El diablo de los números

Sección a cargo de

Javier Fresán

Un experimento de demostración formal de un teorema de nivel intermedio en álgebra*

por

Antoine Chambert-Loir

1. Introducción

Las matemáticas humanas se escriben en el lenguaje corriente, y todos conocemos ejemplos de cómo sus deficiencias a veces conducen a «demostraciones» de resultados falsos. Sabemos también desde hace más de un siglo, gracias en especial a los trabajos de Peano [16] o Whitehead y Russell [19], que es posible escribir las matemáticas usando sistemas axiomáticos y, al menos en teoría, con una sintaxis rígida que evite esos problemas, siempre y cuando el sistema axiomático de partida no dé lugar a contradicciones. Escribo «en teoría» porque este modo de escritura sintáctica rígida es extremadamente verborreico: Whitehead y Russell necesitaron cientos de páginas para demostrar $1 + 1 = 2$. El cómic [5] cuenta la búsqueda de esos fundamentos sólidos de forma agradable para el gran público.

Desde los años 50, el desarrollo de los ordenadores ha llevado a los matemáticos a intentar usar su fuerza mecánica para desarrollar demostraciones completamente formalizadas del corpus matemático. Mencionemos como ejemplo `Automath` de N. G. de Bruijn (1967), `Mizar` de A. Trybulec (1973), el proyecto `Coq` del grupo de G. Huet (1989), `Agda` de C. Coquand (1999) o `Lean` de L. de Moura (2013)...

En los últimos años, estos programas han permitido comprobar algunas partes delicadas del corpus matemático: la demostración de Appel y Haken del teorema de los cuatro colores (se pueden colorear las regiones delimitadas por un grafo plano finito con cuatro colores de modo que dos regiones vecinas tengan colores distintos); la demostración de Feit y Thompson del teorema del orden impar (un grupo finito de orden impar es resoluble), formalizada por Gonthier [6] y Gonthier *et al.* [7] en `Coq`; la demostración de Hales de la conjetura de Kepler (la densidad máxima de un

*Traducido del inglés por Javier Fresán.

apilamiento de esferas se alcanza con el apilamiento piramidal estándar) por Hales *et al.* [8] (en `HOL Light`); siguiendo el desafío de Scholze [17], la demostración de un resultado delicado de álgebra homológica de Clausen y Scholze (en `Lean`, el llamado «Liquid tensor experiment», por Commelin y Topaz en 2022, con la ayuda de mucha más gente); o la demostración de Gromov del h-principio y el teorema de inversión de la esfera por van Doorn, Massot y Nash [4], también en `Lean`.

De hecho, estos últimos resultados no han sido formalizados simplemente en `Lean`, sino en la biblioteca matemática `mathlib`. Dirigida por un grupo de aproximadamente 25 personas, a las que hay que sumar unos 15 revisores, esta biblioteca matemática es el resultado del esfuerzo creciente de alrededor de 300 personas, con (hasta la fecha de hoy) aproximadamente 45 000 definiciones y 110 000 enunciados matemáticos («teoremas») que abarcan muchos campos de las matemáticas, como la combinatoria aditiva, el análisis complejo, la geometría diferencial, la integración de Lebesgue... Para que sea posible un trabajo colectivo, los primeros autores de `mathlib` tuvieron que decidir cuidadosamente la arquitectura y el diseño, tal y como describen en [18]. Como `Lean`/`mathlib` es un proyecto de código abierto, también es relativamente fácil instalarlo en tu propio ordenador y unirse así a la comunidad. A ello también ayuda una página web completa y un tablero de discusión en línea donde los colaboradores comparten sus problemas e ideas de manera muy generosa.

En noviembre de 2021, me embarqué en la aventura de comprobar en `Lean` y en `mathlib` la demostración del hecho de que el grupo alternado de un conjunto de cardinal mayor o igual que 5 es simple. Aunque este resultado es mucho más modesto que los mencionados anteriormente, pertenece al corpus matemático clásico de los estudios universitarios, y me pareció interesante experimentar con el proceso de formalización de un resultado de nivel intermedio. Por razones que intentaré explicar, elegí un enfoque no convencional para hacerlo, lo que me llevó a territorios matemáticos inesperados. Este texto es un relato retrospectivo de este viaje.

Agradecimientos. Doy las gracias a Javier Fresán por su invitación a escribir este artículo y por sus comentarios perspicaces. También a Riccardo Brasca, Filippo Nuccio y Patrick Massot por los suyos, así como a Martin Liebeck y Raphaël Rouquier por su ayuda. Agradezco igualmente a la comunidad de `mathlib` su entusiasmo al dar la bienvenida a los recién llegados como yo, y el apoyo que brindan de manera tan generosa.

2. Resolubilidad y simplicidad

Recordemos primero los términos que aparecen en el enunciado.

Teorema 1. *Sea $n \geq 5$ un entero. El grupo alternado $\mathfrak{A}_n$ es* simple.

(Para $n \leq 2$, el grupo $\mathfrak{A}_n$ es trivial; para $n = 3$, es cíclico de orden 3; para $n = 4$, es el grupo no abeliano resoluble de orden 12, cuyo subgrupo derivado es abeliano de índice 3.)

En el lenguaje `Lean`, este teorema se formula como en el listado 1.

Listado 1: Simplicidad de los grupos alternados en al menos cinco elementos.

```
theorem alternating_group.normal_subgroups {α : Type*}
  [decidable_eq α] [fintype α]
  (hα : 5 ≤ fintype.card α)
  {N : subgroup (alternating_group α)}
  (hnN : N.normal) (ntN : nontrivial N) : N = ⊤
```

El comando `theorem` inicia el enunciado de un teorema, y lo sigue el nombre que le hemos dado, en este caso `alternating_group.normal_subgroups`, así como una secuencia de argumentos rodeados de varios tipos de paréntesis.

El primero de estos argumentos, α, aparece declarado como *tipo*, la noción de base de la «teoría de tipos dependientes», el lenguaje formal de `Lean`. En este caso, α es un conjunto. El siguiente argumento impone que este conjunto es finito, y `hα` es la hipótesis de que tiene al menos cinco elementos. Los siguientes tres parámetros son `N`, declarado como un subgrupo del grupo alternado en α, `hnN` que impone la condición de que es un subgrupo normal, y `ntN` que pide que sea no trivial (lo que en la biblioteca `mathlib` significa que no se reduce al elemento neutro).

La conclusión del teorema aparece después de los dos puntos: `N = ⊤`, que significa que `N` es todo el grupo alternado. En el código de verdad, a estas cinco líneas de texto les sigue el símbolo `:=` y la *demostración* del enunciado.

Todo objeto de la teoría de tipos tiene un tipo, y lo que hace `Lean` es permitir al usuario escribir nuevos tipos o miembros de esos tipos. En el ejemplo anterior, `N` es un miembro del tipo `subgroup (alternating_group α)`. `Lean` proporciona unas cuantas maneras de escribir nuevos tipos a partir de los antiguos; por ejemplo, si α y β son tipos, hay un tipo α → β que representa «funciones» de α en β, en el sentido de que si `f : α → β` es una función y `a : α` (que se lee «`a` es un miembro del tipo α»), entonces `f a` es un miembro del tipo β, con las reglas evidentes en lo que se refiere a la igualdad. Las funciones de más de un argumento se definen «a la Curry»: por ejemplo, si α, β y γ son tipos, entonces `f : α → β → γ` envía `a : α` a `f a : β → γ`, que envía `b : β` a `f a b : γ`, etc. Incluso la expresión `N = ⊤` del listado 1 representa un tipo, a saber, el tipo de demostraciones de la igualdad entre dos miembros `N` y ⊤ del tipo `subgroup (alternating_group α)`, y el código que hemos omitido construye un miembro de ese tipo, es decir, una demostración del enunciado. La teoría de tipos coloca las estructuras matemáticas y los teoremas en el mismo nivel.

Los grupos simples son aquellos grupos (no triviales) cuyos únicos subgrupos normales son los dos ejemplos obvios: todo el grupo y el subgrupo reducido al elemento neutro $\{e\}$. Cuando un grupo no trivial G no es simple, admite un subgrupo normal H tal que $H \neq \{e\}$ y $H \neq G$. La idea es intentar estudiar G por medio de la proyección al grupo cociente G/H, cuyo núcleo es H. Si nos reducimos al caso de los grupos finitos, una descomposición (*dévissage*) total es posible, y una metáfora corriente presenta los grupos finitos simples como las «partículas elementales» de la teoría de grupos finitos. En esta dirección, un teorema legendario, cuya demostración

hizo intervenir a cientos de matemáticos y cientos de artículos escritos a lo largo de un período de cincuenta años, es la clasificación de los grupos finitos simples. Todos ellos aparecen en una lista de grupos del siguiente tipo:

- El grupo cíclico $\mathbf{Z}/p\mathbf{Z}$ de orden un número primo p.
- El grupo alternado $\mathfrak{A}_n$ para un entero $n \geq 5$.
- Listas de grupos finitos «de tipo Lie», relacionados con el álgebra lineal sobre cuerpos finitos, cuyos ejemplos más sencillos son los grupos lineales especiales proyectivos $\mathrm{PSL}(n, \mathbf{F}_q)$ sobre un cuerpo finito de cardinal q, suponiendo $q \geq 4$ si $n = 2$ ($\mathrm{PSL}(2, \mathbf{F}_2)$ y $\mathrm{PSL}(2, \mathbf{F}_3)$ son isomorfos a $\mathfrak{S}_3$ y $\mathfrak{A}_4$, respectivamente, que no son simples).
- Una lista de 26 grupos «esporádicos», relacionados con geometrías combinatorias excepcionales, como los grupos de Mathieu M_{11}, M_{12}, M_{22}, M_{23} y M_{24}.

Lo más difícil en el trabajo de clasificación es ver que esos son los únicos grupos finitos simples, pero aquí nos contentaremos con la parte fácil: ver que son simples.

Gracias al teorema de Lagrange (el orden de un subgrupo divide al orden del grupo), los únicos subgrupos de un grupo de orden primo son el subgrupo trivial y él mismo. Por tanto, los primeros grupos de la lista son simples.

Señalemos también que el centro $Z(G)$ de un grupo G, es decir, el conjunto de elementos $g \in G$ que conmutan con cualquier otro elemento de G, es un subgrupo normal. Por tanto, si G es simple, entonces o bien $Z(G) = G$, en cuyo caso G es abeliano, luego cíclico de orden primo, o bien $Z(G) = \{e\}$. Esto explica por qué, a partir del segundo ítem, todos los grupos de la lista tienen centro trivial.

En segunda posición aparecen los grupos alternados, el tema de esta nota, cuya simplicidad normalmente se demuestra en las clases de álgebra al estudiar la teoría de Galois y la resolubilidad de ecuaciones algebraicas en una variable. Mientras que Abel y Ruffini habían demostrado que una ecuación algebraica general de grado ≥ 5 no se puede resolver por radicales, el teorema de Galois refina ese resultado demostrando que una ecuación algebraica es resoluble por radicales si y solo si su grupo de Galois es resoluble. La noción de grupo de una ecuación fue introducida por Galois, así como la de subgrupo normal y de grupo resoluble, aunque él no tenía un nombre para esos conceptos: el grupo de Galois es el subgrupo de las permutaciones de las raíces que preservan todas las relaciones algebraicas con coeficientes racionales; y un grupo finito G es resoluble si es trivial o, por inducción, admite un subgrupo normal no trivial H que es él mismo resoluble y tal que el grupo cociente G/H sea abeliano. En términos modernos, decimos que un grupo G es resoluble si su «serie derivada» $G, D(G), D(D(G)) \ldots$, la sucesión decreciente de los subgrupos que se obtienen tomando sucesivamente conmutadores, termina en el subgrupo trivial.

Desde este punto de vista, el teorema de Abel-Ruffini se reduce al enunciado de que una ecuación general de grado n tiene como grupo de Galois el grupo simétrico $\mathfrak{S}_n$ y que, para todo $n \geq 5$, este grupo no es resoluble, lo cual es consecuencia del siguiente resultado más preciso.

Proposición 1. *Sea $n \geq 5$ un entero. El subgrupo de conmutadores de $\mathfrak{S}_n$ es el grupo alternado $\mathfrak{A}_n$. El subgrupo de conmutadores del grupo alternado $\mathfrak{A}_n$ es $\mathfrak{A}_n$.*

Demostración. Todo conmutador tiene signatura 1, de modo que $D(\mathfrak{S}_n) \subseteq \mathfrak{A}_n$. Por otra parte, el conmutador de dos transposiciones $(a\,b)$ y $(c\,d)$ es trivial si son iguales o tienen soportes disjuntos, pero, si no, es igual al 3-ciclo

$$(a\,b)(c\,a)(a\,b)(c\,a) = (a\,b\,c).$$

Así vemos que todo 3-ciclo se puede escribir como un conmutador, de modo que el subgrupo $D(\mathfrak{S}_n)$ contiene todos los 3-ciclos, que se sabe que generan el grupo alternado $\mathfrak{A}_n$. (Este argumento funciona para $n \geq 3$.)

Para demostrar que $D(\mathfrak{A}_n)$ es todo $\mathfrak{A}_n$, veamos que el cociente $K = \mathfrak{A}_n/D(\mathfrak{A}_n)$ es el grupo trivial. El grupo $\mathfrak{A}_n$ está generado por 3-ciclos g, cuyas imágenes generan K. La hipótesis $n \geq 5$ implica que todos los 3-ciclos son conjugados en $\mathfrak{A}_n$; por tanto, todos tienen la misma imagen k en K y $K = \langle k \rangle$. Puesto que el cuadrado de un 3-ciclo $g = (a\,b\,c)$ es de nuevo un 3-ciclo, a saber $g^2 = (a\,c\,b)$, se tiene $k = k^2$, luego $k = e$ y $K = \{e\}$. □

La relación con la simplicidad proviene del hecho de que un grupo resoluble no abeliano no puede ser simple. En efecto, los conmutadores forman un subgrupo normal de G; si G es simple, o bien $D(G) = \{e\}$, lo cual quiere decir que G no es abeliano, o bien $D(G) = G$. Así que el teorema de Galois sobre las ecuaciones algebraicas de orden ≥ 5 suele englobarse en el enunciado de que el grupo alternado $\mathfrak{A}_n$ es simple para $n \geq 5$, aunque en realidad basta con el resultado más sencillo de la proposición 1.

A veces se dice que Galois demostró su teorema de simplicidad, pero el único enunciado explícito que he conseguido encontrar en sus obras es el hecho de que el orden más pequeño de un grupo finito simple (él dice «indescomponible») no abeliano es $5 \cdot 4 \cdot 3$, sin decir que corresponde al grupo alternado $\mathfrak{A}_5$. Por otra parte, los teóricos de grupos del siglo XIX, desde Lagrange y Ruffini hasta Jordan, fueron gradualmente desarrollando las herramientas necesarias para entender el teorema de Galois en términos de la simplicidad del grupo alternado.

Hay muchas demostraciones relativamente sencillas de la simplicidad de $\mathfrak{A}_n$ para $n \geq 5$, por ejemplo la que da Jacobson en [10, p. 247], pero ninguna de ellas me parece totalmente evidente, en el sentido de explicar *por qué* funciona. Además, algunas de ellas requieren distinguir casos o hacer razonamientos mentales que, a pesar de ser familiares para nosotros, pueden resultar engorrosos cuando intentamos escribirlos explícitamente, hasta el punto de que no estoy seguro de que nuestras explicaciones sean suficientes para los estudiantes.

Mi idea inicial era encontrar una demostración de naturaleza un poco más sistemática, que usara argumentos más propicios a ser generalizados. El principio de esa demostración, como ya se indica en el libro de Wilson [20], es el criterio de Iwasawa que explico a continuación.

3. El criterio de simplicidad de Iwasawa

Iwasawa [9] propuso en 1941 una demostración de la simplicidad del grupo lineal especial proyectivo $\mathrm{PSL}(n, F)$ de un cuerpo F de cardinal al menos 4. Anteriormente,

el teorema solo se conocía en el caso de cuerpos finitos (Dickson) o de cuerpos de característica distinta de 2 (van der Waerden). De su demostración se puede extraer el siguiente criterio geométrico:

Teorema 2. *Sea G un grupo actuando sobre un conjunto X. Supongamos dado, para cada elemento $x \in X$, un subgrupo $T(x)$ de G, de modo que se cumplan las siguientes propiedades:*

- *Para cada $x \in X$, el grupo $T(x)$ es abeliano.*
- *Para cada $g \in G$ y cada $x \in X$, se tiene $T(g \cdot x) = gT(x)g^{-1}$.*
- *Los grupos $T(x)$ generan G.*

Si, además, la acción de G sobre X es cuasiprimitiva*, entonces cualquier subgrupo normal N de G que no actúe trivialmente sobre X contiene al subgrupo de conmutadores $D(G)$ de G.*

Se dice que una acción de un grupo G sobre un conjunto X es *cuasiprimitiva* si cualquier subgrupo normal H de G que no actúe trivialmente sobre X actúa transitivamente: para todo $x, x' \in X$, existe $h \in H$ tal que $h \cdot x = x'$. Esta propiedad que hoy en día nos puede resultar oscura aparece naturalmente en el marco de las acciones *primitivas*, uno de los temas clásicos de la teoría de grupos del siglo XIX, que sigue siendo muy importante en el estudio de los grupos finitos, pero que por alguna razón parece haber desaparecido del paquete de álgebra que ofrecemos a nuestros estudiantes de grado. Definámosla en términos de particiones de X (es decir, de conjuntos de subconjuntos disjuntos no vacíos de X cuya unión cubre todo X).

Definición 1. *Una acción transitiva de un grupo G sobre un conjunto X es* primitiva *si hay exactamente dos particiones de X que son invariantes bajo G: la partición grosera $\{X\}$ y la partición discreta dada por todos los subconjuntos de un elemento.*

La definición implica, en particular, que X tiene al menos dos elementos.

Si H es un subgrupo normal de G, la partición de X en órbitas bajo la acción de H es una partición invariante; por tanto, si la acción sobre X es primitiva, H tiene que actuar o bien trivialmente o bien transitivamente. Vemos así que las acciones primitivas son cuasiprimitivas.

Las condiciones de transitividad superior proporcionan ejemplos importantes de acciones primitivas.

Lema 1. *Supongamos que la acción de G es doblemente transitiva, es decir, X contiene al menos dos elementos y dados dos pares (x, y) y (x', y') de elementos distintos de X, existe $g \in G$ tal que $g \cdot x = x'$ y $g \cdot y = y'$. Entonces la acción es primitiva.*

La demostración es elemental. Consideremos un conjunto B de una partición Σ de X invariante bajo la acción de G, supongamos que B contiene al menos dos elementos x, y, y demostremos que $B = X$. La conclusión es obvia si X tiene solo dos elementos. Si no, sea $z \in X$ un elemento distinto de x e y. Aplicada a los pares (x, y) y (x, z), la hipótesis de doble transitividad implica que existe $g \in G$ tal que $g \cdot x = x$ y $g \cdot y = z$. El conjunto $g \cdot B$ pertenece a Σ pero tiene un elemento en común

con B, a saber x, de modo que $g \cdot B = B$. En particular, $z \in B$, lo cual demuestra la igualdad $B = X$.

Acabamos de observar que los miembros de una partición G-invariante son subconjuntos B de X con la propiedad de que, o bien $g \cdot B \cap B = \emptyset$, o bien $g \cdot B = B$; en la terminología tradicional de la teoría de grupos, se llaman *bloques*, y los bloques distintos de X y con al menos dos elementos se llaman *bloques de imprimitividad*. Recíprocamente, si B es un bloque no vacío y la acción es transitiva, entonces el conjunto de todos los $g \cdot B$, con $g \in G$, es una partición G-invariante de X.

Como ejemplo de una acción transitiva que no es primitiva, se puede considerar la acción de $\mathfrak{S}_4$ sobre el conjunto de pares de elementos de $\{1, 2, 3, 4\}$. En este caso, existen bloques no triviales, tales como $B = \{\{1, 2\}, \{3, 4\}\}$. Más adelante tendremos que analizar este ejemplo y algunas de sus variantes.

La terminología «primitiva» viene de Galois, en el lenguaje de las ecuaciones: como explica Neumann en [15, p. 390], cuando el grupo de Galois G de una ecuación polinomial irreductible $f(x) = 0$ actúa sobre sus raíces, hay m bloques de tamaño n si y solo si existe una ecuación auxiliar de grado m tal que la adjunción de una de sus raíces permite factorizar f como $f_1 f_2$, con f_1 de grado n.

Las definiciones en `Lean` siguen estas descripciones (véase el listado 2), con algunos ajustes para acomodarse a las convenciones generales de `mathlib`.

Listado 2: Bloques, acciones primitivas.

```
variables (G : Type*) {X : Type*} [has_smul G X]

/-- A trivial block is a subsingleton or ⊤ (it is not necessarily a
    ...block)-/
def is_trivial_block (B : set X) := B.subsingleton ∨ B = ⊤

/-- A block is a set which is either fixed or moved to a disjoint
    subset -/
def is_block (B : set X) := (set.range (λ g : G, g ·
    B)).pairwise_disjoint id

/-- An action is preprimitive if it is pretransitive and
the only blocks are the trivial ones -/
class is_preprimitive
extends is_pretransitive G X : Prop :=
(has_trivial_blocks' : ∀ {B : set X}, (is_block G B) →
    is_trivial_block B)
```

En primer lugar, las definiciones se dan siempre bajo mínimas hipótesis, con la idea de que puedan servir en contextos más generales, evitando así la necesidad de infinitas variaciones de demostraciones que si no serían idénticas. Otra razón para adoptar definiciones lo más generales posible es que cambiarlas más adelante requiere ajustar todos los teoremas que las utilizan, una tarea larga y dolorosa. En nuestro caso, una «acción» de un tipo `G` sobre otro tipo `X` se define simplemente como una aplicación `G → X → X`, incorporada en el predicado `has_smul G X` y designada por

el símbolo $\cdot$, ¡sin ni siquiera pedir que G tenga una estructura multiplicativa interna! Esto recuerda a los «grupos con operadores» introducidos por Bourbaki en el primer capítulo de [1] con intenciones similares.

Un «subconjunto» `B` de `X` (algo llamado `set X`) es un bloque si y solo si los conjuntos `g` $\cdot$ `B`, para `g` en `X`, son dos a dos iguales o disjuntos. Esta (posiblemente) oscura definición utiliza el predicado general `set.pairwise_disjoint` de `mathlib`.

Los bloques triviales se detectan con el predicado `is_trivial_block`, que se define como «subsingletons» (el conjunto vacío o un conjunto de un elemento, con la definición «$\forall x, y \in B,\ x = y$») o el conjunto total $\top$.

Otra de las idiosincrasias de `mathlib` que aparece en las definiciones anteriores es el concepto de acción «pretransitiva», que significa «transitiva pero puede que vacía». Una vez más, la idea es imponer las hipótesis de no vacuidad solo en aquellas afirmaciones que realmente las necesiten de manera explícita. Por lo tanto, definimos una acción como `preprimitiva` si es pretransitiva y si todos los bloques son triviales.

En lo que sigue, será importante utilizar una caracterización equivalente de las acciones primitivas. (Recordemos que el estabilizador G_x de un elemento x de X es el subgrupo de G formado por todos los $g \in G$ tales que $g \cdot x = x$.)

Lema 2. *La acción de G sobre X es primitiva si y solo si es transitiva y, para todo $x \in X$, el estabilizador G_x es un subgrupo maximal*[1] *de G.*

De forma más general, se puede demostrar que, para todo $x \in X$, la aplicación $H \mapsto H \cdot x$ induce una biyección que preserva el orden entre el retículo de subgrupos H de G tales que $G_x \subseteq H \subset G$ y el retículo de bloques B de X que contienen a x. Hemos copiado en el listado 3 la definición en `Lean` de esta biyección que preserva el orden (de hecho, su inversa): toma la forma de una «equivalencia de orden» de tipos, como indican los símbolos `≃o`.

Listado 3: Equivalencia de orden entre los bloques que contienen un punto y los subgrupos que contienen su estabilizador.

```
variables {G: Type*} [group G] {X : Type*} [mul_action G X]
/-- Order equivalence between blocks in X containing a point a
 and subgroups of G containing the stabilizer of a
 (Wielandt, Finite Permutation Groups, th. 7.5)-/
def stabilizer_block_equiv [htGX : is_pretransitive G X] (a : X) :
  { B : set X // a ∈ B ∧ is_block G B } ≃o set.Ici (stabilizer G a) :=
    {
to_fun := λ ⟨B, ha, hB⟩, ⟨stabilizer G B, stabilizer_of_block hB ha⟩,
inv_fun := λ ⟨H, hH⟩, ⟨mul_action.orbit H a,
  mul_action.mem_orbit_self a, is_block_of_suborbit hH⟩,
left_inv := ...,
right_inv := ...,
map_rel_iff' := ...,
end }
```

[1] Recordemos que un subgrupo H de G es maximal si $H \neq G$ y todo subgrupo H' de G que contenga a H es o bien H o bien G.

El primer tipo, `{ B : set X // a ∈ B ∧ is_block G B }`, es el tipo de todos los `B : set X` (básicamente, subconjuntos de `X`) que satisfacen las propiedades `a ∈ B` e `is_block G B`, en las que este último tipo expresa que `B` es un bloque de la acción de `G` sobre `X` (lo cual podría también dejarse implícito, teniendo en cuenta que, al ser `B` miembro de `conjunto X`, se conoce su tipo). `Lean` es capaz de deducir él solo que este tipo hereda la relación de orden dada por la inclusión en `conjunto X`. El segundo tipo, `set.Ici (stabilizer G a)`, designa, en el retículo `subgroup G`, el subconjunto de los subgrupos que contienen `stabilizer G a`. Esta «equivalencia de orden» consta de dos funciones, `to_fun` y `inv_fun`, de demostraciones (`left_inv` y `right_inv`) de que son inversas entre sí, y de una demostración (`map_rel_iff`) de que respetan el orden.

A continuación, se presenta la definición de la función `to_fun`, que manda `B`, junto a los «testigos» `ha : a ∈ B` y `hB : is_block G B`, a `stabilizer G B`, acompañado de `stabilizer_of_block hB ha`. Como uno puede imaginarse, el primero representa al estabilizador de `B` en `G`, junto con la información adicional de que contiene `stabilizer G a`. Este dato lo proporciona la función `stabilizer_of_block : is_block G B → a ∈ B → stabilizer G a ≤ stabilizer G B`, cuyo código, por supuesto, se había dado anteriormente a la fuente. La función inversa `inv_fun` manda `H : subgroup G` junto con `hH : stablizer G a ≤ H` a `mul_action.orbit H a`, que representa la órbita de `a` bajo la acción del subgrupo `H`, junto con las demostraciones relevantes de que este conjunto contiene a `a` y es un bloque. Después vienen tres demostraciones `left_inv` y `right_inv`, que afirman que las dos funciones anteriores son inversas entre sí, y `map_rel_iff`, que dice que respetan la relación de orden. En el listado 3, hemos sustituido estas tres demostraciones por `...`; los códigos de las dos primeras tienen 2 líneas de longitud, y el de la tercera, 17 líneas.

3.1. Demostración del criterio de Iwasawa

Terminemos esta sección con una prueba del criterio de Iwasawa (teorema 2).

Fijemos un elemento $a \in X$, y empecemos demostrando que el subgrupo $\langle N, T(a)\rangle$ generado por N y $T(a)$ es igual a G. La hipótesis es que N actúa transitivamente sobre X. Como N es normal, que la acción sea cuasiprimitiva implica que, para todo $b \in X$, existe $n \in N$ tal que $n \cdot a = b$. Puesto que $nT(a)n^{-1} = T(b)$, esto implica que $\langle N, T(a)\rangle$ contiene $T(b)$. Como b es arbitrario, el subgrupo $\langle N, T(a)\rangle$ contiene al subgrupo generado por todos los $T(x)$, para $x \in X$, que es igual a G.

El subgrupo N es normal; la conclusión de que contiene al subgrupo derivado de G es equivalente a la conmutatividad del cociente G/N. Puesto que $\langle N, T(a)\rangle = G$, la composición $T(a) \to G \to G/N$ es sobreyectiva; como $T(a)$ es abeliano, deducimos que G/N es abeliano, como queríamos demostrar.

4. Subgrupos normales de los grupos simétricos y alternados

En esta sección, consideramos un entero n, que supondremos casi siempre mayor o igual que 5.

El grupo simétrico $\mathfrak{S}_n$ no solo actúa en el conjunto $X = \{1, \ldots, n\}$, sino también en los conjuntos $X^{[k]}$ de subconjuntos de k elementos de X, para todo entero k entre 0 y n. Esta acción es trivial si $k = 0$ o $k = n$, dado que entonces $X^{[k]}$ contiene un único elemento, pero es fiel si $0 < k < n$: el único elemento que actúa trivialmente sobre $X^{[k]}$ es $g = e$. La proposición siguiente afirma que esta acción es además primitiva, salvo si $n = 2k$.

Proposición 2. *Sean k y n enteros tales que $0 < k < n - k < n$. Si $n \geq 4$, las acciones de $\mathfrak{A}_n$ y de $\mathfrak{S}_n$ sobre $X^{[k]}$ son primitivas.*

Gracias a este resultado, el enfoque de Iwasawa nos permite entender los subgrupos normales de los grupos simétricos y alternados. Solo necesitaremos los casos $k = 2$, $k = 3$ y $k = 4$.

4.1. Consideremos primero el caso $k = 2$. Dado un subconjunto $x = \{a, b\}$ de dos elementos de X, sea $T(x)$ el subgrupo abeliano de orden 2 generado por la trasposición $(a\,b)$. La igualdad $(g \cdot a\, g \cdot b) = g(a\,b)g^{-1}$ implica que estos subgrupos satisfacen la relación $T(g \cdot x) = gT(x)g^{-1}$, y como las trasposiciones generan $\mathfrak{S}_n$, también lo hacen los subgrupos $T(x)$. Por tanto, el criterio de Iwasawa implica que si esta acción es primitiva, entonces cualquier subgrupo normal N de $\mathfrak{S}_n$ tal que $N \neq \{e\}$ contiene a $D(\mathfrak{S}_n)$, que como hemos visto, es igual a $\mathfrak{A}_n$. Como $\mathfrak{S}_n/\mathfrak{A}_n$ es de orden 2, los únicos subgrupos de $\mathfrak{S}_n$ que contienen a $\mathfrak{A}_n$ son $\mathfrak{A}_n$ y $\mathfrak{S}_n$.

¿Qué ocurre con la hipótesis de que esta acción es primitiva? Observemos que la acción de $\mathfrak{S}_n$ sobre $X^{[2]}$ no es doblemente transitiva, ya que no se pueden enviar $\{1, 2\}$ y $\{1, 3\}$ a los conjuntos $\{1, 2\}$ y $\{3, 4\}$. Sin embargo, es primitiva, y es aquí donde usamos que $2 < n - 2$, es decir, $n > 4$. Wilson [20, § 2.5.1] demuestra que el estabilizador de cualquier elemento de $X^{[2]}$ es un subgrupo maximal, como explicaremos con mayor generalidad en la sección siguiente, pero se puede también dar una demostración directa, como me explicó G. Chenevier.

Sea B un bloque de imprimitividad de $X^{[2]}$, y sea $\{a, b\}$ un elemento de B.

Supongamos primero que B contiene otro par de la forma $\{a, c\}$. Consideremos $g \in G$ tal que $g \cdot a = c$ y $g \cdot b = a$. Entonces B y $g \cdot B$ comparten el elemento $\{a, c\}$, y por tanto $g \cdot B = B$; se sigue que B contiene el par $\{g \cdot a, g \cdot c\} = \{c, g \cdot c\}$, luego todos los pares de la forma $\{c, d\}$. Repitiendo el argumento para $\{a, c\}$ y $\{c, d\}$, se deduce que B contiene todos los pares, de modo que $B = X^{[2]}$.

Supongamos ahora que B contiene un par $\{c, d\}$ disjunto de $\{a, b\}$. Como $n \geq 5$, existe un quinto elemento e en X; demostremos que $\{c, e\} \in B$. En efecto, existe $g \in \mathfrak{S}_n$ que envía a a a, b a b, c a c y d a e, luego $\{a, b\}$ a sí mismo, y $\{c, d\}$ a $\{c, e\}$. Entonces B y $g \cdot B$ tienen $\{a, b\}$ en común, así que $g \cdot B = B$ y $\{c, e\} \in B$. En particular, B contiene dos pares $\{c, d\}$ y $\{c, e\}$ cuyos soportes no son disjuntos, y la primera parte del argumento implica que $B = X^{[2]}$.

Obtenemos así el siguiente resultado (también consecuencia del teorema 1).

Proposición 3. *Para $n \geq 5$, los subgrupos normales de $\mathfrak{S}_n$ son $\{e\}$, $\mathfrak{A}_n$ y $\mathfrak{S}_n$.*

4.2. Pasemos ahora al caso $k = 3$. Dado un subconjunto $x = \{a, b, c\}$ de tres elementos de X, sea $T(x)$ el grupo alternado en esos tres elementos, visto como

subgrupo de $\mathfrak{A}_n$, es decir, el subgrupo generado por el 3-ciclo $(a\,b\,c)$. Como antes, se cumplen las relaciones $T(g \cdot x) = gT(x)g^{-1}$, y estos subgrupos generan el grupo alternado. Suponiendo que la acción de $\mathfrak{A}_n$ sobre $X^{[3]}$ sea primitiva, deducimos del criterio de Iwasawa que todo subgrupo normal de $\mathfrak{A}_n$ o bien es trivial o bien contiene $D(\mathfrak{A}_n)$; dicho de otro modo, que $\mathfrak{A}_n$ es un grupo simple.

Como veremos en la sección siguiente, la acción es primitiva para todo $n \neq 6$, pero no para $n = 6$ (y explicaremos por qué), de modo que en ese caso se necesita otro argumento.

4.3. Este argumento adicional utiliza el caso $k = 4$. Dado un subconjunto $x = \{a, b, c, d\}$ de cuatro elementos de X, sea $V(x)$ el *Vierergruppe* de Klein en el subgrupo alternado en esos cuatro elementos, visto como subgrupo de $\mathfrak{A}_n$. Es abeliano de orden 4, formado por la identidad y las tres «trasposiciones dobles» $(a\,b)(c\,d)$, $(a\,c)(b\,d)$ y $(a\,d)(b\,c)$. Se trata ya de una definición intrínseca de $V(x)$ (permutaciones con soporte en x con tipo de ciclo vacío o $(2, 2)$), pero también se puede definir como el subgrupo derivado del grupo alternado en esos cuatro elementos. Por consiguiente, se cumplen las relaciones $V(g \cdot x) = gV(x)g^{-1}$. Veamos que los subgrupos $V(x)$ generan $\mathfrak{A}_n$; el argumento usará la condición $n \geq 5$. Partimos de la observación de que $\mathfrak{A}_n$ consiste en las permutaciones que son producto de un número par de trasposiciones. Dos trasposiciones sucesivas en un tal producto con soportes disjuntos pertenecen a uno de los $V(x)$. Si no, sus soportes comparten un elemento a, pongamos $(a\,b)(a\,c)$, así que usando que $n \geq 5$, podemos insertar un producto identidad $(d\,e)(d\,e)$ para que $(a\,b)(d\,e)$ y $(d\,e)(a\,c)$ pertenezcan a uno de los subgrupos de la forma $V(x)$.

Aplicando el criterio de Iwasawa, esta construcción muestra que el grupo alternado $\mathfrak{A}_n$ es simple, suponiendo que la acción de $\mathfrak{A}_n$ sobre $X^{[4]}$ sea primitiva.

4.4. Indiquemos antes de cerrar esta sección que una variante de estos argumentos conduce a una demostración razonablemente sencilla de la simplicidad de $\mathfrak{A}_5$. En efecto, tomando complementarios, las acciones de $\mathfrak{A}_n$ sobre $X^{[k]}$ y sobre $X^{[n-k]}$ son isomorfas. Para $n = 5$, el caso $k = 4$ se reduce al caso $k = 1$, y basta con demostrar que la acción de $\mathfrak{A}_5$ sobre X es primitiva, para lo cual es suficiente con observar que es doblemente (incluso triplemente) transitiva.

5. Primitividad y subgrupos maximales

Para terminar la prueba del teorema 1, nos falta demostrar la proposición 2. El estabilizador de un elemento $\{1, \ldots, k\}$ de $X^{[k]}$ es la intersección de $\mathfrak{A}_n$ con el subgrupo $\mathfrak{S}_k \times \mathfrak{S}_{n-k}$ asociado a la partición de $\{1, \ldots, n\}$ en los subconjuntos $\{1, \ldots, k\}$ y $\{k + 1, \ldots, n\}$. Como la acción de $\mathfrak{A}_n$ sobre $X^{[k]}$ es transitiva, gracias al lema 2 podemos reducirnos a demostrar que este subgrupo de $\mathfrak{A}_n$ es maximal.

Se ve así que la hipótesis $n \neq 2k$ es realmente necesaria para la proposición: el subgrupo $\mathfrak{S}_n \times \mathfrak{S}_n$ de $\mathfrak{S}_{2n}$ no es maximal, puesto que es un subgrupo de índice 2 del estabilizador de la partición $\{\{1, \ldots, n\}, \{n+1, \ldots, 2n\}\}$, un grupo que también puede describirse como el producto trenzado $\mathfrak{S}_n \wr (\mathbf{Z}/2\mathbf{Z})$.

5.1. En el apartado 4.1, vimos una demostración elemental de la proposición 2 en el caso $k = 2$ y $n \geq 5$, y parece probable que una demostración elemental exista para todo k. R. Rouquier me dio una que funciona para $k = 3$ y $n \geq 7$. Sin embargo, quisiera presentar un enfoque distinto, que me explicó M. Liebeck, y que a mi juicio realza el estatus de esa proposición en la teoría de grupos finitos.

Uno de los primeros tratados sobre teoría de grupos es el de Jordan de 1870 [11]. Por aquel entonces, los grupos eran «grupos de permutaciones», que permutaban letras (y, por ende, expresiones algebraicas en estas letras) o raíces de una ecuación polinomial, puesto que los vínculos con la teoría de Galois eran explícitos.

Se había observado que el grupo simétrico en n letras es n veces transitivo, casi por definición. Dados dos sistemas de elementos distintos $x_1, \ldots, x_n$ e $y_1, \ldots, y_n$ de $\{1, \ldots, n\}$, existe una permutación g tal que $g \cdot x_i = y_i$ para todo i, y g es única.

Prácticamente igual de obvio era el hecho de que el grupo alternado en n letras es $n-2$ veces transitivo: dados elementos distintos $x_1, \ldots, x_{n-2}$ e $y_1, \ldots, y_{n-2}$, existen exactamente dos permutaciones g y g' tales que $g \cdot x_i = g' \cdot x_i = y_i$ para todo i, y $g'g^{-1}$ es la permutación que intercambia los dos elementos de $\{1, \ldots, n\}$ que no están en $\{y_1, \ldots, y_{n-2}\}$; en particular, una de ellas es par, y la otra, impar.

También se había observado que, más allá de estos dos casos, un subgrupo de permutación en n letras tiene que actuar de manera mucho menos transitiva, y los matemáticos del siglo XIX demostraron muchos teoremas que buscaban cuantificar este límite. Por ejemplo, Mathieu demostró que, salvo que contenga al grupo alternado, un subgrupo de $\mathfrak{S}_n$ no es $n/2$ veces transitivo, mientras que Jordan [12] demostró que no es m veces transitivo si $n - m$ es un número primo mayor que 2.

Como explica Cameron en [2], una vez que se lograron clasificar los grupos finitos simples, se pudo comprobar examinando la lista que un subgrupo 6 veces transitivo de $\mathfrak{S}_n$ debe ser simétrico o alternado.

Un problema paralelo a la clasificación es el de entender los subgrupos *maximales* de un grupo simple finito dado. En el caso del grupo alternado, M. O'Nan y L. Scott han obtenido una lista explícita de forma independiente. Como indica Cameron [2], esta pregunta está estrechamente relacionada con la descripción de todos los subgrupos del grupo simétrico $\mathfrak{S}_n$ que actúan primitivamente sobre $\{1, \ldots, n\}$.

El enunciado de este teorema de clasificación dice que todo subgrupo estricto de $\mathfrak{A}_n$ o de $\mathfrak{S}_n$ es conjugado a un subgrupo de uno de seis tipos, de los cuales los tres primeros son de la forma:

(a) Un producto $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$, donde $0 < m < n$ — el caso *intransitivo*.

(b) Un «producto trenzado» $\mathfrak{S}_m \wr \mathfrak{S}_p$, donde $n = pm$, es decir, el subgrupo generado por el producto de p grupos simétricos, que actúan sobre p conjuntos disjuntos de m letras (isomorfo a $\mathfrak{S}_m \times \cdots \times \mathfrak{S}_m$), y una permutación que permuta cíclicamente estos p conjuntos — el caso *imprimitivo*.

(c) Un grupo *afín* de un espacio vectorial $\mathbf{F}_p$ de dimensión d, donde $n = p^d$ es una potencia de un número primo.

La clasificación se aplica en particular a los subgrupos maximales, y Leibeck *et al.* [14] establecieron la afirmación recíproca, decidiendo cuáles de los grupos de esta

lista son maximales. El caso (a) es maximal cuando $m \neq n-m$, que es exactamente la situación de la proposición 2. Sin embargo, cuando $n = 2m$, el subgrupo (a) no es maximal, pero el caso (b) proporciona el subgrupo maximal correspondiente. Por ejemplo, para $n = 4$, el subgrupo dado por (b) tiene orden 8 y es, por tanto, un 2-subgrupo de Sylow de $\mathfrak{S}_4$, mientras que el subgrupo $\mathfrak{S}_2 \times \mathfrak{S}_2$ tiene orden 4.

Los casos de la forma (c) fueron de un interés particular para Galois, que demostró que aparecen como grupos de Galois de ecuaciones irreducibles de grado primo que son resolubles por radicales. En otras palabras, los subgrupos resolubles y transitivos de $\mathfrak{S}_p$ pueden ser vistos, después de conjugación, como grupos de permutaciones de la forma $x \mapsto ax+b$ en $\mathbf{F}_p$, donde $a \in \mathbf{F}_p^\times$ y $b \in \mathbf{F}_p$. Dado que la identidad es la única permutación de esa forma que fija dos elementos, Galois obtiene que una ecuación irreducible de grado primo es resoluble por radicales si y solo si cualquiera de sus raíces puede ser expresada racionalmente en términos de cualquier par de ellas.

Galois también definió ecuaciones algebraicas primitivas que corresponden exactamente al caso en el que el grupo de Galois actúa de manera primitiva sobre sus raíces. En el caso resoluble, demostró que el grado debe ser una potencia p^n de un número primo p y, eligiendo una enumeración del espacio vectorial $\mathbf{F}_p^n$, el grupo de Galois G es un subgrupo del grupo de permutaciones de la forma $x \mapsto Ax+b$, donde $A \in \mathrm{GL}(n, \mathbf{F}_p)$ y $b \in \mathbf{F}_p^n$, que contiene todas las traslaciones $x \mapsto x + b$. Además, el subgrupo G_0 de $\mathrm{GL}(n, \mathbf{F}_p)$ que consiste en todos los elementos de G de la forma $x \mapsto Ax$ no tiene ningún subespacio invariante no trivial. El capítulo 14 del libro de Cox [3] da más detalles sobre esta fascinante historia.

5.2. Pero volvamos a la demostración de la proposición 2. Sea G un subgrupo de $\mathfrak{A}_n$ que contiene estrictamente a $(\mathfrak{S}_k \times \mathfrak{S}_{n-k}) \cap \mathfrak{A}_n$, donde $0 < k < n$ y $n \neq 2k$. Queremos demostrar que G coincide con $\mathfrak{A}_n$. Por simetría, podemos suponer que $k < n - k$. El caso $k = 1$ es fácil. De hecho, la acción de $\mathfrak{A}_n$ sobre $\{1, \ldots, n\}$ es $n-2$ veces transitiva, luego doblemente transitiva puesto que $n \geq 4$, y por tanto primitiva. Ahora supongamos que $k \geq 2$, lo que implica $n \geq 5$.

Un teorema de Jordan [11, Nota C en § 398, p. 664] afirma que un subgrupo primitivo de $\mathfrak{S}_n$ que contiene un ciclo de orden primo p es al menos $n-p+1$ veces transitivo. Para $p = 2$, obtenemos que este subgrupo es $n-1$ veces transitivo, así que tiene que ser todo $\mathfrak{S}_n$, mientras que para $p = 3$ es $n-2$ veces transitivo, y no es demasiado difícil deducir que contiene a $\mathfrak{A}_n$. Dado que $1 \leq k < n-k < n$ y $n \geq 5$, tenemos $n - k \geq 3$, y nuestro subgrupo G contiene un ciclo de longitud 3. Para concluir, falta por establecer que actúa primitivamente sobre $\{1, \ldots, n\}$.

Se demuestra primero que G actúa transitivamente sobre $\{1, \ldots, n\}$. De hecho, G contiene los subgrupos $\mathfrak{S}_k$ y $\mathfrak{S}_{n-k}$; en particular, actúa transitivamente sobre los elementos de cada uno de los subconjuntos $\{1, \ldots, k\}$ y $\{k+1, \ldots, n\}$, así que tiene como máximo dos órbitas. Pero dado que contiene estrictamente a $(\mathfrak{S}_k \times \mathfrak{S}_{n-k}) \cap \mathfrak{A}_n$, no puede dejar $\{1, \ldots, k\}$ y $\{k+1, \ldots, n\}$ invariantes.

Razonando como en la prueba de la transitividad, G actúa k veces transitivamente sobre $\{1, \ldots, k\}$ y $n-k$ veces transitivamente sobre $\{k+1, \ldots, n\}$; dado que $2 \leq k < n-k$, actúa en particular doblemente transitivamente, luego primitivamente, sobre ambos conjuntos.

Consideremos ahora bloques de imprimitividad B para la acción de G, suponiendo que tengan al menos dos elementos y sean distintos de $\{1,\dots,n\}$.

Primero observamos que B no puede contener a $\{k+1,\dots,n\}$, porque sus traslaciones $g\cdot B$, para $g\in B$ tal que $g\cdot B\neq B$, tendrían que estar contenidas en $\{1,\dots,k\}$, lo cual es imposible ya que $k<n-k$. En particular, B interseca a $\{k+1,\dots,n\}$ en como máximo un elemento. Si es disjunto de $\{k+1,\dots,n\}$, entonces está contenido en $\{1,\dots,k\}$. Dado que G actúa primitivamente sobre $\{1,\dots,k\}$, se tiene $B=\{1,\dots,k\}$. Consideremos un elemento g de G que no estabilice $\{1,\dots,k\}$. En ese caso, $g\cdot B$ es un bloque distinto de B, luego disjunto de él, de modo que $g\cdot B$ es un bloque contenido en $\{k+1,\dots,n\}$. Por primitividad, $g\cdot B=\{k+1,\dots,n\}$, lo cual contradice el comienzo de la demostración.

En particular, existen elementos $a\in\{1,\dots,k\}\cap B$ y $b\in\{k+1,\dots,n\}\cap B$. Para concluir la demostración por contradicción, basta con probar que B contiene a $\{k+1,\dots,n\}$. Para ello, sea $c\in\{k+1,\dots,n\}$ y consideremos un elemento $g\in G$ que fije $\{1,\dots,k\}$ y tal que $g\cdot b=c$. Entonces, tanto $g\cdot B$ como B contienen a a, luego $g\cdot B=B$ y $c\in B$, como queríamos demostrar.

6. Intermezzo: clases de conjugación del grupo simétrico

Al final, la demostración de la simplicidad del grupo alternado $\mathfrak{A}_6$ necesita de un análisis del subgrupo de Klein de $\mathfrak{A}_4$. Cuando hablamos de este grupo entre colegas, o incluso en clase, el hecho de que sea un subgrupo normalmente se evacúa con un simple «se comprueba que…». Por supuesto, a un ordenador no le basta este argumento, y pasé algún tiempo intentando decidir cuál era la mejor manera de demostrar enunciados de este tipo en un ordenador. La demostración a la que recurrí resultó ser entretenida, aunque algo sofisticada.

Sea $X=\{a,b,c,d\}$ un conjunto de 4 elementos, y sea V el subconjunto de $\mathfrak{S}_X$ formado por la identidad y todas las trasposiciones dobles. Para ver que V es un subgrupo de $\mathfrak{S}_X$, demuestro que V es el único 2-subgrupo de Sylow de $\mathfrak{A}_X$. La demostración funciona como sigue, donde consideramos un 2-subgrupo de Sylow cualquiera S de $\mathfrak{A}_X$.

- Como $\mathfrak{S}_4$ tiene cardinal $4!=24$, el grupo alternado $\mathfrak{A}_4$ tiene cardinal 12, y S cardinal 4.
- El orden de un elemento g de S divide a 4; puesto que sus coeficientes tienen entonces que dividir a 4, el tipo de ciclo de g es $()$, (2), $(2,2)$ o (4). Como el segundo y el último caso dan lugar a permutaciones impares, se tiene $g\in V$.
- El número de permutaciones de tipo de ciclo fijado en un grupo simétrico se puede calcular explícitamente (véase más abajo), y el cálculo muestra que V tiene 4 elementos.
- Como S y V tienen ambos 4 elementos y $S\subseteq V$, deducimos la igualdad $V=S$.

El cálculo del número de permutaciones de tipo de ciclo dado en el grupo simétrico $\mathfrak{S}_X$ es un importante resultado clásico de la combinatoria de grupos finitos. Volviendo al caso general de un conjunto finito X, sea n su cardinal, y consideremos

una partición π del entero n; llamemos m_i al número de partes iguales a i. Una permutación de tipo de ciclo π es de la forma

$$(a_1)(a_2)\cdots(a_{m_1})(b_1\,b_1')(b_2\,b_2')\cdots(b_{m_2}\,b_{m_2}')\cdots,$$

es decir, contiene m_1 ciclos de longitud 1, m_2 ciclos de longitud 2, etc. Así, para contar el número de permutaciones de tipo de ciclo π, basta con llenar las letras con elementos distintos de X, lo cual a simple vista sumaría $n!$ permutaciones. Sin embargo, para cada ciclo de longitud i, solo importa el orden cíclico de los elementos, de modo que tenemos que dividir el resultado por $\prod i^{m_i}$. Tampoco importa el orden en que escribimos los m_i ciclos de longitud i, así que el resultado aún hay que dividirlo por $\prod m_i!$. Obtenemos finalmente el número $n!/(\prod i^{m_i}\prod m_i!)$ de permutaciones de tipo de ciclo π.

Existe un modo más conceptual y más preciso de demostrar esta fórmula. Fijemos una permutación g con tipo de ciclo π. Como la cantidad que queremos calcular es el cardinal de la órbita de g bajo la acción por conjugación, basta con demostrar que el cardinal del centralizador Z_g de g es igual a $\prod i^{m_i}\prod m_i!$.

Si $h \in Z_g$, entonces $hgh^{-1} = g$, de modo que los ciclos que aparecen en hgh^{-1} coinciden con los de g. Dicho de otro modo, Z_g actúa por conjugación sobre el conjunto de ciclos de g preservando sus longitudes. Obtenemos así un morfismo de grupos $\phi\colon Z_g \to \prod_i \mathfrak{S}_{m_i}$.

Este morfismo es sobreyectivo. De hecho, se puede incluso demostrar que ϕ admite una sección. Para verlo, fijemos para cada ciclo c de g un elemento a_c de c; entonces, para cada permutación σ del conjunto de ciclos de g que preserve sus longitudes, existe un único elemento h_σ de Z_g tal que $h_\sigma(a_c) = a_{\sigma(c)}$ para todo c, y la aplicación $\sigma \mapsto h_\sigma$ es un morfismo de grupos.

Por otra parte, el núcleo de ϕ es el subgrupo formado por los elementos $h \in Z_g$ que cumplen $hch^{-1} = c$ para todos los ciclos c de g. Como h tiene que estabilizar el soporte de cada uno de esos c, envía a_c a un iterado de la acción de g sobre a_c. Fijemos un $k_c \in \mathbf{Z}$ (módulo el cardinal n_c del soporte de c) tal que $h(a_c) = g^{k_c}(a_c) = c^{k_c}(a_c)$; usando el hecho de que c es un ciclo, se sigue que h actúa como c^{k_c} sobre el soporte de c. Vemos así que h es el producto de esas potencias c^{k_c}. En otras palabras, $\ker(\phi)$ es el producto de grupos cíclicos $\prod_c(\mathbf{Z}/k_c\mathbf{Z})$, que podemos reescribir como $\prod_i(\mathbf{Z}/i\mathbf{Z})^{m_i}$, teniendo en cuenta que m_i es el número de ciclos c tales que $n_c = i$. En particular, el orden de $\ker(\phi)$ es igual a $\prod i^{m_i}$.

Poniendo todo junto, se tiene

$$\operatorname{Card}(Z_g) = \operatorname{Card}(\operatorname{Im}(\phi))\operatorname{Card}(\ker(\phi)) = \prod_i i^{m_i}\prod_i m_i!,$$

como queríamos demostrar.

7. Simplicidad de los grupos clásicos

7.1. El criterio de simplicidad de Iwasawa no aparece explícitamente en [9], sino que se demuestra y aplica directamente en el caso de la acción del grupo lineal

especial proyectivo $\mathrm{PSL}(n, F)$ sobre el espacio proyectivo $\mathbf{P}_{n-1}(F)$ de rectas de F^n. Salvo que F tenga 2 o 3 elementos, un argumento de álgebra lineal implica que esta acción es doblemente transitiva, y por tanto primitiva.

Para cada recta $\ell \in \mathbf{P}_{n-1}(F)$, consideremos el subgrupo $T(\ell)$ de transvecciones respecto a ℓ, es decir, los elementos $g \in \mathrm{SL}(n, F)$ tales que la imagen de $g - \mathrm{id}$ está contenida en ℓ. Usando que las transvecciones generan $\mathrm{SL}(n, F)$, vemos que los subgrupos $T(\ell)$ cumplen las propiedades del criterio de Iwasawa. Por tanto, cualquier subgrupo normal de $\mathrm{SL}(n, F)$ que no actúe trivialmente sobre $\mathbf{P}_{n-1}(F)$ contiene al subgrupo de conmutadores de $\mathrm{SL}(n, F)$, que es de nuevo $\mathrm{SL}(n, F)$. Por otra parte, los únicos elementos de $\mathrm{SL}(n, F)$ que actúan trivialmente sobre $\mathbf{P}_{n-1}(F)$ son las homotecias, que forman el centro de $\mathrm{SL}(n, F)$, un subgrupo finito isomorfo al conjunto de raíces n-ésimas de la unidad en F. De todo ello se deduce la simplicidad del cociente $\mathrm{PSL}(n, F) = \mathrm{SL}(n, F)/Z(\mathrm{SL}(n, F))$.

7.2. Este razonamiento se puede aplicar también a otros grupos geométricos. El propio Iwasawa indica en su artículo que el mismo método funciona para el grupo simpléctico $\mathrm{PSp}(2n, F)$ («grupo complejo proyectivo» en la antigua terminología) actuando sobre el espacio proyectivo $\mathbf{P}_{2n-1}(F)$. Iwasawa no considera explícitamente la noción de acción primitiva en su artículo, sino que detalla sus argumentos solo en el caso de una acción doblemente transitiva. Sin embargo, en una nota a pie de página menciona que la acción del grupo simpléctico $\mathbf{P}_{2n-1}(F)$ no es doblemente transitiva: es cuasiprimitiva, y con eso es suficiente para su demostración. Por otro lado, King [13] demostró que los estabilizadores de esta acción son subgrupos maximales, de modo que es incluso primitiva.

De hecho, parece que la simplicidad de los grupos de transformaciones geométricas apropiadas se puede demostrar siempre así.

Encuentro notable hasta qué punto este método, que relaciona la simplicidad de un grupo con la estructura de sus subgrupos maximales, está en sintonía con el punto de vista de Jordan y de los primeros teóricos de grupos.

8. Reflexiones sobre las demostraciones formales y el proceso de formalización

Como recordé en la introducción, la implementación de demostración matemáticas en los ordenadores no es una actividad muy reciente, pero los movimientos `Lean` y `mathlib` nos ponen en una encrucijada al hacer por primera vez concebible una biblioteca de demostraciones formalizadas de extensión indefinida. Basándome en el experimento descrito en esta nota, me gustaría arriesgarme a incluir algunas reflexiones sobre esta perspectiva, las esperanzas y los temores que puede generar.

La formalización de las demostraciones matemáticas tiene muchos objetivos.

Algunos de sus defensores plantean la idea de que nos permitirá asegurarnos realmente de la corrección de los nuevos teoremas que demostramos, en un momento en que la revisión por pares tradicional parece alcanzar sus límites, tanto por razones matemáticas como sociológicas.

Algunos artículos son sencillamente tan complicados que nadie puede afirmar que son válidos con absoluta certeza. Fue el caso de la demostración de Hales de la conjetura de Kepler, antes de que él mismo la formalizara liderando un equipo de 21 matemáticos. Y, en cierto sentido, sigue siendo el caso de la clasificación de los grupos simples finitos, cuya longitud y tecnicidad la hacen inaccesible a la mayoría de la comunidad matemática.

Los artículos de investigación son en general más cortos, pero la sociología del área ha evolucionado. La creciente importancia de las becas para la financiación de la investigación, o incluso para obtener plazas fijas, nos ha llevado a una situación en la que la comunidad quiere que sus artículos se publiquen más rápido de lo que tarda en comprobar su incorrección, tal vez incluso en leerlos. Como consecuencia, los artículos se revisan demasiado rápido, su publicación está condicionada a opiniones preliminares, con todos los sesgos que uno puede imaginar, y se crean nuevas revistas para albergar toda esa literatura matemática creciente.

Si pudiéramos comprobar la validez de nuestras demostraciones mediante programas de formalización y entregarlos al mismo tiempo que enviamos un artículo, es probable que ese artículo se pudiera haber escrito de forma diferente: no solo para convencer rápidamente a un árbitro de que las demostraciones son correctas, sino también dedicando más espacio del que actualmente dedicamos a explicar los enunciados, por qué son interesantes, cuál es su contexto, el camino que condujo a la demostración, etc., para poder llegar así a un público más amplio.

Para que esto suceda, necesitamos un *enorme* archivo de demostraciones matemáticas escritas en un lenguaje común, con definiciones comunes. La experiencia de los libros de Bourbaki sugiere que algo así es posible, pero también nos recuerda que no todos los matemáticos estarán dispuestos a adoptar el estilo de escritura matemática de otros.

Si el estilo de Bourbaki a veces se ha definido como demasiado abstracto, no es nada en comparación con el de `mathlib`. Para evitar repetir demostraciones, los autores de esa biblioteca hacen un esfuerzo permanente por poner sus definiciones y afirmaciones en una generalidad natural, pero quizá aterradora. El álgebra lineal comienza con una discusión de semimódulos sobre monoides, para que se pueda aplicar a contextos más exóticos como las álgebras $(\text{máx}, +)$ (Bourbaki dio un paso similar cuando definió «grupos con operadores», pero esta noción no parece haber cuajado). En el análisis complejo, la caracterización de las funciones analíticas como funciones que son diferenciables en el sentido complejo se demuestra utilizando la integral de Kurzweil-Henstock, porque eso permite evitar cualquier hipótesis de integrabilidad de Lebesgue sobre la derivada.

Una de las dificultades al trabajar con varias acciones de grupo al mismo tiempo es que la *teoría de tipos*, el lenguaje interno de `Lean`, no permite los abusos lingüísticos en los que solemos incurrir, sin ni siquiera darnos cuenta, cuando hacemos matemáticas. Tomemos, por ejemplo, un grupo G actuando sobre un conjunto X, un subconjunto A de X y un punto $a \in X \setminus A$. Entonces podemos considerar el estabilizador G_A de A en X y su acción sobre $X \setminus A$, y luego el estabilizador $G_{A,a}$ de a en G_A y su acción sobre $X \setminus (A \cup \{a\})$, que —obviamente— coincide con la acción del estabilizador de $A \cup \{a\}$ sobre su complemento. Sin embargo, estas acciones son

lo suficientemente distintas sintácticamente como para que `Lean` no sea capaz de identificarlas automáticamente. La sugerencia que recibí en el tablero de discusión de *Zulip* fue que no debería intentar identificarlas, sino relacionarlas por medio de *aplicaciones equivariantes*. Si los grupos G y H actúan sobre X e Y, respectivamente, y $\phi\colon G \to H$ es un morfismo de grupos, entonces una aplicación ϕ-equivariante de X en Y es una aplicación $f\colon X \to Y$ tal que $f(g \cdot x) = \phi(g) \cdot f(x)$ para todo $g \in G$ y $x \in X$. Varios resultados básicos nos permiten transferir propiedades de primitividad o transitividad de la acción de G en X a la acción de H en Y, o viceversa. Este es un ejemplo de una definición elemental y de resultados básicos que la acompañan que probablemente no nos atreveríamos a introducir explícitamente en una discusión matemática estándar —demasiado trivial para los especialistas, demasiado oscura para los principiantes—. Aprender a apreciar la relevancia de introducir tales conceptos abstractos lleva tiempo y requiere una comunidad de matemáticos conocedores, así como la voluntad de seguir su punto de vista.

Por otro lado, como el mito de la torre de Babel debería recordarnos, inclinarse hacia alguna generalidad en constante expansión conlleva un alto riesgo de que todo el edificio colapse. Mi propio experimento ha sido lo suficientemente agradable como para desear sinceramente que la comunidad encuentre el modo de evitar ese riesgo.

Referencias

[1] N. Bourbaki, *Algebra I. Chapters 1–3*, Elem. Math., Springer-Verlag, Berlin, 1989.

[2] P. J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), no. 1, 1–22.

[3] D. A. Cox, *Galois Theory*, segunda edición, Pure Appl. Math., John Wiley & Sons, Hoboken, N.J., 2012.

[4] F. van Doorn, P. Massot y O. Nash, Formalising the h-principle and sphere eversion, *Proceedings of the 12th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2023, Boston, January 16-17, 2023)*, 121–134, Association for Computing Machinery, New York, 2023.

[5] A. Doxiadis y C. H. Papadimitriou, *Logicomix—An Epic Search for Truth*, Bloomsbury Press, New York, 2009.

[6] G. Gonthier, Formal proof—the four-color theorem, *Notices Amer. Math. Soc.* **55** (2008), no. 11, 1382–1393.

[7] G. Gonthier, A. Asperti, J. Avigad, Y. Bertot, C. Cohen, F. Garillot, S. Le Roux, A. Mahboubi, R. O'Connor, S. Ould Biha, I. Pasca, L. Rideau, A. Solovyev, E. Tassi y L. Théry, A machine-checked proof of the odd order theorem, *Interactive Theorem Proving*, Lecture Notes in Comput. Sci. **7998**, 163–179, Springer, Berlin, 2013.

[8] T. Hales, M. Adams, G. Bauer, T. D. Dang, J. Harrison, H. Le Truong, C. Kaliszyk, V. Magron, S. McLaughlin, T. T. Nguyen, Q. T. Nguyen, T. Nipkow, S. Obua, J. Pleso, J. Rute, A. Solovyev,

T. H. Ta, N. T. Tran, T. D. Trieu, J. Urban, K. Vu y R. Zumkeller, A formal proof of the Kepler conjecture, *Forum Math. Pi* **5** (2017), e2, 29 pp.

[9] K. Iwasawa, Über die Einfachheit der speziellen projektiven Gruppen, *Proc. Imp. Acad. Tokyo* **17** (1941), 57–59.

[10] N. Jacobson, *Basic Algebra I*, segunda edición, W. H. Freeman and Company, New York, 1985.

[11] C. Jordan, *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris, 1870.

[12] C. Jordan, Sur la limite de transitivité des groupes non alternés, *Bull. Soc. Math. France* **1** (1872), 40–71.

[13] O. King, On some maximal subgroups of the classical groups, *J. Algebra* **68** (1981), no. 1, 109–120.

[14] M. W. Liebeck, C. E. Praeger y J. Saxl, A classification of the maximal subgroups of the finite alternating and symmetric groups, *J. Algebra* **111** (1987), no. 2, 365–383.

[15] P. M. Neumann, The concept of primitivity in group theory and the second memoir of Galois, *Arch. Hist. Exact Sci.* **60** (2006), no. 4, 379–429.

[16] G. Peano, *Arithmetices principia nova methoda exposita*, Fratelli Bocca Editrice, Torino, 1889.

[17] P. Scholze, Liquid Tensor Experiment, *Exp. Math.* **31** (2022), no. 2, 349–354.

[18] The mathlib community, The lean mathematical library, *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020, New Orleans, January 20-21, 2020)*, 367–381, Association for Computing Machinery, New York, 2020.

[19] A. N. Whitehead y B. Russell, *Principia Mathematica*, segunda edición, Cambridge University Press, London, 1927.

[20] R. A. Wilson, *The finite simple groups*, Grad. Texts in Math. **251**, Springer-Verlag, London, 2009.

Antoine Chambert-Loir, Université Paris Cité, Institut de mathématiques de Jussieu—Paris Rive Gauche, 8 place Aurélie Nemours, 75013 Paris

Correo electrónico: antoine.chambert-loir@u-paris.fr

Página web: https://webusers.imj-prg.fr/~antoine.chambert-loir