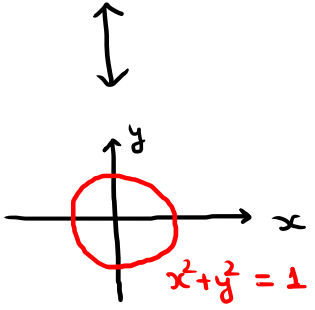
Parte II: Teoría de Anillos y Módulos

Clase 13: Anillos, cuerpos y álgebras

Motivación: Gracias a los trabajos revolucionarios de Alexander GROTHENDIECK, hoy en día sabemos que hay una íntima relación entre anillos (álgebra) y variedades (geometría, análisis, teoría de números, etc).

$$A = \mathbb{R}[x,y]/\langle x^2+y^2-1\rangle$$



Esto ha tenido grandes consecuencias! (eg. $x^n + y^n = z^n$ con $n \geq 3$ y $x,y,z \in \mathbb{Z}$)

§26. Anillos, cuerpos y álgebras (primeras definiciones)

Recordemos la definición de **anillo** y de **cuerpo**:

Def: Sea $(A, +, \cdot)$ un conjunto **no-vacío** con dos leyes de composición interna:

$$+ : A \times A \longrightarrow A \qquad \text{y} \qquad \cdot : A \times A \longrightarrow A$$
$$(a,b) \mapsto a+b \qquad\qquad (a,b) \longmapsto ab$$

Decimos que A es un **anillo** si:

1. $(A, +)$ es un grupo abeliano con neutro $0_A =: 0$
2. $(A, \cdot)$ es un monoide con neutro $1_A =: 1$ ← ⚠ Algunos textos sólo piden semigrupo.
3. Para todos $a, b, c \in A$ se cumple:
$$a(b+c) = ab + ac \quad \text{y} \quad (b+c)a = ba + ca.$$

Ejercicio Probar que $0_A = 1_A \iff A = \{0_A\}$ "anillo trivial"

⚠ **Convención**: A menos que se explicite lo contrario, todos los anillos $(A, +, \cdot)$ serán anillos abelianos, ie,

$$ab = ba \quad \text{para todos } a, b \in A.$$

↝ "Álgebra Conmutativa"! (Referencia clásica: Atiyah - MacDonald)

En la practica, la única excepción serán las matrices $M_n(A)$ con $n \geq 2$.

Def: Un anillo (abeliano) k es un cuerpo si: ("field" en inglés)

a) $k \neq \{0\}$

b) $(k \setminus \{0\}, \cdot)$ es un grupo (ie, todo elem $\neq 0$ posee inverso multiplicativo).

Recuerdo: Si A es un anillo, definimos su grupo de unidades por

$$A^\times = \{ a \in A \text{ tq } \exists b \in A \text{ que cumple } ab = 1 \}$$

Por ejemplo, $k \neq \{0\}$ es un cuerpo $\overset{\text{def}}{\iff}$ $k^\times = k \setminus \{0\}$.

Ejercicio Probar que $0_A \in A^\times \iff A = \{0_A\}$.

Ejemplos: Con la suma y producto usuales, tenemos que:

1. $\mathbb{Z}$ es un anillo, pero $\mathbb{N}$ no lo es.

2. $\mathbb{Z}/n\mathbb{Z}$ es un anillo (finito) y es un cuerpo si y sólo si $n = p$ número primo $\rightsquigarrow \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

3. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos

Def: Sea A un anillo y $n \in \mathbb{N}^{\geq 1}$. Un polinomio con coeficientes en A en n variables es una expresión de la forma:

$$f = \sum_{i_1, \dots, i_n \in \mathbb{N}} a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n} \quad \text{con } a_{i_1 \dots i_n} \in A \text{ y sólo finitos}$$

coeficientes $a_{i_1 \dots i_n}$ son $\neq 0$. Denotamos por $A[x_1, \dots, x_n]$ al correspondiente anillo de polinomios.

Def: Sean A y B anillos. Un **morfismo de anillos** es una función $\varphi: A \to B$ que preserva suma, productos y tal que $\varphi(1_A) = 1_B$. } Algunos textos no lo asumen.

Decimos que φ es un:

a) **isomorfismo** si φ es biyectiva, y escribimos $\varphi: A \xrightarrow{\sim} B$ y $A \cong B$.

b) **endomorfismo** si $A = B$.

c) **automorfismo** si $A = B$ y $\varphi: A \xrightarrow{\sim} A$ isomorfismo. $\rightsquigarrow \mathrm{Aut}(A)$ grupo de automorfismos

Ejercicio Probar que si $\varphi: A \to B$ morfismo de anillos, entonces $\varphi(A^\times) \subseteq B^\times$.

Ejercicio (muy útil!) Probar que $A[X][Y] \cong A[X,Y]$. } Lo usaremos siempre!

Ejercicio Determinar $\mathrm{Aut}(\mathbb{Z})$ como anillo y notar que $\mathrm{Aut}_{\text{anillo}}(\mathbb{Z}) \subsetneq \mathrm{Aut}_{\text{grupo}}(\mathbb{Z})$.

Cultura general Si $k \subseteq K$ son dos cuerpos, la teoría de Galois estudia el grupo

$$\mathrm{Gal}(K/k) = \{\varphi: K \xrightarrow{\sim} K \text{ isomorfismo tq } \varphi(x) = x \ \forall x \in k\}$$

Usando esto, se puede probar que $x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$ no posee fórmula explícita si $n \geq 5$ o que $\int e^{x^2} dx$ no posee primitiva (teo. de Galois diferencial)

Def: Sea A un anillo y $B \subseteq A$ un subconjunto. Decimos que B es un subanillo de A si B es un anillo y la inclusión

$$i : B \hookrightarrow A, \quad b \mapsto b$$

es un morfismo de anillos. En part, $0_B = 0_A$ y $1_B = 1_A$.

Ejemplo: Por definición, si $\varphi : A \to B$ es un morfismo de anillos, entonces la imagen $\mathrm{Im}(\varphi) \subseteq B$ es un subanillo de B. Sin embargo, el kernel

$$\ker(\varphi) := \{ a \in A \text{ tq } \varphi(a) = 0_B \} \subseteq A$$

podría no ser un subanillo de A en general.

Eg. $\varphi : \mathbb{Z}/4\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$, $[a]_4 \mapsto [a]_2$ morfismo de anillos

con $\ker(\varphi) = \{ [0]_4, [2]_4 \} \neq [1]_4$ (no es un anillo con unidad 1_A !)

Def: Sea A un anillo (fijo). Una **A-álgebra** (o **álgebra** si A es claro en el contexto) es un anillo B junto con un morfismo de anillos $\varphi = \varphi_B : A \to B$ llamado **morfismo estructural**.

(Abuso de) Notación: Si $a \in A$ y $b \in B$, escribimos $a \cdot b \overset{\text{def}}{=} \varphi(a) b \in B$.

Ejemplo típico: Si $A = \mathbb{k}$ cuerpo, una $\mathbb{k}$-álgebra es un $\mathbb{k}$-ev. con estructura de anillo (eg. $\Omega \subseteq \mathbb{R}^n$ abierto $\neq \emptyset \rightsquigarrow C^\infty(\Omega)$ es un $\mathbb{R}$-álgebra).

Ejemplo importante (propiedad universal de $A[x_1, \dots, x_n]$): Sea A un anillo.

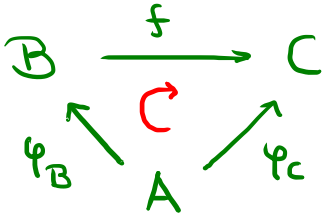
Dados un morfismo de anillos $\varphi : A \to B$ y dados $b_1, \dots, b_n \in B$

$\Rightarrow \exists!\ \pi : A[x_1, \dots, x_n] \to B$ morfismo de anillos tal que $\pi|_A = \varphi$ y $\pi(x_i) = b_i$

Explícitamente:

$$\pi\left(\sum a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}\right) \overset{\text{def}}{=} \sum \varphi(a_{i_1 \dots i_n}) b_1^{i_1} \cdots b_n^{i_n} \quad \blacksquare$$

Def: Sea A un anillo (fijo) y sean $\varphi_B : A \to B$, $\varphi_C : A \to C$ dos A-álgebras. Un morfismo de A-álgebras es un morfismo de anillos $f : B \to C$ que es compatible con los morfismos estructurales, ie,



es conmutativo $\rightsquigarrow$ Concretamente: $f(\varphi_B(a)\, b) = \varphi_C(a)\, f(b)$

ie, $f(a \cdot b) = a \cdot f(b)$ es "A-lineal"

Ejemplo (Propiedad universal de $A[X_1, \dots, X_n]$): Sea A un anillo.

Dada una A-álgebra B y $b_1, \dots, b_n \in B$

$\Rightarrow \exists!\ \pi : A[X_1, \dots, X_n] \to B$ morfismo de A-álgebras tq $\pi(X_i) = b_i \ \forall i \in \{1, \dots, n\}$.

"$A[X_1, \dots, X_n]$ es la A-álgebra más pequeña equipada con una lista de n elementos"

Una de las nociones centrales en Álgebra Conmutativa es: (Tendrá interpretación geométrica)

Def (Emmy Noether, 1921): Un anillo A es un **dominio de integridad** (o **dominio**) si:

a) $A \neq \{0\}$,

b) Para todos $a, b \in A$: $ab = 0$ implica que $a = 0$ ó $b = 0$.

Ejemplos: ① $\mathbb{Z}$ es un dominio ✓

② Todo cuerpo k es un dominio (pues $ab = 0$ y $a \neq 0 \Rightarrow a^{-1}ab = b = 0$ ✓)

③ Si $A \subseteq B$ y B es dominio (eg. cuerpo) $\Rightarrow$ A es un dominio.

④ $\mathbb{Z}/n\mathbb{Z}$ es un dominio $\Leftrightarrow$ n es primo ($\Rightarrow$ si $n = ab \Rightarrow [a]_n[b]_n = [0]_n$)

Ejercicio Probar que si A es un dominio entonces $A[X]$ también.

Corrección: Si A es un dominio entonces $A[X_1, \ldots, X_n]$ también } Muy útil

Una de las tantas utilidades de los dominios es que podemos asociarles cuerpos:

Def: Sea A un dominio. Definimos su cuerpo de fracciones, denotado $Fr(A)$ (o $K(A)$, o K_A, o $Q(A)$, etc), mediante:

$$Fr(A) := (A \times (A \setminus \{0\}))/\sim \quad \text{con} \quad (a,b) \sim (c,d) \overset{\text{def}}{\iff} ad = bc \text{ en } A.$$

Notación: $[(a,b)] := \frac{a}{b} \in Fr(A)$ y $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$ ← bien definidos!

Ejercicio importante Probar que $Fr(A)$ es un cuerpo y que $i_A : A \hookrightarrow Fr(A)$, $a \mapsto \frac{a}{1}$ es un morfismo de anillos inyectivo $\rightsquigarrow A \cong i_A(A) \subseteq Fr(A)$ subanillo.

Ejemplo: ① Si $A = \mathbb{Z}$, entonces $Fr(A) = \mathbb{Q}$.

② Si k es un cuerpo, $Fr(k) \cong k$ (pues $i_k : k \xrightarrow{\sim} Fr(k)$ isomorfismo)

⚠ Si k es un cuerpo, entonces $k[X]$ es un dominio (cf. Ejercicio Pizarra 9), pero no es un cuerpo! (eg. $X \in \mathbb{R}[X]$ no es invertible)

Ejercicio* Sea A un dominio. Probar que $A[X]^\times = A^\times$ son los polinomios constantes no-nulos invertibles en A.

[Indicación: Sean $f = a_n X^n + \dots + a_1 X + a_0$ y $g = b_m X^m + \dots + b_1 X + b_0$. Si $fg = 1$, probar que $a_0, b_0 \in A^\times$, que $a_n b_m = 0$, $a_n^2 b_{m-1} = 0$, $\dots$, $a_n^{m+1} b_0 = 0$ y concluir argumentando por inducción en $\deg(f)$.]

Obs: Si $A = \mathbb{Z}/4\mathbb{Z}$ (no es dominio), $f = 2X+1$ cumple $f^2 = 1$ en $A[X]$.

[Def: Sea A un dominio y $n \in \mathbb{N}^{\geq 1}$. Definimos el cuerpo de funciones racionales con coef. en A en n variables mediante:

$$A(X_1, \dots, X_n) := \mathrm{Fr}(A[X_1, \dots, X_n]) \overset{\text{def}}{=} \left\{ \frac{f(X_1, \dots, X_n)}{g(X_1, \dots, X_n)} \text{ con } f, g \in A[X_1, \dots, X_n] \text{ y } g \neq 0 \right\}$$