

Pokroky matematiky, fyziky a astronomie

Michal Křížek; Lawrence Somer

Abelova cena v roce 2008 udělena za objevy v teorii neabelovských grup

Pokroky matematiky, fyziky a astronomie, Vol. 53 (2008), No. 3, 177--187

Persistent URL: <http://dml.cz/dmlcz/141856>

Terms of use:

© Jednota českých matematiků a fyziků, 2008

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



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

Abelova cena v roce 2008 udělena za objevy v teorii neabelovských grup

Michal Krížek, Praha, Lawrence Somer, Washington

1. Úvod

Letošní Abelovu cenu za matematiku získali John Griggs Thompson z USA a Jacques Tits z Francie. Cenu jim udělila Norská akademie věd a písemnictví (angl. the Norwegian Academy of Sciences and Letters) a předal ji osobně norský král Harald dne 30. května 2008 v hlavní aule univerzity v Oslo. Pro letošní rok byla Abelova cena spojena s částkou 1 200 000 USD. Podle vyjádření prof. Kristiana Seipa, předsedy výběrové komise, cenu dostali za *své hluboké výsledky v algebře a hlavně za zformování moderní teorie grup*.



Obr. 1. John Griggs Thompson a Jacques Tits.

J. G. Thompson působí od r. 1993 jako Graduate Research Professor na University of Florida a je emeritním profesorem na Univerzity of Cambridge v Anglii. Narodil se 13. října 1932 v Kansasu. Na slavné Yale University začal studovat teologii. Po roce však přešel na matematiku a udělal dobře. Saunders Mac Lane jej totiž pozval, aby si udělal doktorát na University of Chicago. Zde se začal intenzivně věnovat konečným grupám symetrií a získal v roce 1959 titul Ph.D. Poté rok působil na Institute for Defense Analysis a dva roky na Harvardově univerzitě. Pak se vrátil do Chicaga a v období 1962–1968 zde byl již profesorem. V roce 1970, kdy ještě nedosáhl ani 40 let,

Prof. RNDr. MICHAL KRÍŽEK, DrSc., Matematický ústav Akademie věd ČR, v.v.i., Žitná 25, 115 67 Praha 1, e-mail: krizek@math.cas.cz

Prof. Dr. LAWRENCE SOMER, Department of Mathematics, Catholic University of America, Washington, D.C. 20064, U.S.A., e-mail: somer@cua.edu

byla Thompsonova práce oceněna Fieldsovou medailí. V letech 1970–1993 pak působil na univerzitě v Cambridge. Získal 4 čestné doktoráty, Wolfovu cenu, Coleovu cenu, Sylvesterovu medaili, Poincarého medaili aj.

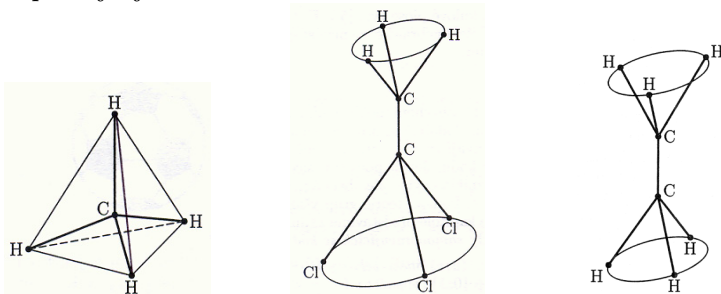
J. Tits je emeritním profesorem na Collège de France, ale je původem z Belgie. Narodil se 12. srpna 1930 v Uccle na předměstí Bruselu. Považovali jej za zázračné dítě. Už jako tříletý uměl počítat a později mu bylo umožněno, že přeskočil několik tříd školní docházky. Ve svých čtrnácti letech tak úspěšně vykonal přijímací zkoušky na Free University of Brussels. V roce 1950, když mu bylo pouhých 19 let, získal titul Ph.D. Působil na řadě univerzit, např. v Bruselu, Bonnu a Paříži. Získal 4 čestné doktoráty a celou řadu dalších ocenění (např. Wolfovu cenu). Je členem mnoha akademií a čestným členem Londýnské matematické společnosti.

V tomto článku bychom chtěli seznámit čtenáře se základy moderní teorie konečných grup. V závěrečné kapitole se pak stručně zmíníme o hlavních výsledcích obou laureátů v této oblasti a jejich přínosu ke sporadickým grupám.

2. Stručně o teorii grup

Připomeňme si nejprve některé základní pojmy. *Grupa* G je množina, na které je definována asociativní binární operace $\circ : G \times G \rightarrow G$ s neutrálním prvkem e a v níž ke každému prvku $g \in G$ existuje právě jeden prvek inverzní $g^{-1} \in G$. Prvkům G se někdy říká *symetrie*, pokud jsou to zobrazení geometrických objektů na sebe.

Studium symetrií má dlouhou historii. Jeho kořeny sahají až do antiky. Například staré egyptské a maurské ornamenty vykazují symetrie všech 17 tapetových grup (tj. dvojrozměrných krystalografických grup, jejichž existenci udává Fjodorovův teorém). Lidé totiž odjakživa obdivují a dávají přednost objektům, které vykazují nějaký druh symetrie. Např. staří Řekové se zabývali platónskými tělesy, jejichž symetrie také tvoří grupy, jak se později zjistilo.



Obr. 2. Symetrie molekuly metanu CH_4 tvoří grupu $o_4! = 24$ prvcích, která je izomorfní¹⁾ symetrické grupě S_4 . Grupa tzv. přímých symetrií, kdy neuvážujeme zrcadlové obrazy molekuly, má jen 12 prvků a je izomorfní s alternující grupou A_4 . Symetrie prostřední molekuly trichlorethanu $\text{H}_3\text{C}-\text{C}\text{Cl}_3$ tvoří cyklickou grupu C_3 o třech prvcích. Dihedrál ní grupa D_3 se skládá ze šesti přímých symetrií molekuly etanu C_2H_6 .

¹⁾ Izomorfismus je vzájemně jednoznačné zobrazení, které zachovává binární grupovou operaci.

Grupou všech permutací prvků $1, 2, \dots, n$ (s operací skládání) nazveme *symetrickou* a označíme ji S_n . Grupou všech sudých permutací prvků $1, 2, \dots, n$ nazveme *alternující²⁾* a označíme ji A_n .

Pojem „grupa“ pochází až od Evarista Galoise, který je všeobecně považován za zakladatele teorie grup. Kolem roku 1830 odvodil z vlastností symetrických grup S_n , že algebraické rovnice stupně vyššího než 4 nejsou obecně řešitelné pomocí odmocnin. Přitom pro řešení tohoto obtížného problému podstatně využil vlastností symetrie mezi jednotlivými kořeny. Niels Henrik Abel dokázal již dříve podobný výsledek pro algebraické rovnice pátého stupně na pouhých šesti stránkách (viz [1], [22]). První knihu o teorii grup publikoval v roce 1870 Camille Jordan. Nazval ji *Traité des substitutions* (viz [12]).

Teorie grup má obrovské množství nejrůznějších praktických aplikací, např. při klasifikaci krystalů, uzlů, symetrií molekul (viz obr. 2), popisu silných, slabých a elektromagnetických interakcí, skládání Lorentzových transformací, v teorii kódování³⁾ (viz [16], [19], [20], [25]). Díky symetriím se značně zjednodušují některé výpočty. S grupami se setkáváme i při řešení různých hlavolamů (viz např. obr. 3).

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

R	A	T	E
Y	O	U	R
<i>m</i>	<i>i</i>	<i>n</i>	<i>d</i>
<i>p</i>	<i>l</i>	<i>a</i>	

Obr. 3. Známa hra *patnáctka* (vlevo) neumožňuje prohodit 15 a 14 v posledním řádku tak, aby poloha ostatních čísel zůstala zachována. Plyne to z vlastností alternujících grup (viz [25, s. 39 a 97]). Na druhé straně *l* a *a* v posledním řádku (vpravo) prohodit lze. Víte proč?

3. Konečné grupy

Dále se budeme zabývat jen konečnými grupami (slovo **konečný** budeme proto většinou vynechávat). Počet prvků G označíme $|G|$ a nazveme *řádem grupy⁴⁾*.

Podgrupa $H \subset G$ je grupa se stejnou operací \circ , ale zúženou na $H \times H$ a s tímž neutrálním prvkem e , jako má G . Nazývá se *vlastní*, je-li $H \neq G$, a *triviální*, je-li $H = \{e\}$.

Věta (Cayleyova). *Každá grupa řádu n je izomorfní nějaké podgrupě symetrické grupy S_n .*

²⁾ Někdy se jí říká též *alternativní* grupa.

³⁾ Například německá armáda používala elektromechanický šifrovací stroj Enigma. Jeho kód v roce 1932 rozšifrovali pomocí teorie grup M. Rejewski, J. Rozycki a H. Zygalski pracující pro polskou tajnou službu. Koncem 2. světové války pak zdokonalený kód rozšifroval Alan Turing, což pomohlo zkrátit válku a ušetřit tak mnoho lidských životů.

⁴⁾ Počet vzájemně neizomorfních grup řádu n se uvádí ve Sloanově *On-line encyclopedia of integer sequences* v položce A000001, např. existuje 257 grup řádu 64, ale jen jedna grupa řádu 65, viz <http://www.research.att.com/~njas/sequences/>

Poznamenejme, že pro $n \geq 3$ je grupa S_n neabelovská (tj. není komutativní).

Věta (Lagrangeova). *Nechť G je grupa řádu n . Jestliže existuje podgrupa $H \subset G$ řádu m , pak m dělí n .*

Jako důsledek dostáváme, že $g^{|G|} = e$ pro každé $g \in G$ (viz [17, s. 131]).

Francouzský matematik Augustin-Louis Cauchy dokázal, že pro každé prvočíslo p , které dělí $|G|$, existuje podgrupa $H \subset G$ taková, že $|H| = p$. Toto tvrzení bylo kolem roku 1872 rozšířeno norským matematikem Ludwigem Sylowem:

Věta (Sylowova). *Je-li p prvočíslo a p^k dělí $|G|$ pro nějaké $k \geq 0$ celé, pak existuje podgrupa $H \subset G$ řádu p^k .*

Alternující grupa A_5 je neabelovská grupa všech sudých permutací z pěti prvků. Podle Sylowovy věty má podgrupy řádu 2, 3, 4 a 5, protože $|A_5| = 5!/2 = 60 = 2^2 \cdot 3 \cdot 5$. Nemá ale podgrupy řádu 15 ani 30 (tj. Lagrangeovu větu nelze obrátit). Poznamenejme ještě, že A_5 je izomorfní s grupou všech přímých symetrií pravidelného dvanáctistěnu (též molekuly fullerenu C_{60} či klasického fotbalového míče).

4. Klasifikace jednoduchých grup

Pro jednoduchost budeme symbol binární operace \circ nadále vynechávat. Podgrupa $H \subset G$ se nazývá *normální*, jestliže $g^{-1}hg \in H$ pro všechna $h \in H$ a $g \in G$. V tomto případě budeme psát $H \triangleleft G$, pokud $H \neq G$.

Například $\{e\} \triangleleft A_3 \triangleleft S_3$, protože alternující grupa A_n je normální podgrupou symetrické grupy S_n pro každé $n = 1, 2, \dots$. Také grupa Rubikovy kostky $3 \times 3 \times 3$ obsahuje normální podgrupu, která se skládá z operací pouze na 8 vrcholových kostičkách (viz [21, s. 49, 135], [25]). Na druhé straně podgrupa A_5 grupy A_6 není normální (jak bude patrné z Galoisovy věty).

Definice. Grupa G se nazývá *jednoduchá*, jestliže $\{e\}$ a G jsou její jediné normální podgrupy.

Protože všechny cyklické grupy C_n jsou abelovské a všechny podgrupy abelovské grupy jsou normální, jednoduché cyklické grupy mají prvočíselný řád. Cyklické grupy s neprvočíselným řádem nejsou jednoduché, kromě případu C_1 . Rovněž dihedralní grupa D_n přímých symetrií pravidelného n -bokého hranolu není jednoduchá pro žádné přirozené $n > 2$.

Pojem „jednoduchá grupa“ také pochází od Galoise, který takto nazval grupy sudých permutací A_n pro $n \geq 5$.

Věta (Galoisova). *Alternující grupa A_n je jednoduchá pro $n \geq 5$.*

Důkaz je uveden v např. v [13, s. 98], [17, s. 542]. Jak již bylo řečeno v kapitole 3, grupa A_5 má několik vlastních netriviálních podgrup. Žádná z nich ale není normální.

Jednoduché grupy tvoří jakési stavební kameny všech grup podobně jako chemické prvky, resp. prvočísla jsou stavebními kameny molekul, resp. přirozených čísel větších než jedna. Jestliže G_2 je maximální vlastní normální podgrupa grupy G_1 , pak podílová grupa $G_1/G_2 = \{gG_2 : g \in G_1\}$ je jednoduchá. Je-li podobně G_3 maximální vlastní

normální podgrupa G_2 , pak G_2/G_3 je také jednoduchá. Tímto způsobem můžeme pokračovat, až dojdeme k $G_{n+1} = \{e\}$. Grupu G lze takto vyjádřit pomocí n jednoduchých grup $G_1/G_2, G_2/G_3, \dots, G_n/G_{n+1}$ a podle Jordanovy-Hölderovy věty z roku 1889 tyto grupy nezávisí na výše uvedené volbě pořadí normálních podgrup (viz [11, s. 249], [13], [15, s. 112]):

Věta (Jordanova-Hölderova). *Nechť grupu G lze rozložit dvěma způsoby ve tvaru $\{e\} = G_{n+1} \triangleleft \dots \triangleleft G_2 \triangleleft G_1 = G$ a $\{e\} = H_{m+1} \triangleleft \dots \triangleleft H_2 \triangleleft H_1 = G$ tak, že každá grupa v obou řetězcích je maximální vlastní normální podgrupou grupy následující. Pak $n = m$ a existuje permutace⁵⁾ π prvků $1, \dots, n+1$ taková, že G_i/G_{i+1} je izomorfní $H_{\pi(i)}/H_{\pi(i+1)}$ pro $i = 1, \dots, n$.*

Mnoho problémů z teorie grup tak lze pomocí indukce převést na úlohy zahrnující jednoduché grupy. Nejmenší jednoduchá nekomutativní grupa je A_5 . Grupy A_1 a A_2 jsou triviální, grupa A_3 je komutativní a izomorfní cyklické grupě řádu 3 a grupa A_4 je sice nekomutativní, ale může být rozložena na dvě abelovské podílové grupy (viz [11, s. 244]). Galois pracoval s grupou S_5 permutací kořenů rovnice pátého stupně, která obsahuje jednoduchou grupu A_5 a nemůže být tedy dále rozložena na cyklické grupy prvočíselných řádů.

Každá jednoduchá grupa patří do jedné z 18 nekonečných (ale spočetných) tříd konečných grup nebo do zvláštní konečné třídy tzv. *sporadických grup*, které nepatří do žádné z těchto 18 nekonečných tříd a kterých je právě 26 (viz tab.). Budeme se jim věnovat v kapitole 5.

Klasifikační věta. *Je-li G jednoduchá grupa, pak patří do právě jedné z následujících skupin:*

- 1) třídy cyklických grup C_p prvočíselného řádu p a řádu 1,
- 2) třídy alternujících grup A_n pro $n \geq 5$,
- 3) 16 nekonečných tříd Lieova typu,⁶⁾
- 4) třídy 26 sporadických grup.

Celková délka důkazu této věty se odhaduje na 15 000 stránek. Klasifikační věta je totiž založena na pěti stech článcích od přibližně 100 autorů, v nichž se podrobně vyšetřují jednotlivé třídy a jejich speciální případy. Samozřejmě vzniká otázka, zda je takto dlouhý důkaz bezchybný. O jedné mezeře v důkazu, kterou se již podařilo zaplnit, pojednává článek [2].

Daniel Gorenstein (zemřel v r. 1992) inicioval projekt, který by důkaz Klasifikační věty zkrátil a dal jej do jednotného stylu. Projektu se ujali Richard Lyons a Ronald Solomon, kteří postupně jednotlivé části důkazu Klasifikační věty zasílají k publikaci do Amer. Math. Soc. Celý důkaz bude systematicky podán v mnoha dílech, z nichž 6 již bylo vydáno. Odhaduje se, že počet stránek tentokrát nepřesáhne 4000.

⁵⁾ Zřejmě $\pi(1) = 1$ a $\pi(n+1) = n+1$.

⁶⁾ Lieovy grupy popisují různé typy geometrií, viz [14], [16], [20]. Šestnáct tříd Lieova typu obsahuje např. speciální konečné podgrupy unitárních, symplektických či ortogonálních grup (viz [10]). Jako konkrétní příklad uveďme grupy symetrií vícerozměrných krychlí.

Díky Jordanově-Hölderově větě a dalším hlubokým výsledkům se podařilo ukončit klasifikaci jednoduchých grup kolem roku 1982. John H. Conway⁷⁾ inicioval projekt „Atlas“ popisující všechny konečné grupy, který je zveřejněn v [6]. Obsáhlý historický přehled o tomto vysoce netriviálním výsledku je podán např. v [9] a [21].

V roce 1904 William Burnside dokázal velmi překvapivou větu (viz [3]):

Věta (Burnsidova). *Žádná jednoduchá grupa nemá řád $p^k q^m$, kde p a q jsou různá prvočísla a $k, m \geq 1$ celá.*

Pokud tedy jednoduchá grupa není cyklická, musí být její řád dělitelný alespoň třemi prvočíslly. Např. řád grup A_5 , A_6 a některých jednoduchých grup Lieova typu je dělitelný právě třemi různými prvočíslly (druhá nejmenší jednoduchá neabelovská grupa má řád $168 = 2^3 \cdot 3 \cdot 7$). Burnside též dokázal, že každá grupa řádu p^2 je abelovská, je-li p prvočísllo (viz [17, s. 531]). Grupa řádu p^3 ale může být neabelovská, je-li p liché prvočísllo. Např. existují dvě neabelovské grupy řádu $3^3 = 27$.

5. Sporadické grupy

Největší sporadická grupa se nazývá *Monstrum* a označuje se M . Jde o zcela výjimečný matematický objekt. Jeho existenci předpověděli v roce 1973 na sobě nezávisle Bernd Fischer a Robert L. Griess. Proto se M někdy také nazývá Fischerovo-Griessovo monstrum. Griess z univerzity v Michiganu jej pak v roce 1983 zkonstruoval jako konečnou grupu rotací v eukleidovském prostoru \mathbb{R}^{196883} . Řád M je vskutku úctyhodný,

$$\begin{aligned} |M| &= 808017424794512875886459904961710757005754368000000000 & (1) \\ &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71. \end{aligned}$$

Cesta ke konstrukci Monstra však byla značně dlouhá a klikatá. První sporadické grupy M_n pro $n = 11, 12, 22, 23, 24$ objevil francouzský matematik Émile L. Mathieu v období 1861–1873. Jsou to zvláštní podgrupy grupy všech permutací S_n , které nepatří do žádné z 18 nekonečných tříd jednoduchých grup. Grupa M_{24} byla objevena jako první v roce 1861.

Nejnsázze zkonstruovatelná sporadická grupa je však M_{12} . Její řád

$$|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040 \quad (2)$$

je sice větší⁸⁾ než $|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8$, ale lze ji definovat pomocí pouhých tří generátorů g_1, g_2, g_3 . Do M_{12} patří všechny permutace, které lze dostat složením konečného počtu

⁷⁾ Conway je také autorem známého algoritmu Life, který simuluje evoluci bakterií ve čtvercové síti.

⁸⁾ Grupa M_{11} je stabilizátorem grupy M_{12} , podrobnosti viz [25, s. 168–170].

následujících permutací (viz [25, s. 166]):

$$g_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 1 & 12 \end{bmatrix},$$

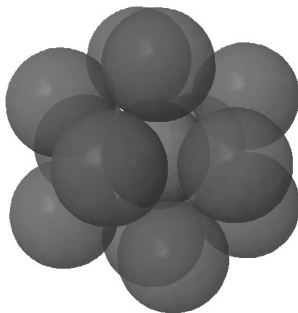
$$g_2 = \begin{bmatrix} 1 & 12 & 2 & 11 & 3 & 6 & 4 & 8 & 5 & 9 & 7 & 10 \\ 12 & 1 & 11 & 2 & 6 & 3 & 8 & 4 & 9 & 5 & 10 & 7 \end{bmatrix},$$

$$g_3 = \begin{bmatrix} 1 & 2 & 3 & 7 & 11 & 8 & 9 & 10 & 5 & 6 & 4 & 12 \\ 1 & 2 & 7 & 11 & 8 & 3 & 9 & 5 & 6 & 4 & 10 & 12 \end{bmatrix}.$$

Lze dokázat, že M_{12} neobsahuje žádnou transpozici ani trojcyklus. Tato grupa je ale 5-tranzitivní,⁹⁾ tj. pro libovolných pět různých prvků i_1, i_2, i_3, i_4, i_5 a dalších pět libovolných různých prvků j_1, j_2, j_3, j_4, j_5 z množiny $\{1, 2, \dots, 12\}$ existuje permutace $s \in M_{12}$ taková, že $s(i_k) = j_k$ pro $k = 1, 2, 3, 4, 5$. Všimněte si také, že řád M_{12} ve vztahu (2) je roven právě počtu možností, jak vybrat 5 prvků z dvanácti, pokud záleží na pořadí.

Termín sporadická grupa se poprvé objevil v práci [4, s. 504] z roku 1911, kde se o Mathieuových grupách píše: *These apparently sporadic simple groups would probably repay a closer examination than they have yet received.* Podle Burnsidovy věty musí být řád každé sporadické grupy číslo složené z vícera prvočinitelů (srov. tab.).

V roce 1965, tj. přibližně sto let po objevu prvních pěti sporadických grup M_i , objevil chorvatský matematik Zvonimír Janko šestou sporadickou grupu označovanou jako J_1 . Existence dalších sporadických grup byla často předpovězena dříve, než byla příslušná grupa zkonstruována. Většina sporadických grup se tak nazývá po autorech, kteří jejich existenci pouze předpověděli. Jde přibližně o období 1965–1975.



Obr. 4. Dvanáct koulí obklopujících centrální kouli v třírozměrném prostoru.

Několik sporadických grup bylo zkonstruováno pomocí tzv. Leechovy mřížky (viz [23]). Při nejhustším uspořádání stejně velkých kruhů v rovině se každý kruh dotýká svých šesti sousedů. Pro pravidelná periodická uspořádání stejně velkých koulí v d -rozměrném prostoru označme maximální počet dotyků vybrané centrální koule se sousedními koulemi symbolem $K(d)$ (angl. *kissing number*). Pak $K(1) = 2$, $K(2) = 6$, $K(3) = 12$ (viz obr. 4), $K(4) = 24$ a $K(8) = 240$. Pro ostatní d jsou známy jen hrubé

⁹⁾ Každá 6-tranzitivní grupa je už buď symetrická, nebo alternující (viz [25]).

Angl. jméno	označení	řád
Mathieu	M_{11}	$7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$
	M_{12}	$95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$
	M_{22}	$443520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
	M_{23}	$10200960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
	M_{24}	$244823040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
Janko	J_1	$175560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
	J_2	$604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
	J_3	$50232960 = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
	J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
Higman-Sims	HS	$44352000 = 2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
McLaughlin	Mc	$898128000 = 2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
Held	He	$4030387200 = 2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
Suzuki	Sz	$448345497600 = 2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
Rudvalis	Ru	$145926144000 = 2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
O’Nan	ON	$460815505920 = 2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
Lyons	Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
Conway	Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
	Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
	Co_3	$495766656000 = 2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Fischer	Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
	Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
	Fi_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
Harada-Norton	HN	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
Thompson	Th	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
Baby Monster	B	$ B \approx 4 \cdot 10^{34}$ viz (3)
Monster	M	$ M \approx 8 \cdot 10^{54}$ viz (1)

Tab. Sporadické grupy.

dolní a horní odhady $K(d)$, kromě případu $d = 24$, kdy je horní odhad roven dolnímu, tj. $K(24) = 196560$ (viz [18], [21, s. 242]).

V 60. letech minulého století se John Leech inspiroval 5-tranzitivní Mathieuovou grupou M_{24} , v níž se permutuje 24 prvků tak, že libovolných pět různých z nich se současně zamění za obecně jiných pět různých prvků předem daných. V eukleidovském prostoru \mathbb{R}^{24} zkonstruoval speciální pravidelnou mřížku středů koulí, které dávají nejhustší uspořádání, kdy je centrální koule obklopena právě 196560 dotýkajícími se koulemi. Symetrie Leechovy mřížky v \mathbb{R}^{24} umožňují zkonstruovat celkem 12 sporadických grup.¹⁰⁾ Některé z nich našly uplatnění v teorii samoopravných kódů (viz [23]), v teorii strun a supergravitace.

¹⁰⁾ Jsou to J_2 , HS , Mc , Sz a dále všechny Mathieuovy a Conwayovy grupy (viz [7], [21, s. 155]).

6. Thompsonův a Titsův přínos k teorii neabelovských grup

Oba noví laureáti Abelovy ceny se podstatně zasloužili o některé části důkazu Klasifikační věty jednoduchých grup (viz [26]). Již v roce 1963 Walter Feit a John G. Thompson publikovali článek [8], který na 255 stránkách přináší důkaz tehdy 60 let staré Burnsidovy domněnky pro jednoduché neabelovské grupy:

Věta (Feitova-Thompsonova). *Každá jednoduchá neabelovská grupa má sudý řád.*

Na druhé straně jediné jednoduché abelovské grupy jsou C_p , kde p je prvočíslo nebo $p = 1$, tj. řád jednoduché grupy C_p je lichý, když $p \neq 2$. Každá grupa s lichým řádem má normální podgrupu a podle Jordanovy-Hölderovy věty může být rozložena pouze na cyklické podílové grupy. Jako netriviální důsledek předchozí věty tak dostáváme (viz [8]):

Věta. *Každou grupu lichého řádu alespoň 3 lze rozložit na jednoduché abelovské grupy prvočíselného řádu.*

Thompson zkonstruoval sporadickou grupu označovanou Th , jejíž řád je $|Th| \approx \approx 9 \cdot 10^{16}$ (viz tab. a obr. 5). Pomohl také svému mladšímu kolegovi J. H. Conwayovi při konstrukci sporadické grupy Co_1 a vypočítal řád některých dalších grup (viz např. [21, s. 153, 184]). Thompson objevil i dvě nové nekonečné grupy označované T a V . Databáze MathSciNet eviduje přes 250 Thompsonových prací především z teorie grup.

Jacques Tits se již od mládí zajímal o Lieovy grupy s konečným řádem. Objevil nové nekonečné třídy takových grup současně (ale nezávisle) s Robertem Steinbergem z Kalifornie. Studoval také grupy symetrií krystalů a pravidelných těles ve vícerozměrných prostorech.¹²⁾ Tzv. Titsova grupa, kterou objevil, má řád $17971200 = 2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$ a patří ke grupám Lieova typu.

Jacques Tits (a nezávisle též Marshall Hall) explicitně zkonstruoval Jankovu grupu J_2 , což je speciální sporadická grupa permutací 100 symbolů (viz tab.). Přitom použil čistě geometrické úvahy. Je autorem známé monografie [24].

Tits také poněkud zjednodušil Griessovu konstrukci Monstra (viz [21, s. 209]). Další zjednodušení se popisuje v článku [5].

Podle prohlášení výběrové komise *Thompson způsobil převrat v teorii konečných grup tím, že dokázal nesmírně obtížné věty, které vedly k položení základů pro úplnou klasifikaci konečných grup, jednoho z největších výsledků matematiky 20. století.*

Tits vytvořil nový a velmi účelný pohled na grupy jako geometrické objekty. Zavedl matematický objekt, který je znám jako Titsova konstrukce (angl. Tits building), jež vyjadřuje algebraickou strukturu lineárních grup v geometrických termínech.

Poznámka. Pokud vám v hlavě stále vrtá paradox z obr. 3 vpravo, pak vám napovíme, že je třeba zaměnit dvě nerozlišitelná R v prvním a druhém řádku.

¹²⁾ Poznamenejme, že nový Vítězný oblouk v La Défense v Paříži je „projekcí“ čtyřrozměrné krychle do trojrozměrného prostoru.

Poděkování. Autoři děkují doc. F. Katrnoškovi, prof. O. Kowalskému, dr. M. Marklovi, dr. V. Pravdovi, prof. A. Pultrovi a dr. V. Vopravilovi za cenné připomínky. Práce byla podpořena granty IAA 100190803 GA AV ČR a 1P05ME749 MŠMT.

L i t e r a t u r a

- [1] ABEL, N. H.: *Mémoire sur les équations algébriques où on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré*, Goendahl, Christiana 1824.
- [2] ASCHBACHER, M.: *The status of the classification of the finite simple groups*, Notices Amer. Math. Soc. 51 (2004), 736–740.
- [3] BURNSIDE, W.: *On groups of order $p^\alpha q^\beta$* , Proc. London Math. Soc. 2 (1904), 388–392.
- [4] BURNSIDE, W.: *Theory of groups of finite order*, Cambridge 1911, Dover Publ., New York 1955 (reprinting 2004).
- [5] CONWAY, J. H.: *A simple construction of the Fischer-Griess monster group*, Invent. Math. 79 (1985), 513–540.
- [6] CONWAY, J. H., CURTIS, R. T., NORTON, S. P., PARKER, R. A., WILSON, R. A.: *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups*, Oxford Univ. Press 1985.
- [7] CONWAY, J. H., SLOANE, N. J. A.: *Sphere packing, lattices and groups*, Springer, Berlin 1988.
- [8] FEIT, W., THOMPSON, J. G.: *Solvability of groups of odd order*, Pacific J. Math. 13 (1963), 775–1029.
- [9] GALLIAN, J. A.: *The search for finite simple groups*, Math. Magazine 49 (1976), 163–180.
- [10] HALL, B. C.: *Lie groups, Lie algebras, and representations*, Springer-Verlag, New York 2003.
- [11] JACOBSON, C.: *Basic algebra I, 2nd ed.*, W. H. Freeman and Company 1985.
- [12] JORDAN, C.: *Traité des substitutions*, Gauthier-Villars, Paris 1870.
- [13] KARGAPOLOV, M. I., MERZJAKOV, JU. I.: *Osnovy teorii grupp*, 2. vyd., Nauka, Moskva 1977.
- [14] KARGER, A., NOVÁK, J.: *Prostorová kinematika a Lieovy grupy*, SNTL, Praha 1987.
- [15] KUROŠ, A. G.: *Kapitoly z obecné algebry*, Academia, Praha 1968.
- [16] LITZMAN, O., SEKANINA, M.: *Užití grup ve fyzice*, Academia, Praha 1982.
- [17] MAC LANE, S., BIRKHOFF, G.: *Algebra*, Alfa, Bratislava 1973.
- [18] PFENDER, F., ZIEGLER, G. M.: *Kissing numbers, sphere packings, and some unexpected proofs*, Notices Amer. Math. Soc. 51 (2004), 873–883.
- [19] PRADLOVÁ, J., KŘÍŽEK, M.: *Grupy kolem nás*, Rozhledy mat.-fyz. 76 (1999), 209–216, 261–267; 77 (2000), 5–12.
- [20] PRAVDA, V.: *Maticové Lieovy grupy a Lieovy algebry*, PMFA 52 (2007), 219–230.
- [21] RONAN, M.: *Symmetry and the Monster. One of the greatest quests of mathematics*, Oxford Univ. Press 2006.
- [22] SYLOW, L., LIE, S.: *Œuvres complètes de Niels Henrik Abel, vol. I, II.*, Nouvelle Edition, Oslo 1881.
- [23] THOMPSON, T. M.: *From error-correcting codes through sphere packing to simple groups*, Math. Assoc. Amer., Washington 1983.
- [24] TITS, J.: *Buildings of spherical type and finite BN-pairs*, LN in Math. 386, Springer, New York 1974.
- [25] TŮMA, J.: *Matematické hlavolamy a základy teorie grup*, Mladá fronta, Praha 1988.
- [26] <http://www.abelprisen.no/en/>