10/08/20 Teoría de números algebraicos

$\alpha \in \overline{\mathbb{Q}}$.

def $\alpha \in \mathbb{C}$ es algebraico si

$$a_n\alpha^n + \dots + a_1\alpha + a_0 = 0, \quad \text{donde } a_i \in \mathbb{Q}, \; a_n \neq 0.$$

si $a_i \in \mathbb{Z}$, $a_n = 1$, se dice que α es un entero algebraico

Ejemplo $\alpha = \frac{1+\sqrt{5}}{2}$. $\alpha^2 - \alpha - 1 = 0$.
es un entero algebraico.

def Campo de números: K exten. finita ($\dim_{\mathbb{Q}} K < \infty$)

$$\begin{array}{c} K \\ |{<}\infty \\ \mathbb{Q} \end{array}$$

Ejemplo $d \in \mathbb{Z}$, libre de cuadrados ($n^2 \nmid d$)

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

$$\begin{array}{c} \mathbb{Q}(\sqrt{d}) \\ |\,2 \\ \mathbb{Q} \end{array}$$

Ejemplo (genérico) Sea $f \in \mathbb{Q}[x]$ irreducible. En este caso $K = \mathbb{Q}[x]/(f)$ es un campo de números.

$$\begin{array}{c} K \\ |\,\deg f. \\ \mathbb{Q} \end{array}$$

Si $\alpha \in \mathbb{C}$ es una raíz de f.

$$\left.\begin{array}{rl} ev: \mathbb{Q}[x] & \longrightarrow \mathbb{C} \\ g & \longmapsto g(\alpha) \end{array}\right] \rightsquigarrow \mathbb{Q}[x]/(f) \cong \mathbb{Q}(\alpha)$$

Recordatorio: Toda extn finita de $\mathbb{Q}$ es de la forma $\mathbb{Q}(\alpha)$ (el t. del elemento primitivo).

Ejemplo $\zeta_n = \exp(2\pi i/n)$ – una raíz n-ésima primitiva de 1

$$\Phi_n = \prod_{\substack{1 \le k \le n-1 \\ (k,n)=1}} (x - \zeta_n^k) \in \mathbb{Z}[x] \text{ es irreducible.}$$

El n-ésimo polinomio ciclotómico.

$\Phi_2 = x+1$, $\Phi_3 = x^2+x+1$, $\Phi_4 = x^2+1$, $\Phi_5 = x^4+x^3+x^2+x+1$

$\Phi_6 = x^2-x+1$, $\Phi_7 = x^6+x^5+\dots+x+1$, $\Phi_8 = x^4+1$

. . . .

El n-ésimo campo ciclotómico

$$\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n)$$

$$\deg \Phi_n = \varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times \implies [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

Se tiene $\left\{ \begin{array}{c} \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n) \\ m < n \end{array} \right\} \iff \left\{ \begin{array}{l} m \text{ impar} \\ n = 2m \end{array} \right\}$

$$\Phi_{2m}(x) = \Phi_m(-x)$$

§ Anillos de números

def $\mathcal{O}$ anillo de números $\quad R \overset{\text{subanillo}}{\subset} K$, $K/\mathbb{Q}$, $[K:\mathbb{Q}] < \infty$

Ejemplo $\mathbb{Z} \subset \mathbb{Q}$.

$\mathbb{Z}[\frac{1}{n}] = \{ \frac{a}{n^k} \mid a \in \mathbb{Z}, k \in \mathbb{N} \}$ $\qquad \mathbb{Z}_{(p)} = \{ \frac{a}{b} \mid p \nmid b \}$

(p – primo fijo)

$\mathbb{Z}[\frac{1}{n}]$, $\mathbb{Z}_{(p)} \subset \mathbb{Q}$.

(localizaciones de $\mathbb{Z}$)

Ejemplo $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Q}(\sqrt{d})$

$\| $

$\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ — $\mathbb{Z}$-módulo libre de rango 2.

(base$/\mathbb{Z}$: $1, \sqrt{d}$)

Ahora, si $d \equiv 1 \pmod 4$ podemos tomar

$$\mathbb{Q}(\sqrt{d}) \supset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \supsetneq \mathbb{Z}[\sqrt{d}]$$

Observación: $\alpha = \frac{1+\sqrt{d}}{2}$ cumple $\alpha^2 - \alpha - \underbrace{\frac{d-1}{4}}_{\in \mathbb{Z}} = 0$.

es un entero algebraico.

Ejemplo $\mathbb{Z}[\zeta_n] \subset \mathbb{Q}(\zeta_n)$

$\mathbb{Z}[\zeta_n] = \{ \sum a_k \zeta_n^k \mid a_k \in \mathbb{Z} \}$.

$\uparrow$ $\mathbb{Z}$-módulo libre de rango $\varphi(n)$

def Un anillo de números $R < K$ es un orden si R es f.g. como un $\mathbb{Z}$-módulo (gpo abeliano)

Nota: K como gpo aditivo no tiene torsión $\Rightarrow$ R es un $\mathbb{Z}$-módulo libre de rango finito.

Ejemplo $\mathbb{Z}[\sqrt{d}]$, $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ (si $d \equiv 1$ (4)), $\mathbb{Z}[\zeta_n]$ son órdenes.

Ejemplo $\mathbb{Q}$, $\mathbb{Z}_{(p)}$ no son órdenes (ejercicio)

Ejemplo Sea $f \in \mathbb{Z}[x]$ polinomio mónico irreducible.

$$\begin{array}{ccc} \mathbb{Z}[\alpha] & \subset & \mathbb{Q}(\alpha) \\ \wr\vert & & \wr\vert \\ \mathbb{Z}[x]/(f) & \subset & \mathbb{Q}[x]/(f) \\ \Big| \; rk = \deg f & & \Big| \; \deg f \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

$\mathbb{Z}[\alpha]$ no es siempre "el mejor" orden en $\mathbb{Q}(\alpha)$

PARI/GP (ejemplos)

- algdep. $\qquad \lim_{n \to \infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}$.
- cálculos en campos de números.

$\mathbb{Q}[x]/(f) = K$

$\quad \Psi$

$g \bmod f$

$$\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/(x^2-2)$$

$$\begin{array}{ccc} \Psi & & \Psi \\ 1+\sqrt{2} & \longleftrightarrow & 1+x \bmod x^2-2 \end{array}$$

- polisirreducible(f)

  factor(f) $\rightsquigarrow$ factores irreducibles.

- Sea p primo. Consideremos

$$g = \sum_{1 \leq k \leq p-1} \left(\frac{k}{p}\right) \zeta_p^k \in \mathbb{Z}[\zeta_p]$$

$$\left(\frac{k}{p}\right) = \begin{cases} +1, & \text{si } k \equiv \square \pmod p \\ -1, & \text{si } k \not\equiv \square \pmod p \end{cases}$$ – el símbolo de Legendre

$$g^2 = (-1)^{\frac{p-1}{2}} \cdot p \quad \text{(Gauss)}$$

$$g = \begin{cases} \sqrt{p}, & p \equiv 1 \ (4) \\ i\sqrt{p}, & p \equiv 3 \ (4) \end{cases}$$

La próxima sesión
- aplicaciones de anillos de números.
- dominios euclidianos,

$$\text{dominios euclidianos} \Rightarrow \text{DIP} \Rightarrow \text{DFU}.$$

enteros de Gauss $\mathbb{Z}[i] \subset \mathbb{Q}(\sqrt{-1})$, enteros de Eisenstein $\mathbb{Z}[\zeta_3] \subset \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$