1 Faktorové grupy

1.1 Zopakovanie definície

Pretože toto je z toho, čo sme zatiaľ brali, asi najťažšia téma, azda nezaškodí dať sem zopár riešených úloh (možno aj s trochu detailnejším vysvetlením).

Najprv stručne zopakujme, čo vieme o faktorových grupách z prednášky.

Ak máme komutatívnu grupu $(G, +)$ a nejakú jej podgrupu H, tak predpis[1]

$$x \sim y \qquad \Leftrightarrow \qquad x - y \in H$$

určuje reláciu ekvivalencie na množine G.

Táto relácia ekvivalencie nám určí rozklad množiny G na triedy ekvivalencie. Môžeme si všimnúť, že trieda neutrálneho prvku je práve podgrupa H. Tiež môže byť užitočné vedieť, že trieda prvku a je presne

$$[a] = \{a + h; h \in H\}.$$

(Niekedy používame aj označenie $a + H$.)

Množinu všetkých tried tejto ekvivalencie označíme ako $[G/H]$, t.j.

$$[G/H] = \{[a]; a \in G\}.$$

Predpis

$$[a] + [b] = [a + b]$$

potom určuje dobre definovanú binárnu operáciu na množine G/H. Dá sa dokázať, že G/H s touto operáciou tvorí grupu. Túto grupu voláme faktorová grupa grupy $(G, +)$ podľa podgrupy H.

1.2 Veta o izomorfizme

V súvislosti s faktorovými grupami sa nám môže hodiť (prvá) veta o izomorfizme. Môžeme ju sformulovať napríklad takto:

Veta 1. *Nech G, G' sú grupy, navyše G je komutatívna.*[2] *Ak $f\colon G \to G'$ je surjektívny homomorfizmus, tak* $\operatorname{Ker} f$ *je podgrupa grupy G a platí*

$$G/\operatorname{Ker} f \cong G',$$

t.j. faktorová grupa G podľa $\operatorname{Ker} f$ *je izomorfná s G'.*

1.3 Príklady

Azda by nebolo zle začať príkladmi, kde máme iba konečne veľa tried. V takomto prípade sa dá vyplniť celá tabuľka a úloha je pomerne jednoduchá.

Úloha 1. *Nech $G = (\mathbb{Z}, +)$, $H = 5\mathbb{Z} = \{5z; z \in \mathbb{Z}\}$. Ukážte, že faktorová grupa G/H je izomorfná s grupou $(\mathbb{Z}_5, +)$.*

[1] Ak by sme označovali operáciu ako $\cdot$, tak by sme tú istú podmienku zapísali ako $xy^{-1} \in H$.

[2] Tento predpoklad je tu iba preto, aby vôbec malo zmysel hovoriť o faktorovej grupe. Ak sa neskôr budete učiť o normálnych podgrupách, tak zistíte, že faktorové grupy sa dajú robiť aj pre nekomutatívne grupy. Vtedy to však nebude fungovať s ľubovoľnou podgrupou. Prinajmenšom matici by sa s tým mali stretnúť na predmete Algebra v druhom ročníku.

Riešenie. Triedy rozkladu sú v tomto prípade

$$\begin{aligned} H &= \{5z; z \in \mathbb{Z}\} = \{0, \pm 5, \pm 10, \dots\} \\ 1 + H &= \{5z + 1; z \in \mathbb{Z}\} = \{\dots, -9, -4, 1, 6, 11, \dots\} \\ 2 + H &= \{5z + 2; z \in \mathbb{Z}\} = \{\dots, -8, -3, 2, 7, 12, \dots\} \\ 3 + H &= \{5z + 3; z \in \mathbb{Z}\} = \{\dots, -7, -2, 3, 8, 13, \dots\} \\ 4 + H &= \{5z + 4; z \in \mathbb{Z}\} = \{\dots, -6, -1, 4, 9, 14, \dots\} \end{aligned}$$

Keďže máme konečne veľa tried, vieme vyplniť celú tabuľku binárnej operácie. Po porovnaní s tabuľkou grupy $\mathbb{Z}_5$ vidíme, že sú to izomorfné grupy.

$+$	$0+H$	$1+H$	$2+H$	$3+H$	$4+H$
$0+H$	$0+H$	$1+H$	$2+H$	$3+H$	$4+H$
$1+H$	$1+H$	$2+H$	$3+H$	$4+H$	$0+H$
$2+H$	$2+H$	$3+H$	$4+H$	$0+H$	$1+H$
$3+H$	$3+H$	$4+H$	$0+H$	$1+H$	$2+H$
$4+H$	$4+H$	$0+H$	$1+H$	$2+H$	$3+H$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

□

Úloha 2. *Nech $G = (\mathbb{R}^*, \cdot)$ a $H = \mathbb{R}^+ = \{x \in \mathbb{R}; x > 0\}$. Ukážte, že faktorová grupa G/H je izomorfná s grupou $(\mathbb{Z}_2, +)$.*

Riešenie. V tomto prípade máme iba dve triedy rozkladu $\mathbb{R}^+ = \{x \in \mathbb{R}; x > 0\}$ a $\mathbb{R}^- = \{x \in \mathbb{R}; x < 0\}$. Teda faktorová grupa G/H je dvojprvková, každá dvojprvková grupa je izomorfná so $(\mathbb{Z}_2, +)$. □

Úloha 3. *Nech $G = (\mathbb{Z} \times \mathbb{Z}, +)$ a $H = \mathbb{Z} \times 2\mathbb{Z}$. Ukážte, že $G/H \cong \mathbb{Z}_2$.*

Riešenie. Aj v tomto prípade si stačí uvedomiť, že máme iba dve triedy rozkladu, konkrétne

$$\begin{aligned} H &= \mathbb{Z} \times 2\mathbb{Z} \\ (0,1) + H &= (0,1) + \mathbb{Z} \times 2\mathbb{Z} = \mathbb{Z} \times (2\mathbb{Z} + 1) \end{aligned}$$

□

Takéto úlohy sú teda pomerne jednoduché a videli ste úlohu takéhoto typu na cviku aj na prednáške. Postup je zhruba taký, že vyplním tabuľky oboch grúp a porovnám ich. (Aj keď možno nezaškodí aj na týchto jednoduchých príkladoch vyskúšať, či nevieme napísať aj riešenie pomocou vety o izomorfizme. Skúste si rozmyslieť, čo by bol vhodný izomorfizmus v predchádzajúcich úlohách.)

Azda sú zaujímavejšie príklady, kde je faktorová grupa nekonečná – a teda úplne presne rovnaký argument nemôžeme použiť.

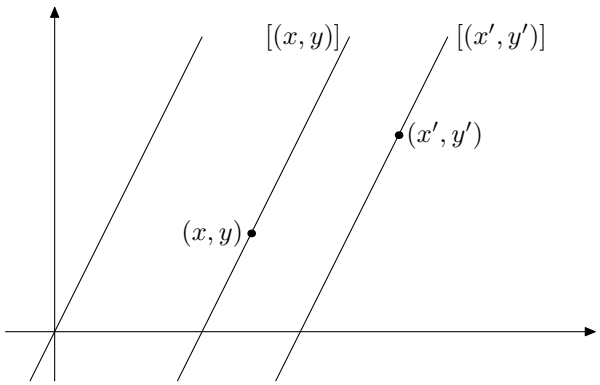
Úloha 4. *Ukážte, že faktorová grupa grupy $G = (\mathbb{R}, +)$ podľa podgrupy $H = \{(t, 2t); t \in \mathbb{R}\}$ je izomorfná s grupou $(\mathbb{R}, +)$.*

Riešenie pomocou definície faktorovej grupy. Overiť, že H je skutočne podgrupa je jednoduché. Stačí si uvedomiť, že $(0,0) \in H$, a teda $H \neq \emptyset$. Súčasne ak $a = (t, 2t)$ a $b = (s, 2s)$ patria do H, tak aj $a - b = (t - s, 2(t - s))$ patrí do H. Má teda zmysel hovoriť o faktorovej grupe – o nej by sme chceli povedať ako vyzerá.

Začnime tým, že si uvedomíme, ako vyzerajú jednotlivé triedy. Trieda prvku (x, y) obsahuje všetky prvky, ktoré dostaneme ako súčet dvojice (x, y) s niektorým prvkom z H. Teda obsahuje práve prvky tvaru $(x, y) + (t, 2t)$.

$$[(x, y)] = \{(x + t, y + 2t); t \in \mathbb{R}\}$$

Vidíme, že trieda $[(x, y)]$ je priamka určená bodom (x, y) a smerovým vektorom $(1, 2)$.



Obr. 1: Triedy sú rovnobežné priamky

Jednotlivé triedy sú teda rovnobežné priamky.

Vieme, že platí

$$G/H = \{[(x, y)]; (x, y) \in \mathbb{R}^2\}.$$

Teda G/H pozostáva zo všetkých priamok rovnobežných z H. Všimnime si, pri zápise, ktorý sme uviedli máme každú triedu zapísanú nekonečne veľakrát. (Každá trieda je niektorá z rovnobežných priamok. My sme do množiny G/H dali túto priamku pre každý bod, ktorý na nej leží.) Takýto zápis je úplne v poriadku. Aby sme však grupe G/H lepšie rozumeli, viac by sa nám ju hodilo popísať tak, aby sme mali zapísanú každú triedu práve raz. Inak povedané, z každej triedy by sme chceli vybrať práve jedného reprezentanta. Z obrázku sa zdá, že vhodným kandidátom by mohol byť priesečník s x-ovou osou - takýto bod leží na každej z rovnobežných priamok. Poďme sa pokúsiť overiť, že to je skutočne tak.

Tvrdíme, že každá trieda obsahuje práve jeden prvok tvaru $(x, 0)$.

Najprv ukážme, že každá trieda obsahuje *aspoň jeden* takýto prvok. Ak máme triedu $[(x, y)]$, tak aj bod $(x - \frac{y}{2}, 0)$ patrí do tej istej triedy, lebo

$$(x, y) - (x - \frac{y}{2}, 0) = (\frac{y}{2}, y) \in H.$$

(Prečo sa nám hodilo voliť práve tento bod? Mohli by sme sa k nemu dopracovať napríklad tak, že sa pýtame, ktorý bod tvaru $(x + t, y + 2t)$ má na druhej súradnici nulu. Dostávame $y + 2t = 0$ a $t = -\frac{y}{2}$.)

Súčasne nemôže nejaká trieda obsahovať *dva rôzne* prvky tohoto tvaru. Skutočne, ak by $(x, 0)$ aj $(x', 0)$ ležali v tej istej triede, tak dostaneme $(x, 0) \sim (x', 0)$, čo znamená, že $(x' - x, 0) \in H$. Lenže ak $(x' - x, 0) = (t, 2t)$ môže nastať iba pre $t = 0$. To znamená, že $(x' - x, 0) = (0, 0)$, a teda aj $x' - x = 0$ a $x = x'$.

Môžeme teda teraz písať

$$G/H = \{[(x, y)]; x \in \mathbb{R}\}.$$

Navyše teraz už vieme, že tento „zoznam“ už obsahuje každú z tried práve raz.

Inak povedané, zobrazenie

$$f\colon x \mapsto [x, 0]$$

je bijekcia z $\mathbb{R}$ do G/H. (Každému $x \in \mathbb{R}$ sme priradili práve jednu triedu.)

Táto bijekcia je však dokonca *homomorfizmus* medzi grupami $(\mathbb{R}, +)$ a $(G/H, +)$, čo môžeme overiť priamo z definície:

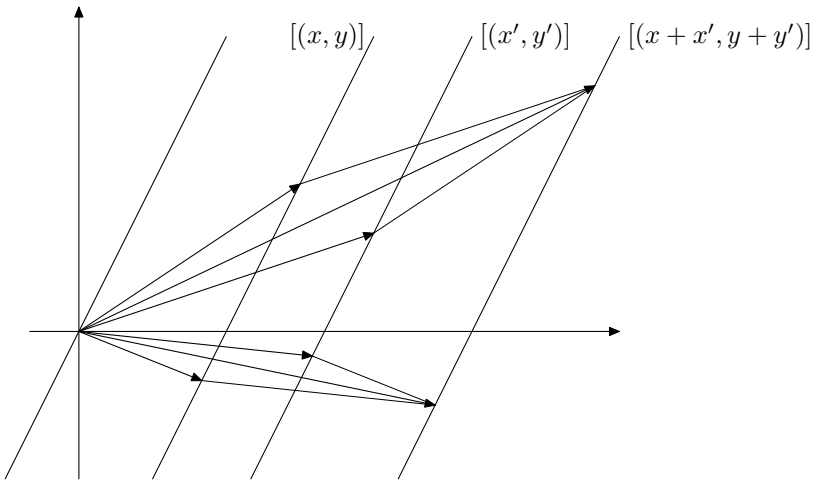
$$f(x) + f(y) = [(x, 0)] + [(y, 0)] = [(x + y, 0)] = f(x + y).$$

(Mali sme teda šťastie, že sme si vhodne zvolili f. Na druhej strane, takáto voľba bijekcie sa zdá byť vcelku prirodzená.)

Našli sme teda izomorfizmus (bijektívny homomorfizmus) medzi $(\mathbb{R}, +)$ a $(G/H, +)$. Tým sme ukázali, že tieto grupy sú skutočne izomorfné. □

Na tomto príklade sa dá celkom dobre ukázať ako funguje binárna operácia, ktorú definujeme na faktorovej grupe. Tu totiž vlastne pracujeme s vektormi v rovine a ich sčitovanie si vieme vcelku dobre predstaviť. (A možno to pomôže aj porozomeniu, prečo je faktorová grupa v tomto prípade naozaj „v podstate rovnaká“ ako grupa reálnych čísel s operáciou sčitovania.)

Všimnime si (obrázok 2), že ak vyberieme ktorýkoľvek vektor z triedy $[(x, y)]$ a ktorýkoľvek vektor z $[(x', y')]$, tak ich súčet vždy padne do tej istej triedy. Je to presne trieda, ktorú potom označujeme $[(x + x', y + y')]$. Presne táto podmienka hovorí, že operácia $+$ na množine tried ekvivalencie je *dobre definovaná*.



Obr. 2: Sčitovanie v G/H

Pokúsme sa vyriešiť tú istú úlohu cez vetu o faktorovom izomorfizme.

Ak ju chceme použiť pre zadané G a H, tak by sme potrebovali surjektívny homomorfizmus f z $(\mathbb{R}^2, +)$ do $(\mathbb{R}, +)$ taký, že jeho jadro, t.j. množina

$$\operatorname{Ker} f = \{(x, y) \in \mathbb{R}^2; f(x, y) = 0\}$$

je rovná práve podgrupe H.

Podgrupa H je určená priamkou $x = t$, $y = 2t$, ktorej všeobecná rovnica je $2x - y = 0$. Teda

$$H = \{(x, y) \in \mathbb{R}^2; 2x - y = 0\}.$$

(Skúste sa detailne presvedčiť, že skutočne platí rovnosť množín $\{(x,y) \in \mathbb{R}^2; 2x - y = 0\} = \{(t, 2t); t \in \mathbb{R}\}$.)

Teda $(x,y) \mapsto 2x - y$ je zobrazenie, pre ktoré je vzor nuly presne množina H. Ak by to náhodou bol aj surjektívny homomorfizmus, tak by sme mali všetko, čo potrebujeme.

Riešenie pomocou vety o izomorfizme. Definujme zobrazenie $f\colon (\mathbb{R}^2, +) \to (\mathbb{R}, +)$ predpisom

$$f(x,y) = 2x - y.$$

Zobrazenie f je grupový homomorfizmus. Skutočne platí

$$f(x,y)+f(x',y') = (2x-y)+(2x'-y') = 2(x+x')-(y+y') = f(x+x', y+y') = f((x,x')+(y,y')).$$

Zobrazenie f je surjektívne. Chceme overiť, či každé $x \in \mathbb{R}$ má v zobrazení f aspoň jeden vzor. Stačí si všimnúť, že pre ľubovoľné $x \in R$ platí

$$f(x/2, 0) = x.$$

Jadro tohoto homomorfizmu je podgrupa H. Priamo z definície jadra máme

$$\operatorname{Ker} f = \{(x,y) \in \mathbb{R}^2; f(x,y) = 0\} = \{(x,y) \in \mathbb{R}^2; 2x - y = 0\} = H.$$

Overili sme, že f spĺňa predpoklady vety o izomorfizme. Na jej základe potom dostávame

$$G/H = G/\operatorname{Ker} f \cong (\mathbb{R}, +).$$

□

Azda na tomto príklade vidno, že homomorfizmus použitý v druhom dôkaze úzko súvisí s tým ako sme vyberali v prvom dôkaze reprezentantov tried (obrázok 3). Skúste si premyslieť, že druhý dôkaz by fungoval takmer rovnako, keby sme použili

$$f(x,y) = x - \frac{y}{2}.$$

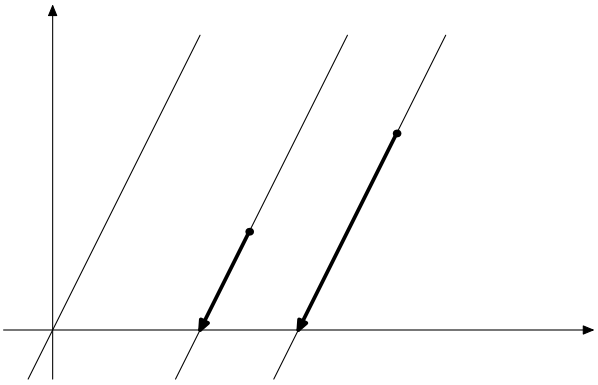
To je presne x-ová súradnica bodu, ktorý je priesečníkom priamky určenej bodom (x,y) s vodorovnou osou – teda bodu, ktorý sme vyberali ako reprezentanta v prvom dôkaze.

Takže vidíme, že úvahami, ktoré sme robili v prvom dôkaze, by sme mohli prísť aj na vhodnú formu homomorfizmu, na ktorý sa dá aplikovať veta o izomorfizme.

Myslím si, že pozrieť sa na takýto konkrétny príklad – kde si všetky veci vieme pomerne dobre predstaviť – by možno mohol pomôcť vniesť trochu svetla aj do dôkazu vety o izomorfizme (ak sú s ním problémy).

Azda vidno, že dôkaz pomocou vety o izomorfizme je o čosi stručnejší a prehľadnejší. Je však náročnejší v tom, že musíme vymyslieť vhodný homomorfizmus. Oba prístupy sa v podstate dajú kombinovať. Mohli by sme úvahami z prvého dôkazu prísť na to, aký homomorfizmus by sa nám hodil. Ale samotný dôkaz už potom môžeme zapísať pomocou vety o izomorfizme - tak sa dá zapísať azda o čosi jednoduchšie; stačí napísať definíciu homomorfizmu, ktorý chceme použiť, a overiť, že spĺňa všetky potrebné podmienky.

Úloha 5. *Nech $G = (\mathbb{C}^*, \cdot)$ a $H = \mathbb{R}^+$. Ukážte, že H je podgrupa G.*
Nech $S = \{c \in \mathbb{C}; |c| = 1\}$. Ukážte, že $(S, \cdot)$ je grupa.
Ukážte tiež, že $G/H \cong S$.
(*Symbol $\cdot$ označuje obvyklé násobenie komplexných čísel.*)



Obr. 3: Homomorfizmus, ktorý sme použili v dôkaze

Riešenie častí, ktoré sa netýkajú faktorizácie. H je podgrupa. Pretože $1 \in H$, vidíme, že $H \neq \emptyset$.

Ak x a y sú kladné reálne čísla, tak aj $\frac{x}{y}$ je kladné reálne číslo. Tým sme overili kritérium podgrupy.

$(S, \cdot)$ je grupa. Ide o podmnožinu $(\mathbb{C}^*, \cdot)$ s rovnakou operáciou. Stačí teda skontrolovať, či je to podgrupa.

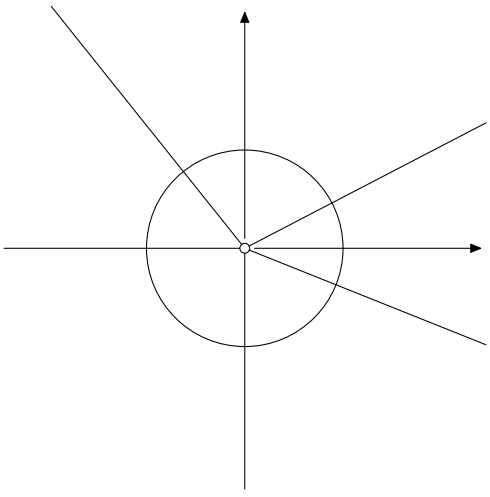
Máme $1 \in S$, a teda $S \neq \emptyset$.

Ak $x, y \in S$, znamená to, že $|x| = |y| = 1$. Potom aj $|xy| = |x| \cdot |y| = 1$, a teda $xy \in S$.

Ak $x \in S$, tak máme $\left|\frac{1}{x}\right| = \frac{1}{|x|} = 1$, teda aj $x^{-1} = \frac{1}{x} \in S$. □

Riešenie pomocou definície faktorovej grupy. Opäť začnime tým, že si rozmyslíme, ako vyzerajú jednotlivé triedy.

Dve komplexné čísla x, y patria do tej istej triedy práve vtedy, keď $\frac{x}{y} = xy^{-1} \in \mathbb{R}^+$. Čiže vtedy a len vtedy, ak $x = yr$ pre nejaké kladné reálne číslo r. Kladné násobky komplexného čísla nám vytvoria v komplexnej rovine polpriamku prechádzajúcu cez toto číslo.



Obr. 4: Triedy rozkladu sú polpriamky

Vidíme, že triedy sú polpriamky vychádzajúce z nuly (obrázok 4).

Opäť by sme chceli nájsť pre každú triedu jedného reprezentanta. Každá takáto polpriamka pretína jednotkovú kružnicu práve v jednom bode. Teda body na jednotkovej kružnici sa zdajú byť vhodnými kandidátmi na reprezentantov. Poďme sa presvedčiť, či to tak skutočne je. (Či sme sa nenakreslili zlý obrázok, alebo či nás neoklamala naša geometrická predstava.)

Tvrdíme teda, že každá trieda $[x]$ obsahuje práve jeden prvok y taký, že $|y| = 1$.

Ak si vezmeme triedu $[x]$, tak číslo

$$y = \frac{x}{|x|}$$

patrí do tej istej triedy. (Dostali sme ho z x vynásobením kladným reálnym číslom $\frac{1}{|x|}$.) Navyše pre toto číslo platí

$$|y| = \left|\frac{x}{|x|}\right| = \frac{|x|}{|x|} = 1,$$

a teda $y \in S$; je to bod na jednotkovej kružnici. (Voľbu y nebolo ťažké uhádnuť, stačilo si rozmyslieť akým číslom treba prenásobiť x, aby výsledok mal absolútnu hodnotu 1.)

Ešte sa pýtame, či v tej istej triede nemôžu byť dve rôzne čísla $y_{1,2}$ také, že $|y_1| = |y_2| = 1$. Ak však platí $y_2 = ry_1$, tak máme aj $|y_2| = |r| \cdot |y_1|$, čo znamená $|r| = 1$. (Tu využívame fakt, že $y_{1,2} \neq 0$.) To však pre $r \in \mathbb{R}^+$ môže nastať iba ak $r = 1$. Lenže v takom prípade $y_2 = 1 \cdot y_1 = y_1$.

Zistili sme teda, že

$$G/H = \{[x]; x \in S\}$$

a navyše funkcia $f\colon S \to G/H$ definovaná predpisom

$$f(x) = [x]$$

je bijekcia. (Každá trieda má práve jedného reprezentanta patriaceho do S.)

Stačí nám už len ukázať, že to je aj izomorfizmus. To je však vcelku priamočiare:

$$f(x \cdot y) = [x \cdot y] = [x] \cdot [y] = f(x) \cdot f(y).$$

□

Poďme sa pozrieť na riešenie pomocou vety o izomorfizme. Už nechám na vás rozmyslieť si, ako v tomto prípade prísť na to, ako by mohol vyzerať vhodný homomorfizmus. (Buď môžete začať rozmýšľať tak, že si uvedomíte, aké má byť jadro a odkiaľ kam má ísť hľadaný homomorfizmus. Alebo sa môžete jednoducho pozrieť na to, čo sme si rozmysleli v predošlom riešení.)

Riešenie pomocou vety o izomorfizme. Definujme $f\colon \mathbb{C}^* \to S$ predpisom

$$f(x) = \frac{x}{|x|}.$$

Všimnime si, že je to skutočne zobrazenie z $\mathbb{C}^*$ do S. Je definované pre každé nenulové komplexné číslo (nemáme nulu v menovateli). A výsledok, je číslo, ktorého absolútna hodnota je rovná jednej:

$$\left|\frac{x}{|x|}\right| = \frac{|x|}{|x|} = 1.$$

Toto zobrazenie je aj *homomorfizmus*:

$$f(x \cdot y) = \frac{x \cdot y}{|x \cdot y|} = \frac{x \cdot y}{|x| \cdot |y|} = \frac{x}{|x|} \cdot \frac{y}{|y|} = f(x) \cdot f(y).$$

Tento homomorfizmus je *surjektívny*; pre číslo $x \in S$ máme

$$f(x) = \frac{x}{|x|} = \frac{x}{1} = x.$$

Teda každé číslo z jednotkovej kružnice má aspoň jeden vzor (konkrétne samého seba).

Jadro tohoto homomorfizmu je množina tých komplexných čísel pre ktoré platí

$$\frac{x}{|x|} = 1.$$

To je ekvivalentné s podmienkou, že $x = |x|$, čo ale nastane práve vtedy, keď x je nezáporné reálne číslo. Nula však nie je v definičnom obore nášho zobrazenia, teda v jadre budú práve kladné reálne čísla:

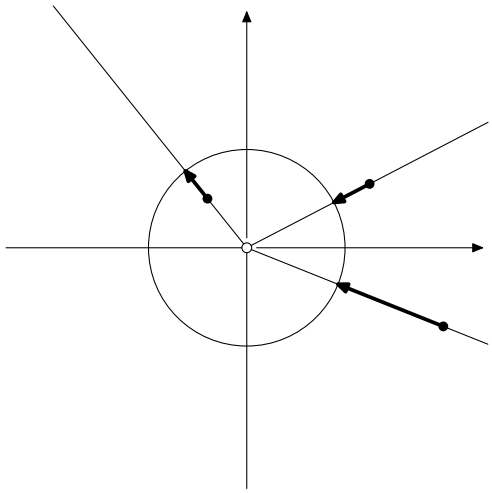
$$\operatorname{Ker} f = \mathbb{R}^+ = H.$$

Zistili sme, že

$$\mathbb{C}^*/\mathbb{R}^+ \cong S.$$

□

Aj v tomto prípade vidno, ako súvisí homomorfizmus použitý v druhom dôkaze s výberom reprezentantov tried (obrázok 5).



Obr. 5: Homomorfizmus, ktorý sme použili v dôkaze