Anillo de enteros

Def: Si $p(x) \in \mathbb{Z}[x]$ no nulo, el **contenido** de $p(x)$, $c(p) = \gcd\{a_0, a_1, \dots, a_n\}$ si

$$p(x) = a_0 + a_1 x + \dots + a_n x^n.$$

Obs: $p(x) \in \mathbb{Z}[x]$, $\dfrac{p(x)}{c(p)} \in \mathbb{Z}[x]$.

Un polinomio se llama **primitivo** si su contenido es 1.

Ejercicio: Si $p, f \in \mathbb{Z}[x]$, $c(p \cdot q) = c(p) \cdot c(f)$.

Demo: • $c(p) \cdot c(f) \mid c(p f)$

$$p(x) = \sum_{i=0}^{N} a_i x^i$$

$$f(x) = \sum_{j=0}^{M} b_j x^j$$

$$p(x) \cdot f(x) = \sum_{i=0}^{N} \sum_{j=0}^{M} a_i b_j x^{i+j}$$

(a_i: $c(f) \mid$, b_j: $c(g) \mid$)

• $c(pf) \mid c(p) \cdot c(f)$, basta probar que si p y f son primitivos $\Rightarrow$ $p \cdot f$ lo es.

Si no lo fuera, $c(p \cdot f) \in \mathbb{N}_{>1}$, $\exists\, \ell$ primo, tal que $\ell \mid c(p \cdot f)$.

$$\overline{p \cdot q} \equiv 0 \pmod{\ell}$$

$$\overline{p} \cdot \overline{f}$$

como $c(p) = 1$, $\overline{p} \not\equiv 0 \pmod{\ell}$

$c(f) = 1$, $\overline{q} \not\equiv 0 \pmod{\ell}$.

$\Rightarrow \mathbb{F}_\ell[x]$ no es íntegro. **Abs!**

Lema (de Gauss). Dado $p(x) \in \mathbb{Z}[x]$. Luego $p(x)$ es reducible en $\mathbb{Q}[x] \iff p(x)$ es reducible en $\mathbb{Z}[x]$.

Obs: $\mathbb{Z}[x]$ no tiene algoritmo de división ($x^2+1 \,|\, 2x+1$?) no obstante, tiene factorización única.

Demo (lema): $\Leftarrow$) obvio.

$\Rightarrow$) queremos ver que si $p = f \cdot g$, $f, g \in \mathbb{Q}[x]$

$\Rightarrow$ $p = \tilde{f} \cdot \tilde{g}$, $\tilde{f}, \tilde{g} \in \mathbb{Z}[x]$ y son "asociados" a f y g.

$p = c(p) \cdot \left(\frac{p}{c(p)}\right)$, basta saber p es primitivo. (primitivo.)

Como $f, g \in \mathbb{Q}[x]$, y $n, m \in \mathbb{N}$, mínimos con la propiedad de que $n \cdot f \in \mathbb{Z}[x]$, $m \cdot g \in \mathbb{Z}[x]$. Luego

$$n \cdot m \, p = (nf)(mg) \quad \text{en } \mathbb{Z}[x].$$

Tomando contenido, (coprimos) $n \cdot m = c(nf) \cdot c(mg)$

$mcd(n, c(nf)) = 1$, pues si $d = mcd(n, c(nf))$,

$\left(\frac{n}{d}\right) \cdot f = \frac{nf}{d} \in \mathbb{Z}[x]$, $\mathbb{Z}/d$ hace a f entero. $\Rightarrow d = 1$.

$\Rightarrow$ $n \mid c(m \cdot g)$ y análogamente $m \mid c(nf)$

$\Rightarrow$ $\frac{mg}{n}$ y $\frac{nf}{m} \in \mathbb{Z}[x] \Rightarrow p = \left(\frac{nf}{m}\right) \cdot \left(\frac{mg}{n}\right)$ en $\mathbb{Z}[x]$ ∎

Sea $K/\mathbb{Q}$ una extensión finita.

Def: un elemento $\alpha \in K$ se dice **entero algebraico** si existe $p(x) \in \mathbb{Z}[x]$ mónico que lo tiene como raíz.

Obs: $\alpha \in K$ es entero algebraico $\Leftrightarrow m_\alpha(x) \in \mathbb{Z}[x]$.

($\Leftarrow$) ✓

($\Rightarrow$) $p(x) \in \mathbb{Z}[x]$ y tiene a α como raíz (mónico), $m_\alpha(x) \mid p(x)$ en $\mathbb{Q}[x]$, o sea $p(x) = m_\alpha(x) \cdot h(x)$.
(mónico = mónico · mónico)

Por el lema de Gauss, $\exists\, a, b \in \mathbb{N}$ mínimos t.q.

$$\underbrace{a b \cdot p}_{\text{múltiplo de } ab} = \underbrace{(a \cdot m_\alpha(x))}_{\text{múltiplo de } a} \cdot \underbrace{(b\, h(x))}_{\text{múltiplo de } b} \quad \text{tomando contenidos}$$

a divide a ab; b divide a ab.

$\Rightarrow c(a\, m_\alpha(x)) = a \Rightarrow m_\alpha(x) \in \mathbb{Z}[x]$. ∎

Ejemplo: $K = \mathbb{Q}[i]$, ¿quiénes son los enteros algebraicos de K?

Si $\alpha \in \mathbb{Q}[i]$, $\alpha = a + bi$, $a, b \in \mathbb{Q}$.

1° caso: si $b = 0$, $\alpha \in \mathbb{Q}$, ¿cuándo es entero? $\Leftrightarrow \alpha \in \mathbb{Z}$
(por Gauss, $\alpha \in \mathbb{Q}$ es raíz de un polinomio con coef. enteros mónico $\Leftrightarrow \alpha \in \mathbb{Z}$). ✓

Lema (Gauss): si $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ y $\frac{p}{q}$ es raíz $\Rightarrow p \mid a_0$, $q \mid a_n$.

2° caso: si $b \neq 0$, $m_\alpha(x) = (x - (a+bi))(x - (a-bi))$

$$= x^2 - \underbrace{2a}_{\in \mathbb{Z}} x + \underbrace{(a^2 + b^2)}_{\in \mathbb{Z}} \in \mathbb{Z}[x].$$

$2a \in \mathbb{Z} \Rightarrow a \in \frac{\mathbb{Z}}{2}$, $a = \frac{\alpha}{2}$, $\alpha \in \mathbb{Z}$

$a^2 + b^2 \in \mathbb{Z} \Rightarrow \frac{\alpha^2}{4} + b^2 = c \in \mathbb{Z} \Rightarrow b^2 = c - \frac{\alpha^2}{4} = \frac{4c - \alpha^2}{4}$

Luego el denominador de b^2 es como mucho 4 $\Rightarrow$ el denominador de b es a lo sumo 2., o sea $b \in \frac{\mathbb{Z}}{2}$, $b = \frac{\beta}{2}$, $\beta \in \mathbb{Z}$.

$\frac{\alpha^2 + \beta^2}{4} \in \mathbb{Z} \rightsquigarrow \alpha^2 + \beta^2 \equiv 0 (4) \Rightarrow \alpha, \beta$ son pares.

$\Rightarrow a \in \mathbb{Z}$, $b \in \mathbb{Z} \Rightarrow \{$enteros algebraicos de $\mathbb{Q}[i]\} = \mathbb{Z}[i]$.

↑ enteros de Gauss

Recordar (1º clase): ¡$\mathbb{Z}[i]$ es un anillo!

Obs: ¡no es obvio que sumas y productos de enteros algebraicos lo sea! ¿Vale siempre?

Teo: Si $K/\mathbb{Q}$ extensión finita ($K \subset \mathbb{C}$), dado $\alpha \in K$, son equivalentes:

1. α es entero algebraico.
2. Existe un $\mathbb{Z}$-módulo finitamente generado $M \subset K$ tal que $\alpha \cdot M \subset M$. ($\exists \{v_1, \dots, v_n\} \subset M$ / $m \in M$, $m = a_1 v_1 + \dots + a_n v_n$, $a_i \in \mathbb{Z}$)

Demo: 1. $\Rightarrow$ 2. $M = \mathbb{Z}[\alpha]$.

$m_\alpha(x) = x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$

$a_i \in \mathbb{Z} \Rightarrow \alpha^d + a_{d-1} \alpha^{d-1} + \dots + a_1 \alpha + a_0 = 0$

o sea, $\alpha^d = -a_{d-1} \alpha^{d-1} - \dots - a_1 \alpha - a_0$, $\alpha^d \in \langle 1, \dots, \alpha^{d-1} \rangle_{\mathbb{Z}}$

Claramente $\alpha \cdot M \subset M$.

2 $\Rightarrow$ 1. $M = \langle v_1, \dots, v_d \rangle_{\mathbb{Z}}$ ("base"), α, mira la función

$M \longrightarrow M$ multiplicar
$v \longrightarrow \alpha \cdot v$ por α.

$\alpha \cdot v_1 \in M \Rightarrow$ existen $a_1^{(1)}, \dots a_d^{(1)} \in \mathbb{Z}$ t.q.

$$\begin{aligned} \alpha \cdot v_1 &= a_1^{(1)} v_1 + \dots + a_d^{(1)} v_d \\ \alpha \cdot v_2 &= a_1^{(2)} v_1 + \dots + a_d^{(2)} v_d \\ &\vdots \\ \alpha v_d &= a_1^{(d)} v_1 + \dots + a_d^{(d)} v_d \end{aligned} \quad \rightsquigarrow \quad \alpha \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} = (a_i^{(j)}) \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}$$

$$\Rightarrow \left(\alpha \cdot Id - (a_i^{(j)}) \right) \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} = \vec{0}.$$

$v_1, \dots, v_d$ no nulos

$\det(xId - M)$

$\Rightarrow \det(\alpha \cdot Id - (a_i^{(j)})) = 0 \Rightarrow \alpha$ es raíz de $\chi(a_i^{(j)})$

$\in \mathbb{Z}[x]$ mónico.

$\Rightarrow \alpha$ es entero algebraico (por definición) ☒

Corolario: Si $\alpha, \beta \in K$ enteros algebraicos, entonces $\alpha + \beta$ y $\alpha \cdot \beta$ son enteros algebraicos.

D/ Como α es entero algebraico, $\mathbb{Z}[\alpha]$ es finitamente generado como $\mathbb{Z}$-módulo $(\langle 1, \dots \alpha^{d-1} \rangle_{\mathbb{Z}})$

Como β es entero algebraico, $\mathbb{Z}[\beta]$ es f.g. $(\langle 1, \dots \beta^{r-1} \rangle_{\mathbb{Z}})$

$M = \mathbb{Z}[\alpha, \beta]$ (como anillo), es finitamente generado (está generado por $\{ \alpha^i \beta^j \}_{\substack{0 \le i \le d-1 \\ 0 \le j \le r-1}}$).

M es un anillo, $\alpha + \beta$ y $\alpha \cdot \beta \in M \Rightarrow (\alpha + \beta) \cdot M \subset M$
$(\alpha \cdot \beta) M \subset M$ ☒

Def: Si $K/\mathbb{Q}$ finita, definimos el anillo de enteros de

K como el conjunto de todos los elementos de K que son enteros algebraicos. Lo denotamos por $\mathcal{O}_K$. ($\mathbb{Z}_K$)

Obs: $\mathcal{O}_K$ es un anillo por el corolario.

Obs2: no es preciso suponer $K/\mathbb{Q}$ es finita, basta suponer algebraica.

Objetivo: entender / calcular $\mathcal{O}_K$. ✓ anillo, $\mathbb{Z}$-módulo.
(generadores).

Problema: ¿es $\mathcal{O}_K$ un $\mathbb{Z}$-módulo finitamente generado?

Rta: Sí, buscamos "medir" qué tan lejos está un conjunto de elementos de $\mathcal{O}_K$ (el generado por ellos) de ser todo $\mathcal{O}_K$.

Supongamos que $\mathcal{O}_K$ es f.g. Luego, $\mathcal{O}_K \sim \mathbb{Z}^r$ (Teo de estructuras) $\quad \mathcal{O}_K = \langle v_1, \dots, v_r \rangle_{\mathbb{Z}}$

¿Quién es r? Si $[K:\mathbb{Q}] = d$

$\mathcal{O}_K = \langle v_1, \dots, v_r \rangle_{\mathbb{Z}}$ (l.i.) $\iff \{v_1, \dots, v_r\}$ son l.i. sobre $\mathbb{Q}$.
(l.i./$\mathbb{Z}$ o sobre $\mathbb{Q}$ es igual.)

Luego si $\mathcal{O}_K \sim \mathbb{Z}^r$, $\boxed{r \leq d}$

Ejercicio: Si $\alpha \in K$, luego algebraico, $\exists\, n \in \mathbb{N}$ t.q. $n\cdot\alpha$ es entero algebraico.

Idea: $m_\alpha(X) \in \mathbb{Q}[X]$, $\quad m_{n\alpha}(X) = n^d\, m_\alpha\left(\frac{X}{n}\right)$ ($d = \operatorname{gr}(m_\alpha(X))$)

$(x-\alpha_1)\cdots$ en $\mathbb{C}[x]$. $(\frac{x}{n}-\alpha)\cdots$

$m_\alpha(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d$, $n^d m_\alpha(\frac{x}{n}) = n^d a_0 + n^{d-1} a_1 x + \cdots + a_{d-1} n x^{d-1} + x^d$.

$\vdots$

$m_{n\alpha}(x)$

Quiero elegir n t.q. $a_i n^{d-i}$ es entero. ∎

Luego, si $\{\alpha_1, \dots, \alpha_d\}$ base de K como $\mathbb{Q}$-e.v.

puedo suponer que todos ellos son enteros algebraicos.

$\Rightarrow \langle \alpha_1, \dots, \alpha_d \rangle_{\mathbb{Z}} \subset \mathcal{O}_K \Rightarrow \boxed{r \geq d}$

l.i.

Con esto, podemos lo siguiente:

Prop: Si $\mathcal{O}_K$ es f.g., su rango es $[K:\mathbb{Q}]$.

Ojo: en $\mathbb{Q}[i]$, $\langle 2, 5i \rangle_{\mathbb{Z}} \subsetneq \mathbb{Z}[i]$

rango 2.

pero no es todo.

Def: Si F/K ext. finita de cuerpos, $\alpha \in F$, definimos

$m_\alpha : F \to F$, m_α es una t.l. de K-e.v.
$a \to \alpha \cdot a$

Luego, puedo construir $[m_\alpha]_{\mathcal{B}}$, $\mathcal{B}$ base de F como K-e.v. Definimos la traza de α, $Tr_{F/K}(\alpha)$ como

$$Tr_{F/K}(\alpha) = Tr([m_\alpha]_{\mathcal{B}}).$$ (no depende de $\mathcal{B}$).

Definimos la norma de α, $Nm_{F/K}(\alpha) = \det([m_\alpha]_{\mathcal{B}})$

$Tr : (F, +) \longrightarrow (k, +)$ morfismo. $Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$

$Nm : (F^\times, \cdot) \longrightarrow (k^\times, \cdot)$ morfismo $Nm(\alpha\beta) = Nm(\alpha) \cdot Nm(\beta)$

$\varphi : F \longrightarrow \{$ a.l. de F en F como k-e.v. $\}$ morfismo de anillos.

$\alpha \longrightarrow m_\alpha$

$\varphi(\alpha+\beta) = m_{\alpha+\beta} = m_\alpha + m_\beta$, $Tr(A+B) = Tr(A) + Tr(B)$

$\varphi(\alpha \cdot \beta) = m_{\alpha\cdot\beta} = m_\alpha \circ m_\beta$, $\det(A \cdot B) = \det(A) \cdot \det(B)$