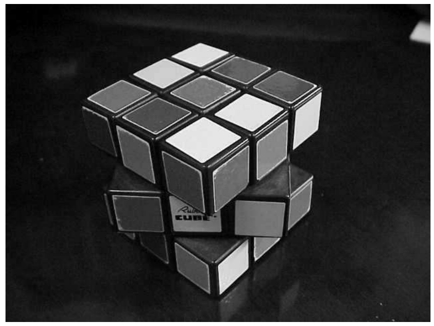
2.12 El cub de Rubik i la teoria de grups

Fa uns quants anys es va posar molt de moda jugar a l'anomenat cub de Rubik. Aquest cub està format (vist des de fora) per 26 cubs més petits; vegeu la figura següent:



Direm que el cub està ben muntat quan els sis quadradets de cada una de les sis cares són del mateix color (cada cara té un color diferent). Els moviments que permet fer el mecanisme interior del cub són: Girar cada una de les sis cares rígidament 90, 180, 270 o 360 graus (en aquests moviments el quadrat del mig de la cara sembla immòbil). L'objectiu general del joc és muntar el cub a partir d'una situació qualsevol (obtinguda girant unes quantes cares prèviament). Aquí no tractarem d'aquest problema, si no que donarem una explicació d'un fet molt curiós que s'observa a partir del cub muntat:

Prenem el cub muntat i fem una successió de moviments, per exemple:

"Movem la cara de dalt 180°, la de la dreta 180° i la de darrere 180°."

Aleshores observem que després de repetir aquest moviment un cert nombre de cops (en aquest cas dotze) el cub es torna a muntar.

La qüestió és que quan es repeteix el mateix moviment inicial, començant d'un cub muntat, després d'un cert nombre de repeticions (de vegades aquest nombre ha de ser gran) el cub es torna a muntar de manera sorprenent.

Donarem una explicació d'aquest fet usant la teoria de grups. Necessitem saber en primer lloc que és un grup. Per a més detalls podeu consultar, per exemple, el llibre de S. Lang, *Álgebra*, Ed. Aguilar, 1971.

Donat un conjunt G, denotem per f, g i h elements qualssevol de G. Suposem a més que els elements de G es poden operar entre ells donant un altre element de G. Denotem per $f * g \in G$ el resultat d'operar f amb g. Direm que el conjunt G amb l'operació $*$ és un grup si es compleixen les tres propietats següents:

- ASSOCIATIVA:
$$(f * g) * h = f * (g * h).$$

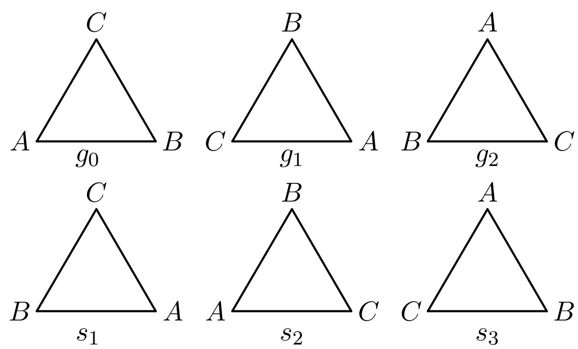
- EXISTÈNCIA D'ELEMENT NEUTRE: Existeix un element de G que denotem $u \in G$, i anomenarem element neutre, tal que
$$f * u = u * f = f$$
per a qualsevol element f de G.

- EXISTÈNCIA D'ELEMENT INVERS: Donat qualsevol element de G, f n'existeix un altre a G, que es denota per $f^{-1} \in G$ de manera que
$$f * f^{-1} = f^{-1} * f = u.$$

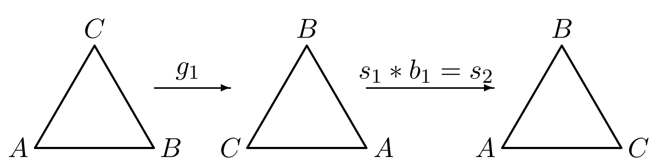
Hi ha molts exemples de conjunts amb una operació que tenen estructura de grup. Per exemple els nombres enters $\mathbb{Z}$ amb l'operació $+$, els nombres reals $\mathbb{R}$ amb l'operació $+$, els nombres $\mathbb{R}\backslash\{0\}$ amb l'operació $\times, \ldots$

Donarem també un exemple més geomètric. Considerem un triangle equilàter. Els elements del nostre grup seran els moviments que deixen invariant la posició del triangle (vegeu també la figura adjunta):

- $g_0 = u$, deixar el triangle immòbil,
- g_1, girar el triangle 120° cap a l'esquerra,
- g_2, girar el triangle 240° cap a l'esquerra,
- s_1, fer simetria respecte a l'altura vertical,
- s_2, fer simetria respecte a l'altura inclinada cap a la dreta,
- s_3, fer simetria respecte a l'altura inclinada cap a l'esquerra.



L'operació $*$ consisteix a fer un moviment rere l'altre, així per exemple $s_1 * g_1$ vol dir agafar el triangle, fer-li el moviment g_1 i al triangle resultant fer-li el moviment s_1. Obtenim que $s_1 * g_1 = s_2$; vegeu la figura següent:



Es pot veure que aquest conjunt de sis elements amb l'operació $*$ és un grup.

Veurem a continuació que si $(G, *)$ és un grup amb un nombre finit d'elements, s'agafa un element qualsevol g i es va operant amb ell mateix

$$g, g * g, g * g * g, \ldots, g \overset{m)}{* \cdots *} g, \ldots$$

arriba un moment k en què $g^k = g \overset{k)}{* \cdots *} g = u$, on recordem que u és l'element neutre de $(G, *)$.

Demostrem, doncs, l'existència d'aquest k. Considerem els elements de G, $g, g^2, \ldots, g^m, \ldots$ Com que G és un conjunt finit i el conjunt anterior és infinit, i tots els seus elements són de

G, ha d'haver-hi almenys dos elements que coincideixin. Els anomenem g^m i g^l i suposem que $m < l$. Tenim, doncs, que $g^m = g^l$.

Ara bé g ha de tenir un invers g^{-1} tal que $g^{-1} * g = u$. Per tant si operem als dos costats la igualtat $g^m = g^l$ amb g^{-1} tenim:

$$\begin{aligned} g^{-1} * g^m &= g^{-1} * g^l, \\ g^{-1} * g * \overset{m)}{\cdots} * g &= g^{-1} * g * \overset{l)}{\cdots} * g, \\ u * g * \overset{m-1)}{\cdots} * g &= u * g * \overset{l-1)}{\cdots} * g, \\ g^{m-1} &= g^{l-1}. \end{aligned}$$

Si repetim el procés $m - 1$ vegades, resulta

$$u = g^{l-m},$$

com volíem veure.

De manera una mica més complicada que en el cas dels moviments que deixen invariant el triangle equilàter, també es pot veure que el conjunt de tots els moviments que es poden fer al cub de Rubik té també estructura de grup G. Aquest grup té $2^{27} \times 3^{14} \times 5^3 \times 7^2 \times 11 = 43\,252\,003\,274\,489\,856\,000$ elements, i l'operació $*$ és la composició de moviments.

Per tant, en el nostre cas, si es pren un moviment qualsevol (g del grup G) i es repeteix k cops (l'operació $*$), s'obté l'element neutre del grup de moviments u (que ha de ser el moviment que no canvia cap de les cares del cub).

Així hem trobat una explicació matemàtica d'un fet molt curiós, que sense usar la teoria de grups costaria molt més d'explicar.