|$.

[9] V české literatuře se někdy používá termín rozkladová třída.



Lagrange a dělitelnost

Ukážeme si nyní jednoduchou aplikaci Lagrangeovy věty. Nejdříve se budeme chvíli zabývat jednoduchou teorií čísel a definujeme novou grupu. Nechť n je přirozené číslo větší než 1. Každé celé číslo x poté můžeme zapsat ve tvaru $x = ny + r$, kde $y \in \mathbb{Z}$, $r \in \{0, 1, \ldots, n-1\}$. Číslo r potom nazýváme *zbytkem* x po dělení číslem n. Toto asi již znáte ze střední a možná i základní školy. Navíc už víme, že množina zbytků vybavených sčítáním modulo n představuje grupu, kterou značíme $\mathbb{Z}_n$. Teď si ukážeme něco navíc. Všimněme si, že součin dvou čísel $x_1 = ny_1 + r_1$ a $x_2 = ny_2 + r_2$ dává po dělení n stejný zbytek jako $r_1 r_2$. Zbytek součinu dvou přirozených čísel tedy závisí pouze na jejich zbytcích, a pokud byly oba tyto zbytky nesoudělné s n, pak je i zbytek součinu nesoudělný s n. Ukážeme, že nesoudělné zbytky spolu s násobením (přičemž vždy bereme jako výsledek zbytek jejich násobku) tvoří grupu. Budeme pro ni používat symbol $\mathbb{Z}_n^\star$ a její řád označíme $\varphi(n)$.[10]

Již jsme si řekli, že součin dvou zbytků nesoudělných s n bude znovu nesoudělný s n. Neutrální prvek je zřejmě 1. A jelikož je normální násobení v $\mathbb{Z}$ asociativní, bude i násobení nesoudělných zbytků asociativní. Stačí nám tedy ukázat, že existují inverzní prvky. To ale není vůbec těžké. Vezměme si libovolné číslo x nesoudělné s n. Uvažujme jeho násobky x, $2x$, $3x$, $\ldots$, nx. Žádná dvě z těchto n čísel nedávají stejný zbytek po dělení n, protože pokud by dvě taková čísla ax, bx stejný zbytek dávala, pak by muselo $n \mid ax - bx = (a-b)x$. Jelikož je n a x nesoudělné, tak $n \mid a - b$, ale dvě různá a, b vzdálená o alespoň n jsme zvolit nemohli. Máme n čísel, a tedy i n různých zbytků. Nutně proto musí existovat číslo $a \in \{1, 2, \ldots, n\}$ takové, že ax dává zbytek 1. Navíc a musí být nutně nesoudělné s n, protože jinak by ax bylo soudělné s n a nedávalo by nesoudělný zbytek 1. Každé číslo ze $\mathbb{Z}_n^\star$ má k sobě inverzní prvek (číslo a), a $\mathbb{Z}_n^\star$ je tím pádem opravdu grupa.

Tvrzení. (Eulerova věta) *Mějme celé číslo $n \geq 2$ a libovolné přirozené číslo a s ním nesoudělné. Potom $n \mid a^{\varphi(n)} - 1$.*

Důkaz. Nejprve přetlumočíme tvrzení do jazyka teorie grup. Chceme ukázat, že pro zbytek r čísla a po dělení n v grupě $\mathbb{Z}_n^\star$ platí $r^{\varphi(n)} = e$. Uvažujme cyklickou podgrupu $\langle r \rangle$. Podle Lagrangeovy věty řád $\langle r \rangle$ dělí řád $\mathbb{Z}_n^\star$, který je roven $\varphi(n)$. Pro řád s cyklické podgrupy $\langle r \rangle$ platí $r^s = e$. Díky tomu, že s dělí $\varphi(n)$, můžeme umocnit obě strany této rovnice číslem $\frac{\varphi(n)}{s}$ a dostaneme $r^{\varphi(n)} = e$, což jsme chtěli ukázat.

Tvrzení. (Malá Fermatova věta) *Mějme prvočíslo p a libovolné přirozené číslo a, které není dělitelné p. Potom už p nutně dělí číslo $a^{p-1} - 1$.*

Důkaz. Toto je pouze speciální případ minulé věty. Zde jsou všechny nenulové zbytky s p nesoudělné, tedy platí $\varphi(p) = p - 1$.

[10] Tato takzvaná *Eulerova* funkce $\varphi(n)$ tedy počítá, kolik existuje čísel menších než n, která jsou s n nesoudělná.

Dokážeme zde ještě jednu větu z teorie čísel, kde již sice nepoužijeme Lagrangeovu větu, ale zužitkujeme nově definovanou grupu $\mathbb{Z}_n^\star$.

Tvrzení. (Wilsonova věta) *Nechť p je prvočíslo. Pak p dělí $(p-1)!+1$.*

Důkaz. Ve výraze máme $(p-1)!$, což značí součin všech přirozených čísel menších nebo rovných $p-1$. Toto jsou právě prvky grupy $\mathbb{Z}_p^\star$. Chceme tedy ukázat, že součin všech prvků grupy $\mathbb{Z}_p^\star$ je roven $p-1$. Každé číslo g z této grupy, které není svým vlastním inverzním prvkem, můžeme dát do dvojice s číslem g^{-1}. Jelikož je $\mathbb{Z}_p^\star$ abelovská grupa, můžeme čísla v součinu libovolně přeuspořádat. Všechny tyto dvojičky můžeme tedy dát vedle sebe, vynásobí se nám na neutrální prvek, a tím pádem zmizí. Zůstanou jen čísla g taková, že inverzní prvek k g je samotné g, což je ekvivalentní s podmínkou $g^2 = e = 1$. K nalezení všech takových g potřebujeme určit, jaké zbytky po dělení p mají čísla x, pro která platí $p \mid x^2 - 1$. Výraz vpravo ale můžeme rozložit na $(x-1)(x+1)$, a protože je p prvočíslo, dělitelnost bude splněna právě tehdy, když bude p dělit $x-1$ nebo $x+1$. Toto odpovídá zbytkům 1 a $p-1$. Tyto dva prvky jsme tedy nemohli v $\mathbb{Z}_p^\star$ s ničím popárovat a zbyly nám v součinu. Zbytek 1 je ale neutrální prvek, takže výsledkem je pouze $p-1$, což jsme chtěli ukázat.

Faktorgrupy

Už jsme zkoumali podgrupy, díky nimž jsme pak celkem přirozeně definovali kosety. Můžeme si nyní použít otázku: netvoří náhodou levé kosety dané podgrupy také grupu? Ale lze vůbec zavést násobení kosetů gH, hH? Nejjednodušší definice by byla, kdyby byl jejich součin prostě $gHhH$.[11] Není vůbec jasné, že je tato operace na kosetech uzavřená – koneckonců, teoreticky by mohla mít množina $gHhH$ až $|H|^2$ různých prvků, a nemusí tedy nutně jít o koset. Zjistíme, že obecně levé kosety podgrupy H grupu netvoří, ale stačí přidat jednu podmínku pro podgrupu H a grupa se nám objeví.

Předpokládejme nyní, že levé kosety podgrupy H s takto zavedeným násobením opravdu tvoří grupu. Nechť gH je neutrální koset. Potom $gHgH$ musí být rovno gH. Do $gHgH$ patří určitě prvek $gege = g^2$, takže $g^2 \in gH$, a proto $g \in H$. A když g je prvkem podgrupy H, musí být $gH = H$. Jediný koset, který by tedy mohl být neutrální, je právě H.

Jaký bude mít koset gH inverz? Musí to nutně být $g^{-1}H$. Prvek e totiž patří do jejich násobku $gHg^{-1}H$, což zjistíme, když za obě H dosadíme její prvek e. A jediný levý koset, který e obsahuje, je právě neutrální H. Takže aby výraz $gHg^{-1}H$ byl kosetem, musí být roven H. Pokud ve výrazu $gHg^{-1}H$ dosadíme za druhé H neutrální prvek e, zjistíme, že gHg^{-1} musí být podmnožinou H, protože jinak by rovnost neplatila. Ukážeme dále, že gHg^{-1} musí být dokonce rovno H pro každé $g \in G$. Stačí nám říct, že pro každé $k \in H$ existuje $l \in H$ takové, že $glg^{-1} = k$. Ale jako l stačí zvolit $g^{-1}kg$, které leží v H, protože i $g^{-1}H(g^{-1})^{-1} = g^{-1}Hg \subseteq H$. Dostaneme $glg^{-1} = gg^{-1}kgg^{-1} = eke = k$, jak jsme chtěli ukázat. Postupnými úvahami jsme tedy došli k nutné podmínce pro to, aby kosety tvořily grupu: $gHg^{-1} = H$ pro všechna $g \in G$. Podgrupa s touto vlastností má dokonce své vlastní jméno.

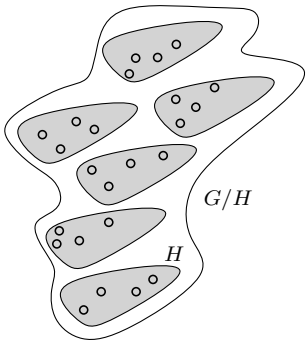
Definice. Podgrupa H grupy G se nazývá *normální*, pokud pro všechna $g \in G$ platí $gHg^{-1} = H$. Tuto skutečnost značíme $H \trianglelefteq G$.

Ukážeme nyní, že je-li pro H splněna tato podmínka, pak už levé kosety skutečně tvoří grupu. Nejdříve ukážeme, že součin libovolných dvou levých kosetů je levý koset: $gHhH = g(hh^{-1})HhH = gh(h^{-1}Hh)H = ghHH = gh(HH) = ghH = (gh)H$. (V předposlední rovnosti jsme využili poslední cvičení.) Z předchozího výpočtu vidíme, že je $H = eH$ neutrálním prvkem – dosazením $g = e$ dostáváme $HhH = hH$, dosazením $h = e$ dostáváme i neměnnost z druhé strany. Inverzem ke gH je zřejmě $g^{-1}H$. A konečně je naše operace asociativní, neboť $(gHhH)iH = (gh)HiH =$

[11] Jak jsme již uvedli, tento součin je tvořen právě prvky tvaru gh_1hh_2, kde za h_1 a h_2 dosazujeme prvky z H. Výsledná množina se skutečně běžně nazývá součinem množin gH a hH.

$((gh)i)H = (g(hi))H = gH(hi)H = gH(hHiH)$ (uprostřed úprav jsme použili asociativitu binární operace v grupě G). Normalita grupy tedy není jen nutnou podmínku k existenci grupy levých kosetů, ale dokonce i podmínkou postačující.

Definice. Nechť G je grupa a $H \trianglelefteq G$. Grupu levých kosetů H s násobením daným vztahem $(gH)(hH) = (gh)H$ nazveme *faktorgrupou* G podle H a budeme ji značit G/H.



Všimněme si, že pokud chceme určit součin dvou kosetů gH, hH, tak nám stačí vzít libovolné jejich prvky jako takzvané *reprezentanty*, ty vynásobit a podívat se, do jakého kosetu nám spadl tento výsledek. Opravdu je tento součin prvkem kosetu $gHhH = (gh)H$ (a žádného jiného). Koncept faktorgrupy nám tedy spojuje prvky grupy do takových „hromádek“, pro které platí, že nezávisle na tom, jaký prvek z nich vybereme, spadnou nám výsledky vždy do jedné „hromádky“.

Příklad. Mějme přirozené číslo n a označme X grupu celých čísel, které jsou zároveň násobky n, se sčítáním. Potom $\mathbb{Z}/X$ je cyklická grupa řádu n (každý z n kosetů obsahuje vždy čísla se stejným zbytkem po dělení n). Tato grupa se chová úplně stejně jako již používaná $\mathbb{Z}_n$.

Dokážeme nyní některá jednoduchá tvrzení týkající se normálních podgrup.
Cvičení 8. Nechť G je abelovská grupa a $H \leq G$. Pak již nutně $H \trianglelefteq G$.

Tvrzení. *Nechť G je grupa, $H \leq G$. Potom $H \trianglelefteq G$ právě tehdy, když její levé a pravé kosety splývají (tedy když pro každé $g \in G$ platí $gH = Hg$).*

Důkaz. Pokud $gHg^{-1} = H$, tak i po vynásobení obou výrazů zprava g dostaneme množinovou rovnost, protože vynásobíme zprava g na obou stranách úplně stejné prvky. Tedy $gHg^{-1}g = Hg$, což upravíme na $gH(g^{-1}g) = Hg$ a dále na $gH = Hg$, což jsme chtěli ukázat. Všechny úpravy ale byly ekvivalentní, otočením postupu proto dokážeme druhou implikaci.

Díky právě dokázanému tvrzení vidíme, že pro podgrupu $H \trianglelefteq G$ v našich množinových rovnostech prvky g a podgrupa H skutečně komutují. Díky tomu se nám před chvílí povedlo zadefinovat příslušnou faktorgrupu.

Normální podgrupy jsme definovali pomocí rovnosti $gHg^{-1} = H$ pro všechna $g \in G$. Rozmysleme si, že stačí dokonce „nerovnost“.
Cvičení 9. Ať $H \leq G$ jsou grupy, přičemž pro všechna $g \in G$ platí $gHg^{-1} \subseteq H$. Potom je $H \trianglelefteq G$.

V předchozím cvičení bylo velmi důležité, že vztah platil pro všechna $g \in G$. Uveďme proto ještě jednu pěknou a zároveň výstražnou úlohu.
Úloha 3. Rozhodněte, zda existují grupy $H \leq G$ takové, že pro nějaký prvek $g \in G$ platí $gHg^{-1} \subset H$, ale tyto dvě množiny se **nerovnají**.

Homomorfismy

Doteď jsme zkoumali, co je to grupa a jak přibližně taková grupa vypadá. Taky jsme si rozmysleli, že v grupě mohou být „schované“ nějaké menší grupy. Teď bychom se ale chtěli zabývat otázkou, jaké vztahy mezi sebou mohou mít libovolné dvě grupy – ty přitom mohou mít úplně rozdílné prvky a také se na první pohled úplně jinak chovat. Budeme se proto zabývat různými zobrazeními mezi grupami.

Nějaké náhodné zobrazení mezi množinami, na nichž jsou grupy G, H definovány, nám ale moc neříká o tom, jak v grupách G, H fungují jejich binární operace, který prvek je identita, co je inverzní k čemu a podobně – strukturu grupy v pozadí vlastně úplně ignoruje. Proto se dále budeme zabývat pouze speciálním druhem zobrazení – takzvanými *homomorfismy*.

Definice. Zobrazení φ z grupy G do grupy H nazveme *homomorfismus*, jestliže pro libovolné dva prvky $g_1, g_2 \in G$ platí

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2).$$

V definici na levé straně provádíme operaci $\cdot$ v grupě G, zatímco na pravé straně ji provádíme v grupě H, jedná se tedy o dvě „naprosto odlišné“ tečky. To sice není úplně šťastné, přesto je ale zápis jasně pochopitelný, neboť celou dobu víme, odkud kam funkce φ vede.

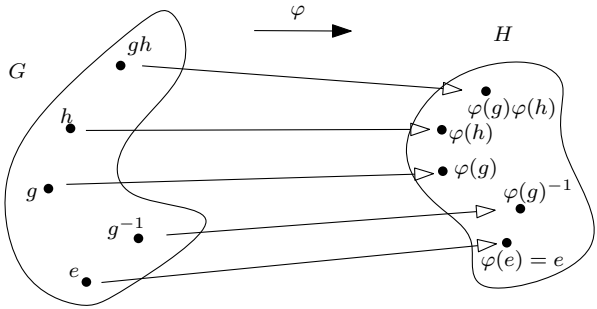
Z definice vidíme, že homomorfismy jsou zobrazení, která se chovají „slušně“ ke grupové binární operaci $\cdot$. Na první pohled ale není zřejmé, jak se homomorfismy chovají k identitám a inverzům.

Cvičení 10. Dokažte, že pro homomorfismus $\varphi : G \to H$ platí:

(1) $\varphi(e) = e$;
(2) $\varphi(g^{-1}) = (\varphi(g))^{-1}$.

Na levé straně opět vystupují příslušné operace v grupě G, na pravé v H. V prvním bodě tedy myslíme označením e na levé straně identitu v grupě G, zatímco na pravé straně identitu v grupě H, a podobně pro invertování. Jak už jsme ale řekli před chvílí, zápis je i tak skoro jednoznačný (a hlavně (po dovysvětlení) pochopitelný).

Homomorfismy jsou tedy taková zobrazení, která respektují celou strukturu grupy. Pokud chceme provést nějakou operaci[12], vyjde nastejno, zda ji nejprve provedeme v grupě G a pak výsledek zobrazíme pomocí φ, nebo jestli naopak nejprve provedeme φ, a až poté s obrazy prvků provedeme naši operaci.



Pokud složíme dva navazující homomorfismy, dostaneme také nějaké zobrazení. Bude to ale nutně znovu homomorfismus?

[12]Jak jsme zavedli dříve, pojmem operace myslíme hledání identity e, invertování a grupovou binární operaci.

Cvičení 11. Mějme grupy G, H, K a homomorfismy $\varphi : G \to H$ a $\psi : H \to K$. Ukažte, že $\psi \circ \varphi$ je homomorfismus z G do K.

Pojďme se tedy nyní podívat na nějaké příklady homomorfismů.

Příklad. V krajním případě můžeme uvažovat homomorfismus, který posílá každý prvek $g \in G$ na $e \in H$. Zjevně je to homomorfismus, neboť k tomu stačí ověřit platný vztah $e = e \cdot e$. Tento homomorfismus není moc zajímavý, a proto mu říkáme *triviální*. Takový triviální homomorfismus přitom vede mezi libovolnými dvěma grupami.

Mezi některými grupami dále mohou (ale nemusí) vést i mnohem „zajímavější“ homomorfismy.

Příklad. Pro grupy $N \trianglelefteq G$ nazýváme *přirozenou projekcí* homomorfismus $\pi : G \to G/N$, který posílá $g \mapsto gN$.

Z definice faktorgrupy platí $\varphi(g)\varphi(h) = gHhH = (gh)H = \varphi(gh)$, takže se opravdu jedná o homomorfismus. Je také vidět, že π (jako funkce) je na. Projekce mu říkáme proto, protože pouze zapomíná rozdíl mezi těmi prvky grupy G, které leží ve stejném kosetu podgrupy H (podobně jako projekce na vodorovnou souřadnicovou osu v geometrii pouze zapomíná, jak vysoko věci jsou).

Jak už jsme uvedli, faktorizováním grupy $\mathbb{Z}$ se sčítáním dostaneme v podstatě grupu $\mathbb{Z}_n$; typickým příkladem netriviálního homomorfismu je tedy zobrazení $\mathbb{Z} \to \mathbb{Z}_n$, které každému číslu přiřazuje jeho zbytek po dělení n.

Izomorfismy

Jak jsme viděli, u homomorfismů není nutné, aby se různé prvky z G zobrazily na různé prvky v H. Také nás nic nenutí, aby obraz grupy G pokryl celou H. Tento „nedostatek“ dohánějí takzvané izomorfismy.

Definice. Zobrazení $\varphi : G \to H$ nazveme *izomorfismem*, jestliže je to homomorfismus a navíc je funkce φ bijekcí prvků G na prvky H.

Pokud je tedy φ izomorfismus, různé prvky z G se musí zobrazit na různé prvky z H a obraz G musí pokrýt celou H. Řečeno lidově, grupy G a H jsou v takovém případě vlastně úplně stejné, jen se jejich prvky jinak jmenují. Funkce φ je pouze „přejmenovávací“, každému prvku grupy G přiřadí jeho přezdívku v H.

Všimněme si, že pro každou grupu G existuje alespoň jeden izomorfismus $\varphi : G \to G$, a to funkce φ, která každý prvek $g \in G$ pošle zpět na g.

Pokud máme izomorfismus $\varphi : G \to H$ a pouze „otočíme“ funkci φ (což jde, protože k bijekci vždy existuje inverzní funkce), dostaneme izomorfismus z H do G.

Pokud mezi grupami G a H existuje nějaký izomorfismus, budeme o nich říkat, že jsou *izomorfní*. Tuto skutečnost značíme $G \simeq H$.

Nakonec si ještě rozmysleme, že pokud pro nějaké tři grupy G, H, K máme $G \simeq H$ a $H \simeq K$, potom už také $G \simeq K$. Pokud jsou totiž první dvě dvojice grup izomorfní, stačí vzít příslušná zobrazení $\varphi : G \to H$, $\psi : H \to K$ a uvážit složené zobrazení $\psi \circ \varphi$. To je zobrazení z G do K. Protože je složením dvou homomorfismů, je to také homomorfismus. Navíc je ale složením dvou bijekcí, takže je to také bijekce. Nutně je to tedy izomorfismus z G do K, a tak jsou tyto dvě grupy izomorfní.

Dohromady to znamená, že všechny grupy na světě (nebo spíš v našem světě) umíme rozdělit do skupinek tak, že dvě grupy jsou izomorfní právě tehdy, když jsou ve stejné skupince. Mohlo by se tedy zdát, že vůbec nemá smysl přemýšlet nad izomorfními grupami jako nad různými ...

Cvičení 12. Nahlédněte, že grupa $(\mathbb{Q}, +)$ racionálních čísel se sčítáním, grupa $(\mathbb{Q} \setminus \{0\}, \cdot)$ nenulových racionálních čísel s násobením a grupa $(\mathbb{Q}_+, \cdot)$ kladných racionálních čísel s násobením nejsou izomorfní (žádné dvě z nich).

Cvičení 13. Rozmyslete si, že grupa $(\mathbb{R}, +)$ reálných čísel se sčítáním a grupa $(\mathbb{R}, \cdot)$ kladných reálných čísel s násobením jsou izomorfní.

... ale jak je vidět, často vůbec není lehké odlišit, které grupy vzájemně izomorfní jsou, a které ne. S jinými překvapujícími příklady izomorfismů se ještě určitě setkáme. Například přímo v druhé seriálové úloze.

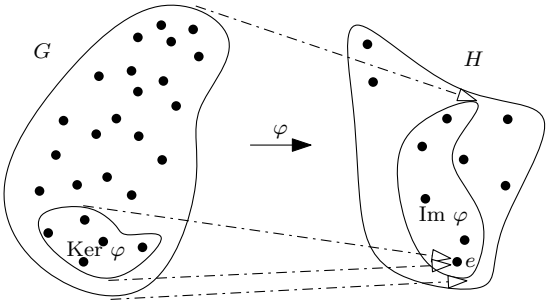
Jádra a obrazy

Některé homomorfismy jsou trochu pitomé (triviální homomorfismy), jiné jsou zase vcelku vznešené, neboť pokrývají tak velkou část cílové grupy, jak dovedou. Ostatní budou někde mezi. Jak ale rozumně zkoumat a hlídat jejich pitomost a vznešenost?

Definice. Pro homomorfismus $\varphi : G \to H$ označíme

(1) $\operatorname{Ker}\varphi$ množinu všech prvků $g \in G$, pro které $\varphi(g) = e$,
(2) $\operatorname{Im}\varphi$ množinu všech prvků $h \in H$, pro které existuje $g \in G$ takové, že $\varphi(g) = h$.

Množinu $\operatorname{Ker}\varphi$ nazýváme *jádro homomorfismu*, množinu $\operatorname{Im}\varphi$ *obraz homomorfismu*.



Jádro homomorfismu φ nám tedy říká, jak moc φ zmenšuje grupu G. Naopak obraz ukazuje, kam všude φ dosáhne. Jak ale mohou jádra a obrazy vypadat?

Tvrzení. *Pro homomorfismus $\varphi : G \to H$ je $\operatorname{Ker}\varphi \leq G$ a $\operatorname{Im}\varphi \leq H$.*

Důkaz. V obou případech stačí ověřit uzavřenost na všechny grupové operace. Mějme tedy $g_1, g_2 \in \operatorname{Ker}\varphi$. Zřejmě $\varphi(e) = e$. Dále také $\varphi(g_1^{-1}) = e \cdot \varphi(g_1)^{-1} = \varphi(g_1)\varphi(g_1)^{-1} = e$, takže $g_1^{-1} \in \operatorname{Ker}\varphi$. Dokonce platí i $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = e \cdot e = e$, čímž jsme hotovi s uzavřeností $\operatorname{Ker}\varphi$.

Nyní se věnujme $\operatorname{Im}\varphi$. Opět máme $e = \varphi(e) \in \operatorname{Im}\varphi$. Jsou-li nyní h_1, $h_2 \in \operatorname{Im}\varphi$, existují nějaká g_1, g_2 splňující $\varphi(g_1) = h_1$ a $\varphi(g_2) = h_2$. Pro inverzní prvky pak dostáváme $h_1^{-1} = \varphi(g_1)^{-1} = \varphi(g_1^{-1}) \in \operatorname{Im}\varphi$, uzavřenost na binární operaci plyne z $h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) \in \operatorname{Im}\varphi$.

Pojďme si tedy rozmyslet, že nezkreslující homomorfismy jsou právě ty, která mají jádro nejmenší možné.

Tvrzení. *Homomorfismus $\varphi : G \to H$ je prostý právě tehdy, když $\operatorname{Ker}\varphi = \{e\}$.*

Důkaz. Ukážeme obě implikace. Pokud je φ prostý, může na $e \in H$ zobrazit nejvýše jeden prvek, a přitom $\varphi(e) = e$, takže skutečně $\operatorname{Ker}\varphi = \{e\}$. Pokud je naopak $\operatorname{Ker}\varphi = e$, vezměme nějaká h_1, $h_2 \in H$ a předpokládejme $\varphi(h_1) = \varphi(h_2)$. Z předchozí rovnosti dostáváme $\varphi(h_1)\varphi(h_2)^{-1} = e$, což dává $\varphi(h_1 h_2^{-1}) = e$, takže $h_1 h_2^{-1} \in \operatorname{Ker}\varphi$. Tím pádem tedy $h_1 h_2^{-1} = e$, což okamžitě dává $h_1 = h_2$, čímž jsme hotovi.

Jak už jsme ukázali, jádra i obrazy jsou podgrupy. O obrazech toho nyní v obecnosti víc neřekneme, neboť každou grupu lze získat jako obraz nějaké vhodné grupy ve vhodném homomorfismu. Jádra ale nejsou jen tak ledajaké podgrupy.

Tvrzení. *Pro homomorfismus $\varphi : G \to H$ je $\operatorname{Ker}\varphi \trianglelefteq G$.*

Důkaz. Označme $K = \operatorname{Ker}\varphi$. Pokud $k \in K = \operatorname{Ker}\varphi$, potom pro libovolné $g \in G$ platí $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)e\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e$, tedy také $gkg^{-1} \in K$. Tím jsme dokázali, že pro všechna $g \in G$ je $gKg^{-1} \subseteq K$. My ale potřebujeme pro naše pevné g dokázat rovnost těchto dvou množin. To už jsme si ale dokázali dříve – předešlý vztah totiž speciálně platí také pro $g^{-1} \in G$, tedy $g^{-1}Kg \subseteq K$, což po vynásobení g zleva a g^{-1} zprava dává $K \subseteq gKg^{-1}$, takže dohromady skutečně $gKg^{-1} = K$.

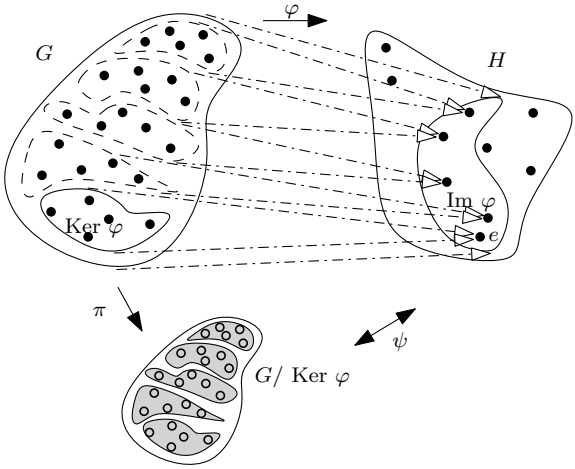
Jak za chvilku uvidíme, jádra nejsou normální pro nic za nic.

Věty o izomorfismech

U některých grup je příšerně těžké poznat, jestli jsou, nebo nejsou izomorfní. Také jde o to, jakým způsobem nám jsou zadány. V některých případech je takový problém dokonce algoritmicky nerozhodnutelný, jindy trvá jeho řešení velmi dlouho. Některé dvojice grup jsou ale izomorfní úplně jasně, a byli bychom hloupí, kdybychom si tím neulehčili práci.

Věta. (První věta o izomorfismu)
Mějme grupy G, H a homomorfismus $\varphi : G \to H$. Potom $G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$.

Důkaz.



Pro přehlednost označíme $\operatorname{Ker}\varphi = K$. Grupa G/K má za prvky skupinky prvků grupy G, které odpovídají „posunutým“ kopiím K. Prvky grupy G jsou ty prvky H, na které φ něco zobrazí.

Nyní nahlédneme, že všechny prvky z jednoho kosetu se zobrazí na stejný prvek H. Prvky v $K = \operatorname{Ker}\varphi$ jsou právě ty prvky z G, které se zobrazily na e. Dva různé prvky ze stejného kosetu se ale liší pouze posunutím o nějaké $k \in K$, které se při φ ztratí. Formálněji, tyto prvky jsou tvaru gk_1, gk_2 pro nějaké $g \in G$ a $k_1, k_2 \in K$, takže $\varphi(gk_1) = \varphi(g)\varphi(k_1) = \varphi(g) = \varphi(g)\varphi(k_2) = \varphi(gk_2)$.

Obrazy prvků g, h z různých kosetů se naopak lišit musí, neboť pokud by $\varphi(g) = \varphi(h)$, pak by $\varphi(h^{-1}g) = e$, takže by $h^{-1}g \in K$. Z této rovnosti ale okamžitě vyplývá $h^{-1}gK = K$, tedy $gK = hK$ a g, h by proto byly z tohoto stejného kosetu, jenž obsahuje jejich součiny s e.

Funkce $\psi : G/K \to \operatorname{Im}\varphi$, která posílá $gH \mapsto \varphi(g)$, je tedy dobře definovanou bijekcí nosných množin[13] těchto grup.

Zjevně je to ale také homomorfismus, protože pro libovolná g, $h \in G$ platí

$$\psi(gKhK) = \psi(ghK) = \varphi(gh) = \varphi(g)\varphi(h) = \psi(gK)\psi(hK),$$

[13]Nosnou množinou grupy G myslíme množinu, na které je grupa G vybudovaná.

čímž je důkaz dokončen.

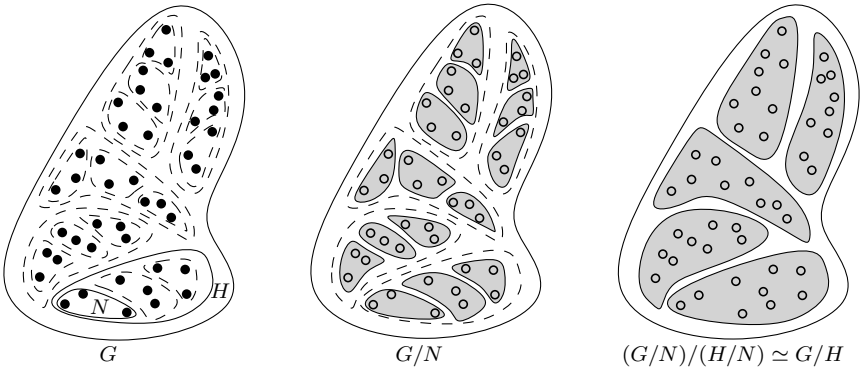
Jak řekl jeden moudrý muž[14], vidíme-li homomorfismus, vždy bychom měli začít slintat po jeho jádru jako Pavlovův pes, neboť znalost jádra a počáteční grupy nám náš homomorfismus **plně** popisuje.

Dodejme několik poznámek. Za prvé, nic z grupy H kromě $\operatorname{Im}\varphi$ nás vlastně vůbec nezajímalo, celou dobu nám šlo pouze o $\operatorname{Im}\psi$, kterým není nutně celé H. Za druhé, zkusme se na chvíli podívat na předešlý důkaz trochu obecněji a netrvejme na tom, abychom vyráběli izomorfismus. Místo toho se spokojíme s homomorfismem.

Úloha 4. Mějme homomorfismus $\varphi : G \to H$ a podgrupu $K \trianglelefteq G$, která navíc splňuje $K \leq \operatorname{Ker}\varphi$. Ať $\pi : G \to G/K$ je přirozená projekce. Dokažte, že existuje právě jeden homomorfismus $\psi : G/K \to H$, který splňuje $\psi \circ \pi = \varphi$.

Věta. (Druhá věta o izomorfismu)[15]
Mějme grupy $N \leq H \leq G$, přičemž $N, H \trianglelefteq G$. Potom $(G/N)/(H/N) \simeq G/H$.

Důkaz. Nejprve si rozmysleme, že uvedené faktorgrupy opravdu existují. Protože je $N \trianglelefteq G$, je také $N \trianglelefteq H$. Zbývá si rozmyslet, že také $H/N \trianglelefteq G/N$. Vezměme tedy libovolné $h \in H$, $g \in G$. Potom $(gN)(hN)(gN)^{-1} = (gN)(hN)(g^{-1}N) = ghg^{-1}N \in H/N$, neboť $ghg^{-1} \in H$ díky normalitě H. Tím jsme pro každé gN z G/N ukázali, že $(gN)(H/N)(gN)^{-1} \subset H/N$. Že pak již musí nastat rovnost, to jsme už dvakrát dokazovali v jiném kontextu.



Dále budeme chtít říct, že ve faktorgrupě $(G/N)/(H/N)$ jsou spláclé dohromady stejné skupinky prvků jako ve faktorgrupě G/H. To je ale jasné – grupa H rozděluje grupu G na kosety velikosti $|H|$, grupa N je ještě podrozděluje dále na menší kosety velikosti $|N|$. Protože $N \leq H$, kopie N podrozdělují H, tím pádem i ostatní kopie H jsou podrozdělené dalšími kopiemi N, takže společné hranice obou rozdělení splývají. Prvky grupy G/H odpovídají kopiím H. Prvky G/N odpovídají (menším) kopiím N, vyfaktorizování podle H/N je ale poslepuje v rámci jednotlivých kopií H.

Vnímáme-li tedy faktorizování jako slepování prvků do stejně velkých skupinek, v obou případech jsme v grupě G poslepovali stejné hromádky – jednou přímo, podruhé s mezikrokem. Přitom ale víme, že po faktorizaci se grupové operace chovají stejně jako na původních prvcích – z příslušných bloků stačí vzít libovolné reprezentanty, s nimi provést příslušné operace a nakonec se podívat, v jakém bloku výsledek skončí. Protože ale obě naše grupy mají stejné bloky, shodují se i jejich operace. Jsme tedy hotovi.

[14] Byl to známý algebraik a autor několika kvalitních knih Joseph J. Rotman.

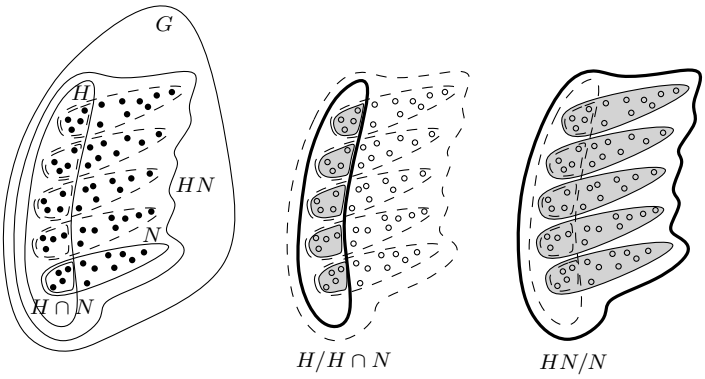
[15] Jak už to tak u „druhých“ a „třetích“ vět bývá, všichni se hádají, která že je vlastně ta druhá, a která je ta třetí.

Všimněme si, že právě dokázané tvrzení se velmi podobá tomu, jak běžně krátíme zlomky. Pokud je G konečná, po použití Lagrangeovy věty dostaneme na obou stranách vskutku stejné číslo, protože $|N|$ se vykrátí.

Pro procvičení si můžete zkusit druhou větu o izomorfismu dokázat z té první pomocí volby vhodného homomorfismu (který není těžké tipnout, neboť znáte jeho jádro i zdrojovou a cílovou grupu).

Věta. (Třetí věta o izomorfismu)
Nechť G je grupa, a $H \leq G$ a $N \trianglelefteq G$. Potom je $(HN)/N \simeq H/(H \cap N)$.

Důkaz. Věnujme se nejprve výrazu nalevo. Pro začátek ukážeme, že HN je podgrupa G. K tomu si stačí všimnout (množinové) rovnosti $HN = NH$. Skutečně z normality N máme pro všechna $n_1 \in N$, $h \in H$ vztah $hn_1h^{-1} = n_2 \in N$, takže $hn_1 = n_2h \in NH$, odkud $HN \subseteq NH$. Stejný argument ale můžeme použít i z druhé strany, čímž dohromady dostáváme rovnost $HN = NH$. Pak už je ale HN nutně grupa.[16] Asociativita plyne z rovnosti $(HN)(HN) = (HN)(NH) = H(NH) = HHN = HN$, existence inverzního prvku ze vztahu $HN = NH = N^{-1}H^{-1}$, identita je v HN zjevně také. Protože $N \trianglelefteq G$, je také $N \trianglelefteq HN$.



Nyní se podívejme na pravou stranu. $H \cap N$ je grupa jakožto průnik dvou podgrup G. Každý prvek $n \in H \cap N$ přitom po zobrazení $n \mapsto hnh^{-1}$ libovolným $h \in H$ bude stále prvkem H (jakožto součin tří prvků z H) i prvkem N (neboť N je normální dokonce v celé G), bude tedy stále ležet v $H \cap N$, takže $(H \cap N) \trianglelefteq H$.

Jak tedy $(HN)/N$ vypadá? Nosná množina grupy HN sestává ze všech prvků, které leží v nějakém kosetu hN pro $h \in H$. Prvky faktorgrupy $(HN)/N$ jsou pak právě tyto kosety. Koset hN přitom protíná H v $h(H \cap N)$, protože násobení prvkem $h \in H$ pošle do H právě ty prvky z N, které tam už byly. Kosety $h(H \cap N)$ jsou ale shodou okolností právě prvky grupy $H/(H \cap N)$. Operace v obou grupách se navíc musejí chovat stejně, neboť se shodují s operacemi na libovolných reprezentantech příslušných kosetů v G. My si tyto reprezentanty v obou případech můžeme zvolit stejné, a to z kosetů určených grupou $H \cap N$. Bijekce $\psi : hN \mapsto h(H \cap N)$ tedy skutečně zprostředkovává hledaný izomorfismus.

Stejně jako v předešlém případě lze třetí větu o izomorfismu také odvodit z té první volbou nějakého vhodného homomorfismu. Ačkoli se mohou zdát věty o izomorfismu na první pohled těžko uchopitelné, často jsou velmi elegantním vyjadřovacím prostředkem.

Pellova rovnice

Na závěr si uděláme ještě jeden krátký výlet do teorie čísel. Takzvaná Pellova rovnice je následující

[16] Tvrzení $HN = NH$ je tomu dokonce ekvivalentní pro libovolné podgrupy H, $N \leq G$.

slavná rovnice s dvěma neznámými $x, y \in \mathbb{Z}$ a pevným koeficientem $d \in \mathbb{N}$:

$$x^2 - dy^2 = 1.$$

Naším úkolem je hledat všechna řešení (x, y) v závislosti na d. Jasně vidíme, že dvojice $(\pm 1, 0)$ je vždy řešením, které budeme nazývat triviálním. Všimněme si, že rovnici můžeme upravit do (na první pohled podivného) tvaru

$$(x + \sqrt{d}y)(x - \sqrt{d}y) = 1.$$

Smyslem Pellovy rovnice je to, že je-li (x, y) její kladné řešení, pak racionální číslo $\frac{x}{y}$ velmi dobře aproximuje odmocninu z d.

Nyní je vidět, že pokud je d druhou mocninou nějakého přirozeného čísla, obě závorky jsou celá čísla, a tak musejí být buď obě rovny 1, nebo -1. Okamžitě pak dopočítáme, že tyto podmínky splňují pouze triviální řešení.

Dále tedy uvažujme pouze ta d, která čtvercem nejsou. Jak to dopadne potom? Už Lagrange dokázal, že pak má Pellova rovnice vždycky alespoň jedno řešení. Důkaz je však mírně technický a moc nesouvisí s teorií grup, a proto se jím nebudeme zabývat. Místo toho se budeme věnovat otázce, kolik řešení tato rovnice má a jaký mezi sebou mají vztah.

Nejprve si všimněme, že z reálného čísla $x + \sqrt{d}y$ lze zpětně určit celá čísla x a y právě jedním způsobem. Pokud totiž $x + \sqrt{d}y = u + \sqrt{d}v$ pro nějaká $x, y, u, v \in \mathbb{Z}$, ekvivalentně dostáváme $x - u = \sqrt{d}(v - y)$, což nám dává $x = u$ a $y = v$. Dále tedy můžeme místo dvojic (x, y) jednoznačně kódovat řešení pomocí reálného čísla $x + \sqrt{d}y$.

Nyní provedeme trik. Pokud v součinu dvou řešení $(x + \sqrt{d}y) \cdot (u + \sqrt{d}v)$ roznásobíme závorky, dostaneme $(xu + dyv) + \sqrt{d}(xv + yu)$, tedy opět výraz typu $a + \sqrt{d}b$, kde a, $b \in \mathbb{Z}$. Vynásobením závorek $(x - \sqrt{d}y) \cdot (u - \sqrt{d}v)$ naopak dostaneme $a - \sqrt{d}b$. Celkem proto

$$a^2 - db^2 = (a + \sqrt{d}b)(a - \sqrt{d}b) = (x + \sqrt{d}y)(u + \sqrt{d}v)(x - \sqrt{d}y)(u - \sqrt{d}v) =$$

$$= (x^2 - dy^2)(u^2 - dv^2) = 1 \cdot 1 = 1,$$

takže $a + \sqrt{d}b$ je také řešením. Běžné násobení reálných čísel (které je asociativní binární operací) tedy ze dvou řešení (v naší trikové reprezentaci) vyrobí opět řešení. Co víc, triviální řešení $1 = 1 + \sqrt{d}0$ se chová jako identita a operace $x + \sqrt{d}y \mapsto x - \sqrt{d}y = x + \sqrt{d}(-y)$ odpovídá invertování. Je to tedy grupa!

Cvičení 14. Rozmyslete si, že jakmile má Pellova rovnice nějaké netriviální řešení, má už jich nekonečně mnoho.

Využíváme vskutku hanebného triku – místo toho, abychom všechna řešení Pellovy rovnice poctivě zkoumali s použitím celých čísel, silou je nacpeme velmi podezřelým způsobem dovnitř jiné algebraické struktury $\mathbb{R}$, která je mnohem složitější, neboť kromě násobení zahrnuje ještě sčítání a lineární uspořádání. Znalost $\mathbb{R}$ nám přitom ušetří práci, takže můžeme v klidu popsat, jak tu naše grupa vypadá. Zmíněnou grupu označme P, platí tedy $P \leq \mathbb{R}$ (s běžným násobením). Ta řešení $x + \sqrt{d}y \in P$, která jsou (jako reálné číslo) kladná, tvoří podgrupu $P^+ \leq P$. Samozřejmě není problém popsat celou P, nás ale vlastně ani celá nezajímá, neboť řešení z $P \setminus P^+$ se od těch kladných liší jen znaménky, stačí tedy popsat pouze P^+.

Tvrzení. *Grupa všech kladných řešení Pellovy rovnice P^+ je izomorfní grupě $\mathbb{Z}$.*

Důkaz. Podle znamének $x, y \in \mathbb{Z}$ ve výrazu $x + \sqrt{d}y$ se prvky P dělí na čtyři skupiny. Z těchto čtyř výrazů jsou nutně dva kladné a dva záporné, protože se liší pouze znaménkem. Ze všech čtyř voleb je největší výraz s $x, y \geq 0$, který je nutně kladný. Jeho inverzem je řešení s $x \geq 0$, $y \leq 0$. Součin těchto dvou výrazů je ale roven 1, takže první zmíněný výraz je z intervalu $\langle 1; +\infty)$, zatímco druhý pak nutně patří do intervalu $(0; 1\rangle$. Zbylé dva výrazy se od právě popsaných liší pouze znaménkem.

Vezměme nyní nějaká dvě kladná řešení Pellovy rovnice (x_1, y_1), (x_2, y_2) z intervalu $\langle 1; +\infty)$. Pro ta dostáváme ekvivalenci

$$(x_1 + \sqrt{d}y_1 < x_2 + \sqrt{d}y_2) \Leftrightarrow (x_1 - \sqrt{d}y_1 > x_2 - \sqrt{d}y_2) \Leftrightarrow (x_1 < x_2) \Leftrightarrow (y_1 < y_2).$$

Podívejme se nyní pouze na interval $(1; +\infty)$, který oproti $\langle 1; +\infty)$ neobsahuje právě řešení $1 \in P$. Mezi řešeními z tohoto intervalu tedy můžeme najít to nejmenší. Je to přesně to řešení, které má nejmenší první složku x, přičemž v každé skupině přirozených čísel umíme najít to nejmenší. Toto nejmenší řešení označme ε. Ukážeme, že ε generuje všechna řešení z $(1; +\infty)$. Pro spor mějme nějaké řešení $\eta \in (\varepsilon; +\infty)$, které není přirozenou mocninou ε. Potom ale existuje nějaké $k \in \mathbb{N}$ takové, že $\varepsilon^n < \eta < \varepsilon^{n+1}$. Jenže po vydělení nerovnosti kladným ε^n dostaneme $1 < \eta^n \varepsilon^{-n} < \varepsilon$, což je ve sporu s minimalitou ε, protože $\eta^n \varepsilon^{-n}$ je také řešením.

Právě dokázané tvrzení tedy říká překvapivou věc – všechna řešení Pellovy rovnice umíme zakódovat jediným (nejmenším) řešením ε, a to tak, že všechna ostatní získáme až na znaménko jako jeho mocniny. Triky předvedené napříč důkazem ale vůbec nebyly „náhodné“. Obohacení racionálních čísel o $\sqrt{2}$, které jsme právě předvedli, se dá zobecnit i pro jiná reálná čísla. Tím vytváříme struktury, které představují něco mezi racionálními a reálnými čísly. A právě studium podobných *rozšíření* racionálních čísel vedlo matematiky po Abelovi k úplnému pochopení neřešitelnosti polynomů pátého a vyššího stupně. To už je ale zase jiný příběh, ke kterému se vrátit nestihneme.

Návody ke cvičením

1. Alespoň jeden existuje z definice. Předpokládejme pro spor, že existují dva různé $e_1 \neq e_2$. Součin $e_1 \cdot e_2$ musí být roven e_1, protože e_2 je neutrální prvek; ale stejně tak musí být roven e_2, protože e_1 je neutrální prvek, a tedy $e_1 = e_1 \cdot e_2 = e_2$, což je ve sporu s předpokladem, že $e_1 \neq e_2$.

2. Alespoň jeden existuje z definice. Předpokládejme pro spor, že existují dva různé prvky $h_1 \neq h_2$ takové, že $gh_1 = gh_2 = e$. Můžeme nyní psát rovnosti $h_1 = h_1 e = h_1 g h_2 = e h_2 = h_2$, což je ve sporu s předpokladem. Existuje tudíž jen jeden inverzní prvek, takže symbol g^{-1} má jednoznačný význam.

Nyní pokud $gh = e$, pak přenásobením tohoto výrazu zleva pomocí g^{-1} dostáváme $g^{-1}gh = g^{-1}$, tedy $h = g^{-1}$. Nyní vynásobením zprava pomocí g dostaneme $hg = g^{-1}g = e$, jak jsme chtěli.

3. Jelikož je g^{-1} inverzní k g, platí dvojice rovností $gg^{-1} = e$, $g^{-1}g = e$. Tyto rovnosti nám ale říkají přesně i to, že je g inverzní prvek k g^{-1}. Takže skutečně $(g^{-1})^{-1} = g$.

4. Inverzní prvek ke g^n (což je n „géček“ vynásobených po sobě) je $(g^{-1})^n$, protože když je vynásobíme, tak se všechny prvky pokrátí na identitu.

5. Chceme najít takový výraz, aby se nám s tím naším hezky krátil. Ukážeme, že můžeme zvolit $b^{-1}a^{-1}$. Musíme ověřit, že když jej vynásobíme z libovolné strany ab (nebo s využitím cvičení 3 jen z jedné strany), dostaneme identitu. Ale to je lehké: $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Obdobně po vynásobení zleva.

6. Potřebujeme ověřit, že je $H \cap K$ uzavřená na všechny grupové operace. Ale pokud uvažujeme libovolné prvky z $H \cap K$, tak to znamená, že všechny jsou jak v H, tak v K. Toto jsou podgrupy uzavřené na všechny grupové operace, takže pokud provedeme jakoukoliv operaci, tak bude výsledek v H i v K, a tedy i v $H \cap K$.

7. Ať dosadíme za první dva výskyty H libovolné dva prvky z H, tak výsledkem bude něco z H, neboť H je jako podgrupa uzavřená na násobení. Proto $HH \subset H$. Naopak každý prvek h z množiny na pravé straně můžeme zapsat jako eh, protože oba prvky e, h jsou jistě v H.

8. Potřebujeme ukázat, že $gHg^{-1} = H$ pro všechna $g \in G$. Jelikož je G abelovská, nezáleží na pořadí násobení, a to ani ve výrazu s množinou. Platí tedy $gHg^{-1} = gg^{-1}H = (gg^{-1})H = eH = H$, což jsme chtěli ukázat.

9. Ukážeme, že pro každé g platí $gHg^{-1} = H$. Vztah ze zadání totiž platí i pro g^{-1}, pro které dostaneme $g^{-1}Hg \subseteq H$. A tedy po úpravě $H \subseteq gHg^{-1}$. Takže nutně $gHg^{-1} = H$ pro každé H.

10.

(1) V grupě G platí $e \cdot e = e$, takže $\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e)$, protože φ je homomorfismus. Platí tedy $\varphi(e) = \varphi(e) \cdot \varphi(e)$. To je rovnost mezi prvky v grupě H. Celou rovnost tedy můžeme vynásobit (z libovolné strany) jednoznačně určeným inverzem $(\varphi(e))^{-1}$, čímž dostáváme rovnost $e = \varphi(e)$, jak jsme chtěli.

(2) Řečeno slovy, máme dokázat, že prvek $\varphi(g^{-1})$ je inverzem k $\varphi(g)$. Přitom víme, že $g \cdot g^{-1} = e$. Platí tedy (s využitím (1) a definice homomorfismu) $e = \varphi(e) = \varphi(g \cdot g^{-1}) = \varphi(g) \cdot \varphi(g^{-1})$. Stejně tak snadno dokážeme také $e = \varphi(g^{-1}) \cdot \varphi(g)$.

11. Jak už jsme řekli dříve, $\psi \circ \varphi$ je zobrazení z G do K. Pro všechna g_1, $g_2 \in G$ máme $(\psi \circ \varphi)(g_1 \cdot g_2) = \psi(\varphi(g_1 \cdot g_2)) = \psi(\varphi(g_1) \cdot \varphi(g_2)) = \psi(\varphi(g_1)) \cdot \psi(\varphi(g_2)) = ((\psi \circ \varphi)(g_1)) \cdot ((\psi \circ \varphi)(g_1))$, a tak je to homomorfismus.

12. Grupa $(\mathbb{Q} \setminus \{0\}, \cdot)$ obsahuje prvek -1, jehož řád je roven dvěma. Zbylé dvě grupy ale obsahují kromě identity pouze prvky nekonečného řádu, přičemž každý izomorfismus řády prvků zachovává. (To není těžké si rozmyslet.) Ani jedna z nich proto nemůže být izomorfní s $(\mathbb{Q}, \cdot)$.

Podívejme se tedy na zbylou dvojici grup. Pokud by byly izomorfní, vezměme nějaký izomorfismus $\varphi : (\mathbb{Q}, +) \to (\mathbb{Q}_+, \cdot)$. Protože je „na“, existuje $x \in \mathbb{Q}$ splňující $\varphi(x) = 2$. Pak ale $2 = \varphi(\frac{x}{2} + \frac{x}{2}) = \varphi(\frac{x}{2}) \cdot \varphi(\frac{x}{2})$. To ale dává $\varphi(\frac{x}{2}) = \sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, což je spor. (Všimněte si, že $\varphi(\frac{x}{2})$ nemůže být $-\sqrt{2}$, neboť se pohybujeme v množině $\mathbb{Q}_+$.)

13. Uvážíme zobrazení f, které prvku x přiřadí 2^x. Toto zobrazení je homomorfismem: $f(x+y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$, $f(-x) = 2^{-x} = (2^x)^{-1} = f(x)^{-1}$, a konečně $f(0) = 2^0 = 1$ – používali jsme zde již značení uvnitř jednotlivých grup, tím myslíme $-x$ pro inverzní prvek a nula pro neutrální prvek vzhledem ke sčítání. Stačí nám ukázat, že je f bijekce, a budeme mít hotovo. Zobrazení f je prosté, jelikož pokud $2^x = 2^y$, pak $x = y$. A f je „na“, protože pro každé kladné reálné y stačí zvolit $x = \log_2 y$, abychom dostali $2^x = y$. Našli jsme tedy mezi těmito dvěma grupami izomorfismus.

14. Jakmile má Pellova rovnice netriviální řešení, splňuje toto řešení $x + \sqrt{d}y \neq \pm 1$. Přitom ale $(x + \sqrt{d}y)(x - \sqrt{d}y) = 1$, takže alespoň jedno z těchto reálných čísel je v absolutní hodnotě ostře větší než jedna. Jeho mocniny proto tvoří rostoucí posloupnost reálných čísel, každý člen této posloupnosti přitom odpovídá nějakému řešení (a ta jsou různá, neboť reálná čísla kódují naše řešení jednoznačně).

Návody k úlohám

1. Pro přehlednost budeme několikanásobné použití operace $\star$ značit pomocí exponentu, jako kdybychom mocnili. To opravdu můžeme právě díky asociativitě operace $\star$. Vezměme nějaký libovolný prvek $b \in M$ a podívejme se na $b \star b = b^2$. To je díky uzavřenosti opět nějaký prvek M, takže se můžeme kouknout na prvek $b^2 \star b^2 = b^4$ a tak dále, čímž vybudujeme posloupnost $b, b^2, b^4, \ldots \in M$. Protože je M konečná, někdy se musí nějaký prvek zopakovat. Tento prvek označme c. Protože se zopakoval, dostáváme rovnost $c^{2^k} = c$ pro nějaké přirozené číslo k. Díky dokázané rovnosti máme $c^{2^k} \star c^{2^k-2} = c \star c^{2^k-2}$, což díky asociativitě zapíšeme jako $c^{2(2^k-1)} = c^{2^k-1}$. To jsme ale přesně chtěli, prvek $a = c^{2^k-1}$ splňuje rovnost $a \star a = a^2 = a$.

2. Pohyb žáby rozložíme na osové souměrnosti. Každý skok odpovídá středové souměrnosti, tedy otočení o $180°$ se středem na kameni. Toto otočení lze proto rozložit do dvou osových souměrností podle os, které jsou na sebe kolmé a protínají se na kameni. Pro jednoduchost zápisu budeme označovat osy i odpovídající souměrnosti stejně. Rozdělme kameny do dvojic $(1,2), (3,4), \ldots, (2n-1, 2n)$. Dvě středové symetrie odpovídající jedné dvojici kamenů lze zapsat jako složení čtyř osových symetrií $o_4 o_3 o_2 o_1$. Osy o_2, o_3 však můžeme volit tak, aby splývaly s přímkou určenou odpovídajícími kameny, takže $o_2 = o_3$. Pak je ale $o_3 o_2 = e$ identické zobrazení, takže $o_4 o_3 o_2 o_1 = o_4 o_1$, přičemž obě tyto osy jsou kolmé na spojnici odpovídajících kamenů, tedy rovnoběžné. Zobrazení $o_4 o_1$ je tedy nějaké posunutí. (To není těžké si rozmyslet.)

Pohyb žáby jsme tedy rozložili do n posunutí, která závisí pouze na pozici kamenů. Složení libovolného počtu posunutí je ale zřejmě také posunutí. Protože se žába první den vrátila na své původní místo, má toto složené posunutí pevný bod, takže se musí jednat o identitu. Ať si tedy žába další den stoupne kamkoli, přeskákání všech kamenů v určeném pořadí na ni vždy zapůsobí stejně jako identické zobrazení – nijak.

3. Jak si už jistě hloubavý čtenář všiml, takové grupy G, H nemohou být konečné, neboť pro konečnou H platí $|gHg^{-1}| = |H|$ pro všechna $g \in G$. Zkusíme tedy zkonstruovat nějaké nekonečné. Vezměme libovolnou nekonečnou množinu X a odpovídající nekonečnou symetrickou grupu S_X. Rozdělme nyní X na dvě nekonečné množiny Y a Z. Grupa H bude obsahovat právě ty permutace z S_X, které nehýbou žádným prvkem z Y. Ověřit uzavřenost H na všechny grupové operace je snadné, takže $H \leq G$. Volme nyní $g \in G$ jako permutaci, která celou množinu Y zobrazuje do sebe, přičemž do ní zobrazuje ještě nějaké $z \in Z$. Díky nekonečnosti obou množin Y, Z taková g skutečně existuje. Permutace z gHg^{-1} pak nechávají na místě dokonce celou $Y \cup \{g\}$. Určitě ale existuje nějaká permutace $h \in H$, která z na místě nenechává. Tím jsme dokázali ostrou inkluzi $gHg^{-1} \subset H$, jak jsme chtěli.

Nedůvěřivý čtenář si může představit například $X = \mathbb{N}$, Y množinu sudých přirozených čísel, Z množinu lichých přirozených čísel. Vyhovující $g \in S_{\mathbb{N}}$ je pak třeba permutace, která k sudým číslům přičítá 2, od lichých čísel kromě jedničky odečítá 2, přičemž jedničku posílá na dvojku. Permutace z H fixují všechna sudá čísla, permutace z gHg^{-1} dokonce i jedničku.

4. Důkaz je úplně analogický důkazu první věty o izomorfismu. Podmínka $\psi \circ \pi = \varphi$ totiž vynucuje, aby hledané zobrazení ψ posílalo $gK \mapsto \varphi(g)$. Stejně jako v uvedeném důkazu první věty o izomorfismu ověříme, že ψ je korektně definované, tedy že $gK = hK \Rightarrow \varphi(g) = \varphi(h)$. To ale okamžitě plyne z inkluze $K \leq \operatorname{Ker}\varphi$. Stejně jako minule, ψ je homomorfismus, neboť $\psi(gKhK) = \varphi(gh) = \varphi(g)\varphi(h) = \psi(gK)\psi(hK)$. To je vše. Na rozdíl od důkazu první věty o izomorfismu ale nemůžeme zaručit, že je ψ na, ani že je prosté (neboť k důkazu prostoty potřebujeme, aby $K \geq \operatorname{Ker}\varphi$, jenže tentokrát máme pouze „nerovnost“ $K \leq \operatorname{Ker}\varphi$).