Álgebra I

Factorización

En $\mathbb{Z}[\sqrt{n}]$

Ejemplo: $11+7i$ $(\mathbb{Z}[i])$

1.- Calcular su norma

$$N(11+7i)=(11+7i)\cdot(11-7i)=11^2+7^2$$

$$N(11+7i)=170$$

2.- Descomponer su norma en primos (En $\mathbb{Z}$)

$$170=2\cdot5\cdot17$$

3.- Cogemos el primer primo (2) y buscamos $\alpha\in\mathbb{Z}[i]$ tq $N(\alpha)=2$, es decir: $\alpha=a+bi\Longrightarrow N(\alpha)=\boxed{a^2+b^2}$

$$a^2+b^2=2\Longrightarrow a=\pm1\wedge b=\pm1$$

$a=1$ $b=1$ $\quad a=-1$ $b=-1$

$a=-1$ $b=1$ $\quad a=1$ $b=-1$

$$\begin{pmatrix}1+i & -1-i\\ -1+i & 1-i\end{pmatrix}$$

4.- Buscamos asociados

(En este caso todos son asociados)

$$1+i\xrightarrow{\cdot-1}-1-i,\quad 1+i\xrightarrow{\cdot i}-1+i,\quad 1+i\xrightarrow{\cdot -i}1-i\Longrightarrow\alpha=1+i$$

5.- Comprobamos la divisibilidad de α

$$\frac{11+7i}{1+i}\cdot\frac{1-i}{1-i}=\frac{11+7i-11i+7}{2}=\frac{18-4i}{2}=9-2i$$

Como $9-2i \in \mathbb{Z}[i] \Longrightarrow 1+i \mid 11+7i$

$$11+7i = (1+i)(9-2i)$$

Ahora nos centraremos en $9-2i$

6.- Repetimos:

$$N(9-2i) = 9^2+2^2 = 85 = 5 \cdot 17$$

$$\alpha \in \mathbb{Z}[i] \quad \text{tq} \quad N(\alpha) = a^2+b^2 = 5$$

$a=1$	$b=2$	$a=2$	$b=1$
$a=1$	$b=-2$	$a=2$	$b=-1$
$a=-1$	$b=2$	$a=-2$	$b=1$
$a=-1$	$b=-2$	$a=-2$	$b=-1$

$\cdot i$ $\quad$ $\cdot i$ $\quad$ $\cdot(-i)$

$\boxed{1+2i}$	$2+i$	$\alpha_1 = 1+2i$
$1-2i$	$\boxed{2-i}$	$\alpha_2 = 2+i$
$-1+2i$	$\boxed{-2+i}$	
$\boxed{-1-2i}$	$-2-i$	

$$\frac{9-2i}{1+2i} \cdot \frac{1-2i}{1-2i} = \frac{9-2i-18i-4}{5} = \frac{5-20i}{5} = 1-4i \quad \boxed{\checkmark}$$

$$\frac{9-2i}{2+i} \cdot \frac{2-i}{2-i} = \frac{18-4i+9i-2}{5} = \frac{16-13i}{5} \notin \mathbb{Z}[i] \quad \boxed{\times}$$

$$1+2i \mid 9-2i \Longrightarrow 9-2i = (1+2i)(1-4i)$$

$$11+7i = (1+i)(1+2i)(1-4i)$$

Álgebra I

$\boxed{\text{MCD y MCM}}$

Ejemplo $(2i, 11+7i)$ y $[2i, 11+7i]$

1.- Factorizamos ambos ($11+7i$ factorizado en el ejercicio anterior)

$2i$: $N(2i) = 2^2 = 4 \Longrightarrow 4 = 2^2 = 2 \cdot 2$

$(\alpha \in \mathbb{Z}[i] \quad \alpha = a+b$ tq $a^2+b^2 = 2$

$\alpha = 1+i$ y asociados

$$\frac{2i}{1+i} \cdot \frac{1-i}{1-i} = \frac{2i+2}{2} = 1+i \Longrightarrow 2i = (1+i)^2$$

2.- Reexpresamos lo que nos piden:

$(2i, 11+7i) = ((1+i)^2, (1+i)(1+2i)(1-4i)) = (1+i)$ //

$[2i, 11+7i] = [(1+i)^2, (1+i)(1+2i)(1-4i)] =$

$= (1+i)^2(1+2i)(1-4i) = 4+18i$ //

MCD $\longrightarrow$ factores comunes con su mínimo exponente

MCM $\longrightarrow$ factores comunes y no comunes con su máximo exponente

Ejemplo: 180 en $\mathbb{Z}[\sqrt{-2}]$

$$180 = 2\cdot 90 = \cancel{2^2 3}\ 2^2\cdot 3^2\cdot 5$$

$$N(2) = 4 \Longrightarrow \alpha\in\mathbb{Z}[\sqrt{-2}] \Longrightarrow N(\alpha) = a^2+2b^2 = 2$$
$$(\alpha = a + b\sqrt{-2})$$

$$a^2+2b^2 = 2 \Longrightarrow a = 0 \wedge b = \pm 1 \Longrightarrow \begin{array}{l}\sqrt{-2}\\ -\sqrt{-2}\end{array}$$

$$\frac{2}{\sqrt{-2}}\cdot\frac{-\sqrt{-2}}{-\sqrt{-2}} = \frac{2\cdot(-\sqrt{-2})}{2} = -\sqrt{-2} \Longrightarrow 2 = \sqrt{-2}\cdot(-\sqrt{-2})$$
$$2 = -(\sqrt{-2})^2$$

$N(3) = 9 \Longrightarrow$ O 3 irreducible o producto de irreducibles

$$\alpha\in\mathbb{Z}[+\sqrt{-2}] \quad N(\alpha) = a^2+2b^2 = 3$$

$$a = \pm 1 \quad b = \pm 1 \Longrightarrow \cdot(-1)\begin{pmatrix} 1+\sqrt{-2} \\ -1-\sqrt{-2}\end{pmatrix} \quad \begin{pmatrix} 1-\sqrt{-2} \\ -1+\sqrt{-2}\end{pmatrix}\cdot(-1)$$

$$\frac{3}{1+\sqrt{-2}}\cdot\frac{1-\sqrt{-2}}{1-\sqrt{-2}} = \frac{3-3\sqrt{-2}}{3} = 1-\sqrt{-2}$$

$$3 = (1+\sqrt{-2})(1-\sqrt{-2})$$

Con el 5, nos damos cuenta de que

$\nexists\,\alpha\in\mathbb{Z}[\sqrt{-2}]$ tq $N(\alpha) = 5 \Longrightarrow 5$ es irreducible

$$180 = (+5)(-\sqrt{-2})^4(1+\sqrt{-2})^2(1-\sqrt{-2})^2 \ /\!/$$

Álgebra I

Factorización de polinomios

En $\mathbb{R}[x]$, los irreducibles son grado 1 y grado 2 de la forma ax^2+bx+c tq $b^2-4ac<0$

Luego, los mónicos $(a=1)$ irreducibles son $x+d$ y x^2+bx+c tq $b^2-4c<0$

Con el criterio de Ruffini podemos listar todos los irreducibles mónicos de grado 2:

- En $\mathbb{Z}_2[x]$: x^2+x+1
- En $\mathbb{Z}_3[x]$: x^2+1, x^2+x+2, x^2+2x+2

Y de grado 3

- En $\mathbb{Z}_2[x]$: x^3+x+1, x^3+x^2+1
- En $\mathbb{Z}_3[x]$: x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+2x^2+1, x^3+x^2+x+2, x^3+x^2+2x+1, x^3+2x^2+x+1, x^3+2x^2+2x+2

Ejemplo 1.- $f=x^4+x^3+x^2+x+1\in\mathbb{Z}_2[x]$

$$\left.\begin{array}{l} f(0)=1\neq 0 \Longrightarrow x\nmid f \\ f(1)=5\neq 0 \Longrightarrow x-1\nmid f \end{array}\right\} \nexists\, p(x)\in\mathbb{Z}_2 \text{ tq } gr(p(x))=1 \wedge p(x)\mid f$$

Y como no hay de grado 1, tampoco habrá de grado 3.

Quedaría la opción de grado 2: x^2+x+1, sin embargo: $f=(x^2+x+1)x^2+(x+1)$

f será irreducible.

Álgebra I

Ejemplo 4: $f = x^5 + 8x^4 + 18x^3 + 11x^2 + 7x + 3$ en $\mathbb{Z}[x]$

En $\mathbb{Q}(x)$, las posibles raices serán ± 1 y ± 3
Probando, obtenemos que $f(-3) = 0$

$$f = (x+3)g \Longrightarrow g = x^4 + 5x^3 + 3x^2 + 2x + 1$$

Las posibles raices de g serán ± 1, pero estas no lo ~~son~~ son al comprobar.
Por el criterio de módulos reducidos

$$R_2(g) = x^4 + x^3 + x^2 + 1 \Longrightarrow R_2(g)(1) = 0 \Longrightarrow x-1 \mid R_2(g)$$

Esto significa que $R_2(g)$ tiene ~~un div~~ de divisores $x-1$ y x^3+x+1 (Que se ha comprobado que es irreducible. No tiene divisores de grado 2, por lo que g tampoco los tiene y, por lo tanto, será irreducible

$$f = (x+3)(x^4 + 5x^3 + 3x^2 + 2x + 1) \text{ en } \mathbb{Z}[x] \;//$$

Criterio de Einstein

$f = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ $\quad a_n \neq 0 \quad c(f) = 1$

f será irreducible si $\exists p \in \mathbb{Z}$ primo tq

1) $p \mid a_i \ \forall i \in \{0, 1, \dots, n-1\}$ pero $p^2 \nmid a_0$

ó

2) $p \mid a_i \ \forall i \in \{1, 2, \dots, n\}$ pero $p^2 \nmid a_n$

Ejemplo: $2x^5 - 6x^3 + 9x^2 - 15$ irreducible por el criterio de Einstein para el primo $p = 3$

Ejemplo 2: $3x^7 - 6x^5 + 14x^2 - 10x^2 + 2x - 18$

Como 2 divide a todos menos a $3x^7$ y $2^2 = 4$ no divide a 18, por el criterio de Einstein es irreducible.

Traslación en la indeterminada

$T_a(f)$ homomorfismo: $T_a : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$

$$T_a(x) = x + a \quad \forall a \in \mathbb{Z}$$

Sea $f \in \mathbb{Z}[x]$. Si $T_a(f)$ es irreducible para algún $a \in \mathbb{Z}$, entonces f también lo será

Ejemplo: $f = x^4 + 1$

$T_1(x^4+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$

Por el criterio de Einstein, $T_1(x^4+1)$ es irreducible por $p = 2 \Longrightarrow f$ también lo será