# Álgebra Moderna II  19 abril

<u>Clase pasada:</u> $\alpha \in \mathbb{C}$ es un entero algebraico si es la raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$.

<u>EJEMPLOS:</u>

1) $n \in \mathbb{Z}$ es entero algebraico pues anula $f(x) = x - n$.

2) $\sqrt{d}$ con $d \in \mathbb{Z}$ es entero algebraico pues anula $f(x) = x^2 - d$

3) $\alpha = \frac{-1 \pm \sqrt{-3}}{2}$ ; $f(x) = x^2 + x + 1$.

---

<u>Hoy:</u> ¿Qué enteros algebraicos hay en $\mathbb{Q}[\sqrt{d}]$? con $d \in \mathbb{Z}$ libre de cuadrados.

Supongamos $\alpha \in \mathbb{C}$ & $f(\alpha) = 0$ con

$f(x)$ mónico en $\mathbb{Q}[x]$. irred.

¿Es $\alpha$ un entero algebraico?

Afirmación: $\alpha$ es un entero algebraico

$\Updownarrow$ =EJER=

$f(x) \in \mathbb{Q}[x]$ mónico e irred el cual anula $\alpha$ de hecho tiene coeficientes en $\mathbb{Z}$.

↳ Eg: $\frac{1}{2}$ NO es un entero algebraico pues $\{2x-1\} = f(x)$.

CONSECUENCIA: Calcularemos los enteros algebraicos del campo

$$\mathbb{Q}[\sqrt{d}] = \mathbb{Q} + \mathbb{Q}\sqrt{d} \qquad d \in \mathbb{Z}$$

libre de cuadrado.

$d = p_1 \cdots p_k$
sin repetidos.

OBSERVEMOS: $\mathbb{Z}+\mathbb{Z}[\sqrt{d}]$ son enteros algebraicos. (aunque ~~a veces~~ habrá ocasiones en las que obtendremos más)

$\boxed{\alpha = a+b\sqrt{d}}$ y $\alpha' = a-b\sqrt{d}$

Satisfacen $(x-\alpha)(x-\alpha') = \underbrace{x^2 - 2ax + a^2 - db^2}$

en $\mathbb{Z}[x]$ si $a,b \in \mathbb{Z}$.

irred. si $b \neq 0$.

entonces si $b \neq 0$,

$\boxed{\alpha \text{ es un entero algebraico}} \Longleftrightarrow \boxed{\begin{array}{c} 2a \in \mathbb{Z} \\ \& \\ a^2 - db^2 \in \mathbb{Z}. \end{array}}$

si $b=0 \Rightarrow \alpha = a$ es un entero algebraico ssi $a \in \mathbb{Z}$.

Caso (1) ($a$ par) $a \in \mathbb{Z}, \Rightarrow b^2 d \in \mathbb{Z}$ (pues $a^2 - db^2 \in \mathbb{Z}$)

$\Rightarrow b^2 \in \mathbb{Z}$ ($d$ es libre de cuadrados)

$\Rightarrow b \in \mathbb{Z}$.

Caso (2) $\quad a \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$ , i.e.

$2a = m$ es un entero impar.

entonces

$$a^2 = \frac{1}{4}m^2 \quad \text{y} \quad 4a^2 = m^2$$

es un entero.

Por tanto $\quad 4db^2$ es un entero y

$$db^2 = \frac{1}{4}n, \text{ con "}n\text{" impar.} \quad (*)$$

$\Rightarrow \quad b = \frac{1}{2}n_0$ , con "$n_0$" entero impar.

Entonces,

$$a^2 - db^2 = \frac{1}{4}m^2 - d\frac{1}{4}n_0^2$$

$$= \frac{1}{4}\underbrace{(m^2 - dn_0^2)}_{\text{entero divisible por 4.}}$$

Sin embargo,

$$m^2 \equiv n_0^2 \equiv 1 \pmod 4 \leftarrow \left(\begin{array}{c}\text{pues } m \text{ \& } \\ n_0 \text{ son} \\ \text{impares}\end{array}\right)$$

$$\Rightarrow \quad d \equiv 1 \pmod 4$$

OBSERVAR QUE $a = \frac{1}{2}m$ & $b = \frac{1}{2}n$.

satisface nuestras condiciones.

Eg: en $\mathbb{Z}[\alpha]$ con $\alpha^2 + \alpha + 1 = 0$,

$a = -\frac{1}{2}$ $b = \frac{1}{2}$ $d = -3$.

---

En Resumen: $d$ entero libre de cuadrados.

1) Si $d \equiv 2, 3 \pmod 4$, entonces los enteros algebraicos en $\mathbb{Q}[\sqrt{d}]$ forman el anillo $\mathbb{Z} + \mathbb{Z}[\sqrt{d}]$.

2) Si $d \equiv 1 \pmod 4$, entonces los enteros algebraicos en $\mathbb{Q}[\sqrt{d}]$ forman el anillo $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$.

El polinomio que ~~satisface~~ anula $\sqrt{d}$

es $x^2-d$.

$\hookrightarrow$ con discriminante $(=b^2-4ac)$

$4d=D$

El polinomio que $\frac{1+\sqrt{d}}{2}$ anula es

$x^2-x+\frac{(1-d)}{4}$ con discriminante

$1-(1-d)=d=D$

El entero $D$ tiene la siguiente propiedad:

a) $D\equiv 0,1 \pmod 4$

b) $D$ ~~es~~ tan libre de cuadrados como es posible dada la condición (a)

= LISTAREMOS LOS ENTEROS ALGEBRAICOS en $\mathbb{Q}[\sqrt{d}]$ USANDO el ENTERO $D$ =

$D<0$, los enteros alg en $\mathbb{Q}[\sqrt{d}] = \mathcal{O}_D$ se les llama

anillo cuadrático imaginario

$D>0$, $\mathcal{O}_D \subseteq \mathbb{Q}[\sqrt{d}]$ son

anillo cuadrático real.

---

$D<0$, $-3, -4, -7, -8, -11, -15, -19,$
$-20, -23, \ldots$

$\mathbb{Z}[\alpha]$ con $\alpha^2+\alpha+1=0$ $\quad$ $\mathbb{Z}[i]$

$D>0$

$5, 8, 12, 13, 17, 21, 24, 28, 29, \ldots$

Moraleja: $\exists$ una infinidad de anillos análogos a $\mathbb{Z}[i]$: ¡UNO POR CADA D PERMISIBLE!

PREGUNTA (GAUSS):

¿Cuales son los discriminantes $D<0$ tal que $\mathcal{O}_D \subseteq \mathbb{Q}[\sqrt{d}]$ el anillo de enteros algebraicos es DOMINIO DE IDEALES PRINCIPALES?

GAUSS: Conjeturó: $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$.

(NUEVE CASOS)

¿Cuales son los discriminantes $D<0$ tal que el anillo de enteros algebraicos $\mathcal{O}_D \subseteq \mathbb{Q}[\sqrt{d}]$ es Dominio euclidiano?

GAUSS: $D = -3, -4,$