Časopis pro pěstování matematiky

Jan Mařík

Překlad grupy do její podgrupy

Časopis pro pěstování matematiky, Vol. 76 (1951), No. 1, 23–34

Persistent URL: http://dml.cz/dmlcz/116996

Terms of use:

© Institute of Mathematics AS CR, 1951

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

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

PŘEKLAD GRUPY DO JEJÍ PODGRUPY

JAN MAŘÍK, Praha.

(Došlo dne 11. VIII. 1950.)

V poslední kapitole *Zassenhausovy* knihy „Lehrbuch der Gruppentheorie (B. G. Teubner, Lipsko-Berlín 1937), nazvané „Verlagerung in eine Untergruppe", je popsána methoda, jak lze v některých grupách najít vlastní normální podgrupy. Touto methodou lze na př. snadno dokázat, že každá jednoduchá grupa řádu lichého a menšího než 5000 má řád prvočíselný. První paragraf uvedené kapitoly je však psán velmi nesrozumitelně; úkolem tohoto článku je vyložit tento paragraf srozumitelněji a doplnit jej. Věty zde uvedené nejsou samy o sobě zvláště zajímavé; mají jen pomocný ráz a používá se jich v dalších paragrafech.

Poznámka 1. Je-li φ zobrazení množiny A do množiny B a je-li $C \subset A$, značí $\varphi(C)$ množinu všech $\varphi(c)$, kde $c \in C$. Obsahuje-li množina $\varphi(C)$ právě jeden prvek, ztotožníme množinu $\varphi(C)$ s prvkem v ní obsaženým.

Poznámka 2. Permutací množiny M nazýváme prosté zobrazení M na M. Mějme nyní zobrazení φ, ψ množiny M do M taková, že platí $\varphi(\psi(m)) = m$ pro každé $m \in M$. Protože $\varphi(\psi(M)) = M$, je tím spíše $\varphi(M) = M$; to znamená, že φ je zobrazení M na M. Je-li $\psi(m_1) = \psi(m_2)$, je $m_1 = \varphi(\psi(m_1)) = \varphi(\psi(m_2)) = m_2$; to znamená, že ψ je zobrazení prosté.*) Existují-li tedy k zobrazení φ zobrazení χ, ψ tak, že pro každé $m \in M$ platí oba vztahy $\varphi(\chi(m)) = m$, $\psi(\varphi(m)) = m$, plyne z prvního vztahu, že φ je zobrazení M na M, z druhého, že φ je zobrazení prosté; pak je tedy φ permutací, $\psi = \chi = \varphi^{-1}$. Máme-li tedy nějakou grupu zobrazení množiny M do M, jsou zobrazení z této grupy jistě permutace.

Věta 1. *Necht jsou splněny tyto předpoklady:*

M je neprázdná množina,

Π je (libovolná) grupa permutací množiny M,

H je grupa,

Φ je množina všech zobrazení M do H.

*) Nijak odtud neplyne, že některé ze zobrazení φ, ψ by musilo být permutací, jak ukazuje tento příklad: Buď M množina všech přirozených čísel; buď $\psi(m) = 2m$, $\varphi(m) = \frac{m}{2}$ resp. $\varphi(m) = \frac{m+1}{2}$ podle toho, je-li m sudé nebo liché. Vidíme ihned, že zobrazení φ, ψ nejsou permutace a že platí $\varphi(\psi(m)) = m$ pro každé přirozené m.

Utvořme množinu $\Pi \times \Phi$ všech dvojic (π, φ), kde $\pi \in \Pi$, $\varphi \in \Phi$. Definujme na množině $\Pi \times \Phi$ operaci takto:

$$(\pi_1, \varphi_1) \cdot (\pi_2, \varphi_2) = (\pi, \varphi),$$

kde prvky π, φ jsou určeny vztahy

$$\begin{aligned} \pi(m) &= \pi_1(\pi_2(m)), \\ \varphi(m) &= \varphi_1(\pi_2(m)) \cdot \varphi_2(m),^{*}) \end{aligned} \qquad (\alpha)$$

Pak je $\Pi \times \Phi$ grupa.

Důkaz. I.

$$[(\pi_1, \varphi_1) \cdot (\pi_2, \varphi_2)] \cdot (\pi_3, \varphi_3) = (\pi, \varphi) \cdot (\pi_3, \varphi_3) = (\pi', \varphi'),$$

kde pro π, φ platí (α) a pro π', φ' platí

$$\begin{aligned} \pi'(m) &= \pi_1(\pi_2(\pi_3(m))), \\ \varphi'(m) &= \varphi(\pi_3(m)) \cdot \varphi_3(m) = \varphi_1(\pi_2(\pi_3(m))) \cdot \varphi_2(\pi_3(m)) \cdot \varphi_3(m) \end{aligned}$$

pro každé $m \in M$.

$$(\pi_1, \varphi_1) \cdot [(\pi_2, \varphi_2), (\pi_3, \varphi_3)] = (\pi_1, \varphi_1) \cdot (\overline{\pi}, \overline{\varphi}) = (\pi'', \varphi''),$$

kde pro $\overline{\pi}, \overline{\varphi}, \pi'', \varphi''$ platí

$$\begin{aligned} \overline{\pi}(m) &= \pi_2(\pi_3(m)), \\ \overline{\varphi}(m) &= \varphi_2(\pi_3(m)) \cdot \varphi_3(m), \\ \pi''(m) &= \pi_1(\pi_2(\pi_3(m))), \\ \varphi''(m) &= \varphi_1(\overline{\pi}(m)) \cdot \overline{\varphi}(m) = \varphi_1(\pi_2(\pi_3(m))) \cdot \varphi_2(\pi_3(m)) \cdot \varphi_3(m) \end{aligned}$$

pro každé $m \in M$.

Vidíme, že $\pi' = \pi''$, $\varphi' = \varphi''$, platí tedy zákon asociativní.

II. Buď j jednotka grupy H. Nechť pro π_0, φ_0 platí

$$\begin{aligned} \pi_0(m) &= m, \\ \varphi_0(m) &= j \end{aligned}$$

pro každé $m \in M$.

Pak pro každý prvek $(\pi_1, \varphi_1) \in \Pi \times \Phi$ platí $(\pi_1, \varphi_1) \cdot (\pi_0, \varphi_0) = (\pi, \varphi)$, kde

$$\begin{aligned} \pi(m) &= \pi_1(\pi_0(m)) = \pi_1(m), \\ \varphi(m) &= \varphi_1(\pi_0(m)) \cdot \varphi_0(m) = \varphi_1(m) \cdot j = \varphi_1(m) \end{aligned}$$

pro každé $m \in M$; to znamená, že $\pi = \pi_1$, $\varphi = \varphi_1$. Je tedy (π_0, φ_0) pravá jednotka v $\Pi \times \Phi$.

III. Zvolme $(\pi_1, \varphi_1) \in \Pi \times \Phi$. Utvořme π_2, φ_2 tak, aby platilo

$$\begin{aligned} \pi_1(\pi_2(m)) &= m, \\ \varphi_1(\pi_2(m)) \cdot \varphi_2(m) &= j \end{aligned}$$

pro každé $m \in M$.

*) Násobení je zde ovšem míněno jako operace v grupě H.

Pak platí $(\pi_1, \varphi_1) \,.\, (\pi_2, \varphi_2) = (\pi_0, \varphi_0)$ (viz II); je tedy (π_2, φ_2) pravým inversním prvkem k prvku (π_1, φ_1).

Poznámka 3. Je-li $M = \{1, 2, \ldots, n\}$, můžeme si prvek (π, φ) znázornit maticí typu n, n, v jejímž i-tém sloupci je na $\pi(i)$-tém místě shora prvek $\varphi(i)$ (pro $i = 1, 2, \ldots, n$) a na všech ostatních místech je symbol 0. Definujeme-li $0 \,.\, 0 = 0 + 0 = 0, 0 \,.\, h = h \,.\, 0 = 0, 0 + h = h + 0 = h$ pro každé $h \in H$ (a podobně pro více sčítanců, z nichž nejvýš jeden je různý od nuly), můžeme utvořit součin takovýchto dvou matic podle obvyklých pravidel. Znázorňuje-li matice (a_{ik}) (resp. (a_{ik}')) prvek (π, φ) (resp. (π', φ')), znázorňuje jejich součin, t. j. matice (b_{ik}), kde $b_{ik} = \sum_{j=1}^{n} a_{ij} \,.\, a_{jk}'$ prvek $(\pi, \varphi) \,.\, (\pi', \varphi')$; pro $j \neq \pi'(k)$ je totiž $a_{jk}' = 0$, takže pro $i = \pi(\pi'(k))$ je $b_{ik} = a_{i,\pi'(k)} \,.\, a_{\pi'(k),k} = \varphi(\pi'(k)) \,.\, \varphi'(k)$, jinak je $b_{ik} = 0$. Volíme-li za Π grupu všech permutací množiny M, dostáváme takto množinu všech matic, které mají v každém řádku a v každém sloupci právě jeden prvek z H a všude jinde nuly. Podobné znázornění můžeme ovšem provést, i když je M libovolná abstraktní množina.

Buď nyní H podgrupa grupy G, $G \neq H$. Budiž

$$G = T_1 + T_2 + \ldots$$

rozklad grupy G v pravé třídy (t. j. v třídy tvaru rH, kde $r \in G$) podgrupy H.*) Budiž dále

$$M = \{1, 2, \ldots\}$$

množina indexů těchto tříd (zatím nemusí být M ani spočetná) a

$$R = \{r_1, r_2, \ldots\}$$

budiž pevně zvolená množina representantů těchto tříd.

Přiřaďme každému $g \in G$ zobrazení $\bar{g}$ množiny M do M (ukáže se, že $\bar{g}$ je permutace) a zobrazení φ_g množiny M do H tak, aby pro každé $i \in M$ platilo

$$gr_i = r_{\bar{g}(i)} \,.\, \varphi_g(i).$$

(Každé gr_i leží v jisté třídě $T_{\bar{g}(i)} = r_{\bar{g}(i)}H$, tedy existuje $\varphi_g(i) \in H$, že platí uvedený vztah.)

Toto označení budeme zachovávat ve všech dalších větách.

Poznámka 4. Všimněme si, že vyjádření prvků grupy G ve tvaru $r_i h$, kde $r_i \in R$, $h \in H$, je jednoznačné; platí-li tedy $r_i h = r_j h'$, kde $r_i, r_j \in R$, $h, h' \in H$, platí $i = j$, $h = h'$.

Věta 2. *Utvořme grupu Π všech permutací množiny M, množinu Φ*

*) Název „pravé třídy" je vzat z *Zassenhause; Speiser* ve své knize „Theorie der Gruppen von endlicher Ordnung" nazývá třídu tvaru rH levou třídou.

všech zobrazení M do H a grupu $\Pi \times \Phi$ podle věty 1. *Pak je přiřazení* $g \to (\bar{g}, \varphi_g)$ *homomorfní zobrazení G do $\Pi \times \Phi$.*

Důkaz. $g_1 g_2 r_i = g_1 \cdot r_{\bar{g}_2(i)} \cdot \varphi_{g_2}(i) = r_{\bar{g}_1(\bar{g}_2(i))} \cdot \varphi_{g_1}(\bar{g}_2(i)) \cdot \varphi_{g_2}(i)$, tedy

$$\overline{g_1 \cdot g_2}(i) = \bar{g}_1(\bar{g}_2(i)),$$
$$\varphi_{g_1 \cdot g_2}(i) = \varphi_{g_1}(\bar{g}_2(i)) \cdot \varphi_{g_2}(i).$$

Vidíme především, že přiřazení $g \to \bar{g}$ je homomorfismus, tedy množina všech $\bar{g}$ je rovněž grupa. Podle poznámky 2 je každé $\bar{g}$ permutace, tedy skutečně $\bar{g} \in \Pi$ pro každé $g \in G$. Vidíme ihned, že platí

$$(\bar{g}_1 \cdot \varphi_{g_1}) \cdot (\bar{g}_2, \varphi_{g_2}) = (\overline{g_1 g_2} \cdot \varphi_{g_1 g_2}),$$

takže přiřazení je homomorfismus.

Poznámka 5. Věty 1, 2 a poznámka 3 jsou uvedeny jen pro zajímavost; v dalším se z nich používá jen celkem zřejmé okolnosti, že každé $\bar{g}$ je permutace a že v případě, že H je v G konečného indexu n, je přiřazení $g \to \bar{g}$ homomorfní zobrazení grupy G na jistou (nejednotkovou) grupu permutací n prvků. — Zobrazení grupy G do grupy prvků tvaru $(\bar{g}, \varphi_g)$, znázorněné maticemi podle poznámky 3, nazývá *Zassenhaus* „monomiale Darstellung".

Poznámka 6. Je-li G libovolná grupa, značí G' (komutant grupy G) podgrupu v G, vytvořenou všemi komutátory, t. j. prvky tvaru $g_1 g_2 g_1^{-1} g_2^{-1}$, kde $g_1, g_2 \in G$. G' je v G úplně invariantní podgrupa, t. j. platí $\omega(G') \subset G'$ pro libovolný operátor ω grupy G. Faktorová grupa G/G' je Abelova; platí tedy $g_1 g_2 G' = g_1 G' g_2 G' = g_2 G' \cdot g_1 G' = g_2 g_1 G'$ pro libovolnou dvojici g_1, g_2 prvků z G. Je-li naopak grupa G/N Abelova, platí $G' \subset N$. Je-li $H \subset G$, značí ovšem H' komutant grupy H a pod. Všimněme si ještě, že se komutant grupy G rovná podgrupě jednotkové, když a jen když je G grupa Abelova.

Nyní se obrátíme k hlavní části tohoto článku. Všude dále budeme předpokládat, že H je v G konečného indexu n, že tedy platí při našem označení

$$M = \{1, 2, \ldots, n\}, \quad R = \{r_1, r_2, \ldots, r_n\}.$$

Přiřaďme každému $g \in G$ třídu (prvek grupy H/H')

$$P_{G \to H}^{(R)}(g) = P(g) = H' \cdot \prod_{i=1}^{n} \varphi_g(i).$$

Podle poznámky 6 můžeme psát též $P(g) = H' \cdot \prod_{i \in M} \varphi_g(i)$, protože na pořadí faktorů zde nezáleží. Zobrazení $P = P_{G \to H}^{(R)}$ nazýváme překladem grupy G do podgrupy H; ukáže se, že toto zobrazení nezávisí na volbě representantů r_i.

Věta 3. *P je homomorfní zobrazení G do H/H'.*

Důkaz. $P(g_1 g_2) = H' \cdot \prod_{i \in M} \varphi_{g_1 g_2}(i) = H' \cdot \prod_{i \in M} \varphi_{g_1}(\bar{g}_2(i)) \cdot \varphi_{g_2}(i) = H' \cdot \prod_{l \in \bar{g}_2(M)} \varphi_{g_1}(l) \cdot H' \cdot \prod_{i \in M} \varphi_{g_2}(i) = P(g_1) \cdot P(g_2)$; při této úpravě jsme použili toho, že $\bar{g}_2$ je permutace množiny M.

Poznámka 7. Mějme homomorfní zobrazení σ grupy G na grupu G_1. Buď G_0 množina všech $x \in G$, pro něž platí $\sigma(x) \in G_1'$ (kde G_1' je komutant grupy G_1). Protože obraz komutátoru je opět komutátor, je každý komutátor grupy G obsažen v G_0, platí tedy

$$G_0 \supset G', \; G_1' = \sigma(G_0) \supset \sigma(G').$$

Avšak grupa $A = \sigma(G)/\sigma(G')$ je homomorfním obrazem grupy G/G', tedy je A grupa Abelova a platí $\sigma(G') \supset G_1'$. Máme tedy $G_1' = \sigma(G')$ neboli $[\sigma(G)]' = \sigma(G')$.

Věta 4. *Buď σ homomorfní zobrazení grupy G na grupu G_1. Buď $H_1 = \sigma(H)$, $n_1 = G_1 : H_1$. Budiž $S = \{s_1, s_2, \ldots, s_{n_1}\}$ množina representantů tříd G_1 podle H_1; buď $P_1 = P^{(S)}_{G_1 \to H_1}$.*

Pak platí pro každé $g \in G$

$$P_1(\sigma(g)) = [\sigma(P(g)]^{\overline{n_1}}.*)$$

Důkaz. Buď H_0 množina všech $g \in G$, pro něž platí $\sigma(g) \in H_1$. Pak $G : H_0 = G_1 : H_1 = n_1$; je-li $n_2 = H_0 : H$, platí tedy

$$n = n_1 n_2.$$

Nechť

$$G = T_1 + T_2 + \ldots + T_n,$$
$$G_1 = V_1 + V_2 + \ldots + V_{n_1},$$

kde T_i resp. V_l jsou třídy podgrup H resp. H_1; množinu $\{1, 2, \ldots, n_1\}$ označme M_1. Očíslování representantů buď tak voleno, aby platilo $r_i \in T_i$, $s_l \in V_l$. Budiž $k(i)$ (pro $i = 1, 2, \ldots, n$) to číslo z M_1, pro něž platí

$$\sigma(T_i) \subset V_{k(i)}.$$

Ke každému V_l existuje n_2 různých T_i, pro něž je $\sigma(T_i) \subset V_l$; ke každému l ($l = 1, 2, \ldots, n_1$) existuje tedy n_2 různých i, pro něž platí $l = k(i)$. Protože $\sigma(r_i) \in V_{k(i)}$, existují prvky $h_1, h_2, \ldots, h_n \in H_1$ tak, že platí

$$\sigma(r_i) = s_{k(i)} \cdot h_i. \qquad (\beta)$$

Zvolme $g \in G$; buď $g_1 = \sigma(g)$. Určíme jako obvykle permutace $\bar{g}, \bar{g}_1$ a zobrazení φ_g, φ_{g_1} tak, aby platilo

$$g r_i = r_{\bar{g}(i)} \cdot \varphi_g(i) \text{ pro } i = 1, 2, \ldots, n, \qquad (\gamma)$$
$$g_1 \cdot s_l = s_{\bar{g}_1(l)} \cdot \varphi_{g_1}(l) \text{ pro } l = 1, 2, \ldots, n_1. \qquad (\delta)$$

Z (γ) pak plyne

$$\sigma(g) \cdot \sigma(r_i) = \sigma(r_{\bar{g}(i)}) \cdot \sigma(\varphi_g(i)),$$

t. j. podle (β)

$$g_1 \cdot s_{k(i)} \cdot h_i = s_{k(\bar{g}(i))} \cdot h_{\bar{g}(i)} \cdot \sigma(\varphi_g(i)),$$

t. j.

$$g_1 \cdot s_{k(i)} = s_{k(\bar{g}(i))} \cdot h_{\bar{g}(i)} \cdot \sigma(\varphi_g(i)) \cdot h_i^{-1}.$$

*) Mocnina je míněna ovšem jako násobení komplexů v G_1.

Srovnáním s (δ) dostáváme (pro $l = k(i)$)

$$\varphi_{g_1}(k(i)) = h_{\bar{g}(i)}^{-} \cdot \sigma(\varphi_g(i)) \cdot h_i^{-1}.^{*}) \qquad (\varepsilon)$$

Podle poznámky 7 je $\sigma(H') = H_1'$. Protože $\bar{g}$ je permutace množiny M, je $H_1' \cdot \prod_{i \in M} h_{\bar{g}(i)}^{-1} \cdot \prod_{i \in M} h_i = H_1' \cdot \prod_{i \in M} (h_i^{-1} \cdot h_i) = H_1'$. Protože v posloupnosti $k(1), k(2), \ldots, k(n)$ je každé číslo z M_1 právě n_2-krát, platí $H_1' \cdot \prod_{i \in M} \varphi_{g_1}(k(i)) = \left(H_1' \cdot \prod_{l \in M_1} \varphi_{g_1}(l)\right)^{n_2} = [P^{(S)}_{G_1 \to H_1}(g_1)]^{n_2}$; dostáváme tedy vztah

$$\sigma(P(g)) = \sigma(H' \cdot \prod_{i \in M} \varphi_g(i)) = \sigma(H') \cdot \prod_{i \in M} \sigma(\varphi_g(i)) = H_1' \cdot \prod_{i \in M} h_{\bar{g}(i)}^{-1} \cdot$$

$$\cdot \varphi_{g_1}(k(i)) \cdot h_i.^{**}) = H_1' \cdot \prod_{i \in M} \varphi_{g_1}(k(i)) = [P_1(\sigma(g))]^{n_1}.$$

Věta 5. *Buď α automorfismus grupy G; nechť $\alpha(H) \subset H$. Pak platí pro libovolné $g \in G$*

$$P(\alpha(g)) = \alpha(P(g)). \qquad (\zeta)$$

Značí-li Q sjednocení všech tříd z $P(G)$, platí

$$Q = \alpha(Q). \qquad (\eta)$$

Důkaz. Ve větě 4 volíme $\sigma = \alpha$, $G_1 = G$. Protože α je isomorfismus, platí

$$n = G : H = \alpha(G) : \alpha(H) = G : \alpha(H) = n_1.$$

Z relace $G : \alpha(H) = (G : H) \cdot (H : \alpha(H))$ tedy plyne

$$H : \alpha(H) = 1, \ \alpha(H) = H.^{**}) \qquad (\vartheta)$$

Věta 4 říká, že při libovolné množině S representantů tříd G podle $\alpha(H) = H$ platí

$$P^{(S)}_{G \to H}(\alpha(g)) = \alpha(P^{(R)}_{G \to H}(g)). \qquad (\iota)$$

Volíme-li zde $S = R$, dostáváme (ζ). Je-li konečně $x \in Q$, existuje $g \in G$, že $x \in P(g)$, tedy $\alpha(x) \in \alpha(P(g)) = P(\alpha(g)) \in P(G)$, tedy $\alpha(x) \in Q$. Tím je dokázáno, že $\alpha(Q) \subset Q$. Protože podle (ϑ) platí $\alpha^{-1}(H) \subset H$, platí podobně též $\alpha^{-1}(Q) \subset Q$, tedy platí (η).

Korolár. Je-li ve větě 5 α identický automorfismus, říká vztah (ι), že $P^{(S)}_{G \to H}(g) = P^{(R)}_{G \to H}(g)$; vidíme, že zobrazení P nezávisí na volbě representantů.

Věta 6. $P_{G \to H}(G') = H'.^{***})$

---

*) Viz poznámku 4; platí ovšem $\varphi_g(i) \in H$, $\sigma(\varphi_g(i)) \in H_1$, tedy též $h_{\bar{g}(i)}^{-} \cdot \sigma(\varphi_g(i)) \cdot h_i^{-1} \in H_1$.

**) Viz (ε).

***) Je-li α automorfismus grupy G a je-li $K \subset G$, může nastat případ $\alpha(K) \subset K$, $\alpha(K) \neq K$. Je-li K v G konečného indexu, pak tento případ nastat nemůže, jak ukazuje (ϑ).

Důkaz. Podle věty 3 je P homomorfní zobrazení grupy G na jistou Abelovu grupu $A \subset H/H'$. Budiž N normální podgrupa všech $g \in G$, pro něž platí $P(g) = H'$. Pak je G/N isomorfní s A, tedy je G/N grupa Abelova, tedy je*) $G' \subset N$.

Protože je $P(N) = H'$, je tím spíše $P(G') = H'$.

Věta 7. *Nechť $K \subset H \subset G$; buď K konečného indexu v G. Pak platí pro každé $g \in G$*

$$P_{G\to K}(g) = P_{H\to K}(P_{G\to H}(g)).$$

Důkaz. Nechť

$$G = r_1H + r_2H + \ldots + r_nH,$$
$$H = s_1K + s_2K + \ldots + s_mK.$$

Pak systém všech prvků tvaru r_is_j tvoří systém representantů tříd G podle K. Zvolme $g \in G$; pak existují h_i $(i = 1, 2, \ldots, n)$, že platí

$$gr_i = r \ldots h_i;$$

ke každému h_i existují k_{ij} $(j = 1, 2, \ldots, m)$, že platí

$$h_is_j = s \ldots k_{ij}$$

a tedy

$$gr_is_j = r \ldots h_is_j = r \ldots s \ldots k_{ij},$$

takže

$$P_{G\to K}(g) = K' \cdot \prod_{i,j} k_{ij} = \prod_{i=1}^{n}\left(K' \cdot \prod_{j=1}^{m} k_{ij}\right) = \prod_{i=1}^{n}(P_{H\to K}(h_i)) =$$

$$P_{H\to K}\left(\prod_{i=1}^{n} h_i\right) = P_{H\to K}\left(H' \cdot \prod_{i=1}^{n} h_i\right)^{**}) = P_{H\to K}(P_{G\to H}(g)).$$

Věta 8. *Zvolme $g \in G$; nechť $G = r_1H + r_2H + \ldots + r_nH$, kde očíslování je tak voleno, aby rozklad permutace $\bar{g}$ množiny M v cykly měl tvar*

$$(1, 2, \ldots, k_1)(k_1 + 1, k_1 + 2, \ldots, k_2) \ldots (k_{t-1} + 1, k_{t-1} + 2, \ldots, k_t),$$

kde t je počet cyklů (přidáme i cykly jednočlenné), $k_t = n$. Označme ještě $k_0 = 0$, $d_i =$ délka i-tého cyklu $= k_i - k_{i-1}$ $(i = 1, 2, \ldots, t)$. Pak platí

$$P_{G\to H}(g) = H' \cdot \prod_{i=1}^{t} r_{k_i}^{-1} \cdot g^{d_i} \cdot r_{k_i}.$$

Je-li speciálně g prvkem centra G, platí tedy

$$P_{G\to H}(g) = H' \cdot g^n.$$

Důkaz. Je-li l různé ode všech k_i, je $\bar{g}(l) = l + 1$; $\bar{g}(k_i) = k_{i-1} + 1$.

*) Viz poznámku 6.

**) Viz větu 6.

Platí tedy na př.

$$gr_1 = r_2 \varphi_g(1),$$
$$gr_2 = r_3 \varphi_g(2),$$
$$\cdots\cdots\cdots\cdots$$
$$gr_{k_1-1} = r_{k_1} \cdot \varphi_g(k_1 - 1),$$
$$g \cdot r_{k_1} = r_1 \cdot \varphi_g(k_1),$$

tedy

$$\varphi_g(k_1 - 1) \cdot \varphi_g(k_1 - 2) \ldots \varphi_g(1) \cdot \varphi_g(k) =$$
$$= r_{k_1}^{-1} \cdot g \cdot r_{k_1-1} \cdot r_{k_1-1}^{-1} \cdot g \cdot r_{k_1-2} \ldots r_2^{-1} \cdot g \cdot r_1 \cdot r_1^{-1} \cdot g \cdot r_{k_1} = r_{k_1}^{-1} \cdot g_1^{d_1} \cdot r_{k_1}.$$

Podobné výrazy dostaneme i pro další cykly; jejich znásobením dostáváme hledaný vztah. Je-li g prvek centra, je ovšem

$$r_{k_i}^{-1} \cdot g^{d_i} \cdot r_{k_1} = g^{d_i},$$

tedy

$$P_{G \to H}(g) = H' \cdot \prod_{i=1}^{t} g^{d_i} = H' \cdot g^{\sum_{i=1}^{t} d_i} = H' \cdot g^n.^*)$$

Věta 9. *Buď H normální v G. Pak platí pro každou dvojici x, g prvků z G*

$$P(g) \cdot x = x \cdot P(g).$$

Důkaz. Ve větě 5 volme za α automorfismus $g \to x^{-1}gx$. Pak platí

$$P(x^{-1}gx) = x^{-1}(P(g))\, x.$$

Protože grupa H/H' je Abelova a zobrazení P je homomorfismus, platí

$$P(g) = P(x^{-1}) \cdot P(g) \cdot P(x) = P(x^{-1}gx) = x^{-1}(P(g))\, x,$$

tedy opravdu

$$x \cdot P(g) = P(g) \cdot x.$$

Věta 10. *Buď H normální Abelova podgrupa v G; buď C centrum grupy G. Pak platí*

$$P(G) \subset C \cap H.$$

Důkaz. Protože $H' = (j)$, je $P(g)$ prvkem H pro každé $g \in G$. Podle věty 9 leží $P(g)$ v centru G.

Poznámka 8. Je-li A Abelova grupa a je-li n přirozené číslo, je přiřazení $x \to x^n$ homomorfní zobrazení A do A. Je-li řád každého prvku z A konečný a nesoudělný s n, je toto přiřazení dokonce automorfismem grupy A; je-li totiž x řádu m, pak existují celá čísla k, l tak, že $km + ln = 1$, tedy

$$(x^l)^n = x^{ln} = x^{km+ln} = x,$$

*) Mimochodem je patrné, že zde platí $g^{d_i} \in H$, tedy též $g^n \in H$. (Každý prvek $r_{k_i}^{-1} \cdot g^{d_i} \cdot r_{k_i}$ je součinem prvků z H.)

tedy má každý prvek vzor; za podobného označení platí implikace

$$x^n = j \Rightarrow j = j^l = x^{ln} = x^{km+ln} = x,$$

tedy je přiřazení isomorfismus.

Věta 11. *Buď H Abelova podgrupa grupy G; buď C centrum G. Budiž dále $K \subset C$; nechť řád každého prvku $k \in K$ je konečný a nesoudělný s $n = G : H$. Pak $P_{G \to H}$ definuje automorfismus grupy K.*

Důkaz. Plyne z věty 8 a poznámky 8.

Věta 12. *Buď H normální Abelova podgrupa grupy G, buď C centrum G; dále buď řád každého prvku z $H \cap C$ konečný a nesoudělný s $G : H$. Pak platí*

$$P(G) = H \cap C.$$

Důkaz. Podle věty 10 platí $P(G) \subset H \cap C$; podle věty 11 je však $P(H \cap C) = H \cap C$, tedy $H \cap C = P(H \cap C) \subset P(G) \subset H \cap C$.

Abychom ukázali užitečnost aspoň některých z odvozených výsledků, obrátíme se nyní ke konečným grupám. Napřed uvedeme bez důkazu několik základních vět. V další části článku jsou všechny grupy konečné.

Buďte $n, \alpha, \alpha', \ldots$ přirozená čísla, $p, p', \ldots$ buďte různá prvočísla; nechť $n = p^{\alpha} p'^{\alpha'} \ldots$ Buď G grupa řádu n. Pak existuje podgrupa $S = S_p$ (grupy G) řádu p^{α}; grupa S se nazývá Sylowovou p-podgrupou grupy G. Všechny Sylowovy p-podgrupy, obsažené v grupě G, jsou navzájem konjugovány (při pevném p). Buď N_s normalisátor (některé) Sylowovy p-podgrupy S; buď i počet všech Sylowových p-podgrup grupy G. Podle předcházejícího ovšem platí $i = G : N_s$ a dále

$$i \equiv 1 \pmod{p}.$$

Je-li p prvočíslo, je každá grupa řádu p cyklická; počet jejích automorfismů je $p - 1$. Grupa řádu p^2 je vždy Abelova; buď je cyklická, pak má $p^2 - p = p(p-1)$ automorfismů, nebo je direktním součinem dvou cyklických grup řádu p a potom má $(p^2 - 1) \cdot (p^2 - p) = (p-1)^2 \cdot p(p+1)$ automorfismů.

Grupa, která nemá žádnou normální podgrupu mimo podgrupu jednotkovou a sebe samu, se nazývá jednoduchá. Grupa řádu p^{α}, kde p je prvočíslo a $\alpha > 1$, nemůže být jednoduchá, protože má centrum různé od podgrupy jednotkové. Je-li toto centrum celá grupa, můžeme najít cyklickou podgrupu řádu p.

Poznamenejme ještě, že budeme v další části článku používat z dokázaných vět jen věty 3 a věty 8, která je dokázána nezávisle na větách 4 až 7.

1. pomocná věta. *Buď A Abelova podgrupa grupy G, N_A její normalisátor. Budiž index $N_A : A$ nesoudělný s počtem automorfismů a_A grupy A. Pak leží A v centru N_A.*

Důkaz. Budiž C_A centralisátor grupy A (t. j. množina (grupa) všech prvků z G, záměnných s každým prvkem grupy A). Každý prvek $x \in N_A$ vytváří automorfismus grupy A, přiřazující prvku $a \in A$ prvek $x^{-1}ax$. Snadno se přesvědčíme, že se takto grupa N_A homomorfně zobrazí na jistou grupu $\mathbf{A}$ automorfismů grupy A. Na identický automorfismus se zobrazí právě všecky prvky z C_A; platí tedy

$$N_A/C_A \cong \mathbf{A}.$$

Řád $\mathbf{A}$ neboli index $N_A : C_A$ je tedy dělitelem řádu grupy všech automorfismů grupy A, to jest čísla a_A. Avšak A je grupa Abelova, platí tedy $A \subset C_A$, $N_A : C_A / N_A : A$. Podle předpokladu je $N_A : A$ a tím spíše $N_A : C_A$ nesoudělné s a_A; je tedy $N_A : C_A = 1$, $N_A = C_A$. Tím je věta dokázána.

2. pomocná věta. *Buď Sylowova p-podgrupa S grupy G obsažena v centru svého normalisátoru N_s. Nechť platí*

$$g \in G,\ s \in S,\ gsg^{-1} \in S.$$

Pak je $s = gsg^{-1}$.

Důkaz. Budiž $s' = gsg^{-1}$; buď $N_{s'}$ normalisátor prvku s'. Protože S je grupa Abelova, platí $xs'x^{-1} = s'$ pro každé $x \in S$; je tedy $S \subset N_{s'}$. Protože platí $s \in S$, platí též $s' = gsg^{-1} \in gSg^{-1}$. Prvek s' leží tedy také v Abelově grupě $S' = gSg^{-1}$; platí rovněž $S' \subset N_{s'}$. Grupy S, S' jsou ovšem též Sylowovými p-podgrupami grupy $N_{s'}$ a jsou tedy v $N_{s'}$ konjugovány. Existuje tedy $y \in N_{s'}$ tak, že platí

$$S = yS'y^{-1} = yg\,S(yg)^{-1}.$$

Vidíme, že platí $yg \in N_s$. Protože S je v centru N_s, platí

$$(yg)\,s(yg)^{-1} = s.$$

Protože $y \in N_{s'}$, máme konečně

$$s = ygsg^{-1}y^{-1} = ys'y^{-1} = s'.$$

Věta 13 (Burnsideova). *Leží-li Sylowova p-podgrupa S grupy G v centru svého normalisátoru N_s, je grupa G homomorfní s grupou S.*

Důkaz. Zvolme $s \in S$. Klademe-li ve větě 8 $H = S$, $g = s$, dostáváme

$$P_{G \to S}(s) = \prod_{i=1}^{t} r_{k_i}^{-1} . s^{d_i} . r_{k_i}.$$

Zvolme libovolně i, $1 \leqq i \leqq t$. Platí ovšem $s^{d_i} \in S$. Prvek $\bar{s} = r_{k_i}^{-1} . s^{d_i} . r_{k_i}$ je součinem několika prvků z S, je tedy též $\bar{s} \in S$. Podle 2. pomocné věty (kde klademe $g = r_{k_i}^{-1}$, $s = s^{d_i}$) je $\bar{s} = s^{d_i}$. Platí tedy

$$P(s) = s^{\Sigma d_i} = s^{G:S}.$$

Protože $G : S$ je nesoudělné s $S : (j)$, definuje podle poznámky 8 $P_{G\to S}$ automorfismus grupy S. Je tedy $P_{G\to S}(S) = S$, tím spíše $P_{G\to S}(G) = S$.

Věta 14. *Řád jednoduché konečné grupy, není-li prvočíslem, je dělitelný buď 12 nebo třetí mocninou nejmenšího prvočísla v něm obsaženého.*

Důkaz. Mějme grupu G. Vynechme případ, že $n =$ řád G je mocnina některého prvočísla. Budiž p nejmenší prvočíslo obsažené v n. Jestliže p^3/n, věta platí. Nechť je nyní v n obsažena nejvýš druhá mocnina p. Utvořme Sylowovu p-podgrupu S_p grupy G. Počet a_s jejích automorfismů je buď $p - 1$ nebo $p(p - 1)$ nebo $(p - 1)^2\, p(p + 1)$, vždy tedy platí

$$a_s/(p - 1)^2\, p(p + 1).$$

Buďte $p', p'', \ldots$ ostatní prvočísla obsažená v n. Index $N_s : S$ grupy S v jejím normalisátoru je součinem mocnin těchto prvočísel. Není-li žádné z nich obsaženo v součinu $(p - 1)^2\, p(p + 1)$, leží podle 1. pomocné věty S v centru N_s a podle věty 13 je G homomorfní s S; není tedy v tomto případě G jednoduchá. Je-li naopak grupa G jednoduchá, musí platit na př.

$$. \quad p'/(p - 1)^2\, p(p + 1).$$

Avšak p je nejmenší prvočíslo obsažené v n; platí tedy $p' > p$, a protože není ani $p'/p - 1$ ani p'/p, máme

$$p'/p + 1.$$

Odtud plyne, že $p = 2$, $p' = 3$.

Snadno nahlédneme, že v tomto případě je n dělitelné 4 a grupa $S_p = S_2$ je čtyřgrupa; jinak bychom podobnou úvahou zjistili, že platí buď

$$3/p - 1 = 1 \text{ nebo } 3/p(p - 1) = 2,$$

což není možné. Protože $p' = 3$, je n dělitelné číslem $4 \cdot 3 = 12$.

Uvedeme ještě jeden příklad na použití Burnsideovy věty ve spojení s větami o Sylowových p-podgrupách.

Žádná grupa řádu 144 není jednoduchá.

Důkaz. Buď G grupa řádu 144. Platí $144 = 2^4 \cdot 3^2$. Buď S_3 řádu 9, $S_3 \subset G$; buď N_s normalisátor grupy S_3. Protože $G : N_s/16$, máme pro $G : N_s$ možnosti

$$1, 2, 4, 8, 16.$$

Protože však musí platit $G : N_s \equiv 1 \pmod 3$, zbývají jen možnosti

$$1, 4, 16.$$

Je-li $G : N_s = 1$, je S_3 normální v G. Je-li $G : N_s = 16$, je $S_3 = N_s$, tedy (protože S_3 je grupa Abelova) leží S_3 v centru svého normalisátoru, tedy je podle věty 13 grupa G homomorfní s grupou S_3. Je-li konečně $G : N_s =$

$= 4$, je podle poznámky 5 grupa G homomorfní s nějakou grupou G_1 permutací čtyř prvků. Protože pro řád n_1 grupy G_1 platí

$$1 < n_1 \leqq 24,$$

vidíme, že ani v tomto případě není G jednoduchá.

Podobným postupem lze ukázat, že žádná grupa řádu menšího než 100 — mimo grupy řádu prvočíselného a alternující grupu permutací 5 prvků — není jednoduchá; provedení mohu přenechat čtenáři. Tento rozbor se poněkud zjednoduší, použijeme-li ještě věty, že grupa řádu $p^n q$, kde p, q jsou prvočísla, není jednoduchá.