AYUDANTÍA XIV

GRUPOS Y ANILLOS (PRIMAVERA 2016)

En esta ayudantía seguiremos estudiando los dominios euclideanos. En particular analizaremos los ideales principales y el máximo común divisor.

1.- **Problema 1:**
Calcule el máximo común divisor entre $3+i$ y $5+i$ en $\mathbb{Z}[i]$. Use esto para determinar un generador del ideal $(3+i, 5+i)$ en $\mathbb{Z}[i]$.

Desarrollo: Observe que $2 = 5+i-(3+i)$. Luego si d divide a $5+i$ y $3+i$ entonces d divide a 2. Por otro lado 2 no divide a $5+i$ ni a $3+i$. Ahora bien $2 = -i(1+i)^2$, donde $(1+i)$ es maximal. Luego debemos buscar entre los divisores de este número el máximo común divisor de $5+i$ y $3+i$. Por otro lado $(1+i)(2-i) = 3+i$ y $(1+i)(3-2i) = 5+i$. Por lo tanto $(2) \subsetneq (3+i, 5+i) \subset (i+1)$. Pero $i+1 = 2(3+i)-(5+i)$. Luego $(3+i, 5+i) = (1+i)$. Esto prueba que el máximo común divosor entre $3+i$ y $5+i$ es $1+i$ y que $(3+i, 5+i) = (1+i)$.

1.- **Ejercicio:** Calcule el maáximo común divisor entre $3+w$ y $5+w$ en $\mathbb{Z}[w]$, donde $w = e^{\frac{2\pi i}{3}}$.

2.- **Problema 2:**
Calcule el máximo común divisor entre 1527 y 321 en $\mathbb{Z}$. Use algoritmo de división. Escriba el máximo común divisor como una combinación lineal entera de 1527 y 321.

Desarrollo: Useamos el algoritmo de división. En efecto tenemos que $1527 = 4\cdot 321 + 243$, $321 = 1\cdot 243 + 78$, $243 = 3\cdot 78 + 9$, $78 = 8\cdot 9 + 6$, $9 = 1\cdot 6 + 3$ y $6 = 2\cdot 3 + 0$. Por lo tanto el máximo común divisor entre 1527 y 321 es 3. Observe que de las igualdades anteriores se desprende la igualdad $3 = 37\cdot 1527 - 176\cdot 321$.

2.- **Ejercicio:** Calcule el máximo común divisor entre 15268976 y 31 en $\mathbb{Z}$.

3.- **Problema 3:**
Sea $A = \mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ y defina el ideal $I_2 = (2, 1+\sqrt{-5})$.
i.- Demuestre que I_2 es un ideal maximal de A.
ii.- Pruebe que I_2 no es un ideal principal.
iii.- Concluya que A no es un DE.
iv.- Pruebe que $I_2^2 = (2)$.

3.- **Desarrollo:**
i.- Observe que $A/I_2 \cong \mathbb{Z}[x]/(2, 1+x, x^2+5) \cong \mathbb{Z}/(2,6) = \mathbb{Z}/2\mathbb{Z}$. Por lo tanto A/I_2 es cuerpo. Esto último es equivalente a que I_2 sea un ideal maximal de A.

ii.- Supongamos que I_2 es un ideal principal, entonces $I_2 = (d)$, para cierto $d = a + b\sqrt{-5} \in A$. Entonces $2 = ad$ y $1 + \sqrt{-5} = bd$, para ciertos $a, b \in A$. Tomando norma compleja en las igualdades anteriores, obtenemos que $N(a)N(d) = 4$ y $N(b)N(d) = 6$. Luego $N(d) \in \{1, 2\}$. Observe que si $N(d) = d\overline{d} = 1$ entonces $d \in A$ es invertible. Por lo tanto $I_2 = (d) = A$, lo que es contradictorio con lo dicho en [i]. Por lo tanto $N(d) = 2$. Luego $a^2 + 5d^2 = 2$ tiene solución con $a, d \in \mathbb{Z}$, lo que es falso. Por ello I_2 no es un ideal principal.

iii.- Sabemos que en un DE todo ideal es principal. Luego si A fuera un DE entonces I_2 sería un ideal principal, lo que contradice [ii].

iv.- Observe que $2 = (1+\sqrt{-5}-2)(1+\sqrt{-5}) - 2\cdot 2 \in I_2^2$. Por lo tanto $(2) \subseteq I_2^2$. Por otro lado, tenemos que el producto de dos elementos cualquiera de I_2 cumple con $(2z + (1+\sqrt{-5})w)(2a + (1+\sqrt{-5})b) = 4az + 2(aw(1+\sqrt{-5}) + zb(1+\sqrt{-5})) + 6wb + 2(1+\sqrt{5})wb \in (2)$. Esto prueba que $(2) \supseteq I_2^2$. Por lo tanto $I_2^2 = (2)$.

3.- **Ejercicio:** Pruebe que $I_3 = (3, 2+\sqrt{-5})$ y $I_3' = (3, 2-\sqrt{-5})$ son ideales maximales distintos y no principales en $\mathbb{Z}[\sqrt{-5}]$. Pruebe además que $I_3 I_3' = (3)$.

4.- **Problema 4:**
Demuestre las siguientes afirmaciones:

i.- Pruebe que $\left(\mathbb{C}[x]/(x^2+5)\right)[y]$ no es un DE.

ii.- Pruebe que $\left(\mathbb{Q}[x]/(x^2+5)\right)[y]$ es un DE.

Desarrollo:

i.- Observe que $\mathbb{C}[x]/(x^2+5) = \mathbb{C}[x]/(x-\sqrt{-5})(x+\sqrt{-5})$, donde $(x-\sqrt{-5}) + (x+\sqrt{-5}) = (1)$. Por lo tanto $\mathbb{C}[x]/(x^2+5) \cong \mathbb{C}[x]/(x-\sqrt{-5}) \times \mathbb{C}[x]/(x+\sqrt{-5}) \cong \mathbb{C}\times\mathbb{C}$. Luego $\mathbb{C}[x]/(x^2+5)$ no es dominio de integridad. Por lo tanto $\left(\mathbb{C}[x]/(x^2+5)\right)[y]$ no es dominio de integridad. En particular no es un dominio euclideano.

ii.- Sabemos que $A = \left(\mathbb{Q}[x]/(x^2+5)\right)[y]$ es un dominio euclideano si y solamente si $B = \mathbb{Q}[x]/(x^2+5)$ es un cuerpo. Es decir A es un DE si y solamente si (x^2+5) es un ideal maximal de $\mathbb{Q}[x]$. Supongamos que (x^2+5) no es maximal, entonces existe un ideal J tal que $(x^2+5) \subsetneq J \subsetneq \mathbb{Q}[x]$. Pero como $\mathbb{Q}[x]$ es un DE tenemos que $J = r(x)$. Luego $r(x)s(x) = x^2+5$. Pero $deg(r(x)) > 1$, pues $J \neq \mathbb{Q}[x]$. Por lo tanto $deg(r(x)) = deg(s(x)) = 1$. Esto implica que existe un racional $u \in \mathbb{Q}$ tal que $u^2 = -5$, lo que nos lleva a una contradicción. Por lo tanto (x^2+5) es maximal en $\mathbb{Q}[x]$. Por lo tanto A es un DE.

4.- **Ejercicio:** Encuentre el máximo común divisor entre x^2+1 y $p(x) = x^3 + (i+5)x^2 + (7+5i)x + 7i$ en $\mathbb{C}[x]$. Evalue $p(x)$ en $\pm i$ y luego divida.