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

Cristo Daniel Alvarado

17 de julio de 2024

Índice general

Capítulo 1

Anillo de Polinomios

1.1. Series de Potencias

Definición 1.1.1
Sea A un anillo. Denotemos por

$$S_A = \left\{ f \middle| f : \mathbb{N} \cup \{0\} \to A \right\}$$

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

$$f = (a_0, a_1, ...)$$

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

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

y,

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

donde

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

Observación 1.1.1
En la definición anterior, se tiene que S_A es un anillo con cero el elemento $(0, 0, ..., 0, ...)$ e inverso $-f = (-a_0, -a_1, ..., -a_k, ...)$ para todo $f \in S_A$. Además, existe un monomorfismo de A en S_A, a saber:

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

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

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

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 $a \in A$:

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

Si A tiene identidad, entonces

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

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:

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

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

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

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

$$f = \sum_{i=0}^{\infty} a_iX^i = a_0 + a_1X + a_2X^2 + ... + a_kX^k + ... \tag{1.1}$$

donde $a_0 := a_0X^0$.

Si $f = \sum_{n=0}^{\infty} a_nX^n$ y $g = \sum_{n=0}^{\infty} b_nX^n$, entonces:

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

siendo $c_n = \sum_{k=0}^{n} a_kb_{n-k}$ 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 $f=\sum_{n=0}^{\infty} a_nX^n \in A[[X]]$, los elementos $a_0, a_1, ... \in A$ son llamados **coeficientes o términos de la serie** f. En particular, a_0 es llamado **coeficiente constante** o **coeficiente lider de la serie** f. El cero de $A[[X]]$ es la serie **serie cero** dada por:

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

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 $f = a_0 + a_1X + ...$

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:

$$1 = 1 + 0X + 0X^2 + ...$$

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

$$f=\sum_{n=\operatorname{ord}(f)}^{\infty} a_nX^n$$

Ejercicio 1.1.1
Sea A un anillo con 1. Si $f=\sum_{n=0}^{\infty} a_nX^n \in A[[X]]$, entonces existe $g=\sum_{n=0}^{\infty} b_nX^n$ tal que $\operatorname{ord}(g) = 0$ y,

$$f = X^{\operatorname{ord}(f)}g$$

Demostración:
Se tienen dos casos:

- $\operatorname{ord}(f) = 0$, en cuyo caso basta tomar $g = f$, con lo que se obtiene que

$$f = X^0 f = f$$

- Suponga que $\text{ord}\,(f) > 0$. Para cada $m \in \mathbb{N} \cup \{0\}$ se define

$$b_m = a_{m+\text{ord}(f)}$$

(siendo $f = a_0 + a_1 X + a_2 X^2 + ... = \sum_{n=0}^{\infty} a_n X^n$). Tomemos así

$$g = \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} a_{n+\text{ord}(f)} X^n$$

como $a_{\text{ord}(f)} \neq 0$, entonces $\text{ord}\,(g) = 0$ ya que $b_0 = a_{\text{ord}(f)} \neq 0$. Además, se cumple que

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

■

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

Demostración:
De (1): Suponga que $f + g \neq 0$, tomemos $h = f + g$ y tomemos $m = \text{ord}\,(h)$. Se tienen tres casos:

- $\text{ord}\,(f) > \text{ord}\,(g)$, en tal caso se tiene que $\text{ord}\,(h) = \text{ord}\,(g) = \text{mín}\,\{\text{ord}\,(f)\,, \text{ord}\,(g)\}$.
- $\text{ord}\,(f) < \text{ord}\,(g)$, el caso es análogo al anterior.
- $k = \text{ord}\,(f) = \text{ord}\,(g)$, se tienen dos casos:
  - $a_k + b_k = 0$, se sigue pues que como $h \neq 0$, entonces $\text{ord}\,(h) > \text{ord}\,(f)\,, \text{ord}\,(g) = k = \text{mín}\,\{\text{ord}\,(f)\,, \text{ord}\,(g)\}$.
  - $a_k + b_k \neq 0$, de donde se sigue de forma inmediata que $\text{ord}\,(h) = k = \text{mín}\,\{\text{ord}\,(f)\,, \text{ord}\,(g)\}$.

por los incisos anteriores se sigue que $\text{ord}\,(f+h) \geq \text{mín}\,\{\text{ord}\,(f)\,, \text{ord}\,(g)\}$.

De (2): Es similar a (1). ■

Corolario 1.1.1
En las condiciones de la proposición anterior, si A es dominio entero, entonces $\text{ord}\,(fg) = \text{ord}\,(f) + \text{ord}\,(g)$. En particular, $fg \neq 0$ y $A[[X]]$ es dominio entero.

Demostración:
Suponga que A es dominio entero. Sean $f, g \in A[[X]]$ como en la proposición anterior tales que $f, g \neq 0$. De una proposición anterior se sabe que existen $f_1, g_1 \in A[[X]]$ tales que

$$f = X^{\text{ord}(f)} f_1 \quad \text{y} \quad g = X^{\text{ord}(g)} g_1$$

con $\text{ord}\,(f_1) = \text{ord}\,(g_1) = 0$. En particular se tiene que $a_{\text{ord}(f)} \neq 0$ y $b_{\text{ord}(g)} \neq 0$, luego

$$\begin{aligned} fg &= (a_{\text{ord}(f)} X^{\text{ord}(f)} + \ldots) \cdot (b_{\text{ord}(g)} X^{\text{ord}(g)}) \\ &= a_{\text{ord}(f)} b_{\text{ord}(g)} X^{\text{ord}(f)+\text{ord}(g)} + \ldots \end{aligned}$$

donde, al ser A dominio entero, sucede que $a_{\text{ord}(f)} b_{\text{ord}(g)} \neq 0$, luego $fg \neq 0$, en particular se tiene que $\text{ord}\,(fg) = \text{ord}\,(f) + \text{ord}\,(g)$. Por ende, $A[[X]]$ es dominio entero. $\blacksquare$

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:
$\Rightarrow$): Suponga que f es unidad de $A[[X]]$, entonces existe $g \in A[[X]]$ tal que

$$fg = 1$$

en particular, se tiene que si $f = \sum_{n=0}^{\infty} a_n X^n$ y $g = \sum_{n=0}^{\infty} b_n X^n$, entonces $a_0 b_0 = 1$, por tanto $a_0 \in A^*$.

$\Leftarrow$): Suponga que $a_0 \in A^*$, entonces existe $b_0 \in A^*$ tal que

$$a_0 b_0 = 1$$

$\blacksquare$

Corolario 1.1.2
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 $K \setminus \{0\}$. $\blacksquare$

Corolario 1.1.3
Si K es campo y $f = \sum_{n=0}^{\infty} a_n X^n \in K[[X]] \setminus \{0\}$, entonce 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 $f = 1 + X + X^2 + \ldots = \sum_{n=0}^{\infty} X^n$. Se tiene que f es invertible y su inversa es $1 - x \in \mathbb{R}[[X]]$.

Demostración:
Ejercicio. $\blacksquare$