Álgebra Moderna II 25 abril

Clase pasada: Describimos el anillo de enteros algebraicos en $\mathbb{Q}[\sqrt{d}]$ con $d \in \mathbb{Z}$ libre de cuadrados.

Hoy: Estudiaremos los ideales & las unidades del anillo de de enteros del campo $\mathbb{Q}[\sqrt{d}]$ para varios valores de d.

Los enteros algebraicos del campo $\mathbb{Q}[\sqrt{d}]$, con $d \in \mathbb{Z}$ libre de cuadrados, son

$$R = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & d \equiv 2, 4 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) & d \equiv 1 \pmod 4 \end{cases}$$

y forman un anillo.

Es decir $$R = \{ a + \sqrt{d} \mid \begin{matrix} a,b \in \mathbb{Z} \\ \text{o} \\ a,b \in \tfrac{1}{2}\mathbb{Z} - \mathbb{Z} \end{matrix} \quad d \equiv 1 \pmod 4 \}$$

Para simplificar, introducimos

$$D = \begin{cases} 4d \equiv 0 \pmod 4 & \leftarrow d \equiv 2,3 \pmod 4 \\ d \equiv 1 \pmod 4 \end{cases}$$

$$\sqrt{D} = \begin{cases} 2\sqrt{d} \\ \sqrt{d} \end{cases}$$

entonces

$$R_D = \mathbb{Z} + \mathbb{Z}\left(\frac{D + \sqrt{D}}{2}\right)$$

es el anillo de enteros algebraicos en $\mathbb{Q}[\sqrt{d}]$.

$D < 0$ Anillos cuadráticos imaginarios

$$D = -3, -4, -7, -8, -11, -15, -19,$$

$\uparrow$

$\mathbb{Z}[i]$

$d = -1$

Observar, existe una norma:

$$\delta := N : R \longrightarrow \mathbb{Z}$$

$$N(a+b\sqrt{d}) = a^2 - db^2 = (a+b\sqrt{d})(a-b\sqrt{d})$$

$$= \alpha \qquad = \alpha'$$

Nota: si $d \equiv 1 \pmod 4 \Rightarrow N(a+b\sqrt{d}) \in \mathbb{Z}$.

= EJER =

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$$

$$= (\alpha\cdot\beta)(\alpha\cdot\beta)' = \alpha\cdot\alpha'\cdot\beta\cdot\beta' = N(\alpha)N(\beta).$$

si $D<0 \Rightarrow N(\alpha) = (a+b\sqrt{d})(a-b\sqrt{d})$

$$= a^2 - db^2 \geq 0$$

Proposición: α es una unidad de R sii

$N(\alpha) = \pm 1$ (unidades de $\mathbb{Z}$).

Demostración: si $\alpha \in R$ es una unidad,

entonces $\exists\, \beta \in R$ t.q. $\alpha \cdot \beta = 1$.

Entonces

$$N(\alpha\beta) = N(\alpha) \cdot N(\beta) = 1$$

$$\Rightarrow N(\alpha) = N(\beta) = \pm 1.$$

Recíprocamente, si $N(\alpha) = \alpha \cdot \alpha' = 1$,

entonces α es una unidad.

COROLARIO: si $D<0$, $\alpha \in R$ es una unidad sii $N(\alpha)=1$.

Más aún, si

$D=-3$, existen 6 unidades

$D=-4$, existen 4 unidades

$D<-4$ " 2 unidades

La razón es: Una unidad $\alpha = a+b\sqrt{d}$ es una solución a

$$(*) \qquad \boxed{a^2-b^2d=1} \qquad a,b \in \mathbb{Z} \text{ ó } a,b \in \mathbb{Z}+\tfrac{1}{2}-\mathbb{Z}.$$

si $b=0 \Rightarrow a^2=1$; $a=\pm 1$.

$b\neq 0 \Rightarrow -b^2d \geq \frac{-d}{4}$ si $-d>4$ la ecuación $(*)$ no tiene solución ($d<0$.)

$|b| \geq \frac{1}{2}$

Si $D>0$, la ecuación $(*)$ tiene ~~un número~~ infinidad de soluciones.

Eg: $D=5$; $R=\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$

$\alpha=\frac{1+\sqrt{5}}{2}$ (razón aurea)

$\alpha\cdot\alpha'=\frac{1-5}{2}=-1 \Rightarrow \alpha$ es una unidad.

$\alpha^2=\frac{3+\sqrt{5}}{2}$ también es una unidad de R

(pues $N(\alpha)=-1$ $N(\alpha^2)=1$)

$\alpha^3=\frac{7+\sqrt{5}}{2}$ es unidad también.

α^n ¡es una unidad! con $n\in\mathbb{N}$.

↳ EJER: Aproximación diofantina.

Ideales de los enteros algebraicos = R_D con $D<0$.

$d=-1$, $\mathbb{Z}[i]$ Dominio euclidiano

$d\equiv 3 \pmod 4$
$d<-1$

entonces $R=\mathbb{Z}+\mathbb{Z}\sqrt{d}$ no es un dominio de factoriza única (DFU).

Eg: $d=-5$ ($\mathbb{Z}+\mathbb{Z}\sqrt{-5}$)

$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$

primos

Demostración: Veamos la factorización de

$$1-d=(1+\sqrt{d})(1-\sqrt{d})=2\cdot\left(\frac{1-d}{2}\right)$$

* 2 es un elemento irreducible de R.
  ↳ pues supongamos $2=\alpha\beta$ con $\alpha,\beta\notin R^*$

$\Rightarrow \quad N(2) = 4 = N(\alpha)N(\beta)$

$\Rightarrow \quad N(\alpha) = N(\beta) = 2$ lo cual es imposible en R.

$\Rightarrow$ 2 es irreducible. = EJER =

Si R es un DFU, $\Rightarrow$ 2 es un elemento primo (EJER)

$\Rightarrow 2 \mid 1-d$ & $2 \mid 1+\sqrt{d}$ ó $2 \mid 1-\sqrt{d}$

lo cual es una contradicción.

$\Rightarrow R_D$ no es un DFU. $\left(d \equiv 3 \ (4) \ \& \ d < -1 \right)$

Más aún, existen ideales $I \subseteq R$ que no son principales.

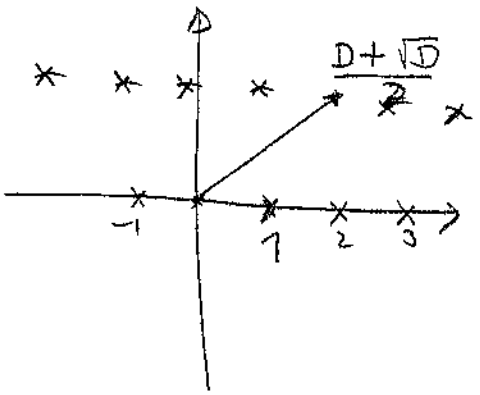
Sin embargo,

Todo ideal $I \leq R$, puede ser generado por 2 elementos, $I = (\alpha, \beta)$.

¿por qué? 1) $I \neq 0$ tiene siempre índice finito en R.

2) Geometría de la retícula generada por I.

↳ $R \leq \mathbb{C}$ gráficamente:



subgrupo discreto de $\mathbb{C}$.

&

I es un subgrupo más pequeño.

ambas cerradas bajo la multiplicación de R.

= EJER =

(basta ver que son cerrados bajo la mult. por $\frac{D+\sqrt{D}}{2}$)