Vlastimil Pták
O větě Frobeniově

Časopis pro pěstování matematiky, Vol. 78 (1953), No. 3, 207--212

Persistent URL: http://dml.cz/dmlcz/117090

Časopis pro pěstování matematiky, roč. 78 (1953)

O VĚTĚ FROBENIOVĚ

VLASTIMIL PTÁK, Praha.

(Došlo 19. ledna 1953.) DT: 519.41/.47

Autor vyšetřuje některé vlastnosti n-tých mocnin v konečné grupě a ukazuje, jak lze pomocí nich jednoduše dokázat Frobeniovu větu o počtu n-tých odmocnin daného prvku.

Před několika lety vznikl na přírodovědecké fakultě Karlovy university kroužek posluchačů matematiky, který si vzal za úkol prostudovat známou knihu: ZASSENHAUS, *Lehrbuch der Gruppentheorie*. Ukázalo se při tom, že na mnohých místech lze důkazy zjednodušit a výklad učinit přístupnějším. Úkolem tohoto článku jest podati jednoduchý důkaz věty Frobeniovy o počtu n-tých odmocnin daného prvku v konečné grupě.

Původní důkaz, uvedený ve zmíněné již učebnici Zassenhausově, je málo srozumitelný, neboť v podstatě používá trojí úplné indukce.

Ukážeme, že věta Frobeniova spočívá na dvou velmi jednoduchých vlastnostech n-tých mocnin v konečné grupě. Užívajíce těchto vlastností, dospějeme k větě Frobeniově užitím jediné indukce. Při důkazu budeme užívat několika velmi jednoduchých úsudků. Aby se důkaz nestal nepřehledným, jsou shrnuty v předběžné části článku. Uvádíme je pro pohodlí čtenáře i s důkazy přes to, že jsou téměř triviální.

§ 1. Označení a pomocné věty.

Budiž G konečná grupa řádu N. Je-li K libovolná část grupy G a n dané přirozené číslo, označíme

$$\mathfrak{A}(G; K, n) = \mathfrak{A}(K, n) = \underset{x}{E}[x \in G,\ x^n \in K] .$$

Počet prvků množiny $\mathfrak{A}(G; K, n)$ označíme $A(G; K, n)$. Cyklickou grupu vytvořenou prvkem x označíme $\{x\}$, řád prvku x označíme $o(x)$. Index podgrupy K v podgrupě H značíme $[H : K]$, normalisátor prvku v značíme $N(v)$. Centrum grupy G budeme značiti $C(G)$.

Nejprve si odvodíme jednoduchou relaci mezi řádem prvku x a řádem jeho n-té mocniny. Bude nám později užitečná pro stanovení řádu prvku x, který splňuje rovnost $x^n = c$, známe-li řád prvku c.

(1,1). *Nechť $x \in G$, n je přirozené číslo. Potom platí*

$$o(x) = (n, o(x)) \,.\, o(x^n) \,.$$

Důkaz: Označme $k = o(x)$ a pišme nejprve $k = (k, n) \,.\, k'$, $n = (k, n) \,.\, n'$, takže k' a n' budou nesoudělná. Máme potom

$$(x^n)^{k'} = x^{(k,n)n'k'} = x^{kn'} = 1 \,,$$

takže $o(x^n) | k'$. Budiž naopak m přirozené číslo takové, že platí $(x^n)^m = 1$. Odtud plyne $k | nm$. Po krácení faktorem (k, n) dostáváme $k' | n'm$. Protože však $(k', n') = 1$, musí $k' | m$. Jest tedy $o(x^n) = k'$, odkud ihned plyne tvrzení věty dosazením do relace $k = (k, n) \,.\, k'$.

Uveďme ještě následující důsledky právě dokázané relace ve dvou krajních případech:

(1,11). *Jestliže přirozené číslo n je nesoudělné s řádem prvku x, potom x^n má stejný řád jako x.*

(1,12). *Nechť prvek x má řád k. Jestliže $k = k_1 k_2$, potom prvek x^{k_1} má řád k_2.*

(1,2). *Nechť $x \in G$, $c \in G$, n je přirozené a nechť platí $x^n = c$. Nechť dále n a $o(c)$ mají následující vlastnost: pro každé prvočíslo p platí implikace*

$$p \mid n \quad \Rightarrow \quad p \mid o(c) \,.$$

Potom jest $o(x) = n \,.\, o(c)$.

Důkaz: Máme rozklad

$$o(x) = (n, o(x)) \,.\, o(c) \,,$$

$$n = (n, o(x)) \,.\, n' \,,$$

při čemž čísla $o(c)$ a n' jsou nesoudělná. Kdyby nyní existovalo prvočíslo p tak, že $p | n'$, bylo by $p | n$ a tedy podle našeho předpokladu též $p | o(c)$. To však není možné, neboť n' a $o(c)$ jsou nesoudělná. Jest tedy $n' = 1$, takže $(n, o(x)) = n$, odkud plyne $o(x) = n \,.\, o(c)$.

(1,3). *Je-li $u = gtg^{-1}$, jest $A(u, n) = A(t, n)$.*

Důkaz: Jest zřejmě $\mathfrak{A}(u, n) = g\mathfrak{A}(t, n)\, g^{-1}$.

(1,4). *Budiž T množina všech prvků konjugovaných s prvkem t. Potom platí*

$$A(T, n) = [G : N(t)] \,.\, A(t, n) \,.$$

Důkaz: Jest zřejmě $\mathfrak{A}(T, n) = \bigcup_{s \in T} \mathfrak{A}(s, n)$ s disjunktními sčítanci. Odtud $A(T, n) = \sum_{s \in T} A(s, n)$. Podle předešlé věty pro každé $s \in T$ platí $A(s, n) = A(t, n)$. Číslo $A(T, n)$ je tedy rovno součinu čísla $A(t, n)$ s počtem prvků množiny T, který je roven $[G : N(t)]$.

(1,5). *Platí rovnost*

$$\mathfrak{A}(G; c, n) = \mathfrak{A}(N(c); c, n) \,.$$

Důkaz: Skutečně, jestliže $x \in G$ splňuje rovnost $x^n = c$, platí

$$xc = xx^n = x^n x = cx ,$$

odkud plyne, že x leží v normalisátoru prvku c. Tím je věta dokázána.

V dalším se nám často vyskytne následující situace: jsou dána dvě přirozená čísla n a r. Uvažme kanonický rozklad čísla n

$$n = p_1^{e_1} \dots p_m^{e_m}$$

(to tedy znamená, že e_i jsou *přirozená* čísla a prvočísla $p_1, \dots, p_m$ jsou všechna *od sebe různá*). Utvořme nyní součin všech faktorů $p_i^{e_i}$ pro ta prvočísla p_i, pro něž $(p_i, r) = 1$. Označme tento součin l. (Může se pochopitelně stát, že žádné takové prvočíslo neexistuje; máme potom prázdný součin, neboli $l = 1$). Podobně označme k součin oněch faktorů $p_i^{e_i}$, pro něž $p_i | r$. Máme tedy rozklad $n = lk$. Budeme říkat, že jsme provedli rozklad čísla n podle čísla r. Čísla l a k budeme nazývat nesoudělnou, resp. soudělnou částí tohoto rozkladu.

(**1,6**). *Nechť* $c \in G$, n *je přirozené číslo. Nechť* l *a* k *znamenají resp. nesoudělnou a soudělnou část rozkladu čísla* n *podle čísla* $o(c)$. *Potom*

$$k | A(c, n) .$$

Důkaz: Tvrzení věty je správné, jestliže $A(c, n) = 0$. Nechť tedy existuje $x \in G$ tak, že $x^n = c$. Vypočtěme si nejprve $o(x)$.

Podle definice čísla k platí implikace

$$p | k \Rightarrow p | o(c) .$$

Protože zřejmě $o(c) | o(x^k)$, platí též

$$p | k \Rightarrow p | o(x^k) .$$

Podle věty (**1,2**) vyplývá odtud ihned

$$o(x) = k \,.\, o(x^k) .$$

Protože dále $(x^k)^l = c$, máme

$$o(x^k) = (l, o(x^k))\, o(c) .$$

Dosazením do předešlé rovnosti dostáváme tedy, že $o(x)$ je dělitelno dokonce součinem $k.o(c)$.

V dalším zavedeme pro stručnost označení $o(c) = r$.

Nechť nyní $x \in \mathfrak{A}(c, n)$. Právě jsme dokázali, že potom $o(x) = tkr$ pro vhodné t. Označme $M(x)$ třídu grupy G podle podgrupy $\{x^{tr}\}$, určenou prvkem x. Dokážeme, že

$$M(x) \subset \mathfrak{A}(c, n) .$$

Skutečně, pro libovolné přirozené j platí

$$(x^{1+jtr})^n = c \,.\, x^{jtrn} = c \,.\, x^{jl.tkr} = c .$$

Množina $M(x)$ má stejný počet prvků jako podgrupa $\{x^{tr}\}$, tedy právě k.

Každému $x \in \mathfrak{A}(c, n)$ je tedy přiřazena jistá množina $M(x)$ o k prvcích taková, že $x \in M(x) \subset \mathfrak{A}(c, n)$. Dokážeme-li, že dvě takové skupiny jsou buď disjunktní nebo totožné, bude tím $\mathfrak{A}(c, n)$ rozdělena do skupin o k prvcích a tvrzení naší věty bude tedy dokázáno.

Nechť tedy x_1 a x_2 jsou dva prvky takové, že $x_1 \in M(x_2)$, $x_2 \in \mathfrak{A}(c, n)$. Existují tedy t_i tak, že $o(x_i) = t_i kr$. Množiny $M(x_i)$ jsou třídy grupy G podle podgrup $\{x_i^{t_i r}\}$. Abychom dokázali rovnost $M(x_1) = M(x_2)$, stačí tedy dokázat rovnost

$$\{x_1^{t_1 r}\} = \{x_2^{t_2 r}\} .$$

To však snadno plyne z následující úvahy. Jest především $x_1 \in \{x_2\}$, tedy též $x_1^{t_1 r} \in \{x_2\}$, takže $\{x_1^{t_1 r}\}$ jest podgrupou řádu k v cyklické grupě $\{x_2\}$. Musí tedy být totožná s $\{x_2^{t_2 r}\}$. Tím je důkaz naší věty úplně dokončen.

(**1,7**). *Budiž M podgrupa řádu m, $M \subset C(G)$. Nechť l je přirozené číslo nesoudělné s m. Potom pro každé $y \in G$ jest*

$$A(G; y, l) = A(G/M; y, l) .$$

Důkaz: Pro $u \in M$ zobrazení $\lambda(u) = u^l$ jest automorfismem grupy M. Označme si $\mathfrak{A}(G; y, l) = \mathfrak{A}$, $\mathfrak{A}(G/M; y, l) = \mathfrak{A}_M$. Pro $x \in \mathfrak{A}$ položme $\tau(x) = xM \in \mathfrak{A}_M$. Tím jest definováno jisté zobrazení $\mathfrak{A}$ do $\mathfrak{A}_M$. Dokažme, že $\tau(\mathfrak{A}) = \mathfrak{A}_M$. Vskutku, budiž $zM \in \mathfrak{A}_M$. Potom $z^l c = y$ pro vhodné $c \in M$, ale v M každý prvek jest l-tou mocninou, tedy $c = d^l$, $d \in M$, tedy

$$(zd)^l = z^l c = y ,$$

takže $zd \in \mathfrak{A}$, $\tau(zd) = zM$. Dokážeme ještě, že zobrazení τ jest prosté. Nechť tedy $x_1, x_2 \in \mathfrak{A}$ a platí $\tau(x_1) = \tau(x_2)$. Potom $x_2 = x_1 c$ pro vhodné $c \in M$, takže $y = x_2^l = x_1^l c^l = y c^l$. Jest tedy $c^l = 1$, odkud $c = 1$, takže $x_1 = x_2$. Tím je naše tvrzení úplně dokázáno.

§ 2. Věta Frobeniova.

(**2,1**). *Buď G konečná grupa řádu N. Nechť n je přirozené číslo. Buď T množina všech prvků konjugovaných s daným prvkem $g \in G$; počet prvků T buď h. (Tedy $h = [G : N(g)]$).*

Potom platí

$$(hn, N) | A(T, n) .$$

Důkaz provedeme indukcí podle řádu grupy G.

Pro jednotkovou grupu je věta zřejmě správná. Nechť tedy G není jednotková a nechť věta je správná pro všechny grupy řádu menšího.

Budeme rozeznávati tři případy:

1. g non $\in C(G)$,
2. $g \in C(G)$, $g \neq 1$,
3. $g = 1$.

1. Nechť g non $\epsilon C(G)$. V tomto případě normalisátor $N(g)$ je vlastní podgrupou grupy G. Protože $h = [G : N(g)]$, máme podle **(1,4)**

$$A(T, n) = hA(g, n) . \tag{1}$$

Podle **(1,5)** platí však

$$A(G; g, n) = A(N(g); g, n) .$$

Použijme nyní idnukčního předpokladu na grupu $N(g)$. Pro řád N' grupy $N(g)$ zřejmě platí $N = h . N'$. Všimneme-li si, že $g \epsilon C(N(g))$, dostaneme podle indukčního předpokladu

$$(n, N') | A(g, n) . \tag{2}$$

Vynásobíme-li tuto relaci číslem h a použijeme-li rovnosti (1), dostaneme

$$(hn, N) = h(n, N') \mid hA(g, n) = A(T, n) ,$$

což bylo dokázati.

2. Nechť $g \epsilon C(G)$, $g \neq 1$. Nechť l a k znamenají opět nesoudělnou resp. soudělnou část rozkladu čísla n podle $o(g)$. Podle věty **(1,6)** máme potom

$$k \mid A(g, n) . \tag{3}$$

Protože $n = lk$, platí

$$\mathfrak{A}(g, n) = \mathfrak{A}(\mathfrak{A}(g, k), l) . \tag{4}$$

Všimněme si nyní, že množina $\mathfrak{A}(g, k)$ obsahuje s každým prvkem zároveň všechny prvky s ním konjugované. Skutečně, jestliže $y \epsilon \mathfrak{A}(g, k)$, potom pro každé $s \epsilon G$

$$(sys^{-1})^k = sy^k s^{-1} = sgs^{-1} = g .$$

Můžeme tedy celou množinu $\mathfrak{A}(g, k)$ rozložit na třídy konjugovaných prvků

$$\mathfrak{A}(g, k) = T_1 \cup \ldots \cup T_s .$$

Odtud a z relace (4) vyplývá potom

$$A(g, n) = \sum_i A(T_i, l) . \tag{5}$$

Uvažme nejprve sčítance $A(T_i, l)$, příslušné třídám T_i, které obsahují více než jeden prvek. Potom můžeme užít výsledku dosaženého v první části důkazu. Dostáváme tedy pro tyto třídy

$$(l, N) \mid A(T_i, l) .$$

Zbývá vyšetřit případ, kdy třída T_i se skládá z jediného prvku y. Musí tedy $y \epsilon C(G)$.

Označme M cyklickou grupu vytvořenou prvkem y. Řád m grupy M je nesoudělný s l, neboť vzhledem k rovnosti $y^k = g$ máme podle **(1,2)**

$$m = o(y) = k . o(g) .$$

Grupa M není jednotková, neboť $y^k = g$ a g jest různé od 1.

Podle věty **(1,7)** máme potom

$$A(y, l) = A(G/M; y, l) .$$

Protože M není jednotková, je řád grupy G/M menší než N, takže užitím indukčního předpokladu na grupu G/M dostáváme

$$(l, N/m) \mid A(y, l) .$$

Protože však $(m, l) = 1$, jest

$$(l, N) = (l, N/m) \mid A(y, l) .$$

Dokázali jsme tedy, že pro každé i platí

$$(l, N) \mid A(T_i, l) .$$

Odtud a z relace (5) vyplývá

$$(l, N) \mid A(g, n) . \tag{6}$$

Nyní stačí si vzpomenout, že $n = lk$, při čemž čísla l a k jsou nesoudělná. Z (3) a (6) výplyne pak žádaný výsledek

$$(n, N) \mid A(g, n) .$$

3. Zbývá případ $g = 1$. Budiž

$$G = T_1 \cup \ldots \cup T_s$$

rozklad grupy G ve třídy konjugovaných prvků, při čemž nechť označení je tak voleno, že třída T_1 se skládá právě z prvku 1. Jest dále

$$G = \bigcup_i \mathfrak{A}(T_i, n)$$

s disjunktními sčítanci, takže

$$N = \sum A(T_i, n) . \tag{7}$$

Budiž $i > 1$. Mohou nastat dva případy. Jestliže třída T_i obsahuje více než jeden prvek, potom podle první části důkazu jest $(n, N) \mid A(T_i, n)$. Skládá-li se třída T_i z jediného prvku y, jest $y \in C(G)$, $y \neq 1$, takže podle druhé části důkazu opět $(n, N) \mid A(T_i, n)$. Ježto zřejmě $(n, N) \mid N$ a platí vztah (7), musí

$$(n, N) \mid A(g, n) .$$

Tím je důkaz úplně dokončen.