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 $\varphi$ 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 $\varphi$, 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 $\varphi$ 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 $\varphi$ inverzní, takže $\varphi$ musí být prosté i na. Ukázali jsme, že je $\varphi$ opravdu automorfismus $\mathbb{Z}^n$.

Navíc $\varphi$ 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 $\psi$, 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 $\psi$ automorfismus $\mathbb{Z}^n$, je obdobný jako u $\varphi$. 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 $\Phi$ 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 $\alpha$. Speciálně sledujme $\alpha_c$ pro nějaké $c \in C$. Šipky barvy $c$ v cayleygrafu $Q$ přesně odpovídají permutaci $\alpha_c$. Protože je $\alpha_c$ 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.

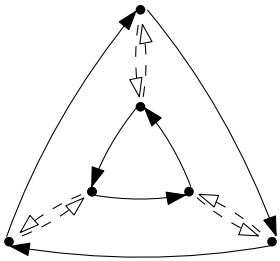
Nyní ukážeme druhý směr tvrzení: k libovolnému zajímavému grafu $Q$ vyrobíme grupu $G$ tak, aby $Q$ byl její cayleygraf. Za grupu $G$ vezměme jednoduše grupu všech symetrií grafu $Q$ – tedy grupu všech permutací jeho vrcholů, které zachovávají směry i barvy šipek. Jak tato $G$ vypadá? Zvolme libovolný 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.

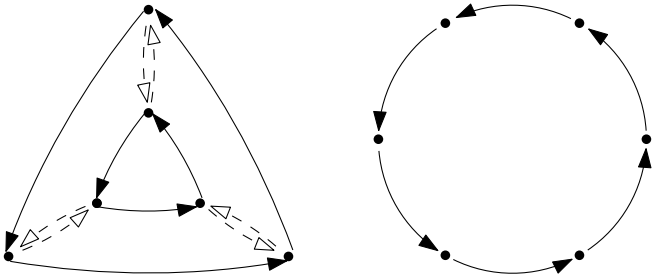
Pojem zajímavého grafu jsme zavedli jen proto, aby bylo v předchozí diskuzi jasně rozlišeno, kdy konstruujeme grupu z grafu a kdy naopak graf z grupy. Protože jsme ale právě nahlédli, že třída zajímavých grafů přesně odpovídá třídě cayleygrafů všech možných grup, budeme dále místo pojmu zajímavý graf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

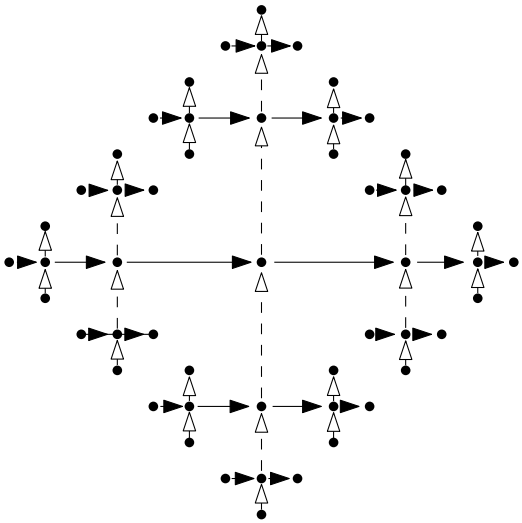
Přestože je volná grupa sama o sobě docela intuitivní objekt, její vyrábění skýtalo několik záludností.[6] Ještě než se posuneme dál, předvedeme si alternativní konstrukci volných grup, a to pomocí cayleygrafů. Tato konstrukce je méně přímočará, zato je však neuvěřitelně elegantní. Následujícímu postupu 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,

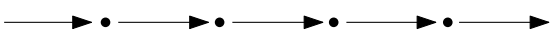
[7] *Stromem* myslíme graf, který neobsahuje žádnou – ani neorientovanou – kružnici.

[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 $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\varphi$ prosté, díky druhému je $\varphi$ 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 $\varphi$ 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 $\varphi$ 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 $\sigma$. 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 $\sigma$. Vezměme si tedy zobrazení $f : \{a, b\} \to D_{2n}$, které posílá $a \mapsto r$, $b \mapsto \sigma$; to lze rozšířit na homomorfismus $\varphi : F_2 \to D_{2n}$.

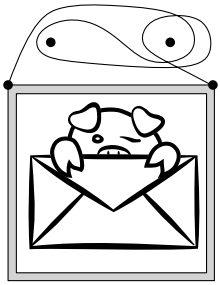
Zbývá nalézt jeho jádro v $F_2$. V grupě $D_{2n}$ platí díky jejímu geometrickému významu identity $r^n = 1$, $\sigma^2 = 1$ a $\sigma r\sigma = r^{-1}$, takže prvky $a^n$, $b^2$, $(ba)^2$ leží v $\operatorname{Ker}\varphi$. Označíme-li $K$ nejmenší normální podgrupu $F$, která obsahuje tyto tři prvky, 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 $\sigma a^k$ 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

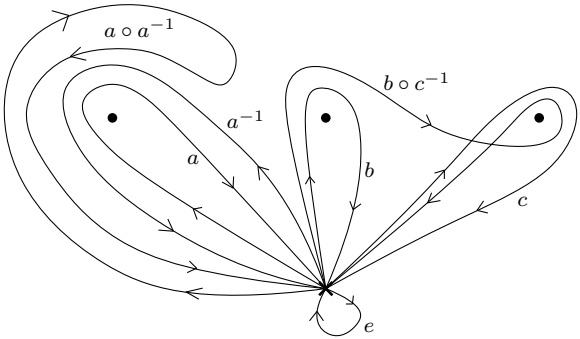
Pojďme si pro změnu hrát s úlohou, která s grupami na první pohled vůbec nesouvisí. Chcete-li se nad ní na chvíli zamyslet sami, vřele to doporučujeme – posléze bude řešení vyzrazeno.

**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.

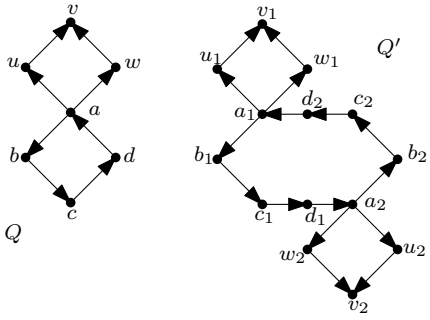
**Definice.** Ať $Q = (V, E)$ je souvislý orientovaný graf. Souvislý orientovaný neprázdný graf $Q' = (V', E')$ nazveme *krytím* grafu $G$, existuje-li *krycí zobrazení* $f : V' \to V$ splňující: Pro každý vrchol $v' \in V'$ existuje bijekce $g$ mezi hranami vycházejícími z vrcholu $v'$ a hranami vycházejícími 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 $f(v') \in V$.

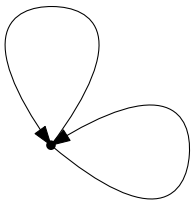
Každý graf triviálně kryje sám sebe, má však i větší krycí grafy. Pro každý graf $Q$ dokonce existuje nekonečný krycí graf $U$, který neobsahuje žádné kružnice, tedy má triviální fundamentální grupu $P_U$. Sestrojit takové $U$ je snadné – stačí vzít $Q$ a „rozmotat ho, jak jen to jde“, tj. začít od jednoho 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.

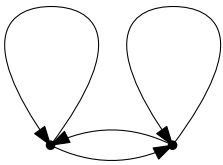
**Příklad.** Graf $Q$ na obrázku má třeba následující krytí. Na posledním z obrázků je jeho krytí $U$.



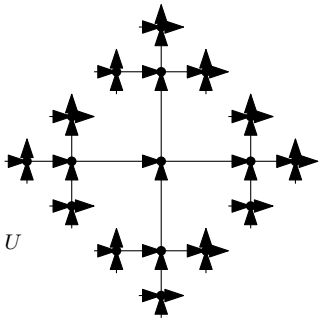

**Příklad.** Všimněme si, že fundamentální grupa grafu z předchozího příkladu je ve skutečnosti důvěrně známá $F_2$. Na následujícím obrázku je jiný graf $Q_1$, který má $F_2$ za fundamentální grupu, nějaký jeho krycí graf $Q_2$ a jeho úplné rozmotání $U$. Všimněme si, že tento $U$ je shodou okolností 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 $\mu$ 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 $\pi$ 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 $\pi$ tedy dává smysl definovat. Protože $U$ je krytím $Q'$ a zobrazení $\pi$ se chová jako $\mu$, 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 $\pi$ 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.*

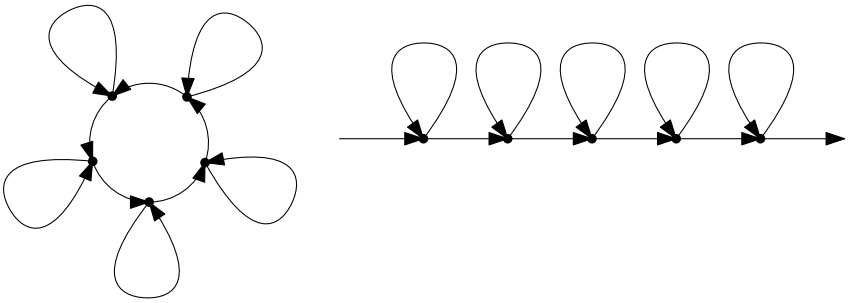
*Důkaz.* Volná grupa s bází $X$ je fundamentální grupou kytice $|X|$ oček – grafu $Q$ s jedním vrcholem, jehož $|X|$ hran v něm začíná i končí. To je okamžitě vidět, neboť takový graf má triviální kostru, takže všechny jeho hrany odpovídají generátorům příslušné fundamentální grupy. Je-li $H \leq G$, 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 $x$.