1. Mellékosztály, Lagrange tétele

1.1. Definíció. *Legyen $(G, \cdot)$ csoport, $H \leq G$ részcsoport és $g \in G$ tetszőleges elem. Ekkor a $\{gh|h \in H\}$ halmazt a H* részcsoport g elem szerinti baloldali mellékosztályának *nevezzük és gH-val jelöljük. A g elemet a gH mellékosztály* reprezentánsának *nevezzük. (A $Hg = \{hg|h \in H\}$* jobboldali mellékosztály *definíciója teljesen hasonló.)*

A mellékosztály fogalma tehát nem mást jelent, mint hogy egy részcsoport minden elemét megszorozzuk (balról, vagy jobbról) ugyanazzal a rögzített csoportelemmel (a reprezentánssal) és a kapott elemek halmazát képezzük.

Példák:

1. Legyen G a síkvektorok csoportja a vektorok összeadásával és legyen H az x-tengelyre eső (vagyis $(x, 0)$ alakú) vektorok részcsoportja. Ha most például $g = (2, 2)$, akkor a $(2, 2) + H$ mellékosztály nyilván az $y = 2$ egyenesre eső (vagyis az $(x, 2)$ alakú) vektorok halmaza. Hasonlóan, a $(4, 5)+H$ mellékosztály az $y = 5$ egyenes vektoraiból áll, de nyilván ugyanezt kapjuk akkor is, ha a $(-2, 5) + H$ mellékosztályt képezzük. Általában, a H szerinti (akár bal-, akár jobboldali) mellékosztályok az x-tengellyel párhuzamos egyenesek.

2. Legyen $G = D_3$ a szabályos háromszög szimmetriacsoportja és H álljon az I identitásból, az f_{120} $120°$-os, és az f_{240} $240°$-os forgatásból. Ekkor könnyen ellenőrizhető, hogy $I \cdot H = f_{120} \cdot H = f_{240} \cdot H = H$, míg $t_1 \cdot H = t_2 \cdot H = t_3 \cdot H = \{t_1, t_2, t_3\}$ (ahol t_1, t_2 és t_3 a három tükrözést jelöli).

3. Legyen most G az $n \times n$-es, nemnulla determinánsú mátrixok csoportja a mátrixszorzással és H álljon az 1 determinánsú mátrixokból. Érdemes végiggondolni, hogy ha most $A \in G$ tetszőleges mátrix, akkor az $A \cdot H$ baloldali mellékosztály (és a $H \cdot A$ jobboldali mellékosztály is) éppen a $\det A$ determinánsú mátrixokból áll. (Ez a determinánsok szorzástételéből következik).

A fenti példákon is megfigyelhető a mellékosztályok néhány nagyon alapvető tulajdonsága: bármely két H szerinti mellékosztály vagy teljesen diszjunkt, vagy egybeesik. Más szóval, a mellékosztályok felvágják G-t diszjunkt részekre és ráadásul ha H véges, akkor minden ilyen rész mérete ugyanakkora. Ezeket a tulajdonságokat fogalmazza meg az alábbi tétel:

Összeállította: Szeszlér Dávid

1.2. Tétel. *Legyen $(G, \cdot)$ csoport és $H \leq G$ részcsoport. Ekkor teljesülnek az alábbiak:*

(1) $g \in gH$ minden $g \in G$-re;

(2) ha $g_1, g_2 \in G$ és $g_1H \cap g_2H \neq \emptyset$, akkor $g_1H = g_2H$;

(3) ha $|H|$ véges, akkor $|H| = |gH|$ minden $g \in G$-re.

Bizonyítás: Mivel H részcsoport, ezért $e \in H$ (ahol e jelöli G egységelemét). Ezért a mellékosztály definíciója szerint $g = g \cdot e \in gH$, amivel *(1)*-et beláttuk.

(2) igazolásához tegyük fel, hogy $a \in g_1H \cap g_2H$. Be fogjuk látni, hogy tetszőleges $b \in g_1H$ esetén $b \in g_2H$ is teljesül, vagyis $g_1H \subseteq g_2H$. Mivel a fordított irányú tartalmazás nyilván ugyanígy belátható, *(2)* ebből már következni fog. Definíció szerint $a \in g_1H \cap g_2H$ azt jelenti, hogy a felírható $a = g_1h_1$ és $a = g_2h_2$ alakban is, ahol $h_1, h_2 \in H$. A $g_1h_1 = g_2h_2$ egyenletet jobbról h_1^{-1}-zel szorozva kapjuk: $g_1 = g_2h_2h_1^{-1}$.

Ha most $b \in g_1H$ tetszőleges, akkor $b = g_1h_3$ valamilyen $h_3 \in H$-ra. Ebbe beírva az előző bekezdés végén kapott alakot: $b = g_1h_3 = g_2h_2h_1^{-1}h_3$. Mivel H részcsoport, ezért $h_2h_1^{-1}h_3 \in H$ teljesül (hiszen minden részcsoport zárt a csoport műveletére és az inverz képzésre). Ez pedig éppen azt jelenti, hogy $b \in g_2H$, így *(2)*-t beláttuk.

Ha $H = \{h_1, h_2, \ldots, h_k\}$, akkor $gH = \{gh_1, gh_2, \ldots, gh_k\}$, ezért nyilván csak azt kell megmutatni, hogy a gh_i elemek mind különbözők. Ez viszont könnyen látható: ha $gh_i = gh_j$ teljesül valamilyen $1 \leq i, j \leq k$-ra, akkor mindkét oldalt balról g^{-1}-zel szorozva $h_i = h_j$ adódik. Ezzel *(3)*-at is beláttuk. □

A fenti tétel egyik érdekes következménye, hogy egy mellékosztály reprezentánsai ugyanazok, mint a mellékosztály elemei. Ugyanis ha X valamelyik (H szerinti, baloldali) mellékosztály és $g \in X$, akkor X-nek és gH-nak van közös eleme (nevezetesen: g), így a *(2)*-es tulajdonság szerint $X = gH$. Más szóval: a mellékosztály tetszőleges eleme egyben reprezentánsa is. Ennek fordítottját pedig (vagyis hogy a reprezentáns eleme is a mellékosztálynak) az *(1)*-es tulajdonság fejezi ki.

Hangsúlyozzuk, hogy a mellékosztály (általában) nem részcsoport (noha a csoport elemeinek egy részhalmaza). Természetesen a H részcsoport maga is H szerinti mellékosztály (hiszen például $H = e \cdot H$), de az összes többi H szerinti mellékosztály nem részcsoport (hiszen például az egységelemet sem tartalmazza).

A fenti tétel állításai baloldali mellékosztályokról szólnak, de nyilván mindegyik állítás megfelelője érvényes jobboldali mellékosztályokra is. A tétel egyszerű, de alapvető fontosságú következménye az alábbi tétel:

1.3. Tétel. [Lagrange tétele]

Legyen G véges csoport, $H \leq G$ részcsoport. Ekkor $|H| \;\Big|\; |G|$. (Szavakban: véges csoport részcsoportjának rendje mindig osztja a csoport rendjét.)

Bizonyítás: A fenti tétel szerint a H szerinti mellékosztályok $|H|$ méretű diszjunkt részekre vágják a G csoportot. Ez nyilván csak akkor lehetséges, ha $|H| \;\Big|\; |G|$. □

A $|G|/|H|$ számot a H részcsoport *indexének* szokták nevezni és $|G : H|$-val jelölik. A Lagrange-tétel egyszerű és fontos következménye az elem rendje és a csoport rendje közötti kapcsolat:

1.4. Következmény. *Legyen G véges csoport és $g \in G$. Ekkor $o(g) \;\Big|\; |G|$. (Szavakban: véges csoport elemének rendje mindig osztja a csoport rendjét.)*

Bizonyítás: Legyen $o(g) = k$ és $H = \{g, g^2, \ldots, g^{k-1}, g^k = e\}$. A felsorolt elemek mind különbözők – ez korábban kiderült annak bizonyítása során, hogy véges csoportban az elemrend is mindig véges. Belátjuk, hogy $H \leq G$, ekkor Lagrange tétele szerint készen leszünk, hiszen $|H| = o(g) = k$.

H zárt a csoport műveletére nézve: ha $g^i, g^j \in H$, akkor $g^i \cdot g^j = g^{i+j}$. Ha most $i + j \leq k$, akkor $g^{i+j} \in H$ nyilvánvaló; egyébként pedig $g^{i+j} = g^{i+j-k} \cdot g^k = g^{i+j-k} \cdot e = g^{i+j-k} \in H$. H zárt az inverz képzésre is: $(g^i)^{-1} = g^{k-i}$, mert $g^i \cdot g^{k-i} = g^k = e$. Így H valóban részcsoport. □

2. Normálosztó, faktorcsoport

A csoportelmélet célja az, hogy valamilyen átfogó tételt tudjon mondani az összes (véges) csoport szerkezetéről. Egy ilyen tételnek számos alkalmazása van a matematikán belül és kívül is. Az eljárás távolról hasonlít az egész számok vizsgálatához, ahol a számelmélet alaptétele egy hasonló, átfogó tétel. Ennek alapgondolata az, hogy ha egy egész számnak megtaláljuk egy osztóját, akkor az osztó és a hányados ismerete sokat elárul az eredeti számról is. Ha a szorzattá alakítást tovább folytatjuk amíg csak lehet, eljutunk a szám prímtényezős felbontásához. A csoportok esetében is hasonló a helyzet: értelmezni fogjuk a *normálosztó* fogalmát, amivel egy csoportot „el lehet osztani”, a hányadosnak megfelelő fogalom pedig a *faktorcsoport* lesz. Ezen a ponton mi megállunk majd ugyan, de érdemes tudni, hogy az út tovább vezet: értelmezni lehet a prímszámnak megfelelő fogalmat (az úgynevezett *egyszerű csoportot*) és be lehet bizonyítani egy tételt csoportokkal kapcsolatban, ami valóban emlékeztet a számelmélet alaptételére (noha jóval bonyolultabb annál).

2.1. Definíció. *Legyen G csoport és $N \leq G$ részcsoport. N-et* normálosztónak *(vagy* normális részcsoportnak*) nevezzük, ha $gN = Ng$ teljesül minden $g \in G$-re. Ennek jele: $N \triangleleft G$.*

A definíciónak fontos eleme, hogy N részcsoport, tehát a normálosztó egy speciális részcsoport. Fontos megjegyezni azt is, hogy a definíció minden $g \in G$-re két halmaz (gN és Ng) egyenlőségét mondja ki. Ez tehát *nem jelenti azt*, hogy $gn = ng$ teljesülne minden $n \in N$-re, csak azt, hogy a gn elemek halmaza és az ng elemek halmaza megegyezik, ha n végigfut N-en.

Példák:

1. Legyen G a síkvektorok csoportja a vektorok összeadásával és legyen H az x-tengelyre eső vektorok részcsoportja. Ekkor bármely $g = (u, v)$ vektorra $(u, v) + H$ és $H + (u, v)$ is az $y = v$ egyenes, így $(u, v) + H = H + (u, v)$. Ezért H normálosztó. Nyilván általában is igaz, hogy Abel-csoportban minden részcsoport egyben normálosztó is.

2. Legyen $G = D_3$ és $H = \{I, f_{120}, f_{240}\}$. Érdemes kipróbálni, hogy ha t_i a háromszög valamelyik tükrözése, akkor $t_i f_{120} = f_{240} t_i$ és $t_i f_{240} = f_{120} t_i$. Ezért $t_i H = H t_i$ teljesül (mindkét oldal a három tükrözésből áll). Ha most f_i valamelyik forgatás (vagy az identitás), akkor is teljesül $f_i H = H f_i$ (mindkét oldal egyenlő H-val). Ezért $H \triangleleft G$. (Általában is könnyű belátni, hogy 2 indexű, vagyis az elemek felét tartalmazó részcsoport mindig normálosztó.)

3. Legyen G az $n \times n$-es, nemnulla determinánsú mátrixok csoportja a mátrixszorzással és H álljon az 1 determinánsú mátrixokból. Említettük, hogy minden $A \in G$-re $A \cdot H$ és $H \cdot A$ is a $\det A$ determinánsú mátrixokból áll, így $H \triangleleft G$.

4. Legyen ismét $G = D_3$, de most legyen $H = \{I, t_1\}$ (ez valóban részcsoport). Érdemes végiggondolni, hogy most $f_{120} H = \{f_{120}, t_3\}$, de $H f_{120} = \{f_{120}, t_2\}$ (ha a tükrözéseket a csúcsok óramutató járásával ellenkező sorrendje szerint számozzuk). Ezért H *nem* normálosztó.

A normálosztó definíciójának számos átfogalmazása van, ezek közül szükségünk lesz az alábbira:

2.2. Állítás. *Legyen $N \leq G$ részcsoport. Ekkor*
$N \triangleleft G \quad \iff \quad g^{-1}ng \in N$ *teljesül minden* $n \in N$ *és* $g \in G$ *esetén.*

Bizonyítás:

$\Rightarrow$: Legyen $g \in G$, $n \in N$. Ekkor $ng \in Ng$. Mivel $N \triangleleft G$, ezért $gN = Ng$, így $ng \in gN$ is igaz, vagyis létezik olyan $n' \in N$, hogy $ng = gn'$. Mindkét oldalt balról g^{-1}-zel szorozva: $g^{-1}ng = n'$, így $g^{-1}ng \in N$ valóban teljesül.

$\Leftarrow$: Belátjuk, hogy $Ng \subseteq gN$; a fordított irányú tartalmazás ugyanígy belátható, amiből következik $N \triangleleft G$. Vegyük Ng egy tetszőleges elemét: ng-t ($n \in N$). Azt akarjuk belátni, hogy $ng \in gN$, vagyis hogy van olyan $n' \in N$, amelyre $ng = gn'$. Legyen $n' = g^{-1}ng$, a feltétel szerint $n' \in N$. Ekkor $gn' = gg^{-1}ng = ng$, vagyis $ng \in gN$ valóban teljesül. □

A normálosztó definíciójára azért van szükség, hogy definiálni tudjuk a faktorcsoport fogalmát:

2.3. Definíció. *Legyen $(G, \cdot)$ csoport és $N \triangleleft G$ normálosztó. Ekkor a G/N-nel jelölt* faktorcsoport *elemei az N szerinti mellékosztályok és a faktorcsoport $*$ műveletét az alábbi képlet szerint értelmezzük:*

$$(gN) * (hN) = (gh)N.$$

(Szavakban: a faktorcsoportban a gN és hN mellékosztályok közötti $*$ művelet eredménye a $(gh)N$ mellékosztály.)

A definícióban nem jelöltük meg, hogy G/N elemei a baloldali, vagy a jobboldali mellékosztályok; erre nincs is szükség, hiszen a normálosztó definíciója szerint ezek között nincs különbség.

Természetesen be kell bizonyítani, hogy a faktorcsoport valóban csoport. Ezelőtt azonban egy ennél is alapvetőbb kérdésre kell megnyugtató választ adni: vajon a faktorcsoport művelete értelmesen lett-e definiálva? Ez a következőt jelenti: legyen X és Y két mellékosztály, például $X = g_1N$ és $Y = h_1N$. Láttuk, hogy ugyanannak a mellékosztálynak különböző reprezentánsai is lehetnek: $X = g_2N$ és $Y = h_2N$ előfordulhat $g_1 \neq g_2$, $h_1 \neq h_2$ esetén is. Mi lesz akkor $X * Y$? A fenti definíció szerint mondhatjuk azt is, hogy $X * Y = (g_1h_1)N$, de mondhatjuk azt is, hogy $X * Y = (g_2h_2)N$. Ha most véletlenül $(g_1h_1)N \neq (g_2h_2)N$, akkor ez azt jelenti, hogy a $*$ művelet definíciója értelmetlen, mert az eredmény függ attól, hogy milyen alakban írjuk fel a mellékosztályokat. (Egy közérthetőbb példa talán megvilágítja, hogy mit jelentene a művelet definíciójának értelmetlensége. Az általános iskola hatodik osztályában sok gyerek használja az $\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$ szabályt a törtek összeadására (a szorzás mintájára). Eszerint a szabály szerint $\frac{1}{2} \oplus \frac{2}{3} = \frac{3}{5}$, de $\frac{2}{4} \oplus \frac{6}{9} = \frac{8}{13}$. Ez éppen azt jelenti, hogy a $\oplus$ művelet definíciója értelmetlen, mert a

művelet eredménye függ attól, hogy az $\frac{1}{2}$ és $\frac{2}{3}$ számok melyik alakját választjuk.) Szerencsére a faktorcsoport műveletének definíciója értelmes, ezt mondja ki az alábbi tétel.

2.4. Tétel. *Legyen $N \triangleleft G$ normálosztó és tegyük fel, hogy $g_1N = g_2N$ és $h_1N = h_2N$ valamely $g_1, g_2, h_1, h_2 \in G$ elemekre. Ekkor $(g_1h_1)N = (g_2h_2)N$.*

Bizonyítás: Elég lesz bebizonyítani, hogy a $(g_1h_1)N$ és $(g_2h_2)N$ mellékosztályoknak van közös eleme, hiszen ekkor az 1.2. tétel *(2)*-es állítása szerint egybeesnek. Vegyük $(g_1h_1)N$ egy tetszőleges elemét: g_1h_1n-et ($n \in N$). Készen leszünk, ha belátjuk, hogy $g_1h_1n \in (g_2h_2)N$. Ez azt jelenti, hogy létezik olyan $n^* \in N$, amelyre $g_1h_1n = g_2h_2n^*$. Ezt az egyenletet balról szorozva előbb g_2^{-1}-zel, majd h_2^{-1}-zel: $h_2^{-1}g_2^{-1}g_1h_1n = n^*$. Annyit kell tehát igazolnunk a tétel bizonyításához, hogy $h_2^{-1}g_2^{-1}g_1h_1n \in N$. Ehhez a következő átalakítások vezetnek:

$$h_2^{-1}g_2^{-1}g_1h_1n \overset{(1)}{=} h_2^{-1}g_2^{-1}g_1h_2n' \overset{(2)}{=} h_2^{-1}g_2^{-1}g_1n''h_2 \overset{(3)}{=}$$
$$\overset{(3)}{=} h_2^{-1}g_2^{-1}g_2n'''h_2 = h_2^{-1}n'''h_2 \overset{(4)}{\in} N$$

Itt az egyes lépések helyességét a következő megjegyzések indokolják:

(1): tudjuk, hogy $h_1N = h_2N$, ezért a $h_1n \in h_1N$ elem felírható $h_1n = h_2n'$ alakban is alkalmas $n' \in N$-re.

(2): mivel N normálosztó, ezért $h_2N = Nh_2$; így a $h_2n' \in h_2N$ elem felírható $h_2n' = n''h_2$ alakban is alkalmas $n'' \in N$-re.

(3): $g_1N = g_2N$, ezért $g_1n'' = g_2n'''$ alkalmas $n''' \in N$-re.

(4): N normálosztó, így a 2.2 állítás alkalmazható. □

Hangsúlyozzuk, hogy a fenti bizonyításban erősen kihasználtuk, hogy N normálosztó. Ha N egy tetszőleges részcsoport volna, előfordulhatna, hogy a faktorcsoport műveletének definíciója értelmetlen; valójában a normálosztó definícióját éppen az indokolja, hogy ezzel lehet garantálni a fenti tétel érvényességét. Beláttuk tehát, hogy a faktorcsoport művelete jól definiált, most már azt is igazolhatjuk, hogy a faktorcsoport valóban csoport.

2.5. Állítás. *Legyen G csoport és $N \triangleleft G$ normálosztó. Ekkor G/N csoport.*

Bizonyítás: Ellenőrizzük az asszociativitást: ha gN, hN és kN mellékosztályok, akkor $(gN * hN) * kN = (gh)N * kN = ((gh)k)N$ és $gN * (hN * kN) = gN * (hk)N = (g(hk))N$. Mivel G csoport, ezért $(gh)k = g(hk)$, így a faktorcsoport $*$ művelete valóban asszociatív.

A faktorcsoport egységeleme $N = eN$, hiszen minden gN mellékosztályra $gN * eN = (ge)N = gN$ és $eN * gN = (eg)N = gN$.

Végül minden mellékosztálynak van inverze: a gN mellékosztályé $g^{-1}N$, hiszen $gN * g^{-1}N = (gg^{-1})N = eN = N$ és hasonlóan $g^{-1}N * gN = (g^{-1}g)N = N$. □

Példák:

1. Legyen G a síkvektorok csoportja a vektorok összeadásával és H álljon az x-tengelyre eső vektorokból. Ekkor a G/H faktorcsoport elemei a H-szerinti mellékosztályok, vagyis az x-tengellyel párhuzamos egyenesek. Az $y = a$ egyenes (vagyis a $(0, a) + H$ mellékosztály) és az $y = b$ egyenes (a $(0, b) + H$ mellékosztály) közti $*$ művelet eredménye a faktorcsoportban a $(0, a + b) + H$ mellékosztály, vagyis az $y = a + b$ egyenes. (Ez tehát azt mutatja, hogy G/H izomorf az $(\mathbb{R}, +)$ csoporttal: az izomorfizmus az $y = a$ egyeneshez az a valós számot rendeli.)

2. Legyen $G = D_3$ és $H = \{I, f_{120}, f_{240}\}$. Ekkor G/H-nak két eleme van, a két H szerinti mellékosztály: $\{I, f_{120}, f_{240}\}$ és $\{t_1, t_2, t_3\}$. Ha az elsőt röviden X-szel, a másodikat Y-nal jelöljük, akkor a faktorcsoportban $X * Y = IH * t_1H = (It_1)H = t_1H = Y$ (ami nem meglepő, hiszen $H = X$ mindig a faktorcsoport egységeleme). Hasonlóan, $X * X = X$, $Y * X = Y$ és $Y * Y = X$. (Vagyis G/H izomorf a C_2 ciklikus csoporttal.)

3. Legyen G az $n \times n$-es, nemnulla determinánsú mátrixok csoportja a mátrixszorzással és H álljon az 1 determinánsú mátrixokból. Ekkor G/H elemei a közös (nemnulla) determinánssal rendelkező $n \times n$-es mátrixok halmazai. Ha X az α determinánsú, Y a β determinánsú mátrixok halmaza — azaz $X = AH$ és $Y = BH$, ahol $\det A = \alpha$ és $\det B = \beta$ —, akkor $X * Y = AH * BH = (AB)H$, ami nem más, mint az $\alpha\beta$ determinánsú mátrixok halmaza. (Ezek szerint G/H izomorf a nemnulla valós számok szorzással vett csoportjával: az izomorfizmus az α determinánsú mátrixok halmazához α-t rendeli.)

3. Homomorfizmus

A fenti példákon láthattuk, hogy a faktorcsoport elemeivel való „számolás” időnként kényelmetlen lehet. Az alábbiakban megismerkedünk egy tétellel, amelynek segítségével könnyebben felismerhetjük, hogy a faktorcsoport milyen, korábbról már esetleg ismerős csoporttal izomorf. Ehhez szükségünk lesz az alábbi fogalmakra.

3.1. Definíció. *Legyenek $(G, \cdot)$ és $(H, \circ)$ csoportok. A $\varphi : G \mapsto H$ függvényt* homomorfizmusnak *nevezzük, ha $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$ teljesül minden $a, b \in G$ esetén.*

A homomorfizmus definíciójában szereplő feltétel (a *művelettartás*) már ismerős lehet az izomorfizmus definíciójából. A két fogalom közti különbség az, hogy izomorfizmus esetén megköveteljük a függvény kölcsönösen egyértelműségét, míg homomorfizmus esetén nem. Az izomorfizmus tehát speciális homomorfizmus.

3.2. Definíció. *Legyen $\varphi : G \mapsto H$ homomorfizmus. Ekkor a* homomorfizmus képének *nevezzük és $\mathrm{Im}\,\varphi$-vel jelöljük φ értékkészletét, vagyis az $\mathrm{Im}\,\varphi = \{h \in H | \exists g \in G, \varphi(g) = h\}$ halmazt. A* homomorfizmus magjának *nevezzük és $\mathrm{Ker}\,\varphi$-vel jelöljük G azon elemeinek halmazát, amelyeknek a φ-vel vett képe H egységeleme, vagyis $\mathrm{Ker}\,\varphi = \{g \in G | \varphi(g) = e_H\}$.*

Példák:

1. G legyen a síkvektorok csoportja a vektorok összeadásával és H legyen az $(\mathbb{R}, +)$ csoport (a valós számok összeadással vett csoportja). A $\varphi : G \mapsto H$ homomorfizmus az $(x, y) \in G$ vektorhoz az $y \in \mathbb{R}$ számot rendelje. Ekkor φ valóban homomorfizmus: $\varphi((x_1, y_1) + (x_2, y_2)) = \varphi((x_1 + x_2, y_1 + y_2)) = y_1 + y_2 = \varphi((x_1, y_1)) + \varphi((x_2, y_2))$ A homomorfizmus képe $\mathrm{Im}\,\varphi = H$, hiszen minden valós szám lehet egy síkvektor második koordinátája. A homomorfizmus magja az x-tengely vektoraiból áll: $\mathrm{Ker}\,\varphi = \{(x, 0) | x \in \mathbb{R}\}$, hiszen ezeknek a vektoroknak a képe 0, ami a $H = (\mathbb{R}, +)$ egységeleme.

2. Legyen $G = D_3$ és $H = \{e, h\}$ a két elemű ciklikus csoport. (H-ban tehát $eh = he = h$ és $e^2 = h^2 = e$.) A $\varphi : G \mapsto H$ homomorfizmus a G-beli forgatásokhoz (és az identitáshoz) e-t, a G-beli tükrözésekhez h-t rendelje. Nem nehéz ellenőrizni, hogy φ valóban homomorfizmus. (Ez azon múlik, hogy a forgatások körüljárástartó, a tükrözések körüljárásváltó transzformációk.) Nyilván $\mathrm{Im}\,\varphi = H$ és $\mathrm{Ker}\,\varphi = \{I, f_{120}, f_{240}\}$.

3. Legyen G az $n \times n$-es, nemnulla determinánsú mátrixok csoportja a mátrixszorzással és $H = (\mathbb{R} \setminus \{0\}, \cdot)$ a nemnulla valós számok csoportja a szorzással. $A \in G$ esetén legyen $\varphi(A) = \det A$. A determinánsok szorzástétele éppen azt mondja ki, hogy φ homomorfizmus. Ekkor $\mathrm{Im}\,\varphi = H$ (hiszen minden valós szám lehet egy alkalmas $n \times n$-es mátrix determinánsa) és $\mathrm{Ker}\,\varphi$ az 1 determinánsú mátrixok halmaza (hiszen $(\mathbb{R} \setminus \{0\}, \cdot)$ egységeleme 1).

A fenti példákból is látszik a homomorfizmusok néhány alapvető tulajdonsága, amelyeket az alábbi tételben foglalunk össze:

3.3. Tétel. *Legyen $\varphi : (G, \cdot) \mapsto (H, \circ)$ homomorfizmus. Ekkor*

(1) $\varphi(e_G) = e_H$ (vagyis G egységelemének képe H egységeleme);

(2) $\varphi(g^{-1}) = (\varphi(g))^{-1}$ minden $g \in G$-re;

(3) $\operatorname{Im}\varphi \leq H$ (vagyis $\operatorname{Im}\varphi$ részcsoport H-ban);

(4) $\operatorname{Ker}\varphi \leq G$, sőt: $\operatorname{Ker}\varphi \triangleleft G$ (vagyis $\operatorname{Ker}\varphi$ normálosztó G-ben).

Bizonyítás: (1) Legyen $\varphi(e_G) = h \in H$. A homomorfizmus definíciójából $h = \varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \circ \varphi(e_G) = h \circ h$. A kapott $h = h^2$ egyenlet mindkét oldalát (H-ban) h^{-1}-zel szorozva $e_H = h$ adódik.

(2) A homomorfizmus definíciójából és az *(1)*-es tulajdonságból: $e_H = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g) \circ \varphi(g^{-1})$. Mindkét oldalt balról $(\varphi(g))^{-1}$-zel szorozva: $(\varphi(g))^{-1} = \varphi(g^{-1})$.

(3) $\operatorname{Im}\varphi$ nyilván nem az üres halmaz, mert G elemeinek képét tartalmazza. $\operatorname{Im}\varphi$ zárt a (H-beli) műveletre: ha $h_1, h_2 \in \operatorname{Im}\varphi$, akkor $h_1 = \varphi(g_1)$ és $h_2 = \varphi(g_2)$ valamilyen $g_1, g_2 \in G$ elemekre; ekkor $h_1 \circ h_2 = \varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 g_2) \in \operatorname{Im}\varphi$. Továbbá $\operatorname{Im}\varphi$ zárt a (H-beli) inverz képzésre: ha $h \in \operatorname{Im}\varphi$, akkor $h = \varphi(g)$ alkalmas $g \in G$-re; ekkor a *(2)*-es tulajdonság szerint $h^{-1} = \varphi(g^{-1}) \in \operatorname{Im}\varphi$. Mindezek miatt $\operatorname{Im}\varphi$ valóban részcsoport.

(4) Először belátjuk, hogy $\operatorname{Ker}\varphi \leq G$. Az *(1)*-es tulajdonság szerint $\operatorname{Ker}\varphi$ nem üres, mert $e_G \in \operatorname{Ker}\varphi$. $\operatorname{Ker}\varphi$ zárt a (G-beli) műveletre: ha $g_1, g_2 \in \operatorname{Ker}\varphi$, akkor $\varphi(g_1) = \varphi(g_2) = e_H$; ekkor $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2) = e_H \circ e_H = e_H$, így $g_1 g_2 \in \operatorname{Ker}\varphi$. $\operatorname{Ker}\varphi$ zárt a (G-beli) inverz képzésre: ha $g \in \operatorname{Ker}\varphi$, akkor $\varphi(g) = e_H$; ekkor a *(2)*-es tulajdonság szerint $\varphi(g^{-1}) = (\varphi(g))^{-1} = e_H^{-1} = e_H$, így $\varphi(g^{-1}) \in \operatorname{Ker}\varphi$. Így $\operatorname{Ker}\varphi$ részcsoport, azt kell még belátni, hogy normálosztó is. Legyen $g \in G$ és $n \in \operatorname{Ker}\varphi$; a 2.2. állítás szerint azt kell csak megmutatni, hogy $g^{-1}ng \in \operatorname{Ker}\varphi$, vagyis $\varphi(g^{-1}ng) = e_H$. Ez pedig igaz, mert $\varphi(g^{-1}ng) = \varphi(g^{-1}) \circ \varphi(n) \circ \varphi(g) = \varphi(g^{-1}) \circ e_H \circ \varphi(g) = \varphi(g^{-1}) \circ \varphi(g) = \varphi(g^{-1}g) = \varphi(e_G) = e_H$. □

A homomorfizmus általában nem kölcsönösen egyértelmű függvény, vagyis különböző G-beli elemeknek lehet azonos a képe. Természetes kérdés, hogy mikor lesz két G-beli elem képe azonos, mik az egyetlen H-beli elemmé „összeejtett” G-beli halmazok. A következő tétel állítása szerint ezek éppen a $\operatorname{Ker}\varphi$ szerinti mellékosztályok.

3.4. Tétel. *Legyen $\varphi : (G, \cdot) \mapsto (H, \circ)$ homomorfizmus és legyen $N = \mathit{Ker}\,\varphi$. Ekkor*

$$g_1 N = g_2 N \qquad \Longleftrightarrow \qquad \varphi(g_1) = \varphi(g_2).$$

Bizonyítás:

$\Rightarrow$: Mivel $g_2 \in g_2 N = g_1 N$, ezért $g_2 = g_1 n$ alkalmas $n \in N$-re. Ezért $\varphi(g_2) = \varphi(g_1 n) = \varphi(g_1) \circ \varphi(n) = \varphi(g_1) \circ e_H = \varphi(g_1)$ (ahol $\varphi(n) = e_H$ azért igaz, mert $n \in N = \mathrm{Ker}\,\varphi$).

$\Leftarrow$: Ha $\varphi(g_1) = \varphi(g_2)$, akkor ezt balról $(\varphi(g_2))^{-1}$-zel szorozva: $(\varphi(g_2))^{-1} \circ \varphi(g_1) = e_H$. Ekkor az előző tétel *(2)*-es állítása szerint $e_H = \varphi(g_2^{-1}) \circ \varphi(g_1) = \varphi(g_2^{-1} g_1)$, így $g_2^{-1} g_1 \in N = \mathrm{Ker}\,\varphi$. Ha most $g_2^{-1} g_1 = n \in N$, akkor mindkét oldalt balról g_2-vel szorozva: $g_1 = g_2 n$. Eszerint tehát $g_1 \in g_2 N$. Másrészt $g_1 \in g_1 N$ nyilvánvaló, vagyis a $g_1 N$ és $g_2 N$ mellékosztályoknak van közös eleme (nevezetesen g_1), így az 1.2. tétel *(2)*-es állítása szerint $g_1 N = g_2 N$. □

A tétel azt állítja, hogy két elem képe akkor egyenlő, ha a két elem ugyanazt a mellékosztályt reprezentálja; az 1.2. tétel szerint persze mondhatjuk azt is, hogy a két kép pontosan akkor egyenlő, ha a két elem ugyanahhoz a mellékosztályhoz tartozik. A most bizonyított tétel alapvető fontosságú következménye az alábbi tétel.

3.5. Tétel. [Homomorfizmus tétel]
Legyen $\varphi : (G, \cdot) \mapsto (H, \circ)$ homomorfizmus. Ekkor

$$G/\,\mathit{Ker}\,\varphi \cong \mathit{Im}\,\varphi.$$

A tétel szerint tehát könnyen meg tudjuk mondani, hogy milyen (esetleg már ismert) csoporttal izomorf valamely G/N faktorcsoport, ha az $N \triangleleft G$ normálosztó valamely $\varphi : G \mapsto H$ homomorfizmus magja: a homomorfizmus képével. Azt, hogy a tétel állításának egyáltalán van értelme, a 3.3. tétel állításainak köszönhetjük. A $G/\,\mathrm{Ker}\,\varphi$ faktorcsoport ugyanis csak akkor értelmezett, ha $\mathrm{Ker}\,\varphi$ normálosztó; ezt a *(4)*-es állítás garantálja. Továbbá a faktorcsoport csak akkor lehet izomorf $\mathrm{Im}\,\varphi$-vel, ha $\mathrm{Im}\,\varphi$ maga is csoport; ezt pedig a *(3)*-as állításból tudjuk.

Bizonyítás: Legyen $N = \mathrm{Ker}\,\varphi$. Meg kell adnunk egy $\psi : G/N \mapsto \mathrm{Im}\,\varphi$ izomorfizmust G/N elemei (a mellékosztályok) és $\mathrm{Im}\,\varphi$ elemei között. Ha X az egyik N szerinti mellékosztály, akkor az előző tétel szerint X minden eleméhez φ ugyanazt a H-beli elemet rendeli; természetes gondolat ψ-t úgy definiálni, hogy X-hez ezt a közös H-beli elemet rendelje. Képletben: $\psi(gN) \stackrel{\text{def}}{=} \varphi(g)$. (Hangsúlyozzuk, hogy ψ definíciójának értelmességét az előző tétel garantálja; ha valamely $g_1, g_2 \in G$-re előfordulhatna, hogy $g_1 N = g_2 N$, de $\varphi(g_1) \neq \varphi(g_2)$, akkor a definíció értelmetlen volna.)

Ekkor ψ valóban G/N-ről $\operatorname{Im}\varphi$-be képez (hiszen $\psi(gN) = \varphi(g) \in \operatorname{Im}\varphi$). Azt kell megmutatnunk, hogy ψ izomorfizmus. A művelettartás teljesül ψ-re: ha $g_1N, g_2N \in G/N$, akkor $\psi(g_1N * g_2N) = \psi(g_1g_2N) = \varphi(g_1g_2) = \varphi(g_1) \circ \varphi(g_2) = \psi(g_1N) \circ \psi(g_2N)$ (itt ψ és $*$ definícióján kívül kihasználtuk, hogy φ homomorfizmus). ψ különböző G/N-beli elemekhez különböző $\operatorname{Im}\varphi$-belieket rendel (azaz ψ injektív): ha $g_1N \neq g_2N$, akkor $\psi(g_1N) = \varphi(g_1) \neq \varphi(g_2) = \psi(g_2N)$, ez éppen az előző tétel állítása. ψ minden $\operatorname{Im}\varphi$-beli elemet felvesz értékként (azaz ψ szürjektív): ha $h \in \operatorname{Im}\varphi$, akkor $h = \varphi(g)$ alkalmas $g \in G$-re, így $\psi(gN) = \varphi(g) = h$.

Ezek szerint ψ művelettartó és kölcsönösen egyértelmű, így izomorfizmus. □

Példák:

1. Legyen G a síkvektorok csoportja a vektorok összeadásával, $H = (\mathbb{R}, +)$ és $\varphi((x, y)) = y$. Ekkor a homomorfizmus tétel állítása szerint $G/(\{(x, 0)|x \in \mathbb{R}\}) \cong (\mathbb{R}, +)$, ahogy azt már korábban is láttuk.

2. Legyen $G = D_3$, $C_2 = H = \{e, h\}$ a két elemű ciklikus csoport és φ a forgatásokhoz e-t, a tükrözésekhez h-t rendelje. Ekkor a homomorfizmus tétel szerint $D_3/(\{I, f_{120}, f_{240}\}) \cong C_2$, a korábbi állításunknak megfelelően.

3. Legyen G az $n \times n$-es, nemnulla determinánsú mátrixok csoportja a mátrixszorzással, $H = (\mathbb{R} \setminus \{0\}, \cdot)$ és $\varphi(A) = \det A$. Most a homomorfizmus tétel azt mondja, hogy $G/(\{1 \text{ determinánsú mátrixok}\}) \cong (\mathbb{R} \setminus \{0\}, \cdot)$, amint az már korábban is kiderült.