ANILLOS

Definición de anillo (= ring)

(Serge Lang "Undergraduate Algebra" Second Edition Springer)

A **ring** R is a set, whose objects can be added and multiplied (i.e. we are given associations $(x, y) \mapsto x + y$ and $(x, y) \mapsto xy$ from pairs of elements of R, into R), satisfying the following conditions:

RI 1. *Under addition, R is an additive (abelian) group.* (neutro = 0)

RI 2. *For all $x, y, z \in R$ we have*

$$x(y + z) = xy + xz \quad \text{and} \quad (y + z)x = yx + zx.$$ (Distrib)

RI 3. *For all $x, y, z \in R$, we have associativity $(xy)z = x(yz)$.* (Asoc.)

RI 4. *There exists an element $e \in R$ such that $ex = xe = x$ for all $x \in R$.* ($e = 1$)

---

5. Si además se verifica que

$\forall x \in R - \{0\}$ existe $x' \in R$ tal que $xx' = x'x = 1$ (i.e. x tiene inverso)

entonces se dice que el anillo R es un cuerpo.

EJEMPLOS

1) $\mathbb{Z}$ con las operaciones $+$ y $\cdot$ habituales es un anillo. Pero no es un cuerpo: el 2 no tiene inverso.

2) $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos e incluso cuerpos. ($2 \cdot 1/2 = 1$)

3) $\mathbb{Z}/n\mathbb{Z}$ con las operaciones habituales es un anillo.

4) $\mathbb{Z}/n\mathbb{Z}$ sólo es un cuerpo cuando n es primo.

(Por ejemplo $\mathbb{Z}/4\mathbb{Z}$ no es un cuerpo porque $\bar{2}$ no tiene inverso: $\begin{cases} \bar{2}\cdot\bar{0}=\bar{0}\neq\bar{1} \\ \bar{2}\cdot\bar{1}=\bar{2}\neq\bar{1} \\ \bar{2}\cdot\bar{2}=\bar{0}\neq\bar{1} \\ \bar{2}\cdot\bar{3}=\bar{2}\neq\bar{1} \end{cases}$

Pero $\mathbb{Z}/5\mathbb{Z}$ sí lo es: $\begin{cases} \bar{1}\cdot\bar{1}=\bar{1} \\ \bar{2}\cdot\bar{3}=\bar{1} \\ \bar{3}\cdot\bar{2}=\bar{1} \\ \bar{4}\cdot\bar{4}=\bar{1} \end{cases}$)

5) Los anillos de polinomios:

$\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{Z}/n\mathbb{Z}[X]$

son, efectivamente, anillos.

Ninguno de éstos es un cuerpo.

(De hecho ningún polinomio de grado ≥ 1 tiene inverso, pues si $f(X)=a_0+a_1X+\cdots+a_nX^n$, con $n\geq 1$ y $a_n\neq 0$, entonces $\forall\, g(X)=b_0+b_1X+\cdots+b_mX^m$, con $b_m\neq 0$, se tiene:

$f(X)g(X)=a_0b_0+(a_1b_0+a_0b_1)X+\cdots+a_nb_mX^{n+m}$

que es un polinomio $\neq 1$; de hecho, como sabemos, es un polinomio de grado $=n+m=\deg(f)+\deg(g)$)

PREGUNTA:

¿Vale este argumento, i.e. vale la relación

$$\boxed{\deg(f\cdot g) = \deg(f)+\deg(g)},$$

en $\mathbb{Z}/n\mathbb{Z}[X]$, (e.g. para $n=6$)?

Si no, buscar otro argumento para este caso.

$\mathbb{Z}/6\mathbb{Z}[X]$: $(1+2X)(1+3X) = 1+5X+6X^2$

deg: $\quad 1 \quad\quad 1$ $\quad\quad 6=0$

Pero en cualquier caso $f(X)=X$ nunca tiene inverso.

$$X\cdot g(X) = X(b_0+b_1X+\cdots+\underset{\neq 0}{b_m}X^m) = b_0+b_1X^2+\cdots+b_mX^{m+1}$$

$$\deg(X\cdot g(X)) = \deg(X)+\deg(g(X)) = 1+\deg(g(X))$$

aunque trabajemos con coeficientes en $\mathbb{Z}/n\mathbb{Z}$.

6) $M_n(K) = \{$matrices $n \times n$ con coef. en el cuerpo $K\}$ con las operaciones $+$ y $\cdot$ habituales es un anillo.

- Elemento neutro respecto de $+$: $M = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \\ 0 & \cdots & 0 \end{pmatrix}$
- " " " " $\cdot$: $I = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$

7) Para cualquier anillo A, el producto cartesiano $A \times A$ con las operaciones $+$ y $\cdot$ definidas coordenada a coordenada es un anillo (e.g. $\mathbb{Z} \times \mathbb{Z}$ ó $\mathbb{Q} \times \mathbb{Q}$)

Los elementos neutros son $(0,0)$ y $(1,1)$ respectivamente.

PREGUNTA: ¿Es $\mathbb{Q} \times \mathbb{Q}$ un cuerpo?

~~SÍ~~: el inverso de $(3,5)$ es $(\frac{1}{3}, \frac{1}{5})$

¿inverso de $(0,1)$? No tiene $\Rightarrow \mathbb{Q} \times \mathbb{Q}$ no es un cuerpo.

8) Del mismo modo lo sería el producto infinito

$$\prod_{i=1}^{\infty} A_i = A \times \cdots \times A \times \cdots \qquad (A_i = A) \qquad (A, \text{anillo})$$

$0 = (0, \ldots 0, \ldots)$

$1 = (1, \ldots 1, \ldots)$

(los elementos son sucesiones infinitas de elementos de A)

Definición. Un anillo A se dice **conmutativo** si $xy = yx$ para todo $x, y \in A$.

(i.e. si es conmutativo respecto de la segunda operación. ¡Respecto de la primera, siempre lo es, por definición!)

• "anillo conmutativo", no se usa la expresión "anillo abeliano"

OBSERVACIÓN: De todos los anillos que han aparecido hasta ahora el único que no es conmutativo es $M_n(K)$.

As with groups, the element e of a ring R satisfying **RI 4** is unique, and is called the **unit element** of the ring. It is often denoted by 1. Note that if $1 = 0$ in the ring R, then R consists of 0 alone, in which case it is called the zero ring.

In a ring R, a number of ordinary rules of arithmetic can be deduced from the axioms. We shall list these.

We have $0x = 0$ *for all* $x \in R$.

Proof. We have

$$0x + x = 0x + ex = (0 + e)x = ex = x.$$

Hence $0x = 0$.

(pues $\forall x \in R$ tendríamos: $x = 1x = 0x = 0 \Rightarrow R = \{0\}$)

- Nosotros suponemos siempre que $1 \neq 0$ i.e. que $R \neq \{0\}$.

Otras propiedades que se verifican automáticamente son:

- *We have* $(-e)x = -x$ *for all* $x \in R$. (i.e. $(-1)x = -x$)

  Proof.

$$(-e)x + x = (-e)x + ex = (-e + e)x = 0x = 0.$$

- *We have* $(-e)(-e) = e$. (i.e. $(-1)(-1) = 1$)

  Proof. We multiply the equation

$$e + (-e) = 0$$

by $-e$, and find

$$-e + (-e)(-e) = 0.$$

Adding e to both sides yields $(-e)(-e) = e$, as desired.

- We leave it as an exercise to prove that

$$(-x)y = -xy \qquad \text{and} \qquad (-x)(-y) = xy$$

for all $x, y \in R$.

- From condition **RI 2**, which is called the **distributive law**, we can deduce the analogous rule with several elements, namely if $x, y_1, \ldots, y_n$ are elements of the ring R, then

$$x(y_1 + \cdots + y_n) = xy_1 + \cdots + xy_n.$$

Similarly, if $x_1, \ldots, x_m$ are elements of R, then

$$(x_1 + \cdots + x_m)(y_1 + \cdots + y_n) = x_1y_1 + \cdots + x_my_n$$
$$= \sum_{i=1}^{m} \sum_{j=1}^{n} x_i y_j.$$

The sum on the right hand side is to be taken over all indices i and j as indicated. These more general rules can be proved by induction, and we shall omit the proofs, which are tedious.

Definición Un subanillo de un anillo A es un subconjunto $A' \subset A$ que es un anillo con las mismas operaciones que A. Esto equivale a decir que A' satisface las siguientes condiciones:

1) $x, y \in R \Rightarrow -x,\ x+y \in R$

2) $1 \in R$

3) $x, y \in R \Rightarrow x \cdot y \in R$.

Ejemplo 9 $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, $\mathbb{Q}$ lo es de $\mathbb{R}$ y $\mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$ lo son de $\mathbb{C}$.

Ejemplo 10. Ya vimos que si A es un anillo, el conjunto de todas las sucesiones con coeficientes en A era un anillo que denotábamos por $S^A = \prod_{\substack{i=0 \\ A_i = A}}^{\infty} A_i = \left\{ (a_n)_{n=1}^{\infty} \,/\, a_n \in A \right\}$

Consideremos el subconjunto siguiente:

$$S_0^A = \bigoplus_{\substack{i=0 \\ A_i = A}}^{\infty} A_i = \left\{ (a_n) \in S^A \,/\, a_n = 0 \text{ salvo para un nº finito de términos} \right\}$$

$\mathcal{F}_0^A$ no es un subanillo porque falla la propiedad de que el $1 = (1, \cdots 1, \cdots) \in \mathcal{F}^A$ no está en $\mathcal{F}_0^A$.

Ejemplo 11 (definición formal del anillo de polinomios). Sea A un anillo conmutativo

A pesar de lo visto en el ejercicio anterior podemos definir en $\mathcal{F}^A$ dos operaciones respecto de las cuales sí va a ser un anillo (aunque no un subanillo del anillo $\mathcal{F}^A$ anterior)

Veamos cuáles son:

Los elementos de $\mathcal{F}_0^A$ son de la forma

$$f = (a_0, a_1, \cdots, a_n, a_{n+1}, a_{n+2}, \cdots)$$

donde $a_{n+1} = a_{n+2} = \cdots = 0$, i.e. $f = (a_0, a_1, \cdots, a_n, 0, \cdots 0, \cdots)$

Si $g = (b_0, b_1, \cdots b_m, b_{m+1}, b_{m+2}, \cdots)$

donde $b_{m+1} = b_{m+2} = \cdots = 0$, i.e. $g = (b_0, b_1, \cdots b_m, 0, \cdots 0, \cdots)$

+) $f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n, \cdots)$

·) $f \cdot g = (a_0 b_0, a_1 b_0 + a_0 b_1, a_2 b_0 + a_1 b_1 + a_0 b_2, \cdots, \sum_{i+j=k} a_i b_j, \cdots)$

Simplifiquemos un poco la notación:

$$a = (a, 0, 0, 0, \dots) \Rightarrow$$

$$1 = (1, 0, 0, 0, \dots)$$

$$X = (0, 1, 0, 0, \dots)$$

$$X^2 = (0, 0, 1, 0 \dots)$$

$$X^3 = (0, 0, 0, 1, \dots) \quad \text{e.tc.}$$

Con esta notación vemos que:

+) $0 = (0, 0, 0 \dots)$ es el elemento neutro respecto de la suma.

·) $1 = (1, 0, 0, \dots 0)$ es el elemento neutro respecto de la multiplicación

(En efecto; $(1, 0, 0, \dots)(b_0, b_1, b_2, \dots, b_n, \dots) =$

$= (1 \cdot b_0, 0b_0 + 1b_1, 0b_0 + 0b_1 + 1 \cdot b_2, \dots) = (b_0, b_1, b_2, \dots)$.

Además, se tiene:

$$X \cdot X = (0,1,0,0,\dots)\cdot(0,1,0,0,\dots) = (0{\cdot}0,\ 1{\cdot}0+0{\cdot}1,\ 0{\cdot}0+1{\cdot}1+0{\cdot}0,\ 0{\cdot}0+0{\cdot}1+1{\cdot}0+0{\cdot}0,\dots) = X^2$$

$a_0\ a_1\ a_2\ a_3 \quad b_0\ b_1\ b_2\ b_3$

$a_0b_0,\ a_1b_0+a_0b_1,\ a_2b_0+a_1b_1+a_0b_2,\ a_3b_0+a_2b_1+a_1b_2+a_0b_3,$

$$X \cdot X^2 = (0,1,0,0,\dots)(0,0,1,0,\dots) = (0,\ 1{\cdot}0+0{\cdot}0,\ 0{\cdot}0+1{\cdot}0+0{\cdot}0,\ 0{\cdot}0+0{\cdot}0+1{\cdot}1+0{\cdot}0,\dots) = X^3$$

$a_1 b_2$

Y, en general, $\boxed{X \cdots X = X^n}$ (n veces) y $\boxed{x^n \cdot x^m = x^{n+m}}$

Con esta notación podemos escribir:

$$f = (a_0, a_1, \dots a_n, 0, 0, \dots) = a_0 + a_1 X + \dots + a_n X^n = \sum_{i=0}^{n} a_i X^i$$

$$g = (b_0, b_1, \dots, b_m, 0, 0, \dots) = b_0 + b_1 X + \dots + b_m X^m = \sum_{j=0}^{m} b_j X^j .$$

$(A[X], +, \cdot)$

$$f + g = \sum (a_k + b_k) X^k$$

$$f \cdot g = a_0 b_0 + (a_1 b_0 + a_0 b_1) X + \dots + \left(\sum_{i+j=k} a_i b_j \right) X^k + \dots + a_n b_m X^{n+m}$$

En otras palabras, este anillo $\mathcal{P}_0^A$ no es más que el anillo de polinomios con coeficientes en un anillo conmutativo arbitrario A y suele denotarse por $A[X]$.

- Naturalmente, $\forall a \in A$ y $\forall f = \sum a_i x^i \in A[X]$ se tiene $a f = \sum a a_i x^i$

En efecto:

$$a f = (a, 0, 0, \dots) \cdot (a_0, a_1, a_2, \dots, a_n, 0, \dots) = (a a_0, a a_1, \dots, a a_n, 0, \dots) = \sum_{i=1}^{n} a a_i X^i$$

Definición. Sea A un anillo conmutativo.

Se dice que $x \in A$ es un **divisor de cero** si

1°) $x \neq 0$, y (y también es div. de cero!)

2°) $\exists\, y \in A$, $y \neq 0$, tal que $xy = 0$.

Si A no tiene divisores de cero, diremos que A es un **anillo íntegro** o un **dominio de integridad** (o, simplemente, un dominio)

Ejemplos: a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son anillos íntegros.

b) $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X]$ y $\mathbb{C}[X]$ también

c) $\mathbb{Z}/6\mathbb{Z}$ no es íntegro (pues $\bar{2}\cdot\bar{3} = \bar{0}$, $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$)

($\bar{2}$ y $\bar{3}$ son divisores de 0)

d) En general, $\mathbb{Z}/n\mathbb{Z}$ es íntegro $\Leftrightarrow$ n es primo

Dem d/

($\Leftarrow$) $\bar{a}\bar{b} = \bar{a}\bar{b} = \bar{0} \Rightarrow ab = \text{mult de } n \Rightarrow n \mid ab \xrightarrow{\text{si es primo}} \begin{cases} n \mid a \\ \text{o} \\ n \mid b \end{cases} \Rightarrow \begin{cases} \bar{a} = 0 \\ \text{o} \\ \bar{b} = 0 \end{cases}$

($\Rightarrow$) $n = ab \Rightarrow \bar{0} = \bar{n} = \bar{a}\bar{b}$

e) $A \times A$ no es íntegro (aunque A lo sea)

(pues $(1,0)\cdot(0,1) = (0,0)$)

Definición. Sea A un anillo conmutativo.

Se dice que $x \in A$ es una **unidad** de A si x tiene inverso respecto de la multiplicación, i.e. si existe $y \in A$ tal que $xy = 1$.

El conjunto de las unidades se suele denotar por A^*.

Observación A es un cuerpo $\Leftrightarrow$ $A^* = A - \{0\}$ (por definición de cuerpo)

Ejemplos i) $\mathbb{Z}^* = \{1, -1\}$ → estos son siempre unidades

ii) $(\mathbb{Z}/6\mathbb{Z})^* = \{\bar{1}, \bar{5}\}$

(pues $\bar{1} \cdot \bar{1} = \bar{1}$ y $\bar{5} \cdot \bar{5} = \bar{1}$)

mientras que $\bar{2}, \bar{3}$ y $\bar{4}$ son divisores de cero.

(pues $\bar{2} \cdot \bar{3} = 0$ y $\bar{4} \cdot \bar{3} = 0$)

iii) Un divisor de cero no puede ser una unidad.

($\left.\begin{array}{l} x'x = 1 \\ xy = 0 \\ \text{con } y \neq 0 \end{array}\right\} \Rightarrow x'xy = x' \cdot 0 = 0 \Rightarrow$

$\Rightarrow 0 = x'xy = 1 \cdot y = y \Rightarrow y = 0$

Contrad.)

iv) Sabemos del curso de Conjuntos y Números que $\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \{ \bar{a} \,/\, (a,n) = 1 \}$

($(a,n) = 1 \overset{\text{I. Bezout}}{\Longrightarrow} 1 = xa + yn \Rightarrow \bar{1} = \bar{x}\bar{a} + \bar{y}\cdot\bar{n} \Rightarrow \bar{1} = \bar{x}\bar{a} \Rightarrow \bar{a}$ y $\bar{x}$ son unidades)

v) Si K es un cuerpo conmutativo, entonces $(K[X])^* = K^*$ ($K^* = K - \{0\}$), i.e ningún polinomio de grado ≥ 1 puede ser una unidad.

(Claro: $\deg(f \cdot g) = \deg(f) + \deg(g)$)

vii) En el anillo $\mathbb{Z}/9\mathbb{Z}[X]$ el $\left(\mathbb{Z}/9\mathbb{Z}[X]\right)^* \supsetneq \left(\mathbb{Z}/9\mathbb{Z}\right)^*$ polinomio $f = 1 + 3X$, de grado $\deg(f) = 1$ sí es una unidad:

$$(1+3X)(1+6X) = 1 + (3+6)X + 18X^2 = 1$$

IDEALES

Excepto que se diga explícitamente otra cosa, de ahora en adelante, todos los anilos serán conmutativos.

Definición Un ideal de un anillo A es un subconjunto $J \subset A$ que satisface las siguientes propiedades:

1) $0 \in J$
2) $x, y \in J \Rightarrow x+y \in J$
3) $a \in A \wedge x \in J \Rightarrow ax \in J$.

Observación: $(J,+)$ es un grupo abeliano (es un subgrupo de $(A,+)$) porque $\forall x \in J \Rightarrow -x = (-1)x \in J$.

Ejemplo 1: $J=\{0\}$ y $J=A$ son ideales

Ejemplo 2: $(6) := \{m6 / m \in \mathbb{Z}\}$ es obviamente un ideal de $\mathbb{Z}$.

(X) es un ideal principal de Q[X]

$x, x^2, (1+3)x, \ldots \in (X)$

$1 \notin (X)$

pues $f \cdot X \neq 1$

$(a) = \{xa / x \in A\}$ ideal principal

Example 3. Let R be a ring, and a an element of R. The set of elements xa, with $x \in R$, is a [redacted] ideal, called the **principal [redacted] ideal** generated by a. (Verify in detail that it is an [redacted] ideal.) We denote it by $(a) = \{xa / x \in R\}$. More generally, let $a_1, \ldots, a_n$ be elements of R. The set of all elements

$$(a_1, \ldots, a_n) = \{x_1 a_1 + \cdots + x_n a_n \mid x_1, x_2, \ldots, x_n \in R\}$$

with $x_i \in R$, is a left ideal, denoted by $(a_1, \ldots, a_n)$. We call $a_1, \ldots, a_n$ **generators** for this ideal.

We shall give a complete proof for this to show how easy it is, [redacted]. If $y_1, \ldots, y_n, x_1, \ldots, x_n \in R$ then

2) $$(x_1 a_1 + \cdots + x_n a_n) + (y_1 a_1 + \cdots + y_n a_n) = x_1 a_1 + y_1 a_1 + \cdots + x_n a_n + y_n a_n = (x_1 + y_1) a_1 + \cdots + (x_n + y_n) a_n.$$

If $z \in R$, then

3) $$z(x_1 a_1 + \cdots + x_n a_n) = z x_1 a_1 + \cdots + z x_n a_n.$$

Finally,

1) $$0 = 0 a_1 + \cdots + 0 a_n.$$

This proves that the set of all elements $x_1 a_1 + \cdots + x_n a_n$ with $x_i \in R$ is an [redacted] ideal.

Observaciones: 1) $A = (1) = \{a \cdot 1 / a \in A\}$

2) Si $I \subset A$ es un ideal se verifica:

$I = A \Leftrightarrow 1 \in I$

Ejemplo 4. $I = \{p(x) = a_0 + a_1 X + \cdots + a_n X^n / a_0 = 0\}$ es un ideal de $A[X]$. De hecho $I = (X)$.

(no es un subanillo: $1 \notin I$)

$p(x) \in I \Rightarrow p(x) = a_1 X + \cdots + a_k X^k = (a_1 + a_2 X + \cdots + a_k X^{k-1}) \cdot X$

$\Rightarrow p(x) \in (X)$

Proposición. 1) Todo ideal I de $\mathbb{Z}$ es principal. De hecho si $I \neq (0)$, se tiene $I=(d)$, donde d es el menor entero >0 en I.

2) Si K es un cuerpo, todo ideal I de $K[X]$ es principal. De hecho, si $I \neq (0)$, se tiene $I=(d(X))$, donde $d(X)$ es un polinomio de grado mínimo en I. (A veces se dice que $\deg(0) = -\infty$)

Demostración. En ambos casos la razón es la misma y es que en $\mathbb{Z}$ y en $K[X]$ tenemos el concepto de división.

1) Sea $m \in I$. Tenemos que ver que $m \in (d)$.

Podemos suponer que $m>0$ pues $m \in I \Leftrightarrow -m \in I$, y si $I=(0)$ el resultado es obvio.

Dividamos: $\begin{matrix} m & \lfloor d \\ r & c \end{matrix}$ c.e. $m = cd + r$, con $r < d \Rightarrow$

$\Rightarrow r = \underset{I}{m} - c\underset{I}{d} \in I$, con $r<d \Rightarrow r=0 \Rightarrow m = cd$ c.q.d.

2) Vale la misma demostración, cambiando m, d, c, r por $m(X), d(X), c(X), r(X)$ y $r<d$ por $\deg(r(x)) < \deg(d(x))$.

Ejemplos. $I=(a,b) \subseteq \mathbb{Z} \Rightarrow I=(d)$, $d = mcd(a,b)$

En efecto: $a=Ad$ y $b=Bd \Rightarrow a,b \in (d) \Rightarrow I \subseteq (d)$

Pero por otra parte: $d = ma+nb$ (Bezout) $\Rightarrow d \in I \Rightarrow (d) \subseteq I$

Y lo mismo para polinomios:

$I=(a(x), b(x)) \subseteq K[X] \Rightarrow I=(d(x))$, $d(X) = mcd(a(x), b(x))$

$I=(15,6) \subseteq \mathbb{Z} \Rightarrow I=(3)$; $I=(X^2+X, X^2-X) \subseteq \mathbb{Q}[X] \Rightarrow I=(X)$.

Ejemplo 6. En el anterior ejemplo es importante que K sea un cuerpo:

- $I=(2,X)\subseteq \mathbb{Q}[X] \Rightarrow I=(1,X) \Rightarrow I=(1)=\mathbb{Q}[X]$
- $I=(2,X)\subseteq \mathbb{Z}[X] \Rightarrow I\neq(p(X)),\ \forall p(X)\in\mathbb{Z}[X]$

En efecto: $(2,X)=(p(X)) \Rightarrow \begin{cases} 2=q_1(X)p(X) \\ X=q_2(X)p(X) \end{cases} \Rightarrow \begin{cases} p(X)=\pm 2 \ (1) \\ p(X)=\pm 1 \ (2) \end{cases}$

(1) no puede ocurrir:

$X=q_2(X)2=(a_0+a_1X)2=2a_0+2a_1X$, con $a_1\in\mathbb{Z}$, es imposible

(2) tampoco puede ocurrir

$(2,X)=(\pm 1)=\mathbb{Z}[X] \Rightarrow 1=2a(X)+Xb(X) \Rightarrow$

$\Rightarrow 1=2(a_0+a_1X+\cdots)+X(b_0+b_1X+\cdots) \Rightarrow 1=2a_0$, con $a_0\in\mathbb{Z}$, es imposible

- El método de Euclides – como recordaréis – daba un método práctico para encontrar el generador.

$I=(270, 192)=(d)$, $d=\text{m.c.d}(270, 192)$

$270 \mid 192$, $78 \mid 1$ $\Rightarrow \begin{cases} 270 = 1\cdot 192 + 1\cdot 78 \\ 78 = 1\cdot 270 + (-1)\cdot 192 \end{cases} \Rightarrow (270, 192) = (192, 78)$

$192 \mid 78$, $36 \mid 2$ $\Rightarrow \begin{cases} 192 = 2\cdot 78 + 1\cdot 36 \\ 36 = 1\cdot 192 + (-2)\cdot 78 \end{cases} \Rightarrow (192, 78) = (78, 36)$

$78 \mid 36$, $6 \mid 2$ $\Rightarrow \begin{cases} 78 = 2\cdot 36 + 6 \\ 6 = 78 - 2\cdot 36 \end{cases} \Rightarrow (78, 36) = (36, 6) = (6) = I$

$p(x) = x^6 + 2x^5 + 2x^4 - 3x^3 - 9x^2 - 9x - 5$; $q(x) = x^4 - x^2 - 2x - 1$

$I = (p(x), q(x)) = (d(x))$ m.c.d.

$$x^6 + 2x^5 + 2x^4 - 3x^3 - 9x^2 - 9x - 5 \;\big|\; x^4 - x^2 - 2x - 1$$
$$-x^6 + x^4 + 2x^3 + x^2 \qquad\qquad x^2 + 2x + 3 = d(x)$$
$$2x^5 + 3x^4 - x^3 - 8x^2 - 9x - 5$$
$$-2x^5 + 2x^3 + 4x^2 + 2x$$
$$3x^4 + x^3 - 4x^2 - 7x - 5$$
$$-3x^4 + 3x^2 + 4x + 3$$
$$x^3 - x^2 - x - 2 = r_1(x)$$

$$x^4 - x^2 - 2x - 1 \;\big|\; x^3 - x^2 - x - 2$$
$$\vdots \qquad\qquad x + 1$$
$$x^2 + x + 1 = r_2(x)$$

$$x^3 - x^2 - x - 2 \;\big|\; x^2 + x + 1$$
$$0 \qquad\qquad x - 2$$

$\Rightarrow (p(x), q(x)) = (q(x), r_1(x)) = (r_1(x), r_2(x)) = (r_2(x), 0) = (r_2(x)) = (x^2 + x + 1)$

c.c. $\boxed{I = (p(x), q(x)) = (x^2 + x + 1)}$

ANILLOS COCIENTE

Di mismo modo que en las teorías de espacios vectoriales y de grupos teníamos el concepto de espacio vectorial cociente (de un espacio por un subespacio) y de grupo cociente (de un grupo por un subgrupo normal), en la teoría de anillos vamos a tener anillos cocientes (de un anillo por un ideal).

Definición. Sea I un ideal de un anillo conmutativo A. Definimos en A la siguiente relación binaria:

$$xRy \Leftrightarrow x-y \in I$$

→ no se involucra la 2ª oper.

Es fácil ver que esta relación es una relación de equivalencia:

1) Reflexiva: $x-x=0 \in I \Rightarrow xRx$

2) Simétrica: $xRy \Rightarrow x-y \in I \Rightarrow -(x-y) \in I$
$\Rightarrow y-x \in I \Rightarrow yRx$

3) Transitiva: $\left.\begin{matrix} xRy \\ yRz \end{matrix}\right\} \Rightarrow \left.\begin{matrix} x-y \in I \\ y-z \in I \end{matrix}\right\} \Rightarrow x-z \in I \Rightarrow xRz$

Denotaremos el conjunto cociente por A/I.

y sus elementos en la forma $\bar{x}$ = clase de x.

o también $x+I$ (pues $x+I=\{x+u / u \in I\}$ son todos los elementos que se relacionan con x, i.e. $\bar{x}=\overline{x+u} \Leftrightarrow u \in I$).

Ejemplo: Conocemos bien el caso en que $A=\mathbb{Z}$ y $I=(n)=n\mathbb{Z}$.

Sabemos que en este ejemplo

$$\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

y que $\mathbb{Z}/(n)$ hereda la estructura de anillo de $\mathbb{Z}$.

Esto va a ser cierto en general:

Operaciones $+$ y $\cdot$ en A/I

$+)$ $\bar{x}+\bar{y} = \overline{x+y}$

$\cdot)$ $\bar{x}\cdot\bar{y} = \overline{xy}$

Proposición. Con estas dos operaciones A/I adquiere la estructura de anillo conmutativo.

Prueba. Esto es muy fácil de comprobar. Por ejemplo, el elemento neutro respecto de $+$ es el $\bar{0}$ y respecto de $\cdot$ es el $\bar{1}$

pues $\overline{x}+\overline{0}=\overline{x+0}=\overline{x}$ y $\overline{x}\cdot\overline{1}=\overline{x\cdot 1}=\overline{x}$

De lo único que hay que preocuparse — como ocurre siempre — en las estructuras cociente es de que las operaciones estén bien definidas, i.e. tenemos que convencernos de que

$$\left.\begin{array}{l}\overline{x}=\overline{x'}\\ \overline{y}=\overline{y'}\end{array}\right\}\Rightarrow\begin{array}{l}\overline{x+y}=\overline{x'+y'}\\ \overline{x\cdot y}=\overline{x'\cdot y'}\end{array}$$

Comprobemos, por ejemplo, la segunda que es un poco más difícil:

$$\left.\begin{array}{l}\overline{x}=\overline{x'}\\ \overline{y}=\overline{y'}\end{array}\right\}\Rightarrow\left.\begin{array}{l}x'=x+u,\ u\in I\\ y'=y+v,\ v\in I\end{array}\right\}\Rightarrow x'y'-xy=(x+u)(y+v)-xy\Rightarrow$$

$$\Rightarrow x'y'-xy=\cancel{xy}+xv+yu+uv-\cancel{xy}\in I\Rightarrow\overline{x'y'}=\overline{xy}\quad \text{c.q.d}$$

($xv+yu+uv\in I$)

Ejemplo/Pregunta: ¿Cuántos elementos tiene el anillo $K[X]/(X)$? Tantos como el cuerpo K.

$\varphi: K\longrightarrow K[X]/(X)$, $\kappa\longmapsto\overline{\kappa}=\kappa+(X)$ es biyectiva

Inyectiva: $\varphi(\kappa_1)=\varphi(\kappa_2)\Rightarrow\overline{\kappa_1}=\overline{\kappa_2}\Rightarrow\kappa_1-\kappa_2\in(X)$
$\Rightarrow\kappa_1-\kappa_2=p(X)\cdot X\Rightarrow\kappa_1-\kappa_2=0\Rightarrow\kappa_1=\kappa_2$

Sobre: $\forall q(X)=a_0+a_1X+\dots+a_nX^n$; $a_i\in K$
$\overline{q(X)}=\overline{a_0}$, pues $q(X)-a_0=X(a_1+\dots+a_nX^{n-1})$

sobre: $a_0\xrightarrow{\varphi}\overline{q(X)}$

Otra pregunta para ayudar a entender por qué necesitamos comprobar que las operaciones en el cociente están bien definidas:

¿Por qué no hacemos el cociente de anillos por subanillos?

- ¿Es que si $A' \subset A$ es un subanillo de A la relación $x R y \Leftrightarrow x - y \in A'$ no es de equiv?

Sí es de equiv. La definición de R sólo involucra a la operación + y $(A', +) \trianglelefteq (A, +)$

- ¿Es que la operación + no estaría bien definida?

Sí, por la misma razón: $\left(\frac{A}{A'}, +\right)$ sería un grupo.

- ¿Es que la operación · no estaría bien definida?

(Probar con $\mathbb{Z} \subset \mathbb{Q}$, $x = 1/2$, $y = 1/3$, $x' = 1/2 + 2$, $y' = 1/3 + 3$)

Q/Z

$\bar{x} = \overline{x'}$ pues $x - x' = -2 \in \mathbb{Z}$
$\bar{y} = \overline{y'}$ " $y - y' = -3 \in \mathbb{Z}$

$\overline{xy} \overset{?}{=} \overline{x'y'} \Leftrightarrow x'y' - xy \overset{?}{\in} \mathbb{Z}$

$x'y' - xy = \left(\frac{1}{2} + 2\right)\left(\frac{1}{3} + 3\right) - \frac{1}{2} \cdot \frac{1}{3} =$

$= \frac{1}{6} + \frac{3}{2} + \frac{2}{3} + 6 - \frac{1}{6} \notin \mathbb{Z}$

Luego · no está bien def en $\mathbb{Q}/\mathbb{Z}$.

IDEALES PRIMOS Y MAXIMALES

Definición

Let R be a commutative ring. Let P be an ideal. We define P to be a **prime ideal** if $P \neq R$ and whenever $a, b \in R$ and $ab \in P$ then $a \in P$ or $b \in P$.

i.e. P es primo si $ab \in P \Rightarrow a \in P$ ó $b \in P$

Ejemplo 1 $(n) \subseteq \mathbb{Z}$ es un ideal primo $\Leftrightarrow$ $\Leftrightarrow$ n es un número primo o $n=0$.

Dem

$\Leftarrow$) Sea n primo. Entonces $ab \in (n) \Rightarrow ab = tn \Rightarrow$
$\Rightarrow n \mid ab \Rightarrow n \mid a$ ó $n \mid b \Rightarrow a \in (n)$ ó $b \in (n)$

$\Rightarrow$) (podemos suponer $n>0$, pues si no $-n>0$) Si $n = n_1 \cdot n_2$, con $n_i < n$ $(i=1,2)$ entonces $n_1 n_2 \in (n)$ pero $n_1 \notin (n)$ y $n_2 \notin (n)$.
$2 \notin (6)$ $3 \notin (6)$

-3 es primo
$-3 = u \cdot v \Rightarrow \begin{cases} u = \pm 1 \\ v = \pm 1 \end{cases}$

Ejemplo 2 . $(p(x)) \subseteq K[x]$ es un ideal primo $\Leftrightarrow$ $p(x)$ es irreducible ó $p(x)=0$.

Observación Un anillo A es un dominio $\Leftrightarrow$ (0) es un ideal primo

Definición

Let R be a commutative ring. Let M be an ideal. We define M to be **maximal ideal** if $M \neq R$ and if there is no ideal J such that $R \supset J \supset M$ and $R \neq J$, $J \neq M$.

Ejemplo 4. Todos los ideales primos no nulos de $\mathbb{Z}$ son maximales. Lo mismo vale para $K[x]$.

(Claro: $(3) \subsetneq (n)$ $\forall n \neq 1$, pero $n=1$ no cuenta porque es todo $\mathbb{Z}$!)

Proposición

a) maximal $\Rightarrow$ primo

b) P es primo $\Leftrightarrow R/P$ es un dominio

c) M es maximal $\Leftrightarrow R/M$ es un cuerpo.

Demostración. ($\bar{x} = x+P$)

b) $\Rightarrow$) $(x+P)(y+P) = 0+P \Leftrightarrow xy \in P \Rightarrow x \in P$ ó $y \in P$

$\Rightarrow x+P = \bar{0}$ ó $y+P = \bar{0}$.

$\Leftarrow$) $xy \in P \Rightarrow (x+P)(y+P) = xy+P = 0+P \Rightarrow$

$\Rightarrow x+P = 0+P$ ó $y+P = 0+P \Rightarrow x \in P$ ó $y \in P$.

c) $\Rightarrow$) $x+M \neq 0+M \Rightarrow x \notin M \Rightarrow M + (x) = R \Rightarrow$

($M \subsetneq M+(x)$ ideal; $0+1\cdot x = x$; I, J ideales $\Rightarrow I+J, I\cap J$ ideales)

$\Rightarrow 1 = m + ax$, para algún $a \in R \Rightarrow$

$\Rightarrow \bar{1} = \bar{m} + \bar{a}\cdot\bar{x} \Rightarrow \bar{a} = (\bar{x})^{-1}$ c.q.d.

($1+M = m+M + (a+M)(x+M)$)

$\Leftarrow$) Supongamos $M \subsetneq J \subset R$, (J un ideal de R)

$\Rightarrow \exists x \in J \setminus M \Rightarrow x+M \neq 0+M \Rightarrow \exists y+M$ tal que

$1+M = (x+M)(y+M) = xy+M \Rightarrow 1 = \underbrace{xy}_{J} + \underbrace{m}_{J}$, para algún $m \in M$ ($m \in M \subset J$)

($1-xy \in M \Rightarrow 1-xy = m \in M$)

$\Rightarrow 1 \in J \Rightarrow J = R$ c.q.d.

a) I maximal $\overset{a)}{\Rightarrow} A/I$ es un cuerpo $\Rightarrow A/I$ es un dominio

$\overset{b)}{\Rightarrow} I$ es primo.

Ejemplo 5. $\mathbb{Z}/(n)$ es un cuerpo $\Leftrightarrow$ n es primo

(como ya sabíamos)

Ejemplo 6 $\dfrac{\mathbb{F}_2[X]}{(X^2+X+1)}$ $(\mathbb{F}_2 = \mathbb{Z}/(2))$ es un cuerpo con **4 elementos**.

Por el Ejemplo 2 para ver que es un cuerpo es suficiente con probar que el polinomio es irreducible.

Y para ello (puesto que su grado es ≤ 3) basta ver que no tiene raíces, y efectivamente ni $\bar{0}$ ni $\bar{1}$ son raíces. Luego es un cuerpo.

¿Y cuántos elementos tiene? 4. A saber:

$0, 1, X, 1+X$ (los de grado ≤ 1) $\rightarrow \overline{x^2+x+1} = \bar{0}$

Y no hay más, porque $X^2 = -1-X = 1+X$,

$X^3 = X \cdot X^2 = X(1+X) = X + X^2 = X + 1 + X = \underline{1}$ etc.

luego el inverso de X es $(1+X)$.

OJO: No confundir el cuerpo con 4 elementos con $\mathbb{Z}/4\mathbb{Z}$, que no es un cuerpo.