Tema 8.- Enteros algebraicos. Los anillos $\mathbb{Z}[i]$ y $\mathbb{Z}[w]$. Aplicaciones a la teoría de números: suma de cuadrados.

8.1 Enteros algebraicos.

El papel que juegan los números enteros en el cuerpo $\mathbb{Q}$, lo juegan los enteros algebraicos en los cuerpos de números.

Sea K un cuerpo de números.

Definición 8.1.1.– Un número $\alpha \in K$ se dice *entero algebraico* (sobre $\mathbb{Z}$) si es raíz de un polinomio **mónico** con coeficientes enteros.

Nota 8.1.2.–

1. Todo número $\alpha \in K$ era raíz de un polinomio con coeficientes enteros, pero no necesariamente mónico.
2. Los números enteros son, evidentemente, enteros algebraicos. Enseguida veremos que son los únicos enteros algebraicos que hay en $\mathbb{Q}$.
3. Los enteros de Gauss son enteros algebraicos. En efecto, si $z = a+bi \in \mathbb{Z}[i]$, entonces se verifica que $z^2 - 2az + (a^2 + b^2) = 0$. También veremos que son los únicos enteros algebraicos que hay en $\mathbb{Q}(i)$.

Lema 8.1.3.– Sea $g \in \mathbb{Z}[X]$ mónico. Si $g = fh$ con $f, h \in \mathbb{Q}[X]$ y f mónico, entonces $f \in \mathbb{Z}[X]$.

DEMOSTRACIÓN: Es una consecuencia elemental del lema de Gauss (cfr. Ejercicio 12 del tema I). □

Corolario 8.1.4.– Sea $z \in \mathbb{C}$ algebraico y $f \in \mathbb{Q}[X]$ su polinomio mínimo. Entonces z es un entero algebraico si y sólo si $f \in \mathbb{Z}[X]$.

DEMOSTRACIÓN: Es una consecuencia del lema anterior y de la proposición **??**.2. □

Corolario 8.1.5.– Un número $a \in \mathbb{Q}$ es entero algebraico si y sólo si $a \in \mathbb{Z}$.

Ejemplo 8.1.6.–

1. El número $z = \frac{1+i\sqrt{3}}{2}$ es un entero algebraico, porque su polinomio mínimo es $X^2 - X + 1$.
2. El número $z = \frac{1+i\sqrt{5}}{2}$ no es un entero algebraico, porque su polinomio mínimo es $X^2 - X + \frac{3}{2}$.

Corolario 8.1.7.– Un número $z \in \mathbb{Q}(i)$ es entero algebraico si y sólo si $z \in \mathbb{Z}[i]$.

DEMOSTRACIÓN: Sea $z = a + bi$ un entero algebraico, con $a, b \in \mathbb{Q}$ y $b \neq 0$. Su polinomio mínimo es $X^2 - 2aX + (a^2 + b^2) \in \mathbb{Z}[X]$, luego $2a = n \in \mathbb{Z}$ y $a^2 + b^2 = m \in \mathbb{Z}$. De aquí se tiene que $(2b)^2 - 4m + n^2 = 0$, por lo que $2b$ es

entero algebraico y por la nota 8.1.2.2 $2b = p \in \mathbb{Z}$. Si p es impar, reduciendo módulo 4 la igualdad $p^2 - 4m + n^2 = 0$ se llega a contradicción. Luego p es par, por lo que $b \in \mathbb{Z}$, y n es par, por lo que $a \in \mathbb{Z}$. □

Proposición 8.1.8.– Sea K un cuerpo de números. Cada elemento $z \in K$ puede ser escrito en la forma $\frac{w}{d}$ donde w es un entero algebraico y $d \in \mathbb{Z}$.

DEMOSTRACIÓN: Si $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Q}[X]$ es el polinomio mínimo de z, quitando denominadores, se tiene que $df(X) = dX^n + p_1 X^{n-1} + \cdots + p_n \in \mathbb{Z}[X]$. Por tanto

$$g(X) = d^n f(X) = (dX)^n + p_1 (dX)^{n-1} + \cdots + p_n d^{n-1} \in \mathbb{Z}[X],$$

sigue teniendo a z como raíz. Luego $dz = w$ es un entero algebraico. □

Ahora hallaremos todos los enteros algebraicos en los cuerpos cuadráticos.

Proposición 8.1.9.– Sea $d \in \mathbb{Z}$ libre de cuadrados. Los enteros algebraicos en $\mathbb{Q}(\sqrt{d})$ son los números de

1. $\mathbb{Z}[\sqrt{d}] = \{p + q\sqrt{d}, \forall p, q \in \mathbb{Z}\}$ si $d \not\equiv 1 (\bmod 4)$.
2. $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{p + q(\frac{1+\sqrt{d}}{2}), \forall p, q \in \mathbb{Z}\}$ si $d \equiv 1 (\bmod 4)$.

DEMOSTRACIÓN: Si $z = p + q\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ con $q \neq 0$, su polinomio mínimo es $X^2 - 2pX + p^2 - q^2 d$, luego es un entero algebraico. Si $z = p + q(\frac{1+\sqrt{d}}{2}) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, su polinomio mínimo es $X^2 - (2p+q)X + p^2 + pq - q^2 \frac{(1-d)}{4}$. Suponiendo que $d \equiv 1 (\bmod 4)$, se tiene que z es un entero algebraico.

Recíprocamente, supongamos que $z = \frac{a+b\sqrt{d}}{2} \in \mathbb{Q}(\sqrt{d})$ es un entero algebraico, con $a, b \in \mathbb{Q}$ y $b \neq 0$. Su polinomio mínimo es $X^2 - aX + \frac{a^2 - b^2 d}{4}$. Luego $a \in \mathbb{Z}$ y $a^2 \equiv db^2 (\bmod 4)$, o bien $db^2 = 4n - a^2$. Poniendo $b = b_1/b_2$, con $b_1, b_2 \in \mathbb{Z}$ y $\mathrm{mcd}(b_1, b_2) = 1$, se tiene que $db_1^2 = b_2^2(4n - a^2)$. Luego $b_2^2 | d$ que por ser libre de cuadrados, implica que $b_2 = \pm 1$, es decir $b \in \mathbb{Z}$.

Si $d \equiv 1 (\bmod 4)$, $a^2 \equiv b^2 (\bmod 4)$ por lo que a y b tienen la misma paridad, luego

$$z = \frac{a + b\sqrt{d}}{2} = \left(\frac{a-b}{2}\right) + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

Si $d \equiv 2, 3 (\bmod 4)$, $a^2 \equiv db^2 (\bmod 4)$ conduce a $a, b \in \mathbb{Z}2$, luego $z \in \mathbb{Z}[\sqrt{d}]$.
□

Corolario 8.1.10.– El conjunto de enteros algebraicos de un cuerpo cuadrático es un anillo. En particular $\mathbb{Z}[i]$ es el anillo de enteros algebraicos de $\mathbb{Q}(i)$, como habíamos anunciado en la nota 8.1.2.

8.2 El anillo $\mathbb{Z}[i]$.

En el tema 2 habíamos visto que el anillo $\mathbb{Z}[i]$ es un dominio euclídeo, y por tanto un DIP y un DFU. Así mismo en la proposición **??**.2 vimos que las unidades de

$\mathbb{Z}[i]$ son los números $z \in \mathbb{Z}[i]$ con $N(z) = 1$; luego las unidades de $\mathbb{Z}[i]$ son ± 1, $\pm i$.

Queremos describir los elementos irreducibles de $\mathbb{Z}[i]$. Ya vimos en la citada proposición que los enteros de Gauss de norma prima son irreducibles. Veamos otros elementos irreducibles en $\mathbb{Z}[i]$.

Proposición 8.2.1.– Sea $p \in \mathbb{Z}_+$ primo. Las condiciones siguientes son equivalentes:

1. p **no** es irreducible en $\mathbb{Z}[i]$.
2. p es suma de dos cuadrados.
3. $p = 2$ o $p \equiv 1 (\bmod 4)$.

Demostración:

$1 \Rightarrow 2$. Si $p = (a + bi)(c + di)$, con ambos factores no unidades, se tiene que $N(a + bi) > 1$ y $N(c + di) > 1$. Tomando normas al principio: $p^2 = N(p) = (a^2 + b^2)(c^2 + d^2)$. Como p es primo, se tiene que $p = a^2 + b^2$.

$2 \Rightarrow 3$. Se deduce de observar que, si $a \in \mathbb{Z}$, $a^2 \equiv 0, 1 (\bmod 4)$.

$3 \Rightarrow 1$. Como $2 = (1+i)(1-i)$, basta considerar el caso $p \equiv 1 (\bmod 4)$. Por el lema de Wilson (cf. Ejercicio 2 del tema III y IV), $(p-1)! = (4q)! \equiv -1 (\bmod 4)$. Agrupando en el anterior factorial cada factor $j \leq 2q$ con $p - j = 4q + 1 - j$, se tiene que $-1 \equiv (4q)! \equiv [(2q)!]^2 (\bmod 4)$. Si r es el resto de dividir $(2q)!$ por p, se tiene $r^2 + 1 \equiv 0 (\bmod 4)$, que equivale a $p|(r^2 + 1) = (r + i)(r - i)$. Pero si $p|(r \pm i)$, $r \pm i = p(m + ni)$, y comparando las partes imaginarias, $pn = \pm 1$, que contradice que p es primo. Por tanto p divide a un producto en $\mathbb{Z}[i]$, pero no divide a ninguno de sus factores, luego p no es irreducible en $\mathbb{Z}[i]$. □

Corolario 8.2.2.– Un número primo $p \in \mathbb{Z}_+$ es irreducible en $\mathbb{Z}[i]$ si y sólo si $p \equiv 3 (\bmod 4)$.

Veamos finalmente que ya hemos descrito todos los numeros irreducibles de $\mathbb{Z}[i]$.

Proposición 8.2.3.– Un entero de Gauss es irreducible si y sólo si es de una de las dos formas siguientes:

1. Es asociado de un número primo $p > 0$, con $p \equiv 3 (\bmod 4)$, *i.e.* p, $-p$,ip, $-ip$.
2. Tiene norma prima.

Demostración: Queda probar que si $z = a+bi \in \mathbb{Z}[i]$ es irreducible, entonces es de una de las formas enunciadas. Si $a = 0$ o $b = 0$, entonces z es asociado con p.

Si $a \neq 0$ y $b \neq 0$, entonces $N(z) = a^2 + b^2 = (a + bi)(a - bi)$ es una descomposición en factores irreducibles. Por ser $\mathbb{Z}[i]$ un DFU, $N(z)$ debe ser un número primo, porque en otro caso una descomposición en $\mathbb{Z}$ sería distinta de la anterior. □

8.3 Sumas de cuadrados.

Enunciamos un problema de Diofanto (250 d.C.): *¿cuándo un número entero es suma de dos cuadrados? ¿de tres cuadrados? ¿de cuatro cuadrados?...*
Nota 8.3.1.– Para cada $a, b, c, d \in \mathbb{Z}$ se tiene que

$$(a^2+b^2)(c^2+d^2) = N(a+bi)N(c+di) = N((a+bi)(c+di)) = (ac-bd)^2+(ad+bc)^2.$$

Teorema 8.3.2.– *(Fermat-Euler 1749).* Un entero positivo n es suma de dos cuadrados, si y sólo si sus factores primos congruentes con 3 módulo 4, aparecen en la factorización de n con exponentes pares.

DEMOSTRACIÓN: Sea $n = m^2q$, de modo que los factores primos de q son 2 o congruentes con 1 módulo 4. Por la proposición 8.2.1 y la nota anterior, se tiene que n es suma de dos cuadrados.

Recíprocamente, supongamos que $n = a^2 + b^2$. La descomposición en $\mathbb{Z}[i]$ en factores irreducibles de $a + bi$ será, por la proposición 8.2.3,

$$a + bi = up_1 \cdots p_r(c_1 + d_1) \cdots (c_s + id_s),$$

donde u es una unidad, $p_1, \ldots, p_r \in \mathbb{Z}$ son números primos, con $p_i \equiv 3 (\bmod 4)$, para $i = 1, \ldots, r$, y $c_j + id_j \in \mathbb{Z}[i]$ son elementos de norma $c_j^2 + d_j^2$, para $j = 1, \ldots, s$, que por la proposición 8.2.1 no puede ser congruente con 3 módulo 4. Conjugando la expresión anterior, se obtiene una descomposición de $a - bi$, y multiplicándolas, queda:

$$n = (a + bi)(a - bi) = p_1^2 \cdots p_r^2(c_1^2 + d_1^2) \cdots (c_s^2 + d_s^2),$$

que verifica lo enunciado. □

Enunciamos sin demostrar los siguientes teoremas. La demostración del primero puede verse en el libro de Delgado-Fuertes-Xambó varias veces citado.
Teorema 8.3.3.– *(Fermat-Lagrange 1770).* Todo entero positivo es suma de cuatro cuadrados.

Teorema 8.3.4.– *(Waring-Hilbert 1909).* Para cada número natural q existe otro w_q tal que todo entero positivo n es suma de w_q potencias q-ésimas:

$$n = a_1^q + \cdots a_{w_q}^q.$$

Se sabe, por ejemplo que $w_2 = 4$, $w_3 = 9$ o que $w_4 = 19$ (1986).