Introducción a la Teoría Analítica de Números

Pablo De Nápoli

clase 11

1. La estructura de $\mathbb{Z}_n^*$ cuando n es una potencia de un primo impar

Teorema 1.1 *Si $n = p^k$ con p un primo impar y $k \geq 1$, $\mathbb{Z}_n^*$ es cíclico. Es decir: existe una raíz primitiva módulo p^k. Probaremos esto en dos etapas:*

i) Si g es una raíz primitiva módulo p tal que $g^{p-1} \not\equiv 1 \pmod{p-1}$, entonces g es también una raíz primitiv módulo p^k para todo $k \geq 1$.

ii) Siempre existe una raíz primitiva módulo p tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$.

Prueba: Ver Apostol, teorema 10.6.

Observación: Como veremos la próxima clase, este teorema no es cierto si $p = 2$ y $k \geq 3$.

2. Caracteres de grupos abelianos finitos

En esta sección, introduciremos una construcción de teoría de grupos que nos será de utilidad para demostrar el teorema de Dirichlet sobre la infinitud de los primos en las progresiones aritméticas.

Recordamos que dados dos grupos, G y H un (homo)-morfismo de grupos es una función $f : G \to H$, que respeta la estructura de grupo: es decir tal que:

$$f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2) \; \forall \; g_1, g_2 \in G$$

El conjunto de (homo)morfismos de G en H se denota $\mathrm{Hom}(G, H)$. Si H es un grupo abeliano entonces Hom es asimismo un grupo abeliano con la operación de producto punto a punto:

$$(f_1 \cdot f_2)(g) = f_1(g) \cdot f_2(g)$$

Recordamos también que $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ es un grupo abeliano con el producto de números complejos como operación.

Definición 2.1 *Sea $(G,\cdot)$ un grupo abeliano finito, definimos el grupo dual de G, o grupo de los caracteres sobre G, notado $\widehat{G}$, por*

$$\widehat{G} = Hom(G, S^1) = \left\{ f : G \to S^1 : f \text{ es un (homo)morfismo de grupos} \right\}$$

Observación: Sea $f \in \widehat{G}$. Si g es un elemento de orden d en G, será $g^d = e$ siendo e el neutro de G, y como $f(e) = 1$, debe ser $f(g)^d = 1$ Por lo tanto, la imagen de un elemento de orden d debe ser una ráiz d-ésima de la unidad. En particular si G tiene orden N, la imagen de f será un subgrupo de las raices N-ésimas de la unidad.

Ejemplo: Si $G = (\mathbb{Z}_n, +)$, un morfismo de grupos $f : \mathbb{Z}_n \to S^1$ queda determinado por su valor en $\overline{1}$, que es un generador de $\mathbb{Z}_n$. Por la observación anterior, $f(\overline{1})$ debe ser una raíz n-ésima de la unidad: Si

$$f(\overline{1}) = e^{2\pi ik/n}$$

entonces

$$f(\overline{m}) = f(\overline{1})^m = e^{2\pi ikm/n}$$

Tenemos pues exactamente n morfismos en $\widehat{\mathbb{Z}_n}$, dados por

$$f_k(\overline{m}) = f(\overline{1})^m = e^{2\pi ikm/n} \ (0 \leq k \leq n-1)$$

y es fácil comprobar que la aplicación $\overline{k} \mapsto f_k$ es un isomorfismo de grupos entre $\mathbb{Z}_n$ y $\widehat{\mathbb{Z}_n}$.

Es usual utilizar la letra χ para los caracteres. Observamos que $\widehat{G}$ tiene un elemento neutro que es el caracter χ_1 dado por:

$$\chi_1(g) = 1 \ \forall \ g \in G$$

χ_1 se denomina el caracter principal o, caracter trivial.

Proposición 2.1 *Si G es un grupo abeliano finito de orden N y $\chi \in \widehat{G}$ es un caracter, entonces*

$$\sum_{g \in G} \chi(g) = \begin{cases} N & si \quad \chi = \chi_1 \\ 0 & si \quad \chi \neq \chi_1 \end{cases}$$

Prueba: Si $\chi = \chi_1$ el resultado es trivial. Si $\chi \neq \chi_1$, sea $g_1 \in G$ tal que $\chi(g_1) \neq 1$. Cuando g recorre G, $g_1 \cdot g$ también recorre G (pues G es un grupo). En consecuencia:

$$\sum_{g \in G} \chi(g_1 \cdot g) = \sum_{g \in G} \chi(g)$$

Dado que χ es un morfismo de grupos, deducimos que:

$$\chi(g_1) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g)$$

y como $\chi_1(g) \neq 1$, la suma del enunciado debe dar cero. $\square$

Sea $V = \{f : G \to \mathbb{C}^n\}$ entonces V es un espacio vectorial sobre $\mathbb{C}$ de dimensión N, donde N es el orden de G, y los caracteres pueden pensarse como elementos de este espacio vectorial.

En V definimos un producto interno de la siguiente manera:

$$\langle f_1, f_2 \rangle = \frac{1}{N} \sum_{g \in G} f_1(g)\overline{f_2(g)} \quad (f_1, f_2 \in V)$$

El resultado anterior tiene entonces la siguiente consecuencia importante:

Proposición 2.2 (Relaciones de ortogonalidad entre los caracteres) *Si $\chi_i, \chi_j \in \widehat{G}$ son dos caracteres, entonces*

$$\langle \chi_i, \chi_j \rangle = \begin{cases} 1 & si \quad \chi_i = \chi_j \\ 0 & si \quad \chi_i \neq \chi_j \end{cases}$$

Prueba:

$$\langle \chi_i, \chi_j \rangle = \frac{1}{N} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)}$$

Pero $\overline{\chi_j(g)} = \chi_j(g)^{-1} = \chi_j^{-1}(g)$, luego:

$$\langle \chi_i, \chi_j \rangle = \frac{1}{N} \sum_{g \in G} (\chi_i \cdot \chi_j^{-1})(g)$$

y como $\chi = \chi_i \cdot \chi_j^{-1}$ es un caracter, y $\chi = \chi_1$ si y sólo si $\chi_i = \chi_j$, el resultado se deduce de la proposición anterior. $\square$

Proposición 2.3 *Si G es un grupo abeliano finito, $\widehat{G}$ es isomorfo a G (aunque no existe un isomorfismo canónicamente definido entre ellos). En particular, el orden (=número de elementos) de $\widehat{G}$ coincide con el de G.*

Prueba: Por el teorema de estructura (de álgebra II), todo grupo abeliano finito es isomorfo al producto directo de ciertos grupos cíclicos, digamos que:

$$G \simeq \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \ldots \times \mathbb{Z}_{k_j}$$

Pero el "functor Hom" tiene la siguiente propiedad distributiva con respecto al producto directo (en la primer variable):

$$\mathrm{Hom}(G_1 \times G_2, H) = \mathrm{Hom}(G_1, H) \times \mathrm{Hom}(G_2, H)$$

Luego,

$$\widehat{G} = \mathrm{Hom}(G, S^1) \simeq \mathrm{Hom}(\mathbb{Z}_{k_1}, S^1) \times \mathrm{Hom}(\mathbb{Z}_{k_2}, S^1) \times \ldots \times \mathrm{Hom}(\mathbb{Z}_{k_j}, S^1)$$

$$\simeq \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \ldots \times \mathbb{Z}_{k_j} \simeq G$$

$\square$

Corolario 2.1 *Si G es un grupo abeliano de orden N, los elementos de $\widehat{G} = \{\chi_1, \chi_2, \ldots, \chi_N\}$ forman una base ortonormal del espacio V.*

Prueba: Como son ortogonales, son linealmente independientes, y como la dimensión de V que es N coincide con el número de elementos de $\widehat{G}$, son una base. Entonces por la proposición anterior, son una base ortonormal. □

Se sigue que si $f \in V$, admite el desarollo

$$f = \sum_{k=1}^{N} c_k \chi_k \quad \text{donde} \quad c_k = \langle f, \chi_k \rangle = \frac{1}{N} \sum_{g \in G} f(g)\overline{\chi_k g}$$

Ejemplo: Si $G = \mathbb{Z}_n$, los elementos de V pueden identificarse natualmente con las funciones aritméticas $f : \mathbb{Z} \to \mathbb{C}$ períodicas con período n (Esto es: tales que $f(k_1) = f(k_2)$ si $k_1 \equiv k_2 \pmod{n}$).

Este resultado dice entonces que cualquier función aritmética períodica con período n admite el desarrollo (finito) de Fourier:

$$f(m) = \sum_{k=1}^{n} c_k e^{2\pi i k m/n} \quad \text{donde} \quad c_k = \frac{1}{n} \sum_{m=1}^{n} f(m) e^{-2\pi i k m/n}$$

Esto muestra que la teoría de los caracteres puede pensarse como una versión abstracta del análisis de Fourier en grupos abelianos finitos[1]

Otro ejemplo:los Caracteres de Dirichlet

El ejemplo más importante para nosotros será cuando $G = (\mathbb{Z}_n^*, .)$. Los elementos del grupo dual $\widehat{\mathbb{Z}_n^*}$ se llaman caracteres de Dirichlet. Un elemento χ de este grupo puede identificarse (y así lo haremos) con la función aritmética períodica con período n definida por:

$$\chi(k) = \begin{cases} \chi(\overline{k}) & \text{si} \quad (k,n) = 1 \\ 0 & \text{si} \quad (k,n) \neq 1 \end{cases}$$

Por el teorema anterior existen exactamente $\varphi(n)$ caracteres de Dirichlet módulo n, y forman una base ortonormal del espacio de las funciones aritméticas períodicas de período n que se anulan en los enteros que no son coprimos con n.

Dirichlet utilizó estas funciones en la prueba de su teorema sobre la infinitud de los primos en progresiones aritméticas.

Cuando n es de la forma p^k con p primo impar (o si $p = 2$ pero $k = 1$ o 2), sabemos que $\mathbb{Z}_n^*$ es cíclico. En este caso podemos dar la siguiente descripción

[1] Existe una versión más general de esta teoría en grupos topológicos abelianos localmente compactos (donde las sumas finitas deben reemplazarse por integrales respecto a una medida invariante por la acción del grupo: la medida de Haar) , que permite unificar en un sólo marco abstracto la teoría de las series y transformadas (integrales) de Fourier.

más explícita de estos caracteres: sea g una raíz primitiva módulo n, entonces la fórmula

$$\chi_k(\overline{g}^m) = e^{2\pi imk/N} \text{ con } N = \varphi(n) \text{ y } 0 \leq k < N$$

define los $\varphi(n)$ caracteres de Dirichlet módulo n.