Propiedades básicas y campos

Facultad de Ciencias UNAM

Introducción

En esta sección haremos 3 cosas:

1. Demostramos algunas reglas aritméticas básicas en anillos. Como veras, la aritmética en un anillo arbitrario es *muy* similar a la aritmética que ya conoces.
2. Calculamos el grado de la suma, multiplicación, y composición de polinomios. Es importante recalcar que las igualdades que daremos para la multiplicación y composición requieren que los polinomios tengan coeficientes en un dominio.
3. Introducimos la clase especial de anillo más fuerte hasta el momento[1]

Cabe recalcar que no hay ninguna relación directa entre estas 3 cosas pero usaremos cada una de ellas y las teníamos que escribir en algún lugar.

[1] De hecho, en la segunda mitad del curso, nos dedicamos a estudiar esta clase especial de anillo.

Unicidad de los inversos aditivos/multiplicativos

Proposición 1

1. Si R es un anillo arbitrario, entonces los inversos aditivos son únicos.
2. Si R es un anillo con 1, entonces los inversos multiplicativos son únicos.

Demostración.

1. Supongamos que $a \in R$ y que $b, b' \in R$ son inversos multiplicativos de a. Entonces

$$b' = b + 0 = b + (a + b') = (b + a) + b' = 0 + b' = b'$$

2. Es análoga al inciso anterior pero suponiendo que $a \in R$ es invertible.

$\square$

Esto justifica nuestra notación "$-a$" y "a^{-1}".

Multiplicar por el 0

Proposición 2

Supongamos que R es un anillo. Si $a, b \in R$, entonces

$$a0 = 0 = 0a.$$

Demostración. Como $0 = 0 + 0$, multiplicando $a \in R$ por la izquierda obtenemos

$$a0 = a(0 + 0) = a0 + a0$$

donde la ultima igualdad es consecuencia de la ley distributiva izquierda. Restando por $a0$, obtenemos $0 = a0$. La otra igualdad se obtiene análogamente multiplicando $a \in R$ por la derecha y usando la ley distributiva derecha. $\square$

Multiplicar por inversos aditivos

Proposición 3

Supongamos que R es un anillo. Si $a, b \in R$, entonces

1. $a(-b) = (-a)b = -(ab)$.
2. $(-a)(-b) = ab$.

Demostración.

1. Para todo $a, b \in R$ tenemos

$$ab + a(-b) = a\left(b + (-b)\right) = a0 = 0.$$

   Sumando $-(ab)$ de ambos lados obtenemos $a(-b) = -(ab)$.
   Análogamente, $(-a)b = -(ab)$.

2. Por el inciso anterior, para toda $a, b \in R$

$$(-a)(-b) = -\left((-a)b\right) = -\left(-(ab)\right) = ab$$

   La ultima igualdad se cumple porque ab es el inverso aditivo de $-(ab)$.

$\square$

El cuadrado de una suma

Proposición 4

Supongamos que R es un anillo. Si $a, b \in R$, entonces

$$(a+b)^2 = a^2 + ba + ab + b^2.$$

Demostración. Por la ley distributiva derecha, tenemos que para todo $a, b \in R$,

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= (a+b)a + (a+b)b\\ &= a^2 + ba + ab + b^2\end{aligned}$$

$\square$

$(na)(mb) = (nm)(ab)$ para todo $n, m \in \mathbb{Z}$

Proposición 5

Supongamos que R es un anillo. Si $a, b \in R$, entonces

$$(na)(mb) = (nm)(ab)$$

para todo $n, m \in \mathbb{Z}$.

Demostración. Por definición,

$$(na)(mb) = (\underbrace{a + \cdots + a}_{n-\text{veces}})(\underbrace{b + \cdots + b}_{m-\text{veces}}) = \underbrace{a(\underbrace{b + \cdots + b}_{m-\text{veces}}) + \cdots + a(\underbrace{b + \cdots + b}_{m-\text{veces}})}_{n-\text{veces}}$$

$$= \underbrace{(\underbrace{ab + \cdots + ab}_{m-\text{veces}}) + \cdots + (\underbrace{ab + \cdots + ab}_{m-\text{veces}})}_{n-\text{veces}} = (\underbrace{ab + \cdots + ab}_{nm-\text{veces}}) = (nm)(ab).$$

$\square$

Comentario

En lo que sigue, calculamos el grado de la suma, multiplicación, y composición de polinomios. De nuevo, recuerda que las igualdades que daremos para la multiplicación y composición requieren que los polinomios tengan coeficientes en un dominio.

El grado de la suma de dos polinomios

Proposición 6

Supongamos que R es un anillo. Si $p(x), q(x) \in R[x]$, entonces

$$\deg\big(p(x)+q(x)\big) \leq \text{máx}\left\{\deg p(x), \deg q(x)\right\}.$$

Demostración. Supongamos que $p(x), q(x) \in R[x]$ son tales que

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad \text{y} \quad q(x) = \sum_{j=0}^{m} b_j x^j$$

con $a_n \neq 0$ y $b_m \neq 0$.

Caso 1. $n = m$.
Entonces

$$p(x) + q(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

Caso 1.1. $a_n = -b_n$.
Entonces

$$p(x) + q(x) = (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

y por lo tanto,

$$\deg\big(p(x) + q(x)\big) \le n - 1 < n = \max\left\{\deg p(x), \deg q(x)\right\}.$$

Caso 1.2. $a_n \neq -b_n$.
Entonces $a_n + b_n$ es el coeficiente delantero de $p(x) + q(x)$ y por lo tanto,

$$\deg\big(p(x) + q(x)\big) = \deg p(x) = \deg q(x) = \max\{\deg p(x), \deg q(x)\}.$$

Caso 2. $n \neq m$. Sin perdida de generalidad, supongamos que $n > m$. Entonces

$$p(x) + q(x) = \sum_{i=m+1}^{n} a_i x^i + \sum_{i=0}^{m} (a_i + b_i)\, x^i$$

y por lo tanto,

$$\deg\big(p(x) + q(x)\big) = \deg p(x) = \max\{\deg p(x), \deg q(x)\}$$

donde la ultima igualdad se cumple porque $\deg p(x) = n > m = \deg q(x)$.

$\square$

En particular, acabamos de demostrar que el *único* caso en que la igualdad

$$\deg\big(p(x) + q(x)\big) = \max\big\{\deg p(x), \deg q(x)\big\}$$

no se satisface, es cuando $\deg p(x) = \deg q(x)$ y los coeficientes delanteros de $p(x)$ y $q(x)$ son inversos aditivos.

El grado del producto de dos polinomios en un dominio

Proposición 7

Supongamos que R es un dominio. Si $p(x), q(x) \in R[x]$, entonces

$$\deg\big(p(x) \cdot q(x)\big) = \deg p(x) + \deg q(x).$$

Mas aun, si R es un dominio con 1, entonces

$$p(x) \in R[x] \text{ es invertible en } R[x] \iff \\ p(x) = u \text{ para alguna } u \in R \text{ invertible.}$$

En particular, $(R[x])^\times = R^\times$.

Demostración. Supongamos que $p(x), q(x) \in R[x]$ son tales que

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad \text{y} \quad q(x) = \sum_{j=0}^{m} b_j x^j$$

con $a_n \neq 0$ y $b_m \neq 0$.

Entonces el coeficiente delantero de $p(x) \cdot q(x)$ es $a_n b_m x^{n+m}$ (recuerda que como R es dominio, entonces $a_n \neq 0$ y $b_m \neq 0$ implica $a_n b_m \neq 0$).

Por lo tanto,

$$\deg \big(p(x) \cdot q(x)\big) = n + m = \deg p(x) + \deg q(x).$$

Por otro lado, supongamos que R es un dominio con 1. La equivalencia

$$\begin{aligned} p(x) \in R[x] \text{ es invertible en } R[x] \iff \\ p(x) = u \text{ para alguna } u \in R \text{ invertible}, \end{aligned}$$

es consecuencia inmediata de la igualdad anterior y la definición $\deg p(x) = 0$ si y solo si $p(x)$ es un polinomio constante no cero. $\square$

El grado de la composición de dos polinomios en un dominio

Proposición 8

Supongamos que R es un dominio. Si $p(x), q(x) \in R[x]$, entonces

$$\deg\big(p(q(x))\big) = \deg p(x) \cdot \deg q(x).$$

Demostración. Usando las igualdades para el grado de la suma y el producto de polinomios, obtenemos la siguiente cadena de igualdades.

$$
\begin{aligned}
\deg p(q(x)) &= \deg \sum_{i=0}^{n} \left\{ a_i \left(\sum_{j=0}^{m} b_j x^j \right)^i \right\} \\
&= \max_{i=0}^{n} \left\{ \deg a_i \left(\sum_{j=0}^{m} b_j x^j \right)^i \right\} \\
&= \max_{i=0}^{n} \left\{ \cancelto{1}{\deg a_i} \cdot \deg \left(\sum_{j=0}^{m} b_j x^j \right)^i \right\} \\
&= \max_{i=0}^{n} \left\{ i \cdot \cancelto{m}{\deg \left(\sum_{j=0}^{m} b_j x^j \right)} \right\} \\
&= \max_{i=0}^{n} \{ i \cdot m \} = n \cdot m.
\end{aligned}
$$

$\square$

Mas propiedades básicas de polinomios sobre dominios

Proposición 9

Si R es un anillo, entonces

- $R[x]$ es un dominio si y solo si R es un dominio.
- $R[x]$ es un domino entero si y solo si $R[x]$ es un domino entero.

Demostración.

1. $\Longrightarrow$) Como $R \subset R[x]$ y todo subanillo de un dominio es un dominio, entonces R es un dominio.

   $\Longleftarrow$) Supongamos que $p(x), q(x) \in R[x]$ son distintos de 0. Si tienen coeficientes delanteros $a, b \in R \setminus \{0\}$ respectivamente, entonces el coeficiente delantero de $p(x)q(x)$ es[2] $ab \neq 0$. En particular, $p(x)q(x) \neq 0$.
2. Es consecuencia inmediata del inciso anterior y de la equivalencia

$$R \text{ es conmutativo} \iff R[x] \text{ es conmutativo.}$$

$\square$

[2] Recuerda que la hipotesis "R es un dominio" es necesaria para que esto sea cierto: en este caso, $a \neq 0$ y $b \neq 0$ implica $ab \neq 0$.

Comentario

Terminamos esta sección introduciendo el concepto de campo.

Definición

Un **campo** es un anillo conmutativo con división.

En otras palabras, $(R, +, \times)$ es un campo si (i) $(R, +)$ y $(R - \{0\}, \times)$ son grupos abelianos y (ii) se satisfacen las leyes de distributividad.

Hasta este momento, los únicos campos que conocemos son $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, y $\mathbb{Z}_p$ cuando p es primo. El único otro anillo con división que conocemos son los cuaterniones pero estos no son conmutativos.

En la sección anterior, demostramos que "dominio finito con 1 $\implies$ anillo con división". Por lo tanto (agregando conmutatividad a la hipótesis), tenemos que dominio entero finito con 1 $\implies$ campo (finito).

Campos y subanillos

Definición

Supongamos que F es un campo y que $S \subset F$ es un subconjunto de F. Decimos que S es un *subcampo* de F si S es un campo con las mismas operaciones que F (pero restringidas a S). Es fácil verificar que esto es equivalente a que

$$\forall a, b \in S \left(a - b \in S \quad \text{y} \quad ab^{-1} \in S \right).$$

Cabe recalcar que los conceptos subanillo y subcampo *no son equivalentes*. Por ejemplo, $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$ que no es un subcampo.