Álgebra II Práctica (clase 10)

Guido Arnone

Universidad de Buenos Aires

19 de Mayo de 2020

Prerrequisitos

Para leer estas diapositivas se recomienda haber leído el apunte teórico hasta el comienzo de la Sección 2.4.

Más ejemplos de anillos

Si $X \subset \mathbb{R}^n$ es un subconjunto, las funciones continuas

$$\mathscr{C}(X) = \{f : X \to \mathbb{R} : \ f \text{ es continua}\}$$

son un anillo, con las operaciones

$$(f+g)(x) := f(x) + g(x) \quad \text{y} \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

Más ejemplos de anillos

Si $X \subset \mathbb{R}^n$ es un subconjunto, las funciones continuas

$$\mathscr{C}(X) = \{f : X \to \mathbb{R} : \ f \text{ es continua}\}$$

son un anillo, con las operaciones

$$(f+g)(x) := f(x) + g(x) \quad \text{y} \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

Si X es un abierto, las funciones de clase $\mathscr{C}^n$ con $n \in \mathbb{N}$ o $\mathscr{C}^\infty$ son subanillos de $\mathscr{C}(X)$,

$$\mathscr{C}^\infty(X) \subset \mathscr{C}^n(X) \subset \mathscr{C}(X).$$

Más ejemplos de anillos (cont.)

Otro ejemplo algebraico, además de los ya vistos, es el de las series formales de potencias $A[\![X]\!]$ con coeficientes en un anillo conmutativo A.

Más ejemplos de anillos (cont.)

Otro ejemplo algebraico, además de los ya vistos, es el de las series formales de potencias $A[\![X]\!]$ con coeficientes en un anillo conmutativo A.

Sus elementos son expresiones de la forma $\sum_{n\geq 0} a_n X^n$, donde todos los coeficientes a_n pueden ser no nulos. Formalmente las podemos pensar como sucesiones $(a_i)_{i\geq 0} \in A^{\mathbb{N}_0}$. Las operaciones aquí son

$$\left(\sum_{n\geq 0} a_n X^n\right) + \left(\sum_{n\geq 0} b_n X^n\right) := \sum_{n\geq 0} (a_n + b_n) X^n$$

y

$$\left(\sum_{n\geq 0} a_n X^n\right) \cdot \left(\sum_{n\geq 0} b_n X^n\right) := \sum_{n\geq 0} \left(\sum_{i+j=n} a_i b_j\right) X^n.$$

Más ejemplos de anillos (cont.)

Los polinomios con coeficientes en $A[X]$ son un subanillo de las series formales: se corresponden con las expresiones $\sum_{n\geq 0} a_n X^n$ con finitos coeficientes no nulos. En particular A es un subanillo de $A[\![X]\!]$.

Más ejemplos de anillos (cont.)

Los polinomios con coeficientes en $A[X]$ son un subanillo de las series formales: se corresponden con las expresiones $\sum_{n\geq 0} a_n X^n$ con finitos coeficientes no nulos. En particular A es un subanillo de $A[\![X]\!]$.

Otro ejemplo es el de los enteros de Gauß o enteros gaussianos: son el subanillo de $\mathbb{C}$ dado por

$$\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\},$$

con la suma y producto de números complejos.

Unidades, divisores de cero y dominios

Recordemos que si A es un anillo, un elemento $a \in A$ se dice:

Unidades, divisores de cero y dominios

Recordemos que si A es un anillo, un elemento $a \in A$ se dice:

- una unidad si existen $b, c \in A$ tales que $ab = ca = 1$. Las unidades forman un grupo con la multiplicación de A.

Unidades, divisores de cero y dominios

Recordemos que si A es un anillo, un elemento $a \in A$ se dice:

- una unidad si existen $b, c \in A$ tales que $ab = ca = 1$. Las unidades forman un grupo con la multiplicación de A.
- un divisor de cero si $a \neq 0$ y existe $b \in A \setminus \{0\}$ tal que $ab = 0$ ó $ba = 0$.

Unidades, divisores de cero y dominios

Recordemos que si A es un anillo, un elemento $a \in A$ se dice:

- una unidad si existen $b, c \in A$ tales que $ab = ca = 1$. Las unidades forman un grupo con la multiplicación de A.
- un divisor de cero si $a \neq 0$ y existe $b \in A \setminus \{0\}$ tal que $ab = 0$ ó $ba = 0$.

Decimos también que un anillo A es un dominio si no posee divisores de cero, es decir, si $ab = 0$ implica $a = 0$ ó $b = 0$ para todo $a, b \in A$.

Unidades, divisores de cero y dominios

Observación

Sea A un anillo y $a \in A$ una unidad. Existen entonces $b, c \in A$ tales que $ab = 1 = ca$. Esto implica que $b = c$, pues

$$c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b.$$

Por lo tanto, un elemento $a \in A$ es una unidad si y sólo si existe $b \in A$ tal que $ba = ab = 1$.

En tal caso, el elemento $b \in A$ es el único inverso (a izquierda y a derecha) de a, pues si $xa = 1$ entonces $b = x(ab) = x$, y similarmente si $ax = 1$ entonces $x = (ba)x = b(ax) = b$. Notamos a^{-1} al inverso de A.

Unidades, divisores de cero y dominios (cont.)

Proposición

Sea A un anillo. Si $a \in A$ es una unidad, no es un divisor de cero.

Unidades, divisores de cero y dominios (cont.)

Proposición

Sea A un anillo. Si $a \in A$ es una unidad, no es un divisor de cero.

Demostración.

Supongamos que existe $a' \in A$ tal que $aa' = 0$. Como a es una unidad, sabemos por otro lado que existe $c \in A$ tal que $ca = 1$. Multiplicando por c en la primera igualdad es

$$0 = caa' = (ca)a' = 1 \cdot a' = a'.$$

De la misma forma, multiplicando por el inverso a derecha vemos que si $a'a = 0$, entonces $a' = 0$. □

Unidades, divisores de cero y dominios (cont.)

Proposición

Sea A un anillo. Si $a \in A$ es una unidad, no es un divisor de cero.

Demostración.

Supongamos que existe $a' \in A$ tal que $aa' = 0$. Como a es una unidad, sabemos por otro lado que existe $c \in A$ tal que $ca = 1$. Multiplicando por c en la primera igualdad es

$$0 = caa' = (ca)a' = 1 \cdot a' = a'.$$

De la misma forma, multiplicando por el inverso a derecha vemos que si $a'a = 0$, entonces $a' = 0$. □

Corolario

Un cuerpo es un dominio.

Unidades, divisores de cero y dominios (cont.)

Veamos ahora algunos ejemplos de cálculo de unidades y divisores de cero.

Ejemplo

Si $m \in \mathbb{N}$, el grupo $\mathbb{Z}_m$ de enteros módulo es un anillo conmutativo con producto $[x] \cdot [y] := [xy]$.

Cuando m es compuesto, este anillo no es un dominio: si $1 \neq d | m$ es un divisor propio y $m = d \cdot s$, entonces $[d], [s] \neq 0$ pero $[d \cdot s] = 0$.

De hecho,

Unidades, divisores de cero y dominios (cont.)

Veamos ahora algunos ejemplos de cálculo de unidades y divisores de cero.

Ejemplo

Si $m \in \mathbb{N}$, el grupo $\mathbb{Z}_m$ de enteros módulo es un anillo conmutativo con producto $[x] \cdot [y] := [xy]$.

Cuando m es compuesto, este anillo no es un dominio: si $1 \neq d | m$ es un divisor propio y $m = d \cdot s$, entonces $[d], [s] \neq 0$ pero $[d \cdot s] = 0$.

De hecho,

Proposición

El anillo $\mathbb{Z}_m$ es un dominio si y sólo si es un cuerpo, y esto sucede exactamente cuando m es primo.

Para verlo pueden resolver el ejercicio 5 de la práctica 4, que entre otras cosas pide probar que el grupo de unidades de $\mathbb{Z}_m$ es

$$\mathcal{U}_m := \{[n] \in \mathbb{Z}_m : (n : m) = 1\}.$$

Unidades, divisores de cero y dominios (cont.)

Supongamos ahora que B es un anillo y $A \subset B$ un subanillo. En general, no es cierto que si $a \in A$ es una unidad como elemento de B, lo sea como elemento de A.

Unidades, divisores de cero y dominios (cont.)

Supongamos ahora que B es un anillo y $A \subset B$ un subanillo. En general, no es cierto que si $a \in A$ es una unidad como elemento de B, lo sea como elemento de A.

Por ejemplo, como $\mathbb{C}$ es un cuerpo es $\mathcal{U}(\mathbb{C}) = \mathbb{C} \setminus \{0\}$, pero sin embargo no todo de elemento no nulo de $\mathbb{Z}[i]$ es una unidad: si $z = 1 + i$ y $a, b \in \mathbb{Z}$ entonces

$$1 = (a + ib)(1 + i) = (a - b) + i(a + b)$$

implicaría $a = b + 1$ y $0 = a + b = 2b + 1$, lo que es absurdo pues b es un entero.

Unidades, divisores de cero y dominios

Otro ejemplo es el siguiente: el polinomio $1 - X$ no es una unidad en $\mathbb{R}[X]$, pues si $f \neq 0$ es tal que $f \cdot (1 - X) = 1$ entonces tomando grado vemos que $\deg f + 1 = 0$, y esto es absurdo.

Sin embargo, como serie formal este polinomio es inversible: en $\mathbb{R}[\![X]\!]$ es

$$\left(\sum_{n\geq 0} X^n\right)(1 - X) = \sum_{n\geq 0} X^n - \sum_{n\geq 1} X^n = X^0 = 1.$$

Unidades, divisores de cero y dominios (cont.)

Antes de seguir, volvamos a un ejemplo analítico: el ejercicio 4 de la práctica 4 pide caracterizar las unidades y los divisores de cero de $\mathscr{C}[0,1]$. Para resolverlo son necesarias algunas nociones de topología en $\mathbb{R}$ como las que se ven en Taller de Cálculo Avanzado.

Para entender un poco las propiedades de este anillo, veamos que la función $f : [0,1] \to \mathbb{R}$ definida por $f(x) := |x|$ no es una unidad ni un divisor de cero.

Unidades, divisores de cero y dominios (cont.)

Antes de seguir, volvamos a un ejemplo analítico: el ejercicio 4 de la práctica 4 pide caracterizar las unidades y los divisores de cero de $\mathscr{C}[0,1]$. Para resolverlo son necesarias algunas nociones de topología en $\mathbb{R}$ como las que se ven en Taller de Cálculo Avanzado.

Para entender un poco las propiedades de este anillo, veamos que la función $f : [0,1] \to \mathbb{R}$ definida por $f(x) := |x|$ no es una unidad ni un divisor de cero.

Si f fuera una unidad, existiría $g : [0,1] \to \mathbb{R}$ tal que $f \cdot g \equiv 1$. Sin embargo esto supone una contradicción, pues evaluando en 0 tendríamos que $1 = (f \cdot g)(0) = f(0) \cdot g(0) = 0 \cdot g(0) = 0$.

Unidades, divisores de cero y dominios (cont.)

Antes de seguir, volvamos a un ejemplo analítico: el ejercicio 4 de la práctica 4 pide caracterizar las unidades y los divisores de cero de $\mathscr{C}[0,1]$. Para resolverlo son necesarias algunas nociones de topología en $\mathbb{R}$ como las que se ven en Taller de Cálculo Avanzado.

Para entender un poco las propiedades de este anillo, veamos que la función $f : [0,1] \to \mathbb{R}$ definida por $f(x) := |x|$ no es una unidad ni un divisor de cero.

Si f fuera una unidad, existiría $g : [0,1] \to \mathbb{R}$ tal que $f \cdot g \equiv 1$. Sin embargo esto supone una contradicción, pues evaluando en 0 tendríamos que $1 = (f \cdot g)(0) = f(0) \cdot g(0) = 0 \cdot g(0) = 0$.

Tampoco es f un divisor de cero: supongamos que $f \cdot g \equiv 0$ para cierta $g \in \mathscr{C}([0,1])$. Evaluando en cada $x \neq 0$ vemos que $0 = |x| \cdot g(x)$, y entonces $g(x) = 0$. Como g es continua, al anularse en $[0,1] \setminus \{0\}$ debe también anularse en 0, y por lo tanto $g \equiv 0$.

Morfismos de Anillos

Recordemos que si R y S son dos anillos, un morfismo de anillos es una función $f : R \to S$ tal que:

- $f(x+y) = f(x) + f(y)$ para todo $x, y \in R$.
- $f(xy) = f(x)f(y)$ para todo $x, y \in R$.
- $f(1) = 1$.

Si A es un subanillo de B, la inclusión $A \hookrightarrow B$ es un morfismo de anillos.

Veamos algunos ejemplos más.

Morfismos de Anillos - Ejemplos

- Si A es un anillo y $n \in \mathbb{N}$, entonces $i\colon a \in A \mapsto a \cdot I_n \in \mathrm{M}_n A$ es un morfismo de anillos, donde $(a \cdot I_n)_{ij} = a \cdot \delta_{ij}$.

Morfismos de Anillos - Ejemplos

- Si A es un anillo y $n \in \mathbb{N}$, entonces $i\colon a \in A \mapsto a \cdot I_n \in \mathrm{M}_n A$ es un morfismo de anillos, donde $(a \cdot I_n)_{ij} = a \cdot \delta_{ij}$.
- Si $f : R \to S$ es un morfismo de anillos, se tiene un morfismo de anillos $M_n f : M_n R \to M_n S$ definido como $(M_n f)(A)_{ij} := f(a_{ij})$. Es decir, aplicamos f coeficiente a coeficiente.

Morfismos de Anillos - Ejemplos

- Si A es un anillo y $n \in \mathbb{N}$, entonces $i\colon a \in A \mapsto a \cdot I_n \in \mathrm{M}_n A$ es un morfismo de anillos, donde $(a \cdot I_n)_{ij} = a \cdot \delta_{ij}$.
- Si $f : R \to S$ es un morfismo de anillos, se tiene un morfismo de anillos $M_n f : M_n R \to M_n S$ definido como $(M_n f)(A)_{ij} := f(a_{ij})$. Es decir, aplicamos f coeficiente a coeficiente.
- La conjugación $c\colon z \in \mathbb{C} \mapsto \overline{z} \in \mathbb{C}$ resulta un automorfismo de anillos.

Morfismos de Anillos - Ejemplos

- Si A es un anillo y $n \in \mathbb{N}$, entonces $i\colon a \in A \mapsto a \cdot I_n \in \mathrm{M}_n A$ es un morfismo de anillos, donde $(a \cdot I_n)_{ij} = a \cdot \delta_{ij}$.
- Si $f : R \to S$ es un morfismo de anillos, se tiene un morfismo de anillos $M_n f : M_n R \to M_n S$ definido como $(M_n f)(A)_{ij} := f(a_{ij})$. Es decir, aplicamos f coeficiente a coeficiente.
- La conjugación $c\colon z \in \mathbb{C} \mapsto \overline{z} \in \mathbb{C}$ resulta un automorfismo de anillos.
- Si V es un k-espacio vectorial de dimensión finita y $B = \{v_1, \ldots, v_n\}$ una base de V, entonces tenemos un isomorfismo de anillos

$$\begin{aligned} \varphi\colon \mathrm{End}_k(V) &\to \mathrm{M}_n k \\ f &\longmapsto [f]_B \end{aligned}$$

donde $[f]_B$ es la matriz de f en la base B. Esto induce un isomorfismo de grupos entre las unidades de ambos anillos,

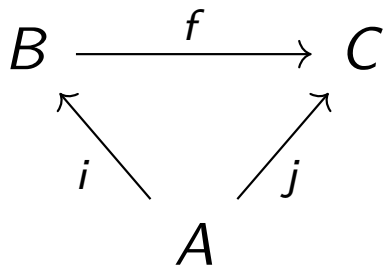
$$f \in \mathrm{Aut}_k(V) \mapsto [f]_B \in \mathrm{GL}_n k.$$

Álgebras

Recordemos que si A es un anillo, una A-álgebra es un anillo B junto con un morfismo de anillos $i : A \to B$, que llamamos morfismo estructural.

Por ejemplo, si A es un anillo entonces $A[X]$ y $\mathrm{M}_n A$ son A-álgebras con los morfismos $A \hookrightarrow A[X]$ e $i : a \in A \to aI_n \in \mathrm{M}_n A$.

Un morfismo entre dos A-álgebras B y C con morfismos estructurales $i : A \to B$ y $j : A \to C$ es un morfismo de anillos $f : B \to C$ tal que $fi = j$, es decir, conmuta el siguiente diagrama:



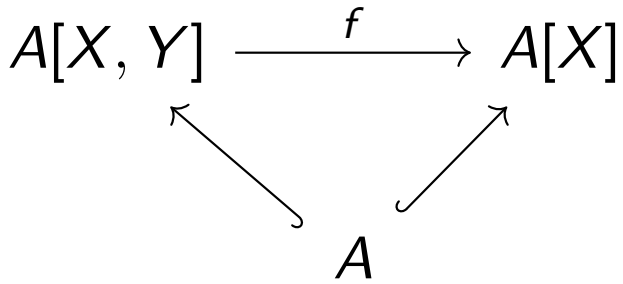
Álgebras (cont.)

En los ejemplos anteriores, el morfismo estructural es inyectivo o directamente una inclusión. Al menos intuitivamente, podemos pensar en la definición general a partir de estos ejemplos, donde una A-álgebra es un anillo que contiene una copia de A.

Así, un morfismo de álgebras es un morfismo de anillos que "envía una copia de A en la otra". Por ejemplo, el morfismo de anillos

$$f : p(X, Y) \in A[X, Y] \mapsto p(X, X) \in A[X]$$

es un morfismo de A-álgebras, ya que si $p(X, Y) = a$ es constante también lo es $p(X, X) = a$.



Morfismo de Evaluación

Un caso particular de la Proposición 2.2.11 del apunte teórico nos dice lo siguiente:

Proposición

Sea B una A-álgebra y $b \in B$. Existe entonces un único morfismo de A-álgebras $ev_b : A[X] \to B$ tal que $ev_a(X) = b$.

Concretamente, si $p = a_0 + a_1X + \cdots + a_nX^n$ y $j : A \to B$ es el morfismo estructural de B, entonces

$$ev_a(p) = j(a_0) + j(a_1)b + \cdots j(a_n)b^n.$$

Morfismo de Evaluación

Si k es un cuerpo y V un k-espacio vectorial, entonces $\mathrm{End}_k(V)$ es una k-álgebra con el morfismo $i : \lambda \mapsto f_\lambda \in \mathrm{End}_k(V)$ donde $f_\lambda(v) := \lambda \cdot v$ es la función lineal que multiplica por un escalar $\lambda \in k$.

Fijada una función lineal $f : V \to V$, el morfismo evaluación $ev_f : k[X] \to \mathrm{End}_k(V)$ es

$$ev_f(a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) = a_0 + a_1f + a_2f^2 + \cdots + a_nf^n$$

donde $f^i = \overbrace{f \circ \cdots \circ f}^{i \text{ veces}}$.

Morfismo de Evaluación

Si k es un cuerpo y V un k-espacio vectorial, entonces $\mathrm{End}_k(V)$ es una k-álgebra con el morfismo $i : \lambda \mapsto f_\lambda \in \mathrm{End}_k(V)$ donde $f_\lambda(v) := \lambda \cdot v$ es la función lineal que multiplica por un escalar $\lambda \in k$.

Fijada una función lineal $f : V \to V$, el morfismo evaluación $ev_f : k[X] \to \mathrm{End}_k(V)$ es

$$ev_f(a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) = a_0 + a_1f + a_2f^2 + \cdots + a_nf^n$$

donde $f^i = \overbrace{f \circ \cdots \circ f}^{i \text{ veces}}$.

Cuando V tiene dimensión finita, sabemos que existe algún polinomio para el cual $p(f) := ev_f(p) = 0$. En estos términos, el polinomio minimal de f es el polinomio no nulo $m_f \in \ker ev_f$ de grado mínimo. Un procedimiento similar para la k-álgebra $\mathrm{M}_n k$ nos permite evaluar un polinomio en una matriz y definir su polinomio minimal.

Ideales

Si A es un anillo, un ideal es un subconjunto $I \subset A$ que "es cerrado por sumas y absorbe productos".

Concretamente, decimos que $I \subset A$ es un ideal

- a izquierda si $a \cdot b \in I$ y $b + b' \in I$ para todo $b, b' \in I$ y $a \in A$.
- a derecha si $b \cdot a \in I$ y $b + b' \in I$ para todo $b, b' \in I$ y $a \in A$.
- bilátero si es un ideal a izquierda y a derecha. Notamos $I \lhd A$.

Ideales

Si A es un anillo, un ideal es un subconjunto $I \subset A$ que "es cerrado por sumas y absorbe productos".

Concretamente, decimos que $I \subset A$ es un ideal

- a izquierda si $a \cdot b \in I$ y $b + b' \in I$ para todo $b, b' \in I$ y $a \in A$.
- a derecha si $b \cdot a \in I$ y $b + b' \in I$ para todo $b, b' \in I$ y $a \in A$.
- bilátero si es un ideal a izquierda y a derecha. Notamos $I \lhd A$.

Podemos escribir compactamente estas condiciones como $I + I \subset I$ y $RI \subset I, IR \subset I$ o $RIR \subset I$ según corresponda.

Ideales

Si A es un anillo, un ideal es un subconjunto $I \subset A$ que "es cerrado por sumas y absorbe productos".

Concretamente, decimos que $I \subset A$ es un ideal

- a izquierda si $a \cdot b \in I$ y $b + b' \in I$ para todo $b, b' \in I$ y $a \in A$.
- a derecha si $b \cdot a \in I$ y $b + b' \in I$ para todo $b, b' \in I$ y $a \in A$.
- bilátero si es un ideal a izquierda y a derecha. Notamos $I \lhd A$.

Podemos escribir compactamente estas condiciones como $I + I \subset I$ y $RI \subset I, IR \subset I$ o $RIR \subset I$ según corresponda.

Si A es conmutativo, los tres conceptos coinciden.

Ideales (cont.)

Si $f : R \to S$ es un morfismo de anillos, entonces

$$\ker f = \{r \in R : f(r) = 0\}$$

es cerrado por sumas pues en particular f es un morfismo de grupos. Además, si $a, a' \in A$ y $b \in \ker f$ tenemos que

$$f(ab) = f(a)f(b) = f(a)0 = 0 = 0f(a') = f(b)(a') = f(ba')$$

y por lo tanto $ab, ba' \in \ker f$. Es decir, el núcleo de un morfismo de anillos es un ideal bilátero.

Ideales (cont.)

Si $f : R \to S$ es un morfismo de anillos, entonces

$$\ker f = \{r \in R : f(r) = 0\}$$

es cerrado por sumas pues en particular f es un morfismo de grupos. Además, si $a, a' \in A$ y $b \in \ker f$ tenemos que

$$f(ab) = f(a)f(b) = f(a)0 = 0 = 0f(a') = f(b)(a') = f(ba')$$

y por lo tanto $ab, ba' \in \ker f$. Es decir, el núcleo de un morfismo de anillos es un ideal bilátero.

En analogía con los subgrupos normales, tomando el cociente de un anillo por un ideal bilátero se puede ver que todo ideal bilátero es el núcleo de un morfismo de anillos.

Ideales (cont.)

Algunos ejemplos:

- En $\mathrm{M}_n\mathbb{Z}$ tenemos que $I = \{A \in \mathrm{M}_n\mathbb{Z} : A_{ij} \text{ es par } \ (\forall i, j \in [\![n]\!])\}$ es un ideal bilátero.

Ideales (cont.)

Algunos ejemplos:

- En $\mathrm{M}_n\mathbb{Z}$ tenemos que $I = \{A \in \mathrm{M}_n\mathbb{Z} : A_{ij} \text{ es par } \ (\forall i, j \in [\![n]\!])\}$ es un ideal bilátero.
- El subconjunto $\langle X - 2\rangle := \{f \cdot (X - 2) : f \in \mathbb{R}[X]\}$ es un ideal bilátero de $\mathbb{R}[X]$.

Ideales (cont.)

Algunos ejemplos:

- En $\mathrm{M}_n\mathbb{Z}$ tenemos que $I = \{A \in \mathrm{M}_n\mathbb{Z} : A_{ij} \text{ es par } \ (\forall i, j \in [\![n]\!])\}$ es un ideal bilátero.
- El subconjunto $\langle X - 2\rangle := \{f \cdot (X - 2) : f \in \mathbb{R}[X]\}$ es un ideal bilátero de $\mathbb{R}[X]$.
- Si $t \in [0, 1]$, entonces $\mathfrak{m}_t := \{f \in \mathscr{C}([0, 1]) : f(t) = 0\} \triangleleft \mathscr{C}([0, 1])$.

Ejercicio

Encontrar morfismos de anillos cuyos núcleos sean los anteriores ideales biláteros.

Cocientes

Si I es un ideal bilátero de un anillo A, es un subgrupo normal del grupo abeliano $(A, +)$ así que podemos considerar el cociente A/I. Vimos que en A/I podemos definir una única estructura de anillo tal que la proyección canónica $\pi\colon a \in A \mapsto [a] \in I$ sea morfismo de anillos. Concretamente, se define $[a] \cdot [b] := [ab]$.

Cocientes

Si I es un ideal bilátero de un anillo A, es un subgrupo normal del grupo abeliano $(A,+)$ así que podemos considerar el cociente A/I. Vimos que en A/I podemos definir una única estructura de anillo tal que la proyección canónica $\pi\colon a \in A \mapsto [a] \in I$ sea morfismo de anillos. Concretamente, se define $[a]\cdot[b] := [ab]$.

Recordemos además que como un morfismo $f\colon R \to S$ de anillos es un morfismo de grupos para $(R,+)$ y $(S,+)$, pasa al cociente. Es decir, se tiene un morfismo de grupos $\overline{f}\colon [a] \in A/I \mapsto f(a) \in S$. Lo anterior nos dice que en realidad $\overline{f}$ es un morfismo de anillos, pues

$$\overline{f}([a]\cdot[b]) = \overline{f}([ab]) = f(ab) = f(a)f(b) = \overline{f}([a])\overline{f}([b]).$$

Este morfismo es además el único tal que $f = \overline{f}\pi$.

Cocientes (cont.)

Como vimos en el Teorema 2.4.7 del apunte teórico, lo anterior nos da un teorema de isomorfismo para anillos. Si $f : R \to S$ es un morfismo de anillos, entonces $R/\ker f \simeq \mathrm{im} f$.

Cocientes (cont.)

Como vimos en el Teorema 2.4.7 del apunte teórico, lo anterior nos da un teorema de isomorfismo para anillos. Si $f : R \to S$ es un morfismo de anillos, entonces $R/\ker f \simeq \mathrm{im} f$.

Además, tenemos una correspondencia biyectiva

$$\{J \lhd R : J \supset \ker f\} \rightleftarrows \{\mathfrak{I} \lhd \mathrm{im} f\}$$

que envía un ideal bilátero $J \lhd R$ que contiene a $\ker f$ a $f(J)$, y un ideal bilátero $\mathfrak{I}$ de $\mathrm{im} f$ a $f^{-1}(\mathfrak{I})$.

Cocientes (cont.)

Como vimos en el Teorema 2.4.7 del apunte teórico, lo anterior nos da un teorema de isomorfismo para anillos. Si $f : R \to S$ es un morfismo de anillos, entonces $R/\ker f \simeq \mathrm{im} f$.

Además, tenemos una correspondencia biyectiva

$$\{J \lhd R : J \supset \ker f\} \rightleftarrows \{\mathfrak{I} \lhd \mathrm{im} f\}$$

que envía un ideal bilátero $J \lhd R$ que contiene a $\ker f$ a $f(J)$, y un ideal bilátero $\mathfrak{I}$ de $\mathrm{im} f$ a $f^{-1}(\mathfrak{I})$.

En particular, si aplicamos esto a la proyección al cociente $\pi : A \to A/I$, se obtiene una biyección

$$\{J \lhd R : J \supset I\} \rightleftarrows \{\mathfrak{I} \lhd A/I\}$$

tomando imagen y preimagen por π como antes.

Cocientes - Ejemplos

- La función $r_m : \mathbb{Z} \to \mathbb{Z}_m$ que asigna a un entero su resto en la división por $m \in \mathbb{Z}$ es un morfismo de anillos sobreyectivo. Se tiene entonces un isomorfismo $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$.

Cocientes - Ejemplos

- La función $r_m : \mathbb{Z} \to \mathbb{Z}_m$ que asigna a un entero su resto en la división por $m \in \mathbb{Z}$ es un morfismo de anillos sobreyectivo. Se tiene entonces un isomorfismo $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$.
- Sea k un cuerpo y $p = X - \lambda \in k[X]$ un polinomio lineal. El morfismo de evaluación $ev_\lambda : q \in k[X] \mapsto q(\lambda) \in k$ es sobreyectivo, pues $ev_r(X - \lambda + t) = t$ para todo $t \in k$, y tiene núcleo exactamente

$$\langle X - \lambda \rangle = \{(X - \lambda) \cdot f : f \in k[X]\}.$$

Por lo tanto, es $k[X]/\langle X - \lambda \rangle \simeq k$.

Cocientes - Ejemplos (cont.)

- Si $X \subset \mathbb{R}^n$ y $p \in X$, tenemos un morfismo de anillos $\mathrm{ev}_p : f \in \mathscr{C}(X) \mapsto f(p) \in \mathbb{R}$. Como las funciones constantes son continuas ev_p es sobryectivo, y su núcleo es

$$\mathfrak{m}_p = \{f \in \mathscr{C}(X) : f(p) = 0\}.$$

  Vemos entonces que $\mathscr{C}(X)/\mathfrak{m}_p \simeq \mathbb{R}$.

Cocientes - Ejemplos (cont.)

- Si $X \subset \mathbb{R}^n$ y $p \in X$, tenemos un morfismo de anillos $\mathrm{ev}_p : f \in \mathscr{C}(X) \mapsto f(p) \in \mathbb{R}$. Como las funciones constantes son continuas ev_p es sobryectivo, y su núcleo es

$$\mathfrak{m}_p = \{f \in \mathscr{C}(X) : f(p) = 0\}.$$

  Vemos entonces que $\mathscr{C}(X)/\mathfrak{m}_p \simeq \mathbb{R}$.

- Dado $p \in \mathbb{N}$ primo, podemos considerar la composición de morfismos sobreyectivos

$$\mathbb{Z}[X] \xrightarrow{ev_0} \mathbb{Z} \xrightarrow{r_p} \mathbb{Z}_p$$

  que envía un polinomio $p = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$ a $r_p(a_0)$. El núcleo de este morfismo son los polinomios tales que p divide a su coeficiente independiente, y esto a su vez es el ideal $\langle p, X \rangle$ generado por p y X (¿por qué?). Por lo tanto $\mathbb{Z}[X]/\langle p, X \rangle \simeq \mathbb{Z}_p$.

Ideales Primos y Maximales

Un ideal bilátero $I \triangleleft A$ se dice primo si $I \subsetneq A$ y $ab \in I$ implica $a \in I$ ó $b \in I$. Decimos que I es maximal si $I \subsetneq A$ y $J \supsetneq I$ implica $J = A$ para todo ideal $J \triangleleft A$.

Cuando A es conmutativo, la Proposición 2.4.17 del apunte teórico nos dice que $I \triangleleft A$ es primo si y sólo si A/I es un dominio e I es maximal si y sólo si A/I es un cuerpo. En particular, un ideal maximal es primo e $I = \{0\}$ es primo si y sólo si A es un dominio.

Ideales Primos y Maximales

Un ideal bilátero $I \lhd A$ se dice primo si $I \subsetneq A$ y $ab \in I$ implica $a \in I$ ó $b \in I$. Decimos que I es maximal si $I \subsetneq A$ y $J \supsetneq I$ implica $J = A$ para todo ideal $J \lhd A$.

Cuando A es conmutativo, la Proposición 2.4.17 del apunte teórico nos dice que $I \lhd A$ es primo si y sólo si A/I es un dominio e I es maximal si y sólo si A/I es un cuerpo. En particular, un ideal maximal es primo e $I = \{0\}$ es primo si y sólo si A es un dominio.

En estos términos, vimos que $\langle X - \lambda \rangle$ es un ideal maximal de $k[X]$ y que $m\mathbb{Z} \subset \mathbb{Z}$ es maximal si y sólo si m es un número primo. Los ideales primos de $\mathbb{Z}$ son en cambio los de la forma $m\mathbb{Z}$ con $m = 0$ ó m primo.

Ideales Primos y Maximales

Un ideal bilátero $I \lhd A$ se dice primo si $I \subsetneq A$ y $ab \in I$ implica $a \in I$ ó $b \in I$. Decimos que I es maximal si $I \subsetneq A$ y $J \supsetneq I$ implica $J = A$ para todo ideal $J \lhd A$.

Cuando A es conmutativo, la Proposición 2.4.17 del apunte teórico nos dice que $I \lhd A$ es primo si y sólo si A/I es un dominio e I es maximal si y sólo si A/I es un cuerpo. En particular, un ideal maximal es primo e $I = \{0\}$ es primo si y sólo si A es un dominio.

En estos términos, vimos que $\langle X - \lambda \rangle$ es un ideal maximal de $k[X]$ y que $m\mathbb{Z} \subset \mathbb{Z}$ es maximal si y sólo si m es un número primo. Los ideales primos de $\mathbb{Z}$ son en cambio los de la forma $m\mathbb{Z}$ con $m = 0$ ó m primo.

También son maximales los ideales $\mathfrak{m}_p \lhd \mathscr{C}(X)$. De hecho, si X es compacto estos son todos los ideales maximales de este anillo.

Ideales Primos y Maximales

Un ideal bilátero $I \lhd A$ se dice primo si $I \subsetneq A$ y $ab \in I$ implica $a \in I$ ó $b \in I$. Decimos que I es maximal si $I \subsetneq A$ y $J \supsetneq I$ implica $J = A$ para todo ideal $J \lhd A$.

Cuando A es conmutativo, la Proposición 2.4.17 del apunte teórico nos dice que $I \lhd A$ es primo si y sólo si A/I es un dominio e I es maximal si y sólo si A/I es un cuerpo. En particular, un ideal maximal es primo e $I = \{0\}$ es primo si y sólo si A es un dominio.

En estos términos, vimos que $\langle X - \lambda \rangle$ es un ideal maximal de $k[X]$ y que $m\mathbb{Z} \subset \mathbb{Z}$ es maximal si y sólo si m es un número primo. Los ideales primos de $\mathbb{Z}$ son en cambio los de la forma $m\mathbb{Z}$ con $m = 0$ ó m primo.

También son maximales los ideales $\mathfrak{m}_p \lhd \mathscr{C}(X)$. De hecho, si X es compacto estos son todos los ideales maximales de este anillo.

El ideal $\langle X \rangle \lhd \mathbb{Z}[X]$ es primo pero no maximal, ya que por ejemplo está contenido en $\langle p, X \rangle \subsetneq \mathbb{Z}[X]$ con $p \in \mathbb{Z}$ un primo. También podemos verlo calculando el cociente $\mathbb{Z}[X]/\langle X \rangle \simeq \mathbb{Z}$.

Ejercicios

Ejercicio

Probar que $\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Sugerencia: considerar $N : a + ib \in \mathbb{Z}[i] \mapsto a^2 + b^2 \in \mathbb{Z}$ *y observar que* $N(zw) = N(z)N(w)$ *para todo* $z, w \in \mathbb{Z}[i]$.

Ejercicio

Sea A un anillo conmutativo. Probar que A es un dominio si y sólo si $A[\![X]\!]$ lo es.

Ejercicio

Sea A un anillo y $P \lhd A$ un ideal primo que no contiene divisores de cero. Probar que A es un dominio.