Normas en anillos y campos cuadráticos

Facultad de Ciencias UNAM

Introducción

En esta sección introducimos el concepto de norma sobre un anillo. De la misma manera que una norma de un espacio métrico, una norma sobre un anillo nos permite (i) hablar sobre el *tamaño* de un elemento (un concepto geométrico) y (ii) nos da una noción de orden sobre los elementos del anillo.

Cabe recalcar que el concepto de norma sobre un anillo *no* va a aparecer mucho en el resto del curso. De hecho, para ver su utilidad, también introducimos unos subanillos de $\mathbb{C}$ (un anillo distintamente geométrico).

Normas en anillos

Definición

Supongamos que R es un anillo.

- Una **norma** en R es una función $N : R \to \mathbb{Z}_{\geq 0}$ tal que $N(0) = 0$.
- Una **campo-norma** en R es una función $\mathcal{N} : R \to \mathbb{R}$ tal que $N(0) = 0$.

Ejemplos básicos

- Sea $N : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ tal que

$$N(k) = |k|.$$

  Claramente, N es una norma sobre $\mathbb{Z}$.
- Sea $\mathcal{N} : \mathbb{R} \to \mathbb{R}_{\geq 0}$ tal que

$$\mathcal{N}(x) = |x|.$$

  Claramente, $\mathcal{N}$ es una campo-norma sobre $\mathbb{R}$.
- Sea $N : \mathbb{R}[x] \to \mathbb{Z}_{\geq 0}$ tal que

$$N(p(x)) = \deg p(x).$$

  Claramente, N es una norma en $\mathbb{R}[x]$ que además satisface $N(p(x)q(x)) = N(p(x)) + N(q(x))$.

Campos cuadráticos

Definición

Supongamos que $D \in \mathbb{Q}$ es tal que $\sqrt{D} \notin \mathbb{Q}$. Definimos

$$\mathbb{Q}(\sqrt{D}) := \{a + b\sqrt{D} \in \mathbb{C} \mid a, b \in \mathbb{Q}\}.$$

Cabe recalcar que pusimos $a + b\sqrt{D} \in \mathbb{C}$ (y no $a + b\sqrt{D} \in \mathbb{Q}$) porque como no pedimos $D > 0$, no sabemos si $\sqrt{D} \in \mathbb{R}$. Ahora bien, como para toda $a, b, c, d \in \mathbb{Q}$

$$(a + b\sqrt{D}) \pm (c + d\sqrt{D}) = (a \pm c) + (b \pm d)\sqrt{D}$$
$$(a + b\sqrt{D}) \cdot (c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D},$$

entonces $\mathbb{Q}(\sqrt{D})$ es un subanillo de $\mathbb{C}$; y si $D > 0$, entonces $\mathbb{Q}(\sqrt{D})$ es subanillo de $\mathbb{R}$. Mas aun, es claro que $\mathbb{Q}(\sqrt{D})$ es un anillo conmutativo con 1.

$\mathbb{Q}(\sqrt{D})$ es un campo

Proposición 1

Supongamos que $D \in \mathbb{Q}$ es tal que $\sqrt{D} \notin \mathbb{Q}$. Entonces $\mathbb{Q}(\sqrt{D})$ es un campo. A los campos de esta forma, los llamamos **campos cuadráticos**.

Demostración. Antes que nada, notemos que para toda $x, y \in \mathbb{Q}$ tenemos que

$$(x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - y^2 D. \tag{1}$$

Ahora bien, para ver que $\mathbb{Q}(\sqrt{D})$ es un campo, supongamos que $a + b\sqrt{D} \neq 0$ y veamos que tiene un inverso multiplicativo. Claramente, $a + b\sqrt{D} \neq 0$ implica $a \neq 0$ o $b \neq 0$. Veamos que en cualquier caso, $a^2 - b^2 D \neq 0$.

Procedemos por contradicción: es decir supongamos que $a^2 = b^2 D$.

- Si $a \neq 0$, entonces ($a^2 = b^2 D$ implica que) $b^2 = 0$. Por lo tanto, podemos dividir por b^2 para obtener $D = \frac{a^2}{b^2} \in \mathbb{Q}$. Contradiciendo $\sqrt{D} \in \mathbb{Q}$.
- Si $b \neq 0$, entonces (de nuevo), $D = \frac{a^2}{b^2} \in \mathbb{Q}$. Contradiciendo $\sqrt{D} \in \mathbb{Q}$.

En resumen, $a^2 - b^2 D \neq 0$ cuando $a + b\sqrt{D} \neq 0$. Por lo tanto, la igualdad (1) implica que

$$(a + b\sqrt{D}) \cdot \left(\frac{a - b\sqrt{D}}{a^2 - b^2 D} \right) = 1$$

Por lo tanto, $\mathbb{Q}(\sqrt{D})$ es un campo. $\square$

Unicidad de los coeficientes en $\mathbb{Q}(\sqrt{D})$

Proposición 2

Supongamos que $D \in \mathbb{Q}$ es tal que $\sqrt{D} \notin \mathbb{Q}$ y que $a, b, c, d \in \mathbb{Q}$. Si $a + b\sqrt{D} = c + d\sqrt{D}$, entonces $a = c$ y $b = d$.

Demostración. Primero veamos que $b = d$. De lo contrario,
$a + b\sqrt{D} = c + d\sqrt{D} \implies (b-d)\sqrt{D} = c - a \Longrightarrow^{1} \sqrt{D} = \frac{c-a}{b-d} \in \mathbb{Q}$.
Contradiciendo $\sqrt{D} \notin \mathbb{Q}$. Por lo tanto $b = d$. Usando esto y que $a + b\sqrt{D} = c + d\sqrt{D}$ es inmediato que $a = c$. □

[1] Podemos dividir porque $b \neq d$ implica $b - d \neq 0$.

Enteros cuadráticos

Definición

Un **entero cuadrático** es un numero complejo que es solución de una ecuación de la forma $x^2 + bx + c = 0$ donde $b, c \in \mathbb{Z}$. Por la famosa "formula chicharronera", los enteros cuadráticos son números de la forma

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2} \in \mathbb{C}$$

Ahora definimos un subanillo muy importante de $\mathbb{Q}(\sqrt{D})$. Para motivar un poquito su definición, presentamos un resultado de teoría de números que desafortunadamente, no nos vamos a dar el tiempo de demostrar.

Lema motivacional

Lema 3

Supongamos que $D \in \mathbb{Z}$ es tal que $k^2 \nmid D$ para toda $k \in \mathbb{Z}_{>1}$. Entonces $x \in \mathbb{Q}(\sqrt{D})$ es un entero cuadrático si y solo si existen $a, b \in \mathbb{Z}$ tales que

$$x = a + \omega b$$

donde

$$\omega := \begin{cases} \sqrt{D} & \text{si } D \not\equiv 1 \mod 4 \\ \frac{1+\sqrt{D}}{2} & \text{si } D \equiv 1 \mod 4 \end{cases}$$

El anillo $\mathbb{Z}[\sqrt{D}]$

Definición

Supongamos que $D \in \mathbb{Z}$ es tal que $k^2 \nmid D$ para toda $k \in \mathbb{Z}_{>1}$ (o equivalentemente[2], D es un producto de primos distintos si $D \neq \pm 1$). Definimos,

$$\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}.$$

Como $k^2 \nmid D$, entonces $\sqrt{D} \notin \mathbb{Q}$ y por lo tanto, el campo cuadrático $\mathbb{Q}(\sqrt{D})$ esta bien definido. Claramente, $\mathbb{Z}[\sqrt{D}]$ es un subgrupo aditivo de $\mathbb{Q}(\sqrt{D})$ y usando la ecuación

$$(x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - y^2 D$$

vemos que $\mathbb{Z}[\sqrt{D}]$ también es cerrado bajo multiplicación. Por lo tanto, $\mathbb{Z}[\sqrt{D}]$ es un subanillo de $\mathbb{Q}(\sqrt{D})$.

[2] Por el teorema fundamental de la aritmética.

El anillo $\mathbb{Z}[(1+\sqrt{D})/2]$

Lema 4

Supongamos que $D \in \mathbb{Z}$ es tal que $k^2 \nmid D$ para toda $k \in \mathbb{Z}_{>1}$. Si $D \equiv 1 \mod 4$, entonces

$$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] := \left\{a + b\frac{1+\sqrt{D}}{2} \in \mathbb{C} \mid a, b \in \mathbb{Z}\right\}$$

es un subanillo de $\mathbb{Q}(\sqrt{D})$.

Demostración. Para ver que es un subconjunto de $\mathbb{Q}(\sqrt{D})$, basta notar que

$$a + b\frac{1+\sqrt{D}}{2} = \left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{D} \in \mathbb{Q}(\sqrt{D}).$$

Además, es claro que es un subgrupo aditivo y es cerrado bajo multiplicación porque para cualesquiera $a, b \in \mathbb{Z}$ tenemos

$$\left(a + b\frac{1+\sqrt{D}}{2}\right)\left(c + d\frac{1+\sqrt{D}}{2}\right) =$$

$$\left(ac + bd\frac{D-1}{4}\right) + (ad + bc + bd)\frac{1+\sqrt{D}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$$

Donde la pertenencia se cumple porque $D \equiv 1 \mod 4$ implica $\frac{D-1}{4} \in \mathbb{Z}$. $\square$

El anillo de enteros de un campo cuadrático

Definición

Para cada $D \in \mathbb{Z}$ tal que $k^2 \nmid D$ para toda $k \in \mathbb{Z}_{>1}$, definimos

$$\mathcal{O}(D) := \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

donde

$$\omega := \begin{cases} \sqrt{D} & \text{si } D \not\equiv 1 \mod 4 \\ \frac{1+\sqrt{D}}{2} & \text{si } D \equiv 1 \mod 4 \end{cases}$$

Al subanillo $\mathcal{O}(D)$ de $\mathbb{Q}(\sqrt{D})$ lo llamamos el **anillo de enteros**[3] **del campo cuadrático** $\mathbb{Q}(\sqrt{D})$. Por el lema anterior, $\mathcal{O}(D)$ es precisamente el conjunto de enteros cuadráticos en $\mathbb{Q}(\sqrt{D})$.

[3] El nombre viene del hecho de que los elementos del subanillo $\mathcal{O}(D)$ del campo $\mathbb{Q}(\sqrt{D})$ tienen muchas propiedades análogas a los elementos de $\mathbb{Z}$ en el campo $\mathbb{Q}$.

Los enteros Gaussianos

Definición

Si $D = -1$ o equivalentemente, $\sqrt{D} = \sqrt{-1} = i \in \mathbb{C}$, entonces

$$\mathbb{Z}[i] = \left\{ a + bi \mid a, b \in \mathbb{Z} \right\}.$$

Este caso es particularmente importante y tiene nombre: **los enteros Gaussianos**.

Notemos que como $-1 \not\equiv 1 \mod 4$, entonces

$$\mathcal{O}(-1) = \mathbb{Z}[i].$$

En palabras, los enteros Gaussianos son el anillo de enteros del campo cuadrático $\mathbb{Q}(i)$.

La campo-norma en $\mathbb{Q}(\sqrt{D})$ y la norma en $\mathcal{O}(D)$

Definición

Supongamos que $D \in \mathbb{Q}$ es tal que $\sqrt{D} \notin \mathbb{Q}$. Sea $\mathcal{N}_D : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ la campo-norma en $\mathbb{Q}(\sqrt{D})$ dada por

$$\mathcal{N}_D(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D \in \mathbb{Q}$$

Esta norma da una noción de "tamaño" en el campo $\mathbb{Q}(\sqrt{D})$. Por ejemplo, en el caso $D = -1$,

$$\mathcal{N}_{-1}(a + bi) = \mathcal{N}_{-1}\left(a + b\sqrt{-1}\right) = a^2 - b^2(-1) = a^2 + b^2$$

y por lo tanto, $\mathcal{N}_{-1}(a + ib)$ es el cuadrado de la distancia de $a + bi$ considerado como un vector en el plano complejo.

Estudiemos un poquito mas a $\mathcal{N}_D$.

$\mathcal{N}_D$ es multiplicativa

Proposición 5

Supongamos que $D \in \mathbb{Q}$ es tal que $\sqrt{D} \notin \mathbb{Q}$. Si $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$, entonces

$$\mathcal{N}_D(\alpha\beta) = \mathcal{N}_D(\alpha) \cdot \mathcal{N}_D(\beta)$$

Demostración. Supongamos que $\alpha = a + b\sqrt{D}$ y $\beta = c + d\sqrt{D}$. Entonces calculando directamente obtenemos

$$\begin{aligned}\mathcal{N}_D(\alpha)\mathcal{N}_D(\beta) &= \mathcal{N}_D(a + b\sqrt{D})\mathcal{N}_D(c + d\sqrt{D}) \\ &= \left(a^2 - b^2 D\right)\left(c^2 - d^2 D\right) \\ &= a^2c^2 - a^2d^2D - b^2c^2D + b^2d^2D^2\end{aligned}$$

y

$$\begin{aligned}\mathcal{N}_D(\alpha\beta) &= \mathcal{N}_D\left((a + b\sqrt{D})(c + d\sqrt{D})\right) \\ &= \mathcal{N}_D\left((ac + bdD) + (ad + bc)\sqrt{D}\right) \\ &= (ac + bdD)^2 - (ad + bc)^2 D \\ &= a^2c^2 + 2acbdD + b^2d^2D^2 - a^2d^2D - 2adbcD - b^2c^2D \\ &= a^2c^2 + b^2d^2D^2 - a^2d^2D - b^2c^2D.\end{aligned}$$

Comparando estas igualdades obtenemos lo deseado. □

$\mathcal{N}_D$ en $\mathcal{O}(D)$

Proposición 6

Supongamos que $D \in \mathbb{Z}$ es tal que $k^2 \nmid D$ para toda $k \in \mathbb{Z}_{>1}$. Si $a, b \in \mathbb{Z}$, entonces

$$\begin{aligned} \mathcal{N}_D(a+b\omega) &= (a+b\omega)(a+b\overline{\omega}) \qquad (2) \\ &= \begin{cases} a^2 - b^2 D & \text{si } D \not\equiv 1 \mod 4 \\ a^2 + ab + \frac{1-D}{4} b^2 & \text{si } D \equiv 1 \mod 4 \end{cases} \end{aligned}$$

donde

$$\overline{\omega} = \begin{cases} -\sqrt{D} & \text{si } D \not\equiv 1 \mod 4 \\ \frac{1-\sqrt{D}}{2} & \text{si } D \equiv 1 \mod 4 \end{cases}$$

La demostración es puras cuentas y por eso dejamos su verificación al lector.

Una consecuencia inmediata de esta proposición es que para toda $\alpha \in \mathcal{O}(D)$ tenemos que $\mathcal{N}_D(\alpha) \in \mathbb{Z}$. Por lo tanto, podemos hacer la siguiente definición.

La norma en $\mathcal{O}(D)$

Definición

Sea $N_D : \mathcal{O}(D) \to \mathbb{Z}_{\geq 0}$ la norma en $\mathcal{O}(D)$ dada por

$$N_D(a + b\sqrt{D}) = \left|\mathcal{N}_D(a + b\sqrt{D})\right| = \left|a^2 - b^2 D\right|.$$

Cabe recalcar (i) que N_D sigue siendo multiplicativa y (ii) que si $D < 0$, no necesitamos poner el valor absoluto y por lo tanto, en este caso, $N_D = \mathcal{N}_D \restriction_{\mathcal{O}(D)}$.

En lo que sigue (y en las siguientes secciones) usaremos a $\mathcal{N}_D$ y a N_D para estudiar a $\mathbb{Q}(\sqrt{D})$ y a $\mathcal{O}(D)$.

La utilidad de N_D

Proposición 7

Supongamos que $D \in \mathbb{Z}$ es tal que $k^2 \nmid D$ para toda $k \in \mathbb{Z}_{>1}$. Si $\alpha \in \mathcal{O}(D)$, entonces

$$\alpha \text{ es invertible} \iff N_D(\alpha) = \pm 1$$

Demostración.

$\Longrightarrow$) α es invertible $\implies$ $\alpha\beta = 1$ para alguna $\beta \in \mathcal{O}$ $\implies$
$N_D(\alpha)N_D(\beta) = N_D(\alpha\beta) = N_D(1) = 1 \implies$ [4] $N_D(\alpha) = \pm 1$.

$\Longleftarrow$) $N_D(\alpha) = \pm 1 \implies$ [5] $(a + b\omega)(a + b\overline{\omega}) = \pm 1 \implies$ $a + b\omega$ es invertible y mas aun, $(a + b\omega)^{-1} = \pm(a + b\overline{\omega})$.

□

[4] Pues $N_D(\alpha)$ y $N_D(\beta)$ son enteros

[5] Usando (2) y suponiendo que $\alpha = a + b\omega$.

Por ejemplo,

- Cuando $D = -1$, los elementos invertibles en $\mathcal{O}(D) = \mathcal{O}(-1) = \mathbb{Z}[i]$ son los $a + bi$ tales que $a^2 + b^2 = 1$. Por lo tanto, los elementos invertibles en los enteros Gaussianos son precisamente $\{\pm 1, \pm i\}$.
- Cuando $D = -3$, los elementos invertibles en $\mathcal{O}(-3) = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ son los $a + bi$ tales que $a^2 + ab + b^2 = \pm 1$ o equivalentemente, los $a + bi$ tales que $(2a + b)^2 + 3b^2 = \pm 4$. Sin embargo, no podemos tener $(2a + b)^2 + 3b^2 = -4$ porque $(2a + b)^2 + 3b^2 \geq 0$. Por lo tanto, $(2a + b)^2 + 3b^2 = 4$. Esta ecuación se puede resolver haciendo observaciones como la siguiente: si $b \neq 0$, entonces $b = \pm 1$: de lo contrario (como es entero) $3b^2 \geq 3(2)^2 = 12$. Lo cual es imposible porque $(2a + b)^2 + 3b^2 = 4$ y $(2a + b)^2 \geq 0$. Usando esto, podemos despejar a y obtener que el conjunto de los elementos invertibles en $\mathcal{O}(-3)$ esta dado por $\{\pm 1, \pm\rho, \pm\rho^2\}$ donde $\rho = \frac{-1+\sqrt{-3}}{2}$.

- Cuando $D < 0$ y $D \neq -1, -3$ se puede verificar (de manera análoga) que los únicos elementos invertibles en $\mathcal{O}(D)$ son $\{\pm 1\}$.
- Cuando $D > 0$ se puede demostrar que $\mathcal{O}(D)$ tiene una cantidad infinita de elementos invertibles. Por ejemplo, cuando $D = 2$, es fácil verificar (usando la caracterización de elementos invertibles en $\mathbb{Z}[\sqrt{D}]$) que $1 + \sqrt{2}$ es invertible en $\mathcal{O}(2) = \mathbb{Z}[\sqrt{2}]$ y mas aun, que para toda $n \in \mathbb{Z}$, $\pm(1 + \sqrt{2})^n$ es invertible.