

Notas de Álgebra Moderna III:  
Una Introducción a la Teoría de Galois Finita

Cristo Daniel Alvarado

27 de mayo de 2024

# Índice general

1. Anillo de Polinomios	2
1.1. Series de Potencias . . . . .	2

# Capítulo 1

## Anillo de Polinomios

### 1.1. Series de Potencias

#### Definición 1.1.1

Sea  $A$  un anillo. Denotemos por

$$S_A = \left\{ f \mid f : \mathbb{N} \cup \{0\} \rightarrow A \right\}$$

es decir que  $S_A$  es el **conjunto de sucesiones de  $A$** . Si  $f \in S_A$  escribimos a  $f$  como:

$$f = (a_0, a_1, \dots)$$

Sobre  $S_A$  se definen dos operaciones, la **suma** y **producto**. A saber, si  $f = (a_0, a_1, \dots)$  y  $g = (b_0, b_1, \dots)$ , entonces:

$$f + g = (a_0 + b_0, a_1 + b_1, \dots, a_k + b_k, \dots)$$

y,

$$fg = f \cdot g = (c_0, c_1, \dots, c_k, \dots)$$

donde

$$\begin{aligned} c_k &= \sum_{i=0}^k a_i b_{k-i} \\ &= a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0 \\ &= \sum_{i=0}^k a_{k-i} b_i \\ &= \sum_{i+j=k} a_i b_j \end{aligned}$$

#### Observación 1.1.1

En la definición anterior, se tiene que  $S_A$  es un anillo con cero el elemento  $(0, 0, \dots, 0, \dots)$  e inverso  $-f = (-a_0, -a_1, \dots, -a_k, \dots)$  para todo  $f \in S_A$ . Además, existe un monomorfismo de  $A$  en  $S_A$ , a saber:

$$A \hookrightarrow S_A, a \mapsto (a, 0, \dots, 0, \dots)$$

Por lo cual  $A$  está encajado en  $S_A$ . Debido a esto, se denotará de ahora en adelante como

$$a = (a, 0, \dots, 0, \dots), \quad \forall a \in A$$

**Definición 1.1.2**

Sean  $A$  y  $X$  un objeto tal que  $X \notin A$ .  $X$  es llamado una **indeterminada para  $A$** . Definimos para todo  $n \in \mathbb{N} \cup \{0\}$  y para todo  $a \in A$ :

$$aX^n = (\underbrace{0, 0, 0, \dots, 0, 0, 0, a, 0, \dots}_{n+1\text{-ésima entrada}})$$

Si  $A$  tiene identidad, entonces

$$1X^n = X^n = (\underbrace{0, 0, 0, \dots, 0, 0, 0, 1, 0, \dots}_{n+1\text{-ésima entrada}})$$

En caso que  $n = 1$ ,  $1X^1 = X^1 = x$  y si  $n = 0$ ,  $1X^0 = X^0 = 1$  (abusando en este caso de la notación). Se tiene entonces que

$$X^n \in S_A, \quad \forall n \in \mathbb{N} \cup \{0\}$$

Ahora, independientemente de si  $A$  tiene o no identidad, tenemos que:

$$\begin{aligned} (a_0, a_1, a_2, \dots, a_k, \dots) &= (a_0, 0, 0, \dots) \\ &\quad + (0, a_1, 0, \dots) \\ &\quad + (0, 0, a_2, \dots) \\ &\quad + (0, 0, \dots, a_k, \dots) \\ &\quad + \dots \\ &= a_0X^0 + a_1X + a_2X^2 + \dots \end{aligned}$$

Por lo tanto, si  $f = (a_0, a_1, a_2, \dots, a_k, \dots)$ , entonces:

$$\begin{aligned} f &= \sum_{i=0}^{\infty} a_i X^i \\ &= a_0 + a_1X + a_2X^2 + \dots + a_kX^k + \dots \end{aligned}$$

así pues, podemos decir que una serie es una expresión algebraica de la forma:

$$f = \sum_{i=0}^{\infty} a_i X^i = a_0 + a_1X + a_2X^2 + \dots + a_kX^k + \dots \quad (1.1)$$

donde  $a_0 := a_0X^0$ .

Si  $f = \sum_{n=0}^{\infty} a_n X^n$  y  $g = \sum_{n=0}^{\infty} b_n X^n$ , entonces:

$$\begin{aligned} f + g &= \sum_{n=0}^{\infty} (a_n + b_n) X^n \\ f \cdot g &= \sum_{n=0}^{\infty} c_n X^n \end{aligned}$$

siendo  $c_n = \sum_{k=0}^n a_k b_{n-k}$  para todo  $n \in \mathbb{Z}_{\geq 0}$ . Con estas operaciones  $S_A$  es un anillo, cambiándose el símbolo por  $A[[X]]$ , en este caso  $A[[X]]$  es llamado **anillo de series de potencias con coeficientes en  $A$  en la indeterminada  $X$** .

Si  $f = \sum_{n=0}^{\infty} a_n X^n \in A[[X]]$ , los elementos  $a_0, a_1, \dots \in A$  son llamados **coeficientes o términos de la serie  $f$** . En particular,  $a_0$  es llamado **coeficiente constante** o **coeficiente líder de la serie  $f$** . El cero de  $A[[X]]$  es la serie **serie cero** dada por:

$$0 = \sum_{n=0}^{\infty} a_n X^n, \quad a_n = 0 \quad \forall n \in \mathbb{Z}_{\geq 0}$$

### Observación 1.1.2

Una serie de potencias  $f \in A[[X]]$  cumple que  $f = 0$  si y sólo si  $a_n = 0$  para todo  $a_n = 0, \forall n \in \mathbb{Z}_{\geq 0}$ .

En el caso de que  $f$  tenga coeficientes cero, éstos no se expresan dentro de  $f$ , es decir que no se expresan dentro de la sumatoria de tipo  $f = a_0 + a_1 X + \dots$ .

### Observación 1.1.3

En el caso de que el anillo  $A$  tenga identidad,  $A[[X]]$  también lo tiene y es la identidad de  $A$ , a saber:

$$1 = 1 + 0X + 0X^2 + \dots$$

En tal caso,  $1X^n = X^n$  para todo  $n \in \mathbb{N}$ .

### Observación 1.1.4

Si  $n, m \in \mathbb{Z}_{\geq 0}$ , entonces  $X^n, X^m \in A[[X]]$  y,

$$X^n \cdot X^m = X^{n+m} \in A[[X]]$$

### Observación 1.1.5

Si  $A$  es un anillo conmutativo, entonces  $A[[X]]$  también lo es (se verifica de forma inmediata de la definición de producto en  $A[[X]]$ ).

### Definición 1.1.3

Sea  $A$  un anillo. Para cada serie  $f = \sum_{n=0}^{\infty} a_n X^n \neq 0$  en  $A[[X]]$  se define el **orden de  $f$** , denotado por  $\text{ord}(f)$  como el mínimo entero no negativo  $m$  tal que  $a_m \neq 0$ . Así, si  $f$  es una serie de potencias no cero, entonces:

$$f = \sum_{n=\text{ord}(f)}^{\infty} a_n X^n$$

### Ejercicio 1.1.1

Sea  $A$  un anillo con 1. Si  $f = \sum_{n=0}^{\infty} a_n X^n \in A[[X]]$ , entonces existe  $g = \sum_{n=0}^{\infty} b_n X^n$  tal que  $\text{ord}(g) = 0$  y,

$$f = x^{\text{ord}(f)} g$$

### Demostración:

Ejercicio. ■

### Proposición 1.1.1

Sea  $A$  anillo y  $f = \sum_{n=0}^{\infty} a_n X^n$  y  $\sum_{n=0}^{\infty} b_n X^n$  dos series de potencias no cero en  $A[[X]]$ . Entonces:

1.  $f + g = 0$  ó  $\text{ord}(f + g) \geq \min\{\text{ord}(f), \text{ord}(g)\}$ .

2.  $fg = 0$  ó  $\text{ord}(fg) \geq \text{ord}(f) + \text{ord}(g)$ .

---

**Demostración:**

Ejercicio. ■

---

**Proposición 1.1.2**

Sean  $A$  anillo conmutativo con 1 y  $f = \sum_{n=0}^{\infty} a_n X^n \in A[[X]]$  una serie de potencias no cero. Entonces  $f$  es unidad de  $A[[X]]$  (esto es, elemento invertible de  $A[[X]]$ ) si y sólo si  $a_0$  (el término constante de  $f$ ) es unidad de  $A$ .

---

**Demostración:**

Pendiente. ■

---

**Corolario 1.1.1**

Si  $K$  es campo, entonces  $f = \sum_{n=0}^{\infty} a_n X^n$  en  $K[[X]] \setminus \{0\}$  es unidad si y sólo si  $a_0 \neq 0$ .

---

**Demostración:**

Es inmediata de la proposición anterior y del hecho que las unidades de  $K$  son  $K \setminus \{0\}$ . ■

---

**Corolario 1.1.2**

Si  $K$  es campo y  $f = \sum_{n=0}^{\infty} a_n X^n \in K[[X]] \setminus \{0\}$ , entonces existe una única serie de potencias  $g \in K[[X]]$  invertible tal que  $f = x^{\text{ord}(f)} g$ .

---

**Ejemplo 1.1.1**

Considere en  $\mathbb{R}[[X]]$  la serie de potencias  $f = 1 + X + X^2 + \dots = \sum_{n=0}^{\infty} X^n$ . Se tiene que  $f$  es invertible y su inversa es  $1 - x \in \mathbb{R}[[X]]$ .

**Demostración:**

Ejercicio. ■