Álgebra

Ignacio Cordón Castillo

Álgebra conmutativa

Tema 1: Anillos e ideales

Tema 3: Bases de Groebner y algoritmos básicos

Definición. *R anillo. Un R módulo (izquierda) es un grupo abeliano M, junto a una operación externa* $\$ \begin{array}{c} RM\& \longrightarrow \&M \\ (r,x)\& \mapsto \&rx\$ \end{array}$

verificando, $\forall x, y \in M, \forall r, s \in R$

- $r(x+y) = rx + ry$
- $(r+s)x = rx + sx$
- $r(sx) = (rs)x$
- $1x = x$

Definición. *Una R álgebra es un anillo S que tiene estructura de R módulo tal que* $(rx)y = r(xy) = x(ry) \quad \forall r \in R, \quad \forall x, y \in S$

También puede caracterizarse una R álgebra como un anillo S junto a un homomorfismo de anillos $\lambda : R \longrightarrow S$. El homomorfismo λ se llama homomorfismo de estructura de la R álgebra S.

Si $R = K$ cuerpo, λ es inyectiva, S es K álgebra que contiene a K como subanillo.

Como caso particular, todo anillo es una $\mathbb{Z}$ álgebra.

Definición. *Dadas S_1, S_2 \$R-\$álgebras. Un homomorfismo de \$R-\$álgebras de S_1 en S_2 es un homomorfismo de anillos $f : S_1 \longrightarrow S_2$ que es también homomorfismo de R módulos.*

Proposición. ***Propiedad universal de*** $R[X_1, \dots X_n]$

Sea S anillo, $f : R \longrightarrow S$ homomorfismo de anillos. Sean $s_1, \dots s_n \in S$ elementos arbitrarios. Entonces $\exists f_{s_1,\dots s_n} : R[X_1, \dots X_n] \longrightarrow S$ homomorfismo de R álgebras verificando $f_{s_1,\dots s_n}(X_i) = s_i$ y $f_{s_1,\dots s_n} \circ \lambda = f$ que además es único.

Definición. *Una R álgebra S se llama finitamente generada si existe un homomorfismo de R álgebras sobreyectivo $f : R[X_1, \dots X_n] \longrightarrow S$*

Dado $F \in K[X_1, \dots X_n]$, $\qquad F = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$

$\{X^\alpha : \alpha \in \mathbb{N}^n\}$ es K base de $K[X_1, \dots, X_n]$

Cualquier orden en $\mathbb{N}^n$ induce un orden en $\{X^\alpha : \alpha \in \mathbb{N}^n\}$

Definición. *Un orden $\leq$ en $\mathbb{N}^n$ diremos que es* ***compatible*** *si siempre que $\alpha \geq \beta$ entonces $\alpha + \gamma \geq \beta + \gamma \qquad \forall \gamma \in \mathbb{N}^n$.*

Diremos que es ***monótono*** *si 0 es mínimo en $\mathbb{N}^n$*

Diremos que un orden es ***monomial*** *si es compatible, total y monótono.*

Proposición. *Si $\leq$ es orden monomial en $\mathbb{N}^n$ entonces se verifica que dados $\alpha, \beta \in \mathbb{N}^n$:*

$$\alpha \leq_{pr} \beta \Longrightarrow \alpha \leq \beta$$

Ejercicios

Ejercicio 1.12

Demuestra que si un anillo verifica que cada elmento x verifica $x^n = x$

para algún $n \geq 2$ (dependiente de x) entonces todo ideal primo es maximal.

Ejercicio 1.16

Un anillo R se dice anillo de Boole si $x^2 = x$ para todo $x \in R$. Probar que en un anillo de Boole se tiene:

1. $2x = 0$ para todo $x \in R$
2. Cada ideal primo Π es maximal y R/Π es un cuerpo con dos elementos.
3. Cada ideal finitamente generado es principal.

1-

Se tiene:

$$2x^2 = 2x = (2x)^2 = 4x^2$$

Luego $2x^2 = 0$.

2-

Sea Π ideal primo. Entonces R/Π es dominio de integridad. Pero dado $x + \Pi \in R/\Pi$, x no unidad, se tiene $(x + \Pi) + (x + \Pi) = (2x + \Pi) = \Pi$ que por ser dominio de integridad $x \in Pi$. Luego R/Π es cuerpo con dos elementos y Π maximal.

3-

Solución propuesta por M42

Por inducción, $(a, b) = (a + b + ab)$ ya que $a(a + b + ab) = a^2 = a$ y análogo b.

Y el paso de inducción es trivial.

Ejercicio 1.17

En un anillo R sea Σ el conjunto de todos los ideales en los que cada elemento es un divisor de cero. Probar que el conjunto Σ tiene elementos maximales y que cada elemento maximal de Σ es un ideal primo. Por tanto el conjunto de los divisores de cero en R es una unión de ideales primos.

Ejercicio 1.18

Sea K un cuerpo, demuestra que el ideal $(X^3 - Y^2) \subseteq K[X,Y]$ es un ideal primo del anillo $K[X,Y]$.

Se puede probar, con una discusión de casos, escribiendo $X^3 - Y^2$ como producto de dos polinomios en $K[X,Y]$ que no puede ocurrir esta circunstancia, luego $X^3 - Y^2$ es irreducible en $K[X,Y]$ y por tanto, al ser K cuerpo, $(X^3 - Y^2)$ es primo.

Ejercicio 1.25

Sean α y β ideales de un anillo R

1. Demuestra que $\alpha + \beta = R$ si y sólo si $\alpha^n + \beta^n = R$ para cada natural n$
2. Demuestra que si α, β son ideales comaximales propios entonces $\alpha, \beta \subsetneq J(R)$
3. Demuestra que si $\alpha_1, \ldots \alpha_t$ son ideales comaximales dos a dos, entonces $\alpha_1 + (\alpha_2, \cdots \alpha_t)^n = R$ para cada $n \in \mathbb{N}$.

1-

La implicación hacia la izquierda es trivial tomando $n = 1$.

Hacia la derecha, $n = 1$ obvio

Por inducción, supuesto que se cumple hasta $n \in \mathbb{N}$

Existen $u + v = 1, \quad u \in \alpha^n, v \in \beta^n$. Desarrollando $(u+v)^{n+1} = 1$ es fácil comprobar que pertenece a $\alpha^n + \beta^n$

2-

Supuesto sin pérdida de generalidad que $\alpha \subset J(R)$.

Como existen $x \in \alpha$, $y \in \beta$ verificando $x + y = 1$ por ser comaximales, $y = 1 - x \in U(R)$ por caracterización de radical de Jacobson, luego $\beta = R$, contradicción.

3-

Si son primos dos a dos $\exists x_{i1} \in \alpha_1, y_i \in \alpha_i$ verificando $1 = x_i + y_i$ para todo $i \geq 2$. Luego:

$$\prod_{i=1}^{t}(1 - x_{i1}) = 1 + z = y_1 \cdots y_n \in \alpha_1, \cdots \alpha_t$$

con $z \in \alpha_1$. Luego $1 \in \alpha_1 + (\alpha_1, \cdots \alpha_t)$. Y la caracterización del apartado 1 acaba teniendo en cuenta que:

$$\alpha_1^n + (\alpha_1, \cdots \alpha_t)^n \subset \alpha_1 + (\alpha_1, \cdots \alpha_t)^n$$

Ejercicio 1.24

Sea R un anillo y $\mathcal{N}$ su nilradical. Demostrar que son equivalentes:

1. R tiene exactamente un ideal primo.
2. Cada elemento de R es o una unidad o nilpotente.

3. $R/\mathcal{N}$ es un cuerpo.

$1 \Longrightarrow 2$. Entonces $\mathcal{N}$ es maximal en R, por existir los ideales maximales en un anillo, ser todo ideal maximal primo y ser $Nil(R) = \{x \in \mathbb{R} : \exists n, x^n = 0\} = \bigcap_{\Pi \in Spec(R)} \Pi$ y en particular R es anillo local con maximal $\mathcal{N} \iff R - \mathcal{N} \subseteq U(R)$ lo que nos da el resultado.

$2 \Longrightarrow 3$. Trivialmente, ya que todo elemento no nulo es invertible.

$3 \Longrightarrow 1$. Los ideales primos de $R/\mathcal{N}$ son de la forma $\alpha + \mathcal{N}$ con α ideal primo de R. Pero como $R/\mathcal{N}$ es cuerpo, se tiene que sus únicos ideales son el total y $N \equiv 0$. Es decir $\alpha \subseteq \mathcal{N} \subseteq \alpha$ donde el último contenido viene dado por ser $\mathcal{N}\infty = \bigcap_{\Pi \in Spec(R)} \Pi$.

Luego $\alpha = \mathcal{N}$ único ideal primo de R.

Resumen de Álgebra III

Proposición. *El elemento α es algebraico sobre F si y solo si la extension $F(\alpha)/F$ es finito.*

Proposición. *Si la extensión K/F es finita, entonces es algebraica*

Definición. *La extensión K/F es finita si y solo si K está generado por un número finito de elementos algebraicos sobre F. De hecho, una extensión generada por elementos de grado $n_1, \ldots, n_k$ tiene grado menor o igual $n_1 n_2 \ldots n_k$*

Teorema. *K algebraico sobre F y L algebraico sobre K entonces L es algebraico sobre F*

Cuerpos de descomposición

Definición. *Sea K cuerpo, E/K extensión. $f(X) \in K[X]$ descompone en E si en $E[X]$ se factoriza como:*

$$f(X) = a(X - a_1) \cdots (X - a_n), \qquad a \in K, \quad a_1, \ldots a_n \in E$$

Cada $(X - a_i)$ *es un factor lineal.*

Si no existe F *verificando* $K \subseteq F \subseteq E$ *y que* $f(X)$ *descompone en* $F[X]$, $E[X]$ *se llama cuerpo de descomposición.*

Se deduce que $E = K(\alpha_1, \dots, \alpha_n)$ *donde* α_i *son raíces de* $f(X)$ *en* $E[X]$. *Por tanto todo polinomio* $f(X) \in K[X]$ *tiene un cuerpo de descomposición sobre* K

Proposición. *Un cuerpo de descomposición de un polinomio de grado* n *sobre* F *es de grado como mucho* $n!$ *sobre* F. *Si el grado es* $n!$ *entonces el polinomio es irreducible. El recíproco no se verifica.*