COMUNICACIONES DEL CIMAT

CENTRO DE INVESTIGACION EN MATEMATICAS

Apartado Postal 402
Guanajuato, Gto.
México
Tels. (473) 2-25-50
1 2-02-58

INTRODUCCION A LAS ESTRUCTURAS ALGEBRAICAS Y GEOMETRICAS.

FAUSTO ONGAY

I. INTRODUCCIÓN.

El objetivo de estas notas, dirigidas básicamente a profesores de enseñanza media superior, es despertar en el lector el interés por los temas citados en el título. En efecto, pretender que una exposición tan breve como ésta pueda dar algo más que un simple asomo a tan ricas disciplinas sería absurdo; un curso entero apenas podría hacerles justicia. Sin embargo, considero que es fundamental que los profesores de enseñanza media se "inicien" en este tipo de material relativamente avanzado: las matemáticas que se enseñan usualmente a nivel preparatoria son en general matemáticas de principios del siglo XIX (e incluso XVIII) y, aunque no hay nada intrínsecamente malo en ello, es conveniente tener una cierta perspectiva de éstas desde el mirador que nos proporcionan los conocimientos más recientes.

La elección de los tópicos que se discutirán aquí está obviamente determinada por mis inclinaciones personales, empero, no es una elección arbitraria: una de las características más sobresalientes de las matemáticas modernas, y que en cierto sentido es la base de su extraordinario éxito en las aplicaciones, es el énfasis que éstas hacen sobre las construcciones generales, más que sobre las instancias particulares de un cierto problema.

Dicho de manera un poco más explícita, la metodología usual de las matemáticas consiste en analizar un cierto problema abstrayendo de él ciertas características que se consideran básicas (y susceptibles de análisis): mediante este proceso de abstracción se pasa del problema original dado a un "modelo matemático del problema", que describe toda una gama de problemas relacionados y que como un caso particular incluye al problema original. La manipulación que se hace del modelo matemático ya no depende sin embargo de la naturaleza intrínseca del problema original, sino sólo de la lógica interna de las matemáticas. Y, aunque es claro que en este proceso hay cierta pérdida de información, las ventajas que ofrece este método son claras y sus éxitos así lo confirman: hoy día, la matematización de las ciencias, que hasta principios de este siglo parecía confinarse a la física (de ahí el nombre "ciencias exactas"), se ha extendido de manera casi explosiva para aplicarse a casi todas las disciplinas científicas.

En esta dirección, y dentro de las matemáticas mismas, los éxitos más espectaculares son tal vez aquellos obtenidos por el álgebra contemporánea, cuyo grado de abstracción y rigor han alcanzado niveles extremos, con la consiguiente generalidad de aplicación; en efecto, una vez liberada el álgebra de su "encajonamiento" como "aritmética con símbolos", las técnicas algebraicas se han vuelto tan poderosas que en la actualidad, acompañando a casi todas las teorías con algún origen "físico", como la geometría o la topología, se tiene una "versión algebraica" de la misma. La razón de este éxito no es difícil de detectar:

Estas son las notas preliminares para un curso dictado en la Universidad de San Luis Potosí, destinado a profesores de enseñanza media superior. Deseo agradecer a los organizadores del evento su fina atención.

gracias a su gran generalidad, los problemas algebraicos suelen ser problemas menos profundos o menos complicados y por lo tanto más fáciles de atacar. (De alguna manera, la "algebraización" de los problemas matemáticos es un paso adicional en ese proceso de simplificación a que hacíamos alusión arriba y, en general, las soluciones que se obtienen de estas aplicaciones del álgebra a otras ramas de las matemáticas son casi invariablemente sólo respuestas parciales y, todavía más, usualmente respuestas negativas, en el sentido que sólo permiten decidir que dos cosas no son iguales porque no comparten cierta propiedad algebraica, o bien, que alguna construcción no es posible porque no se satisface cierta condición algebraica, etc..)

Esta tendencia a la generalidad y a la abstracción hace que el énfasis en las teorías algebraicas sea en las llamadas estructuras algebraicas que se pueden imponer en un conjunto dado y es en éstas que estamos interesados aquí. Vagamente hablando, una estructura algebraica es una operación que se puede realizar con los elementos del conjunto y que satisface ciertas reglas especificadas como axiomas para la operación. En estas notas consideraremos algunas estructuras algebraicas, centrando nuestra atención en los grupos, que son una de las estructuras más básicas, así como en su relación con la geometría y este enfoque nos permitirá describir con bastante precisión lo que es una estructura geométrica.

Antes de cerrar esta introducción conviene aclarar que, aunque el carácter de estas es notas muy elemental, supondremos que el lector está familiarizado con las nociones básicas de la teoría de conjuntos y también con algunas definiciones elementales del álgebra lineal, como matrices y determinantes. Por otra parte, aunque daremos con precisión las definiciones, no se pretende aquí dar un "curso relámpago" en teoría de grupos y por lo mismo, ni presentaremos todas las nociones que podrían considerarse como básicas, ni daremos demostraciones completas.

II. Un poco de historia sobre el concepto de grupo.

Probablemente la estructura algebraica más sencilla de asimilar es la de **grupo**, concepto que definiremos con precisión en la siguiente sección. De hecho, una autoridad tan grande como Henri Poincaré opinaba que el ser humano tiene un cierto conocimiento a priori de lo que es un grupo o, al menos de cierto tipo de grupos (en particular del grupo de transformaciones rígidas del espacio) y, aunque esta posición tal vez sea un poco extrema, ilustra bien lo fundamental de esta noción: en efecto, (independientemente de que los sistemas númericos fundamentales –como los números enteros– posean una estructura de grupo), si analizamos los argumentos típicos de la geometría euclideana, tal y como se describen en Los Elementos de Euclides, observaremos que en ellos se hace un uso sistemático de la posibilidad de trasladar rígidamente las figuras para la demostración de los teoremas; esto es algo que no está explícitamente contemplado dentro de los axiomas de Euclides y es un ejemplo de la acción de un grupo. Y sin embargo, el comprender que existe tal estructura fue un proceso largo y complejo.

En cualquier caso alrededor de 1760 encontramos ya ciertos resultados, en especial en los trabajos de Euler en teoría de números y de Lagrange dentro de la teoría de ecuaciones, que son indiscutiblemente parte de la teoría de grupos. Un poco más adelante, en 1776, el mismo Euler consigue describir completamente las llamadas **isometrías** del espacio euclideano $\mathbf{R}^3$ lo que también puede considerarse un resultado de teoría de grupos aplicada a la geometría.

En los años siguientes aparecen dentro de estas disciplinas una gran cantidad de resultados que pueden ser también catalogados como parte de la teoría de grupos: Abbatti, Ruffini y Cauchy obtienen resultados sobre grupos de permutaciones, fundamentalmente en conexión con la teoría de ecuaciones; Gauss publica en 1801 su importantísimo tratado *Disquisitiones Arithmetica* donde estudia los llamados ahora **grupos cíclicos** o **modulares**, esto en conexión con la teoría de números, y Monge, Poncelet, Möbius y otros utilizan, de manera más o menos explícita, grupos de transformaciones en sus estudios geométricos.

Todos estos hechos aparecen sin embargo un tanto aislados, desde la perspectiva de la teoría de grupos, y casi todo mundo está de acuerdo en señalar los años 1830-1832, en que Evariste Galois escribe sus geniales trabajos sobre la solubilidad de ecuaciones por radicales, como la fecha de nacimiento de la teoría de grupos propiamente dicha.

En el siguiente periodo, las ideas de Galois comenzaron a ser esclarecidas y profundizadas por otros grandes matemáticos, como Cayley y Sylow, al tiempo que el desarrollo de la geometría se veía cada vez más ligado al de la teoría de grupos, como se puede apreciar en la obra de Chasles, Hessel y Plücker entre otros, y un nuevo clímax se alcanza hacia 1870, con la aparición del *Traité des substitutions et des équations algébriques* de Camille Jordan (1870), el programa de Erlangen de Felix Klein (1872), en el que Klein identifica el estudio de una geometría con el de su grupo de isometrías, y con los trabajos de Sophus Lie sobre los llamados "grupos continuos". Todo esto marcó la pauta para que en 1882 W. Dyck y H. Weber publicaran artículos donde la lista de axiomas que definen un grupo aparece ya en su forma definitiva.

III. Definiciones y resultados básicos de la teoría de grupos.

En esta sección describiremos las nociones más elementales de la teoría de grupos, que como hemos mencionado es una de las más importantes estructuras algebraicas.

Definición 1: Una **operación binaria** en un conjunto X, que denotaremos por $*$, es una función

$$*: X \times X \to X \quad ; \quad (x, y) \mapsto x * y.$$

Un **grupo** es un conjunto G junto con una operación binaria que satisface las siguientes propiedades:

i) La operación es **asociativa**:

$$\forall\, x, y, z \in G \quad ; \quad (x * y) * z = x * (y * z)$$

y en virtud de que la posición de los paréntesis es intrascendente, usualmente escribimos simplemente $x * y * z$.

ii) Existencia de un **neutro**:

$$\exists e \in G \quad \forall\, x \in G \quad ; \quad e * x = x * e = e.$$

iii) Existencia de **inversos**:

$$\forall\, x \in G \quad \exists\, x^{-1} \quad ; \quad x * x^{-1} = x^{-1} * x = e.$$

iv) El grupo G es **conmutativo** o **abeliano** si se satisface además

$$\forall\, x, y \in G \quad ; \quad x * y = y * x.$$

Si G es un grupo la cardinalidad de G (i.e., el número de elementos de G) se llama el **orden** de G.

Antes de seguir adelante y para fijar un poco las ideas, citemos algunos ejemplos:

i) Tal vez el grupo que nos es más familiar es el de los números enteros $\mathbf{Z}$ junto con la operación binaria de la adición; el neutro es en este caso el 0 en tanto que el inverso de un número es su negativo (por ejemplo, el inverso de -3 es $-(-3) = 3$). Notemos, sin embargo, que $\mathbf{Z}$ con el producto no es un grupo (faltan los inversos).

ii) Más generalmente, los sistemas numéricos usuales $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ así como los espacios vectoriales $\mathbf{R}^n$ junto con las operaciones de suma en los objetos respectivos son ejemplos de grupos

iii) Otro grupo bien conocido es el de los números reales $\neq 0$ con el producto; en este caso el neutro es 1 en tanto que los inversos son precisamente los inversos multiplicativos.

iv) Un instructivo ejemplo de grupos son los grupos de enteros módulo algún entero fijo, que se construyen como sigue: Para $n \in \mathbf{Z}$, $n > 0$ definimos $G = \{0, 1, \ldots, n-1\}$ y definimos la operación como "suma módulo n", es decir como el residuo que se obtiene al dividir la suma usual por n. Estos grupos, que denotamos por $\mathbf{Z}_n$, son por supuesto finitos y, de hecho, el orden de $\mathbf{Z}_n$ es n. En estos casos (dado que el orden es finito), es posible en principio escribir una tabla completa para la operación en el grupo; a título de ilustración, aquí están las tablas para $\mathbf{Z}_2$ y $\mathbf{Z}_3$:

	0	1
0	0	1
1	1	0

;

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Todos estos grupos son abelianos, sin embargo, aunque más adelante veremos que los grupos no conmutativos "existen en abundancia" y son de gran importancia, para disipar cualquier duda, el siguiente ejemplo es de un grupo no abeliano de orden 6:

v) El grupo D_3 es el grupo cuyos elementos son $\{e, a, a*a, b, b*a, b*a*a\}$, donde se satisfacen las siguientes propiedades:

$$a*a*a = e\ ;\ b*b = e\ ;\ b*a = a*a*b.$$

Es fácil verificar que D_3 es un grupo y que no es abeliano, ya que

$$a = b*(b*a) \neq (b*a)*b = a*a.$$

Invitamos al lector a escribir la tabla de la operación de D_3.

Notación: En lo sucesivo, y como es usual, en vez de escribir $a * b$ escribiremos ab, en vez de aa, a^2, en vez de aaa, a^3, etc.. Por otro lado, también nos referiremos a la operación en un grupo, especialmente si no sabemos que éste es abeliano, como **el producto** del grupo.

Aunque los axiomas para un grupo son muy sencillos, podemos ya extraer algunas consecuencias de esta definición, por ejemplo:

Proposición 1: *i)* En cualquier grupo G el neutro es único. Asimismo, para todo $x \in G$ su inverso x^{-1} es único.
ii) $\forall\, x, y \in G \quad ; \quad (xy)^{-1} = y^{-1}x^{-1}$.

Dem. Probemos la primera afirmación, dejando las otras al lector (notemos, sin embargo, que si el grupo no es abeliano en general no es cierto que $(xy)^{-1} = x^{-1}y^{-1}$, el orden de los factores es importante): supongamos, en efecto, que existiera otro neutro, digamos e'; entonces

$$e' = ee' = e,$$

donde la primera igualdad ocurre porque e **es** neutro, en tanto que la segunda se debe a que suponemos que e' es también un neutro.

En matemáticas, una de las estrategias más fundamentales y útiles para el estudio de un conjunto con estructura dado, es el estudio de los subconjuntos que comparten dicha estructura (o al menos parte de ella); dentro de la teoría de grupos la construcción pertinente es ésta:

Definición 2: Sea G un grupo y H un subconjunto de G. Decimos que H es un **subgrupo** de G si cuando restringimos la operación en G a H, éste satisface los axiomas de grupo. De manera más precisa, H es un subgrupo de G si:
i) $\forall\, x, y \in H \quad ; \quad xy \in H$.
ii) $\forall\, x \in H \quad ; \quad x^{-1} \in H$.

Es claro que todo grupo G admite al menos dos subgrupos (llamados por esta razón triviales): G mismo y $\{e\}$; sin embargo es también claro que no todo subconjunto de un grupo es un subgrupo, ya que todo subgrupo contiene al menos a e. En este sentido una proposición interesante, pues es uno de los primeros resultados generales que se establecieron dentro de la teoría de grupos, es el llamado **teorema de Lagrange** (resultado conocido por él –en un caso particular– desde 1770):

Proposición 2: Si G es un grupo finito y H es un subgrupo de G entonces el orden de H divide al orden de G.

Un corolario que resulta inmediatamente es que si el orden de un grupo finito es primo, entonces el grupo no admite más subgrupos que los triviales. Así por ejemplo, los grupos $\mathbf{Z}_2, \mathbf{Z}_3$ y $\mathbf{Z}_5$ no admiten ningún subgrupo no trivial, en tanto que $\mathbf{Z}_4$ admite el subgrupo formado por $\{0, 2\}$.

Otro sencillo resultado es el siguiente:

Proposición 3: Todo subgrupo de un grupo abeliano es abeliano.

Un aspecto fundamental relacionado con la noción de subgrupo es éste: si $H \subset G$ es un subgrupo de G, entonces H define una partición de G; los "trozos" (clases de equivalencia) de esta partición, llamados **clases laterales izquierdas**, son todos de la misma cardinalidad; estas clases laterales se construyen como sigue: $x, y \in G$ están en la misma clase lateral si existe $h \in H$ tal que $x = yh$. La clase lateral a que pertenece $x \in G$ se denota por xH y no es difícil ver que la cardinalidad de éstas es precisamente la cardinalidad de H (lo que en particular prueba el teorema de Lagrange).

Finalmente, una construcción sencilla que permite obtener nuevos grupos a partir de grupos dados es la siguiente:

Definición 3: Si G y H son dos grupos, el **producto directo** de G con H es $G \times H$, junto con la operación

$$(x, h)(y, k) = (xy, hk) \quad ; \quad x, y \in G \, , h, k \in H.$$

En esta fórmula, la operación en las primeras coordenadas es la operación en G, en tanto que en las segundas es la de H.

IV. Homomorfismos y Grupos Cociente.

Dentro de la matemática contemporánea se tiene una especie de "unión indisoluble" entre los conjuntos con estructura (como los grupos que hemos estado considerando) y las funciones que "respetan" dicha estructura. En nuestro contexto tales funciones se llaman homomorfismos de grupos y la definición precisa es la siguiente:

Definición 4: Sean H y G dos grupos. Un **homomorfismo** entre H y G es una función $f\colon H \to G$ que satisface: $\forall\, x, y \in H$; $f(xy) = f(x)f(y)$, donde las operaciones ocurren en los grupos respectivos.

Si un homomorfismo es inyectivo decimos que es un **monomorfismo**, si es suprayectivo se llama **epimorfismo** y si es biyectivo **isomorfismo**. Es claro que la función inversa de un isomorfismo es también isomorfismo y, si existe un isomorfismo entre los grupos H y G, decimos que estos son **isomorfos** y escribimos $H \simeq G$.

Conviene refrasear esta definición de la siguiente manera, menos precisa pero quizá más intuitiva: "f es homomorfismo si da lo mismo efectuar primero la operación en H y luego aplicar f que aplicar primero f y luego efectuar la operación en G". En particular, cuando dos grupos son isomorfos, la conclusión que obtenemos es que es totalmente equivalente trabajar en uno o en otro y por lo tanto distinguirlos es, en tanto que grupos, superfluo. Por esta razón una de las tareas básicas dentro de la teoría de grupos es clasificar los grupos para decidir cuando son y cuando no son isomorfos entre sí.

Ejemplos:

i) Uno de los ejemplos más importantes de homomorfismo de grupos es la función exponencial $\exp\colon \mathbf{R} \to \mathbf{R}^*$ (aquí $\mathbf{R}^*$ denota el grupo multiplicativo de los reales $\neq 0$); en efecto, la bien conocida propiedad de la exponencial $\exp(x+y) = \exp(x)\exp(y)$ dice precisamente que exp es un homomorfismo entre estos grupos. Notemos que exp es un monomorfismo, pero no es un isomorfismo (ya que $\exp(x) > 0$ para toda x). Sin embargo, si en vez de

$\mathbf{R}^*$ consideramos $\mathbf{R}^+ = \{ x \in \mathbf{R} \ ; \ x > 0\}$, que es claramente un subgrupo de $\mathbf{R}^*$, y restringimos el codominio de exp a este conjunto, exp se vuelve un isomorfismo, con inversa log.

ii) Otro ejemplo sencillo de grupos isomorfos es el siguiente: el conjunto $\{-1, 1\}$ es un subgrupo de $\mathbf{R}^*$ y es claramente isomorfo a $\mathbf{Z}_2$ (el isomorfismo explícito es $0 \mapsto 1$; $1 \mapsto -1$). Más generalmente, $\mathbf{Z}_n$ es isomorfo al grupo de **raíces enésimas de la unidad**, que son los números complejos de la forma $e^{2\pi ki/n}$; $k = 0, \ldots, n-1$, mediante el isomorfismo que envía $k \in \mathbf{Z}_n$ en $e^{2\pi ki/n}$. Estos números complejos se representan geométricamente como puntos uniformemente distribuidos en el círculo de radio 1 en el plano complejo y este isomorfismo que acabamos de describir nos muestra que la manera en que el reloj marca la hora ¡está descrita matemáticamente por $\mathbf{Z}_{12}$!

De nueva cuenta, es posible obtener resultados muy generales a partir de la simple definición de homomorfismo, por ejemplo:

Proposición 4: *i)* Si G_1, G_2, G_3 son grupos, y $f\colon G_1 \to G_2$; $g\colon G_2 \to G_3$ son homomorfismos, entonces $g \circ f\colon G_1 \to G_3$ es homomorfismo. Además la composición de monomorfismos (resp. epimorfismos, isomorfismos) es monomorfismo (resp. epimorfismo, isomorfismo).

ii) Si denotamos por e_1, e_2 a los neutros de G_1 y G_2 respectivamente entonces $f(e_1) = e_2$; asimismo, para todo $x \in G_1$, $f(x^{-1}) = (f(x))^{-1}$. En particular, la imagen de G_1 bajo f es un subgrupo de G_2.

iii) Un homomorfismo $f\colon G_1 \to G_2$ es monomorfismo si y sólo si $f(x) = e_2 \quad \Rightarrow \quad x = e_1$

Dem: Probaremos solamente *iii)*, dejando al lector la restantes afirmaciones. Ahora bien, si f es inyectivo entonces *ii)* implica inmediatamente que la condición es necesria. Para probar la suficiencia, supongamos que $f(x) = f(y)$ y queremos ver que $x = y$. Pero

$$f(x) = f(y) \quad \Rightarrow \quad f(x)\, f(y^{-1}) = e_2$$

$$\Rightarrow \quad f(xy^{-1}) = e_2 \quad \Rightarrow \quad xy^{-1} = e_1 \quad \Rightarrow \quad x = y$$

que es lo que queríamos probar.

Otra propiedad inmediata, que sin embargo es más sorprendente, es la siguiente:

Proposición 5: Sea $f\colon H \to G$ un homomorfismo de grupos y sea e el neutro de G, Entonces $\ker f = \{x \in H \ ; \ f(x) = e\}$ es un subgrupo de H.

Dem: Basta verificar que si $x, y \in \ker f$ entonces $xy \in \ker f$, lo que es inmediato.

El subgrupo descrito en la proposición anterior se llama el **núcleo** (o como se suele decir, utilizando el término alemán correpondiente, el **kernel**) de f. En este punto surgen de manera natural dos preguntas: ¿es cierto que todo subgrupo de un grupo dado puede construirse como la imagen de un homomorfismo apropiado? y ¿es cierto que todo subgrupo de un grupo dado puede construirse como el núcleo de un homomorfismo apropiado? Aunque parecidas, la primera pregunta es en cierto modo trivial, ya que todo subgrupo

puede verse como la imagen de la inclusión, que claramente (¿por qué?) es un homomorfismo. Sin embargo, la segunda es una cuestión más profunda, que se puede responder mediante la siguiente definición.

Definición 5: Sea $H \subset G$ un subgrupo de G. Decimos que H es **normal** si para toda $x \in G$, $h \in H$ se tiene $xhx^{-1} \in H$.

Conviene observar que en un grupo abeliano todo subgrupo es normal, ya que $xhx^{-1} = h$, pero en los grupos no abelianos en general no es así. Por otro lado, una primera relación entre los núcleos de homomorfismos y los subgrupos normales es la siguiente proposición (cuya demostración es muy sencilla y se deja al lector):

Proposición 6: Sea $f\colon H \to G$ un homomorfismo de grupos; entonces $\ker f$ es un subgrupo normal de H

Así pues, los núcleos de homomorfismos son, aparentemente, una clase especial de subgrupos normales, nuestro objetivo ahora es ver que **todos** los subgrupos normales aparecen de esta forma, y para ello necesitamos la siguiente construcción.

Supongamos que $H \subset G$ es un subgrupo de G y denotemos por G/H al conjunto de clases laterales de H en G; los elementos de G/H se pueden escribir en la forma xH ; $x \in G$, donde xH denota al conjunto $\{\ xh\ ;\ h \in H\}$. Quisieramos ahora definir una operación en G/H que convierta a este conjunto en un grupo. Para ello es natural suponer que necesitaremos la operación que ya tenemos, a saber la de G, y un poco de reflexión debe bastar para convencernos que la operación binaria natural en G/H es la siguiente: el producto de xH y yH es $xH\,yH = xyH$. Esta operación es claramente asociativa, pues el producto en G lo es, el inverso de $xH \in G/H$ es $x^{-1}H$ y el neutro es $eH = H$. ¿Dónde requerimos la normalidad de H? La respuesta es: para probar que la operación está bien definida; en efecto, cada clase lateral xH se puede escribir de muchas maneras distintas, remplazando a x por $y = xh$ para cualquier $h \in H$; por ello necesitamos ver que este producto no depende de como escribimos a la clase lateral, sino sólo de la clase lateral.

Sin embargo, si $H \subset G$ es normal y $xH = yH$, de modo que existe $k \in H$ tal que $y = xk$ y zH es otra clase lateral cualquiera

$$xH\,zH = \{\ xzh\ ;\ h \in H\} \quad \text{y} \quad yH\,zH = \{\ yzh\ ;\ h \in H\}$$

y queremos ver que estos dos conjuntos son iguales. Pero que H sea normal significa que para cualquier $h \in H$ existe $b \in H$ tal que $zhz^{-1} = b \iff zh = bz$. Luego si $yzh \in yzH$ entonces

$$yzh = yk^{-1}kzh = xkzh = xzbh \in xzH$$

de modo que el producto está bien definido; de hecho, en el fondo ésta es la razón que subyace la definición de subgrupo normal.

Lo anterior justifica asimismo la siguiente definición:

Definición 6: Si $H \subset G$ es un subgrupo normal de G el conjunto de clases laterales G/H con la operación definida arriba se llama el **grupo cociente** de G por H.

Tenemos ahora el siguiente resultado, cuya demostración dejamos al lector:

Proposición 7: La función $\pi\colon G \to G/H$ definida por $\pi(x) = xH$, está bien definida y es un homomorfismo de grupos, cuyo núcleo es precisamente H.

Conviene una vez más refrasear estas nociones como sigue: En G/H identificamos cada clase lateral con un punto. La función π descrita arriba, llamada la **proyección natural** de G en G/H, se puede definir aun si H no es normal y simplemente nos recuerda en que clase lateral se encuentra cada $x \in G$; sin embargo, si además H es normal todas estas construcciones "conservan" una estructura de grupo y la moraleja de esta proposición es entonces que los grupos normales y los núcleos de homomorfismos son esencialmente la misma cosa. Esto nos lleva al último resultado general que citaremos en esta breve excursión por la teoría de grupos, el llamado **primer teorema de isomorfismo**, que cierra y redondea nuestra discusión:

Teorema 1: Si $f\colon H \to G$ es un epimorfismo de grupos con núcleo $K \subset H$, entonces la función $F\colon H/K \to G$, definida por $F(xH) = f(x)$ está bien definida (i.e., no depende de que representante de la clase lateral escojamos) y es un isomorfismo.

Dem: Para ver que F está bien definida, consideramos dos representantes distintos de la clase lateral xK, digamos x y y, y queremos ver que $f(x) = f(y)$; pero entonces, existe $h \in K$ tal que $y = xh$, y por consiguiente

$$f(y) = f(xh) = f(x)\, f(h) = f(x)\, e = f(x).$$

y F es claramente un homomorfismo de grupos, por la definición del producto en H/K.

Veamos ahora que F es inyectiva dejando al lector el cuidado de verificar la suprayectividad de F: esto es sin embargo inmediato de la definición de F, de la proposición 4.*iii)* y del hecho que el neutro de H/K es precisamente K.

Como última observación, notemos que el teorema de isomorfismo se puede escribir quitando la hipótesis de que f sea epimorfismo: simplemente hay que remplazar en la conclusión a G por la imagen de f.

V. Algunos ejemplos de grupos.

Veremos a continuación algunos ejemplos un poco menos elementales de grupos, acercandonos en el camino a la conexión que existe entre los grupos y la geometría.

V.1 Grupos de permutaciones. Dado un conjunto X arbitrario, existe de manera natural un grupo asociado a él: el grupo de las funciones (o como se suele decir en este contexto **transformaciones**) invertibles del conjunto en sí mismo, que denotaremos por S_X. Las reglas bien conocidas para la composición de funciones garantizan que ésta define una operación binaria y asociativa. El neutro de esta operación es por supuesto la función identidad en el conjunto, que escribimos 1_X, en tanto que los inversos existen porque sólo consideramos funciones invertibles. Cuando el conjunto es finito, usualmente llamamos a estas transformaciones las **permutaciones** del conjunto; en este caso siempre podemos identificar a X con $\{1, \ldots, n\}$, donde n es la cardinalidad de X, y usamos la notación $S_X = S_n$ y un resultado bien conocido, probado por Ruffini en 1799, es que el orden de S_n es $n!$.

Como nuestro conjunto es finito, es posible describir las permutaciones explícitamente como sigue: dada la permutación $\sigma \in S_n$, ésta queda descrita por

$$\begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}.$$

Así por ejemplo,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

describe la permutación que envía $1 \mapsto 2$; $2 \mapsto 3$; $3 \mapsto 1$ y $4 \mapsto 4$.

Esta es una notación muy explícita, que sin embargo es un tanto "engorrosa", ya que el primer renglón es siempre el mismo y por consiguiente no aporta ninguna información (excepto el que la cardinalidad de X es n). Por ello conviene introducir una notación más eficiente, llamada notación de **ciclos.** Un ciclo de una permutación consiste simplemente en "seguir la ruta" que describe un elemento dado cuando le aplicamos repetidas veces la permutación (esto es lo que se llama la **órbita** del elemento). Por ejemplo, en la permutación descrita arriba la órbita del 1 consiste en los elementos $\{1, 2, 3\}$ (al igual que la de 2 y la de 3), "visitados" en el orden apropiado, en tanto que la órbita del 4 es el 4 mismo. Podemos entonces describir esta permutación de la siguiente forma, como **producto de ciclos:**

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1\ 2\ 3)(4) = (1\ 2\ 3)$$

En la última igualdad hemos suprimido el ciclo (4) ya que es claro que $4 \mapsto 4$ (por definición de función biyectiva). Por otro lado, es intuitivamente claro que para describir el ciclo, no importa en que elemento de la órbita empezamos el recorrido, de modo que podemos escribir$(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$; es decir, podemos efectuar una **permutación circular** de los elementos del ciclo sin alterarlo, y las diferentes maneras de escribir el ciclo quedan determinadas por el primer elemento del ciclo que escribimos.

Veamos otro ejemplo:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (2\ 5\ 1)(4\ 3) = (4\ 3)(2\ 5\ 1)$$

Aquí en la última igualdad hemos intercambiado el orden de los ciclos, ya que como los elementos de un ciclo no aparecen en el otro, la permutación "no mezcla" a los elementos de los distintos ciclos; dicho en lenguaje más técnico, ciclos ajenos conmutan.

Finalmente, un resultado importante, es que esta descomposición en ciclos ajenos es esencialmente única, en el sentido que sólo podemos cambiar el orden en que escribimos los ciclos (y por supuesto el primer elemento que escribimos dentro de cada ciclo).

Los ciclos son pues una especie de "permutaciones elementales", que nos permiten describir a las demás permutaciones; sin embargo, no son las permutaciones no triviales más simples: éstas son las **transposiciones**, que son las permutaciones que intercambian sólo dos elementos, dejando fijos a los demás. Las transposiciones determinan la descomposición

más fina que se puede hacer de una permutación arbitraria, esta afirmación es cierta en virtud de que cualquier ciclo se puede descomponer en transposiciones; de hecho, una forma explícita de hacerlo es

$$(1\ 2\ \cdots\ r) = (1\ r)(1\ r-1)\cdots(1\ 2).$$

Por ejemplo, tenemos la siguiente descomposición del ciclo (1 2 3 4):

$$(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2).$$

Para convencernos de la validez de esta descomposición, podemos recurrir a la siguiente matriz que describe explícitamente el efecto de cada transposición:

$$\begin{matrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \\ 4 & 2 & 1 & 3 \\ 4 & 1 & 2 & 3 \end{matrix}$$

que muestra que en efecto se obtiene la misma permutación cíclica original.

Observación: Podemos preguntarnos en este punto que sentido tiene introducir a los ciclos, si con las transposiciones se puede recuperar toda la información de una permutación; la respuesta es que esta descomposición en transposiciones no es única, ni por el número de transposiciones, ni por el orden de éstas, además de que las transposiciones que ocurren no son en general ajenas y por consiguiente no conmutan. Así pues, la descomposición en ciclos aporta efectivamente información adicional.

Vamos a analizar ahora, brevemente, la estructura de S_n. En primer lugar,

Proposición 8: Si $n \geq 3$ entonces S_n no es abeliano.

Dem: Es claro que todo S_n con $n \geq 3$ contiene un subgrupo isomorfo a S_3 (simplemente considérense las permutaciones que fijan los elementos del 4 en adelante), en virtud de la proposición **3.** basta entonces con que veamos que S_3 no es conmutativo. Sin embargo,

$$(1\ 2)(1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3)(1\ 2)$$

de modo que en efecto S_3 no es abeliano.

La proposición anterior muestra además que en efecto los grupos no abelianos son muy comunes, como se mencionó en la sección **III.**

A continuación vamos a describir un importante subgrupo de S_n; primero una definición:

Definición 7: Si $\sigma \in S_n$ definimos el **signo** de σ como 1 si σ se puede expresar como un número par de transposiciones y -1 en caso contrario. En el primer caso decimos que la permutación es par y en el segundo que es impar.

Aunque no es inmediato (recuérdese la observación hecha arriba), se puede demostrar que el signo de las permutaciones está bien definido, independientemente de la descomposición

de la permutación en transposiciones; una forma de ver esto es estudiar el signo de los ciclos (recuérdese que la descomposición en ciclos sí es única): se puede demostrar que el signo de un ciclo de longitud r es $(-1)^{r-1}$. De este modo, el signo de las permutaciones parte a S_n en dos clases de equivalencia y se tiene el siguiente resultado

Proposición 9: El conjunto de las permutaciones pares es un subgrupo normal de S_n de orden $n!/2$ llamado el **grupo alternante** en n elementos.

Dem: En primer lugar, es claro que el signo de la permutación identidad es 1. Por otro lado, no es difícil ver que el signo del producto de permutaciones es el producto de los signos. Usando el lenguaje que hemos desarrollado, esto nos dice que el signo es un homomorfismo de grupos entre S_n y el grupo $\{-1, 1\}$ descrito anteriormente, y cuyo núcleo es precisamente el grupo alternante, de modo que $S_n/A_n \simeq \mathbf{Z}_2$

V.2 Grupos de matrices invertibles. Otra fuente importante de grupos es el álgebra lineal. En efecto, las transformaciones lineales invertibles de un espacio en sí mismo forman de acuerdo a lo dicho en la subsección anterior, un grupo bajo composición. Cuando identificamos a nuestro espacio vectorial, mediante la elección de una base, con $\mathbf{R}^n$ las transformaciones lineales invertibles se identifican con matrices y la composición de funciones se convierte en multiplicación de las matrices correspondientes: el grupo que obtenemos de esta forma se denota por $\mathrm{GL}(n, \mathbf{R})$ y se llama el **grupo lineal general.** Por ejemplo, $\mathrm{GL}(2, \mathbf{R})$ consiste de las matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ sujetas a la condición $\det A = ad - bc \neq 0$, con el producto usual de matrices.

Como se ve en este ejemplo, en la definición de $\mathrm{GL}(n, \mathbf{R})$, la hipótesis de invertibilidad se puede expresar en términos del determinante de las matrices, ya que una matriz A es invertible si y sólo si $\det A \neq 0$. De este modo vemos que el determinante es una función entre los grupos $\mathrm{GL}(n, \mathbf{R})$ y $\mathbf{R}^*$, que es, además, un homomorfismo de grupos por la propiedad bien conocida de los determinantes

$$\det AB = \det A \det B.$$

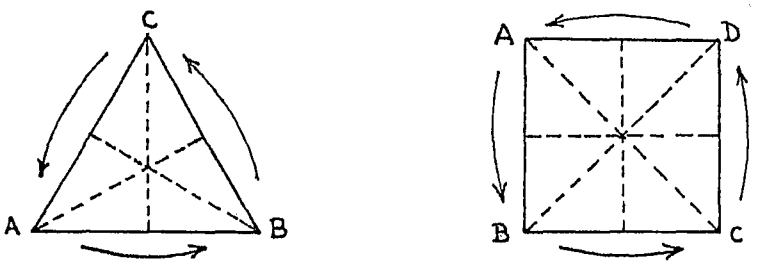
Por medio del determinante podemos construir varios subgrupos importantes de $\mathrm{GL}(n, \mathbf{R})$, siendo tal vez el más importante de ellos el núcleo del determinante, que se denota por $\mathrm{SL}(n, \mathbf{R})$ y se llama el **grupo lineal especial**; dicho en otrs palabras, $\mathrm{SL}(n, \mathbf{R})$ es el grupo de las matrices cuyo determinante es 1.

Finalmente, otro método para construir subgrupos de $\mathrm{GL}(n, \mathbf{R})$ es pedir que las matrices que forman el subgrupo preserven lo que se llama una **forma bilineal.** Para no complicar la exposición, nos contentaremos con describir el caso más simple, que corresponde al llamado **grupo ortogonal.** Este es el subgrupo de $\mathrm{GL}(n, \mathbf{R})$ de matrices que preservan la forma bilineal $x_1y_1 + x_2y_2 + \ldots + x_ny_n$ y que se denota $\mathrm{O}(n)$. Podemos obtener una condición geométrica más sencilla de interpretar (y que es equivalente) si escogemos a los vectores $(x_1, \ldots, x_n)$ y $(y_1, \ldots, y_n)$ iguales, ya que en este caso la forma bilineal corresponde simplemente al cuadrado de la norma (o magnitud) del vector; así pues, podemos decir que el grupo ortogonal es el grupo de transformaciones lineales que preservan la norma de los vectores. Por otro lado, las matrices que forman el grupo ortogonal admiten una sencilla caracterización: $A \in \mathrm{O}(n) \iff A^{-1} = A^t$ donde A^t denota a la matriz transpuesta.

V.3 Grupos de simetrías de figuras regulares. En este ejemplo consideraremos los grupos de simetrías de polígonos regulares así como de los cinco sólidos regulares.

i) El grupo de simetrías de un polígono regular con n lados es el **grupo dihédrico** D_n. En efecto, todas las simetrías de un polígono regular pueden expresarse en términos de dos simetrías elementales: una rotación que permute vértices sucesivos del polígono y una reflexión a lo largo de alguno de los ejes de simetría de la figura.

Los casos más sencillos son por supuesto los de las simetrías del triángulo equilátero y del cuadrado, como los mostrados en la figura:



En el caso del triángulo, es claro que las simetrías son las rotaciones y las reflexiones a lo largo de las medianas del triángulo. Pero cualquier rotación se puede obtener iterando la rotación que gira los vértices en el sentido positivo, y que utilizando la notación de ciclos desarrollada en **V.1** se puede escribir como $(A\ B\ C)$, en tanto que cualquier reflexión se puede obtener a partir de la reflexión $(A\ B)$, aplicando una rotación primero. Si denotamos $a = (A\ B\ C)$; $b = (A\ B)$, resulta inmediatamente que el grupo dihédrico descrito aquí coincide con el grupo dihédrico descrito abstractamente en la sección **III.**

Nota: Por otro lado, no es difícil ver (e invitamos al lector a que se convenza de ello) que este grupo también coincide con el grupo S_3 descrito anteriormente; de hecho, es posible demostrar que sólo hay dos clases de isomorfismo de grupos de orden 6: el grupo cíclico $\mathbf{Z}_6$, que es abeliano y el grupo S_3, que es no conmutativo. Para grupos de orden menor que 6 la clasificación es también muy simple: de orden 2, 3 y 5 sólo hay un grupo: $\mathbf{Z}_2$, $\mathbf{Z}_3$ y $\mathbf{Z}_5$ respectivamente (esto se puede ver utilizando el teorema de Lagrange, ya que 2, 3 y 5 son primos), en tanto que de orden cuatro hay dos grupos esencialmente distintos $\mathbf{Z}_4$ y $\mathbf{Z}_2 \times \mathbf{Z}_2$, ambos abelianos; invitamos al lector a que verifique que estos últimos no son isomorfos escribiendo las tablas de los productos respectivos.

La clasificación de los grupos aumenta en complejidad rápidamente, conforme aumenta el orden del grupo, por lo que no proseguiremos más en esta línea.

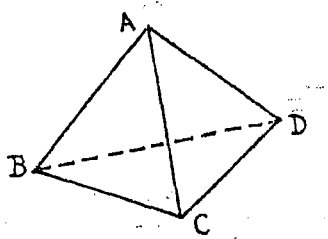
El análisis para el grupo de simetrías del cuadrado, que es la siguiente figura en complejidad, es muy semejante: las únicas simetrías del cuadrado son rotaciones, reflexiones a lo largo de una diagonal o reflexiones a lo largo de una recta que bisecte un lado del cuadrado perpendicularmente: Sin embargo, por ejemplo la reflexión en el eje AC se puede obtener reflejando primero en la recta que bisecta el lado AD y luego rotando en sentido positivo. Vemos así que en efecto basta con una rotación y una reflexión para obtener todas las simetrías del cuadrado.

Regresando a los grupos dihédricos en general, el análisis del caso de polígonos con n lados es muy semejante y ya no lo haremos aquí , y el último resultado que citaremos, y que es inmediato de la definición, es que el orden de D_n es $2n$ (en particular es claro que

para $n > 3$, $D_n \not\cong S_n$).

ii) Describiremos ahora los grupos de simetrías rotacionales de los sólidos regulares, tratando con cierto detalle los casos del tetraedro y del cubo.

Cosideremos un tetraedro como el mostrado en la figura

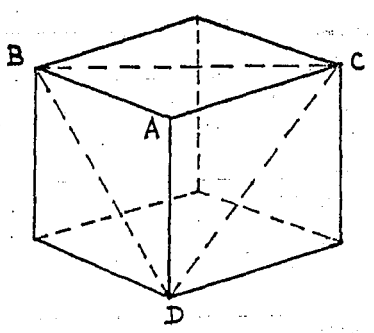


Si etiquetamos los vértices del tetraedro como en la figura, es claro que el grupo de simetrías de éste, que denotaremos por lo pronto por G, es un subgrupo de S_4. Si consideramos todas las simetrías que fijan un vértice del tetraedro, digamos el vértice A, vemos que éstas son simplemente rotaciones del tríangulo BCD, de las que dos son no triviales y la otra es la identidad. Vistas como permutaciones de estos vértices son ciclos de longitud 3, por lo que todas estas permutaciones son pares. Repitiendo este proceso para los restantes vértices del tetraedro obtenemos un total de 8 rotaciones no triviales, junto con la identidad.

Este no puede ser el total de rotaciones de los vértices del tetraedro, pues como hemos dicho, G es un subgrupo de S_4, de modo que su orden debe dividir a 24, que es el orden de S_4. Como el único divisor de 24 mayor que 9 es 12, y dado que G tiene al menos 9 elementos, nos hacen falta otras 3 rotaciones. Estas se obtienen considerando parejas ajenas de vértices, por ejemplo $\{A, B\}$ y $\{C, D\}$ y la rotación que manda la arista AB en la arista CD. En el lenguaje de permutaciones, éstas corresponden al producto de transposiciones $(A\ B)\,(C\ D)$, que también son permutaciones pares. De éstas hay 3 posibles y esto agota todas las posibilidades par los elementos de G, pues G no puede contener ninguna reflexión (las reflexiones invertirían la orientación del tetraedro, en tanto que las rotaciones la preservan). Así, en definitiva $G = A_4$.

Nota: De hecho, el argumento anterior muestra que el grupo de todas las simetrías del tetraedro es S_4.

El caso del cubo se puede discutir de manera semejante. Por ejemplo, si consideramos las rotaciones del cubo que fijan un vértice, éstas dejarán fijo el vértice diametralmente opuesto y corresponderán a rotaciones en el plano perpendicular, que contiene 3 de los vértices del cubo, como se ve en la figura siguiente, de modo que obtenemos de esta forma 8 rotaciones no triviales más la identidad:



De hecho, el argumento usado arriba indica que si conocemos la posición final de un vértice dado, también conocemos la posición del vértice que le es diametralmente opuesto. Esto implica que el grupo de rotaciones del cubo es algún subgrupo de S_4 (y no de S_8, como podría pensarse a priori), y por lo que vimos al considerar el caso del tetraedro, no puede tratarse mas que de A_4 o de S_4.

Vamos a ver que en este caso el grupo es S_4 lo que es fácil, pues para ello basta con ver que el grupo de simetrías del cubo tiene más de 12 elementos; como hemos visto, las simetrías que fijan al menos uno de los vértices de una de las caras totalizan 9; por otro lado, las simetrías (no triviales) que fijan esta cara, rotando los vértices de la cara son otras 3, lo que totaliza 12; pero es claro que hay otras rotaciones por ejemplo, la que manda una cara en la que está diametralmente opuesta; esta simetría no fija ningún vértice de la cara original ni es una rotación de los vértices de ésta, por lo que es una simetría distinta de las consideradas anteriormente. Esto completa la demostración de que el grupo de simetrías rotacionales del cubo es S_4 (sin embargo, en este caso el grupo de todas las simetrías del cubo es un poco más delicado de describir, ya que depende de que es lo que entendemos por simetría del cubo).

Una caractéristica notable de los sólidos regulares es que, si tomamos los baricentros de las caras de un sólido regular, el resultado es otro sólido regular; en el caso del tetraedro, el resultado es otro tetraedro, pero en el caso de las otras figuras, ocurren apareamientos no triviales: para el cubo, el resultado es un octaedro (y viceversa), en tanto que para el dodecaedro el resultado es un icosaedro (y viceversa). Esta propiedad de los sólidos regulares es lo que se conoce como **principio de dualidad**, y en nuestro caso tiene la consecuencia que el grupo de simetrías de cada sólido es el mismo que el de su dual (pues es claro que cada simetría de uno induce una simetría del otro). Así, el grupo de simetrías del octaedro es también S_4.

Finalmente, un análisis similar al hecho para los casos anteriores, combinado con el principio de dualidad, nos muestra que el grupo de simetrías rotacionales del dodecaedro y del icosaedro es S_5.

VI. Otras estructuras algebraicas.

Haremos ahora una breve mención de otras estructuras algebraicas que aparecen con frecuencia.

VI.1 Anillos. En el primer ejemplo de grupo que citamos, el grupo de los enteros $\mathbf{Z}$, es claro que existe otra operación binaria: el producto de enteros. Los conjuntos que tienen dos operaciones que satisfacen las mismas propiedades básicas de las operaciones en $\mathbf{Z}$ se llaman anillos; la definición precisa es la siguiente:

Definición 8: Un **anillo** A es un conjunto con dos operaciones, que denotamos $+$ y $*$ respectivamente y tal que

i) A junto con la operación $+$, que llamamos la adición en el anillo, es un grupo abeliano. Denotamos al neutro de esta operación por 0, y al inverso de $a \in A$ por $-a$.

ii) La operación $*$, que llamamos el producto en el anillo, es asociativa.

iii) Las operaciones de A satisfacen la ley de distributividad

$$a*(b+c)=(a*b)+(a*c) \quad ; \quad (a+b)*c=(a*c)+(b*c) \quad \forall\, a,b,c\in A$$

iv) El anillo tiene **elemento unidad** o **neutro multiplicativo** si existe un elemento $1\in A$ tal que $1*a=a*1=a \quad \forall a\in A$

v) Si además la operación $*$ es conmutativa decimos que el anillo es conmutativo.

De nueva cuenta, varias propiedades pueden extraerse inmediatamente de la definición, veamos sin demostración algunas de las más sencillas.

Proposición 10: *i)* En todo anillo $a*0=0$ para todo $a\in A$. Además, si $0=1$ el anillo consta de un sólo elemento: $A=\{0\}$.

ii) $\forall a\in A \quad (-1)*a=a*(-1)=-a$

iii) $\forall a,b\in A \quad (-a)*b=a*(-b)=-(ab)$.

Como antes, para simplificar la escritura, usualmente se omite el $*$ y la costumbre, es dar "preferencia" al producto, de modo que por ejemplo la ley distributiva se escribe simplemente $a(b+c)=ab+ac$, etc. Por otro lado, cabe señalar que aunque no hay consenso en ello, lo más usual es pedir que los anillos tengan unidad y más aún, para que la teoría no sea trivial, que $0\neq 1$.

Veamos algunos ejemplos:

Ejemplos: *i)* Aparte de los ejemplos "obvios", como $\mathbf{Q}$, $\mathbf{R}$ y $\mathbf{C}$, un ejemplo sencillo de anillo es $\mathbf{Z}_2$ con la adición módulo 2, definida como antes y junto con el **producto módulo 2**, definido de la manera natural. Dejamos al lector la tarea de escribir la tabla de este producto y verificar que los axiomas de anillo se satisfacen.

ii) Tal vez el ejemplo más importante de anillo, aparte de los ya citados, es el del anillo de polinomios con coeficientes en $\mathbf{R}$ o en $\mathbf{C}$. Una vez más, es un ejercicio sencillo ver que los axiomas se satisfacen.

iii) El último ejemplo que citaremos es el del anillo de todas las matrices cuadradas de $n\times n$ (invertibles o no), junto con la suma y producto de matrices. Este ejemplo muestra que no todos los anillos son conmutativos.

Como en el caso de los grupos, es posible definir subanillos y homomorfismos de anillos. Las definiciones deben de contemplar en ambos casos el hecho que los anillos tienen dos operaciones; por ejemplo, para definir un homomorfismo entre los anillos A y B, consideramos una función $f\colon A\to B$ tal que

$$f(a+b)=f(a)+f(b) \quad \text{y} \quad f(ab)=f(a)\,f(b)$$

donde las operaciones se efectúan en los anillos correspondientes y si además, en la definición de anillo pedimos que estos tengan unidad, entonces pedimos también $f(1)=1$, etc.

Como antes, la imagen de un anillo bajo un homomorfismo de anillos será un subanillo del codominio, sin embargo, la situación con los núcleos en este caso es un poco más sutil; veamos las definiciones pertinentes:

Definición 9: *i)* El núcleo de un homomorfismo de anillos $f\colon A \to B$ es $\ker f = \{a \in A\ ;\ f(a) = 0\}$

ii) Un ideal $\mathcal{I} \subset A$ es un subgrupo del grupo aditivo que tiene la siguiente propiedad

$$\forall a \in A\ ;\ j \in \mathcal{I} \quad aj \in \mathcal{I}$$

Es importante notar que los ideales no son subanillos, ya que si el anillo tiene unidad y $1 \in \mathcal{I} \Rightarrow \mathcal{I} = A$; sin embargo, los ideales son el análogo apropiado de los subgrupos normales para el caso de anillos:

Proposición 11: *i)* El núcleo de un homomorfismo de anillos $f\colon A \to B$ es un ideal de A.

ii) Todo ideal $\mathcal{I}$ de un anillo A define una partición del anillo. El conjunto de clases laterales de un anillo, $A/\mathcal{I}$, hereda una estructura de anillo de modo que la proyección natural de A en $A/\mathcal{I}$ es un homomorfismo de anillos.

iii) (Teorema de isomorfismo) Si $f\colon A \to B$ es un epimorfismo de anillos con núcleo $\mathcal{I}$ entonces f induce un isomorfismo $F\colon A/\mathcal{I} \to B$.

Observación: Como sugieren los resultados que hemos enunciado en la proposición anterior, una gran cantidad de construcciones de la teoría de grupos pasan a la teoría de anillos. Aunque no podemos detenernos aquí a explicar este fenómeno en detalle, sí quisieramos insistir en que no es un hecho aislado, sino que es algo que sucede en muchas de las estructuras algebraicas. Este tipo de fenómenos se han sistematizado en la moderna teoría de categorías, que puede cosiderarse como el "sumum" de la abstracción de lo que es una estructura algebraica.

VI.2 Campos, espacios vectoriales y álgebras. Señalemos finalmente que existen tantas estructuras algebraicas que comentar en todas ellas nos sería imposible; por ello nos contentaremos con mencionar las definiciones y dar algunos ejemplos de las estructuras que se indican en el título de esta subsección:

Un campo es un anillo conmutativo con $1 \neq 0$ y donde los elementos distintos de cero forman un grupo bajo el producto. Los campos son tal vez la estructura algebraica más rica en propiedades, y sirven como base para muchas otras construcciones algebraicas, pero también para las construcciones geométricas y para el análisis. Los ejemplos más sencillos son por supuesto los bien conocidos "campos numéricos" $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, pero existen otros muchos campos, por ejemplo, $\mathbf{Z}_2$ con las operaciones citadas arriba es un campo.

Los espacios vectoriales sobre un campo dado son grupos abelianos que tienen además un **producto por escalares** que satisface ciertas propiedades, como distributividad del producto por escalares con respecto de la suma. Ejemplos de espacios vectoriales incluyen por supuesto a los espacios $\mathbf{R}^n$, pero también a los espacios de funciones que satisfacen propiedades apropiadas, por ejemplo, el espacio de las funciones continuas sobre el intervalo $[0, 1]$ es un espacio vectorial con las operaciones de suma de funciones y de producto por números reales.

Finalmente, las álgebras combinan las estructuras de espacio vectorial y de anillo; dos ejemplos de álgebras que ya hemos mencionado antes son el álgebra de todas las matrices cuadradas de $n \times n$ y el álgebra de funciones continuas. Cabe mencionar que no en todos los espacios vectorriales de dimensión finita se puede imponer una estructura de álgebra, esto es posible por ejemplo en dimensiones 1 (los números reales), 2 (los números complejos) y 4 (los cuaternios de Hamilton), pero $\mathbf{R}^3$ con el producto cruz no es un álgebra, ya que este producto no es asociativo; sin embargo, existen modificaciones de la definición de álgebra que hemos dado aquí que incluyen este caso y otros similares.

Con estos breves ejemplos de estructuras terminamos nuestra pequeña excursión por el mundo del álgebra contemporánea, no sin antes señalar que aunque en todos estos ejemplos se tiene más estructura que en los grupos, es posible obtener resultados interesantes incluso con menos estrucutra, pero además, por supuesto, es posible considerar construcciones algebraicas totalmente ajenas a la de grupo.

VII. Esbozo del desarrollo histórico del concepto de geometría.

En esta sección describiremos brevemente el desarrollo histórico de la geometría, básicamente con el fin de establecer la conexión con la teoría de grupos esbozada antes.

En primer lugar notamos la etapa anterior a la Grecia clásica, desrrollada fundamentalmente en Babilonia, Egipto y China, donde los conocimientos geométricos son más bien empíricos.

A esta etapa sigue la formalización de la geometría dada por los griegos, que se inicia alrededor del siglo VI antes de nuestra era con Tales de Mileto y que, pasando por grandes nombres como Pitágoras, culmina en los elementos de Euclides, escritos alrededor del año 300 A.C.. Esta etapa griega, que incluye matemáticos tan destacados como Arquímedes y Apolonio, termina alrededor del año 300 D.C. con la destrucción final de la biblioteca de Alejandría.

La geometría experimenta un resurgimiento real sólo hasta el siglo XVII, cuando alrededor de 1640 Desargues y Pascal reinician el estudio de la geometría proyectiva (usando métodos sintéticos, es decir, sin coordenadas, siguiendo en cierto modo el espíritu original de la geometría clásica griega) y de manera especial con la aparición en 1637 del tratado *La géométrie* de Descartes, donde por vez primera se hace un uso sistématico de coordenadas par el estudio de problemas geométricos.

Paralelamente, cabe mencionar los numerosos estudios suscitados por el famoso "quinto postulado" o postulado de las paralelas de Euclides. Este postulado, que nos es más conocido en la forma enunciada por Playfair hacia mediados del siglo XVIII, pero que es equivalente a la original, siempre fue causa de sospechas, debido más que nada a que hace una afirmación sobre el comportamiento de las rectas "al infinito", razón por la cual su validez no es realmente "obvia". Mucho esfuerzo se dedicó a tratar de demostrarlo en base a los restantes postulados, y entre los más destacados intentos cabe citar los trabajos de Saccheri alrededor de 1730. Estos esfuerzos estaban sin embargo destinados al fracaso, pues como sabemos ahora este postulado es independiente de los otros. (De hecho, es algo curioso observar que en los trabajos de Saccheri se encuentra prácticamente la demostración de este hecho, aunque Saccheri mismo nunco lo entendió así.)

Hacia la segunda mitad del siglo XVIII y principios del siglo XIX, la línea de investigación en geometría sintética fue considerablemente impulsada por Gaspard Monge y sus seguidores en la École Polytéchnique de Francia, como Chasles y Poncelet, y un poco más tarde, con las notables contribuciones de Steiner, Plücker y Möbius, entre otros, fuera de ese país.

Por otro lado, la geometría analítica, como se puede apreciar en el tratado de Lagrange *Éléments de Géométrie*, se fue poco a poco convirtiendo en una rama del cálculo, creado por Newton y Leibniz a fines del siglo XVII, y buena parte de los resultados nuevos, como los famosos teoremas de Meusnier y Euler sobre curvas en superficies, utilizaron esta nueva y poderosa herramienta. Probablemente el clímax en el desarrollo de este aspecto de la geometría se alcanza con el artículo *Disquisitiones generales circa superficies curvas* publicado por Gauss en 1827.

En este mismo periodo surge una auténtica revolución dentro de la concepción que los matemáticos del siglo XIX tenían de la geometría con la aparición de las llamadas geometrías no euclideanas: en efecto, hasta las primeras décadas del siglo XIX los matemáticos, influidos sin duda por filosofías como la sustentada por Kant, creían que la Naturaleza privilegiaba a la geometría euclideana, en el sentido que ésta era la única que podía describir la naturaleza del espacio físico. Sin embargo, la aparición hacia 1830 de los trabajos de Lobachevsky y Bolyai sobre geometrías esencialmente distintas de la euclideana, cimbró completamente las bases de estas convicciones. (Aquí es interesante notar que Gauss tenía conocimiento cabal de estas nuevas geometrías unos 20 años antes de la aparición de los trabajos de Lobachevsky y Bolyai, pero que precisamente por no entrar en conflicto con estas posiciones filosóficas nunca publicó sus propios resultados.)

Un hito especial en el desarrollo de la geometría lo marca el discurso inaugural de Riemann, leído en 1854 ante la academia de Götingen, en el cual se abren opciones para la geometría que a la larga rebasarían el ámbito de la geometría propiamente dicha, por ejemplo con el Analysis situs de Poincaré, que es el precursor de la topología moderna.

Sin embargo, para los fines de nuestra historia, conviene cerrar nuestro relato señalando los nombres de Cayley, Sylvester, Beltrami, Klein y el propio Poincaré, cuyas contribuciones quedan epitomizadas en el programa de Erlangen ya mencionado, y que acabaron de establecer los estrechos vínculos que existen entre el estudio de la geometría y la teoría de grupos.

VIII. Estructuras geométricas y grupos de isometrías.

Describiremos ahora muy brevemente como intervienen en el estudio de la geometría los grupos de isometrías, para lo cual consideraremos dos ejemplos sencillos: la geometría euclideana y la geometría proyectiva en el plano. Para ello, es conveniente identificar el plano $\mathbf{R}^2$ con $\mathbf{C}$, el campo de los números complejos.

Recordemos ante todo que el plano euclideano es $\mathbf{R}^2$ junto con la distancia $d(x,y) = ((x_1-y_1)^2+(x_2-y_2)^2)^{1/2}$. Si identificamos el plano con $\mathbf{C}$, la distancia al origen se puede expresar por $|z| = (z\bar{z})^{1/2}$.

VIII.1 Isometrías en el plano euclideano. Con estos preliminares, el estudio de las isometrías del plano se puede atacar dividiendo el problema en casos. La primera etapa consiste básicamente en probar que las isometrías que conocemos intuitivamente son en efecto

isometrías (es decir, efectivamente preservan la distancia euclideana), que por supuesto es la parte sencilla. Después de esto hay que dividir a las isometrías en casos apropiados. Finalmente, hay que probar que cualquier isometría cae dentro de los casos considerados, que es la etapa más interesante.

Proposición 12: Las siguientes son isometrías de $\mathbf{C}$

i) Las traslaciones por un vector c: $z \mapsto z + c$; $c \in \mathbf{C}$

ii) Las rotaciones por un ángulo θ: $z \mapsto e^{i\theta} z$; $0 \leq \theta < 2\pi$

iii) La reflexión a lo largo de una recta con ángulo θ: $z \mapsto (e^{i\theta}\bar{z})$

La demostración de estas afirmaciones es casi inmediata de las definiciones.

Siguiendo entonces con nuestro programa, queremos ahora ver que tipos de isometrías se tienen y para ello, la estrategia correcta es estudiar cuantos puntos fijan las isometrías. Tres casos conviene distinguir: aquellas que no fijan ningún punto, las que fijan un sólo punto, y aquellas que fijan más de un punto. Si estudiamos las isometrías descritas en la proposición anteriar es más o menos inmediato ver que las traslaciones no fijan puntos, las rotaciones fijan un sólo punto, el origen, en tanto que las reflexiones fijan toda una recta: la recta en que reflejamos.

Con este conocimiento, podemos pasar a la última etapa: demostrar que las isometrías son todas de los tipos descritos anteriormente, o composiciones de ellas; recogemos el resultado final en la siguiente proposición:

Proposición 13: Las isometrías del plano se dividen en dos categorías:

i) Las isometrías que preservan la orientación, que son las de la forma: $z \mapsto e^{i\theta} z + c$.

ii) Las isometrías que invierten la orientación, que son las de la forma: $z \mapsto e^{i\theta}\bar{z} + c$.

Dem: A título de ilustración demostremos, dos casos particulares:

Lema 1: Si una simetría fija el 0 y el 1 y no es la identidad, entonces es la reflexión $z \mapsto \bar{z}$

Dem: Sea α la isometría y sea z cualquier punto del plano; como α fija 0 y 1, y preserva las distancias, la imagen de z bajo α debe estar contenida en la intersección del círculo de centro 0 y radio $|z|$ y del círculo de centro 1 y radio $|z-1|$. Pero la interscción de estos dos círculos es un sólo punto, si $z \in \mathbf{R}$ y dos puntos en caso contrario. Como estamos suponiendo que α no es la identidad, en este último caso $\alpha(z) \neq z$ y por lo tanto $\alpha(z) = \bar{z}$. Por supuesto, estas consideraciones geométricas que hemos hecho aquí se pueden demostrar analí ticamente, escribiendo las ecuaciones correspondientes.

Lema 2: Si una isometría α envía 0 en c, y τ es la traslación $z \mapsto z + c$ entonces la isometría $\alpha \circ \tau^{-1}$ fija el origen.

Dem: Basta con ver que la inversa también fija el 0, pero esto es inmediato de las definiciones.

Por último, describamos brevemente la estructura del conjunto de isometrías del plano.

Proposición 14: El conjunto de todas las isometrías del plano es un grupo. El conjunto de las isometrías que preservan orientación es un subgrupo normal de éste, que llamamos el grupo de **transformaciones rígidas** o de **congruencias**; el grupo cociente es $\mathbf{Z}_2$.

Dentro del grupo de congruencias hay dos subgrupos especiales: el de las traslaciones, que es $\mathbf{C}$ y el de las rotaciones, que denotamos U(1); este último es un subgrupo normal del grupo de congruencias y el cociente es isomorfo a $\mathbf{C}$.

Notá: El grupo de congruencias no es isomorfo al producto directo de U(1) con $\mathbf{C}$, es una construcción un poco más complicada, pero también de importancia, llamada **producto semidirecto**, la que interviene aquí.

VIII.2 "Isometrías" proyectivas: el grupo de Möbius. Como colofón de estas notas, describiremos de manera un tanto informal los resultados para el caso de la geometría proyectiva. En este caso, la propiedad que se preserva no es una distancia, sino la llamada **razón cruzada** de 4 puntos en el plano, definida como

$$R(z_1, z_2, z_3, z_4) = \frac{z_3 - z_1}{z_3 - z_2} \Big/ \frac{z_4 - z_1}{z_4 - z_2}$$

que describe el hecho que las **proporciones** son las que se preservan en geometría proyectiva. Todas las isometrías del plano son transformaciones que preservan la razón cruzada, pero no son las únicas; existen otras dos clases fundamentales de transformaciones proyectivas, que son las **dilataciones** con respecto de algún punto fijo y las **inversiones**; estas corresponden a proyectar un punto desde el centro de un círculo dado, que queda fijo bajo la inversión, y de suerte que la razón cruzada se preserve. Para describirlas en lenguaje analítico, y contentándonos con los ejemplos más simples, mencionemos que la dilatación con respecto del origen corresponde a multiplicar por un número real positivo, en tanto que la inversión de centro 0 y que fija el círculo unitario en el plano es $z \mapsto 1/z$.

Si escribimos la composición de esta nuevas transformaciones proyectivas con las isometrías generales del plano, las transformaciones proyectivas que resultan son de la forma:

$$z \mapsto \frac{az + b}{cz + d}$$

donde $a, b, c, d \in \mathbf{C}$; $ad - bc \neq 0$. El grupo que se obtiene de esta forma es el llamado grupo de Möbius, y se puede demostrar que éste es el grupo de todas las transformaciones proyectivas.

Con esta sumaria descripción de la geometría proyectiva concluimos nuestra exposición.

Centro de Investigación en Matemáticas. Guanajuato, Gto. 36000. México