

DIARIO/NOTE DEL CORSO DI ANALISI DI FOURIER DISCRETA

DOCENTE: SANDRO MATTAREI

(I riquadri costituiscono il diario del corso tenuto nell'anno accademico 2005/06, e di norma precedono gli argomenti svolti nella lezione corrispondente. Sono state tenute complessivamente 40 ore di lezione.)

Prima settimana. Lezione di lunedì 12 settembre 2005 (due ore): Introduzione al corso mediante esempi: cenni alle serie di Fourier; decomposizione di uno spazio di funzioni in funzioni pari e dispari.

ESEMPI INTRODUTTIVI

0.1. Cenni alle serie di Fourier. [Questo argomento verrà ripreso ed approfondito in seguito.] Sia f una funzione reale di variabile reale, periodica di periodo 2π . (Se f è periodica di periodo T , ci si può ridurre a questo caso mediante una *dilatazione*, cioè rimpiazzando f con g data da $g(t) = f(t \cdot 2\pi/T)$.) Sotto opportune condizioni su f , questa si può esprimere come

$$f(t) = \frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \cos(kt) + b_k \sin(kt)),$$

da interpretare opportunamente, dove

$$a_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \cos(kt) dt, \quad b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \sin(kt) dt.$$

Qui ci concentreremo sull'aspetto algebrico, lasciando i problemi di convergenza ad altri corsi. Usando il fatto che $e^{ikt} = \cos(kt) + i\sin(kt)$ e ponendo $c_k = (a_k - ib_k)/2$ e $c_{-k} = (a_k + ib_k)/2$ (dove $b_0 = 0$) otteniamo l'espressione piú compatta ed elegante

$$f(t) = \sum_{k=-\infty}^{\infty} c_k e^{ikt}.$$

La sequenza di coefficienti c_k , pensata come funzione di k (quindi definita sugli interi), è la *trasformata di Fourier* di f . Indicando quest'ultima con la notazione \hat{f} (o talvolta $\mathcal{F}(f)$), vale a dire ponendo $\hat{f}(k) = c_k$ per $k \in \mathbb{Z}$, la situazione si riassume nelle formule

$$f(t) = \sum_{k=-\infty}^{\infty} \hat{f}(k) e^{ikt}, \quad \text{dove} \quad \hat{f}(k) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(t) e^{-ikt} dt.$$

Visto che queste coinvolgono numeri complessi, è piú naturale ammettere che f possa essere una funzione a valori complessi, cioè $f : \mathbb{R} \rightarrow \mathbb{C}$. Anzi, poiché ci limitiamo a funzioni f periodiche, possiamo anche pensare f come $f : \mathbb{R}/2\pi\mathbb{Z} \rightarrow \mathbb{C}$. La funzione $\hat{f} : \mathbb{Z} \rightarrow \mathbb{C}$ è la *trasformata di Fourier* di f , ed f è l'*antitrasformata di Fourier* di \hat{f} .

Facciamo alcune osservazioni, che approfondiremo in seguito.

Date: A. A. 2005/06. Aggiornato il 28 luglio 2006.

Osservazione. Le formule che danno la trasformata \hat{f} di f , e l'antitrasformata f di \hat{f} , sono molto simili, a parte

- (1) il coefficiente $1/2\pi$ nella seconda (che si potrebbe far in modo di eliminare),
- (2) la presenza di e^{ikt} nella prima e del suo inverso e^{-ikt} nella seconda (questo è intrinseco e non eliminabile),
- (3) l'uso di una serie nella prima e di un integrale nella seconda (ma questi sono concetti analoghi, la serie altro non è che un integrale sull'insieme \mathbb{Z} dotato della misura discreta).

Osservazione. Dunque trasformata e antitrasformata sono essenzialmente date dalla stessa formula, solo che le due funzioni sono definite su spazi diversi (in questo caso), $\mathbb{R}/2\pi\mathbb{Z}$ e \mathbb{Z} . Si noti che oltre che spazi con misura, questi sono gruppi (anzi, gruppi topologici). Come gruppi, essi sono uno il *duale* dell'altro. Approfondiremo questo in seguito.

Osservazione. La struttura di gruppo è utilizzata in modo essenziale nella definizione di trasformata di Fourier, e la distingue da decomposizioni di f rispetto ad un sistema ortonormale completo (o base topologica) qualsiasi per lo spazio delle funzioni considerate. Le funzioni $t \mapsto e^{ikt}$ in cui abbiamo scelto di decomporre f , sono i *caratteri* di $\mathbb{R}/2\pi\mathbb{Z}$, cioè gli omomorfismi di gruppo $\mathbb{R}/2\pi\mathbb{Z} \mapsto \mathbb{C}^*$ (anzi, $\mathbb{R}/2\pi\mathbb{Z} \mapsto \mathbb{T}$, dove $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$). (Il punto è che i caratteri sono esattamente le *autofunzioni* per l'azione naturale del gruppo G su $L^2(G)$, un fatto che riprenderemo in seguito.)

Osservazione. Nel calcolo numerico dei coefficienti di una serie di Fourier bisogna discretizzare lo spazio $\mathbb{R}/2\pi\mathbb{Z}$ su cui è definita f , e quindi rimpiazzare l'integrale con una somma. In pratica $\mathbb{R}/2\pi\mathbb{Z}$ viene diviso in n intervalli della stessa lunghezza $2\pi/n$, e quindi rimpiazzato con la sua versione discreta $(2\pi/n)\mathbb{Z}/2\pi\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$. Avendo rimpiazzato il gruppo $\mathbb{R}/2\pi\mathbb{Z}$ con un suo *sottogruppo* (il suo unico sottogruppo di *ordine* n , in questo caso), il suo gruppo duale \mathbb{Z} viene rimpiazzato con un suo *gruppo quoziente* (il suo unico sottogruppo di *indice* n , cioè $\mathbb{Z}/n\mathbb{Z}$). Riprenderemo anche questo in seguito, ma per ora pensiamo alle forti analogie con la teoria dello spazio duale in algebra lineare: a sottospazi di uno spazio vettoriale corrispondono spazi quoziente dello spazio duale, e viceversa.

0.2. Decomposizione di funzioni in parti pari e dispari. Ogni $f : \mathbb{R} \rightarrow \mathbb{R}$ si decompone in modo unico nella somma di una funzione pari f_+ e di una funzione dispari f_- :

$$f = f_+ + f_-, \quad \text{dove} \quad \begin{cases} f_+(x) = \frac{1}{2}(f(x) + f(-x)) \\ f_-(x) = \frac{1}{2}(f(x) - f(-x)) \end{cases}$$

Qui c'è sotto (anche se un po' nascosta) una trasformata di Fourier sul gruppo ciclico con due elementi. Almeno dovrete riconoscere $e^{2\pi ai/2} = \pm 1$, per $a = \mathbb{Z}/2\mathbb{Z}$, nei coefficienti di $f(x)$ e $f(-x)$, e l'ordine del gruppo nel 2 ai denominatori.

Esercizio 1. Consideriamo l'applicazione lineare $L : \mathbb{R}^{\mathbb{R}} \rightarrow \mathbb{R}^{\mathbb{R}}$, dello spazio delle funzioni reali di variabile reale in se stesso, definita da $(Lf)(x) = (2f(x) + f(-x))/3$ per $x \in \mathbb{R}$. Per n intero positivo indichiamo con L^n , come è naturale, la n -esima iterata di L rispetto alla composizione. Dimostrate che $L^n f$ tende a f_+ (nel senso della convergenza puntuale) per $n \rightarrow \infty$.

(Suggerimento: Notate che le funzioni pari e quelle dispari sono tutte autovettori per l'operatore L , e notate i corrispondenti autovalori.)

Lezione di venerdì 16 settembre 2005 (due ore): Lo spazio di Hilbert $L^2(G)$, dove $G = \mathbb{Z}/n\mathbb{Z}$. Convulsione in $L^2(G)$.

1. LA TRASFORMATA DI FOURIER SU $\mathbb{Z}/n\mathbb{Z}$

1.1. **Lo spazio $L^2(\mathbb{Z}/n\mathbb{Z})$.** Inizieremo studiando la trasformata di Fourier sul gruppo ciclico di ordine n . Conviene prendere $G = \mathbb{Z}/n\mathbb{Z}$ come una delle tante realizzazioni di tale gruppo, ma ne ricordiamo un'altra: l'insieme

$$U_n = \{z \in \mathbb{C} : z^n = 1\} = \{e^{2\pi ia/n} : a = 0, \dots, n-1\}$$

delle radici n -esime dell'unità in \mathbb{C} è un gruppo ciclico di ordine n , quindi isomorfo a G . Un isomorfismo di G su U_n è ad esempio $x + n\mathbb{Z} \mapsto e^{2\pi ix/n}$.

Esercizio 2. Determinate tutti gli omomorfismi di gruppi $\mathbb{Z}/n\mathbb{Z} \rightarrow U_n$. Quanti e quali di essi sono isomorfismi?

Possiamo anche vedere questi isomorfismi come $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}^*$. Esistono altri omomorfismi $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}^*$ oltre a questi?

Determinate tutti gli omomorfismi di gruppi $\mathbb{Z} \rightarrow \mathbb{C}^*$. Quali di questi hanno immagine in $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$?

Lo spazio $L^2(G) = \{f : G \rightarrow \mathbb{C}\}$ delle funzioni su G a valori complessi è spazio di Hilbert (di dimensione n) con il prodotto scalare (o, meglio, Hermitiano) $\langle f, g \rangle := \sum_{x \in G} f(x)\overline{g(x)}$. Esso induce la norma $\|f\| = \|f\|_2 = \langle f, f \rangle^{1/2}$.

Osservazione. La notazione $L^2(G)$ è quella standard per lo spazio delle funzioni di quadrato integrabile sullo spazio G . Qui G è dotato della misura discreta, cioè ogni sottoinsieme è misurabile e la sua misura coincide con la sua cardinalità. Essendo G finito, in questo caso $L^2(G) = L^1(G) = L^\infty(G) = \dots$ coincidono con l'intero spazio \mathbb{C}^G . (Le corrispondenti norme $\|\cdot\|_2, \|\cdot\|_1, \|\cdot\|_\infty, \dots$, sono diverse, ma naturalmente tutte equivalenti (cioè inducono la stessa topologia su \mathbb{C}^G), essendo \mathbb{C}^G uno spazio di dimensione finita [Ter, p. 104].)

Osservazione. Una scelta alternativa, piú conveniente per certi motivi che si capiranno in seguito, sarebbe dare a G misura 1, nel qual caso $\langle f, g \rangle$ sarebbe $\frac{1}{n} \sum_{x \in G} f(x)\overline{g(x)}$.

Se v_1, \dots, v_n è una base ortonormale di $L^2(G)$ allora ogni $f \in L^2(G)$ si scrive $f = \sum_{i=1}^n \langle f, v_i \rangle v_i$. Le funzioni delta δ_i definite da

$$\delta_i(j) = \begin{cases} 1 & \text{se } i = j \text{ (ovvero se } i \equiv j \pmod{n}, \text{ pensando } i, j \text{ come interi)} \\ 0 & \text{altrimenti} \end{cases}$$

per $i \in G$ (o, in modo meno rigoroso, per $i = 0, \dots, n-1$) formano una base ortonormale di $L^2(G)$, ed infatti $f = \sum_{i \in G} \langle f, \delta_i \rangle \delta_i = \sum_{i \in G} f(i) \delta_i$.

1.2. **Convulsione.** La *convulsione* di $f, g \in L^2(G)$ è $f * g \in L^2(G)$ definita da

$$(f * g)(x) = \sum_{y \in G} f(y)g(x-y).$$

Esercizio 3. Mostrate che la convulsione di funzioni è commutativa ed associativa.

Osservazione. Piú in generale, si può eseguire la convulsione di funzioni definite su un gruppo arbitrario G , anche non commutativo. Scrivendo l'operazione del gruppo in notazione moltiplicativa, la convulsione di f e g sarà data dalla formula $(f * g)(x) = \sum_{y \in G} f(y)g(y^{-1}x)$.

Esempi di convoluzione: $\delta_a * \delta_b = \delta_{a+b}$; $(f * \delta_a)(x) = f(x - a)$.

Data $f \in L^2(G)$ definiamo la *funzione riflessa* f° ponendo $f^\circ(x) := f(-x)$. Allora vale

$$(f * g)^\circ = f^\circ * g^\circ.$$

C'era da aspettarselo, ciò rispecchia il fatto che la mappa che manda ciascun elemento di un gruppo commutativo nel suo inverso è un automorfismo (il che è falso per gruppi non commutativi).

Seconda settimana. Lezione di lunedì 19 settembre 2005 (tre ore):

La moltiplicazione di polinomi come convoluzione dei coefficienti. Esempi di applicazione al metodo delle funzioni generatrici.

1.3. Un'analogia: moltiplicazione di polinomi come convoluzione. Un esempio di convoluzione visto al primo anno è la moltiplicazione di polinomi (o, piú in generale, serie formali, o anche polinomi o serie di Laurent) in una variabile:

$$\left(\sum_i a_i x^i\right) \left(\sum_j b_j x^j\right) = \sum_i (a * b)_i x^i,$$

dove la sequenza dei coefficienti del prodotto è la convoluzione $(a * b)_i = \sum_j a_j b_{i-j}$ delle sequenze dei coefficienti dei fattori (pensate come funzioni $i \mapsto a_i$ definite sul gruppo additivo \mathbb{Z}).

La corrispondenza

$$\left\{\text{funzione polinomiale: } x \mapsto \sum_i a_i x^i\right\} \rightarrow \left\{\text{sequenza dei coefficienti: } i \mapsto a_i\right\}$$

è molto simile ad una trasformata di Fourier, e come essa trasforma moltiplicazioni di funzioni in convoluzioni. Questa è una delle ragioni del successo del metodo delle *funzioni generatrici*, in varie parti della matematica. Verso la fine del corso riprenderemo l'interpretazione della moltiplicazione di polinomi come trasformata di Fourier, usando un po' di analisi complessa. (Vedremo cosí anche un legame fra serie di Fourier e serie di Taylor).

Esempio. I coefficienti binomiali $\binom{n}{k}$ possono essere definiti dall'identità binomiale $(1+x)^n = \sum_{i \geq 0} \binom{n}{i} x^i$; in altre parole, questa è la loro *funzione generatrice*.

Problema: esiste un'espressione piú semplice per la somma $\sum_i \binom{n}{i} \binom{m}{k-i}$, in funzione di n , m e k ?

Soluzione: Si sta chiedendo di calcolare la convoluzione delle funzioni $i \mapsto \binom{n}{i}$ e $j \mapsto \binom{m}{j}$. Per farlo, basta moltiplicare le loro funzioni generatrici. Infatti,

$$\begin{aligned} \sum_k \left(\sum_i \binom{n}{i} \binom{m}{k-i}\right) x^k &= \sum_i \binom{n}{i} x^i \left(\sum_k \binom{m}{k-i} x^{k-i}\right) = \left(\sum_i \binom{n}{i} x^i\right) \left(\sum_j \binom{m}{j} x^j\right) \\ &= (1+x)^n (1+x)^m = (1+x)^{m+n} = \sum_k \binom{m+n}{k} x^k, \end{aligned}$$

e quindi $\sum_i \binom{n}{i} \binom{m}{k-i} = \binom{m+n}{k}$.

Esercizio 4. Il coefficiente binomiale $\binom{n}{k}$ ha l'interpretazione combinatoria come numero dei sottoinsiemi di cardinalità k di un insieme di cardinalità n . Infine, per $n, k \geq 0$ abbiamo $\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{1 \cdot 2 \cdots k} = \frac{n!}{k!(n-k)!}$. Mettete in relazione le tre interpretazioni viste (come coefficiente di $(1+x)^n$, quella combinatoria, e l'espressione esplicita appena scritta), mostrando come mostrare ognuna partendo da ciascuna delle altre due.

Esercizio 5. Dimostrate le identità fondamentali $\binom{n}{n-k} = \binom{n}{k}$ e $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$, possibilmente partendo da ciascuna delle tre interpretazioni dei coefficienti binomiali.

Esercizio 6. Mostrate che $\sum_k \binom{n}{k} = 2^n$ e che $\sum_k (-1)^k \binom{n}{k} = 0$.

Esercizio 7. Usando l'identità dell'esempio, mostrate che $\sum_k \binom{n}{k}^2 = \binom{2n}{n}$.

Esercizio 8. Trovate una dimostrazione combinatoria dell'identità (convoluzione di Vandermonde) $\sum_j \binom{n}{j} \binom{m}{k-j} = \binom{m+n}{k}$.

Lezione di venerdì 23 settembre 2005 (tre ore): La trasformata di Fourier su $\mathbb{Z}/n\mathbb{Z}$. Le sue proprietà principali, con varie dimostrazioni.

1.4. **La trasformata di Fourier discreta.** Per $a, x \in \mathbb{Z}/n\mathbb{Z}$ è ben definita

$$e_a(x) = \exp(2\pi i ax/n).$$

Al variare di $a \in \mathbb{Z}/n\mathbb{Z}$, le mappe $e_a : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{T}$ sono tutti gli omorfismi di gruppi da $\mathbb{Z}/n\mathbb{Z}$ in \mathbb{T} (o, equivalentemente, in \mathbb{C}^*), cioè i *caratteri* del gruppo $\mathbb{Z}/n\mathbb{Z}$.

Osservazione. L'insieme dei caratteri di $\mathbb{Z}/n\mathbb{Z}$ è indicato con $\widehat{\mathbb{Z}/n\mathbb{Z}}$ (ma in altri contesti sono in uso anche altre notazioni, come $X(\mathbb{Z}/n\mathbb{Z})$ o $\text{Irr}(\mathbb{Z}/n\mathbb{Z})$). Il prodotto di due caratteri (come funzioni su $\mathbb{Z}/n\mathbb{Z}$, cioè il prodotto puntuale $(e_a e_b)(x) := e_a(x)e_b(x)$) è un carattere, e $\widehat{\mathbb{Z}/n\mathbb{Z}}$ è a sua volta un gruppo, il *gruppo duale* di $\mathbb{Z}/n\mathbb{Z}$. È isomorfo a $\mathbb{Z}/n\mathbb{Z}$, ed un isomorfismo è dato dalla mappa $\mathbb{Z}/n\mathbb{Z} \rightarrow \widehat{\mathbb{Z}/n\mathbb{Z}}$ tale che $a \mapsto e_a$. (Notate il ruolo simmetrico di a ed x nella formula che definisce $e_a(x) = e_1(ax)$, per cui $e_a e_b = e_{a+b}$.)

Per sottolineare il ruolo diverso di $\widehat{\mathbb{Z}/n\mathbb{Z}}$ in sé dalla copia isomorfa che usiamo per rappresentare il suo duale $\widehat{\widehat{\mathbb{Z}/n\mathbb{Z}}}$ secondo l'isomorfismo $a \mapsto e_a$, cercheremo (almeno inizialmente, e diversamente da [Ter]) di usare le lettere x, y, z, \dots per gli elementi del primo, e le lettere a, b, c, \dots per il secondo, come esemplificato dalla scrittura $e_a(x)$.

La *trasformata di Fourier discreta* (o *DFT*) di $f \in L^2(\mathbb{Z}/n\mathbb{Z})$ è la funzione $\mathcal{F}f \in L^2(\widehat{\mathbb{Z}/n\mathbb{Z}})$, scritta anche \hat{f} , data da

$$\mathcal{F}f(a) = \hat{f}(a) = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} f(x)e_a(-x) = \langle f, e_a \rangle$$

Un esempio importante di trasformata di Fourier $\mathcal{F}\delta_x(a) = e_a(-x)$, cioè $\mathcal{F}\delta_x = e_{-x}$; in particolare, $\mathcal{F}\delta_0 = 1$ (la funzione costante 1).

Osservazione. Qui anche $\mathcal{F}f$ appartiene a $L^2(\mathbb{Z}/n\mathbb{Z})$, come f , ma anticipo che in generale la trasformata di Fourier di una funzione sul gruppo abeliano G è una funzione sul gruppo duale \hat{G} . Quindi sarebbe più corretto considerare $\mathcal{F}f$ come un elemento di $L^2(\widehat{\mathbb{Z}/n\mathbb{Z}})$, scrivendo quindi $\mathcal{F}f(e_a) = \langle f, e_a \rangle$ anziché $\mathcal{F}f(a) = \langle f, e_a \rangle$. Ad esempio, la trasformata di δ_x appena vista, che abbiamo scritto come $e_{-x} \in \hat{G}$, e quindi una funzione su G , è in realtà una funzione su \hat{G} , la "valutazione" (del generico carattere $e_a \in \hat{G}$) sull'elemento $-x$ di G .

Lemma (Ortogonalità dei caratteri di $\mathbb{Z}/n\mathbb{Z}$).

$$\langle e_a, e_b \rangle = \begin{cases} n & \text{se } a \equiv b \pmod{n}, \\ 0 & \text{altrimenti.} \end{cases}$$

In altre parole, le funzioni $n^{-1/2}e_a$ per $a \in \mathbb{Z}/n\mathbb{Z}$ formano una base ortonormale per $L^2(\mathbb{Z}/n\mathbb{Z})$.

Dimostrazione. Conviene porre $\omega := e_1(1) = e^{2\pi i/n}$, e quindi avremo $e_a(x) = \omega^{ax}$. Notiamo anche che il coniugato di un numero complesso di modulo uno è il suo inverso, per cui $\overline{e_b(x)} = e_b(-x)$. (Questa osservazione estende il significato e la validità del Lemma a campi diversi da \mathbb{C} .) Avremo quindi

$$\langle e_a, e_b \rangle = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} e_a(x)e_b(-x) = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \omega^{ax}\omega^{-bx} = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \omega^{(a-b)x}.$$

Se $a \equiv b \pmod{n}$ allora $\omega^{(a-b)} = 1$, e quindi $\langle e_a, e_b \rangle = n$. Altrimenti, moltiplichiamo la somma per $\omega^{a-b} \neq 1$, ottenendo

$$\omega^{a-b} \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \omega^{(a-b)x} = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \omega^{(a-b)(x+1)} = \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \omega^{(a-b)y},$$

e quindi $\sum_{x \in \mathbb{Z}/n\mathbb{Z}} \omega^{(a-b)x} = 0$. □

Osservazione. Essendo

$$\langle e_a, e_b \rangle = \sum_x e_a(x)e_b(-x) = \sum_x e_a(x)e_{-b}(x) = \sum_x e_{a-b}(x) = \langle e_{a-b}, e_0 \rangle$$

potevamo anche calcolare il caso speciale $\langle e_a, e_0 \rangle$ e poi dedurne il caso generale.

Esercizio 9. Talvolta, in situazioni piú generali (e meno ovvie), la relazione di ortogonalità contenuta nel Lemma è detta *prima relazione di ortogonalità*. A partire da questa dimostrate la *seconda relazione di ortogonalità*, dove i ruoli di a ed x (vale a dire di G e \hat{G}) sono scambiati:

$$\sum_x e_a(x)e_a(-y) = \begin{cases} n & \text{se } x \equiv y \pmod{n}, \\ 0 & \text{altrimenti.} \end{cases}$$

Esercizio 10. Il passo cruciale della dimostrazione del Lemma è il fatto che se ω è una radice n -esima primitiva dell'unità in \mathbb{C} (o anche in un campo qualsiasi), allora $\sum_j \omega^{ij}$ vale n se $n \equiv 0 \pmod{n}$ (cioè se $\omega^i = 1$), e zero altrimenti. Date un'altra dimostrazione di questo fatto, basandovi sull'identità $\sum_{i=0}^{n-1} x^i = (1-x^n)/(1-x)$ (cioè la formula per sommare una progressione geometrica).

Osservazione. Piú in generale, omomorfismi distinti di un gruppo arbitrario nel gruppo moltiplicativo \mathbb{F}^* di un campo \mathbb{F} sono funzioni linearmente indipendenti su \mathbb{F} .

Un'applicazione del Lemma è che $\mathcal{F}e_x(a) = n\delta_x(a)$, cioè $\mathcal{F}e_x = n\delta_x$; in particolare, $\mathcal{F}1 = n\delta_0$.

Teorema (Proprietà fondamentali della trasformata di Fourier su $G = \mathbb{Z}/n\mathbb{Z}$).

- (1) $\mathcal{F} : L^2(G) \rightarrow L^2(G)$ è una mappa lineare biettiva.
- (2) *Convoluzione:* $\mathcal{F}(f * g)(x) = \mathcal{F}f(x)\mathcal{F}g(x)$ per ogni $x \in G$.
- (3) *Inversione:*

$$f(x) = \frac{1}{n} \mathcal{F}\mathcal{F}f(-x) = \frac{1}{n} \sum_{a \in G} \hat{f}(a)e_a(x).$$

- (4) *Teorema di Plancherel, o Uguaglianza di Parseval:* $\langle f, f \rangle = \frac{1}{n} \langle \hat{f}, \hat{f} \rangle$. Piú in generale, vale $\langle f, g \rangle = \frac{1}{n} \langle \hat{f}, \hat{g} \rangle$.

Osservazione. Notate che $L^2(G)$ diventa un anello (anzi, una \mathbb{C} -algebra, essendo anche un \mathbb{C} -spazio vettoriale) in due modi diversi, a seconda che scegliamo come moltiplicazione la moltiplicazione ordinaria (cioè puntuale) di funzioni, o la convoluzione. La proprietà (2), assieme alla linearità, ci dice che \mathcal{F} è un isomorfismo di \mathbb{C} -algebre (cioè di spazi vettoriali ma anche di anelli) fra $L^2(G)$ con la convoluzione e $L^2(G)$ (o meglio, a rigore, $L^2(\hat{G})$) con la moltiplicazione puntuale di funzioni.

Osservazione. La proprietà (3), ovvero la *formula di inversione*, che possiamo scrivere in modo più compatto come $f = \frac{1}{n} \sum_{a \in G} \hat{f}(a) e_a$, ci dice che, a parte la costante moltiplicativa $1/n$ (che non compare qui in altre normalizzazioni), $\mathcal{F}f(a) = \hat{f}(a)$ è il coefficiente di e_a nella *decomposizione di Fourier* di f come combinazione lineare dei caratteri di G . Ma c'è anche un'altro aspetto importante: la formula che esprime tale coefficiente (cioè la formula dell'*antitrasformata di Fourier*) è quasi la stessa che per la trasformata stessa, a parte il coefficiente $1/n$ ed il $-x$ al posto di x . In altre parole, la composta $\mathcal{F} \circ \mathcal{F}$ è quasi l'applicazione identica, trasformando $f(x)$ in $nf(-x)$. Si confronti con un'osservazione analoga fatta in precedenza nel caso delle serie di Fourier.

Osservazione. Talvolta si chiama *formula di sintesi* la formula di inversione (3), e *formula di analisi* la formula che definisce la trasformata di Fourier.

Osservazione. Grazie alla formula di inversione (3), possiamo scambiare i ruoli di G e \hat{G} (cioè di trasformata e antitrasformata), e quindi avremo $\mathcal{F}(fg)(a) = \frac{1}{n} \mathcal{F}f(a) * \mathcal{F}g(a)$, la formula “duale” di (2). Potremmo chiamare quest'ultima *formula della moltiplicazione*, se chiamiamo la (2) *formula della convoluzione*. Notate che abbiamo dovuto inserire il fattore $1/n$ perché vogliamo usare la stessa definizione di convoluzione per funzioni su $\mathbb{Z}/n\mathbb{Z}$ e funzioni sul suo duale, che è anch'esso isomorfo a $\mathbb{Z}/n\mathbb{Z}$. (Si veda l'osservazione successiva.)

Osservazione. La proprietà (4) ci dice che la trasformata di Fourier moltiplicata per $n^{-1/2}$ è un'isometria di $L^2(G)$ su se stesso. In realtà a rigore, tenendo distinti G ed il suo duale, sarebbe un'isometria di $L^2(G)$ su $L^2(\hat{G})$. Inoltre, in vista di una generalizzazione importante, un modo migliore di liberarsi del coefficiente $1/n$ nella proprietà (4) sarebbe dare a G la misura discreta, ed al suo duale la misura dove ogni elemento ha misura $1/n$ (o viceversa, mettendo allora $1/n$ nella formula della trasformata di Fourier e togliendolo dalla formula di inversione). Corrispondentemente anche la formula della convoluzione su \hat{G} cambierebbe, venendo moltiplicata per $1/n$.

Una conseguenza importante dell'essere un'isometria, in situazioni più generali, è che la trasformata di Fourier e la sua inversa sono continue nella norma L^2 . (Nel caso di G finito questa asserzione è banale in quanto isomorfismi di \mathbb{C} -spazi vettoriali di dimensione finita sono automaticamente continui, proprio in quanto tutte le norme sono equivalenti.) Dal punto di vista pratico ciò significa che la trasformata di Fourier commuta con l'operazione di limite. In altre parole, una sequenza di funzioni in $L^2(G)$ converge se e solo la sequenza delle loro trasformate converge; inoltre, possiamo anche calcolare il limite della sequenza di funzioni calcolando l'antitrasformata della sequenza delle trasformate. Vedremo ciò in azione in applicazioni.

Dimostrazione. La linearità è chiara. La biiettività seguirà da (3). Diamo una prima dimostrazione di (2), (3) e (4) facendo brutalmente i conti.

Per mostrare (2) calcoliamo

$$\begin{aligned}
 \mathcal{F}(f * g)(a) &= \sum_x (f * g)(x) e_a(-x) \\
 &= \sum_x \sum_y f(y) g(x - y) e_a(-x) \\
 &= \sum_x \sum_y f(y) g(x) e_a(-x - y) \\
 &= \left(\sum_y f(y) e_a(-y) \right) \left(\sum_x g(x) e_a(-x) \right) = \hat{f}(a) \hat{g}(a).
 \end{aligned}$$

Per mostrare (3) calcoliamo

$$\begin{aligned}
 \mathcal{F}\mathcal{F}f(x) &= \sum_a \mathcal{F}f(a) e_x(-a) \\
 &= \sum_a \sum_y f(y) e_a(-y) e_x(-a) \\
 &= \sum_y f(y) \sum_a e_{-y}(a) e_x(-a) \\
 &= \sum_y f(y) \langle e_{-y}, e_x \rangle = n f(-x)
 \end{aligned}$$

grazie al Lemma.

Per mostrare (4) calcoliamo, ad esempio,

$$\begin{aligned}
 \langle \hat{f}, \hat{g} \rangle &= \sum_a \hat{f}(a) \overline{\hat{g}(a)} \\
 &= \sum_a \sum_x f(x) e_a(-x) \sum_y \overline{g(y) e_a(-y)} \\
 &= \sum_x \sum_y f(x) \overline{g(y)} \sum_a e_a(-x) e_a(y) \\
 &= n \sum_x f(x) \overline{g(x)} = n \langle f, g \rangle.
 \end{aligned}$$

Naturalmente potevamo anche partire da $\langle f, g \rangle$, espandendo i suoi argomenti mediante la formula di inversione. (In questa seconda forma si tratta di un caso speciale del calcolo piú generale della terza dimostrazione piú sotto.) \square

Seconda dimostrazione di (2), (3) e (4). Essendo \mathcal{F} una mappa lineare, è sufficiente verificare (3) sugli elementi di una base, vale a dire per $f = \delta_a$, semplificando quindi i calcoli.

Analogamente possiamo procedere per dimostrare (3) e (4), essendo la convoluzione bilineare ed il prodotto hermitiano sesquilineare (cioè lineare nella prima componente e coniugata lineare nella seconda), e quindi limitarci a verificarle per $f = \delta_a$ e $g = \delta_b$. \square

Esercizio 11. Completare i dettagli della seconda dimostrazione.

Terza dimostrazione di (3) e (4). Le funzioni $n^{-1/2} e_a$, per $a \in G = \mathbb{Z}/n\mathbb{Z}$, formano una base ortonormale di $L^2(G)$. Data una qualsiasi base ortonormale u_a , per $a \in G = \mathbb{Z}/n\mathbb{Z}$,

ogni $f \in L^2(G)$ si scrive in modo unico come $f = \sum_a \langle f, u_a \rangle u_a$, e chiaramente varrà $\langle f, g \rangle = \sum_a \langle f, u_a \rangle \overline{\langle g, u_a \rangle}$. Per $u_a = n^{-1/2} e_a$ si ottengono (3) e (4). \square

Esercizio 12. Completate i dettagli della terza dimostrazione.

Osservazione. Daremo un'ulteriore dimostrazione della formula di inversione di Fourier nell'Esercizio 34, mediante la formula di interpolazione di Lagrange.

Terza settimana. Lezione di lunedì 26 settembre 2005 (tre ore): La matrice della DFT. Determinante di Vandermonde. Esempi di DFT. Applicazione della DFT: i poligoni derivati convergono al baricentro (inizio).

Osservazione. Rispetto alla base $\delta_0, \delta_1, \dots, \delta_{n-1}$ di $L^2(G)$ la trasformata di Fourier ha matrice

$$F_n = (\omega^{-(j-1)(k-1)})_{j,k},$$

dove $\omega = e_1(1) = \exp(2\pi i/n)$. Notate che la matrice F_n è simmetrica. La proprietà (4) della trasformata di Fourier equivale al fatto che la matrice $\Phi_n = n^{-1/2} F_n$ è unitaria, cioè ${}^t \Phi_n \Phi_n = I_n$, la matrice identità.

La matrice F_n è il caso particolare di una matrice di Vandermonde. Se x_1, \dots, x_n sono numeri, o indeterminate, la matrice di Vandermonde $(x_j^{k-1})_{j,k}$ ha determinante $\prod_{i < j} (x_j - x_i)$ (il *determinante di Vandermonde*). In particolare, tale determinante si annulla se e solo se almeno due fra x_1, \dots, x_n coincidono. Poiché F_n è la matrice di Vandermonde con $x_j = \omega^{-(j-1)}$, e questi sono fra loro distinti, la matrice è invertibile, il che fornisce una dimostrazione indipendente che la trasformata di Fourier è biiettiva.

1.5. Esempi ed altro. Esempi di trasformata di Fourier. (Iniziamo con un paio di esercizi di ripasso.)

Esercizio 13. Verificate formalmente che $\exp(x+y) = \exp(x)\exp(y)$, dove $\exp(x) = e^x := \sum_n \frac{1}{n!} x^n$ è la serie esponenziale. (Qui *formalmente* significa senza preoccuparsi della convergenza delle serie. A rigore, significa farlo nell'anello di serie formali $\mathbb{C}[[x, y]]$ in due indeterminate.)

Esercizio 14. Definiamo le serie formali $\cos(x)$ e $\sin(x)$ come le parti pari e dispari di e^{ix} , e quindi

$$\begin{aligned} \cos(x) &:= \frac{1}{2}(e^{ix} + e^{-ix}) = \sum_{n \text{ pari}} (ix)^n/n! = \sum_k (-1)^k x^{2k}/(2k)!, \\ \sin(x) &:= \frac{1}{2i}(e^{ix} - e^{-ix}) = \frac{1}{i} \sum_{n \text{ dispari}} (ix)^n/n! = \sum_k (-1)^k x^{2k+1}/(2k+1)!, \end{aligned}$$

per cui $\exp(ix) = \cos(x) + i\sin(x)$. Usando l'esercizio precedente, deducetene le note formule per esprimere $\sin(\alpha \pm \beta)$ e $\cos(\alpha \pm \beta)$ in termini di \sin e \cos di α e β .

Esercizio 15. Verificate ciascuna delle seguenti trasformate di Fourier (se non già fatto), usando scorciatoie quando possibile. Notate che la trasformata di Fourier di una funzione

pari (risp. dispari) è una funzione reale (risp. immaginaria pura) per a reale.

f (o $f(x)$)	$\mathcal{F}f$ (o $\mathcal{F}f(a)$)
δ_y	e_{-y}
e_b	$n\delta_b$
$\frac{1}{2}(\delta_1 + \delta_{-1})(x)$	$\cos(2\pi a/n)$
$\frac{1}{3}(\delta_{-1} + \delta_0 + \delta_1)(x)$	$\frac{1}{3}(1 + 2\cos(2\pi a/n))$
$\frac{1}{2}(\delta_0 + \delta_1)(x)$	$\exp(-\pi i a/n) \cos(\pi a/n)$
$\frac{1}{2}(\delta_1 - \delta_{-1})(x)$	$-i \sin(2\pi a/n)$
$(\delta_0 - \delta_1)(x)$	$2i \exp(-\pi i a/n) \sin(\pi a/n)$
$(\delta_{-1} - \delta_0)(x)$	$2i \exp(\pi i a/n) \sin(\pi a/n)$
$(\delta_{-1} - 2\delta_0 + \delta_1)(x)$	$-2(1 - \cos(2\pi a/n))$

1.6. Varie proprietà della trasformata di Fourier [Ter, p. 45]. Per $y \in \mathbb{Z}/n\mathbb{Z}$ definiamo l'operatore di traslazione $T_y : L^2(\mathbb{Z}/n\mathbb{Z}) \rightarrow L^2(\mathbb{Z}/n\mathbb{Z})$ ponendo $T_y f(x) = f(x - y)$. Vale allora

$$\widehat{T_y f} = \widehat{\delta_y * f} = e_{-y} \hat{f}, \quad \text{cioè} \quad \widehat{T_y f}(a) = \exp(-2\pi i a y/n) \hat{f}(a).$$

Dunque a traslazioni della f (nel dominio *dei tempi*, secondo un'interpretazione comune della trasformazione di Fourier) corrispondono moltiplicazioni per caratteri della sua DFT. Simmetricamente avremo

$$\widehat{e_b f} = \frac{1}{n} n\delta_b * \hat{f} = \widehat{T_b f}$$

e quindi a moltiplicazioni della f per caratteri (talvolta dette *modulazioni* in campo ingegneristico) corrispondono traslazioni della sua DFT.

Se per a invertibile in $\mathbb{Z}/n\mathbb{Z}$ definiamo l'operatore di dilatazione $D_\gamma : L^2(\mathbb{Z}/n\mathbb{Z}) \rightarrow L^2(\mathbb{Z}/n\mathbb{Z})$ ponendo $D_\gamma f(x) = f(\gamma x)$, avremo la formula

$$\widehat{D_\gamma f} = D_{\gamma^{-1}} \hat{f}.$$

Ricordando che f° è definita da $f^\circ(x) = f(-x)$, aggiungiamo altre due proprietà della DFT. La prima è la *formula di riflessione* $\widehat{f^\circ} = (\hat{f})^\circ$ (per cui potremo scrivere semplicemente \hat{f}° , senza pericolo di ambiguità). In parole, la trasformata di Fourier commuta col cambiare segno all'argomento della funzione. Come per il comportamento della convoluzione rispetto a $^\circ$ visto in precedenza, ciò rispecchia il fatto che la mappa che manda ciascun elemento di un gruppo commutativo nel suo inverso è un automorfismo. L'altra proprietà è la *formula di coniugio*, che è $\widehat{\hat{f}} = \overline{f^\circ}$ in notazione compatta, e $\mathcal{F}\hat{f}(a) = \overline{\mathcal{F}f(-a)}$ in forma piú esplicita.

Lezione di venerdì 30 settembre 2005 (tre ore): Applicazioni della DFT: i poligoni derivati convergono al baricentro (conclusione); determinazione dei poligoni simili al loro derivato (inizio).

2. ALCUNE APPLICAZIONI IN GEOMETRIA, ANALISI, ALGEBRA

2.1. I poligoni derivati convergono al baricentro. (Si veda [Ter, Capitolo 7].)

Osservazione. Non è difficile rendersi conto che il baricentro di un sistema di punti, pensati tutti di massa unitaria, definito come in Fisica (o, piú precisamente, Statica) ha come coordinate la media aritmetica delle coordinate dei punti. Il baricentro di un poligono poi coincide con il baricentro dell'insieme dei suoi vertici. (Non so o non ricordo come si mostra quest'ultimo fatto in modo elementare, se qualcuno lo sa me lo spieghi...)

Osservazione. È chiaro che il baricentro di un poligono coincide con quelli di tutti i suoi poligoni derivati. Ne segue che se i poligoni derivati convergono ad un punto, allora quel punto è il comune baricentro. Il problema è dimostrare la convergenza, questo è l'oggetto della sezione. (L'obiettivo, la convergenza dei poligoni derivati ad un punto, va interpretato come *tutti i vertici dei poligoni derivati convergono ad uno stesso punto.*)

Forse la dimostrazione data in [Ter] è più chiara non assumendo fin dall'inizio che l'origine sia il baricentro, diciamolo $B = \frac{1}{k} \sum_{x \in \mathbb{Z}/k\mathbb{Z}} z(x)$, cosicché il calcolo finale diviene

$$\lim_{r \rightarrow \infty} \mathcal{F}(D^r z)(a) = \lim_{r \rightarrow \infty} \exp(-r\pi i a/k) \cos(\pi a/k)^r \cdot \mathcal{F}z(a) = \begin{cases} \mathcal{F}z(0) = kB & \text{se } a = 0, \\ 0 & \text{altrimenti,} \end{cases}$$

da cui concludiamo che

$$\lim_{r \rightarrow \infty} D^r z(x) = \mathcal{F}^{-1}(kB\delta_0)(x) = Be_0(x) = B.$$

Quarta settimana. Lezione di lunedì 3 ottobre 2005 (tre ore): Determinazione dei poligoni simili al loro derivato (conclusione). Variazioni sul tema. Proprietà della trasformata di Fourier rispetto a traslazioni, dilatazioni, riflessione e coniugio.

2.2. Altre applicazioni della DFT allo studio dei poligoni derivati. Vediamo ora di sfruttare questo metodo della DFT per qualche altra applicazione simile. Ad esempio, è chiaro che il caso dei triangoli è alquanto speciale: il triangolo derivato è simile al triangolo originale (geometria elementare). Questo si spiega facilmente anche in termini della nostra formula per il poligono derivato. Infatti, se supponiamo, come possiamo, che il baricentro sia l'origine, che si traduce in $z(0) + z(1) + z(2) = 0$, ovvero $(\delta_0 + \delta_1 + \delta_2) * z = 0$, ne segue che

$$Dz = \frac{1}{2}(\delta_0 + \delta_1) * z = -\frac{1}{2}\delta_2 * z.$$

Questa formula ci dice proprio che il poligono Dz è simile a z , con fattore di similitudine $-1/2$ (o, con linguaggio più comune, con fattore di similitudine $1/2$ e rotazione di un angolo piatto rappresentata da $-1 = e^{\pi i}$), e con un cambio di nomi (traslazione) dei vertici rappresentato da $\delta_2 *$. (Se disegnate il triangolo diviso in quattro triangoli simili e numerate i vertici di z e Dz vi sarà tutto chiaro.)

Potremmo anche dirlo con la DFT, ma sarebbe come sparare con un cannone ad un moscerino. Invece la DFT diventa praticamente essenziale se vogliamo dimostrare che solo i triangoli mostrano questo comportamento in generale, cioè per ogni possibile z . (Naturalmente per ogni k ci sono particolari poligoni simili ai loro derivati, ad esempio quelli equilateri.) Premettiamo che due poligoni con il baricentro nell'origine sono simili (in modo *proprio*, cioè tramite un'omotetia ed una rotazione, ma senza riflessioni) se e solo se le corrispondenti z sono proporzionali (o, equivalentemente, le loro DFT \hat{z} sono proporzionali), per una scelta delle numerazioni dei vertici conforme nei due poligoni. Il modulo del fattore di proporzionalità è il fattore di omotetia, ed il suo argomento è l'angolo di rotazione. Si avrà invece una similitudine *impropria* se e solo se le corrispondenti z sono l'una proporzionale alla coniugata dell'altra (con la stessa accortezza nella numerazione dei vertici). Inoltre, cambiare ciclicamente la numerazione dei vertici di un poligono corrisponde ad operare la convoluzione della sua z con una certa δ_y (cioè moltiplicare \hat{z} per il carattere e_{-y}). Infine, invertire l'ordine nella numerazione dei vertici,

che però non ci servirà nel nostro problema, corrisponde a rimpiazzare $z(x)$ con $z(-x)$, ovvero a rimpiazzare $\hat{z}(a)$ con $\hat{z}(-a)$.

Nei prossimi due esercizi non serve assumere che il baricentro sia nell'origine. Piuttosto, al fine di evitare casi degeneri, assumete che i vertici del poligono siano distinti. Permettiamo invece che i poligoni abbiano qualche angolo piatto o nullo, cioè che tre vertici consecutivi siano allineati.

Esercizio 16. Assumendo che l'origine non sia un vertice del poligono z (per evitare quale situazione?), mostrate che questo è simmetrico rispetto all'origine se e solo se k è pari e $\hat{z}(a) = 0$ per ogni a pari. (In particolare, ne segue che $\hat{z}(0) = 0$, cioè il baricentro è nell'origine, naturalmente.)

(Suggerimento: Non essendo l'origine un vertice, è chiaro che k deve essere pari. Assumete allora che il simmetrico di $z(a)$ sia $z(a + \frac{k}{2})$.)

Osservazione. Abbiamo assunto che l'origine non sia un vertice del poligono per poter concludere che k sia pari e che la simmetria in questione conservi l'ordine ciclico dei vertici del poligono. Se il poligono ha un vertice nell'origine, diciamo $z(0)$, e quindi k è dispari, si vede che il simmetrico di $z(a)$ è $z(-a)$, e quindi la simmetria inverte l'ordine ciclico dei vertici. Per un poligono con un vertice nell'origine la condizione per la simmetria è $z(x) + z(-x) = 0$ per ogni x , cioè $z(a) + z(-a) = 0$ per ogni a . (In tal caso il poligono è intrecciato, e i tre vertici $z(-1)$, $z(0)$ e $z(1)$ sono allineati, una possibilità che non abbiamo escluso.)

Esercizio 17. Mostrate che il poligono z , supposto avente il vertice $z(0)$ sull'asse reale, è simmetrico rispetto all'asse reale se e solo se $\hat{z}(a)$ è reale per ogni a . (Simmetrie rispetto ad assi inclinati diversamente si possono ottenere componendo con rotazioni. Rimane escluso il caso, un po' più complicato, di un poligono con un numero pari di vertici, nessuno dei quali è sull'asse reale.)

(Suggerimento: In questo caso il simmetrico di $z(a)$ è $z(-a)$.)

Vogliamo ora determinare i poligoni di k lati che sono propriamente simili ai loro poligoni derivati. Per un poligono z di k lati, dove possiamo supporre $k \geq 3$, ed assumendo come in precedenza il baricentro nell'origine, cioè $\hat{z}(0) = 0$, questo avviene se e solo se

$$Dz = \alpha \delta_y * z$$

per un opportuni $\alpha \in \mathbb{C}$ e $y \in \mathbb{Z}/k\mathbb{Z}$. Prendendo le DFT di entrambi i membri otteniamo

$$\widehat{Dz} = \alpha e_{-y} \hat{z}.$$

Poiché, come abbiamo visto, $\widehat{Dz}(a) = \exp(-\pi ia/k) \cos(\pi a/k) \hat{z}(a)$, questa equazione è equivalente a

$$\exp(-\pi ia/k) \cos(\pi a/k) \hat{z}(a) = \alpha e_{-y}(a) \hat{z}(a) \quad \text{per ogni } a \in \mathbb{Z}/k\mathbb{Z},$$

ovvero a

$$(\text{sim}) \quad \cos(\pi a/k) = \alpha \exp(\pi ia(1 - 2y)/k) \quad \text{per ogni } a \in \mathbb{Z}/k\mathbb{Z} \text{ tale che } \hat{z}(a) \neq 0.$$

Sarà conveniente usare gli interi $-k/2 < a \leq k/2$ come rappresentanti per gli elementi di $\mathbb{Z}/k\mathbb{Z}$, piuttosto che la solita scelta $0 \leq a < k$. Poiché il valore assoluto del secondo membro, che è $|\alpha|$, è indipendente da a , anche quello del primo membro lo deve essere. Esaminando l'andamento della funzione $\cos(t)$ per $-\pi/2 \leq t \leq \pi/2$ vediamo che una condizione necessaria affinché si verifichi (sim) è che $\hat{z}(a)$ sia non nullo al più per due soli valori di a , che siano l'uno l'opposto dell'altro, diciamo per $a = \pm b$.

Trattiamo separatamente il caso in cui $\hat{z}(a)$ è non nullo per un unico valore di a , diciamo $a = b$ (con $b \neq 0$), che corrisponde ad un poligono regolare. Notate che per $b \neq \pm 1$ il poligono è intrecciato, ma questo non sarà un problema. Piuttosto, se b non è primo con k il vertici del poligono non sono tutti distinti: infatti si tratta di un poligono con un numero di lati un divisore proprio di k , percorso un certo numero di volte. Converrà escludere questa situazione assumendo che $(b, k) = 1$. A questo punto, assegnando y arbitrariamente possiamo sempre fare in modo che (sim) sia soddisfatta: lo sarà con $\alpha = \exp(\pi ib(2y-1)/k) \cos(\pi b/k)$. Notate che il valore assoluto del rapporto di similitudine α , che è $\cos(\pi a/k)$, è il rapporto fra l'apotema ed il raggio del poligono regolare. Naturalmente, al variare di y otteniamo k similitudini distinte. Assumendo $(b, k) = 1$ come annunciato sopra, se k è dispari ce n'è esattamente una fra esse con α reale, cioè con $(2y-1)/k \in \mathbb{Z}$, e in quel caso $\alpha = (-1)^b \cos(\pi b/k)$ è positivo o negativo a seconda che b sia pari o dispari. Invece se k è pari non ce n'è nessuna con α reale (cioè ogni similitudine di z su Dz coinvolge una rotazione di un angolo diverso da nullo o piatto).

Ora occupiamoci del caso in cui $\hat{z}(a)$ è non nullo esattamente per $a = \pm b$. Possiamo assumere $\pm b$ diversi da zero, perché abbiamo supposto $\hat{z}(0) = 0$, e da $k/2$ nel caso k sia pari, altrimenti il poligono sarebbe contenuto nell'asse reale. Quindi $-b \neq b$. Dato che $\cos(\pi a/k)$ assume lo stesso valore per $a = \pm b$, lo stesso deve valere per il secondo membro di (sim), se questa vale. Ne segue che $b(1-2y)$ deve essere multiplo di k . Come in precedenza, possiamo assumere $(b, k) = 1$. Quindi, se vale (sim), $1-2y$ deve essere multiplo di k . In particolare, k deve essere dispari, e quindi $\alpha = (-1)^b \cos(\pi b/k)$. Viceversa, per k dispari, scegliendo y tale che $2y-1$ sia un multiplo di k (ad esempio, $y = (k+1)/2$ ed $\alpha = (-1)^b \cos(\pi b/k)$), è soddisfatta la (sim) qualunque valori assegniamo a $\hat{z}(b) =: \beta$ e $\hat{z}(-b) =: \gamma$. Dunque il generico poligono z simile al suo derivato Dz è

$$z(x) = \beta \exp(2\pi ibx/k) + \gamma \exp(-2\pi ibx/k)$$

dove i numeri complessi $\beta = \frac{1}{k} \hat{z}(b)$ e $\gamma = \frac{1}{k} \hat{z}(-b)$ si possono assegnare arbitrariamente. Grazie al prossimo esercizio, esso è l'immagine di un poligono regolare sotto un'arbitraria mappa \mathbb{R} -lineare di \mathbb{C} in se stesso. (Attenzione, sotto la nostra ipotesi che $\beta\gamma \neq 0$ tale immagine non è essa stessa un poligono regolare. A differenza del caso regolare, non abbiamo k distinte similitudini, ma solo una: qualunque scelta di un multiplo $2y-1$ di k è equivalente a quella fatta poco fa.)

Esercizio 18. Mostrate che ogni mappa \mathbb{R} -lineare di \mathbb{C} in se stesso si può esprimere nella forma $z \mapsto \alpha z + \beta \bar{z}$ per opportuni $\alpha, \beta \in \mathbb{C}$ unicamente determinati.

(Suggerimento: Espandete ciascuno di z, α, β nella somma di parte reale e parte immaginaria. Un modo alternativo è mostrare che gli automorfismi $z \mapsto z$ e $z \mapsto \bar{z}$ del campo \mathbb{C} sono linearmente indipendenti su \mathbb{C} , ed poi ragioni di dimensione. In questa seconda forma è un caso speciale di un fatto generale di teoria di Galois.)

Mostrate anche che $z \mapsto \alpha z + \beta \bar{z}$, come mappa \mathbb{R} -lineare, ha determinante $|\alpha|^2 - |\beta|^2$, e quindi è iniettiva se e solo se α e β hanno modulo diverso. In particolare, questa è la condizione che dovremo richiedere sui coefficienti α, β affinché il generico poligono trovato sopra (propriamente simile al suo derivato) non sia contenuto in una retta.

Concludiamo risolvendo il problema con cui abbiamo iniziato, quello che ha per soluzione $k = 3$. Supponiamo che, per un certo k , ogni poligono di k lati sia simile al suo derivato. Allora per ogni z con $\hat{z}(0) = 0$ (essendo il baricentro nell'origine) devono esistere α e y , dipendenti da z , tale che valga (sim). In particolare possiamo scegliere z tale che $\hat{z}(a) \neq 0$ per ogni $a \neq 0$, e quindi per $k-1$ valori di a . Ma abbiamo visto che se

vale (sim) allora $\hat{z}(a) \neq 0$ per al massimo due valori di a . Quindi $k - 1 \leq 2$, e pertanto $k = 3$.

Esercizio 19. Il fatto che ogni triangolo sia simile al suo derivato è anche conseguenza della nostra determinazione di tutti i poligoni simili al loro derivato ottenuta in precedenza. Il motivo è che ogni triangolo con baricentro nell'origine è immagine di un triangolo equilatero con baricentro nell'origine, sotto un'opportuna mappa lineare. Dimostrate quest'ultimo fatto.

(Suggerimento: Facile algebra lineare in uno spazio di dimensione due.)

Esercizio 20. Nella determinazione dei poligoni simili al loro derivato mediante una similitudine propria che abbiamo visto sopra, abbiamo assunto di numerare i vertici di z e Dz nello stesso senso. In effetti questa appare come l'unica scelta possibile, ed almeno per poligoni convessi ha il significato seguente: *se percorro z in senso antiorario, e voglio trasferire questa numerazione su Dz mediante una similitudine propria, allora anche Dz dovrà essere percorso in senso antiorario.* Ma proviamo a dubitare della nostra intuizione.

Ripercorrete lo studio fatto sopra facendo l'altra scelta, cioè rovesciando la numerazione su uno fra z e Dz , e mostrate che i poligoni propriamente simili con il loro derivato secondo questa scelta di numerazione sono degeneri, nel senso che stanno su una retta.

(Suggerimento: Partite da $Dz = \alpha\delta_y * w$ dove $w(x) = z(-x)$. Stavolta le $k - 1$ equazioni (per $a \in \mathbb{Z}/k\mathbb{Z}$ con $a \neq 0$) che precedono (sim) non sono indipendenti, nel senso che ciascuna coinvolge sia $\hat{z}(a)$ che $\hat{z}(-a)$. Ragionando con i valori assoluti deducetene che $\hat{z}(a)$ può essere non nullo solo per $a = \pm b$, per un certo b , e che $\hat{z}(b)$ e $\hat{z}(-b)$ hanno lo stesso valore assoluto.)

Esercizio 21. (Non è piú difficile da svolgere dei precedenti, ma le interpretazioni geometriche finali lo sono.) Determinate i poligoni simili al loro derivato mediante una similitudine impropria.

(Suggerimento: In questo caso è naturale invertire la numerazione dei vertici in uno dei poligoni. Dunque partite da $Dz = \alpha\delta_y * w$ dove $w(x) = \overline{z(-x)}$ ed applicate di seguito la formula di coniugio e quella di riflessione. Ripercorrete il ragionamento visto sopra fino a mostrare che $\hat{z}(a)$ vale zero ad eccezione che per $a = \pm b$, e poi naturalmente assumete $(b, k) = 1$. Supponete $\hat{z}(\pm b) \neq 0$ per escludere il caso dei poligoni regolari, che certo è una soluzione, mostrate che gli argomenti di $\hat{z}(b)$ e $\hat{z}(-b)$ (presi qui modulo π anziché il consueto 2π) devono differire per un multiplo dispari di $\pi b/k$. Se $b = 1$ per semplicità, e k è dispari, è la stessa cosa che dire che differiscono per un multiplo arbitrario di π/k ; geometricamente ¹ significa che il poligono è immagine di un poligono regolare mediante una mappa lineare diagonalizzabile ed avente autospazi ortogonali, uno dei quali è un asse del poligono (che quindi rimane asse di simmetria anche per il poligono modificato). Se $b = 1$ e k è pari significa che il poligono è immagine di un poligono regolare mediante una mappa lineare diagonalizzabile ed avente autospazi ortogonali, che bisecano gli angoli formati dagli assi del poligono.)

Esercizio 22. Mostrate che i poligoni simili (mediante una similitudine propria) al loro derivato secondo sono esattamente le immagini dei poligoni regolari (con k dispari o pari) sotto una qualsiasi mappa lineare. (Notate, in particolare, che per k dispari le soluzioni del problema sono gli stessi poligoni simili al loro derivato primo, mentre per k pari non è così.)

¹(13/10/05) Rivedendo l'esercizio con uno studente ci è parso che questa interpretazione geometrica fosse sbagliata. Mi riservo di pensarci e correggere questo punto.

Lezione di venerdì 7 ottobre 2005 (tre ore): Altri problemi sui poligoni derivati. Un'altra applicazione della DFT: una disuguaglianza per l'area di un poligono.

Esercizio 23. Sia z un poligono di k lati. Mostrate che se k è dispari ed un poligono derivato successivo $D^r z$ è regolare, per qualche $r \geq 1$, allora anche z lo è.

Mostrate che se k è pari ed un poligono derivato successivo $D^r z$ è regolare, per qualche $r \geq 2$, allora anche Dz lo è.

Costruite (in modo geometrico) un poligono z tale che Dz sia un quadrato senza che z lo sia.

Determinate tutti i poligoni z (trovando le loro possibili DFT) con un numero pari k di lati tali che Dz sia un poligono regolare.

Esercizio 24. Nella figura I.25 a pagina 122 di [Ter], la forma dei successivi poligoni derivati (che naturalmente diventano sempre più piccoli, convergendo al baricentro) si avvicina sempre più a quella di un poligono regolare. In effetti così avviene per un poligono “tipico”, o “generico”, ovvero un poligono “scelto a caso”. Giustificate questa affermazione. Per farlo in modo sufficientemente rigoroso, vi converrà preliminarmente determinare una condizione necessaria e sufficiente su \hat{z} affinché ciò avvenga. Potete inoltre descrivere geometricamente tutti i poligoni per cui ciò invece non avviene?

Concludiamo con un'altro esempio di applicazione della DFT ai poligoni (ma stavolta non c'entrano i poligoni derivati). Determiniamo i poligoni z di k lati, con k pari, tali che lati opposti siano congruenti e paralleli. È facile rendersi conto che, salvo situazioni degeneri, questo equivale alla condizione che valga zero la somma di lati opposti visti come vettori orientati seguendo l'ordinamento ciclico dei vertici. Questo si traduce facilmente (ad esempio) in

$$(\delta_0 - \delta_{-1} + \delta_{k/2} - \delta_{k/2-1}) * z = 0,$$

e quindi, prendendo le DFT, in $(e_0 - e_{-1} + e_{k/2} - e_{k/2+1})\hat{z} = 0$, che possiamo anche scrivere come

$$(e_0 - e_{-1})(e_0 + e_{k/2})\hat{z} = 0.$$

Essendo

$$(e_0 - e_{-1})(a) \cdot (e_0 + e_{k/2})(a) = \begin{cases} 2(1 - e^{2\pi ia/k}) & \text{se } a \text{ è pari,} \\ 0 & \text{se } a \text{ è dispari,} \end{cases}$$

concludiamo che la nostra condizione equivale a

$$\hat{z}(a) = 0 \quad \text{per ogni } a \text{ pari e diverso da zero.}$$

Ad esempio, nel caso $k = 4$ otteniamo che z deve essere un'arbitraria combinazione lineare di e_1 ed e_{-1} . Come abbiamo visto in precedenza, questi poligoni sono le immagini di un quadrato sotto arbitrarie mappe lineari, e quindi sono tutti i parallelogrammi, come ci aspettiamo.

Esercizio 25. Determinate tutti i poligoni con un numero pari di lati tali che i lati di posto dispari (scelto una numerazione ciclica dei lati) possano essere spostati parallelamente a se stessi in modo da formare un poligono di $k/2$ lati, dopo aver mostrato che per tali poligoni anche i lati di posto pari soddisfano la stessa condizione.

(Suggerimento: I poligoni cercati sono esattamente quelli tali che la somma a segni alterni dei loro lati (orientati) valga zero. Dovreste trovare la condizione $\hat{z}(k/2) = 0$ (in aggiunta a $\hat{z}(0) = 0$ solo se richiedete che il baricentro sia nell'origine).)

2.3. Una disuguaglianza per l'area di un poligono. (Si veda [Ter, Capitolo 7].)

Esercizio 26. Mostrare che l'uguaglianza in $A \leq B/2$ vale se e solo se il poligono è un quadrato con centro nell'origine, con i vertici numerati in senso antiorario.

Esercizio 27. La dimostrazione prova che vale anzi $A \leq \gamma_k B/2$ per ogni poligono di k lati, dove $\gamma_k = \max\{\sin(2\pi a/k) \mid a = 0, \dots, k-1\}$. Calcolare questo massimo più esplicitamente (cioè determinare per quale valore di a si realizza il massimo), distinguendo a seconda della classe resto di k modulo 4.

Per quali poligoni si raggiunge l'uguaglianza in $A \leq \gamma_k B/2$? (In generale si tratta di poligoni intrecciati!)

Quinta settimana. Lezione di lunedì 10 ottobre 2005 (tre ore): Altre applicazioni della DFT: la disuguaglianza isoperimetrica per i poligoni equilateri; la disuguaglianza di Wirtinger. Svolgimento in classe di alcuni esercizi assegnati in precedenza.

2.4. La disuguaglianza isoperimetrica per i poligoni. (Si veda [Ter, Capitolo 7].)

2.5. Una versione discreta della disuguaglianza di Wirtinger. (Si veda [Ter, Capitolo 7].)

Esercizio 28. Pensando la funzione z come rappresentante un poligono, come fatto in precedenza, mostrate che l'uguaglianza nella disuguaglianza di Wirtinger si verifica se e solo se z è un poligono regolare non intrecciato (escludendo casi di poligoni degeneri).

Osservazione. Nel caso continuo della disuguaglianza di Wirtinger accennato in [Ter, pag. 126], le sole funzioni che realizzano l'uguaglianza sono le combinazioni lineari di $\sin(t)$ e $\cos(t)$.

Lezione di venerdì 14 ottobre 2005 (tre ore): Ripasso informale di teoria di Galois: le estensioni cicliche di ordine primo sono estensioni radicali. Applicazione della DFT alla risoluzione delle equazioni di terzo grado. Svolgimento in classe di alcuni esercizi assegnati in precedenza. La trasformata di Fourier diagonalizza le traslazioni (inizio).

2.6. Applicazione alla risoluzione delle equazioni di secondo e terzo grado.

Usiamo la DFT per risolvere mediante radicali l'equazione di terzo grado. La generica equazione di terzo grado è $x^3 - a_1x^2 + a_2x - a_3 = 0$, dove, a rigore, a_1, a_2, a_3 sono indeterminate. Se z_1, z_2, z_3 sono le radici dell'equazione in un campo di spezzamento, il primo membro dell'equazione deve coincidere con $(x - z_1)(x - z_2)(x - z_3)$, da cui

$$a_1 = z_1 + z_2 + z_3, \quad a_2 = z_1z_2 + z_1z_3 + z_2z_3, \quad a_3 = z_1z_2z_3.$$

Risolvere l'equazione equivale a risolvere questo sistema nelle indeterminate z_1, z_2, z_3 . Per semplificare la trattazione (anche se è indispensabile) conviene assumere $a_1 = 0$, il che si può sempre ottenere mediante una traslazione nella x dall'equazione originale (ponendo $x' := x - a_1/3$). Risolveremo dunque l'equazione $x^3 + px + q = 0$. Le tre radici z_1, z_2, z_3 soddisfano

$$z_1 + z_2 + z_3 = 0, \quad z_1z_2 + z_2z_3 + z_3z_1 = p, \quad z_1z_2z_3 = -q.$$

Considerando le radici $z_0 := z_3, z_1, z_2$ come una funzione su $\mathbb{Z}/3\mathbb{Z}$, potremo esprimerle in funzione della sua trasformata di Fourier $\hat{z}_0, \hat{z}_1, \hat{z}_2$, che è data da

$$\hat{z}_0 = z_0 + z_1 + z_2 = 0, \quad \hat{z}_1 = z_0 + \omega z_1 + \bar{\omega} z_2, \quad \hat{z}_2 = z_0 + \bar{\omega} z_1 + \omega z_2,$$

dove $\omega = e^{-2\pi i/3}$, e quindi $\omega^2 + \omega + 1 = 0$. Avremo allora

$$\hat{z}_1 \hat{z}_2 = z_0^2 + z_1^2 + z_2^2 - p = (z_0 + z_1 + z_2)^2 - 3a = -3p$$

e

$$\begin{aligned} \hat{z}_1^3 + \hat{z}_2^3 &= z_0^3 + z_1^3 + z_2^3 + 3\omega(z_0^2 z_1 + z_1^2 z_2 + z_2^2 z_0) + 3\bar{\omega}(z_0 z_1^2 + z_1 z_2^2 + z_2 z_0^2) + 6z_0 z_1 z_2 \\ &\quad + z_0^3 + z_1^3 + z_2^3 + 3\bar{\omega}(z_0^2 z_1 + z_1^2 z_2 + z_2^2 z_0) + 3\omega(z_0 z_1^2 + z_1 z_2^2 + z_2 z_0^2) + 6z_0 z_1 z_2 \\ &= 2(z_0^3 + z_1^3 + z_2^3) - 3(z_0^2 z_1 + z_1^2 z_2 + z_2^2 z_0 + z_0 z_1^2 + z_1 z_2^2 + z_2 z_0^2) + 12z_0 z_1 z_2 \\ &= 2(z_0 + z_1 + z_2)^3 - 9(z_0^2 z_1 + z_1^2 z_2 + z_2^2 z_0 + z_0 z_1^2 + z_1 z_2^2 + z_2 z_0^2) \\ &= -9(z_0^2 z_1 + z_1^2 z_2 + z_2^2 z_0 + z_0 z_1^2 + z_1 z_2^2 + z_2 z_0^2) + 27z_0 z_1 z_2 \\ &= -9(z_0 + z_1 + z_2)(z_0 z_1 + z_1 z_2 + z_2 z_0) + 27z_0 z_1 z_2 \\ &= 27z_0 z_1 z_2 = -27q. \end{aligned}$$

Dunque \hat{z}_1^3 e \hat{z}_2^3 sono le due radici dell'equazione $y^2 + 27q - 27p^2 = 0$, cioè

$$\hat{z}_1^3 = \frac{27}{2}q + \frac{3}{2}\sqrt{-3d} \quad \text{e} \quad \hat{z}_2^3 = \frac{27}{2}q - \frac{3}{2}\sqrt{-3d},$$

dove $d = -4p^3 - 27q^2$ è il *discriminante* dell'equazione (che poi vale $\prod_{0 \leq i < j \leq 2} (z_i - z_j)^2$, cioè il quadrato del determinante di Vandermonde fatto con le radici). A questo punto \hat{z}_1 e \hat{z}_2 sono determinati a meno di moltiplicarli ciascuno per una radice cubica dell'unità. Scegliendoli (in uno dei tre modi giusti fra i nove possibili) in modo da soddisfare $\hat{z}_1 \hat{z}_2 = -3p$, otterremo a loro volta le radici dell'equazione tramite la formula di inversione di Fourier, cioè

$$z_0 = \frac{1}{3}(\hat{z}_1 + \hat{z}_2), \quad z_1 = \frac{1}{3}(\bar{\omega} \hat{z}_1 + \omega \hat{z}_2), \quad z_2 = \frac{1}{3}(\omega \hat{z}_1 + \bar{\omega} \hat{z}_2).$$

Esercizio 29. Risolvere in modo analogo l'equazione di secondo grado $x^2 + bx + c = 0$.

Sesta settimana. Lezione di lunedì 17 ottobre 2005 (tre ore): La trasformata di Fourier diagonalizza le traslazioni (conclusione). Diagonalizzazione di matrici circolanti.

I caratteri come autovettori per gli operatori di traslazione. Introduzione al gruppo duale: caratteri (unitari) del gruppo \mathbb{Z} e dualità fra \mathbb{Z} e \mathbb{T} (inizio).

3. I CARATTERI COME AUTOFUNZIONI.

3.1. La trasformata di Fourier diagonalizza le traslazioni [Ter, pp. 59–61, attenzione perché la parte finale della dim del Teorema 2 non è corretta]. Gli operatori di traslazione T_y per elementi y di $G = \mathbb{Z}/n\mathbb{Z}$, che sono mappe lineari invertibili di $L^2(G)$ in se stesso, sono diagonalizzabili, ed anzi si possono diagonalizzare contemporaneamente. Infatti ciascun carattere e_z , per $z \in G$, è un autovettore per ogni T_y , essendo

$$T_y e_z(x) = e_z(x - y) = e_z(-y) e_z(x),$$

cioè $T_y e_z = e_z(-y) e_z$, con corrispondente autovalore $e_z(-y)$. Notate che l'autovalore corrispondente a e_z non dipende solo da z , ma anche dal particolare operatore T_y

considerato. Dato che i caratteri sono $n = |G|$ elementi di $L^2(G)$ linearmente indipendenti (essendo ortogonali rispetto al prodotto hermitiano), essi formano una base di autovettori, simultaneamente per tutte le traslazioni T_y . (Questo è il ragionamento giusto perché funziona anche per gruppi G non ciclici, ma nel nostro caso speciale di $G = \mathbb{Z}/n\mathbb{Z}$ potevamo anche evitare di usare l'ortogonalità dei caratteri, semplicemente deducendo la loro indipendenza dal fatto che i corrispondenti autovalori $e_z(1) = e^{2\pi iz/n}$ per l'operatore T_1 sono distinti.)

Se pensiamo alla base costituita dalle funzioni δ_z come la base piú naturale per $L^2(G)$, possiamo affermare che una mappa lineare che diagonalizza T_y è data dalla trasformazione di Fourier \mathcal{F} , nel senso che

$$\mathcal{F}T_y\mathcal{F}^{-1}\delta_z = e_z(-y)\delta_z, \quad \text{o anche} \quad \mathcal{F}T_y\mathcal{F}^{-1}\delta_z = \hat{\delta}_y(z)\delta_z,$$

deducibile dalla precedente formula esprimendo e_z come $n\mathcal{F}^{-1}\delta_z$. In termini di matrici, se W_y è la matrice dell'operatore T_y rispetto alla base $\delta_0, \dots, \delta_{n-1}$ di $L^2(G)$, cioè $W_y = W^y$, dove

$$W = W_1 = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

allora

$$F_n W_y F_n^{-1} = \text{diag}(e_{-y}(0), e_{-y}(1), \dots, e_{-y}(n-1)) = \text{diag}(\hat{\delta}_y(0), \hat{\delta}_y(1), \dots, \hat{\delta}_y(n-1)).$$

(Se preferiamo, possiamo anche scrivere $F_n W_y F_n^{-1}$ come $\bar{F}_n^{-1} W_y \bar{F}_n$, essendo $F_n^{-1} = n^{-1} \bar{F}_n$.) Ne segue per linearità che, piú in generale, la *matrice circolante*

$$C = \begin{bmatrix} c_0 & c_{n-1} & c_{n-2} & \cdots & c_1 \\ c_1 & c_0 & c_{n-1} & \cdots & c_2 \\ c_2 & c_1 & c_0 & \cdots & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_0 \end{bmatrix} = (c_{i-j})_{i,j=1,\dots,n}$$

è diagonalizzabile, essendo $C = c_0 I + c_1 W + c_2 W^2 + \cdots + c_{n-1} W^{n-1}$, e

$$F_n C F_n^{-1} = \text{diag}(\hat{c}(0), \hat{c}(1), \dots, \hat{c}(n-1)),$$

dove $c = c_0 \delta_0 + \cdots + c_{n-1} \delta_{n-1}$ è la funzione $c \in L^2(G)$ tale che $c(j) = c_j$ per ogni j . In particolare, scopriamo che

$$\det(C) = \det(F_n C F_n^{-1}) = \prod_{j=0}^{n-1} \hat{c}(j).$$

Cosí, ad esempio, se $c_0 + c_1 + \cdots + c_{n-1} = 0$ allora $\det(C) = 0$.

Esercizio 30. Mostrate direttamente, cioè senza usare l'espressione per $\det(C)$ appena trovata, che se $c_0 + c_1 + \cdots + c_{n-1} = 0$ allora $\det(C) = 0$. Piú in generale (ma in modo analogo), mostrate direttamente che $\det(C) = 0$ se $c_0 + c_1 \omega + \cdots + c_{n-1} \omega^{n-1} = 0$ per una certa radice n -esima dell'unità ω .

Esercizio 31. Considerate la matrice n per n le cui entrate sulla diagonale principale valgono zero, e tutte le altre valgono uno. Calcolatene il determinante usando la formula trovata per il determinante di una matrice circolante.

Ora determinate esplicitamente gli autospazi della matrice (che è diagonalizzabile in quanto simmetrica), ricalcolando in tal modo il determinante.

Tuttavia, il modo piú efficiente per calcolare il determinante della matrice è probabilmente ottenerlo dal termine costante del suo polinomio caratteristico. Calcolate il polinomio caratteristico della matrice.

(Suggerimento per la terza parte: Notate che la matrice si ottiene sottraendo la matrice identità I_n alla matrice che ha tutte le entrate uguali ad uno. Il polinomio caratteristico cercato si può ricavare dal polinomio caratteristico di quest'ultima, che a sua volta è facile da scrivere, partendo dagli autovalori della matrice, che sono piuttosto evidenti.)

Esempio. Esaminiamo il risultato ottenuto sulle matrici circolanti per valori piccoli di n . È chiaro che per $n = 2$ abbiamo $\begin{vmatrix} x & y \\ y & x \end{vmatrix} = x^2 - y^2 = (x+y)(x-y)$. Per $n = 3$ scopriamo che il polinomio $\begin{vmatrix} x & y & z \\ z & x & y \\ y & z & x \end{vmatrix} = x^3 + y^3 + z^3 - 3xyz$ si scompone nel prodotto di fattori di primo grado $(x+y+z)(x+\omega y+\bar{\omega}z)(x+\bar{\omega}y+\omega z)$. Per $n = 4$,

$$\begin{vmatrix} x & y & z & t \\ t & x & y & z \\ z & t & x & y \\ y & z & t & x \end{vmatrix} = x^4 - y^4 + z^4 - t^4 - 4x^2yt + 4xy^2z - 4yz^2t + 4xzt^2 - 2x^2z^2 + 2y^2t^2$$

fattorizza come $(x+y+z+t)(x+iy-z-it)(x-y+z-t)(x-iy-z+it)$.

Esempio. Il determinante

$$\begin{vmatrix} x & y & z & t \\ y & x & z & t \\ z & t & x & y \\ t & z & y & x \end{vmatrix} = x^4 + y^4 + z^4 + t^4 - 2x^2y^2 - 2x^2z^2 - 2x^2t^2 - 2y^2z^2 - 2y^2t^2 - 2z^2t^2 + 8xyzt$$

è analogo al determinante di una matrice circolante, salvo che le varie righe contengono le indeterminate x, y, z, t permutate secondo il (o meglio, la rappresentazione regolare del) gruppo di Klein

$$V_4 = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$$

(il sottogruppo normale di ordine quattro del gruppo simmetrico S_4) anziché il gruppo ciclico $\{\text{id}, (1234), (13)(24), (1423)\}$. Non è difficile scoprire direttamente che il determinante fattorizza come $(x+y+z+t)(x+y-z-t)(x-y+z-t)(x-y-z+t)$. Analogamente alle matrici circolanti questo è strettamente legato alla trasformata di Fourier (ovvero, alla teoria delle rappresentazioni) del gruppo V_4 .

Lezione di venerdì 21 ottobre 2005 (tre ore): Altro sulle matrici circolanti. Ripasso di algebra: estensioni semplici di anelli, il polinomio minimo. Ripasso di algebra lineare: polinomio caratteristico e polinomio minimo, il teorema di Hamilton-Cayley, forma canonica di Jordan, matrice compagna di un polinomio.

Esercizio 32. Calcolate gli autovalori della matrice W , indipendentemente dal ragionamento fatto in precedenza, mostrando che essa ha polinomio caratteristico $t^n - 1$. (In particolare, la matrice è diagonalizzabile perché ha n autovalori distinti.)

(Suggerimento: Non mi pare semplice calcolare il determinante di $tI_n - W$ mediante operazioni elementari sulle righe e/o colonne. Infatti, alla fine della procedura, avendo portato W in forma triangolare, sulla diagonale dovrebbero comparire gli autovalori $e^{2\pi iz/n}$, e quindi è praticamente tanto difficile quanto calcolarsi gli autovettori “andando ad occhio”.

Piuttosto, un modo rapido di calcolare il polinomio caratteristico è calcolare il determinante di $tI_n - W$ usando la formula

$$\det(a_{j,k}) = \sum_{\sigma \in S_n} (-1)^\sigma a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

per il determinante. Un altro modo, piú concettuale, è usare il fatto che il polinomio minimo di una matrice, che in questo caso è $t^n - 1$, divide sempre il polinomio caratteristico grazie al teorema di Hamilton-Cayley.)

Teorema (di Hamilton-Cayley). *Sia $A = (a_{ij})$ una matrice n per n , e sia $p_A(t) = \det(tI_n - A)$ il suo polinomio caratteristico. Allora $p_A(A) = 0$. In altre parole, ogni matrice quadrata è radice del (ovvero, è annullata dal) suo polinomio caratteristico.*

Dimostrazione (omessa). Segue subito dalla teoria delle forme canoniche (razionale o di Jordan) per le matrici (si veda, ad esempio, [Jac]).

Tuttavia, per dimostrare il teorema è in realtà sufficiente sapere che ogni matrice quadrata a coefficienti complessi si può mettere in forma triangolare (e trovate una tale dimostrazione su [Lan]). \square

Una formulazione equivalente del teorema è la seguente: il polinomio minimo $p_A(t)$ di una matrice quadrata divide sempre il suo polinomio caratteristico $m_A(t)$. Un complemento importante al teorema è il fatto che il polinomio minimo ha le stesse radici, e quindi gli stessi fattori lineari in $\mathbb{C}[t]$, del polinomio caratteristico. Questo fatto segue immediatamente dal teorema stesso se notiamo che ogni autovalore λ di A è radice del polinomio minimo: infatti se $v \neq 0$ è un corrispondente autovettore, cioè $Av = \lambda v$, avremo $0 = m_A(A)v = m_A(\lambda)v$, e quindi $m_A(\lambda) = 0$.

3.2. Matrici circolanti non diagonalizzabili in caratteristica $p > 0$. La trasformata discreta su $\mathbb{Z}/n\mathbb{Z}$ si può fare anche su un campo di caratteristica positiva p , e le sue proprietà fondamentali continuano a valere (con l'esclusione dell'uguaglianza di Parseval, che dipende dall'esistenza di un prodotto Hermitiano nel caso complesso), purché il campo contenga una radice primitiva n -esima dell'unità (e quindi n radici n -esime distinte dell'unità, le sue potenze). Eventualmente ampliando il campo (o assumendolo algebricamente chiuso), ciò è possibile se e solo se il polinomio $t^n - 1$ ha radici distinte, vale a dire, grazie al criterio della derivata (cioè che $t^n - 1$ e la sua derivata nt^{n-1} siano polinomi coprimi), se e solo se n non è multiplo di p . Ad esempio, se $n = 6$ o 8 , la DFT non è definita sul campo con $p = 5$ elementi, ma lo è su quello con $p^2 = 25$ elementi. In particolare, la matrice W studiata in precedenza (cioè la matrice della traslazione di 1 rispetto alla base di $L^2(\mathbb{Z}/n\mathbb{Z})$ data dalle funzioni δ_i) rimane diagonalizzabile in caratteristica positiva p (su un campo sufficientemente grande) se (e solo se) p non divide n .

Il fallimento peggiore della DFT avviene, se vogliamo, quando n è una potenza di p . In tal caso 1 è l'unica radice n -esima dell'unità, essendo $t^n - 1 = (t - 1)^n$. In particolare, la matrice

$$W = [\delta_{(\text{mod } p)}(i, j + 1)]_{i,j=0,\dots,p-1} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

non è diagonalizzabile, anzi: il suo polinomio minimo coincide con il suo polinomio caratteristico $t^p - 1$. Dalla teoria della forma canonica di Jordan segue che W è simile ad un singolo blocco di Jordan (corrispondente all'unico autovalore 1). Ci possiamo chiedere quale sia una matrice (di cambiamento di base) che porta W in forma triangolare, e più precisamente nella forma canonica di Jordan, e quindi giochi un ruolo simile alla matrice della trasformata di Fourier, che qui non esiste.

Introduciamo la matrice (volendo anche infinita ma qui ci serve troncata p per p)

$$B = \left[\binom{i}{j} \right]_{i,j \geq 0} = \begin{bmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ \vdots & & & & \ddots \end{bmatrix}$$

La sua inversa è

$$B^{-1} = \left[(-1)^{i+j} \binom{i}{j} \right]_{i,j \geq 0} = \begin{bmatrix} 1 & & & & \\ -1 & 1 & & & \\ 1 & -2 & 1 & & \\ -1 & 3 & -3 & 1 & \\ \vdots & & & & \ddots \end{bmatrix}$$

Infatti l'entrata di posto (i, k) del prodotto della prima per la seconda vale

$$\begin{aligned} \sum_j \binom{i}{j} (-1)^{j+k} \binom{j}{k} &= \sum_j (-1)^{j+k} \frac{i!}{j!(i-j)!} \cdot \frac{j!}{k!(j-k)!} \\ &= \sum_j (-1)^{j+k} \frac{i!}{k!(i-k)!} \cdot \frac{(i-k)!}{(i-j)!(j-k)!} \\ &= \binom{i}{k} \sum_j (-1)^{j+k} \binom{i-k}{i-j} = \delta(i, k). \end{aligned}$$

Affermo che $B^{-1}WB = J^{-1}$, dove

$$J = [\delta(i, j) + \delta(i, j-1)]_{i,j} = \begin{bmatrix} 1 & 1 & 0 & 0 & \\ 0 & 1 & 1 & 0 & \\ 0 & 0 & 1 & 1 & \\ 0 & 0 & 0 & 1 & \\ & & & & \ddots \end{bmatrix}.$$

Equivalentemente, basta mostrare che $WBJ = B$. Infatti, l'entrata di posto (i, k) di WB è

$$\sum_j (\delta(i, j+1) + \delta(i, 0)\delta(j, p-1)) \binom{j}{k} = [i > 0] \binom{i-1}{k} + [i = 0] \binom{p-1}{k} \equiv \binom{i-1}{k},$$

tenendo conto che $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$. Perciò l'entrata di posto (i, k) di WBJ è

$$\sum_j \binom{i-1}{j} (\delta(i, j) + \delta(i, j-1)) = \binom{i-1}{k} + \binom{i}{k} = \binom{i-1}{k},$$

che è la corrispondente entrata di B .

Settima settimana. Lezione di lunedì 24 ottobre 2005 (tre ore): Relazioni fra trasformata di Fourier su $\mathbb{Z}/n\mathbb{Z}$ e $\mathbb{Z}/mn\mathbb{Z}$. La trasformata di Fourier veloce, o FFT. Uso della FFT per eseguire moltiplicazioni rapide.

4. LA TRASFORMATA DI FOURIER VELOCE O FFT (FAST FOURIER TRANSFORM)

4.1. Relazioni fra la DFT su un gruppo (ciclico) e su un suo sottogruppo o quoziente. Siano m, n interi positivi. Allora ciascuno dei gruppi ciclici di ordine m ed n si può vedere come sottogruppo, o anche come quoziente, del gruppo ciclico di ordine mn . (Infatti quest'ultimo ha un unico sottogruppo di ordine n , ad esempio, ed il corrispondente quoziente è ciclico di ordine m .) Per fissare le idee, consideriamo $\mathbb{Z}/n\mathbb{Z}$ come quoziente di $\mathbb{Z}/mn\mathbb{Z}$ modulo il suo sottogruppo $m\mathbb{Z}/mn\mathbb{Z}$ (che è ciclico di ordine n e quindi isomorfo a $\mathbb{Z}/n\mathbb{Z}$, un isomorfismo essendo associato ad esempio all'isomorfismo $m\mathbb{Z} \rightarrow \mathbb{Z}$ dato da $mx \mapsto x$). Più precisamente, abbiamo la sequenza esatta

$$0 \longrightarrow n\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

che dà luogo alla corrispondente sequenza esatta dei gruppi duali

$$1 \longleftarrow \widehat{n\mathbb{Z}/mn\mathbb{Z}} \longleftarrow \widehat{\mathbb{Z}/mn\mathbb{Z}} = \mu_{mn} \longleftarrow \widehat{\mathbb{Z}/n\mathbb{Z}} = \mu_n \longleftarrow 1.$$

(Qui abbiamo identificato $\widehat{\mathbb{Z}/n\mathbb{Z}}$ con il gruppo μ_n delle radici n -esime complesse dell'unità secondo l'isomorfismo $\chi \mapsto \chi(1)$.)

Se $f \in L^2(\mathbb{Z}/n\mathbb{Z})$ possiamo ottenerne una funzione $g \in L^2(\mathbb{Z}/mn\mathbb{Z})$ in modo naturale (che potremmo chiamare *ripetizione*) componendo con la proiezione $\mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, cioè ponendo $g(x) = f(x \bmod n)$. Allora

$$\hat{g}(a) = \begin{cases} m \hat{f}(a/m) & \text{se } m \mid a, \\ 0 & \text{altrimenti,} \end{cases}$$

che è, a parte il coefficiente m l'estensione a zero della trasformata di f .

D'altra parte, se $f \in L^2(m\mathbb{Z}/mn\mathbb{Z})$ possiamo ottenerne una funzione $g \in L^2(\mathbb{Z}/mn\mathbb{Z})$ in modo naturale estendendola a zero al di fuori del sottogruppo $m\mathbb{Z}/mn\mathbb{Z}$, cioè ponendo

$$g(x) = \begin{cases} f(x) & \text{se } m \mid x, \\ 0 & \text{altrimenti.} \end{cases}$$

Se preferiamo, visto che $m\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$, possiamo anche partire con $f \in L^2(\mathbb{Z}/n\mathbb{Z})$, nel qual caso porremo

$$g(x) = \begin{cases} f(x/m) & \text{se } m \mid x, \\ 0 & \text{altrimenti.} \end{cases}$$

In ogni caso avremo $\hat{g}(a) = \hat{f}(a \pmod{n})$.

Dunque la DFT, a parte un eventuale costante moltiplicativa, scambia i ruoli della ripetizione e della estensione a zero. C'era da aspettarselo, visto che questi sono i due modi naturali di estendere una funzione da un quoziente o un sottogruppo, e prendere i gruppi duali (e quindi anche passare alla DFT) rovescia il senso della sequenza esatta.

Esercizio 33. Verificare le formule espone per la DFT di una ripetizione e di una estensione a zero.

Esempio. Per capire meglio facciamo un esempio con $m = 3$ e $n = 2$. Rappresentiamo una funzione f su $\mathbb{Z}/k\mathbb{Z}$ con il vettore $(f(0), f(1), \dots, f(n-1))$ dei valori che essa assume su $0, 1, \dots, k-1$. Se (a, b) è una funzione su $\mathbb{Z}/2\mathbb{Z}$, ed (A, B) è la sua DFT (cioè, in

questo caso, $A = a + b$ e $B = a - b$), allora la funzione su $\mathbb{Z}/6\mathbb{Z}$ ottenuta per ripetizione è (a, b, a, b, a, b) , e la sua trasformata di Fourier è $(3A, 0, 0, 3B, 0, 0)$. Invece, se (a, b, c) è una funzione su $\mathbb{Z}/3\mathbb{Z} \cong 2\mathbb{Z}/6\mathbb{Z}$, ed (A, B, C) è la sua DFT, allora la funzione su $\mathbb{Z}/6\mathbb{Z}$ ottenuta per estensione a zero è $(a, 0, b, 0, c, 0)$, e la sua trasformata di Fourier è (A, B, C, A, B, C) .

Esempio. La funzione $f = \sum_{j=0}^{m-1} \delta_{jn} \in L^2(\mathbb{Z}/mn\mathbb{Z})$ si può pensare sia come ripetizione della funzione $\delta_0 \in L^2(\mathbb{Z}/n\mathbb{Z})$ che come estensione a zero della funzione $1 = e_0 \in L^2(\mathbb{Z}/m\mathbb{Z})$. In un modo o nell'altro (oltre che per calcolo diretto) otteniamo che la sua trasformata di Fourier è $\hat{f} = m \sum_{j=0}^{n-1} \delta_{jm} \in L^2(\mathbb{Z}/mn\mathbb{Z})$.

Notate che $\text{supp}(f) \cdot \text{supp}(\hat{f}) = mn = |G|$, dove $G = \mathbb{Z}/mn\mathbb{Z}$. In effetti in generale vale $\text{supp}(f) \cdot \text{supp}(\hat{f}) \leq |G|$ per ogni $f \in L^2(G)$ non identicamente nulla, si veda [Ter, p. 224]. Questa è una (anche se piuttosto banale) di varie versioni del *principio di indeterminazione* (il *principio di indeterminazione di Heisenberg* della meccanica quantistica è anch'esso legato a questo fatto), che un po' alla buona si può esprimere come segue: una funzione e la sua trasformata di Fourier non possono essere entrambe molto "concentrate".

4.2. La FFT. Supponiamo che $n = 2m$, poniamo $\omega_n = e^{2\pi i/n}$, $\omega_m = e^{2\pi i/m} = \omega_n^2$, e sia $f \in L^2(\mathbb{Z}/n\mathbb{Z})$. Allora

$$\begin{aligned} \hat{f}(a) &= \sum_{x=0}^{n-1} \omega_n^{-ax} f(x) = \sum_{y=0}^{m-1} \omega_n^{-a2y} f(2y) + \sum_{y=0}^{m-1} \omega_n^{-a(2y+1)} f(2y+1) = \\ &= \sum_{y=0}^{m-1} \omega_m^{-ay} f_0(y) + \omega_n^{-a} \sum_{y=0}^{m-1} \omega_m^{-ay} f_1(y) = \\ &= \hat{f}_0(a \pmod m) + \omega_n^{-a} \hat{f}_1(a \pmod m), \end{aligned}$$

dove abbiamo definito le funzioni $f_0, f_1 \in L^2(\mathbb{Z}/m\mathbb{Z})$ ponendo $f_0(x) = f(2x)$ e $f_1(x) = f(2x+1)$.

Osservazione. Abbiamo scritto f come la somma dell'estensione a zero della funzione f_0 e di una traslata dell'estensione a zero di f_1 . Quindi la formula per \hat{f} seguirebbe anche dalla discussione precedente sulla trasformata di Fourier di estensioni a zero. Nelle implementazioni pratiche della FFT (che qui non trattiamo) è conveniente adottare questo punto di vista.

Trascurando il calcolo delle potenze di ω_n , che possiamo supporre calcolate una volta per tutte, il calcolo della DFT \hat{f} (cioè di tutti i suoi valori) di una funzione f su $\mathbb{Z}/n\mathbb{Z}$ secondo la definizione comporta n^2 moltiplicazioni di numeri complessi (ed all'incirca lo stesso numero di addizioni). Lo abbiamo ridotto al calcolo delle DFT di due funzioni su $\mathbb{Z}/m\mathbb{Z}$, che insieme comportano $2m^2 = n^2/2$ moltiplicazioni (ed all'incirca lo stesso numero di addizioni). Per combinare i due risultati servono infine m moltiplicazioni (essendo $\omega_n^{a+m} = -\omega_n^a$, e $2m$ addizioni).

Se $n = 2^k$ possiamo iterare la procedura k volte. Poiché ogni volta si dimezza quasi il numero di moltiplicazioni, con k iterazioni tale numero dovrebbe diventare all'incirca $n^2/2^k = n$. In realtà un conto più preciso porta a $n(k+2)/2$ moltiplicazioni, che è circa $n \log_2 n$. Infatti, procedendo per induzione su k si vede che bastano tre moltiplicazioni quando $k = 1$, la base dell'induzione. Per il passo supponiamo di sapere che servono

$n(k+1)/4$ per la DFT su $\mathbb{Z}/(n/2)\mathbb{Z}$, cioè con $k-1$ iterazioni. Allora per la DFT su $\mathbb{Z}/n\mathbb{Z}$ servono $2 \cdot n(k+1)/4 + n/2 = n(k+2)/2$ operazioni, come si intendeva mostrare.

4.3. Uso della FFT per eseguire moltiplicazioni veloci. L'idea è che moltiplicare due numeri in forma decimale o binaria è molto simile a moltiplicare due polinomi, a coefficienti reali ma con valori in $\{0, \dots, 9\}$ o $\{0, 1\}$, con la differenza che ci sono i riporti. Come abbiamo visto in precedenza, moltiplicare due polinomi equivale a calcolare la convoluzione delle sequenze dei coefficienti. D'altra parte, un polinomio di grado minore di n è determinato in modo unico dai valori che assume su n numeri reali o complessi distinti. Quindi, se abbiamo due polinomi di grado minore di $n/2$, un modo per moltiplicarli è

- (1) valutarli entrambi su n numeri complessi distinti,
- (2) moltiplicare i rispettivi valori, ed infine
- (3) risalire all'unico polinomio di grado minore di n che assume questi valori.

Il secondo passaggio richiede solo n moltiplicazioni, invece che le circa $n^2/4$ necessarie a calcolare la convoluzione delle sequenze dei coefficienti. Purtroppo, se gli n numeri complessi su cui sono valutati i polinomi sono scelti arbitrariamente, il passo (1) richiede da solo circa $n^2/2$ moltiplicazioni. Ma se scegliamo come punti le radici n -esime complesse dell'unità, il passo (1) diventa una DFT ed il passo (3) la sua inversa (e quindi essenzialmente una DFT). Usando la FFT dovrebbero quindi bastare all'incirca (a meno di una costante moltiplicativa) $n \log n$ moltiplicazioni, che in realtà sono $n(\log n)(\log \log n)$ tenendo conto di dettagli che qui abbiamo trascurato.

Osservazione. In generale, il passo (3) della procedura descritta, cioè la ricostruzione di un polinomio $f(x)$ di grado minore di n dai valori che assume su n numeri complessi distinti $\alpha_1, \dots, \alpha_n$ si può eseguire mediante la formula di interpolazione di Lagrange $f(x) = \sum_j f(\alpha_j) \prod_{k \neq j} (x - \alpha_k) / (\alpha_j - \alpha_k)$. Dato che i polinomi $\prod_{k \neq j} (x - \alpha_k) / (\alpha_j - \alpha_k)$ di grado $n-1$ si possono pensare come precalcolati, considerando i numeri α_j come fissati una volta per tutte, e variabili solo i valori $f(\alpha_j)$, vediamo che il passo (3) comporta n^2 moltiplicazioni di numeri complessi.

Esercizio 34. Applicate la formula di interpolazione di Lagrange al caso in cui i numeri $\alpha_1, \dots, \alpha_n$ sono le radici n -esime dell'unità $1, \omega, \dots, \omega^{n-1}$, dove $\omega = e^{2\pi i/n}$. Ritrovate così la formula di inversione di Fourier, nella forma

$$f(x) = \frac{1}{n} \sum_k \left(\sum_j f(\omega^j) \omega^{-jk} \right) x^k.$$

(Suggerimento: Calcolando il termine noto del polinomio $((x+1)^n - 1) / ((x+1) - 1)$ trovate che $\prod_{k \neq 0} (\omega^k - 1) = (-1)^{n-1} n$, e quindi $\prod_{k \neq 0} (1 - \omega^k) = n$. Ne segue che $\prod_{k \neq j} (\omega^j - \omega^k) = n \omega^{-j}$. Infine, $\prod_{k \neq j} (x - \omega^k) = (x^n - 1) / (x - \omega^j) = \sum_l x^l (\omega^j)^{n-1-l}$.)

Lezione di venerdì 28 ottobre 2005 (tre ore): Cenni alla struttura dei gruppi abeliani finiti. Caratteri e trasformata di Fourier per un gruppo abeliano finito. [Omesso: operatori diagonalizzabili che commutano sono diagonalizzabili simultaneamente.]

Introduzione al gruppo duale: caratteri (unitari e continui) del gruppo \mathbb{T} e dualità fra \mathbb{T} e \mathbb{Z} (continuazione).

[Omessi: indipendenza lineare dei caratteri di \mathbb{T} , di \mathbb{R} e di un gruppo qualsiasi; relazione fra serie di Fourier e serie di Taylor.]

5. LA TRASFORMATA DI FOURIER SU GRUPPI ABELIANI FINITAMENTE GENERATI

5.1. Struttura dei gruppi abeliani finitamente generati. Ogni gruppo abeliano finito G è isomorfo ad un prodotto diretto di gruppi ciclici finiti (senza dimostrazione):

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

I numeri n_1, \dots, n_r sono unicamente determinati se richiediamo che ciascuno divida il successivo. Il numero minimo di generatori di G è r . Più in generale, ogni gruppo abeliano finitamente generato è isomorfo al prodotto diretto di un numero finito di gruppi ciclici:

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}.$$

(o anche la stessa formula precedente, se ammettiamo che gli n_i da un certo punto in poi possano valere zero, essendo $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$). Di nuovo, i numeri n_1, \dots, n_r sono unicamente determinati se richiediamo che ciascuno divida il successivo, ed unicamente determinato è anche il numero di copie di \mathbb{Z} (il *rango libero* di G).

5.2. Caratteri dei gruppi abeliani finitamente generati, e la relativa trasformata di Fourier. Fissato un sistema di generatori g_1, g_2, \dots per G corrispondente alla decomposizione in prodotto diretto di gruppi ciclici scritta sopra, diciamo $g_1 = (1, 0, \dots, 0)$, $g_2 = (0, 1, \dots, 0)$, e così via, un carattere $\chi : G \mapsto \mathbb{T}$ è determinato in modo unico dai valori che prende su g_1, g_2, \dots, g_r . Inoltre dovrà valere $\chi(g_j)^{n_j} = \chi(0) = 1$ per ogni j , cioè $\chi(g_j)$ dovrà essere una radice n_j -esima dell'unità (da interpretare come una condizione vuota se $n_j = 0$). A parte questa condizione, i valori $\chi(g_j)$ possono essere assegnati arbitrariamente (naturalmente con $\chi(g_j) \in \mathbb{T}$ se $n_j = 0$). Perciò, nel caso in cui G è finito, il suo gruppo dei caratteri \hat{G} è isomorfo a $\mu_1 \times \cdots \times \mu_r$, e quindi a G stesso (ma l'isomorfismo non è canonico, dipendendo dalla scelta dei generatori g_1, g_2, \dots). Nel caso più generale in cui G è solo finitamente generato, il gruppo dei caratteri è $\mu_1 \times \cdots \times \mu_r \times \mathbb{T} \times \cdots \times \mathbb{T}$.

Nel caso di G finito l'ortogonalità dei caratteri di G si dimostra in modo analogo al caso di $\mathbb{Z}/n\mathbb{Z}$, e nello stesso modo seguono le proprietà principali (1)–(4) della trasformata di Fourier, che per $f \in L^2(G)$ è la funzione $\hat{f} \in L^2(\hat{G})$ data da

$$\hat{f}(\chi) = \sum_{x \in G} f(x)\chi(-x) = \langle f, \chi \rangle.$$

In particolare, vale la formula di inversione

$$f(x) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x).$$

Nel caso di G finitamente generato, il gruppo \hat{G} è dotato di una misura opportunamente definita (la *misura di Haar*, che è l'unica misura su \hat{G} che sia invariante per traslazioni e tale che G abbia misura totale 1), e la formula di inversione è data dall'integrale

$$f(x) = \int_{\hat{G}} \hat{f}(\chi)\chi(x) d\chi.$$

Notate che anche in questo caso caratteri distinti sono linearmente indipendenti (ne vedremo una dimostrazione nella prossima sezione, in un contesto più generale), ma non ha nemmeno senso parlare di ortogonalità, in quanto se G è infinito essi non appartengono nemmeno allo spazio $L^2(G)$.

5.3. La trasformata di Fourier su \mathbb{Z} . Consideriamo un po' in dettaglio il caso di $G = \mathbb{Z}$. Un carattere χ è determinato dal valore di $\chi(1)$; questo è un elemento di \mathbb{T} , diciamo $e^{2\pi ia}$ per qualche $a \in [0, 1)$, che può essere assegnato arbitrariamente. Qui stiamo identificando il gruppo dei caratteri \mathbb{T} con \mathbb{R}/\mathbb{Z} , rappresentato in pratica dall'intervallo $[0, 1)$. L'ordinaria misura di Lebesgue su $[0, 1)$, meglio pensata su \mathbb{R}/\mathbb{Z} , è certo invariante per traslazioni, e l'intero spazio ha misura 1; quindi essa è proprio la misura di Haar. (Se preferiamo parametrizzare gli elementi di \mathbb{T} come e^{ia} per qualche $t \in [0, 2\pi)$ o, equivalentemente, $t \in (-\pi, \pi]$, la misura di Haar sarà la misura di Lebesgue su $t \in [0, 2\pi)$ divisa per 2π .) La definizione di trasformata di Fourier e la formula di inversione diventano

$$\hat{f}(a) = \sum_{x \in \mathbb{Z}} f(x) e^{-2\pi i a x} \quad \text{e} \quad f(x) = \int_0^1 \hat{f}(a) e^{2\pi i a x} da,$$

valide per $f \in L^2(\mathbb{Z})$, nel qual caso abbiamo $\hat{f} \in L^2(\mathbb{T})$, e vale l'uguaglianza di Parseval $\|f\|_2 = \|\hat{f}\|_2$, cioè

$$\sum_{x \in \mathbb{Z}} |f(x)|^2 = \int_0^1 |\hat{f}(a)|^2 da.$$

Naturalmente, le formule per la trasformata di Fourier su \mathbb{Z} e la sua inversa sono essenzialmente le stesse, ma scambiate di ruolo, che le note formule per le serie di Fourier (che sono la trasformata di Fourier su \mathbb{T}) ripassate all'inizio del corso.

Esercizio 35. Verificate che, se n è un intero non negativo (anche se, interpretando opportunamente, vale per ogni n reale non negativo), la trasformata di Fourier della funzione su \mathbb{Z} definita da $x \mapsto \binom{n}{x}$ è la funzione su \mathbb{R}/\mathbb{Z} , cioè in pratica su $[0, 1)$, data da $a \mapsto 2^n \cos^n(\pi a) \exp(-\pi i n a)$. In particolare, per n pari la funzione $x \mapsto \binom{n}{n/2+x}$ (che è la precedente traslata in modo da divenire simmetrica) ha come trasformata di Fourier la funzione $a \mapsto 2^n \cos^n(\pi a)$.

Notate che, in entrambi i casi dell'Esercizio, la trasformata di Fourier è la potenza n -esima (nel senso normale della moltiplicazione di funzioni) della stessa per $n = 1$. Infatti la funzione $x \mapsto \binom{n}{x}$ è la potenza n -esima rispetto alla convoluzione della funzione $x \mapsto \binom{1}{x} = \delta_0 + \delta_1$, grazie all'Esercizio 8, e come sappiamo la trasformata di Fourier scambia moltiplicazione e convoluzione di funzioni.

5.4. Operatori diagonalizzabili che commutano sono diagonalizzabili contemporaneamente. Il fatto che gli operatori di traslazione per elementi di G siano diagonalizzabili contemporaneamente (e siano diagonalizzati dalla trasformata di Fourier) continua a valere per ogni gruppo abeliano finito. Infatti i caratteri formano una base per $L^2(G)$ e sono autovettori per gli operatori di traslazione: per ogni carattere χ abbiamo $T_y \chi(x) = \chi(x - y) = \chi(-y) \chi(x)$, cioè $T_y \chi = \chi(-y) \chi$.

In realtà la diagonalizzabilità simultanea degli operatori di traslazione viene anche come conseguenza del seguente risultato molto più generale (quindi senza bisogno di esibire esplicitamente degli autovettori come appena fatto): se \mathcal{A} è un insieme di operatori lineari diagonalizzabili su uno spazio vettoriale V di dimensione finita, e gli elementi di \mathcal{A} commutano fra loro, allora essi sono diagonalizzabili contemporaneamente.

Cenno di dimostrazione. Il punto cruciale è che se due operatori lineari F, G su V commutano, allora gli autospazi di ciascuno sono invarianti sotto l'azione dell'altro. Infatti, se $v \in V$ è un autovettore per F con autovalore α , allora $FGv = GFv = \alpha Gv$, cioè anche Gv è autovettore per F con autovalore α . Ne segue che se $V = \bigoplus_{\alpha} V_{\alpha}$ e $V = \bigoplus_{\beta} W_{\beta}$

sono le decomposizioni in autospazi per F e G , allora $V_\alpha = \bigoplus_\beta (V_\alpha \cap W_\beta)$, e quindi $V = \bigoplus_\alpha \bigoplus_\beta (V_\alpha \cap W_\beta)$. Poiché sia F che G agiscono scalarmente su ciascuna intersezione $V_\alpha \cap W_\beta$, le abbiamo “diagonalizzate” entrambe contemporaneamente. Iterando opportunamente questo ragionamento si giunge alla conclusione. \square

Piú in generale, nello stesso modo si mostra che se \mathcal{A} è un insieme di operatori lineari (arbitrari) su uno spazio vettoriale V di dimensione finita, e gli elementi di \mathcal{A} commutano fra loro, allora essi si possono portare simultaneamente in forma triangolare (superiore, diciamo), diagonalizzando quelli fra loro che sono diagonalizzabili.

Sotto certe condizioni il fatto appena dimostrato si può generalizzare ancora molto (ai gruppi di matrici (di Lie, o algebrici) connessi risolubili, per i quali si chiama *Teorema di Lie-Kolchin*).

6. LA TRASFORMATA DI FOURIER SU \mathbb{T}

6.1. Un punto di vista nuovo sui caratteri del gruppo ciclico di ordine n . Se, invece del gruppo ciclico $\mathbb{Z}/n\mathbb{Z}$, prendiamo il gruppo ad esso isomorfo (tramite la mappa $x \mapsto e^{2\pi i x/n}$)

$$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\},$$

cioè il gruppo delle radici complesse n -esime dell'unità, i caratteri prendono una forma particolarmente semplice: essi sono le mappe $z \mapsto z^a$, per $a = 0, \dots, n-1$ (o anche $a \in \mathbb{Z}/n\mathbb{Z}$, se vogliamo). Infatti le mappe “potenza” $z \mapsto z^a$ per $a \in \mathbb{Z}$ sono tutte distinte come mappe di \mathbb{C} in \mathbb{C} , o anche solo (e qui piú appropriatamente) di \mathbb{T} in \mathbb{T} , ma ristrette al sottogruppo finito μ_n di \mathbb{T} coincidono per valori dell'indice a congrui modulo n . Vediamo quindi come il gruppo dei caratteri del gruppo ciclico μ_n si possa pensare naturalmente come il quoziente $\mathbb{Z}/n\mathbb{Z}$ del gruppo \mathbb{Z} , corrispondente all'insieme delle mappe potenza rispetto alla composizione. (Ricordate che in precedenza abbiamo visto come il gruppo dei caratteri di $\mathbb{Z}/n\mathbb{Z}$ si identifichi naturalmente con μ_n , associando ad ogni carattere il suo valore su $1 \in \mathbb{Z}/n\mathbb{Z}$. Qui accade esattamente il contrario, e non c'è da sorprendersi.)

Questo punto di vista illustra bene un aspetto della dualità fra un gruppo ed il suo gruppo dei caratteri che abbiamo già considerato nelle sezioni precedenti: a sottogruppi del gruppo corrispondono quozienti del suo gruppo dei caratteri, e viceversa. Infatti se m è un multiplo di n allora μ_n è un sottogruppo di μ_m , mentre il gruppo dei caratteri di μ_n è un quoziente del gruppo dei caratteri di μ_m (essendo, alla buona, costituito dalle stesse mappe $z \mapsto z^a$ con $a \in \mathbb{Z}/m\mathbb{Z}$ ma leggendo l'indice a modulo il divisore n di m).

È istruttivo riscrivere la formula della trasformata di Fourier su un gruppo ciclico finito e la formula di inversione nella notazione appena introdotta, cioè per funzioni definite su μ_n . La trasformata di Fourier di $f \in L^2(\mu_n)$ è la funzione $\hat{f} \in L^2(\mathbb{Z}/n\mathbb{Z})$ data da

$$\hat{f}(a) = \sum_{z \in \mu_n} f(z) z^{-a},$$

e la formula di inversione è

$$f(z) = \frac{1}{n} \sum_{a \in \mathbb{Z}/n\mathbb{Z}} \hat{f}(a) z^a.$$

6.2. I caratteri di \mathbb{T} , e la relativa trasformata di Fourier. Alla buona, possiamo pensare ai gruppi μ_n , al crescere di n , come a delle approssimazioni sempre migliori del gruppo continuo (cioè topologico) \mathbb{T} . È chiaro che fra i caratteri del gruppo $\mu_\infty = \bigcup_{n=1}^{\infty} \mu_n$ delle radici dell'unità (di ordine arbitrario) ci sono le mappe potenza $z \mapsto z^a$ per $a \in \mathbb{Z}$ (che stavolta sono tutte distinte). Di nuovo, notate che abbiamo costruito μ dai suoi sottogruppi finiti μ_n , ed il suo duale \mathbb{Z} dai suoi quozienti finiti $\mathbb{Z}/n\mathbb{Z}$.

Osservazione. Le mappe potenza non sono *tutti* i caratteri di μ , cioè gli omomorfismi di gruppo di μ in \mathbb{T} , o, equivalentemente, in μ stesso). Anzi, esse formano una minoranza fra i caratteri di μ , che corrispondono invece al gruppo $\hat{\mathbb{Z}}$ (in questo caso il segno $\hat{}$ sopra a \mathbb{Z} ha un significato diverso da quello con cui l'abbiamo utilizzato noi), la *chiusura profinita* di \mathbb{Z} . Dunque, come gruppo discreto, μ ha per duale il gruppo compatto $\hat{\mathbb{Z}}$. Però le mappe potenza sono i soli caratteri continui, nella topologia usuale di μ , come sottoinsieme di \mathbb{C} .

Naturalmente le mappe potenza sono anche caratteri di \mathbb{T} (che è la chiusura topologica di μ in \mathbb{C}). Anzi, esse sono tutti i caratteri continui di \mathbb{T} : il gruppo duale di \mathbb{T} , cioè il gruppo dei caratteri di \mathbb{T} , è isomorfo a \mathbb{Z} .

Esercizio 36. Mostrate almeno che le funzioni potenza sono tutti i caratteri *differenziabili* di \mathbb{T} . (In questo caso poi la differenziabilità è una conseguenza della continuità (senza dimostrazione), e quindi le mappe potenza $z \mapsto z^a$ per $a \in \mathbb{Z}$ sono tutti i caratteri continui di \mathbb{T} .) Per farlo vi conviene mettervi in una situazione più generale, notando che \mathbb{T} è isomorfo a \mathbb{R}/\mathbb{Z} come gruppo topologico (tramite $x \mapsto e^{ix}$): mostrate che tutti i caratteri differenziabili (unitari, cioè con immagine in \mathbb{T}) del gruppo \mathbb{R} sono dati dalle mappe $x \mapsto e^{iax}$, al variare di $a \in \mathbb{R}$. (Dunque il duale di \mathbb{R} è \mathbb{R} stesso. Per questo la trasformata di Fourier di una funzione definita su \mathbb{R} è anch'essa definita su \mathbb{R} .) Ne segue che i caratteri differenziabili di \mathbb{T} sono quelli fra questi che hanno \mathbb{Z} nel nucleo, cioè quelli con $a \in \mathbb{Z}$.

(Suggerimento: Per definizione, un carattere differenziabile $\chi : \mathbb{R} \mapsto \mathbb{T} \subseteq \mathbb{C}$ soddisfa $\chi(x+y) = \chi(x)\chi(y)$ per ogni $x, y \in \mathbb{R}$. Derivando rispetto ad y e quindi ponendo $y = 1$ trovate l'equazione differenziale $\chi'(x) = \chi(0)\chi(x)$ che, risolta e tenendo conto dell'unitarietà, porta alla conclusione desiderata.)

A proposito dello svolgimento di quest'ultimo esercizio, notate che nel caso continuo (in questo caso di $G = \mathbb{T}$, oppure $G = \mathbb{R}$ nel caso della trasformata di Fourier di funzioni definite su \mathbb{R}) l'operatore di derivazione gioca un ruolo simile a quello degli operatori di traslazione (o convoluzione con delle funzioni delta) del caso discreto. Infatti l'operatore di derivazione si può pensare come un operatore di traslazione *infinitesimale*:

$$\frac{d}{dx} = \lim_{h \rightarrow 0} \frac{T_{-h} - T_0}{h}$$

(Volendo, anche qui possiamo pensare la traslazione $T_{-h}f$ come convoluzione $\delta_h * f$, solo che δ_h va letto non come la funzione che vale 1 in h e zero altrove, bensì come una distribuzione, di massa unitaria concentrata in h .) Dunque nel caso continuo la trasformata di Fourier diagonalizza non solo gli operatori di traslazione (o, più in generale, di convoluzione) ma anche gli operatori differenziali. (In realtà tutti questi operatori, di traslazione e differenziali, si possono interpretare come casi speciali di operatori di convoluzione con opportune distribuzioni.) Da qui segue l'utilità delle serie di Fourier, o più in generale della trasformata di Fourier su \mathbb{R} (o della sua estensione, la trasformata di Laplace) per il trattamento delle equazioni differenziali.

Esercizio 37. Mostrate che i caratteri (continui) di \mathbb{T} (cioè le funzioni potenza $x \mapsto x^a$ per $a \in \mathbb{Z}$) sono linearmente indipendenti.

(Suggerimento: Avete a che fare essenzialmente (per $a \geq 0$) con funzioni polinomiali, ristrette al sottoinsieme \mathbb{T} di \mathbb{C} . La conclusione segue dal fatto che \mathbb{T} è infinito, mentre una funzione polinomiale non nulla ha un numero finito di zeri.)

La conclusione dell'esercizio precedente segue anche dal prossimo esercizio, che tratta una situazione più generale.

Esercizio 38. Mostrate che i caratteri (unitari e continui, quindi in realtà differenziabili) di \mathbb{R} (cioè le funzioni $x \mapsto e^{iax}$ per $a \in \mathbb{R}$) sono linearmente indipendenti.

(Suggerimento: Scritta una combinazione lineare nulla di r caratteri distinti, differenziatele $n - 1$ volte, e ricordate il determinante di Vandermonde.)

In realtà l'indipendenza lineare dei caratteri è un fatto più generale, che non dipende affatto dalla loro differenziabilità. (La dimostrazione che stiamo per dare è una versione discreta della dimostrazione differenziale dell'esercizio precedente.) Il fatto generale è il seguente: omomorfismi distinti di un gruppo G nel gruppo moltiplicativo di un campo K (anzi, volendo, di un monoide G nel monoide moltiplicativo di un campo K) sono linearmente indipendenti.

Dimostrazione. Supponiamo che esista una relazione lineare non banale $\alpha_1\chi_1 + \dots + \alpha_r\chi_r = 0$ fra omomorfismi distinti $\chi_1, \dots, \chi_r : G \mapsto K^*$, con r minimo. Chiaramente $r > 1$, essendo gli omomorfismi χ_j funzioni non nulle. Essendo r minimo, tutti i coefficienti $\alpha_1, \dots, \alpha_r$ sono non nulli. Essendo $\chi_1 \neq \chi_2$, esiste $h \in G$ tale che $\chi_1(h) \neq \chi_2(h)$. Per ogni $g \in G$ avremo allora

$$0 = \alpha_1\chi_1(gh) + \dots + \alpha_r\chi_r(gh) = \alpha_1\chi_1(g)\chi_1(h) + \dots + \alpha_r\chi_r(g)\chi_r(h),$$

e quindi $\alpha_1\chi_1(h)\chi_1 + \dots + \alpha_r\chi_r(h)\chi_r = 0$. Sottraendo da questa relazione iniziale moltiplicata per $\chi_1(h)$ otteniamo la relazione non banale

$$\alpha_2(\chi_2(h) - \chi_1(h))\chi_2 + \dots + \alpha_r(\chi_r(h) - \chi_1(h))\chi_r = 0,$$

che fornisce una contraddizione con la nostra assunzione che r fosse minimo. \square

Ora dotiamo il gruppo \mathbb{T} della misura di Haar, cioè l'unica misura invariante per traslazioni e tale che \mathbb{T} abbia misura complessiva 1. Specificare una misura su \mathbb{T} equivale a specificare l'integrale su \mathbb{T} di una funzione arbitraria f : si tratta dell'integrale curvilineo

$$\frac{1}{2\pi i} \int_{\mathbb{T}} f(z)z^{-1}dz = \int_0^1 f(e^{2\pi it})dt$$

(cioè stiamo considerando la misura su \mathbb{T} associata al differenziale $dz/2\pi iz$). Lo spazio $L^2(\mathbb{T})$ è spazio di Hilbert rispetto al prodotto Hermitiano

$$\langle f, g \rangle = \frac{1}{2\pi i} \int_{\mathbb{T}} f(z)\overline{g(z)}z^{-1}dz.$$

Avendo assunto la misura totale di G uguale ad 1, ogni carattere di \mathbb{T} ha norma 1. La trasformata di Fourier di $f \in L^2(\mathbb{T})$ è la funzione $\hat{f} \in L^2(\mathbb{Z})$ data da $\hat{f}(a) = \langle f, \chi_a \rangle$, dove χ_a è il carattere $z \mapsto z^a$. Quindi

$$\hat{f}(a) = \frac{1}{2\pi i} \int_{\mathbb{T}} f(z)z^{-a-1}dz,$$

e si mostra che vale la formula di inversione

$$f(z) = \sum_{a \in \mathbb{Z}} \hat{f}(a) z^a.$$

Naturalmente queste sono, scritte in notazione diversa, le familiari formule per le serie di Fourier ricordate all'inizio del corso.

Notate che le formule per la trasformata di Fourier su \mathbb{T} si possono formalmente ottenere a quelle scritte in precedenza per la trasformata di Fourier su μ_n , facendo tendere n a infinito, dopo aver spostato il fattore $1/n$ dalla formula di inversione alla definizione di trasformata di Fourier.

6.3. Una relazione fra serie di Fourier e serie di Taylor. La formula di inversione per la trasformata di Fourier su \mathbb{T} come scritta sopra assomiglia formalmente alla serie di Taylor (se $\hat{f}(a) = 0$ per $a < 0$, ma piú in generale una serie di Laurent) per una funzione f , dove i valori $\hat{f}(a)$ assumono il ruolo di coefficienti di Taylor.

In effetti, se f è una funzione olomorfa su un'aperto di \mathbb{C} contenente \mathbb{T} , allora essa ammette un'espansione come serie bilatera $f(z) = \sum_{a \in \mathbb{Z}} c_a z^a$ in una regione aperta a forma di anello e contenente \mathbb{T} , ed i coefficienti c_a si possono calcolare come $c_a = \frac{1}{2\pi i} \int_{\mathbb{T}} f(z) z^{-a-1} dz$.

Dato che il trattamento delle serie bilatere si riduce a trattare separatamente la parte positiva e quella negativa, limitiamoci ad una situazione piú semplice, quella di una funzione f olomorfa su un'aperto di \mathbb{C} contenente il disco chiuso $= \{z \in \mathbb{C} \mid |z| \leq 1\}$. In questo caso la sua serie di Taylor ha raggio di convergenza ρ maggiore di 1, ed in particolare converge a f su D : $f(z) = \sum_{a=0}^{\infty} c_a z^a$ per ogni $z \in D$. Il coefficiente c_a si può allora calcolare come il residuo della funzione $f(z) z^{-a-1}$ nell'origine, e quindi come l'integrale $c_a = \frac{1}{2\pi i} \int_{\mathbb{T}} f(z) z^{-a} dz$ (dove al posto di T avremmo potuto mettere qualsiasi curva chiusa contenuta in $D \setminus \{0\}$ che passi intorno all'origine esattamente una volta in senso antiorario). Dunque in questo caso speciale l'inversione di Fourier segue da noti risultati di analisi complessa. La stessa ortogonalità dei caratteri corrisponde al fatto che la funzione $z \mapsto z^a z^{-b-1}$ ha residuo 0 nell'origine ad eccezione di quando $a = b$, nel qual caso essa ha residuo 1.

Naturalmente la situazione appena descritta rende conto solo del caso in cui la funzione su \mathbb{T} di cui studiamo la trasformata di Fourier è la restrizione di una funzione olomorfa f su un aperto contenente D . Se cosí è, la f su D si può ricavare dalla sua restrizione a \mathbb{T} mediante la formula integrale di Cauchy $f(w) = \frac{1}{2\pi i} \int_{\mathbb{T}} \frac{f(z)}{z-w} dz$. D'altra parte, anche le trasformate di Fourier trattabili in questo modo sono lontane dall'essere funzioni generiche in $L^2(\mathbb{Z})$ (anche a parte la condizione che $\hat{f}(a) = 0$ per $a < 0$): come minimo dovranno essere funzioni L^1 , a causa della condizione che la serie $\sum_{a=0}^{\infty} c_a z^a$ abbia raggio di convergenza maggiore di 1, da cui $\sum_{a=0}^{\infty} |c_a| < \infty$.

RIFERIMENTI BIBLIOGRAFICI

- [Lan] Serge Lang, *Algebra Lineare*, Boringhieri, 1970.
- [Jac] Nathan Jacobson, *Basic Algebra I*, W. Freeman and Company, San Francisco, 1974.
- [Ter] Audrey Terras, *Fourier Analysis on Finite Groups and Applications*, LMS Student Text, vol. 43, Cambridge University Press, 1999.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI TRENTO, VIA SOMMARIVE 14, 38050 POVO (TRENTO)

E-mail address: mattarei@science.unitn.it