Cohomología de grupos profinitos

Estas son las notas correspondientes al seminario del mismo nombre celebrado en la Universidad Autónoma de Madrid durante el curso 2019/2020. Están basadas en el libro *Cohomology of Number Fields* de J. Neukirch, A. Schmidt y K. Wingberg, el cual puede consultarse para usos no comerciales en `https://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/`.

Grupos profinitos

Prerrequisitos:

- Topología y álgebra al nivel de tercero del grado.
- Saber qué es un límite inverso y el producto tensorial.

Estos grupos topológicos aparecen al considerar los grupos de Galois de extensiones infinitas de cuerpos.

Definición/Proposición 1. Decimos que un espacio topológico Hausdorff T es profinito si satisface alguna de las tres siguientes propiedades equivalentes:

i) T es el límite inverso de espacios finitos discretos.

ii) T es compacto y todo punto tiene una base de entornos formada por conjuntos clopen.

iii) T es compacto y totalmente desconectado.

Demostración. i) $\Rightarrow$ ii): el límite inverso de espacios compactos es compacto. Esto se debe a que $\varprojlim X_i$ es un subespacio cerrado de $\prod_{i\in I} X_i$, que a su vez es compacto por el teorema de Tychonoff.

Recordemos que la topología del límite inverso es la más fina tal que las proyecciones $\pi_i : T \to X_i$ son continuas, luego en cualquier punto podemos encontrar una base de entornos de la forma $\{\pi_i^{-1}(U)\}$ donde $U \subset X_i$ es clopen.

ii) $\Rightarrow$ iii): sea C_t la componente conexa de $t \in T$. Como T es compacto y Hausdorff, C_t es la intersección de todos los conjuntos clopen que contienen a t; i.e. $C_t = \{t\}$.

iii) $\Rightarrow$ i): sea I el conjunto de relaciones de equivalencia R tal que al cocientar T/R es finito y discreto en la topología del cociente. I está parcialmente ordenado por inclusión y todo par R_1, R_2 tiene cota superior $R_1 \cap R_2$, luego I es dirigido. Afirmo que $\phi : T \to \varprojlim T/R$ es un homeomorfismo.

Demostramos primero que ϕ es sobreyectivo: sea $\{t_R\}_{R\in I} \in \varprojlim T/R$. Nótese que los conjuntos $(p_R \circ \phi)^{-1}(t_R)$ son no vacíos y compactos (son preimagenes de un compacto y T, T/R son compacto y Hausdorff respectivamente). Al ser I dirigido esto implica que intersecciones finitas de estos conjuntos tambien son no vacías y por compacidad obtenemos que $\phi^{-1}(\{t_R\}_{R\in I}) = \cap_{R\in I}(p_R \circ \phi)^{-1}(t_R)$ también es no vacío. (Un espacio es compacto si y solo si cualquier colección de subconjuntos cerrados con la propiedad de intersección finita tiene interseccion no vacía).

Para ver que ϕ es inyectiva es suficiente demostrar que para $t, s \in T$ distintos, existe $R \in I$ tal que $(t, s) \notin R$. Como T es totalmente desconectado $s \notin C_t$. Por la caracterización nombrada anteriormente, existe un subconjunto clopen $U \subseteq T$ tal que $t \in U$, $s \notin U$ y definimos una relación de equivalencia R: $(x, y) \in R$ si y solo si x e y están ambos en U o U^c. R cumple la condición requerida luego ϕ es una biyección entre espacios compactos, es decir, un homeomorfismo. □

Definición/Proposición 2. Decimos que un grupo topológico Hausdorff G es un grupo profinito si satisface alguna de las siguiente condiciones equivalentes:

i) G es el límite inverso topológico de grupos finitos discretos.

ii) G es compacto y el elemento neutro tiene una base de entornos formada por subgrupos normales clopen.

iii) G es compacto y totalmente desconectado.

Demostración. i) $\Rightarrow$ iii): el límite inverso de espacios compactos y totalmente desconectados es a su vez compacto y totalmente desconectado.

ii) $\Rightarrow$ i): sea $\{N_e\}$ el conjunto de entornos de $e \in G$ que son subgrupos normales abiertos. Afirmo que el homomorfismo canónico $\phi : G \to \varprojlim_U G/U$ es un isomorfismo. Es fácil ver que es inyectiva: si no lo fuese, existiría un $g \in G$ tal que $g \in N_e$ para todo entorno de la colección, lo cual contradice que G es Hausdorff.

Demostramos ahora que es sobreyectiva. Sea $x = \{x_U\}_U \in \varprojlim_U G/U$. Sea $\phi_U : G \to G/U$ la proyección canónica. Tenemos una igualdad:

$$\phi^{-1}(x) = \bigcap_U \phi_U^{-1}(x_U).$$

Nótese que la intersección de la derecha es no vacía utilizando el mismo argumento que en la demostración de 1. Por lo tanto ϕ es biyectiva y de hecho también es una aplicación abierta, luego es un homeomorfismo. Por otra parte, es claro que para cada U, G/U es compacto y discreto, luego es finito.

iii) $\Rightarrow$ ii): el espacio topológico que subyace a G es profinito por 1, luego todo punto tiene una base de entornos formada por conjuntos clopen. Nótese que un subconjunto abierto es automáticamente cerrado porque es el complementario de la unión de sus clases laterales no triviales, que son abiertas. Sea U un entorno clopen de $e \in G$, definimos:

$$V := \{v \in U | Uv \subseteq U\} \text{ y } H := \{h \in V | h^{-1} \in V\}.$$

Afirmo que $H \subseteq U$ is un subgrupo clopen en G. Primero demostraremos que V es abierto: sea $v \in V$. Por definición $uv \in V$ para todo $u \in U$, luego existen entornos U_u de u y V_u de v tal que $U_u V_u \subseteq U$. Los conjuntos abiertos $\{U_u\}$ cubren el espacio compacto U, luego existe un subrecubrimiento finito $U_{u_1}, ..., U_{u_n}$.

Sea $V_v := V_{u_1} \cap \cdots \cap V_{u_n}$. V_v es un entorno abierto de v contenido en V, luego V es abierto y $H := V \cap V^{-1}$ porque invertir es un homeomorfismo. Solo falta demostrar que H es un subgrupo. Es claro que $e \in H$ y que $H^{-1} = H$, luego nos queda comprobar que si $x, y \in H$ entonces $xy \in H$. Nótese pprimero que $Uxy \subseteq Uy \subset U$, por lo que $xy \in V$. Con el mismo razonamiento uno obtiene que $(xy)^{-1} \in V$, luego $xy \in H$. Es decir, H es un subgrupo abierto de G contenido en U. En particular, H tiene índice finito en G y solo hay

un número finito de conjugados de H. La intersección de estos conjugados es un subgrupo clopen normal de G contenido en U. □

De ahora en adelante, todos los homomorfismos entre grupos profinitos serán continuos salvo que se indique lo contrario. De la misma manera, todos los subgrupos serán cerrados. Como ya se dijo anteriormente, los subgrupos abiertos son inmediatamente cerrados y por compacidad, es sencillo ver que los subgrupos cerrados son abiertos si y solo si tienen índice finito.

Si H es un subgrupo de un grupo profinito G, el conjunto G/H de clases laterales es un espacio profinito con la topología del cociente. Si H es un subgrupo normal, G/H es un grupo profinito en la manera natural de cocientar. En general, toda la teoría de grupos tiene un análogo para el caso de grupos topológicos profinitos. A continuación veremos ejemplos de este paralelismo.

Definición 1. Un **número supernatural** es un producto formal $\prod_p p^{n_p}$, donde p recorre los primos y n_p son enteros no negativos o ∞.

Podemos multiplicar números supernaturales sumando los exponentes de la manera natural. También existen las nociones de máximo común divisor y mínimo común múltiplo.

Definición 2. Sean G un grupo profinito y A un grupo abeliano con torsión.

i) El **índice** de un subgrupo cerrado H de G es el número supernatural:

$$(G : H) = \text{m.c.m.}\{(G/U : H/H \cap U)\},$$

donde U recorre los subgrupos normales abiertos de G.

ii) El **orden** de G se define como $\#G = (G : 1) = \text{m.c.m.}\{\#(G/U)\}_U$.

iii) El **orden** de A se define como $\#A = \text{m.c.m.}\{\#B\}$, donde $B \leq A$ recorre los subgrupos finitos de A.

Dada una cadena de subgrupos cerrados $N \leq H \leq G$ el índice se comporta de manera multiplicativa, es decir:

$$(G : N) = (G : H)(H : N)$$

Observamos que el orden de un grupo abeliano con torsión A coincide con el orden del grupo profinito $\text{Hom}(A, \mathbb{Q}/\mathbb{Z})$.

Definición 3. Sea G un grupo profinito. Un **G-módulo abstracto** M es un grupo abeliano M con una acción:

$$G \times M \to M, (g, m) \mapsto g(m)$$

tal que $1(m) = m$, $(gh)(m) = g(h(m))$ y $g(m + n) = g(m) + g(n)$ para todo $g, h \in G$ y $m, n \in M$.

Un **G-módulo topológico** M es un grupo topológico abeliano y Hausdorff con la estructura de un G-módulo abstracto tal que la acción $G \times M \to M$ es continua.

Proposición 1. *Sean G un grupo profinito y M un G-módulo abstracto. Las siguientes condiciones son equivalentes:*

i) M es un G-módulo (topológico) discreto; es decir, la acción $G \times M \to M$ es continua con la topología discreta en M.

ii) Para todo $m \in M$ el estabilizador $G_m := \{g \in G | g(m) = m\}$ es abierto.

iii) $M = \bigcup M^U$, donde U recorre los subgrupos abiertos de G.

Demostración. i) $\Rightarrow$ ii): si restringimos la acción a $G \times \{m\}$, tenemos que la preimagen de m es G_m. Al ser la acción continua por hipótesis, G_m es abierto.

ii) $\Rightarrow$ iii): trivial porque $m \in M^{G_m}$ y los G_m son abiertos por hipótesis.

iii) $\Rightarrow$ i): sea $(g, m) \in G \times M$. Sabemos que existe un subgrupo abierto U tal que $m \in M^U$, luego $gU \times \{m\}$ es un entorno abierto de (g, m) que va a parar a $g(m)$. Luego la acción es continua. □

En lo que a estas notas respecta nos centraremos en G-módulos topológicos discretos y normalmente omitiremos tanto la terminología *abstracto* como *topológico* cuando nos refitamos a estos.

Ejemplos de operaciones con G-módulos:

1. Dada una familia $(A_i)_{i \in I}$ de G-módulos discretos, la suma directa $\bigoplus_{i \in I} A_i$ es también un G-módulo discreto donde G actúa en cada coordenada: $g((a_i)_{i \in I}) = (g(a_i))_{i \in I}$.

   Esto no es cierto en general para el producto directo.

2. El producto tensorial $A \otimes B$ sobre $\mathbb{Z}$ de dos G-módulos discretos es de nuevo un G-módulo discreto con la acción diagonal de G: $g(a \otimes b) = g(a) \otimes g(b)$.

3. Al conjunto $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ se le puede dar la estructura de G-módulo abstracto definiendo la acción $g(\phi)(a) = g(\phi(g^{-1}(a)))$.

   Si $A = A^U$ para algún subgrupo abierto $U \leq G$, entonces $\mathrm{Hom}(A, B)$ es un G-módulo discreto. Esto ocurre por ejemplo cuando G es finito o si A es finitamente generado como $\mathbb{Z}$-módulo.

4. Los grupos $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}$ y $\mathbb{F}_q$ se pueden ver como G-módulos discretos con acción trivial.

Hasta ahora, todos los grupos que hemos considerado han sido compactos y totalmente desconectado.

Grupos de cohomología

Sea G un grupo profinito, en esta sección todos los G-modulos serán discretos. Consideremos el diagrama:

$$\cdots \substack{\rightrightarrows \\ \rightrightarrows \\ \rightrightarrows} G \times G \times G \substack{\rightrightarrows \\ \rightrightarrows} G \times G \rightrightarrows G,$$

donde las flechas representan las proyecciones $d_i : G^{n+1} \to G_n$ para $i = 0, 1, ..., n$ dadas por:

$$d_i(\sigma_0, ..., \sigma_n) = (\sigma_0, ..., \hat{\sigma}_i, ..., \sigma_n)$$

donde $\hat{\sigma_i}$ significa que omitimos ese término. Dado un G-módulo A definimos el grupo abeliano:

$$X^n(G, A) = \mathrm{Map}(G^{n+1}, A)$$

de funciones continuas $x : G^{n+1} \to A$. X^n tiene estructura natural de G-módulo con la acción:

$$(\sigma x)(\sigma_0, ..., \sigma_n) = \sigma x(\sigma^{-1}\sigma_0, ..., \sigma^{-1}\sigma_n).$$

Obsérvese que la proyección d_i induce un G-homomorfismo $d_i^* : X^{n-1} \to X^n$, y podemos formar la suma:

$$\partial^n = \sum_{i=0}^{n} (-1)^i d_i^*.$$

Explícitamente, para $x \in X^{n-1}, \partial^n x$ es la función:

$$(\partial^n x)(\sigma_0, ..., \sigma_n) = \sum_{i=0}^{n} (-1)^i x(\sigma_0, ..., \hat{\sigma_i}, ..., \sigma_n).$$

Tenemos además otro G-homomorfismo $\partial^0 : A \to X^0$ definido como $a \mapsto x$ donde x es la functión constante con valor a.

Proposición 2. *La sucesión:*

$$0 \longrightarrow A \xrightarrow{\partial^0} X^0 \xrightarrow{\partial^1} X^1 \xrightarrow{\partial^2} X^2 \longrightarrow \cdots$$

es exacta.

Demostración. La comprobación de que $\operatorname{im} \partial^i \subseteq \ker \partial^{i+1}$ es directa. Para comprobar que es exacta consideramos las funciones $D^{-1} : X^0 \to A, D^{-1}x = x(1)$ y para $n \geq 0$:

$$D^n : X^{n+1} \to X^n, (D^n x)(\sigma_0, ..., \sigma_n) = x(1, \sigma_0, ..., \sigma_n).$$

Los D^n son homomorfismos de grupos abeliano pero no de G-módulos. Es fácil comprobar que:

$$D^n \circ \partial^{n+1} + \partial^n \circ D^{n-1} = \mathrm{id},$$

luego si $x \in \ker \partial^{n+1}$ entonces $x = \partial^n(D^{n-1}x)$. Es decir $\ker \partial^{n+1} \subseteq \operatorname{im} \partial^n$. □

Definición 4. A una sucesión exacta de G-módulos:

$$0 \to A \to X^0 \to X^1 \to \cdots$$

se le llama una **resolución** de A. A ésta en concreto se le denomina la resolución estándar. A una familia $(D^n)_{n \geq 1}$ como la de la demostración anterior se le llama una homotopía.

A continuación vamos a seleccionar los elementos G-invariantes de $X^n(G, A)$ y los vamos a denotar $C^n(G, A) = X^n(G, A)^G$. Es decir aquellas funciones $x : G^{n+1} \to X$ tal que para todo $\sigma \in G$:

$$x(\sigma\sigma_0, ..., \sigma\sigma_n) = \sigma x(\sigma_0, ..., \sigma_n).$$

A C^n le llamamos la n-cocadenas de G con coeficientes en A. Aplicando el functor $A \mapsto A^G$ a toda la resolución estándar obtenemos una secuencia que en general deja de ser exacta:

$$C^0(G,A) \xrightarrow{\partial^1} C^1(G,A) \xrightarrow{\partial^2} C^2(G,A) \longrightarrow \cdots$$

Sin embargo todavía se verifica que $\partial\partial = 0$ y normalmente se le llama el complejo de cocadenas homogéneas de G con coeficientes en A.

Definición 5. Definimos los n-cociclos como:

$$Z^n(G,A) = \ker \partial^{n+1}.$$

Definimos los n-cobordes como:

$$B^n(G,A) = \operatorname{im} \partial^n.$$

Obsérvese que la condicion $\partial\partial = 0$ garantiza que $B^n(G,A) \subseteq Z^n(G,A)$.

Para $n \geq 0$ definimos **grupo de cohomología** n-dimensional de G con coeficientes en A:

$$H^n(G,A) = Z^n(G,A)/B^n(G,A).$$

En muchas ocasiones trabajaremos con una versión ligeramente modificada de los grupos de cohomología que reduce el número de variables de las cocadenas. Sea $\mathscr{C}^0(G,A) = A$ y para $n \geq 1$ $\mathscr{C}^n(G,A)$ el grupo abeliano de funciones continuas $y : G^n \to A$. Tenemos isomorfismos:

$$C^0(G,A) \to \mathscr{C}^0(G,A), x(\sigma) \mapsto x(1)$$

y para $n \geq 1$ $C^n \to \mathscr{C}^n(G,A)$:

$$x(\sigma_0, ..., \sigma_n) \mapsto y(\sigma_1, ..., \sigma_n) = x(1, \sigma_1, \sigma_1\sigma_2, ..., \sigma_1...\sigma_n).$$

Obsérvese que el inverso de este isomorfismo viene dado por:

$$y(\sigma_1, ..., \sigma_n) \mapsto x(\sigma_0, ..., \sigma_n) = \sigma_0 y(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, ..., \sigma_{n-1}^{-1}\sigma_n).$$

Esto nos permite reescribrir los operadores coborde:

$$\partial^{n+1} : \mathscr{C}^n(G,A) \to \mathscr{C}^{n+1}(G,A),$$

dados por:

$$\begin{aligned} (\partial^1 a)(\sigma) &= \sigma a - a && \text{for } a \in A = \mathscr{C}^0(G,A), \\ (\partial^2 y)(\sigma,\tau) &= \sigma y(\tau) - y(\sigma\tau) + y(\sigma) && \text{for } y \in \mathscr{C}^1(G,A). \end{aligned}$$

Para el resto:

$$(\partial^{n+1}y)(\sigma_1,...,\sigma_{n+1}) = \sigma_1 y(\sigma_2,...,\sigma_{n+1}) + \sum_{i=1}^{n}(-1)^i y(\sigma_1,...,\sigma_{i-1},\sigma_i,\sigma_{i+1},\sigma_{i+2},...,\sigma_{n+1}) + (-1)^{n+1}y(\sigma_1,...,\sigma_n),$$

donde $y \in \mathscr{C}^N(G,A)$. Si ahora definimos:

$$\mathscr{L}^n(G,A) = \ker \partial^{n+1}$$
$$\mathscr{B}^n(G,A) = \operatorname{im} \partial^n,$$

los isomorfismos $C^n(G,A) \simeq \mathscr{C}^n(G,A)$ inducen isomorfismos:

$$H^n(G,A) \simeq \mathscr{L}^n(G,A)/\mathscr{B}^n(G,A).$$

A estos/as n-cocadenas, n-cociclos y n-cobordes se les denomina inhomogéneos.

Interpretando el grupo $H^0(G,A)$: recordamos que hay un isomorfismo $C^0(G,A) \to A$ dado por $x \mapsto x(1)$. Según hemos visto arriba, $(\partial^1 a)(\sigma) = \sigma(a) - a$. Es decir:

$$H^0(G,A) = \ker \partial^1 A^G.$$

Interpretando el grupo $H^1(G,A)$: de nuevo recordamos que los 1-cociclos inhomogéneos vienen dados por funciones $x : G \to A$ tal que para todo $\sigma, \tau \in G$:

$$x(\sigma\tau) = x(\sigma) + \sigma x(\tau).$$

Los 1-cobordes son las funciones dados por $x(\sigma) = \sigma(a) - a$ para $a \in A$ fijo. Obsérvese que si G actúa trivialmente, $H^1(G,A)$ es simplement $\operatorname{Hom}_{cts}(G,A)$. De manera más general, la motivación para definir H^1 viene de considerar una sucesión corta exacta:

$$0 \longrightarrow A \xrightarrow{\ i\ } B \xrightarrow{\ j\ } C \longrightarrow 0.$$

Si tomamos los elementos fijados por G, en general un elemento de C^G no puede ser representado por uno de B^G y la sucesión deja de ser exacta por la derecha:

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G.$$

En este caso H^1 mide cuánto de lejos está de ser exacta esa sucesión. De hecho, hay un isomorfismo canónico:

$$\delta : C^G \to H^1(G, A)$$

que extiende a una sucesión que exacta:

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G, A).$$

(Durante el seminario, se hará una demostración de *diagram chase*).

Para dar una interpretación aún más concreta introduciremos el concepto de *torsor*. Para poder explotarlo a fondo olvidaremos la hipótesis de que A es abeliano, lo cual nos obliga a hacer algunas modificaciones:

Definición 6. Un **G-grupo** A es un grupo no necesariamente abeliano con la topología discreta y acción de G continua. La acción de G suele denotarse con a^σ.

Un **cociclo** de G con coeficientes en A es una función continua $\sigma \mapsto a(\sigma)$ tal que:

$$a(\sigma\tau) = a(\sigma)a(\tau)^\sigma.$$

Al conjunto de cociclos lo denominamos $\mathscr{L}^1(G, A)$. Dos cociclos son cohomólogos si existe algún $b \in A$ tal que:

$$a'(\sigma) = b^{-1}a(\sigma)b^\sigma.$$

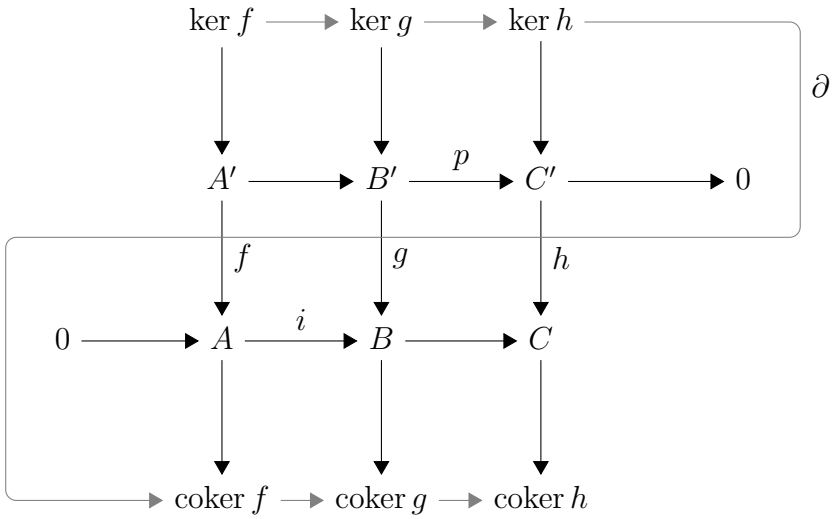
Esto es una relación de equivalencia y al cociente le denominamos $H^1(G, A)$ (pointed set).

La sucesión exacta

A continuación estudiaremos cómo se comporta H^n con respecto a homomorfisms ode G-módulos $f : A \to B$. Este f induce un homomorfismo entre las cocadenas $f : C^n(G, A) \to C^n(G, B)$ que conmuta con δ, luego también induce un homomorfismo:

$$f : H^n(G, A) \to H^n(G, B).$$

Proposición 3. *Snake Lemma:*



El hecho crucial que podemos demostrar con este lema es que dada una sucesión exacta:

$$0 \to A \to B \to C \to 0$$

existe un homomorfismo canónico para todo $n \geq 0$:

$$\delta : H^n(G, C) \to H^{n+1}(G, A)$$

que nos da la siguiente sucesión exacta:

$$H^n(G,A) \longrightarrow H^n(G,B) \longrightarrow H^n(G,C) \rightarrow H^{n+1}(G,A) \longrightarrow H^{n+1}(G,B) \longrightarrow H^{n+1}(G,C).$$