$g(X) = \sum_{i\in\mathbb{N}_{>0}} b_i X^i$, allora l'espressione

$$f(g(X)) = a_0 + a_1 g(X) + a_2 g(X)^2 + \cdots + a_i g(X)^i + \cdots$$

dà una serie formale, poiché per determinare il coefficiente di X^i è necessario solo un numero finito di operazioni tra coefficienti delle due serie date (si noti che questo sarebbe falso se l'ordine di $g(X)$ fosse nullo) per ogni i, e quindi definisce univocamente una serie formale.

Allo stesso modo, oppure passando ai quozienti, possiamo definire la sostituzione di una serie d'ordine positivo in una serie di Laurent.

0.5.1. Associatività della sostituzione. Se indichiamo con $f \circ g(X) = f(g(X))$ il risultato della sostituzione di $g(X)$ in $f(X)$, allora $f \circ (g \circ h)(X) = (f \circ g) \circ h(X)$.

0.5.2. Inversi per sostituzione. *Sia $f(X) \in K[\![X]\!]$ e $\mathrm{ord}_X f(X) = 1$. Allora esiste una unica $g(X) \in K[\![X]\!]$, necessariamente con $\mathrm{ord}_X g(X) = 1$, tale che $f(g(X)) = X$ (come serie formale). Inoltre anche $g(f(X)) = X$.*

L'esistenza e l'unicità seguono insieme e facilmente per induzione, scrivendo il sistema infinito di equazioni che determinano i coefficienti della serie cercata $g(X)$: da $\sum_{i=1}^{\infty} a_i g(X)^i = X$ otteniamo

$$\begin{cases} a_1 b_1 = 1 \\ a_1 b_2 + a_2 b_1^2 = 0 \\ a_1 b_3 + 2a_2 b_1 b_2 + a_3 b_1^3 = 0 \\ \cdots \\ a_1 b_i + \displaystyle\sum_{i=2}^{i} a_i c_i(\underline{b}) = 0 \qquad \text{ove} \quad c_i(\underline{b}) \in \mathbb{Z}[b_1, \ldots, b_{i-1}] \\ \cdots \end{cases}$$

ad ogni passo, b_i compare come incognita lineare in una espressione in cui compaiono solo $b_1, \ldots, b_{i-1}$, note dai passi precedenti.

Per mostrare l'ultima affermazione, basta osservare che da $f(g(X)) = X$ segue $g(f(g(X))) = g(X)$ e che sostituendo ad X l'unica $h(X)$ tale che $g(h(X)) = X$ otteniamo $g(f(X)) = g(f(g(h(X)))) = g(h(X)) = X$, e per l'unicità concludiamo che $f(X) = h(X)$.

Per esempio è ben noto che le serie $e(X) = \exp(X) - 1 = \sum_{i=1}^{\infty} X^i/i!$ è inversa per composizione della serie $l(X) = \log(1+X) = \sum_{i=1}^{\infty} (-)^{i-1} X^i/i$. Similmente, l'inversa per composizione di $(1+X)^n - 1$ è la serie $(1+X)^{1/n} - 1$. Chi sono gli inversi per composizione di $\sum_{i>0} X^i$, di $\cos(x)$ e di $\sin(X) - 1$?

0.5.3. Automorfismi e sostituzioni d'ordine uno. *È chiaro che ogni $g(X)$ d'ordine 1 determina una sostituzione d'ordine 1 e quindi un automorfismo (di K-algebra) di $K[\![X]\!]$. Viceversa ogni tale automorfismo è dato da una sostituzione d'ordine 1 per un ben determinato $g(X)$.*

Si osservi però che il risultato non è proprio banale: certamente, se $\varphi : K[\![X]\!] \to K[\![X]\!]$ è l'automorfismo dato, la serie $g(X)$ candidata è l'immagine di X tramite φ; è chiaro che per ogni polinomio $p(X)$ si avrà $\varphi(P(X)) = P(\varphi(X))$ (per ipotesi φ è morfismo di K-algebre), ma bisogna estendere il risultato alle serie arbitrarie, e questo si ottiene con considerazioni topologiche (un automorfismo di algebre di $K[\![X]\!]$ è continuo per la topologia indotta dalla ultrametrica X-adica, e quindi è determinato dal valore su ogni sottinsieme denso come è $K[X]$).

0.6. Teorema (Lemma di Hensel di rialzamento degli zeri). *Sia $f(X,Y) \in K[\![X]\!][Y]$ (polinomio in Y a coefficienti in $K[\![X]\!]$), e supponiamo che $f(0,Y) \in K[Y]$ ammetta uno zero $y \in K$ tale che ($f(0,y) = 0$ e) $f'(0,y) \neq 0$ (derivata rispetto a Y). Allora esiste $y(X) \in K[\![X]\!]$ tale che $f(X, y(X)) = 0$ e $y(0) = y$. Cioè ogni zero $y \in K$ di $f(0,Y) \in K[Y]$ che non annulli la derivata si rialza ad uno zero $y(X) \in K[\![X]\!]$ di $f(X,Y) \in K[\![X]\!][Y]$.*

Dimostrazione. Procediamo alla costruzione di $y(X) = \sum_i a_i X^i$ per induzione sull'indice i, con un procedimento simile al metodo delle tangenti di Newton. Vogliamo costruire una successione di polinomi $y_n(X) = \sum_{i=0}^{n} a_i X^i$ tali che per ogni n si abbia $f(X, y_n(X)) \equiv 0 \pmod{X^{n+1}}$.

Chiaramente, per ipotesi possiamo usare $y_0(X) = a_0$.