3 Formula di inversione di Möbius

Denotiamo con M l'*insieme delle funzioni aritmetiche moltiplicative*, diverse dalla funzione costante su 0. Abbiamo già notato che:

$$f \in M \Rightarrow f(1) = 1 \quad (\text{infatti, } f(n) = f(n \cdot 1) = f(n)f(1), \text{ con } n \geq 2)$$

quindi $M \subset A := \{f \ : \ f \text{ è una funzione aritmetica con } \ f(1) \neq 0\}$.

Proposizione 3.1. **(a)** *Presi comunque $f, g \in M$, allora $f * g \in M$.*
(b) *Siano $f, g \in A$. Se $f \in M$ e $f * g \in M$ allora $g \in M$.*
(c) *$(M, *)$ è un gruppo abeliano, sottogruppo di $(A, *)$.*

Dimostrazione. (a) La dimostrazione è del tutto simile a quella della Proposizione 1.4. Siano $n, m \in \mathbb{N}^+$ con $\text{MCD}(n, m) = 1$. Allora:

$$\begin{aligned}
[(f*g)(n)][(f*g)(m)] &= \left[\sum_{d|n} f(d)g\left(\frac{n}{d}\right)\right]\left[\sum_{d'|m} f(d')g\left(\frac{m}{d'}\right)\right] = \\
&= \sum_{d|n}\sum_{d'|m} f(d)f(d')g\left(\frac{n}{d}\right)g\left(\frac{m}{d'}\right) = \\
&= \sum_{dd'|nm} f(dd')g\left(\frac{nm}{dd'}\right) = \\
&= \sum_{e|nm} f(e)g\left(\frac{nm}{e}\right) = (f*g)(nm)
\end{aligned}$$

dove d (rispettivamente, d'; e) varia tra tutti i divisori positivi di n (rispettivamente, m; nm).

(b) Procediamo per assurdo: supponiamo che $g \notin M$. Siano $n, m \in \mathbb{N}^+$ con $\text{MCD}(n, m) = 1$ e con nm minimo in modo tale che $g(nm) \neq g(n)g(m)$.

Caso 1: $nm = 1$. Allora $n = m = 1$. In tal caso, si avrebbe che $g(1) \neq g(1)g(1)$ e, quindi, $g(1) \neq 1$. Pertanto:

$$(f * g)(1) = f(1)g(1) \neq f(1) = 1$$

e ciò è assurdo perché $f * g$ è moltiplicativa e quindi $(f * g)(1) = 1$.

Caso 2: $nm > 1$. Presi comunque $a, b \in \mathbb{N}^+$ con $\text{MCD}(a, b) = 1$ ed $ab < nm$, per la minimalità di nm, abbiamo che

$$g(ab) = g(a)g(b) \ .$$

D'altro lato

$$\begin{aligned}
(f*g)(nm) &= (g*f)(nm) = \sum_{\substack{a\,|n\\ b\,|m\\ ab\neq nm}} g(ab)f\left(\frac{nm}{ab}\right) + g(nm)f(1) = \\
&= \left(\sum_{\substack{a\,|n\\ a<n}} g(a)f\left(\frac{n}{a}\right)\right)\left(\sum_{\substack{b\,|m\\ b<m}} g(b)f\left(\frac{m}{b}\right)\right) + g(nm) = \\
&= \left(\sum_{a\,|n} g(a)f\left(\frac{n}{a}\right)\right)\left(\sum_{b\,|m} g(b)f\left(\frac{m}{b}\right)\right) - g(n)g(m) + g(nm) = \\
&= [(g*f)(n)][(g*f)(m)] - g(n)g(m) + g(nm) = \\
&= [(f*g)(n)][(f*g)(m)] - g(n)g(m) + g(nm)
\end{aligned}$$

Quindi, poiché $g(nm) - g(n)g(m) \neq 0$ si avrebbe che

$$(f*g)(nm) \neq [(f*g)(n)][(f*g)(m)]$$

e ciò è assurdo.

(c) Da (b) segue immediatamente che

$$f \in M \Rightarrow f^{-1} \in M$$

poiché $f * f^{-1} = u \in M$. Pertanto, M è un gruppo, sottogruppo di A (rispetto al prodotto di Dirichlet), infatti, da quanto sopra, si ricava immediatamente che:

$$f, g \in M \Rightarrow f * g^{-1} \in M \ .$$

□

Teorema 3.2. (R. Dedekind, 1857) **(a)** *L'applicazione:*

$$- * \mathbf{1} : A \longrightarrow A \ , \quad f \mapsto \sigma_f = f * \mathbf{1} \ ,$$

è una biiezione avente come inversa l'applicazione:

$$- * \mu : A \longrightarrow A \ , \quad F \mapsto F * \mu \ .$$

La restrizione di $- * \mathbf{1}$ *ad* M*, cioè:*

$$- * \mathbf{1} : M \to M \ , \quad f \mapsto f * \mathbf{1} \ ,$$

è anch'essa una biiezione avente come inversa l'applicazione:

$$- * \mu : M \to M \ , \quad F \mapsto F * \mu \ .$$

(b) ***(Formula di inversione di A.F. Möbius).*** *Presa comunque una funzione $F \in A$ (rispettivamente, $F \in M$) esiste un'unica funzione $f \in A$ (rispettivamente, $f \in M$) tale che:*

$$F(n) = \sum_{d|n} f(d) \ , \quad \text{per ogni } n \in \mathbb{N}^+ \ .$$

Tale funzione f è tale che

$$f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) \ , \quad \text{per ogni } n \in \mathbb{N}^+ \ .$$

Dimostrazione. (a) discende immediatamente dal fatto $\mathbf{1} * \mu = u$ (Proposizione 2.3) e dal fatto che, se $f, F \in M$, allora $f * \mathbf{1}$ e $F * \mu$ appartengono ancora ad M (Proposizione 3.1(a)).

(b) è una semplice riformulazione di (a).

□

3 Esercizi e Complementi

3.1. Sia $n \geq 1$. Un numero complesso del tipo $z = \cos\alpha + i \sin\alpha = e^{i\alpha}$, con $\alpha \in \mathbb{R}$, è detto una *radice n–esima dell'unità* se $z^n = 1$ ed è detto una *radice n–esima primitiva dell'unità* se, inoltre, $z^k \neq 1$ per $1 \leq k \leq n-1$. È ben noto che $\zeta_n := e^{\frac{2\pi i}{n}}$ è una radice primitiva n–esima dell'unità. Nel seguito porremo, per semplicità, ζ al posto di ζ_n, qualora ciò non sia causa di ambiguità. È subito visto che:

$$\{\zeta^k : 1 \leq k \leq n \text{ e } \mathrm{MCD}(k,n) = 1\}$$

coincide con l'insieme delle radici primitive n–esime dell'unità.

Il polinomio nell'indeterminata X (a coefficienti — a priori — complessi)

$$\Phi_n(X) := \prod_{\substack{1 \leq k \leq n \\ \mathrm{MCD}(k,n)=1}} (X - \zeta^k)$$

è detto *n–esimo polinomio ciclotomico*. Esso ha grado $\varphi(n)$ ed ha ovviamente come radici (nel campo $\mathbb{C}$ dei numeri complessi) tutte e sole le radici primitive n–esima dell'unità (le quali sono tra loro distinte e sono in numero di $\varphi(n)$).

Utilizzando opportunamente la formula di inversione di Möbius, mostrare che, per ogni $n \geq 1$:

(a) $$\mu(n) = \sum_{\substack{1 \leq k \leq n \\ \mathrm{MCD}(k,n)=1}} \zeta^k \ ;$$

(b) $$X^n - 1 = \prod_{d|n} \Phi_d(X) \quad \text{e} \quad \Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} \ ;$$

(c) Dedurre da (b) che $\Phi_n(X) \in \mathbb{Z}[X]$.

[*Suggerimento*. (a) Per ogni $n \geq 1$, poniamo:

$$f(n) := \sum_{\substack{1 \leq k \leq n \\ \mathrm{MCD}(k,n)=1}} \zeta^k \in \mathbb{C} \ .$$

Allora, $F(n) := \sum_{d|n} f(d)$ è la somma di *tutte* le radici n–esime dell'unità (cioè di tutte le radici del polinomio $X^n - 1$), quindi:

$$F(n) = \sum_{k=1}^{n} \zeta^k = \sum_{k=1}^{n} e^{\frac{2\pi k i}{n}} = \left\{ \begin{array}{l} 0, \text{ se } n > 1 \\ 1, \text{ se } n = 1 \end{array} \right\} = u(n)$$

(essendo la somma di tutte le radici di un polinomio monico di grado $n \geq 1$ a coefficienti complessi uguale all'opposto del coefficiente del termine di grado $n-1$). Pertanto $F = f * \mathbf{1} = u$, dunque $\mu = \mu * u = f$.

(b) Dal momento che le radici di $X^n - 1$ sono le radici di un polinomio $\Phi_d(X)$ per un qualche $d \mid n$, si ha:

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

cioè

$$\log(X^n - 1) = \sum_{d|n} \log \Phi_d(X) \ .$$

da cui ricaviamo che:

$$\log \Phi_n(X) = \sum_{d|n} \mu(d) \log(X^{\frac{n}{d}} - 1)$$

e dunque:

$$\Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} \ .$$

(c) è una conseguenza immediata di (b).]

3.2. Sia $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ la fattorizzazione in primi irriducibili di $n \geq 2$ (con $e_i \geq 1$ per $1 \leq i \leq r$). Sia $t \in \mathbb{C}$ fissato. Si definisca:

$$\omega_t(n) := \begin{cases} 1 & \text{se } n = 1; \\ t^r, & \text{altrimenti} \ . \end{cases}$$

Mostrare che:

(a) $\omega_t : \mathbb{N}^+ \to \mathbb{C}$ è una funzione moltiplicativa.

(b) $\sum_{d|n} \omega_t(d) = \sum_{i=1}^{r} (1 + e_i t)$.

[*Dimostrazione*. (a) è di immediata verifica. (b) Essendo ω_t una funzione moltiplicativa anche σ_{ω_t} è una funzione moltiplicativa. È facile verificare che, per ogni primo p e per ogni intero $e \geq 1$, si ha:

$$\sigma_{\omega_t}(p^e) = \sum_{d|p^e} \omega_t(d) = 1 + \underbrace{t + \cdots + t}_{e\text{–volte}} = 1 + et \ .]$$

3.3. Sia $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ la decomposizione di $n \geq 2$ (con $e_i \geq 1$ per $1 \leq i \leq r$) come prodotto di fattori primi distinti. Sia t un numero complesso fissato. Si ponga

$$\lambda_t(n) := \begin{cases} 1, & \text{se } n = 1; \\ t^{\left(\sum_{i=1}^{r} e_i\right)}, & \text{altrimenti} \ . \end{cases}$$

Mostrare che:

(a) $\lambda_t : \mathbb{N}^+ \to \mathbb{C}$ è una funzione totalmente moltiplicativa.

(b) $\sum_{d|n} \lambda_t(d) = \sum_{i=1}^{r} \frac{(t^{e_i+1}-1)}{(t-1)}$.

[*Dimostrazione*. (a) è di verifica immediata. (b) Poiché λ_t è totalmente moltiplicativa, σ_{λ_t} è moltiplicativa. Non è difficile assicurarsi che:

$$\sigma_{\lambda_t}(p^e) = \sum_{d|p^e} \sigma_{\lambda_t}(d) = 1 + t + t^2 + \cdots + t^e = \frac{t^{e+1}-1}{t-1} \ .]$$

3.4. (Funzione di J. Liouville).
Si consideri la funzione introdotta nell'Esercizio 3.3 per $t = -1$. Si chiama *funzione di Liouville* la funzione totalmente moltiplicativa

$$\lambda(n) := \begin{cases} 1, & \text{se } n = 1; \\ (-1)^{\left(\sum_{i=1}^{r} e_i\right)}, & \text{altrimenti;} \end{cases}$$

dove $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ è la fattorizzazione in primi distinti di $n \geq 2$ (con $e_i \geq 1$ per $1 \leq i \leq r$). Mostrare che:

(a) $\sum_{d|n} \lambda(d) = \begin{cases} 1, & \text{se } n \text{ è un quadrato;} \\ 0, & \text{altrimenti;} \end{cases}$

(b) $\lambda^{-1} = \mu\lambda = |\mu|$;

(c) $\sum_{d|n} \lambda^{-1}(d) = \begin{cases} 1, & \text{se } n = 1; \\ 2^r, & \text{altrimenti .} \end{cases}$

[*Suggerimento:* (a) Osserviamo che σ_λ è una funzione moltiplicativa perché λ è una funzione totalmente moltiplicativa. Notiamo anche che n è un quadrato se e soltanto se e_i è pari, per ogni $1 \leq i \leq r$.

Inoltre, per ogni primo p e per ogni intero $e \geq 1$, abbiamo

$$\sigma_\lambda(p^e) = 1 + (-1) + 1 + \cdots + (-1)^e = \begin{cases} 1, & \text{se } e \text{ è pari;} \\ 0, & \text{se } e \text{ è dispari .} \end{cases}$$

(b) Poiché λ è totalmente moltiplicativa, $\lambda^{-1}(n) = \mu(n)\lambda(n)$ per ogni $n \in \mathbb{N}^+$ (Proposizione 2.10). Si noti che

$$\mu(n)\lambda(n) = \left\{ \begin{array}{ll} 1, & \text{se } n = 1 \\ (-1)^r \cdot (-1)^r, & \text{se } e_i = 1, \ \forall\, i \\ 0 \cdot (-1)^{\left(\sum_{i=1}^{r} e_i\right)}, & \text{altrimenti} \end{array} \right\} = \mu(n)\mu(n) = |\mu(n)|$$

(c) Da (b) sappiamo che $\lambda^{-1} = |\mu|$ è una funzione moltiplicativa. Inoltre, per ogni primo p e per ogni intero $e \geq 1$, abbiamo:

$$\sigma_{\lambda^{-1}}(p^e) = \sigma_{|\mu|}(p^e) = 1 + |\mu(p)| = 2 \ .$$

Si noti che $\sigma_{\lambda^{-1}} = \omega_2$ (funzione definita nell'Esercizio 3.2 per $t = 2$), cioè, per ogni $n \geq 1$,

$$\sum_{d|n} \lambda^{-1}(d) = \omega_2(n) \ .$$

n	1	2	3	4	5	6	7	8	9	10	11	12	...
$\lambda(n)$	1	-1	-1	1	-1	1	-1	-1	1	1	-1	-1	...
$\sigma_\lambda(n)$	1	0	0	1	0	0	0	0	1	0	0	0	...
$\lambda^{-1}(n)$	1	1	1	0	1	1	1	0	0	1	1	0	...
$\sigma_{\lambda^{-1}}(n)$	1	2	2	2	2	4	2	2	2	4	2	4	...