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

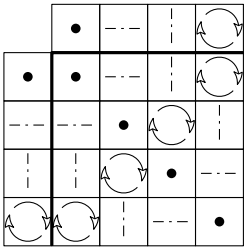
V minulé části jsme si zadefinovali grupu a bavili jsme se o tom, jak s ní zhruba můžeme pracovat. Pár konkrétních příkladů jsme již viděli, ale teď si ukážeme, že grupy mohou nabývat ještě mnohem rozmanitějších podob. A to je fajn – kdyby nebylo grupou hodně různých konkrétních objektů v matematice,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

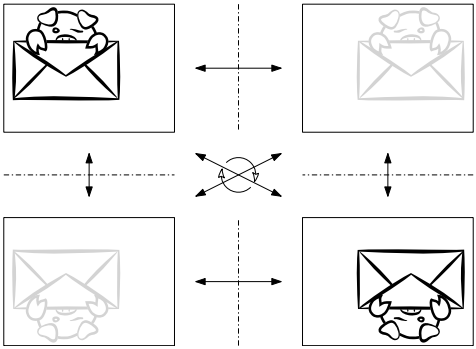
Příklad. Nejhloupějším a nejtriviálnějším příkladem grupy je grupa obsahující pouze jeden prvek, který musí být nutně neutrální (tento prvek musí v každé grupě existovat).

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.

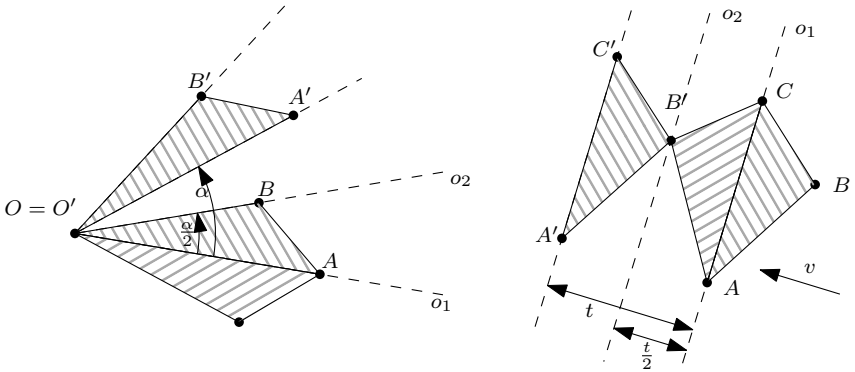
Tvrzení. *Grupa shodných zobrazení v rovině je generována osovými souměrnostmi.*

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:

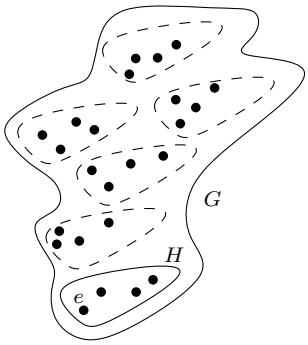
$$x = g_1h = g_1eh = g_1(h_1h_1^{-1})h = (g_1h_1)h_1^{-1}h = g_2h_2h_1^{-1}h = g_2(h_2h_1^{-1}h);$$

$h_2h_1^{-1}h$ 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.

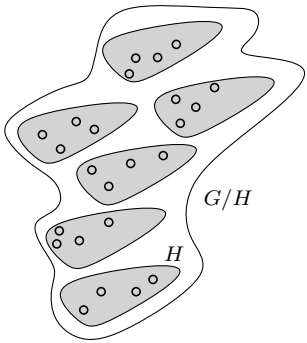
Definice. Podgrupa H grupy G se nazývá *normální*, pokud pro všechna $g \in G$ platí $gHg^{-1} = H$. Tuto skutečnost značíme $H \trianglelefteq G$.

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.

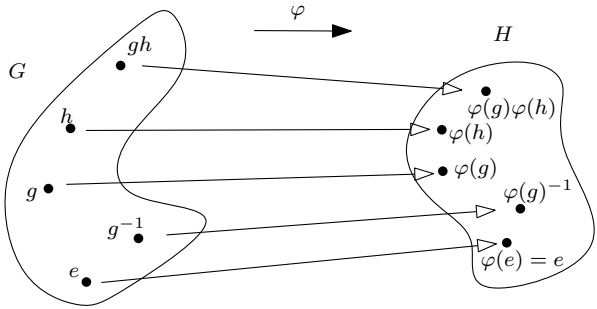
Z definice vidíme, že homomorfismy jsou zobrazení, která se chovají „slušně“ ke grupové binární operaci $\cdot$. Na první pohled ale není zřejmé, jak se homomorfismy chovají k identitám a inverzům.

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.

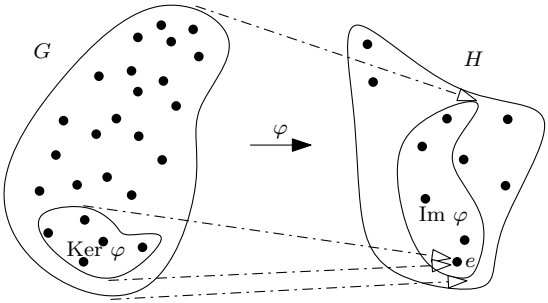
Jádra a obrazy

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 $gKg^{-1} = K$.

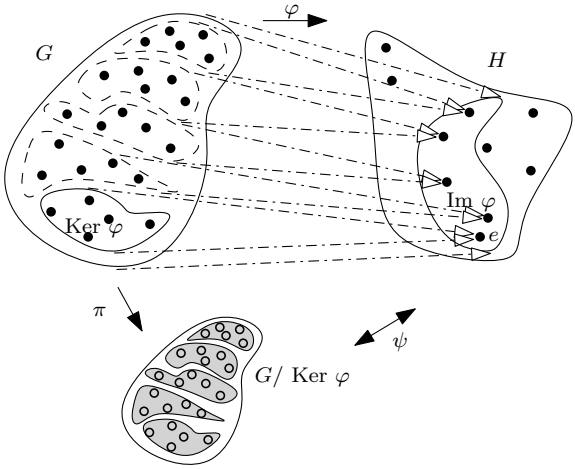
Jak za chvilku uvidíme, jádra nejsou normální pro nic za nic.

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.

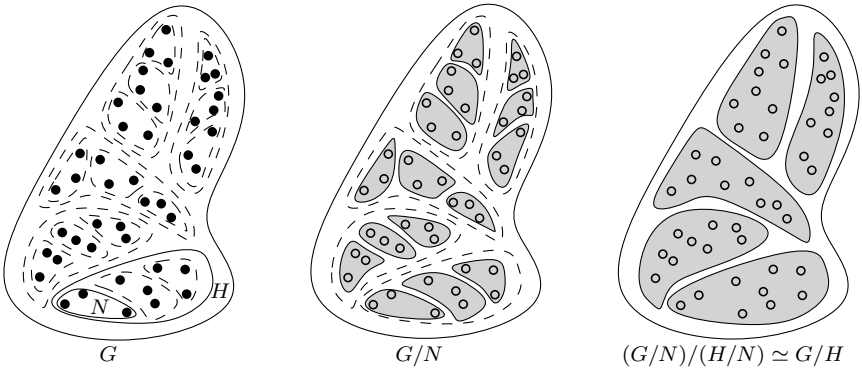
Jak řekl jeden moudrý muž[14], vidíme-li homomorfismus, vždy bychom měli začít slintat po jeho jádru jako Pavlovův pes, neboť znalost jádra a počáteční grupy nám náš homomorfismus **plně** popisuje.

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.

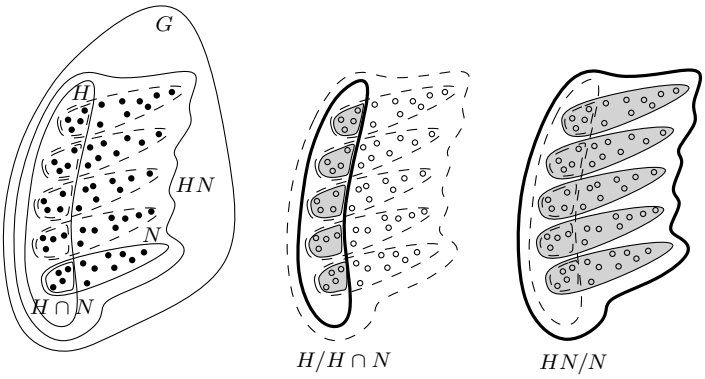
[15] Jak už to tak u „druhých“ a „třetích“ vět bývá, všichni se hádají, která že je vlastně ta druhá, a která je ta třetí.

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“ $K \leq \operatorname{Ker}\varphi$).

Milý příteli,

první seriálová série už je dávno za námi a my Tě vítáme u druhého dílu seriálu o teorii grup. Doufáme, že Tě první díl zaujal a že se Ti bude líbit i ten druhý. Ani pokud jsi prvnímu dílu porozuměl jen zčásti, určitě nevěš hlavu – ne vše je k pochopení zbytku potřeba. Druhý díl by určitě neměl být oproti prvnímu těžší na pochopení. Pro toho, kdo uspěšně vstřebal nejdůležitější pojmy první části, bude dokonce o dost snazší.

V seriálu se ale nacházejí i pasáže, které úplně snadné nejsou – především kapitolka o Pólyových polynomech k pochopení ostatního textu (a řešení soutěžních úloh) nutně potřeba není. Pokud se tedy v právě zmíněné části ztratíš, můžeš v klidu pokračovat dál.

Stejně jako v dílu prvním je text proložen spoustou cvičení a úloh, jejichž řešení jsou uvedena na konci. Cvičení jsou typicky lehčí a slouží k lepšímu pochopení tématu. Určitě si je tedy zkus vyřešit dřív, než si jejich řešení najdeš. Cvičení jsou na rozdíl od úloh nedílnou součástí textu, takže pokud je nevyřešíš (což není žádná tragédie, ne všechna jsou úplně snadná), přečti si jejich řešení dřív, než budeš pokračovat ve čtení.

Příjemné a zábavné čtení přejí
Filip Bialas a Kuba Löwit

Teorie grup II – Procitnutí symetrií

Group Theory is the branch of mathematics that answers the question, "What is symmetry?"
Nathan C. Carter

Prolog II

S devatenáctým stoletím přicházejí noví lidé s novými nápady a získávají trochu víc nadhledu nad tím, co se to v matematice vlastně zrovna děje. Z hlediska dějin teorie grup je klíčové, že se Cauchy intenzivně zabývá permutacemi a jako první je vnímá jako funkce (které lze skládat).

Posléze přichází mladičký francouzský matematik Galois. Navzdory velkému talentu má s přijetím na univerzitu značné potíže, neboť jeho myšlenky zkoušející nezvládají sledovat. Navíc do Francie přichází politické vlnobití, kterého se mladý Galois (ve stopách svého otce) účastní. Mezitím výrazně prohlubuje Abelovu práci – daří se mu dokonce přesně klasifikovat polynomy, jejichž kořeny se dají zapsat pomocí jejich koeficientů a základních aritmetických operací. Při tom v podstatě objevuje grupy jako takové. S vydáním své práce má ale problémy – jednou je jeho spis nepochopen, podruhé se ztratí, jindy je požádán o přepracování.

Kvůli svým politickým aktivitám se Galois dostává i do vězení (kde pokračuje ve své práci). Ve věku dvaceti let je vyzván k souboji. Příčiny jsou nejisté – mohlo jít o nešťastnou lásku, možná však byly motivy čistě politické. Noc před soubojem Galois tráví psaním dopisů, ve kterých se mimo jiné snaží sepsat celé své dílo. Druhého dne je zastřelen, v lese jej umírajícího nachází neznámý sedlák.

Během zbytku devatenáctého století přichází mnoho dalších. Klein cílevědomě spojuje grupy a geometrii, Cayley se blíží jejich abstraktní definici, podobně Burnside po něm. V Norsku plodně pracují Abelovi následovníci Sylow a Lie. Devatenácté století vrcholí důležitým počinem – vznikem naší dobře známé definice.

Návrat k normalitě

Když jsme si definovali normální grupy, mohlo se naše počínání zdát trochu podivné a náhodné. Nyní už ale máme dostatek znalostí na to, abychom normálnost lépe pochopili a docenili. Čím víc budeme grupám rozumět, tím přirozenější tento pojem bude.

Už jsme si algebraicky odvodili, že podle normálních podgrup umíme faktorizovat. Také jsme viděli, že podle žádných nenormálních podgrup faktorizovat nejde. Ukážeme si nyní mnohem kratší argument. Pokud totiž pro nějakou podgrupu $H \leq G$ umíme korektně definovat faktorgrupu G/H, dostáváme společně s ní přirozenou projekci $\pi : G \to G/H$, jejímž jádrem $\operatorname{Ker} \pi$ je přesně H. Jádra jsou ale vždy normální.

Normální jsou tedy **přesně** ty podgrupy, podle kterých můžeme faktorizovat. Podobně můžeme díky existenci faktorizací říct, že normální jsou **přesně** ty podgrupy, které jsou jádrem nějakého homomorfismu. Znalost všech normálních podgrup dané grupy G nám podle první věty o izomorfismu říká, jaké obrazy mohou mít homomorfismy z G do libovolné jiné grupy – ty jsou totiž vždy izomorfní nějaké faktorgrupě grupy G. Grupy, které mají málo normálních podgrup, jsou tedy jistým způsobem zajímavé.

Definice. Grupa G je *jednoduchá*, jestliže triviální podgrupa $\{e\}$ a celá grupa G jsou její jediné normální podgrupy.

K jednoduchým grupám ještě párkrát zabrousíme, nyní se ale podíváme na to, jak normalita souvisí s jedním speciálním typem izomorfismů.

Automorfismy a jejich grupy

Definice. *Automorfismus* grupy G je izomorfismus $\psi : G \to G$.

Automorfismy jsou tedy bijekce $G \to G$, které navíc zachovávají strukturu grupy. Každé dva automorfismy lze složit, čímž získáme opět automorfismus $G \to G$. Jak už dávno víme, skládání funkcí je asociativní. Ke každému automorfismu ψ navíc zjevně existuje inverzní automorfismus ψ^{-1}, který je pouze jeho „otočením“ a společně s ním se složí na identickou funkci $G \to G$. Identická funkce se přitom vzhledem ke skládání chová jako neutrální prvek. Všechny automorfismy grupy G tedy se skládáním tvoří grupu! Tu budeme značit $\mathrm{Aut}(G)$.

Jakkoli je tato myšlenka krásná, grupa automorfismů grupy G se obecně zkoumá dosti špatně. Naštěstí má jednu velmi bohatou podgrupu, se kterou se ještě mnohokrát setkáme – tzv. grupu vnitřních automorfismů.

Vyberme si libovolný pevný prvek $g \in G$ a definujme zobrazení $\varphi_g : G \to G$ předpisem $h \mapsto ghg^{-1}$. Víme, že obě funkce $h \mapsto gh$, $h \mapsto hg^{-1}$ jsou bijekce $G \to G$, přičemž φ_g je jejich složením (v libovolném pořadí), takže je to také bijekce $G \to G$. Co víc, pro libovolné h_1, $h_2 \in G$ platí $\varphi_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \varphi_g(h_1)\varphi_g(h_2)$, takže φ_g je dokonce automorfismus grupy G.

Definice. Pro libovolné $g \in G$ označíme φ_g automorfismus tvaru $h \mapsto ghg^{-1}$. Takovým automorfismům říkáme *vnitřní*.

Tyto automorfismy nazýváme vnitřní, protože je „zevnitř“ zprostředkovávají samotné prvky grupy G. Vnitřní automorfismy odpovídající různým prvkům grupy G mohou a nemusí být úplně stejné.

Identická funkce na G je zjevně vnitřním automorfismem φ_e. Automorfismy φ_g a $\varphi_{g^{-1}}$ jsou k sobě inverzní, neboť $(\varphi_{g^{-1}} \circ \varphi_g)(a) = g^{-1}gag^{-1}g = a = \varphi_e(a)$. Složení $\varphi_g \circ \varphi_h$ je přitom rovné φ_{gh}, neboť $(\varphi_g \circ \varphi_h)(a) = ghah^{-1}g^{-1} = \varphi_{gh}(a)$. Tím jsme dokázali, že vnitřní automorfismy tvoří podgrupu grupy všech automorfismů grupy G.[1] Budeme ji značit $\mathrm{Inn}(G)$.

Cvičení 1. Grupa G má triviální grupu vnitřních automorfismů právě tehdy, když je abelovská.

Automorfismy přitom jakýmsi způsobem působí na celou grupu G a míchají její prvky. Protože víme, že obrazem každé grupy při jakémkoli homomorfismu je zase grupa, platí dokonce, že automorfismus zobrazí každou podgrupu grupy G na některou podgrupu G. Příslušné podgrupy navíc musejí být izomorfní. Normální podgrupy jsou **přesně** ty podgrupy $H \leq G$, se kterými žádný z **vnitřních** automorfismů ani nehne (přestože může přepermutovat jejich vnitřek). Formálněji: Grupa $H \leq G$ je normální právě tehdy, když s každým h obsahuje i $\varphi_g(h)$ pro každý vnitřní automorfismus φ_g.

Cvičení 2. Dokažte, že pro libovolnou grupu G je $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Ještě zmíníme, co přesněji provádějí vnitřní automorfismy s prvky G.

Definice. Prvek $a \in G$ nazveme *konjugovaným* s prvkem $b \in G$, existuje-li nějaký $\varphi_g \in \mathrm{Inn}(G)$ takový, že $\varphi_g(a) = b$.

Všimněme si, že každý prvek je konjugovaný sám se sebou díky identickému automorfismu $\varphi_e \in \mathrm{Inn}(G)$. Dále, je-li $gag^{-1} = \varphi_g(a) = b$, je také $a = g^{-1}bg = \varphi_{g^{-1}}(b)$, konjugovanost je tudíž symetrický vztah. Navíc, je-li $\varphi_h(a) = b$, $\varphi_g(b) = c$, je už také $\varphi_{gh}(a) = gha(gh)^{-1} = ghah^{-1}g^{-1} = gbg^{-1} = c$. Pokud je proto a konjugovaný s b a b s c, je i a konjugovaný s c. Dohromady tedy vidíme,

[1] Dokonce jsme dokázali, že zobrazení $G \to \mathrm{Aut}(G)$, které posílá prvek $g \in G$ na φ_g, je homomorfismus, jehož obrazem je právě $\mathrm{Inn}(G)$.

že konjugovanost rozděluje všechny prvky G do disjunktních skupinek, ve kterých je každý prvek konjugovaný s každým.

Symetrické grupy a parita permutací

Celých sto let se teorie grup zabývala výhradně symetrickými grupami a s trochou nadsázky se dá říct, že celá tato teorie vznikla na a bydlí v symetrických grupách. Bylo by tedy krajně nezodpovědné neprozkoumat je trochu detailněji.

Připomeňme nejprve, že permutací množiny X myslíme zkrátka jakoukoli bijekci $X \to X$ a že symetrická grupa S_X je grupa všech těchto permutací. Dále se v tomto textu zaměříme pouze na konečné množiny X. Už jsme se bavili o tom, že libovolnou takovou permutaci umíme jednoznačně rozložit na cykly. Nyní prozkoumáme, jak takový rozklad souvisí s konjugováním.

Tvrzení. *Dvě permutace jsou v S_X konjugované právě tehdy, když mají stejnou cyklovou strukturu*[2].

Důkaz. Mějme nějakou permutaci $\sigma \in S_X$ a zkoumejme, jak vypadají permutace $\tau\sigma\tau^{-1}$ pro libovolné $\tau \in S_X$. Permutace τ, τ^{-1} jsou k sobě inverzní, permutace $\tau\sigma\tau^{-1}$ tedy nejdřív přejmenuje prvky X pomocí τ^{-1}, poté je (podle jejich nových jmen) propermutuje využitím σ a nakonec je zase přejmenuje nazpátek permutací τ. Ověřte si sami, že pokud například σ zobrazuje $1 \mapsto 2$, pak $\tau\sigma\tau^{-1}$ zobrazí $\tau(1) \mapsto \tau(2)$.

To nám říká dvě věci. Na jedné straně mají permutace σ a $\tau\sigma\tau^{-1}$ nutně mají stejnou cyklovou strukturu, pouze s jinými „popisky“, které jsou pozměněné permutací τ. Konjugované permutace tedy mají stejnou cyklovou strukturu.

Protože ale S_X obsahuje všechny permutace, můžeme na druhé straně tyto popisky vhodnou volbou τ změnit, jak se nám zachce, čímž dokážeme vyrobit libovolnou jinou permutaci se stejnou cyklovou strukturou. Každé dvě permutace se stejnou cyklovou strukturou jsou tedy konjugované.

Pokud se tedy zabýváme symetrickými grupami, konjugování odpovídá pouhému přejmenování prvků množiny X. Přejmenováváním tak získáme některé automorfismy S_X – a to právě vnitřní automorfismy této grupy. Normální podgrupy S_X jsou tedy právě ty, které s každou permutací obsahují i všechny její kamarády se stejnou cyklovou strukturou.

Kromě rozkladu na cykly umíme permutace rozložit ještě jiným, neméně zajímavým způsobem. Tento druh zápisu sice nebude jednoznačný, přesto nám toho ale o permutačních grupách hodně řekne.

Tvrzení. *Každou permutaci σ konečné množiny lze napsat jako složení konečného počtu transpozic (tj. cyklů délky dva). Parita počtu těchto transpozic přitom nezávisí na konkrétním rozkladu původní permutace.*

Důkaz. Nejprve si rozmyslíme, že nějaký takový rozklad existuje. Víme, že σ je jednoznačně určena tím, jak zamíchá prvky příslušné konečné množiny. Každé takové zamíchání přitom můžeme provést postupným prohazováním vhodných dvojiček prvků.[3] To je ale jinými slovy právě složení konečného počtu transpozic.

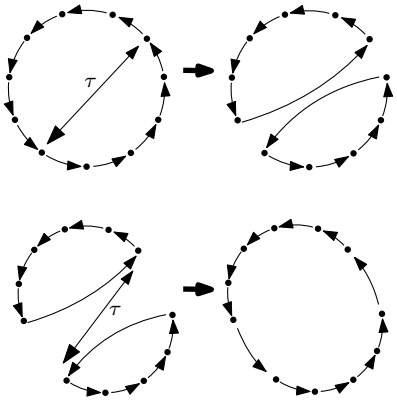
Mohli jsme postupovat i o trochu explicitněji. Permutaci σ lze rozložit na cykly, takže ji můžeme zapsat jako složení permutací odpovídajících těmto cyklům (v libovolném pořadí). Cyklus $(a_1 a_2 \dots a_k)$ přitom lze zapsat jako složení $k-1$ transpozic $(a_1 a_k) \cdots (a_1 a_3)(a_1 a_2)$.

Nyní ukážeme, že parita počtu transpozic v libovolném takovém rozkladu je skutečně stejná. Na to půjdeme trošku oklikou. Dokážeme, že pokud $\sigma \in S_n$ je nějaká permutace, která sestává z m cyklů, a $\tau \in S_n$ nějaká transpozice, pak složení $\tau\sigma$ sestává z $m-1$ nebo $m+1$ cyklů (přičemž zde započítáváme i cykly délky 1). To je dobře vidět z obrázku. Pokud totiž τ prohazuje dva prvky

[2] Tj. když je počet jednocyklů v obou stejný, stejně tak i počet dvojcyklů, trojcyklů atd.

[3] To je skutečně snadné – dokonce bychom si například mohli usmyslet, že budeme prohazovat vždy dva sousední prvky.

uvnitř stejného cyklu permutace σ, tento zasažený cyklus se rozpadne na dva. Pokud naopak τ prohazuje dva prvky z různých cyklů, v permutaci $\tau\sigma$ se tyto dva cykly spojí do jednoho. V obou případech přitom všechny ostatní cykly zůstanou nezměněny.



Po vynásobení jednou transpozicí se tedy změní parita počtu cyklů v rozkladu σ. Pokud by tudíž σ měla rozklad zároveň na sudý i na lichý počet transpozic, tyto dva rozklady na sebe umíme převést vynásobením lichým počtem transpozic. Pak by ale σ musela mít ve svém jednoznačném rozkladu na cykly zároveň sudý i lichý počet cyklů, což je spor.

Díky právě dokázanému tvrzení si tedy permutace můžeme rozdělit na dva druhy – na ty, které mají ve svém libovolném rozkladu sudý počet transpozic, a na ty, které mají ve svém libovolném rozkladu lichý počet transpozic. Aby se nám o nich lépe mluvilo, budeme této vlastnosti permutace říkat *parita*.

Definice. *Parita*[4] permutace σ, kterou budeme značit $\operatorname{sign}(\sigma)$, je číslo 1 nebo -1 podle toho, jestli má σ ve svém libovolném rozkladu sudý, nebo lichý počet transpozic. Pokud je $\operatorname{sign}(\sigma) = 1$, říkáme, že je σ *sudá*. V opačném případě o ní mluvíme jako o *liché*.

Z důkazu předešlého tvrzení navíc vyplývá, jak paritu rychle zjistit. Pro permutace konečné množiny velikosti $n \in \mathbb{N}$ se totiž identická permutace $\mathrm{id} \in S_n$ skládá přesně z n (jednoprvkových) cyklů, přičemž je sudá. Je-li tedy n sudé, odpovídá parita libovolné permutace $\sigma \in S_n$ paritě počtu jejích cyklů. Pokud je n liché, je parita permutace opačná než parita počtu cyklů σ.

Je přirozené dívat se na sign jako na funkci z konečné grupy S_n do množiny $\{1, -1\}$. Jak se sign chová při skládání permutací? Pokud máme dvě permutace σ, τ rozložené na transpozice, jejich složení umíme okamžitě rozložit jednoduše tak, že oba rozklady napíšeme ve správném pořadí za sebe. Parita $\sigma\tau$ proto odpovídá součinu parit permutací σ a τ. Právě jsme tedy „omylem“ ověřili, že sign je pro libovolné $n \in \mathbb{N}$ homomorfismus z S_n do grupy $\{1, -1\}$ s běžným násobením. Ta je přitom izomorfní aditivní grupě $\mathbb{Z}_2$. Z toho pak hned vidíme, že pro libovolnou $\sigma \in S_n$ je $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma^{-1})$. Zřejmě také pro identickou permutaci platí $\operatorname{sign}(\mathrm{id}) = 1$.

Dalším důležitým pozorováním je, že složením dvou sudých permutací opět dostaneme sudou permutaci. Sudé permutace proto (na rozdíl od lichých) tvoří podgrupu grupy S_n. Ta si zasluhuje své vlastní jméno.

Definice. Pro libovolné $n \in \mathbb{N}$ budeme podgrupu grupy S_n sestávající ze všech sudých permutací označovat jako *alternující grupu* A_n.

Cvičení 3. Rozmyslete si, že pro všechna přirozená n je $A_n \trianglelefteq S_n$.

[4] Někdy též *znaménko*.

Z předešlého ale vůbec není jasné, kolik je lichých a kolik sudých permutací množiny dané velikosti. Zkoušet je počítat přímo by bylo trochu nepříjemné, s našimi znalostmi je to ale hračka.

Tvrzení. *Pro přirozené $n \geq 2$ je sudých permutací v grupě S_n stejně jako lichých.*

Důkaz. Jakmile je $n \geq 2$, obsahuje S_n alespoň jednu lichou permutaci τ. Násobení zleva permutací τ je pak bijekcí na nosné množině grupy S_n. Díky vlastnostem parity ale tato bijekce páruje prvky s jinými znaménky. Tím pádem je nutně sudých permutací v S_n stejně jako těch lichých.

Pojďme to samé dokázat ještě jednou.[5] Jakmile je $n \geq 2$, je zobrazení $\operatorname{sign} : S_n \to \{-1, 1\}$ na, přičemž A_n je jeho jádrem. Podle první věty o izomorfismu $S_n/A_n \simeq \{-1, 1\} \simeq \mathbb{Z}_2$, takže $[S_n : A_n] = 2$. Vzhledem k podgrupě A_n se tedy S_n rozpadá na dva kosety, a protože jsou kosety stejně velké, požadovaný výsledek je dokázaný.

Ještě než se vrhneme dál, bylo by celkem férové prozradit jednu malou pikantnost ohledně alternujících grup. Alternující grupy A_n pro $n \geq 5$ jsou totiž jednoduché, to jest nemají žádné vlastní normální podgrupy. Jednoduché grupy jsou vcelku zajímavé objekty a alternující grupy jsou jejich pěkným a ilustrativním příkladem. Důkazu jejich jednoduchosti se ale vyhneme.[6] Přesto si ale ukážeme, k čemu je něco takového dobré. V následujícím cvičení proto zkuste jednoduchosti A_n využít (posléze se ho můžete pokusit vyřešit i bez ní).

Cvičení 4. Pro $n \geq 5$ je sign jediný netriviální homomorfismus $S_n \to \{1, -1\}$.[7]

Proč vychvalujeme symetrické grupy?

To je dobrá otázka. Už několikrát jsme zmínili jejich historický význam, vůbec jsme se ale nezabývali otázkou, jaké postavení mají vůči jiným grupám. Nyní podáme odpověď – jejich postavení je výsostné.

Věta. (Cayleyho) *Každá grupa G je izomorfní některé podgrupě nějaké symetrické grupy.*

Důkaz. Nejdříve si musíme vybrat, do které symetrické grupy budeme G vnořovat. Vhodným kandidátem je S_G, grupa všech permutací nosné množiny grupy G. Nyní si musíme rozmyslet, jaké permutaci z S_G by měl odpovídat prvek $g \in G$. My už ale naštěstí známe jednu skvělou věc. Násobení zleva libovolným prvkem $g \in G$ je bijekce $G \to G$, což je nějaký prvek S_G. Zbývá dokázat, že toto trikové přiřazení opravdu vyrobí podgrupu S_G, která je izomorfní s G.

Definujme si tedy zobrazení $\psi : G \to S_G$ právě popsaným způsobem. Protože pro $g, h \in G$ odpovídají obě zobrazení $\psi(gh)$ a $\psi(g)\psi(h)$ permutaci indukované násobením prvkem gh, jsou si rovna, takže ψ je homomorfismus. Jeho jádro je přitom triviální, neboť každý prvek $g \in G$, $g \neq e$ indukuje neidentickou permutaci (například protože $ge = g$). Obraz $\operatorname{Im}\psi \leq S_G$ je proto skutečně izomorfní grupě G.

Ačkoli se to může zdát neuvěřitelné, zkoumání symetrických grup a jejich podgrup je proto stejně obecné jako zkoumání všech možných abstraktních grup. Samozřejmě bychom neměli úplně přehánět. Existují i jiné stejně „obecné“ druhy grup. Některé grupy navíc odpovídají i permutacím mnohem menších množin, než jaké nám dává právě uvedená Cayleyho věta – například na S_n se radši díváme jako na grupu všech permutací na n prvcích než jako na grupu vybraných permutací na $n!$ prvcích.

Tři, dva, jedna... Akce!

Jak jsme slibovali od začátku, grupy můžeme chápat jako „symetrie různých věcí“. Samotné symetrické grupy mají svou množinu, kterou si ve chvílích volna radostně permutují. Pokud ale dostaneme

[5] A tvařme se přitom mnohem světaznaleji.

[6] Není těžký, pouze trochu otravný. Je zkrátka potřeba dokázat, že jakmile nějaká podgrupa A_n obsahuje něco jiného než identitu, umíme invertováním, skládáním a konjugováním vyrobit kterýkoli další prvek.

[7] Jak už jsme říkali, je dvouprvková grupa $\{1, -1\}$ s násobením izomorfní grupě $\mathbb{Z}_2$.

pod stromeček nějakou abstraktní grupu, bude pro nás celkem složité představit si, symetrie čeho že nám to Ježíšek vlastně nadělil. Možná bychom měli na Štědrý večer mnohem větší radost, kdybychom dostali současně s abstraktní grupou i nějaký předmět, na jehož symetrie by prvky naší grupy pasovaly. Navíc by bylo určitě slušností dodat i návod, jak na onen předmět prvky přidělat. A právě tomu říkáme akce...

Definice. *Akcí* (nebo *působením*) grupy G na množině X nazýváme libovolný homomorfismus $\alpha : G \to S_X$.

Množina X je naším předmětem, homomorfismus α je příslušný návod k použití symetrií z grupy G. Přesto bychom si rádi představovali, že množinu X permutují přímo prvky grupy G. Zavedeme proto následující značení. Pro libovolné $g \in G$ bude α_g značit permutaci $\alpha(g) \in S_X$; pro libovolné $a \in X$ pak je $\alpha_g(a)$ ten prvek z množiny X, na který obraz prvku g při akci α posílá a.[8] Často nás budou zajímat akce, kde každé dva prvky z G představují jinou symetrii, což odpovídá podmínce $\operatorname{Ker}\alpha = \{e\}$. Takovým akcím se říká *věrné*.

Znalost nějaké akce nám obecně může být na dvě věci. Za prvé, předmět X může být ve skutečnosti trochu složitější a permutace z $\operatorname{Im}\alpha$ mohou uznávat jeho strukturu, vhodná akce je pak velmi elegantní způsob práce s jeho symetriemi. Za druhé, znalost nějaké akce grupy G nám může prozradit mnoho o ní samotné – grupu G s akcí si můžeme mnohem lépe představit, akce nám poodhalí nějaké její podgrupy, strukturu a podobně.

Pojďme si nyní ukázat, jak nějaké akce mohou vypadat. Pomineme přitom triviální akci, kdy se celá grupa zobrazí na identickou permutaci množiny X.

Příklad. Symetrická grupa S_X věrně působí zřejmým způsobem na množině X. Homomorfismus α přitom odpovídá identické funkci $S_X \to S_X$, která skutečně má triviální jádro.

Příklad. Připomeňme, že Kleinova grupa[9], kterou si označíme V, odpovídá symetriím obdélníkového listu papíru. Na definici grupy V jsme přesto žádný obdélník ani symetrie nepotřebovali, prvky grupy V jsou „prostě jen písmena“. Naštěstí ale existuje pěkná věrná akce $\alpha : V \to S_4$, která prvky V zobrazí na jisté permutace čtyř vrcholů obdélníku. Dokonce jsou to právě ty permutace, po jejichž provedení dostaneme opět obdélník (tj. právě jeho symetrie).

Příklad. Podobně vidíme, že dihedrální grupa[10] D_{2n} věrně působí na n-tici vrcholů pravidelného n-úhelníka. To nám o ní například prozrazuje, že ji lze nagenerovat dvěma prvky – nejmenší rotací a jednou reflexí, popřípadě dvěma vedlejšími reflexemi[11]. Okamžitě také vidíme, že obsahuje cyklickou podgrupu R generovanou nejmenší rotací, neboť R obsahuje právě všechny přímé[12] symetrie n-úhelníka, což jsou shodou okolností přesně ty symetrie, v jejichž libovolném zápisu je sudý počet reflexí. Parita počtu reflexí se navíc ani po konjugaci libovolným prvkem nezmění, takže $R \trianglelefteq D_{2n}$.

Další velmi přirozené akce všech možných grup potkáme později.

Burnsideovo lemma

Nyní se budeme snažit zkoumat symetrické objekty pomocí akcí grup jejich symetrií. Začneme dvěma užitečnými pojmy.

Definice. Mějme akci α grupy G na množině X. Pro libovolný prvek $a \in X$ pak definujeme

(1) *stabilizátor* G_a jako množinu těch prvků $g \in G$, pro které je $\alpha_g(a) = a$;
(2) *orbitu* $\mathcal{O}(a)$ jako množinu těch $b \in X$, pro které existuje $h \in G$ splňující $\alpha_h(a) = b$.

[8] Značení akcí velmi často záleží na konkrétní literatuře a kontextu, každé má své výhody a nevýhody. My se budeme držet toho právě zavedeného.

[9] Viz první díl seriálu, kapitola *Příklady grup*.

[10] Tamtéž.

[11] Vedlejšími myslíme osové symetrie, jejichž osy svírají nejmenší možný kladný úhel.

[12] Tj. bez zrcadlení.

Je snadné si uvědomit, že stabilizátor libovolného prvku $a \in X$ je podgrupou G. Skutečně: $\alpha_e(a) = a$, rovnost $\alpha_g(a) = a$ použitím $\alpha_{g^{-1}}$ přechází v $a = \alpha_{g^{-1}}(a)$, a nakonec, pokud $g, h \in G_a$, okamžitě dostáváme $\alpha_{gh}(a) = \alpha_g(\alpha_h(a)) = \alpha_g(a) = a$.

Orbity jsou naopak podmnožiny X, které ji rozdělují na disjunktní části. Pro každé $a \in X$ díky identitě platí $a \in \mathcal{O}(a)$. Pokud dále α_g posílá $a \mapsto b$, inverzní bijekce $\alpha_{g^{-1}}$ vrací $b \mapsto a$. Dále vidíme, že když $\alpha_g : a \mapsto b$ a $\alpha_h : b \mapsto c$, pak složené zobrazení α_{gh} posílá $a \mapsto c$. Dohromady jsme tedy ukázali, že každý prvek $a \in X$ je v nějaké orbitě a orbity každých dvou různých prvků jsou buď stejné, nebo disjunktní.

Když místo celé množiny X uvážíme pouze některou orbitu (případně sjednocení libovolného počtu z nich), lze mluvit o akci G na této menší množině – příslušné permutace zkrátka zúžíme jen na vybrané orbity. Na jiných podmnožinách $Y \subset X$ naopak G takto působit nemůže, neboť by naše permutace některé prvky posílaly ven z Y. Základními kousky nějaké akce grupy G jsou tedy přesně tyto menší akce na jejích jednotlivých orbitách, jejichž „slepením“ získáme původní akci. Takové akce mají své jméno.

Definice. Akce se nazývá *tranzitivní*, jestliže má jedinou orbitu.

Jak už jsme uvedli, je zúžení akce na kteroukoliv orbitu $\mathcal{O}(a)$ tranzitivní akcí. Tranzitivní akce se chovají vcelku krotce. Především mají všechny prvky stejně velký stabilizátor. Vezmeme-li totiž dva prvky $a, b \in X$, z tranzitivity existuje $g \in G$, které posílá $a \mapsto b$. Díky tomuto vztahu ale snadno dostáváme ekvivalenci $h \in G_b \iff \alpha_h(b) = b \iff \alpha_h(\alpha_g(a)) = \alpha_g(a) \iff \alpha_{g^{-1}}\alpha_h(\alpha_g(a)) = a \iff \alpha_{g^{-1}hg}(a) = a \iff g^{-1}hg \in G_a$. Tím jsme tedy odvodili množinovou rovnost $G_a = g^{-1}G_b g$.

Obecně je velmi snadné najít vztah mezi velikostí nějaké orbity, velikostí stabilizátoru jejího libovolného prvku a velikostí působící grupy G.

Tvrzení. *Mějme akci α grupy G na množině X. Potom pro libovolné $a \in X$ platí $|\mathcal{O}(a)| = [G : G_a]$.*

Důkaz. Vezměme libovolné $g \in G$ a odpovídající koset gG_a. Libovolný prvek gk tohoto kosetu (kde $k \in G_a$) pak na prvek a působí stejným způsobem jako g, neboť $\alpha_{gk}(a) = \alpha_g(\alpha_k(a)) = \alpha_g(a)$. Pokud jsou naopak kosety gG_a, hG_a různé, prvek $g^{-1}h$ nepatří do G_a, takže $\alpha_{g^{-1}h}(a) \neq a$, což po provedení α_g dává $\alpha_h(a) \neq \alpha_g(a)$. Různá posunutí prvku a v rámci jeho orbity tedy odpovídají jednotlivým kosetům podgrupy G_a – těchto posunutí (prvků $\mathcal{O}(a)$) je proto přesně $[G : G_a]$.

Speciálně jsme si tím znovu ukázali, že velikosti stabilizátorů všech prvků z jedné orbity jsou stejné. Nyní už akce známe dost na to, abychom si ukázali známé Burnsideovo lemma.

Věta. (Burnsideovo lemma) *Ať α je akce konečné grupy G na konečné množině X. Počet orbit této akce na množině X označme Ω. Potom platí*

$$\Omega = \frac{1}{|G|} \sum_{a \in X} |G_a|.$$

Důkaz. Rovnost můžeme upravit do tvaru

$$\Omega \cdot |G| = \sum_{a \in X} |G_a|.$$

Toto nyní nahlédneme kombinatoricky. Číslo Ω odpovídá počtu orbit naší akce, pokud si tedy z každé orbity $\mathcal{O}(a)$ vybereme právě jednoho zástupce a, bude těchto zástupců přesně Ω. Na každý z těchto vybraných prvků nyní vypustíme všechny prvky G, čímž dostaneme celkem $\Omega|G|$ ne nutně různých prvků množiny X. Levá strana dokazované rovnosti proto představuje jeden způsob, jak spočítat, kolik prvků jsme dostali. Ukážeme, že i suma na pravé straně představuje počet získaných prvků.

Každý z našich Ω vybraných zástupců dostaneme právě tolikrát, jaká je velikost jeho stabilizátoru v grupě G. Na každé z orbit působí grupa G tranzitivně, neboli každý prvek $b \in \mathcal{O}(a)$ dostaneme jako $\alpha_g(a)$ pro nějaké $g \in G$. Co víc, v rámci důkazu předchozího tvrzení jsme si rozmysleli, že prvek $b = \alpha_g(a)$ dostaneme přesně $|G_a|$-krát. To je ale podle předešlého tvrzení přesně velikost jeho stabilizátoru G_b. Levá strana je tedy skutečně rovna součtu velikostí stabilizátorů všech prvků, tj. sumě na pravé straně. Tím je důkaz dokončen.

Při praktickém použití této věty, o kterém se dočtete v příští kapitole, se často hodí dívat se na pravou stranu trochu jinak. Suma na pravé straně odpovídá počtu všech dvojiček $g \in G$ a $x \in X$ takových, že α_g fixuje[13] x. Můžeme ji proto dostat také sčítáním počtů takových x přes všechny prvky $g \in G$.

Počítání náhrdelníků

Burnsideovo lemma je velmi elegantní a často z něj vyplývají další zajímavá obecná tvrzení, ještě častěji nám ale pomůže počítat velmi konkrétní věci. Představme si následující situaci. Popelka dostala od macechy nepříjemný úkol, který ji má zákeřně připravit o návštěvu plesu. Macecha totiž z hrášku, čočky, rýže a lecčeho dalšího, co jí přišlo pod ruku, vyrobila všechny možné kruhové náramky. Popelka má za úkol spočítat, kolik druhů náramků na zemi leží. Holoubci jsou bohužel z takové směsi trochu zmatení; mají problém poznat, které náramky jsou stejné, a které nikoli. Co by mohlo zoufalé Popelce pomoci? Burnsideovo lemma!

Množina X nyní nebude popisovat vnitřní struktury nějakého objektu, místo toho v ní budou ležet všechna „nakreslení“ našich barevných náramků. Akce vhodné grupy G pak bude říkat, které obrázky zachycují stejný náramek. Zvolíme ji totiž tak lišácky, aby dva obrázky zachycovaly stejný náramek právě tehdy, když budou ležet ve stejné orbitě. Znalost počtu všech obrázků a grupy G nám společně s Burnsideovým lemmatem přesně řekne, kolik různých náramků na zemi leží.

Pojďme si to tedy zkusit na příkladech.

Příklad. Mějme sedm černých a šest bílých korálků. Kolik různých náramků z nich lze vyrobit, musíme-li použít všechny? Dva náramky považujeme za různé, pokud je na sebe nelze převést pohybováním v prostoru.

Řešení. Zajímáme se o nějaké náramky délky 13. Dva náramky podle zadání považujeme za stejné právě tehdy, když na sebe jejich nakreslení lze převést pomocí nějakých rotací a reflexí. Jinými slovy, počet takových náramků je přesně roven počtu orbit při očividné akci grupy D_{26} na množině všech třináctiúhelníků se sedmi černými a šesti bílými vrcholy. Tato množina má $\binom{13}{7}$ prvků.[14] Identická permutace fixuje právě všech $\binom{13}{7}$ prvků. Protože je ale 13 prvočíslo, žádná jiná rotace žádný různobarevný náramek fixovat nemůže. A konečně každá z osových symetrií fixuje přesně ty náramky, které jsou symetrické podle příslušné osy. Snadno si rozmyslíme, že těch je $\binom{6}{3}$. Z Burnsideova lemmatu dostáváme celkem $\frac{1}{26}\left(\binom{13}{7} + 12 \cdot 0 + 13 \cdot \binom{6}{3}\right)$ různých náramků.

Cvičení 5. Mějme hromadu modrých, zelených, červených a růžových korálků. Kolik existuje různých náhrdelníků z přesně patnácti takových korálků? Dva náhrdelníky považujeme za různé, pokud je na sebe nelze převést pohybováním v prostoru.

Cvičení 6. Mějme nekonečnou čtvercovou mřížku obarvenou černou a bílou. Přitom víme, že pro každé celé x, y mají políčka se souřadnicemi $[x, y+9], [x, y-9], [x+9, y]$ a $[x-9, y]$ stejnou barvu jako políčko se souřadnicemi $[x, y]$. Kolik takových obarvení roviny existuje? Dvě obarvení považujeme za stejná, pokud se liší pouze posunutím.

[13] Tímto slovem myslíme, že se daný prvek v daném zobrazení zobrazí sám na sebe.

[14] Použitý symbol představuje tzv. *kombinační číslo*, což je velmi důležitý pojem z kombinatoriky. Kdo se s ním ještě nepotkal, snadno si ho dohledá.

Výsledky předchozích cvičení velmi závisely na prvočíselném rozkladu zadaných čísel, což není náhoda. Podobným způsobem bychom mohli vyřešit mnoho dalších příkladů. Zkusme si nyní něco zajímavějšího. V následující úloze totiž bude potřeba lišácky vybrat množinu i působící grupu.

Úloha 1. Ať m, n jsou libovolná přirozená čísla. Dokažte, že potom číslo n dělí součet[15]

$$\sum_{i=1}^{n} m^{\mathrm{NSD}(n,i)},$$

kde $\mathrm{NSD}(a,b)$ značí největšího společného dělitele čísel a, b.

Pólyovy poly(a)nomy

Ještě než opustíme kouzelný svět Burnsideova lemmatu, ukážeme si jeho zobecněnou verzi. Už umíme snadno spočítat, kolik různých náhrdelníků pevné délky dostaneme kombinováním neomezeného počtu korálků různých barev. Také umíme spočítat, kolik náhrdelníků dostaneme použitím přesně daných počtů korálků jednotlivých barev. Pro jiné rozložení barev korálků bychom ale museli celou úlohu řešit znovu. Pólyova věta nám říká, jak takovou úlohu vyřešit pro všechna možná rozložení barev naráz.

Definice. Mějme grupu $G \leq S_X$ pro nějakou konečnou množinu X velikosti n. Pak *polyanomem*[16] prvku $g \in G$ nazveme polynom $P_g(x_1, \ldots, x_n) = x_1^{q_1} x_2^{q_2} \cdots x_n^{q_n}$, kde x_i jsou proměnné a q_i značí počet cyklů délky i v permutaci g.

Všimněme si, že pro přehlednost nemluvíme o obecných akcích, ale rovnou o podgrupách konečných symetrických grup. Nebyl by samozřejmě problém vše definovat i pro obecné akce, pro své potřeby bychom tím ale vůbec nic nezískali. Jakmile máme polyanom pro jeden prvek grupy, nic nám nebrání všechny takové polyanomy sečíst.

Definice. Mějme grupu $G \leq S_X$ pro nějakou konečnou množinu X velikosti n. *Polyanomem*[17] grupy G pak nazveme polynom

$$P_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} P_g(x_1, \ldots, x_n).$$

Zdůrazněme, že opět pracujeme pouze s konečnými grupami, tyto definice proto dávají dobrý smysl. Polyanom P_G přitom jakýmsi prazvláštním způsobem zachycuje, jakou strukturu mají permutace z G.

V duchu předchozích úloh o barvení nyní budeme chtít barvit kousky (korálky) nějakého většího celku (náhrdelníku), který má jakousi složitější vnitřní strukturu (korálky jsou na provázku). Tuto vnitřní strukturu odráží nějaká vhodně zvolená grupa G. Na barvený předmět se tedy díváme pouze jako na množinu X barvených kousků (korálků), které budeme barvit pomocí barev z konečné množiny C. To nám dává soubor všech možných obarvení množiny X, kterých je $|C|^{|X|}$; ten příhodně označíme C^X. Některé prvky C^X ale odpovídají stejnému předmětu. Grupa G současně působí na C^X tak, že prohazuje barvy jednotlivých prvků z X. Stačí tedy zvolit G tak, aby různé předměty odpovídaly různým orbitám, a nechat ji zapůsobit.

Úmluva. Ať X je konečná množina, $G \leq S_X$ a C konečná množina barev. Potom označme β akci grupy G na množině C^X, kde pro $g \in G$ prvek β_g přiřazuje nějakému obarvení $a \in C^X$ to obarvení $\beta_g(a) \in C^X$, v němž je každý prvek $x \in X$ obarven tou barvou, kterou je obarven jeho

[15] Ten lze pomocí Eulerovy funkce φ zapsat i jako $\sum_{d|n} \varphi(\frac{n}{d}) m^d$.

[16] Jak už si čtenář možná všiml, autoři mají zálibu v hrátkách se slovy. Tento pojem se běžně nepoužívá.

[17] V běžné literatuře se vyskytuje termín *cyklický index*.

vzor při permutaci g v obarvení a. (Lidsky řečeno: Vždycky vezmeme obarvený předmět a pustíme na něj permutaci g.)

Doteď jsme jen (dost formálně) shrnuli to, co už jsme dávno sami od sebe dělali v minulé sekci. Naším cílem je nyní vyjádřit, kolik různě obarvených předmětů dostaneme z kterého rozložení barev.

Definice. Mějme množinu C sestávající z k barev $c_1, c_2, \ldots, c_k$. Potom si pro každé $i \in \{1, 2, \ldots, k\}$ označme $g_i = c_1^i + c_2^i + \cdots + c_k^i$, kde všechna c_i vnímáme jako proměnné.

Na první pohled se může zdát naše počínání trochu pomatené, ne-li podezřelé. Jak mohou být barvy zároveň proměnné? Naše polyanomy ale nebudou určené k tomu, aby se do nich nedej bože něco dosazovalo. Jedná se o takzvané *formální* polynomy. Budeme pouze zkoumat, co se děje s jejich koeficienty při různých výpočtech.

Věta. (Pólyova) *Ať X je nějaká konečná množina velikosti n, $G \leq S_X$. Prvky X obarvujme barvami z $C = \{c_1, \ldots, c_k\}$, soubor všech takových obarvení označme C^X. Počet těch orbit akce β grupy G na množině C^X, jejichž prvky využívají barvu c_i přesně r_i-krát pro $i \in \{1, \ldots, k\}$, je pak roven koeficientu u členu $c_1^{r_1} \cdots c_k^{r_k}$ v polyanomu $P_G(g_1, \ldots, g_n)$.*

Důkaz. Pro libovolná taková r_i tedy musíme dokázat rovnost koeficientu u členu $c_1^{r_1} \cdots c_k^{r_k}$ v polynomu $P_G(g_1, \ldots, g_n)$ a počtu orbit akce β, jejichž prvky využívají barvu c_i přesně r_i-krát pro každé i. Označme pro přehlednost $R(g_1, \ldots, g_n) = |G| \cdot P_G(g_1, \ldots, g_n)$.

Zkoumejme dále akci β pouze na množině Y sestávající z těch obarvení z C^X, která obsahují právě r_i prvků barvy c_i pro každé i. Tuto ořezanou akci označme β' – to dobře definovaná akce, neboť Y je sjednocením některých orbit akce β. Díky Burnsideovu lemmatu nám pak stačí ukázat, že koeficient l u členu $c_1^{r_1} \cdots c_k^{r_k}$ v polynomu $R(g_1, \ldots, g_n)$ je roven součtu velikostí všech stabilizátorů této akce β'.

To je ale to samé jako tvrdit, že koeficient l je roven sumě $\sum_{g \in G} F(g)$, kde $F(g)$ značí počet prvků množiny Y, jež jsou fixovány permutací β'_g. Poslední zmíněnou rovnost nahlédneme dokonce trochu jemněji. Ukážeme, že číslo $F(g)$ je rovno koeficientu u $c_1^{r_1} \cdots c_k^{r_k}$ v polyanomu $P_g(g_1, \ldots, g_n)$. Tím budeme hotovi, neboť máme za úkol dokázat rovnost pro součty takových výrazů přes všechna $g \in G$, přičemž $R(g_1, \ldots, g_n)$ je přesně součet $P_g(g_1, \ldots, g_n)$ přes všechna $g \in G$.

Z definice polyanomu prvku máme $P_g(x_1, \ldots, x_n) = x_1^{q_1} \cdots x_n^{q_n}$, kde q_i značí počet cyklů délky i v permutaci g. Které prvky množiny C^X taková permutace fixuje? Přesně ty, které mají v každém jejím cyklu všechny prvky obarvené stejnou barvou.[18] Nás ale zajímá, kolik fixuje prvků pouze z množiny Y.

Dosazení polynomů $g_i = c_1^i + \cdots + c_k^i$ za x_i kombinatoricky odpovídá tomu, že každý cyklus zkoušíme obarvit každou barvou. Přesněji, za každé x_i dosazujeme polynom $g_i = c_1^i + \cdots + c_k^i$. Než roznásobený polynom upravíme sčítáním, je před každým členem koeficient 1. Otázkou je proto pouze to, kolikrát který člen při roznásobování dostaneme. Za každý cyklus permutace g je navíc v součinu právě jeden činitel. Samotné roznásobování přitom probíhá tak, že z každé závorky tvaru $(c_1^i + \cdots + c_k^i)$ vybereme jeden člen, což kombinatoricky odpovídá obarvení všech i prvků daného cyklu permutace g vybranou barvou. Různých obarvení, která pro všechna i využívají barvu c_i přesně r_i-krát, je pak právě tolik, kolik po roznásobení dostaneme členů $c_1^{r_1} \cdots c_k^{r_k}$. To je po úpravě rovno koeficientu u tohoto členu.

Pojďme nyní okusit sladké plody své dosavadní práce na příkladě. Ten by byl určitě řešitelný i méně pokročilými metodami, znalost polyanomů ho ale mnohonásobně zpřehlední. Navíc tím dostáváme návod, jak řešit mnohem komplikovanější příklady.

Příklad. Uvažme všechny různé grafy[19] na čtyřech nerozlišitelných vrcholech. Jeden z nich si

[18] Takových prvků je $k^{q_1 + \cdots + q_n}$.

[19] Kdo neví, co je to *graf*, nemusí zoufat. Odpověď snadno nalezne třeba v PraSečím seriálu *Letem grafovým světem*.

náhodně vybereme. Jaká je pravděpodobnost, že má počet hran dělitelný dvěma?

Řešení. Spočteme tedy počet všech takových grafů a počet všech grafů se sudým počtem hran. Graf B na n vrcholech je jednoznačně určen výčtem hran, které má. Možných hran je přitom $m = \binom{n}{2} = \frac{n(n-1)}{2}$. To, jestli hrana leží v B, nebo ne, můžeme vzájemně jednoznačně reprezentovat pomocí obarvování – hrany z B budou černé, ty ostatní bílé. Označme proto X množinu všech možných hran, dále ať $C = \{a, b\}$ je dvouprvková množina barev.

Dva grafy přitom považujeme dle zadání za stejné, lze-li vrcholy jednoho převést na vrcholy druhého permutací, která zachovává hrany – tj. spojené dvojice vrcholů zobrazuje na spojené, nespojené na nespojené. Hledáme tedy nějakou podgrupu $G \leq S_m$, jejíž orbity by stejnost grafů vystihovaly.

Vezmeme-li libovolnou permutaci vrcholů $g \in S_n$, získáme z ní jednoznačně určenou permutaci hran $\varphi(g) \in S_m$, která posílá hranu mezi vrcholy u, v na hranu mezi vrcholy $g(u), g(v)$. Přitom φ je prostý homomorfismus, takže $\operatorname{Im}\varphi \leq S_m$.

Označme $G = \operatorname{Im}\varphi$. Orbity příslušné akce β grupy S_n na množině C^X pak ale přesně odpovídají různým grafům na čtyřech nerozlišitelných vrcholech. Dva grafy B, B' s nerozlišitelnými vrcholy jsou stejné právě tehdy, když existuje permutace vrcholů $g \in S_n$, která zachovává hrany, tj. právě tehdy, když existuje permutace $h \in \operatorname{Im}\varphi$, která posílá barevnou reprezentaci B v množině C^X na barevnou reprezentaci B' v množině C^X.

Doteď jsme pracovali obecně pro libovolné pevné n. Tak bychom samozřejmě mohli pokračovat, raději se ale vrátíme ke konkrétnímu případu $n = 4$. Nejprve musíme spočítat polyanom grupy $\operatorname{Im}\varphi \leq S_6$, která obsahuje $24 = |S_4|$ prvků. Pro S_4 přímo víme, jaké „druhy“ prvků obsahuje: identitu, 6 transpozic, 3 dvojtranspozice, 8 trojcyklů a 6 čtyřcyklů. My ale hledáme polynom grupy $\operatorname{Im}\varphi$. S tužkou a papírem si není těžké rozmyslet, že φ zobrazuje identitu na identitu, transpozici na dvojtranspozici, dvojtranspozici také na dvojtranspozici, trojcyklus na dva trojcykly a čtyřcyklus na čtyřcyklus s transpozicí. Dostáváme proto polyanom

$$P_{\operatorname{Im}\psi}(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{24}\left(x_1^6 + 9x_1^2x_2^2 + 8x_3^2 + 6x_2x_4\right).$$

Zbývá dosadit $x_i = g_i = a^i + b^i$ a podívat se na správné koeficienty. Dostáváme polynom

$$\begin{aligned}(a, b) &= \frac{1}{24}\left((a+b)^6 + 9(a+b)^2(a^2+b^2)^2 + 8(a^3+b^3)^2 + 6(a^2+b^2)(a^4+b^4)\right) = \\ &= a^6 + a^5b + 2a^4b^2 + 3a^3b^3 + 2a^2b^4 + b^5a + b^6.\end{aligned}$$

Pokud tedy třeba b značí černou a a bílou, máme celkem $1 + 2 + 2 + 1 = 6$ různých grafů se sudým počtem hran. Počet všech grafů je naopak roven součtu koeficientů, což je 11. Hledaná pravděpodobnost je proto $\frac{6}{11}$.

Předchozí příklad chvilku zabral, zejména protože jsme důkladně zdůvodňovali, co děláme. Vlastní výpočet byl ale poměrně krátký a efektivní.

Cvičení 7. Kolik existuje různých pravidelných čtyřstěnů v prostoru, jejichž hrany jsou obarveny azurovou a blankytnou? Kolik takových čtyřstěnů má modrých hran stejně jako blankytných? A co jiná rozložení barev?

Ačkoli to tak na první pohled vůbec nemusí vypadat, Pólyova věta se v „běžném životě“ opravdu hodí. Jedná se o velmi praktický nástroj například při určování počtů různých druhů chemických sloučenin. Podobně má důsledky i při zkoumání hudebních akordů. A to ani nemluvíme o všech možných použitích při různých kombinatorických a algebraických výpočtech, kterých jsme byli svědky před chvílí.

Akce grupy na sobě samé

V předešlých částech jsme si předvedli, jak nám akce G na X může říci hodně jak o grupě G, tak o předmětu X. Co ale využít obě výhody akce naráz a použít ji na grupu samotnou? Takové akce jsou velmi přirozené a dokonce jsme se s nimi už nevědomky setkali...

Definice. Mějme grupu G. Působení grupy G *translací* na sobě samé je akce $\alpha : G \to S_G$, která prvku g přiřazuje permutaci z S_G odpovídající násobení zleva prvkem g v grupě G.

Přitom je třeba si uvědomit, že takto definovaná α je skutečně akcí, tedy homomorfismem $G \to S_G$. Už víme, že násobení zleva prvkem g je skutečně permutace množiny G. Pokud jsou $g, h \in G$, chceme ukázat $\alpha(gh) = \alpha(g)\alpha(h)$. Levá strana odpovídá té permutaci z S_G, která násobí prvky G zleva prvkem gh. Pravá strana zase odpovídá té permutaci, která vznikne složením násobení zleva prvkem h a násobením zleva prvkem g v tomto pořadí. Tyto dvě permutace jsou ale díky asociativitě operace $\cdot$ v grupě G stejné, což jsme přesně chtěli.

Tuto akci jsme již před časem nevědomky potkali. Je to přesně ten homomorfismus z Cayleyho věty, který vnořuje libovolnou grupu G do příslušné symetrické grupy S_G. Jde o věrnou akci.

Všimněme si, že toto lze obecněji provádět pro kosety nějaké pevné podgrupy $H \leq G$.

Definice. Mějme grupy $H \leq G$. Označme X množinu všech levých kosetů H v G. Působením grupy G *translací* na množině X rozumíme akci $\alpha : G \to S_X$, která prvku $g \in G$ přiřazuje permutaci z S_X určenou násobením kosetů zleva prvkem g.

Opět bychom si měli zkontrolovat, že takto definovaná α je opravdu akce. Protože prvek $g \in G$ permutuje prvky G a koset zobrazí na koset, permutuje i kosety. To, že je α homomorfismus, opět plyne z asociativity $\cdot$ v grupě G. Vůbec ale není jasné, zda je taková akce věrná, či nikoli. To záleží na konkrétní volbě G a H.

Pojďme si ukázat, jak nám mohou nabyté znalosti pomoci s na první pohled velmi nepřístupnými úlohami.

Věta. *Ať G je nekonečná jednoduchá grupa. Potom v ní neexistuje vlastní*[20] *podgrupa $H < G$ s konečným indexem.*

Důkaz. Ať pro spor taková H existuje. Provedeme drobné kouzlo. Uvažme působení α grupy G translací na množině X všech levých kosetů grupy H. Podívejme se na $\operatorname{Ker}\alpha$. Je-li $g \in \operatorname{Ker}\alpha$, musí α_g fixovat všechny kosety podgrupy H. Musí proto fixovat také H samotnou, odkud $gH = H$. To ale speciálně znamená $g = ge \in H$. Tím pádem máme $\operatorname{Ker}\alpha \leq H$, přičemž H je podle předpokladu vlastní podgrupa G. Takže nutně musí být $\operatorname{Ker}\alpha < G$. Jádra jsou ale normální, takže $\operatorname{Ker}\alpha \trianglelefteq G$. Protože $\operatorname{Ker}\alpha \neq G$ a G je jednoduchá, je už pak nutně $\operatorname{Ker}\alpha$ triviální, takže α je prosté. Potom je ale $G \simeq \operatorname{Im}\alpha \leq S_X$, jenže $|S_X| = [G : H]!$; tím jsme vnořili nekonečnou G do konečné S_X, což zřejmě nejde.

Podobně jako jsme definovali působení translací, které mluví o permutacích vytvořených násobením prvky grupy g zleva, můžeme si zavést akci, která bude říkat něco o konjugování.

Definice. Mějme grupu G. Působením G *konjugací* na sobě samé myslíme akci $\varphi : G \to S_G$, která prvku g přiřazuje permutaci danou konjugováním prvkem g.

Tuto akci už jsme také potkali. Permutace φ_g přiřazená prvku g je totiž přesně vnitřní automorfismus daný tímto prvkem. Přiřazení φ je skutečně homomorfismus, což opět vyplývá z asociativity binární operace $\cdot$ na grupě G.

Před nějakou dobou jsme také potkali pojem konjugovaných prvků a ukázali si, že konjugace rozděluje prvky grupy G do skupinek, ve kterých jsou spolu každé dva navzájem konjugované. To je nyní zřejmé, neboť to jsou přesně orbity akce φ_g.

Navíc jsme už viděli, že vnitřní automorfismy zobrazují podgrupy na podgrupy a normální podgrupy přitom nechávají na místě. Speciálně, je-li $H \leq G$, potom G působí konjugací na množině podgrup konjugovaných s H. Tyto vlastnosti konjugování ještě bohatě využijeme při práci se *Sylowovými větami*, které elegantně mluví o vnitřní struktuře konečných grup.

[20] *Vlastní* je taková podgrupa H, která se nerovná celé grupě G, tj. symbolicky $H \leq G$, $H \neq G$. Tuto skutečnost značíme přirozeným způsobem jako $H < G$.

Než přejdeme k dalším tématům, zadáme si jednu pěknou a notně trikovou úlohu, která s působením konjugací úzce souvisí.

Úloha 2. Ať G je konečná grupa, $A = \{a_1, \ldots, a_n\}$ nějaká její podmnožina. Dále víme, že každý prvek $g \in G$ je v G konjugovaný s nějakým prvkem množiny A. Dokažte, že $G = \langle A \rangle$.

Direktní součin

V matematice se často hodí uvažovat uspořádané n-tice nějakých čísel – třeba když chceme popisovat body v rovině či v prostoru. Nabízí se otázka, zda by uspořádané n-tice prvků, kde by v každé složce byly prvky nějaké grupy, náhodou netvořily novou grupu. Není těžké vidět, že tomu tak skutečně je.

Definice. *Direktním součinem* grup G, H rozumíme grupu $G \times H$ uspořádaných dvojic (g, h), kde $g \in G, h \in H$. Dva prvky násobíme tzv. po složkách: $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$, kde v první složce používáme operaci z grupy G a ve druhé operaci z grupy H.

Rychle si rozmyslíme, že se opravdu jedná o grupu. Operace bude asociativní, protože jsou původní operace asociativní. Neutrálním prvkem bude zřejmě (e, e), kde v první složce je neutrální prvek G a v druhé neutrální prvek H. Jelikož ale ze zápisu jednoznačně poznáme, o který neutrální prvek se jedná, můžeme je značit pro zjednodušení zápisů oba stejně. Inverzním prvkem k (g, h) bude (g^{-1}, h^{-1}).

Není těžké tuto definici rozšířit na více než dvě grupy. Zavedeme též přirozené značení $G^n = G \times G \times \cdots \times G$, kde G násobíme samo se sebou n-krát.

Příklad. Vektory v klasickém prostoru $\mathbb{R}^3$ spolu se sčítáním vyhovují naší definici jako prvky grupy $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$.

Cvičení 8. Nechť G', H' jsou podgrupy G, H. Rozmyslete si, že $G' \times H'$ je podgrupa $G \times H$.

Grupy G, H dostaneme přirozeným způsobem jako podgrupy $G \times H$. Jednoduše vidíme, že $G \simeq G \times \{e\} \leq G \times H$; stačí nám ztotožnit každý prvek g grupy G s prvkem (g, e) grupy $G \times H$. Obdobně můžeme vidět, že H je izomorfní podgrupě $\{e\} \times H$. Označme tyto podgrupy jako $\tilde{G}, \tilde{H}$. Není těžké ukázat, že se jedná dokonce o normální podgrupy $G \times H$ – můžete si to zkusit jako cvičení:

Cvičení 9. Nechť G, H jsou grupy. Pak $\tilde{G}$ i $\tilde{H}$ jsou normální podgrupy $G \times H$.

Navíc vidíme, že platí $\tilde{G} \cap \tilde{H} = \{(e, e)\}$ a $\tilde{G}\tilde{H} = G \times H$. Proč to tu ale tak dlouho rozebíráme? Ukážeme, že platí i v jistém smyslu opačné tvrzení. Zatím jsme se totiž na problém koukali jen jako na skládání menších grup, ale bylo by fajn, kdybychom zvládli někdy i o nějaké větší grupě zjistit, že je izomorfní direktnímu součinu nějakých menších. A k tomu se nám bude hodit následující tvrzení:

Tvrzení. *Nechť G je grupa a K, H dvě její normální podgrupy takové, že $K \cap H = \{e\}, KH = G$. Pak $G \simeq K \times H$.*

Důkaz. Víme, že $KH = G$. Každý prvek $g \in G$ můžeme tedy zapsat jako $g = kh$, kde $k \in K, h \in H$. Dokážeme nejdříve, že je tento zápis jednoznačný. Nechť $g = k_1 h_1 = k_2 h_2$; pak $k_2^{-1} k_1 = h_2 h_1^{-1}$. Na levé straně je prvek podgrupy K, na pravé podgrupy H – jediný prvek ležící v obou podgrupách je ale e. Takže nutně $k_2^{-1} k_1 = e = h_2 h_1^{-1}$, z čehož dostáváme $k_2 = k_1, h_2 = h_1$. Proto je tento zápis skutečně jednoznačný.

Uvažujme nyní zobrazení $\varphi : K \times H \to G$ takové, že $\varphi((k, h)) = kh$. Rádi bychom ukázali, že je toto zobrazení izomorfismus. Jistě se jedná o zobrazení na, neboť $G = KH$, a z předchozího odstavce plyne, že je i prosté. Stačí nám tedy ukázat, že se jedná o homomorfismus. Uvažme libovolné dva prvky $(k_1, h_1), (k_2, h_2)$ grupy $K \times H$. Potom $\varphi((k_1, h_1)(k_2, h_2)) = \varphi((k_1 k_2, h_1 h_2)) = k_1 k_2 h_1 h_2$, zatímco $\varphi((k_1, h_1))\varphi((k_2, h_2)) = k_1 h_1 k_2 h_2$. Chceme tedy ukázat, že $k_1 k_2 h_1 h_2 = k_1 h_1 k_2 h_2$. To lze přepsat jako $k_2 h_1 = h_1 k_2$ neboli $k_2 h_1 k_2^{-1} h_1^{-1} = e$. Ukážeme-li, že výraz na levé straně patří do H i do K, víme už, že se nutně musí rovnat e. Jelikož je H normální, dostaneme konjugací h_1 prvkem

k_2 prvek z H a vynásobením prvkem h_1^{-1} znovu prvek z H. Obdobně z normality K máme, že $h_1 k_2^{-1} h_1^{-1} \in K$, takže i $k_2(h_1 k_2^{-1} h_1^{-1}) \in K$, jak jsme chtěli ukázat. Dokázali jsme tedy, že je φ homomorfismus, a tím i izomorfismus.

Cvičení 10. Ukažte, že grupa $\mathbb{Q}^\times$ všech racionálních čísel kromě nuly s násobením je izomorfní direktnímu součinu $\mathbb{Q}_+^\times \times \mathbb{Z}_2$, kde $\mathbb{Q}_+^\times$ je grupa všech kladných racionálních čísel s násobením.

Cvičení 11. Nechť G, H jsou grupy. Pak $G \simeq (G \times H)/\tilde{H}$ a podobně $H \simeq (G \times H)/\tilde{G}$.

Čínská zbytková věta

Čínská zbytková věta je tvrzení z teorie čísel, které se týká situace, kdy máme n po dvou nesoudělných čísel $m_1, \ldots, m_n$ a pro zkoumané číslo m známe zbytek po dělení každým z těchto čísel. Tím je totiž jednoznačně určený zbytek čísla m po dělení jejich součinem $m_1 \cdots m_n$. (A samozřejmě také naopak – tento zbytek jednoznačně určuje zbytky po dělení jednotlivými činiteli.) Podíváme se na tuto větu z pohledu teorie grup.

Tvrzení. *Nechť $m_1, m_2, \ldots, m_n$ jsou po dvou nesoudělná přirozená čísla. Pak $\mathbb{Z}_{m_1 m_2 \cdots m_n} \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$.*

Důkaz. Označme $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$. Uvažme zobrazení $\varphi : \mathbb{Z} \to G$, které číslu $a \in \mathbb{Z}$ přiřadí n-tici $(r_1, r_2, \ldots, r_n) \in G$, kde r_i je zbytek a po dělení m_i. Je lehce vidět, že se jedná o homomorfismus.

Jaké je jeho jádro? Aby se celé číslo zobrazilo na neutrální prvek v G, musí být dělitelné všemi čísly m_i. Jelikož jsou po dvou nesoudělná, nevyskytuje se žádné prvočíslo v rozkladu více než jednoho z nich. Pokud tedy chceme, aby bylo a dělitelné všemi z nich, musí být dělitelné jejich součinem. A také naopak – když je a dělitelné jejich součinem, tak se zobrazí na identitu. Takže jádro φ je cyklická podgrupa generovaná $m_1 m_2 \cdots m_n$, kterou označme K.

Z první věty o izomorfismu platí $\mathbb{Z}/K \simeq \operatorname{Im}\varphi$. Ale v prvním dílu jsme si přímo definovali grupu $\mathbb{Z}_n$ jako faktorgrupu $\mathbb{Z}$ podle podgrupy generované n. Takže $\mathbb{Z}/K = \mathbb{Z}_{m_1 m_2 \cdots m_n}$. Máme tedy izomorfismus mezi $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ a $\operatorname{Im}\varphi$, což je podgrupa G. Jedná se o dvě konečné grupy, takže $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ a $\operatorname{Im}\varphi$ musejí mít stejně prvků. To ale znamená, že $\operatorname{Im}\varphi$ musí být celé G (protože $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ i G mají $m_1 m_2 \cdots m_n$ prvků). Tím je tvrzení dokázáno.

Homomorfismus φ z důkazu má obraz **celé** $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ a na každý prvek z této grupy zobrazuje právě jeden koset podgrupy K v $\mathbb{Z}$. Ale z toho již plyne Čínská zbytková věta, neboť v jednom kosetu jsou právě všechna celá čísla, která dávají po dělení $m_1 m_2 \cdots m_n$ stejný zbytek.

Konečné grupy

Ve zbytku druhého dílu se zaměříme na konečné grupy a ukážeme si několik tvrzení, která nám říkají, co všechno takové grupy musejí splňovat. O struktuře malých grup je toho známo spoustu. Ví se třeba, jak vypadají až na izomorfismus všechny grupy až do řádu 2047. Když tedy v praxi narazíme na nějakou grupu řádu n, můžeme i vylučovacím způsobem zjistit, s jakou známou grupou je izomorfní.

Pokud bychom chtěli hloupě najít všechny možné grupy, tak by nám to zabralo hrozně moc času. Grupa je určena svou multiplikativní tabulkou a nejjednodušší odhad na počet grup řádu n je tudíž n^{n^2}. To je již pro dost malá n obrovské číslo, které bychom sice mohli díky svým znalostem o dost zmenšit, ale stejně se nejedná o žádnou lehkou práci. Hledat takové grupy tedy nemůžeme ani pomocí počítače úplně hloupě. V silách tohoto seriálu by bylo klasifikovat všechny grupy řádu nejvýše 15, ale i to by zabralo spoustu času, takže to nebudeme dělat. Místo toho si ukážeme nějaké příklady vět a myšlenek, které se při hledání všech možných grup používají. Tyto věty nejsou užitečné jen ke klasifikaci konečných grup, také nám dávají lepší náhled na to, co se v grupě vlastně může dít.

Začneme krátkým tvrzením, které už nám samo o sobě dá výčet všech grup řádu n pro nekonečně mnoho různých n.

Tvrzení. *Pokud G je grupa prvočíselného řádu p, pak $G \simeq \mathbb{Z}_p$.*

Důkaz. Jelikož má G alespoň dva prvky, existuje prvek, který není neutrální. Jaký může mít tento prvek řád? Jeho řád musí podle Lagrangeovy věty z prvního dílu dělit p. Protože se nejedná o neutrální prvek, musí řád navíc být větší než jedna. Proto je roven p. Cyklická podgrupa generovaná tímto prvkem má tedy p různých prvků a jedná se přímo o G. Grupa G je tedy cyklická, a proto izomorfní s $\mathbb{Z}_p$.

Pro grupy, které nemají prvočíselný řád, situace tak lehká není. V předchozím důkazu jsme použili Lagrangeovu větu. Při pohledu na její znění bychom si mohli položit otázku: „Už víme, že řád každé podgrupy dělí řád původní grupy G; platí ale také, že pro každý dělitel řádu grupy G existuje nějaká podgrupa takového řádu?“ Bohužel se ukazuje, že svět není tak krásný, aby tato věta platila.

Cvičení 12. Ukažte, že alternující grupa A_4 (grupa řádu 12) nemá žádnou podgrupu řádu 6. (Nebo si můžete najít jiný vlastní protipříklad.)

Obecné tvrzení tedy neplatí. Platí ale alespoň nějaká jeho část? Co kdybychom se třeba omezili na prvočíselné dělitele? Existuje pro každé prvočíslo p, které dělí řád grupy, podgrupa s řádem p? Už jsme ukázali, že každá taková podgrupa by musela být cyklická. Platnost tohoto tvrzení nyní ukážeme tím, že najdeme v grupě G prvek řádu p, který bude hledanou podgrupu generovat.

Věta. (Cauchyho) *Nechť G je konečná grupa a p prvočíslo, které dělí řád G. Pak existuje $a \in G$, jehož řád je roven p.*

Důkaz. Uvažme množinu X všech uspořádaných p-tic $(a_1, a_2, \ldots, a_p)$ prvků z G takových, že $a_1 a_2 \cdots a_p = e$. Tato množina má $|G|^{p-1}$ prvků, neboť prvních $p-1$ složek můžeme zvolit libovolně a pro poslední máme potom vždy právě jednu možnost, jak ji zvolit, aby součin všech byl neutrální prvek. Proč si vybíráme takhle divnou množinu? Budeme chtít ukázat, že v ní leží nějaká p-tice, která má všechny prvky stejné a různé od e. Pak řád tohoto prvku musí dělit p, ale přitom nemůže být roven jedné. A to je přesně to, co chceme dokázat.

Uvažme nyní následující akci α grupy $\mathbb{Z}_p$ na této množině. Prvek $g \in \{0, \ldots, p-1\}$ bude působit jako jakási rotace složek: $\alpha_g((a_1, \ldots, a_p)) = (a_{1+g}, \ldots, a_{p+g})$, kde dodefinujeme přirozeně $a_{p+i} = a_i$ pro každé $i \geq 1$. Ověřme, že se skutečně jedná o akci. Nejdříve není vůbec jasné, zda pro každé $g \in G$ obraz každého prvku X znovu leží v X, není ale těžké to ukázat. Pokud platí $a_1 a_2 \cdots a_p = e$, pak vynásobením a_1^{-1} zleva a a_1 zprava získáme $a_2 \cdots a_p a_1 = a_1^{-1} a_1 = e$. Obdobně můžeme pokračovat dál a ukázat pro všechny „orotované“ p-tice, že opravdu leží v X.

Musíme ještě ověřit, že α je skutečně homomorfismus z G do S_X. Tedy, že pro každé $g, h \in \mathbb{Z}_p$ platí $\alpha_g \circ \alpha_h = \alpha_{gh}$. Pro libovolné $(a_1, \ldots, a_p) \in X$ máme $(\alpha_g \circ \alpha_h)((a_1, \ldots, a_p)) = \alpha_g((a_{1+h}, \ldots, a_{p+h})) = (a_{1+h+g}, \ldots, a_{p+h+g}) = \alpha_{g+h}((a_1, \ldots, a_p))$, jak jsme chtěli ukázat.

Víme tedy, že je α skutečně akce. Prozkoumejme nyní její orbity. Pro velikost orbity prvku $a = (a_1, \ldots, a_p)$ máme $|\mathcal{O}(a)| = \frac{|\mathbb{Z}_p|}{|G_a|} = \frac{p}{|G_a|}$. Proto $|\mathcal{O}(a)| = p$ nebo $|\mathcal{O}(a)| = 1$. Jak ale vypadají p-tice, které mají orbitu o velikosti jedna? Každé $g \in \mathbb{Z}_p$ je musí nechat na místě, takže musejí mít nutně všechny prvky stejné. A také naopak – pokud má p-tice z X všechny prvky stejné, pak její orbita bude mít velikost jedna. Součet velikostí všech orbit je dělitelný p, takže i počet orbit o velikosti jedna musí být dělitelný p (p dělí všechny ostatní orbity). Aspoň jedna orbita velikosti jedna existuje – orbita prvku $(e, \ldots, e)$, který zřejmě leží v X. Proto jich musí existovat alespoň p, a musí tedy existovat nějaké $g \neq e$ takové, že $(g, \ldots, g) \in X$. Takový prvek bude mít řád p, jak jsme si už zdůvodnili v prvním odstavci.

Obecně platí, že pokud $n \mid |G|$ a n je mocnina některého prvočísla, pak v G existuje podgrupa řádu n.[21] Podgrupy jiných řádů sice grupa mít může, ale u všech to platit nemusí. Vidíme teď, že

[21] V seriálu ale ukážeme jen, že taková podgrupa existuje, když je n největší mocninou prvočísla,

protipříklad pro neexistenci podgrup všech „přípustných“ řádů z předešlého cvičení byl nejmenší možný – žádné přirozené číslo menší než 12 neobsahuje vlastního dělitele, který by nebyl mocninou nějakého prvočísla.

Ve zbytku tohoto dílu si dokážeme další střípek mozaiky – ukážeme, že pokud α je největší mocnina p v prvočíselném rozkladu $|G|$, pak G obsahuje podgrupu řádu p^α. Přitom si o takových podgrupách řekneme i něco víc. Základní věty o těchto podgrupách se jmenují po norském matematiku Sylowovi.

Sylowovy věty

Definice. Podgrupu H konečné grupy G nazveme *sylowovskou p-podgrupou*, pokud je její řád mocninou[22] prvočísla p a neexistuje žádná jiná podgrupa G s řádem mocniny p, která ji celou obsahuje.

Tvrzení. *Mějme konečnou grupu G a prvočíslo p, které dělí její řád. Pak existuje netriviální sylowovská p-podgrupa.*

Důkaz. Z Cauchyho věty víme, že existuje podgrupa G s řádem p. Vezměme nyní ze všech podgrup, jejichž řád je mocninou prvočísla p, tu s největším řádem a označme ji P. Tato podgrupa je sylowovskou p-podgrupou, neboť pokud by jiná podgrupa s řádem mocniny p celou P obsahovala, pak bychom vybrali místo P ji.

Věta. (Sylowovy věty) *Nechť G je konečná grupa, p prvočíslo, které dělí její řád, a n_p počet jejích sylowovských p-podgrup. Pak platí následující:*

(1) *Pro každé dvě sylowovské p-podgrupy P, Q existuje prvek $g \in G$ takový, že $gPg^{-1} = Q$;*
(2) *$p \mid n_p - 1$ a zároveň $n_p \mid |G|$;*
(3) *každá sylowovská p-podgrupa má řád p^k, kde p^k je největší mocnina p, která dělí $|G|$.*

Podgrupy, pro které platí podmínka z první části tvrzení, nazýváme *konjugované v G*. Z toho, že zobrazení $h \mapsto ghg^{-1}$ je (vnitřní) automorfismus, plyne, že P a Q musejí být izomorfní. Ukážeme si nejdříve na příkladu, co si pod uvedenými pojmy a skutečnostmi můžeme představit.

Příklad. Nechť S_p je symetrická grupa na p prvcích, kde p je prvočíslo. Rádi bychom našli její sylowovské p-podgrupy. Řád G je roven $p!$. Největší mocnina p, která dělí tento řád, je právě p. Každá podgrupa s řádem p musí být cyklická. O jaké podgrupy se jedná? Řád permutace je roven nejmenšímu společnému násobku délek jejích cyklů,[23] takže jediné permutace řádu p jsou ty, kde se nachází pouze jediný cyklus, a to délky p. Právě podgrupy generované nějakým takovým prvkem budou tedy sylowovskými p-podgrupami.

Ověříme, že pro ně opravdu platí zformulovaná tvrzení. Pokud vezmeme dvě takové podgrupy P, Q a nějaké jejich generátory π, σ, pak díky stejné cyklové struktuře nutně existuje nějaká permutace ψ taková, že $\psi\pi\psi^{-1} = \sigma$. Vynásobením této rovnosti i-krát dostáváme $\psi\pi^i\psi^{-1} = \sigma^i$. Takže ψ opravdu konjugací zobrazuje prvky z P právě na prvky z Q – podgrupy P, Q jsou tedy v S_p konjugované.

Kolik jich je? Máme $p!$ způsobů, jak za sebe napsat čísla 1 až p, ale každý cyklus takto dostaneme v p různých otočeních. Takže cyklů o délce p existuje $(p-1)!$. Navíc každá sylowovská p-podgrupa obsahuje identitu a $p-1$ takových cyklů. Každý z těchto cyklů generuje celou podgrupu, a nemůže proto patřit ani do žádné jiné. Všechny cykly generují tedy dohromady jen $n_p = \frac{(p-1)!}{p-1} = (p-2)!$

---

která dělí $|G|$. Potom by již stačilo pouze ukázat, že pokud má grupa řád mocniny prvočísla, pak už obsahuje podgrupy všech řádů, které ho dělí. To není o nic těžší než zbylé důkazy v seriálu, zabývat se tím již ale nebudeme.

[22] Mocninou prvočísla p myslíme libovolné číslo ve tvaru p^n, kde n je celé nezáporné.

[23] To si můžete rozmyslet jako snadné cvičení.

podgrup. Z Wilsonovy věty platí v grupě $\mathbb{Z}_p^\star$ identita $(p-1)! = p-1$, z níž vynásobením $(p-1)^{-1}$ dostáváme $(p-2)! = 1$. Takže skutečně $p \mid n_p - 1$. Navíc zřejmě $n_p \mid |S_p|$, neboť $(p-2)! \mid p!$.

Poslední část tvrzení je už zřejmá. Největší mocnina p, která dělí $p!$, je totiž p^1 a námi popisované podgrupy mají přesně tento řád.

Předtím, než se pustíme do samotného důkazu, zmiňme ještě jedno zajímavé tvrzení plynoucí ze Sylowových vět.

Tvrzení. *Nechť G je konečná grupa a p prvočíslo, které dělí její řád. Pak sylowovská p-podgrupa P je normální v G právě tehdy, když je jediná.*

Důkaz. Pokud je P v G normální, tak pro všechna $g \in G$ platí $gPg^{-1} = P$. Nemůže tedy existovat žádná další sylowovská p-podgrupa, protože by nebyla s P konjugovaná.

Pokud naopak P v G normální není, existuje nějaké $g \in G$ takové, že $gPg^{-1} \neq P$. Označme $Q = gPg^{-1}$. Jedná se o grupu stejného řádu, neboť konjugace prvkem g dává vnitřní automorfismus G. Podle třetí části Sylowových vět má také řád největší mocniny p, která dělí řád G, takže je také sylowovská. Našli jsme tedy další sylowovskou p-podgrupu, a tím ukázali, že jediná sylowovská p-podgrupa existuje opravdu pouze tehdy, když je normální v G.

Dokažme si nyní postupně všechna tři tvrzení ze Sylowových vět. Nenechte se vyděsit délkou tohoto důkazu. Mohli bychom ho napsat kratší – používá se v něm ale několik originálních myšlenek, které jsme pro (snad) lepší pochopení rozepsali více.

Důkaz. Nechť X je množina všech podgrup grupy G. Grupu G necháme na tuto množinu působit konjugací. Označme tuto akci α; pro libovolné $g \in G$ a $H \in X$ tedy bude $\alpha_g(H) = gHg^{-1}$. (To, že je α skutečně akcí, jsme již zmínili dříve.)

Naší metou bude ukázat, že všechny sylowovské p-podgrupy leží v jedné orbitě této akce. To je přesně to, co chceme, neboť pokud leží dvě podgrupy H, K ve stejné orbitě, tak existuje nějaké $g \in G$ takové, že $\alpha_g(H) = K$. Jinými slovy jsou tyto dvě grupy v G konjugované. K tomuto cíli budeme směřovat v následujících asi sedmi odstavcích.

Již víme, že nějaká sylowovská p-podgrupa existuje, vyberme si tedy libovolnou z nich a označme ji P. Orbitu $\mathcal{O}(P)$ akce α označme O. V O budou jistě pouze sylowovské p-podgrupy. Předpokládejme totiž pro spor, že by nějaká $R \in O$ sylowovská nebyla – tedy, že by pro nějakou $R \in O$ existovala větší podgrupa V s řádem mocniny p, která by R obsahovala. Jelikož P, R leží ve stejné orbitě akce α, existuje $g \in G$ takové, že $\alpha_g(R) = P$. Potom ale $\alpha_g(V)$ je podgrupa s řádem mocniny p větším než řád P, která obsahuje P. To je ve sporu s tím, že je P sylowovská.

Vezměme nyní libovolnou další[24] sylowovskou p-podgrupu Q a ukažme, že Q leží v O. K tomu definujeme další akci β. Tentokrát půjde o akci grupy Q konjugací na množině O. Pro každé $q \in Q$ a $R \in O$ tedy definujeme $\beta_q(R) = qRq^{-1}$. Tato akce vypadá na první pohled hrozně divně a není vůbec jasné, zda je dobře definovaná. U α nám stačilo ověřit, že obraz podgrupy v konjugaci je znovu podgrupa. Zde ale máme jen několik podgrup, takže musíme nejdříve říct, že $\beta_q(R)$ vždy leží v O. Pro $q \in Q$ a $R \in O$ se ale β chová úplně stejně jako α, tj. $\beta_q(R) = \alpha_q(R)$. Navíc O je orbita akce α, takže skutečně $\beta_q(R) = \alpha_q(R) \in O$ pro všechna $q \in Q$ a $R \in O$. To, že je β homomorfismus, by se ověřilo úplně stejně jako u normální konjugace.

Zatím to vypadá, že jen definujeme čím dál tím divnější věci a konec důkazu je v nedohlednu. Není tomu ale tak. Nyní nám už jen stačí spočítat počet prvků v O. Ukážeme, že $p \mid |O| - 1$ a zároveň že pokud by $Q \notin O$, pak by $|O|$ bylo dělitelné p; z toho už bude jasné, že nutně $Q \in O$.

Akce β má dovoleno působit pouze některými prvky, může se tedy stát, že O se rozpadne na více orbit vzhledem k akci β, protože ta $g \in G$, která podgrupy v O „spojovala“, v Q nebudou. Jak velké budou orbity akce β? Když jsme si definovali akce, dokázali jsme, že velikost orbity obsahující prvek a je rovna indexu stabilizátoru tohoto prvku v grupě, kterou působíme. Takže velikost orbity je rovna řádu této grupy děleného něčím. Řád Q je ale mocnina p, tím pádem i velikost každé orbity musí být mocnina prvočísla – je tedy buď dělitelná p, nebo rovna 1. Prověříme nyní, kdy se

[24] Může ale být i $Q = P$.

může stát, že je rovna jedné. Ukážeme, že pokud $Q \in O$, stane se to právě jednou, a pokud $Q \notin O$, nestane se to nikdy.

Předpokládejme tedy, že existuje nějaká $R \in O$ taková, že je v orbitě sama. To znamená, že $qRq^{-1} = R$ pro všechna $q \in Q$. Později dokážeme, že potom každé $q \in Q$ nutně leží v R. Věřte nám ale na chvíli, že toto opravdu platí.

Pak dostáváme, že je Q podgrupa R. Pokud by $R \neq Q$, pak by R byla větší podgrupa než Q s řádem mocniny prvočísla, která Q obsahuje. Taková ale nemůže existovat, neboť je Q sylowovská. Musí tedy být $R = Q$. Na druhé straně, platí-li $R = Q$, pak zřejmě $qRq^{-1} = R$ pro všechna $q \in R = Q$.

Orbita velikosti jedna vznikne tedy právě tehdy, když je $Q \in O$, a v tom případě bude pouze jedna. Všimněme si nyní, že původní sylowovská podgrupa P v O leží. Pokud zvolíme $Q = P$, bude v O jedna orbita velikosti jedna a velikosti všech zbylých budou dělitelné p. Dostaneme tedy $p \mid |O| - 1$. Pokud by nyní existovala $Q \notin O$, tak by platilo také $p \mid |O|$, což už nelze. (Pak by muselo p dělit i rozdíl těchto dvou čísel, což je jedna.)

Až na jedno přeskočené tvrzení jsme tedy ukázali, že každé dvě sylowovské p-podgrupy jsou v G konjugované (všechny leží ve stejné orbitě) a že platí $p \mid |O| - 1$. Ale $|O|$ je rovno počtu všech sylowovských p-podgrup n_p. Dostali jsme tedy $p \mid n_p - 1$. V důkazu zbytku se bohužel neobejdeme bez jednoho nového pojmu a pár technických lemmat. Slibujeme ale, že už nic nebude tak dlouhé.

Normalizátory

Definice. Uvažujme opět akci α grupy G na množině jejích podgrup definovanou jako $\alpha_g(R) = gRg^{-1}$ pro všechna $R \leq G$ a $g \in G$. To nám umožňuje pro každou grupu G a její podgrupu P definovat *normalizátor* podgrupy P v grupě G jako stabilizátor P vzhledem k této akci. Normalizátor je tedy podgrupou G a budeme ho značit $N_G(P)$.

Normalizátor není tedy nic exotičtějšího než stabilizátor v jedné konkrétní akci. Z jeho pojmenování můžeme odtušit, že by mohl mít něco společného s normalitou. A opravdu má:

Cvičení 13. Podgrupa P grupy G je normální právě tehdy, když $N_G(P) = G$.

Cvičení 14. Nechť G je grupa a H její podgrupa. Pak $H \trianglelefteq N_G(H)$.

Na normalizátor podgrupy H se tudíž můžeme dívat i jako na největší podgrupu, ve které je H normální. Řečené vlastnosti normalizátoru nyní aplikujeme v důkazu Sylowových vět.

Lemma. *Nechť G je konečná grupa a P její sylowovská p-podgrupa. Pak $p \nmid [N_G(P) : P]$.*

Důkaz. Již víme, že $P \trianglelefteq N_G(P)$. Uvažme tedy faktorgrupu $H = N_G(P)/P$. Předpokládejme pro spor, že p dělí index grupy P v $N_G(P)$ – tedy, že dělí řád H. Podle Cauchyho věty pak existuje nějaký prvek řádu p v H. Označme ho aP, kde a je nějaký prvek $N_G(P)$ neležící v P (jinak by měl koset $aP = P$ řád jedna). Ukážeme, že když do P „přidáme“ tento prvek a, dostaneme větší podgrupu s řádem mocniny p. Formálně definujme podgrupu Q generovanou množinou $P \cup a$. Dokážeme, že má tato grupa $p \cdot |P|$ prvků.

Podgrupa Q je uzavřená na grupové operace. Nachází se v ní a i celá grupa P. Proto tam musí ležet i prvky ze všech kosetů tvaru a^iP, kde $i \in \{0, 1, \ldots, p-1\}$. Koset aP má řád p – tím pádem jsou všechny takové kosety různé a máme $p|P|$ prvků, které musí ležet v Q. Ukážeme, že vzniklá množina už je uzavřená na grupové operace. Neutrální prvek v ní leží, protože ten leží už v P. Pokud jsou $g, h \in Q$, tak $g \in a^iP$ a $h \in a^jP$ pro nějaká $i, j \in \{0, 1, \ldots, p-1\}$. Inverzní prvek ke g tedy leží v $a^{p-i}P \subset Q$ a stejně tak $gh \in a^{i+j}P \subset Q$. Tím pádem je Q podgrupa, která má počet prvků rovný mocnině p, obsahuje P a je větší než P. To je ale ve sporu se skutečností, že je P sylowovská p-podgrupa. Tím je důkaz lemmatu dokončen.

Důkaz přeskočeného tvrzení pořád chybí, ale pokud si na něj vydržíme ještě chvíli počkat, ukážeme již celkem jednoduše, že řád sylowovské p-podgrupy je skutečně ten největší možný:

Jelikož je velikost orbity rovna indexu stabilizátoru libovolného jejího prvku a stabilizátor v konjugaci podgrup je normalizátor, platí $[G : N_G(P)] = |O|$. Dále víme, že $p \nmid [N_G(P) : P]$. Pro konečné grupy je index roven podílu velikostí. Proto dostáváme $\frac{|G|}{|P|} = \frac{|G|}{|N_G(P)|}\frac{|N_G(P)|}{|P|} = [G : N_G(P)] \cdot [N_G(P) : P] = |O|[N_G(P) : P]$. Ani jeden z činitelů vpravo není dělitelný p (víme, že $p \mid |O| - 1$), takže $|P|$ musí být dělitelné stejnou mocninou p jako $|G|$. Protože navíc víme, že $|O| = n_p$, dostáváme z uvedené rovnosti i další požadované tvrzení: $n_p \mid |G|$. A to je vše, co jsme chtěli dokázat.

K dokončení nám tedy stačí již jen důkaz onoho neustále přeskakovaného tvrzení, které zformulujeme jako následující lemma:

Lemma. *Nechť G je konečná grupa a p prvočíslo, které dělí její řád. Dále ať R je sylowovská p-podgrupa. Pokud má $q \in N_G(R)$ řád mocniny p, pak $q \in R$.*

Je to přesně to, co potřebujeme? V důkazu Sylowových vět působíme sylowovskou p-podgrupou Q konjugací na další sylowovskou p-podgrupu R. Víme dále, že $qRq^{-1} = R$ pro všechna $q \in Q$ – tedy Q leží uvnitř normalizátoru $N_G(R)$. Navíc z Lagrangeovy věty víme, že řád každého $q \in Q$ musí dělit $|Q|$, což je mocnina p. Takže i řád q musí být mocninou prvočísla p.

Důkaz. Pro spor předpokládejme, že $q \notin R$. Ve faktorgrupě $N_G(R)/R$ není tedy qR neutrálním prvkem. Označíme-li jeho řád r, víme tedy, že $r > 1$. Ukážeme, že r dělí řád q v Q, který označíme s. Můžeme psát $s = kr + l$, kde $k \in \mathbb{Z}$, $l \in \{0, 1, \ldots, r-1\}$. Máme $q^s = e$, tedy $q^s \in R$ a nutně $(qR)^s = R$. Ale i $(qR)^{kr} = ((qR)^r)^k = R^k = R$, takže $(qR)^l = (qR)^{s-kr} = RR^{-1} = R$. Pokud $l > 0$, byli bychom ve sporu s tím, že má qR řád r. Proto $l = 0$.

Řád r prvku qR v grupě $N_G(R)/R$ je tedy dělitelem řádu q v Q, což je mocnina prvočísla p. Jelikož $r > 1$, musí tím pádem p dělit r. Víme tedy, že p dělí řád $qR \in N_G(R)/R$, a z Lagrangeovy věty proto plyne, že p dělí i $|N_G(R)/R|$. To je ale ve sporu s předešlým lemmatem.

Tím je důkaz Sylowových vět konečně dokončen. Všimněte si, že v důkazu posledního lemmatu jsme využili jen vlastnosti normalizátoru, rozhodně ne něco ze Sylowových vět – to je důležité, jinak by totiž šlo o důkaz kruhem.

Sylowovy věty útočí

Chvilku to trvalo, ale nyní se už můžeme pustit do využívání Sylowových vět na konkrétní případy. Pokud si věříte, můžete si zkusit následující příklad sami.

Příklad. Neexistuje žádná jednoduchá grupa řádu 12.

Důkaz. Chceme ukázat, že každá dvanáctiprvková grupa má nějakou normální podgrupu. Jak to můžeme udělat bez toho, abychom se dívali na všechny takové grupy? Pomocí Sylowových vět! Stačí nám ukázat, že vždy existuje pouze jedna sylowovská 2-podgrupa nebo pouze jedna sylowovská 3-podgrupa.

Kolik může být sylowovských 3-podgrup? Trojka musí dělit jejich počet zmenšený o jedna a navíc jejich počet musí dělit dvanáctku. Může se tedy jednat pouze o přirozená čísla menší než 12 a z těch těmto podmínkám vyhovuje pouze 1 a 4. Pokud $n_3 = 1$, tak máme hotovo – sylowovská 3-podgrupa bude normální, a protože má řád 3, bude také vlastní. Zbývá nám tedy vyšetřit již jen případ $n_3 = 4$.

V tomto případě ukážeme, že existuje pouze jedna sylowovská 2-podgrupa. Každá ze čtyř sylowovských 3-podgrup má řád 3. Obsahuje identitu a další dva prvky, které musejí mít řád 3. Žádné dvě z těchto podgrup nemohou mít netriviální průnik, neboť každý jiný prvek je generátorem dané podgrupy, takže by nám vyšly dvě stejné. V grupě tedy existuje alespoň 8 prvků řádu 3. Sylowovská 2-podgrupa má řád největší mocniny dvojky, která dělí dvanáct – tedy 4. Nemůže ale obsahovat žádný z prvků řádu 3 – to by bylo ve sporu s Lagrangeovou větou. Musí tedy obsahovat právě ty čtyři zbývající prvky, a proto je pouze jedna. Takže je normální a vlastní – ani v tomto případě nedostaneme jednoduchou grupu.

Toto využití bylo velmi specifické. Stejný nástroj ale můžeme použít i na některé nekonečné třídy. Ukázali jsme si již, jak vypadají všechny grupy prvočíselného řádu. Dalším krokem by třeba mohlo být zkoumání, jak vypadají grupy, jejichž řád je součinem dvou různých prvočísel.

Tvrzení. *Nechť G je grupa řádu pq, kde $p < q$ jsou prvočísla a $p \nmid q-1$. Pak již $G \simeq \mathbb{Z}_{pq}$.*[25]

Důkaz. Nejdříve ukážeme, že $n_p = n_q = 1$. Víme ze Sylowových vět, že $n_p \mid pq$ i $n_q \mid pq$. Jsou ale jen čtyři různá přirozená čísla, která dělí pq, a to $1, p, q, pq$. Dále ze Sylowových vět víme, že $n_q = kq+1$ pro nějaké nezáporné celé k. Toto číslo není nikdy dělitelné q, takže nám nemůže vyjít q ani pq. Navíc $n_q = 1$ nebo $n_q \geq q+1 > q > p$, takže nemůže vyjít ani p a musí být nutně $n_q = 1$. Stejně tak dostaneme, že n_p není p ani pq. Pokud by bylo $n_p = q$, tak $lp + 1 = q$ pro nějaké l. Z toho ale plyne, že $p \mid q-1$, což jsme si v předpokladu zakázali. Musí proto nutně být i $n_p = 1$.

Sylowovská p-podgrupa i q-podgrupa jsou tedy normální – označme je P, Q. Mají prvočíselný řád, takže musí být nutně $P \simeq \mathbb{Z}_p, Q \simeq \mathbb{Z}_q$. Pokud ukážeme, že $P \cap Q = \{e\}$ a zároveň $PQ = G$, dostaneme již z věty o direktním součinu, že $G \simeq P \times Q \simeq \mathbb{Z}_p \times \mathbb{Z}_q$. A o té grupě jsme si již dokázali, že je izomorfní $\mathbb{Z}_{pq}$.

Proč $P \cap Q = \{e\}$? Všechny prvky P kromě neutrálního mají řád p v G. Stejně tak v grupě Q mají řád $q \neq p$. Žádné se tedy nemohou rovnat.

Označme a nějaký generátor grupy P, b generátor grupy Q (generátory existují, protože jsou P, Q cyklické). Ukážeme, že $G = \{a^i b^j\}$, kde $0 \leq i < p$, $0 \leq j < q$. Popsali jsme pq výrazů; abychom dokázali, že nám takto vyjdou všechny prvky G, stačí nám ukázat, že se žádné dva různé nerovnají. Nechť tedy $a^{i_1} b^{j_1} = a^{i_2} b^{j_2}$. Pak vynásobením b^{-j_1} zprava a a^{-i_2} zleva dostáváme $a^{-i_2} a^{i_1} = b^{j_2} b^{-j_1}$. Číslo vlevo patří do podgrupy P, číslo vpravo do Q. Jelikož mají pouze triviální průnik, tak se nutně obě strany rovnají e. Tím pádem $i_2 = i_1, j_2 = j_1$, neboli dva prvky se rovnají pouze tehdy, mají-li úplně stejné vyjádření.

Konečně do PQ patří jistě všechny prvky v tomto tvaru, takže G je částí PQ. Ale žádné další prvky dostat nemůžeme. Nutně tedy $PQ = G$ a máme hotovo.

Sylowovy věty tedy dávají takový číselněteoretický vhled do konečných grup. Velmi elegantním způsobem totiž postulují poměrně silné podmínky, které musí struktura konečné grupy dané velikosti splňovat. Jejich důkaz byl složitější, ale samotné znění nijak zvlášť komplikované není a můžeme pomocí nich dokázat spoustu věcí, které by bez nich byly velice obtížné. Dokážete si třeba představit, jak byste se snažili dokázat minulé tvrzení bez jejich znalosti?

Tím jsme důkladně prozkoumali symetrie a některé konečné objekty. Za dveřmi ale zatím leží obrovský svět těch nekonečných, které jsou neméně zajímavé, komplikované i užitečné. Těšme se na ně.

[25] Grupy, jejichž řád je součinem dvou různých prvočísel, se dají popsat i bez dodatečných předpokladů, museli bychom ale vybudovat ještě další nástroje, jako je například semidirektní součin grup. V takových případech navíc mohou existovat i grupy neizomorfní $\mathbb{Z}_{pq}$ – jako třeba D_{2q}.

Návody ke cvičením

1. Grupa G je abelovská právě tehdy, když pro libovolné $g, h \in G$ platí $gh = hg$, což je ekvivalentní faktu, že pro všechna $g, h \in G$ platí $\varphi_g(h) = ghg^{-1} = h$, což znamená, že všechny vnitřní automorfismy odpovídají identitě. Tím jsme dokázali celou ekvivalenci.

2. Ať $\varphi_g \in \mathrm{Inn}(G)$, $\psi \in \mathrm{Aut}(G)$. Potom homomorfismus $\psi\varphi_g\psi^{-1}$ libovolný prvek $h \in G$ posílá na prvek $\psi(g\psi^{-1}(h)g^{-1}) = \psi(g)h(\psi(g))^{-1}$, toto složené zobrazení tedy odpovídá homomorfismu $\varphi_{\psi(g)} \in \mathrm{Inn}(G)$. Takže $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

3. Protože pro libovolné $\sigma, \tau \in S_n$ platí $\mathrm{sign}(\tau\sigma\tau^{-1}) = \mathrm{sign}(\tau)\,\mathrm{sign}(\sigma)\,\mathrm{sign}(\tau^{-1})$ a $\mathrm{sign}(\tau) = \mathrm{sign}(\tau^{-1})$, zachovává konjugování paritu (tedy speciálně zachovává sudost), takže A_n je normální.

Trochu stylověji, $A_n = \mathrm{Ker}(\mathrm{sign})$ v našem zobrazení $\mathrm{sign} : S_n \to \{1, -1\}$ a jádra jsou normální.

4. Každý homomorfismus φ do $\{1, -1\}$ je určený svým jádrem $\mathrm{Ker}\,\varphi$, které je normální podgrupou S_n. My si ale s pomocí jednoduchosti A_n dokážeme něco mnohem silnějšího, a sice, že jediné normální podgrupy S_n pro $n \geq 5$ jsou $\{e\}$, A_n a S_n samotná.

Pro spor ať K je normální podgrupa takové S_n, ale je různá od těch jmenovaných. Protože průnik normálních podgrup je také normální, je pak i $K \cap A_n \trianglelefteq S_n$, je tedy normální i v A_n. Díky jednoduchosti je proto $K \cap A_n$ buď A_n, nebo $\{e\}$.

Pokud je ale $K \cap A_n = A_n$, máme z předpokladu $A_n < K < S_n$. Jenže potom $\frac{|S_n|}{2} = |A_n| < |K| < |S_n|$. To ale není možné, neboť $|K|$ potom nemůže být dělitelem $|S_n|$.

Pokud je naopak $K \cap A_n = \{e\}$, musí K obsahovat kromě identity pouze liché permutace. Protože je ale normální, s každou permutací obsahuje i všechny další permutace z S_n se stejnou cyklovou strukturou. Jakmile je tedy K netriviální a obsahuje nějakou lichou permutaci, díky podmínce $n \geq 5$ určitě obsahuje alespoň 4 prvky. Potom z ní ale lze vybrat dvě liché permutace π_1, π_2, které k sobě nejsou inverzní. Jenže potom je $\pi_1\pi_2 \in K$, $\pi_1\pi_2 \neq e$ a konečně $\mathrm{sign}(\pi_1\pi_2) = \mathrm{sign}(\pi_1)\,\mathrm{sign}(\pi_2) = 1$, což je spor.

Grupy $\{e\}$, A_n a S_n jsou tedy skutečně veškeré normální podgrupy S_n. To zároveň charakterizuje obrazy všech homomorfismů z S_n podle první věty o izomorfismu. Netriviální homomorfismus $S_n \to \{1, -1\}$ musí být na, proto jeho jádro musí mít v S_n index 2. Toto jádro je tedy nutně rovno $A_n = \mathrm{Ker}(\mathrm{sign})$, tedy sign je skutečně jediný takový homomorfismus (protože homomorfismy do dvouprvkové grupy jsou jednoznačně určené svým jádrem).

5. Dva náhrdelníky tedy považujeme za stejné, pokud na sebe jejich nakreslení lze převést pomocí nějakých rotací a reflexí. Uvažme proto akci grupy D_{30} na množině všech patnáctiúhelníků obarvených čtyřmi barvami; těch je 4^{15}. Identická permutace fixuje všech 4^{15} prvků. Rotace o k prvků pro k nesoudělná s patnácti fixují pouze ta čtyři nakreslení, která mají všechny korálky stejné. Rotace o $3k$ pak fixuje přesně ty náhrdelníky, ve kterých se periodicky opakuje sekvence tří korálků[26]; těch je 4^3. Podobně rotace o $5k$ fixuje 4^5 náhrdelníků. Každá z patnácti reflexí potom fixuje právě ta nakreslení, která jsou symetrická podle příslušné osy. Těch je 4^8.

Z Burnsideova lemmatu tudíž plyne

$$O = \frac{1}{30}(4^{15} + 8 \cdot 4 + 4 \cdot 4^3 + 2 \cdot 4^5 + 15 \cdot 4^8),$$

což se rovná hledanému počtu různých náhrdelníků.

6. Díky zadaným podmínkám je každé takové dláždění jednoznačně určeno svým vzhledem na pevném čtverci 9×9. Trochu lépe řečeno, čtverečky, které se liší v obou souřadnicích o násobky 9, můžeme považovat za stejné. To nám dává 2^{81} způsobů obarvení. Některá obarvení ale považujeme za stejná. Uvažme grupu G, jejíž prvky odpovídají posunutím čtvercové mřížky o $i \in \{0, 1, \ldots, 8\}$ doprava a o $j \in \{0, 1, \ldots, 8\}$ nahoru (později se v seriálu dozvíme, že se tato grupa jmenuje $\mathbb{Z}_9 \times \mathbb{Z}_9$).

[26] To, že nefixuje žádné jiné náhrdelníky, plyne z toho, že pět je prvočíslo.

Grupa G má 81 prvků. Identita fixuje všech 2^{81} nakreslení. Posunutí o i nahoru a j doprava pak může fixovat pouze taková nakreslení, ve kterých se opakuje obdélník s rozměry $i \times j$. Navíc se ale musí opakovat celý čtverec 9×9. Snadno proto vidíme, že posunutí o i nahoru a j doprava fixuje právě ta nakreslení, ve kterých se opakuje obdélník s rozměry $\mathrm{NSD}(i,9) \times \mathrm{NSD}(j,9)$. Počet takových fixovaných nakreslení tedy závisí pouze na dělitelnosti čísel i, j čísly 3 a 9. To nám dává 9 různých „druhů“ prvků z G. Z Burnsideova lemmatu pak dostáváme počet orbit jako

$$6 \cdot 6 \cdot 2^1 + 6 \cdot 2 \cdot 2^3 + 6 \cdot 2 \cdot 2^3 + 6 \cdot 2^9 + 6 \cdot 2^9 + 2 \cdot 2 \cdot 2^9 + 2 \cdot 2^{27} + 2 \cdot 2^{27} + 2^{81},$$

což můžeme upravit do přehlednějšího tvaru

$$2^3 + 2^8 + 2^{13} + 2^{29} + 2^{81}.$$

7. Čtyřstěn má šest hran, nejprve je třeba určit vhodnou podgrupu S_6. Podobně jako minule, symetrie čtyřstěnu jsou určeny permutacemi jeho čtyř vrcholů. Některé z nich ale převracejí jeho orientaci (podobně jako osové symetrie převracejí orientaci trojúhelníků v rovině). Dva nepřímo shodné (obarvené) čtyřstěny v prostoru ale pro nás stejné být nemusí, takové permutace nás proto nezajímají. Jednou nepřímou symetrií je reflexe podle roviny určené dvěma vrcholy a středem protější strany, ta odpovídá transpozici v S_4. Takové transpozice přitom generují celou S_4, snadno tedy vidíme, že přípustné permutace vrcholů tvoří dvanáctiprvkovou grupu A_4. My ale opět musíme najít, jaké grupě permutací hran $G \leq S_6$ tyto permutace vrcholů odpovídají.

Po chvilce rozmýšlení dostáváme polyanom

$$P_G(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{12}\left(x_1^6 + 8x_3^2 + 3x_1^2x_2^2\right).$$

Dosazením barevných polynomů $g_i = a^i + b^i$ a roznásobením dostáváme polynom

$$Q(a,b) = a^6 + a^5b + 2a^4b^2 + 4a^3b^3 + 2a^2b^4 + ab^5 + b^6.$$

Koeficienty tohoto polyanomu pak odpovídají počtům čtyřstěnů s příslušnými rozloženími barev – celkem je jich 12, tři hrany od každé barvy mají 4 různé čtyřstěny atd.

8. Stačí ověřit, že je $G' \times H'$ uzavřená na všechny grupové operace. Identita (e,e) zde leží; součin $(g_1', h_1')(g_2', h_2') = (g_1'g_2', h_1'h_2') \in G' \times H'$; $(g_1', h_1')^{-1} = ({g_1'}^{-1}, {h_1'}^{-1}) \in G' \times H'$.

9. Ukážeme to pro $\tilde{G}$ (pro druhý případ se důkaz provede analogicky). V minulém cvičení jsme si již rozmysleli, že se jedná o podgrupy. Nyní tedy ukážeme normalitu. Nechť (g,h) je libovolný prvek $G \times H$ a (g_0, e) libovolný prvek $\tilde{G}$. Pak $(g,h)(g_0,e)(g^{-1},h^{-1}) = (gg_0g^{-1}, heh^{-1}) = (gg_0g^{-1}, e) \in \tilde{G}$, takže skutečně $\tilde{G} \trianglelefteq G \times H$.

10. Zvolme $H = \mathbb{Q}_+^\times$, K podgrupu generovanou prvkem -1 (obsahující jen -1 a 1), která je zřejmě izomorfní se $\mathbb{Z}_2$. Chceme ukázat, že $H \times K \simeq \mathbb{Q}^\times$. Podle předchozí věty nám k tomu stačí, že $HK = \mathbb{Q}^\times, H \cap K = \{1\}, H \trianglelefteq \mathbb{Q}^\times, K \trianglelefteq \mathbb{Q}^\times$. Ale každé racionální číslo kromě nuly dostaneme jako součin kladného racionálního čísla s jedničkou nebo minus jedničkou; z čísel $1, -1$ je kladné jen 1; podgrupy jsou normální, jelikož je grupa $\mathbb{Q}^\times$ abelovská.

11. Vyřešíme pouze první část tvrzení. Stačí zvolit zobrazení, které prvku g přiřadí koset $(g,e)\tilde{H}$. O tomto zobrazení se jednoduše ukáže, že se jedná o izomorfismus.

12. Rozmyslete si, že grupa A_4 obsahuje kromě identity tři permutace, které prohazují dvě dvojice různých prvků, a osm trojcyklů fixujících zbylý prvek. Hledaná podgrupa by měla mít index dva, takže podle cvičení z předešlého dílu by měla být normální. Aspoň jeden trojcyklus musí obsahovat (jinak by měla maximálně 4 prvky) – označme ho (abc) a poslední číslo nechť je d. Musí tedy obsahovat i $(abc)^2 = (acb)$. Pokud konjugujeme tyto dva trojcykly postupně prvky A_4

$(ab)(cd), (ac)(bd), (ad)(bc)$, dostaneme, že všechny trojcykly musí ležet uvnitř naší podgrupy. Trojcyklů je ale osm, což je ve sporu s tím, že má podgrupa 6 prvků. Žádná podgrupa řádu 6 tedy existovat nemůže. (Pokud přijmeme v seriálu nedokázaný fakt, že jsou grupy A_n pro $n \geq 5$ jednoduché, tak dalšími příklady mohou být právě všechny takové A_n, protože neobsahují podgrupu řádu $\frac{|A_n|}{2} = \frac{n!}{4}$.)

13. Pokud $N_G(P) = G$, pak pro každé $g \in G$ platí $gPg^{-1} = P$, což je přesně definice normality. Na druhé straně, pokud pro každé $g \in G$ platí $gPg^{-1} = P$, pak každé $g \in G$ nechává P na místě – tedy patří do stabilizátoru P v akci konjugace.

14. Pro každý prvek g grupy $N_G(H)$ platí $gHg^{-1} = H$. Proto je H v $N_G(H)$ normální.

Návody k úlohám

1. Uvažme všechny možné kolotoče s n sedátky obarvenými m barvami. Dva takové kolotoče budeme považovat za stejné, jestliže se na sebe dají převést pouze otočením (nikoli zrcadlením). Různým kolotočům pak vzájemně jednoznačně odpovídají orbity akce α grupy $\mathbb{Z}_n$, která prvku $k \in \mathbb{Z}_n$ přiřazuje otočení o k pozic po směru hodinových ručiček. Otočení α_k o k pozic přitom fixuje přesně ty kolotoče, ve kterých se barvy sedátek opakují s periodou $\mathrm{NSD}(n,k)$. (Takové otočení totiž fixuje pouze kolotoče s periodou k, každá perioda ale musí dělit délku celého kolotoče n.) Otočení α_k tedy fixuje přesně $m^{\mathrm{NSD}(n,k)}$ nakreslení kolotočů, z Burnsideova lemmatu je proto počet různých kolotočů roven $\frac{1}{n}\sum_{i=1}^{n} m^{\mathrm{NSD}(n,i)}$. Počet různých kolotočů je určitě přirozené číslo, takže n zadanou sumu skutečně dělí.

2. Začneme slíbeným fíglem – dokážeme následující tvrzení: Je-li G konečná grupa a $H < G$, potom G není rovno sjednocení $\bigcup \{gHg^{-1} \mid g \in G\}$, tj. sjednocení všech množin gHg^{-1} přes všechna $g \in G$. Jinak řečeno, je-li H nějaká ostře menší podgrupa G, nelze určitě jejím konjugováním vyrobit všechny prvky G. Jak to dokážeme? Pomocí akcí.

Označme X množinu všech podgrup G, jež jsou konjugovány s H. Jejich počet označme k. Potom G působí konjugací na X a toto působení je tranzitivní. Stabilizátor H v této akci označme $N_G(H)$. Potom dle tvrzení z kapitoly o akcích platí $k = [G : N_G(H)] = \frac{|G|}{|N_G(H)|}$.

Přitom ale $N_G(H) \geq H$, neboť $hHh^{-1} = H$ pro každé $h \in H$. Z předešlého vztahu proto máme $k \leq \frac{|G|}{|H|}$, tedy $k|H| \leq |G|$.

Pokud by bylo $k = 1$, platí $N_G(H) = G$, takže se H při konjugování ani nehne[27] – a proto existují prvky G, které konjugováním H nedostaneme. Pokud je však $k \geq 2$, máme $\left|\bigcup \{gHg^{-1} \mid g \in G\}\right| < k|H|$, neboť sice sjednocujeme přesně k množin velikosti $|H|$, každě dvě z nich ale obsahují ve svém průniku alespoň e, takže nerovnost je ostrá. Celkem potom máme $\left|\bigcup \{gHg^{-1} \mid g \in G\}\right| < k|H| = |G|$, sjednocení tedy nemohlo vytvořit celou G.

Vraťme se nyní k úloze a označme $H = \langle A \rangle$. Pro spor ať $H < G$. Dle předešlého potom konjugováním H nelze vyrobit celou G. Jenže každé $g \in G$ je konjugované s nějakým $a_i \in A$, takže konjugováním H skutečně vznikne celá G. To je spor, takže $H = G$ a jsme hotovi.

[27] Což mimochodem znamená, že v takovém případě je H normální.

Milý příteli,

jsme rádi, že jsi otevřel(a) i poslední díl seriálu. Některé kapitolky sice opět nejsou nejlehčí, ale pokud jsi prošel (prošla) první dva díly, tak už by pro Tebe ten třetí měl být příjemným zážitkem. Oproti předchozím dílům však teď budeme mnohem víc pracovat s grafy, a to hlavně s těmi orientovanými. Pokud ses s nějakými grafy už někdy setkal(a), neměl by to být žádný problém. Pokud ne, nevadí – orientovaný graf jsou prostě jenom tečky a šipky mezi nimi. Pro rychlé seznámení s grafy případně doporučujeme třeba začátek PraSečího seriálu *Letem grafovým světem*.

A na co se tentokrát můžeš těšit? Kromě teoretických částí týkajících se abelovských grup a nově definovaných volných grup například i na způsoby, jak se opravdu (ne)vyplatí věšet obraz na zeď.

Příjemné chvilky při čtení přejí
Filip Bialas a Kuba Löwit

Teorie grup III – Svoboda pro grupy

All of mathematics is a tale about groups.

Henri Poincaré

Prolog III

Ve dvacátém století už teorie grup odpovídá na otázky napříč matematikou. Grupy se důkladně proplétají algebrou, geometrií, kombinatorikou i analýzou. Rychle se rozvíjejí další oblasti algebry, přičemž jedna z nejslavnějších matematiček Emmy Noetherová formuluje obecněji například věty o izomorfismu.

Je tu ale jedna poměrně palčivá otázka. Jaké všechny grupy vlastně existují (až na izomorfismus)? Jenže to je složité, protože nekonečné neabelovské grupy mohou být nesmírně pestré a komplikované. S nekonečny to ale bývalo složité vždycky, držme se tedy při zemi. Bylo by alespoň užitečné vědět, jak mohou vypadat všechny konečné grupy. Částečnou odpovědí by ale aspoň bylo určit všechny konečné grupy bez netriviálních normálních podgrup – konečné jednoduché grupy.

Po položení této „nevinné“ otázky následuje přes půl století práce a více než patnáct tisíc stran článků od více než sta lidí. Výsledkem je úplná *klasifikace všech konečných jednoduchých grup*, která obsahuje nekonečný počet grup několika typů a na závěr hromádku dvaceti šesti obrovských, divných a (alespoň ve světle toho, co je zatím známé) úplně náhodných grup v čele s takzvanou *Monster simple group*. Důkazu správnosti této klasifikace ale dnes do všech detailů na světě nikdo nerozumí.[1] V teorii grup stále existují neznámé věci. Určitě tedy nejsme na konci...

Abelovské grupy

Začněme starým vtipem.

„What is commutative and purple?“ „An abelian grape.“

V této části se budeme zabývat abelovskými grupami. Je konvencí používat při studiu čistě abelovských grup aditivní notaci a i my se jí budeme dále držet – grupa bude mít jednu binární operaci $+$, inverzní prvek k a je $-a$, neutrální prvek je 0. Několikanásobné sečtení budeme značit intuitivně $n \cdot a$, kde n je celé číslo a a je prvek grupy (záporné n znamená, že sčítáme prvky $-a$). Navíc značení kosetů je teď smysluplné ve tvaru $g + H$ místo gH a budeme ho takto používat. Připomeňme ještě, že když je grupa abelovská, tak je každá její podgrupa normální.

Naším cílem bude abelovské grupy klasifikovat – přesně popsat, jak všechny vypadají. Avšak abelovské grupy mohou být nekonečné a v matematice se nekonečné objekty často chovají dost jinak nebo složitěji, takže s takto obecným problémem si neporadíme. Na druhé straně, starat se pouze o konečné grupy by byla škoda – například bychom nemohli mluvit ani o celých číslech. Uděláme tedy takový kompromis a budeme se zajímat pouze o konečně generované abelovské grupy. (Tento předpoklad je pro další tvrzení nutný – neděláme ho jen proto, abychom si trochu zjednodušili práci.)

Definice. Grupa je *konečně generovaná*, pokud má nějakou konečnou množinu generátorů.

[1] A kvůli jeho délce se najdou dokonce tací, kteří mu nevěří.

Připomeňme si, že grupa má nějakou množinu generátorů, pokud každý prvek této grupy můžeme zapsat jako konečný součin (nebo teď v případě abelovských součet) generátorů nebo jejich inverzů. Toto je ekvivalentní podmínce, že každá podgrupa obsahující všechny generátory už musí být celá původní grupa.

Cvičení 1. Nechť G je abelovská grupa a X její podmnožina splňující $G = \langle X \rangle$. Potom každý prvek $g \in G$ můžeme zapsat ve tvaru $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$, kde a_i jsou celá čísla a x_i po dvou různé prvky X.[2]

Cvičení 2. Pro každé přirozené číslo n je $\mathbb{Z}^n$ konečně generovaná.

Cvičení 3. Abelovská grupa racionálních čísel se sčítáním $\mathbb{Q}$ není konečně generovaná.

Tvrzení. *Abelovská grupa G je konečně generovaná s maximálně n-prvkovou množinou generátorů právě tehdy, když je izomorfní $\mathbb{Z}^n/H$, kde H je některá podgrupa $\mathbb{Z}^n$.*

Důkaz. Grupa $\mathbb{Z}^n/H$ je generovaná maximálně n-prvkovou množinou kosetů

$$\{(1,0,\ldots,0)+H, (0,1,\ldots,0)+H, \ldots, (0,\ldots,0,1)+H\},$$

protože každý prvek grupy $\mathbb{Z}^n$ je generovaný množinou prvků s jedničkami v jedné souřadnici a nulami ve zbytku. Druhá implikace je jen o trošičku těžší:

Generátory označme postupně $x_1, \ldots, x_n$. Uvažujme zobrazení $\varphi : \mathbb{Z}^n \to G$ definované vztahem $\varphi((a_1, a_2, \ldots, a_n)) = a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$. Lehce se dá ověřit, že je toto zobrazení homomorfismem (ale využíváme přitom komutativitu sčítací operace).

Protože $x_1, \ldots, x_n$ jsou generátory, lze každé $g \in G$ vyjádřit ve tvaru $a_1 \cdot x_1 + \cdots + a_n \cdot x_n$; proto $\operatorname{Im}\varphi = G$. Jádro φ označme H. Podle první věty o izomorfismu máme $\mathbb{Z}^n/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$, což můžeme přepsat jako $\mathbb{Z}^n/H \simeq G$, a to jsme chtěli přesně dokázat.

Právě dokázané tvrzení nám říká, že každá konečně generovaná abelovská grupa je faktorgrupou $\mathbb{Z}^n$. Tuto skutečnost budeme potřebovat k důkazu následující věty:

Věta. (Klasifikace konečně generovaných abelovských grup) *Každá konečně generovaná abelovská grupa je izomorfní direktnímu součinu konečně mnoha cyklických grup.*

Tato věta říká, že struktura konečně generovaných abelovských grup je vlastně hrozně jednoduchá. Jedná se o direktní součin cyklických grup, takže každý prvek lze popsat pomocí n-tice prvků ležících v těchto cyklických grupách. Každá konečná cyklická grupa je navíc izomorfní $\mathbb{Z}_n$ pro nějaké n a každá nekonečná je izomorfní $\mathbb{Z}$. Triviální abelovskou grupu $\{e\}$ můžeme v jistém smyslu vnímat jako součin nulového počtu cyklických grup, ale to je stejně tak nanicovatý případ, že se v důkaze jistě stačí omezit na grupy obsahující alespoň dva prvky.

Hledaný direktní součin samozřejmě nebude jednoznačný. Už v minulém díle jsme si v kapitole Čínská zbytková věta ukazovali, že pro nesoudělná p, q platí $\mathbb{Z}_{pq} \simeq \mathbb{Z}_p \times \mathbb{Z}_q$. Díky tomuto tvrzení bychom po důkazu zmiňované věty mohli tvrdit i to, že každá konečně generovaná abelovská grupa je izomorfní direktnímu součinu konečně mnoha cyklických grup, z nichž každá má řád buď nekonečný, nebo rovný mocnině nějakého prvočísla. (Každou, která nemá řád mocniny prvočísla, můžeme totiž izomorfně rozdělit na direktní součin těch, které takový řád mají.)

Důkaz. Jak jsme již ukázali, každá konečně generovaná abelovská grupa je izomorfní $\mathbb{Z}^n/H$, kde $H \leq \mathbb{Z}^n$, pro nějaké přirozené n. Stačí nám tedy dokázat, že pro $H \trianglelefteq \mathbb{Z}^n$ je $\mathbb{Z}^n/H$ izomorfní direktnímu součinu konečně mnoha cyklických grup. Důkaz provedeme indukcí podle tohoto n.

Pro $n = 1$ si stačí uvědomit, jak vypadají všechny podgrupy grupy $\mathbb{Z}$. Pokud bude $H = \{0\}$, tak $\mathbb{Z}/H \simeq \mathbb{Z}$ je cyklická (a tedy direktní součin jedné cyklické grupy). Uvažujme tudíž případ, kdy H není triviální. Z nenulových celých čísel z H vyberme to, jehož absolutní hodnota je nejmenší. Označme toto číslo a. Pak jistě i $-a \in H$, takže také $|a| \in H$. Protože se jedná o grupu, musí navíc

[2] Ovšem pozor, je-li X nekonečná, nejsou prvky $x_1, \ldots, x_n$ určeny pevně, nýbrž závisejí na tom, který prvek g právě vyjadřujeme.

do H patřit i každé $k \cdot a$ pro $k \in \mathbb{Z}$. Předpokládejme pro spor, že se v H nachází i nějaké další číslo b. Pak zbytek čísla b po vydělení $|a|$ je roven přirozenému číslu většímu než nula a menšímu než $|a|$. Toto číslo navíc dokážeme zapsat jako $b - k \cdot |a|$ pro nějaké $k \in \mathbb{Z}$, takže patří do H. To je ale ve sporu s minimalitou $|a|$. Proto $H = \{k \cdot a \mid k \in \mathbb{Z}\}$. Tím pádem přímo z definice plyne $\mathbb{Z}/H \simeq \mathbb{Z}_{|a|}$, což je cyklická grupa.

Případ pro $n = 1$ jsme vlastně ani nemuseli řešit zvlášť, jak bude vidno z indukčního kroku. Nicméně to byl jednoduchý příklad principu, který budeme používat dále. V minulém odstavci jsme ukázali, že podgrupa H je generována jen jedním prvkem a, a to pomocí snahy minimalizovat jeho velikost. V obecném případě uděláme něco podobného, jen budeme o nalezení takového „áčka“ usilovat jen v jedné souřadnici.

Mějme nyní konečně generovanou abelovskou grupu G, která je izomorfní $\mathbb{Z}^n/H$, kde n je nějaké pevné přirozené číslo větší než jedna. Pokud je podgrupa $H = \{e\}$, tak máme $\mathbb{Z}^n/H \simeq \mathbb{Z}^n$. Vyšetřovaná grupa je tedy direktním součinem n cyklických grup.

V opačném případě má grupa H alespoň jeden nenulový prvek. Každý prvek $h \in H$ můžeme psát jako $h = (h_1, \ldots, h_n)$. Pro $H \leq \mathbb{Z}^n$ označme symbolem $m(H)$ minimální nenulovou absolutní hodnotu h_i, která se vyskytuje v některém prvku $h \in H$ (tj. „nejmenší kladné číslo, které se kdekoli v celé grupě H vyskytuje“). Z těch H, pro něž $G \simeq \mathbb{Z}^n/H$, vyberme takovou H, aby výraz $m(H)$ byl nejmenší možný. Z této pevné grupy H nyní vezmeme prvek a, v němž pro některé i platí $a_i = m(H)$. Bez újmy na obecnosti můžeme popřeházet souřadnice, takže dále předpokládejme, že $i = 1$.

Nyní pro všechna $h \in H$ musí nutně platit $a_1 \mid h_1$, neboť jinak bychom mohli obdobně jako v případě $n = 1$ vydělit tato dvě čísla se zbytkem a dostat prvek grupy H, který bude mít první souřadnici nenulovou a v absolutní hodnotě menší než a_1.

Podobně ukážeme, že můžeme zvolit generující množinu X grupy H takovou, že $a \in X$ a pro všechna ostatní $x \in X$ platí $x_1 = 0$. Pro každé $h \in H$ různé od a dejme do X prvek $h' = h - \frac{h_1}{a_1} \cdot a$. Když do X nakonec přihodíme i a, dostáváme (obrovskou) generující množinu, protože každý prvek $h \in H$ jde nagenerovat jako součet h' a konečně mnoha a nebo $-a$.

Nyní provedeme opravdový trik. Naším cílem bude nějakým způsobem zařídit, aby se a rovnalo $(a_1, 0, \ldots, 0)$. Nejdříve sporem ukážeme, že naše volba H zajišťuje, aby $a_1 \mid a_i$ pro všechna $2 \leq i \leq n$. Pokud by tomu tak pro nějaké i nebylo, mohli bychom dělit se zbytkem a psát $a_i = qa_1 + r$. Jak nyní dojdeme ke sporu? Vezmeme jinou množinu generátorů! Uvažme zobrazení φ, které jde ze $\mathbb{Z}^n$ do $\mathbb{Z}^n$ a prvku $(g_1, \ldots, g_{i-1}, g_i, g_{i+1}, \ldots, g_n)$ přiřadí $(g_1, \ldots, g_{i-1}, g_i - qg_1, g_{i+1}, \ldots, g_n)$. Ukážeme, že je φ automorfismus. To, že se jedná o homomorfismus, by se ověřilo úplně snadno. Navíc snadno zjistíme, že $\chi : \mathbb{Z}^n \to \mathbb{Z}^n$, které prvku $(g_1, \ldots, g_{i-1}, g_i, g_{i+1}, \ldots, g_n)$ přiřadí $(g_1, \ldots, g_{i-1}, g_i + qg_1, g_{i+1}, \ldots, g_n)$, je k zobrazení φ inverzní, takže φ musí být prosté i na. Ukázali jsme, že je φ opravdu automorfismus $\mathbb{Z}^n$.

Navíc φ zobrazí generující množinu X na množinu X', ve které se vyskytuje prvek $(a_1, \ldots, a_{i-1}, r, a_{i+1}, \ldots, a_n)$. Zřejmě také $\varphi(\langle X \rangle) = \langle X' \rangle$, a tedy i $\mathbb{Z}^n/H = \mathbb{Z}^n/\langle X \rangle \simeq \varphi(\mathbb{Z}^n)/\varphi(\langle X \rangle) = \mathbb{Z}^n/\langle X' \rangle$. Oboje platí díky tomu, že automorfismus úplně zachovává strukturu grup. Ale tímto se dostáváme do sporu s volbou grupy H jako takovou, protože $a_1 = m(H)$ mělo být nejmenší možné, jenže $r \geq m(\langle X' \rangle)$ je ještě menší.

Podobně jako při důkazu existence X, v níž je první složka nenulová pouze u prvku a, nyní ukážeme, že můžeme předpokládat, že máme X, v níž je a navíc nulový ve všech ostatních složkách. Už víme, že můžeme brát X tak, aby v prvku a platilo $a_1 \mid a_i$ pro všechna $2 \leq i \leq n$. Uvažme nyní zobrazení ψ, které prvku $(g_1, g_2, \ldots, g_n) \in \mathbb{Z}^n$ přiřadí prvek $(g_1, g_2 - \frac{a_2}{a_1} \cdot a_1, \ldots, g_n - \frac{a_n}{a_1} \cdot a_1)$. Důkaz, že je ψ automorfismus $\mathbb{Z}^n$, je obdobný jako u φ. Navíc zobrazí prvek a na $(a_1, 0, \ldots, 0)$ a ostatní prvky z X na prvky, které mají první složku pořád nulovou. Existuje tedy grupa $\tilde{H} = \langle \tilde{X} \rangle$, pro niž $\mathbb{Z}^n/H \simeq \mathbb{Z}^n/\tilde{H}$ a jejíž množina generátorů je ve tvaru $\tilde{X} = \{(a_1, 0, \ldots, 0)\} \cup Y$, kde Y obsahuje pouze prvky, které mají nulovou první složku. Ve zbytku důkazu budeme bez újmy na obecnosti předpokládat, že jsme tuto šikovnou grupu H zvolili již na začátku, takže už nebudeme

psát vlnky nad H a X.[3]

Již jsme skoro u konce. Ukážeme, že $\mathbb{Z}^n/\langle X\rangle \simeq \mathbb{Z}/\langle a_1\rangle \times \mathbb{Z}^{n-1}/\langle Y'\rangle$, kde Y' je množina, která obsahuje prvky z Y bez první složky. Chceme tedy $\mathbb{Z}^n/H \simeq \mathbb{Z}_{|a_1|} \times \mathbb{Z}^{n-1}/\langle Y'\rangle$, přičemž poslední grupa je z indukčního předpokladu direktním součinem cyklických grup a budeme ji nadále značit A. K důkazu tohoto izomorfismu nám stačí uvážit zobrazení $\Phi : \mathbb{Z}^n \to \mathbb{Z}_{|a_1|} \times A$, které prvku $(g_1, \ldots, g_n)$ přiřadí prvek $(g_1 + \langle a_1\rangle, (g_2, \ldots, g_n) + \langle Y'\rangle)$.

To, že je Φ homomorfismus, by se zase ověřilo snadno. Navíc je na, protože na prvek $(g_1 + \langle a_1\rangle, (g_2, \ldots, g_n) + \langle Y'\rangle)$ se zobrazí $(g_1, g_2, \ldots, g_n)$. Stačí nám již jen ukázat, že $\operatorname{Ker}\Phi = H$. Prvky $g = (g_1, \ldots, g_n) \in \mathbb{Z}^n$, které se zobrazí na nulu, musejí mít v první složce násobek a_1 a ve zbytku složek nějaký konečný součet prvků z Y nebo jejich inverzů. Ale pak musí být $g \in H$, neboť $H = \langle X\rangle = \langle\{(a_1, 0, \ldots, 0)\} \cup Y\rangle$. A naopak je také jasné, že se všechny prvky z H zobrazí na nulu. Tím pádem je skutečně $\operatorname{Ker}\Phi = H$ a z první věty o izomorfismu dostáváme kýžený izomorfismus $\mathbb{Z}^n/H \simeq \mathbb{Z}_{|a_1|} \times A$, čímž jsme s důkazem hotovi.

Důkaz byl trochu delší, ale výsledek je skvělý. Neumíme sice klasifikovat úplně všechny abelovské grupy, ale třeba ty konečné máme zvládnuté dokonale. Pokud chceme znát všechny abelovské grupy nějakého pevného řádu, tak nám stačí podívat se na prvočíselný rozklad tohoto řádu a vyzkoušet několik možností.

Cayleygrafy

V předchozích částech seriálu nás už grupy mnohokrát přesvědčily o tom, že jsou symetriemi rozličných objektů. Představme si proto ještě jeden druh objektu, jehož symetrie jsou překvapivě bohaté. Přesněji, budeme se zabývat některými orientovanými grafy. Pojďme se tedy domluvit na několika pojmech.

Úmluva. *Orientovaným grafem* $Q = (V, E)$ myslíme množinu *vrcholů* V společně s množinou orientovaných hran E, jimž někdy budeme říkat *šipky*[4]. Je-li C množina barev, *barevným orientovaným grafem* nazveme orientovaný graf Q, jehož každá hrana má právě jednu barvu z C.

Po celou dobu přitom povolujeme i nekonečné grafy, práce s nimi však v rámci seriálu nebude skrývat žádné velké nástrahy.

Nyní si definujme takzvané *Cayleyho grafy*, zkráceně *cayleygrafy*.

Definice. Ať G je grupa a C nějaká množina jejích generátorů. *Cayleygrafem grupy* G vzhledem k C nazveme orientovaný barevný graf Q, jehož vrcholy odpovídají prvkům G a z vrcholu u vede do vrcholu v hrana barvy c právě tehdy, když $v = cu$.

Ano, na prvky množiny C se díváme zároveň jako na generátory grupy G i jako na barvy, a vůbec nám to nevadí – právě naopak. Přechod po šipce barvy c v grafu odpovídá násobení generátorem c.

Definice. Ať C je nějaká množina barev. *Zajímavým* grafem nazveme jakýkoli barevný orientovaný graf $G = (V, E)$, který splňuje následující tři axiomy:

(1) mezi každými dvěma vrcholy grafu G vede (ne nutně orientovaná) cesta (*souvislost*),
(2) do každého vrcholu i ven z něho vede právě jedna hrana od každé barvy (*regularita*),
(3) pro každé dva vrcholy $u, v \in V$ existuje nějaká permutace vrcholů, která zobrazuje $u \mapsto v$ a přitom zachovává barevné šipky (*homogenita*).

[3] Komu tento přístup vadí, může si buď vlnky všude doplnit, nebo si představovat, že jsme na začátku jednak požadovali, aby bylo co nejmenší $m(H)$, jednak to, aby v prvku a byl co nejmenší součet absolutních hodnot v ostatních souřadnicích.

[4] Povolujeme i násobné hrany a hrany se stejným začátkem a koncem. Druhé uvedené se běžně nazývají „smyčky“, my však tento výraz máme rezervovaný pro něco jiného – budeme je proto označovat jako *očka*. Předem však prozradíme, že pro nás v této pasáži nijak zajímavé nebudou a klidně bychom je mohli i zakázat.

Ještě by se slušelo trochu osvětlit třetí z podmínek. Říkáme, že permutace $\sigma \in S_V$ *zachovává barevné šipky*, jestliže z vrcholu x vede hrana barvy c do vrcholu y právě tehdy, když z vrcholu $\sigma(x)$ vede hrana barvy c do vrcholu $\sigma(y)$. Homogenita vyjadřuje, že pokud nás někdo postaví do libovolného vrcholu u grafu G, chozením barevnými cestičkami nemáme šanci určit, do kterého vrcholu jsme byli postaveni.

Proč by nás ale měly zrovna zajímavé grafy zajímat?

Tvrzení. *Každý cayleygraf je zajímavý, každý zajímavý graf je cayleygrafem nějaké grupy.*

Důkaz. Nejprve ukažme, že každý cayleygraf je zajímavý. Ať tedy Q je cayleygraf grupy G. Pokud se podíváme na vrchol odpovídající prvku $e \in G$, můžeme z něj postupným násobením zprava prvky z generující množiny C a jejich inverzy získat libovolný prvek $g \in G$. Proto z vrcholu e vede cesta do vrcholu g; nalezneme ji tak, že budeme postupně zprava číst součin odpovídající prvku g, za generátor c se posuneme ve směru hrany c, za jeho inverz v protisměru. Každé dva vrcholy Q jsou proto spojeny přes vrchol e, tedy Q je souvislý.

Podívejme se na to, jak na sobě G působí levou translací; toto působení označme α. Speciálně sledujme α_c pro nějaké $c \in C$. Šipky barvy c v cayleygrafu Q přesně odpovídají permutaci α_c. Protože je α_c bijekce, je Q regulární. Elementárněji řečeno, z daného vrcholu u vede právě jedna šipka barvy c, a to do vrcholu cu; do daného vrcholu u vede právě jedna šipka barvy c, a to z vrcholu $c^{-1}u$, .

Konečně, ať u, v jsou nějaké vrcholy Q. Vezměme si permutaci vrcholů, která je daná násobením prvkem $u^{-1}v$ zprava (tj. jedná se o působení **pravou** translací). Ta posílá $u \mapsto uu^{-1}v = v$. Navíc tato permutace zachovává barevné šipky: v cayleygrafu Q vede z vrcholu g do vrcholu h šipka barvy c právě tehdy, když $h = cg$, což po vynásobení prvkem vu^{-1} zprava dává ekvivalentní rovnost $hvu^{-1} = cgvu^{-1}$. Z vrcholu gvu^{-1} tedy vede hrana barvy c do vrcholu hvu^{-1}, čímž jsme ověřili homogenitu.

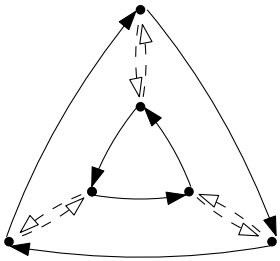
Nyní ukážeme druhý směr tvrzení: k libovolnému zajímavému grafu Q vyrobíme grupu G tak, aby Q byl její cayleygraf. Za grupu G vezměme jednoduše grupu všech symetrií grafu Q – tedy grupu všech permutací jeho vrcholů, které zachovávají směry i barvy šipek. Jak tato G vypadá? Zvolme libovolný vrchol grafu Q a označme jej e. Každá symetrie grafu Q posílá e na nějaký vrchol Q. Díky homogenitě však pro každý vrchol v skutečně existuje symetrie převádějící $e \mapsto v$.

Souvislost a regularita Q však zaručují, že taková symetrie existuje nejvýše jedna: Do libovolného vrcholu w se dá dojít po hranách z vrcholu e. Protože však naše symetrie zachovává barvy i orientace hran, do obrazu v musíme z vrcholu v dojít jednoznačně určenou cestou po stejných barvičkách. Tím jsme spárovali vrcholy Q s jednotlivými symetriemi z G. Symetrie odpovídající posunutí e do vedlejšího vrcholu ve směru nějaké šipky jsou přesně naznačeny šipkami odpovídající barvy. Vezmeme-li tedy těchto $|C|$ symetrií za generátory G, zkonstruováním příslušného cayleygrafu dostaneme nazpátek graf Q. To je vše.

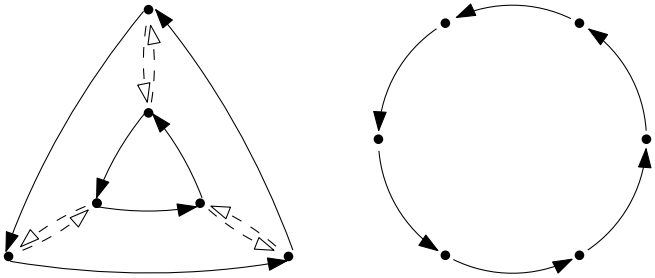
Pojem zajímavého grafu jsme zavedli jen proto, aby bylo v předchozí diskuzi jasně rozlišeno, kdy konstruujeme grupu z grafu a kdy naopak graf z grupy. Protože jsme ale právě nahlédli, že třída zajímavých grafů přesně odpovídá třídě cayleygrafů všech možných grup, budeme dále místo pojmu zajímavý graf používat pojem cayleygraf.

Zdůrazněme jednu skvělou věc, kterou jsme mimoděk dokázali. Povedlo se nám totiž ukázat, že libovolná grupa G je izomorfní grupě symetrií svého cayleygrafu. Takový cayleygraf tedy dokonale vystihuje svou grupu. Získáváme tak nový způsob, jak si grupy představovat. Jednu grupu tak můžeme znázornit mnoha velmi rozdílnými grafy – stačí volit různé množiny jejích generátorů. Tyto grafy sice musejí mít vždy stejný počet vrcholů (který odpovídá řádu grupy), šipky v nich ale mohou vypadat velmi odlišně.

Příklad. Grupa $D_6 \simeq S_3$ s množinou generátorů tvořenou minimální rotací r a translací σ má následující cayleygraf se šesti vrcholy:



Příklad. Abelovská grupa $\mathbb{Z}_6$ má také šest prvků. První z následujících cayleygrafů odpovídá jednoprvkové množině generátorů obsahující pouze číslo 1. Druhý odpovídá volbě dvojice generátorů 2, 3.



V cayleygrafech je na první pohled vidět mnoho algebraických vlastností příslušné grupy. Třeba abelovskost grupy G je ekvivalentní následující podmínce: Kdykoli vezmeme dvě barvy c, d a libovolný vrchol v, cesty z v po barvách cd a dc skončí ve stejném vrcholu. K abelovskosti G totiž zřejmě stačí, aby spolu komutovaly všechny generátory grupy G.

Mějme například grupy $H \leq G$ a vhodně zvolené množiny jejich generátorů po řadě C', C takové, aby $C' \subseteq C$. Vezměme si příslušný cayleygraf grupy G. Pokud z něj smažeme všechny hrany s barvami z $C \setminus C'$, rozpadne se na nějaké menší grafy. Nějaký vrchol grafu Q přitom reprezentoval identitu $e \in G$. Komponenta obsahující tento vrchol vzniklá smazáním hran s barvami z $C \setminus C'$ je pak zřejmě cayleygrafem grupy H. Jenže díky homogenitě grafu Q mohlo být e libovolným vrcholem Q. Graf se tedy rozpadl na menší cayleygrafy odpovídající kopím cayleygrafu grupy H, které přesně odpovídají pravým kosetům podgrupy H v G.

Podobně je velmi snadné poznat, kdy je $H \trianglelefteq G$. To nastává právě tehdy, když pravé a levé kosety H v G splývají. Není těžké si rozmyslet, že to přesně odpovídá případu, kdy akce G levou translací na sobě samé permutuje pravé kosety podgrupy H, což stačí ověřit pro generátory G. A to se stane přesně tehdy, když všechny šipky každé barvy z $C \setminus C'$ vedou z každého cayleygrafu grupy H do právě jednoho jiného. Když se pak podíváme na kopie cayleygrafu grupy H jako na vrcholy a necháme v grafu šipky s barvami z $C \setminus C'$, dostaneme cayleygraf faktorgrupy G/H.

Právě uvedené „obrázkové“ vlastnosti grup si můžete hezky rozmyslet na dvou cayleygrafech znázorněných výše. Při vhodné volbě generátorů je vidět, že se liší pouze vzájemnou orientací trojcyklů. Pro jejich vlastnosti to však má velké důsledky: $\mathbb{Z}_6$ je abelovská, zatímco S_3 ani omylem, $\mathbb{Z}_6$ má normální podgrupy řádu 3 i 2, zatímco S_3 má jedinou normální podgrupu řádu 3 atd.

Jak vyrobit... volné grupy!

Když jsme se v předešlých dílech seriálu zabývali nějakou konkrétní grupou, typicky v ní platilo hodně „bonusových rovností“ mezi prvky, které abstraktní definice grupy nijak nevynucuje. (Například spolu některé prvky mohly komutovat, některý prvek mohl splňovat $g^3 = e$, pro trojici generátorů g_1, g_2, g_3 mohlo platit $g_1^7 g_2^{-3} g_3^{-1} g_2^2 = e$ apod.) Nyní se pokusíme o výrobu úplného

protikladu – zkonstruujeme grupy, ve kterých žádné vztahy „navíc“ neplatí. Tyto prototypy grup se nazývají *volné grupy*.

Předem vyslovíme drobné varování: s volnými grupami budeme pracovat poměrně formálně a opatrně. To se na první pohled může zdát až přehnané, některá tvrzení o volných grupách (jako třeba jejich samotná existence) se mohou zdát úplně zjevná. Čím víc toho ale o nich zjistíme, tím méně zjevná se nám budou zdát. Některá jiná zřejmá tvrzení o volných grupách ve skutečnosti ani neplatí – opatrnost je proto na místě.

Konstrukce. (krácením slov)

Mějme tedy neprázdnou (klidně i nekonečnou) množinu X, jejíž prvky budou jakási *písmena*. Tato písmena budou představovat generátory naší volné grupy F. Pokud má být F grupa, každý její prvek musí mít inverz. Vezměme si tedy novou množinu stejně velkou jako X, kterou příhodně označíme X^{-1}. Množina X^{-1} obsahuje pro každé písmeno $x \in X$ jednoznačně určené inverzní písmeno, které budeme příhodně značit x^{-1}. Žádné další prvky v X^{-1} neleží.

Nyní pomocí disjunktních X a X^{-1} vyrobíme množinu W, která sestává ze všech konečných řetězců symbolů z $X \cup X^{-1}$. Prvkům W budeme říkat *slova*. Speciálně W obsahuje i prázdné slovo, které budeme značit e.[5] Zdůrazněme, že na W zatím neexistují žádné grupové operace.

Naším snem je, aby W byla nosnou množinou grupy F. Jako binární operace se doslova nabízí takzvané *zřetězení* – psaní slov za sebe. Zřetězení je na množině W určitě asociativní, prázdné slovo e se navíc chová jako identita. Je tu ale malý zádrhel ohledně invertování – napsáním dvou slov za sebe nelze žádné z nich zkrátit. Chtěli bychom, aby slovo $abcc^{-1}b^{-1}a^{-1}$ bylo ve skutečnosti prázdné slovo, z pohledu množiny W jsou to ale dva různé prvky.

Jinými slovy, má-li přiřazení $x \mapsto x^{-1}$ odpovídat invertování prvků písmen z X, samy axiomy grupy už vynucují rovnosti některých slov. Například slova $abaa^{-1}$, ab, $b^{-1}bab$ musejí reprezentovat stejný prvek grupy F. Očividným řešením této těžkosti je takové prvky za stejné skutečně považovat. Formálněji, dva prvky $u, v \in W$ budeme považovat za stejné, pokud je na sebe lze převést postupným vepisováním resp. mazáním sousedících písmen xx^{-1} resp. $x^{-1}x$ pro libovolné $x \in X$. Na množině W' takových skupinek bychom pak rádi definovali grupové operace stejně jako původně, což už opravdu jde.

A proč že to jde? Skutečně totiž není jasné, jestli výsledek zřetězení náhodou nezávisí na volbě konkrétní slovní reprezentace. Stačilo by ukázat, že každý prvek W' lze reprezentovat jednoznačně určeným *zkráceným* slovem, tj. slovem, které neobsahuje žádnou sousedící dvojičku písmen tvaru xx^{-1} resp. $x^{-1}x$. To ponecháme jako hravé cvičení.

Cvičení 4. Dokažte, že každý prvek W' lze reprezentovat jednoznačně určeným zkráceným slovem.

Za nosnou množinu grupy F tudíž můžeme jednoduše vzít množinu všech takových zkrácených slov a binární operací pak bude zřetězení s případným promazáním sousedících dvojiček xx^{-1} resp. $x^{-1}x$. Prázdné slovo e je potom skutečně identitou, invertování prvků X přiřazením $x \mapsto x^{-1}$ lze roztáhnout na všechny prvky F pomocí předpisu $(ab)^{-1} = b^{-1}a^{-1}$. Asociativita teď úplně jasná není, důkladným rozborem několika možností by ji však nebyl problém dokázat.

Podle potřeby někdy budeme vnímat volnou grupu jako „grupu všech zkrácených slov“, jindy se na ni formálně budeme dívat jako na „grupu sestávající ze skupinek ekvivalentních slov“. Dle právě provedeného rozboru to ale vyjde nastejno.

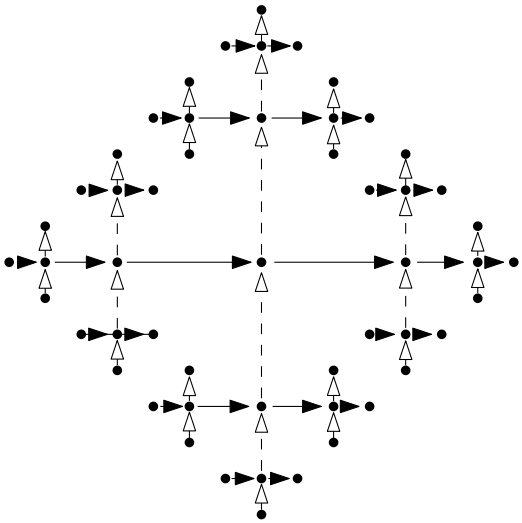
Přestože je volná grupa sama o sobě docela intuitivní objekt, její vyrábění skýtalo několik záludností.[6] Ještě než se posuneme dál, předvedeme si alternativní konstrukci volných grup, a to pomocí cayleygrafů. Tato konstrukce je méně přímočará, zato je však neuvěřitelně elegantní. Následujícímu postupu se někdy (podle jeho tvůrce) přezdívá *van der Waerdenův trik*.

Konstrukce. (van der Waerdenův trik)

[5] Nejlepší by bylo značit ji prázdný místem, to je ale typicky špatně vidět.

[6] Kombinatorický rozbor asociativity jsme z lenosti a hlavně pro úsporu místa ani neprovedli.

Opět začneme s množinou X. Sestrojíme nekonečný cayleygraf Q jako na obrázku: Bude to nekonečný strom[7], z každého jeho vrcholu bude vycházet po jedné šipce od každé barvy z množiny X. Do každého vrcholu také bude vcházet jedna šipka každé barvy. Přesněji, začneme jedním vrcholem, nakreslíme všech $2|X|$ jeho šipek, na konec každé dáme nový vrchol… a tak budeme pokračovat dál. Žádná nově vytvořená šipka nevede do už vytvořeného vrcholu – strom se neustále rozrůstá do dalších a dalších pater.



Je vcelku zřejmé, že Q je cayleygraf (největší rozmýšlení vyžaduje homogenita). Označme tedy F jeho grupu symetrií. Okamžitě víme, že F je skutečně dobře definovaná grupa a její binární operace je skládání symetrií grafu Q. Zvolme si libovolný vrchol e grafu Q. Každá symetrie Q jednoznačně odpovídá posunutí e do některého vrcholu v. V grafu Q jsou však každé dva vrcholy spojeny jednoznačně určenou posloupností hran. Každou symetrii $g \in F$ tedy můžeme ztotožnit s touto jednoznačně určenou posloupností hran z e do v, kterou lze popsat jednoznačně určeným slovem z písmen $X \cup X^{-1}$ (písmena odpovídají barvám na zmíněné posloupnosti hran, exponenty jejich směru). To je vše.[8]

Na závěr si ještě uvedeme několik příkladů volných grup. Obecně budeme volnou grupu na písmenech z množiny X značit jako F_X. Pro n-prvkovou množinu X budeme někdy příslušnou volnou grupu značit jako F_n.[9]

Příklad. Zvolme jednoprvkovou bázi X, její jediný prvek označme a. Jak pak vypadá odpovídající volná grupa F_1? Množina W všech konečných slov nad $X \cup X^{-1}$ obsahuje pouze konečné posloupnosti písmen a, a^{-1}. Nosná množina grupy F_1 pak odpovídá zkráceným slovům z W. Zkrácená slova ale nutně obsahují nejvýše jeden ze symbolů a, a^{-1}. Označíme-li napsání písmene a přesně k-krát za sebe jako a^k, napsání písmene a^{-1} přesně k-krát za sebe jako a^{-k} a prázdné slovo jako a^0, sestává nosná množina grupy F právě ze slov tvaru a^k pro $k \in \mathbb{Z}$. Okamžitě tedy vidíme,

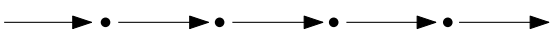
[7] *Stromem* myslíme graf, který neobsahuje žádnou – ani neorientovanou – kružnici.

[8] Nedůvěřivý čtenář si snadno může zkontrolovat, že jsme zkonstruovali tu stejnou grupu F jako původně.

[9] Pro stejně velké množiny generátorů nám výše uvedená konstrukce samozřejmě vyrobí izomorfní grupy. Volné grupy na stejně velkých množinách písmen tedy můžeme považovat v podstatě za stejné.

že volná grupa F na jednom generátoru je izomorfní nekonečné cyklické grupě $\mathbb{Z}$ (skrz izomorfismus $a^k \mapsto k$).

Cayleygraf této grupy představuje pouze nekonečná orientovaná cesta:



Jak už jsme nastínili dříve, pro bázi s velikostí alespoň dva je situace o poznání zajímavější.

Příklad. Vezměme dvouprvkovou bázi $X = \{a, b\}$ a uvažme příslušnou volnou grupu F_2. Na její nosnou množinu se můžeme dívat jako na množinu všech zkrácených slov nad písmeny a, b, a^{-1}, b^{-1}. Taková slova už ale na rozdíl od minulého příkladu nijak lépe popsat neumíme. Když budeme provádět jejich zřetězení, může docházet k dosti nepřehlednému krácení písmen. Zkoumání struktury F_2 už tedy může být poměrně zajímavé. Její cayleygraf je zvěčněn na obrázku uprostřed konstrukce volných grup.

Popis grupy F_2 zakončíme několika cvičeními, ze kterých by mělo být patrné, s jakou opatrností je potřeba k volným grupám přistupovat.

Cvičení 5. Grupa F_2 je zřejmě generována dvěma prvky. Zdůvodněte, že jeden generátor nestačí.

Naopak ale platí následující mírně překvapivé lumpárny.

Cvičení 6. Najděte vlastní podgrupu $H < F_2$ takovou, že $H \simeq F_2$.

Úloha 1. Najděte podgrupu $H \leq F_2$ takovou, že $H \simeq F_3$.

Úloha 2. Ukažte, že existuje podgrupa $K \leq F_2$, která je izomorfní F_X pro nějakou nekonečnou množinu X.

Důkazy předchozích dvou úloh bylo možné provést bez použití nějaké hlubší teorie. My se naštěstí v průběhu seriálu naučíme mnohem sofistikovanější finty, pomocí kterých budou tvrzení podobného rázu mnohem jasnější.

Grupa F_2 tedy obsahuje podgrupy, které jsou volné s bází velikosti n pro libovolné $n \in \mathbb{N}$, a dokonce i takové, jejichž báze svou velikostí odpovídá množině přirozených čísel. Jenže všechny tyto její podgrupy opět obsahují podgrupu izomorfní s F_2 ... legrační, ne?

Volné grupy zbavené pout

Když už jsme si dali tolik práce s výrobou volných grup, bylo by vhodné je chvíli obecně zkoumat. V předešlé části jsme je konstruovali velmi konkrétně (z dané množiny X jsme vyrobili příslušnou volnou grupu). Volné grupy však lze ekvivalentně definovat následujícím mnohem abstraktnějším způsobem.

Tvrzení. (univerzální vlastnost volných grup) *Grupa F je volná právě tehdy, když existuje podmnožina $X \subseteq F$ taková, že pro každou grupu H a každé zobrazení $f : X \to H$ existuje právě jeden homomorfismus $\varphi : F \to H$, který se na prvcích X shoduje s f. (Podmnožina X se pak nazývá volná báze).*

Důkaz. Nejprve dokážeme, že libovolná volná grupa zkonstruovaná v předešlé části splňuje podmínku z tvrzení. Ať tedy X je libovolná množina a F_X příslušná volná grupa; množinu všech slov nad $X \cup X^{-1}$ označme opět W. Nahlédneme, že X je volnou bází F_X. Je tedy třeba ověřit, že pro libovolné zobrazení $f : X \to H$ existuje právě jeden homomorfismus $\varphi : F_X \to H$, který rozšiřuje f. Protože $F = \langle X \rangle$, takový homomorfismus f může existovat nejvýše jeden. Každé slovo $w \in W$ je pouze konečnou posloupností písmen z $X \cup X^{-1}$. Má-li být φ homomorfismus, musí nutně posílat $x^{-1} \mapsto f(x)^{-1}$, označme proto f' zobrazení $X \cup X^{-1} \to H$, které tímto způsobem rozšiřuje f i na prvky X^{-1}. Dále musí být prvek $\varphi(w) \in H$ roven součinu obrazů jednotlivých písmen w v zobrazení f' (ve stejném pořadí).

Pokud tímto způsobem φ můžeme definovat na všech slovech z W, triviálně už to bude homomorfismus $F \to H$. Je tedy třeba ukázat, že různé slovní reprezentace stejného prvku grupy F toto φ opravdu pošle na stejný prvek v H. To je ale jasné – takové slovní reprezentace se liší pouze

konečnou posloupností připisování a mazání dvojiček xx^{-1} a $x^{-1}x$, které se ale tak jako tak po provedení zobrazení f' v grupě H pokrátí. Tím je první část důkazu u konce.

Nyní už jen vypozorujeme následující: Pro každou velikost[10] volné báze X existuje až na izomorfismus nejvýše jedna grupa s volnou bází této velikosti. Potom už budeme hotovi, neboť touto jednoznačně určenou grupou je dle první části důkazu právě F_X.

Mějme tedy dvě grupy G, H s volnými bázemi po řadě X, Y, mezi kterými existuje bijekce (tu označme f). Protože je X volná báze G, existuje homomorfismus $\varphi : G \to H$ rozšiřující f. Protože je Y volná báze H, existuje homomorfismus $\psi : H \to G$ rozšiřující f^{-1}. Jenže homomorfismus $\psi \circ \varphi : G \to G$ rozšiřuje identické zobrazení $f^{-1} \circ f$, tedy (opět díky vlastnostem volné báze) je $\psi \circ \varphi$ identické zobrazení na G. Obdobně je $\varphi \circ \psi$ identické zobrazení na H. Z prvního ze vztahů je ale φ prosté, díky druhému je φ na. Tím jsme našli izomorfismus grup G a H.

Z právě provedeného důkazu plyne, že množina X jednopísmenných slov z konstrukce volné grupy F_X je volnou bází této grupy. Nijak ale není zaručeno, že je to jediná taková množina. Trochu nás však může uklidnit alespoň následující tvrzení.

Tvrzení. *Ať F_X, F_Y jsou volné grupy s bázemi po řadě X, Y. Jsou-li X a Y různě velké, pak grupy F_X a F_Y nejsou izomorfní.*

Důkaz. Tvrzení budeme dokazovat jen pro konečně velké X, Y. Obecně funguje velmi podobný argument, my se však nekonečnům raději vyhneme. Uvažme podgrupu $K \leq F_X$, která obsahuje právě všechny prvky tvaru g^2 pro $g \in F_X$. Přitom $K \trianglelefteq F_X$, neboť pro libovolné $h \in F_X$ platí $hg^2h^{-1} = (hgh^{-1})^2$ (což platí zcela obecně v každé grupě). Faktorgrupa F_X/K je tedy dobře definovaná a každý její prvek má řád 2, je tedy dokonce abelovská[11].

Ukážeme, že F_X/K je izomorfní direktnímu součinu $|X|$ grup $\mathbb{Z}_2$. Na to dle minulého dílu stačí stačí nalézt $|X|$ jejích normálních podgrup, které ji generují a zároveň má každá z nich triviální průnik s grupou generovanou všemi ostatními. To je ale snadné, stačí vzít cyklické podgrupy generované jednotlivými kosety tvaru xK pro písmena $x \in X$. Všechny tři podmínky pak triviálně platí.

Díky tomu je nutně F_X/K izomorfní direktnímu součinu $\mathbb{Z}_2^{|X|}$, má tedy přesně $2^{|X|}$ prvků. Pro různé velikosti X je tedy F_X/K různě velká. Z čísla $2^{|X|}$ lze ale zpětně jednoznačně určit velikost $|X|$, takže volné grupy s různě velkými bázemi izomorfní být nemohou.

Jak už bylo řečeno dříve, pokud je $|X| = |Y|$, volné grupy F_X a F_Y izomorfní jsou (pouze se písmena v jejich bázích jmenují jinak). Různých volných grup tedy existuje přesně tolik, kolik je různě velkých množin – pro každou velikost jedna.

Podobně jako se každá grupa dá vnořit do vhodné symetrické grupy, každá grupa se dá vyfaktorizovat z šikovné volné grupy. Volné grupy jsou proto v jistém dalším smyslu prototypem grup:

Tvrzení. *Každá grupa je izomorfní faktorgrupě nějaké volné grupy.*

Důkaz. Vezměme si tedy libovolnou grupu G. Dále si vezměme (možná dost velikou) volnou grupu F s bází velikosti G. Ta má volnou bázi velikosti $|G|$, existuje tedy zobrazení f z této báze do grupy G, které je na. Díky univerzální vlastnosti volných grup pak existuje homomorfismus $\varphi : F \to G$ rozšiřující f. Zobrazení φ je tedy tím spíše na. Dle první věty o izomorfismu platí $F/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi = G$, což jsme chtěli.

V předchozím důkazu jsme na velikosti volné grupy ani v nejmenším nešetřili. Většinou nám přitom stačí mnohem menší volná grupa. Pokud bude obraz f obsahovat nějakou množinu generátorů grupy G, bude už nutně $\operatorname{Im}\varphi = G$. Pro libovolnou množinu generátorů X lze tedy grupu G vyfaktorizovat dokonce z volné grupy F_X.

[10] Dvě nekonečné množiny jsou stejně velké právě tehdy, když mezi nimi existuje bijekce – tak je pojem „velikosti“ definován.

[11] Jak by řešitelé první seriálové série měli vědět.

Tento abstraktní fakt vede k velmi praktickému způsobu vytváření a zaznamenávání grup – takzvaným prezentacím. Chceme-li zachytit nějakou grupu G, stačí ji vyfaktorizovat z nějaké volné grupy F pomocí vhodného homomorfismu φ a zapamatovat si velikost grupy F společně s její normální podgrupou $\operatorname{Ker}\varphi$. Není však nutné pamatovat si celou $\operatorname{Ker}\varphi$ – postačí zapamatovat si něco jako její „generátory“. Protože je $\operatorname{Ker}\varphi$ normální (a my líní), stačí si dokonce pamatovat jen množinu jejích prvků, z nichž lze vytvořit celou $\operatorname{Ker}\varphi$ pomocí grupových operací a **konjugování** prvky z F.

Definice. *Prezentace* grupy sestává z množiny *generátorů* X a množiny *relací* $R \subseteq F_X$. Tato dvojice pak definuje grupu $G = F_X/K$, kde K je nejmenší normální podgrupa F obsahující množinu R. To značíme jako $G = \langle X \mid R\rangle$.

Na relace se můžeme dívat i mnohem intuitivnějším způsobem. Na celou grupu G nahlížíme jako na slova nad abecedou $X \cup X^{-1}$. Některá různá slova ale zachycují stejný prvek G (tak tomu je dokonce i v případě, kdy je G volná). My bychom rádi poznali, která slova odpovídají stejným prvkům. Je-li grupa G definována jako $G = \langle X \mid R\rangle$, potom dvě slova odpovídají stejnému prvku G právě tehdy, když je na sebe lze převést konečnou posloupností vepisování a mazání dvojiček xx^{-1}, $x^{-1}x$ a **libovolné relace z** R. Relace jsou vzorová slovíčka, která při faktorizaci zmizí.

V tomto smyslu jsou volné grupy grupami „bez nadbytečných relací“ – jediné jejich relace jsou ty, které jsou vynuceny axiomy grup.

Z historických důvodů se relace často zapisují pomocí rovností. Například relace a^2b^{-1} se občas zapisuje jako rovnost $a^2 = b$, pomocí které lze „upravovat slova“ bez toho, abychom měnili prvek G, který pojmenovávají.

Příklad. Zkusíme nalézt nějakou prezentaci dihedrální grupy D_{2n}. Tu lze nagenerovat dvěma prvky – nejmenší rotací r (v libovolném směru) a nějakou reflexí σ. Určitě ji proto lze vyfaktorizovat z volné grupy F_2. Označme si $\{a, b\}$ volnou bázi F_2. Budeme chtít, aby slovo a odpovídalo rotaci r a slovo b odpovídalo reflexi σ. Vezměme si tedy zobrazení $f : \{a, b\} \to D_{2n}$, které posílá $a \mapsto r$, $b \mapsto \sigma$; to lze rozšířit na homomorfismus $\varphi : F_2 \to D_{2n}$.

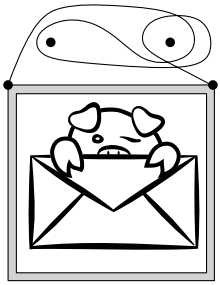
Zbývá nalézt jeho jádro v F_2. V grupě D_{2n} platí díky jejímu geometrickému významu identity $r^n = 1$, $\sigma^2 = 1$ a $\sigma r\sigma = r^{-1}$, takže prvky a^n, b^2, $(ba)^2$ leží v $\operatorname{Ker}\varphi$. Označíme-li K nejmenší normální podgrupu F, která obsahuje tyto tři prvky, máme tedy $K \subseteq \operatorname{Ker}\varphi$. Faktor F_2/K ale obsahuje nejvýše $2n$ prvků, neboť díky uvedeným třem relacím leží v každém jeho kosetu alespoň jeden prvek tvaru a^k či σa^k pro $k \in \{0, 1, \ldots, n-1\}$, a těch je dohromady jen $2n$. Nutně tedy $[G : K] \geq [G : \operatorname{Ker}\varphi]$, takže dokonce $K = \operatorname{Ker}\varphi$. Celkem je proto $\langle a, b \mid a^n, b^2, (ba)^2\rangle$ skutečně prezentací grupy D_{2n}.

Prezentace grup je velmi silný prostředek. Opravdu efektivně popisuje známé grupy, a navíc dává návod, jak lze libovolnou grupu vyrobit – stačí si vybrat nějakou volnou grupu a množinu našich oblíbených relací. Nevýhodou prezentací je, že z nich může být velmi těžké určit některé vlastnosti vyrobené grupy, jako je třeba už jenom její velikost. I když bude generátorů i relací pouze konečně mnoho, nelze ani algoritmicky rozhodnout, zda zadané slovo reprezentuje identitu.

Jak nevěšet obraz na zeď

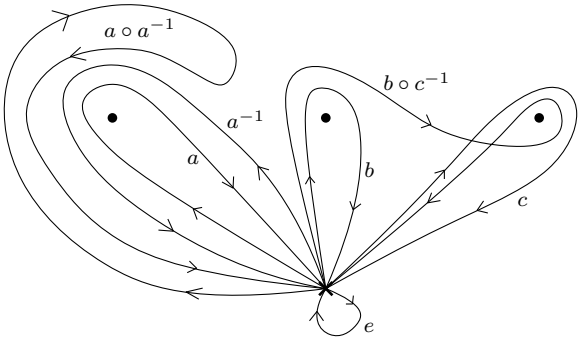
Pojďme si pro změnu hrát s úlohou, která s grupami na první pohled vůbec nesouvisí. Chcete-li se nad ní na chvíli zamyslet sami, vřele to doporučujeme – posléze bude řešení vyzrazeno.

Úloha. (Obraz na zdi) Ve zdi jsou zatlučeny dva hřebíky, za které chceme provázkem zavěsit obraz. Oba konce provázku jsou přitom připevněné k obrazu. Lze to udělat tak, aby obraz na zdi držel, ale po vyndání libovolného hřebíku spadl?



Při řešení této úlohy narážíme na problém, jak si věšení obrazu jednoduše představit. Jedním z nejsilnějších matematických triků je ale umění zapomínat. Při věšení obrazu na zeď nám může být úplně jedno, jak daleko jsou od sebe oba hřebíky. Může nám být také úplně jedno, kudy přesně provázek vede. Přitom ale musíme zapomínat chytře – musíme si pamatovat, z jakých stran a v jakém pořadí provázek prochází kolem hřebíků.

Abychom mohli věšení obrazu dobře uchopit, budeme se na něj dívat následujícím způsobem. Stěnu, na které má obraz viset, si představíme jako běžnou eukleidovskou rovinu. Dále si pevně zvolíme bod O, ve kterém budou oba konce provázku připevněny k obrazu (obraz samotný nás očividně nezajímá, stačí se zabývat motáním smyčky z provázku okolo hřebíků). Hřebíky pro nás budou další různé body v rovině. A konečně – konkrétní omotání provázku kolem hřebíků si představíme jako orientovanou křivku[12] v rovině, která začíná i končí v bodě O.



Dvě takové orientované křivky pro nás budou ekvivalentní, jestliže je na sebe lze spojitě přetransformovat bez projetí některým hřebíkem. Navíc tato spojitá transformace musí zachovat směr křivky. Pokud by v rovině žádný hřebík nebyl, budou všechny křivky ekvivalentní. Jakmile v ní však alespoň jeden hřebík je, dostáváme dokonce nekonečný počet neekvivalentních křivek – různé počty obtočení provázku kolem některého hřebíku dávají neekvivalentní křivky. Množinu všech skupin ekvivalentních křivek označme P.

Všimněme si, že každé dvě z našich křivek lze *zřetězit* – jejich slepením za sebe opět dostáváme nějakou orientovanou křivku, která začíná i končí v O. To nám zní trochu povědomě. Určitě navíc existuje triviální křivka, která žádný hřebík neobtáčí, tedy je ekvivalentní degenerované jednobodové křivce odpovídající bodu O. Vzhledem k zřetězování se proto chová jako identita. Navíc ke každé křivce existuje křivka opačného směru, ty se spolu vždy složí na triviální křivku.

Právě popsané operace přitom lze provádět s celými skupinami křivek, tj. prvky z P. Stačí totiž vzít libovolné prvky z příslušných skupinek a podívat se, do které skupiny výsledek padne. Že

[12] S pojmem křivky budeme rámci seriálu pracovat pouze intuitivně.

výsledek nezávisí na konkrétní volbě křivek, je intuitivně zřejmé. Dohromady jsme tedy na množině P definovali všechny grupové operace.

Je-li ve zdi zatlučeno n hřebíků, označme pro $i \in \{1, \ldots, n\}$ symbolem a_i skupinu křivek odpovídajících jednomu obtočení ve směru hodinových ručiček kolem i-tého hřebíku. Každé zamotání provázku kolem hřebíků lze dostat zřetězením a_i a jejich inverzů. Grupu P tedy je možné vyfaktorizovat z F_n. Intuitivně ale vidíme, že každé netriviální zkrácené slovo odpovídá netriviální křivce. Jádro této faktorizace je proto triviální, dle první věty o izomorfismu je proto $F_n \simeq P$.

Shrneme, co víme: neekvivalentní omotání provázku kolem n hřebíků jednoznačně odpovídají různým slovům v grupě F_n s písmeny $\{a_1, \ldots, a_n\}$, přičemž jednopísmenná slova odpovídají smyčkám kolem jednotlivých hřebíků. Nyní už máme nabito na sestřelení obecnější verze motivační úlohy.

Tvrzení. *Ve zdi je zatlučeno $n \in \mathbb{N}$ hřebíků. Potom lze pověsit obraz tak, aby spadl po odebrání libovolného hřebíku.*

Důkaz. Budeme hledat vhodné slovo w_n v grupě F_n, které odpovídá hledanému odmotání. Odebrání i-tého hřebíku způsobí právě zmizení všech výskytů znaků a_i, a_i^{-1} z tohoto slova, neboť se tím každá smyčka okolo i-tého hřebíku stane ekvivalentní triviální smyčce. Trochu přesněji (v řeči prezentací), odebrání i-tého hřebíku přesně odpovídá přidání relace $a_i = 1$.

Chceme tedy nalézt takové redukované slovo $w_n \in F_n$, které se po smazání všech výskytů a_i, a_i^{-1} pro libovolné dané i změní na slovo ekvivalentní prázdnému slovu 1. Pro $n = 1$ triviálně funguje jednopísmenné slovo $w_1 = a_1$. Pro $n = 2$ funguje slovo $w_2 = a_1 a_2 a_1^{-1} a_2^{-1}$, které se skutečně po vyndání libovolného hřebíku zkrátí až na prázdné slovo. Induktivně není problém pokračovat dál, stačí vzít $w_n = w_{n-1} a_n w_{n-1}^{-1} a_n^{-1}$. To je zkrácené slovo, které zřejmě není prázdné. Po odebrání n-tého hřebíku dostaneme slovo $w_{n-1} w_{n-1}^{-1}$, které je ekvivalentní prázdnému slovu. Odebráním libovolného a_i pro $i \in \{1, \ldots, n-1\}$ budou z indukčního předpokladu obě slova w_{n-1}, w_{n-1}^{-1} ekvivalentní prázdnému slovu, takže i celé w_n bude ekvivalentní prázdnému slovu.

Intuitivně je přitom jasné, že na konkrétní volbě počátečního bodu O vůbec nezáleželo. Grupu P, se kterou jsme pracovali, lze sestrojit i pro jiné prostory než „rovinu s dírami“. Jedná se o takzvanou *fundamentální grupu* příslušného prostoru a jde se o velmi důležitý nástroj pro zkoumání takových prostorů.

Předchozí konstrukce však vyrábí velmi dlouhá slova, na pověšení obrazu by pak byl třeba provázek exponenciální délky v závislosti na n (slovo w_n je totiž víc než dvakrát delší než w_{n-1}). Nabízí se otázka, jak moc je možné ušetřit.

Úloha 3. Nalezněte zamotání provázku kolem n hřebíků, které řeší naši úlohu a přitom používá nejvýše $2n^2$ otáček.

Volnost podgrup a krycí grafy

Tvrzení o volných grupách mluví o krácení uvnitř konečných slov – jsou to tedy tvrzení kombinatorického rázu. Jak už jsme viděli, někdy mohou být velmi překvapivá. Chování volných grup má navíc důsledky i v dalších oblastech matematiky (vzpomeňme si na věšení obrazů). Třídu všech volných grup přitom známe velmi přesně – pro každou velikost volné báze existuje právě jedna.

Nabízí se zajímavá otázka: dědí podgrupy volnost? Po chvíli zamyšlení není odpověď vůbec jasná. Nic nám na první pohled nezaručuje, že by podgrupa volné grupy měla mít nějakou volnou bázi. Její generátory totiž mohou být velmi komplikovaná slova, která spolu mohou podezřelými způsoby interagovat. Volné grupy jsou velmi bohaté objekty (každá grupa z nich jde vyfaktorizovat!), dá se tedy čekat, že i jejich podgrupy budou velmi různorodé.

Překvapivě ale podgrupy volných grup ve skutečnosti opravdu volné jsou. Důkaz tohoto poznatku však vůbec není snadný. Samozřejmě je možné jej celkem rychle provést pomocí teorie zdaleka přesahují poznatky tohoto textu. Se zatnutím zubů a hromadou práce jej lze dokázat i

čistě kombinatoricky. My nastíníme velmi pěkný a trikový důkaz, který nám ukáže další souvislost grup, grafů a geometrie.

Úmluva. Souvislým orientovaným grafem[13] $Q = (V, E)$ nyní budeme myslet množinu vrcholů V společně s množinou orientovaných hran E, přičemž každé dva vrcholy jsou spojeny nějakou posloupností (libovolně orientovaných) hran. Opět povolujeme i násobné hrany a očka.[14]

Na graf se můžeme dívat jako na hromadu ostrůvků spojených mosty. Každý most je průchozí v obou směrech, jeho orientace pouze říká, jak se tyto směry jmenují. Ostrůvky a mosty tvoří jakýsi prostor, ve kterém se můžeme vydat na procházku. V každém prostoru se ale skrývá jedna grupa, a to ta fundamentální.

Na rozdíl od roviny je ale graf dost hranatý objekt, při našem výletu bude nutné přejít daný most vždy celý naráz. Výlety po grafu můžeme kódovat velmi snadno. Každé hraně přiřadíme nějaké písmeno x. Její projití ve směru orientace bude odpovídat symbolu x, projití v protisměru symbolu x^{-1}. Každou procházku pak můžeme zakódovat slovem, jehož písmena odpovídají navazujícím hranám.

Zvolme si nějaký pevný vrchol $o \in V$ a uvažme všechny procházky, které začínají i končí ve vrcholu o. Takové výlety lze přirozeným způsobem řetězit i invertovat, přičemž prázdná procházka se chová jako identita. Zřetězení dvou procházek bude odpovídat napsání jejich slov za sebe zleva doprava. Procházky odpovídající ekvivalentním slovům budeme v jistém smyslu považovat za stejné. Dvě procházky tedy budou ekvivalentní, pokud je na sebe lze převést přidáváním a odebíráním zacházek typu „tam a zpátky“, tj. navazujících dvojic písmen xx^{-1} resp. $x^{-1}x$. Každou takovou skupinu ekvivalentních procházek (které začínají i končí v bodě o) nazveme *smyčkou*. Na množině smyček pak lze definovat pomocí zřetězení libovolných reprezentantů grupu P_Q.

Ta má i pěkný geometrický význam. Na ostrově o jsme se před začátkem výletu přivázali provázkem, pak jsme se prošli a nakonec jsme opět skončili v o. Dvě procházky odpovídají stejné smyčce právě tehdy, když se provázek jedné z nich dá v rámci mostů přetvarovat na provázek druhé z nich. Grupa P_Q je tedy vlastně fundamentální grupou našich ostrůvků s mosty (grafu Q).

Později se nám bude hodit uvažovat i procházky, které mohou začínat i končit v libovolných (klidně různých) vrcholech grafu. To má jediný problém – takové procházky obecně není možné řetězit, grupu z nich tudíž jednoduše vyrobit nelze. Pokud na sebe však některé dvě náhodou navazují, zřetězit je můžeme. I takové (ne nutně uzavřené) procházky lze rozdělit do skupinek podle toho, zda jsou ekvivalentní. Těmto skupinám budeme říkat *polosmyčky*.

Je jasné, že grupa P_Q vůbec nezávisí na tom, jak jsme si označili směry jednotlivých cest. Díky souvislosti Q dokonce P_Q nezávisí ani na volbě počátečního vrcholu o – uzavřené smyčky z vrcholu o_1 lze pomocí obousměrné procházky mezi o_1 a o_2 převést na uzavřené smyčky z o_2, přičemž toto převedení respektuje ekvivalenci procházek i grupové operace s nimi. Grupa P_Q se tím pádem dokonce dá získat uvažováním všech možných smyček v grafu Q, tedy bez fixování nějakého konkrétního vrcholu (pro řetězení je ovšem nutné obě smyčky reprezentovat uzavřenou procházkou se stejným začátkem).

Tvrzení. *Fundamentální grupa P_Q libovolného souvislého grafu Q je volná.*

Důkaz. Naším úkolem tedy je najít nějakou její volnou bázi. Začněme volbou libovolného počátečního vrcholu o. Zvolme si libovolnou neorientovanou kostru[15] grafu Q. Tato kostra T díky souvislosti grafu Q obsahuje všechny jeho vrcholy – v opačném případě by bylo možné přidat hranu a nevytvořit kružnici. Protože T neobsahuje kružnice, všechny smyčky v ní jsou ekvivalentní.

[13] Přívlastky „souvislý“ a „orientovaný“ budeme v textu dále často vynechávat.

[14] Na rozdíl od cayleygrafů se nám ale nyní očka a násobné hrany hodit budou. Připomínáme, že očkem myslíme hranu, která vede do téhož vrcholu, z něhož vychází.

[15] *Kostrou* nazýváme libovolný podgraf, který neobsahuje žádné neorientované kružnice, ale po přidání libovolné hrany už kružnici obsahovat bude.

Označme A množinu těch hran Q, které neleží v T. Zvolme libovolné $a \in A$. K jejímu počátečnímu vrcholu lze z vrcholu o dojít jednoznačně určenou polosmyčkou p v rámci T, podobně existuje jednoznačně určená polosmyčka p' v rámci T z konce a do o. Prvku a pak přiřadíme smyčku tvaru $p_a = pap'$. Vytvořené smyčky p_a určitě generují celou P_Q, neboť libovolnou procházku umíme získat chozením v rámci T (které odpovídá identitě) společně s procházením jednotlivých p_a.

Zbývá ukázat, že mezi různými smyčkami p_a neexistují žádné netriviální relace. To lze snadno nahlédnout ze slovní reprezentace jejich procházek. Je-li totiž slovo odpovídající některé procházce ekvivalentní prázdnému slovu, musí se na něj dát převést přidáváním a odebíráním dvojiček xx^{-1}, $x^{-1}x$. Pokud se však mosty z množiny A nezkrátí triviálně, dalším výletováním po grafu T je dokrátit nelze. Smyčky p_a pak odpovídají volné bázi grupy P_Q.

Nyní si definujeme velmi důležitý grafový pojem, který nám otevře dveře ke krásným trikům.

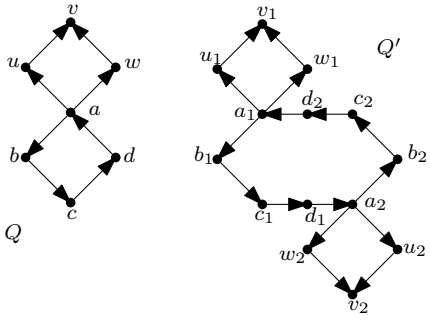
Definice. Ať $Q = (V, E)$ je souvislý orientovaný graf. Souvislý orientovaný neprázdný graf $Q' = (V', E')$ nazveme *krytím* grafu G, existuje-li *krycí zobrazení* $f : V' \to V$ splňující: Pro každý vrchol $v' \in V'$ existuje bijekce g mezi hranami vycházejícími z vrcholu v' a hranami vycházejícími z vrcholu $f(v')$ taková, že je-li h' hrana z v' do u', potom je $g(h')$ hrana z $f(v')$ do $f(u')$; analogicky pro hrany vstupující do v' a $f(v')$.

Pro jistotu ještě jednou zdůrazněme, že všechny uvažované grafy jsou souvislé. Krycí zobrazení vlastně omotává graf Q' na graf Q takovým způsobem, že nejbližší okolí každého vrcholu $v' \in V'$ vypadá stejně jako nejbližší okolí $f(v') \in V$.

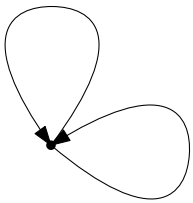
Každý graf triviálně kryje sám sebe, má však i větší krycí grafy. Pro každý graf Q dokonce existuje nekonečný krycí graf U, který neobsahuje žádné kružnice, tedy má triviální fundamentální grupu P_U. Sestrojit takové U je snadné – stačí vzít Q a „rozmotat ho, jak jen to jde“, tj. začít od jednoho počátečního vrcholu nulté úrovně, k němu dokreslit všechny potřebné šipky a na konec každé nakreslit vrchol první úrovně; dále vždy k vrcholům i-té úrovně dokreslit všechny scházející šipky dovnitř i ven a na jejich opačné konce přikreslit nové vrcholy úrovně $i + 1$.

Abychom si uměli představit, jak krytí a krycí zobrazení vlastně fungují, ukážeme si nejprve dva příklady.

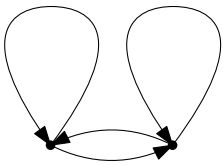
Příklad. Graf Q na obrázku má třeba následující krytí. Na posledním z obrázků je jeho krytí U.



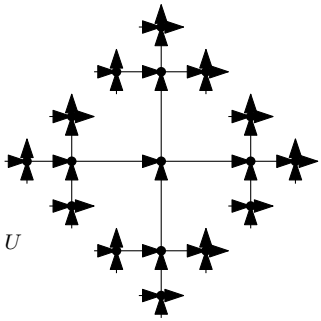
Příklad. Všimněme si, že fundamentální grupa grafu z předchozího příkladu je ve skutečnosti důvěrně známá F_2. Na následujícím obrázku je jiný graf Q_1, který má F_2 za fundamentální grupu, nějaký jeho krycí graf Q_2 a jeho úplné rozmotání U. Všimněme si, že tento U je shodou okolností přesně cayleygrafem grupy F_2. Tato souvislost není náhodná.



Q_0



Q_1



U

Než se pustíme dál, rozmysleme si následující snadné cvičení.

Cvičení 7. Kryje-li Q' graf Q pomocí krycího zobrazení f, potom je f na.

Zobrazení f podle své definice funguje jenom na vrcholech grafu V, očividným způsobem jej však lze rozšířit i na hrany – je-li $d' \in E'$ hrana z vrcholu u' do v', z vrcholu $f(u')$ pak s použitím bijekce g mezi hranami z vrcholu u a vrcholu u' vede jednoznačně určená hrana d odpovídající hraně d', jejíž koncový vrchol je roven $f(v')$. Tuto skutečnost nám nic nebrání označit jako $f(d') = d$. Všimněte si, že toto rozšířené zobrazení f se chová pěkně k začátkům a koncům hran, přičemž dodržuje i jejich směr. Bez problémů tedy můžeme f rozšířit dokonce na libovolné procházky, jejich obrazy budou opět procházky. Pochopitelně toto f zobrazuje ekvivalentní procházky na ekvivalentní procházky. Dává tedy přirozeně vzniknout šikovnému zobrazení f_*, které zobrazuje polosmyčky v grafu Q' na nějaké polosmyčky v Q, přičemž obrazy smyček jsou opět smyčky.

V předchozím odstavci jsme popsali, jak lze krycí zobrazení f rozšířit na všechno, co nás grafech momentálně zajímá. Rádi bychom však uměli postupovat i v opačném směru. To jednoznačně provést nelze, neboť krytí f typicky nebude prosté. Díky lokální podobnosti obou grafů je to ale proveditelné alespoň skoro.

Lemma. (zvedací) *Ať graf $Q' = (V', E')$ je krytím grafu $Q = (V, E)$ skrz krycí zobrazení f. Dále ať $o \in V$ je jeho libovolný vrchol a o' je nějaký jeho vzor v zobrazení f. Potom lze každou procházku p z bodu o v grafu Q jednoznačně „zvednout“ na takovou procházku p' z bodu o' v grafu Q', že $f(p') = p$.*

Důkaz. Lemma je v zásadě těžší vyřknout než dokázat. Takovou procházku p' jsme nuceni zrekonstruovat postupně po hranách. Protože je ale zobrazení f krycí, v každou chvíli máme na výběr právě jednu hranu, kterou nám daruje sama definice krycího zobrazení. Induktivně tak lze zkonstruovat právě jednu vyhovující cestu p'.

Proceduru z předchozího lemmatu si můžeme představit jako částečné rozmotání procházky v Q na procházku v Q'. Stejně jako před chvílí dává zvedání smysl i pro smyčky a polosmyčky.

Když už víme, co jsou krycí grafy, odhalíme jejich vztah s grupami.

Tvrzení. *Je-li $Q' = (V', E')$ krytí $Q = (V, E)$, potom $P_{Q'} \leq P_Q$.*

Důkaz. Ať f je nějaká krycí funkce $Q' \to Q$. Zvolme si libovolné $o' \in V'$, dále ať $o = f(o')$, příslušné fundamentální grupy budou obsahovat smyčky se začátkem a koncem v o', resp. o. Je-li $p \in P_{Q'}$, je to smyčka se začátkem i koncem v o', takže $f(p)$ je smyčka začínající i končící v o, tedy $f(p) \in P_Q$. Zobrazení f respektuje zřetězení smyček, takže je to dokonce grupový homomorfismus $P_{Q'} \to P_Q$.

Zbývá ukázat, že je prostý, neboť pak bude $P_{Q'} \simeq f(Q') \leq P_Q$. To však plyne ze zvedací vlastnosti krytí: Každá smyčka p v grafu Q se začátkem v o má jednoznačný vzor v grafu Q' se začátkem v o'. Pozor, tento vzor už nemusí být smyčkou, neboť může končit v jiném vzoru bodu o.

Každopádně, je-li smyčka $p \in P_Q$ triviální, dá se reprezentovat slovem, které se zkrátí. Jeho jednoznačný vzor v Q' se pak ale také musí zkrátit, zvednutí triviální smyčky je tedy triviální

smyčka. To ale znamená, že netriviální smyčky v $P_{Q'}$ homomorfismus f zobrazuje na netriviální smyčky v P_Q, tedy má triviální jádro, takže je prostý.

Tvrzení intuitivně říká, že v krycím grafu Q' jsou některé kružnice grafu Q „rozmotány“, takže jejich netriviální smyčky v Q se v Q' trivializují. Jiné smyčky tímto přechodem nezmizí, tyto přeživší smyčky pak nutně odpovídají nějaké podgrupě původní grupy P_Q.

Uvedená korespondence však překvapivě funguje i na druhou stranu, jak odhaluje následující silné a pěkné tvrzení.

Tvrzení. *Ať Q je souvislý graf. Potom pro každou podgrupu $H \leq P_Q$ existuje jeho krytí Q' takové, že $H \simeq P_{Q'}$.*

Důkaz. Naším úkolem tedy je rozmotat graf Q „tak akorát“ – takovým způsobem, aby toto rozmotání přežily právě prvky H. Začněme tím, že ho rozmotáme úplně, tedy vyrobíme nekonečný strom U, jehož fundamentální grupa je triviální. Označme si ještě μ krycí zobrazení, které zprostředkovává krytí grafu Q grafem U. Vyberme počáteční vrchol o grafu U, za počáteční vrchol Q pak považujme $\mu(o)$. Díky zvedání má každá procházka v Q z bodu $\mu(o)$ jednoznačnou vzorovou procházku v U začínající v o.

Pokud byla grupa H triviální, U je hledaný graf. Pokud je H netriviální, je nyní potřeba graf U zase trochu zmenšit poslepováním některých vrcholů, čímž vznikne graf Q'. Kde ho ale vyhrabeme? Explicitně jej popsat by bylo obtížné, my ho naopak fikaně donutíme, aby se vyrobil sám.

Definujme graf Q' následujícím způsobem. Jeho vrcholy budou odpovídat skupinám vrcholů z U, podobně jeho hrany. Vezměme dva vrcholy u, v grafu U. Protože je U strom, existuje v něm jednoznačná zkrácená procházka mezi o a u a jednoznačná zkrácená procházka mezi o a v. Z nich lze vytvořit jednoznačnou polosmyčku p_u z o do u a jednoznačnou polosmyčku $p_{v^{-1}}$ z v do o. Vrcholy u, v dáme do stejné skupinky (což označíme $u \sim v$) právě tehdy, pokud lze smyčky $\mu_*(p_u)$ a $\mu_*(p_{v^{-1}})$ v grafu Q zřetězit (tj. druhá začíná tam, kde první končí, neboli $\mu(u) = \mu(v)$) a pokud je toto zřetězení dokonce prvkem H.

Dávají takové skupinky vůbec smysl? Protože H obsahuje identitu, každý prvek je ve skupince se sebou samým. Díky existenci inverzů v H nastane $u \sim v$ právě tehdy, když $v \sim u$. A je-li $u \sim v$ a $v \sim w$, díky uzavřenosti H na zřetězení je i $u \sim w$. Rozdělení na skupinky je tedy skutečně smysluplné a lepení se dá provést.

Hrany v Q' pak zvolíme přirozeným způsobem: pro daný vrchol u' grafu Q' si vezmeme libovolného jeho reprezentanta u uvnitř grafu U a podíváme se na hrany z u. Pak projdeme všechny vrcholy s, do nichž vede hrana z u, a za každou takovou hranu z u do s pak do Q' nakreslíme právě jednu hranu z u' do s'. Nezávisí však tento postup na volbě reprezentanta u'? Skutečně ne. Je-li $u \sim v$, bylo možné slepit příslušné cesty v Q, takže $\mu(u) = \mu(v)$. Ze zvedací vlastnosti tedy mají body u, v stejná okolí. Vede-li tedy z u hrana d_s do nějakého jeho souseda s a zároveň $u \sim v$, vede též z vrcholu v nějaká hrana d_t do takového t, že $\mu(s) = \mu(t)$. Potom však lze polosmyčky $\mu(p_s)$ a $\mu(p_t)$ v grafu Q zřetězit, přičemž výsledná smyčka je (smazáním triviální zacházky tvaru $\mu(d_s)\mu(d_t)^{-1}$) ekvivalentní smyčce $\mu(p_u)\mu(p_{v^{-1}}) \in H$.

Fikaně definovaný graf Q' tedy skutečně existuje, zobrazení přiřazující vrcholu $u \in U$ jeho skupinku v Q' je díky předchozímu odstavci dokonce krycí. Označme π zobrazení vrcholů Q' na vrcholy Q, které každému vrcholu u' grafu Q' přiřadí $\mu(u)$, kde u je jeho libovolný reprezentant v U. Jsou-li $u \sim v$ dva vzory u' v grafu U, smyčky $\mu(p_u), \mu(p_{v^{-1}})$ bylo možné zřetězit, takže speciálně $\mu(u) = \mu(v)$, zobrazení π tedy dává smysl definovat. Protože U je krytím Q' a zobrazení π se chová jako μ, je také krycí.

Konečně nahlédneme, že $P_{Q'} \simeq H$. Za počáteční vrchol grafu Q' zvolme projekci o' vrcholu o. Rozmyslíme si, jak vypadají smyčky v $P_{Q'}$. Vezměme si tedy nějakou polosmyčku p' v grafu Q', která začíná v o'. Ať p je jí příslušná jednoznačně určená polosmyčka v U, která začíná v bodě o. Polosmyčka p' je prvkem $P_{Q'}$ právě tehdy, když také končí v bodě o, což nastane právě v případě, kdy jsme slepili začátek a konec procházky p. Jenže ty jsme slepili právě v případě, když $\pi(p') = \mu(p) \in H$. Zobrazení π indukuje prostý homomorfismus $P_{Q'} \to P_Q$, jehož obraz je dle předešlého

přesně H, což jsme chtěli.

Všimněme si, že důkaz předchozího tvrzení skutečně nijak neříká, jak bude graf Q' přesně vypadat. Namísto toho se nám povedlo pomocí vlastností podgrupy H jeho existenci zařídit. Skutečná explicitní výroba takového grafu by obecně byla složitá, neboť zahrnuje hromadu kombinatorického krácení slov, které geometricky odpovídá kolabování grafu U. Předem ohlašovanou větu o podgrupách volných grup nyní dostaneme jako snadný důsledek.

Věta. *Každá podgrupa volné grupy je volná.*

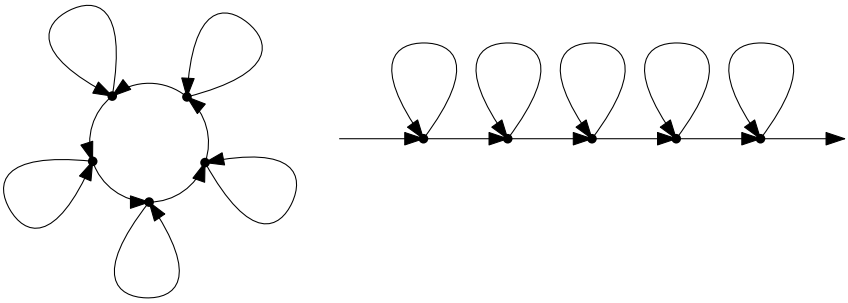
Důkaz. Volná grupa s bází X je fundamentální grupou kytice $|X|$ oček – grafu Q s jedním vrcholem, jehož $|X|$ hran v něm začíná i končí. To je okamžitě vidět, neboť takový graf má triviální kostru, takže všechny jeho hrany odpovídají generátorům příslušné fundamentální grupy. Je-li $H \leq G$, potom H je fundamentální grupou nějakého grafu Q' (který dokonce kryje Q). Grupa H je tedy také volná, neboť fundamentální grupy všech grafů jsou volné.

Pro ilustraci síly právě dokázaného výroku si na závěr rozmysleme několik faktů, které z něj okamžitě plynou.

Přestože lze každou grupu vyfaktorizovat z nějaké volné, podgrupy volných grup jsou pouze volné grupy. Volné grupy v sobě skrytě nesou struktury všech jiných grup, aniž by je samy obsahovaly jako podgrupy.

Také si vzpomeňme, jak složité je algoritmicky uchopit grupu zadanou nějakou prezentací $G = \langle X \mid R \rangle$. Přitom je ale normální podgrupa K příslušná relacím také volná. Sice tedy víme (až na počet generátorů), jak bude K vypadat, přesto algoritmicky neumíme najít, jak se v F_X schovává.

Dávno už víme, že F_2 obsahuje podgrupy izomorfní volným grupám s mnohem větší bází. Tento překvapivý fakt ale nyní dokážeme pochopit hlouběji. Podgrupy volné grupy F_2 odpovídají krytím grafu Q, který je tvořen jediným vrcholem a dvěma hranami (které začínají i končí v onom vrcholu). Podgrupy izomorfní s F_1 a F_2 obsahuje triviálně. Pro $n \geq 3$ zvolme krycí graf Q' jako $(n-1)$-cyklus, který má v každém vrcholu smyčku, z jehož existence plyne existence podgrupy grupy F_2 izomorfní s F_n. Existenci podgrupy izomorfní s $F_{\mathbb{N}}$ dostáváme volbou krycího grafu Q', který odpovídá nekonečné cestě se smyčkou v každém vrcholu. Jiným pěkným krycím grafem Q', který odpovídá takové grupě, je třeba nekonečná čtvercová mřížka. Z těchto grafů pak lze zpětně získat jim příslušné podgrupy.



Pomocí popsané korespondence volných grup a grafů dostávají volné grupy krásný geometrický význam, jehož sílu jsme právě mohli okusit. Chceme-li například pro nějakou podgrupu volné grupy najít velikost její báze, stačí najít krycí graf, který jí odpovídá, a podívat se, kolik hran v něm zbude po odebrání maximální kostry.

Síla vybudované teorie tkví přesně v tom, že jsme získali „slovník“, který nám umožňuje překlad

mezi kombinatorikou na slovech a geometrií grafů. My zde však zkoumání volných grup ukončíme.

Závěr

Pokud jste dočetli až sem, cítíme se velice polichoceni. Ačkoli je nám to líto, budeme se nyní muset rozloučit. Přitom doufáme, že jste si naši dobrodružnou procházku teorií grup co nejvíc užili. Naším textem samozřejmě nic nekončí – pokud byste se chtěli dozvědět z teorie grup a moderní algebry více, můžeme vám doporučit třeba pěknou knížku od Josepha J. Rotmana „An Introduction to the Theory of Groups“.

Těšíme se na vaše řešení třetí seriálové série a v tomto roce se s vámi se seriálem loučíme.

Návody ke cvičením

1. Víme, že můžeme každé $g \in G$ zapsat jako součet konečně mnoha prvků z X a jejich inverzů. Prvky X, které byly v daném součtu použity (buď přímo, nebo v podobě svých inverzů), označíme po řadě x_i. Jelikož je G abelovská, sčítání komutuje. Tím pádem můžeme seskupit všechny výskyty x_1 a $-x_1$, za nimi shluknout všechny výskyty x_2 a $-x_2$ a tak dále. Číslo a_i potom bude udávat počet výskytů x_i mínus počet výskytů $-x_i$.

2. Dá se jednoduše ověřit, že $\mathbb{Z}^n = \langle (1,0,\ldots,0), (0,1,\ldots,0), \ldots, (0,0,\ldots,1) \rangle$. Tím pádem má n-prvkovou, a tedy konečnou množinu generátorů.

3. Předpokládejme pro spor, že má konečnou množinu generátorů X. Nechť $X = \{\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_n}{q_n}\}$, kde p_i jsou celá a q_i přirozená. Potom pro libovolná celá $a_1, \ldots, a_n$ bude mít racionální číslo $a_1 \cdot \frac{p_1}{q_1} + a_2 \cdot \frac{p_2}{q_2} + \cdots + a_n \cdot \frac{p_n}{q_n}$ v základním tvaru jmenovatel $q_1 q_2 \cdots q_n$ nebo dokonce nějaký dělitel tohoto čísla. Tím pádem jistě nedokážeme vygenerovat třeba $\frac{1}{q_1 q_2 \cdots q_n + 1}$ a dostáváme spor s předpokladem, že můžeme vygenerovat celé $\mathbb{Q}$.

5. Ačkoli se tvrzení zdá zřejmé, je třeba najít rozumný důvod, který jej vynutí. Jednou z možných argumentací je ta následující: Kdyby bylo možné F_2 nagenerovat jedním prvkem, byla by cyklická, tedy i abelovská. Jenže zkrácená slova a, b spolu nekomutují – slova ab, ba jsou zkrácená, jedná se tedy o různé prvky F_2.

6. Ať F_2 je vyrobena z množiny písmen $X = \{a, b\}$. Volme $H = \langle a^2, b^2 \rangle$. To je vlastní podgrupa grupy F_2, neboť všechna její slova obsahují sudý počet znaků z $\{a, a^{-1}\}$ a sudý počet znaků z $\{b, b^{-1}\}$ (přičemž krácení či vkládání dvojic vzájemně inverzních písmen tuto paritu nemění). Snadno navíc můžeme ověřit, že přiřazení $a^2 \mapsto a$, $b^2 \mapsto b$ lze rozšířit na izomorfismus $\psi : H \to F_2$.

7. Protože je Q' z definice neprázdný, na některý vrchol u grafu Q se něco zobrazit muselo. Protože je Q souvislý, existuje v něm z vrcholu v procházka do libovolného vrcholu u. Této procházce ale díky lokální podobnosti obou grafů odpovídá nějaká procházka v Q', její poslední vrchol je proto vzorem v.

Návody k úlohám

1. Vezměme třeba podgrupu $H = \langle a^2, b^2, ab \rangle$. První dva její generátory obsahují sudý počet písmen z $\{a, a^{-1}\}$ a sudý počet písmen z $\{b, b^{-1}\}$. Ten se ale při přidávání a mazání povolených dvojiček nemění, slovo ab pomocí nich tedy nagenerovat nelze. Nyní ukážeme, že pomocí prvků a^2, ab nelze nagenerovat b^2. To bychom museli získat napsáním slov $\{a^2, a^{-2}, ab, b^{-1}a^{-1}\}$ za sebe. Pro spor předpokládejme, že jsme vyrobili slovo w, které je ekvivalentní slovu b^2. Protože je b^2 redukované a každá třída ekvivalentních slov obsahuje právě jedno redukované slovo, lze w převést na b^2 pouze mazáním. Nejdříve tedy zkraťme sousední slova z množiny $\{a^2, a^{-2}, ab, b^{-1}a^{-1}\}$, která k sobě byla inverzní. Může se nyní některé písmeno b pokrátit? Vezměme momentálně nejbližší dvojici písmen b, b^{-1}, která se spolu mohou ještě někdy pokrátit. Potom ale mezi nimi je a v nějaké sudé nenulové mocnině, pokud tedy už jenom mažeme, nikdy se nepokrátí. Poslední ze tří dvojic nemůže generovat a^2 díky symetrickému argumentu. Zobrazení přiřazující prvkům a^2, b^2, ab prvky volné báze F_3 pak díky jejich nezávislosti umíme rozšířit na homomorfismus. Ten je triviálně na a díky nezávislosti našich generátorů má triviální jádro, tedy je to hledaný izomorfismus.

2. To dokážeme pomocí předchozí úlohy. Už umíme nalézt podgrupu $H_0 < F_2$, která je izomorfní s F_3, takové tři prvky jsou třeba $\langle a^2, b^2, ab \rangle$. Také už víme $F_2 \simeq F_2' = \langle a^2, b^2 \rangle$. Na F_2' tedy můžeme předvedený postup aplikovat znovu, což dává podgrupu $H_1 < F_2'$ definovanou jako $\langle ab, a^2b^2, a^4, b^4 \rangle$. Díky vlastnostem H_0 však ab nelze nagenerovat pomocí zbytku, díky vlastnostem H_1 jsou na sobě nezávislé i prvky a^2b^2, a^4, b^4. Induktivně pokračujme dál. Grupa $K = \langle ab, a^2b^2, a^4b^4, \ldots \rangle$ je pak volná grupa s nekonečnou bází. Stejně jako minule totiž lze její generátory bijektivně zobrazit na generátory volné grupy $F_{\mathbb{N}}$, přičemž vlastností H_i jsou její generátory nezávislé.

To samozřejmě není jediný předpis takové divné podgrupy. Funguje třeba i $\langle bab^{-1}, b^2ab^{-2}, b^3ab^{-3}\rangle$ nebo $\langle ab, a^2b^2, a^3b^3, \dots\rangle$ a mnoho dalších, což si s trochou opatrnosti není problém rozmyslet.

3. Pro přehlednost zavedeme pro prvky x, y nějaké grupy značení $[x,y] = xyx^{-1}y^{-1}$. Předchozí dlouhé řešení tedy můžeme zapsat ve tvaru $w_n = [[\dots[[a_1,a_2],a_3],\dots],a_n]$. Rapidně ušetřit dokážeme následujícím trikem. Místo rozdělování písmen a_i v každém kroku na „poslední“ a „zbytek“ je zkusíme rozdělit přibližně na poloviny.

Vyrobme tedy slova v_n následujícím rekurzivním způsobem: Slovo v_n bude tvořeno písmeny z vhodné n-prvkové abecedy. Opět mějme $v_1 = a_1$. Máme-li už všechna slova v_i pro $i \le n-1$, nejprve označme[16] $m = \lceil \frac{n}{2} \rceil$ a $m' = \lfloor \frac{n}{2} \rfloor$ a následně definujme $v_n = [u_m, u'_{m'}]$, kde u_m značí slovo v_m na prvních m písmenech a $u'_{m'}$ značí slovo $v_{m'}$ na posledních m' písmenech. Je-li tedy $2^{j-1} \le n < 2^j$, je třeba při této rekurzivní definici v_n použít hranaté závorky nejvýše j-krát. Spočtěme tedy, kolikrát se každé a_i může nejvýše vyskytovat v v_n. Pro $n = 1$ se tam vyskytuje jednou. Každé další použití závorek nejvýše zdvojnásobí počet výskytů pevného a_i, takových kroků je nejvýše $j = \log_2 n + 1$, takže výskytů a_i je nejvýše $2^{\log_2 n+1} = 2n$. Slovo v_n používá n písmen, takže jeho délka je nejvýše $2n^2$.

[16] Symbolem $\lceil x \rceil$ se označuje nejmenší celé číslo, které je alespoň tak velké jako x, podobně symbolem $\lfloor x \rfloor$ značíme největší celé číslo, které není větší než x.