24/08 § Operaciones aritméticas con ideales

def $I, J \subseteq R$ ideales

·) $I + J = \{\alpha + \beta \mid \alpha \in I,\ \beta \in J\}$

$(\alpha_1, \dots, \alpha_m) + (\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_m, \beta_1, \dots \beta_n)$

·) $I \cap J$

·) $IJ = \{\sum_i \alpha_i \beta_i \mid \alpha_i \in I,\ \beta_i \in J\}$

$(\alpha_i)_i \cdot (\beta_j)_j = (\alpha_i \beta_j)_{i,j}$.

Nota: $IJ \subseteq I \cap J$.

Propiedades esperadas: $+, \cdot$ operaciones asociativas, conmutativas,

$I + (0) = I$

$I + R = R$ $\qquad (I+J)H = IH + JH$

$I \cdot (0) = (0)$

$I \cdot R = I$ $\qquad$ Potencias: $I^n = \underbrace{I \cdots I}_{n}$

$R \supseteq I \supseteq I^2 \supseteq I^3 \supseteq \dots$

Nota $IJ \neq \{\alpha\beta \mid \alpha \in I, \beta \in J\}$

Ejemplo $I = (p, x) \subset \mathbb{Z}[x]$, $p \in \mathbb{Z}$ primo.

$I^2 = (p^2, px, x^2)$

$f = p^2 + x^2 \in I^2$, pero $f \neq gh$ para $g, h \in I$. $\triangle$

Nota ·) $J = IH \Rightarrow J \subseteq H,\ J \subseteq I$

·) $\alpha \mid \beta \iff (\alpha) \supseteq (\beta)$

Def $I \mid J \overset{def}{\iff} J \subseteq I$.

Nota En gral, $J \subseteq I \not\Rightarrow \left\{ \begin{array}{l} \exists\ H \subset R \text{ t.q.} \\ J = IH \end{array} \right.$

Def I, J son coprimos si $I + J = R$.

Nota En un DIP $(\alpha) + (\beta) = (\alpha, \beta) = (\gamma)$

$\gamma = mcd(\alpha, \beta)$

Ejemplo $R = k[x,y]$. $\operatorname{mcd}(x,y) = 1$.

$(x)+(y) = (x,y) \neq R$: de hecho, $R/(x,y) \simeq k$.

Ejemplo En $R = \mathbb{Z}[\sqrt{-5}]$.

$\operatorname{mcd}(2,\ 1+\sqrt{-5}) = 1$, pero

$(2,\ 1+\sqrt{-5}) \neq \mathbb{Z}[\sqrt{-5}]$. (ejercicio)

En un DFU. $\left.\begin{array}{l}\operatorname{mcd}(\alpha,\beta)=1\\ \alpha\beta = \gamma^n\end{array}\right\} \Rightarrow \left.\begin{array}{l}\alpha \sim \alpha'^n\\ \beta \sim \beta'^n\end{array}\right\}$

Ejemplo cuando R no es un DFU.

$$\underbrace{(2+3\sqrt{-5})\,(2-3\sqrt{-5})}_{\text{irred. no asociados}} = 7^2$$

Pasamos a los ideales $I = (2+3\sqrt{-5})$

$J = (2-3\sqrt{-5})$

$H = (7)$

$$\begin{cases} IJ = H^2 \\ I+J = R \end{cases}$$

$I+J=R \Longleftrightarrow 1 = \alpha+\beta$ donde $\alpha \in I$, $\beta \in J$ (ejercicio!)

$(I+H)^2 = I^2 + IH + H^2 = I^2 + IH + IJ$

$= I(\underbrace{I+H+J}_{=R}) = I\cdot R = I$.

Similar: $(J+H)^2 = J$.

$(2\pm 3\sqrt{-5}) = (7,\ 2\pm 3\sqrt{-5})^2$

no es principal.

(sino, $(2\pm 3\sqrt{-5}) = (\alpha)^2$

$\Longleftrightarrow$

$2\pm 3\sqrt{-5} \sim \alpha^2$)

Teorema Sean $I, J \subset R$ ideales t.q. $I+J=R$.

luego, si $I\cdot J = H^n \Rightarrow (I+H)^n = I$

$(J+H)^n = J$.

(**Ejemplo**: $(I+H)^3 = I^3 + I^2H + IH^2 + H^3$

$= I^3 + I^2H + IH^2 + IJ$

$= I\cdot(\underbrace{I^2 + IH + H^2 + J}) = I$)

$+, \cdot$ asociativas, conmutativas,

$\cdot$ es distributivo respecto a $+$

•) No hay "$-I$" porque $I + I = I$

implicaría $I = 0$.

•) Sí se pueden añadir "I^{-1}" t.q.

$I \cdot I^{-1} = R$. (la siguiente clase)

Lema Si $I + J = R$, entonces $IJ = I \cap J$.

Dem. $1 = \alpha + \beta$, donde $\alpha \in I$, $\beta \in J$.

Ahora si $\gamma \in I \cap J \Rightarrow \gamma = \gamma \cdot 1 = \gamma(\alpha + \beta)$

$$= \underbrace{\gamma \cdot \alpha + \gamma\beta}_{\in IJ}.$$

▥

Teorema Chino del resto

Si $I + J = R$, entonces hay iso natural

$$R/IJ \simeq R/I \times R/J.$$

$$(x + IJ) \mapsto (x + I, x + J)$$

Dem $\varphi: R \twoheadrightarrow R/I \times R/J$

$x \mapsto (x + I, x + J)$

•) φ sobreyectivo:

$1 = a + b$, $a \in I$, $b \in J$.

$$\begin{cases} a \equiv 1 \pmod{J} \\ b \equiv 1 \pmod{I} \end{cases}$$

$x = a\alpha + b\beta \overset{\varphi}{\mapsto} (\alpha + I, \beta + J)$

•) $\ker\varphi = I \cap J = IJ$.

$\leadsto$ φ induce $R/IJ \simeq R/I \times R/J$. ▥

Ejemplo $p \equiv 1\ (4) \Rightarrow p = \pi \cdot \bar{\pi}$ en $\mathbb{Z}[i]$

$(\pi) + (\bar{\pi}) = \mathbb{Z}[i]$

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\bar{\pi}). \Leftarrow TCR.$$

$$\begin{array}{ccccc} \mathbb{Z}[i]/(p) & \simeq & \mathbb{Z}[i]/(\pi) & \times & \mathbb{Z}[i]/(\bar{\pi}) \\ \wr\| & & \wr\| & & \wr\| \\ \mathbb{F}_p[x]/(x^2+1) & \simeq & \mathbb{F}_p[x]/(x - \text{"}\sqrt{-1}\text{"}) & \times & \mathbb{F}_p[x]/(x + \text{"}\sqrt{-1}\text{"}) \end{array}$$

$\left(\frac{-1}{p}\right) = +1 \iff p \equiv 1 \ (4)$

$\iff x^2+1$ es reducible en $\mathbb{F}_p[x]$.

§ Ideales primos y maximales

elementos $\rightsquigarrow$ ideales

$\alpha \in R$ $\qquad$ $I \subseteq R$

primos $\rightsquigarrow$ ideales

$\pi \in R$ $\qquad$ primos $\mathfrak{p} \subset R$.

Def $\mathfrak{p} \subset R$ es primo si

a) $\mathfrak{p} \neq R$ y $\alpha\beta \in \mathfrak{p} \Rightarrow \alpha \in \mathfrak{p}$ ó $\beta \in \mathfrak{p}$.

a') $\mathfrak{p} \neq R$ y $IJ \subseteq \mathfrak{p} \Rightarrow I \subseteq \mathfrak{p}$ ó $J \subseteq \mathfrak{p}$

b) $R/\mathfrak{p}$ es un dominio. (* (0) no se considere como un dominio)

$\operatorname{Spec} R = \{ \mathfrak{p} \subset R \mid \text{ideal primo} \}$ – el espectro de R.

$\mathfrak{m} \subset R$ es maximal si

a) $\mathfrak{m} \neq R$ y $\mathfrak{m} \subseteq I \subsetneq R \Rightarrow I = \mathfrak{m}$.

b) $R/\mathfrak{m}$ es un campo.

Note maximal $\Rightarrow$ primo.

(campo $\Rightarrow$ dominio)

Ejemplo R – DIP. $\mathfrak{p} = (\pi)$ es primo $\iff$ π es primo.

para $\pi \neq 0$.

$\operatorname{Spec} R = \{(0)\} \cup \underbrace{\{(\pi) \mid \pi \in R \text{ primo}\}}_{\text{ideales maximales}}$

$(R/(\pi)$ es un campo$)$

$\operatorname{Spec} \mathbb{Z} = \{(0)\} \cup \underbrace{\{(2), (3), (5), (7), (11), \ldots\}}_{\text{ideales maximales}}$

$(\mathbb{Z}/(p) \simeq \mathbb{F}_p$ es un campo$)$

Ejemplo $R = \mathbb{Z}[\sqrt{-5}]$ $\quad \mathfrak{p} = (7, 3+\sqrt{-5})$

$\overline{\mathfrak{p}} = (7, 3-\sqrt{-5})$

Ejercicio: 7, $3 \pm \sqrt{-5}$ son irreducibles, no asociados

$(7, 3 \pm \sqrt{-5}) \neq (\gamma)$ no es principal.

$$1 = 7 - (3+\sqrt{-5}) - (3-\sqrt{-5}) \in \mathfrak{p} + \overline{\mathfrak{p}}$$

$$\mathfrak{p} + \overline{\mathfrak{p}} = \mathbb{Z}[\sqrt{-5}] \quad \text{(coprimos)}$$

$$\mathfrak{p}\overline{\mathfrak{p}} = (7, 3+\sqrt{-5})(7, 3-\sqrt{-5})$$
$$= (7^2, 7(3+\sqrt{-5}), 7(3-\sqrt{-5}), 7\cdot 2)$$
$$= (7)\cdot \underbrace{(7, 3+\sqrt{-5}, 3-\sqrt{-5}, 2)}_{=R} = 7R$$

$\mathfrak{p}$ y $\overline{\mathfrak{p}}$ son propios. Para verlo, notamos que

$\mathrm{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q}) = \{1, \sigma: \sqrt{-5} \mapsto -\sqrt{-5}\}$

$\quad \overset{\shortparallel}{G} \curvearrowright \mathbb{Z}[\sqrt{-5}]$. $\quad \overline{\mathfrak{p}} = \sigma(\mathfrak{p})$

$\overline{\mathfrak{p}} = R \iff \mathfrak{p} = R$. pero $\mathfrak{p}\overline{\mathfrak{p}} = 7R \neq R$.

$\Rightarrow \mathfrak{p}, \overline{\mathfrak{p}} \neq R$.

Ejercicio $\quad \mathfrak{p} = (7, 3+\sqrt{-5})$ $\quad$ Si $1 \in \mathfrak{p} \Rightarrow$

$$1 = (a+b\sqrt{-5})\cdot 7 + (c+d\sqrt{-5})(3+\sqrt{-5})$$
$$= \ldots\ldots$$

•) $\mathfrak{p}$ y $\overline{\mathfrak{p}}$ son maximales

$$\varphi: \mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_7[x]/(3+x) \simeq \mathbb{F}_7 \quad \boxed{3^2 \equiv -5 \ (7)}$$
$$a + b\sqrt{-5} \longmapsto a + b\bar{x} \longmapsto a - 3b.$$

$\mathrm{im}\,\varphi = \mathbb{F}_7$ campo.

$\ker\varphi = \mathfrak{p} = (7, 3+\sqrt{-5})$

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} \simeq \mathbb{F}_7 \Rightarrow \mathfrak{p} \text{ es maximal.}$$

$\mathbb{Z}[\sqrt{-5}]/\bar{\mathfrak{p}} \simeq \mathbb{F}_7 \Rightarrow \bar{\mathfrak{p}}$ es maximal.

Ejercicio Si $\varphi: S \to R$ es un homomorfismo $\Rightarrow$ $\mathfrak{p} \subset R$ primo $\Rightarrow \varphi^{-1}(\mathfrak{p}) \subset S$ tb. primo.

Ejemplo $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-5}] \rightsquigarrow \operatorname{Spec} \mathbb{Z}[\sqrt{-5}] \to \operatorname{Spec} \mathbb{Z}$

$$\mathfrak{p} \longmapsto \mathfrak{p} \cap \mathbb{Z}$$

$$(7, 3 I \sqrt{-5}) \cap \mathbb{Z} = 7\mathbb{Z}$$

Proposición Dado $I \subsetneq R$ ideal propio, existe $m \subset R$ maximal t.q. $I \subseteq m$.

Dem Lema de Zorn ($\Leftrightarrow$ axioma de elección) ▨

Def. R es un anillo local si R tiene único ideal maximal.

Ejemplo $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ es local.

$m = p\mathbb{Z}_{(p)}$

Proposición Si (R, m) es local $\Rightarrow R^{\times} = R \setminus m$.

Dem $\alpha \notin R^{\times} \Leftrightarrow (\alpha) \subsetneq R \Leftrightarrow (\alpha) \subseteq m$ ▨

§ Ideales en anillos de números

$$\left.\begin{array}{l} I \subset R \subset K \\ \qquad\qquad | <\infty. \\ \qquad\qquad \mathbb{Q} \end{array}\right\}$$

Lema $I \neq 0 \Rightarrow I \cap \mathbb{Z} \neq (0)$.

Dem $\alpha \in I \Rightarrow$

$\alpha \neq 0$

$$\overbrace{a_n\alpha^n + \dots + a_1\alpha}^{\in I} + a_0 = 0.$$

donde s.p.d.g.

$a_i \in \mathbb{Z}$, $a_0 \neq 0$.

$\Rightarrow a_0 \in I$ ▨

Corolario $\mathfrak{p} \subset R$ primo $\Rightarrow \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$

para $p = 2, 3, 5, 7, \ldots$

Teorema $\forall\, I \subset R$, $I \neq 0$, $\#(R/I) < \infty$.

Dem Cuando R es f.g. como $\mathbb{Z}$-módulo.

$$R \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \leq [K:\mathbb{Q}]}$$

lema: $\exists\, n > 0$ t.q. $n \in I$.

$$R/(n) \simeq \mathbb{Z}/n \oplus \cdots \oplus \mathbb{Z}/n$$

$$\#(R/I) \leq \#(R/(n)) \leq n^r \leq n^{[K:\mathbb{Q}]}$$ ▨

la próxima clase: las consecuencias de $\#(R/I) < \infty$.

- noetheriano
- $\dim R = 0$ ó 1. $\Leftrightarrow$ todo primo no nulo es maximal