Polinomios generadores de primos de Euler

Alejandro Aguilar Zavoznik

En 1772, Euler notó que el polinomio

$$f(x) = x^2 - x + 41$$

toma valores primos para $-39 \leq x \leq 0$.
Estos son:

41	43	47	53
61	71	83	97
113	131	151	173
197	223	251	281
313	347	383	421
461	503	547	593
641	691	743	797
853	911	971	1033
1097	1163	1231	1301
1373	1447	1523	1601

En 1798, Legendre afirmo lo mismo para

$$g(x) = x^2 + x + 41$$

con $0 \leq x \leq 39$.
Estas dos observaciones son equivalentes ya que $f(x) = g(-x)$.

En 1913, Rabinovitch, relacionó las observaciones anteriores con el problema de clasificar los campos cuadráticos imaginarios que son dominios de ideales principales.

En 1913, Rabinovitch, relacionó las observaciones anteriores con el problema de clasificar los campos cuadráticos imaginarios que son dominios de ideales principales. En 1966 y 1967, Baker y Stark probaron de forma independiente que los únicos campos cuadráticos imaginarios que tienen esta propiedad son

$$\mathbb{Q}(\sqrt{d}), \qquad d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

En 1913, Rabinovitch, relacionó las observaciones anteriores con el problema de clasificar los campos cuadráticos imaginarios que son dominios de ideales principales. En 1966 y 1967, Baker y Stark probaron de forma independiente que los únicos campos cuadráticos imaginarios que tienen esta propiedad son

$$\mathbb{Q}(\sqrt{d}), \qquad d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Uniendo lo anterior, los únicos polinomios de la forma

$$f(x) = x^2 + x + p$$

tales que $f(x)$ es primo para $0 \leq x \leq p - 2$ son aquellos con $p = 2, 3, 5, 11, 17, 41$.

Esta plática se dividirá en dos partes:

1. Antecedentes: Factorización utilizando ideales.
2. Demostración del teorema sobre polinomios de Euler (omitiendo la parte que corresponde al teorema de Stark).

Campos cuadráticos

Sea $d \in \mathbb{Z}$ libre de cuadrados.

$$\mathbb{F} = \mathbb{Q}(\sqrt{d}) = \left\{ a_1 + a_2\sqrt{d} : a_1, a_2 \in \mathbb{Q} \right\}$$

es un campo cuadrático.

1. Si $d > 0$, $\mathbb{F}$ es un campo cuadrático real.
2. Si $d < 0$, $\mathbb{F}$ es un campo cuadrático imaginario.

Anillo de enteros

Si $\mathbb{F}$ es un campo cuadrático, su anillo de enteros, denotado $\mathcal{O}_{\mathbb{F}}$, se define como:

$$\mathcal{O}_{\mathbb{F}} = \{\alpha \in \mathbb{F} : \alpha \text{ es raíz de } f(x) = x^2 + rx + t, \text{ para algunos } r, t \in \mathbb{Z}\}.$$

Si d es de la forma

$$d = 4n + 1$$

para algún $n \in \mathbb{Z}$, el anillo de enteros es

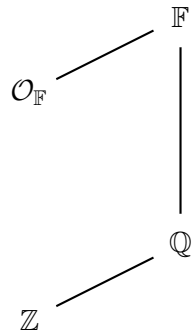
$$\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) = \left\{ a_1 + a_2\left(\frac{1+\sqrt{d}}{2}\right) : a_1, a_2 \in \mathbb{Z} \right\}.$$

Por otra parte, si d es

$$d = 4n + 2 \quad \text{o} \quad d = 4n + 3,$$

$\mathcal{O}_{\mathbb{F}}$ es

$$\mathbb{Z} + \mathbb{Z}\sqrt{d} = \left\{ a_1 + a_2\sqrt{d} : a_1, a_2 \in \mathbb{Z} \right\}.$$



Nos interesa estudiar la factorización en números primos de los elementos de $\mathcal{O}_{\mathbb{F}}$. A los elementos del conjunto $\mathbb{Z}$ les llamaremos enteros racionales para evitar confundirlos con los enteros algebraicos.

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{10})$. El anillo de enteros de $\mathbb{F}$ es

$$\mathcal{O}_{\mathbb{F}} = \mathbb{Z} + \mathbb{Z}\sqrt{10} = \left\{ a_1 + a_2\sqrt{10} : a_1, a_2 \in \mathbb{Z} \right\}.$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{10})$. El anillo de enteros de $\mathbb{F}$ es

$$\mathcal{O}_{\mathbb{F}} = \mathbb{Z} + \mathbb{Z}\sqrt{10} = \left\{ a_1 + a_2\sqrt{10} : a_1, a_2 \in \mathbb{Z} \right\}.$$

El polinomio irreducible de

$$\frac{2}{3} + \frac{5}{4}\sqrt{10}$$

es

$$x^2 - \frac{4}{3}x - \frac{1093}{72}.$$

por lo que éste es un número algebraico, pero no es un entero algebraico.

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{10})$. El anillo de enteros de $\mathbb{F}$ es

$$\mathcal{O}_{\mathbb{F}} = \mathbb{Z} + \mathbb{Z}\sqrt{10} = \left\{ a_1 + a_2\sqrt{10} : a_1, a_2 \in \mathbb{Z} \right\}.$$

El polinomio irreducible de

$$\frac{2}{3} + \frac{5}{4}\sqrt{10}$$

es

$$x^2 - \frac{4}{3}x - \frac{1093}{72}.$$

por lo que éste es un número algebraico, pero no es un entero algebraico.

Por otro lado,

$$7 + 16\sqrt{10}$$

es raíz de

$$x^2 - 14x - 2511,$$

por lo que es un entero algebraico y está en $\mathcal{O}_{\mathbb{F}}$.

El polinomio irreducible de

$$3 + 5\left(\frac{1+\sqrt{10}}{2}\right)$$

es

$$x^2 - 11x - \frac{129}{4}$$

así, no es un entero algebraico.

Dado $\mathbb{F} = \mathbb{Q}(\sqrt{-15})$, su anillo de enteros es

$$\mathcal{O}_{\mathbb{F}} = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-15}}{2}\right) = \left\{a_1 + a_2\left(\frac{1+\sqrt{-15}}{2}\right) : a_1, a_2 \in \mathbb{Z}\right\}.$$

Dado $\mathbb{F} = \mathbb{Q}(\sqrt{-15})$, su anillo de enteros es

$$\mathcal{O}_{\mathbb{F}} = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-15}}{2}\right) = \left\{a_1 + a_2\left(\frac{1+\sqrt{-15}}{2}\right) : a_1, a_2 \in \mathbb{Z}\right\}.$$

En este caso

$$7 - 3\left(\frac{1+\sqrt{-15}}{2}\right)$$

está en Ω pues su polinomio irreducible es

$$x^2 - 11x + 64.$$

Aritmética en campos cuadráticos

Dado un anillo de enteros $\mathcal{O}_{\mathbb{F}}$ y $\alpha, \beta \in \mathcal{O}_{\mathbb{F}}$, diremos que α divide a β si existe $\gamma \in \mathcal{O}_{\mathbb{F}}$ tal que

$$\beta = \alpha\gamma.$$

Usaremos la notación $\alpha \mid \beta$ para indicar que α divide a β.

Aritmética en campos cuadráticos

Dado un anillo de enteros $\mathcal{O}_{\mathbb{F}}$ y $\alpha, \beta \in \mathcal{O}_{\mathbb{F}}$, diremos que α divide a β si existe $\gamma \in \mathcal{O}_{\mathbb{F}}$ tal que

$$\beta = \alpha\gamma.$$

Usaremos la notación $\alpha \mid \beta$ para indicar que α divide a β.

Por ejemplo, en el anillo de enteros de $\mathbb{F} = \mathbb{Q}(\sqrt{26})$

$$722 + 13\sqrt{26} = (3 + 4\sqrt{26})(-2 + 7\sqrt{26}).$$

Dado lo anterior,

$$3 + 4\sqrt{26} \mid 722 + 13\sqrt{26},$$
$$-2 + 7\sqrt{26} \mid 722 + 13\sqrt{26}.$$

Dados, $\alpha, \beta, \omega \in \mathcal{O}_{\mathbb{F}}$, diremos que α es congruente con β módulo ω, denotado

$$\alpha \equiv \beta \pmod{\omega},$$

si se cumple

$$\omega \mid (\alpha - \beta).$$

Dados, $\alpha, \beta, \omega \in \mathcal{O}_{\mathbb{F}}$, diremos que α es congruente con β módulo ω, denotado

$$\alpha \equiv \beta \pmod{\omega},$$

si se cumple

$$\omega \mid (\alpha - \beta).$$

El criterio sobre la forma del anillo de enteros se puede reescribir:

$$\begin{array}{ll} d = 4n + 1 & d \equiv 1 \pmod{4} \\ d = 4n + 2 & d \equiv 2 \pmod{4} \\ d = 4n + 3 & d \equiv 3 \pmod{4} \end{array}$$

Por ejemplo, si $\mathbb{F} = \mathbb{Q}(\sqrt{10})$,

$$\alpha = 2 + a\sqrt{10}, \qquad \beta = 2 + b\sqrt{10},$$

entonces

$$\alpha - \beta = (a - b)\sqrt{10},$$

por lo que

$$\alpha \equiv \beta \pmod{\sqrt{10}}.$$

Por ejemplo, si $\mathbb{F} = \mathbb{Q}(\sqrt{10})$,

$$\alpha = 2 + a\sqrt{10}, \qquad \beta = 2 + b\sqrt{10},$$

entonces

$$\alpha - \beta = (a - b)\sqrt{10},$$

por lo que

$$\alpha \equiv \beta \pmod{\sqrt{10}}.$$

$$1 + 2\sqrt{10} \equiv 11 + 3\sqrt{10} \pmod{\sqrt{10}}$$

pues

$$1 + 2\sqrt{10} - (11 + 3\sqrt{10}) = -10 - \sqrt{10} = \sqrt{10}\left(-\sqrt{10} - 1\right).$$

Ideales

Dado un anillo de enteros $\mathcal{O}_{\mathbb{F}}$, un ideal es un conjunto $\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{F}}$ que cumple:

1. $\mathfrak{a}$ es un anillo.
2. Si se multiplica $\alpha \in \mathfrak{a}$ por $\beta \in \mathcal{O}_{\mathbb{F}}$, el resultado

$$\alpha\beta \in \mathfrak{a}.$$

De aquí en adelante, cuando usemos la palabra ideal nos referiremos a ideales distintos de $\{0\}$.

En $\mathbb{Z}$, el conjunto de los números pares

$$\mathfrak{a} = 2\mathbb{Z} = \{2a : a \in \mathbb{Z}\}$$

es un ideal.

1. Si sumamos, restamos o multiplicamos dos números pares, el resultado está en $2\mathbb{Z}$.
2. Si multiplicamos un par por un entero, el producto es par.

Al conjunto de los múltiplos de 2 en $\mathbb{Z}$ lo denotaremos

$$\mathfrak{a} = \langle 2 \rangle .$$

Dado $n \in \mathbb{Z}$, el ideal generado por n es el conjunto

$$\mathfrak{a} = \langle n \rangle = \{na : a \in \mathbb{Z}\}.$$

Los elementos de $\mathfrak{a}$ son los múltiplos de n.

Dado $n \in \mathbb{Z}$, el ideal generado por n es el conjunto

$$\mathfrak{a} = \langle n \rangle = \{na : a \in \mathbb{Z}\}.$$

Los elementos de $\mathfrak{a}$ son los múltiplos de n.

1. $\mathfrak{a}$ es un anillo, la suma, resta o multiplicación de dos elementos de $\mathfrak{a}$ está en $\mathfrak{a}$.
2. Si $a \in \mathfrak{a}$ y $b \in \mathbb{Z}$, entonces $a = nc$ para algún $c \in \mathbb{Z}$.

$$ab = ncb = n(cb),$$

de donde $ab \in \mathfrak{a}$.

Otra forma usual de representar al ideal generado por n es

$$\langle n \rangle = n\mathbb{Z}.$$

El ideal generado por $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$ se define como:

$$\langle a, b \rangle = \{ax + by : x, y \in \mathbb{Z}\}.$$

El ideal generado por $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$ se define como:

$$\langle a, b \rangle = \{ax + by : x, y \in \mathbb{Z}\}.$$

En general

$$\langle a_1, a_2, \ldots, a_n \rangle = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : a_i \in \mathbb{Z}, i = 1, 2, \ldots n\}.$$

$$\langle a, b\rangle = \{ax + by : x, y \in \mathbb{Z}\}.$$

Como

$$m = \text{mcd}(a, b) = ax + by$$

para algunos $x, y \in \mathbb{Z}$, y m divide a cualquier combinación lineal de a y b, entonces

$$\langle a, b\rangle = \Big\langle \text{mcd}(a, b) \Big\rangle.$$

$$\langle a, b\rangle = \{ax + by : x, y \in \mathbb{Z}\}.$$

Como

$$m = \text{mcd}(a, b) = ax + by$$

para algunos $x, y \in \mathbb{Z}$, y m divide a cualquier combinación lineal de a y b, entonces

$$\langle a, b\rangle = \Big\langle \text{mcd}(a, b) \Big\rangle.$$

Otra forma de representar el ideal generado por dos elementos es

$$a\mathbb{Z} + b\mathbb{Z}.$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{10})$ y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros.
El ideal generado por $4 + 5\sqrt{10}$ es el conjunto:

$$\left\langle 4 + 5\sqrt{10} \right\rangle_{\mathbb{F}} = \left(4 + 5\sqrt{10}\right) \mathcal{O}_{\mathbb{F}} = \left\{ \left(4 + 5\sqrt{10}\right) \alpha : \alpha \in \mathcal{O}_{\mathbb{F}} \right\}.$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{10})$ y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros.
El ideal generado por $4 + 5\sqrt{10}$ es el conjunto:

$$\left\langle 4 + 5\sqrt{10} \right\rangle_{\mathbb{F}} = \left(4 + 5\sqrt{10}\right) \mathcal{O}_{\mathbb{F}} = \left\{ \left(4 + 5\sqrt{10}\right) \alpha : \alpha \in \mathcal{O}_{\mathbb{F}} \right\}.$$

El ideal generado por varios elementos se define de forma análoga

$$\left\langle 4 + 5\sqrt{10}, 26 + 7\sqrt{10} \right\rangle_{\mathbb{F}} = \left(4 + 5\sqrt{10}\right) \mathcal{O}_{\mathbb{F}} + \left(26 + 7\sqrt{10}\right) \mathcal{O}_{\mathbb{F}} = \left\langle 2 + \sqrt{10} \right\rangle_{\mathbb{F}}.$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{10})$ y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros.
El ideal generado por $4 + 5\sqrt{10}$ es el conjunto:

$$\left\langle 4 + 5\sqrt{10} \right\rangle_{\mathbb{F}} = \left(4 + 5\sqrt{10}\right) \mathcal{O}_{\mathbb{F}} = \left\{ \left(4 + 5\sqrt{10}\right) \alpha : \alpha \in \mathcal{O}_{\mathbb{F}} \right\}.$$

El ideal generado por varios elementos se define de forma análoga

$$\left\langle 4 + 5\sqrt{10}, 26 + 7\sqrt{10} \right\rangle_{\mathbb{F}} = \left(4 + 5\sqrt{10}\right) \mathcal{O}_{\mathbb{F}} + \left(26 + 7\sqrt{10}\right) \mathcal{O}_{\mathbb{F}} = \left\langle 2 + \sqrt{10} \right\rangle_{\mathbb{F}}.$$

Lo anterior es debido a que

$$\operatorname{mcd}\left(4 + 5\sqrt{10}, 26 + 7\sqrt{10}\right) = 2 + \sqrt{10}.$$

Dados $\alpha, \beta \in \mathcal{O}_{\mathbb{F}}$, no siempre existe $\operatorname{mcd}(\alpha, \beta)$.

Dado un ideal $\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{F}}$, diremos que $\mathfrak{a}$ es un ideal principal si existe $\alpha \in \mathfrak{a}$ tal que

$$\mathfrak{a} = \langle \alpha \rangle_{\mathbb{F}} .$$

Unidades

Dado un anillo de enteros $\mathcal{O}_{\mathbb{F}}$, diremos que μ es una unidad si existe $\mu^{-1} \in \mathcal{O}_{\mathbb{F}}$ tal que

$$\mu\mu^{-1} = 1.$$

Al conjunto de unidades de $\mathcal{O}_{\mathbb{F}}$ lo denotaremos $\mathcal{O}_{\mathbb{F}}^*$.

Unidades

Dado un anillo de enteros $\mathcal{O}_{\mathbb{F}}$, diremos que μ es una unidad si existe $\mu^{-1} \in \mathcal{O}_{\mathbb{F}}$ tal que

$$\mu\mu^{-1} = 1.$$

Al conjunto de unidades de $\mathcal{O}_{\mathbb{F}}$ lo denotaremos $\mathcal{O}_{\mathbb{F}}^*$.

Dado $\mathbb{F} = \mathbb{Q}(\sqrt{2})$,

$$\mu = 7 + 5\sqrt{2}$$

es una unidad en $\mathcal{O}_{\mathbb{F}}$ pues

$$(7 + 5\sqrt{2})(-7 + 5\sqrt{2}) = -49 + 25(2) = 1$$

donde

$$\mu^{-1} = -7 + 5\sqrt{2}.$$

De hecho, si $\mathbb{F} = \mathbb{Q}(\sqrt{2})$,

$$\mathcal{O}_{\mathbb{F}}^{*} = \left\{ \pm \left(1 + \sqrt{2}\right)^{n} : n \in \mathbb{Z} \right\}.$$

Es decir, hay un número infinito de unidades. En particular

$$\mu = 7 + 5\sqrt{2} = \left(1 + \sqrt{2}\right)^{3}.$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Si $d > 0$, existe una unidad μ tal que

$$\mathcal{O}_{\mathbb{F}}^{*} = \{\pm\mu^{n} : n \in \mathbb{Z}\}.$$

En este caso, diremos que μ es la unidad fundamental de $\mathbb{F}$.

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Si $d > 0$, existe una unidad μ tal que

$$\mathcal{O}_{\mathbb{F}}^{*} = \{\pm\mu^{n} : n \in \mathbb{Z}\}.$$

En este caso, diremos que μ es la unidad fundamental de $\mathbb{F}$.
Si $d < 0$,

$$\mathcal{O}_{\mathbb{F}} = \begin{cases} \{\pm 1, \pm i\} & d = -1 \\ \left\{\pm 1, \pm\dfrac{1+\sqrt{-3}}{2}, \pm\dfrac{1-\sqrt{-3}}{2}\right\} & d = -3 \\ \{\pm 1\} & d \notin \{-1, -3\} \end{cases}$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Si $d > 0$, existe una unidad μ tal que

$$\mathcal{O}_{\mathbb{F}}^* = \{\pm\mu^n : n \in \mathbb{Z}\}.$$

En este caso, diremos que μ es la unidad fundamental de $\mathbb{F}$.
Si $d < 0$,

$$\mathcal{O}_{\mathbb{F}} = \begin{cases} \{\pm 1, \pm i\} & d = -1 \\ \left\{\pm 1, \pm\dfrac{1+\sqrt{-3}}{2}, \pm\dfrac{1-\sqrt{-3}}{2}\right\} & d = -3 \\ \{\pm 1\} & d \notin \{-1, -3\} \end{cases}$$

Las unidades de $\mathbb{Z}$ son:

$$\mathbb{Z}^* = \{\pm 1\}.$$

Si $\mathcal{O}_{\mathbb{F}}$ es un anillo de enteros, $\alpha \in \mathcal{O}_{\mathbb{F}}$, $\mu \in \mathcal{O}_{\mathbb{F}}^*$, entonces

$$\langle \alpha\mu \rangle_{\mathbb{F}} = \langle \alpha \rangle_{\mathbb{F}} .$$

Si $\mathcal{O}_{\mathbb{F}}$ es un anillo de enteros, $\alpha \in \mathcal{O}_{\mathbb{F}}$, $\mu \in \mathcal{O}_{\mathbb{F}}^*$, entonces

$$\langle \alpha\mu \rangle_{\mathbb{F}} = \langle \alpha \rangle_{\mathbb{F}} .$$

$$\langle 2 \rangle = \langle -2 \rangle .$$

Si $\mathcal{O}_{\mathbb{F}}$ es un anillo de enteros, $\alpha \in \mathcal{O}_{\mathbb{F}}$, $\mu \in \mathcal{O}_{\mathbb{F}}^*$, entonces

$$\langle \alpha\mu \rangle_{\mathbb{F}} = \langle \alpha \rangle_{\mathbb{F}} .$$

$$\langle 2 \rangle = \langle -2 \rangle .$$

Si $\mathbb{F} = \mathbb{Q}(\sqrt{2})$

$$\left\langle 3 + 7\sqrt{2} \right\rangle_{\mathbb{F}} = \left\langle -1 + 2\sqrt{2} \right\rangle_{\mathbb{F}}$$

pues

$$-1 + 2\sqrt{2} = \left(3 + 7\sqrt{2}\right)\left(3 - 2\sqrt{2}\right) = \left(3 + 7\sqrt{2}\right)\left(1 + \sqrt{2}\right)^{-2} .$$

Si $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$,

$$\langle 5 \rangle_{\mathbb{K}} = \left\langle \frac{5 - 5\sqrt{3}}{2} \right\rangle_{\mathbb{K}}$$

ya que

$$\frac{5 - 5\sqrt{3}}{2} = 5\left(\frac{1 - \sqrt{3}}{2}\right).$$

Elementos asociados

Si $\mathcal{O}_{\mathbb{F}}$ es un anillo de enteros, diremos que α, β son asociados si existe una unidad μ tal que

$$\alpha = \mu\beta.$$

Elementos asociados

Si $\mathcal{O}_{\mathbb{F}}$ es un anillo de enteros, diremos que α, β son asociados si existe una unidad μ tal que

$$\alpha = \mu\beta.$$

En $\mathbb{Z}$, 2 y -2 son asociados.

En $\mathbb{Q}(\sqrt{2})$, $3 + 7\sqrt{2}$ y $-1 + 2\sqrt{2}$ son asociados.

En $\mathbb{Q}(\sqrt{-3})$, 5 y $\dfrac{5 - 5\sqrt{3}}{2}$ son asociados.

Congruencia módulo un ideal

La definición de congruencia se puede redefinir usando ideales. Dado $\mathcal{O}_{\mathbb{F}}$ un anillo de enteros, $\alpha, \beta \in \mathcal{O}_{\mathbb{F}}$ y $\mathfrak{a}$ un ideal de $\mathcal{O}_{\mathbb{F}}$, diremos que

$$\alpha \equiv \beta \pmod{\mathfrak{a}}$$

si

$$\alpha - \beta \in \mathfrak{a}.$$

Esta es una relación de equivalencia.

Norma de un ideal

Dado un anillo de enteros $\mathcal{O}_{\mathbb{F}}$, un ideal $\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{F}}$ y $\alpha \in \mathcal{O}_{\mathbb{F}}$, la clase de equivalencia de α se define como

$$[\alpha]_{\mathfrak{a}} = \Big\{ \beta \in \mathcal{O}_{\mathbb{F}} : \alpha \equiv \beta \pmod{\mathfrak{a}} \Big\}.$$

Norma de un ideal

Dado un anillo de enteros $\mathcal{O}_{\mathbb{F}}$, un ideal $\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{F}}$ y $\alpha \in \mathcal{O}_{\mathbb{F}}$, la clase de equivalencia de α se define como

$$[\alpha]_{\mathfrak{a}} = \Big\{ \beta \in \mathcal{O}_{\mathbb{F}} : \alpha \equiv \beta \pmod{\mathfrak{a}} \Big\}.$$

El cociente de $\mathcal{O}_{\mathbb{F}}$ con $\mathfrak{a}$ es

$$\mathcal{O}_{\mathbb{F}}/\mathfrak{a} = \Big\{ [\alpha]_{\mathfrak{a}} : \alpha \in \mathcal{O}_{\mathbb{F}} \Big\}.$$

Norma de un ideal

Dado un anillo de enteros $\mathcal{O}_{\mathbb{F}}$, un ideal $\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{F}}$ y $\alpha \in \mathcal{O}_{\mathbb{F}}$, la clase de equivalencia de α se define como

$$[\alpha]_{\mathfrak{a}} = \left\{ \beta \in \mathcal{O}_{\mathbb{F}} : \alpha \equiv \beta \pmod{\mathfrak{a}} \right\}.$$

El cociente de $\mathcal{O}_{\mathbb{F}}$ con $\mathfrak{a}$ es

$$\mathcal{O}_{\mathbb{F}}/\mathfrak{a} = \left\{ [\alpha]_{\mathfrak{a}} : \alpha \in \mathcal{O}_{\mathbb{F}} \right\}.$$

La cardinalidad del cociente es finita y le llamamos la norma de $\mathfrak{a}$:

$$\mathrm{N}(\mathfrak{a}) = \left| \mathcal{O}_{\mathbb{F}}/\mathfrak{a} \right|.$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros.
Las clases módulo $\mathfrak{a} = \langle 2 \rangle_{\mathbb{F}}$ son

$$0, \qquad 1, \qquad \sqrt{d}, \qquad 1 + \sqrt{d}.$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros.
Las clases módulo $\mathfrak{a} = \langle 2 \rangle_{\mathbb{F}}$ son

$$0, \qquad 1, \qquad \sqrt{d}, \qquad 1 + \sqrt{d}.$$

$$17 + 28\sqrt{d} \;=\; 2(8 + 14\sqrt{d}) + 1 + 0\sqrt{d}.$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros.
Las clases módulo $\mathfrak{a} = \langle 2 \rangle_{\mathbb{F}}$ son

$$0, \qquad 1, \qquad \sqrt{d}, \qquad 1 + \sqrt{d}.$$

$$\begin{aligned} 17 + 28\sqrt{d} &= 2(8 + 14\sqrt{d}) + 1 + 0\sqrt{d}. \\ 33 + 5\sqrt{d} &= 2(16 + 2\sqrt{d}) + 1 + 1\sqrt{d}. \end{aligned}$$

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros.
Las clases módulo $\mathfrak{a} = \langle 2 \rangle_{\mathbb{F}}$ son

$$0, \qquad 1, \qquad \sqrt{d}, \qquad 1+\sqrt{d}.$$

$$\begin{aligned} 17+28\sqrt{d} &= 2(8+14\sqrt{d})+1+0\sqrt{d}. \\ 33+5\sqrt{d} &= 2(16+2\sqrt{d})+1+1\sqrt{d}. \end{aligned}$$

$$\mathrm{N}\big(\langle 2 \rangle_{\mathbb{F}}\big) = 4.$$

Producto de ideales

Si $\mathfrak{a}, \mathfrak{b}$ son ideales de $\mathcal{O}_{\mathbb{F}}$, definimos el producto como

$$\mathfrak{ab} = \left\{ \sum_{k=1}^{m} \alpha_i \beta_i : \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{b} \right\}.$$

Producto de ideales

Si $\mathfrak{a}, \mathfrak{b}$ son ideales de $\mathcal{O}_{\mathbb{F}}$, definimos el producto como

$$\mathfrak{ab} = \left\{ \sum_{k=1}^{m} \alpha_i \beta_i : \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{b} \right\}.$$

En $\mathbb{Z}$

$$\langle a \rangle \langle b \rangle$$

los elementos son una suma de números de la forma

$$(ax)(by) = ab(xy)$$

por lo que

$$\langle a \rangle \langle b \rangle = \langle ab \rangle .$$

Así, el producto de ideales en $\mathbb{Z}$ es un reflejo del producto de elementos en $\mathbb{Z}$.
Lo mismo sucede con los ideales en cualquier anillo de enteros.

El conjunto $\mathbb{Z}$ es un dominio de factorización única (DFU), esto quiere decir que cualquier elemento se puede factorizar de forma única como producto de primos.

El conjunto $\mathbb{Z}$ es un dominio de factorización única (DFU), esto quiere decir que cualquier elemento se puede factorizar de forma única como producto de primos.

$$10 = (2)(5) = (5)(2) = (-5)(-2).$$

El conjunto $\mathbb{Z}$ es un dominio de factorización única (DFU), esto quiere decir que cualquier elemento se puede factorizar de forma única como producto de primos.

$$10 = (2)(5) = (5)(2) = (-5)(-2).$$

Cuando decimos factorización única, debemos de entender que el orden es irrelevante y, por otra parte, si los factores se cambian por números asociados apropiados, encontraremos otra, pero consideraremos que estas son iguales.

Consideremos el anillo de enteros de $\mathbb{F} = \mathbb{Q}(\sqrt{10})$.

$$10 = (2)(5) = (\sqrt{10})^2.$$

Consideremos el anillo de enteros de $\mathbb{F} = \mathbb{Q}(\sqrt{10})$.

$$10 = (2)(5) = (\sqrt{10})^2.$$

Si 2 y $\sqrt{10}$ son asociados, existe $\mu \in \mathcal{O}_{\mathbb{F}}^*$ tal que

$$2 = \mu\sqrt{10} \qquad \mu = \frac{2}{\sqrt{10}}.$$

El polinomio irreducible de $\frac{2}{\sqrt{10}}$ es

$$f(x) = x^2 - \frac{2}{5},$$

por lo que no es un entero algebraico; esto quiere decir que 2 y $\sqrt{10}$ no son asociados.

Bibliografía

1. Alaca, S., Williams, K.S., Introductoty Algebraic Number Theory. Cambridge University Press, 2003.
2. Ireland, K., Rosen, M.. A classical introduction to modern number theory. GTM 84 Springer Verlag, 1990.
3. Stewart, I., Tall, D.. Algebraic number theory. A K Peters, 2020.
4. Ribenboim, P.. El famoso polinomio generador de primos de Euler y el número de clase de los cuerpos cuadráticos imaginarios. Revista Colombiana de Matemáticas. Vol. XXI, 1987. p.p. 263-284.