Teoría de números, Universidad del Valle

Teoría algebraica de números

Javier Mejía-18638

UVG
UNIVERSIDAD DEL VALLE DE GUATEMALA

November 25, 2021

Contents

Enunciado

Teorema

Todo entero positivo puede escribirse como la suma de los cuadrados de cuatro enteros.

(Lagrange,1770)
El teorema fue demostrado por Lagrange utilizando aritmética y herramientas avanzadas de teoría de números. Ahora lo demostramos usando herramientas de álgebra.

Herramientas

- Anillos, ideales, e isomorfismos (Anillo cociente, ideales maximales, etc.)
- ¡Cuaternios!
  - Cuaternios reales Q (Anillo con división y norma)
  - Anillo de Hurwitz de Cuaternios reales H (anillo con división izquierda)
  - Cuaternios sobre los enteros módulo p, W_p (anillo finito)
- Teorema de Wedderburn

Anillos, ideales, e isomorfismos, repaso

Definición

Un anillo $(R, +, *)$ es una estructura algebraica donde $(R, +)$ es un grupo abeliano, $(R, *)$ es un monoide con identidad, y $*$ se distribuye respecto a $+$. Nótese que no es necesario que $(R, *)$ sea conmutativo.

Definición

Un subconjunto no vacío de un anillo $I \subseteq R$ es llamado un **ideal** izquierdo de R si $x + y \in I$ y $rx \in I, \forall x, y \in I, r \in R$. Similarmente un ideal derecho cumple con $xr \in I$, y un ideal bilateral es tanto un ideal izquierdo como uno derecho.

Anillos, ideales, e isomorfismos, repaso

Definición

Un ideal $I \subseteq R$ de un anillo R es llamado máximo o maximal si, para todo ideal M de R se tiene que $I \subseteq M \subseteq R \implies I = M$ o $R = M$

Definición

Sea $(R, +, *)$ un anillo y I un ideal bilateral de R. De forma similar a como se define el grupo cociente, definimos el anillo cociente R/I como el conjunto de las clases de equivalencia de R/I (Grupo cociente) con las operaciones:

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = (ab) + I$$

Anillos, ideales, e isomorfismos, repaso

Definición

Sean $(R, +, *)$ y $(S, +, *)$ anillos. Un homomorfismo de anillos $f : R \to S$ es un mapeo que cumple que, para todo $a, b \in R$

$$f(a +_R b) = f(a) +_S f(b)$$

$$f(a *_R b) = f(a) *_S f(b)$$

Cuando esta función es biyectiva, se le llama un isomorfismo de anillos.

Anillos, ideales, e isomorfismos, repaso

Definición

Un dominio entero R es llamado anillo euclideano si existe una función $d : R \to \mathbb{Z}^+$ tal que, para cualesquiera $a, b \in R$:

$$d(a) \leq d(ab)$$

$$\exists t, r \in R \ni a = tb + r, d(r) < d(b)$$

Teorema de Wedderburn

Todo anillo de división finito es un campo.

Nos interesa el converso de este teorema, que nos dice que si tenemos un anillo finito que no es un campo, entonces no puede ser un anillo de división. La prueba se encuentra en la sección 7.2 de Hernstein.

Cuaternios

Los cuaternios son una extensión de los números reales, la idea es parecida a la de los números complejos, en 4 dimensiones. Definimos las unidades imaginarias i, j, k tales que

$$i^2 = j^2 = k^2 = ijk = -1$$

Los cuaternios reales son el conjunto

$$Q = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$$

Que es una anillo con división, es decir que es casi un campo pero la multiplicación no es conmutativa.
De forma similar podemos definir los cuaternios sobre otros campos. Cuando se definen sobre $\mathbb{Z}_p$

$$W_p = \{a + bi + cj + dk | a, b, c, d \in \mathbb{Z}_p\}$$

tenemos un anillo finito y no conmutativo para todo $p > 2$.

Es un resultado conocido que si un anillo finito con unidad R tiene como únicos ideales derechos a (0) y R, entonces R es un anillo con división.
Aplicando este resultado a W_p los cuaternios sobre $\mathbb{Z}_p$.
Notamos que este es un anillo finito con unidad que NO ES CONMUTATIVO, lo que implica por el teorema de Wedderburn que R no es un anillo con división. Luego, W_p tiene un ideal izquierdo no trivial.

Anillo de Hurwitz

Sea $\zeta = \frac{1}{2}(1 + i + j + k)$, definimos

$$H = \{a\zeta + bi + cj + dk | a, b, c, d \in \mathbb{Z}\}$$

Llamado el anillo de Hurwitz de cuaternios reales. Nótese que $H \subseteq Q$ es un subanillo de Q. Este anillo es sumamente especial, pues es un anillo con división y norma, pero no es conmutativo. Esto permite caracterizar completamente a sus ideales izquierdos, lo cual será la herramienta clave para demostrar el teorema de Lagrange.

Norma en Q

Definición

Sea $x = a + bi + cj + dk \in Q$, definimos el adjunto de x como $x* = a - bi - cj - dk$

- $x** = x$
- $(ax + by)* = ax* + by*$
- $(xy)* = y*x*$

Definición

Sea $x \in Q$, definimos la norma de x como

$$N(x) = xx* = a^2 + b^2 + c^2 + d^2$$

, y notamos que es un número real positivo.

También notamos que $x^{-1} = \frac{1}{N(x)}x*$

Identidad de Lagrange

Para $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4$ números reales, tenemos que

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 +$$

$$(a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 +$$

$$(a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 +$$

$$(a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2 . (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2 .$$

Es decir, el producto de sumas de 4 cuadrados es la suma de 4 cuadrados. Para demostrarlo absta con notar que el enunciado es equivalente a

$$N(x)N(y) = xx*(yy*) = x(yy*)x* = (xy)(y*x*) = (xy)(xy)* = N(xy), x, y \in Q$$

El anillo de Hurwitz

Ahora veremos las propiedades más importantes del anillo de Hurwitz, que nos llevarán a caracterizar sus ideales izquierdos.

Teorema

Para $x \in H$, $x* \in H$ y $N(x) \in \mathbb{Z}^+$

Este teorema lleva a que H tiene (algunos) inversos multiplicativos, cuando $N(x) = 1$.

Teorema

(ALGORTIMO DE LA DIVISIÓN IZQUIERDA) Sean $a, b \in H$ con $b \neq 0$. Entonces existen $c, d \in H$ tales que $a = cb + d$ y $N(d) < N(b)$

Basta con notar que N cumple las funciones de $d - valor$ en H, y que es casi un anillo euclideano excepto que H no es conmutativo.

El anillo de Hurwitz

Teorema

Sea L un ideal izquierdo de H. Entonces existe un elemento $u \in L$ tal que todo elentento en L es un múltiplo izquierdo de u : en otras palabras, existe $u \in L$ tal que todo $x \in L$ es de la forma $ru, r \in H$.

Demostración Si $L = (0)$ nada hay que probar. simplemente hacemos $u = 0$. Podemos pues suponer que L tiene elementos distintos del cero. Las normas de los elementos distintos de cero son enteros positivos de donde hay un elemento $u \neq 0$ en L cuya norma es minima entre las de los elementos distintos de cero de L. Si $x \in L$, $x = cu + d$ donde $N(d) < N(u)$. Pero d esta en L porque x y u, y por tanto cu, estan en L que es un ideal izquierdo. Luego $N(d) = 0$ y, por tanto, $d = 0$. De donde es una consecuencia que $x = cu$.

Un resultado de Euler

Teorema

Si $2a = x_0^2 + x_1^2 + x_2^2 + x_3^2$ con a, x_0, x_1, x_2, x_3 números enteros, entonces $a = y_0^2 + y_1^2 + y_2^2 + y_3^2$

Demostración:

Como $2a$ es par, tenemos 3 casos: todos los x son pares, todos los x son impares, o hay 2 x pares y 2 x impares. En cualquier caso podemos renumerar y aparear los x para hacer:

$$y_0 = \frac{x_0 + x_1}{2}, y_1 = \frac{x_0 - x_1}{2}, y_2 = \frac{x_2 + x_3}{2}, y_3 = \frac{x_2 - x_3}{2}$$

con todos los y enteros.

Teorema de Lagrange

Teorema

Todo entero positivo puede escribirse como la suma de los cuadrados de cuatro enteros.

Demostración:
Por la identidad de Lagrange, podemos reducir el problema a demostrar que todo número primo p puede escribirse como la suma de cuatro cuadrados enteros, pues cualquier otro número entero es producto de primos.
Podemos descartar rápidamente el caso de 2 con $2 = 1^2 + 1^2 + 0^2 + 0^2$. Con lo que limitamos el problema a los primos impares.

El teorema de Lagrange

Sea p un primo impar. Definamos el siguiente ideal bilateral V de H como

$$V = \{x_0\zeta + x_1 i + x_2 j + x_3 k : p | x_0, x_1, x_2, x_3\}$$

, y notamos que H/V es isomorfo a W_p (De forma similar a como Z/pZ es $\mathbb{Z}_p$). Por lo que V no puede ser maximal, de lo contrario $H/V \equiv W_p$ sería un campo.
Entonces existe un ideal izquierdo L de H tal que $V \subset L \subset H$.
Entonces, existe un elemento $u \in L$ tal que todo elemento de L es un múltiplo izquierdo de u, nótese que $u \ni nV$ pues de lo contrario $Ru = V \neq L$. Si $p \in V \implies p \in L \implies \exists c \in H \ni p = cu$. c no puede tener un inverso en H, pues de lo contrario $u = c^{-1}p$ estaría en V.

El teorema de Lagrange

De lo anterior, como c no tiene inverso en H, $N(c) > 1$. De forma análoga como u no puede tener inverso en H, porque entonces $L = H$. Entonces $N(c) > 1$. Ahora como $p = cu$, tenemos

$$p^2 = N(p) = N(cu) = N(c)N(u)$$

como p es primo y $N(c), N(u)$ son enteros, debe de ser el caso que $p = N(c) = N(u)$
Expresamos u de forma extendida
$u = m_0\zeta + m_1 i + m_2 j + m_3 k, m_0, m_1, m_2, m_3 \in \mathbb{Z}$ Luego
$2u = (m_0 + m_0 i + m_0 j + m_0 k) + 2m_1 i + 2m_2 j + 2m_3 k =$
$m_0 + (2m_1 + m_0)i + (2m_2 + m_0)j + (2m_3 + m_0)k$ con lo que calculamos

$$N(2u) = m_0^2 + (2m_1 + m_0)^2 + (2m_2 + m_0)^2 + (2m_3 + m_0)^2 = N(2)N(p) = 4p$$

El teorema de Lagrange

Hasta ahora tenemos que $4p$ es la suma de 4 cuadrados, $4p = m_0^2 + (2m_1 + m_0)^2 + (2m_2 + m_0)^2 + (2m_3 + m_0)^2$, con el resultado de Euler, tenemos que $2p$ también es la suma de 4 cuadrados, y luego p también es la suma de 4 cuadrados.

Referencias

- Herstein, I. N. (1991). Topics in Algebra (2nd ed.) [E-book]. John Wiley Sons.
- HARDY, G. H. y WRIGHT, E. M., An Introduction lo the The theory of Numbers, segunda edicion. Clarendon Press, Oxford, Inglaterra, 1945.
- ALBERT, A. A., Fundamental Concepts of Higher Algebra. University of Chicago Press, Chicago, 1956.