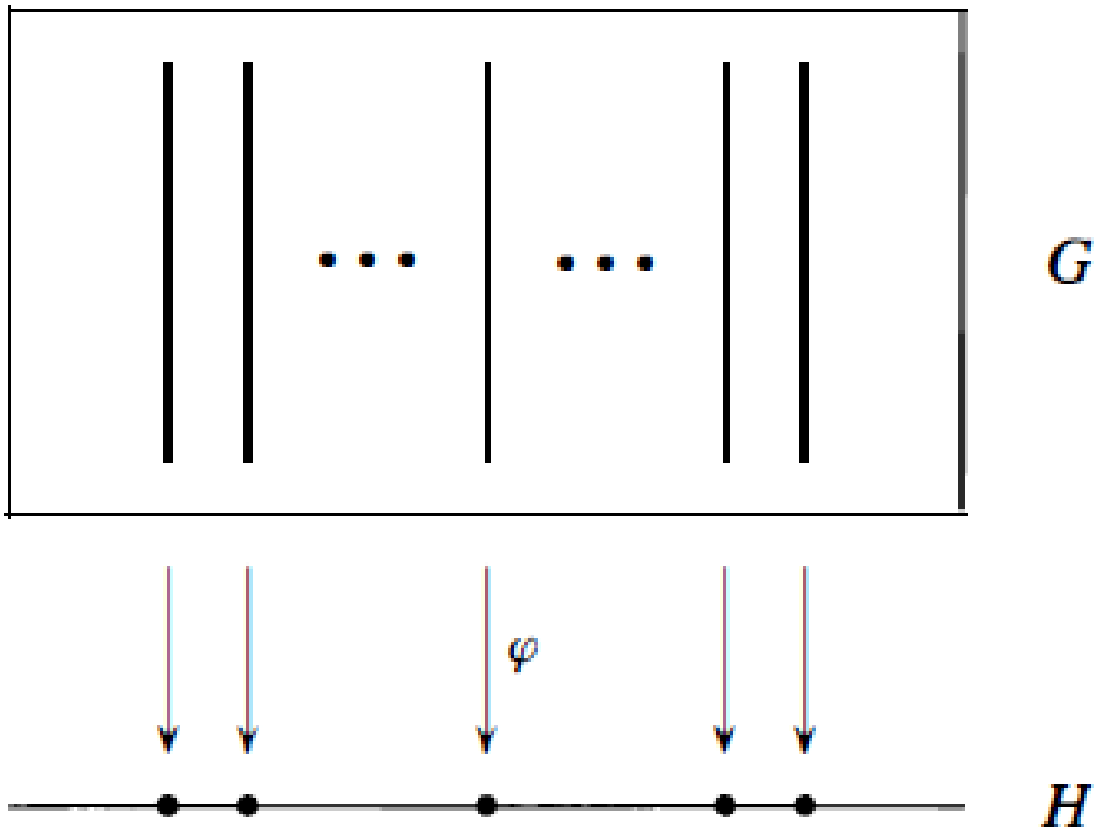
Grupy a reprezentace 3

Zpracováno na základě poznámek J. Mareše a s jejich využitím

wiki-skripta

Studium struktury grupy skrze faktor grupu

Mějme grupy G a H a homomorfismus $\varphi : G \to H$. ***Vláknem*** *homomorfismu φ příslušejícím prvku $x \in H$ nazýváme množinu $\{y \in G | \varphi(y) = x\}$, tedy množina všech prvků, které se zobrazí na x.*



Obrázek: Znázornění vláken homomorfismu. Převzato z Dummit,Foote

Homomorfismus $\varphi : \mathbb{Z} \to \mathbb{Z}_5$

Example

-5	-4	-3	-2	-1	
0	1	2	3	4	
5	6	7	8	9	
...	...	...	...	...	$\mathbb{Z}$
± 15	1 ± 15	2 ± 15	3 ± 15	4 ± 15	
...	...	...	...	...	
$\pm n5$	$1 \pm n5$	$2 \pm n5$	$3 \pm n5$	$4 \pm n5$	
0	1	2	3	4	$\mathbb{Z}_5$

Vlákno jsou složené z prvků v sloupci, vlákno jsou všechny prvky ve sloupci.
Definice:
Jádro homomorfismu $\varphi : G \to H$ jsou všechny prvky G, které se zobrazí na e_H.

$$\text{Ker } \varphi \equiv \{g \in G |\ \varphi(g) = e_H\}$$

Corollary

Pro homomorfismus $\varphi : G \to H$ *platí:*

1. $\varphi(e_G) = e_H$
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$ *pro* $\forall q \in G$
3. $\varphi(g^n) = \varphi(g)^n$ *pro* $\forall n \in \mathbb{Z}$
4. $Ker\ \varphi \leq G$
5. $\varphi(G) \leq H$

Důkaz.

1. $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) \implies$ (krácení v H) $\varphi(e_G) = e_H$.
2. $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H$, tedy $\varphi(g^{-1}) = \varphi(g)^{-1}$.
3. Indukcí na n.
4. Stačí dokázat $g_1, g_2 \in \text{Ker } \varphi \implies g_1 g_2^{-1} \in \text{Ker } \varphi$. platí $e_G \in \text{Ker } \varphi$, tj. jádro je neprázdné. Nechť $g_1, g_2 \in \text{Ker } \varphi$. Pak $\varphi(g_1) = \varphi(g_2) = e_G$. Potom $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = e_H$.
5. Stejně jako předchozí bod, jen předpoklad $h_1 = \varphi(g_1)$.

Faktor grupa

Rozklad do tříd ekvivalence: $a, b \in G, a \sim b \Leftrightarrow \exists k \in K, ka = b$

Mějme homomorfismus $\varphi : G \to H$ s jádrem Ker $\varphi = K$. Potom **faktor grupa** G/K (G modulo K) je grupa, jejíž prvky tvoří vlákna homomorfismu φ a operace násobení mezi vlákny je definovaná pomocí násobením mezi příslušnými obrazy homomorfismu v grupě H.

pokud X je vlákno nad a a Y je vlákno nad b, pak prvek $XY \in G/K$ je vlákno nad ab.

Navíc jednotkovým prvkem ve faktor grupě je jádro homomorfismu - podgrupa K.

To, že faktor grupa má skutečně vlastnosti grupy, se lehce ověří z platnosti těchto vlastností v H.

Theorem

Mějme homomorfismus $\varphi : G \to H$ s jádrem $Ker\ \varphi = K$ a nechť $X_a \in G/K$ je vlákno nad $a \in H$, tedy $X_a = \varphi^{-1}(a)$. Potom platí:

1. $\forall u \in X_a$ *je* $X_a = \{uk | k \in K\}$,
2. $\forall u \in X_a$ *je* $X_a = \{ku | k \in K\}$.

Důkaz.

Dokážeme pouze první bod (druhý se dokazuje analogicky).

- *Označme* $uK = \{uk | k \in K\}$, *mějme* $u \in X_a$ *(tedy* $\varphi(u) = a$*) a ukážeme, že* $uK \subset X_a$*:* $\varphi(uk) = \varphi(u)\varphi(k) = \varphi(u)e = a$. *(Využili jsme nejprve toho, že* φ *je homomorfismus a pak toho, že* k *je z jádra.)*
- *Pro důkaz opačné inkluze* $X_a \subset uK$ *mějme libovolné* $g \in X_a$ *a vezměme* $k = u^{-1}g$. *Jelikož*

$$\varphi(k) = \varphi(u^{-1}g) = \varphi(u^{-1})\varphi(g) = a^{-1}a = e,$$

k patří do jádra. Dále zřejmě $g = uk$, *tedy* $g \in uK$.

□

Levé a pravé třídy

Právě dokázaná věta nás opravňuje považovat vlákna a množiny $uK = Ku$ za třídy ekvivalence vzhledem k ekvivalenci $a \sim b \Leftrightarrow a = kb$ pro nějaké $k \in K$. (Triviální ověření vlastností ekvivalence je přenecháno čtenáři.)

> *Pro libovolnou $H \leq G$ a libovolné $g \in G$ nazýváme množiny $gH = \{gh | h \in H\}$ respektive $Hg = \{hg | h \in H\}$* ***levé*** *respektive* ***pravé třídy*** *H v G. Libovolný prvek třídy nazýváme jejím* ***reprezentantem****.*

Že to neplatí obecně: D_6, $K \equiv \{E, A\}$ a máme vevou a pravou třídu $BK = \{B, D\}$, ale $KB = \{B, F\}$

Theorem

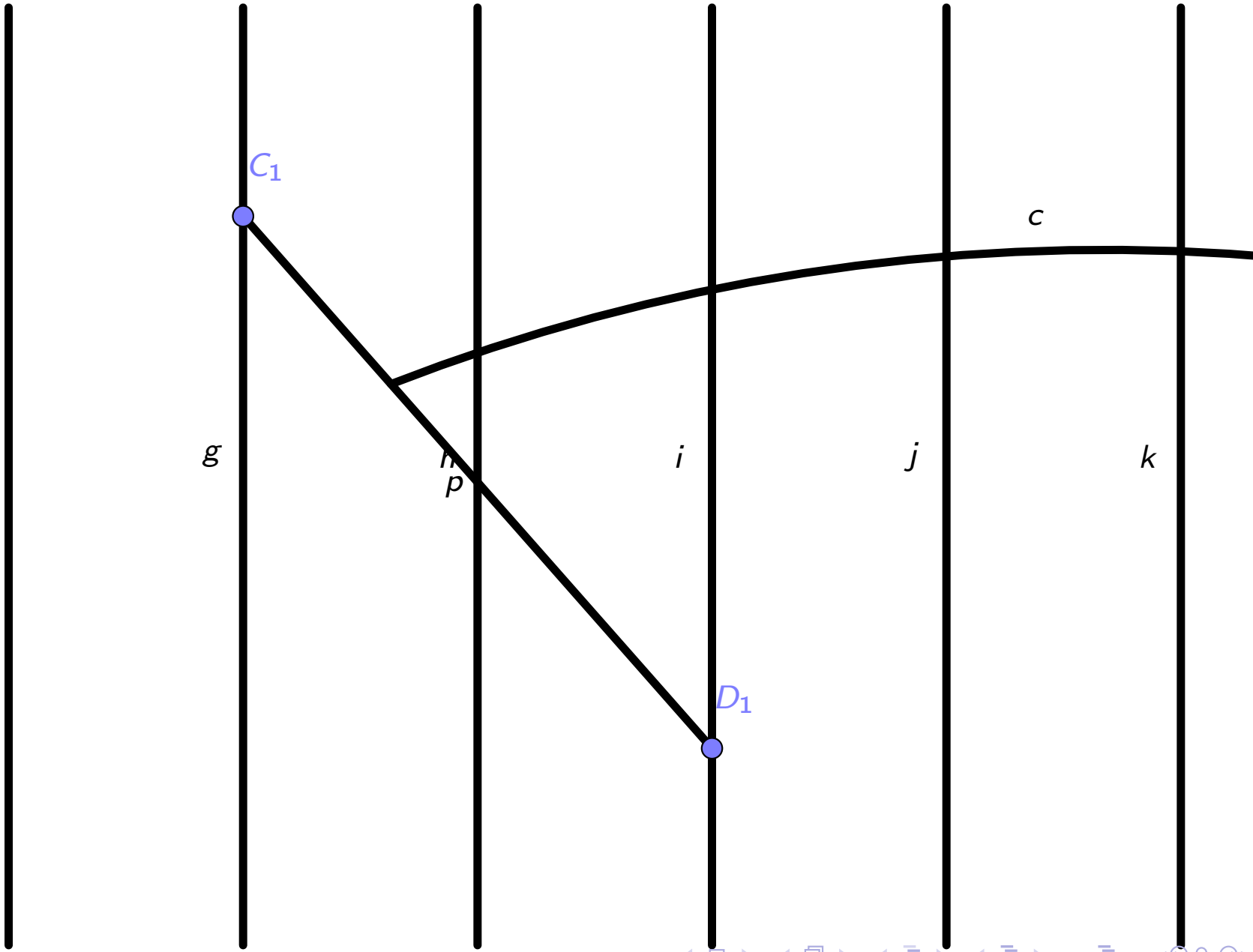
Buď G grupa a K jádro nějakého homomorfismu φ z G do nějaké grupy. Potom množina levých tříd K v G s operací definovanou jako $aK \circ bK = (ab)K$ je grupa G/K. Tedy tato operace je dobře definovaná (nezávisí na výběru reprezentanta).

Důkaz.

Mějme $X, Y \in G/K$, $X = \varphi^{-1}(a)$, $Y = \varphi^{-1}(b)$ a $Z = XY \in G/K$. Podle definice operací v G/K je $Z = \varphi^{-1}(ab)$. Z věty 3 víme, že prvky G/K jsou levé třídy K. Je třeba ukázat, že i operace, kterou zde definuje pomocí reprezentantů odpovídá původní definici násobení v G/K bez ohledu na výběr reprezentanta. Mějme $u \in X$ a $v \in Y$, tedy $\varphi(u) = a$, $\varphi(v) = b$ a $X = uK$ a $Y = vK$. Určíme, zda $uv \in Z$.

$$\varphi(uv) = \varphi(u)\varphi(v) = ab$$

Odtud tedy plyne, že $uv \in Z$, a tedy $Z = uvK$. □


C_1
c
g
h
p
i
j
k
D_1

Theorem

Nechť $N \leq G$, potom množina levých tříd N v G tvoří rozklad G (jejich sjednocením je G a jednotlivé třídy mají prázdný průnik). Dále $\forall u, v \in G$ platí $uN = vN$ právě tehdy, když $u^{-1}v \in N$, tedy když u a v jsou reprezentanty stejné třídy.

Důkaz.

Nejprve ukážeme, že sjednocením levých tříd je celé G. Jelikož N je grupa, pak $e \in N$, a tedy platí:

$$\bigcup_{g \in G} gN \supset \bigcup_{g \in G} ge = G.$$

Pro důkaz druhé části vezmeme $uN \cap vN \neq \emptyset$ a ukážeme, že potom platí $uN = vN$. Vezměme $x \in uN \cap vN$, tedy x můžeme napsat jako $x = un_1 = vn_2$ pro nějaká $n_1, n_2 \in N$. Rovnost vynásobíme zprava n_1^{-1} a dostaneme $u = vn_2n_1^{-1} = vn_3$ pro nějaké $n_3 \in N$. Tedy vidíme, že $u \in vN$. Dále pro libovolné $t \in uN$ platí $t = un_4 = (vn_3)n_4 = vn_5$, takže $t \in vN$ pro $\forall t \in uN$, tedy $uN \subset vN$. Opačnou inkluzi dostaneme záměnou role u a v. Jelikož víme, že $u = vn_3$, pak platí $v^{-1}u = n_3$, tedy $v^{-1}u \in N$ a to platí pro libovolné reprezentanty tříd. □

Dobře definovaná operace

Právě dokázaná věta říká, že levé třídy jsou třídy ekvivalence vzhledem k ekvivalenci $a \sim b \Leftrightarrow a = nb$ pro nějaké $n \in N$ a G je tedy rozloženo do tříd ekvivalence.

Definice

Operace $\circ$ na levých třídách N v G je **dobře definovaná**, když $\forall u, v \in G$ platí

$$u, u_1 \in uN, \quad v, v_1 \in vN \Rightarrow (uv)N = (u_1 v_1)N = uN \circ vN$$

Theorem

Buď G grupa a $N \leq G$. Potom:

1. *Operace na levých třídách definovaná jako $uN \circ vN = (uv)N$ je dobře definovaná právě tehdy, když $(gng^{-1} \in N)(\forall g \in G \text{ a } \forall n \in N)$.*
2. *Je-li výše uvedená operace dobře definovaná, pak je množina levých tříd N s touto operací grupou, jednotkovým prvkem eN a inverzními prvky $(gN)^{-1} = g^{-1}N$.*

Důkaz 1

($\Rightarrow$) Nechť je operace na levých třídách dobře definovaná, tedy

$$(\forall u, v \in G)(u, u_1 \in uN \text{ a } v, v_1 \in vN \rightarrow uvN = u_1 v_1 N).$$

Nechť $g \in G$ a $n \in N$ libovolné. Položíme $u = e$, $u_1 = n$ a $v = v_1 = g^{-1}$ a z předpokladu dostaneme

$$g^{-1}N = ng^{-1}N$$

Protože $e \in N$, $ng^{-1} \in g^{-1}N$. Tedy $ng^{-1} = g^{-1}n_1$, pro nějaké $n_1 \in N$. Vynásobením g zleva dostáváme požadovanou rovnost $gng^{-1} = n_1 \in N$.

($\Leftarrow$) Předpokládáme $(gng^{-1} \in N)(\forall g \in G \text{ a } \forall n \in N)$ a vezmeme $u, u_1 \in uN$ a $v, v_1 \in vN$. Pak můžeme psát $u_1 = un$ a $v_1 = vm$ pro nějaké $n, m \in N$. Musíme ukázat, že $u_1 v_1 \in uvN$:

$$u_1 v_1 = (un)(vm) = u(vv^{-1})nvm = (uv)(v^{-1}nv)m = (uv)(n_1)m = uvn_2$$

kde $n_1 = v^{-1}nv = (v^{-1})n(v^{-1})^{-1} \in N$ z předpokladu a $n_2 = n_1 m \in N$ z definice. Protože $u_1 v_1 \in uvN \cap u_1 v_1 N$, plyne z předchozí věty rovnost $uvN = u_1 v_1 N$.

Důkaz 2

Je-li operace na levých třídách dobře definovaná, axiomy grupy se přenášejí z G. Pro $\forall u, v, w \in G$
Asociativita:

$$(uN) \circ (vN \circ wN) = uN \circ (vwN) = u(vw)N = (uv)wN = (uN \circ vN) \circ (wN).$$

Z definice násobení je vidět že jednotka v G/N je N a $g^{-1}N$ je inverze gN.

A tudíž jsem schopen vytvořit faktor grupu na levých třídách.

Normální podgrupy

Definice:
Normální podgrupou H v G nazvenme každou podgrupu, kterou normalizuje celá grupa, značíme $H \trianglelefteq G$, tj.

$$H \trianglelefteq G \Leftrightarrow N_G(H).$$

Vlatnost$\trianglelefteq$ není tranzitivní, zatímco $\leq$ je tranzitivní.
Definice:

1. Prvek $m = gng^{-1}$ se nazývá **konjugovaný** k n prvkem g.
2. Buď $A \subset G$ libovolná podmnožina grupy. Množina $M = gAg^{-1}$ se nazývá **konjugovaná** k A prvkem g.

   Pro ověření, zda podgrupa $N \leq G$ je normální, stačí ověřit, že komutuje s generátory množiny $G \setminus N$ (množinový rozdíl), pokud tyto generátory známe.

Theorem

Nechť $N \leq G$, potom následující tvrzení jsou ekvivalentní:

1. $N \trianglelefteq G$
2. $N_G(N) = G$
3. $gN = Ng$ *pro* $\forall g \in G$.
4. *Operace na třídách je dobře definovaná.*
5. $gNg^{-1} \subset N$ *pro* $\forall g \in G$.

Důkaz přímo z definice.

Theorem

Nechť $N \leq G$, potom $N \trianglelefteq G$ právě tehdy když $\exists$ homomorfismus $\varphi(G)$ takový, že $N = Ker\ \varphi$.

Důkaz.

($\Leftarrow$) *Podle jedné z předchozích vět víme, že levé a pravé třídy dke jádra homomorfismu jsou stejné ($gN = Ng$), což je podle věty ekvivalentní normálnosti grupy.*

($\Rightarrow$) *Nyní máme $N \trianglelefteq G$ a označíme $H = G/N$. Operace na levých třídách pro normální grupu je dobře definovaná. Definujeme zobrazení $\pi : G \to G/N$ jako $\pi(g) = gN$ pro $\forall g \in G$. Z definice operací v G/N platí pro $\forall f, g \in G$: $\pi(fg) = (fg)N = fNgN = \pi(f)\pi(g)$, tedy π je homomorfismus. Jeho jádro je: $Ker\ (\pi) = \{g \in G | \pi(g) = eN\} = \{g \in G | gN = eN\} = \{g \in G | g \in N\} = N$.*

□

Nyní můžeme faktorizovat podle normální podgrupy G/N, aniž bychom měli homomorfismus.

Definice:

Buď $N \trianglelefteq G$, pak zobrazení $\pi : G \to G/N : \pi(g) = gN$ nazýváme ***přirozená projekce*** *G na G/N.*

Shrnutí:

Homomorfismus $\to$ jádro $\to$ faktor grupa $\to$ dobře definovaná operace $\to$ normální podgrupa $\to$ přirozená projekce (homomorfismus)

Theorem

Nechť $N \trianglelefteq G$. Množina levých tříd G dle N tvoří rozklad G dle N,

$$G = N \cup a_1 N \cup a_2 N \cup a_3 N \cup \dots$$

a platí:

$$\forall u, v \in G \quad je \quad uN = vN \Leftrightarrow v^{-1}u \in N.$$

Důkaz.

$(\Leftarrow)$ $uk = vk' \Leftarrow v^{-1}u = k'k^{-1} \in N$
$(\Rightarrow)$ *Nechť* $k = v^{-1}u \in N$, *tj.*
$N = kN = (v^{-1}u)N = v^{-1}N \circ uN \Rightarrow (vN)^{-1} \circ uN = N, \Rightarrow vN = uN$ □

Theorem (Lagrange)

Nechť G je konečná, $H \leq G$, potom $|H|$ dělí $|G|$. Navíc počet levých tříd H v G je roven $\frac{|G|}{|H|}$.

Důkaz.

Nejprve ukážeme, že všechny levé třídy mají stejně prvků. Definujme zobrazení $f : aH \to bH$ mezi libovolnými dvěma levými třídami aH a bH předpisem $f(x) = ba^{-1}x$. Protože zobrazení s předpisem $f^{-1}(y) = ab^{-1}y$ je zřejmě inverzní k f, je f bijekce mezi levými třídami, a ty tedy mají stejný počet prvků.
Označme $|H| = |eH| = n$ a k počet levých tříd. G rozděleno na k levých tříd o n prvcích, platí $|G| = kn$, a tedy $k = \frac{|G|}{n}$. □

První část důkazu (všechny levé třídy mají stejně prvků) platí i pro nekonečné grupy.

Důsledky:

- Grupa G prvočíselného řádu nemůže mít netriviální normální podgrupu. Tato grupa je cyklická a $G \simeq \mathbb{Z}_p$

  Důkaz:
  $e \neq x \in G$, a navíc $|\langle x \rangle| > 1$. $|\langle x \rangle|$ dělí $|G|$. Ale $|G|$ je prvočíslo, proto $|x| = p$.

- $$x^{|G|} = e$$

  Z Lagrangeovy věty $|G|$ je násobek $|x|$, $\frac{|G|}{|x|} = m$ tj. $x^{|x|m} = e = x^{|G|}$
- !! Obráceně neplatí: pokud m dělí $|G|$, potom nemusí existovat podgrupa řádu m !! (A_4 nemá podgrupu řádu 6)

Index podgrupy

Buď G grupa (i nekonečného řádu) a $H \leq G$. Potom počet levých tříd H v G nazýváme ***index*** *H v G a značíme $|G : H|$.*

Pro konečné grupy platí

$$|G : H| = \frac{|G|}{|H|}.$$

Důsledek:
Podgrupa s indexem 2 je normální.

$$\forall g \in G,\ gG = G = H \cup gH,\ g \notin H,\ Gg = G = H \cup Hg \Rightarrow gH = Hg$$