El grupo de Galois y el grupo fundamental

Alexey Beshenov (cadadr@gmail.com)

3 de Marzo de 2017

Los **grupos de Galois** fueron descubiertos en 1830 por Évariste Galois (1811–1832), y el **grupo fundamental** fue descubierto en 1895 por Henri Poincaré (1854–1912). El punto de vista moderno, popularizado por Alexander Grothendieck (1928–2014), quien definió en los 60 el **grupo fundamental étale**, dice que la teoría de Galois y la del grupo fundamental son diferentes facetas de la misma teoría general.

Primero voy a revisar la teoría de Galois en su forma infinita. Asumo que el lector conoce por lo menos el caso finito.

Teoría de Galois infinita

Para simplificar las condiciones, sea F un **cuerpo perfecto** (esto quiere decir que F es de característica 0, o de característica p tal que el **endomorfismo de Frobenius** $x \mapsto x^p$ es un automorfismo de F).

Un caso interesante es $F = \mathbb{Q}$. Las extensiones finitas de $\mathbb{Q}$ reciben el nombre de **cuerpos de números**.

La teoría de Galois funciona para las **extensiones de Galois**. A saber, se dice que una extensión algebraica K/F es una **extensión de Galois** si es **normal**: todo polinomio irreducible $f(X) \in F[X]$ que tiene una raíz en K, tiene automáticamente todas sus raíces en K. Por ejemplo, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es una extensión de Galois, pero $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es una extensión de Galois.

A toda extensión de cuerpos K/F se asocia el grupo

$$\operatorname{Aut}(K/F) := \{\text{automorfismos } f\colon K \to K \mid f(x) = x \quad \text{para } x \in F\}.$$

Para una extensión de Galois, este grupo se denota por $\operatorname{Gal}(K/F)$. Es el **grupo de Galois** de K/F.

Una extensión finita L/F es de Galois si y solamente si $|\operatorname{Aut}(L/F)| = [L : F]$.

Para nuestro cuerpo F podemos escoger una **clausura algebraica** $\overline{F}$, y la extensión $\overline{F}/F$ es de Galois. Por la definición, el **grupo de Galois absoluto** de F es el grupo

$$G_F := \operatorname{Gal}(\overline{F}/F).$$

Existe un isomorfismo canónico

$$G_F := \operatorname{Gal}(\overline{F}/F) \xrightarrow{\cong} \varprojlim_{\substack{F \subseteq L \\ L/F \text{ finito de Galois}}} \operatorname{Gal}(L/F).$$

Este isomorfismo significa lo siguiente: se puede considerar G_F como un **grupo topológico**, donde la topología es la inducida por la topología discreta sobre cada $\operatorname{Gal}(L/F)$ en el límite inverso. La topología que se obtiene sobre G_F se llama la **topología profinita**.

Un ejemplo particular: si $F = \mathbb{F}_q$ es un cuerpo finito, entonces para todo n existe precisamente una extensión de grado n, y su grupo de Galois es isomorfo a $\mathbb{Z}/n\mathbb{Z}$. La extensión de grado m está contenida en la extensión de grado n si y solamente si $m \mid n$. Se sigue que

$$G_{\mathbb{F}_q} \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

Este grupo recibe el nombre de **enteros profinitos** y se denota por $\widehat{\mathbb{Z}}$.

El **teorema fundamental de la teoría de Galois** toma la forma de una biyección natural

$$\{\text{extensiones } F \subset L \subset \overline{F}\} \longleftrightarrow \{\text{subgrupos cerrados } H \subset G_F\}$$

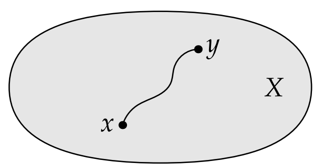
dada por

$$\begin{array}{rcl} L/F & \mapsto & G_L = \mathrm{Gal}(\overline{F}/L) \subset G_F, \\ \overline{F}^H & \leftarrow\!\shortmid & H \subset G_F, \end{array}$$

donde $\overline{F}^H$ es el subcuerpo de elementos fijos por la acción de H.

El grupo fundamental

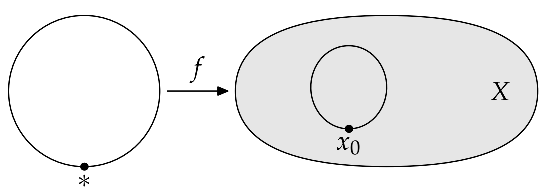
Sea X un espacio topológico. Para evitar ejemplos patológicos, supongamos que X es conexo por caminos (dos puntos $x, y \in X$ siempre pueden ser conectados por un camino).



Fijemos algún punto $x_0 \in X$. Tenemos otro espacio topológico, que es la circunferencia S^1, donde también podemos fijar algún punto $* \in S^1$. Por la definición, un **lazo** basado en el punto $x_0 \in X$ es una aplicación

$$f\colon (S^1, *) \to (X, x_0),$$

tal que $f(*) = x_0$.

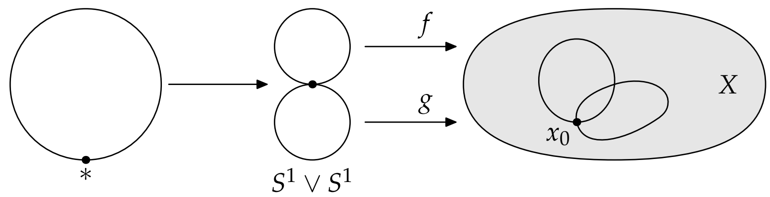


Por la definición, el **grupo fundamental** $\pi_1(X, x_0)$ es el grupo de lazos módulo **homotopía**. A saber, dos lazos f, g son homotópicos, si existe una aplicación continua

$$H\colon S^1 \times [0,1] \to X,$$

tal que $H(s,0) = f(s)$ y $H(s,1) = g(s)$, y $H(*, t) = x_0$ para todo $t \in [0,1]$. Intuitivamente, esto quiere decir que un lazo puede ser deformado en el otro de manera continua.

La estructura del grupo sobre $\pi_1(X, x_0)$ corresponde a la composición de lazos. La composición $f \cdot g$ corresponde al lazo que primero aplica S^1 en $S^1 \vee S^1$, y luego aplica f y g a cada copia de S^1 respectivamente.



El grupo fundamental es **funtorial**: toda aplicación continua $f\colon (Y, y_0) \to (X, x_0)$ induce un homomorfismo de grupos $f_*\colon \pi_1(Y, y_0) \to \pi_1(X, x_0)$ tal que $\mathrm{id}_* = \mathrm{id}$ y $(f \circ g)_* = f_* \circ g_*$.

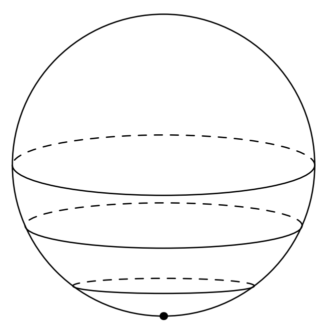
Dos espacios homeomorfos (o en general homotópicamente equivalentes) tienen grupos fundamentales isomorfos. Por ejemplo, $\mathbb{R}^n$ es contraíble (homotópicamente equivalente a un punto), y por lo tanto

$$\pi_1(\mathbb{R}^n, x_0) = \pi_1(\text{punto}) = \{1\}.$$

He aquí algunos ejemplos de grupos fundamentales:

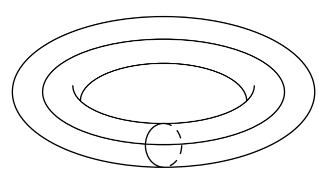
- Si $X = S^1$, entonces $\pi_1(S^1, *) \cong \mathbb{Z}$. A saber, una aplicación $(S^1, *) \to (S^1, *)$ salvo homotopía está definida por un parámetro, que es el **índice**, el número de vueltas ("winding number" en inglés), cuyo signo "$+$" o "$-$" corresponde al sentido horario o contrarreloj.

- Para la esfera $X = S^2$ tenemos $\pi_1(S^2, *) = \{1\}$, porque todo lazo es homotópico a un punto.



  Cuando X es conexo (por caminos) y $\pi_1(X) = \{1\}$, se dice que X es **simplemente conexo**. Entonces, la esfera es un ejemplo de espacio simplemente conexo. Los espacios $\mathbb{R}^n$ son también simplemente conexos, pero por una razón más tonta: son contraíbles, mientras que S^2 no lo es.

- Si $X = T = S^1 \times S^1$ es el toro, entonces $\pi_1(X, x_0) \cong \mathbb{Z} \oplus \mathbb{Z}$. Los generadores de este grupo corresponden a un meridiano y un paralelo.



El grupo fundamental está relacionado con otros objetos geométricos llamadods **recubrimientos** de X. A saber, un recubrimiento es una aplicación continua $p\colon (Y, y_0) \to (X, x_0)$, donde $p(y_0) = x_0$ y se cumple la siguiente propiedad.

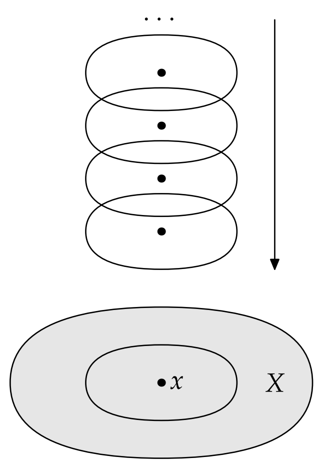
Para todo $x \in X$ existe un entorno abierto $U \ni x$ junto con un homeomorfismo

$$\phi\colon p^{-1}(x) \times U \xrightarrow{\cong} p^{-1}(U)$$

donde $p^{-1}(x)$ es un conjunto discreto y

$$p \circ \phi(a, u) = u \quad \textit{para todo } a \in p^{-1}(x),\ u \in U.$$

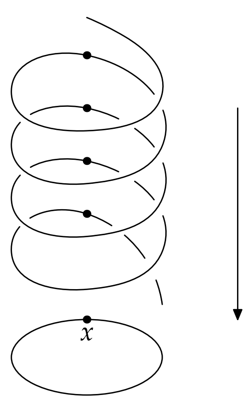
En este caso Y se llama un **espacio recubridor**. El conjunto $p^{-1}(x)$ se denomina la **fibra** sobre x. Hay que tener en mente la siguiente imagen: sobre todo entorno abierto $U \ni x$ hay una pila de tortillas y cada una se proyecta de modo homeomorfo a U.



Un ejemplo de esta situación es la aplicación

$$\begin{gathered}(\mathbb{R}, 0) \to (S^1, *),\\ x \mapsto e^{2\pi i x}\end{gathered}$$

(usando la parametrización del círculo en el plano complejo). Esto se puede visualizar como una hélice que se proyecta al círculo:



De modo similar, tenemos un recubrimiento del toro por el plano

$$(\mathbb{R} \times \mathbb{R},\ (0,0)) \to (T, *).$$

Es el producto de dos copias del recubrimiento de arriba.

Estos dos ejemplos son especiales: el espacio recubridor es simplemente conexo en ambos casos. En tal situación se dice que tenemos el **recubrimiento universal de** X. El artículo "el" viene del hecho de que si

$$q'\colon (\widetilde{X}', \widetilde{x}'_0) \to (X, x_0) \quad \text{y} \quad q''\colon (\widetilde{X}'', \widetilde{x}''_0) \to (X, x_0)$$

son dos recubrimientos universales, entonces existe un homeomorfismo canónico entre $\widetilde{X}'$ y $\widetilde{X}''$ que conmuta con q' y q'':

$$\begin{tikzcd}
(\widetilde{X}', \widetilde{x}'_0) \arrow[rr, "\cong"] \arrow[dr, "q'"'] & & (\widetilde{X}'', \widetilde{x}''_0) \arrow[dl, "q''"] \\
& (X, x_0) &
\end{tikzcd}$$

La palabra "universal" significa lo siguiente: *si* $q\colon (\widetilde{X}, \widetilde{x}_0) \to (X, x_0)$ *es un recubrimiento universal y* $p\colon (Y, y_0) \to (X, x_0)$ *cualquier otro recubrimiento con* Y *conexo, entonces existe un recubrimiento canónico* $(\widetilde{X}, \widetilde{x}_0) \to (Y, y_0)$ *que conmuta con* p *y* q.

$$\begin{tikzcd}
(\widetilde{X}, \widetilde{x}_0) \arrow[rr, dashed] \arrow[dr, "q"'] & & (Y, y_0) \arrow[dl, "p"] \\
& (X, x_0) &
\end{tikzcd}$$

Para buenos espacios X, el recubrimiento universal $\widetilde{X}$ siempre existe.

Si tenemos un recubrimiento $p\colon (Y, y_0) \to (X, x_0)$, sus **automorfismos** son los homeomorfismos $(Y, y_0) \to (Y, y_0)$ que conmutan con p.

$$\begin{tikzcd}
(Y, y_0) \arrow[rr] \arrow[dr, "p"'] & & (Y, y_0) \arrow[dl, "p"] \\
& (X, x_0) &
\end{tikzcd}$$

Estos homeomorfismos forman un grupo $\operatorname{Aut}((Y, y_0) \xrightarrow{p} (X, x_0))$ ("deck transformation group" en inglés).

Por ejemplo, en el caso del recubrimiento $\mathbb{R}^1 \to S^1$, se ve que este grupo corresponde a los desplazamientos de $\mathbb{R}^1$ por un número entero $n \in \mathbb{Z}$ (o rotaciones de la hélice por un número entero de turnos, si tenemos en mente la misma imagen de arriba). De modo similar, en el caso de $\mathbb{R}^2 \to T$, tenemos los desplazamientos del plano por $(m, n) \in \mathbb{Z} \oplus \mathbb{Z}$. Esto no es una coincidencia: el grupo fundamental es siempre isomorfo al grupo de los automorfismos del recubrimiento universal:

$$\pi_1(X, x_0) \cong \operatorname{Aut}(\widetilde{X} \to X).$$

En general, tenemos una biyección

$$\{\text{recubrimientos } (Y, y_0) \to (X, x_0)\} \longleftrightarrow \{\text{subgrupos de } \pi_1(X, x_0)\}.$$

dada por

$$\begin{array}{rcl} (Y, y_0) \xrightarrow{p} (X, x_0) & \mapsto & p_* \pi_1(Y, y_0), \\ \Gamma \backslash \widetilde{X} & \leftarrow & \Gamma. \end{array}$$

El espacio recubridor universal viene con una acción canónica de $\pi_1(X, x_0)$, y $\Gamma \backslash \widetilde{X}$ denota el cociente por esta acción.

La analogía entre G_F y $\pi_1(X)$

Tenemos la siguiente correspondencia entre la situación algebraica y la topológica:

$$\begin{array}{rcl} \text{cuerpo perfecto } F & \leftrightarrow & \text{espacio conexo por caminos } (X, x_0) \\ \text{extensiones } L/F & \leftrightarrow & \text{recubrimientos } (Y, y_0) \to (X, x_0) \\ \text{selección de clausura algebraica } \overline{F}/F & \leftrightarrow & \text{selección de recubrimiento universal } (\widetilde{X}, \widetilde{x}_0) \\ \text{el grupo de Galois absoluto } G_F & \leftrightarrow & \text{el grupo fundamental } \pi_1(X, x_0) \end{array}$$

La correspondencia de Galois en el caso algebraico es entre las extensiones de F y subgrupos cerrados de G_F, y en el caso topológico es entre los recubrimientos de (X, x_0) y subgrupos de $\pi_1(X, x_0)$.

Alexander Grothendieck introdujo un contexto general, conocido ahora como la **teoría de Galois de Grothendieck**, que incluye ambas situaciones como un caso particular, y además permite definir el grupo fundamental en la situación algebraica.

Para todo **esquema** X (un espacio cuyos pedazos locales corresponden a anillos conmutativos), se puede definir el **grupo fundamental étale** $\pi_1^{\text{ét}}(X)$. En la situación algebraica ya no se puede definir lazos y homotopías, pero sí se puede encontrar un buen análogo de recubrimientos (algo que se conoce como "recubrimientos étales") y considerar sus automorfismos. En particular, $\pi_1^{\text{ét}}(k) \cong G_k$ es el grupo de Galois.

Referencias

- Hendrik Lenstra, *Galois theory for schemes*.
  http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf
- Para el grupo fundamental en topología: Tammo tom Dieck, *Algebraic Topology* (capítulos 2 y 3) y J.P. May, *A Concise Course in Algebraic Topology* (capítulos 1, 2, 3).
- Para el grupo fundamental étale: J.P. Murre, *Lectures on an introduction to Grothendieck's theory of the fundamental group*.
- Tamas Szamuely, *Galois Groups and Fundamental Groups*.
- Régine Douady, Adrien Douady, *Algèbre et théories galoisiennes*.