Algebraické struktury

KMA/ALG

Sylabus

Teorie grup - grupy, podgrupy, normální podgrupy, faktorgrupy, Lagrangeova věta. Homomorfismus grup, věty o izomorfismu grup, cyklické grupy a jejich struktura. Direktní součet grup, Abelovy grupy, direktní rozklad torzní Abelovy grupy a konečné Abelovy p-grupy. Sylowovy p-podgrupy a jejich vlastnosti. Okruhy a tělesa - podokruhy, ideály, faktorokruh, dělitelé nuly, základní vlastnosti těles. Čínské věty o zbytku. Reprezentace grup.

Literatura

L. Procházka a kol.: Algebra - Academia Praha 1990,
S. Mac Lane, G. Birkhoff: Algebra - Alfa Bratislava 1973,
J. Lambek: Okruhy a moduly - 1966, ruský překlad Mír Moskva 1971,
L. Fuchs: Nekonečné Abelovy grupy - 1970, ruský překlad Mír Moskva 1974,
L. Procházka: Úvod do studia reprezentací grup, Karolinum Praha 1999.

Požadavky na zápočet - pochopení učiva.
Požadavky na zkoušku - teoretické i praktické zvládnutí probírané látky.

RNDr. Libuše Tesková, CSc.

1 Grupy

Lemma 1.1 *Nechť* $m, n \in \mathbf{Z}$, $m, n \neq 0$. *Označíme-li* $d = (m, n)$ *největší společný dělitel čísel* m, n , *potom existují čísla* $u, v \in \mathbf{Z}$ *tak, že* $um + vn = d$.
Specielně: jsou-li m, n *čísla nesoudělná, existují čísla* $u, v \in \mathbf{Z}$ *tak, že* $um + vn = 1$.

Důkaz Označme $K = \{|rm + sn| \ ; \ r, s \in \mathbf{Z}, \ rm+sn \neq 0\}$. Tato množina je neprázdná, a má tedy nejmenší prvek - označme ho $|r_0m + s_0n|$. Potom je $d = \pm(r_0m + s_0n)$.

■

Definice 1.1 *Řekneme, že množina* G *je grupa, jestliže na* G *je definována binární operace*
$G \times G \longrightarrow G$
$(g, h) \longmapsto g \cdot h \qquad \forall g, h \in G$
taková, že platí:

(1) $(g \cdot h) \cdot k = g \cdot (h \cdot k) \qquad \forall g, h, k \in G$.

(2) Existuje prvek $g_0 \in G$ *takový, že pro všechny prvky* $g \in G$ *je* $g \cdot g_0 = g_0 \cdot g = g$.

(3) Pro každý prvek $g \in G$ *existuje prvek* $g^{-1} \in G$ *tak, že* $g \cdot g^{-1} = g^{-1} \cdot g = g_0$.

Přesně lze psát $(G, \cdot)$ *je grupa s operací* $\cdot$.

Poznámka 1.1
1. Znak $\cdot$ pro grupovou operaci se většinou nepíše, a tedy gh je totéž jako $g \cdot h$.
2. Prvek g_0 je určen jednoznačně, nazývá se jednotkový prvek a označuje 1 .
3. Pro každý prvek $g \in G$ je prvek g^{-1} určen jednoznačně a nazývá se inverzní prvek k prvku g .

Definice 1.2 *Jestliže* G *je grupa, v níž pro každé dva prvky* $g, h \in G$ *platí* $gh = hg$, *potom grupa* G *se nazývá komutativní nebo též Abelova grupa.*

Poznámka 1.2 Je-li G Abelova grupa, bývá zvykem operaci psát znakem $+$, tedy $g + h$. Prvek g_0 se potom nazývá nulový prvek grupy G a značí 0 . Pro každý prvek $g \in G$ se inverzní prvek nyní označuje $-g$ a nazývá se prvek opačný k prvku g .
Takovou grupu budeme přesně označovat $(G, +)$.

Lemma 1.2 *Nechť* G *je grupa, potom platí:*

1. $(g^{-1})^{-1} = g \qquad \forall g \in G$;
2. $(gh)^{-1} = h^{-1}g^{-1} \qquad \forall g, h \in G$;
3. $1^{-1} = 1$.

Definice 1.3 *Neprázdná část* $H \subseteq G$ *, kde* $(G, \cdot)$ *je grupa, se nazývá podgrupa grupy* G *, jestliže* $1 \in H$ *,* $ab \in H \quad \forall a, b \in H$ *,* $a^{-1} \in H \quad \forall a \in H$ *.*
Budeme psát $H \leq G$ *.*

Lemma 1.3 *Nechť* $(G, \cdot)$ *je grupa,* H *neprázdná část množiny* G *. Potom platí:*
$H \leq G \Leftrightarrow ab^{-1} \in H \quad \forall a, b \in H$ *.*

Důkaz Implikace $\Rightarrow$ je zřejmá.
Implikace $\Leftarrow$: $H \neq \emptyset \Rightarrow \exists a \in H \Rightarrow 1 = aa^{-1} \in H$. $\forall a \in H \quad a^{-1} = 1a^{-1} \in H$.
$\forall a, b \in H \quad a \in H, b^{-1} \in H \Rightarrow ab = a(b^{-1})^{-1} \in H$.

■

Definice 1.4 *Buď* H *podgrupa grupy* G *, buď* $g \in G$ *, potom množina*
$gH = \{gh \ ; \ h \in H\}$ *se nazývá levá rozkladová třída grupy* G *podle podgrupy* H *určená prvkem* g *;*
$Hg = \{hg \ ; \ h \in H\}$ *se nazývá pravá rozkladová třída grupy* G *podle podgrupy* H *určená prvkem* g *.*

Věta 1.1 *Nechť* H *je podgrupa grupy* G *, potom pro každé* $g, h \in G$ *platí:*

1. $\bigcup_{g \in G} gH = G$, $\qquad\qquad$ $\bigcup_{g \in G} Hg = G$;
2. $gH \cap hH \neq \emptyset \Rightarrow gH = hH$, $\qquad\qquad$ $Hg \cap Hh \neq \emptyset \Rightarrow Hg = Hh$;
3. $gH = hH \Leftrightarrow h^{-1}g \in H$, $\qquad\qquad$ $Hg = Hh \Leftrightarrow gh^{-1} \in H$.

Důkaz ad 1) - zřejmé
ad 2) $gH \cap hH \neq \emptyset \Rightarrow \exists x \in gH \cap hH \Rightarrow \exists h_1 \in H$ tak, že $x = gh_1$, $\exists h_2 \in H$ tak, že $x = hh_2$. Potom $\forall y \in gH$ je $y = gk$, kde $k \in H \Rightarrow y = gk = g1k = g(h_1 h_1^{-1})k = (gh_1)(h_1^{-1}k) = x(h_1^{-1}k) = (hh_2)(h_1^{-1}k) = h(h_2 h_1^{-1}k) \in hH$. Tedy $gH \subseteq hH$. Stejně $hH \subseteq gH$.
ad 3) Jestliže $gH = hH \Rightarrow g = g1 \in gH = hH \Rightarrow \exists k \in H$ tak, že $g = hk$, potom $h^{-1}g = h^{-1}hk = 1k = k \in H$.
Jestliže $h^{-1}g \in H \Rightarrow h^{-1}g = k$, kde $k \in H$, potom $g = g1 \in gH$, $g = hk \in hH$, a tedy $g \in gH \cap hH$. Tím $gH \cap hH \neq \emptyset$, a tedy podle 2) $gH = hH$.

■

Poznámka 1.3 Označme $\mathcal{A}$ množinu všech navzájem různých levých rozkladových tříd grupy G podle podgrupy H a $\mathcal{B}$ množinu všech navzájem různých pravých rozkladových tříd grupy G podle podgrupy H . Nyní můžeme definovat zobrazení $\varphi: \mathcal{A} \longrightarrow \mathcal{B}$ takto: $\varphi: gH \longmapsto Hg^{-1}$.
Toto zobrazení je vzájemně jednoznačné, a tedy $|\mathcal{A}| = |\mathcal{B}|$.
Tedy počet levých rozkladových tříd grupy G podle podgrupy H se rovná počtu pravých rozkladových tříd grupy G podle H - toto číslo se označuje $[G : H]$ a nazývá index podgrupy H v grupě G .

Věta 1.2 *(Lagrangeova)*
Je-li H *podgrupa grupy* G *, potom* $|G| = |H| \cdot [G : H]$.

Důkaz Zobrazení $\varphi: H \longrightarrow gH$ definované předpisem
$\varphi: h \longmapsto gh \qquad \forall h \in H$
je bijekce H na gH , a tedy $|H| = |gH|$.

■

Věta 1.3 *Průnik libovolného neprázdného souboru podgrup grupy* G *je opět podgrupa grupy* G .

Důkaz Nechť $H_i \leq G \quad \forall i \in I$, potom $\forall a, b \in \bigcap_{i \in I} H_i$ je $a, b \in H_i \quad \forall i \in I$, a tedy $ab^{-1} \in H_i \quad \forall i \in I$. Tím $ab^{-1} \in \bigcap_{i \in I} H_i$.

■

Definice 1.5 *Buď* X *podmnožina grupy* G *. Průnik všech podgrup grupy* G *, které obsahují množinu* X *, je opět podgrupa grupy* G *, obsahuje množinu* X *, a nazývá se podgrupa generovaná množinou* X *. Budeme ji značit* $\langle X \rangle$.
Je-li $\langle X \rangle = G$ *, potom* X *se nazývá množina generátorů grupy* G .
Jestliže grupa G *je generovaná jediným prvkem* $g \in G$ *, tj.* $G = \langle \{g\} \rangle$ *, říkáme, že grupa* G *je cyklická a píšeme zkráceně* $G = \langle g \rangle$.
Jestliže $g \in G$ *je prvek grupy* G *, potom číslo* $|\langle g \rangle|$ *se nazývá řád prvku* g *v grupě* G *a značí* $o(g)$.
Grupa G *se nazývá konečná, jestliže* $|G|$ *je konečné číslo.*
Grupa G *se nazývá konečně generovaná, jestliže existuje konečná množina* X *, která generuje grupu* G *, tj.* $|X|$ *je konečné číslo a* $\langle X \rangle = G$.

Důsledek 1 Je-li G konečná grupa, potom pro každý prvek $g \in G$ platí $o(g) \mid |G|$.

Důkaz Je to přímý důsledek Lagrangeovy věty.

■

Lemma 1.4 *Buď* G *cyklická grupa generovaná prvkem* g *, potom* $G = \{g^k \ ; \ k \in \mathbf{Z}\}$.

Důkaz Označíme-li $X = \{g^k \ ; \ k \in \mathbf{Z}\}$, potom snadno vidíme, že X je podgrupa grupy G , $g \in X$. Tím $G = \langle g \rangle \subseteq X \subseteq G$.

■

Poznámka 1.4 Analogicky lze vyslovit takovéto tvrzení:
Je-li X podmnožina grupy G , potom
$\langle X \rangle = \{h \ ; \ h \in G, \ h = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}, \text{ kde } x_1, x_2, ..., x_n \in X \ , k_1, k_2, ...k_n \in \mathbf{Z}\}$.

Definice 1.6 *Řekneme, že podgrupa* H *grupy* G *je normální podgrupa grupy* G *, jestliže pro každé* $g \in G$ *a pro každé* $h \in H$ *je* $g^{-1}hg \in H$.

Poznámka 1.5 V komutativní grupě je zřejmě každá podgrupa normální.

Věta 1.4 *Nechť H je podgrupa grupy G, potom následující podmínky jsou ekvivalentní.*

1. *H je normální podgrupa grupy G.*
2. *$g^{-1}Hg \subseteq H \qquad \forall g \in G$.*
3. *$g^{-1}Hg = H \qquad \forall g \in G$.*
4. *$gH = Hg \qquad \forall g \in G$.*
5. *Každá levá rozkladová třída G podle H se rovná nějaké pravé rozkladové třídě G podle H.*

Důkaz
1. $\Rightarrow$ 2. $\quad \forall g \in G\ \forall h \in H\ \ g^{-1}hg \in H \ \Rightarrow\ g^{-1}Hg \subseteq H$.
2. $\Rightarrow$ 3. $\quad (g^{-1})^{-1}Hg^{-1} \subseteq H \ \Rightarrow\ gHg^{-1} \subseteq H \ \Rightarrow\ H \subseteq g^{-1}Hg$.
3. $\Rightarrow$ 4. $\quad g^{-1}Hg = H \ \Rightarrow\ Hg = gH$.
4. $\Rightarrow$ 5. $\quad gH = Hg$.
5. $\Rightarrow$ 1. $\quad \forall g \in G\ \forall h \in H\ \ \exists g' \in G$ tak, že $g^{-1}H = Hg' \ \Rightarrow\ g^{-1} \in Hg' \cap Hg^{-1} \ \Rightarrow$ $Hg' = Hg^{-1} \ \Rightarrow\ g^{-1}H = Hg^{-1}\ \ \exists h' \in H\ \ g^{-1}h = h'g^{-1} \ \Rightarrow\ g^{-1}hg = h' \in H$.

■

Poznámka 1.6 Jestliže H je podgrupa grupy G taková, že $[G : H] = 2$, potom H je normální podgrupa grupy G.

Definice 1.7 *Jestliže H je normální podgrupa grupy G, potom na množině levých rozkladových tříd můžeme zavést grupovou operaci*

$$aH \cdot bH = abH.$$

Potom množina levých rozkladových tříd s touto operací tvoří opět grupu, která se nazývá faktorgrupa grupy G podle normální podgrupy H a značí G/H.

Definice 1.8 *Nechť G, H jsou grupy, nechť $\varphi: G \longrightarrow H$ je zobrazení. Toto zobrazení se nazývá homomorfismus, jestliže pro každé $a, b \in G$ je $\varphi(ab) = \varphi(a)\varphi(b)$.*
Jestliže φ je prostý homomorfismus, potom se nazývá monomorfismus.
Jestliže φ je homomorfismus na H, potom se nazývá epimorfismus.
Jestliže φ je vzájemně jednoznačný homomorfismus, potom se nazývá izomorfismus.
Grupy G, H se nazývají izomorfní a značí se $G \cong H$.

Věta 1.5 *Nechť $\varphi: G \longrightarrow H$ je homomorfismus grupy G do grupy H, potom platí:*

1. *$\varphi(1_G) = 1_H$.*

2. $\varphi(g^{-1}) = \varphi(g)^{-1} \qquad \forall g \in G$.

3. $\varphi(g^k) = \varphi(g)^k \qquad \forall g \in G \ \ \forall k \in \mathbf{Z}$.

Důkaz
1. $\varphi(1_G)1_H = \varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G) \quad \Rightarrow \quad \varphi(1_G) = 1_H$.
2. $\varphi(g)\varphi(g)^{-1} = 1_H = \varphi(1_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$.
3. Pro $k > 0$ je $\varphi(g^k) = \varphi(gg\cdots g) = \varphi(g)\varphi(g)\cdots\varphi(g) = \varphi(g)^k$.
Pro $k = 0$ je $\varphi(g^0) = \varphi(1_G) = 1_H = \varphi(g)^0$.
Pro $k < 0$ je $\varphi(g^k) = \varphi((g^{-1})^{-k}) = \varphi(g^{-1})^{-k} = (\varphi(g)^{-1})^{-k} = \varphi(g)^k$.

■

Definice 1.9 *Nechť* $\varphi\colon G \longrightarrow H$ *je homomorfismus grupy* G *do grupy* H *. Pro podmnožinu* $K \subseteq H$ *se množina*
$\varphi_{-1}(K) = \{g \in G \ ; \ \varphi(g) \in K\}$
nazývá úplný vzor množiny K *. Specielně množina*
$\varphi_{-1}(1_H) = \{g \in G \ ; \ \varphi(g) = 1_H\}$
se nazývá jádro homomorfismu φ *a značí se* $\operatorname{Ker}\varphi$ *.*
Pro podmnožinu $L \subseteq G$ *se množina*
$\varphi(L) = \{\varphi(g) \ ; \ g \in L\}$
nazývá obaz množiny L *při homomorfismu* φ *. Specielně množina*
$\varphi(G) = \{\varphi(g) \ ; \ g \in G\}$
se nazývá obraz homomorfismu φ *a značí se* $\operatorname{Im}\varphi$ *.*

Věta 1.6 *Nechť* $\varphi\colon G \longrightarrow H$ *je homomorfismus grup, potom platí:*

1. *Je-li* K *podgrupa grupy* H *, potom* $\varphi_{-1}(K)$ *je podgrupa grupy* G *.*
2. *Je-li* K *normální podgrupa grupy* H *, potom* $\varphi_{-1}(K)$ *je normální podgrupa grupa* G *.*
3. $\operatorname{Ker}\varphi$ *je normální podgrupa grupy* G *.*
4. *Je-li* L *podgrupa grupy* G *, potom* $\varphi(L)$ *je podgrupa grupy* H *.*
5. $\operatorname{Im}\varphi$ *je podgrupa grupy* H *.*
6. *Je-li* L *normální podgrupa grupy* G *, potom* $\varphi(L)$ *je normální podgrupa grupy* $\operatorname{Im}\varphi$ *.*

Důkaz
ad 1) $\forall a, b \in \varphi_{-1}(K) \ \ \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} \in K$.
ad 2) $\forall g \in G \ \forall h \in \varphi_{-1}(K) \ \ \varphi(g^{-1}hg) = \varphi(g)^{-1}\varphi(h)\varphi(g) \in K$.
ad 3) 1 je normální podgrupa grupy H .
ad 4) $\forall c, d \in \varphi(L) \ \ \exists a, b \in L$ tak, že $\varphi(a) = c, \ \varphi(b) = d$, potom $cd^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \in \varphi(L)$.

ad 5) G je podgrupa grupy G .
ad 6) $\varphi(L)$ je podgrupa grupa $\mathrm{Im}\varphi$. $\forall x \in \mathrm{Im}\varphi,\ \forall y \in \varphi(L)\ \exists g \in G\ \varphi(g) = x$
$\exists h \in L\ \varphi(h) = y$, potom $x^{-1}yx = \varphi(g)^{-1}\varphi(h)\varphi(g) = \varphi(g^{-1}hg) \in \varphi(L)$.

■

Poznámka 1.7 Je-li $\varphi: G \longrightarrow H$ homomorfismus grup, potom platí: φ je injektivní právě tehdy, když $\mathrm{Ker}\,\varphi = \{1\}$.

Definice 1.10 *Nechť H je normální podgrupa grupy G , potom lze definovat zobrazení*
$\pi: G \longrightarrow G/H$
$\pi: g \longmapsto gH \qquad \forall g \in G$.
Toto zobrazení se nazývá přirozená projekce grupy G na faktorgrupu G/H .

Lemma 1.5 *Nechť H je normální podgrupa grupy G , $\pi: G \longrightarrow G/H$ přirozená projekce, potom π je epimorfismus a $\mathrm{Ker}\,\pi = H$.*

Důkaz $\forall g, h \in G\ \pi(gh) = ghH = (gH)(hH) = \pi(g)\pi(h)$.
$g \in \mathrm{Ker}\,\pi \Leftrightarrow \pi(g) = 1_{G/H} \Leftrightarrow gH = 1_{G/H} = 1H \Leftrightarrow 1^{-1}g \in H \Leftrightarrow g \in H$.

■

Věta 1.7 *(o homomorfismu)*
Nechť K je normální podgrupa grupy G , nechť $\pi: G \longrightarrow G/K$ je přirozená projekce. Potom pro každý homomorfismus $\varphi: G \longrightarrow H$ takový, že $K \subseteq \mathrm{Ker}\,\varphi$, existuje právě jediný homomorfismus $\psi: G/K \longrightarrow H$ tak, že $\pi\psi = \varphi$ a $\mathrm{Ker}\,\psi = \mathrm{Ker}\,\varphi/K$.

Důkaz Budeme definovat zobrazení $\psi: G/K \longrightarrow H$ takto:
$\psi: gK \longmapsto \varphi(g) \qquad \forall gK \in G/K$.

■

Věta 1.8 *(1. věta o izomorfismu)*
Nechť $\varphi: G \longrightarrow H$ je homomorfismus grup, potom $G/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi$.
Jestliže φ je epimorfismus, potom $G/\mathrm{Ker}\,\varphi \cong H$.

Důkaz Podle věty 1.7 existuje $\psi: G/\mathrm{Ker}\,\varphi \longrightarrow H$ tak, že $\pi\psi = \varphi$.
Potom $\psi: G/\mathrm{Ker}\,\varphi \longrightarrow \mathrm{Im}\varphi$ a ψ je izomorfismus.

■

Věta 1.9 *(2. věta o izomorfismu)*
Nechť H, K jsou normální podgrupy grupy G takové, že $K \subseteq H$, potom H/K je normální podgrupa grupy G/K a platí $(G/K)/(H/K) \cong G/H$.

Důkaz $\forall gK \in G/K\ \forall hK \in H/K\ (gK)^{-1}(hK)(gK) = (g^{-1}hg)K \in H/K$.
Definujeme $\varphi: G/K \longrightarrow G/H$ takto:
$\varphi: gK \longmapsto gH \qquad \forall gK \in G/K$.
Tvrzení potom plyne z věty 1.8.

■

Lemma 1.6 *Nechť H, K jsou podgrupy grupy G, nechť alespoň jedna z nich je normální podgrupa grupy G, potom $\langle H \cup K \rangle = HK = KH$.*

Věta 1.10 *(3. věta o izomorfismu) Nechť H, K jsou podgrupy grupy G takové, že H je normální podgrupa grupy G, potom $H \cap K$ je normální podgrupa grupy K a platí $HK/H \cong K/(K \cap H)$.*

Důkaz Definujeme zobrazení $\varphi: K \longrightarrow HK/H$ takto:
$\varphi: k \longmapsto kH \qquad \forall k \in K$.
Tvrzení věty plyne podle věty 1.8.

■

Cyklické grupy

Je-li $G = \langle g \rangle$, potom $G = \{g^k \ ; \ k \in \mathbf{Z}\}$.
Pro každé $a, b \in G$ existuje $k \in \mathbf{Z}$, $l \in \mathbf{Z}$ tak, že $a = g^k$, $b = g^l$, potom $ab = g^k g^l = g^{k+l} = g^{l+k} = g^l g^k = ba$, a tedy každá cyklická grupa je komutativní.

Věta 1.11 *Buď $G = \langle a \rangle$ cyklická grupa generovaná prvkem a , potom jsou pouze tyto dvě možnosti:*

buď $\forall r, s \in \mathbf{Z}$, $r \neq s$ je $a^r \neq a^s$, potom G je nekonečná cyklická grupa.

nebo $\exists n \in \mathbb{N}$ tak, že pro $t \in \mathbf{Z}$ $a^t = 1 \Leftrightarrow n \mid t$. Potom $|G| = o(a) = n$,
$G = \{ \ a, a^2, a^3, ..., a^{n-1}, a^n = 1 \ \}$.

Důkaz Definujeme zobrazení $\varphi: \mathbf{Z} \longrightarrow G$ předpisem
$\varphi: r \longmapsto a^r \qquad \forall r \in \mathbf{Z}$.

■

Věta 1.12 *Každá nekonečná cyklická grupa je izomorfní s aditivní grupou celých čísel $\mathbf{Z}$. Každá konečná cyklická grupa řádu n je izomorfní s faktorgrupou $Z_{(n)} = \mathbf{Z}/n\mathbf{Z}$.*

Důkaz Je-li $G = \langle a \rangle$, potom zobrazení $\varphi: \mathbf{Z} \longrightarrow G$ definované předpisem
$\varphi: k \longmapsto a^k \qquad \forall k \in \mathbf{Z}$ dává tvrzení věty podle 1. věty o izomorfismu - věty 1.8.

■

Věta 1.13 *Každá podgrupa a každý homomorfní obraz cyklické grupy je opět cyklická grupa. Každá nejednotková podgrupa nekonečné cyklické grupy je opět nekonečná.*

Důkaz Nechť $G = \langle a \rangle$, H podgrupa grupy G , potom $\exists n \in \mathbb{N}$ tak, že $a^n \in H$, nechť n je takové nejmenší. Potom snadno ukážeme, že $H = \langle a^n \rangle$.
Nechť $\varphi: G = \langle a \rangle \longrightarrow K$ je epimorfismus, potom $K = \langle \varphi(a) \rangle$.

■

Věta 1.14 *Nechť $G = \langle a \rangle$ je konečná cyklická grupa řádu n , potom pro $k \in \mathbf{Z}$ je $G = \langle a^k \rangle \Leftrightarrow (k, n) = 1$.*

Důkaz Tvrzení plyne užitím lemmatu 1.1.

■

Věta 1.15 *Nechť $G = \langle a \rangle$ je konečná cyklická grupa řádu n , nechť $d, m \in \mathbb{N}$ jsou taková čísla, že $dm = n$, potom $\langle a^d \rangle$ je jediná podgrupa grupy G řádu m .*

Důkaz Označíme-li $t = o(a^d)$, potom $t = m$, a tedy $\langle a^d \rangle$ je podgrupa grupy G řádu m . Snadno ukážeme, že je jediná.

■

Věta 1.16 *Buď* $G = \langle a \rangle$ *konečná cyklická grupa řádu* n *, buď* $k \in \mathbb{N}$ *a* $d = (k, n)$ *, tedy* $d \mid n$ *a existuje* $m \in \mathbb{N}$ *tak, že* $dm = n$ *. Potom* $H = \langle a^k \rangle$ *je podgrupa grupy* G *řádu* m *.*

Důkaz Ukážeme, že $H = \langle a^k \rangle = \langle a^d \rangle$, potom tvrzení plyne z věty 1.15.

■

Důsledek 2 Každá grupa prvočíselného řádu je cyklická. Cyklické grupy prvočíselného řádu jsou právě všechny Abelovy grupy, které nemají netriviální normální podgrupy.

Definice 1.11 *Buď* G *grupa a* $\{H_i \ ; \ i \in I\}$ *soubor normálních podgrup grupy* G *. Jestliže,* $\langle \bigcup_{i \in I} H_i \rangle = G$ *, a pro každé* $i \in I$ *je* $H_i \cap \langle \bigcup_{\substack{j \in I \\ j \neq i}} H_j \rangle = \{1\}$ *, říkáme, že grupa* G *je direktním součtem svých podgrup* H_i *a píšeme* $G = \bigoplus_{i \in I} H_i$ *.*

Je-li I *konečná množina,* $|I| = n$ *, potom píšeme* $G = \bigoplus_{i=1}^{n} H_i = H_1 \oplus H_2 \oplus \cdots \oplus H_n$ *.*

Věta 1.17 *Buď* $\{H_i \ ; \ i \in I\}$ *soubor podgrup grupy* G *, potom* $G = \bigoplus_{i \in I} H_i$ *právě tehdy, když platí následující dvě podmínky:*

1. $\forall h_i \in H_i, \ \forall h_j \in H_j \quad h_i h_j = h_j h_i \quad \forall i, j \in I, \ \ i \neq j$ *.*
2. *Každé* $g \in G, \ \ g \neq 1$ *lze až na pořadí právě jediným způsobem zapsat ve tvaru* $g = h_1 h_2 \cdots h_n$ *, kde* $\forall i = 1, ..., n \ \ h_i \neq 1, \ \ h_i \in H_{k_i}$ *, a pro každé* $i \neq j$ *je* $k_i \neq k_j$ *.*

Důkaz

⇒ Pro každé $i \in I$ je H_i normální podgrupa grupy G , tím $h_i^{-1}(h_j^{-1} h_i h_j) = (h_i^{-1} h_j^{-1} h_i) h_j \in H_i \cap H_j \subseteq H_i \cap \langle \bigcup_{\substack{j \in I \\ j \neq i}} H_j \rangle = 1$. Protože $G = \langle \bigcup_{i \in I} H_i \rangle$, lze každý prvek $g \in G$ psát ve tvaru $g = x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}$, kde $x_1, x_2, ...x_m \in \bigcup_{i \in I} H_i$. Prvky z různých podgrup H_i spolu komutují, a tedy prvek lze psát v požadovaném tvaru $g = h_1 h_2 \cdots h_n$.

⇐ Pro každé $i \in I$ a pro všechny prvky $g \in G$, $h \in H_i$ je $g^{-1} h g = (h_1 h_2 \cdots h_n)^{-1} h (h_1 h_2 \cdots h_n)$. Jestliže $\exists j = 1, ..., n$ tak, že $i = k_j$, potom $g^{-1} h g = h_j^{-1} h h_j \in H_i = H_{k_j}$. Jestliže $\forall j = 1, ..., n$ je $i \neq k_j$, potom $g^{-1} h g = h \in H_i$. Tím je H_i normální podgrupa grupy G pro každé $i \in I$.
Z druhé podmínky snadno již plyne tvrzení.

■

Poznámka 1.8 Mějme grupy $H_1, H_2, ..., H_n$, potom na množině

$$G = \{(h_1, h_2, ..., h_n) \ ; \ h_i \in H_i \quad \forall i = 1, ..., n\}$$

lze definovat grupovou operaci následovně:
$(h_1, h_2, ..., h_n) \cdot (g_1, g_2, ..., g_n) = (h_1 g_1, h_2 g_2, ..., h_n g_n) \quad \forall (h_1, h_2, ..., h_n), (g_1, g_2, ..., g_n) \in G$.
Množina G s touto operací je grupa.
Pro každé $i = 1, ..., n$ můžeme definovat zobrazení $\iota_i \colon H_i \longrightarrow G$ předpisem
$\iota_i \colon h \longmapsto (1, ..., 1, h, 1, ..., 1)$, kde prvek h stojí na i-tém místě.
Toto zobrazení je monomorfismus, a tedy $H_i \cong \bar{H}_i$, $\bar{H}_i$ je podgrupa grupy G .
Snadno vidíme, že $G = \bar{H}_1 \oplus \bar{H}_2 \oplus \cdots \oplus \bar{H}_n$. Tato grupa G se často nazývá vnější direktní součet grup H_i .

Věta 1.18 *Nechť H, K jsou podgrupy grupy G takové, že $G = H \oplus K$, potom $G/H \cong K$.*

Důkaz Tvrzení věty plyne z 3. věty o izomorfismu - věty 1.10.

■

2 Abelovy grupy

Abelova grupa je komutativní grupa a bývá zvykem operaci Abelovy grupy označovat $+$. Je-li $(G,+)$ Abelova grupa, potom význačný prvek se označuje 0 a nazývá nulový prvek. Ke každému prvku $g \in G$ existuje prvek opačný, označovaný $-g$.

Definice 2.1 *Abelova grupa G se nazývá grupa bez torze, jestliže všechny nenulové prvky mají nekonečný řád.*
Abelova grupa G se nazývá torzní grupa, jestliže všechny její prvky mají konečný řád.
Abelova grupa G se nazývá p-grupa, jestliže každý prvek grupy G má konečný řád, který se rovná mocnině prvočísla p.
Abelova grupa G se nazývá smíšená grupa, jestliže má nenulové prvky konečného i nekonečného řádu.
Je-li G Abelova grupa, potom množina $G_T = \{g\ ;\ g \in G,\ \ o(g) < \infty\}$ se nazývá torzní část grupy G.
Pro prvočíslo p potom množina $G_{(p)} = \{g \in G\ ;\ o(g) = p^k,\ \text{kde}\ \ 0 \leq k,\ k \in \mathbf{Z}\}$ se nazývá p-primární komponenta grupy G.

Poznámka 2.1
1. Abelova grupa G je p-grupa právě tehdy, když $G = G_{(p)}$.
2. Homomorfní obraz p-grupy je opět p-grupa.

Věta 2.1 *Nechť G je Abelova grupa, potom platí:*

1. *G_T je podgrupa grupy G.*
2. *Pro každé prvočíslo p je $G_{(p)}$ podgrupa grupy G.*
3. *G/G_T je grupa bez torze.*

Důkaz Tvrzení 1. a 2. jsou zřejmá.
3. Nechť $g+G_T \in G/G_T,\ \ o(g+G_T) < \infty$, potom $\exists m \in \mathbb{N}$ tak, že $m(g+G_T) = 0+G_T$. Tím $mg \in G_T$, potom $\exists n \in \mathbb{N}$ tak, že $(nm)g = n(mg) = 0$, a tedy $g \in G_T$. Tím $g + G_T = G_T = 0 + G_T$, a tedy každý nenulový prvek grupy G/G_T má nekonečný řád.
■

Věta 2.2 *Nechť G je torzní Abelova grupa, potom $G = \bigoplus_p G_{(p)}$.*

Důkaz Buď p prvočíslo, $g \in G_{(p)} \cap \langle \bigcup_{q \neq p} G_{(q)} \rangle$, $g \neq 0$, potom $g = g_1 + g_2 + \cdots + g_n$, kde $\forall i = 1, ..., n\ \ g_i \neq 0\ \ g_i \in G_{(p_i)}\ \ p_i \neq p$, a lze předpokládat, že $p_i \neq p_j$ pro $i \neq j$. Označme $\forall i = 1, ..., n\ \ o(g_i) = p_i^{k_i}$, potom $(p_1^{k_1} \cdots p_n^{k_n})g = 0$, a tedy $\exists s \in \mathbb{N}$ tak, že $o(g)s = p_1^{k_1} \cdots p_n^{k_n}$. To je spor, neboť $p \neq p_i\ \ \forall i = 1, ..., n$. Tím $G_{(p)} \cap \langle \bigcup_{q \neq p} G_{(q)} \rangle = 0$. Nechť nyní $g \in G$ je libovolný prvek. Je-li $g = 0$, potom $g \in \langle \bigcup G_{(p)} \rangle$. Nechť tedy $g \neq 0$, potom $o(g) = m$, kde $m \in \mathbb{N}$, a $m = p_1^{k_1} \cdots p_n^{k_n}$ je prvočíselný rozklad čísla m.

Položme $m_i = \dfrac{m}{p_i^{k_i}} \quad \forall i = 1, ..., n$. Čísla $m_1, ..., m_n$ jsou nesoudělná, a tedy existují čísla $u_1, ..., u_n \in \mathbf{Z}$ tak, že $u_1 m_1 + \cdots + u_n m_n = 1$. Tím $g = u_1 m_1 g + \cdots + u_n m_n g$, a pro každé $i = 1, ..., n$ je $p_i^{k_i}(u_i m_i g) = u_i m g = 0$, a tím $u_i m_i g \in G_{(p_i)}$. Potom $g \in \langle \bigcup_p G_{(p)} \rangle$.

■

Lemma 2.1 *Buď G Abelova p-grupa obsahující prvek g největšího řádu $o(g) = p^k$, t.j. $o(x) \leq p^k \quad \forall x \in G$. Potom existuje podgrupa H grupy G taková, že $G = \langle g \rangle \oplus H$.*

Důkaz Označme $\mathcal{H} = \{K \ ; \ K \leq G, \ K \cap \langle g \rangle = 0\}$.
Protože $0 \in \mathcal{H}$, je $\mathcal{H} \neq \emptyset$. Množina $\mathcal{H}$, uspořádaná inkluzí $\subseteq$, je nahoru induktivní, a tedy podle Zornova lemmatu existuje prvek $H \in \mathcal{H}$, který je maximální v $\mathcal{H}$. H je podgrupa grupy G , $H \oplus \langle g \rangle \subseteq G$. Ukážeme, že $H \oplus \langle g \rangle = G$.
Označme $\bar{G} = H \oplus \langle g \rangle$ a předpokládejme, že $\bar{G} \neq G$. Potom $G/\bar{G} \neq 0$, a tedy existuje $x' \in G \setminus \bar{G}$ tak, že $x' + \bar{G} \neq 0$. Protože $G/\bar{G}$ je p-grupa, existuje $l \in \mathbb{N}$ takové, že $o(x' + \bar{G}) = p^l$.
Položme $\bar{x} = p^{l-1}(x' + \bar{G})$, potom $\bar{x} = x + \bar{G}$, kde $x \in G \setminus \bar{G}$ a $o(\bar{x}) = p$.
$0 = p\bar{x} = p(x + \bar{G}) = px + \bar{G}$, tím $px \in \bar{G} = H \oplus \langle g \rangle$, a tedy $px = h + ng$, kde $h \in H, \ n \in \mathbf{Z}$. Protože $o(x) \leq p^k$, je $0 = p^k x = p^{k-1}(px) = p^{k-1}h + p^{k-1}ng$, a protože $p^{k-1}ng = -p^{k-1}h \in \langle g \rangle \cap H = 0$, je $p^{k-1}ng = 0$, a tím $n = pm$, kde $m \in \mathbf{Z}$. Potom $h = p(x - mg)$. Protože $x \notin \bar{G}$, $x - mg \notin H$, a tím $H \subset \langle H \cup \langle x - mg \rangle \rangle$. Protože H byl maximální prvek množiny $\mathcal{H}$, $\langle H \cup \langle x - mg \rangle \rangle \notin \mathcal{H}$. Tím existuje prvek $y \neq 0$ takový, že $y \in \langle H \cup \langle x - mg \rangle \rangle \cap \langle g \rangle$, tedy $y = rg = h' + s(x - mg)$, kde $r, s \in \mathbf{Z}, \ h' \in H$.
Protože $y \neq 0$, $s(x - mg) \notin H$, a tím čísla p, s jsou nesoudělná. Pro $u, v \in \mathbf{Z}$ je $us + vp = 1$, a tím $x = (us + vp)x = u(sx) + v(px) \in \bar{G}$, což je spor. Tím $G = H \oplus \langle g \rangle$.

■

Věta 2.3 *Každá konečná Abelova p-grupa G je direktním součtem cyklických grup.*

Důkaz Označme $|G| = m$ - důkaz probíhá indukcí podle m .
Pro $m = 1$ je $G = 0 = \langle 0 \rangle$, pro $m = p$ je G cyklická grupa.
Nechť G je řádu m , nechť tvrzení platí pro grupy řádu menšího, potom grupa G má prvek největšího řádu, tedy $g \in G$ takový prvek, že $o(g) = p^k$, a pro každé $x \in G$ je $o(x) \leq p^k$. Podle lemmatu 2.1 existuje podgrupa H grupy G tak, že $G = \langle g \rangle \oplus H$. Potom $m = |G| = |\langle g \rangle| \cdot [G : \langle g \rangle] = p^k \cdot [G : \langle g \rangle]$. Protože $G/\langle g \rangle \cong H$, je $m = |G| = p^k \cdot |H|$. Tím $|H| < m$, a tedy
buď $H = 0$ a $G = \langle g \rangle$, a tím grupa G je cyklická,
nebo $H \neq 0$, a potom podle indukčního předpokladu je H direktní suma cyklických grup, a tím i G je direktním součtem cyklických grup.

■

Poznámka 2.2 Je-li G konečná Abelova p-grupa, potom $G = \bigoplus_{i=1}^{n} \langle g_i \rangle$, a pro každé $i = 1, ..., n$ je $o(g_i) = p^{k_i}$. Tím je $\langle g_i \rangle \cong Z_{(p^{k_i})}$, a tedy $G \cong Z_{(p^{k_1})} \oplus Z_{(p^{k_2})} \oplus \cdots \oplus Z_{(p^{k_n})}$, kde můžeme grupy seřadit tak, že $k_1 \geq k_2 \geq \cdots \geq k_n$.

Věta 2.4 *Nechť G je konečná Abelova p-grupa, nechť $G \cong Z(p^{k_1}) \oplus Z(p^{k_2}) \oplus \cdots \oplus Z(p^{k_n})$ je její direktní rozklad na cyklické grupy a $k_1 \geq k_2 \geq \cdots \geq k_n > 0$. Potom posloupnost čísel $(k_1, k_2, ..., k_n)$ je grupou G určena jednoznačně.*

Důkaz Nejdříve si uvědomme, že pro čísla $r \leq s$ je $p^r Z_{(p^s)} = Z_{(p^{s-r})}$.
Jestliže nyní máme dva direktní rozklady grupy G , $G \cong Z_{(p^{k_1})} \oplus Z_{(p^{k_2})} \oplus \cdots \oplus Z_{(p^{k_n})} = Z_{(p^{l_1})} \oplus Z_{(p^{l_2})} \oplus \cdots \oplus Z_{(p^{l_t})}$, $k_1 \geq k_2 \geq \cdots \geq k_n$, $l_1 \geq l_2 \geq \cdots \geq l_t$, potom podle důkazu věty 2.3 je $Z_{(p^{k_1})}$ i $Z_{(p^{l_1})}$ cyklická podgrupa maximálního řádu, tedy $k_1 = l_1$.
Nechť již $k_1 = l_1$, ..., $k_{i-1} = l_{i-1}$, ale $k_i < l_i$, potom
$p^{k_i} G \cong Z_{(p^{k_1-k_i})} \oplus \cdots \oplus Z_{(p^{k_{i-1}-k_i})} = Z_{(p^{l_1-k_i})} \oplus \cdots \oplus Z_{(p^{l_{i-1}-k_i})} \oplus Z_{(p^{l_i-k_i})}$. Protože $k_i < l_i$, je $Z_{(p^{l_i-k_i})} \neq 0$, a věta je dokázána sporem.

■

Důsledek 3 Každá konečná Abelova grupa G je direktním součtem cyklických grup, z nichž každá má řád mocninu prvočísla. Řády těchto grup a čísla udávající počet sčítanců stejného řádu jsou grupou G určeny jednoznačně.

Důkaz Podle vět 2.2 a 2.4 je $G \cong \bigoplus_p (Z_{(p^{k_1})} \oplus \cdots \oplus Z_{(p^{k_n})})$.

■

Věta 2.5 *Buď G konečná Abelova grupa řádu n , buď p prvočíslo, které dělí n , potom grupa G obsahuje prvek řádu p , a tedy i podgrupu řádu p .*

Důkaz Podle důsledku věty 2.4 je $G \cong \bigoplus_{i=1}^{m} (S_{(p_i^{k_{1i}})} \oplus \cdots \oplus Z_{(p_i^{k_{ni}})})$. Protože $p \mid n$, existuje $i = 1, ..., n$ tak, že $p = p_i$. Tím grupa G obsahuje cyklickou podgrupu $\langle a \rangle$ řádu $o(a) = p_i^{k_{1i}} = p^{k_{1i}}$, tedy $a \in G$ a $\langle a \rangle \cong Z_{(p^{k_{1i}})}$. Potom prvek $g = p^{k_{1i}-1} a \in G$, tento prvek g má řád p . $\langle g \rangle$ je podgrupa řádu p grupy G .

■

Důsledek 4 Je-li G konečná Abelova p-grupa, potom $|G| = p^l$, kde $l \in \mathbb{N}_0$.

Důkaz Označme $|G| = m$, nechť $m = p^l s$ a $(p, s) = 1$. Kdyby $s > 1$, potom existuje prvočíslo q tak, že $q \mid s$, a tedy $q \mid m$. Protože $(p, s) = 1$, je $p \neq q$. Podle věty 2.5 existuje prvek $g \in G$ řádu q , což je spor, neboť G je p-grupa.

■

3 Sylowovy podgrupy

Definice 3.1 *Nechť* $(G, \cdot)$ *je grupa (obecně nekomutativní). Řekneme, že prvek* g *grupy* G *je konjugovaný s prvkem* h *grupy* G *, jestliže existuje prvek* $x \in G$ *takový, že* $g = x^{-1}hx$ *.*

Poznámka 3.1 Relace R na množině G daná vztahem $xRy \Leftrightarrow x$ je konjugovaný s y , je na G ekvivalence, a tedy množinu G můžeme rozložit na třídy konjugovaných prvků.
Jestliže $g \in G$, potom třída prvků konjugovaných s prvkem g je jednoprvková právě tehdy, když prvek g komutuje s každým prvkem grupy G .

Definice 3.2 *Nechť* G *je grupa, potom množina* $C(G) = \{g \in G \ ; \ gh = hg \ \ \forall h \in G\}$ *se nazývá centrum grupy* G *.*
Je-li M *neprázdná podmnožina grupy G, pak množina* $N_G(M) = \{g \in G \ ; \ g^{-1}Mg = M\}$ *se nazývá normalizátor množiny* M *v grupě* G *. Je-li* $M = \{a\}$ *, potom píšeme* $N_G(a) = \{g \in G \ ; \ g^{-1}ag = a\}$ *.*

Poznámka 3.2 Centrum i normalizátor jsou podgrupy grupy G .

Lemma 3.1 *Nechť* G *je grupa, nechť* $x \in G$ *je její libovolný prvek. Označíme-li* A *množinu všech prvků konjugovaných s prvkem* x *, potom* $|A| = [G : N_G(x)]$ *.*

Důkaz Budeme definovat zobrazení $\varphi\colon G/N_G(x) \longrightarrow A$ předpisem
$\varphi\colon gN_G(x) \longmapsto gxg^{-1} \qquad \forall g \in G$.
Toto zobrazení je korektně definované a je to vzájemně jednoznačné zobrazení faktorgrupy $G/N_G(x)$ na množinu A .

■

Věta 3.1 *Nechť* G *je konečná grupa, nechť* R *je množina reprezentantů vybraných po jednom z každé alespoň dvouprvkové třídy konjugovaných prvků z* G *, potom*

$$|G| = |C(G)| + \sum_{x \in R} [G : N_G(x)].$$

Důkaz Podle poznámky 3.1 je $|C(G)|$ roven počtu jednoprvkových tříd konjugovaných prvků. Podle lemmatu 3.1 je počet prvků konjugovaných s prvkem x roven $[G : N_G(x)]$, pro každý prvek $x \in R$.

■

Věta 3.2 *Je-li* G *netriviální grupa taková, že* $|G| = p^k$ *, kde* $k \in \mathbb{N}$ *a* p *je prvočíslo, potom* $C(G) \neq 1$ *.*

Důkaz Podle věty 3.1 je $|C(G)| = |G| - \sum_{x \in R} [G : N_G(x)]$. Prvočíslo $p \mid |G|$ a podle Lagrangeovy věty $p \mid [G : N_G(x)]$, pro každé $x \in R$. Tím p dělí $|C(G)|$, a tedy $C(G) \neq 1$.

■

Definice 3.3 *Nechť konečná grupa G má řád $n = p^k m$, kde p je prvočíslo, $k \in \mathbb{N}$ a $(p, m) = 1$. Potom každá podgrupa H grupy G taková, že $|H| = p^k$, se nazývá Sylowova p-podgrupa grupy G (též sylowovská p-podgrupa grupy G).*

Věta 3.3 *Nechť G je konečná grupa řádu n, nechť prvočíslo p dělí n, potom grupa G obsahuje alespoň jednu Sylowovu p-podgrupu grupy G.*

Důkaz Indukcí podle n.
Nechť $n = p$, potom G je Sylowova p-podgrupa grupy G.
Nechť $n > p$, potom $n = p^k m$, kde $k \in \mathbb{N}$, $(p, m) = 1$.

a) Jestliže existuje vlastní podgrupa G_1 grupy G taková, že p nedělí $[G : G_1]$, potom podle Lagrangeovy věty p dělí $|G_1|$, a tedy podle indukčního předpokladu existuje H Sylowova p-podgrupa grupy G_1. H je také Sylowova p-podgrupa grupy G.

b) Jestliže pro každou podgrupu G_1 grupy G prvočíslo p dělí $[G : G_1]$, podle věty 3.1 prvočíslo p dělí $|C(G)|$. Grupa $C(G)$ je Abelova, a tedy podle věty 2.5 existuje podgrupa H_1 grupy $C(G)$ taková, že $|H_1| = p$. Podle Lagrangeovy věty $[G : H_1] = |G/H_1| = p^{k-1}m$. Jestliže $k = 1$, je H_1 Sylowova p-podgrupa grupy G. Jestliže $k > 1$, potom podle indukčního předpokladu existuje $\bar{H}$ Sylowova p-podgrupa grupy G/H_1, $\left|\bar{H}\right| = p^{k-1}$. Potom existuje podgrupa H grupy G taková, že $\bar{H} = H/H_1$. Tím $|H| = |H_1| \cdot [H : H_1] = |H_1| \cdot \left|\bar{H}\right| = p \cdot p^{k-1} = p^k$, a tedy H je Sylowova p-podgrupa grupy G.

■

Lemma 3.2 *Nechť G je konečná grupa řádu n, nechť prvočíslo p dělí n, nechť $\mathcal{M}$ je třída konjugovaných Sylowových p-podgrup grupy G, potom $|\mathcal{M}|$ dělí n a $(|\mathcal{M}|, p) = 1$.*

Důkaz Buď $P \in \mathcal{M}$, potom $\mathcal{M} = \{g^{-1}Pg \ ; \ g \in G\}$, P je Sylowova p-podgrupa grupy G, $|G| = n = p^k m$, kde $k \in \mathbb{N}$, $(p, m) = 1$, $|P| = p^k$.
Podle důkazu lemmatu 3.1 je $|\mathcal{M}| = [G : N_G(P)]$. Podle Lagrangeovy věty je $p^k m = n = |G| = |N_G(P)| \cdot [G : N_G(P)] = |N_G(P)| \cdot |\mathcal{M}|$. Tím $|\mathcal{M}|$ dělí n. Protože $P \leq N_G(P)$, je $|N_G(P)| = p^k s$, kde $s \in \mathbb{N}$. Potom $p^k m = n = p^k s \cdot |\mathcal{M}|$, a tedy $m = s \cdot |\mathcal{M}|$. Tím $(|\mathcal{M}|, p) = 1$.

■

Lemma 3.3 *Buď G konečná grupa, buď P její Sylowova p-podgrupa. Jestliže H je p-podgrupa grupy $N_G(P)$, potom $H \subseteq P$.*

Důkaz Označme opět $|G| = n = p^k m$, kde $k \in \mathbb{N}$, $(p, m) = 1$, $|P| = p^k$. Protože H je p-podgrupa, je $|H| = p^l$. Podgrupa P je normální podgrupa grupy $N_G(P)$, H je podgrupa grupy $N_G(P)$, potom podle 3. věty o izomorfismu je $PH/P \cong H/P \cap H$.

Tím $p^l = |H| = |P \cap H| \cdot [H : P \cap H]$, a tedy $|H/P \cap H| = p^t \leq p^l$. Dále $|PH| = |P| \cdot |PH/P| = p^k \cdot p^t = p^{k+t}$. Protože PH je p-podgrupa grupy G , a P je Sylowova p-podgrupa grupy G , je $t = 0$. Tím $H/P \cap H = 1$, a tedy $H = P \cap H$ a $H \subseteq P$.

■

Věta 3.4 *(1. Sylowova věta)*
Každá p-podgrupa H konečné grupy G je obsažena v některé Sylowově p-podgrupě grupy G .

Důkaz Nechť $|H| = p^l$, kde $l \in \mathbb{N}$. Podle věty 3.3 existuje Q Sylowova p-podgrupa grupy G , potom $|Q| = p^k$, kde $|G| = n = p^k m$, $k \in \mathbb{N}$, $(p, m) = 1$. Označme $\mathcal{M} = \{g^{-1}Qg \ ; \ g \in G\}$, tedy třídu konjugovaných Sylowových p-podgrup. Vezměme libovolnou podgrupu $P \in \mathcal{M}$ a označme $\mathcal{M}_P = \{xPx^{-1} \ ; \ x \in H\}$. Potom pro podgrupu $H_P = \{x \in H \ ; \ x^{-1}Px = P\}$ opět platí $|\mathcal{M}_P| = [H : H_P] = |H/H_P|$. Tím $|\mathcal{M}_P| = p^t \leq p^l = |H|$. Množinu $\mathcal{M}$ můžeme rozdělit na navzájem disjunktní podmnožiny, tedy $\mathcal{M} = \bigcup_P \mathcal{M}_P$, a tím $|\mathcal{M}| = \sum_P |\mathcal{M}_P|$. Protože $(|\mathcal{M}|, p) = 1$, existuje $P \in \mathcal{M}$ tak, že $|\mathcal{M}_P| = p^0 = 1$. Tím pro každé $x \in H$ je $xPx^{-1} = P$, a tedy $H \leq N_G(P)$, a podle lemmatu 3.3 je $H \subseteq P$.

■

Poznámka 3.3 Uvědomme si, že jsme vlastně dokázali tvrzení silnější. Dokázali jsme, že pro každou p-podgrupu H grupy G existuje $P \in \mathcal{M}$ taková, že $H \subseteq P$. Tedy existuje Sylowova p-podgrupa z dané třídy konjugovaných Sylowových p-podgrup.

Věta 3.5 *(2. Sylowova věta)*
Libovolné dvě Sylowovy p-podgrupy konečné grupy G jsou spolu konjugované.

Důkaz Nechť P_1, P_2 jsou dvě Sylowovy p-podgrupy grupy G .
Označme $\mathcal{M} = \{g^{-1}P_1 g \ ; \ g \in G\}$, tedy třídu Sylowových p-podgrup grupy G konjugovaných s P_1 . P_2 je p-podgrupa, a tedy podle poznámky 3.3 existuje $P \in \mathcal{M}$ tak, že $P_2 \subseteq P$. Protože podgrupy P_2, P jsou obě Sylowovy, je $|P_2| = |P|$, a tudíž $P_2 = P$. Protože $P \in \mathcal{M}$, je podgrupa P_2 konjugovaná s P_1 .

■

Věta 3.6 *(3. Sylowova věta)*
Je-li r počet všech Sylowových p-podgrup konečné grupy G , potom r dělí $|G|$ a $r = 1 + sp$, kde $s \in \mathbf{Z}$, $s \geq 0$.

Důkaz Zvolme pevně Sylowovu p-podgrupu Q grupy G a označme $\mathcal{M}$ množinu všech Sylowových p-podgrup grupy G . Tedy $|\mathcal{M}| = r$. Pro $P_1 \in \mathcal{M}$ vytvoříme $\mathcal{M}_{P_1} = \{xP_1x^{-1} \ ; \ x \in Q\}$. Buď $\mathcal{M}_{P_1} = \mathcal{M}$, nebo existuje $P_2 \in \mathcal{M} \setminus \mathcal{M}_{P_1}$, a potom vytvoříme $\mathcal{M}_{P_2} = \{xP_2x^{-1} \ ; \ x \in Q\}$. Protože $\mathcal{M}_{P_1} \cap \mathcal{M}_{P_2} = \emptyset$, a množina $\mathcal{M}$ je konečná, získáme po konečně mnoha krocích disjunktní rozklad množiny $\mathcal{M} = \mathcal{M}_{P_1} \cup \mathcal{M}_{P_2} \cup \cdots \cup \mathcal{M}_{P_t}$. Podgrupa $Q \in \mathcal{M}$, a tedy existuje i tak, že $Q \in \mathcal{M}_{P_i}$. Předpokládejme očíslování tak,

že $Q \in \mathcal{M}_{P_1}$. Potom $\mathcal{M}_{P_1} = \mathcal{M}_Q = \{Q\}$, tím $|\mathcal{M}_{P_1}| = 1$.
Pro každé $i = 2, ..., t$, pro třídu $\mathcal{M}_{P_i}$ konjugovaných Sylowových p-podgrup označme $Q_{P_i} = \{x \in Q \ ; \ x^{-1}P_i x = P_i\}$, potom $|\mathcal{M}_{P_i}| = [Q : Q_{P_i}] = |Q/Q_{P_i}|$. Podle Lagrangeovy věty je $|Q| = [Q : Q_{P_i}] \cdot |Q_{P_i}| = |\mathcal{M}_{P_i}| \cdot |Q_{P_i}|$, a tedy $|\mathcal{M}_{P_i}| = p^{k_i} \leq p^k = |Q|$. Potom $r = |\mathcal{M}| = |\mathcal{M}_{P_1}| + |\mathcal{M}_{P_2}| + \cdots + |\mathcal{M}_{P_t}| = 1 + p^{k_2} + \cdots + p^{k_t}$.
Kdyby existoval index $i = 2, ..., t$ tak, že $|\mathcal{M}_{P_i}| = p^0 = 1$, potom $\{P_i\} = \mathcal{M}_{P_i} = \{xP_ix^{-1} \ ; \ x \in Q\}$, a potom $Q \subseteq N_G(P_i)$, tudíž $Q = P_i$. To však není možné, tedy pro každé $i = 2, ..., t$ je $k_i \geq 1$, a tedy $r = 1+p^{k_2}+\cdots+p^{k_t} = 1+p(p^{k_2-1}+\cdots+p^{k_t-1}) = 1+ps$.
■

Důsledek 5 Nechť p, q jsou různá prvočísla, nechť G je konečná grupa řádu pq . Je-li $q < p$, potom grupa G obsahuje právě jedinou podgrupu řádu p a tato podgrupa je normální v G .

Důkaz Podle věty 3.3 existuje Sylowova p-podgrupa P grupy G , $|P| = p$. Je-li r počet všech Sylowových p-podgrup grupy G , potom podle věty 3.6 je $r = 1 + ps$, kde $s \in \mathbf{Z}$, $s \geq 0$, a existuje $u \in \mathbb{N}$ tak, že $ru = pq$. Potom $pq = ru = (1 + sp)u$, tím $p \mid u$, a tedy $u \geq p$. Kdyby $s > 0$, potom $1 + sp > p$, a tedy $u < q$, tím $u < p$, což je spor. Tedy $s = 0$, a tudíž $r = 1$.
Protože pro každé $g \in G$ je $g^{-1}Pg$ Sylowova p-podgrupa grupy G , a protože P je jediná Sylowova p-podgrupa grupy G , je $g^{-1}Pg = P$ pro každé $g \in G$.
■

Důsledek 6 Nechť G je grupa řádu p^2 , kde p je prvočíslo. Potom G je Abelova grupa, která je buď cyklická řádu p^2 nebo je direktním součtem dvou cyklických grup řádu p .

Důkaz Protože $|G| = p^2$, je podle věty 3.2 $C(G) \neq 1$, $p^2 = |G| = |C(G)| \cdot [G : C(G)]$. Je-li $[G : C(G)] = 1$, $|C(G)| = p^2$, potom G je Abelova.
Je-li $[G : C(G)] = p$, $|C(G)| = p$, potom grupa $G/C(G)$ je cyklická, a tedy existuje $a \in G \setminus C(G)$ tak, že $G/C(G) = \langle aC(G)\rangle$. Tím $G = \langle a\rangle C(G)$. Pro každé $g_1, g_2 \in G$ je $g_1 = a^n h_1$, $g_2 = a^m h_2$, kde $m, n \in \mathbf{Z}$, $h_1, h_2 \in C(G)$, potom $g_1g_2 = a^n h_1 a^m h_2 = a^{n+m} h_1 h_2 = a^m h_2 a^n h_1 = g_2g_1$. Tím je grupa G Abelova a tvrzení plyne z věty 2.3.
■

4 Okruhy a tělesa

Definice 4.1 *Mějme neprázdnou množinu* R *se dvěma operacemi* $\star$, $\circ$, *pro něž platí:*

1. $(R, \star)$ *je Abelova grupa.*
2. *Pro každé* $a, b, c \in R$ *je*

$$a \circ (b \star c) = (a \circ b) \star (a \circ c),$$

$$(b \star c) \circ a = (b \circ a) \star (c \circ a).$$

Potom R *se nazývá okruh.*
Jestliže operace $\circ$ *je asociativní, t.j.* $(a \circ b) \circ c = a \circ (b \circ c)$ *pro každé* $a, b, c \in R$, *potom okruh* R *je asociativní okruh.*
Jestliže operace $\circ$ *je komutativní, t.j.* $a \circ b = b \circ a$ *pro každé* $a, b \in R$, *potom* R *je komutativní okruh.*
Prvek $e \in R$ *okruhu* R *se nazývá jednotkový prvek okruhu* R , *jestliže* $a \circ e = e \circ a = a$ *pro každé* $a \in R$.

Poznámka 4.1

1. Bývá zvykem operaci $\star$ značit $+$ a nazývat sčítání v okruhu R a operaci $\circ$ značit $\cdot$ a nazývat násobení v okruhu R .
2. V okruhu $(R, +, \cdot)$ platí:
   $a \cdot 0 = 0 \cdot a = 0$ $\quad \forall a \in R$,
   $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ $\quad \forall a, b \in R$,
   $(na) \cdot b = n(a \cdot b) = a \cdot (nb)$ $\quad \forall a, b \in R$, $\forall n \in \mathbf{Z}$.
3. Má-li okruh R jednotkový prvek, potom je tento prvek určen jednoznačně a značí se 1 .

Definice 4.2 *Jsou-li* R, S *dva okruhy a* $\varphi \colon R \longrightarrow S$ *zobrazení, potom* φ *je homomorfismus okruhů, jestliže pro každé* $a, b \in R$ *je*

$$\varphi(a + b) = \varphi(a) + \varphi(b),$$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Definice 4.3 *Číslo* $n \in \mathbb{N}$ *se nazývá charakteristika okruhu* R , *jestliže* n *je nejmenší přirozené číslo takové, že* $na = 0$ *pro každé* $a \in R$.
Jestliže v nějakém okruhu R *takové* n *neexistuje, potom klademe charakteristiku okruhu* R *rovnou* 0 .
Píšeme: $\mathrm{char} R$.

Lemma 4.1

1. *Jestliže* R *je okruh s jednotkovým prvkem* 1 *, potom platí:*

   (a) *Jestliže pro každé* $n \in \mathbb{N}$ *je* $n \cdot 1 \neq 0$ *, potom* $\mathrm{char}R = 0$ *.*

   (b) *Jesliže* n *je nejmenší přirozené číslo takové, že* $n \cdot 1 = 0$ *, potom* $\mathrm{char}R = n$ *.*

2. *Jestliže* $\mathrm{char}R = n$ *a existuje* $m \in \mathbb{N}$ *takové, že* $m \cdot a = 0$ *pro každé* $a \in R$ *, potom* $n > 0$ *a* $n \mid m$ *.*

Důkaz
1. $na = n(1 \cdot a) = (n \cdot 1) \cdot a$ pro každé $a \in R$.
2. $m = nq + r$, kde $0 \leq r < n$, potom $0 = ma = (nq+r)a = q(na)+ra = q \cdot 0 + ra = ra$.
Protože $r < n$ a n bylo takové nejmeší přirozené číslo, je $r = 0$. Tím $n \mid m$.

■

Věta 4.1 *Nechť* R *je konečný okruh s charakteristikou* $\mathrm{char}R = p$ *, kde* p *je prvočíslo, potom existuje* $k \in \mathbb{N}$ *tak, že* $|R| = p^k$ *.*
Navíc pro grupu $(R, +)$ *platí:* $(R, +) = \bigoplus_{i=1}^{k} G_i$ *, kde pro každé* $i = 1, ..., k$ *je* $G_i \cong Z_{(p)}$ *.*

Důkaz Protože $pa = 0$ pro každé $a \in R$, je $(R, +)$ Abelova p-grupa, a tedy podle věty 3.3 je $(G, +) = \bigoplus_{i=1}^{k} G_i$, kde pro každé $i = 1, ..., k$ je G_i cyklická p-grupa. Protože $pa = 0$ pro každé $a \in R$, je $G_i \cong Z_{(p)}$. Tím také $|G| = p^k$.

■

Definice 4.4 *Nechť* $(R, +, \cdot)$ *je okruh a* S *je neprázdná podmnožina množiny* R *. Řekneme, že* S *je podokruh okruhu* R *, jestliže* $(S, +, \cdot)$ *je okruh.*

Poznámka 4.2

1. S je podokruh okruhu R právě tehdy, když pro každé $a, b \in S$ je $a - b \in S$ a $a \cdot b \in S$.

2. Jestliže pro každé $i \in I$ je S_i podokruh okruhu R , potom také $\bigcap_{i \in I} S_i$ je podokruh okruhu R .

3. Jestliže pro každé $i \in \mathbb{N}$ je S_i podokruh okruhu R a $S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots$, potom $\bigcup_{i \in \mathbb{N}} S_i$ je podokruh okruhu R .

4. Je-li okruh R asociativní nebo komutativní a S je jeho podokruh, potom S je též asociativní či komutativní.

5. Je-li R okruh s jednotkovým prvkem 1_R a S je podokruh okruhu R , potom S nemusí mít jednotkový prvek nebo může mít jednotkový prvek 1_S , ale je možné, že $1_R \neq 1_S$.

Definice 4.5 *Nechť* $(R,+,\cdot)$ *je okruh.*
Podgrupa I *aditivní grupy* $(R,+)$ *se nazývá levý ideál okruhu* R *, jestliže pro každé* $b\in I$ *a pro každé* $r\in R$ *je* $r\cdot b\in I$ *.*
Podgrupa I *aditivní grupy* $(R,+)$ *se nazývá pravý ideál okruhu* R *, jestliže pro každé* $b\in I$ *a pro každé* $r\in R$ *je* $b\cdot r\in I$ *.*
Řekneme, že I *je ideál okruhu* R *, jestliže* I *je levý a současně pravý ideál okruhu* R *.*

Definice 4.6 *Řekneme, že levý ideál* I *okruhu* R *je maximální, jestliže* $I\neq R$ *a v množině všech levých ideálů okruhu* R *s uspořádáním* $\subseteq$ *je tento ideál maximální prvek, t.j. neexistuje levý ideál* J *takový, že* $I\subset J\subset R$ *a* $I\neq J$ *,* $J\neq R$ *.*
Analogicky lze definovat maximální pravý ideál okruhu R *nebo maximální ideál okruhu* R *.*

Definice 4.7 *Nechť* I *je ideál okruhu* $(R,+,\cdot)$ *, potom* $(R/I,+)$ *je Abelova grupa se sčítáním*

$$(a+I)+(b+I)=(a+b)+I.$$

Jestliže na tuto množinu definujeme násobení předpisem

$$(a+I)\cdot(b+I)=(a\cdot b)+I$$

pro každé $a+I,b+I\in R/I$ *, získáme okruh* $(R/I,+,\cdot)$ *, který nazýváme faktorokruh okruhu* R *podle ideálu* I *.*
Zobrazení $\pi\colon R\longrightarrow R/I$ *definované předpisem*
$\pi\colon a\longmapsto a+I \qquad \forall a\in R$
je homomorfismus okruhu R *na faktorokruh* R/I *a nazývá se přirozená projekce okruhu* R *na* R/I *.*

Poznámka 4.3 Je-li $\varphi\colon R\longrightarrow S$ homomorfismus okruhů, potom obraz

$$\operatorname{Im}\varphi=\{s\in S\ ;\ \exists r\in R\quad \varphi(r)=s\}$$

je podokruh okruhu S a jádro

$$\operatorname{Ker}\varphi=\{r\in R\ ;\ \varphi(r)=0\}$$

je podokruh, dokonce ideál okruhu R .

Věta 4.2 *(o izomorfismu)*
Nechť $\varphi\colon R\longrightarrow S$ *je homomorfismus okruhu* R *do okruhu* S *, potom*

$$R/\operatorname{Ker}\varphi\cong\operatorname{Im}\varphi.$$

Důkaz Zobrazení $\psi\colon R/\operatorname{Ker}\varphi\longrightarrow\operatorname{Im}\varphi$ definované předpisem
$\psi\colon a+\operatorname{Ker}\varphi\longmapsto\varphi(a) \qquad \forall a+\operatorname{Ker}\varphi\in R/\operatorname{Ker}\varphi$
je hledaný, korektně definovaný izomorfismus.

■

Definice 4.8 *Netriviální asociativní okruh* R *se nazývá těleso, jestliže* $(R \setminus \{0\}, \cdot)$ *je grupa.*

Lemma 4.2 *Těleso nemá dělitele nuly,*
t.j. v tělese R *pro každé* $a, b \in R$, $a \neq 0$, $b \neq 0$ *je* $a \cdot b \neq 0$.

Důkaz Nechť $a, b \in R$, $a \neq 0$, $b \neq 0$ a $a \cdot b = 0$. Protože R je těleso, existuje $a^{-1} \in R$ takový, že $a \cdot a^{-1} = a^{-1} \cdot a = 1$, potom $0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1 \cdot b = b \neq 0$, což je spor.

■

Věta 4.3 *Nechť* R *je asociativní okruh, jehož násobení není nulové. Potom následující podmínky jsou ekvivalentní.*

1. 0 *a* R *jsou jediné levé ideály okruhu* R .
2. R *je těleso.*
3. 0 *a* R *jsou jediné pravé ideály okruhu* R .

Důkaz
2. $\Rightarrow$ 1. Buď I nenulový levý ideál okruhu R , potom existuje $a \in I$, $a \neq 0$. Protože R je těleso, existuje $a^{-1} \in R$. Tím $1 = a^{-1} \cdot a \in I$, a tedy pro každé $r \in R$ je $r = r \cdot 1 \in I$.
1. $\Rightarrow$ 2. Označme $I = \{a \in R \,;\, R \cdot a = 0\}$. Tato množina I je ideál (levý i pravý) okruhu R . Podle 1. podmínky je nyní buď $I = 0$ nebo $I = R$. Protože násobení na R není nulové, je $I = 0$, tedy pro každé $a \in R$, $a \neq 0$ je $R \cdot a \neq 0$.
Nyní $R \cdot a = \{r \cdot a \,;\, r \in R\}$ je zřejmě levý ideál okruhu R . Opět podle 1. podmínky je $R \cdot a = R$ pro každé $a \in R$, $a \neq 0$.
Nyní označme $A = \{x \in R \,;\, x \cdot a = 0\}$, kde $a \in R$, $a \neq 0$. Tato množina je opět levý ideál okruhu R a podle 1. podmínky je buď $A = 0$ nebo $A = R$. Protože pro $a \neq 0$ je $R \cdot a = R$, je $A = 0$. Tedy pro každé $a \in R$, $a \neq 0$ a pro každé $x \in R$, $x \neq 0$ je $x \cdot a \neq 0$.
Nyní vezměme libovolné $a \in R$, $a \neq 0$, potom je $R \cdot a = R$, a tedy existuje $e \in R$ tak, že $a = e \cdot a$. Pro každé $b \in R$, $b \neq 0$ je $b \cdot a = b \cdot (e \cdot a) = (b \cdot e) \cdot a$, a tedy $(b - b \cdot e) \cdot a = 0$. Protože $a \neq 0$, je $b = b \cdot e$. Dále pro každé $b \in R$, $b \neq 0$ je $a \cdot b = (a \cdot e) \cdot b = a \cdot (e \cdot b)$, tím $a \cdot (b - e \cdot b) = 0$, a tedy $b = e \cdot b$. Tím jsme ukázali, že pro každé $b \in R$, $b \neq 0$ je $b \cdot e = e \cdot b = b$. Protože také $0 \cdot e = e \cdot 0 = 0$, je e jednotkový prvek okruhu R .
Nyní pro každé $a \in R$, $a \neq 0$ je $R \cdot a = R$, a tedy existuje $b \in R$ tak, že $b \cdot a = e$. Je jasné, že $b \neq 0$, potom $R \cdot b = R$, a tedy existuje $c \in R$ tak, že $c \cdot b = e$. Tím $b \cdot a = e = c \cdot b$ a zřejmě $c \neq 0$. Nyní je $a = e \cdot a = (c \cdot b) \cdot a = c \cdot (b \cdot a) = c \cdot e = c$, tím $b \cdot a = a \cdot b = e$, a tedy $b = a^{-1}$.
2. $\Leftrightarrow$ 3. se dokazuje analogicky.

■

Důsledek 7 Je-li $\varphi: R \longrightarrow S$ homomorfismus těles, potom buď $\varphi = 0$ nebo φ je prosté zobrazení.

Důkaz $\operatorname{Ker}\varphi$ je levý ideál tělesa R, a tedy buď $\operatorname{Ker}\varphi = R$ nebo $\operatorname{Ker}\varphi = 0$.

■

Důsledek 8 Nechť R je asociativní okruh, I je ideál okruhu R takový, že $R \cdot R \not\subseteq I$, potom platí:
R/I je těleso právě tehdy, když I je maximální levý ideál okruhu R.

Důkaz R/I je těleso právě tehdy, když $0 = I/I$ a R/I jsou jediné levé ideály okruhu R/I a to je právě tehdy, když I je maximální levý ideál okruhu R.

■

Definice 4.9 *Nechť R je asociativní, komutativní okruh s jednotkou, nechť I je ideál okruhu R. Řekneme, že prvky $a, b \in R$ jsou kongruentní modulo ideál I, jestliže $a - b \in I$.*
Píšeme: $a \equiv b \pmod{I}$.

Lemma 4.3 *Nechť R je asociativní, komutativní okruh s jednotkou, nechť I_1, I_2 jsou ideály okruhu R takové, že $I_1 + I_2 = R$. Mějme $\lambda_1, \lambda_2 \in R$ libovolné prvky okruhu R, potom existuje prvek $\lambda \in R$ takový, že $\lambda \equiv \lambda_1 \pmod{I_1}$ a $\lambda \equiv \lambda_2 \pmod{I_2}$.*

Důkaz Protože $\lambda_1 \in R = I_1 + I_2$, existují prvky $\lambda_{11} \in I_1$ a $\lambda_{12} \in I_2$ tak, že $\lambda_1 = \lambda_{11} + \lambda_{12}$. Stejně $\lambda_2 \in R = I_1 + I_2$, a tedy existují prvky $\lambda_{21} \in I_1$ a $\lambda_{22} \in I_2$ tak, že $\lambda_2 = \lambda_{21} + \lambda_{22}$.
Nyní položme $\lambda = \lambda_{12} + \lambda_{21}$.
Potom $\lambda - \lambda_1 = \lambda_{12} + \lambda_{21} - \lambda_{11} - \lambda_{12} = \lambda_{21} - \lambda_{11} \in I_1$, a tedy $\lambda \equiv \lambda_1 \pmod{I_1}$.
Stejně $\lambda - \lambda_2 = \lambda_{12} + \lambda_{21} - \lambda_{21} - \lambda_{22} = \lambda_{12} - \lambda_{22} \in I_2$, a tedy $\lambda \equiv \lambda_2 \pmod{I_2}$.

■

Věta 4.4 *(čínská věta o zbytku)*
Nechť R je asociativní, komutativní okruh s jednotkou, nechť $I_1, I_2, ..., I_n$ jsou ideály okruhu R takové, že pro každé $i = 1, 2, ..., n$ je $I_i + \bigcap_{\substack{j=1 \\ j \neq i}}^{n} I_j = R$. Mějme libovolné prvky $\lambda_1, \lambda_2, ..., \lambda_n \in R$, potom existuje prvek $\lambda \in R$ takový, že pro každé $i = 1, 2, ..., n$ je

$$\lambda \equiv \lambda_i \pmod{I_i}.$$

Důkaz Indukcí podle n.
Pro $n = 2$ - viz lemma 4.3.
Nechť $k \leq n$ a nechť tvrzení platí pro $k - 1$.
Pro každé $i = 1, ..., k-1$ je $I_i + \bigcap_{\substack{j=1 \\ j \neq i}}^{k-1} I_j \supseteq I_i + \bigcap_{\substack{j=1 \\ j \neq i}}^{n} I_j = R$, a tedy podle indukčního

předpokladu existuje $\lambda' \in R$ takové, že pro každé $i = 1, ..., k-1$ je $\lambda' \equiv \lambda_i \pmod{I_i}$.
Nyní $I_k + \bigcap_{j=1}^{k-1} I_j \supseteq I_k + \bigcap_{\substack{j=1 \\ j\neq k}}^{n} I_j = R$, a tedy podle lemmatu 4.3 existuje prvek $\lambda \in R$ tak, že $\lambda \equiv \lambda' \pmod{\bigcap_{j=1}^{k-1} I_j}$ a $\lambda \equiv \lambda_k \pmod{I_k}$.

Nyní pro každé $i = 1, ..., k-1$ je $\lambda' - \lambda_i \in I_i$ a $\lambda - \lambda' \in \bigcap_{j=1}^{k-1} I_j \subseteq I_i$, tedy
$\lambda - \lambda_i = (\lambda - \lambda') + (\lambda' - \lambda_i) \in I_i$.
Tím pro každé $i = 1, ..., k$ je $\lambda \equiv \lambda_i \pmod{I_i}$.

■

Věta 4.5 *(čínská věta o zbytku)*
Nechť R je asociativní, komutativní okruh s jednotkou 1 , nechť $I_1, I_2, ..., I_n$ jsou ideály okruhu R takové, že pro každé $i \neq j$ je $I_i + I_j = R$. Potom pro libovolné prvky $\lambda_1, \lambda_2, ..., \lambda_n \in R$ existuje prvek $\lambda \in R$ takový, že pro každé $i = 1, ..., n$ je

$$\lambda \equiv \lambda_i \pmod{I_i} .$$

Důkaz Ukážeme, že pro každé $i = 1, ..., n$ je $I_i + \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j = R$.

Vezměme $i \in \{1, ..., n\}$, potom pro každé $j \in \{1, ..., n\}$, $j \neq i$ je $I_i + I_j = R$, a tedy $1 = l_{ij} + l_j$, kde $l_{ij} \in I_i$ a $l_j \in I_j$. Potom $1 = 1 \cdot 1 \cdot 1 \cdots 1 = \prod_{\substack{j=1 \\ j\neq i}}^{n} (l_{ij} + l_j) =$
$(l_1 \cdot l_2 \cdots l_{i-1} \cdot l_{i+1} \cdots l_n) + x$, kde $(l_1 \cdot l_2 \cdots l_{i-1} \cdot l_{i+1} \cdots l_n) \in \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j$ a $x \in I_i$. Protože
$1 \in \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j + I_i$, je $R = \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j + I_i$.
Tvrzení věty nyní plyne z věty 4.4.

■

Věta 4.6 *(důsledek čínské věty o zbytku)*
Nechť R je asociativní, komutativní okruh s jednotkou, nechť $I_1, I_2, ..., I_n$ jsou po dvou různé maximální ideály okruhu R . Potom pro libovolné prvky $\lambda_1, \lambda_2, ..., \lambda_n \in R$ existuje prvek $\lambda \in R$ takový, že pro každé $i = 1, ..., n$ je

$$\lambda \equiv \lambda_i \pmod{I_i} .$$

Důkaz Pro každé $i \neq i$ jsou I_i a I_j různé maximální ideály okruhu R , a tedy $I_i + I_j = R$. Tvrzení nyní plyne z věty 4.5.

■

5 Reprezentace grup

V celé kapitole bude G konečná grupa, V_n vektorový prostor dimenze n nad tělesem T.
Označme:

$$\operatorname{Aut} V_n = \{\varphi \mid \varphi: V_n \longrightarrow V_n \text{ je automorfismus}\}$$

Uvědomíme si, že $\operatorname{Aut} V_n$ s operací skládání $\circ$ je grupa.

Je-li $b_1, b_2, ..., b_n$ báze prostoru V_n, potom pro každé $\varphi \in \operatorname{Aut} V_n$ označme $\mathbf{A}_\varphi$ matici automorfismu φ v bázi $b_1, b_2, ..., b_n$, t.j. $\mathbf{A}_\varphi = [\widehat{\varphi(b_1)} \mid \widehat{\varphi(b_2)} \mid ... \mid \widehat{\varphi(b_n)}]$. Protože automorfismus je izomorfismus z prostoru V_n na stejný prostor V_n, je matice $\mathbf{A}_\varphi$ regulární.

Definice 5.1 *Je-li G konečná grupa, V_n vektorový prostor dimenze n nad tělesem T, potom každý homomorfismus $h: G \longrightarrow \operatorname{Aut}(V_n)$ se nazývá reprezentace grupy G ve V_n. Dimenze prostoru V_n se nazývá stupeň reprezentace h.*

Je-li h reprezentace grupy G ve V_n, potom pro každé $g_1, g_2 \in G$ je $h(g_1 g_2) = h(g_1) \circ h(g_2)$, t.j. pro každé $x \in V_n$ je $h(g_1 g_2)(x) = (h(g_1) \circ h(g_2))(x) = h(g_1)(h(g_2)(x))$.

Je-li $b_1, b_2, ..., b_n$ báze prostoru V_n, potom pro reprezentaci $h: G \longrightarrow \operatorname{Aut} V_n$ je pro každé $g \in G$ prvek $h(g) \in \operatorname{Aut} V_n$, a tedy v bázi $b_1, b_2, ..., b_n$ má regulární matici $h^M(g)$ řádu n.
Označíme:

$$\mathcal{R}_n = \{\ \mathbf{A} \mid \mathbf{A} \text{ je regulární matice řádu } n\ \}$$

Zobrazení $h^M: G \longrightarrow \mathcal{R}_n$ je homomorfismus, protože při skládání zobrazení se matice násobí, a tím $h^M(g_1 g_2) = h^M(g_1) h^M(g_2)$.
Lze tedy mluvit o maticové reprezentaci h^M grupy G.

Definice 5.2 *Říkáme, že dvě reprezentace $h: G \longrightarrow \operatorname{Aut} V_n$, $k: G \longrightarrow \operatorname{Aut} W_m$ jsou ekvivalentní, jestliže existuje izomorfismus $f: V_n \longrightarrow W_m$ tak, že pro každý prvek $g \in G$ je $f \circ h(g) = k(g) \circ f$.*

Potom nutně $m = n$.

Zvolíme-li $b_1, b_2, ..., b_n$ bázi V_n, $w_1, w_2, ..., w_m$ bázi prostoru W_m, potom reprezentace $h: G \longrightarrow \operatorname{Aut} V_n$, $k: G \longrightarrow \operatorname{Aut} W_m$ jsou ekvivalentní, právě tehdy, když jsou ekvivalentní maticové reprezentace a to je právě tehdy, když $m = n$ a existuje regulární matice F taková, že pro každé $g \in G$ je $F h^M(g) = k^M(g) F$.

Odvození regulární reprezentace h^r.
Nechť G konečná grupa, $|G| = m$, nechť $G = \{g_1, g_2, ..., g_m\}$ jsou všechny prvky grupy G.
Buď V_m vektorový prostor dimenze m, buď báze prostoru V_m označena $e_{g_1}, e_{g_2}, ..., e_{g_m}$.
Definujme zobrazení $h^r: G \longrightarrow \operatorname{Aut} V_m$ tak, že pro každé $g \in G$ je $h^r(g) \in \operatorname{Aut} V_m$ definován tak, že $h^r(g)(e_{g_i}) = e_{g g_i}$.
Toto zobrazení je reprezentace konečné grupy G ve V_m.

Definice 5.3 *Každá reprezentace konečné grupy G, která je ekvivalentní s touto reprezentací h^r, se nazývá regulární reprezentace.*

Věta 5.1 *Reprezentace h konečné grupy G ve W_m je regulární právě tehdy, když $|G| = m$ a existuje prvek $w_0 \in W_m$ takový, že množina m vektorů $\{v_g = h(g)(w_0) \mid g \in G\}$ tvoří bázi prostoru W_m.*

Důkaz Nechť h je regulární reprezentace. Potom h je ekvivalentní s h^r, a tedy existuje izomorfismus $f: V_m \longrightarrow W_m$ takový, že pro každé $g \in G$ je $f \circ h^r(g) = h(g) \circ f$.
Označíme-li $G = \{g_1, ..., g_m\}$, $e_{g_1}, ..., e_{g_m}$ bázi V_m, potom $h^r: G \longrightarrow \operatorname{Aut} V_m$, kde $h^r(g_j)(e_{g_i}) = e_{g_j g_i}$ je regulární reprezentace. Tím $\dim W_m = \dim V_m = m = |G|$.
Protože $G = \{g_1, g_2, ..., g_m\}$, potom existuje $s \in \{1, ..., m\}$ takové, že $1 = g_s$. Tím pro každé $g_j \in G$ je $h^r(g_j)(e_{g_s}) = e_{g_j g_s} = e_{g_j 1} = e_{g_j}$, a tedy $\{h^r(g_j)(e_{g_s}) \mid j = 1, ..., m\} = \{e_{g_1}, ..., e_{g_m}\}$, je to tedy báze V_m.
Položme $w_0 = f(e_{g_s})$.
Potom $h(g_j)(f(e_{g_s})) = f(h^r(g_j)(e_{g_s})) = f(e_{g_j})$ pro každé $j = 1, ..., m$, a tím $v_{g_j} = h(g_j)(w_0) = h(g_j)(f(e_{g_s})) = f(e_{g_j})$. Protože f je izomorfismus, je $v_{g_1}, ..., v_{g_m}$ báze W_m.
Nechť naopak $|G| = m$ a existuje prvek $w_0 \in W_m$ takový, že množina m vektorů $\{v_g = h(g)(w_0) \mid g \in G\}$ tvoří bázi prostoru W_m. Nechť V_m je vektorový prostor dimenze m, nechť $e_{g_1}, ..., e_{g_m}$ je báze V_m, kde $G = \{g_1, ..., g_m\}$. Buď $h^r: G \longrightarrow V_m$, kde $h^r(g_j)(e_{g_i}) = e_{g_j g_i}$ pro každé $i, j = 1, ..., m$, regulární reprezentace. Ukážeme, že reprezentace h, h^r jsou ekvivalentní. Definujme zobrazení $f: V_m \longrightarrow W_m$ tak, že pro každé $i = 1, ..., m$ je $f(e_{g_i}) = v_{g_i}$. Potom pro každé $x \in V_m$ je $x = \lambda_1 e_{g_1} + \cdots + \lambda_m e_{g_m}$, a tím můžeme definovat $f(x) = \lambda_1 v_{g_1} + \cdots + \lambda_m v_{g_m}$. Toto zobrazení je izomorfismus. Protože pro každé $i, j = 1, ..., m$ je $(f \circ h^r(g_j))(e_{g_i}) = f(h^r(g_j)(e_{g_i})) = f(e_{g_j g_i}) = v_{g_j g_i} = h(g_j g_i)(w_0) = h(g_j)(h(g_i)(w_0)) = h(g_j)(v_{g_i}) = h(g_j)(f(e_{g_i})) = (h(g_j) \circ f)(e_{g_i})$, je také $(f \circ h^r(g_j))(x) = (h(g_j) \circ f)(x)$ pro každé $g_j \in G$ a pro každé $x \in V_m$, a tedy $f \circ h^r(g) = h(g) \circ f$ pro každé $g \in G$.

■

Definice 5.4 *Nechť V_n je vektorový prostor dimenze n, nechť U je podprostor prostoru V_n, nechť $h: G \longrightarrow V_n$ je reprezentace konečné grupy G ve V_n. Říkáme, že podprostor U je G-invariantní vůči reprezentaci h, jestliže pro každé $g \in G$ je $h(g)(U) \subseteq U$.*

Věta 5.2 *Nechť V_n je vektorový prostor nad $\mathbb{C}$ dimenze n se skalárním součinem (u, v) pro každé $u, v \in V_n$. Nechť $h: G \longrightarrow \operatorname{Aut} V_n$ je reprezentace konečné grupy G ve V_n. Potom lze pro každé $u.v \in V_n$ definovat funkci*

$$((u, v)) = \sum_{g \in G} (h(g)(u), h(g)(v)).$$

Takto definovaná funkce je skalární násobení na V_n.
Navíc pro každé $g \in G$ platí $((h(g)(u), h(g)(v))) = ((u, v))$ pro každé $u, v \in V_n$.

Důkaz $\forall g \in G$, $\forall u, v \in V_n$ je $(h(g)(u), h(g)(v)) \in \mathbb{C}$, proto pro každou konečnou grupu G je $\sum_{g \in G} (h(g)(u), h(g)(v)) \in \mathbb{C}$.

$$((v, u)) = \sum_{g \in G} (h(g)(v), h(g)(u)) = \sum_{g \in G} \overline{(h(g)(u), h(g)(v))} = \overline{\sum_{g \in G} (h(g)(u), h(g)(v))} = \overline{((u, v))};$$

$((\lambda u, v)) = \sum_{g\in G}(h(g)(\lambda u), h(g)(v)) = \sum_{g\in G}\lambda(h(g)(u), h(g)(v)) = \lambda\sum_{g\in G}(h(g)(u), h(g)(v)) =$
$\lambda((u, v))$;
$((u + w, v)) = \sum_{g\in G}(h(g)(u + w), h(g)(v)) = \sum_{g\in G}(h(g)(u) + h(g)(w), h(g)(v)) =$
$\sum_{g\in G}(h(g)(u), h(g)(v)) + \sum_{g\in G}(h(g)(w), h(g)(v)) = ((u, v)) + ((w, v))$;
$((u, u)) = \sum_{g\in G}(h(g)(u), h(g)(u)) \geq 0$ pro každé $u \in V_n$;
$((u, u)) = 0 \iff \sum_{g\in G}(h(g)(u), h(g)(u)) = 0 \iff (h(g)(u), h(g)(u)) = 0\ \forall g \in G \iff$
$h(g)(u) = 0\ \forall g \in G \iff u = 0$.
Tím jsme ukazali, že $((u, v))$ je skalární násobení na V_n.
Pro každé $g \in G$ a pro každé $u, v \in V_n$ je
$((h(g)(u), h(g)(v))) = \sum_{x\in G}(h(x)(h(g)(u)), h(x)(h(g)(v))) = \sum_{x\in G}(h(xg)(u), h(xg)(v)) =$
$\sum_{xg\in G}(h(xg)(u), h(xg)(v)) = ((u, v))$.

■

Věta 5.3 *Je-li V_n vektorový prostor nad $\mathbb{C}$ dimenze n se skalárním součinem (u, v) pro každé $u, v \in V_n$, je-li $h\colon G \longrightarrow \operatorname{Aut} V_n$ reprezentace konečné grupy G ve V_n, je-li $((u, v))$ skalární násobení na V_n dané reprezentací h, potom platí:*

(*i*) *Jsou-li W_1, W_2 G-invariantní podprostory prostoru V_n vůči h, potom podprostory $W_1 \cap W_2$, $W_1 + W_2 = \langle W_1 \cup W_2\rangle$ jsou také G-invariantní podprostory prostoru V_n vůči h.*

(*ii*) *Je-li W G-invariantní podprostor prostoru V_n vůči h, potom jeho ortgonální doplněk při skalárním násobení $((u, v))$*

$$W^{\#} = \{v \in V_n \mid ((v, w)) = 0\ \forall w \in W\}$$

je také G-invariantní podprostor prostoru V_n vůči h.

Důkaz
1. Pro každé $g \in G$ je $h(g)(W_1) \subseteq W_1$, $h(g)(W_2) \subseteq W_2$, potom $h(g)(W_1 \cap W_2) \subseteq W_1 \cap W_2$. Pro každé $w \in W_1 + W_2$ je $w = w_1 + w_2$, kde $w_1 \in W_1$, $w_2 \in W_2$. Potom $h(g)(w) = h(g)(w_1 + w_2) = h(g)(w_1) + h(g)(w_2) \in W_1 + W_2$, a tedy $h(g)(W_1 + W_2) \subseteq W_1 + W_2$.
2. $W^{\#} = \{v \in V_n \mid ((v, w)) = 0\ \forall w \in W\}$ je ortogonální doplněk podprostoru W v prostoru V_n při skalárním násobení $((u, v))$. Ukážeme, že $W^{\#}$ je G-invariantní podprostor. Pro každé $g \in G$ a pro každé $v \in W^{\#}$ a pro každé $w \in W$ je $((h(g)(v), w)) = ((h(g^{-1})(h(g)(v)), h(g^{-1})(w))) = ((h(g^{-1}g)(v), h(g^{-1})(w))) = ((h(1)(v), h(g^{-1})(w))) =$
$((v, h(g^{-1})(w)))$. Protože W je G-inavriantní, je prvek $h(g^{-1})(w) \in W$, $v \in W^{\#}$, a proto $((h(g)(v), w)) = ((v, h(g^{-1})(w))) = 0$. Tím $h(g)(v) \in W^{\#}$, a podprostor $W^{\#}$ je G-invariantní.

■

Definice 5.5 *Nechť $h\colon G \longrightarrow \operatorname{Aut} V_n$ je reprezentace konečné grupy G ve V_n, nechť W je G-invariantní podprostor prostoru V_n vůči h. Potom pro každé $g \in G$ je $h(g)|_W \in \operatorname{Aut} W$, a tedy zobrazení $h^W\colon G \longrightarrow \operatorname{Aut} W$ definované předpisem $h^W(g) = h(g)|_W$ pro každé $g \in G$ je reprezentace grupy G v W. Tato reprezentace h^W se nazývá podreprezentace reprezentace h na W (reprezentace subdukovaná).*

Definice 5.6 *Reprezentace h konečné grupy G ve V_n se nazývá ireducibilní reprezentace, jestliže jedinými G-invariantními podprostory vůči h jsou 0 a V_n.*
Jestliže reprezentace h není ireducibilní, nazývá se reducibilní reprezentace, t.j. existuje G-invariantní podprostor W vůči h takový, že $W \neq 0$, $W \neq V_n$.
Reprezentace h konečné grupy G ve V_n se nazývá rozložitelná, jestliže existují nenulové G-invariantní podprostory W_1, W_2 vůči h takové, že $V_n = W_1 \oplus W_2$.
Reprezentace h konečné grupy G se nazývá úplně reducibilní, jestliže pro každý G-invariantní podprostor W vůči h existuje G-invariantní podprostor W' vůči h tak, že $W \oplus W' = V_n$.

Věta 5.4 *Je-li V_n vektorový prostor nad $\mathbb{C}$ se skalárním součinem, potom každá reprezentace h konečné grupy G ve V_n je úplně reducibilní.*

Důkaz Je-li W G-invariantní podprostor prostoru V_n, potom při skalárním násobení $((u,v)) = \sum_{g\in G}(h(g)(u), h(g)(v))$ je $W^{\#}$ ortogonálním doplňkem, tedy $W \oplus W^{\#} = V_n$, a $W^{\#}$ je G-invariantní podprostor ve V_n podle věty 5.3.

■

Definice 5.7 *Řekneme, že podprostor W prostoru V_n je ireducibilní (resp. reducibilní)vůči reprezentaci h konečné grupy G ve V_n, jestliže W je G-invariantní vůči h a subdukovaná reprezentace h^W, kde $h^W(g) = h(g)|_W$ pro každé $g \in G$, je ireducibilní (resp. reducibilní).*

Věta 5.5 *Nechť V_n je úplně reducibilní prostor vůči reprezentaci h konečné grupy G ve V_n. Potom platí:*

- *(i) Jsou-li W_1, W_2 úplně reducibilní podprostory prostoru V_n vůči h, potom také $W_1 \cap W_2$ a $W_1 + W_2$ jsou úplně reducibilní podprostory vůči h.*
- *(ii) Je-li W úplně reducibilní podprostor prostoru V_n vůči h, potom existuje W' úplně reducibilní podprostor prostoru V_n vůči h tak, že $W \oplus W' = V_n$.*

Důkaz 1. Ukážeme, že $h^{W_1\cap W_2}$ je úplně reducibilní. Buď $W_3 \subseteq W_1 \cap W_2$ podprostor, který je G-invariantní vůči $h^{W_1\cap W_2}$. Ukážeme, že W_3 je direktním sčítancem ve $W_1 \cap W_2$.
Protože W_3 je G-invariantní vůči $h^{W_1\cap W_2}$, je také G-invariantní vůči h. Protože V_n je úplně reducibilní prostor, existuje W_4 podprostor V_n, který je G-invariantní vůči h tak, že $W_3 \oplus W_4 = V_n$. Potom $W_1 \cap W_2 = (W_1 \cap W_2) \cap V_n = (W_1 \cap W_2) \cap (W_3 \oplus W_4) = W_3 \oplus (W_1 \cap W_2 \cap W_4)$. Protože $W_1 \cap W_2 \cap W_4$ je G-invartiantní vůči h, $W_1 \cap W_2 \cap W_4 \subseteq W_1 \cap W_2$, je $W_1 \cap W_2 \cap W_4$ G-invartiantní vůči $h^{W_1\cap W_2}$.
Pro $W_1 + W_2$ důkaz probíhá obdobně.
2. Je-li W úplně reducibilní vůči h, je W G-invariantní vůči h, a protože V_n je úplně reducibilní, existuje G-invariantní podprostor W' vůči h takový, že $W \oplus W' = V_n$.

■

Důsledek 9 Každá reprezentace h konečné grupy G ve V_n nad tělesem T, která je úplně reducubilní, určuje rozklad prostoru V_n na direktní sumu G-invariantních podprostorů ireducibilních vůči h.

Důsledek 10 Každá reprezentace h konečné grupy G ve V_n nad $\mathbb{C}$ určuje rozklad prostoru V_n v direktní sumu G-invariantních podprostorů ireducibilních vůči h.

Důkaz Tvrzení plyne podle věty 5.4 a podle předchozího důsledku.

■

Věta 5.6 Maschkeova věta
Nechť V_n je vektorový prostor dimenze n nad tělesem T, nechť h je reprezentace konečné grupy G ve V_n, nechť char$T$ $\not|$ $|G|$. *Potom reprezentace h je úplně reducibilní.*

Důkaz Věta je zobecněním věty 5.4. Tuto větu již nebudeme dokazovat.

■

Věta 5.7 Schurovo lemma
Nechť $h\colon G \longrightarrow \operatorname{Aut} V_n$, $k\colon G \longrightarrow \operatorname{Aut} W_m$ jsou ireducibilí reprezentace konečné grupy G. Jestliže $f\colon Vn \longrightarrow W_m$ je takový homomorfismus, že pro každé $g \in G$ je $f \circ h(g) = k(g) \circ f$, potom buď $f = 0$ nebo f je izomorfismus a tím $m = n$.

Důkaz Je-li $f = 0$, jsme hotovi.
Předpokládejme, že $f \neq 0$. Potom $\operatorname{Ker} f$ je podprostor prostoru V_n a $\operatorname{Ker} f \neq V_n$. Ukážeme, že $\operatorname{Ker} f$ je G-invariantní vůči h. Pro každé $g \in G$ a pro každé $v \in \operatorname{Ker} f$ je $f(h(g)(v)) = k(g)(f(v)) = k(g)(0) = 0$, tedy $h(g)(v) \in \operatorname{Ker} f$. Protože h je ireducibilní, $\operatorname{Ker} f$ je G-invariantní vůči h, $\operatorname{Ker} f \neq V_n$, je $\operatorname{Ker} f = 0$.
Stejně ukážeme, že $\operatorname{Im} f$ je G-invariantní vůči h. Pro každé $g \in G$ a pro každé $w \in \operatorname{Im} f$ existuje $v \in V_n$ tak, že $f(v) = w$. Potom $k(g)(w) = k(g)(f(v)) = f(h(g)(v)) \in \operatorname{Im} f$. Tím $\operatorname{Im} f = V_n$, neboť k je ireducibilní.
Tedy $\operatorname{Ker} f = 0$, $\operatorname{Im} f = V_n$, a proto f je izomorfismus a $m = n$.

■

Věta 5.8 Schurovo lemma - maticový tvar
Nechť $h\colon G \longrightarrow \operatorname{Aut} V_n$, $k\colon G \longrightarrow \operatorname{Aut} W_m$ jsou ireducibilí reprezentace konečné grupy G. Jestliže $\mathbf{F}$ je taková matice typu m/n, že pro každé $g \in G$ je $\mathbf{F}h^M(g) = k^M(g)\mathbf{F}$, potom buď $\mathbf{F} = 0$ nebo $\mathbf{F}$ je regulární matice a tím $m = n$.

Důkaz Homomorfismus $f\colon V_n \longrightarrow W_m$ má v daných bázích matici $\mathbf{F}$. Potom podle předchozí věty $f = 0$ nebo f je izomorfismus, tím $\mathbf{F} = \mathbf{0}$ nebo $\mathbf{F}$ je regulární matice a $m = n$.

■

Co znamená, že reprezentace h je reducibilní?
Jestliže $h\colon G \longrightarrow \operatorname{Aut} V_n$ je reducibilní reprezentace konečné grupy G ve V_n, potom existuje G-invariantní podprostor U prostoru V_n takový, že $U \neq 0$, $U \neq V_n$. Zvolíme-li $u_1, u_2, ..., u_k$ bázi podprostoru U, potom ve V_n ji lze doplnit na bázi celého prostoru V_n, tedy $u_1, ..., u_k, u_{k+1}, ..., u_n$ je báze V_n. Protože U je G-invariantní, pro každé $g \in G$ je $h(g)(U) \subseteq U$. Tím
$h(g)(u_1) = \lambda_{11}u_1 + \cdots + \lambda_{k1}u_k + 0u_{k+1} + \cdots + 0u_n,$
.....
$h(g)(u_k) = \lambda_{1k}u_1 + \cdots + \lambda_{kk}u_k + 0u_{k+1} + \cdots + 0u_n,$
$h(g)(u_{k+1}) = \lambda_{1k+1}u_1 + \cdots + \lambda_{kk+1}u_k + \lambda_{k+1k+1}u_{k+1} + \cdots + \lambda_{nk+1}u_n,$
.....
$h(g)(u_n) = \lambda_{1n}u_1 + \cdots + \lambda_{kn}u_k + \lambda_{k+1n}u_{k+1} + \cdots + \lambda_{nn}u_n.$
Tím $h^M(g) = \begin{bmatrix} \lambda_{11} & \cdots & \lambda_{1k} & \lambda_{1k+1} & \cdots & \lambda_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \lambda_{k1} & \cdots & \lambda_{kk} & \lambda_{kk+1} & \cdots & \lambda_{kn} \\ 0 & \cdots & 0 & \lambda_{k+1k+1} & \cdots & \lambda_{k+1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \lambda_{nk+1} & \cdots & \lambda_{nn} \end{bmatrix}$.
Proto reprezentace h konečné grupy G je reducibilní právě tehdy, když existuje maticová reprezentace taková, že pro každé $g \in G$ je $h^M(g) = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{C} \end{bmatrix}$, kde $\mathbf{A}$ je matice typu k/k, $\mathbf{B}$ je matice typu $k/(n-k)$, $\mathbf{C}$ je matice typu $(n-k)/(n-k)$ a $k \neq 0$, $k \neq n$.

Co znamená, že reprezentace h je rozložitelná?
Jestliže $h\colon G \longrightarrow \operatorname{Aut} V_n$ je rozložitelná reprezentace konečné grupy G ve V_n, potom existují G-invariantní podprostory U_1, U_2 prostoru V_n takové, že $U_1 \neq 0$, $U_2 \neq 0$ a $V_n = U_1 \oplus U_2$. Zvolíme-li $u_1, u_2, ..., u_k$ bázi podprostoru U_1, $u_{k+1}, ..., u_n$ bázi podprostoru U_2, potom $u_1, ..., u_k, u_{k+1}, ..., u_n$ je báze V_n. Protože U_1 i U_2 jsou G-invariantní, pro každé $g \in G$ je $h(g)(U_1) \subseteq U_1$ a $h(g)(U_2) \subseteq U_2$. Tím
$h(g)(u_1) = \lambda_{11}u_1 + \cdots + \lambda_{k1}u_k + 0u_{k+1} + \cdots + 0u_n,$
.....
$h(g)(u_k) = \lambda_{1k}u_1 + \cdots + \lambda_{kk}u_k + 0u_{k+1} + \cdots + 0u_n,$
$h(g)(u_{k+1}) = 0u_1 + \cdots + 0u_k + \lambda_{k+1k+1}u_{k+1} + \cdots + \lambda_{nk+1}u_n,$
.....
$h(g)(u_n) = 0u_1 + \cdots + 0u_k + \lambda_{k+1n}u_{k+1} + \cdots + \lambda_{nn}u_n.$

Tím $h^M(g) = \begin{bmatrix} \lambda_{11} & \cdots & \lambda_{1k} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \lambda_{k1} & \cdots & \lambda_{kk} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \lambda_{k+1k+1} & \cdots & \lambda_{k+1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \lambda_{nk+1} & \cdots & \lambda_{nn} \end{bmatrix}$.
Proto reprezentace h konečné grupy G je rozložitelná právě tehdy, když existuje maticová reprezentace taková, že pro každé $g \in G$ je $h^M(g) = \begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{C} \end{bmatrix}$, kde $\mathbf{A}$ je matice typu k/k, $\mathbf{C}$ je matice typu $(n-k)/(n-k)$ a $k \neq 0$, $k \neq n$.

Protože matice automorfismu v různých bázích jsou podobné, můžeme vyslovit následující větu.

Věta 5.9 *Nechť h je reprezentace konečné grupy G ve V_n. Potom platí:*

(*i*) *h je reducibilní právě tehdy, když pro každé $g \in G$ je matice $h^M(g)$ podobná matici* $\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{C} \end{bmatrix}$,

(*ii*) *h je rozložitelná právě tehdy, když pro každé $g \in G$ je matice $h^M(g)$ podobná matici* $\begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{C} \end{bmatrix}$,

(*iii*) *h je úplně reducibilní právě tehdy, když pro každé $g \in G$ platí: je-li matice $h^M(g)$ podobná matici* $\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{C} \end{bmatrix}$, *potom je $h^M(g)$ podobná matici* $\begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{C} \end{bmatrix}$.

Důsledek 11 Jsou-li reprezentace h, k konečné grupy G ekvivalentní, potom reprezentace h je ireducubilní právě tehdy, když je ireducibilní reprezentace k.

Věta 5.10 *Je-li h reprezentace konečné grupy G ve V_n nad $\mathbb{C}$, potom pro každé $g \in G$ je matice $h^M(g)$ podobná matici*

$$\begin{bmatrix} h_1^M(g) & 0 & & 0 \\ 0 & h_2^M(g) & & 0 \\ & & \ddots & \\ 0 & 0 & & h_r^M(g) \end{bmatrix},$$

kde pro každé $i = 1, ..., r$ je h_i ireducibilní reprezentace grupy G.

Důkaz Protože každá reprezentace ve V_n nad $\mathbb{C}$ je úplně reducibilní, je $V_n = W_1 \oplus W_2 \oplus \cdots \oplus W_r$, kde pro každé $i = 1, ..., r$ je W_i G-invariantní vůči h a pro každé $g \in G$ je $h(g)|_{W_i}$ ireducibilní na W_i.
Označme
$w_1, ..., w_{i_1}$ bázi W_1,

$w_{i_1+1}, ..., w_{i_2}$ bázi W_2,
.....
$w_{i_{r-1}+1}, ..., w_{i_r}$ bázi W_r.
Protože pro každé $i = 1, ..., r$ je W_i G-invariantní, je pro každé $g \in G$

$$h^M(g) = \begin{bmatrix} \mathbf{A}_1 & 0 & & 0 \\ 0 & \mathbf{A}_2 & & 0 \\ & & \ddots & \\ 0 & 0 & & \mathbf{A}_r \end{bmatrix},$$

kde pro každé $i = 1, ..., r$ je $\mathbf{A}_i = (h(g)|_{W_i})^M$.
Označíme-li $h_i \colon G \longrightarrow \mathrm{Aut}\,(W_i)$, kde $h_i(g) = h(g)|_{W_i}$ pro každé $g \in G$, potom h_i je ireducibilní a $\mathbf{A}_i = h_i^M(g)$.

■

Definice 5.8 *Je-li* $\mathbf{A} = [a_{ij}]$ *čtvercová matice řádu* n*, potom prvek*

$$\mathrm{Tr}\,\mathbf{A} = a_{11} + a_{22} + \cdots + a_{nn}$$

se nazývá stopa matice $\mathbf{A}$*.*

Věta 5.11 *Jsou-li* $\mathbf{A}, \mathbf{B}$ *čtvercové matice řádu* n*, potom* $\mathrm{Tr}\,(\mathbf{AB}) = \mathrm{Tr}\,(\mathbf{BA})$.

Důkaz $\mathrm{Tr}\,(\mathbf{AB}) = \sum_{j=1}^{n} a_{1j}b_{j1} + \sum_{j=1}^{n} a_{2j}b_{j2} + \cdots + \sum_{j=1}^{n} a_{nj}b_{jn} = \sum_{k=1}^{n}(\sum_{j=1}^{n} a_{kj}b_{jk}) = \sum_{j=1}^{n}(\sum_{k=1}^{n} a_{kj}b_{jk}) = \sum_{j=1}^{n}(\sum_{k=1}^{n} b_{jk}a_{kj}) = \mathrm{Tr}\,(\mathbf{BA})$.

■

Důsledek 12 Jsou-li $\mathbf{A}, \mathbf{B}$ čtvercové matice řádu n podobné, potom $\mathrm{Tr}\,\mathbf{A} = \mathrm{Tr}\,\mathbf{B}$.

Důkaz Jestliže $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$, potom $\mathrm{Tr}\,\mathbf{B} = \mathrm{Tr}\,(\mathbf{P}^{-1}\mathbf{AP}) = \mathrm{Tr}\,(\mathbf{APP}^{-1}) = \mathrm{Tr}\,(\mathbf{A})$.

■

Důsledek 13 Stopa čtvercové matice $\mathbf{A}$ se rovná součtu vlastních čísel matice $\mathbf{A}$.

Věta 5.12 *Pro čtvercové matice nad koplexními čísly platí:*

(*i*) *Je-li* $\mathbf{D} = \mathbf{D}_1 \oplus \mathbf{D}_2 \oplus \cdots \oplus D_r$*, potom* $\mathrm{Tr}\,\mathbf{D} = \sum_{i=1}^{r} \mathrm{Tr}\,\mathbf{D}_i$.

(*ii*) *Je-li* $\mathbf{I}$ *jednotková matice řádu* n*, potom* $\mathrm{Tr}\,\mathbf{I} = n$.

(*iii*) *Je-li* $\mathbf{A}$ *regulární matice řádu* n *s vlastními čísly* $\lambda_1, ..., \lambda_n$*, potom inverzní matice* $\mathbf{A}^{-1}$ *má vlastní čísla* $\lambda_1^{-1}, ..., \lambda_n^{-1}$.

(*iv*) *Jestliže pro matici* $\mathbf{A}$ *existuje* $k \in \mathbb{N}$ *tak, že* $\mathbf{A}^k = \mathbf{I}$*, potom* $\mathrm{Tr}\,\mathbf{A}^{-1} = \overline{\mathrm{Tr}\,\mathbf{A}}$ *a* $\mathrm{Tr}\,\mathbf{A}$ *je součet* k*-tých odmocnin z čísla* 1.

Důkaz 1. a 2. tvrzení je jasné.
3. Je-li λ vlastní číslo regulární matice $\mathbf{A}$, potom $\lambda h = \mathbf{A}h$, kde $h \neq 0$ je vlastní vektor příslušný vlastnímu číslu λ, $\lambda \neq 0$. Potom $\mathbf{A}^{-1}\lambda h = \mathbf{A}^{-1}\mathbf{A}h$, tím $\lambda\mathbf{A}^{-1}h = h$, a proto $\mathbf{A}^{-1}h = \lambda^{-1}h$. Tím λ^{-1} je vlastní číslo matice $\mathbf{A}^{-1}$ a h je vlastní vektor matice $\mathbf{A}^{-1}$ příslušný vlastnímu číslu λ^{-1}.
4. Jestliže $\mathbf{A}^k = \mathbf{I}$ pro nějaké $k \in \mathbb{N}$, potom $(\det \mathbf{A})^k = det(\mathbf{A}^k) = \det \mathbf{I} = 1$, tedy matice $\mathbf{A}$ je regulární. Potom $\mathbf{A} = \mathbf{T}\mathbf{J}\mathbf{T}^{-1}$, kde Jordanova matice $\mathbf{J}$ má na diagonále nenulová vlastní čísla $\lambda_1, ..., \lambda_n$ matice $\mathbf{A}$. Tím $\mathbf{J} = \mathbf{T}^{-1}\mathbf{A}\mathbf{T}$, a proto $\mathbf{J}^k = (\mathbf{T}^{-1}\mathbf{A}\mathbf{T})^k = \mathbf{T}^{-1}\mathbf{A}^k\mathbf{T} = \mathbf{I}$. Matice $\mathbf{J}^k$ má na diagonále $\lambda_1^k, ..., \lambda_n^k$, proto $\lambda_j^k = 1$, a tedy λ_j je k-tá odmocnina z jedné pro každé $j = 1, ..., n$.
Jestliže $\lambda_j = \alpha + \beta i$, pak $|\alpha + \beta i| = 1$, a protože $(\alpha + \beta i)(\alpha - \beta i) = \alpha^2 + \beta^2 = |\alpha + \beta i|^2 = 1$, je $\lambda_j^{-1} = \alpha - \beta i = \overline{\lambda_j}$. Proto $\mathrm{Tr}\,(\mathbf{A}^{-1}) = \sum_{j=1}^{n} \lambda_j^{-1} = \sum_{j=1}^{n} \overline{\lambda_j} = \overline{\sum_{j=1}^{n} \lambda_j} = \overline{\mathrm{Tr}\,(\mathbf{A})}$.

■

Je-li $h\colon G \longrightarrow \mathrm{Aut}\, V_n$ reprezentace konečné grupy G ve V_n, potom pro každé $g \in G$ je $h(g)$ automorfismus vektorového prostoru V_n. Je-li $\mathbf{A}_g$ matice automorfismu $h(g)$ v bázi $b_1, ..., b_n$ prostoru V_n a $\mathbf{B}_g$ matice stejného automorfismu $h(g)$ jen v jiné bázi $v_1, ..., v_n$, potom matice $\mathbf{A}_g$ a $\mathbf{B}_g$ jsou podobné, a tudíž mají stejnou stopu, tedy $\mathrm{Tr}\,\mathbf{A}_g = \mathrm{Tr}\,\mathbf{B}_g$. Můžeme proto mluvit o stopě automorfismu $h(g)$, je to stopa matice automorfismu $h(g)$ v libovolné bázi prostoru V_n.

Definice 5.9 *Nechť $h\colon G \longrightarrow \mathrm{Aut}\, V_n$ je reprezentace konečné grupy G ve V_n nad tělesem T. Potom zobrazení $\chi\colon G \longrightarrow T$ dané předpisem $\chi(g) = \mathrm{Tr}\, h^M(g)$ pro každé $g \in G$ se nazývá charakter reprezentace h.*

Věta 5.13 *Nechť h je reprezentace konečné grupy G ve V_n nad tělesem $\mathbb{C}$, nechť χ je charakter reprezentace h. Potom platí:*

- *(i) Nechť $W_1, ..., W_r$ jsou G-invariantní podprostory prostoru V_n vůči h, nechť prostor $V_n = W_1 \oplus \cdots \oplus W_r$. Pro každé $i = 1, ..., r$ $h_i(g) = h(g)|_{W_i}$ pro každé $g \in G$ je reprezentace grupy G ve W_i, označme χ_i charkter reprezentace h_i. Potom pro každé $g \in G$ platí $\chi(g) = \sum_{i=1}^{r} \chi_i(g)$.*
- *(ii) Označíme-li* id $\in \mathrm{Aut}\, V_n$ *identický automorfismu prostoru V_n, potom $\chi(\mathrm{id}\,) = n$.*
- *(iii) $\chi(g_1 g_2) = \chi(g_2 g_1)$ pro každé $g_1, g_2 \in G$.*
- *(iv) $\chi(g_1^{-1} g_2 g_1) = \chi(g_2)$ pro každé $g_1, g_2 \in G$.*
- *(v) $\chi(g^{-1}) = \overline{\chi(g)}$ pro každé $g \in G$.*

Důkaz 1. Zvolíme-li
$b_1, ..., b_{k_1}$ bázi W_1,
$b_{k_1+1}, ..., b_{k_2}$ bázi W_2,
. . . . . .
$b_{k_{r-1}+1}, ..., b_{k_r}$ bázi W_r,

Potom $b_1, ..., b_{k_r}$ je báze V_n, a v této bázi pro každé $g \in G$ je

$$h^M(g) = \begin{bmatrix} h_1^M(g) & 0 & & 0 \\ 0 & h_2^M(g) & & 0 \\ & & \ddots & \\ 0 & 0 & & h_r^M(g) \end{bmatrix}.$$

Proto pro každé $g \in G$ je $\chi(g) = \mathrm{Tr}\,(h^M(g)) = \sum_{i=1}^{r} \mathrm{Tr}\,(h_i^M(g)) = \sum_{i=1}^{r} \chi_i(g)$.
2. $\chi(1) = \mathrm{Tr}\,(\mathbf{I}) = n$.
3. $\chi(g_1g_2) = \mathrm{Tr}\,(h^M(g_1g_2)) = \mathrm{Tr}\,(h^M(g_1)h^M(g_2)) = \mathrm{Tr}\,(h^M(g_2)h^M(g_1)) = \mathrm{Tr}\,(h^M(g_2g_1)) = \chi(g_2g_1)$.
4. $\chi(g_1^{-1}g_2g_1) = \chi(g_2g_1g_1^{-1}) = \chi(g_2)$.
5. $\chi(g^{-1}) = \mathrm{Tr}\,(h^M(g^{-1})) = \mathrm{Tr}\,((h^M(g))^{-1}) = \overline{\mathrm{Tr}\,(h^M(g))} = \overline{\chi(g)}$.

■

Věta 5.14 *Nechť h je reprezentace konečné grupy G ve V_n, nechť k je reprezentace konečné grupy G ve W_m, nechť reprezentace h, k jsou ekvivalentní. Potom tyto reprezentace mají stejné charaktery, tedy $\chi^{(h)} = \chi^{(k)}$.*

Důkaz Protože reprezentace h, k jsou ekvivalentní, existuje izomorfismus $f: V_n \longrightarrow W_m$ takový, že pro každé $g \in G$ a pro každé $v \in V_n$ je $k(g)(f(v)) = f(h(g)(v))$, $m = n$. V daných bázích prostorů V_n a W_m je $h^M(g)$ matice $h(g)$, $k^M(g)$ matice $k(g)$ a $\mathbf{F}$ matice izomorfismu f a $\mathbf{F}h^M(g) = k^M(g)\mathbf{F}$ pro každé $g \in G$. Protože matice izomorfismu $\mathbf{F}$ je regulární, je $h^M(g) = \mathbf{F}^{-1}k^M(g)\mathbf{F}$ pro každé $g \in G$, a tedy $\chi^{(h)}(g) = \mathrm{Tr}\,(h^M(g)) = \mathrm{Tr}\,(\mathbf{F}^{-1}k^M(g)\mathbf{F}) = \mathrm{Tr}\,(k^M(g)) = \chi^{(k)}(g)$.

■

Protože pro další vlastnosti budeme potřebovat předpoklad, že těleso T je algebraicky uzavřené a char$T \not| |G|$, omezíme se v celém dalším povídání na těleso komplexních čísel $\mathbb{C}$.

Lemma 5.1 *Nechť h je reprezentace konečné grupy G ve V_n, nechť k je reprezentace grupy G ve W_m, nechť $\mathbf{M}$ je libovolná matice typu n/m nad $\mathbb{C}$. Jestliže matici typu n/m označíme $\mathbf{P} = \sum_{x \in G} h^M(x)\mathbf{M}k^M(x^{-1})$, potom pro každé $g \in G$ platí $h^M(g)\mathbf{P} = \mathbf{P}k^M(g)$.*

Důkaz Pro každé $x \in G$ je $h^M(x)$ matice typu n/n, $k^M(x)$ je matice typu m/m, proto $\mathbf{P}$ je matice typu n/m.
$h^M(g)\mathbf{P} = h^M(g)(\sum_{x \in G} h^M(x)\mathbf{M}k^M(x^{-1})) = \sum_{x \in G} h^M(g)h^M(x)\mathbf{M}k^M(x^{-1}) =$
$\sum_{x \in G} h^M(gx)\mathbf{M}k^M(x^{-1}) = \sum_{x \in G} h^M(gx)\mathbf{M}k^M(x^{-1})k^M(g^{-1})k^M(g) =$
$\sum_{x \in G} h^M(gx)\mathbf{M}k^M(x^{-1}g^{-1})k^M(g) = (\sum_{gx \in G} h^M(gx)\mathbf{M}k^M((gx)^{-1}))k^M(g) = \mathbf{P}k^M(g)$.

■

Věta 5.15 *Nechť G je konečná grupa, nechť h, k jsou dvě neekvivalentní ireducibilní reprezentace grupy G. Je-li $h\colon G \longrightarrow \operatorname{Aut} V_n$ reprezentace G ve V_n, $h^M(g)$ matice reprezentace h řádu n pro každé $g \in G$, potom označme pro každé $i, j = 1, ..., n$ prvek v matici $h^M(g)$ na místě ij symbolem $h^M_{ij}(g)$. Je-li $k\colon G \longrightarrow \operatorname{Aut} W_m$ reprezentace G ve W_m, $k^M(g)$ matice reprezentace k řádu m pro každé $g \in G$, potom označme pro každé $r, s = 1, ..., m$ prvek v matici $k^M(g)$ na místě rs symbolem $k^M_{rs}(g)$. Potom pro každé $i, j = 1, ..., n$ a pro každé $r, s = 1, ..., m$ platí*

$$\sum_{g\in G} h^M_{ij}(g)k^M_{rs}(g^{-1}) = 0.$$

Důkaz Zvolme libovolnou matici $\mathbf{M}$ typu n/m a položme podle předchozího lemmatu $\mathbf{P} = \sum_{x\in G} h^M(x)\mathbf{M}k^M(x^{-1})$, potom pro každé $g \in G$ je $h^M(g)\mathbf{P} = \mathbf{P}k^M(g)$.
Pro ireducibilní reprezentace je podle věty 5.8 $\mathbf{P} = \mathbf{0}$ nebo $\mathbf{P}$ je regulární matice. Kdyby matice $\mathbf{P}$ byla regulární, reprezantace h, k by byly ekvivalentní, což podle předpokladu nejsou. Proto $\mathbf{P} = \mathbf{0}$, tedy $\sum_{x\in G} h^M(x)\mathbf{M}k^M(x^{-1}) = \mathbf{0}$.
Označíme-li $\mathbf{M} = [m_{ij}]$, potom pro každé $i = 1, ..., n$ a pro každé $s = 1, ..., m$ máme
$[h^M(x)\mathbf{M}k^M(x^{-1})]_{is} = \sum_{v=1}^{m}(\sum_{u=1}^{n} h^M_{iu}(x)m_{uv})k^M_{vs}(x^{-1}) = \sum_{v=1}^{m}\sum_{u=1}^{n} h^M_{iu}(x)m_{uv}k^M_{vs}(x^{-1})$, a tedy
$0 = \sum_{x\in G}(\sum_{v=1}^{m}\sum_{u=1}^{n} h^M_{iu}(x)m_{uv}k^M_{vs}(x^{-1}))$.
Pro libovolné $j = 1, ..., n$ a pro libovolné $r = 1, ..., m$ zvolme matici $\mathbf{M} = [m_{ij}]$ takovou, že $m_{jr} = 1$, $m_{uv} = 0$ pro každé $u \neq j$, $v \neq r$. Potom
$0 = \sum_{x\in G}(\sum_{v=1}^{m}\sum_{u=1}^{n} h^M_{iu}(x)m_{uv}k^M_{vs}(x^{-1})) = \sum_{x\in G}(\sum_{v=1}^{m} h^M_{ij}(x)m_{jv}k^M_{vs}(x^{-1})) =$
$\sum_{x\in G}(h^M_{ij}(x)m_{jr}k^M_{rs}(x^{-1})) = \sum_{x\in G} h^M_{ij}(x)k^M_{rs}(x^{-1})$.

■

Věta 5.16 *Nechť G je konečná grupa, nechť $h\colon G \longrightarrow \operatorname{Aut} V_n$ je ireducibilní reprezentace grupy G ve V_n, nechť pro každé $g \in G$ je $h^M(g)$ matice reprezentace h v dané bázi prostoru V_n, nechť $h^M_{ij}(g)$ označuje prvek na místě ij v matici $h^M(g)$. Potom pro každé $i, j, k, l = 1, ..., n$ platí*

$$n\sum_{g\in G} h^M_{ij}(g)h^M_{kl}(g^{-1}) = \delta_{il}\delta_{jk}|G|,$$

kde δ označuje Kroneckerovo delta.

Důkaz Zvolme libovolnou čtvercovou matici $\mathbf{M}$ řádu n a opět položme
$\mathbf{P} = \sum_{g\in G} h^M(g)\mathbf{M}h^M(g^{-1})$.
Potom $\operatorname{Tr}\mathbf{P} = \operatorname{Tr}(\sum_{g\in G} h^M(g)\mathbf{M}h^M(g^{-1})) = \sum_{g\in G}\operatorname{Tr}(h^M(g)\mathbf{M}h^M(g^{-1})) = \sum_{g\in G}\operatorname{Tr}(\mathbf{M}) =$
$|G|\operatorname{Tr}\mathbf{M}$. Podle lemmatu 5.1 je $h^M(g)\mathbf{P} = \mathbf{P}h^M(g)$ pro každé $g \in G$.
Buď $\lambda \in \mathbb{C}$ vlastní číslo matice $\mathbf{P}$, tedy $\det(\lambda\mathbf{I} - \mathbf{P}) = 0$. Potom pro každé $g \in G$ je

$h^M(g)(\lambda\mathbf{I}-\mathbf{P}) = h^M(g)\lambda - h^M(g)\mathbf{P} = \lambda h^M(g) - \mathbf{P}h^M(g) = (\lambda\mathbf{I}-\mathbf{P})h^M(g)$. Podle věty 5.8 je $\lambda\mathbf{I}-\mathbf{P} = \mathbf{0}$ nebo matice $\lambda\mathbf{I}-\mathbf{P}$ je regulární. Protože však $\det(\lambda\mathbf{I}-\mathbf{P}) = 0$, je $\lambda\mathbf{I}-\mathbf{P} = \mathbf{0}$, tedy $\mathbf{P} = \lambda\mathbf{I}$.
Tím $|G|\mathrm{Tr}\,\mathbf{M} = \mathrm{Tr}\,\mathbf{P} = \mathrm{Tr}\,(\lambda\mathbf{I}) = n\lambda$.
Označíme-li $\mathbf{P} = [p_{il}]$, potom $p_{ii} = \lambda$ pro každé $i = 1, ..., n$ a $p_{il} = 0$ pro každé $i \neq l$, tedy $p_{il} = \lambda\delta_{il}$.
Označíme-li $\mathbf{M} = [m_{uv}]$, potom
$\lambda\delta_{il} = p_{il} = \sum_{g\in G}(\sum_{v=1}^{n}\sum_{u=1}^{n} h^M_{iu}(g)m_{uv}h^M_{vl}(g^{-1}))$.
Pro každé $i, l = 1, ..., n$ a pro každé $j, k = 1, ...n$ zvolme matici $\mathbf{M}$ tak, že $m_{uv} = 1$ pro $u = j$, $v = k$ a $m_{uv} = 0$ pro všechna $u \neq j$ a pro všechna $v \neq k$. Potom
$\lambda\delta_{il} = p_{il} = \sum_{g\in G}(\sum_{v=1}^{n}\sum_{u=1}^{n} h^M_{iu}(g)m_{uv}h^M_{vl}(g^{-1})) = \sum_{g\in G}(\sum_{v=1}^{n} h^M_{ij}(g)m_{jv}h^M_{vl}(g^{-1})) =$
$\sum_{g\in G} h^M_{ij}(g)m_{jk}h^M_{kl}(g^{-1}) = \sum_{g\in G} h^M_{ij}(g)h^M_{kl}(g^{-1})$. Tím
$n\sum_{g\in G} h^M_{ij}(g)h^M_{kl}(g^{-1}) = n\lambda\delta_{il} = |G|\delta_{jk}\delta_{il}$, neboť $n\lambda = \mathrm{Tr}\,(\lambda\mathbf{I}) = |G|\mathrm{Tr}\,(\mathbf{M}) = |G|\delta_{jk}$, protože $m_{jk} = 1$ a ostatní jsou 0.

■

Pro x, y prvky grupy G budeme označovat $x \sim y$, jestliže jsou prvky x, y konjugované, t.j. existuje prvek $g \in G$ tak, že $x = gyg^{-1}$. Označíme-li $C_1, C_2, ..., C_r$ třídy konjugovaných prvků grupy G, potom $G = C_1 \cup C_2 \cup \cdots \cup C_r$.
Vždy bude očíslování tříd konjugovaných prvků takové, že $1 \in C_1$. Potom $C_1 = \{1\}$.
Pro každé $i = 1, ..., r$ označme $x_i \in C_i$ reprezentant třídy C_i.
Pro každé $i = 1, ..., r$ označme $t_i = |C_i|$.
Uvědomíme si, že pro každé $i = 1, ..., r$ je $C_i^{-1} = \{x^{-1} \mid x \in C_i\}$ opět třída konjugovaných prvků, tedy existuje $l \in \{1, ..., r\}$ tak, že $C_i^{-1} = C_l$.
Navíc $|C_i^{-1}| = |C_i| = t_i$ pro každé $i = 1, ..., r$.

Věta 5.17 *Je-li $h\colon G \longrightarrow \mathrm{Aut}\,V_n$ reprezentace konečné grupy G ve V_n nad $\mathbb{C}$, je-li χ charakter reprezentace h, potom zobrazení χ je konstantní na třídě konjugovaných prvků grupy G.*

Důkaz Jsou-li $x, y \in G$ takové, že existuje $g \in G$ tak, že $x = gyg^{-1}$, potom $\chi(x) = \chi(gyg^{-1}) = \mathrm{Tr}\,(h^M(gyg^{-1})) = \mathrm{Tr}\,(h^M(g)h^M(y)h^M(g^{-1})) = \mathrm{Tr}\,(h^M(g)h^M(y)h^M(g)^{-1}) = \mathrm{Tr}\,(h^M(y)) = \chi(y)$.

■

Věta 5.18 *Je-li $h\colon G \longrightarrow \mathrm{Aut}\,V_n$ ireducibilní reprezentace konečné grupy G ve V_n nad $\mathbb{C}$, je-li χ její charakter, potom platí*

$$\sum_{g\in G} \chi(g)\chi(g^{-1}) = |G|.$$

Důkaz Označíme-li $h_{ij}^M(g)$ prvky matice $h^M(g)$ pro každé $g \in G$, potom
$\chi(g) = \mathrm{Tr}\, h^M(g) = \sum_{i=1}^{n} h_{ii}^M(g)$. Tím
$\sum_{g\in G} \chi(g)\chi(g^{-1}) = \sum_{g\in G}(\sum_{i=1}^{n} h_{ii}^M(g) \sum_{k=1}^{n} h_{kk}^M(g^{-1})) = \sum_{i=1}^{n}\sum_{k=1}^{n}(\sum_{g\in G} h_{ii}^M(g)h_{kk}^M(g^{-1}))$.
Podle věty 5.16 pro $i = j$, $k = l$ získáváme
$n \sum_{g\in G} h_{ii}^M(g)h_{kk}^M(g^{-1}) = \delta_{ik}\delta_{ik}|G| = \delta_{ik}|G|$. Proto

$$\sum_{g\in G} \chi(g)\chi(g^{-1}) = \sum_{i=1}^{n}\sum_{k=1}^{n} \frac{1}{n}\delta_{ik}|G| = \sum_{i=1}^{n} \frac{1}{n}\delta_{ii}|G| = \sum_{i=1}^{n} \frac{1}{n}|G| = n\frac{1}{n}|G| = |G|.$$

■

Poznámka 5.1 Věta 5.18 platí i pro ireducibilní reprezentace h konečné grupy G ve V_n nad tělesem T, ovšem těleso T musí být algebraicky uzavřené a char$T \not| |G|$.

Věta 5.19 *Nechť h_1, h_2 jsou neekvivalentní ireducibilní reprezentace konečné grupy G, nechť χ_1, χ_2 jsou jejich charaktery. Potom platí*

$$\sum_{g\in G} \chi_1(g)\chi_2(g^{-1}) = 0.$$

Důkaz Buď $h_1 \colon G \longrightarrow \mathrm{Aut}\, V_n$, $\chi_1(g) = \mathrm{Tr}\,(h_1^M(g))$ pro každé $g \in G$,
$h_2 \colon G \longrightarrow \mathrm{Aut}\, W_m$, $\chi_2(g) = \mathrm{Tr}\,(h_2^M(g))$ pro každé $g \in G$.
Podle věty 5.15 pro každé $i, j = 1, ...,$ a pro každé $r, s = 1, ..., m$ máme
$\sum_{g\in G} h_{1_{ij}}^M(g)h_{2_{rs}}^M(g^{-1}) = 0$, potom
$\sum_{g\in G} \chi_1(g)\chi_2(g^{-1}) = \sum_{g\in G}(\mathrm{Tr}\,(h_1^M(g))\mathrm{Tr}\,(h_2^M(g^{-1}))) = \sum_{g\in G}(\sum_{i=1}^{n}(h_{1_{ii}}^M(g)) \sum_{r=1}^{m}(h_{2_{rr}}^M(g^{-1}))) =$
$\sum_{i=1}^{n}\sum_{r=1}^{m}(\sum_{g\in G}(h_{1_{ii}}^M(g))(h_{2_{rr}}^M(g^{-1}))) = \sum_{i=1}^{n}\sum_{r=1}^{m} 0 = 0.$

■

Poslední dvě věty lze formulovat společně.

Věta 5.20 *Nechť h_1, h_2 jsou neekvivalentní ireducibilní reprezentace konečné grupy G, nechť χ_1, χ_2 jsou jejich charaktery. Potom pro $i, j \in \{1, 2\}$ platí*

$$\sum_{g\in G} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij}|G|.$$

Věta 5.21 *Nechť h_1, h_2 jsou neekvivalentní ireducibilní reprezentace konečné grupy G, nechť χ_1, χ_2 jsou jejich charaktery. Potom pro $i, j \in \{1, 2\}$ platí*

$$\sum_{k=1}^{r} t_k\chi_i(x_k)\chi_j(x_k^{-1}) = \delta_{ij}|G|.$$

Důkaz Podle věty 5.20 pro $i, j = 1, 2$ máme $\sum_{g\in G} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij}|G|$.
Protože $G = C_1 \cup C_2 \cup \cdots \cup C_r$, kde pro každé $k = 1, ..., r$ je C_r třída konjugovaných prvků, $C_1 = \{1\}$,máme
$\delta_{ij}|G| = \sum_{g\in G} \chi_i(g)\chi_j(g^{-1}) = \sum_{k=1}^{r}(\sum_{g\in C_k} \chi_i(g)\chi_j(g^{-1}))$.
Podle věty 5.17 je $\sum_{g\in C_k} \chi_i(g) = t_k\chi_i(x_k)$, $\sum_{g\in C_k} \chi_j(g^{-1}) = t_k\chi_j(x_k^{-1})$.
Potom $\sum_{g\in C_k} \chi_i(g)\chi_j(g^{-1}) = t_k\chi_i(x_k)\chi_j(x_k^{-1})$, a proto
$\delta_{ij}|G| = \sum_{k=1}^{r}(\sum_{g\in C_k} \chi_i(g)\chi_j(g^{-1})) = \sum_{k=1}^{r} t_k\chi_i(x_k)\chi_j(x_k^{-1})$.

■

Definice 5.10 *Nechť G je konečná grupa, nechť $C_1, ..., C_r$ jsou třídy konjugovaných prvků grupy G. Každou funkci $\alpha: G \longrightarrow T$, která je konstantní na každé třídě konjugovaných prvků grupy G, T je těleso, nazveme třídová funkce na grupě G nad T. Množinu všech třídových funkcí na grupě G nad T označíme* $\mathrm{Cl}\,(G, T)$.

Poznámka 5.2 Jednoduše vidíme.

(*i*) Je-li h reprezentace konečné grupy G ve V_n nad T, potom její charakter χ je třídová funkce, tedy $\chi \in \mathrm{Cl}\,(G, T)$.

(*ii*) Pro každé $i = 1, ..., r$ je C_i třída konjugovaných prvků grupy G, $x_i \in C_i$ reprezentant třídy C_i. Pro každé $\alpha \in \mathrm{Cl}\,(G, T)$ máme $[\alpha(x_1), ..., \alpha(x_r)]^T \in T_r$, tím lze definovat zobrazení $\varphi: \mathrm{Cl}\,(G, T) \longrightarrow T_r$ předpisem $\varphi(\alpha) = [\alpha(x_1), ..., \alpha(x_r)]^T$. Toto zobrazení je zřejmě izomorfismus, proto $\mathrm{Cl}\,(G, T) \cong T_r$ a $\dim \mathrm{Cl}\,(G, T) = r$.

(*iii*) Je-li $T = \mathbb{C}$, potom pro $\alpha \in \mathrm{Cl}\,(G, \mathbb{C})$ označme

$$v(\alpha) = [\alpha(x_1), ..., \alpha(x_r)]^T,$$

$$w(\alpha) = \left[\frac{t_1\alpha(x_1^{-1})}{|G|}, ..., \frac{t_r\alpha(x_r^{-1})}{|G|}\right],$$

kde $x_i \in C_i$ je reprezentant třídy C_i, $t_i = |C_i|$ pro každé $i = 1, ..., r$.
Pro každé $\alpha, \beta \in \mathrm{Cl}\,(G, \mathbb{C})$ a pro každé $c \in \mathbb{C}$ platí
$v(\alpha + \beta) = v(\alpha) + v(\beta)$,
$w(\alpha + \beta) = w(\alpha) + w(\beta)$,
$v(c\alpha) = cv(\alpha)$,
$w(c\alpha) = cw(\alpha)$.

Věta 5.22 *Nechť $h_1, ..., h_s$ jsou ireducibilní a po dvou neekvivalentní reprezentace konečné grupy G, nechť $\chi_1, ..., \chi_s$ jsou jejich charaktery. Potom charaktery $\chi_1, ..., \chi_s$ jako prvky vektorového prostoru* $\mathrm{Cl}\,(G, \mathbb{C})$ *jsou lineárně nezávislé, proto $s \leq r = \dim \mathrm{Cl}\,(G, \mathbb{C})$.*

Důkaz Nechť $\lambda_1\chi_1+\lambda_2\chi_2+\cdots+\lambda_s\chi_s = 0$. Potom pro každé $j = 1, ..., s$ je $0 = w(\chi_j)v(0) = w(\chi_j)v(\lambda_1\chi_1 + \lambda_2\chi_2 + \cdots + \lambda_s\chi_s) = \lambda_1 w(\chi_j)v(\chi_1) + \lambda_2 w(\chi_j)v(\chi_2) + \cdots + \lambda_s w(\chi_j)v(\chi_s)$.
Ovšem pro každé $i = 1, ..., s$ je $w(\chi_j)v(\chi_i) = \sum_{u=1}^{r} \frac{t_u\chi_j(x_u^{-1})}{|G|}\chi_i(x_u) = \frac{1}{|G|}\sum_{u=1}^{r} t_u\chi_j(x_u^{-1})\chi_i(x_u)$
$= \frac{1}{|G|}\delta_{ij}|G| = \delta_{ij}$ podle věty 5.21.
Tím $0 = \lambda_j w(\chi_j)v(\chi_j) = \lambda_j$, a tedy charaktery $\chi_1, ..., \chi_s$ jsou lineárně nezávislé.

■

Označme $\mathcal{K}$ třídu ekvivalentních reprezentací konečné grupy G. Podle důsledku 11 jsou buď všechny reprezentace v $\mathcal{K}$ ireducibilní, nebo jsou všechny reprezentace v $\mathcal{K}$ reducibilní. Označme $\mathcal{K}_1$,...,$\mathcal{K}_s$ všechny různé třídy ireducibilních reprezentací konečné grupy G. Podle věty 5.22 je $s \leq r = \dim \mathrm{Cl}\,(G, \mathbb{C})$.

Je-li $h\colon G \longrightarrow \mathrm{Aut}\, V_n$ reprezentace konečné grupy G nad $\mathbb{C}$, potom podle věty 5.10 je reprezentace h ekvivalentní s $h_1 \oplus \cdots \oplus h_z$, kde pro každé $i = 1, ..., z$ je h_i ireducibilní reprezentace grupy G. Některé z těchto reprezentací mohou být ekvivalentní, proto reprezentace h je ekvivalentní s $(m_1 \times h_1) \oplus \cdots \oplus (m_s \times h_s)$, kde $m_i \times h_i = \underbrace{h_i \oplus \cdots \oplus h_i}_{m_i}$, h_i je ireducibilní reprezentace konečné grupy G, $m_i \in \mathbb{Z}$, $m_i \geq 0$ pro každé $i = 1, ..., s$.

Věta 5.23 *Nechť $h^r\colon G \longrightarrow \mathrm{Aut}\, V_m$ je regulární reprezentace konečné grupy G ve V_m nad $\mathbb{C}$, $m = |G|$, nechť h^r je ekvivalentní s $(m_1 \times h_1) \oplus \cdots \oplus (m_s \times h_s)$, kde h_i je ireducibilní reprezentace konečné grupy G, $m_i \in \mathbb{Z}$, $m_i \geq 0$ pro každé $i = 1, ..., s$. Potom platí:*

(*i*) $m_i = n_i$, *kde n_i je stupeň ireducibilní reprezentace h_i pro každé $i = 1, ..., s$.*

(*ii*) $\sum_{i=1}^{s} n_i^2 = |G|$.

(*iii*) $\sum_{i=1}^{s} n_i\chi_i(x_k) = 0$ *pro každé $k = 2, ..., r$, kde χ_i označuje charakter reprezentace h_i.*

Důkaz Podle věty 5.14 mají ekvivalentní reprezentace stejné charaktery, proto
$\chi = m_1\chi_1 + m_2\chi_2 + \cdots + m_s\chi_s$,
kde χ je charakter regulární reprezentace h^r. Podle definice regulární reprezentace je $\chi(1) = m = |G|$ a $\chi(g) = 0$ pro každé $g \in G,\ g \neq 1$.
Pro každé $i = 1, ..., s$ máme
$w(\chi)v(\chi_i) = w(m_1\chi_1 + \cdots + m_s\chi_s)v(\chi_i) = m_1 w(\chi_1)v(\chi_i) + \cdots + m_s w(\chi_s)v(\chi_i) =$
$\sum_{j=1}^{s} m_j w(\chi_j)v(\chi_i) = \sum_{j=1}^{s} m_j\delta_{ij} = m_i$ podle věty 5.21 - již jsme dokazovali v důkazu věty 5.22.
Z druhé strany však pro každé $i = 1, ..., s$ máme
$w(\chi)v(\chi_i) = \sum_{k=1}^{r} \frac{t_k\chi(x_k^{-1})}{|G|}\chi_i(x_k) = \frac{t_1\chi(x_1^{-1})}{|G|}\chi_i(x_1) = \frac{t_1\chi(1^{-1})}{|G|}\chi_i(1) = \frac{t_1|G|}{|G|}\chi_i(1) =$
$1\chi_i(1) = n_i$.
Tím $m_i = w(\chi)v(\chi_i) = n_i$ pro každé $i = 1, ..., s$ - ukázali jsme první tvrzení.

Potom $\chi = m_1\chi_1 + \cdots + m_s\chi_s = n_1\chi_1 + \cdots + n_s\chi_s$, a tedy pro prvek $g = 1$ máme $|G| = m = \chi(1) = n_1\chi_1(1) + \cdots + n_s\chi_s(1) = n_1n_1 + \cdots + n_sn_s = n_1^2 + \cdots + n_s^2$ - ukázali jsme druhé tvrzení.
Pro každý prvek $g \in G$, $g \neq 1$ je $\chi(g) = 0$, a proto pro každé $k = 2, ..., r$ je $\chi(x_k) = 0$. Tím $0 = \chi(x_k) = n_1\chi_1(x_k) + \cdots + n_s\chi_s(x_k) = \sum_{i=1}^{s} n_i\chi_i(x_k)$ pro každé $k = 2, ..., r$ - ukázali jsme třetí tvrzení věty.

■

Lemma 5.2 *Jsou-li $C_1, ..., C_r$ třídy konjugovaných prvků konečné grupy G, potom pro každé $i, j, k \in \{1, ..., r\}$ je buď $C_k \cap C_iC_j = \emptyset$ nebo $C_k \subseteq C_iC_j$.*

Důkaz Je-li $C_k \cap C_iC_j \neq \emptyset$, potom existuje prvek $z \in C_k \cap C_iC_j$, a tedy $z \in C_k$, $z = xy$, kde $x \in C_i$, $y \in C_j$. Pro každé $z' \in C_k$ existuje $g \in G$ tak, že $z' = gzg^{-1}$. Tím $z' = gzg^{-1} = gxyg^{-1} = gxg^{-1}gyg^{-1}$, a proto $z' \in C_iC_j$. Tím $C_k \subseteq C_iC_j$.

■

Lemma 5.3 *Nechť $C_1, ..., C_r$ jsou třídy konjugovaných prvků konečné grupy G, nechť nyní $C_k \subseteq C_iC_j$ pro $i, j, k \in \{1, ..., r\}$, nechť $z \in C_k$ je libovolný prvek. Jestliže označíme $z = x^{(1)}y^{(1)} = x^{(2)}y^{(2)} = \cdots = x^{(t)}y^{(t)}$ všechna různá vyjádření prvku z v C_iC_j, potom každý prvek $z' \in C_k$ má právě t různých vyjádření ve tvaru součinu prvků z C_i a C_j.*

Důkaz Pro každé $z' \in C_k$ existuje $g \in G$ tak, že $z' = gzg^{-1}$. Definujeme-li zobrazení $\Omega_g \colon G \longrightarrow G$ předpisem $\Omega_g(x) = gxg^{-1}$ pro každé $x \in G$, potom toto zobrazení je automorfismus a nazývá se vnitřní automorfismus.
Potom $z' = gzg^{-1} = \Omega_g(z) = \Omega_g(x^{(1)})\Omega_g(y^{(1)}) = \Omega_g(x^{(2)})\Omega_g(y^{(2)}) = \cdots = \Omega_g(x^{(t)})\Omega_g(y^{(t)})$. Protože Ω_g je automorfismus, je toto t různých vyjádření prvku z'.
Kdyby prvek z' měl t' různých vyjádření, kde $t' > t$, potom i prvek $z = \Omega_g^{-1}(z')$ by měl t' různých vyjádření, což je spor. Proto každý prvek $z' \in C_k$ má právě t různých vyjádření.

■

Definice 5.11 *Nechť $C_1, ..., C_r$ jsou třídy konjugovaných prvků konečné grupy G, nechť $i, j, k \in \{1, ..., r\}$. Jestliže $C_k \subseteq C_iC_j$, potom položme $t_{ijk} = t$, kde t je číslo z lemmatu 5.3, t.j. každý prvek z C_k má právě t různých vyjádření ve tvaru součinu prvků z C_i, C_j. Jestliže $C_k \cap C_iC_j = \emptyset$, potom položme $t_{ijk} = 0$. Čísla t_{ijk} se nazývají konstanty pro násobení tříd grupy G.*

Věta 5.24 *Nechť $h \colon G \longrightarrow \mathrm{Aut}\, V_n$ je ireducibilní reprezentace konečné grupy G ve V_n nad $\mathbb{C}$, nechť $C_1, ..., C_r$ jsou třídy konjugovaných prvků grupy G. Pro každé $i = 1, ..., r$ definujme matici*

$$\mathbf{S}_i = \sum_{x \in C_i} h^M(x).$$

Potom pro každé $i = 1, ..., r$ je matice $\mathbf{S}_i$ skalární, t.j. existuje číslo $\lambda_i \in \mathbb{C}$ tak, že $\mathbf{S}_i = \lambda_i\mathbf{I}$. Pro čísla λ_i platí:

(i) $\lambda_i\lambda_j = \sum_{k=1}^{r} t_{ijk}\lambda_k$ *pro každé* $i, j \in \{1, ..., r\}$

(ii) $\lambda_i = \frac{1}{n} t_i \chi(x_i)$ *pro každé* $i = 1, ..., r$, *kde* $x_i \in C_i$ *je reprezentant třídy* C_i, $t_i = |C_i|$, χ *je charakter reprezentace* h.

Důkaz Pro každé $g \in G$ a pro každé $j = 1, ..., r$ máme
$h^M(g)\mathbf{S}_j h^M(g^{-1}) = h^M(g)(\sum_{x\in C_j} h^M(x))h^M(g^{-1}) = \sum_{x\in C_j} h^M(g)h^M(x)h^M(g^{-1}) =$
$\sum_{x\in C_j} h^M(gxg^{-1}) = \mathbf{S}_j$, a tedy pro každé $g \in G$ je $h^M(g)\mathbf{S}_j = \mathbf{S}_j h^M(g)$.
Buď $\lambda_j \in \mathbb{C}$ vlastní číslo matice $\mathbf{S}_j$, tedy $\det(\lambda_j\mathbf{I} - \mathbf{S}_j) = 0$. Potom pro každé $g \in G$ můžeme psát $h^M(g)(\lambda_j\mathbf{I} - \mathbf{S}_j) = h^M(g)\lambda_j\mathbf{I} - h^M(g)\mathbf{S}_j = \lambda_j h^M(g) - \mathbf{S}_j h^M(g) = (\lambda_j\mathbf{I} - \mathbf{S}_j)h^M(g)$, a proto podle věty 5.8 je matice $\lambda_j\mathbf{I} - \mathbf{S}_j = \mathbf{0}$ nebo je to regulární matice. Protože však $\det(\lambda_j\mathbf{I} - \mathbf{S}_j) = 0$, je tato matice nulová, a proto $\mathbf{S}_j = \lambda_j\mathbf{I}$.
Počítejme
$\mathbf{S}_i\mathbf{S}_j = (\sum_{x\in C_i} h^M(x))(\sum_{y\in C_j} h^M(y)) = \sum_{x\in C_i}\sum_{y\in C_j} h^M(x)h^M(y) = \sum_{x\in C_i}\sum_{y\in C_j} h^M(xy) =$
$\sum_{k=1}^{r} t_{ijk}(\sum_{z\in C_k} h^M(z)) = \sum_{k=1}^{r} t_{ijk}\mathbf{S}_k$, neboť pro $C_k \cap C_iC_j = \emptyset$ je $t_{ijk} = 0$ a pro $C_k \subseteq C_iC_j$ máme pro každé $z \in C_k$ právě t_{ijk} různých vyjádření ve tvaru xy, kde $x \in C_i$, $y \in C_j$.
Tím pro každé $i, j = 1, ..., r$ získáváme $(\lambda_i\lambda_j)\mathbf{I} = (\lambda_i\mathbf{I})(\lambda_j\mathbf{I}) = \mathbf{S}_i\mathbf{S}_j = \sum_{k=1}^{r} t_{ijk}\mathbf{S}_k =$
$\sum_{k=1}^{r} t_{ijk}(\lambda_k\mathbf{I}) = (\sum_{k=1}^{r} t_{ijk}\lambda_k)\mathbf{I}$, a tedy $\lambda_i\lambda_j = \sum_{k=1}^{r} t_{ijk}\lambda_k$.
Dále pro každé $i = 1, ..., r$ máme
$\lambda_i n = \mathrm{Tr}\,(\lambda_i\mathbf{I}) = \mathrm{Tr}\,(\mathbf{S}_i) = \mathrm{Tr}\,(\sum_{x\in C_i} h^M(x)) = \sum_{x\in C_i} \mathrm{Tr}\,(h^M(x)) = \sum_{x\in C_i} \chi(x) = \chi(x_i)t_i$.
Proto $\lambda_i = \frac{1}{n} t_i \chi(x_i)$.

■

Věta 5.25 *Nechť* $h_1, ..., h_s$ *jsou ireducibilní a po dvou neekvivalentní reprezentace konečné grupy* G, *nechť* $\chi_1, ..., \chi_s$ *jsou jejich charaktery. Potom platí:*

$$\sum_{l=1}^{s} \chi_l(x_i)\chi_l(x_j^{-1}) = \frac{|G|}{t_i}\delta_{ij} = \frac{|G|}{t_j}\delta_{ij}.$$

Důkaz Pro každé $l = 1, ..., s$ je h_l ireducibilní reprezentace, χ_l její charakter, a proto podle věty 5.24 je $\mathbf{S}_i^{(l)} = \sum_{x\in C_i} h_l^M(x) = \lambda_i^{(l)}\mathbf{I}$, $\lambda_i^{(l)}\lambda_j^{(l)} = \sum_{k=1}^{r} t_{ijk}\lambda_k^{(l)}$, $\lambda_i^{(l)} = \frac{1}{n_l} t_i \chi_l(x_i)$. Proto
$\frac{1}{n_l} t_i \chi_l(x_i) \frac{1}{n_l} t_j \chi_l(x_j) = \sum_{k=1}^{r} t_{ijk} \frac{1}{n_l} t_k \chi_l(x_k)$
Vynásobíme-li tuto rovnost n_l^2, získáme
$t_i\chi_l(x_i)t_j\chi_l(x_j) = \sum_{k=1}^{r} t_{ijk} n_l t_k \chi_l(x_k)$,

která platí pro každé $l = 1, ..., s$ - všechny tyto rovnosti sečteme.
$\sum_{l=1}^{s} t_i\chi_l(x_i)t_j\chi_l(x_j) = \sum_{l=1}^{s}(\sum_{k=1}^{r} t_{ijk}n_l t_k\chi_l(x_k))$,
$t_it_j\sum_{l=1}^{s}\chi_l(x_i)\chi_l(x_j) = \sum_{k=1}^{r} t_{ijk}t_k(\sum_{l=1}^{s} n_l\chi_l(x_k))$.
Podle věty 5.23 je $\sum_{l=1}^{s} n_l\chi_l(x_k) = 0$ pro každé $k = 2, ..., r$. Pro $k = 1$ je $\sum_{l=1}^{s} n_l\chi_l(x_1) = \sum_{l=1}^{s} n_l\chi_l(1) = \sum_{l=1}^{s} n_l n_l = \sum_{l=1}^{s} n_l^2 = |G|$ podle věty 5.23. Tím získáváme
$t_it_j\sum_{l=1}^{s}\chi_l(x_i)\chi_l(x_j) = \sum_{k=1}^{r} t_{ijk}t_k(\sum_{l=1}^{s} n_l\chi_l(x_k)) = t_{ij1}t_1(\sum_{l=1}^{s} n_l\chi_l(x_1)) = t_{ij1}1|G| = t_{ij1}|G|$.
Protože $C_1^{-1}, C_2^{-1}, ..., C_r^{-1}$ jsou opět všechny třídy konjugovaných prvků G, existuje pro každé $j = 1, ..., r$ index $p = 1, ..., r$ tak, že $C_j = C_p^{-1}$.
Číslo t_{ij1} udává, kolikrát se v součinu $C_iC_j = C_iC_p^{-1}$ objeví 1.
$1 \notin C_iC_j = C_iC_p^{-1}$ právě tehdy, když $t_{ij1} = 0$,
$t_{ij1} \neq 0$ právě tehdy, když $1 = xy$, kde $x \in C_i$, $y \in C_j = C_p^{-1}$, ale z toho nutně $p = i$. Tím pro $t_{ij1} \neq 0$ je $t_{ij1} = t_i$.

Potom dosazením do rovnosti $t_it_j\sum_{l=1}^{s}\chi_l(x_i)\chi_l(x_j) = t_{ij1}|G|$ získáváme

$t_it_p\sum_{l=1}^{s}\chi_l(x_i)\chi_l(x_p^{-1}) = \delta_{ip}t_i|G|$. Vydělelím rovnosti čísly t_it_p máme tvrzení věty
$\sum_{l=1}^{s}\chi_l(x_i)\chi_l(x_p^{-1}) = \delta_{ip}\frac{|G|}{t_p} = \delta_{ip}\frac{|G|}{t_i}$.

■

Věta 5.26 *Nechť G je konečná grupa, nechť s je počet všech různých tříd $\mathcal{K}_1, ..., \mathcal{K}_s$ ekvivalentních ireducibilních reprezentací, nechť r je počet tříd $C_1, ..., C_r$ konjugovaných prvků grupy G. Potom $s = r$.*

Důkaz Podle věty 5.22 je $s \leq r$.
Vezměme pro každé $i = 1, ..., s$ $\chi_i \in \mathcal{K}_i$, χ_i je charakter ireducibilní reprezentace h_i. Reprezentace $h_1, ..., h_s$ jsou po dvou neekvivalentní.
Označme pro každé $i, j = 1, ..., r$ vektory $\tilde{v}_i = [\chi_1(x_i), \chi_2(x_i), ..., \chi_s(x_i)]^T$
$\tilde{w}_j = [\chi_1(x_j^{-1}), \chi_2(x_j^{-1}), ..., \chi_s(x_j^{-1})]$. Potom podle věty 5.25 máme
$\tilde{w}_j\tilde{v}_i = \sum_{l=1}^{s}\chi_l(x_i)\chi_l(x_j^{-1}) = \frac{|G|}{t_i}\delta_{ij} = \frac{|G|}{t_j}\delta_{ij}$.
Ukážeme, že vektory $\tilde{v}_1, \tilde{v}_2, ..., \tilde{v}_r$ jsou lineárně nezávislé.
Nechť $\xi_1\tilde{v}_1 + \xi_2\tilde{v}_2 + \cdots + \xi_r\tilde{v}_r = 0$.
Potom pro každé $j = 1, ..., r$ máme
$0 = \tilde{w}_j 0 = \tilde{w}_j(\xi_1\tilde{v}_1 + \xi_2\tilde{v}_2 + \cdots + \xi_r\tilde{v}_r) = \xi_1\tilde{w}_j\tilde{v}_1 + \xi_2\tilde{w}_j\tilde{v}_2 + \cdots + \xi_r\tilde{w}_j\tilde{v}_r = \sum_{i=1}^{r}\xi_i\tilde{w}_j\tilde{v}_i =$

$\sum_{i=1}^{r} \xi_i \delta_{ij} \frac{|G|}{t_j} = \xi_j \frac{|G|}{t_j}$.
Protože $|G| \neq 0$, je $\xi_i = 0$ pro každé $i = 1, ..., r$, tím jsou vektory $\tilde{v}_1, \tilde{v}_2, ..., \tilde{v}_r$ ineárně nezávislé, a proto $r \leq s$.

■

Důsledek 14 Je-li konečná grupa G komutativní, potom počet neekvivalentních ireducibilních reprezentací grupy G se rovná řádu $|G|$ a navíc každá ireducibilní reprezentace má stupeň 1.

Definice 5.12 *Je-li G grupa, potom podgrupa grupy G generovaná prvky $x^{-1}y^{-1}xy$ pro každé $x, y \in G$ se nazývá komutatnt grupy G a značí G'.*

Poznámka 5.3 Pro každou grupu G je komutant G' normální podgrupa grupy G a faktorgrupa G/G' je Abelova.

Věta 5.27 *Je-li G konečná grupa, potom počet neekvivalentních ireducibilních reprezentací stupně 1 grupy G se rovná $[G : G']$, tedy indexu komutantu G' v grupě G.*

Důkaz Je-li h reprezentace grupy G stupně 1, potom $h\colon G \longrightarrow \operatorname{Aut} V_1$. Protože grupa $\operatorname{Aut} V_1$ je Abelova, je $G/\operatorname{Ker} h \cong \operatorname{Im} h$, tím grupa $G/\operatorname{Ker} h$ je také Abelova, a proto G' je podgrupa $\operatorname{Ker} h$.
Budeme definovat zobrazení $\overline{h}\colon G/G' \longrightarrow \operatorname{Aut} V_1$ předpisem
$\overline{h}(gG') = h(g)$ pro každé $g \in G$.
Jestliže $gG' = g_1G'$, potom $g_1^{-1}g \in G'$, tím $g_1^{-1}g \in \operatorname{Ker} h$, a proto $h(g) = h(g_1)$. Předpis $\overline{h}$ je opravdu zobrazení. Protože $\overline{h}((gG')(g_1G')) = \overline{h}(gg_1G') = h(gg_1) = h(g) \circ h(g_1) = \overline{h}(gG')\overline{h}(g_1G')$, je $\overline{h}$ homomorfismus, a tedy reprezentace grupy G/G' ve V_1.
Můžeme tedy definovat zobrazení Φ, které každé reprezentaci h grupy G ve V_1 přiřadí reprezentaci $\overline{h}$ grupy G/G' ve V_1. Ukážeme, že toto zobrazení Φ je bijekce.
Nechť $\tilde{h}$ je reprezentace grupy G/G' ve V_1. Potom zobrazení $h\colon G \longrightarrow \operatorname{Aut} V_1$ dané předpisem $h(g) = \tilde{h}(gG')$ pro každé $g \in G$ je reprezentace grupy G ve V_1. Označíme-li $\Phi(h) = \overline{h}$, pak pro každé $g \in G$ je $\overline{h}(gG') = h(g) = \tilde{h}(gG')$, tedy $\Phi(h) = \tilde{h}$ a zobrazení Φ je na.
Jsou-li h, k reprezentace grupy G ve V_1 takové, že $\Phi(h) = \Phi(k)$, potom pro každé $g \in G$ je $h(g) = \overline{h}(gG') = \Phi(h)(gG') = \Phi(k)(gG') = \overline{k}(gG') = k(g)$, tedy $h = k$, a proto Φ je prosté.
Tím jsme ukázali, že počet různých reprezentací grupy G ve V_1 je roven počtu různých reprezentací grupy G/G' ve V_1 a to je $|G/G'| = [G : G']$, protože G/G' je Abelova grupa.

■