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.

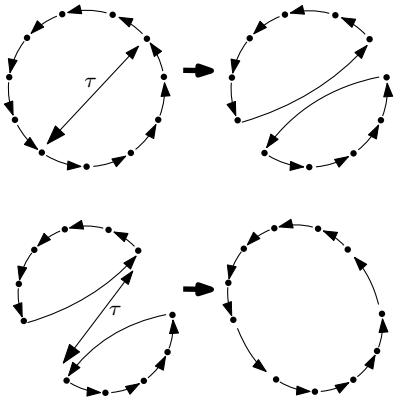
Mohli jsme postupovat i o trochu explicitněji. Permutaci σ lze rozložit na cykly, takže ji můžeme zapsat jako složení permutací odpovídajících těmto cyklům (v libovolném pořadí). Cyklus $(a_1 a_2 \dots a_k)$ přitom lze zapsat jako složení $k-1$ transpozic $(a_1 a_k) \cdots (a_1 a_3)(a_1 a_2)$.

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.