LOS IDEALES PRIMOS DE $\mathbb{Z}[i]$ Y SUS CUERPOS DE RESIDUOS

MARIANO SUÁREZ-ÁLVAREZ

1. Primos que son sumas de dos cuadrados

Si p es un primo impar y $a \in \mathbb{Z}$ es coprimo con p, ponemos

$$(a/p) = \begin{cases} 1, & \text{si existe } x \in \mathbb{Z} \text{ tal que } a \equiv x^2 \mod p; \\ -1, & \text{en caso contrario.} \end{cases}$$

Llamamos a (a/p) el ***símbolo de Legendre***.

Proposición 1 (Euler, 1748 [1, 2])**.** *Si p es un primo impar y $a \in \mathbb{Z}$ es coprimo con p, entonces*

$$a^{(p-1)/2} \equiv (a/p) \mod p$$

Demostración. Si $a \in \mathbb{F}_p^\times$ es un cuadrado, de manera que existe $x \in \mathbb{F}_p^\times$ con $x^2 = a$, entonces $a^{(p-1)/2} = x^{p-1} = 1$ por el teorema de Fermat. Bastará entonces que probemos que $a^{(p-1)/2} = -1$ si a no es un cuadrado.

Ahora bien, el polinomio $f(X) = X^{(p-1)/2} - 1 \in \mathbb{F}_p[X]$ tiene a lo sumo $(p-1)/2$ raíces en $\mathbb{F}_p$, y acabamos de mostrar que cada uno de los cuadrados de $\mathbb{F}_p^\times$ es una raíz de f. Como hay exactamente $(p-1)/2$ cuadrados en $\mathbb{F}_p^\times$, vemos que las raíces de f son *precisamente* esos cuadrados.

Si ahora $a \in \mathbb{F}_p^\times$ no es un cuadrado, del teorema de Fermat sabemos que

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 = 0,$$

y como $a^{(p-1)/2} - 1 = f(a) \neq 0$, debe ser $a^{(p-1)/2} + 1 = 0$, como queríamos. □

Proposición 2 (Fermat, 1640)**.** *Un primo impar es suma de dos cuadrados sii es congruente a* 1 *módulo* 4 *.*

Este teorema fue anunciado por Fermat, aunque no dio ninguna prueba. La primera prueba conocida fue dada por Euler en 1749 en [3]. La prueba que damos abajo es de Richard Dedekind, y apareció en el Suplemento XI a las *Vorlesungen über Zahlentheorie* de Peter Gustav Lejeune Dirichlet en 1894.

Demostración. Un cuadrado es congruente a 0 o a 1 módulo 4, así que la suma de dos cuadrados es congruente a 0, a 1 o a 2. Si esa suma es un primo impar, debe ser entonces congruente a 1 módulo 4. Esto prueba la necesidad de la condición. Vamos ahora la suficiencia.

Date: 29 de agosto, 2014.

Sea $n \in \mathbb{N}$ tal que $p = 4n + 1$. Como sólo la mitad de los elementos de $\mathbb{F}_p^\times$ son cuadrados, la proposición anterior nos dice que existe $a \in \mathbb{Z}$ coprimo con p tal que $a^{(p-1)/2} \equiv -1 \mod p$. El número $m = a^n$ es entonces tal que $p \mid m^2 + 1$.

En particular, tenemos que $p \nmid m$, así que $p \nmid m + i$ y $p \nmid m - i$ en $\mathbb{Z}[i]$. Como $p \mid (m + i)(m - i)$, esto nos dice que p no es primo en $\mathbb{Z}[i]$. El anillo $\mathbb{Z}[i]$ es un dominio de factorización única, así que existen primos $p_1, \ldots, p_r$ de $\mathbb{Z}[i]$ tales que $p = p_1 \cdots p_r$. Tomando normas, vemos que $p^2 = N(p) = N(p_1) \cdots N(p_r)$ y, como cada una de las normas $N(p_j)$ es un entero positivo distinto de 1, esto implica inmediatamente que $r = 2$. Como $p_1 p_2$ es un número real positivo, p_1 y p_2 tienen que ser números complejos conjugados y si $p_1 = x + iy$, con x, $y \in \mathbb{Z}$, entonces es inmediato que $p = x^2 + y^2$. □

2. Los ideales primos de $\mathbb{Z}[i]$ y sus cuerpos de residuos

Si A es un anillo conmutativo, escribimos $\operatorname{Spec} A$ al conjunto de todos los ideales primos de A. Si $\phi : A \to B$ es un morfismo de anillos conmutativos, entonces para cada $\mathfrak{p} \in \operatorname{Spec} B$ la preimagen $\phi^{-1}(\mathfrak{p})$ es un elemento de $\operatorname{Spec} A$, así que ϕ induce una función $\phi^* : \mathfrak{p} \in \operatorname{Spec} B \mapsto \phi^{-1}(\mathfrak{p}) \in \operatorname{Spec} A$. Notemos que si A es un subanillo de B y ϕ es la inclusión, entonces $\phi^*(\mathfrak{p}) = \mathfrak{p} \cap A$ para todo $\mathfrak{p} \in \operatorname{Spec} B$.

Proposición 3. *La función*

$$\iota^* : \mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[i] \longmapsto \mathfrak{p} \cap \mathbb{Z} \in \operatorname{Spec} \mathbb{Z}$$

inducida por la inclusión $\iota : \mathbb{Z} \to \mathbb{Z}[i]$ es sobreyectiva. Si p es un primo racional, hay dos posibilidades:

- (*i*) *Si $p \equiv 3 \mod 4$, entonces la fibra de $p\mathbb{Z}$ por ι^* tiene exactamente un elemento, el ideal $p\mathbb{Z}[i]$. Cualquier generador de este ideal tiene norma p^2.*
- (*ii*) *Si $p \equiv 1 \mod 4$ o si $p = 2$, entonces la fibra de $p\mathbb{Z}$ por ι^* tiene exactamente dos elementos. Si $p = x^2 + y^2$ con x, $y \in \mathbb{Z}$, entonces esos dos elementos son los ideales $(x + iy)$ y $(x - iy)$. Cualquiera de los generadores de estos dos ideaes tiene norma p.*

Finalmente, la preimagen del ideal nulo de $\mathbb{Z}$ por ι^* tiene un elemento, el ideal nulo de $\mathbb{Z}[i]$.

Demostración. Sea $p \in \mathbb{N}$ un primo racional y sea $p = p_1 \cdots p_r$ la factorización de p como producto de elementos irreducibles en $\mathbb{Z}[i]$. Tomando norma, vemos que $p^2 = N(p) = N(p_1) \cdots N(p_r)$ y, como cada uno de lo $N(p_j)$ es un entero mayor que 1 (porque los p_j no son unidades) vemos que $r \leq 2$. Si $r = 2$, el producto $p_1 p_2$ es un número real positivo, así que p_1 y p_2 son complejos conjugados; si $p_1 = x + iy$, entonces $p = p_1 p_2 = x^2 + y^2$. Recíprocamente, si existen x, $y \in \mathbb{Z}$ tales que $p = x^2 + y^2$, entonces $a = x + iy \in \mathbb{Z}[i]$ es un irreducible —porque su norma es p— y $p = a\bar{a}$, así que $r = 2$; notemos que esto último implica que la escritura de p como suma de dos cuadrados es única salvo signos y permutación. Concluimos así que p es irreducible en $\mathbb{Z}[i]$ si $p \equiv 3 \mod 4$, y que es producto de exactamente dos irreducibles si $p \equiv 1 \mod 4$.

Sea ahora $\mathfrak{p}$ un ideal primo de $\mathbb{Z}[i]$ tal que $\mathfrak{p} \cap \mathbb{Z} = (p)$. Como $\mathfrak{p}$ es primo, no nulo y propio, existe un elemento irreducible $a \in \mathbb{Z}[i]$ tal que $\mathfrak{p} = (a)$ y, como $p \in \mathfrak{p}$,

tenemos que a divide a p en $\mathbb{Z}[i]$. Así, todo elemento de la fibra de (p) por ι^* está generado por un divisor irreducible de p. En consecuencia, si $p \equiv 3 \mod 4$ la fibra de (p) tiene exactamente un elemento, el ideal $p\mathbb{Z}[i]$, y si $p \equiv 1 \mod 4$ la fibra de (p) tiene dos elementos, los ideales $(x+iy)$ y $(x-iy)$, con $x, y \in \mathbb{Z}$ tales que $x^2+y^2=p$. Esto prueba las dos primeras afirmaciones del enunciado.

Por otro lado, si $\mathfrak{p}$ es un ideal primo no nulo de $\mathbb{Z}[i]$, de manera que existe $a = x+it \in \mathfrak{p}$ distinto de cero, entonces $0 \neq a\bar{a} = x^2+y^2 \in \mathfrak{p} \cap \mathbb{Z}$, y esto prueba que $\mathfrak{p} \cap \mathbb{Z} \neq 0$. Vemos así que el único ideal en la fibra de 0 por ι^* es el ideal nulo. □

Proposición 4. *Sea p un número primo y sea $\mathfrak{p}$ un ideal primo no nulo de $\mathbb{Z}[i]$ tal que $\mathfrak{p} \cap \mathbb{Z} = (p)$. El cuerpo $K = \mathbb{Z}[i]/\mathfrak{p}$ tiene característica p. Si $p \equiv 3 \mod 4$, entonces K es una extensión cuadrática de su cuerpo primo, y si $p \equiv 1 \mod 4$, entonces K coincide con su cuerpo primo.*

Demostración. Como $p \in \mathfrak{p}$, es claro que $p = 0$ en $K = \mathbb{Z}[i]/\mathfrak{p}$, así que necesariamente la característica de K debe ser p. Si $a \in \mathbb{Z}[i]$ es un elemento irreducible de $\mathbb{Z}[i]$ tal que $\mathfrak{p} = (a)$, hay una sucesión exacta

$$0 \longrightarrow \mathbb{Z}[i] \xrightarrow{m_a} \mathbb{Z}[i] \longrightarrow K \longrightarrow 0$$

en la que la aplicación m_a es la multiplicación por a, $m_a : x \in \mathbb{Z}[i] \mapsto ax \in \mathbb{Z}[i]$. Como grupo abeliano, $\mathbb{Z}[i]$ tiene al conjunto $\{1, i\}$ como base, y con respecto a esa base, la matrix de la función m_a es

$$A = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

Sabemos entonces que el orden del grupo abeliano K es igual a

$$|\det A| = x^2+y^2 = N(a).$$

De acuerdo a la proposición anterior, sabemos que $N(a) = p^2$ si $p \equiv 3 \mod 4$ y que $N(a) = p$ si $p \equiv 1 \mod 4$. Esto prueba la proposición. □

Referencias

[1] Leonard Euler. *Theoremata circa divisores numerorum.* Novi Commentarii academiae scientiarum Petropolitanae 1, 1750, pp. 20-48. Disponible en http://eulerarchive.maa.org/pages/E134.html

[2] Leonard Euler. *Theoremata circa residua ex divisione potestatum relicta.* Novi Commentarii academiae scientiarum Petropolitanae 7, 1761, pp. 49-82. Disponible en http://eulerarchive.maa.org/pages/E262.html

[3] Leonard Euler. Carta a Goldbach. Disponible en http://www.math.dartmouth.edu/~euler/correspondence/letters/OO0852.pdf