CAPITOLO 1

# Aspetti algebrici delle serie di potenze

*Marco Manetti per il corso di Istituzioni di Geometria Superiore 2024-25.*
*Versione (molto) preliminare del 23 dicembre 2024*

## 1.1. Serie di potenze formali

Una **serie formale** a coefficienti in un campo $\mathbb{K}$ nelle indeterminate (o lettere) $x_1, \ldots, x_n$ è una espressione del tipo

$$\phi = \sum_{i_1,\ldots,i_n=0}^{\infty} a_{i_1\cdots i_n} x_1^{i_1} \cdots x_n^{i_n}, \qquad \text{dove } a_{i_1\cdots i_n} \in \mathbb{K} \text{ per ogni } i_1, \ldots, i_n \in \mathbb{N}.$$

Per semplicità di notazione, scriveremo spesso una serie formale come $\phi = \sum_{I\in\mathbb{N}^n} a_I x^I$, dove per ogni multiindice $I = (i_1, \ldots, i_n) \in \mathbb{N}^n$ si intende $x^I = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. Chiameremo $a_I$ il coefficiente di $x^I$ nella serie $\phi$.

Una serie formale in $n$ lettere a coefficienti in $\mathbb{K}$ non è altro che un diverso modo di rappresentare un'applicazione $a_\bullet \colon \mathbb{N}^n \to \mathbb{K}$; in particolare, due serie formali $\phi = \sum a_I x^I$ e $\psi = \sum b_I x^I$ coincidono se e solo se $a_I = b_I$ per ogni $I \in \mathbb{N}^n$; la serie formale nulla è quella con tutti i coefficienti $a_I$ uguali a 0.

L'insieme di tutte le serie formali a coefficienti in $\mathbb{K}$ nelle indeterminate $x_1, \ldots, x_n$ viene denotato con

$$\mathbb{K}[[x_1, \ldots, x_n]].$$

Tale insieme ha una ovvia struttura di spazio vettoriale su $\mathbb{K}$, rispetto alla quale l'anello dei polinomi $\mathbb{K}[x_1, \ldots, x_n]$ è un sottospazio vettoriale (ogni polinomio può essere pensato come una serie formale in cui i coefficienti sono diversi da 0 per al più un numero finito di multiindici). Possiamo anche estendere il prodotto tra polinomi alle serie di potenze.

Definizione 1.1.1. Il **prodotto di Cauchy** di due serie formali si definisce come

$$\left(\sum_{I\in\mathbb{N}^n} a_I x^I\right)\left(\sum_{J\in\mathbb{N}^n} b_J x^J\right) = \sum_{H\in\mathbb{N}^n} \left(\sum_{\substack{I,\,J\,\in\,\mathbb{N}^n \\ I+J=H}} a_I b_J\right) x^H.$$

Tale formula ha perfettamente senso perché per ogni $H \in \mathbb{N}^n$ esistono al più un numero finito di coppie $(I, J) \in \mathbb{N}^n \times \mathbb{N}^n$ tali che $I + J = H$; per la precisione, se $H = (h_1, \ldots, h_n)$ ci sono esattamente $\prod_{i=1}^n (h_i + 1)$ coppie.

Si verifica facilmente che con tale prodotto lo spazio vettoriale delle serie formali diventa un anello commutativo con unità. Il motivo per cui si sceglie il prodotto di Cauchy, e non altri, per estendere l'usuale prodotto di polinomi, seguirà dalle prossime considerazioni di natura topologica (oltre che dalla teoria delle serie di potenze in una variabile).

Definizione 1.1.2. Il **grado** di un multiindice $I = (i_1, \ldots, i_n) \in \mathbb{N}^n$ è il numero naturale $|I| = i_1 + \cdots + i_n$.

Il **supporto** di una serie formale $\phi = \sum a_I x^I$ è $\operatorname{Supp}(\phi) = \{I \in \mathbb{N}^n \mid a_I \neq 0\}$.

L'**ordine** di una serie formale $\phi \neq 0$ è $\operatorname{ord}(\phi) = \min\{|I| \mid I \in \operatorname{Supp}(\phi)\}$. Per convenzione si pone $\operatorname{ord}(0) = +\infty$.

Le proprietà fondamentali dell'ordine sono:

(1) $\operatorname{ord}(\phi + \psi) \geq \min(\operatorname{ord}(\phi), \operatorname{ord}(\psi))$ e vale la maggiorazione stretta solo se $\operatorname{ord}(\phi) = \operatorname{ord}(\psi)$;
(2) $\operatorname{ord}(\phi\psi) = \operatorname{ord}(\phi) + \operatorname{ord}(\psi)$.

Le disuguaglianze $\operatorname{ord}(\phi+\psi) \geq \min(\operatorname{ord}(\phi), \operatorname{ord}(\psi))$ e $\operatorname{ord}(\phi\psi) \geq \operatorname{ord}(\phi)+\operatorname{ord}(\psi))$ seguono immediatamente dalle definizioni. Per provare che $\operatorname{ord}(\phi\psi) \leq \operatorname{ord}(\phi)+\operatorname{ord}(\psi)$ possiamo chiaramente supporre $\phi, \psi \neq 0$. Se $a = \operatorname{ord}(\phi)$ e $b = \operatorname{ord}(\psi)$ possiamo scrivere $\phi = \phi_a + \tilde{\phi}$ con $\phi_a$ polinomio omogeneo non nullo di grado $a$ e $\operatorname{ord}(\tilde{\phi}) > a$; alla stessa maniera scriviamo $\psi = \psi_b + \tilde{\psi}$. Basta adesso osservare che l'anello dei polinomi è un dominio di integrità e quindi il grado di $\phi_a\psi_b$ è esattamente $a+b$, mentre i prodotti $\phi_a\tilde{\psi}, \tilde{\phi}\psi_b$ e $\tilde{\phi}\tilde{\psi}$ hanno tutti ordine strettamente maggiore di $a+b$.

Per ogni serie formale $\phi \in \mathbb{K}[[x_1, \dots, x_n]]$ ed ogni intero $n \geq 0$ denotiamo

$$U_n(\phi) = \{\eta \in \mathbb{K}[[x_1, \dots, x_n]] \mid \operatorname{ord}(\phi - \eta) > n\}.$$

LEMMA 1.1.3. *La famiglia di tutti i sottoinsiemi del tipo $U_n(\phi)$ è una base di una topologia metrizzabile su $\mathbb{K}[[x_1, \dots, x_n]]$, detta* ***topologia $\mathfrak{m}$-adica****.*

DIMOSTRAZIONE. Per le proprietà fondamentali dell'ordine, se $\eta \in U_n(\phi)$, allora $U_l(\eta) \subseteq U_n(\phi)$ per ogni $l \geq n$; da questo segue che per ogni $l > n$ ed ogni serie formale $\phi$ si ha $U_n(\phi) = \cup\{U_l(\eta) \mid \eta \in U_n(\phi)\}$.

Siccome $\phi \in U_n(\phi)$ per ogni $\phi$ ed ogni $n$, per provare che tale famiglia è una base di una topologia basta dimostrare che se $\eta \in U_n(\phi) \cap U_m(\psi)$ allora esiste $l \in \mathbb{N}$ tale che $U_l(\eta) \subseteq U_n(\phi) \cap U_m(\psi)$; per quanto visto sopra, basta prendere $l = \max(n, m)$.

Proviamo adesso che l'applicazione

$$\delta\colon \mathbb{K}[[x_1, \dots, x_n]] \times \mathbb{K}[[x_1, \dots, x_n]] \to \mathbb{R}, \quad \delta(\phi, \psi) = \frac{1}{1 + \operatorname{ord}(\phi - \psi)},$$

è una distanza che induce la topologia $\mathfrak{m}$-adica. È chiaro che $\delta(\phi, \psi) = \delta(\psi, \phi) \geq 0$ e vale $\delta(\phi, \psi) = 0$ se e solo se $\phi = \psi$. Per quanto riguarda la disuguaglianza triangolare $\delta(\phi, \psi) \leq \delta(\phi, \eta) + \delta(\eta, \psi)$, se $a = \operatorname{ord}(\phi - \eta)$ e $b = \operatorname{ord}(\psi - \eta)$, allora

$$\delta(\phi, \psi) \leq \frac{1}{1 + \min(a, b)} \leq \max\left(\frac{1}{1+a}, \frac{1}{1+b}\right) = \max(\delta(\phi, \eta), \delta(\eta, \psi)).$$

Per ogni $r \leq 1$, la palla aperta di centro $\phi$ e raggio $r$ coincide con $U_n(\phi)$, dove $n$ è la parte intera di $1/r - 1$ e quindi la topologia indotta da $\delta$ è esattamente quella generata dalla base $U_n(\phi)$. □

Dunque, una successione $\phi_i$ di serie formali converge a $\eta$ nella topologia $\mathfrak{m}$-adica se e solo se la successione di interi positivi $\operatorname{ord}(\eta - \phi_i)$ è divergente; nella stessa situazione, scriveremo $\phi = \sum_{i=0}^{\infty} \phi_i$ se la successione delle somme parziali $\sum_{i=0}^{d} \phi_i$ converge a $\phi$.

La topologia $\mathfrak{m}$-adica in $\mathbb{K}[[x_1, \dots, x_n]]$ è di Hausdorff ed è immediato osservare che il sottoanello dei polinomi $\mathbb{K}[x_1, \dots, x_n]$ è un sottoinsieme denso, e che le operazioni di somma e prodotto sono le uniche estensioni continue delle corrispondenti operazioni tra polinomi.

Possiamo scrivere ogni serie formale $\phi$ nella forma $\phi = \sum_{i \geq 0} \phi_i$, dove $\phi_i \in \mathbb{K}[x_1, \dots, x_n]$ è un polinomio omogeneo di grado $i$, possibilmente nullo. In tale rappresentazione, se $\phi \neq 0$ si ha che $\operatorname{ord}(\phi)$ è il più piccolo intero $m \geq 0$ tale che $\phi_m \neq 0$.

LEMMA 1.1.4. *Sia $\phi_0, \phi_1, \dots \in \mathbb{K}[[x_1, \dots, x_n]]$ una successione di serie formali tali che $\lim_{i\to\infty} \operatorname{ord}(\phi_i) = +\infty$. Allora esiste ed è unica la serie $\sum_{i=0}^{\infty} \phi_i$.*

DIMOSTRAZIONE. La condizione $\lim_{i\to\infty} \operatorname{ord}(\phi_i) = +\infty$ equivale a dire che per ogni multiindice $I$, solo un numero finito di serie $\phi_i$ ha il coefficiente di $x^I$ diverso da 0. Possiamo quindi, per ogni $I$ fissato alla volta, fare la somma di tali coefficienti e ottenere una serie formale $\phi$. La convergenza a $\phi$ della serie $\sum_{i=0}^{\infty} \phi_i$ è immediata. □

TEOREMA 1.1.5 (di sostituzione). *Siano $\phi_1, \dots, \phi_m \in \mathbb{K}[[x_1, \dots, x_n]]$ serie di ordine positivo. Allora esiste un unico omomorfismo continuo di anelli*

$$\Phi^*\colon \mathbb{K}[[y_1, \dots, y_m]] \to \mathbb{K}[[x_1, \dots, x_n]]$$

*tale che $\Phi^*(a) = a$ per ogni $a \in \mathbb{K}$ e $\Phi^*(y_i) = \phi_i$.*

DIMOSTRAZIONE. Per quanto riguarda l'unicità, se $f \in \mathbb{K}[y_1, \dots, y_m]$ la condizione che $\Phi^*$ sia un omomorfismo di anelli che lascia fisse le costanti implica che $\Phi^*(f) = f(g_1, \dots, g_m)$ è la serie ottenuta sostituendo ogni $\phi_i$ a $y_i$. Se $f = \sum_{d \geq 0} f_d$ con ogni $f_d$ omogeneo di grado $d$, la continuità di $\Phi^*$ implica

$$\Phi^*(f) = \sum_{d \geq 0} f_d(\phi_1, \dots, \phi_m), \tag{1.1}$$

con la somma su $d$ ben definita poiché ogni $f_d(\phi_1, \dots, \phi_m)$ è una serie di ordine $\geq d$.

Viceversa, la Formula (1.1) definisce un omomorfismo di anelli continuo. Nel seguito di queste note scriveremo $f(\phi_1,\dots,\phi_m)=\Phi^*(f)$ anche quando $f$ non è un polinomio. □

**Una digressione.** In queste note, il prossimo lemma di geometria convessa verrà usato solamente nell'Esercizio 1.7, che a sua volta può essere usato per dimostrare il teorema di fattorizzazione unica per le serie di potenze a coefficienti in un campo finito. Tuttavia, si tratta di un risultato dalle molteplici applicazioni e merita pertanto di essere palesato.

LEMMA 1.1.6. *Siano $S_1,\dots,S_m$ sottoinsiemi non vuoti di $\mathbb{N}^n$ e $U$ un sottospazio aperto e non vuoto di $(0,+\infty)^n\subseteq\mathbb{R}^n$. Esiste allora un vettore $v=(v_1,\dots,v_n)\in U\cap\mathbb{Q}^n$ tale che la restrizione di*

$$f_v\colon \mathbb{R}^n\to\mathbb{R},\quad f_v(x)=\sum_i v_i x_i,$$

*a ciascun $S_j$ possieda un unico punto di minimo assoluto.*

DIMOSTRAZIONE. Non è restrittivo supporre che nessun $S_j$ contenga il multiindice $(0,\dots,0)$ e che $U=\prod_{i=1}^n(a_i,b_i)$ con $0<a_i<b_i<+\infty$ per ogni $i$.
Siano $a=\min(a_i)$, $b=\max(b_i)$, $d_j=\min\{|I|\mid I\in S_j\}$ e, per ogni $u\in U$, denotiamo

$$f_u\colon\mathbb{N}^n\to\mathbb{R},\qquad f_u(x)=\sum_i u_i x_i.$$

Per ogni $u\in U$ si ha $\inf(f_u(S_j))<bd_j$ e $f_u(I)>a|I|$ per ogni $I\in\mathbb{N}^n$; questo implica che $\inf(f_u(S_j))$ coincide con il valore minimo di $f_u$ nell'insieme finito $S_j':=\{I\in S_j\mid |I|\le bd_j/a\}$.
Siano $\xi_i\in(a_i,b_i)$, con $i=1,\dots,n$, numeri reali linearmente indipendenti su $\mathbb{Q}$, ad esempio opportuni multipli razionali dei logaritmi di $n$ primi distinti, oppure di $n$ potenze intere distinte di un numero trascendente. Allora l'applicazione $f_\xi\colon\mathbb{Z}^n\to\mathbb{R}$ è iniettiva e questo prova che l'aperto

$$V=\bigcap_{j=1}^m V_j,\quad \text{dove } V_j=\{u\in U\mid f_u(x)\neq f_u(y)\ \forall x\neq y\in S_j'\}$$

è non vuoto. Per concludere, possiamo prendere come $v$ un qualsiasi elemento di $V\cap\mathbb{Q}^n$. □

### 1.1.1. Esercizi.

ESERCIZIO 1.1. Dimostrare che ogni omomorfismo continuo di anelli

$$\Phi^*\colon\mathbb{K}[[y_1,\dots,y_m]]\to\mathbb{K}[[x_1,\dots,x_n]]$$

tale che $\Phi^*(a)=a$ per ogni $a\in\mathbb{K}$ è ottenuto per sostituzione come nel Teorema 1.1.5

## 1.2. Serie di potenze convergenti

Sia $\mathbb{K}$ un campo, una **norma** su $\mathbb{K}$ è un'applicazione $|\cdot|\colon\mathbb{K}\to\mathbb{R}$ che soddisfa le seguenti proprietà:

(1) $|a|\ge 0$ per ogni $a\in\mathbb{K}$.
(2) $|a|=0$ se e solo se $a=0$.
(3) $|a+b|\le|a|+|b|$ per ogni $a,b\in\mathbb{K}$ (disuguaglianza triangolare).
(4) $|ab|=|a||b|$ per ogni $a,b\in\mathbb{K}$.

Si noti che $|1|=|-1|=1$. Ogni norma induce una struttura di spazio metrico con distanza $d(a,b)=|a-b|$; il campo normato $(\mathbb{K},|\cdot|)$ si dice completo se lo spazio metrico $(\mathbb{K},d)$ è completo.

ESEMPIO 1.2.1 (norma euclidea). Se $\mathbb{K}$ è un sottocampo di $\mathbb{C}$, allora il valore assoluto usuale induce una norma su $\mathbb{K}$.

ESEMPIO 1.2.2 (norma discreta). Sia $\mathbb{K}$ un campo qualsiasi, la funzione $|0|=0$, $|a|=1$ per ogni $a\neq 0$, è una norma che induce la topologia discreta.

ESEMPIO 1.2.3 (norma $p$-adica). Sia $\mathbb{K}=\mathbb{Q}$ e sia $p$ un numero primo. La norma $p$-adica $|\cdot|_p\colon\mathbb{Q}\to\mathbb{R}$ si definisce nel modo seguente: se $a=p^r\dfrac{b}{c}\neq 0$ con $b,c,r\in\mathbb{Z}$ e $b,c$ non divisibili per $p$, allora $|a|_p=p^{-r}$. Non è arduo dimostrare che si tratta di una norma.

OSSERVAZIONE 1.2.4. Una norma $|\cdot|$ si dice **archimedea** se per ogni $a,b\neq 0$ esiste un intero positivo $n$ tale che $|na|>|b|$. Non tutte le norme sono archimedee; ad esempio, sia la norma discreta che la norma $p$-adica non sono archimedee poiché soddisfano la disuguaglianza $|a+b|\le\max(|a|,|b|)$.

Siano adesso $(\mathbb{K}, |\cdot|)$ un campo normato e $n \geq 0$ un intero fissati. Chiameremo **multiraggio** una qualunque successione $r = (r_1, \ldots, r_n)$ di $n$ numeri reali positivi. Dati due multiraggi $r = (r_1, \ldots, r_n)$ e $R = (R_1, \ldots, R_n)$ scriveremo $r < R$ se $r_i < R_i$ per ogni indice $i$.

Se $r = (r_1, \ldots, r_n)$ è un multiraggio e $I = (i_1, \ldots, i_n)$ è un multiindice si pone $r^I = r_1^{i_1} r_2^{i_2} \cdots r_n^{i_n}$. Per ogni serie formale $\phi = \sum a_I x^I$ ed ogni multiraggio $r$ definiamo

$$\|\phi\|_r := \sum_I |a_I| r^I := \lim_{d\to\infty} \sum_{|I|\leq d} |a_I| r^I \in [0, +\infty].$$

LEMMA 1.2.5. *Per ogni $\phi, \psi \in \mathbb{K}[[x_1, \ldots, x_n]]$ ed ogni multiraggio $r$ si ha:*

(1) $\|\phi + \psi\|_r \leq \|\phi\|_r + \|\psi\|_r$;
(2) $\|\phi\psi\|_r \leq \|\phi\|_r \|\psi\|_r$ *(con la convenzione che $0 \cdot +\infty = 0$);*
(3) *per ogni numero reale $0 < t \leq 1$ vale $\|\phi\|_{tr} \leq t^{\mathrm{ord}(\phi)} \|\phi\|_r$.*

DIMOSTRAZIONE. Se $\phi = \sum a_J x^J$ e $\psi = \sum b_H x^H$, allora per ogni multiindice $I$ si ha

$$|a_I + b_I| \leq |a_I| + |b_I|, \quad \left| \sum_{J+H=I} a_J b_H \right| \leq \sum_{J+H=I} |a_J||b_H|,$$

e, per ogni intero positivo $d$,

$$\sum_{|J+H|\leq d} |a_J||b_H| r^{J+H} \leq \left( \sum_{|J|\leq d} |a_J| r^J \right) \left( \sum_{|H|\leq d} |b_H| r^H \right),$$

e passando al limite per $d \to \infty$ si conclude.

Per l'ultimo punto basta osservare che se $a_J \neq 0$ allora $|J| \geq \mathrm{ord}(\phi)$ e $(tr)^J \leq t^{\mathrm{ord}(\phi)} r^J$. Dunque $|a_J|(tr)^J \leq t^{\mathrm{ord}(\phi)} |a_J| r^J$ per ogni multiindice $J$. □

Il Lemma 1.2.5 ci consente di definire, per ogni multiraggio $r$, il seguente sottoanello di $\mathbb{K}[[x_1, \ldots, x_n]]$:

$$B_r = \{\phi \in \mathbb{K}[[x_1, \ldots, x_n]] \mid \|\phi\|_r < +\infty\}.$$

Se $r < R$ allora $B_R \subseteq B_r$ e da questo segue che anche l'unione di tutti i $B_r$, al variare di $r$ tra tutti i possibili multiraggi, è un sottoanello.

DEFINIZIONE 1.2.6. Il sottoanello delle **serie convergenti** è definito come

$$\mathbb{K}\{x_1, \ldots, x_n\} = \{\phi \in \mathbb{K}[[x_1, \ldots, x_n]] \mid \text{ esiste } r \in (0, +\infty)^n \text{ tale che } \|\phi\|_r < +\infty\} = \cup_r B_r.$$

OSSERVAZIONE 1.2.7. Se $r < (1, 1, \ldots, 1)$ è un semplice esercizio provare che

$$\sum_I r^I = \prod_{i=1}^n \frac{1}{1 - r_i} < +\infty.$$

Questo prova che ogni serie formale è convergente nella norma discreta su $\mathbb{K}$; in particolare, tutti i risultati validi per l'anello $\mathbb{K}\{x_1, \ldots, x_n\}$ delle serie convergenti rispetto ad una norma qualunque valgono anche per $\mathbb{K}[[x_1, \ldots, x_n]]$.

Prima di proseguire vediamo gli analoghi del Lemma 1.1.4 per gli spazi $B_r$ e del teorema di sostituzione per le serie convergenti.

LEMMA 1.2.8. *Sia $\phi_0, \phi_1, \ldots$ una successione di serie formali tali che $\lim_{i\to\infty} \mathrm{ord}(\phi_i) = +\infty$. Allora per ogni multiraggio $r$ si ha*

$$\left\| \sum_{i=0}^{\infty} \phi_i \right\|_r \leq \sum_{i=0}^{\infty} \|\phi_i\|_r.$$

*In particolare, se $\phi_i \in B_r$ per ogni $i$ e $\sum_{i=0}^{\infty} \|\phi_i\|_r < +\infty$, allora $\phi \in B_r$.*

DIMOSTRAZIONE. Basta considerare il caso in cui $M := \sum_{i=0}^{\infty} \|\phi_i\|_r < +\infty$. Se $\phi_i = \sum_I a_{I,i} x^I$ e $\phi = \sum_I a_I x^I$. Sia $H$ un sottoinsieme finito di $\mathbb{N}^n$ e scegliamo un intero $d$ tale che $\mathrm{ord}(\phi_i) > |I|$ per ogni $i > d$ ed ogni $I \in H$. Allora $a_I = \sum_{i=0}^{d} a_{I,i}$ per ogni $I \in H$ e

$$\sum_{I\in H} |a_I| r^I \leq \sum_{i=0}^{d} \sum_{I\in H} |a_{I,i}| r^I \leq \sum_{i=0}^{d} \|\phi_i\|_r \leq M.$$

La precedente disuguaglianza vale per ogni $H$ e questo implica $\|\phi\|_r \leq M$. □

TEOREMA 1.2.9 (di sostituzione). *Siano $\phi_1, \dots, \phi_m \in \mathbb{K}\{x_1, \dots, x_n\}$ serie convergenti di ordine positivo. Allora esiste un unico omomorfismo continuo di anelli*

$$\Phi^* \colon \mathbb{K}\{y_1, \dots, y_m\} \to \mathbb{K}\{x_1, \dots, x_n\}$$

*tale che $\Phi^*(a) = a$ per ogni $a \in \mathbb{K}$ e $\Phi^*(y_i) = \phi_i$.*

DIMOSTRAZIONE. Anche in questo caso la continuità è intesa rispetto alla topologia $\mathfrak{m}$-adica. Dato che $\mathbb{K}\{x_1, \dots, x_n\}$ è un sottoanello di $\mathbb{K}[[x_1, \dots, x_n]]$, dal Teorema 1.1.5 sappiamo che se $f = \sum_{d \geq 0} f_d \in \mathbb{K}\{y_1, \dots, y_m\}$ con ogni $f_d$ polinomio omogeneo di grado $d$, allora

$$\Phi^*(f) = \sum_{d \geq 0} f_d(\phi_1, \dots, \phi_m),$$

ed ogni serie $f_d(\phi_1, \dots, \phi_m) \in \mathbb{K}\{x_1, \dots, x_n\}$ ha ordine $\geq d$. Per il Lemma 1.2.8 basta quindi dimostrare che esiste un multiraggio $r = (r_1, \dots, r_n)$ tale che $\sum_{d \geq 0} \|f_d(\phi_1, \dots, \phi_m)\|_r < \infty$.

Sia $R = (R_1, \dots, R_m)$ tale che $\|f\|_R = \sum_{d \geq 0} \|f_d\|_R < \infty$ e $s = (s_1, \dots, s_n)$ tale che $\phi_i \in B_s$ per ogni $i$. Dato che ogni $\phi_i$ ha ordine positivo, per ogni numero reale $0 < t \leq 1$ si ha $\|\phi_i\|_{ts} \leq t\|\phi_i\|_s$. Basta allora prendere $r = ts$ con $t$ sufficientemente piccolo tale che $\|\phi_i\|_r \leq R_i$ per ogni $i$ ed osservare che, per il Lemma 1.2.5, dato un qualsiasi polinomio $p \in \mathbb{K}[y_1, \dots, y_m]$ vale $\|p(\phi_1, \dots, \phi_m)\|_r \leq \|p\|_R$. □

ESEMPIO 1.2.10 (Cambi lineari di coordinate). Sia $(a_{ij}) \in M_{n,n}(\mathbb{K})$ una matrice invertibile con inversa $(b_{ij})$. Allora l'omomorfismo $\mathbb{K}\{y_1, \dots, y_n\} \to \mathbb{K}\{x_1, \dots, x_n\}$ dato dalle sostituzioni $y_i = \sum_j a_{ij} x_j$ è un isomorfismo il cui inverso è dato dalle sostituzioni $x_i = \sum_j b_{ij} y_j$.

Se $\phi \in \mathbb{K}\{x_1, \dots, x_n\}$ è sempre definito il valore $\phi(0) \in \mathbb{K}$ (è il coefficiente di $x^0$, detto anche "termine costante") ma in generale, a meno che il campo normato non sia completo, non definisce alcuna funzione in un intorno di 0.

COROLLARIO 1.2.11. *Una serie convergente $f$ è un elemento invertibile dell'anello $\mathbb{K}\{x_1, \dots, x_n\}$ se e solo se $f(0) \neq 0$. Equivalentemente, $\mathbb{K}\{x_1, \dots, x_n\}$ è un anello locale con ideale massimale $\mathfrak{m} = \{f \mid f(0) = 0\} = \{f \mid \operatorname{ord}(f) > 0\}$.*

DIMOSTRAZIONE. Se esiste $g$ tale che che $fg = 1$, allora $0 = \operatorname{ord}(1) = \operatorname{ord}(f) + \operatorname{ord}(g)$ e quindi $\operatorname{ord}(f) = 0$. Viceversa, se $\operatorname{ord}(f) = 0$ possiamo scrivere $f = a - g$ con $0 \neq a \in \mathbb{K}$ e $g$ di ordine positivo. Il polinomio $a - y$ è invertibile in $\mathbb{K}\{y\}$ con inverso

$$h(y) = \frac{1}{a - y} = \frac{1/a}{1 - y/a} = \sum_{i=0}^{\infty} \frac{y^i}{a^{i+1}}.$$

Per il teorema di sostituzione, l'inverso di $a - g$ è uguale a $h(g) = \sum_{i=0}^{\infty} \frac{g^i}{a^{i+1}}$. □

**Esercizi.**

ESERCIZIO 1.1. Dimostrare che in un campo finito esiste un'unica norma (quella discreta).

ESERCIZIO 1.2. Sia $(\mathbb{K}, |\cdot|)$ un campo normato completo di caratteristica 0. Provare che se $|2| > 1$, allora $\mathbb{K}$ è connesso. (Sugg.: per assurdo, sia $\mathbb{K}$ unione disgiunta di due chiusi non vuoti $A, B$, con $0 \in A$. Sia $x_0 \in B$ e per ogni intero $n \geq 0$ siano

$$a_n = \min\{m \in \mathbb{N} \mid m \leq 2^n,\ mx_0/2^n \in B\}, \quad x_n = a_n x/2^n, \quad y_n = (a_n - 1)x/2^n.$$

Provare che $\lim x_n = \lim y_n$.)

ESERCIZIO 1.3. Sia $|\ |$ una norma su $\mathbb{Q}$ tale che $|p| \leq 1$ per qualche primo $p > 1$. Dimostrare che $|q| \leq 1$ per ogni numero intero. Provare inoltre che, se $|p| < 1$ e $p$ non divide $q$, allora $|q| = 1$. (Sugg.: scrivere $q^n$ in base $p$ e fare tendere $n \to +\infty$.)

ESERCIZIO 1.4. Sia $s$ un intero positivo fissato. Provare che una serie formale $\sum a_I x^I$ è convergente se e solo se esiste un numero reale positivo $R$ tale che $|a_I||I|^s \leq R^{|I|}$ per ogni multiindice $I$.

ESERCIZIO 1.5. Se $(\mathbb{K}, |\ |)$ è un campo completo e $\phi \in \mathbb{K}\{x_1, \dots, x_n\}$, allora $\phi$ definisce, in un intorno di 0 in $\mathbb{K}^n$, una funzione continua a valori in $\mathbb{K}$. (Nota: se il campo non è completo, una serie convergente non definisce in generale una funzione in un intorno di 0.)

ESERCIZIO 1.6. Sia $(\mathbb{K}, |\ |)$ un campo normato e siano $a_1, \dots, a_n \in \mathbb{K}$ tali che $|a_i| = 1$ per ogni $i = 1, \dots, n$; denotiamo con $A \subset \mathbb{K}$ il sottoanello unitario generato dalle funzioni simmetriche elementari di $a_1, \dots, a_n$. Provare che, se l'insieme $\{a \in A \mid |a| \leq 2^{n-1}\}$ è finito, allora $a_1, \dots, a_n$ sono radici dell'unità. (Sugg.: i polinomi $p_r(x) = \prod_i (x - a_i^r)$, con $r \in \mathbb{Z}$, non possono essere tutti distinti.)

Dedurre che le matrici ortogonali a coefficienti interi hanno ordine finito nel gruppo $O(n, \mathbb{R})$.

ESERCIZIO 1.7. Nelle notazioni della Sezione 1.3. Dimostrare che se $(\mathbb{K}, |\ |)$ è completo, allora $(B_r, \|\ \|_r)$ è uno spazio di Banach per ogni multiraggio $r$.

## 1.3. I teoremi di Weierstrass

In questa sezione dimostreremo che per le serie convergenti, in qualunque campo normato, valgono i teoremi di divisione e preparazione di Weierstrass. In entrambi i teoremi una variabile gioca un ruolo privilegiato rispetto alle altre: per esaltare tale differenza indicheremo con $t$ l'indeterminata "nobile" e con $x_1, \dots, x_n$ le indeterminate "plebaglia".

DEFINIZIONE 1.3.1. Una serie $\phi \in \mathbb{K}\{x_1, \dots, x_n, t\}$ si dice:

(1) uno **pseudopolinomio** di grado $N$ in $t$ se la serie $\phi(0, \dots, 0, t)$ è non nulla di ordine $N$; in tal caso diremo che $\phi$ è monico se $\phi(0, \dots, 0, t) = t^N + \text{termini superiori}$;
(2) un **polinomio di Weierstrass** di grado $N$ in $t$ se

$$\phi = t^N + \sum_{i=1}^{N} \phi_i(x) t^{N-i}$$

con ogni $\phi_i \in \mathbb{K}\{x_1, \dots, x_n, t\}$ di ordine positivo.

In particolare, ogni polinomio di Weierstrass di grado $N$ è anche uno pseudopolinomio di grado $N$.

L'applicazione lineare

$$L \colon \mathbb{K}\{x_1, \dots, x_n, t\} \to \mathbb{K}\{x_1, \dots, x_n, t\}, \qquad L(\sum_{i \geq 0} f_i(x) t^i) = \sum_{i \geq N} f_i(x) t^{i-N}$$

risulta ben definita. Per ogni multiraggio $r = (r_1, \dots, r_n)$, e ogni reale positivo $s$ ed ogni intero $0 \leq d \leq N$ si ha

$$\left\| L(t^{N-d} \sum_{i \geq 0} f_i(x) t^i) \right\|_{(r,s)} = \sum_{i \geq d} \|f_i\|_r s^{i-d} \leq \frac{1}{s^d} \sum_{i \geq 0} \|f_i\|_r s^i = \frac{1}{s^d} \left\| \sum_{i \geq 0} f_i(x) t^i \right\|_{(r,s)}.$$

In particolare, per $d = N$ si ottiene $L(B_{(r,s)}) \subseteq B_{(r,s)}$.

LEMMA 1.3.2. *Sia $\phi \in B_{(r,s)} \subseteq \mathbb{K}\{x_1, \dots, x_n, t\}$ uno pseudopolinomio in $t$ di grado $N \geq 0$. Allora esiste un multiraggio $(R, S) < (r, s)$ tale che l'applicazione*

$$V \colon B_{(R,S)} \to B_{(R,S)}, \qquad V(f) = L(\phi f),$$

*è un isomorfismo di spazi vettoriali.*

DIMOSTRAZIONE. Possiamo scrivere

$$\phi = t^N + t^N e(x, t) + \sum_{i=1}^{N} \phi_i(x) t^{N-i},$$

con $e \in \mathbb{K}\{x_1, \dots, x_n, t\}$ e $\phi_i \in \mathbb{K}\{x_1, \dots, x_n\}$ serie di ordine positivo. Si noti che $e = t^N L(\phi) \in B_{(r,s)}$ e $\phi_i \in B_r$ per ogni $i$.

Sia $\varepsilon = \frac{1}{2(N+1)}$ e scegliamo un multiraggio $(R, S) < (r, s)$ tale che

$$\|e\|_{(R,S)} < \varepsilon, \qquad \|\phi_i\|_R < \epsilon S^i;$$

ad esempio, si può moltiplicare prima la coppia $(r, s)$ per un numero reale sufficientememte piccolo in modo tale che $\|e\|_{(r,s)} < \varepsilon$ e poi moltiplicare ancora $r$ per un reale positivo sufficientemente piccolo. Dimostriamo che $V \colon B_{(R,S)} \to B_{(R,S)}$ è invertibile.

Consideriamo adesso l'applicazione lineare

$$H \colon B_{(R,S)} \to B_{(R,S)}, \quad H(f) = f - L(\phi f), \quad H = \mathrm{Id} - V.$$

Allora

$$H(f) = L((t^N - \phi) f) = L(-t^N e f - \sum_i \phi_i t^{N-i} f) = -ef - \sum_i \phi_i L(t^{N-i} f)$$

$$\|H(f)\|_{(R,S)} \leq \|e\|_{(R,S)}\|f\|_{(R,S)} + \sum_{i=1}^{N} \|\phi_i\|_R S^{-i}\|f\|_{(R,S)} \leq \frac{1}{2}\|f\|_{(R,S)}.$$

Sia adesso $H^i$ la composizione di $H$ con se stessa $i$ volte e dimostriamo che per ogni $f \in \mathbb{K}[[x_1,\dots,x_n,t]]$ si ha $\lim_{i\to\infty} H^i(f) = +\infty$. A tale scopo consideriamo l'ordine pesato

$$\mu\colon \mathbb{K}[[x_1,\dots,x_n,t]] \to \mathbb{N}\cup\{+\infty\},$$

come $\mu(0) = +\infty$ e, mentre $f \neq 0$ poniamo $\mu(f)$ uguale minimo di $(N+1)|I| + j$ al variare dei multiindici $(I,j) \in \mathbb{N}^n \times \mathbb{N}$ nel supporto di $f$. Siccome $\operatorname{ord}(f) \geq \mu(f)/(N+1)$ per avere la divergenza della successione $\operatorname{ord}(H^i(f))$ ci basta provare che $\mu(H(f)) > \mu(f)$ per ogni $f$.

Come per l'ordine usuale, anche per quello pesato valgono le disuguaglianze $\mu(f+g) \geq \min(\mu(f),\mu_g))$ e $\mu(fg) \geq \mu(f) + \mu(g)$. Per concludere basta osservare che $\mu(e) > 0$, $\mu(\phi_i) \geq N+1$ e $\mu(L(t^d f)) \geq \mu(f) + d - N$ per ogni $d \geq 0$.

Riepilogando, per ogni $f \in B_{(R,S)}$ la successione $H^i(f)$ soddisfa le ipotesi del Lemma 1.2.8 e quindi esiste $\sum_{i=0}^{\infty} H^i(f) \in B_{(R,S)}$. Siccome l'operatore $V = I - H$ non cambia l'ordine pesato $\mu$, si ottiene che $V(\sum_{i=0}^{\infty} H^i(f)) = f$. □

TEOREMA 1.3.3 (di divisione). *Sia $\phi \in \mathbb{K}\{x_1,\dots,x_n,t\}$ uno pseudopolinomio di grado $N$ in $t$. Allora per pgni $f \in \mathbb{K}\{x_1,\dots,x_n,t\}$ esistono unici $g \in \mathbb{K}\{x_1,\dots,x_n,t\}$ e $q \in \mathbb{K}\{x_1,\dots,x_n\}[t]$ di grado $< N$ in $t$ tali che*

$$f = \phi g + q.$$

DIMOSTRAZIONE. Non è restrittivo supporre $\phi$ pseudopolinomio monico. Sia $(r,s)$ un poliraggio sufficientemente piccolo tale che $f \in B_{(r,s)}$. Per il Lemma 1.3.2 esiste un poliraggio $(R,S) < (r,s)$ ed una serie $g \in B_{(R,S)}$ tale che $L(f) = L(\phi g)$. Ma questo equivale a dire che $L(f - \phi g) = 0$, ossia che $f - \phi g$ è un polinomio in $t$ di grado minore di $N$.

Per quanto riguarda l'unicità di $g$ (ed di conseguenza quella di $q$), se $\phi(g - g')$ è un polinomio in $t$ di grado minore di $N$ allora $V(g - g') = 0$ e basta applicare di nuovo il Lemma 1.3.2 ad un poliraggio $(r,s)$ tale che $g - g' \in B_{(R,s)}$. □

TEOREMA 1.3.4 (di preparazione). *Sia $\phi \in \mathbb{K}\{x_1,\dots,x_n,t\}$ uno pseudopolinomio di grado $N$ in $t$. Allora esiste unica $e \in \mathbb{K}\{x_1,\dots,x_n,t\}$ invertibile tale che $\phi e$ sia un polinomio di Weierstrass, ossia*

$$\phi e = t^N + \sum_{i=1}^{N} \psi_i(x) t^{N-i}, \qquad \operatorname{ord}(\psi_i) > 0.$$

DIMOSTRAZIONE. Per il teorema di divisione esiste unica una serie di potenze convergente $e$ tale che

$$t^N = \phi e - \sum_{i=1}^{N} \psi_i(x) t^{N-i}, \quad \psi_i \in \mathbb{K}\{x_1,\dots,x_n\}.$$

Con la sostituzione $x_1 = \cdots = x_n = 0$ si ottiene

$$t^N = e(0,t)\phi(0,t) - \sum_{i=1}^{N} \psi_i(0) t^{N-i}.$$

e siccome la serie $\phi(0,t)$ ha ordine $N$ deve per forza essere $\psi_i(0)$ per ogni $i$ e $e(0,0) \neq 0$. □

**Esercizi.**

ESERCIZIO 1.8. Sia $p(y_1,\dots,y_s,t) \in \mathbb{C}\{y_1,\dots,y_s\}[t]$ un polinomio monico in $t$ e sia $\phi(y_1,\dots,y_s) \in \mathbb{C}[[y_1,\dots,y_s]]$ tale che $p(y_1,\dots,y_s,\phi(y)) = 0$. Dimostrare che la serie $\phi$ è convergente.

## 1.4. Fattorizzazione unica negli anelli di serie convergenti

In questa sezione dimostriamo che per ogni campo normato infinito $\mathbb{K}$ l'anello $\mathbb{K}\{x_1,\dots,x_n\}$ è un dominio a fattorizzazione unica; se il campo è finito il risultato è ancora vero ma, oltre ad essere irrilevante per le nostre applicazioni, richiede una diversa (e più difficile) dimostrazione.

Prima della dimostrazione è utile richiamare, dai corsi di algebra, alcuni concetti base riguardanti il concetto di fattorizzazione unica su anelli commutativi più generali di $\mathbb{Z}$ e $\mathbb{K}[t]$. Nel seguito tutti gli anelli sono intesi commutativi e con unità e la scrittura $a|b$ significa che $a$ divide $b$.

(1) Un elemento $a \neq 0$ in un anello si dice:
   (a) **irriducibile** se non è invertibile e se $a = bc$ implica che uno tra $b$ e $c$ è invertibile.

(b) **primo** se non è invertibile e se $a|bc$ implica che $a|b$ oppure $a|c$.
In un dominio di integrità ogni primo è irriducibile, ma il viceversa è generalmente falso, vedi Esercizio 1.4.

(2) un insieme $a_1, \dots, a_n$ di elementi in un anello $A$ si dice **senza fattori comuni** se ogni divisore comune è invertibile, e cioè $b \in A$ divide $a_1, \dots, a_n$ solo se $b$ è invertibile. Un polinomio in $A[t]$ di dice **primitivo** se è diverso da 0 e se i suoi coefficienti non hanno fattori comuni.

(3) Un dominio di integrità di dice a **fattorizzazione unica**, o anche **fattoriale**, se:
   (a) *ogni elemento non nullo e non invertibile è un prodotto finito di irriducibli;*
   (b) *ogni irriducibile è primo.*
   Grossolanamente, (a) equivale all'esistenza della fattorizzazione come prodotto di irriducibili e (b) all'unicità, intesa come al solito a meno dell'ordine e di moltiplicazione per invertibili.

(4) Per ogni campo $\mathbb{K}$, l'anello $\mathbb{K}[t]$ è un dominio a fattorizzazione unica. (L'esistenza della fattorizzazione è ovvia conseguenza del fatto che il grado del prodotto è uguale alla somma dei gradi, mentre dimostrare che ogni irriducibile è primo richiede l'algoritmo di divisione Euclidea).

(5) (Lemma di Gauss). Siano $A$ un dominio a fattorizzazione unica e $\mathbb{K}$ il suo campo delle frazioni. Se $p(t), q(t) \in A[t]$ con $p(t)$ primitivo e $p(t)$ divide $q(t)$ in $\mathbb{K}[t]$, allora $p(t)$ divide $q(t)$ in $A[t]$.

(6) Segue facilmente dal lemma di Gauss che se $A$ è un dominio a fattorizzazione unica allora anche $A[t]$ lo è. Inoltre, due polinomi $p, q \in A[t]$ hanno un fattore comune di grado positivo in $t$ nell'anello $A[t]$ se e solo se lo stesso vale in $\mathbb{K}[t]$.

ESEMPIO 1.4.1. La serie $f(x,y) = x^2 - y^3 \in \mathbb{C}\{x,y\}$ è irriducibile. Infatti, se fosse $f = gh$, con $g(0) = h(0) = 0$, guardando le componenti omogenee di grado più basso si deve avere $g = ax + \tilde{g}$, $h = a^{-1}x + \tilde{h}$, con $a \in \mathbb{C} - \{0\}$ e $\tilde{g}, \tilde{h}$ non nulle e di ordine $> 1$. A meno di moltiplicare $g, h$ per delle costanti possiamo supporre $a = 1$ e quindi $x^2 - y^3 = x^2 + x(\tilde{g} + \tilde{h}) + \tilde{g}\tilde{h}$. Ma questo è assurdo perché il termine $y^3$ può comparire solo nel prodotto $\tilde{g}\tilde{h}$ che però ha ordine $\geq 4$.

PROPOSIZIONE 1.4.2. *L'anello $\mathbb{K}\{t\}$ è un dominio ad ideali principali: più precisamente ogni ideale non banale è generato da $t^n$ per qualche $n \geq 0$.*

DIMOSTRAZIONE. Sia $I \neq 0$ un ideale e sia $f \in I$ di ordine minimo $m$, siccome $t^m$ divide ogni $g \in I$ basta dimostrare che $t^m \in I$. Si può scrivere $f = t^m\phi$ con $\phi(0) \neq 0$; dato che $\phi$ è invertibile vale $t^m = f\phi^{-1} \in I$. □

LEMMA 1.4.3. *Siano $f, g \in \mathbb{K}\{x_1, \dots, x_n\}[t]$ con $g$ polinomio di Weierstrass. Se $f = hg$ con $h \in \mathbb{K}\{x_1, \dots, x_n, t\}$, allora anche $h \in \mathbb{K}\{x_1, \dots, x_n\}[t]$.*

Si noti che se $g$ non è di Weierstrass il risultato è falso, si consideri ad esempio il caso $n = 0, f = t^3$ e $g = t + t^2$.

DIMOSTRAZIONE. Sia $g = t^s + \sum g_i(x)t^{s-i}$, $g_i(0) = 0$, $f = \sum_{i=0}^{r} f_i(x)t^{r-i}$, $h = \sum_i h_i(x)t^i$, bisogna dimostrare che $h_i = 0$ per ogni $i > r - s$. Si assuma per assurdo che esista $j > r - s$ tale che $h_j \neq 0$, si può allora supporre che l'ordine di $h_j$ sia minimo fra tutte gli ordini di $h_i$, $i > r - s$. Vale l'uguaglianza $0 = h_j + \sum g_i h_{j+i}$ e siccome tutte le $g_i$ hanno ordine positivo si ottiene una contraddizione. □

LEMMA 1.4.4. *Sia $f \in \mathbb{K}\{x_1, \dots, x_n\}[t]$ un polinomio di Weierstrass in $t$:*

(1) *Se $f$ è invertibile in $\mathbb{K}\{x_1, \dots, x_n, t\}$, allora è invertibile anche in $\mathbb{K}\{x_1, \dots, x_n\}[t]$ (il viceversa è ovvio).*
(2) *Se $f$ è irriducibile in $\mathbb{K}\{x_1, \dots, x_n, t\}$, allora è irriducibile anche in $\mathbb{K}\{x_1, \dots, x_n\}[t]$.*
(3) *Se $f$ è primo in $\mathbb{K}\{x_1, \dots, x_n\}[t]$, allora è primo anche in $\mathbb{K}\{x_1, \dots, x_n, t\}$.*

DIMOSTRAZIONE. Il primo punto segue dal fatto che l'unico polinomio di Weierstrass di ordine 0 è quello di grado 0.

Assumiamo $f$ irriducibile in $\mathbb{K}\{x_1, \dots, x_n, t\}$ e siano $g_1, g_2 \in \mathbb{K}\{x_1, \dots, x_n\}[t]$ tali che $f = g_1g_2$. A meno di scambio di indici si può $g_1$ polinomio invertibile in $\mathbb{K}\{x_1, \dots, x_n, t\}$, e cioè tale che $g_1(0) \neq 0$. Siccome $g_1(0,t)$ divide $f(0,t) = t^N$ deve necessariamente essere $g_1(0,t) = at^s$ per qualche $a \neq 0$ e qualche $s$ e poiché $g_1(0) \neq 0$ deve essere $s = 0$, ossia $g_1 = a$ costante invertibile.

Supponiamo adesso che $f$ sia primo in $\mathbb{K}\{x_1, \dots, x_n\}[t]$ e supponiamo $f|gh$, con $g, h \in \mathbb{K}\{x_1, \dots, x_n, t\}$. Possiamo trovare due costanti $a, b \in \{0, 1\}$ tali che entrambe le serie $g + af$ e $h + bf$ siano pseudo-polinomi in $t$, e $f$ divide il prodotto $(g + af)(h + bf)$. Per il teorema di preparazione si può scrivere

$g + af = \phi e$ e $h + bf = \psi\epsilon$, con $\phi, \psi \in \mathbb{K}\{x_1, \dots, x_n\}[t]$ e $e, \epsilon$ invertibili. Ma allora $f$ divide $\phi\psi$ in $\mathbb{K}\{x_1, \dots, x_n, t\}$, di conseguenza lo divide anche nell'anello $\mathbb{K}\{x_1, \dots, x_n\}[t]$, dove $f$ è primo. Ma allora $f$ divide almeno uno tra $\phi$ e $\psi$ e quindi $f$ divide in $\mathbb{K}\{x_1, \dots, x_n, t\}$ almeno uno tra $g + af$ e $h + bf$. □

TEOREMA 1.4.5 (E. Lasker, 1905). *Sia $\mathbb{K}$ un campo normato. Allora l'anello $\mathbb{K}\{x_1, \dots, x_n, t\}$ è un dominio a fattorizzazione unica.*

DIMOSTRAZIONE. Come preannunciato dimostriamo il teorema con l'ipotesi aggiuntiva che $\mathbb{K}$ sia infinito. L'anello $\mathbb{K}\{t\}$ è un dominio ad ideali principali e quindi è a fattorizzazione unica per fatti generali. Per induzione su $n$ possiamo quindi supporre che $\mathbb{K}\{x_1, \dots, x_n\}$ sia fattoriale e quindi, che anche l'anello $\mathbb{K}\{x_1, \dots, x_n\}[t]$ sia un dominio a fattorizzazione unica.

Data $f \in \mathbb{K}\{x_1, \dots, x_n, t\}$ non nullo e non invertibile, ossia con $0 < \operatorname{ord}(f) < +\infty$. Tra tutti i modi di scrivere $f$ come prodotto di serie di ordine positivo scegliamone uno con il maggior numero di fattori (tale numero è dominato dall'ordine di $f$). I predetti fattori devono essere necessariamente irriducibili.

Per dimostrare che ogni irriducibile $f \in \mathbb{K}\{x_1, \dots, x_n, t\}$ è primo trattiamo prima il caso particolare in cui $f$ è uno pseudopolinomio in $t$; per il teorema di preparazione non è restrittivo supporre che $f$ sia un polinomio di Weierstrass e per il Lemma 1.4.4 $f$ è primo in $\mathbb{K}\{x_1, \dots, x_n, t\}$

Ogni isomorfismo di anelli trasforma irriducibili in irriducibili, e primi in primi. Nel caso generale basta quindi dimostrare che per ogni $0 \neq f \in \mathbb{K}\{x_1, \dots, x_n, t\}$ esiste un isomorfismo

$$\Phi^* \colon \mathbb{K}\{x_1, \dots, x_n, t\} \to \mathbb{K}\{y_1, \dots, y_n, t\}$$

tale che $\phi^*(f)$ sia uno pseudopolinomio in $t$. Sia $m = \operatorname{ord}(f)$ e scriviamo $f = f_m + \tilde{f}$ con $f_m$ omogeneo di grado $m$ e $\operatorname{ord}(\tilde{f}) > m$. Siccome $tf_m \neq 0$ e $\mathbb{K}$ è infinito, esiste un vettore $v \in \mathbb{K}^{n+1}$ tale che $v_{n+1} f_m(v) \neq 0$; allora la serie $f(y_1 + v_1 t, \dots, y_n + v_n t, v_{n+1} t)$, ottenuta da $f$ con un cambio lineare di coordinate, è uno pseudopolinomio in $t$ di grado esattamente $m$.

Nota: Se il campo $\mathbb{K}$ è finito si ripete lo stesso ragionamento usando però una sostituzione di indeterminate del tipo $x_i = y_i + t^{a_i}$ per opportuni interi positivi $a_1, \dots, a_n$ (vedi Esercizio 1.7). □

OSSERVAZIONE 1.4.6. Se $A$ è dominio di integrità, allora anche l'anello $A[[x_1, \dots, x_n]]$ delle serie formali a coefficienti in $A$ è un dominio di integrità. Invece, a differenza del caso polinomiale, se $A$ è un dominio a fattorizzazione unica, non è detto che anche $A[[x_1, \dots, x_n]]$ lo sia (i controesempi non sono banali).

### 1.4.1. Esercizi.

ESERCIZIO 1.2. Dimostrare che la serie $f(x, y) = x^2 - y^k \in \mathbb{C}\{x, y\}$ è irriducibile se e solo se $k$ è dispari.

ESERCIZIO 1.3. Dimostrare che la definizione di dominio a fattorizzazione unica data al precedente punto (3) coincide con quella più tradizionale in cui il punto (b) è sostituito con l'unicità della fattorizzazione, ossia:

(b') se $f_1 \cdots f_n = g_1 \cdots g_m$ con gli $f_i$ e $g_j$ irriducibili, allora $n = m$ ed a meno di permutazioni degli indici si ha che per ogni $i$ gli elementi $f_i$ e $g_i$ differiscono per moltiplicazione con un invertibile.

ESERCIZIO 1.4. Dimostrare che, per ogni intero dispari $\delta \geq 5$, nel sottoanello $\mathbb{Z}[i\sqrt{\delta}] \subseteq \mathbb{C}$ formato dai numeri complessi del tipo $a + ib\sqrt{\delta}$, con $a, b \in \mathbb{Z}$, il numero 2 è irriducibile ma non è primo. (Lo stesso vale anche per $\delta = 3$ ma la dimostrazione è più difficile. È invece noto dai corsi di algebra che l'anello $\mathbb{Z}[i]$ degli interi di Gauss è un dominio a fattorizzazione unica, ed infatti $2 = (1 + i)(1 - i)$ non è irriducibile.)

ESERCIZIO 1.5. Sia $A = \mathbb{C}[t^2, t^3] \subseteq \mathbb{C}[t]$ il sottoanello dei polinomi con il coefficiente di $t$ nullo. Provare che $A$ non è un dominio a fattorizzazione unica.

ESERCIZIO 1.6. Si consideri il sottoanello $A \subseteq \mathbb{C}[t] \times \mathbb{C}[t]$ formato dalle coppie $(p(t), q(t))$ tali che $p(0) = q(0)$; si noti che $A$ non è un dominio di integrità. Provare che $(t, 0)$ è primo ma non irriducibile in $A$.

ESERCIZIO 1.7. Dimostrare che per ogni $f \in \mathbb{K}\{y_1, \dots, y_n, t\}$ esistono $n$ interi positivi $a_1, \dots, a_n$ tali che la serie

$$g(x_1, \dots, x_n, t) = f(x_1 + t^{a_1}, \dots, x_n + t^{a_n}, t)$$

sia uno pseudopolinomio in $t$.

Nota: non si richiede che il campo $\mathbb{K}$ sia infinito. La sostituzione effettuata è reversibile, con inversa

$$f(y_1, \dots, y_n, t) = g(y_1 - t^{a_1}, \dots, y_n - t^{a_n}, t).$$

Suggerimento: siano $f = \sum_{h \geq 0} f_h(y)t^h$ e $S \subseteq \mathbb{N}^n$ l'unione dei supporti delle serie $f_h$; per il Lemma 1.1.6 esistono $n$ numeri razionali positivi $v_1, \dots, v_n$ tali che l'applicazione

$$\gamma \colon S \to \mathbb{Q}, \quad \gamma(j_1, \dots, j_n) = \sum_{p=1}^{n} v_p j_p,$$

possiede un unico punto $I = (i_1, \dots, i_n) \in S$ di minimo assoluto. Sia $d$ il più piccolo intero tale che $I \in \mathrm{Supp}(f_d)$. Dunque se $m_h = \min(\gamma(\mathrm{Supp}(f_h)))$ si ha $m_h \geq m_d$ per ogni $h > d$ e $m_h > m_d$ per ogni $h < d$. Sia $M > 0$ un intero tale che $Mv_i \in \mathbb{N}$ per ogni $i$ e $M(m_h - m_d) > d - h$ per ogni $h < d$. Provare che gli interi $a_i = Mv_i$ soddisfano la condizione richiesta.

Esercizio 1.9. Sia $\mathbb{K}$ il campo delle frazioni globali di un dominio a fattorizzazione unica $A$ e sia $f \in A$ irriducibile. Mostrare che esiste un'unica norma su $\mathbb{K}$ tale che $|f| = \dfrac{1}{2}$ e $|g| = 1$ per ogni $g \in A$ non divisibile per $f$.

Esercizio 1.10 ($*$). Provare che per ogni multiraggio $r > 0$, il sottoanello $B_r \subseteq \mathbb{C}\{x_1, \dots, x_n\}$ non è a fattorizzazione unica. (Sugg.: mostrare che esiste una catena non stazionaria di ideali principali.)