Università degli Studi di Pisa


Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica

# Funzioni simmetriche e polinomi di Newton

26 settembre 2008

Tesi di Laurea

Candidato
**Maurizio Monge**
maurizio.monge@gmail.com

Relatore
**Prof. Roberto Dvornicich**
Università di Pisa

Controrelatore
**Prof. Rocco Chirivì**
Università di Pisa

Anno Accademico 2007/2008

# Introduzione

> There's a fine line between fishing and
> standing on the shore looking like an idiot.
>
> *Steven Wright*

In questa tesi presentiamo la teoria classica delle funzioni simmetriche con le sue applicazioni allo studio dei caratteri del gruppo simmetrico. Studiamo inoltre il problema di stabilire quando il campo delle funzioni simmetriche in $n$ variabili sia generato da polinomi di Newton.

Mostriamo più da vicino di cosa si tratta. Se $x_1, \dots, x_n$ sono elementi algebricamente indipendenti su $\mathbb{Q}$, possiamo considerare il campo delle funzioni razionali $F = \mathbb{Q}(x_1, \dots, x_n)$, i cui elementi sono frazioni di polinomi in $x_1, \dots, x_n$. Sia inoltre $S \subset F$ il sottocampo costituito dalle funzioni simmetriche in $x_1, \dots, x_n$, ovvero dagli elementi di $F$ lasciati invariati da qualunque permutazione delle variabili $x_1, \dots, x_n$.

L'$r$-esimo polinomio di Newton (o somma di potenze) in $x_1, \dots, x_n$ è definito come

$$N_r = x_1^r + \cdots + x_n^r.$$

È chiaro che il campo generato su $\mathbb{Q}$ da una qualunque collezione di tali polinomi deve essere contenuto nel campo delle funzioni simmetriche $S$, essendo essi tutti simmetrici.

Una problema tutt'altro che banale è però quello di stabilire quando il campo generato dai polinomi di Newton $N_{a_1}, \dots, N_{a_m}$, per qualche $m$-upla di interi distinti $a = (a_1, \dots, a_m)$, sia tutto $S$.

È possibile trovare immediatamente alcune condizioni necessarie, in particolare è necessario che $m \geq n$, perché in caso contrario il grado di trascendenza su $\mathbb{Q}$ del campo generato dagli $N_{a_1}, \dots, N_{a_m}$ è minore di $n$, il numero di variabili.

È inoltre necessario che gli $a_1, \dots, a_m$ siano coprimi. Qualora essi abbiano un fattore comune $d \neq 1$ il campo che si ottiene è infatti un sottocampo del campo $S^{(d)}$ delle funzioni simmetriche nelle potenze $d$-esime $x_1^d, \dots, x_n^d$, e quindi è contenuto strettamente in $S$.

Restringendoci al caso in due variabili, non è difficile stabilire che due soli polinomi di Newton non generano mai l'intero campo simmetrico, a meno che non si tratti della coppia $N_1, N_2$ o della coppia $N_1, N_3$. Questo fatto ad esempio segue immediatamente dai risultati ottenuti da Mead e Stein in [MS98], dove

viene fornita una formula esplicita per il grado $[S : \mathbb{Q}(N_a, N_b)]$ per ogni coppia di interi distinti e coprimi $a, b$.

Se invece consideriamo il campo generato da tre tali polinomi

$$N_a = x^a + y^a, \qquad N_b = x^b + y^b, \qquad N_c = x^c + y^c,$$

con $a, b, c$ interi positivi, distinti e tali che $(a, b, c) = 1$, abbiamo che essi sono sempre sufficienti per generare l'intero campo delle funzioni simmetriche in caratteristica zero.

Questo è un risulato di Dvornicich e Zannier pubblicato in [DZ03] che dà una risposta affermativa a una congettura di Mead e Stein apparsa in [MS98]. La dimostrazione di questo risultato fa uso della teoria delle derivazioni sui campi e del teorema di esistenza Riemman, impiegato al fine di ottenere il gruppo di Galois di un particolare polinomio che risulterà essere una relazione fra certi elementi coniugati sul campo generato da $N_a, N_b, N_c$. Si mostra che tale gruppo deve essere l'intero gruppo delle permutazioni delle radici, e che se il campo generato da $N_a, N_b, N_c$ non dovesse essere tutto $S$ è possibile giungere rapidamente un assurdo agendo con il gruppo di Galois su alcune equazioni che devono essere soddisfatte da tali elementi.

Un lavoro originale di questa tesi mira a ottenere un risultato analogo in caratteristica positiva. Mostreremo in particolare che se si richiede addizionalmente che $a, b, c, a - b, a - c, b - c$ siano primi con la caratteristica $p$, allora anche in questo caso $N_a, N_b, N_c$ sono sufficienti per generare l'intero campo delle funzioni simmetriche. Qualora queste ipotesi non siano soddisfatte, esibiremo inoltre una famiglia di controesempi, che in particolare mostra che è necessario richiedere che le differenze $a - b, a - c, b - c$ siano prime con $p$.

La dimostrazione del risultato positivo si vedrà essere conseguenza dell'irriducibilità di polinomi simmetrici che costituiscono una relazione fra i coniugati di $x$. Per ottenere questo risultato sarà necessaria una dimostrazione *ad hoc* che presenta alcuni tratti in comune con il critero di irriducibilità di Eisenstein e fa inoltre uso della simmetria di tali polinomi, più uno studio separato di una particolare famiglia di essi sulla quale non è possibile applicare tale strategia. Senza avere quindi ottenuto informazioni sul gruppo di Galois di tali polinomi simmetrici mostriamo quindi come sia sufficiente l'irriducibilità per concludere, in altre parole che è possibile far giocare alla simmetria delle relazioni un ruolo simile a quello della più profonda simmetria ottenibile studiando il gruppo di Galois.

Mostriamo che i polinomi in questione possono fattorizzarsi qualora $a-b, a-c, b-c$ non siano tutti primi con $p$, ed esibiamo alcuni interessanti casi in cui essi si fattorizzano come prodotto di fattori di primo grado.

È necessario rimarcare che esistono comunque casi in cui tali polinomi si fattorizzano ma $N_a, N_b, N_c$ generano lo stesso tutto $S$. Esibiremo tuttavia per ogni $p$ una famiglia di casi, strettamente collegati con dette fattorizzazioni in termini di primo grado, in cui il campo generato è contenuto strettamente in $S$, e determineremo il grado di tale estensione non banale.

Per quanto riguarda lo studio del problema in più variabili, $n$ poniamo, presentiamo la dimostrazione di un teorema di Kakeya ([Kak25], [Kak27]) che

fornisce una curiosa condizione sufficiente sugli interi distinti $a_1, \ldots, a_n$ perché i polinomi di Newton $N_{a_1}, \ldots, N_{a_n}$ generino l'intero campo simmetrico.

Per la precisione, abbiamo che $N_{a_1}, \ldots, N_{a_n}$ generano $S$ qualora l'insieme

$$\mathbb{N}^+ \setminus \{a_1, \ldots, a_n\},$$

il complementare di $\{a_1, \ldots, a_n\}$, sia chiuso rispetto all'addizione. Presentiamo la dimostrazione data da Foulkes ([Fou56]) di questo risultato, che fornisce anche una costruzione esplicita di una famiglia di generatori fondamentali di $S$ usando gli strumenti combinatori della teoria classica delle funzioni simmetriche.

Dobbiamo infine citare il risultato analogo in più variabili di quello esposto precedentemente, in particolare che dati $n+1$ interi $a_1, \ldots, a_{n+1}$ coprimi e distinti allora $N_{a_1}, \ldots, N_{a_{n+1}}$ sono sempre sufficienti a generare l'intero campo simmetrico in $n$ variabili. Non forniremo tutti i dettagli su questo risultato ottenuto da Dvornicich e Zannier in [DZ08], ma dando per buono un risultato relativo all'irriducibilità e al calcolo del gruppo di Galois di una importante classe di polinomi relativa a questo problema, daremo una dimostrazione originale del passo finale mostrando, analogamente a quanto fatto in due variabili, come sia sufficiente usare l'irriducibilità per ottenere la conclusione voluta.

Nel *Capitolo 1* trattiamo alcuni preliminari di combinatoria riguardanti le partizioni di interi, diagrammi di Young e *tableau*, mostriamo alcune identità fondamentali fra le quantità combinatorie associate alle partizioni, e diamo alcuni cenni sul $t$-core e il $t$-quoziente di una partizione.

Definiamo quindi, nel *Capitolo 2*, l'anello delle funzioni simmetriche $\Lambda$ in infinite variabili e studiamo le famiglie principali di generatori di $\Lambda$ come $\mathbb{Z}$-modulo indicizzate dalle partizioni di interi $\lambda$, ovvero le funzioni simmetriche monomiali $m_\lambda$, elementari $e_\lambda$, complete $h_\lambda$ e le somme di potenze $p_\lambda$.

Nello stesso capitolo esaminiamo quindi le funzioni generatrici delle $e_\lambda, h_\lambda, p_\lambda$ ricavando le fondamentali relazioni fra di esse, e introduciamo l'involuzione $\omega$ sull'anello $\Lambda$, studiando la sua azione sulle basi fondamentali. Osserviamo come già in questa circostanza vengano alla luce strutture del gruppo simmetrico, e forniamo alcuni esempi elementari di applicazioni della teoria delle funzioni simmetriche, tra cui il teorema di Pólya con applicazione allo studio delle colorazioni, e la caratterizzazione dei numeri di Stirling del primo e del secondo tipo come funzioni simmetriche elementari e complete valutate in un intervalli di interi.

Nel successivo *Capitolo 3* introduciamo la base delle funzioni di Schur $s_\lambda$, e ricaviamo la fondamentale formula di Jacobi-Trudi che permette di scrivere gli $s_\lambda$ in termini degli $e_\lambda$ e $h_\lambda$. Caratterizziamo inoltre la scrittura delle somme di potenze $p_\rho$ nelle funzioni di Schur $s_\lambda$ in termini delle decomposizioni dei diagrammi delle partizioni $\lambda$ in strisce di bordo.

Definiamo quindi un prodotto scalare $\mathbb{Z}$-lineare su $\Lambda$ che rende duali le basi $m_\lambda$ e $h_\lambda$, e vediamo che tale prodotto scalare è simmetrico, definito positivo, e che le funzioni di Schur $s_\lambda$ sono una base ortonormale rispetto ad esso, e i $p_\lambda$ una base ortogonale. Tale prodotto scalare permette inoltre di definire

le funzioni di Schur *skew* $s_{\lambda/\mu}$, e vedremo come attraverso lo studio di esse sia possibile caratterizzare i coefficienti dei monomi $m_\nu$ nelle funzioni di Schur $s_\lambda$, detti numeri di Kostka, che per ogni coppia di partizioni $\lambda, \nu$ risulteranno corrispondere al numero di tableau di forma $\lambda$ e peso $\nu$.

Nel *Capitolo 4* vediamo le relazioni fondamentali fra le matrici che definiscono la scrittura di una base in termini di un'altra base, e come tali matrici di transizione fra le basi introdotte possano essere scritte in termini di alcune matrici fondamentali. Presentiamo inoltre la dimostrazione della regola di Littlewood-Richardson che fornisce una caratterizzazione combinatoria del prodotto di due funzioni di Schur.

Nel *Capitolo 5* presentiamo le applicazioni della teoria delle funzioni simmetriche allo studio di caratteri del gruppo simmetrico: vedremo che è in particolare possibile definire un isomorfismo isometrico fra l'anello delle funzioni simmetriche e l'algebra delle rappresentazioni del gruppo simmetrico equipaggiata con una particolare moltiplicazione.

In tale isomorfismo le funzioni di Schur $s_\lambda$ per tutte le partizioni $\lambda$ di $n$ corrispondono ai caratteri irriducibili di $S_n$, e i coefficienti nella scrittura dei $p_\nu$ in termini degli $s_\lambda$ risultano essere precisamente i valori di tali caratteri irriducibili nelle classi di coniugio degli elementi che hanno decomposizione in cicli di tipo $\nu$. Diamo inoltre un cenno alla teoria del pletismo.

Infine nel *Capitolo 6* presentiamo lo studio relativo al problema della generazione del campo simmetrico da parte dei polinomi di Newton. Il capitolo si articola in una parte preliminare, dove presentiamo i risultati elementari fondamentali e alcuni richiami della teoria delle derivazioni sui campi.

Segue quindi lo studio del problema in due variabili, dove presentiamo il risultato positivo di Dvornicich e Zannier e i risultati originali relativi allo studio in caratteristica positiva $p$.

Nell'ultima sezione trattiamo il caso in $n$ variabili, e dimostriamo quindi il teorema di Kakeya, per concludere con una dimostrazione alternativa del passo conclusivo del risultato di Dvornicich e Zannier sulla generazione del campo simmetrico con $n + 1$ polinomi di Newton.

Desidero ringraziare tutti i professori con cui ho studiato, e mi sento in particolare grato nei confronti di Alberto Abbondandolo, Ilaria Del Corso, Giovanni Gaiffi, Fulvio Lazzeri, Giuseppe Puglisi e Umberto Zannier, e soprattutto del mio relatore Roberto Dvornicich.

Un ringraziamento va a chi ha scritto, mantenuto e contribuito ai software liberi che mi hanno reso possibile scrivere questa tesi, in particolare Linux, Fedora, KDE, Firefox, Kile, Ssh, Git che ho usato come sistema di controllo versioni, Axiom con il quale ho potuto produrre abbondanti esempi nei problemi che stavo studiando, e LaTeX più tutti i relativi pacchetti e documentazioni.

Ringrazio inoltre tutti i miei amici con cui ho passato piacevoli giornate.

# Indice

# Capitolo 1

# Preliminari di combinatoria

> Da chimico un giorno avevo il potere
> di sposar gli elementi e farli reagire,
> ma gli uomini mai mi riuscì di capire
> perché si combinassero attraverso l'amore
> affidando ad un gioco la gioia e il dolore.
>
> *Fabrizio De André*, "Un chimico"

In questo capitolo rivediamo alcuni preliminari di combinatoria e fissiamo la notazione che useremo successivamente per trattare più agevolmente le funzioni simmetriche.

Gran parte degli oggetti che tratteremo nel seguito saranno indicizzati dalle partizioni dei naturali, e in particolare le basi come $\mathbb{Z}$-modulo dell'anello delle funzioni simmetriche. Sarà anche utile aver definito alcune quantità associate a tali partizioni, ordinamenti e oggetti combinatori detti tableau. Nell'ultima sezione diamo le definizioni del $t$-core e del $t$-quoziente di una partizione.

La nostra trattazione segue principalmente [Mac95], e abbiamo aggiunto diagrammi di partizioni e figure ovunque essi potessero facilitare la lettura.

## 1.1 Partizioni

Chiameremo *partizione* una successione (anche infinita) di interi non negativi in ordine decrescente

$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r, \dots), \qquad \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq \dots$$

contenente solo un numero finito di termini non nulli. Per comodità non faremo distinzioni fra partizioni che differiscano soltanto per una successione di zeri alla fine. Considereremo quindi $(5, 3)$, $(5, 3, 0)$ e $(5, 3, 0, 0, \dots)$ come la stessa partizione.

I $\lambda_i$ non nulli saranno detti le *parti* di $\lambda$. Il numero i parti sarà la *lunghezza* di $\lambda$, denotata con $\ell(\lambda)$, e la somma delle parti sarà detta il *peso* di $\lambda$, indicata

con $|\lambda|$:

$$|\lambda| = \lambda_1 + \lambda_2 + \lambda_3 + \dots.$$

Se $|\lambda| = n$ diremo che $\lambda$ è una *partizione* di $n$. L'insieme di tutte le partizioni di $n$ sarà denotato con $\mathscr{P}_n$, e l'insieme di tutte le partizioni $\mathscr{P}$. In particolare $\mathscr{P}_0$ conterrà un unico elemento, la partizione di zero che indicheremo con 0. È talvolta comodo usare una notazione che indica quante volte compare cascun intero come parte:

$$\lambda = (1^{m_1} 2^{m_2} \dots r^{m_r} \dots)$$

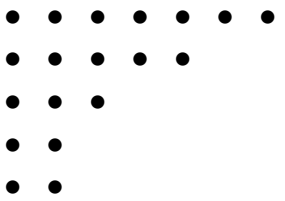
significa che esattamente $m_i$ parti sono uguali a $i$. Il numero

$$m_i = m_i(\lambda) = \left|\{j : \lambda_j = i\}\right| \tag{1.1}$$

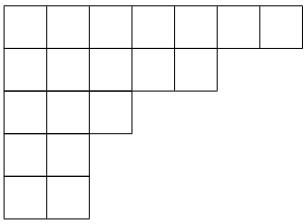
è detto la *molteplicità* di $i$ in $\lambda$.

## 1.2 Diagrammi

Il *diagramma*[1] di una partizione $\lambda$ è definito come l'insieme dei punti $(i, j) \in \mathbb{Z}^2$ tali che $1 \leq j \leq \lambda_i$. Per disegnare i diagrammi usiamo la notazione "anglosassone" (simile a quella usata per la matrici): la prima coordinata, $i$, indica la riga e cresce verso il basso, la seconda, $j$, indica la colonna e cresce da sinistra a destra. Ad esempio, il diagramma della partizione (75322) è:



È spesso preferibile disegnare delle caselle quadrate piuttosto che non dei punti, ad esempio



[1] Questi diagrammi sono spesso indicati col nome di *diagrammi di Ferrers*, o *diagrammi di Young*. Precisiamo che i *tableau di Young* (che verranno introdotti più avanti) sono oggetti combinatori diversi dai diagrammi.

Commettiamo il leggero abuso di notazione di indicare il diagramma di una partizione $\lambda$ con lo stesso simbolo $\lambda$.

La *coniugata* della partizione $\lambda$ è la partizione $\lambda'$ il cui diagramma è il trasposto del diagramma di $\lambda$, cioè il diagramma ottenuto tramite una riflessione lungo la diagonale principale. Ad esempio, la coniugata di (75322) è (5532211). Osserviamo che $\lambda'_i$ è il numero di caselle nella $i$-esima colonna di $\lambda$, o equivalentemente

$$\lambda'_i = \Big|\big\{j : \lambda_j \geq i\big\}\Big|. \tag{1.2}$$

In particolare, $\lambda'_1 = \ell(\lambda)$ e $\lambda_1 = \ell(\lambda')$. Inoltre chiaramente $\lambda'' = \lambda$.

Dalle (1.1) e (1.2) segue che

$$m_i(\lambda) = \lambda'_i - \lambda'_{i+1}.$$

Un'altra notazione che può essere utile è la seguente, detta di Frobenius. Supponiamo che $\lambda$ abbia la diagonale principale di $r$ caselle $(i,i)_{1\leq i\leq r}$. Sia $\alpha_i = \lambda_i - i$ il numero di caselle nella $i$-esima riga di $\lambda$ a destra di $(i,i)$, e $\beta_i = \lambda'_i - i$ il numero di caselle nella $i$-esima colonna sotto $(i,i)$, per $i = 1,\dots,r$. Allora $\alpha_1 > \alpha_2 > \cdots > \alpha_r \geq 0$ e $\beta_1 > \beta_2 > \cdots > \beta_r \geq 0$, e indichiamo la partizione $\lambda$ con

$$\lambda = (\alpha_1,\dots,\alpha_r|\beta_1,\dots,\beta_r) = (\alpha|\beta).$$

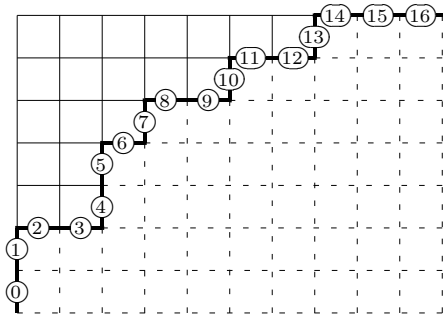
La coniugata di $(\alpha|\beta)$ chiaramente è $(\beta|\alpha)$. Ad esempio nel caso di $\lambda = (75322)$ abbiamo $\lambda = (\alpha|\beta)$, con $\alpha = (630)$ e $\beta = (430)$ (si noti che la partizione $(\alpha|\beta)$, per $\alpha = (63)$ e $\beta = (43)$, è differente).

**Proposizione 1.2.1.** *Sia $\lambda$ una partizione, e $m \geq \lambda_1$, $n \geq \lambda'_1$. Allora gli $m+n$ numeri*

$$\lambda_i + n - i \quad (i = 1,\dots,n), \qquad n - 1 + j - \lambda'_j \quad (j = 1,\dots,m)$$

*sono una permutazione di $\{0, 1, \dots, m+n-1\}$*

*Dimostrazione.* Infatti il diagramma di $\lambda$ è contenuto nel rettangolo $n \times m$ (che è anche il diagramma della partizione $(m^n)$). Se numeriamo i segmenti che delimitano il diagramma di $\lambda$ dal complementare con i numeri $0, 1, \dots, m+n-1$ partendo dal fondo, possiamo osservare che i numeri al termine della $i$-esima riga sono esattamente $\lambda_i + n - i$, per $i = 1,\dots,n$, mentre quelli al termine della $j$-esima colonna sono $m+n-1-(\lambda'_j+m-j) = n-1+j-\lambda'_j$, per $j = 1,\dots,m$.




**Esempio per $\lambda = (75322)$, $m = 10$ e $n = 7$.** □

Per ogni partizione $\lambda$ definiamo la quantità

$$n(\lambda) \;=\; \sum_{i\geq 1}(i-1)\lambda_i, \tag{1.3}$$

che è anche la somma dei numeri che compaiono scrivendo uno 0 nella prima riga, un 1 nella seconda, e così via:

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | | |
| 2 | 2 | 2 | | | | |
| 3 | 3 | | | | | |
| 4 | 4 | | | | | |

Sommando i numeri in ciascuna colonna, possiamo vedere che:

$$n(\lambda) \;=\; \sum_{i\geq 1}\binom{\lambda'_i}{2}.$$

Se $\lambda$ è una partizione, la *lunghezza del gancio* di $\lambda$ in $x=(i,j)\in\lambda$ è definita come

$$h(x) \;=\; h(i,j) \;=\; \lambda_i+\lambda'_j-i-j+1. \tag{1.4}$$

Possiamo ottenere un'elegante formula per il prodotto delle lunghezze dei ganci nel seguente modo: applichiamo la proposizione a $\lambda'$ ponendo $m\geq\lambda'_1$ e $n=\lambda_1$, in modo da ottenere la seguente identità polinomiale

$$\sum_{j=1}^{\lambda_1} t^{\lambda'_j+\lambda_1-j}+\sum_{j=1}^{m} t^{\lambda_1-1+j-\lambda_j} \;=\; \sum_{j=0}^{\lambda_1+m-1} t^j.$$

Se ora poniamo $\mu_i=\lambda_i+m-i$ $(i=1,\dots,m)$, l'identità diventa, dopo aver rimosso il termine in $t^0$ da entrambi i membri:

$$\sum_{j=1}^{\lambda_1} t^{h(1,j)}+\sum_{j=2}^{m} t^{\mu_1-\mu_j}=\sum_{j=1}^{\mu_1} t^j.$$

Scrivendo questa identità per la partizione $(\lambda_i,\lambda_{i+1},\dots)$, e sommando su $i=1,2,\dots,m$ abbiamo

$$\sum_{x\in\lambda} t^{h(x)}+\sum_{1\leq i<j\leq m} t^{\mu_i-\mu_j}=\sum_{i=1}^{m}\sum_{j=1}^{\mu_i} t^j.$$

Considerando l'uguaglianza termine a termine dei monomi possiamo trasformare questa somma in un prodotto:

$$\begin{aligned}\prod_{x\in\lambda}(1-t^{h(x)}) &= \frac{\prod_{i=1}^{m}\prod_{j=1}^{\mu_i}(1-t^j)}{\prod_{1\le i<j\le m}(1-t^{\mu_i-\mu_j})}\\ &= \frac{\prod_{i=1}^{m}\varphi_{\mu_i}(t)}{\prod_{1\le i<j\le m}(1-t^{\mu_i-\mu_j})},\end{aligned} \tag{1.5}$$

dove $\varphi_r(t) = (1-t)(1-t^2)\dots(1-t^r)$. In particolare se dividiamo entrambi i membri per $(1-t)^{|\lambda|}$ e poniamo $t=1$ otteniamo:

$$\prod_{x\in\lambda} h(x) \;=\; \frac{\prod_{i=1}^{m}\mu_i!}{\prod_{1\le i<j\le m}(\mu_i-\mu_j)}.$$

Per ogni $x=(i,j)\in\lambda$ definiamo inoltre il *contenuto* di $x$ come

$$c(x) \;=\; j-i. \tag{1.6}$$

Se $n$ è un qualunque intero $\geq \ell(\lambda)$, allora i numeri $n+c(x)$ nella $i$-esima riga di $\lambda$ sono $n-i+1, n-i+2, \dots, n-i+\lambda_i$, e abbiamo quindi che

$$\prod_{x\in\lambda}(1-t^{n+c(x)}) \;=\; \prod_{i=1}^{n}\frac{\varphi_{\lambda_i+n-i}(t)}{\varphi_{n-i}(t)}, \tag{1.7}$$

dove come sopra abbiamo posto $\varphi_r(t) = (1-t)(1-t^2)\dots(1-t^r)$.

Calcoliamo ora le somme di $h(x)$ e $c(x)$ per $x\in\lambda$. Possiamo verificare facilmente che

$$\sum_{x\in\lambda} h(x) \;=\; n(\lambda)+n(\lambda')+|\lambda|, \tag{1.8}$$

ad esempio ragionando per induzione sul numero di caselle nel diagramma di $\lambda$. Se $\lambda=0$ allora l'identità è banalmente vera, mentre se $\lambda=\mu\sqcup\{x\}$ per qualche partizione $\mu$ e $x=(i,j)\in\lambda$, la differenza dei termini al secondo membro è

$$n(\lambda)+n(\lambda')+|\lambda|-n(\mu)-n(\mu')-|\mu| \;=\; \lambda_i+\lambda'_j-1,$$

e inoltre la casella aggiunta contribuisce di uno alle lunghezze dei ganci della sua riga e della sua colonna, che sono $\lambda_i+\lambda'_j-1$ in totale.

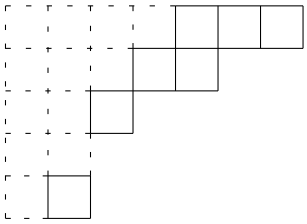
Inoltre

$$\sum_{x\in\lambda} c(x) \;=\; n(\lambda')-n(\lambda), \tag{1.9}$$

come si può verificare immediatamente dalla definizione di $n(\lambda)$.

## 1.3 Diagrammi *skew* e *tableau*

Se $\lambda$ e $\mu$ sono partizioni, scriveremo $\lambda \supseteq \mu$ per intendere che il diagramma di $\lambda$ contiene il diagramma di $\mu$, ovvero $\lambda_i \geq \mu_i$, per ogni $i \geq 1$. Se $\lambda \supseteq \mu$, la differenza di insiemi dei diagrammi $\lambda$ e $\mu$ è detta *diagramma skew* e si indica con $\vartheta = \lambda/\mu$. Per esempio se $\lambda = (75322)$ e $\mu = (43221)$, il diagramma skew $\lambda/\mu$ è la regione indicata nella figura:



Un *cammino* in un diagramma skew $\vartheta$ è una successione di caselle $x_0, \ldots, x_m$ in $\vartheta$ tali che $x_{i-1}$ e $x_i$ hanno un lato in comune, per $i = 1, \ldots, m$. Un sottoinsieme $\varphi$ di $\vartheta$ è detto *connesso* se ogni coppia di caselle in $\varphi$ può essere collegata da un cammino in $\varphi$. I sottoinsiemi connessi massimali di $\vartheta$ sono anch'essi diagrammi skew, e sono detti *componenti connesse* di $\vartheta$. Nell'esempio ci sono tre componenti connesse.

Il *coniugato* di un diagramma skew $\vartheta = \lambda/\mu$ è $\vartheta' = \lambda'/\mu'$. Poniamo $\vartheta_i = \lambda_i/\mu_i$, $\vartheta'_i = \lambda'_i/\mu'_i$, e come per le partizioni definiamo il peso $|\vartheta|$ come

$$|\vartheta| = \sum \vartheta_i = |\lambda| - |\mu|.$$

Un diagramma skew $\vartheta$ è una *m-striscia orizzontale* (risp. *verticale*) se $|\vartheta| = m$ e, per ogni $i \geq 1$, $\vartheta'_i \leq 1$ (risp. $\vartheta_i \leq 1$). Una striscia orizzontale occupa quindi al più una casella per colonna (analogamente per una striscia verticale). Una condizione necessaria e sufficiente perché $\vartheta = \lambda/\mu$ sia una striscia orizzontale è che $\lambda$ e $\mu$ siano interlacciati, ovvero $\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \mu_2 \geq \ldots$.

Un diagramma skew $\vartheta$ è una *striscia di bordo* (detta anche *gancio skew*) se $\vartheta$ è connesso e non contiene nessun quadrato $2 \times 2$, in modo che ogni coppia di righe (o colonne) contigue occupate entrambe da $\vartheta$, se traslate in modo da sovrapporsi, si incontrino in precisamente una casella. La *lunghezza* di una striscia di bordo $\vartheta$ è il numero totale $|\vartheta|$ di caselle, e la sua *altezza* $ht(\vartheta)$ è definita come il numero di righe occupate meno uno. Se disegniamo una striscia di bordo $\vartheta$ con dei punti invece che con caselle e connettiamo i nodi contigui con un segmento, allora otteniamo una specie di scala, e l'altezza di $\vartheta$ è precisamente il numero di segmenti verticali.

Se $\lambda = (\alpha_1, \ldots, \alpha_r|\beta_1, \ldots, \beta_r)$ e $\mu = (\alpha_2, \ldots, \alpha_r|\beta_2, \ldots, \beta_r)$, allora $\lambda/\mu$ è una striscia di bordo, detta *bordo* di $\lambda$.

Un *tableau* (stretto sulle colonne) $T$ è una successione di partizioni

$$\mu = \lambda^{(0)} \subseteq \lambda^{(1)} \subseteq \cdots \subseteq \lambda^{(r)} = \lambda$$

tali che per $i = 1, \dots, r$ ciascun diagramma skew $\vartheta^{(i)} = \lambda^{(i)}/\lambda^{(i-1)}$ sia una striscia orizzontale. Possiamo dare una descrizione grafica del tableau $T$ scrivendo $i$ in ciascuna casella del diagramma skew $\vartheta^{(i)}$, ed è spesso comodo pensare ad un tableau in questo modo, come a un diagramma skew numerato. I numeri scritti in $\lambda/\mu$ devono crescere strettamente scendendo lungo ogni colonna (da cui 'stretto sulle colonne'), e debolemente da sinistra a destra sulle righe. Il diagramma skew $\lambda/\mu$ è detto *forma* del tableau $T$, e la successione $(|\vartheta^{(1)}|, |\vartheta^{(2)}|, \dots, |\vartheta^{(r)}|)$ è detta *peso* di $T$. È anche possibile considerare tableau a crescita stretta sulle righe anziché sulle colonne, ma se non specificato altrimenti considereremo sempre un tableau come stretto sulle colonne.

Un *tableau standard* è un tableau $T$ che contiene ciascun numero $1, 2, \dots, r$ esattamente una volta, e ha quindi peso $(1, 1, \dots, 1)$.

## 1.4 Operazioni sulle partizioni

Siano $\lambda$ e $\mu$ partizioni. Definiamo $\lambda + \mu$ come la somma termine a termine delle successioni che definiscono $\lambda$ e $\mu$:

$$\lambda + \mu \;=\; (\lambda_1 + \mu_1, \lambda_2 + \mu_2, \dots, \lambda_r + \mu_r, \dots).$$

Definiamo inoltre $\lambda \cup \mu$ come la partizione le cui parti sono l'unione di quelle di $\lambda$ e $\mu$, riarrangiate in ordine decrescente. Ad esempio se $\lambda = (321)$ e $\mu = (22)$, allora $\lambda + \mu = (541)$ e $\lambda \cup \mu = (32221)$.

Definiamo $\lambda\mu$ come il prodotto termine a termine delle successioni $\lambda$, $\mu$:

$$\lambda\mu \;=\; (\lambda_1\mu_1, \lambda_2\mu_2, \dots, \lambda_r\mu_r, \dots),$$

e definiamo $\lambda \times \mu$ come la partizione le cui parti sono $\min(\lambda_i, \mu_j)$, per $i = 1, \dots, \ell(\lambda)$ e $j = 1, \dots, \ell(\mu)$, arrangiate in ordine decrescente.

Le operazioni $+$ e $\cup$ sono reciprocamente duali, e lo stesso per le due moltiplicazioni:

$$\begin{aligned}(\lambda \cup \mu)' &= \lambda' + \mu' \\ (\lambda \times \mu)' &= \lambda'\mu'.\end{aligned}$$

*Dimostrazione.* Il diagramma di $\lambda \cup \mu$ si ottiene mettendo insieme le righe di $\lambda$ e $\mu$, e risistemandole in ordine decrescente. La lunghezza della $k$-esima colonna è quindi la somma delle lunghezze delle $k$-esime colonne di $\lambda$ e di $\mu$, segue che $(\lambda \cup \mu)'_k = \lambda'_k + \mu'_k$.

La lunghezza della $k$-esima colonna di $\lambda \times \mu$ è invece uguale al numero di coppie $(i, j)$ tali che $\lambda_i \geq k$ e $\mu_j \geq k$, che è $\lambda'_k\mu'_k$, e quindi $(\lambda \times \mu)'_k = \lambda'_k\mu'_k$. □

## 1.5 Ordinamenti

Sull'insieme $\mathscr{P}_n$ definiamo l'*ordinamento lessicografico* come il sottoinsieme $L_n$ di $\mathscr{P}_n \times \mathscr{P}_n$ contenente tutte le coppie $(\lambda, \mu)$ tali che $\lambda = \mu$, oppure la prima

differenza non nulla $\lambda_i - \mu_i$ è positiva. $L_n$ è un ordinamento totale, e scriviamo $\lambda \geq_{\text{lex}} \mu$ se $(\lambda, \mu) \in L_n$.

Un altro ordinamento totale su $\mathscr{P}_n$ è $L'_n$, l'insieme di tutte le coppie $(\lambda, \mu)$ tali che $\lambda = \mu$, oppure l'ultima differenza non nulla $\lambda_i - \mu_i$ è negativa, e in questo caso scriviamo $\lambda \geq_{\text{lex}'} \mu$. Gli ordinamenti $L_n$ e $L'_n$ sono distinti non appena $n \geq 6$, ed inoltre abbiamo che se $\lambda, \mu \in \mathscr{P}_n$ allora

$$\lambda \geq_{\text{lex}} \mu \quad \Leftrightarrow \quad \mu' \geq_{\text{lex}'} \lambda'$$

*Dimostrazione.* Basta considerare i diagrammi di $\lambda$ e $\mu$: se $\lambda >_{\text{lex}} \mu$ e $i$ è il minimo intero tale $\lambda_i > \mu_i$, poniamo $k = \lambda_i$: la $k$-esima colonna è l'ultima colonna diversa, ed inoltre $\lambda'_k > \mu'_k$, e quindi $\mu' \geq_{\text{lex}'} \lambda'$. Analogamente si dimostra il contrario. □

Un altro ordinamento (parziale) più importante di entrambi gli ordinamenti sopra definiti è l'*ordinamento naturale* $N_n$ su $\mathscr{P}_n$ (detto anche ordinamento parziale di *dominazione*), che è definito da:

$$(\lambda, \mu) \in N_n \quad \Leftrightarrow \quad \lambda_1 + \cdots + \lambda_i \ \geq \ \mu_1 + \cdots + \mu_i \qquad \text{per tutti gli } i \geq 1.$$

Non appena $n \geq 6$, $N_n$ non è più un ordinamento totale. Scriveremo per comodità $\lambda \geq \mu$ per indicare che $(\lambda, \mu) \in N_n$. Le relazioni d'ordine sopra definite sono messe in relazione dalla seguente:

**Proposizione 1.5.1.** *Siano $\lambda, \mu \in \mathscr{P}_n$. Allora*

$$\lambda \geq \mu \quad \Rightarrow \quad \lambda \geq_{\text{lex}} \mu \ \wedge \ \lambda \geq_{\text{lex}'} \mu$$

*Dimostrazione.* Supponiamo $\lambda \geq \mu$. Allora se $\lambda \neq \mu$ e $i$ è il minimo intero tale che $\lambda_i \neq \mu_i$, siccome $\lambda_1 + \cdots + \lambda_i \ \geq \ \mu_1 + \cdots + \mu_i$ si deve necessariamente avere che $\lambda_i > \mu_i$, e quindi $\lambda \geq_{\text{lex}} \mu$. D'altra parte se invece $\lambda \neq \mu$ e $j$ è il massimo intero tale che $\lambda_j \neq \mu_j$, siccome $\lambda_1 + \cdots + \lambda_{j-1} \ \geq \ \mu_1 + \cdots + \mu_{j-1}$, e $|\lambda| = |\mu| = n$, dobbiamo avere che $\lambda_j < \mu_j$ e quindi $\lambda \geq_{\text{lex}'} \mu$. □

**Nota.** *In generale $N_n \neq L_n \cap L'_n$. Per esempio, per $n = 12$, $\lambda = (63^2)$, $\mu = (5^2 1^2)$, abbiamo che $\lambda \geq_{\text{lex}} \mu$ e $\lambda \geq_{\text{lex}'} \mu$, ma $\lambda$ e $\mu$ non sono confrontabili con l'ordinamento naturale.*

L'ordinamento naturale $\geq$ è antisimmetrico rispetto al coniugio. Più precisamente:

**Proposizione 1.5.2.** *Siano $\lambda, \mu \in \mathscr{P}_n$. Allora*

$$\lambda \geq \mu \quad \Leftrightarrow \quad \mu' \geq \lambda'$$

*Dimostrazione.* Per simmetria basta dimostrare una delle due implicazioni, e possiamo quindi supporre $\lambda \geq \mu$. Vogliamo dimostrare che la somma delle lunghezze delle prime $k$ colonne di $\mu$ è maggiore o uguale della somma delle

lunghezze delle prime $k$ colonne di $\lambda$, per ogni $k \geq 1$. Consideriamo di diagrammi delle partizioni

$$\begin{aligned} \pi &= (\max(\lambda_1 - k, 0), \dots, \max(\lambda_r - k, 0), \dots), \\ \rho &= (\max(\mu_1 - k, 0), \dots, \max(\mu_r - k, 0), \dots), \end{aligned}$$

o, equivalentemente,

$$\begin{aligned} \pi' &= (\lambda'_{k+1}, \lambda'_{k+2}, \dots), \\ \rho' &= (\mu'_{k+1}, \mu'_{k+2}, \dots), \end{aligned}$$

ottenuti traslando a sinistra di $k$ passi i diagrammi di $\lambda$ e $\mu$, e cancellando le $k$ colonne uscite dal diagramma a sinistra. È facile vedere che $|\pi| \geq |\rho|$, perché infatti se $i = \ell(\rho)$ è l'indice dell'ultima riga di $\mu$ più lunga di $k$:

$$\begin{aligned} ki + |\rho| &= \mu_1 + \cdots + \mu_i \\ &\leq \lambda_1 + \cdots + \lambda_i \\ &\leq ki + (\max(\lambda_1 - k, 0) + \cdots + \max(\lambda_i - k, 0)) \\ &\leq ki + |\pi|. \end{aligned}$$

Ma il numero di caselle nelle prime $k$ colonne di $\lambda$ e $\mu$ è rispettivamente $n - |\pi|$ e $n - |\rho|$, e abbiamo quindi che:

$$\mu'_1 + \cdots + \mu'_k \;\geq\; \lambda'_1 + \cdots + \lambda'_k,$$

cioè che $\mu' \geq \lambda'$, essendo $k$ un intero positivo arbitrario. □

## 1.6 Operatori di *raising*

Definiamo ora un altro strumento combinatorio operando non più sulle partizioni, ma sui vettori di interi $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$. Il gruppo simmetrico $S_n$ agisce su $\mathbb{Z}^n$ permutando le coordinate, e l'insieme

$$P_n = \left\{ b \in \mathbb{Z}^n : b_1 \geq b_2 \geq \cdots \geq b_n \right\}$$

è un dominio fondamentale per questa azione, cioè la $S_n$-orbita di ciascun $a \in \mathbb{Z}^n$ incontra $P_n$ in esattamente un punto, che chiameremo $a^+$. Quindi $a^+$ è ottenuto riarrangiando gli $a_1, \dots, a_n$ in ordine decrescente.

Se $a, b \in \mathbb{Z}^n$, definiamo come prima l'ordinamento naturale $a \geq b$ intendendo che

$$a_1 + \cdots + a_i \;\geq\; b_1 + \cdots + b_i \qquad \forall i = 1, \dots, n. \tag{1.10}$$

**Proposizione 1.6.1.** *Sia $a \in \mathbb{Z}^n$. Allora*

$$a \in P_n \;\Leftrightarrow\; a \geq wa \qquad \textit{per ogni } w \in S_n.$$

*Dimostrazione.* Sia $a \in P_n$, e quindi $a_1 \geq \cdots \geq a_n$. Se $b = wa$ per qualche $w \in S_n$, allora $(b_1, \ldots, b_n)$ è una permutazione di $(a_1, \ldots, a_n)$, e segue immediatamente che la (1.10) deve essere vera, cioè $a \geq b$.

D'altra parte se $a \geq wa$ per ogni $w \in S_n$, allora questo è vero per le trasposizioni $(i, i+1)$ per $i = 1, \ldots, n-1$, e quindi

$$a_1 + \cdots + a_{i-1} + a_i \geq a_1 + \cdots + a_{i-1} + a_{i+1},$$

ovvero $a_i \geq a_{i+1}$ e $a \in P_n$. □

Sia ora $\delta = (n-1, n-2, \ldots, 1, 0) \in P_n$.

**Proposizione 1.6.2.** *Sia $a \in P_n$. Allora $(a + \delta - w\delta)^+ \geq a$ per ogni $w \in S_n$.*

*Dimostrazione.* Infatti siccome $\delta \in P_n$, $\delta \geq w\delta$ per la proposizione 1.6.1, e quindi $a + \delta - w\delta \geq a$. Applicando nuovamente la 1.6.1:

$$(a + \delta - w\delta)^+ \;\geq\; a + \delta - w\delta \;\geq\; a. \qquad \square$$

Per ogni coppia di interi $i, j$ tali che $1 \leq i < j \leq n$, definamo $R_{ij} : \mathbb{Z}^n \to \mathbb{Z}^n$ come:

$$R_{ij}(a) = (a_1, \ldots, a_i + 1, \ldots, a_j - 1, \ldots, a_n).$$

Qualunque prodotto $R = \prod_{i<j} R_{ij}^{r_{ij}}$ è detto *operatore di raising*. Si noti che l'ordinamento dei fattori nel prodotto è irrilevante, perché gli $R_{ij}$ commutano tutti fra di loro.

**Proposizione 1.6.3.** *Sia $a \in \mathbb{Z}^n$, e $R$ un operatore di raising. Allora*

$$Ra \geq a.$$

*Dimostrazione.* Ci basta considerare il caso $R = R_{ij}$, nel qual caso la tesi è ovvia. □

Al contrario:

**Proposizione 1.6.4.** *Siano $a, b \in \mathbb{Z}^n$ tali che $a \leq b$ e $a_1 + \cdots + a_n = b_1 + \cdots + b_n$. Allora $b = Ra$ per qualche operatore di raising $R$.*

*Dimostrazione.* Possiamo infatti prendere

$$R \;=\; \prod_{k=1}^{n-1} R_{k,k+1}^{r_k}, \qquad \text{con} \quad r_k = \sum_{i=1}^{k} (b_i - a_i). \qquad \square$$

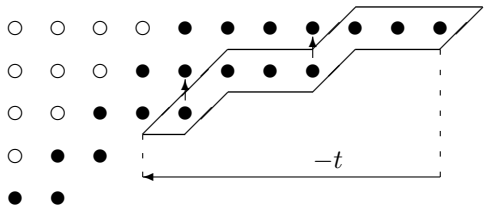
**Proposizione 1.6.5.** *Siano $\lambda, \mu$ partizioni di $n$, con $\lambda > \mu$ e adiacenti secondo l'ordinamento naturale (nel senso che se $\lambda \geq \nu \geq \mu$ allora $\nu = \lambda$ o $\nu = \mu$). Allora $\lambda = R_{ij}\mu$ per qualche $1 \leq i < j \leq n$.*

*Dimostrazione.* A meno di rimuovere un certo numero di righe iniziali da $\lambda$ e $\mu$, possiamo supporre senza perdita di generalità che $\lambda_1 > \mu_1$. Sia ora $i \geq 2$ il minimo intero tale che $\lambda_1 + \cdots + \lambda_i = \mu_1 + \cdots + \mu_i$: allora $\mu_i > \lambda_i \geq \lambda_{i+1} \geq \mu_{i+1}$. Quindi $\nu = R_{1i}\mu$ è una partizione, e vediamo immediatamente che $\lambda \geq \nu > \mu$, e conseguentemente $\lambda = \nu = R_{1i}\mu$. □

**Nota.** *Usando questa proposizione otteniamo immediatamente una dimostrazione alternativa della 1.5.2: infatti è sufficiente considerare il caso in cui $\lambda = R_{ij}\mu$, che si vede immediatamente essere vero.*

## 1.7 Il $t$-*core* e il $t$-quoziente di una partizione

Sia $t$ un intero $\geq 2$. Siano $\lambda, \mu$ partizioni di lunghezza $\leq m$ tali che $\lambda \supseteq \mu$, e tali che $\lambda/\mu$ è una striscia di bordo di lunghezza $t$. Sia come al solito $\delta_m = (m-1, m-2, \ldots, 1, 0)$, e chiamiamo $\xi = \lambda + \delta_m$ e $\eta = \mu + \delta_m$. Allora $\eta$ è la partizione che si ottiene da $\xi$ sottraendo $t$ da una sua parte e riarrangiando le parti in ordine decrescente, come possiamo osservare esaminando i diagrammi di $\lambda$ e $\mu$ 'inclinati' (e vedendoli come parte dei diagrammi di $\xi$ e $\eta$):




**Rimozione di una striscia di bordo da $\lambda = (75322)$ a $\mu = (42222)$.**

Con la stessa notazione, supponiamo che $\xi$ abbia $m_r$ parti $\xi_i$ congrue a $r$ modulo $t$, per ciascun $r = 0, 1, \ldots, t-1$. Questi $\xi_i$ possono essere scritti nella forma $t\xi_k^{(r)} + r$, $k = 1, \ldots, m_r$, dove $\xi_1^{(r)} > \xi_2^{(r)} > \cdots > \xi_{m_r}^{(r)} \geq 0$, cioè $\xi^{(r)}$ è una partizione stretta per ogni $r = 0, 1, \ldots, t-1$.

Sia $\lambda_k^{(r)} = \xi_k^{(r)} - m_r + k$, e sia $\lambda^{(r)} = (\lambda_i^{(r)}, \ldots, \lambda_{m_r}^{(r)})$ la partizione corrispondente (anche definibile come l'unica $\lambda^{(r)}$ tale che $\lambda^{(r)} + \delta_{m_r} = \xi^{(r)}$). La collezione $\lambda^* = (\lambda^{(0)}, \lambda^{(1)}, \ldots, \lambda^{(t-1)})$ è detta *t-quoziente* di $\lambda$. L'operazione di cambiare il numero $m \geq \ell(\lambda)$ scelto inizialmente ha l'effetto di permutare i $\lambda^{(r)}$ ciclicamente, per cui può essere comodo immaginarsi $\lambda^*$ come un 'collana' di partizioni.

Gli $m$ numeri $st + r$, al variare di $r$ in $0, 1, \ldots, t-1$ e di $s$ in $0, 1, \ldots, m_r - 1$, sono tutti distinti. Possiamo quindi arrangiarli in ordine decrescente, e poniamo siamo $\tilde{\xi}_1 > \cdots > \tilde{\xi}_m$, e definire una partizione $\tilde{\lambda}$ tramite $\tilde{\lambda}_i = \tilde{\xi}_i - m + i$, per $i = 1, 2, \ldots, m$ (o equivalentemente l'unica tale che $\tilde{\lambda} + \delta_m = \tilde{\xi}$, visto che $\tilde{\xi}$ è una partizione stretta). Questa partizione $\tilde{\lambda}$ è detta *t-core* di $\lambda$. Sia $\tilde{\lambda}$ che $\lambda^*$ (a meno di permutazione ciclica) sono indipendenti dalla scelta di $m$, purché $m \geq \ell(\lambda)$.

Se $\lambda = \tilde{\lambda}$ (cioè se $\lambda^*$ contiene solo partizioni vuote), si dice che la partizione $\lambda$ è un $t$-core. Per esempio, gli unici 2-core sono le partizioni fatte a 'scala' $\delta_m = (m-1, m-2, \ldots, 1)$.

Può essere comodo visualizzare questa costruzione in termini di un abaco formato da $t$ righe orizzontali, una per ciascuna classe di resto $r = 0, 1, \ldots, t-1$, e ponendo sulla riga $r$-esima una pallina in ciascun punto di coordinate $(\xi_k^{(r)}, r)$, per $k = 1, 2, \ldots, m_r$ (secondo la notazione sopra definita). Rimuovere una striscia di bordo di lunghezza $t$ da $\lambda$ corrisponde a spostare una pallina di un posto a sinistra sull'abaco (e questa mossa è concessa se e solo se il posto a sinistra non era già occupato da un'altra pallina), e quindi il passaggio da $\lambda$ al suo $t$-core corrisponde a muovere tutte le palline dell'abaco il più a sinistra possibile.

La costruzione aritmetica del $p$-quoziente e del $p$-core è un analogo per le partizioni dell'algoritmo di divisione con resto degli interi per sottrazioni successive (a cui si riduce se la partizione ha una sola parte).

Il $t$-core di una partizione $\lambda$ si può ottenere graficamente nel seguente modo. Si rimuova ad ogni passo una striscia di bordo di lunghezza $t$ dal diagramma di $\lambda$ in modo che ciò che rimane sia ancora il diagramma di una partizione, e si continui a rimuovere striscie di bordo di lunghezza $t$ fino a quando non è più possibile. Ciò che resta alla fine di questo processo è il $t$-core $\tilde{\lambda}$ di $\lambda$, e non dipende dalla scelta delle rimozioni di striscie di bordo.

È anche possibile leggere il $t$-quoziente di $\lambda$ dal diagramma di $\lambda$ come segue. Per $u, v = 0, 1, \ldots, t-1$, siano

$$\begin{aligned} R_u &= \Big\{(i,j) \in \lambda : \lambda_i - i \equiv u \pmod t\Big\}, \\ C_v &= \Big\{(i,j) \in \lambda : j - \lambda'_j \equiv v \pmod t\Big\}, \end{aligned}$$

cosicché $R_u$ consiste delle righe di $\lambda$ la cui ultima casella a destra ha contenuto congruo a $u$ modulo $t$, e analogamente per $C_t$. Se ora $(i,j) \in R_u \cap C_v$, la lunghezza del gancio in $(i,j)$ è

$$h(i,j) = \lambda_i + \lambda'_j - i - j + 1 \equiv s - t + 1 \pmod t,$$

e quindi $t$ divide $h(i,j)$ se e solo se $t \equiv s+1 \pmod t$.

D'altra parte, se $\xi_i = t\xi_k^{(r)} + r$ secondo la scrittura precedentemente definita, le lunghezze dei ganci di $\lambda$ nella $i$-esima riga sono gli elementi della successione ottenuta da $(1, 2, \ldots, \xi_i)$ dopo aver cancellato $\xi_i - \xi_{i+1}, \ldots, \xi_i - \xi_m$ (infatti a ogni gancio lungo $h$ corrisponde una striscia di bordo della stessa lunghezza, e le striscie di bordo che partono dall'ultima casella della riga $i$-esima corrispondono agli interi positivi minori o uguali a $\xi_i$ che sono diversi da ciascun $\xi_i - \xi_j$ per $j > i$, per quanto detto all'inizio della sezione).

Quindi quelle divisibili per $t$ sono gli elementi della successione $(t, 2t, \ldots, t\xi_k^{(r)})$ dopo la cancellazione di $t(\xi_k^{(r)} - \xi_{k+1}^{(r)}), \ldots, t(\xi_k^{(r)} - \xi_{m_r}^{(r)})$, e conseguentemente esse sono le lunghezze dei ganci nella $k$-esima riga di $\lambda^{(r)}$ moltiplicate per $t$, e in particolare il loro numero è precisamente $\lambda_k^{(r)}$.

Ne segue che ciascun $\lambda^{(r)}$ è immerso dentro $\lambda$ come $R_s \cap C_{s+1}$, dove $s \equiv r-m \pmod t$, e che le lunghezze dei ganci in $\lambda^{(r)}$ sono quelle delle corrispondenti caselle in $R_s \cap C_{s+1}$, divise per $t$. In particolare se $m$ è un multiplo di $t$ (cosa che possiamo assumere senza perdita di generalità) allora $\lambda^{(r)} = \lambda \cap R_r \cap C_{r+1}$ per ogni $r$ (dove intendiamo che $C_t = C_0$).

Da quanto detto precedentemente segue che il $t$-core e il $t$-quoziente della partizione coniugata $\lambda'$ sono rispettivamente i coniugati del $t$-core e del $t$-quoziente di $\lambda$. Date due partizioni $\lambda, \mu$, scriviamo

$$\lambda \sim_t \mu$$

per indicare che $\tilde{\lambda} = \tilde{\mu}$, cioè che $\lambda$ e $\mu$ hanno lo stesso $t$-core. Come sopra, poniamo $\xi = \lambda + \delta_m$ e $\eta = \mu + \delta_m$, dove $m \geq \max(\ell(\lambda), \ell(\mu))$. Abbiamo allora che $\lambda \sim_t \mu$ se e solo se $\eta \equiv w\xi \pmod t$ per qualche permutazione $w \in S_m$, e inoltre $\lambda \sim_t \mu$ se e solo se $\lambda' \sim_t \mu'$.

Abbiamo dalle definizioni che $\lambda$ è univocamente determinato dal suo $t$-core $\tilde{\lambda}$ e dal suo $t$-quoziente $\lambda^*$. Siccome $|\lambda| = |\tilde{\lambda}| + t|\lambda^*|$, la funzione generatrice per le partizioni con un $t$-core fissato $\tilde{\lambda}$ è

$$\sum_{\tilde{\mu}=\tilde{\lambda}} x^{|\mu|} \;=\; x^{|\tilde{\lambda}|} P(x^t)^t,$$

dove $P(x) = \prod_{n\geq 1}(1-x^n)^{-1}$ è la funzione generatrice delle partizioni. Quindi la funzione generatrice per i $t$-core è

$$\begin{aligned} \sum x^{|\tilde{\lambda}|} &= P(x)/P(x^t)^t \\ &= \prod_{n\geq 1} \frac{(1-x^{nt})^t}{1-x^n}, \end{aligned}$$

e in particolare per $t = 2$ abbiamo ottenuto l'identità

$$\sum_{m\geq 1} x^{m(m-1)/2} = \prod_{n\geq 1}(1-x^{2n})(1+x^n),$$

o espandendo alternativamente $\prod_n (1-x^n) = \prod_n (1-x^{2n})(1-x^{2n-1})$

$$= \prod_{n\geq 1} \frac{1-x^{2n}}{1-x^{2n-1}}.$$

# Capitolo 2

# Funzioni simmetriche

> Anyone who uses the phrase 'easy as taking candy from a baby' has never tried taking candy from a baby.
>
> *Unknown*

In questo capitolo presentiamo la teoria fondamentale delle funzioni simmetriche, seguendo principalmente [Mac95].

Per studiare le proprietà combinatorie delle basi fondamentali di questo anello, considerare le funzioni simmetriche in infinite variabili costituisce di fatto una semplificazione, e il primo passo nello studio di queste proprietà si ottiene scrivendo le funzioni generatrici dei generatori fondamentali (come anello), e le formule che mettono in relazioni tali funzioni generatrici.

Nelle formule che collegano alcune di queste basi vengono alla luce importanti strutture del gruppo simmetrico, e nei prossimi capitoli vedremo come esse siano un caso particolare di uno schema più generale nel quale entrano in gioco i caratteri del gruppo simmetrico.

## 2.1 L'anello delle funzioni simmetriche

Consideriamo l'anello $\mathbb{Z}[x_1, \ldots, x_n]$ dei polinomi in $n$ indeterminate $x_1, \ldots, x_n$ a coefficienti interi. Il gruppo simmetrico $S_n$ agisce su questo anello permutando le variabili, e un polinomio è *simmetrico* se è invariante sotto questa azione. I polinomi simmetrici formano il sottoanello degli invarianti

$$\Lambda_n = \mathbb{Z}[x_1, \ldots, x_n]^{S_n}.$$

$\Lambda_n$ eredita la graduazione di $\mathbb{Z}[x_1, \ldots, x_n]$, e abbiamo che

$$\Lambda_n = \bigoplus_{k \geq 0} \Lambda_n^k,$$

dove $\Lambda_n^k$ consiste dei polinomi simmetrici omogenei di grado $k$, più il polinomio zero.

Per $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, chiameremo $x^\alpha$ il monomio

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}.$$

Se $\lambda$ è una partizione di lunghezza $\leq n$, il polinomio

$$m_\lambda(x_1, \ldots, x_n) = \sum x^\alpha,$$

sommando su tutte le permutazioni distinte $\alpha$ di $\lambda$, è simmetrico e inoltre gli $m_\lambda$ (al variare di $\lambda$ fra tutte le partizioni di lunghezza $\leq n$) formano una base di $\Lambda_n$ come $\mathbb{Z}$-modulo. In particolare gli $m_\lambda$ con $\ell(\lambda) \leq n$ e $|\lambda| = k$ sono una $\mathbb{Z}$-base di $\Lambda_n^k$, e non appena $n \geq k$ gli $m_\lambda$ per tutti i $\lambda$ tali che $|\lambda| = k$ formano una $\mathbb{Z}$-base di $\Lambda_n^k$ (infatti la condizione $\ell(\lambda) \leq n$ è automaticamente verificata).

Solitamente nella teoria delle funzioni simmetriche il numero di variabili è irrilevante purché sia grande abbastanza, e risulta quindi comodo lavorare direttamente con funzioni simmetriche in infinite variabili. Per formalizzare questo concetto, sia $m \geq n$ e consideriamo l'omomorfismo

$$\mathbb{Z}[x_1, \ldots, x_m] \ \to \ \mathbb{Z}[x_1, \ldots, x_n]$$

definito mandando tutti gli $x_{n+1}, \ldots, x_m$ in zero, e tutti gli altri $x_i$ in se stessi. La restrizione a $\Lambda_m$ ci dà l'omomorfismo

$$\rho_{m,n} : \Lambda_m \ \to \ \Lambda_n, \tag{2.1}$$

che possiamo descrivere facilmente anche in termini della base $(m_\lambda)$:

$$m_\lambda(x_1, \ldots, x_m) \ \mapsto \ \begin{cases} m_\lambda(x_1, \ldots, x_n) & \text{se } \ell(\lambda) \leq n, \\ 0 & \text{altrimenti.} \end{cases}$$

Ne segue che $\rho_{m,n}$ è surgettiva, e la restrizione a $\Lambda_m^k$ ci dà l'omomorfismo

$$\rho_{m,n}^k : \Lambda_m^k \ \to \ \Lambda_n^k \qquad \text{per } k \geq 0 \text{ e } m \geq n,$$

che è sempre surgettivo, e bigettivo se $n \geq k$. Inoltre $\rho_{\ell,n}^k = \rho_{\ell,m}^k \circ \rho_{m,n}^k$ per $\ell \geq m \geq n$.

Possiamo quindi considerare il limite inverso

$$\Lambda^k \ = \ \varprojlim_n \Lambda_n^k$$

degli $\mathbb{Z}$-moduli $\Lambda_n^k$ tramite gli omomorfismi $\rho_{m,n}^k$: un elemento di $\Lambda^k$ è per definizione una successione $f = (f_n)_{n \geq 0}$, tale che $f_n \in \Lambda_n^k$ e $f_n = \rho_{m,n}^k(f_m)$ per ogni $m \geq n$, ovvero ciascun $f_m(x_1, \ldots, x_m)$ è un polinomio simmetrico in $m$ variabili e $f_n(x_1, \ldots, x_n) = f_m(x_1, \ldots, x_n, 0, \ldots, 0)$. Siccome $\rho_{m,n}^k$ è un isomorfismo per $m \geq n \geq k$, la proiezione

$$\rho_n^k : \Lambda^k \ \to \ \Lambda_n^k$$

(che manda $f$ in $f_n$) è un isomorfismo per $n \geq k$, e quindi $\Lambda^k$ ha una $\mathbb{Z}$-base, detta delle *funzioni simmetriche monomiali*, degli $m_\lambda$ definiti da

$$\rho_n^k(m_\lambda) = m_\lambda(x_1, \ldots, x_n)$$

per ogni $\lambda$ partizione di $k$, e $n \geq k$ (la definizione non dipende dall'$n$, purché $n \geq k$). Il altre parole gli $m_\lambda(x_1, \ldots, x_n)$, per $n \geq k = |\lambda|$, definiscono un ben preciso elemento del limite inverso $\Lambda^k$. Abbiamo quindi che $\Lambda^k$ è uno $\mathbb{Z}$-modulo libero di rango $p(k)$, il numero di partizioni di $k$.

Sia ora

$$\Lambda = \bigoplus_{k \geq 0} \Lambda^k,$$

che è uno $\mathbb{Z}$-modulo libero generato dai $m_\lambda$ per tutte le possibili partizioni $\lambda$. Abbiamo gli omomorfismi surgettivi

$$\rho_n = \bigoplus_{k \geq n} \rho_n^k : \Lambda \to \Lambda_n$$

per ogni $n \geq 0$, e $\rho_n$ è un isomorfismo per i gradi $k \leq n$. Possiamo ora trasportare la struttura di anello dei $\Lambda_n$ su $\Lambda$, trasformando $\Lambda$ in un anello graduato su cui i $\rho_n$ sono omomorfismi di anelli. L'anello graduato $\Lambda$ appena definito è detto l'*anello delle funzioni simmetriche*[1] in un'infinità numerabile di variabili $x_1, x_2, \ldots$ .

**Nota.** *$\Lambda$ non è il limite inverso (nella categoria degli anelli) degli anelli $\Lambda_n$ relativamente agli omomorfismi $\rho_{m,n}$. Tale limito inverso, $\hat{\Lambda}$ poniamo, ad esempio contiene il prodotto infinito $\prod_{i=0}^{\infty}(1 + x_i)$, che non appartiene a $\Lambda$, perché gli elementi di $\Lambda$ hanno grado finito essendo combinazioni intere finite delle funzioni simmetriche monomiali $m_\lambda$. $\Lambda$ è comunque il limite inverso dei $\Lambda_n$ nella categoria degli anelli* graduati.

**Nota.** *Al posto di $\mathbb{Z}$ è possibile usare un qualunque altro anello commutativo $A$, nel qual caso si ottiene $\Lambda_A \cong \Lambda \otimes_{\mathbb{Z}} A$.*

## 2.2 Funzioni simmetriche elementari

Per ogni $r \geq 0$, la $r$-esima *funzione simmetrica elementare* $e_r$ è la somma di tutti i prodotti di $r$ variabili distinte $x_i$, e quindi $e_0 = 1$ e

$$e_r \;=\; m_{(1^r)} \;=\; \sum_{i_1 < i_2 < \cdots < i_r} x_{i_1} x_{i_2} \ldots x_{i_r} \qquad \text{per } r \geq 1.$$

La funzione generatrice degli $e_r$ è

$$E(t) \;=\; \sum_{r \geq 0} e_r t^r \;=\; \prod_{i \geq 1} (1 + x_i t) \tag{2.2}$$

[1] Gli elementi di $\Lambda$ non sono più polinomi (a differenza degli elementi quelli di $\Lambda_n$), ma sono somme formali infinite di monomi. Si usa quindi il nome 'funzioni simmetriche'.

(dove $t$ è una nuova indeterminata), come è possibile verificare espandendo il prodotto che compare sulla destra. Se il numero di variabili è finito, $n$ poniamo, allora $e_r$ (o meglio $\rho_n(e_r)$, che quando il numero di variabili è chiaro del contesto chiameremo anche $e_r$ con leggero abuso di notazione) è zero per tutti gli $r \geq n$, e la (2.2) prende la forma

$$\sum_{r=0}^{n} e_r t^r \;=\; \prod_{i=1}^{n}(1+x_i t),$$

dove ambo i membri sono elementi di $\Lambda_n[t]$. Similarmente, sarà possibile applicare questa osservazione a molte delle formule che compariranno nel seguito, passando dal caso in infinite variabili a quello con un numero finito di variabili.

Definiamo ora per ogni partizione $\lambda = (\lambda_1, \lambda_2, \dots)$:

$$e_\lambda \;=\; e_{\lambda_1} e_{\lambda_2} \cdots \;.$$

**Proposizione 2.2.1.** *Sia $\lambda$ un partizione, e $\lambda'$ la sua coniugata. Allora*

$$e_{\lambda'} \;=\; \mu_\lambda + \sum_{\mu<\lambda} a_{\lambda\mu} m_\mu,$$

*dove gli $a_{\lambda\mu}$ sono non-negativi, e la somma è su tutte le partizioni $\mu < \lambda$ nell'ordinamento naturale.*

*Dimostrazione.* Espandendo il prodotto $e_{\lambda'} = e_{\lambda'_1} e_{\lambda'_2} \dots$, otteniamo una somma di monomi ciascuno dei quali ha la forma

$$x^\alpha \;=\; (x_{i_1} x_{i_2} \dots)(x_{j_1} x_{j_2} \dots) \dots,$$

dove $i_1 < i_2 < \cdots < i_{\lambda'_1}$, $j_1 < j_2 < \cdots < j_{\lambda'_2}$, etc. Scriviamo ora i numeri $i_1, i_2, \dots, i_{\lambda'_1}$ in ordine crescente dall'alto in basso nella prima colonna di $\lambda$, i numeri $j_1, j_2, \dots, j_{\lambda'_2}$ in ordine crescente nella seconda, e così via. È chiaro che per ogni $r \geq 1$ tutti i simboli $\leq r$ inseriti nel diagramma di $\lambda$ devono necessariamente comparire nelle prime $r$ righe. Abbiamo quindi che, essendo ogni $\alpha_i$ il numero di occorrenze di $i$ nel diagramma, $\alpha_1 + \cdots + \alpha_r \leq \lambda_1 + \cdots + \lambda_r$ per ogni $r$, ovvero $\alpha \leq \lambda$. Quindi

$$e_{\lambda'} \;=\; \sum_{\mu\leq\lambda} a_{\lambda\mu} m_\mu$$

con $a_{\lambda\mu} \geq 0$ per ogni $\mu \leq \lambda$. Questo argomento ci permette inoltre di dedurre che il monomio $x^\lambda$ occorre esattamente una volta, per cui $a_{\lambda\lambda} = 1$. □

**Proposizione 2.2.2.** *Abbiamo che*

$$\Lambda \;=\; \mathbb{Z}[e_1, e_2, \dots],$$

*e gli $e_r$ sono algebricamente indipendenti su $\mathbb{Z}$.*

*Dimostrazione.* Gli $m_\lambda$ sono una base di $\Lambda$ come $\mathbb{Z}$-modulo, e la proposizione 2.2.1 ci dice che gli $e_\lambda$ sono un'altra base: in altre parole, ogni elemento di $\Lambda$ si scrive in modo unico come polinomio negli $e_r$. □

**Nota.** *Nel caso con solo una quantità finita di variabili $x_1, \ldots, x_n$, la proposizione 2.2.2 ci dice che $\Lambda_n = \mathbb{Z}[e_1, \ldots, e_n]$ e che gli $e_1, \ldots, e_n$ sono algebricamente indipendenti. Così è solitamente enunciato il 'teorema fondamentale delle funzioni simmetriche'.*

## 2.3 Funzioni simmetriche complete

Per ogni $r \geq 0$, la $r$-esima *funzione simmetrica completa* $h_r$ è la somma di tutti i monomi di grado totale $r$ nelle variabili $x_1, x_2, \ldots$, ovvero

$$h_r \;=\; \sum_{|\lambda|=r} m_\lambda.$$

In particolare, $h_0 = 1$ e $h_1 = e_1$. È conveniente inoltre definire $e_r = h_r = 0$ per $r < 0$.

La funzione generatrice delle $h_r$ è

$$H(t) \;=\; \sum_{r\geq 0} h_r t^r \;=\; \prod_{i\geq 1} (1 - x_i t)^{-1}. \tag{2.3}$$

Per convincersi di questa uguaglianza, è sufficiente osservare che

$$(1 - x_i t)^{-1} \;=\; \sum_{k\geq 0} x_i^k t^k,$$

e moltiplicando insieme tutte queste serie geometriche otteniamo che il coefficiente di $t^r$ è precisamente la somma di tutti i monomi di grado $r$ in $x_1, x_2, \ldots$, cioè $h_r$.

Dalle (2.2) e (2.3) abbiamo che

$$H(t)E(-t) \;=\; 1 \tag{2.4}$$

o, equivalentemente,

$$\sum_{r=0}^{n} (-1)^r e_r h_{n-r} \;=\; 0, \qquad \text{per ogni } n \geq 1. \tag{2.4'}$$

Siccome gli $e_r$ sono algebricamente indipendenti (prop. 2.2.2), possiamo definire un omomorfismo di anelli graduati

$$\omega : \Lambda \to \Lambda$$

come

$$\omega(e_r) \;=\; h_r \tag{2.5}$$

per ogni $r \geq 0$. La simmetria delle relazioni (2.4') rispetto alle $e$ e alle $h$ ci permette di osservare che:

**Proposizione 2.3.1.** *$\omega$ è un'involuzione, ovvero $\omega^2$ è la mappa identica.*

Quindi $\omega$ è un automorfismo di $\Lambda$, e dato che come già sappiamo gli $e_r$ generano $\Lambda$ e sono algebricamente indipendenti:

**Proposizione 2.3.2.** *Abbiamo che*

$$\Lambda \;=\; \mathbb{Z}[h_1, h_2, \dots],$$

*e gli $h_r$ sono algebricamente indipendenti su $\mathbb{Z}$.*

**Nota.** *Se il numero di variabili è finito, n poniamo (cosicché $e_r = 0$ per $r > n$), la mappa $\omega : \Lambda_n \to \Lambda_n$ è definita da $\omega(e_r) = h_r$ per $1 \le r \le n$ ed è ancora un'involuzione grazie alla (2.4'). Quindi $\Lambda_n = \mathbb{Z}[h_1, \dots, h_n]$ con $h_1, \dots, h_n$ algebricamente indipendenti, ma gli $h_{n+1}, h_{n+2}, \dots$ sono polinomi non nulli negli $h_1, \dots, h_n$ (o, volendo, negli $e_1, \dots, e_n$). Si noti che non è però più vero che $\omega(e_r) = h_r$ per gli $r > n$, in altre parole se chiamiamo $\omega_n$ l'involuzione appena definita su $\Lambda_n$, e $\rho_n$ è la mappa di restrizione $\Lambda \to \Lambda_n$, allora $\omega_n \circ \rho_n \neq \rho_n \circ \omega$.*

Come per gli $e_\lambda$, definiamo

$$h_\lambda \;=\; h_{\lambda_1} h_{\lambda_2} \dots$$

per ogni partizione $\lambda = (\lambda_1, \lambda_2, \dots)$. Per la 2.3.2 gli $h_\lambda$ sono una $\mathbb{Z}$-base di $\Lambda$. Abbiamo quindi tre basi: gli $m_\lambda$, gli $e_\lambda$ e gli $h_\lambda$, gli ultime due dei quali sono in corrispondenza tramite l'involuzione $\omega$. Se ora per una partizione $\lambda$ definiamo

$$f_\lambda \;=\; \omega(m_\lambda),$$

gli $f_\lambda$ sono una quarta $\mathbb{Z}$-base di $\Lambda$ (sono le funzioni simmetriche 'dimenticate', e non hanno una semplice descrizione diretta).

Dalle relazioni (2.4) è possibile ricavare un'importante identità dei determinanti di matrici associate alle funzioni generatrici $H(t)$ e $E(t)$. Sia $N$ un intero positivo, e consideriamo le matrici di $N+1$ righe e colonne

$$H \;=\; (h_{i-j})_{0 \le i,j \le N}, \qquad E \;=\; ((-1)^{i-j} e_{i-j})_{0 \le i,j \le N}$$

usando la convenzione di porre $h_r = e_r = 0$ per $r < 0$. Si noti che esse sono le matrici di Toeplitz di ordine $n+1$ associate alle serie $H(t)$ e $E(-t)$, e ricordiamo che moltiplicare due matrici di Toepliz associate a delle serie equivale a passare alla matrice di Toeplitz associata al prodotto delle serie.

Nel nostro caso $H$ e $E$ sono triangolari inferiori, con tutti 1 sulla diagonale, e quindi $\det H = \det E = 1$, ed inoltre la (2.4) ci dice che le matrici $H$ e $E$ sono una l'inversa dell'altra. Ne segue che ogni minore di $H$ è uguale al cofattore complementare di $E^t$, la trasposta di $E$ (per convincersi di questo basta ad esempio vedere il determinante di un minore di $H$ come il coefficiente del termine di grado massimo in $t$ del polinomio $\det(tM + H) = \det(tME + 1)$, per una opportuna matrice $M$ che è l'identità sul complementare del minore e 0 altrove).

Siano $\lambda, \mu$ partizioni di lunghezza $\leq p$, con $\lambda'$ e $\mu'$ di lunghezza $\leq q$, per qualche $p, q$ tali che $p+q = N+1$. Consideriamo il minore di $H$ individuato dalle righe $\lambda_i + p - i$ (per $i = 1, \ldots, p$) e dalle colonne $\mu_j + p - j$ (per $j = 1, \ldots, p$). Per la proposizione 1.2.1, i cofattori complementari di $E^t$ hanno righe $p - 1 + k - \lambda'_k$ (per $k = 1, \ldots, q$), e colonne $p - 1 + \ell - \mu'_\ell$ (per $\ell = 1, \ldots, q$). Abbiamo quindi che

$$\det(h_{\lambda_i - \mu_j - i + j})_{1 \leq i,j \leq p} \;=\; (-1)^{|\lambda| + |\mu|} \det((-1)^{\lambda'_k - \mu'_\ell - k + \ell} e_{\lambda'_k - \mu'_\ell - k + \ell})_{1 \leq k,\ell \leq q}.$$

I segni meno si cancellano, e quindi abbiamo l'identità

$$\det(h_{\lambda_i - \mu_j - i + j})_{1 \leq i,j \leq p} \;=\; \det(e_{\lambda'_k - \mu'_\ell - k + \ell})_{1 \leq k,\ell \leq q}, \tag{2.6}$$

e in particolare, se $\mu = 0$:

$$\det(h_{\lambda_i - i + j})_{1 \leq i,j \leq p} \;=\; \det(e_{\lambda'_k - k + \ell})_{1 \leq k,\ell \leq q}. \tag{2.7}$$

## 2.4 Somme di potenze

Per ogni $r \geq 1$, l'$r$-esima *somma di potenze* è

$$p_r \;=\; \sum x_i^r \;=\; m_{(r)}.$$

La funzione generatrice per i $p_r$ è

$$\begin{aligned} P(t) = \sum_{r \geq 1} p_r t^{r-1} \;&=\; \sum_{i \geq 1} \sum_{r \geq 1} x_i^r t^{r-1} \\ &= \sum_{i \geq 1} \frac{x_i}{1 - x_i t} \\ &= \sum_{i \geq 1} \frac{\mathrm{d}}{\mathrm{d}t} \log \frac{1}{1 - x_i t}, \end{aligned}$$

da cui

$$P(t) \;=\; \frac{\mathrm{d}}{\mathrm{d}t} \log \prod_{i \geq 1} (1 - x_i t)^{-1} \;=\; \frac{\mathrm{d}}{\mathrm{d}t} \log H(t) = \frac{H'(t)}{H(t)}, \tag{2.8}$$

e allo stesso modo

$$P(-t) \;=\; \frac{\mathrm{d}}{\mathrm{d}t} \log E(t) \;=\; \frac{E'(t)}{E(t)}. \tag{2.9}$$

Le (2.8) e (2.9) ci dicono che

$$n h_n = \sum_{r=1}^{n} p_r h_{n-r}, \tag{2.8'}$$

$$n e_n = \sum_{r=1}^{n} (-1)^{r-1} p_r e_{n-r} \tag{2.9'}$$

per ogni $n \geq 1$, e queste equazioni ci permettono di esprimere gli $h_r$ e gli $e_r$ in termini dei $p_r$, e viceversa. Le (2.9') risalgono a Isaac Newton, e sono note come *formule di Newton*. Dalle (2.8') è chiaro che $h_n \in \mathbb{Q}[p_1, \dots, p_n]$, e (ricordando che $h_0 = 1$) anche $p_n \in \mathbb{Q}[h_1, \dots, h_n]$, e quindi

$$\mathbb{Q}[p_1, \dots, p_n] \;=\; \mathbb{Q}[h_1, \dots, h_n].$$

Siccome gli $h_r$ sono algebricamente indipendenti su $\mathbb{Z}$ (e quindi anche su $\mathbb{Q}$), ne segue la:

**Proposizione 2.4.1.** *Abbiamo che*

$$\Lambda_{\mathbb{Q}} \;=\; \Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \;=\; \mathbb{Q}[p_1, p_2, \dots],$$

*e i $p_r$ sono algebricamente indipendenti su $Q$.*

Quindi se definiamo

$$p_\lambda \;=\; p_{\lambda_1} p_{\lambda_2} \cdots$$

per ogni partizione $\lambda = (\lambda_1, \lambda_2, \dots)$, allora i $p_\lambda$ formano una base di $\Lambda_{\mathbb{Q}}$ come $\mathbb{Q}$-modulo. Notiamo però che *non* sono una base di $\Lambda$ come $\mathbb{Z}$-modulo: per esempio, $h_2 = \frac{1}{2}(p_1^2 - p_2)$ non ha coefficienti interi quando è scritto in termini dei $p_\lambda$.

Vediamo ora come si comporta l'involuzione $\omega$ sui $p_r$: siccome $\omega$ scambia $E(t)$ e $H(t)$, segue dalle (2.8) e (2.9) che

$$\omega(p_n) \;=\; (-1)^{n-1} p_n, \qquad \text{per ogni } n \geq 1,$$

e quindi per una qualunque partizione $\lambda$ abbiamo che

$$\omega(p_\lambda) \;=\; \varepsilon_\lambda p_\lambda,$$

dove $\varepsilon_\lambda = \prod_{i=1}^{\ell(\lambda)} (-1)^{\lambda_i - 1} = (-1)^{|\lambda| - \ell(\lambda)}$.

Infine, esprimiamo ora gli $h_r$ e $e_r$ come combinazioni lineari dei $p_\lambda$. Ma vediamo prima alcuni esempi:

$$\begin{aligned}
e_1 &= p_1, \\
2e_2 &= p_1^2 - p_2, \\
6e_3 &= p_1^3 - 3p_1p_2 + 2p_3, \\
24e_4 &= p_1^4 - 6p_1^2p_2 + 3p_2^2 + 8p_1p_3 - 6p_4, \\
&\dots
\end{aligned}$$

Uno schema interessante viene alla luce, perché i coefficienti dei $p_\lambda$ sono le cardinalità delle classi di coniugio del gruppo simmetrico $S_n$ costituite dagli elementi che hanno decomposizione in cicli[2] di tipo $\lambda$ (ovvero $m_i(\lambda)$ è il numero degli $i$-cicli), e il segno è il segno delle permutazioni nella classe, ovvero $\varepsilon_\lambda$.

[2]Ricordiamo infatti che ciascun elemento di $S_n$ si decompone come prodotto di cicli disgiunti, e che le cardinalità dei cicli determinano univocamente la classe di coniugio.

Data una partizione $\lambda$, definiamo

$$z_\lambda = \prod_{i\geq 1} i^{m_i(\lambda)} \cdot m_i(\lambda)!.$$

Si noti che, se $n = |\lambda|$, il numero di elementi del gruppo $S_n$ che hanno decomposizione in cicli di tipo $\lambda$ è:

$$\frac{\prod_{i=1}^{\ell(\lambda)} \binom{\lambda_i+\cdots+\lambda_{\ell(\lambda)}}{\lambda_i}(\lambda_i-1)!}{\prod_{i\geq 1} m_i!} = \frac{n!}{\prod_{i\geq 1} i^{m_i}\cdot m_i!} = \frac{n!}{z_\lambda}.$$

Mostreremo allora che

$$H(t) = \sum_\lambda z_\lambda^{-1} p_\lambda t^{|\lambda|}, \tag{2.10}$$

$$E(t) = \sum_\lambda \varepsilon_\lambda z_\lambda^{-1} p_\lambda t^{|\lambda|}, \tag{2.11}$$

o equivalentemente:

$$h_n = \sum_{|\lambda|=n} z_\lambda^{-1} p_\lambda, \tag{2.10'}$$

$$e_n = \sum_{|\lambda|=n} \varepsilon_\lambda z_\lambda^{-1} p_\lambda. \tag{2.11'}$$

*Dimostrazione.* È sufficiente dimostrare la formula con le $h_r$, perché quella con le $e_r$ segue immediatamente da questa applicando l'involuzione $\omega$ e usando la (2.4). Siccome $P(t) = \frac{\mathrm{d}}{\mathrm{d}t}\log H(t)$ per la (2.8), abbiamo che

$$\begin{aligned} H(t) &= \exp\sum_{r\geq 1}\frac{p_r t^r}{r} \\ &= \prod_{r\geq 1}\exp\frac{p_r t^r}{r} \\ &= \prod_{r\geq 1}\sum_{m_r=0}^{\infty}\frac{(p_r t^r)^{m_r}}{r^{m_r}\cdot m_r!} \\ &= \sum_\lambda z_\lambda^{-1} p_\lambda t^{|\lambda|}. \end{aligned}$$

□

Prima di concludere la sezione ricaviamo alcune formule determinantali che mettono relazione i $p_n$ e gli $e_r$ e $h_r$.

Dalle (2.8') abbiamo che

$$\begin{pmatrix} 1 & & & & \\ e_1 & 1 & & & \\ e_2 & e_1 & 1 & & \\ \vdots & \vdots & & \ddots & \\ e_{n-1} & e_{n-2} & e_{n-3} & \dots & 1 \end{pmatrix} \begin{pmatrix} p_1 \\ -p_2 \\ p_3 \\ \vdots \\ (-1)^{n-1}p_n \end{pmatrix} = \begin{pmatrix} e_1 \\ 2e_2 \\ 3e_3 \\ \vdots \\ ne_n \end{pmatrix},$$

e anche che

$$\begin{pmatrix} 1 & & & & \\ p_1 & 2 & & & \\ p_2 & p_1 & 3 & & \\ \vdots & \vdots & & \ddots & \\ p_{n-1} & p_{n-2} & p_{n-3} & \dots & n \end{pmatrix} \begin{pmatrix} e_1 \\ -e_2 \\ e_3 \\ \vdots \\ (-1)^{n-1}e_n \end{pmatrix} = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_n \end{pmatrix}.$$

Risolvendole con Cramer rispettivamente in $(-1)^{n-1}p_n$ e in $(-1)^{n-1}e_n$, e semplificando i segni, otteniamo che

$$p_n = \det \begin{pmatrix} e_1 & 1 & & & \\ 2e_2 & e_1 & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \\ {\scriptstyle (n-1)}e_{n-1} & e_{n-2} & e_{n-3} & \dots & 1 \\ ne_n & e_{n-1} & e_{n-2} & \dots & e_1 \end{pmatrix}, \tag{2.12}$$

e che

$$n! \cdot e_n = \det \begin{pmatrix} p_1 & 1 & & & \\ p_2 & p_1 & 2 & & \\ \vdots & \vdots & \vdots & \ddots & \\ p_{n-1} & p_{n-2} & p_{n-3} & \dots & n-1 \\ p_n & p_{n-1} & p_{n-2} & \dots & p_1 \end{pmatrix}. \tag{2.13}$$

Ripetendo il conto con gli $h_n$, o applicando l'involuzione $\omega$ e facendo attenzione ai segni, abbiamo le formule duali

$$(-1)^{n-1}p_n = \det \begin{pmatrix} h_1 & 1 & & & \\ 2h_2 & h_1 & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \\ {\scriptstyle (n-1)}h_{n-1} & h_{n-2} & h_{n-3} & \dots & 1 \\ nh_n & h_{n-1} & h_{n-2} & \dots & h_1 \end{pmatrix}, \tag{2.14}$$

e

$$n! \cdot h_n = \det \begin{pmatrix} p_1 & -1 & & & \\ p_2 & p_1 & -2 & & \\ \vdots & \vdots & \vdots & \ddots & \\ p_{n-1} & p_{n-2} & p_{n-3} & \dots & -n+1 \\ p_n & p_{n-1} & p_{n-2} & \dots & p_1 \end{pmatrix}. \tag{2.15}$$

## 2.5 Applicazioni

Raccogliamo in questa sezione alcune applicazioni della teoria delle funzioni simmetriche. In particolare, osserviamo che siccome gli $h_r$ (e gli $e_r$) sono algebricamente indipendenti, sarà possibile definire un omomorfismo da $\Lambda$ in qualunque anello $A$ mandando gli $h_r$ (o degli $e_r$) in elementi arbitrari di $A$.

Alternativamente, possiamo porre $H(t)$ (o $E(t)$) uguale ad una qualunque serie di potenze formale in $t$ a coefficienti nell'anello $A$, e dedurre proprietà degli $h_r$, $e_r$, $p_r$, etc.

In queste applicazioni della teoria delle funzioni simmetriche seguiamo essenzialmente [Mac95], e [Com74] per quanto riguarda alcune parti più strettamente combinatorie.

### 2.5.1 La funzione generatrice delle partizioni

Ad esempio, se imponiamo che

$$H(t) \;=\; \prod_{i=1}^{\infty}(1-t^i)^{-1} \in \mathbb{Z}[[t]],$$

la funzione generatrice delle partizioni, abbiamo che $h_n = p(n)$, il numero di partizioni di $n$. Allora $E(-t) = \prod_{i=1}^{\infty}(1-t^i)$, e per il teorema dei numeri pentagonali di Eulero $e_n = 0$ a meno che $n$ non sia un numero pentagonale, ovvero della forma $n = (3k^2+k)/2$ con $k \in \mathbb{Z}$, e in questo caso $(-1)^n e_n = (-1)^k$, e quindi $e_n = (-1)^{k(k+1)/2}$. Inoltre

$$\begin{aligned} P(t) = \;& \frac{\mathrm{d}}{\mathrm{d}t}\log H(t) \;=\; \sum_{i=n}^{\infty}\frac{nt^{n-1}}{1-t^n} \\ =\; & \sum_{i=n}^{\infty}(nt^{n-1}+nt^{2n-1}+nt^{3n-1}+\dots), \end{aligned}$$

ed è quindi chiaro che $p_r = \sigma(r)$, la somma dei divisori di $r$. La (2.8') ci permette ora di ricavare che

$$p(n) \;=\; \frac{1}{n}\sum_{r=1}^{n}\sigma(r)p(n-r).$$

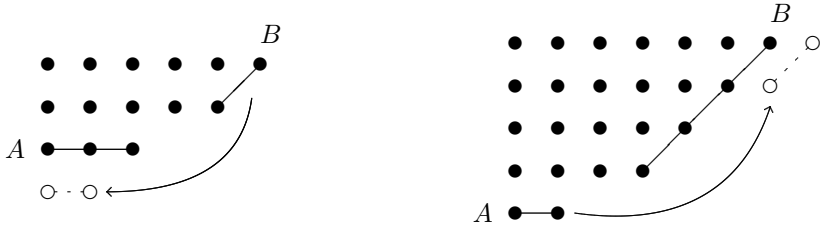
**Il teorema dei numeri pentagonali di Eulero.** Prima di procedere con le applicazioni, esponiamo per completezza l'enunciato e la dimostrazione del teorema. Siano $q_{\mathrm{even}}(n)$ e $q_{\mathrm{odd}}(n)$ rispettivamente il numero di partizioni strette di $n$ costituite da un numero pari e dispari di parti. Il teorema dei numeri pentagonali di Eulero dice allora che

$$q_{\mathrm{even}}(n) - q_{\mathrm{odd}}(n) \;=\; \begin{cases} (-1)^k & \text{se } n = \frac{3k^2+k}{2} \text{ per qualche } k \in \mathbb{Z} \\ 0 & \text{altrimenti.} \end{cases}$$

Consideriamo infatti il diagramma di Ferrers di una partizione stretta $\xi$ di $n$, e sia $A$ l'insieme dei punti nell'ultima riga, e $B$ l'insieme dei punti che sono contenuti nella partizione e che hanno coordinate $(1+k, \xi_1 - k)$ per qualche $k \geq 0$, ovvero quelli che stanno sulla retta inclinata di 45° che parte dall'ultimo punto della prima riga.

Supponiamo che $A$ e $B$ abbiano intersezione vuota. Se $|A| > |B|$ possiamo spostare i punti di $B$ formando una nuova parte di $B$ elementi sotto $A$, mentre

se invece $|A| \leq |B|$ possiamo spostare i punti di $A$ a destra di quelli di $B$, aumentando di uno le prime $A$ parti. Inoltre se applichiamo questa operazione due volte otteniamo la partizione di partenza, e chiaramente il numero di parti varia di uno ogni volta.




D'altra parte se invece $A$ e $B$ si intersecano in un punto, allora possiamo eseguire comunque l'operazione a meno che $|A| = |B|$ o $|A| = |B| + 1$. Per $n$ fissato esiste al più una partizione in cui questo può verificarsi, e se esiste una tale partizione, con $k$ righe poniamo, allora rispettivamente $n = (3k^2 - k)/2$ o $n = (3k^2 + k)/2$, a seconda se si fosse nel caso in cui $|A| = |B|$ o $|A| = |B| + 1$.


Abbiamo quindi costruito una corrispondenza biunivoca fra tutte le partizioni di $n$ con un numero pari e quelle con un numero dispari di parti, tralasciandone al più una, la quale ha $|k|$ parti, nel caso in cui $n = (3k^2 + k)/2$ per qualche $k \in \mathbb{Z}$. Per tali $n$ abbiamo quindi che

$$q_{\text{even}}(n) - q_{\text{odd}}(n) \;=\; (-1)^k,$$

mentre per gli altri questa differenza è zero.

**La funzione generatrice delle partizioni in $k$ parti.** Consideriamo ora le serie di potenze formali

$$\Phi(t,u) \;=\; \prod_{i=1}^{\infty}(1-t^iu)^{-1}, \qquad \Psi(t,u) \;=\; \prod_{i=1}^{\infty}(1+t^iu), \tag{2.16}$$

e osserviamo che il coefficiente di $t^nu^k$ in $\Phi(t,u)$ è precisamente il numero di partizioni di $n$ con $k$ parti, mentre il coefficiente in $\Psi(t,u)$ è il numero di partizioni *strette* di $n$ formate da $k$ parti. Si noti che $\Phi(t,u)\Psi(t,-u) = 1$.

Il teorema di Eulero ci dice allora precisamente che il coefficiente di $t^n$ in $\Psi(t,-1)$, che è una somma in cui vengono contate $+1$ le partizioni di $n$ con

un numero pari di parti e $-1$ quelle con un numero dispari di parti, è $(-1)^k$ se $n = (3k^2 + k)/2$ per qualche $k \in \mathbb{Z}$ e zero altrimenti. Abbiamo quindi provato la osservazione fatta nell'esempio, visto che avevamo $H(t) = \Phi(t, 1)$ e $E(-t) = \Psi(t, -1)$.

È possibile espandere $\Phi(t, u)$ e $\Psi(t, u)$ come

$$\Phi(t,u) \;=\; \prod_{i=1}^{\infty}(1-t^i u)^{-1} \;=\; \sum_{k=0}^{\infty}\frac{t^k}{(1-t)(1-t^2)\dots(1-t^k)}u^k, \tag{2.17}$$

$$\Psi(t,u) \;=\; \prod_{i=1}^{\infty}(1+t^i u) \;=\; \sum_{k=0}^{\infty}\frac{t^{k(k+1)/2}}{(1-t)(1-t^2)\dots(1-t^k)}u^k. \tag{2.17'}$$

Queste espressioni si ricavano facilmente rimpiazzando $u$ con $tu$ nella definizione di $\Phi(t, u)$ e $\Psi(t, u)$, ottenendo le relazioni funzionali

$$\Phi(t,tu) \;=\; (1-tu)\Phi(t,u), \qquad (1+tu)\Psi(t,tu) \;=\; \Psi(t,u),$$

e conseguentemente una relazione ricorrente per i coefficienti di $u^k$.

Le espansioni hanno però anche una interpretazione combinatoria interessante, perché il coefficiente di $t^n$ in $t^k \prod_{i=1}^{k}(1-t^i)^{-1}$, che è anche il coefficiente di $t^{n-k}$ in $\prod_{i=1}^{k}(1-t^i)^{-1}$, è il numero di partizioni di $n-k$ con le parti tutte $\le k$. Aggiungendo a ogni tale partizione una parte di lunghezza $k$ e coniugando, otteniamo tutte le partizioni di $n$ in esattamente $k$ parti, e il loro numero è precisamente il coefficiente di $t^n u^k$ in $\Phi(t, u)$.

Analogamente si può dare l'interpretazione combinatoria dei coefficienti di $\Psi(t, u)$, perché il coefficiente di $t^n$ in $t^{k(k+1)/2}\prod_{i=1}^{k}(1-t^i)^{-1}$ è numero di partizioni di $n - k(k+1)/2$ con parti $\le k$, che passando alle coniugate sono tante quante le partizioni in al più $k$ parti. Sommando a ciascuna tale partizione la partizione $\delta = (k, k-1, \dots, 2, 1)$ otteniamo tutte le partizioni strette di $n$ in $k$ parti, e quindi il coefficiente di $t^n u^k$ in $\Psi(t, u)$.

**L'identità del triplo prodotto di Jacobi.** Se sostituiamo nella (2.17') $t$ con $t^2$ e $u$ con $t^{-1}u$, e se moltiplichiamo l'uguaglianza ottenuta per $\prod_{i\ge1}(1-t^{2i})$, otteniamo che

$$\begin{aligned}
&\prod_{i\ge1}(1-t^{2i})\cdot\prod_{i\ge1}(1+t^{2i-1}u)\\
&= \prod_{i\ge1}(1-t^{2i})\cdot\sum_{j\ge0}\frac{t^{j^2}u^j}{(1-t^2)(1-t^4)\dots(1-t^{2j})}\\
&= \sum_{j\ge0}\left[t^{j^2}u^j\cdot\prod_{i\ge1}(1-t^{2j+2i})\right],
\end{aligned}$$

e inoltre possiamo estendere la somma ai $j \in \mathbb{Z}$, perché per ogni $j < 0$ il prodotto nell'equazione ha almeno un fattore zero.

Consideriamo ora l'espansione del prodotto nella (2.17') dopo aver sostituito $t$ con $t^2$ e $u$ con $-t^{2j}$. Essa ci permette di espandere ulteriormente

$$\begin{aligned} &= \sum_{j\in\mathbb{Z}} \left[ t^{j^2} u^j \cdot \sum_{m\geq 0} \frac{(-1)^m t^{m^2+m+2mj}}{(1-t^2)(1-t^4)\dots(1-t^{2m})} \right] \\ &= \sum_{m\geq 0} \left[ \frac{(-tu^{-1})^m}{(1-t^2)(1-t^4)\dots(1-t^{2m})} \cdot \sum_{j\in\mathbb{Z}} t^{(m+j)^2} u^{m+j} \right] \\ &= \sum_{m\geq 0} \frac{(-tu^{-1})^m}{(1-t^2)(1-t^4)\dots(1-t^{2m})} \cdot \sum_{j\in\mathbb{Z}} t^{j^2} u^j. \end{aligned}$$

Se ora sostituiamo nella (2.17) $t$ con $t^2$ e $u$ con $-(tu)^{-1}$, otteniamo un'identità che ci permette ritrasformare la prima somma in un prodotto ottenendo

$$= \prod_{i\geq 1} (1+t^{2i-1}u^{-1})^{-1} \cdot \sum_{j\in\mathbb{Z}} t^{j^2} u^j.$$

Mettendo insieme la prima e l'ultima espressione della catena di uguaglianze, otteniamo l'*identità del triplo prodotto di Jacobi*

$$\prod_{i\geq 1} (1-t^{2i})(1+t^{2i-1}u)(1+t^{2i-1}u^{-1}) \;=\; \sum_{j\in\mathbb{Z}} t^{j^2} u^j. \tag{2.18}$$

Si noti che ponendo $t = t^{3/2}$ e $u = t^{1/2}$ segue immediatamente il teorema dei numeri pentagonali di Eulero.

Esiste anche una interessante dimostrazione combinatoria di questa identità: siccome $\prod_{i\geq 1}(1-t^{2i})^{-1} = \sum_{m\geq 0} p(m)t^{2m}$, si tratta di dimostrare che

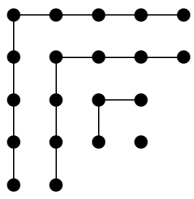
$$\prod_{i\geq 1} (1+t^{2i-1}u)(1+t^{2i-1}u^{-1}) \;=\; \sum_{m\geq 0} p(m)t^{2m} \cdot \sum_{j\in\mathbb{Z}} t^{j^2} u^j.$$

Consideriamo ora il coefficiente di $t^n u^k$ in entrambi i membri, per $n, k \geq 0$. Infatti siccome l'espressione resta invariata sostituendo $u$ con $u^{-1}$ possiamo restringerci ai $k$ non negativi.

Si noti che $\prod_{i\geq 1}(1+t^{2i-1}u)$ è anche la funzione generatrice delle partizioni strette con tutte le parti dispari, che da ora chiameremo semplicemente dispari.

Nell'espressione a sinistra il coefficiente di $t^n u^k$ è quindi il numero di coppie di partizioni strette dispari $\lambda, \mu$ tali che $|\lambda| + |\mu| = n$ e $\ell(\lambda) - \ell(\mu) = k$. Nell'espressione di destra invece il coefficiente di $t^n u^k = t^{2m+j^2} u^j$ è $p(\frac{n-k^2}{2})$, dove abbiamo esteso la funzione delle partizioni ponendo $p(x) = 0$ se $x$ non è intero. Ci basta quindi dimostrare che il numero di coppie di partizioni che soddisfano le condizioni suddette è uguale a $p(\frac{n-k^2}{2})$, per ogni $n$ e $k$.

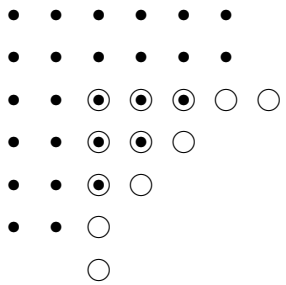
Esiste una esplicita corrispondenza biunivoca fra le partizioni strette dispari e le partizioni invarianti per coniugio, che fa corrispondere a una partizione stretta dispari $\lambda$ la partizione che scritta nella notazione di Frobenius è $(\alpha|\alpha)$, con $\alpha_i = (\lambda_i - 1)/2$ per $i = 1, 2, \dots, \ell(\lambda)$. Diremo che $(\alpha|\alpha)$ è il diagramma *autoconiugato* di $\lambda$.



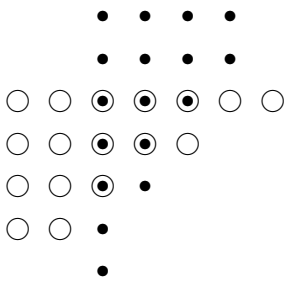
**Il diagramma autoconiugato di** $(9, 7, 3, 1)$**.**

La dimostrazione combinatoria della formula di Jacobi procede ora costruendo una esplicita corrispondenza biunivoca fra le coppie di partizioni $\lambda, \mu$ strette dispari tali che $|\lambda| + |\mu| = n$ e $\ell(\lambda) - \ell(\mu) = k$, e le partizioni di $(n - k^2)/2$.

Date $\lambda, \mu$ che soddisfano le condizioni richieste, disegniamo il digramma autoconiugato di $\lambda$ e sovrapponiamo ad esso il diagramma autoconiugato di $\mu$ traslato di $k$ posizioni lungo la diagonale principale. Ad esempio, se $n = 38$, $k = 2$, e $\lambda = (11, 9, 5, 1)$ e $\mu = (9, 3)$, abbiamo



dove abbiamo disegnato un $\bullet$ nei punti corrispondenti a $\lambda$, e un $\bigcirc$ in quelli corrispondenti a $\mu$. Osserviamo che i punti sulla diagonale, tranne i primi $k$, appartengono sia al diagramma di $\lambda$ che al diagramma di $\mu$. Possiamo ora rimuovere il quadrato di punti $k \times k$ in alto a sinistra, e trasformare sotto la diagonale del diagramma tutti i $\bullet$ in $\bigcirc$ e i $\bigcirc$ in $\bullet$.



Il diagramma risultante è composto dal diagramma traslato a destra di $k$ colonne di una partizione di $(n - k^2)/2$, corrispondente ai $\bullet$, più il diagramma coniugato traslato in basso di $k$ righe, corrispondente ai $\bigcirc$. Questa operazione

può essere chiaramente invertita, passando da una partizione di $(n-k^2)/2$ a una coppia di partizioni $\lambda, \mu$ come sopra, e questo permette di concludere la dimostrazione.

Questa dimostrazione combinatoria dell'identità di Jacobi è quella data da Lewis in [Lew84], con piccole modifiche alla notazione.

**Rappresentazioni come somme di quadrati.** Se imponiamo che

$$E(t) \;=\; \prod_{n\geq 1} \frac{1+t^n}{1-t^n},$$

abbiamo che, sostituendo due volte $\prod(1-t^n) = \prod(1-t^{2n})(1-t^{2n-1})$,

$$\begin{aligned} H(-t) = \prod_{n\geq 1} \frac{1-t^n}{1+t^n} \;&=\; \prod_{n\geq 1} \frac{(1-t^{2n})(1-t^{2n-1})}{1+t^n} \\ &= \prod_{n\geq 1} (1-t^n)(1-t^{2n-1}) \\ &= \prod_{n\geq 1} (1-t^{2n})(1-t^{2n-1})^2 \;=\; \sum_{n\in\mathbb{Z}} (-1)^n t^{n^2} \end{aligned}$$

grazie alla (2.18) in cui si sia posto $u=-1$. Abbiamo quindi che per $r\geq 1$, $h_r = 2$ se $r$ è un quadrato e 0 altrimenti.

Per calcolare i $p_r$, scriviamo invece

$$\begin{aligned} P(-t) = \frac{\mathrm{d}}{\mathrm{d}t} \log E(t) \;&=\; \sum_{n\geq 1} \frac{2nt^{n-1}}{1-t^{2n}} \\ &= 2\sum_{n\geq 1} (nt^{n-1} + nt^{3n-1} + nt^{5n-1} + \dots), \end{aligned}$$

da cui

$$p_n \;=\; 2(-1)^{n-1}\sigma'(n),$$

dove $\sigma'(n)$ è la somma dei divisori $d\geq 1$ di $n$ tali che $n/d$ è dispari.

Siccome $H(t) = \sum_{n\in\mathbb{Z}} t^{n^2}$, abbiamo che

$$H(t)^r \;=\; \sum_{n\geq 0} N_r(n) t^n$$

dove $N_r(n)$ è il numero di rappresentazioni di $n$ come somma di $r$ quadrati, cioè il numero di tuple $(x_1,\dots,x_r)\in\mathbb{Z}^r$ tali che $x_1^2+\dots+x_r^2 = n$.

Se usiamo ora la (2.15) per mettere in relazione gli $\hat{h}_n$ e $\hat{p}_n$ definiti da $\hat{H}(t) = H(t)^r$, e quindi $\hat{P}(t) = rP(t)$, abbiamo che

$$N_r(n) \;=\; \frac{(2r)^n}{n!} \cdot \det \begin{pmatrix} \sigma'(1) & 1/2r & & & \\ \sigma'(2) & \sigma'(1) & 2/2r & & \\ \vdots & \vdots & \vdots & \ddots & \\ \sigma'(n-1) & \sigma'(n-2) & \sigma'(n-3) & \dots & (n-1)/2r \\ \sigma'(n) & \sigma'(n-1) & \sigma'(n-2) & \dots & \sigma'(1) \end{pmatrix}.$$

### 2.5.2 Indicatrice dei cicli e teorema di Pólya

In questa sezione introduciamo alcune tecniche che verrano sviluppate più avanti per studiare il gruppo simmetrico $S_n$. L'*indicatrice dei cicli* del sottogruppo $G$ di $S_n$ è la funzione simmetrica

$$c(G) \;=\; \frac{1}{|G|}\sum_{|\rho|=n} n_G(\rho)p_\rho \;=\; \frac{1}{|G|}\sum_{g\in G} p_{\rho(g)},$$

dove $n_G(\rho)$ è il numero di elementi di $G$ che hanno decomposizione di cicli di tipo $\rho$, e $\rho(g)$ la partizione che indica la decomposizione in cicli di $g \in G$. In particolare

$$c(S_n) \;=\; \sum_{|\rho|=n} z_\rho^{-1} p_\rho \;=\; h_n$$

per la (2.10'), e per il gruppo alternante $A_n$ abbiamo

$$\begin{aligned} c(A_n) &= \frac{2}{n!}\sum_{|\rho|=n} n_{A_n}(\rho)p_\rho \\ &= 2\sum_{\substack{|\rho|=n\\ \rho \text{ pari}}} z_\rho^{-1}p_\rho \\ &= \sum_{|\rho|=n} z_\rho^{-1}p_\rho + \sum_{|\rho|=n} \varepsilon_\rho z_\rho^{-1}p_\rho \\ &= h_n + e_n. \end{aligned}$$

Se $G$ è un sottogruppo di $S_n$ e $H$ sottogruppo di $S_m$, allora $G \times H$ è un sottogruppo di $S_n \times S_m \subseteq S_{n+m}$, e abbiamo che, siccome $\rho((g,h)) = \rho(g) \cup \rho(h)$

$$\begin{aligned} c(G\times H) &= \frac{1}{|G\times H|}\sum_{(g,h)\in G\times H} p_{\rho((g,h))} \\ &= \frac{1}{|G|\cdot|H|}\sum_{(g,h)\in G\times H} p_{\rho(g)}p_{\rho(h)} \\ &= c(G)c(H). \end{aligned}$$

Sia $G$ un sottogruppo di $S_n$, e sia $\Sigma = (\mathbb{N}^+)^n$ l'insieme di tutte le tuple $\alpha = (\alpha_1, \ldots, \alpha_n)$ di $n$ interi positivi. Per ciascuna tupla $\alpha$, definiamo $x_\alpha = x_{\alpha_1}\ldots x_{\alpha_n}$. Il gruppo $G$ agisce su $\Sigma$ permutando gli elementi della tupla, e la funzione $\alpha \mapsto x_\alpha$ è costante su ogni $G$-orbita (anzi per ogni $S_n$-orbita). Allora

$$c(G) \;=\; \sum_{\alpha\in\Sigma/G} x_\alpha$$

al variare di $\alpha$ in un (qualunque) insieme $\Sigma/G$ di rappresentanti delle orbite di $G$ in $\Sigma$. Questa caratterizzazione è nota come *teorema di Pólya*.

*Dimostrazione.* Consideriamo infatti la funzione

$$\frac{1}{|G|} \sum_{\substack{(g,\alpha)\in G\times\Sigma \\ g\alpha=\alpha}} x_\alpha,$$

dove la somma è su tutte le coppie $(g, \alpha) \in G \times \Sigma$ tali che $g\alpha = \alpha$. Allora

$$\sum_{\alpha\in\Sigma/G} x_\alpha \;=\; \frac{1}{|G|} \sum_{\substack{(g,\alpha)\in G\times\Sigma \\ g\alpha=\alpha}} x_\alpha$$

perché, se ci restringiamo a ogni orbita, a sinistra sto prendendo un elemento per orbita, e a destra tutti gli elementi tante volte quanto è lo stabilizzatore di ogni elemento, e dividendo per $|G|$ ho l'uguaglianza grazie alla formula orbita-stabilizzatore.

Ora se invece $g$ è un elemento fissato di $G$ che ha decomposizione in cicli di tipo $\rho$, allora gli $\alpha$ tali che $g\alpha = \alpha$ sono quelli tali che $\alpha_i = \alpha_j$ se $i$ e $j$ appartengono a uno stesso ciclo di $g$, e abbiamo che

$$\begin{aligned}\sum_{\substack{\alpha\in\Sigma \\ g\alpha=\alpha}} x_\alpha &= \sum_{\substack{\alpha\in\Sigma \\ g\alpha=\alpha}} \prod_i x_{\alpha_i} \\ &= \prod_j \sum_k x_k^{\rho_j} \\ &= p_\rho,\end{aligned}$$

e quindi abbiamo anche che

$$\begin{aligned}c(G) &= \frac{1}{|G|} \sum_{g\in G} p_{\rho(g)} \\ &= \frac{1}{|G|} \sum_{\substack{(g,\alpha)\in G\times\Sigma \\ g\alpha=\alpha}} x_\alpha.\end{aligned}$$

□

**Applicazione del teorema di Pólya.** L'importanza in combinatoria del teorema di Pólya nasce dal fatto che esso permette di contare facilmente il numero di modi in cui si può etichettare il certo insieme di oggetti indistinguibili sui quali agisce un certo gruppo di permutazione, e in cui due etichettamenti sono considerati equivalenti se esiste un elemento del gruppo che trasforma uno nell'altro.

Ad esempio, possiamo calcolare il numero di modi in cui è possibile colorare le facce di un cubo con $k$ colori, considerando equivalenti due colorazioni se è possibile ottenere una dall'altra tramite una rotazione. Le rotazioni che mandano il cubo in se stesso sono un sottogruppo $G$ del gruppo simmetrico delle permutazioni delle facce, e non è difficile verificare che l'indicatrice dei cicli di $G$ è

$$c(G) \;=\; \frac{1}{24}(p_1^6 + 6p_1^2p_4 + 3p_1^2p_2^2 + 8p_3^2 + 6p_2^3).$$

Ad esempio, il termine $8p_3^2$ proviene dalle rotazioni di 120° attraverso gli assi passanti per le coppie di vertici opposti, ce ne sono due per ciascuno dei quattro assi e hanno decomposizione in cicli di tipo $(3^2)$, il termine $3p_1^2p_2^2$ dalle rotazioni di 180° attorno l'asse passante per il centro di due facce opposte, che sono tre e hanno decomposizione in cicli di tipo $(2^21^2)$, e così via.

È ora chiaro che una colorazione delle facce di un cubo con $k$ colori si può vedere come una tupla $\alpha \in \Sigma = [1,k]^n$, e che le orbite tramite l'azione di $G$ corrispondono a classi di colorazioni essenzialmente distinte. Il teorema di Pólya ci dice ora che un monomio $x_\alpha$ compare nell'indicatrice dei cicli $c(G)$ tante volte quante sono le $G$-orbite in $\Sigma$ di tuple che sono una permutazione di $\alpha$.

Quindi, se stiamo considerando le colorazioni distinte di un cubo con due colori, ci basta espandere ciascun $p_r$ come $x^r + y^r$ ottenendo

$$c(G) \;=\; x^6 + x^5y + 2x^4y^2 + 2x^3y^3 + 2x^2y^4 + xy^5 + y^6,$$

da cui deduciamo che il numero di colorazioni distinte con due facce rosse e le altre blu è il coefficiente di $x^2y^4$, e quindi 2. Il numero totale di colorazioni distinte con due colori è invece la somma dei coefficienti, e quindi 10.

### 2.5.3 Espansioni e polinomi di Bell

Consideriamo le serie di potenze formali

$$f(t) \;=\; \sum_{n=0}^{\infty} f_n \frac{t^n}{n!} \qquad g(t) \;=\; \sum_{n=1}^{\infty} g_n \frac{t^n}{n!}$$

con coefficienti in una $\mathbb{Q}$-algebra commutativa, e tali che $g$ ha termine costante zero. Possiamo allora considerare la composizione

$$H(t) \;=\; f(g(t)) \;=\; \sum_{n=0}^{\infty} H_n \frac{t^n}{n!},$$

e si osservi che ciascun coefficiente $H_n$ è della forma

$$H_n \;=\; \sum_{k=1}^{n} f_k B_{n,k}(g), \tag{2.19}$$

dove i $B_{n,k}$ sono polinomi nel coefficienti di $g$, detti *polinomi di Bell parziali*.

La trasformazione $f(t) \to f(g(t)) = H(t)$ corrisponde alla moltiplicazione del vettore infinito $(f_n)$ per la matrice (dipendente da $g$) dei $B_{n,k}$:

$$\begin{pmatrix} B_{1,1} & & & & \\ B_{2,1} & B_{2,2} & & & \\ B_{3,1} & B_{3,2} & B_{3,3} & & \\ B_{4,1} & B_{4,2} & B_{4,3} & B_{4,4} & \\ \vdots & & & & \ddots \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ \vdots \end{pmatrix} \;=\; \begin{pmatrix} H_1 \\ H_2 \\ H_3 \\ H_4 \\ \vdots \end{pmatrix} \tag{2.19'}$$

Siccome ciascun $H_n$ è lineare nei coefficienti di $f$, per calcolare i $B_{n,k}$ possiamo prendere $f_n = u^n$ dove $u$ è una nuova indeterminata, ovvero $f(t) = \exp(ut)$. I $B_{n,k}$ sono quindi definiti dalle due (equivalenti) espressioni

$$\begin{aligned} \exp(ug(t)) &= \sum_{n,k} u^k B_{n,k}(g) \frac{t^n}{n!}, \\ \frac{g(t)^k}{k!} &= \sum_{n=k}^{\infty} B_{n,k}(g) \frac{t^n}{n!}, \qquad \text{per ogni } k \geq 1. \end{aligned}$$

Se poniamo $u = 1$, allora i coefficenti di $\exp(g(t))$ sono detti *polinomi di Bell completi*, ovvero

$$\exp(g(t)) \;=\; \sum_n B_n(g) \frac{t^n}{n!}, \qquad B_n(g) \;=\; \sum_{k=1}^{n} B_{n,k}(g).$$

Se imponiamo ora che $H(t)$ sia la funzione generatrice delle funzioni simmetriche complete

$$\exp(ug(t)) \;=\; H(t) \;=\; \sum_{n=1}^{\infty} h_n t^n,$$

otteniamo usando la (2.8) che

$$P(t) \;=\; \frac{\mathrm{d}}{\mathrm{d}t} \log H(t) \;=\; ug'(t) \;=\; \sum_{n=1}^{\infty} u g_n \frac{t^{n-1}}{(n-1)!},$$

e quindi $p_n = ug_n/(n-1)!$ per tutti gli $n \geq 1$. Quindi per la (2.10')

$$H_n \;=\; n! \cdot h_n \;=\; \sum_{|\lambda|=n} \frac{n!}{z_\lambda} p_\lambda$$

e di conseguenza, uguagliando i coefficienti dei termini in $u^k$

$$B_{n,k} \;=\; \sum_{\lambda} c_\lambda g_\lambda, \qquad c_\lambda \;=\; \frac{n!}{\prod_{i \geq 1} m_i(\lambda)! \cdot (i!)^{m_i(\lambda)}} \tag{2.20}$$

dove la somma è su tutte le partizioni di $n$ di lunghezza $k$, e $g_\lambda \;=\; g_{\lambda_1} g_{\lambda_2} \dots$ .

I coefficienti $c_\lambda$ sono interi, perché $c_\lambda$ è il numero di divisioni non ordinate di un insieme di $n$ elementi in sottoinsiemi contenenti $\lambda_1, \lambda_2, \dots$ elementi. Ciascun $B_{n,k}$ è quindi un polinomio nei $g_n$ a coefficienti interi, ed è anzi facile osservare che è omogeneo di grado $k$, e omogeneo di peso $n$ (dove il peso è il grado pesato secondo cui $g_n$ ha grado $n$).

**I numeri di Stirling (del primo tipo).** Consideriamo ora il caso particolare in cui $g(t) = log(1+t)$. Abbiamo allora che $g_n = (-1)^{n-1}(n-1)!$, e i $B_{n,k} = s(n,k)$ sono i *numeri di Stirling del primo tipo*.

In particolare scrivendo

$$s(n,k) \;=\; \sum_{\lambda} c_\lambda g_\lambda \;=\; (-1)^{n-k} \sum_{\lambda} \frac{n!}{z_\lambda}$$

dove la somma è sulle partizioni di $n$ di lunghezza $k$, otteniamo che $|s(n,k)|$ è il numero di elementi di $S_n$ che sono il prodotto di $k$ cicli.

Dalla definizione dei polinomi di Bell abbiamo inoltre che

$$\sum_{n,k} u^k s(n,k) \frac{t^n}{n!} \;=\; \exp(u \log(1+t)) \;=\; (1+t)^u \;=\; \sum_{n \geq 0} \binom{u}{n} t^n.$$

Usando il simbolo di Pochhammer $(u)_n = u(u-1)\dots(u-n+1)$ per fattoriale discendente, otteniamo allora che

$$\sum_{k=1}^{n} s(n,k) u^k \;=\; (u)_n. \tag{2.21}$$

Abbiamo quindi che $s(n,k)$ è la $(n-k)$-esima funzione simmetrica elementare di $-1, -2, \dots, -n+1$. Questa caratterizzazione permette ad esempio di ottenere immediatamente la relazione ricorrente

$$s(n,k) \;=\; (-n+1) \cdot s(n-1,k) + s(n-1,k-1).$$

**I numeri di Stirling (del secondo tipo).** Se prendiamo $g(t) = e^t - 1$, e quindi $g_n = 1$ per $n \geq 1$, allora i $B_{n,k} = S(n,k)$ sono i *numeri di Stirling del secondo tipo*. Siccome

$$S(n,k) = \sum_{\lambda} c_\lambda$$

sommando sulle partizioni di $n$ di lunghezza $k$, $S(n,k)$ è anche il numero di divisioni non ordinate di un insieme di $n$ elementi in $k$ sottoinsiemi disgiunti.

Questa caratterizzazione ci fornisce immediatamente la relazione ricorrente

$$S(n,k) \;=\; S(n-1,k-1) + k \cdot S(n-1,k),$$

che si ottiene contando il numero di divisioni di un insieme di $n$ elementi mettendo da parte un elemento $x$, e considerando il numero modi in cui $x$ forma una parte da solo e il numero di modi in cui forma una parte insieme a una parte degli $n-1$ elementi rimanenti.

Espandendo a sua volta $S(n-1,k) = S(n-2,k-1) + k \cdot S(n-2,k)$, e poi anche $S(n-2,k)$, e così via, e tendo conto che $S(n,k) = 0$ non appena $n < k$, otteniamo che

$$S(n,k) \;=\; \sum_{i \geq 0} k^i S(n-1-i, k-1).$$

Questa identità ci permette di osservare, ragionando per induzione su $k$, che $S(n,k)$ è la $(n-k)$-esima funzione simmetrica completa di $1, 2, \dots, k$.

Siccome le operazioni di comporre una funzione con $log(1+t)$ e con $e^t - 1$ sono una l'inversa dell'altra, le matrici corrispondenti all'operazione di composizione (della (2.19')) devono essere una inversa dell'altra, e applicando questa osservazione alla (2.21) otteniamo la formula duale

$$\sum_{k=1}^{n} S(n,k)(u)_k \;=\; u^n. \tag{2.21'}$$

Se ora $\Delta$ è l'operatore di differenza in avanti $\Delta P(u) = P(u+1) - P(u)$, e $\Delta^r$ è la $r$-esima iterata, abbiamo che

$$\Delta^r (u)_m \;=\; (m)_r (u)_{m-r}, \qquad \Delta^r u^m \;=\; \sum_{i=0}^{r} (-1)^{r-i} \binom{r}{i} (u+i)^m.$$

Applicando $\Delta^k$ alla (2.21') e valutando in $u = 0$, otteniamo l'espressione

$$S(n,k) \;=\; \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} \binom{k}{i} i^n.$$

Questa formula è anche ottenibile in modo combinatorio, perché $k! \cdot S(n,k)$ è anche il numero di funzioni *surgettive* da un insieme di $n$ elementi in uno di $k$ elementi, l'intervallo di interi $\{1, 2, \ldots, k\}$ poniamo. Applicando il principio di inclusione-esclusione agli insiemi $A_i$ delle funzioni la cui immagine non contiene $i$, per $i = 1, 2, \ldots, k$, abbiamo infatti che

$$k! \cdot S(n,k) \;=\; k^n - \binom{k}{1}(k-1)^n + \binom{k}{2}(k-2)^n + \ldots \;.$$

Per ulteriori informazioni sui numeri di Stirling e sulle partizioni di insiemi si veda ad esempio [Com74].

**Polinomi di Bell ordinari.** Siano ora date le serie di potenze

$$f(t) \;=\; \sum_{n=0}^{\infty} f_n t^n, \qquad g(t) \;=\; \sum_{n=1}^{\infty} g_n t^n,$$

dove questa volta i coefficienti non sono moltiplicati da $1/n!$. Nuovamente possiamo considerare la composizione

$$H(t) \;=\; f(g(t)) \;=\; \sum_{n=0}^{\infty} H_n t^n,$$

e scrivere i coefficienti come

$$H_n \;=\; \sum_{k=1}^{n} f_k \hat{B}_{n,k}(g).$$

I polinomi $\hat{B}_{n,k}$ sono talvolta detti *polinomi di Bell parziali ordinari*, per distinguerli da quelli *esponenziali* definiti precedentemente.

Partendo dalla (2.20), o con un conto diretto, si può ricavare che

$$\hat{B}_{n,k}(g) \;=\; \sum_{\lambda} u_\lambda g_\lambda, \qquad u_\lambda \;=\; \frac{\ell(\lambda)!}{\prod_{i\geq 1} m_i(\lambda)!}, \tag{2.22}$$

dove la somma è sulle partizioni di $n$ di lunghezza $k$.

Diamo la dimostrazione diretta, che fornisce una caratterizzazione combinatoria interessante dei coefficienti $u_\lambda$: $\hat{B}_{n,k}(g)$ è il coefficiente di $t^n$ in $g(t)^k$, e vale quindi

$$\sum_{\alpha} g_\alpha$$

sommando sulle tuple di interi positivi $\alpha = (\alpha_1, \ldots, \alpha_k)$ tali che $\alpha_1 + \cdots + \alpha_k = n$, e quindi vale anche

$$\sum_{\lambda} u_\lambda g_\lambda$$

dove la somma è sulle partizioni di $n$ di lunghezza $k$, e dove il coefficiente $u_\lambda$ deve essere la cardinalità dell'orbita di $\lambda$ sotto l'azione del gruppo simmetrico $S_k$ sulle tuple di $k$ elementi (ovvero il numero di $k$-tuple $\alpha$ che riordinate sono uguali a $\lambda$). Calcolando questa cardinalità come $k!$ diviso la cardinalità dello stabilizzatore abbiamo precisamente la definizione degli $u_\lambda$ della (2.22).

Usiamo ora quanto detto per ricavare la scrittura dei $p_n$ in termini degli $h_\lambda$. Sia $H^+(t) = \sum_{n\geq 1} h_n t^n$, cosicché $H(t) = 1 + H^+(t)$ e

$$\log(1 + H^+(t)) \;=\; H^+(t) - \frac{H^+(t)^2}{2} + \frac{H^+(t)^3}{3} - \ldots \;.$$

Abbiamo allora che

$$\begin{aligned} p_n &= \; n \sum_{k\geq 1} \frac{(-1)^{k-1}}{k} \hat{B}_{n,k}(H^+) \\ &= \; n \sum_{|\lambda|=n} \frac{(-1)^{\ell(\lambda)-1}}{\ell(\lambda)} u_\lambda h_\lambda. \end{aligned}$$

Applicando l'involuzione $\omega$ otteniamo la scrittura in termini degli $e_\lambda$

$$p_n \;=\; n \sum_{|\lambda|=n} \frac{\varepsilon_\lambda}{\ell(\lambda)} u_\lambda e_\lambda.$$

Se ora espandiamo invece $E(-t) \;=\; 1 - H^+(t) + H^+(t)^2 - \ldots$, otteniamo

$$\begin{aligned} e_n &= \; \sum_{k\geq 1} (-1)^{k-n} \hat{B}_{n,k}(H^+) \\ &= \; \sum_{|\lambda|=n} \varepsilon_\lambda u_\lambda h_\lambda. \end{aligned}$$

**Inversione e formula di Lagrange.** Sia $g(t) = \sum_{i\geq 1} g_i t^i$, con $g_1 \neq 0$. Se ora $t$ è definito implicitamente come $g(t) = u$, ci riproponiamo di scrivere una serie di potenze in $t$ in funzione di $u$ e dei $g_i$. Supponiamo che $t = g^{\#}(u)$, e per $k$ fissato siano $b_m = \hat{B}_{m,k}(g^{\#})$ i coefficienti di $u$ in

$$t^k = g^{\#}(u)^k = \sum_{m\geq 1} b_m u^m$$

Abbiamo allora che

$$kt^{k-1}\mathrm{d}t \;=\; \sum_{m\geq 1} m b_m u^{m-1}\mathrm{d}u,$$

e quindi $b_m$ è il residuo del differenziale[3]

$$\frac{kt^{k-1}}{mu^m}\mathrm{d}t \;=\; \frac{kt^{k-1}}{mg(t)^m}\mathrm{d}t,$$

ed è anche uguale al coefficiente del termine di grado $-k$ nella scrittura di $k/mg(t)^m$ come serie di Laurent. Chiamiamo $[\![f(t)]\!]_m$ il coefficiente di $t^m$ in $f(t)$. Abbiamo allora ottenuto la rimarchevole

$$[\![g^{\#}(t)^k]\!]_m \;=\; \frac{k}{m}[\![g(t)^{-m}]\!]_{-k}, \tag{2.23}$$

detta *formula di inversione di Lagrange*.

È ora possibile definire un'altra involuzione sull'anello $\Lambda$ come segue. Sia

$$u \;=\; tH(t) \;=\; t + h_1 t^2 + h_3 t^3 + \dots\ .$$

Allora $t$ si può scrivere come serie di potenze in $u$, poniamo ad esempio

$$t \;=\; uH^*(u) \;=\; u + h_1^* u^2 + h_2^* u^3 + \dots,$$

con i coefficienti $h_r^* \in \Lambda^r$ per ogni $r \geq 1$. Le formule mostrano che l'omomorfismo di anelli $\psi : \Lambda \to \Lambda$ definito da $\psi(h_r) = h_r^*$ per ogni $r \geq 1$ è un'*involuzione* su $\Lambda$. Per una qualunque $f \in \Lambda$, chiameremo $f^* = \psi(f)$. Quindi ad esempio $h_\lambda^* = h_{\lambda_1}^* h_{\lambda_2}^* \dots$ per ogni partizione $\lambda$, e gli $h_\lambda^*$ formano una $\mathbb{Z}$-base di $\Lambda$.

Possiamo utilizzare la (2.23) per calcolare gli $h_n^*$ esplicitamente. Ponendo $g(t) = tH(t)$ e applicando la formula con $m = n+1$ e $k = 1$ otteniamo in particolare che

$$h_n^* \;=\; \frac{1}{n+1}[\![g(t)^{-n-1}]\!]_{-1} \;=\; \frac{1}{n+1}[\![H(t)^{-n-1}]\!]_n.$$

[3]Visto che di tratta serie di potenze formali (o di Laurent) un chiarimento è d'obbligo. È possibile definire formalmente il residuo $\mathrm{Res}_u f(u)$ di una serie di Laurent come il coefficiente del termine in $1/u$, e valgono molte delle proprietà che ha in analisi complessa, ad esempio $f(u)$ è una derivata se e solo se $\mathrm{Res}_u f(u) = 0$, e $\mathrm{Res}_u f(u) = u'(t)\mathrm{Res}_t f(u(t))$.

Se scriviamo come abbiamo fatto prima $H(t) = 1 + H^+(t)$, abbiamo che

$$H(t)^{-n-1} \;=\; \sum_{i\geq 0}(-1)^i\binom{n+i}{n}H^+(t)^i,$$

e quindi

$$h_n^* \;=\; \frac{1}{n+1}\sum_{|\lambda|=n}(-1)^{\ell(\lambda)}\binom{n+\ell(\lambda)}{n}u_\lambda h_\lambda,$$

dove gli $u_\lambda$ sono definiti nella (2.22).

Per quanto riguarda gli $e_n$, abbiamo che $t/E(-t) = u$ e $u/E^*(-u) = t$. Se poniamo $g(t) = t/E(-t)$ e applichiamo la (2.23) con $m = n-1$ e $k = -1$, otteniamo che

$$(-1)^n e_n^* \;=\; \frac{-1}{n-1}[\![g(t)^{-n+1}]\!]_1 \;=\; \frac{-1}{n-1}[\![E(-t)^{n-1}]\!]_n.$$

Scrivendo $E(-t)$ come $1 + E^+(-t)$, abbiamo

$$E(-t)^{n-1} \;=\; \sum_i \binom{n-1}{i}E^+(-t)^i,$$

e quindi

$$\begin{aligned} e_n^* = \;& \frac{(-1)^{n+1}}{n-1}\sum_{|\lambda|=n}\binom{n-1}{\ell(\lambda)}(-1)^n u_\lambda e_\lambda \\ =\; & -\frac{1}{n-1}\sum_{|\lambda|=n}\binom{n-1}{\ell(\lambda)}u_\lambda e_\lambda. \end{aligned}$$

È anche possibile ottenere un'espressione per i $p_n^*$ nel seguente modo. Siccome $t = uH^*(u)$, abbiamo grazie alla (2.8) che

$$\log t \;=\; \log u + \sum_{i\geq 1}\frac{p_i^*}{i}u^i,$$

e quindi

$$\frac{\mathrm{d}t}{t} \;=\; \frac{\mathrm{d}u}{u} + \sum_{i\geq 1}p_i^* u^{i-1}\mathrm{d}u.$$

Segue che per $n \geq 1$, $p_n$ è il residuo del differenziale $\mathrm{d}t/tu^n$, e quindi il coefficiente del termine di grado $n$ in

$$\frac{t^n}{u^n} \;=\; H(t)^{-n} \;=\; \exp\Big(-n\sum_{i\geq 1}\frac{p_i}{i}t^i\Big).$$

Espandendo abbiamo che

$$\begin{aligned} p_n^* &= \sum_{|\lambda|=n} u_\lambda \frac{(-n)^{\ell(\lambda)} p_\lambda}{\ell(\lambda)! \cdot \prod_{i=1}^{\ell(\lambda)} \lambda_i} \\ &= \sum_{|\lambda|=n} (-n)^{\ell(\lambda)} z_\lambda^{-1} p_\lambda. \end{aligned}$$

# Capitolo 3

# Funzioni di Schur e ortogonalità

> If I have ever made any valuable discoveries, it has been owing more to patient attention, than to any other talent.
>
> *Isaac Newton*

In questo capitolo introduciamo una nuova base dell'anello delle funzioni simmetriche, le funzioni di Schur, e un prodotto scalare $\mathbb{Z}$-lineare rispetto al quale esse sono una base ortonormale.

Questa costruzione permetterà successivamente di ricalcare la struttura delle rappresentazioni del gruppo simmetrico, giustificando lo studio della combinatoria relativa a tale base in termini di tableau e diagrammi delle partizioni.

## 3.1 Le funzioni di Schur

Supponiamo inizialmente che il numero di variabili sia finito, $x_1, \dots, x_n$ poniamo. Sia $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ un monomio, e consideriamo il polinomio $a_\alpha$ ottenuto antisimmetrizzando $x^\alpha$, cioè

$$a_\alpha \;=\; a_\alpha(x_1, \dots, x_n) \;=\; \sum_{w \in S_n} \varepsilon(w) \cdot w(x^\alpha), \tag{3.1}$$

dove $\varepsilon(w)$ è il *segno* ($\pm 1$) della permutazione $w$, e $w(x^\alpha) = x_{w(1)}^{\alpha_1} \dots x_{w(n)}^{\alpha_n}$ è il monomio ottenuto applicando $w$ alle variabili di $x^\alpha$. Questo polinomio $a_\alpha$ è antisimmetrico, ovvero

$$w(a_\alpha) \;=\; \varepsilon(w) a_\alpha \qquad \text{per ogni } w \in S_n.$$

In particolare $a_\alpha$ si annulla se gli $\alpha_1, \dots, \alpha_n$ non sono tutti distinti. Ci possiamo allora restringere al caso in cui $\alpha_1 > \alpha_2 > \dots > \alpha_n \geq 0$ (a patto

cambiare eventualmente il segno di $a_\alpha$ riordinando la tupla $(\alpha_1, \ldots, \alpha_n)$), e scriviamo quindi $\alpha$ come $\alpha = \lambda + \delta$, dove $\lambda$ è una partizione di lunghezza $\leq n$ e $\delta = (n-1, n-2, \ldots, 1, 0)$. Allora

$$a_\alpha \;=\; a_{\lambda+\delta} \;=\; \sum_w \varepsilon(w) \cdot w(x^{\lambda+\delta}),$$

che possiamo anche scrivere come determinante:

$$a_{\lambda+\delta} \;=\; \det(x_i^{\lambda_j+n-j})_{1\leq i,j\leq n}.$$

Questo determinante è divisibile in $\mathbb{Z}[x_1, \ldots, x_n]$ per ciascuna delle differenze $x_i - x_j$ (per $1 \leq i < j \leq n$), e quindi per il loro prodotto che è il *determinante di Vandermonde*

$$\prod_{1\leq i<j\leq n} (x_i - x_j) \;=\; \det(x_i^{n-j})_{1\leq i,j\leq n} = a_\delta.$$

Quindi $a_{\lambda+\delta}$ è divisibile per $a_\delta$ in $\mathbb{Z}[x_1, \ldots, x_n]$, e il quoziente

$$s_\lambda \;=\; s_\lambda(x_1, \ldots, x_n) \;=\; a_{\lambda+\delta}/a_\delta \tag{3.2}$$

è *simmetrico*, cioè un elemento di $\Lambda_n$. Esso è detto *funzione di Schur* nelle variabili $x_1, \ldots, x_n$ corrispondente alla partizione $\lambda$ (dove $\ell(\lambda) \leq n$), ed è omogeneo di grado $|\lambda|$.

Si noti che la definizione (3.2) ha senso per qualunque vettore intero $\lambda \in \mathbb{Z}^n$ tale che $\lambda + \delta$ non ha componenti negative. Se i numeri $\lambda_i + n - i$, per $i = 1, \ldots, n$, non sono tutti distinti allora $s_\lambda = 0$. Se invece sono tutti distinti, allora $\lambda + \delta = w(\mu + \delta)$ per qualche partizione $\mu$ e permutazione $w \in S_n$, e in tal caso $s_\lambda = \varepsilon(w) s_\mu$.

I polinomi $a_{\lambda+\delta}$, al variare di $\lambda$ fra tutte le partizioni di lunghezza $\leq n$, formano una base dello $\mathbb{Z}$-modulo $A_n$ dei polinomi antisimmetrici nelle variabili $x_1, \ldots, x_n$. La moltiplicazione per $a_\delta$ è un isomorfismo fra gli $\mathbb{Z}$-moduli $\Lambda_n$ e $A_n$ ($A_n$ è anche il $\Lambda_n$-modulo libero generato da $a_\delta$), e quindi:

**Proposizione 3.1.1.** *Le funzioni di Schur $s_\lambda(x_1, \ldots, x_n)$, al variare di $\lambda$ fra le partizioni di lunghezza $\leq n$, formano una base di $\Lambda_n$ come $\mathbb{Z}$-modulo.*

Analizziamo ora cosa succede aumentando il numero di variabili. Se $\ell(\lambda) \leq n$ e, come al solito, $\delta_m = (m-1, m-2, \ldots, 1, 0)$, tenendo conto della definizione di $a_\alpha(x_1, \ldots, x_k)$ come determinante di una matrice di ordine $k$, è chiaro che

$$\begin{aligned} s_\lambda(x_1, \ldots, x_n) &= \frac{a_{\lambda+\delta_n}(x_1, \ldots, x_n)}{a_{\delta_n}(x_1, \ldots, x_n)} \\ &= \frac{a_{\lambda+\delta_{n+1}}(x_1, \ldots, x_n)}{a_{\delta_{n+1}}(x_1, \ldots, x_n)} \\ &= \frac{a_{\lambda+\delta_{n+1}}(x_1, \ldots, x_n, 0)}{a_{\delta_{n+1}}(x_1, \ldots, x_n, 0)} \\ &= s_\lambda(x_1, \ldots, x_n, 0). \end{aligned}$$

Ne segue che per ogni partizione $\lambda$, i polinomi $s_\lambda(x_1,\dots,x_n)$, per $n \to \infty$, definiscono nel limite inverso un unico elemento $s_\lambda \in \Lambda$, che è omogeneo di grado $|\lambda|$. Dalla proposizione 3.1.1 segue anche immediatamente che

**Proposizione 3.1.2.** *Gli $s_\lambda$ formano una $\mathbb{Z}$-base di $\Lambda$, e per ogni $k \geq 0$ gli $s_\lambda$ per tutti i $|\lambda| = k$ formano una $\mathbb{Z}$-base di $\Lambda^k$.*

Cercheremo ora delle formule che permettano di esprimere gli $s_\lambda$ come polinomi nelle funzioni simmetriche elementari $e_r$, e come polinomi nelle funzioni simmetriche complete $h_r$: le proposizioni 2.2.2 e 2.3.2 garantiscono infatti che una tale scrittura esiste ed è unica. Le formule sono:

$$s_\lambda = \det(h_{\lambda_i - i+j})_{1\leq i,j\leq n} \qquad \text{per } n \geq \ell(\lambda), \text{ e} \tag{3.3}$$

$$s_\lambda = \det(e_{\lambda'_i - i+j})_{1\leq i,j\leq m} \qquad \text{per } m \geq \ell(\lambda'). \tag{3.4}$$

Esse sono note come formule di Jacobi-Trudi. Grazie alla (2.7), è sufficiente dimostrare una di queste due formule, la (3.3) poniamo. Lavorando con $n$ variabili $x_1,\dots,x_n$, sia $e_r^{(k)}$ per $k = 1,2,\dots,n$ la $r$-esima funzione simmetrica elementare nelle variabili $x_1,\dots,x_{k-1},x_{k+1},\dots,x_n$ (rimuovendo $x_k$), e sia $M$ la matrice $n \times n$ definita come

$$M = \big((-1)^{n-i} e_{n-i}^{(k)}\big)_{1\leq i,k\leq n}.$$

La (3.3) sarà una conseguenza della seguente:

**Proposizione 3.1.3.** *Per qualunque $\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{N}^n$, consideriamo le matrici $n \times n$ definite da*

$$A_\alpha = (x_j^{\alpha_i})_{1\leq i,j\leq n}, \qquad H_\alpha = (h_{\alpha_i - n+j})_{1\leq i,j\leq n}.$$

*Allora $A_\alpha = H_\alpha M$.*

*Dimostrazione.* Sia

$$E^{(k)}(t) = \sum_{r=0}^{n-1} e_r^{(k)} t^r = \prod_{\substack{1\leq i\leq n \\ i\neq k}} (1 + x_i t).$$

Allora

$$H(t)E^{(k)}(-t) = (1 - x_k t)^{-1}.$$

Uguagliando i coefficienti di $t^{\alpha_i}$ in entrambi i membri, abbiamo che

$$\sum_{j=1}^{n} h_{\alpha_i - n+j} \cdot (-1)^{n-j} e_{n-j}^{(k)} = x_k^{\alpha_i},$$

che, espandendo il prodotto $H_\alpha M$, ci dice precisamente che $H_\alpha M = A_\alpha$. □

Se ora passiamo ai determinanti nella proposizione 3.1.3, otteniamo che per qualunque $\alpha \in \mathbb{N}^n$

$$a_\alpha \;=\; \det(A_\alpha) \;=\; \det(H_\alpha)\det(M),$$

e in particolare $\det M = a_\delta$, visto che $\det(H_\delta) = 1$. Quindi

$$a_\alpha \;=\; a_\delta \det(H_\alpha), \tag{3.5}$$

che possiamo anche scrivere come

$$a_\alpha \;=\; a_\delta \sum_{w\in S_n} \varepsilon(w) h_{\alpha - w\delta}. \tag{3.5'}$$

Se prendiamo $\alpha = \lambda + \delta$, dalla (3.5) segue immediatamente la (3.3), e dalla (3.5') segue che

$$s_\lambda \;=\; \sum_{w\in S_n} \varepsilon(w) h_{\lambda+\delta-w\delta}. \tag{3.3'}$$

Le (3.3) e (3.4) ci fanno capire come si comportano gli $s_\lambda$ tramite l'involuzione $\omega$, ovvero che

$$\omega(s_\lambda) \;=\; s_{\lambda'}, \qquad \text{per ogni partizione } \lambda.$$

Sempre dalle (3.3) e (3.4) otteniamo le formule per i casi particolari:

$$s_{(n)} \;=\; h_n, \qquad s_{(1^n)} \;=\; e_n. \tag{3.6}$$

Infine, le (3.3) e (3.3'), che esprimono $s_\lambda$ come polinomio negli $h_r$, si possono anche esprimere in termini degli operatori di raising:

$$s_\lambda \;=\; \prod_{i<j}(1 - R_{ij}) h_\lambda, \tag{3.3"}$$

dove, dato un operatore di raising $R$, per $Rh_\lambda$ intendiamo $h_{R\lambda}$.[1]

*Dimostrazione.* Nell'anello $\mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, abbiamo

$$\begin{aligned}
\sum_{w\in S_n} \varepsilon(w) x^{\lambda+\delta-w\delta} \;&=\; x^{\lambda+\delta} a_{-\delta} \;=\; x^{\lambda+\delta} \prod_{1\le i<j\le n} (x_i^{-1} - x_j^{-1}) \\
&= \prod_{1\le i<j\le n} (1 - x_i x_j^{-1}) \cdot x^\lambda \\
&= \prod_{1\le i<j\le n} (1 - R_{ij}) x^\lambda,
\end{aligned}$$

[1] Si noti che dati due operatori di raising $R$ e $R'$, $RR'h_\lambda = h_{RR'\lambda}$ non è necessariamente uguale a $R(R'h_\lambda)$, perché infatti $R'\lambda$ potrebbe avere delle componenti negative, ma $RR'\lambda$ no, nel qual caso $R'h_\lambda = 0$ ma $RR'h_\lambda \neq 0$.

dove $R(x^\lambda) = x^{R\lambda}$ per qualunque operatore di raising $R$. Se ora applichiamo la mappa $\mathbb{Z}$-lineare $\varphi : \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] \to \Lambda_n$, definita da $\varphi(x_r) = h_r$ (e quindi $\varphi(x^\alpha) = h_\alpha$ per ogni $\alpha \in \mathbb{Z}^n$, sempre con la convenzione di porre $h_r = 0$ se $r < 0$), abbiamo che

$$\sum_{w \in S_n} \varepsilon(w) h_{\lambda+\delta-w\delta} \;=\; \prod_{i<j} (1 - R_{ij}) h_\lambda,$$

da cui la (3.3") grazie alla (3.3'). □

### 3.1.4 Relazioni con le somme di potenze

In questa sezione diamo una caratterizzazione combinatoria della scrittura del prodotto $s_\mu p_\rho$ in termini dei $s_\lambda$, tratteremo più avanti il viceversa (che dedurremo facilmente dopo aver introdotto un prodotto scalare su $\Lambda$ come $\mathbb{Z}$-modulo), e vedremo in particolare come entrano in gioco caratteri del gruppo simmetrico.

Sia $\mu = (\mu_1, \ldots, \mu_n)$ una partizione di lunghezza $\leq n$, dove $n$ è il numero di variabili $x_1, \ldots, x_n$, e $r$ un intero positivo. Allora abbiamo che

$$a_{\mu+\delta} p_r \;=\; \sum_{q=1}^{n} a_{\mu+\delta+r\varepsilon_q}, \tag{3.7}$$

dove $\varepsilon_q$ è la $n$-tupla con 1 nella $q$-esima componente e 0 altrove. Riarrangiamo la tupla $\mu + \delta + r\varepsilon_q$ in ordine discendente: se ha due termini uguali, allora non contribisce alla (3.7). Restringendoci quindi ai termini non nulli della somma, possiamo assumere per qualche indice $p \leq q$ di avere che

$$\mu_{p-1} + n - (p-1) \;>\; \mu_q + n - q + r > \mu_p + n - p,$$

e in questo caso $a_{\mu+\delta+r\varepsilon_q} = (-1)^{q-p} a_{\lambda+\delta}$, dove $\lambda$ è la partizione

$$\lambda \;=\; (\mu_1, \ldots, \mu_{p-1}, \mu_q + p - q + r, \mu_p + 1, \ldots, \mu_{q-1} + 1, \mu_{q+1}, \ldots, \mu_n),$$

e quindi $\vartheta = \lambda - \mu$ è una striscia di bordo di lunghezza $r$ (si confronti quanto detto all'inizio della sezione 1.7, in particolare che sottraendo $r$ da una parte di $\lambda + \delta$ e riarrangiando, se si ottiene una partizione stretta $\mu + \delta$ allora $\lambda/\mu$ è una striscia di bordo lunga $r$).

Richiamando la definizione data in 1.3 dell'*altezza* $ht(\vartheta)$ di una striscia di bordo, che è il numero di righe occupate dalla striscia meno uno, osserviamo che l'intero $q - p$ che determina il cambio di segno è precisamente l'altezza di $\vartheta$ (che è anche il numero di parti 'scavalcate' dalla parte di $\lambda + \delta$ da cui abbiamo sottratto $r$).

Il discorso appena fatto mostra che

$$s_\mu p_r \;=\; \sum_{\lambda} (-1)^{ht(\lambda/\mu)} s_\lambda,$$

dove la somma è su tutte le partizioni $\lambda \supset \mu$ tali che $\lambda/\mu$ è una striscia di bordo di lunghezza $r$. Da questa uguaglianza segue che date partizioni $\lambda, \mu, \rho$ tali che $|\lambda| = |\mu| + |\rho|$, il coefficiente di $s_\lambda$ in $s_\mu p_\rho$ è

$$\chi_\rho^{\lambda/\mu} \;=\; \sum_S (-1)^{ht(S)} \tag{3.8}$$

dove la somma è su tutte le successioni di partizioni $S = (\lambda^{(0)}, \lambda^{(1)}, \dots, \lambda^{(m)})$ tali che $\mu = \lambda^{(0)} \subset \lambda^{(1)} \subset \cdots \subset \lambda^{(m)} = \lambda$, e in cui ciascun $\lambda^{(i)}/\lambda^{(i-1)}$ è una striscia di bordo di lunghezza $\rho_i$, e dove $ht(S)$ è definita come

$$ht(S) \;=\; \sum_i ht(\lambda^{(i)}/\lambda^{(i-1)}).$$

È interessante osservare che $\rho$ non deve essere necessariamente una partizione, ma è sufficiente che sia una qualunque tupla di interi. Questo ci dice che nel valutare $\chi_\rho^{\lambda/\mu}$ possiamo considerare le decomposizioni di $\lambda/\mu$ in striscie di bordo fissando un arbitrario ordine delle lunghezze $\rho_i$.

## 3.2 Ortogonalità

Siano $x = (x_1, x_2, \dots)$ e $y = (y_1, y_2, \dots)$ due successioni finite o infinite di variabili indipendenti. Denoteremo le funzioni simmetriche degli $x$ con $m_\lambda(x)$, $s_\lambda(x)$, $p_\lambda(x)$, etc, e le funzioni simmetriche degli $y$ con $m_\lambda(y)$, $s_\lambda(y)$, $p_\lambda(y)$, etc.

Diamo ora tre differenti espansioni in serie per il prodotto

$$\prod_{i,j} (1 - x_i y_j)^{-1}.$$

La prima di queste è

$$\prod_{i,j} (1 - x_i y_j)^{-1} \;=\; \sum_\lambda z_\lambda^{-1} p_\lambda(x) p_\lambda(y), \tag{3.9}$$

sommando su tutte le partizioni $\lambda$.

Essa segue immediatamente dalla (2.10) applicata all'insieme di variabili $x_i y_j$ ponendo $t = 1$, e dalla semplice osservazione che, se $(xy)$ è l'insieme dei prodotti $x_i y_j$,

$$p_r(xy) \;=\; \sum_{i,j} (x_i y_j)^r \;=\; \Big(\sum_i x_i^r\Big) \cdot \Big(\sum_i y_i^r\Big) \;=\; p_r(x) p_r(y).$$

Successivamente, abbiamo

$$\prod_{i,j} (1 - x_i y_j)^{-1} \;=\; \sum_\lambda h_\lambda(x) m_\lambda(y) \;=\; \sum_\lambda m_\lambda(x) h_\lambda(y), \tag{3.10}$$

sommando su tutte le partizioni $\lambda$.

*Dimostrazione.* Infatti

$$\begin{aligned}\prod_{i,j}(1-x_iy_j)^{-1} &= \prod_j H(y_j)\\ &= \prod_j \sum_{r=0}^{\infty} h_r(x)y_j^r\\ &= \sum_\alpha h_\alpha(x)y^\alpha \qquad (3.10")\\ &= \sum_\lambda h_\lambda(x)m_\lambda(y),\end{aligned}$$

dove $\alpha$ varia fra le successioni $(\alpha_1, \alpha_2, \dots)$ di interi non negativi tutti nulli tranne al più una quantità finita, e $\lambda$ fra tutte le partizioni. □

La terza identità è:

$$\prod_{i,j}(1-x_iy_j)^{-1} \;=\; \sum_\lambda s_\lambda(x)s_\lambda(y), \qquad (3.11)$$

sommando su tutte le partizioni $\lambda$.

*Dimostrazione.* Essa è conseguenza della (3.10) e della scrittura degli $s_\lambda$ in termini degli $h_\lambda$ data dalla (3.5'). Supponiamo di avere una quantità finita di variabili $x = (x_1, \dots, x_n)$ e $y = (y_1, \dots, y_n)$, e sia $\delta = (n-1, n-2, \dots, 1, 0)$. Allora dalla (3.10") abbiamo:

$$\begin{aligned}a_\delta(x)a_\delta(y)\prod_{i,j=1}^{n}(1-x_iy_j)^{-1} &= a_\delta(x)\sum_{\substack{\alpha\in\mathbb{N}^n\\ w\in S_n}} h_\alpha(x)\varepsilon(w)y^{\alpha+w\delta}\\ &= a_\delta(x)\sum_{\substack{\beta\in\mathbb{N}^n\\ w\in S_n}} \varepsilon(w)h_{\beta-w\delta}(x)y^\beta\\ &= \sum_{\beta\in\mathbb{N}^n}\Big(a_\delta(x)\sum_{w\in S_n}\varepsilon(w)h_{\beta-w\delta}(x)\Big)y^\beta\\ &= \sum_{\beta\in\mathbb{N}^n} a_\beta(x)y^\beta\end{aligned}$$

per la (3.5'). Siccome $a_{w\beta} = \varepsilon(w)a_\beta$, il coefficiente di $y^\beta$ differisce da quello di $y^{w\beta}$ per il segno $\varepsilon(w)$ di $w$, e quindi l'ultima somma è uguale a $\sum a_\gamma(x)a_\gamma(y)$ sommando sulle $n$-tuple $\gamma_1 > \gamma_2 > \cdots > \gamma_n \geq 0$, ovvero a

$$\sum_\lambda a_{\lambda+\delta}(x)a_{\lambda+\delta}(y) \;=\; a_\delta(x)a_\delta(y)\sum_\lambda s_\lambda(x)s_\lambda(y),$$

sommando sulle partizioni $\lambda$ di lunghezza $\leq n$. Questo dimostra la (3.11) con $n$ variabili $x_1, \dots, x_n$ e $n$ variabili $y_1, \dots, y_n$, ora è sufficiente mandare $n \to \infty$. □

Definiamo ora un prodotto scalare su $\Lambda$, ovvero una forma bilineare $\langle u, v\rangle$ a valori in $\mathbb{Z}$, imponendo che le basi $h_\lambda$ e $m_\lambda$ siano reciprocamente duali:

$$\langle h_\lambda, m_\mu\rangle = \delta_{\lambda\mu} \tag{3.12}$$

per tutte le partizioni $\lambda$ e $\mu$, e dove $\delta_{\lambda\mu}$ è la delta di Kronecker. Vedremo a posteriori che questa forma bilineare è simmetrica e definita positiva.

**Proposizione 3.2.1.** *Siano $(u_\lambda)$, $(v_\lambda)$ delle $\mathbb{Q}$-basi di $\Lambda_\mathbb{Q}$, tali che per ogni $n \geq 0$ gli elementi indicizzati dalle partizioni di $n$ sono $\mathbb{Q}$-basi di $\Lambda^n_\mathbb{Q}$ . Allora sono fatti equivalenti:*

1. *$\langle u_\lambda, v_\mu\rangle = \delta_{\lambda\mu}$ per tutti i $\lambda, \mu$;*
2. *$\sum_\lambda u_\lambda(x)v_\lambda(y) = \prod_{i,j}(1 - x_i y_j)^{-1}$.*

*Dimostrazione.* Scriviamo gli $u_\lambda$ e $v_\mu$ come

$$u_\lambda = \sum_\rho a_{\lambda\rho} h_\rho, \qquad v_\mu = \sum_\sigma b_{\mu\sigma} m_\sigma.$$

Allora

$$\langle u_\lambda, v_\mu\rangle = \sum_\rho a_{\lambda\rho} b_{\mu\rho},$$

e il punto 1 è equivalente a

$$\sum_\rho a_{\lambda\rho} b_{\mu\rho} = \delta_{\lambda\mu}. \tag{1'}$$

Ma d'altra parte il punto 2 è equivalente all'identità

$$\sum_\lambda u_\lambda(x)v_\lambda(y) = \sum_\rho h_\rho(x) m_\rho(y)$$

per la (3.10), e quindi equivalente alla

$$\sum_\lambda a_{\lambda\rho} b_{\lambda\sigma} = \delta_{\rho\sigma}. \tag{2'}$$

Ma le (1') e (2') sono equivalenti (perché se $A$ e $B$ sono due matrici, $AB = 1$ se e solo se $BA = 1$), e quindi anche le condizioni enunciate in 1 e 2 sono equivalenti. □

Dalla proposizione e dall'identità (3.9) segue che

$$\langle p_\lambda, p_\mu\rangle = \delta_{\lambda\mu} z_\lambda \tag{3.13}$$

e quindi i $p_\lambda$ formano una base *ortogonale* di $\Lambda_\mathbb{Q}$. Allo stesso modo grazie all'identità (3.11), abbiamo che

$$\langle s_\lambda, s_\mu\rangle = \delta_{\lambda\mu}, \tag{3.14}$$

e quindi gli $s_\lambda$ formano una base *ortonormale* di $\Lambda$, e gli $s_\lambda$ per $|\lambda| = n$ sono una base ortonormale di $\Lambda^n$.

Qualunque altra base ortonormale di $\Lambda^n$ deve quindi ottenersi dalla base $(s_\lambda)$ tramite una trasformazione definita da una matrice ortogonale intera. Ma le uniche tali matrici sono le matrici di permutazione con segno, e quindi la (3.14) caratterizza univocamente gli $s_\lambda$ a meno di ordine e segno.

Sempre dalla (3.13) o dalla (3.14) possiamo osservare che

**Proposizione 3.2.2.** *La forma bilineare $\langle u, v\rangle$ è simmetrica e definita positiva.*

**Proposizione 3.2.3.** *L'involuzione $\omega$ è un'isometria, cioè $\langle \omega u, \omega v\rangle = \langle u, v\rangle$.*

*Dimostrazione.* Infatti basta usare il fatto che $\omega(p_\lambda) = \varepsilon_\lambda p_\lambda = \pm p_\lambda$, e che i $p_\lambda$ sono una $\mathbb{Q}$-base di $\Lambda_{\mathbb{Q}}$ ortogonale rispetto a $\langle \cdot, \cdot\rangle$. □

**Nota.** *Applicando l'involuzione $\omega$ alle funzioni simmetriche nelle variabili $x$, otteniamo dalle* (3.9)*,* (3.10) *e* (3.11) *tre espansioni in serie per il prodotto*

$$\prod_{i,j}(1 + x_i y_j) = \prod_j E(y_j)$$

*(infatti applicando $\omega$ ai coefficienti di $H(t)$ otteniamo $E(t)$), e precisamente:*

$$\prod_{i,j}(1 + x_i y_j) = \sum_\lambda \varepsilon_\lambda z_\lambda^{-1} p_\lambda(x) p_\lambda(y) \tag{3.9'}$$

$$= \sum_\lambda e_\lambda(x) m_\lambda(y) = \sum_\lambda m_\lambda(x) e_\lambda(y) \tag{3.10'}$$

$$= \sum_\lambda s_{\lambda'}(x) s_\lambda(y) = \sum_\lambda s_\lambda(x) s_{\lambda'}(y), \tag{3.11'}$$

*dove abbiamo scritto anche le espansioni che si ottengono analogamente applicando $\omega$ alle variabili $y$.*

## 3.3 Le funzioni di Schur *skew*

Ogni funzione simmetrica $f \in \Lambda$ è univocamente determinata dei suoi prodotti scalari con gli $s_\lambda$, per l'esattezza

$$f = \sum_\lambda \langle f, s_\lambda\rangle s_\lambda,$$

visto che gli $s_\lambda$ formano una base ortonormale di $\Lambda$. Siano ora $\lambda$ e $\mu$ partizioni, definiamo le funzioni simmetriche $s_{\lambda/\mu}$ imponendo che siano verificate le relazioni

$$\langle s_{\lambda/\mu}, s_\nu\rangle = \langle s_\lambda, s_\mu s_\nu\rangle \tag{3.15}$$

per tutte le partizioni $\nu$. Gli $s_{\lambda/\mu}$ sono detti *funzioni di Schur skew*. Equivalentemente, se gli interi $c^\lambda_{\mu\nu}$ sono definiti da

$$s_\mu s_\nu = \sum_\lambda c^\lambda_{\mu\nu} s_\lambda, \tag{3.16}$$

allora abbiamo che

$$s_{\lambda/\mu} = \sum_\lambda c^\lambda_{\mu\nu} s_\nu. \tag{3.17}$$

È in particolare chiaro che $s_{\lambda/0} = s_\lambda$, dove 0 è la partizione zero. Inoltre $c^\lambda_{\mu\nu} = 0$ se $\lambda$, $\mu$ e $\nu$ non soddisfano $|\lambda| = |\mu| + |\nu|$, e quindi $s_{\lambda/\mu}$ è omogeneo di grado $|\lambda| - |\mu|$, e può essere diverso da zero solo se $|\lambda| \geq |\mu|$ (anzi vedremo ora che perché $s_{\lambda/\mu}$ non sia nullo è necessario che $\lambda \supseteq \mu$).

Siano ora $x = (x_1, x_2, \dots)$ e $y = (y_1, y_2, \dots)$ due insiemi di variabili. Allora

$$\begin{aligned} \sum_\lambda s_{\lambda/\mu}(x) s_\lambda(y) &= \sum_{\lambda,\nu} c^\lambda_{\mu\nu} s_\nu(x) s_\lambda(y) \\ &= \sum_\nu s_\nu(x) s_\mu(y) s_\nu(y) \end{aligned} \tag{3.18}$$

per le (3.16) e (3.17), e quindi

$$\sum_\lambda s_{\lambda/\mu}(x) s_\lambda(y) \;=\; s_\mu(y) \sum_\nu h_\nu(x) m_\nu(y)$$

per le espansioni date dalle (3.10) e (3.11). Supponiamo ora che $y = (y_1, \dots, y_n)$, in modo da restringere la somma ai $\lambda$ e $\nu$ di lunghezza $\leq n$. Allora, ponendo come al solito $\delta = (n-1, n-2, \dots, 1, 0)$, l'equazione precedente si può riscrivere nella forma

$$\begin{aligned} \sum_\lambda s_{\lambda/\mu}(x) a_{\lambda+\delta}(y) &= \sum_\nu h_\nu(x) m_\nu(y) a_{\mu+\delta}(y) \\ &= \sum_{\alpha \in \mathbb{N}^n} h_\alpha(x) \sum_{w \in S_n} \varepsilon(w) y^{\alpha + w(\mu+\delta)} \\ &= \sum_{\beta \in \mathbb{N}^n} \sum_{w \in S_n} h_{\beta - w(\mu+\delta)}(x) \varepsilon(w) y^\beta. \end{aligned}$$

Quindi $s_{\lambda/\mu}(x)$ è uguale al coefficiente di $y^{\lambda+\delta}$ nella somma, e abbiamo che

$$s_{\lambda/\mu} \;=\; \sum_{w \in S_n} \varepsilon(w) h_{\lambda+\delta-w(\mu+\delta)},$$

con la solita convenzione di porre $h_\alpha = 0$ se $\alpha = (\alpha_1, \dots, \alpha_n)$ ha una qualche componente negativa. Questa formula si può anche scrivere come determinante

$$s_{\lambda/\mu} \;=\; \det(h_{\lambda_i - \mu_j - i + j})_{1 \leq i,j \leq n}, \qquad \text{per } n \geq \ell(\lambda). \tag{3.19}$$

Quando $\mu = 0$, la (3.19) diventa la (3.3) per gli $s_\lambda$ che già conosciamo. Grazie all'identità (2.6), otteniamo la scrittura in termini degli $e_r$

$$s_{\lambda/\mu} \;=\; \det(e_{\lambda'_i-\mu'_j-i+j})_{1\le i,j\le m}, \qquad \text{per } m \ge \ell(\lambda'), \tag{3.20}$$

da cui segue immediatamente che

$$\omega(s_{\lambda/\mu}) = s_{\lambda'/\mu'}.$$

Dalla (3.19) segue anche che $s_{\lambda/\mu} = 0$ se $\lambda \not\supseteq \mu$: supponiamo infatti che $\lambda_r < \mu_r$ per qualche $r$, e consideriamo la matrice che compare nella (3.19). Allora per tutti gli $(i, j)$ tali che $1 \le j \le r \le i \le n$ abbiamo che

$$\lambda_i - \mu_j - i + j \;\le\; \lambda_r - \mu_r - r + r \;=\; \lambda_r - \mu_r \;<\; 0.$$

Conseguentemente la matrice $(h_{\lambda_i-\mu_j-i+j})$ ha un blocco $(n-r+1)\times r$ di zeri nell'angolo in basso a sinistra, e ha quindi determinante zero. Lo stesso argomento permette di dedurre che se $\lambda \supseteq \mu$ e $\mu_r \ge \lambda_{r+1}$, la matrice $(h_{\lambda_i-\mu_j-i+j})$ è della forma $\left(\begin{smallmatrix} A & C \\ 0 & B \end{smallmatrix}\right)$ con $A$ e $B$ matrici quadrate di ordine $r$ e $n-r$, e dove il blocco 0 ha dimensione $(n-r)\times r$, e quindi il determinante è $\det(A)\det(B)$. Se il diagramma skew $\lambda/\mu$ è formato da due componenti disgiunte $\vartheta, \varphi$ (ciascuna delle quali è a sua volta un diagramma skew), allora $s_{\lambda/\mu} = s_\vartheta \cdot s_\varphi$.

Abbiamo dimostrato la

**Proposizione 3.3.1.** *La funzione di Schur skew $s_{\lambda/\mu}$ può essere diversa da zero solo se $\lambda \supseteq \mu$, e in tal caso dipende solo dal diagramma skew $\lambda/\mu$. Se $\vartheta_i$ sono le componenti (definite in 1.3) di $\lambda/\mu$, allora $s_{\lambda/\mu} = \prod s_{\vartheta_i}$.*

Se il numero di variabili $x_i$ è finito possiamo anche dire che

**Proposizione 3.3.2.** *In $n$ variabili $x_1, \dots, x_n$, $s_{\lambda/\mu}$ può essere diverso da 0 solo se $0 \le \lambda'_i - \mu'_i \le n$ per tutti gli $i \ge 1$.*

*Dimostrazione.* Supponiamo che esista un $r$ tale che $\lambda'_r - \mu'_r > n$. Allora, siccome $e_{n+1} = e_{n+2} = \cdots = 0$, la matrice $(e_{\lambda'_i-\mu'_j-i+j})$ risulta avere un rettangolo di zeri nell'angolo in alto a destra di dimensione $r \times (n-r+1)$, e quindi il determinante nella (3.20) si annulla. □

Siano ora $x = (x_1, x_2, \dots)$, $y = (y_1, y_2, \dots)$ e $z = (z_1, z_2, \dots)$ tre insiemi distinti di indeterminate. Allora grazie alla (3.18), e usando la (3.11), abbiamo che

$$\begin{aligned} \sum_{\lambda,\mu} s_{\lambda/\mu}(x) s_\lambda(z) s_\mu(y) &= \sum_{\nu,\mu} s_\nu(x) s_\mu(z) s_\nu(z) s_\mu(y) \\ &= \sum_\mu s_\mu(y) s_\mu(z) \cdot \prod_{i,k} (1 - x_i z_k)^{-1} \\ &= \prod_{i,k} (1 - x_i z_k)^{-1} \cdot \prod_{j,k} (1 - y_j z_k)^{-1}, \end{aligned} \tag{3.21}$$

che è quindi anche uguale a

$$\sum_{\lambda} s_\lambda(x,y)s_\lambda(z) \tag{3.22}$$

dove $s_\lambda(x,y)$ è la funzione di Schur corrispondente a $\lambda$ nell'insieme di variabili $(x,y) = (x_1, x_2, \dots, y_1, y_2, \dots)$. Uguagliando i coefficienti di $s_\lambda(z)$ nelle (3.21) e (3.22) possiamo concludere che

$$\begin{aligned} s_\lambda(x,y) &= \sum_{\mu} s_{\lambda/\mu}(x)s_\mu(y) \\ &= \sum_{\mu,\nu} c^\lambda_{\mu\nu} s_\nu(x)s_\mu(y). \end{aligned} \tag{3.23}$$

Più in generale si ottiene che

$$s_{\lambda/\mu}(x,y) = \sum_{\nu} s_{\lambda/\nu}(x)s_{\nu/\mu}(y), \tag{3.24}$$

sommando su tutte le partizioni $\nu$ tali che $\lambda \supseteq \nu \supseteq \mu$.

*Dimostrazione.* Dalla (3.23), abbiamo che

$$\begin{aligned} \sum_{\mu} s_{\lambda/\mu}(x,y)s_\mu(z) &= s_\lambda(x,y,z) \\ &= \sum_{\nu} s_{\lambda/\nu}(x)s_\nu(y,z) \\ &= \sum_{\mu,\nu} s_{\lambda/\nu}(x)s_{\nu/\mu}(y)s_\mu(z) \end{aligned}$$

usando nuovamente la (3.23). Se ora uguagliamo i coefficienti di $s_\mu(z)$, ne segue la (3.24). □

La (3.24) può essere facilmente generalizzata come segue. Siano $x^{(1)}, \dots, x^{(n)}$ $n$ diversi insiemi di variabili, e siano $\lambda$ e $\mu$ partizioni. Allora

$$s_{\lambda/\mu}(x^{(1)}, \dots, x^{(n)}) = \sum_{(\nu)} \prod_{i=1}^{n} s_{\nu^{(i)}/\nu^{(i-1)}}(x^{(i)}) \tag{3.25}$$

sommando su tutte le successioni $(\nu) = (\nu^{(0)}, \nu^{(1)}, \dots, \nu^{(n)})$ di partizioni tali che $\mu = \nu^{(0)} \subseteq \nu^{(1)} \subseteq \cdots \subseteq \nu^{(n)} = \lambda$.

Possiamo applicare la (3.25) nel caso in cui ciascuno degli insiemi di variabili $x^{(i)}$ contenga la singola variabile $x_i$. Per un singolo $x$, segue dalla proposizione 3.3.2 che $s_{\lambda/\mu}(x)$ può essere diverso da zero solo se $\lambda/\mu$ è una *striscia orizzontale*, nel qual caso $s_{\lambda/\mu}(x) = x^{|\lambda/\mu|}$. Quindi ciascuno dei prodotti nella somma al lato destro della (3.25) è un monomio $x_1^{\alpha_1} \dots x_n^{\alpha_n}$, dove $\alpha_i = |\nu^{(i)}/\nu^{(i-1)}|$, e abbiamo espresso $s_{\lambda/\mu}(x_1, \dots, x_n)$ come somma di monomi $x^\alpha$, un monomio per ciascun

*tableau* $T$ di forma $\lambda/\mu$. Il peso del tableau $T$ corrispondente alla successione $(\nu)$ è precisamente $\alpha = (\alpha_1, \ldots, \alpha_n)$, e scriviamo $x^T$ per intendere $x^\alpha$.

Allora:

$$s_{\lambda/\mu} \;=\; \sum_T x^T \tag{3.26}$$

sommando su tutti i tableau di forma $\lambda/\mu$.

Per ogni partizione $\nu$ tale che $|\nu| = |\lambda/\mu|$, indichiamo con $K_{\lambda/\mu,\nu}$ il numero di tableau di forma $\lambda/\mu$ e peso $\nu$. Dalla (3.26) abbiamo che

$$s_{\lambda/\mu} \;=\; \sum_\nu K_{\lambda/\mu,\nu} \cdot m_\nu \tag{3.27}$$

e quindi

$$K_{\lambda/\mu,\nu} \;=\; \langle s_{\lambda/\mu}, h_\nu \rangle = \langle s_\lambda, s_\mu h_\nu \rangle \tag{3.28}$$

cosicché

$$s_\mu h_\nu = \sum_\lambda K_{\lambda/\mu,\nu} \cdot s_\lambda. \tag{3.29}$$

In particolare, sia $\nu = (r)$ la partizione con un'unica parte $r$. Allora

$$K_{\lambda/\mu,(r)} \;=\; \begin{cases} 1 & \text{se } \lambda/\mu \text{ è una } r\text{-striscia orizzontale,} \\ 0 & \text{altrimenti.} \end{cases}$$

Quindi abbiamo dalla (3.29) la seguente formula (detta *formula di Pieri*):

$$s_\mu h_r = \sum_\lambda s_\lambda,$$

sommando sui $\lambda$ tali che $\lambda/\mu$ è una $r$-striscia orizzontale. Applicando l'involuzione $\omega$ abbiamo la formula duale

$$s_\mu e_r = \sum_\lambda s_\lambda,$$

sommando sui $\lambda$ tali che $\lambda/\mu$ è una $r$-striscia verticale.

## 3.4 Specializzazioni e $q$-binomiale

In questa sezione studiamo alcune specializzazioni dalle quali è possibili ottenere importanti informazioni qualitative sulle basi di funzioni simmetriche $e_\lambda, h_\lambda, s_\lambda, \ldots$ .

Sia $q$ un'indeterminata. Chiameremo $\varphi_r(q)$ il polinomio

$$\varphi_r(q) \;=\; (1-q)(1-q^2)\ldots(1-q^{r-1})(1-q^r).$$

Il *$q$-binomiale* (talvolta anche detto *binomiale gaussiano*) è definito come

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \;=\; \frac{\varphi_n(q)}{\varphi_{n-k}(q)\varphi_k(q)} \;=\; \frac{(1-q^{n-k+1})\ldots(1-q^{n-1})(1-q^n)}{(1-q)(1-q^2)\ldots(1-q^k)},$$

ed è una funzione razionale dell'indeterminata $q$.

Altri $q$-analoghi sono ad esempio il $q$-bracket e il $q$-fattoriale:

$$[n]_q \;=\; \frac{1-q^n}{1-q}, \qquad [n]_q! \;=\; \frac{(1-q)(1-q^2)\dots(1-q^n)}{(1-q)^n},$$

ed essi godono di un certo numero di proprietà interessanti, e in particolare il limite per $q \to 1$ è precisamente il corrispondente classico

$$\lim_{q\to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q \;=\; \binom{n}{k}, \quad \lim_{q\to 1}[n]_q \;=\; n, \quad \lim_{q\to 1}[n]_q! \;=\; n!.$$

Non è nostra intenzioni addentrarci nella teoria dei $q$-analoghi, ci accontenteremo di conoscere i più importanti di essi e di avere un'idea di quale sia la connessione con il loro corrispondente classico. Per un approfondimento in materia si veda ad esempio [KC02].

Una proprietà interessante del $q$ binomiale è la seguente: se poniamo $q = p^e$, per $p$ primo e $e \geq 1$, allora $\begin{bmatrix} n \\ k \end{bmatrix}_q$ è il numero di sottospazi vettoriali di dimensione $k$ di uno spazio vettoriale di dimensione $n$ su $\mathbb{F}_q$.

È inoltre facile verificare che valgono le seguenti identità, sempre in stretta analogia con le corrispondenti identità classiche

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \;=\; q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q, \tag{3.30}$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \;=\; \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q. \tag{3.30'}$$

Di fatto queste identità equivalgono a una definizione per ricorrenza, e mostrano immediatamente che il $q$-binomiale è sempre un polinomio in $q$.

Supponiamo ora nell'anello delle funzioni simmetriche $\Lambda$ di porre $x_i = q^{i-1}$ per $i = 1, 2, \dots, n$, e $x_i = 0$ per $i > n$. Abbiamo allora che

$$E(t) \;=\; \prod_{i=0}^{n-1}(1+q^i t) \;=\; \sum_{r=0}^{n} q^{r(r-1)/2} \begin{bmatrix} n \\ r \end{bmatrix}_q t^r,$$

e che

$$H(t) \;=\; \prod_{i=0}^{n-1}(1-q^i t)^{-1} \;=\; \sum_{r=0}^{n} \begin{bmatrix} n+r-1 \\ r \end{bmatrix}_q t^r.$$

Le espansioni come somme si dimostrano per induzione su $n$ utilizzando le (3.30) e (3.30'). Abbiamo quindi che

$$e_r \;=\; q^{r(r-1)/2} \begin{bmatrix} n \\ r \end{bmatrix}_q, \qquad h_r \;=\; \begin{bmatrix} n+r-1 \\ r \end{bmatrix}_q. \tag{3.31-e,h}$$

Da questo segue che $h_r$ è anche la funzione generatrice in $q$ delle partizioni tali che $\ell(\lambda) \leq r$ e $\ell(\lambda') \leq n-1$, mentre $e_r$ è la funzione generatrice di tali

partizioni con tutte le parti distinte (questa osservazione può verificare immediatamente per induzione, scrivendo l'espressione ricorrente per il numero tali partizioni e applicando le (3.30) e (3.30')).

Per quanto riguarda gli $m_\lambda$, abbiamo che in $n$ variabili e per $\ell(\lambda) \leq n$, usando il teorema orbita-stabilizzatore

$$\begin{aligned} m_\lambda(x_1, \ldots, x_n) &= \frac{\sum_{w \in S_n} \prod x^{w(\lambda)}}{|\{w \in S_n : w(\lambda) = \lambda\}|} \\ &= \frac{\operatorname{perm}(x_i^{\lambda_j})_{1 \leq i,j \leq n}}{\prod_{i \geq 0} m_i(\lambda)!}, \end{aligned}$$

dove $\operatorname{perm}(x_i^{\lambda_j})_{1 \leq i,j \leq n}$ è il *permanente* della matrice $(x_i^{\lambda_j})_{1 \leq i,j \leq n}$, e dove per $m_0(\lambda)$ intendiamo il numero di parti zero fino a $\lambda_n$, ovvero $n - \ell(\lambda)$. Nel caso che stiamo studiando in cui abbiamo posto $x_i = q^{i-1}$ per $i = 1, \ldots, n$ abbiamo quindi

$$m_\lambda \;=\; \frac{\operatorname{perm}(q^{(i-1)\lambda_j})_{1 \leq i,j \leq n}}{\prod_{i \geq 0} m_i(\lambda)!}. \tag{3.31-m}$$

Consideriamo ora le funzioni di Schur $s_\lambda$. Se $\lambda$ è una partizione di lunghezza $\leq n$ abbiamo che

$$a_\lambda \;=\; \det(q^{(i-1)(\lambda_j + n - j)})_{1 \leq i,j \leq n},$$

che è un determinante di Vandermonde nelle variabili $q^{\lambda_j + n - j}$ per $j = 1, \ldots, n$, e quindi

$$\begin{aligned} a_\lambda &= \prod_{1 \leq i < j \leq n} (q^{\lambda_j + n - j} - q^{\lambda_i + n - i}) \\ &= q^{n(\lambda) + n(n-1)(n-2)/6} \cdot \prod_{1 \leq i < j \leq n} (1 - q^{\lambda_j - \lambda_i - i + j}). \end{aligned}$$

Grazie alla (1.5) abbiamo quindi che

$$a_\lambda \;=\; q^{n(\lambda) + n(n-1)(n-2)/6} \cdot \frac{\prod_{i=1}^{n} \varphi_{\lambda_i + n - i}(q)}{\prod_{x \in \lambda} (1 - q^{h(x)})},$$

dove $h(x)$ è la lunghezza del gancio in $x \in \lambda$, definita nella (1.4), e di conseguenza

$$a_{\lambda + \delta} / a_\delta \;=\; \frac{q^{n(\lambda)}}{\prod_{x \in \lambda} (1 - q^{h(x)})} \prod_{i=1}^{n} \frac{\varphi_{\lambda_i + n - i}(q)}{\varphi_{n-i}(q)}.$$

Dalla (1.7) segue allora che

$$s_\lambda \;=\; q^{n(\lambda)} \prod_{x \in \lambda} \frac{1 - q^{n + c(x)}}{1 - q^{h(x)}}, \tag{3.31-s}$$

dove $c(x)$ è il contenuto di $x \in \lambda$, definito nella (1.6). Questa formula è vera per ogni $\lambda$ perché se $\ell(\lambda) > n$ allora $(1 - q^{n + c(x)}) = 0$ per qualche $x \in \lambda$, e anche $s_\lambda = 0$.

Per ogni partizione $\lambda$ definiamo

$$\begin{bmatrix} n \\ \lambda \end{bmatrix}_q \;=\; \prod_{x\in\lambda} \frac{1-q^{n-c(x)}}{1-q^{h(x)}},$$

che quando $\lambda = (r)$ vale $\begin{bmatrix} n \\ r \end{bmatrix}_q$, e quindi è in accordo con la notazione per il $q$-binomiale. Abbiamo allora ottenuto che

$$s_\lambda \;=\; q^{n(\lambda)} \begin{bmatrix} n \\ \lambda' \end{bmatrix}_q . \tag{3.31-s'}$$

Questa scrittura ci dice che $\begin{bmatrix} n \\ \lambda \end{bmatrix}_q$ è un polinomio in $q$, e il suo grado è

$$d \;=\; \sum_{x\in\lambda} (n - c(x) - h(x)) \;=\; \sum_{i=1}^{n} (n+1-2i)\lambda'_i$$

grazie alle (1.8) e (1.9). Inoltre se $a_i$ è il coefficiente di $q^i$ in $\begin{bmatrix} n \\ \lambda \end{bmatrix}_q$, allora $a_i = a_{d-i}$ per $i = 0, 1, \ldots, d$, ed è possibile mostrare che $\begin{bmatrix} n \\ \lambda \end{bmatrix}_q$ è anche *unimodale*, ovvero $a_0 \le a_1 \le \cdots \le a_{\lfloor d/2 \rfloor}$ ([Mac95, Esempio 4, sez. 8, cap. 1]).

Cosideriamo ora il caso in cui come sopra $x_i = q^{i-1}$ per $i = 1, \ldots, n$, e mandiamo $n \to \infty$. Abbiamo allora che

$$\begin{aligned} E(t) \;&=\; \prod_{i=0}^{\infty} (1+q^i t) \;=\; \sum_{r=0}^{\infty} \frac{q^{r(r-1)/2}}{\varphi_r(q)} t^r, \\ H(t) \;&=\; \prod_{i=0}^{\infty} (1-q^i t)^{-1} \;=\; \sum_{r=0}^{\infty} \frac{1}{\varphi_r(q)} t^r \end{aligned}$$

(si confrontino queste formule con le (2.17) e (2.17')). Segue quindi che

$$e_r \;=\; \frac{q^{r(r-1)/2}}{\varphi_r(q)}, \qquad h_r \;=\; \frac{1}{\varphi_r(q)}. \tag{3.32-e,h}$$

Sembra complicato dire qualcosa riguardo gli $m_\lambda$, ma è però possibile esibire una scrittura concisa dei $p_r$, poiché

$$P(t) \;=\; \frac{H(t)'}{H(t)} \;=\; \sum_{i=0}^{\infty} \frac{q^i}{1-q^i t},$$

e quindi raccogliendo i coefficienti di $t^{r-1}$ otteniamo

$$p_r \;=\; \sum_{i=0}^{\infty} q^{ir} \;=\; (1-q^r)^{-1}. \tag{3.32-p}$$

Inoltre dalla (3.31-s) abbiamo che

$$s_\lambda \;=\; q^{n(\lambda)} \prod_{x\in\lambda} \frac{1}{1-q^{h(x)}} \;=\; \frac{q^{n(\lambda)}}{H_\lambda(q)}, \tag{3.32-s}$$

dove $H_\lambda(q)$ è il *polinomio delle lunghezze dei ganci*:

$$H_\lambda(q) \;=\; \prod_{x\in\lambda} (1-q^{h(x)}). \tag{3.33}$$

Poniamo ora $x_i = 1$ per $i = 1, \dots, n$ e $x_i = 0$ per $i > n$. Ponendo $q = 1$ nella (3.31-e,h) possiamo ricavare che

$$e_r \;=\; \binom{n}{r}, \qquad h_r \;=\; \binom{n+r-1}{r}, \tag{3.34-e,h}$$

che sono infatti rispettivamente uguali al numero di scelte e di scelte con ripetizioni di $r$ elementi in un insieme di $n$ elementi.

Dalla (3.31-m) otteniamo

$$m_\lambda \;=\; \frac{n!}{\prod_{i\geq 0} m_i(\lambda)!} \;=\; u_\lambda \binom{n}{\ell(\lambda)}, \tag{3.34-m}$$

dove gli $u_\lambda$ sono le cardinalità dell'orbita della tupla $\lambda = (\lambda_1, \lambda_2, \dots)$ sotto l'azione di $S_{\ell(\lambda)}$, ovvero gli stessi che avevamo definito nella (2.22).

Dalla (3.31-s) abbiamo che

$$s_\lambda \;=\; \prod_{x\in\lambda} \frac{n+c(x)}{h(x)} \;=\; \binom{n}{\lambda'}, \tag{3.34-s}$$

dove abbiamo posto

$$\binom{n}{\lambda} \;=\; \prod_{x\in\lambda} \frac{n-c(x)}{h(x)},$$

che è una generalizzazione del binomiale a cui si riduce qualora $\lambda = (r)$ per qualche $r$.

Osserviamo che porre $x_i = 1$ per $i = 1, 2, \dots, n$ equivale a porre $p_r = n$ per ogni $r$, o equivalentemente $E(t) = (1+t)^n$, e che le formule che abbiamo ottenuto per gli $e_n, h_n, m_\lambda$ e $s_\lambda$ sono polinomi in $n$. Quindi se $X$ è un'indeterminata e poniamo $p_r = X$, o equivalentemente $E(t) = (1+t)^X$, allora

$$e_r \;=\; \binom{X}{r}, \qquad h_r \;=\; \binom{X+r-1}{r}. \tag{3.35-e,h}$$

Queste formule sono corrette ponendo $X = n$ per ogni intero $n$, e quindi devono essere identicamente vere. Analogamente abbiamo che

$$m_\lambda \;=\; u_\lambda \binom{X}{\ell(\lambda)} \tag{3.35-m}$$

dove gli $u_\lambda$ sono definiti nella (2.22), e che

$$s_\lambda \;=\; \prod_{x\in\lambda} \frac{X+c(x)}{h(x)} \;=\; \binom{X}{\lambda'}, \tag{3.35-s}$$

dove per ogni partizione $\lambda$ abbiamo definito

$$\binom{X}{\lambda} \;=\; \prod_{x\in\lambda} \frac{X-c(x)}{h(x)},$$

che è una generalizzazione del polinomio binomiale coerente con il binomiale classico nel caso in cui $\lambda=(r)$ per qualche intero positivo $r$. Si verifica inoltre facilmente che

$$\binom{X}{\lambda'} \;=\; (-1)^{|\lambda|}\binom{-X}{\lambda}. \tag{3.36}$$

Un'altra specializzazione interessante si ottiene ponendo $x_i = 1/n$ per $i = 1,\dots,n$, $x_i = 0$ per $i > n$ e considerando il limite per $n\to\infty$. Dalla (3.34-e,h) abbiamo che

$$e_r \;=\; \lim_{n\to\infty} \frac{1}{n^r}\binom{n}{r} \;=\; \frac{1}{r!}, \tag{3.37-e}$$

e allo stesso modo anche $h_r = 1/r!$. Questa è quindi la specializzazione che corrisponde a porre $E(t) = H(t) = e^t$. In questo caso abbiamo $p_1 = 1$ e $p_r = 0$ per ogni altro $r > 1$, e inoltre $m_\lambda = 0$ eccetto se $\lambda = (1^r)$ per qualche $r \ge 1$ (e in questo caso ricordiamo che $m_{(1^r)} = e_r$).

Dalla (3.34-s) abbiamo inoltre che con questa specializzazione abbiamo

$$s_\lambda \;=\; \lim_{n\to\infty} \frac{1}{n^{|\lambda|}} \prod_{x\in\lambda} \frac{n+c(x)}{h(x)} \;=\; \prod_{x\in\lambda} h(x)^{-1}. \tag{3.37-s}$$

### 3.4.1 Identità fra serie e numero di tableau

Consideriamo ora l'espansione (3.11') del prodotto nella variabili $(x_1, x_2, \dots)$ e $(y_1, y_2, \dots)$, che rienunciamo:

$$\prod_{i,j}(1+x_i y_j) \;=\; \sum_\lambda s_\lambda(x) s_{\lambda'}(y).$$

Poniamo $y_i = t$ per $i = 1,\dots,n$ e $y_i = 0$ per $i > n$, e scriviamo $s_\lambda = s_\lambda(x)$. L'equazione si traduce nella

$$E(t)^n \;=\; \sum_\lambda \binom{n}{\lambda} s_\lambda t^{|\lambda|}$$

grazie alla (3.34-s), perché $s_{\lambda'}(y) = \binom{n}{\lambda} t^{|\lambda|}$.

Anche in questo caso i coefficienti di entrambi i membri sono polinomi in $n$ che assumono gli stessi valori su tutti gli $n$ interi positivi, e quindi devono

essere identicamente uguali. Di conseguenza abbiamo che se $X$ è una qualunque indeterminata

$$E(t)^X \;=\; \sum_\lambda \binom{X}{\lambda} s_\lambda t^{|\lambda|}.$$

Sostituendo $X$ con $-X$ e $t$ con $-t$ abbiamo anche che

$$H(t)^X \;=\; \sum_\lambda \binom{X}{\lambda'} s_\lambda t^{|\lambda|},$$

grazie alla (3.36).

Poniamo $y_i = q^{i-1}$ per $i = 1, \ldots, n$, e $y_i = 0$ per $i > n$. Grazie alla (3.31-s') abbiamo che

$$\prod_{i=1}^{n} E(q^{i-1}) \;=\; \sum_\lambda q^{n(\lambda')} \begin{bmatrix} n \\ \lambda \end{bmatrix}_q s_\lambda,$$

e allo stesso modo dalla (3.11) possiamo ricavare che

$$\prod_{i=1}^{n} H(q^{i-1}) \;=\; \sum_\lambda q^{n(\lambda)} \begin{bmatrix} n \\ \lambda' \end{bmatrix}_q s_\lambda.$$

In queste formule possiamo considerare il limite per $n \to \infty$, e ottenere (direttamente o usando la (3.32-s))

$$\prod_{i,j} (1 + x_i q^{j-1}) \;=\; \sum_\lambda \frac{q^{n(\lambda')}}{H_\lambda(q)} s_\lambda, \tag{3.38}$$

$$\prod_{i,j} (1 - x_i q^{j-1})^{-1} \;=\; \sum_\lambda \frac{q^{n(\lambda)}}{H_\lambda(q)} s_\lambda, \tag{3.39}$$

dove $H_\lambda(q)$ è polinomio delle lunghezze dei ganci relativo alla partizione $\lambda$, come definito nella (3.33).

Poniamo ora $y_i = t/n$ per $i = 1, 2, \ldots, n$, e $y_i = 0$ per $i > n$. Abbiamo allora, grazie alla (3.34-s), che per $n$ fissato

$$\prod_i \left(1 + \frac{x_i t}{n}\right)^n \;=\; \sum_\lambda \frac{1}{n^{|\lambda|}} \binom{n}{\lambda} s_\lambda t^{|\lambda|}.$$

Consideriamo il limite per $n \to \infty$. Abbiamo allora che

$$\prod_i \left(1 + \frac{x_i t}{n}\right)^n \;\to\; \prod_i \exp(x_i t) \;=\; \exp(e_1 t),$$

e inoltre

$$\frac{1}{n^{|\lambda|}} \binom{n}{\lambda} \;\to\; \prod_{x \in \lambda} h(x)^{-1} \;=\; h(\lambda)^{-1},$$

dove $h(\lambda)$ è il prodotto delle lunghezze dei ganci di $\lambda$. Abbiamo quindi che

$$\exp(e_1 t) \;=\; \sum_{\lambda} \frac{s_\lambda}{h(\lambda)} t^{|\lambda|},$$

e questo ci dice che

$$\frac{e_1^n}{n!} \;=\; \sum_{|\lambda|=n} \frac{s_\lambda}{h(\lambda)}.$$

Calcolando il prodotto scalare con $s_\lambda$, questa è equivalente grazie all'ortonormalità degli $s_\lambda$ alla

$$\langle e_1^n, s_\lambda \rangle \;=\; \frac{n!}{h(\lambda)}.$$

Siccome $e_1 = h_1$ abbiamo quindi che

$$K_{\lambda,(1^n)} \;=\; \langle s_\lambda, h_1^n \rangle \;=\; \frac{n!}{h(\lambda)}. \tag{3.40}$$

Essendo $K_{\lambda,(1^n)}$ anche il numero di tableau standard di forma $\lambda$, abbiamo ottenuto che il numero di tali tableau è uguale a $n!/h(\lambda)$.

# Capitolo 4

# Matrici di transizione

> The important thing in science is not so much to obtain new facts as to discover new ways of thinking about them.
>
> *Sir William Bragg*

In questo capitolo tratteremo matrici le cui righe e colonne sono indicizzate dalle partizioni di un intero positivo $n$. Supporremo per convenienza che le partizioni di $n$ siano arrangiate decrescendo secondo l'ordine lessicografico, partendo da $(n)$ per finire con $(1^n)$. Segue dalla proposizione 1.5.1 che $\lambda \geq_{\text{lex}} \mu$ se $\lambda \geq \mu$ (ma non vale il viceversa in generale), in altre parole $\geq_{\text{lex}}$ è un modo per estendere l'ordinamento naturale parziale $\geq$ ad un ordinamento totale.

Una matrice $(M_{\lambda\mu})$ indicizzata dalla partizioni di $n$ è detta *strettamente triangolare superiore* se $M_{\lambda\mu} = 0$ eccetto eventualmente se $\lambda \geq \mu$, e *strettamente unitriangolare superiore* se inoltre abbiamo che $M_{\lambda\lambda} = 1$ per ogni $\lambda$. Allo stesso modo definiamo le matrici *strettamente triangolari inferiori* e *strettamente unitriangolari inferiori*. Sia $U_n$ (risp. $U_n'$) l'insieme delle matrici strettamente unitriangolari superiori (risp. inferiori) con coefficienti interi, e indicizzate dalle partizioni di $n$.

**Proposizione 4.0.2.** *$U_n$ e $U_n'$ sono gruppi (rispetto alla moltiplicazione di matrici).*

*Dimostrazione.* Supponiamo $M, N \in U_n$. Allora $(MN)_{\lambda\mu} = \sum_\nu M_{\lambda\nu} N_{\nu\mu}$ e i termini della somma sono nulli eccetto eventualmente nel caso in cui $\nu$ soddisfi $\lambda \geq \nu \geq \mu$, e quindi la somma è nulla a meno che non si abbia $\lambda \geq \mu$. Per lo stesso motivo, $(MN)_{\lambda\lambda} = M_{\lambda\lambda} N_{\lambda\lambda} = 1$, e quindi $MN \in U_n$.

Sia ora $M \in U_n$, e consideriamo l'insieme di equazioni

$$\sum_\mu M_{\lambda\mu} x_\mu \;=\; y_\lambda.$$

Per ipotesi $y_\lambda$ dipende solo dai $x_\mu$ con $\mu \leq \lambda$. Per dimostrare che $M^{-1} \in U_n$,

consideriamo ora l'insieme di equazioni equivalenti

$$\sum_{\mu}(M^{-1})_{\lambda\mu}y_\mu \;=\; x_\lambda,$$

prendiamo un $x_\lambda$ minimale (secondo $\leq$) che per assurdo non sia una combinazione intera dagli $y_\mu$ con $\mu \leq \lambda$. Ma noi sappiamo che

$$x_\lambda \;=\; y_\lambda - \sum_{\mu<\lambda} M_{\lambda\mu}x_\mu$$

e sostituendo a ciascun $x_\mu$, $\mu \leq \lambda$, la sua scrittura in termini degli $y_\nu$, $\nu \leq \mu < \lambda$, abbiamo che $x_\lambda$ è combinazione intera degli $y_\nu$ per $\nu \leq \lambda$, e il coefficiente con cui $x_\lambda$ dipende da $y_\lambda$ è 1. Abbiamo quindi dimostrato che $M^{-1} \in U_n$. □

Chiamiamo $J$ la matrice che rappresenta l'operazione di coniugare di una partizione:

$$J_{\lambda\mu} \;=\; \begin{cases} 1 & \text{se } \lambda' = \mu, \\ 0 & \text{altrimenti.} \end{cases}$$

Si noti che $J = J^{-1}$, essendo l'operazione inversa del coniugio il coniugio stesso.

**Proposizione 4.0.3.** *$M$ è strettamente triangolare (risp. unitriangolare) superiore se e solo se $JMJ$ è strettamente triangolare (risp. unitriangolare) inferiore.*

*Dimostrazione.* Infatti se $N = JMJ$, $N_{\lambda\mu} = M_{\lambda'\mu'}$, e per la proposizione 1.5.2 $\lambda' \geq \mu'$ se e solo se $\mu \geq \lambda$, da cui la tesi. □

Se $(u_\lambda)$ e $(v_\lambda)$ sono due $\mathbb{Q}$-basi di $\Lambda^n_{\mathbb{Q}}$, ciascuna indicizzata dalle partizioni di $n$, indicheremo con $M(u,v)$ la matrice $(M_{\lambda\mu})$ dei coefficienti nella scrittura

$$u_\lambda = \sum_\mu M_{\lambda\mu}v_\mu.$$

$M(u,v)$ è detta la *matrice di transizione* dalla base $(u_\lambda)$ alla base $(v_\lambda)$, ed è una matrice non-singolare a coefficienti razionali. Le matrici di transizione godono delle seguenti proprietà, di dimostrazione immediata:

**Proposizione 4.0.4.** *Siano $(u_\lambda)$, $(v_\lambda)$ e $(w_\lambda)$ tre $\mathbb{Q}$-basi di $\Lambda^n_{\mathbb{Q}}$. Allora*

$$M(u,v)M(v,w) = \; M(u,w), \tag{4.1a}$$

$$M(u,v) = \; M(v,u)^{-1}. \tag{4.1b}$$

*Se $(u'_\lambda)$, $(v'_\lambda)$ sono le basi duali di $(u_\lambda)$, $(v_\lambda)$ rispettivamente (rispetto al prodotto scalare (3.12)). Allora*

$$M(u',v') \;=\; M(v,u)^t \;=\; M(u,v)^*, \tag{4.1c}$$

*dove $M^t$ è la trasposta, e $M^*$ l'inversa della trasposta della matrice $M$. Inoltre*

$$M(\omega u, \omega v) \;=\; M(u,v), \tag{4.1d}$$

*dove $\omega : \Lambda \to \Lambda$ è l'involuzione della (2.5).*

Consideriamo ora le cinque $\mathbb{Z}$-basi di $\Lambda^n$ definite precedentemente: $(e_\lambda)$, $(f_\lambda)$, $(h_\lambda)$, $(m_\lambda)$, $(s_\lambda)$. Mostreremo che tutte le matrici di transizione che collegano una coppia di queste basi possono essere scritte in termini della matrice

$$K \;=\; M(s,m)$$

e la matrice corrispondente al coniugio $J$. Siccome $(m_\lambda)$ e $(h_\lambda)$ sono basi duali, e la base $(s_\lambda)$ è autoduale, abbiamo che

$$M(s,h) \;=\; K^* \tag{4.2}$$

grazie alla proposizione. Ricordando che $\omega(s_\lambda) = s_{\lambda'}$, possiamo osservare che

$$M(\omega s, s) \;=\; J,$$

e quindi abbiamo che

$$M(s,e) \;=\; M(\omega s, h) \;=\; M(\omega s, s)M(s,h) \;=\; JK^*.$$

Possiamo ora usare le (4.1a) e (4.1b) per completare la seguente tabella di matrici di transizione, in cui l'entrata con riga $u$ e colonna $v$ è $M(u,v)$:

**Matrici di transizione**

| | $e$ | $h$ | $m$ | $f$ | $s$ |
|---|---|---|---|---|---|
| $e$ | 1 | $K^tJK^*$ | $K^tJK$ | $K^tK$ | $K^tJ$ |
| $h$ | $K^tJK^*$ | 1 | $K^tK$ | $K^tJK$ | $K^t$ |
| $m$ | $K^{-1}JK^*$ | $K^{-1}K^*$ | 1 | $K^{-1}JK$ | $K^{-1}$ |
| $f$ | $K^{-1}K^*$ | $K^{-1}JK^*$ | $K^{-1}JK$ | 1 | $K^{-1}J$ |
| $s$ | $JK^*$ | $K^*$ | $K$ | $JK$ | 1 |

Alcune delle matrici di transizione nella tabella hanno un'interpretazione combinatoria. Dalla (3.27) segue che

**Proposizione 4.0.5.** *I numeri $K_{\lambda,\mu}$ sono il numero di tableau di forma $\lambda$ e peso $\mu$.*

I numeri $K_{\lambda,\mu}$ sono talvolta detti *numeri di Kostka*. Dalla caratterizzazione sopra enunciata sappiamo che sono non-negativi. Inoltre

**Proposizione 4.0.6.** *La matrice $(K_{\lambda,\mu})$ è strettamente unitriangolare superiore.*

*Dimostrazione.* Se $T$ è un tableau di forma $\lambda$ e peso $\mu$, allora per ciascun $r \geq 1$ ci sono $\mu_1 + \cdots + \mu_r$ simboli $\leq r$ in $T$, che devono tutti trovarsi nelle $r$ righe superiori di $T$ (perché $T$ è *stretto*, cioè i numeri in ciascuna colonna crescono strettamente). Quindi $\mu_1 + \cdots + \mu_r \leq \lambda_1 + \cdots + \lambda_r$ per ogni $r \geq 1$, ovvero $\mu \leq \lambda$. Quindi $K_{\lambda\mu}$ può essere diverso da zero solo se $\lambda \geq \mu$, e lo stesso ragionamento permette di ottenere che $K_{\lambda\lambda} = 1$. □

Dalla tabella e dalla proposizione sopra enunciata è possibile ottenere che:

**Proposizione 4.0.7.** *1. $M(s,h)$ e $M(h,s)$ sono strettamente triangolari inferiori.*

*2. $M(s,m)$ e $M(m,s)$ sono strettamente triangolari superiori.*

*3. $M(e,m) = M(h,f)$ ed è simmetrica.*

*4. $M(e,f) = M(h,m)$ ed è simmetrica.*

*5. $M(e,h) = M(h,e) = M(m,f)^t = M(f,m)^t$.*

*6. $M(h,s) = M(s,m)^t$.*

*7. $M(e,s) = M(s,f)^t$.*

In realtà come vedremo più avanti è anche possibile dire che $M(e,h)$ è strettamente triangolare superiore (vedasi la prop. 4.1.1). Possiamo inoltre dare la seguente caratterizzazione delle matrici $M(e,m)$ e $M(h,m)$:

**Proposizione 4.0.8.** *1. $M(e,m)_{\lambda\mu} = \sum_\nu K_{\nu\lambda}K_{\nu'\mu}$ è il numero di matrici di zeri e uni la cui somma sulle righe è $\lambda_i$ e la somma sulle colonne è $\mu_j$.*

*2. $M(h,m)_{\lambda\mu} = \sum_\nu K_{\nu\lambda}K_{\nu\mu}$ è il numero di matrici di interi non-negativi la cui somma sulle righe è $\lambda_i$ e la somma sulle colonne è $\mu_j$.*

*Dimostrazione.* Consideriamo il coefficiente del monomio $x^\mu$ (dove $\mu$ è una partizione di $n$) in $e_\lambda = e_{\lambda_1}e_{\lambda_2}\dots$ . Ciascun monomio in $e_{\lambda_i}$ è della forma $\prod_j x_j^{a_{ij}}$, dove $a_{ij}$ è 0 o 1, e $\sum_j a_{ij} = \lambda_i$. Dobbiamo quindi avere

$$\prod_{i,j} x_j^{a_{ij}} \;=\; \prod_j x_j^{\mu_j},$$

e quindi $\sum_i a_{ij} = \mu_j$. La matrice $(a_{ij})$ ha dunque somma sulle righe $\lambda_i$ e sulle colonne $\mu_j$, dato che contribuisce al coefficiente del monomio $x^\mu$. D'altra parte ogni tale matrice identifica un prodotto di monomi nell'espansione del prodotto $e_\lambda = e_{\lambda_1}e_{\lambda_2}\dots$ che contribuisce 1 al coefficiente di $x^\mu$.

La dimostrazione per $M(h,m)$ è simile: l'unica differenza è che $e_\lambda$ deve essere rimpiazzato con $h_\lambda$, e quindi gli esponenti $a_{ij}$ possono essere arbitrari interi non negativi. □

**Nota.** *Dalle proposizioni 4.0.5 e 4.0.8 segue che il numero di matrici di* 0 *e* 1 *con somma sulle righe $\lambda_i$ e somme sulle colonne $\mu_j$ è uguale al numero di coppie di tableau di forma coniugata e peso $\lambda$ e $\mu$, e di fatto è possibile costruire una esplicita corrispondenza biunivoca (corrispondenza duale di Knuth). Allo stesso modo, c'è un'esplicita corrispondenza biunivoca tra le matrici di interi non negativi con somme $\lambda_i$ sulle righe e $\mu_j$ sulle colonne e le coppie di tableau della stessa forma e pesi $\lambda$ e $\mu$.*

Consideriamo ora le matrici di transizione in cui compare la $\mathbb{Q}$-base $(p_\lambda)$. A questo scopo introduciamo la seguente notazione: se $\lambda$ è una partizione di lunghezza $r$, e $f$ è una funzione dall'intervallo di interi $[1,r] \to \mathbb{N}^+$ negli interi positivi, chiameremo $f(\lambda)$ il vettore la cui $i$-esima componente è

$$f(\lambda)_i \;=\; \sum_{\substack{1\le j\le r\\ f(j)=i}} \lambda_j, \qquad \text{per ogni } i \ge 1.$$

Quindi $f(\lambda)$ è una successione di interi non negativi le cui componenti sono somme di parti di $\lambda$, e in cui ogni parte $\lambda_i$ contribuisce precisamente ad un elemento della successione, che è selezionato dal valore di $f(i)$. Inoltre ogni tale successione si ottiene come $f(\lambda)$ per qualche $f : [1,r] \to \mathbb{N}^+$.

Sia ora $L$ la matrice di transizione $M(p,m)$:

$$p_\lambda = \sum_\mu L_{\lambda\mu} m_\mu.$$

Usando la notazione appena introdotta, abbiamo la

**Proposizione 4.0.9.** *$L_{\lambda\mu}$ è uguale al numero di $f$ tali che $f(\lambda) = \mu$.*

*Dimostrazione.* Espandendo il prodotto $p_\lambda = p_{\lambda_1} p_{\lambda_2} \dots$, otteniamo una somma di monomi della forma $x_{f(1)}^{\lambda_1} x_{f(2)}^{\lambda_2} \dots$, sommando su tutte le $f : [1, \ell(\lambda)] \to \mathbb{N}^+$. Quindi

$$p_\lambda \;=\; \sum_f x^{f(\lambda)}$$

da cui il risultato, essendo $L_{\lambda\mu}$ uguale al coefficiente di $x^\mu$ in $p_\lambda$. □

Se $\mu = f(\lambda)$, le parti $\mu_i$ di $\mu$ sono somme parziali dei $\lambda_i$, o equivalentemente, $\lambda$ è della forma $\bigcup_{i\ge1} \lambda^{(i)}$, dove ciascun $\lambda^{(i)}$ è a sua volta una partizione di $\mu_i$. Se questo succede, diremo che $\lambda$ è un *raffinamento* di $\mu$ e scriveremo $\lambda \le_{\text{ref}} \mu$. Chiaramente $\le_{\text{ref}}$ è un ordinamento parziale sull'insieme $\mathscr{P}_n$ delle partizioni di $n$, e abbiamo che:

$$\lambda \le_{\text{ref}} \mu \;\Rightarrow\; \lambda \le \mu. \tag{4.3}$$

*Dimostrazione.* Sia $I_k = f([1,k])$, per $k = 1, \dots, \ell(\lambda)$. Siccome $\mu_i = \sum_{f(j)=i} \lambda_j$, abbiamo che

$$\lambda_1 + \dots + \lambda_k \;\le\; \sum_{i\in I_k} \mu_i \;\le\; \mu_1 + \dots + \mu_k,$$

dove l'ultima disuguaglianza è vera perché $I_k$ ha al più $k$ elementi. □

**Nota.** *Il contrario della* (4.3) *è falso, perché per esempio due distinte partizioni $\lambda, \mu$ di $n$ tali che $\ell(\lambda) = \ell(\mu)$ non sono mai confrontabili per $\le_{\text{ref}}$, ma potrebbero benissimo esserlo per $\le$.*

Dalla proposizione 4.0.9 e dalla (4.3) segue che $L_{\lambda\mu}$ può essere diverso da zero solo se $\lambda \leq_{\text{ref}} \mu$ e quindi $\lambda \leq \mu$. La matrice $L$ è quindi strettamente triangolare inferiore.

Le matrici di transizione $M(p,e)$, $M(p,f)$ e $M(p,h)$ possono ora essere espresse in termini di $L$:

**Proposizione 4.0.10.** *1.* $M(p,e) = \varepsilon z L^*$,

*2.* $M(p,f) = \varepsilon L$,

*3.* $M(p,h) = zL^*$,
*dove come al solito abbiamo indicato con $L^*$ l'inversa trasposta di $L$, e $\varepsilon$ e $z$ sono rispettivamente le matrici diagonali $(\varepsilon_\lambda)$ e $(z_\lambda)$.*

*Dimostrazione.* Siccome le basi duali di $(h_\lambda)$ e $(p_\lambda)$ sono rispettivamente $(m_\lambda)$ e $(z_\lambda^{-1} p_\lambda)$, abbiamo dalla proposizione 4.0.4 che

$$M(p,h) \;=\; M(z^{-1}p, m)^* \;=\; (z^{-1}L)^* \;=\; zL^*.$$

Quindi abbiamo anche che

$$\begin{aligned} M(p,e) &= M(\omega p, \omega e) \;=\; M(\varepsilon p, h) \;=\; \varepsilon z L^*, \qquad \text{e} \\ M(p,f) &= M(\omega p, \omega f) \;=\; M(\varepsilon p, m) \;=\; \varepsilon L. \end{aligned}$$ □

Infine, abbiamo

$$M(p,s) \;=\; M(p,m)M(s,m)^{-1} = LK^{-1}.$$

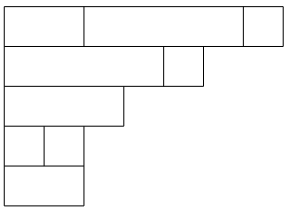
Questa matrice, che abbiamo già caratterizzato in 3.1.4 in termini delle decomposizioni di una partizione $\lambda$ in striscie di bordo di lunghezza $\mu_i$, si vedrà nel prossimo capitolo essere precisamente la tabella dei caratteri del gruppo simmetrico $S_n$.

## 4.1 Transizione fra funzioni complete e elementari

Dimostriamo ora che la matrice $M(e,h)$ è strettamente triangolare superiore, come abbiamo accennato precedentemente:

**Proposizione 4.1.1.** *La matrice $M(e,h)$ è strettamente triangolare superiore (e quindi $M(m,f) = M(e,h)^t$ è strettamente triangolare inferiore).*

*Dimostrazione.* Chiamiamo *domino* una striscia orizzontale connessa, ovvero un insieme di caselle consecutive nella stessa riga. Se $\lambda$ e $\mu$ sono partizioni di $n$, un *domino tabloid* di forma $\lambda$ e tipo $\mu$ è un modo di riempire il diagramma di $\lambda$ di domino di lunghezza $\mu_1, \mu_2, \ldots$ senza sovrapposizioni, senza fare distinzioni fra i domino della stessa lunghezza. Un domino tabloid è in altre parole un modo per riempire il diagramma di $\lambda$ di domino senza sovrapposizioni, in modo che ci siano esattamente $m_i(\mu)$ domino di lunghezza $i$.



**Un domino tabloid di forma $\lambda = (75322)$ e tipo $\mu = (443221111)$.**

Sia $d_{\lambda,\mu}$ il numero di domino tabloid di forma $\lambda$ e tipo $\mu$. Abbiamo allora che

$$M(e,h)_{\lambda\mu} \;=\; M(h,e)_{\lambda\mu} \;=\; \varepsilon_\mu d_{\lambda,\mu},$$

dove come al solito $\varepsilon_\mu = (-1)^{|\mu|-\ell(\mu)}$.

Infatti siccome

$$E(t) \;=\; H(-t)^{-1} \;=\; \Big(1 - \sum_{i\geq 1}(-1)^{i-1}h_i t^i\Big)^{-1} \;=\; \sum_{r\geq 0}\Big(\sum_{i\geq 1}(-1)^{i-1}h_i t^i\Big)^r$$

segue che, per ogni $n \geq 0$,

$$e_n \;=\; \sum_\alpha \varepsilon_\alpha h_\alpha$$

sommando su tutte le successioni finite $\alpha = (\alpha_1, \alpha_2, \dots)$ di interi positivi tali che $\sum \alpha_i = n$, e dove $\varepsilon_\alpha = (-1)^{\sum(\alpha_i - 1)}$. Quindi per una partizione $\lambda$ abbiamo che

$$e_\lambda \;=\; \sum_\beta \varepsilon_\beta h_\beta$$

sommando su tutte le successioni di interi positivi $\beta = (\beta_1, \dots, \beta_k)$ che possono essere partizionate in blocchi consecutivi di somma $\lambda_1, \lambda_2, \dots$ . Tali successioni sono in corispondenza biunivoca con i domino tabloid di forma $\lambda$.

Segue che $M(e,h)_{\lambda\mu}$ può essere diverso da zero solo se $\mu \leq_{\text{ref}} \lambda$. Inoltre se $\varepsilon$ è la matrice diagonale $(\varepsilon_\lambda)$, la matrice $M(e,h)\varepsilon$ è una matrice strettamente unitriangolare superiore costituita da interi non negativi. □

## 4.2 La regola di Littlewood-Richardson

Se $\mu$ e $\nu$ sono partizioni, il prodotto $s_\mu s_\nu$ è una combinazione lineare di funzioni di Schur:

$$s_\mu s_\nu = \sum_\lambda c^\lambda_{\mu\nu} s_\lambda$$

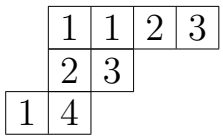
o, equivalentemente

$$s_{\lambda/\mu} = \sum_\nu c^\lambda_{\mu\nu} s_\nu. \tag{4.4}$$

I coefficienti $c^\lambda_{\mu\nu}$ sono interi non negativi, perché come mostreremo nella prop. 5.0.6 e per la (5.4), $c^\lambda_{\mu\nu} = \langle \chi^\lambda, \chi^\mu \cdot \chi^\nu \rangle$ è la molteplicità di $\chi^\lambda$ nel carattere $\chi^\mu \cdot \chi^\nu$. Inoltre $c^\lambda_{\mu\nu} = 0$ a meno che non si abbia che $|\lambda| = |\mu| + |\nu|$ e $\mu, \nu \subseteq \lambda$.

In questa sezione diamo l'enunciato e la dimostrazione di una regola combinatoria per calcolare i $c_{\mu\nu}^{\lambda}$ dovuta a Littlewood e Richardson.

Sia $T$ un tableau. Da $T$ deriviamo una *parola* o successione $w(T)$ leggendo i simboli in $T$ da destra a sinistra riga per riga, a partire dalla riga in alto. Per esempio, se $T$ è il tableau



allora $w(T)$ è la parola 32113241. Se una tale parola $w$ deriva in questo modo da un tableau di forma $\lambda/\mu$, diremo che $w$ è *compatibile* con $\lambda/\mu$. Una parola $w = a_1 a_2 \dots a_N$ nei simboli $1, 2, \dots, n$ è detta *permutazione di reticolo* se per $1 \leq r \leq N$ e $1 \leq i \leq n-1$, il numero di occorrenze del simbolo $i$ in $a_1 a_2 \dots a_r$ è almeno il numero di occorrenze di $i+1$.

Possiamo ora enunciare la regola di Littlewood-Richardson:

**Proposizione 4.2.1.** *Siano $\lambda, \mu, \nu$ partizioni. Allora $c_{\mu\nu}^{\lambda}$ è uguale al numero di tableau $T$ di forma $\lambda/\mu$ e peso $\nu$ tali che $w(T)$ è una permutazione di reticolo.*

La dimostrazione che daremo della 4.2.1 dipende dalla seguente proposizione. Se $\lambda, \mu, \pi$ sono partizioni tali che $\lambda \supseteq \mu$, denotiamo con $\mathrm{Tab}(\lambda/\mu, \pi)$ l'insieme dei tableau $T$ di forma $\lambda/\mu$ e peso $\pi$, e sia $\mathrm{Tab}^0(\lambda/\mu, \pi)$ il sottoinsieme dei $T$ tali che $w(T)$ è una permutazione di reticolo. Dalla (3.28) abbiamo che

$$\big|\mathrm{Tab}(\lambda/\mu, \pi)\big| \;=\; K_{\lambda/\mu,\pi} \;=\; \langle s_{\lambda/\mu}, h_\pi \rangle. \tag{4.5}$$

Dimostreremo che

**Proposizione 4.2.2.** *Esiste una bigezione*

$$\mathrm{Tab}(\lambda/\mu, \pi) \xrightarrow{\sim} \coprod_{\nu} \big(\mathrm{Tab}^0(\lambda/\mu, \nu) \times \mathrm{Tab}(\nu, \pi)\big).$$

Prima di dimostrare la 4.2.2, mostriamo come da essa segua la 4.2.1. Dalla 4.2.2 e dalla (4.5), abbiamo che

$$\langle s_{\lambda/\mu}, h_\pi \rangle \;=\; \sum_{\nu} \big|\mathrm{Tab}^0(\lambda/\mu, \nu)\big| \langle s_\nu, h_\pi \rangle$$

per tutte le partizioni $\pi$, e quindi

$$s_{\lambda/\mu} \;=\; \sum_{\nu} \big|\mathrm{Tab}^0(\lambda/\mu, \nu)\big| s_\nu.$$

Il confronto di questa identità con la (4.4) ci mostra che $c_{\mu\nu}^{\lambda} = \big|\mathrm{Tab}^0(\lambda/\mu, \nu)\big|$.

Per costruire la bigezione necessaria per la 4.2.2, usiamo l'ingegnoso metodo inventato da Littlewood e Robinson, che consiste nel partire da un tableau $T$ di forma $\lambda/\mu$ e modificarlo successivamente fino a che la parola $w(T)$ non sia

diventata una permutazione di reticolo, costruendo durante il procedimento un tableau $M$, che serve a registrare le mosse fatte.

Se $w = a_1 a_2 \dots a_N$ è una qualunque parola nei simboli $1, 2, \dots$, sia $m_r(w)$ il numero di occorrenze di $r$ in $w$. Per $p = 1, \dots, N$ e $r \geq 2$, la differenza $m_r(a_1 \dots a_p) - m_{r-1}(a_1 \dots a_p)$ è detta *$r$-indice* di $a_p$ in $w$. Si osservi che $w$ è una permutazione di reticolo se e solo se tutti gli indici sono $\leq 0$.

Per $r$ fissato, sia $m$ il massimo valore degli $r$-indici in $w$, e supponiamo che sia $m > 0$. Prendiamo il primo elemento di $w$ in cui il massimo è raggiunto (che sarà chiaramente un $r$), e rimpiazzamolo con $r - 1$. Chiamiamo il risultato di questa operazione $S_{r-1,r}(w)$ (sostituzione di $r - 1$ al posto di $r$). Osserviamo che $S_{r-1,r}(w)$ ha $r$-indice massimo $m - 1$ (a meno che $m = 1$, nel qual caso potrebbe anche essere $-1$ quando si stia sostituendo il primo elemento di $w$).

**Proposizione 4.2.3.** *L'operazione $S_{r-1,r}$ è uno-a-uno.*

*Dimostrazione.* Sia $w' = S_{r-1,r}(w)$. Per ricostruire $w$ da $w'$, sia $m'$ il massimo $r$-indice in $w'$. Se $m' \geq 0$, si prenda l'ultimo simbolo $w'$ con $r$-indice $m'$, e si converta il simbolo successivo (che deve essere un $r - 1$) in un $r$. Se $m' < 0$, il primo simbolo in $w'$ deve essere un $r - 1$, e questo è convertito in un $r$. In ogni caso il risultato è $w$, che è quindi univocamente determinato da $w'$ e $r$. □

**Proposizione 4.2.4.** *Sia $w' = S_{r-1,r}(w)$. Allora $w'$ è compatibile con $\lambda/\mu$ se e solo se $w$ è compatibile con $\lambda/\mu$.*

*Dimostrazione.* Siano $w = w(T), w' = w(T')$, dove $T$ e $T'$ sono diagrammi di forma $\lambda/\mu$. Essi differiscono in una sola casella, $x$ poniamo, che in $T$ è occupata da $r$ e in $T'$ da $r - 1$.

Supponiamo che $T$ sia un tableau. Se $T'$ non è un tableau deve verificarsi una delle seguenti possibilità: (a) la casella immediatamente a sinistra di $x$ è occupata da un $r$, o (b) quella immediatamente sopra è occupata da un $r - 1$.

Nel caso (a) il simbolo $r$ nella casella $y$ dovrebbe avere un $r$-indice maggiore in $w(T)$ della casella contenente $x$, e questo è impossibile. Nel caso (b), la casella $x$ in $T$ sarà l'ultima a sinistra di una stringa di $s$, poniamo, case occupate dal simbolo $r$, e immediatamente sopra a questa stringa dovrà esserci una stringa di $s$ caselle occupate dal simbolo $r - 1$. Abbiamo quindi che $w(T)$ contiene un segmento della forma

$$(r-1)^s \dots r^s$$

dove i simboli non scritti tra le due stringhe sono tutti o $< r - 1$ o $> r$, e l'ultimo $r$ è quello che sta venendo rimpiazzato con un $r - 1$ per formare $w'$. Ma l'$r$-indice di questo $r$ è uguale a quello dell'elemento di $w$ immediatamente prima della stringa degli $(r - 1)$ (che esiste, perché l'$r$-indice è diverso da zero), e questo è nuovamente impossibile. Quindi se $T$ è un tableau, anche $T'$ lo è.

L'implicazione inversa si dimostra similarmente, usando la strategia fornita nella dimostrazione della proposizione 4.2.3 per ritornare a $w$ da $w'$. □

Supponiamo ora che la parola $w$ abbia la proprietà di essere una permutazione di reticolo rispetto $(1, 2, \dots, r - 1)$ ma non rispetto $(r - 1, r)$, in altre parole

che gli $s$-indici siano tutti $\leq 0$ per $s = 1, 2, \ldots, r-1$ ma non per $s = r$. Questa è l'unica situazione un cui useremo l'operatore $S_{r-1,r}$. L'effetto di rimpiazzare un $r$ con $r-1$ in $w$ tramite $S_{r-1,r}$ può distruggere la proprietà di essere una permutazione di reticolo rispetto a $(r-2, r-1)$, ovvero potrebbe produrre qualche $(r-1)$-indice uguale a $+1$. In questo caso applichiamo $S_{r-2,r-1}$ per ottenere

$$S_{r-2,r}(w) \;=\; S_{r-2,r-1}S_{r-1,r}(w).$$

A questo punto gli $(r-1)$ indici saranno nuovamente $\leq 0$, ma potrebbe esserci qualche $(r-2)$-indice uguale a $+1$, e così via. Questo procedimento dovrà a un certo punto terminare, e avremo a questo punto ottenuto un

$$S_{a,r}(w) \;=\; S_{a,a+1}\ldots S_{r-1,r}(w)$$

per qualche $a$ tale che $1 \leq a \leq r-1$, e la parola $S_{a,r}(w)$ ha nuovamente la proprietà di essere una permutazione di reticolo rispetto a $(1, 2, \ldots, r-1)$, e $r$-indice massimale strettamente minore di quello di $w$.

A questo punto abbiamo bisogno del seguente lemma chiave:

**Lemma 4.2.5.** *Se $w$, $w' = S_{a,r}(w)$ e $w'' = S_{b,r}(w')$ hanno tutti la proprietà di essere permutazioni di reticolo rispetto a $(1, 2, \ldots, r-1)$, allora $b \leq a$.*

*Dimostrazione.* Sia $w = x_1x_2x_3\ldots$ . Dobbiamo studiare in dettaglio il processo con cui si passa da $w$ a $w'$. Si incomincia applicando $S_{r-1,r}$, ovvero rimpiazzando il primo $r$ in $w$ con $r$-indice $m$, dove $m$ è il massimo $r$-indice, con $r-1$.

Supponiamo che questo succeda in $x_{p_0}$. Allora per ogni $s \geq 1$, l'$(r-1)$-indice di $x_s$ rimane inalterato se $s < p_0$, ed è aumentato di 1 se $s \geq p_0$. L'elemento su cui agisce $S_{r-2,r-1}$ è quindi al $p_1$-esimo posto, dove $p_1$ è il minimo intero $\geq p_0$ tale che $x_{p_1}$ ha $(r-1)$-indice in $w$ uguale a 0. Allo stesso modo, l'elemento su cui opera $S_{r-3,r-2}$ è il $p_2$-esimo posto, con $p_2$ il minimo intero $\geq p_1$ per cui $x_{p_2}$ ha $(r-2)$-indice zero, e così via.

I questo modo otteniamo una successione

$$p_0 \leq p_1 \leq \cdots \leq p_{r-a-1}$$

con la proprietà che, per ogni $i \geq 1$, $x_{p_i}$ è il primo elemento che non precede $x_{p_{i-1}}$ in cui l'$(r-i)$-indice è 0. Si osservi che in $w'$ l'elemento al $p_i$-esimo posto ha ancora $(r-i)$-indice zero, per ogni $i \geq 1$ (anche se non sarà più il primo con questa proprietà che non precede $x_{p_{i-1}}$, a meno che non si abbia $p_i = p_{i-1}$).

Consideriamo ora il passaggio da $w' = y_1y_2y_3\ldots$ a $w''$. In $w'$ il massimo $r$-indice è ora $m-1$ (che stiamo supponendo essere ancora positivo), e questo massimo è raggiunto per la prima volta in un posto $q_0 < p_0$ (questo è perché l'$r$-indice aumenta e diminuisce sempre in passi di al più uno, e quindi l'$r$-indice $m-1$ è raggiunto in $w$ per la prima volta in un elemento a sinistra di $x_{p_0}$, e quindi anche in $w'$ visto che gli elementi a sinistra di $x_{p_0}$ restano fissi). In $w'$ l'$(r-1)$-indice di $y_{p_1}$ è zero, e quindi è $+1$ in $S_{r-1,r}(w')$. Quindi $S_{r-1,r}(w')$ ha ancora bisogno di una sostituzione $S_{r-2,r-1}$, che avrà luogo al $q_1$-esimo posto, dove $q_1$ è il primo intero $\geq q_0$ tale che l'$(r-1)$-indice di $y_{q_1}$ in $w'$ è 0, e quindi

$q_0 \leq q_1 \leq p_1$ per quanto detto. Continuando in questo modo otteniamo una successione

$$q_0 \leq q_1 \leq q_2 \leq \cdots \leq q_{r-a-1}$$

con la proprietà che $q_i \leq p_i$ per $i = 1, \ldots, r-a-1$, e a $w'$ può essere applicato l'operatore $S_{a,r}$. Se $S_{a,r}(w') = w''$, allora $b = a$, altrimenti $S_{a,r}(w')$ ammette ulteriori sostituzioni $S_{a-1,a}, \ldots$, fino a raggiungere $w'' = S_{b,r}(w')$, nel qual caso $b < a$, e abbiamo quindi dimostrato in ogni caso che si deve avere $b \leq a$. □

Descriviamo ora l'algoritmo di Littlewood e Robinson che costruisce da un tableau di forma $\lambda/\mu$ e peso $\pi$, dove $\lambda, \mu, \pi$ sono partizioni, una coppia $(L, M)$, dove $L \in \mathrm{Tab}^0(\lambda/\mu, \nu)$ per qualche partizione $\nu$, e $M \in \mathrm{Tab}(\nu, \pi)$.

Se $A$ è una tabella (non necessariamente un tableau), e $a, r$ interi positivi tali che $a < r$, denotiamo con $R_{a,r}(A)$ il risultato ottenuto spostando l'ultimo l'elemento a destra della $r$-esima riga di $A$ in alto a destra della $a$-esima riga.

L'algoritmo inizia con la parola $w_1 = w(T)$ e la tabella $M_1$ che consiste di $\pi_1$ volte 1 nella prima riga, $\pi_2$ volte 2 nella seconda, e così via (ovvero $M_1$ è anche l'unico tableau di forma $\pi$ e peso $\pi$).

Operiamo ora su $w_1$ con $S_{1,2}$ fino a che non ci sono più 2-indici positivi, e simultaneamente su $M_1$ con $R_{1,2}$ lo stesso numero di volte: poniamo

$$w_2 \;=\; S_{1,2}^m(w_1), \qquad M_2 \;=\; R_{1,2}^m M_1$$

Successiavamente operiamo su $w_2$ con $S_{2,3}$ o $S_{1,3}$ come necessario fino a far sparire anche i 3-indici positivi, e simultaneamente su $M_2$ con $R_{2,3}$ o $R_{1,3}$, ad esempio

$$w_3 \;=\; \ldots S_{a_2,3} S_{a_1,3}(w_2), \qquad M_3 \;=\; \ldots R_{a_2,3} R_{a_1,3} M_2$$

dove ogni $a_1, a_2$ è 1 o 2.

Continuiamo in questo modo fino ad ottenere una coppia $(w_\ell, M_\ell)$, dove $\ell = \ell(\pi)$. Chiaramente $w_\ell$ è ora una permutazione di reticolo per costruzione. Dalla proposizione 4.2.4 abbiamo che $w_\ell$ è compatibile con $\lambda/\mu$, e quindi $w_\ell = w(L)$ dove $L \in \mathrm{Tab}^0(\lambda/\mu, \nu)$ per qualche partizione $\nu$. Secondo, abbiamo che per costruzione in ogni istante la lunghezza $\ell_i(M_r)$ della $i$-esima riga della tabella $M_r$ è uguale alla molteplicità $m_i(w_r)$ del simbolo $i$ nella parola corrispondente $w_r$, e quindi la tabella finale $M = M_\ell$ ha forma $\nu$ e peso $\pi$ (il peso infatti resta invariato).

Dobbiamo ora mostrare che $M_\ell$ è un *tableau*. Per fare questo, proveremo per induzione su $r$ che le prime $r$ righe di $M_r$ formano un tableau. Questo è chiaro se $r = 1$, quindi supponiamo che $r > 1$ e l'asserzione vera per $r - 1$.

Consideriamo i passi che conducono da $M_{r-1}$ a $M_r$: ad esempio abbiamo

$$M_r \;=\; R_{a_m,r} \ldots R_{a_1,r}(M_{r-1}),$$

e poniamo per comodità

$$M_{r-1,i} \;=\; R_{a_i,r} \ldots R_{a_1,r}(M_{r-1}),$$

e allo stesso modo

$$w_{r-1,i} \;=\; S_{a_i,r} \dots S_{a_1,r}(w_{r-1}),$$

dove ogni parola $w_{r-1,i}$ ha la proprietà di essere una permutazione di reticolo rispetto a $(1, 2, \dots, r-1)$. Ogni tabella $M_{r-1,i}$ è ottenuta dalla precedente $M_{r-1,i-1}$ (o $M_{r-1}$ se $i = 1$) spostando in alto un singolo simbolo $r$ dalla $r$-esima riga alla $a_i$-esima. Per la nostra costruzione la lunghezza $\ell_j(M_{r-1,i})$ della $j$-esima riga di $M_{r-1,i}$ è uguale alla molteplicità $m_j(w_{r-1,i})$ di $j$ in $w_{r-1,i}$, per ogni $j \geq 1$, e siccome ogni $w_{r-1,i}$ è permutazione di reticolo rispetto a $(1, 2, \dots, r-1)$, ne segue che

$$\ell_1(M_{r-1,i}) \geq \dots \geq \ell_{r-1}(M_{r-1,i}).$$

Inoltre per il lemma 4.2.5 gli interi $a_i$ soddisfano $a_1 \geq \dots \geq a_m$. Da questo segue che nessuna coppia di simboli $r$ può comparire nella stessa colonna in nessun momento, e di conseguenza le prime $r$ righe di $M_r$ formano un tableau.

L'algoritmo ci ha quindi fornito una mappa

$$\mathrm{Tab}(\lambda - \mu, \pi) \to \coprod_{\nu} (\mathrm{Tab}^0(\lambda - \mu, \nu) \times \mathrm{Tab}(\nu, \pi)).$$

e per completare la dimostrazione della proposizione dobbiamo dimostrare che questa mappa è di fatto una bigezione. A questo scopo ci basta mostrare che, per ogni $r \geq$, possiamo univocamente ritornare indietro sui nostri passi da $(w_r, M_r)$ a $(w_{r-1}, M_{r-1})$. Con la notazione sopra introdotta, abbiamo che

$$w_r \;=\; S_{a_m,r} \dots, S_{a_1,r}(w_{r-1}),$$

e la successione $(a_1, \dots, a_m)$ può essere letta nella tabella $M_r$, poiché gli $a_i$ sono gli indici minori di $r$ delle righe in cui sono disposti i simboli $r$, arrangiati in ordine discendente $a_1 \geq a_2 \geq \dots \geq a_m$ (sempre grazie al lemma 4.2.5). Siccome per la prop. 4.2.3 ogni $S_{a,r}$ è reversibile, ne segue che $(w_{r-1}, M_{r-1})$ è univocamente determinato da $(w_r, M_r)$. Infine, grazie alla prop. 4.2.4, se $w_r$ è compatibile con $\lambda - \mu$, allora anche $w_{r-1}$ lo è e la dimostrazione è a questo punto completa. □

# Capitolo 5

# I caratteri del gruppo simmetrico

> 'Beauty is truth, truth beauty,' - that is all ye know on earth, and all ye need to know.
>
> *John Keats*

In questo capitolo daremo per buoni i fatti elementari sulle rappresentazioni e i caratteri dei gruppi finiti, e la trattazione seguirà principalmente [Mac95]. Una ottimo testo di riferimento in materia è [FH91], come anche [Ser77].

Se $G$ è un gruppo finito, e $f$ e $g$ sono funzioni da $G$ in una $\mathbb{Q}$-algebra commutativa, il *prodotto scalare* di $f$ e $g$ è definito come

$$\langle f, g\rangle_G \;=\; \frac{1}{|G|}\sum_{x\in G} f(x)g(x^{-1}).$$

Se $H$ è un sottogruppo di $G$ e $f$ è un carattere di $H$, denoteremo con $\mathrm{Ind}_H^G(f)$ il carattere indotto di $G$. Se invece $g$ è un carattere di $G$, la sua restrizione ad $H$ sarà indicata con $\mathrm{Res}_G^H(g)$.

Ogni permutazione $w \in S_n$ si fattorizza unicamente come prodotto di cicli, se gli ordini di questi cicli (inclusi gli 1-cicli) sono $\rho_1 \geq \rho_2 \geq \dots$, indichiamo con $\rho(w)$ la partizione $(\rho_1, \rho_2, \dots)$, il *tipo di decomposizione in cicli* di $w$. Essa determina univocamente $w$ a meno di coniugio in $S_n$, e le classi di coniugio in $S_n$ sono conseguentemente indicizzate dalle partizioni di $n$.

Definiamo ora la mappa $\psi : S_n \to \Lambda^n$ come segue:

$$\psi(w) = p_{\rho(w)}.$$

Se $m$ e $n$ sono interi positivi, possiamo immergere $S_m \times S_n$ in $S_{m+n}$ facendo agire $S_m$ e $S_n$ su sottoinsiemi complementari di $\{1, 2, \dots, m+n\}$. Ovviamente ci sono molti modi diversi per fare questo, ma i sottogruppi $S_{m+n}$ che si ottengono sono tutti coniugati. Quindi se $v \in S_m$ e $w \in S_n$, $v \times w \in S_{m+n}$ è ben definito a

meno di coniugio in $S_{m+n}$, e ha decomposizione in cicli $\rho(v \times w) = \rho(v) \cup \rho(w)$, cosicché

$$\psi(v \times w) = \psi(v)\psi(w). \tag{5.1}$$

Sia $R^n$ lo $\mathbb{Z}$-modulo generato dai caratteri irriducibili di $S_n$, e sia

$$R \;=\; \bigoplus_{n \geq 0} R^n,$$

con la convenzione di porre $S_0 = \{1\}$, per cui $R^0 = \mathbb{Z}$. Lo $\mathbb{Z}$-modulo $R$ ha una struttura di anello, definita come segue. Siano $f \in R^m$ e $g \in R^n$, e immergiamo $S_n \times S_m$ in $S_{m+n}$. Allora $f \times g$ è un carattere di $S_m \times S_n$, e possiamo quindi definire

$$f \cdot g \;=\; \mathrm{Ind}_{S_m \times S_n}^{S_{m+n}}(f \times g),$$

che è un carattere di $S_{m+n}$, cioè un elemento di $R^{m+n}$, che non dipende dalla scelta dell'immersione $S_m \times S_n \to S_{m+n}$. Abbiamo quindi definito una moltiplicazione bilineare $R^m \times R^n \to R^{m-n}$, e non è difficile verificare che con questa moltiplicazione $R$ è un anello graduato associativo, commutativo e con unità.

Inoltre, $R$ porta con sé il prodotto scalare definito sui caratteri: se $f, g \in R$, poniamo $f = \sum f_n$ e $g = \sum g_n$ con $f_n, g_n \in R^n$, definiamo

$$\langle f, g \rangle \;=\; \sum_{n \geq 0} \langle f_n, g_n \rangle_{S_n}.$$

Definiamo ora una mappa $\mathbb{Z}$-lineare

$$\mathrm{ch} : R \;\to\; \Lambda_{\mathbb{C}} = \Lambda \otimes_{\mathbb{Z}} \mathbb{C}$$

come segue: se $f \in R^n$, allora

$$\mathrm{ch}(f) \;=\; \langle f, \psi \rangle_{S_n} \;=\; \frac{1}{n!} \sum_{w \in S_n} f(w)\psi(w)$$

(essendo $\psi(w) = \psi(w^{-1})$). Se $f_\rho$ è il valore di $f$ in un elemento di tipo $\rho$, abbiamo che

$$\mathrm{ch}(f) = \sum_{|\rho| = n} z_\rho^{-1} f_\rho p_\rho. \tag{5.2}$$

$\mathrm{ch}(f)$ è detto *caratteristica* di $f$, e ch è detta *mappa caratteristica*. Dalla (5.2) e dalla (3.13) segue che, per $f, g \in R^n$,

$$\langle \mathrm{ch}(f), \mathrm{ch}(g) \rangle \;=\; \sum_{|\rho| = n} z_\rho^{-1} f_\rho g_\rho \;=\; \langle f, g \rangle_{S_n},$$

e quindi ch è una *isometria*. Il punto chiave è ora che

**Proposizione 5.0.6.** *La mappa caratteristica è un isomorfismo isometrico di $R$ in $\Lambda$.*

*Dimostrazione.* Verifichiamo come prima cosa che ch è un omomorfismo di anelli. Se $f \in R^m$ e $g \in R^n$, abbiamo che

$$\begin{aligned} \mathrm{ch}(f \cdot g) = &\ \langle \mathrm{Ind}_{S_m \times S_n}^{S_{m+n}}(f \times g), \psi \rangle_{S_{m+n}} \\ = &\ \langle f \times g, \mathrm{Res}_{S_{m+n}}^{S_m \times S_n}(\psi) \rangle_{S_m \times S_n} \end{aligned}$$

grazie alla reciprocità di Frobenius,

$$= \ \langle f, \psi \rangle_{S_m} \langle g, \psi \rangle_{S_n} \ = \ \mathrm{ch}(f) \cdot \mathrm{ch}(g)$$

per la (5.1). Sia ora $\eta_n$ il carattere identico di $S_n$. Allora

$$\mathrm{ch}(\eta_n) \ = \ \sum_{|\rho|=n} z_\rho^{-1} p_\rho \ = \ h_n$$

per le (5.2) e (2.10'). Se $\lambda = (\lambda_1, \lambda_2, \dots)$ è una qualunque partizione di $n$, chiamiamo $\eta_\lambda$ il prodotto $\eta_{\lambda_1}\eta_{\lambda_2}\dots$ . Allora $\eta_\lambda$ è un carattere di $S_n$, per la precisione il carattere indotto dai caratteri identici di $S_\lambda = S_{\lambda_1} \times S_{\lambda_2} \times \dots$, e abbiamo che $\mathrm{ch}(\eta_\lambda) = h_\lambda$.

Definiamo ora, per ogni partizione $\lambda$ di $n$,

$$\chi^\lambda = \det(\eta_{\lambda_i - i + j})_{1 \le i,j \le n} \in R^n, \tag{5.3}$$

cioè $\chi^\lambda$ è un carattere (eventualmente virtuale) di $S_n$, e per la (3.3) abbiamo che

$$\mathrm{ch}(\chi^\lambda) \ = \ s_\lambda. \tag{5.4}$$

Siccome ch è un'isometria, segue dalla (3.14) che $\langle \chi^\lambda, \chi^\mu \rangle = \delta_{\lambda\mu}$ per ogni coppia di partizioni $\lambda, \mu$, e quindi in particolare che gli $\chi^\lambda$ sono, a meno eventualmente del segno, i caratteri irriducibili di $S_n$.

Dato che il numero di classi di coniugio in $S_n$ è uguale al numero di partizioni di $n$, questi caratteri esauriscono tutti i caratteri irriducibili di $S_n$. Quindi i $\chi^\lambda$ per $|\lambda| = n$ formano una base di $R^n$, e quindi ch è un isomorfismo di $R^n$ su $\Lambda^n$ per ogni $n$, e quindi anche un isomorfismo da $R$ in $\Lambda$. □

**Proposizione 5.0.7.** *1. I caratteri irriducibili di $S_n$ sono i $\chi^\lambda$, per $|\lambda| = n$, definiti nella* (5.3)*.*

*2. Il grado di $\chi^\lambda$ è $K_{\lambda,(1^n)}$, il numero di tableau standard di forma $\lambda$.*

*Dimostrazione.* Dalla dimostrazione della proposizione 5.0.6 segue che ci basta mostrare che $\chi^\lambda$ è un carattere irriducibile, e non $-\chi^\lambda$. A questo scopo ci basta vedere che $\chi^\lambda(1) \ge 0$. Abbiamo ora dalla (5.2) e dalla (5.4) che

$$s_\lambda \ = \ \mathrm{ch}(\chi^\lambda) \ = \ \sum_\rho z_\rho^{-1} \chi_\rho^\lambda p_\rho$$

dove $\chi_\rho^\lambda$ è il valore di $\chi^\lambda$ sugli elementi che hanno decomposizione in cicli $\rho$. Quindi

$$\chi_\rho^\lambda \ = \ \langle s_\lambda, p_\rho \rangle \tag{5.5}$$

per la (3.13), e in particolare

$$\chi^\lambda(1) \;=\; \chi^\lambda_{(1^n)} \;=\; \langle s_\lambda, p_1^n\rangle$$

da cui

$$h_1^n \;=\; p_1^n \;=\; \sum_{|\lambda|=n} \chi^\lambda(1) s_\lambda$$

e quindi $\chi^\lambda(1) = M(h,s)_{(1^n),\lambda} = K_{\lambda,(1^n)}$. □

Dalla (5.5) segue anche la:

**Proposizione 5.0.8.** *La matrice di transizione $M(p,s)$ è la tabella dei caratteri del gruppo simmetrico $S_n$, cioè*

$$p_\rho = \sum_\lambda \chi^\lambda_\rho s_\lambda,$$

*e quindi $\chi^\lambda_\rho$ è uguale al coefficiente di $x^{\lambda+\delta}$ in $a_\delta p_\rho$.*

**Nota.** *Dalla tabella delle matrici di transizione segue che*

$$h_\lambda \;=\; s_\lambda + \sum_{\mu>\lambda} K_{\mu\lambda} s_\mu, \qquad e_{\lambda'} \;=\; s_\lambda + \sum_{\mu<\lambda} K_{\mu'\lambda'} s_\mu,$$

*e quindi*

$$\eta_\lambda \;=\; \chi^\lambda + \sum_{\mu>\lambda} K_{\mu\lambda}\chi^\mu, \qquad \varepsilon_{\lambda'} \;=\; \chi^\lambda + \sum_{\mu<\lambda} K_{\mu'\lambda'}\chi^\mu.$$

*Queste relazioni forniscono due decomposizioni dei moduli indotti*

$$H_\lambda \;=\; \mathrm{Ind}_{S_\lambda}^{S_n}(1), \qquad E_{\lambda'} \;=\; \mathrm{Ind}_{S_{\lambda'}}^{S_n}(\varepsilon).$$

*Conseguentemente $H_\lambda$ e $E_\lambda$ hanno un'unica componente irriducibile in comune, per la precisione l'$S_n$-modulo irriducibile con carattere $\chi^\lambda$. Grazie a questa osservazione è possibile fornire una costruzione esplicita degli $S_n$-moduli irriducibili (come vedremo più avanti).*

Siano $\lambda, \mu, \nu$ partizioni di $n$, e sia

$$\begin{aligned}\gamma_{\lambda\mu\nu} &= \langle \chi^\lambda, \chi^\mu\chi^\nu\rangle_{S_n} \\ &= \frac{1}{n!}\sum_{w\in S_n} \chi^\lambda(w)\chi^\mu(w)\chi^\nu(w),\end{aligned}$$

che è simmetrico in $\lambda, \mu$ e $\nu$. Abbiamo quindi, dati due distinti insiemi di variabili $x = (x_1, x_2, \dots)$ e $y = (y_1, y_2, \dots)$

$$s_\lambda(xy) \;=\; \sum_{\mu,\nu} \gamma_{\lambda\mu\nu} s_\mu(x) s_\nu(y), \tag{5.6}$$

dove per $(xy)$ intendiamo l'insieme dei prodotti $x_i y_j$ (Si confronti questa formula con la (3.23), che ha una forma simile, ma è diversa).

*Dimostrazione.* Per ogni partizione $\rho$ abbiamo che $p_\rho(xy) = p_\rho(x)p_\rho(y)$ e quindi grazie alla proposizione 5.0.8

$$\sum_\lambda \chi^\lambda s_\lambda(xy) \;=\; \sum_{\mu,\nu} \chi^\mu \chi^\nu s_\mu(x) s_\nu(y)$$

e quindi $s_\lambda(xy)$ è il coefficiente di $\chi^\lambda$ nel secondo membro. □

Siano $f, g \in \Lambda^n$, con $f = \mathrm{ch}(u), g = \mathrm{ch}(v)$ poniamo, dove $u, v$ sono funzioni di classe su $S_n$. Il *prodotto interno* di $f$ e $g$ è definito come

$$f * g = \mathrm{ch}(uv)$$

dove $uv$ è la funzione $w \mapsto u(w)v(w)$ su $S_n$. Rispetto a questo prodotto, $\Lambda^n$ diventa un anello commutativo e associativo, in cui l'identità è $h_n$.

È utile estendere questo prodotto per linearità su tutto $\Lambda$, e di fatto al suo completamento $\hat{\Lambda}$. Se

$$f \;=\; \sum_{n\geq 0} f^{(n)}, \qquad g \;=\; \sum_{n\geq 0} g^{(n)}$$

con $f^{(n)}, g^{(n)} \in \Lambda^n$, definiamo

$$f * g \;=\; \sum_{n\geq 0} f^{(n)} * g^{(n)}.$$

Rispetto a questo prodotto $\hat{\Lambda}$ è un anello commutativo con unità $\hat{1} = \sum h_n$, e $\Lambda$ è un sottoanello (che però non contiene l'identità). Se $\lambda, \mu, \nu$ sono partizioni di $n$, abbiamo che

$$s_\lambda * s_\mu = \sum_\nu \gamma_{\nu\lambda\mu} s_\nu$$

e quindi la (5.6) e la simmetria dei coefficienti $\gamma_{\nu\lambda\mu}$ ci danno che

$$s_\lambda(xy) \;=\; \sum_\mu s_\mu(x)(s_\lambda * s_\mu)(y).$$

Abbiamo inoltre che

$$p_\lambda * p_\mu = \delta_{\lambda\mu} z_\lambda p_\lambda \tag{5.7}$$

e quindi gli elementi $z_\lambda^{-1} p_\lambda \in \Lambda^n_{\mathbb{Q}}$ sono idempotenti a due a due ortogonali, e la loro somma su tutte le partizioni $\lambda$ di $n$ è per la (2.10') l'elemento identico $h_n$ di $\Lambda_n$. Infine, dati $f, g \in \Lambda$ abbiamo che

$$\langle f, g \rangle \;=\; (f * g)(1)$$

dove per $(f * g)(1)$ intendiamo $f * g$ valutata in $(x_1, x_2, \dots) = (1, 0, 0, \dots)$ (Per linearità è sufficiente verificare l'uguaglianza per $f = p_\lambda$ e $g = p_\mu$, e in questo caso segue immediatamente dalle (5.7) e (3.13), visto che $p_\lambda(1) = 1$ per ogni partizione $\lambda$).

## 5.1 I moduli di Specht

In generale se $A$ è un qualunque anello e $x, y \in A$, allora $Axy$ è un sottomodulo di $Ay$ ed è l'immagine di $Ax$ tramite l'omomorfismo $a \mapsto ay$ per $a \in A$, ed è quindi isomorfo ad un quoziente di $Ax$.

Sia ora $\lambda$ una partizione di $n$ e $T$ una numerazione delle caselle nel diagramma di $\lambda$ in cui i numeri $1, 2, \ldots, n$ compaiono precisamente una volta. Sia $R$ (risp. $C$) il sottogruppo di $S_n$ che stabilizza ciascuna riga (risp. colonna) di $T$, in modo che $R \cong S_\lambda$ e $C \cong S_{\lambda'}$. Sia $A = \mathbb{Q}[S_n]$ l'algebra di gruppo di $S_n$, e sia

$$a \;=\; \sum_{u \in C} \varepsilon(u) u, \qquad s \;=\; \sum_{v \in R} v.$$

Abbiamo allora che $As$ è il modulo indotto $\mathrm{Ind}_R^{S_n}(1)$, isomorfo a $H_\lambda$, e allo stesso modo $Aa \cong E_{\lambda'}$.

Sia $e = as \in A$. Poiché $R \cap C = \{1\}$, i prodotti $uv$ per $u \in C, v \in R$ sono tutti distinti, e quindi

$$e \;=\; 1 + \ldots \;\neq\; 0. \tag{5.8}$$

Grazie all'osservazione fatta all'inizio, $M_\lambda = Ae$ è un sottomodulo di $As$ ed è isomorfo a un quoziente di $Aa$. La nota che segue la prop. 5.0.8 ci dice inoltre che $M_\lambda$ è l'$A$-modulo (o $S_n$-modulo) irriducibile con carattere $\chi^\lambda$.

Sia $\varphi : A \to A$ la mappa di moltiplicazione a destra per $e$. Allora

$$\varphi(M_\lambda) \;=\; M_\lambda e \;=\; Ae^2 \;\subseteq\; Ae \;=\; M_\lambda.$$

Poiché $M_\lambda$ è irriducibile, segue dal lemma di Schur che $\varphi|_{M_\lambda}$ è la moltiplicazione per uno scalare $c \in \mathbb{Q}$, e quindi $e^2 = \varphi(e) = ce$. Quindi $\varphi^2 = c\varphi$, e gli unici autovalori di $\varphi$ sono 0 e $c$, e l'autovalore $c$ ha molteplicità uguale alla dimensione di $M_\lambda$. Quindi

$$\mathrm{Tr}\,\varphi \;=\; c \dim M_\lambda \;=\; cn!/h(\lambda)$$

per la prop. 5.0.7 e la (3.40). Abbiamo inoltre dalla (5.8) che per ciascun $w \in S_n$ il coefficiente di $w$ in $\varphi(w) = we$ è uguale a 1, e quindi rispetto alla base di $A$ costituita dagli elementi di $S_n$ la matrice di $\varphi$ ha tutti gli elementi diagonali uguali a 1, e

$$\mathrm{Tr}\,\varphi \;=\; n!.$$

Dalla (5.1) e dalla (5.1) segue che $c = h(\lambda)$, e quindi che $\hat{e} = h(\lambda)^{-1} as$ è un idempotente primitivo di $A$ corrispondente al carattere $\chi^\lambda$.

Indichiamo con $m_T \in \mathbb{Q}[x_1, \ldots, x_n]$ il monomio $x_1^{d(1)} \ldots x_n^{d(n)}$, dove $d(i) = r - 1$ se $i$ si trova nella $r$-esima riga di $T$, e sia $f_T$ il prodotto $\prod(x_i - x_j)$ su tutte le coppie $(i, j)$ tali che $j$ in $T$ si trova a nord di $i$. Allora $f_T$ è il prodotto dei determinanti di Vandermonde corrispondenti alle colonne di $T$, e $m_T$ è il termine di testa, per cui $f_T = am_T$ (secondo l'azione di $\mathbb{Q}[S_n]$ su $\mathbb{Q}[x_1, \ldots, x_n]$).

Sia $\vartheta : A \to \mathbb{Q}[x_1, \ldots, x_n]$ la mappa $u \mapsto um_T$. Dato che $d(i) = d(j)$ se e solo se $i$ e $j$ si trovano nella stessa riga di $T$, segue che il sottogruppo di $S_n$

che lascia fisso $m_T$ è lo stabilizzatore delle righe di $T$, e quindi $\vartheta(A) = As$. Di conseguenza $\vartheta|_{M_\lambda}$ è un isomorfismo, e possiamo quindi identificare $M_\lambda$ con la sua immagine

$$\vartheta(M_\lambda) \;=\; Aasm_T \;=\; Aam_T \;=\; Af_t.$$

Questa realizzazione di $M_\lambda$ è il *modulo di Specht* corrispondente alla partizione $\lambda$: esso è il $\mathbb{Q}$-spazio vettoriale generato da tutti gli $n!$ polinomi $f_T$, per tutte le numerazioni $T$ del diagramma di $\lambda$, e il gruppo simmetrico agisce su di esso permutando gli $x_i$.

La dimensione di $M_\lambda$ è uguale al numero di tableau standard di forma $\lambda$ per la prop. 5.0.7.

Di fatto mostreremo ora che i polinomi $f_T$, dove $T$ è un tableau standard, sono linearmente indipendenti su ogni campo, e formano quindi una *base* di $M_\lambda$.

Introduciamo l'ordinamento sui monomi definito da

$$x^\alpha < x^\beta \;\Leftrightarrow\; \alpha <_{\text{lex}} \beta,$$

noto come *ordinamento monomiale lessicografico*.

Supponiamo ora che $i < j$ e $d(i) < d(j)$ in $T$, e sia $w \in S_n$ la trasposizione $(ij)$. Allora $m_T < m_{wT}$, visto che in $m_T$ il fattore $x_i^{d(i)}x_j^{d(j)}$ diventa $x_i^{d(j)}x_j^{d(i)}$. Quindi se $T$ è un tableau standard

$$f_T \;=\; m_T + \text{monomi successivi}, \tag{5.9}$$

perché $f_T = am_T$, e $a$ è una combinazione di elementi di $C$, i quali lasciano invariate le colonne e sono prodotto di trasposizioni di elementi nella stessa colonna.

Siano $T_1, \ldots, T_r$ i tableau standard di forma $\lambda$. I monomi $m_{T_1}, \ldots, m_{T_r}$ sono tutti distinti, e a meno di riordinare eventualmente i $T_i$ possiamo assumere che $m_{T_1} < \cdots < m_{T_r}$. Grazie alla (5.9) segue immediatamente che gli $f_{T_i}$ sono linearmente indipendenti.

Grazie a quanto detto precedentemente, abbiamo che $f_T$ per una qualunque numerazione di $\lambda$ con i numeri $1, 2, \ldots, n$ è una combinazione lineare degli $f_{T_i}$, ed è anzi possibile osservare che i coefficienti di tale combinazione devono essere interi, essendo gli $f_{T_i}$ monici rispetto all'inverso dell'ordinamento monomiale definito. Infatti possiamo operare una riduzione sottraendo un multiplo intero opportuno di $f_{T_1}$ da $f_T$ in modo da annullare il coefficiente di $m_{T_1}$, poi sottrarre un multiplo di $f_{T_2}$ annullando il coefficiente di $m_{T_2}$, e così via.

## 5.2 Il pletismo

In questa sezione studiamo brevemente un'altra moltiplicazione in $\Lambda$, detta *pletismo* o *composizione*, e definita come segue. Siano $f, g \in \Lambda$, e scriviamo $g$ come somma di monomi

$$g \;=\; \sum_\alpha u_\alpha x^\alpha.$$

Introduciamo ora un'altro insieme di variabili fittizie $y_i$ definite da

$$\prod(1 + y_i t) \;=\; \prod_{\alpha}(1 + x^{\alpha} t)^{u_\alpha},$$

e definiamo

$$f \circ g \;=\; f(y_1, y_2, \dots).$$

Se $f \in \Lambda^m$ e $g \in \Lambda^n$, allora chiaramente $f \circ g \in \Lambda^{mn}$. Inoltre $e_1$ agisce come identità bilatera: $f \circ e_1 = e_1 \circ f = f$ per tutti gli $f \in \Lambda$. Dalla definizione (5.2) è chiaro che

**Proposizione 5.2.1.** *Per ogni $g \in \Lambda$, la mappa $f \mapsto f \circ g$ è un endomorfismo dell'anello $\Lambda$.*

Passando ai logaritmi in entrambi i membri della (5.2) otteniamo

$$p_n(y) = \sum_{\alpha} u_\alpha (x^\alpha)^n \qquad \text{per } n \geq 1,$$

per cui

$$p_n \circ g \;=\; g \circ p_n \;=\; g(x_1^n, x_2^n, \dots) \tag{5.10}$$

per tutti i $g \in \Lambda$. In particolare,

$$p_n \circ p_m \;=\; p_m \circ p_n \;=\; p_{mn}. \tag{5.11}$$

Dalla (5.10) segue la

**Proposizione 5.2.2.** *Per ogni $n \geq 1$, la mappa $g \mapsto p_n \circ g$ è un endomorfismo dell'anello $\Lambda$.*

Il pletismo è associativo: per ogni $f, g, h \in \Lambda$ abbiamo che

$$(f \circ g) \circ h \;=\; f \circ (g \circ h).$$

*Dimostrazione.* Siccome i $p_n$ generano $\Lambda_{\mathbb{Q}}$, in virtù delle prop. 5.2.1 e 5.2.2 è sufficiente dimostrare l'associatività quando $f = p_n$ e $g = p_m$, nel qual caso è ovvia grazie alle (5.10) e (5.11). □

Per pletismi con le funzioni di Schur ci sono le seguenti formule: dalla (3.23) segue che

$$\begin{aligned} s_\lambda \circ (g + h) &= \sum_{\mu,\nu} c^\lambda_{\mu\nu} (s_\mu \circ g)(s_\nu \circ h) \\ &= \sum_{\mu} (s_{\lambda/\mu} \circ g)(s_\mu \circ h) \end{aligned}$$

sommando sulle partizioni $\mu, \nu \subseteq \lambda$, mentre dalla (5.6) abbiamo che

$$s_\lambda \circ (gh) \;=\; \sum_{\mu,\nu} \gamma_{\lambda\mu\nu} (s_\mu \circ g)(s_\nu \circ h)$$

sommando sulle partizioni $\mu, \nu$ tali che $|\mu| = |\nu| = |\lambda|$.

Infine, siano $\lambda$ e $\mu$ partizioni. Allora $s_\lambda \circ s_\mu$ è una combinazione lineare di funzioni di Schur,

$$s_\lambda \circ s_\mu \;=\; \sum_\pi a^\pi_{\lambda\mu} s_\pi$$

poniamo, sommando su tutte le partizioni $\pi$ tali che $|\pi| = |\lambda| \cdot |\mu|$, ed è possibile mostrare che tali coefficienti $a^\pi_{\lambda\mu}$ sono tutti $\geq 0$ ([Mac95, Appendice A]).

# Capitolo 6

# Campi di funzioni simmetriche e polinomi di Newton

> The art of doing mathematics consists in finding that special case which contains all the germs of generality.
>
> *David Hilbert*

## 6.1 Introduzione

In questo capitolo lavoreremo su un campo $k$ che lasceremo sottointeso e chiameremo campo delle costanti, e che potrà essere di qualunque caratteristica se non diversamente specificato.

Sia $F = k(x_1, \ldots, x_n)$ il campo delle funzioni razionali[1] a coefficienti in $k$ nelle indeterminate $x_1, \ldots, x_n$ algebricamente indipendenti su $k$, che indicheremo anche con $F^k$ quando si voglia rendere esplicito il campo delle costanti. È un'estensione puramente trascendente di $k$ con grado di trascendenza uguale $n$, e possiamo considerare il campo delle funzioni simmetriche $S = S^k = F^{S_n}$ formato dalle funzioni invarianti sotto l'azione del gruppo simmetrico. $F$ è il campo di spezzamento del polinomio

$$X^n - e_1 X^{n-1} + e_2 X^{n-2} - \cdots + (-1)^n e_n \in S[X],$$

dove gli $e_n$ sono le funzioni simmetriche elementari in $x_1, \ldots, x_n$, e il gruppo di Galois dell'estensione $F/S$ è precisamente $S_n$ (questa è una conseguenza diretta

[1] Se non specificato altrimenti, in questo capitolo chiameremo 'funzioni razionali' le frazioni di polinomi (come in geometria algebrica), mettendo da parte il significato che era stato dato precedentemente a 'funzione' come sinonimo di 'polinomio simmetrico in infinite variabili'.

del teorema di Artin, visto che $S$ è per definizione proprio il campo lasciato fisso da $S_n$).

Sia

$$N_r = x_1^r + \cdots + x_n^r \in S$$

l'$r$-esimo polinomio di Newton (o somma di potenze) nelle variabili $x_1, \ldots, x_n$. Useremo questa notazione invece di quella precedentemente adottata in cui indicavamo le somme di potenze con $p_r$ per evitare di discostarci troppo dalla letteratura. In questo capitolo studiamo il seguente:

**Problema.** *Per quali tuple di interi $a_1, \ldots, a_m$ succede che*

$$S \;=\; k(N_{a_1}, \ldots, N_{a_m}),$$

*ovvero $N_{a_1}, \ldots, N_{a_m}$ generano l'intero campo simmetrico? In generale, se l'estensione è comunque un'estensione algebrica finita, qual è il grado?*

Per comodità di notazione supporremo gli $a_i$ tutti distinti. Inoltre per ogni tupla di interi distinti $a = (a_1, \ldots, a_m)$ definiamo, per alleggerire la notazione,

$$\mathcal{N}_a \;=\; \mathcal{N}_a^k \;=\; \mathcal{N}_{a_1,\ldots,a_m} \;=\; k(N_{a_1}, \ldots, N_{a_m}),$$

ovvero il campo generato da $N_{a_1}, \ldots, N_{a_m}$ su $k$.

Si possono notare subito alcune condizioni necessarie perché gli $N_{a_i}$ generino $S$, e in particolare siccome il grado di trascendenza di $S/k$ è $n$, è necessario che $m \geq n$, in caso contrario $S$ è un'estensione trascendente di $\mathcal{N}_a$ (vedremo che questa condizione è anche sufficiente perché l'estensione sia algebrica finita in caratteristica zero).

Inoltre se gli $a_i$ non sono primi fra loro, e il massimo comun divisore è $d = (a_1, \ldots, a_m)$ poniamo, allora il campo generato è contenuto dentro al campo simmetrico $S^{(d)} = k(x_1^d, \ldots, x_n^d)^{S_n}$, il campo delle funzioni simmetriche nelle potenze $x_1^d, \ldots, x_n^d$. Esso è quindi contenuto strettamente dentro $S$, e vedremo che il grado può essere studiato riconducendosi al caso in cui gli $a_i$ siano primi fra loro.

Sebbene questo problema nella massima generalità non sia ancora completamente risolto, vedremo molti risultati interessanti: in particolare in caratteristica zero se gli $a_i$ sono primi fra loro e $m = n + 1$ allora gli $N_{a_i}$ sono sempre sufficienti per generare l'intero campo simmetrico (vedasi [DZ08], [DZ03] per il caso in due variabili). Vedremo anche, nel caso in due variabili, alcune ipotesi addizionali sotto le quali anche in caratteristica positiva tre polinomi di Newton sono sufficienti per generare il campo simmetrico, che è un risultato originale di questa tesi.

Eccetto che per $n = 2$ (o $n = 1$, nel qual caso il problema è pressoché banale), in generale sembra difficile stabilire quale sia il grado algebrico di $S$ sul campo generato da $n$ polinomi di Newton, ma vedremo che sotto una curiosa ipotesi sulla tupla $a_1, \ldots, a_n$, allora anche $n$ polinomi sono sufficienti per generare l'intero campo simmetrico in caratteristica zero.

In questo capitolo daremo per buoni i risultati elementari di teoria di Galois e supporremo familiarità con il linguaggio della geometria algebrica, mentre ricapitolemo i risultati più importanti di cui avremo bisogno. Ottimi testi di riferimento per la teoria di Galois sono ad esempio [Mil08b] e [Lan02], per i requisiti di geometria algebrica si veda invece [Mil08a] e [Har77].

Siccome lavoreremo con campi che contengono elementi trascendenti sul campo base $k$ (che però potrebbero avere fra di essi relazioni algebriche non banali), indicheremo le variabili di definizione dei polinomi con le lettere maiuscole $X, Y, Z, \ldots$, e useremo le lettere minuscole $x, y, z, \ldots$ per indicare gli elementi dei campi in questione. Quindi un polinomio come $X^2 - yz$ sarà in generale un elemento di $k(y, z)[X]$, con $y, z$ elementi di qualche estensione $K$ di $k$ e non necessariamente algebricamente indipendenti.

## 6.2 Preliminari

Raccogliamo in questa sezione alcuni risultati che sarà necessario tenere presente nel seguito. La seguente proposizione permette di ricondursi agevolmente a considerare i campi $\mathcal{N}_a$ con gli interi $a = (a_1, \ldots, a_m)$ tutti primi fra loro:

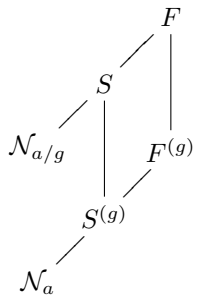
**Proposizione 6.2.1.** *Supponiamo che $g$ sia un fattore comune degli $a_1, \ldots, a_m$, e sia $a/g$ la tupla di interi $(a_1/g, \ldots, a_m/g)$. Allora se $n$ è il numero di varibili*

$$[S : \mathcal{N}_a] \;=\; g^n \cdot [S : \mathcal{N}_{a/g}],$$

*nel senso che ogni qual volta uno dei due membri esiste finito allora anche l'altro è finito e uguale.*

Si noti però che in generale $\mathcal{N}_{a/g}$ non è un'estensione di $\mathcal{N}_a$, basti porre $a = (2)$ e $g = 2$, e in questo caso abbiamo che $N_1$ e $N_2$ sono algebricamente indipendenti se il numero $n$ di variabili è $\geq 2$ (questo fatto è, ad esempio, conseguenza diretta della (2.9')).

*Dimostrazione.* Siano $F^{(g)}$ e $S^{(g)}$ i campi delle funzioni e delle funzioni simmetriche a coefficienti in $k$ nelle potenze $x_1^g, \ldots, x_n^g$. Abbiamo allora che




e che la catena di estensioni in basso è isomorfa a quella in alto, e in particolare si ottiene da essa tramite gli isomorfimi definiti da $x_i \mapsto x_i^g$ per $i = 1, \ldots, n$.

Ci basta quindi verificare che $[F : F^{(g)}] = g^n$. Ma se $L$ è un qualunque campo e $x$ trascendente su $L$, abbiamo che l'estensione ottenuta aggiungendo una radice $g$-esima $x$ di $x^g$ ha grado precisamente $g$ su $L(x^g)$, e prendendo $x = x_i$ e $L = k(x_1, \ldots, x_{i-1}, x_{i+1}^g, \ldots, x_n^g)$ per $i = 1, \ldots, n$, ci basta osservare che $F/F^{(g)}$ è la composizione di precisamente $n$ tali estensioni. □

Osserviamo che dalla dimostrazione si ricava anche che in caratteristica $p$ se $p^k$ è la massima potenza di $p$ che divide $g$, e $g = p^k g^*$ poniamo, allora il grado separabile dell'estensione $F/F^{(g)}$ è $(g^*)^n$, e quello inseparabile $p^{nk}$ (vedasi [Lan02, prop. 6.1, cap. V]). Questa osservazione ci permette in particolare di calcolare il grado separabile (e quello inseparabile) dell'estensione $S/\mathcal{N}_a$ sapendo quello di $S/\mathcal{N}_{a/g}$.

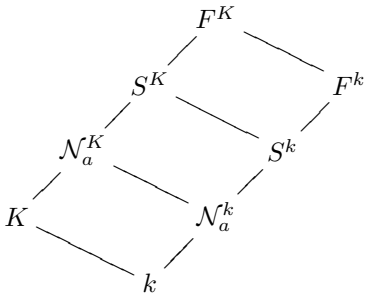
Un'altra proposizione fondamentale è la seguente, che ci svincola dalla dipendenza dal campo base $k$ e ci garantisce che è equivalentemente studiare il problema in qualunque altro campo con la stessa caratteristica di $k$ (ad esempio $\mathbb{Q}$ o $\mathbb{C}$ in caratteristica zero, $\mathbb{F}_p$ o $\bar{\mathbb{F}}_p$ in caratteristica positiva $p$).

**Proposizione 6.2.2.** *Sia $K/k$ una qualunque estensione di $k$ tale che $x_1, \ldots, x_n$ siano trascendenti indipendenti su $K$. Allora*

$$[S^k : \mathcal{N}_a^k] \;=\; [S^K : \mathcal{N}_a^K],$$

*nel senso che ogni qual volta uno di questi gradi esiste finito anche l'altro esiste ed è uguale, e dove i campi sono visti tutti come sottocampi di $F^K = K(x_1, \ldots, x_n)$.*

*Dimostrazione.* Consideriamo il seguente diagramma di estensioni:




Siccome $x_1, \ldots, x_n$ sono trascendenti su $K$, abbiamo che $K$ e $F^k$ sono linearmente disgiunti su $k$ ([Lan02, prop. 3.3, cap. VIII]). Da questo fatto segue immediatamente che $\mathcal{N}_a^K$ e $S^k$ sono linearmente disgiunte su $\mathcal{N}_a^k$ ([Lan02, prop. 3.1, cap. VIII]), e quindi l'uguaglianza nella formula qualora $S^k/\mathcal{N}_a^k$ o $S^K/\mathcal{N}_a^K$ sia un'estensione algebrica finita. □

### 6.2.3 Derivazioni

Un'importante strumento di cui avremo bisogno è la teoria di base delle derivazioni sui campi (vedasi [Lan02, sec. 5, cap. VIII]), di cui riassumiamo i punti

fondamentali. Definiamo formalmente una *derivazione* sul campo $K$ come una mappa $D : K \to K$ che soddisfa le solite regole, ovvero

$$D(x+y) \;=\; Dx + Dy, \qquad D(xy) \;=\; xDy + yDx.$$

Ad esempio se $K = k(x_1, \ldots, x_n)$ con $x_1, \ldots, x_n$ trascendenti su $k$, allora la derivata parziale $\partial/\partial x_i$ calcolata secondo le solite regole è una derivazione su $K$. Si noti che la derivazione banale tale che $Dx = 0$ per ogni $x \in K$ è una derivazione, se $k$ è un sottocampo di $K$ e $D$ una derivazione su $K$ diremo che $D$ è *banale su* $k$ se $Dx = 0$ per ogni $x \in k$. Una derivazione è sempre banale sul campo primo, perché $D(1) = D(1 \cdot 1) = 2D(1)$, e quindi $D(1) = 0$.

Supponiamo ora che $L = K(x) = K(x_1, \ldots, x_n)$ sia un'estensione di $K$ generata dagli elementi $x_1, \ldots, x_n$. Se $D$ è una derivazione su $K$, una derivazione $D^*$ su $L$ che coincida con $D$ su $K$ deve soddisfare la seguente condizione: per ogni relazione di dipendenza algebrica $f(X) \in K[X]$ che si annulli su $(x)$ allora dobbiamo avere che

$$0 \;=\; D^* f(x) \;=\; f^D(x) + \sum \frac{\partial f}{\partial x_i} D^* x_i, \tag{6.1}$$

dove $f^D$ è il polinomio ottenuto applicando $D$ ai coefficienti di $f$, e abbiamo indicato con $\partial f/\partial x_i$ il polinomio $\partial f/\partial X_i$ valutato in $x$. Un'estensione $D^*$ della derivazione $D$ deve soddisfare tale equazione per tutti gli $f$ che si annullano su $(x)$, che sono un ideale in $K[X]$ detto ideale determinato da $(x)$. È quindi sufficiente imporre che l'equazione sia verificata per un insieme di generatori di tale ideale.

D'altra parte è possibile verificare che questa condizione per l'esistenza di una derivazione è anche sufficiente ([Lan02, teo. 5.1, cap. VIII]), e nel caso di un'estensione monogenica $L = K(x)$, con $(x)$ formato da un solo elemento $x$, possiamo distinguere i seguenti tre casi:

*Caso* 1. $x$ è algebrico separabile. Allora $D$ si estende in modo unico a $K(x)$, e l'estensione è unicamente determinata dalla (6.1).

*Caso* 2. $x$ è trascendente su $K$. $D$ si estende e $D^*x$ può essere scelto arbitrariamente in $K(x)$.

*Caso* 3. $x$ è algebrico puramente inseparabile, ad esempio $x^{p^r} - a = 0$ con $a \in K$. Allora $D$ si estende a $K(x)$ se e solo se $Da = 0$. In particolare $D$ si estende se è banale su $K$, e $D^*x$ può essere scelto arbitrariamente in $K(x)$.

Siccome un'estensione qualunque è il composto delle estensioni monogeniche contenute in essa (eventualmente di una quantità infinita di esse), dalla distinzione per casi appena ricavata otteniamo immediatamente il seguente criterio: un'estensione $L/K$ è algebrica separabile se e solo se la derivazione banale su $K$ si può estendere solo con la derivazione banale su $L$ (per ulteriori dettagli vedasi la [Lan02, prop. 5.2, cap. VIII]).

Abbiamo inoltre la seguente proposizione, che svolgerà un ruolo importante nello studio del problema che stiamo trattando:

**Proposizione 6.2.4.** *Sia dato il campo $K$, e elementi $(x) = (x_1, \dots, x_n)$ in qualche estensione. Supponiamo che esistano $n$ polinomi $f_1, \dots, f_n \in K[X]$ tali che*

1. *$f_i(x) = 0$ per ogni $i = 1, \dots, n$, e*
2. *$\det(\partial f_i / \partial x_j)_{1 \le i,j \le n} \neq 0$.*

*Allora l'estensione $L = K(x)$ è algebrica separabile.*

*Dimostrazione.* Grazie al criterio sopra enunciato, ci basta vedere che la derivazione banale $D$ su $K$ si estende solo con la derivazione banale di $L$. Ma per ogni estensione $D^*$ di $D$ dobbiamo avere che $f_i^{D^*} = 0$ per $i = 1, \dots, n$, e scrivendo $n$ volte la (6.1) con $f_1, \dots, f_n$ al posto di $f$ abbiamo un sistema lineare non degenere che implica che $D^* x_i = 0$ per ogni $i = 1, \dots, n$, e quindi $D^*$ deve essere la derivazione banale su $L$, e quindi $L/K$ è algebrica separabile. □

Possiamo immeditamente applicare questo risultato al nostro problema, ricavando la seguente:

**Proposizione 6.2.5.** *Sia $a = (a_1, \dots, a_n)$ un tupla di interi positivi tutti distinti, e sia come sopra $S$ il campo delle funzioni simmetriche in $n$ variabili. Se il campo base $k$ è di caratteristica positiva $p$, supponiamo anche che gli $a_i$ siano tutti primi con $p$. Allora l'estensione $S/\mathcal{N}_a$ è algebrica finita separabile.*

*Dimostrazione.* Dimostriamo che l'estensione $F/\mathcal{N}_a$ è algebrica separabile. Essa è generata su $\mathcal{N}_a$ dagli $x_1, \dots, x_n$, ed essi soddisfano le relazioni

$$f_i(x) \;=\; x_1^{a_i} + x_2^{a_i} + \cdots + x_n^{a_i} - N_{a_i} = 0, \qquad \text{per } i = 1, \dots, n.$$

Il determinante della matrice $(\partial f_i / \partial x_j)_{1 \le i,j \le n} \neq 0$ è però anche uguale a

$$\det(a_i x_j^{a_i - 1})_{1 \le i,j \le n} \;=\; \frac{\prod_i a_i}{\prod_j x_j} \cdot \det(x_j^{a_i})_{1 \le i,j \le n},$$

che è un multiplo non nullo dell'antisimmetrizzato del monomio $x^a = x_1^{a_1} x_2^{a_2} \dots$ (come era stato definito nella (3.1)), che è diverso da zero in ogni caratteristica. Siccome l'estensione è algebrica e finitamente generata (dagli $x_1, \dots, x_n$) abbiamo quindi immediatamente anche che deve essere finita. □

Se la caratteristica è $p$ e qualche $a_i$ è divisibile per $p$, allora poniamo $a_i = \tilde{a}_i a_i^*$, dove $\tilde{a}_i$ è la massima potenza di $p$ che divide $a_i$, e sia $a^* = (a_1^*, \dots, a_n^*)$. Allora se gli $a_i^*$ sono tutti distinti abbiamo che $S/\mathcal{N}_{a^*}$ è algebrica finita separabile, e $\mathcal{N}_{a^*}$ è un'estensione di $N_a$ puramente inseparabile di grado $\prod \tilde{a}_i$ (visto che in caratteristica $p$ infatti $N_{a_i} = N_{a_i^*}^{\tilde{a}_i}$).

Notiamo che segue anche immediatamente che $n$ polinomi di Newton distinti $N_{a_1}, \dots, N_{a_n}$ in $n$ variabili sono sempre algebricamente indipendenti, a meno che la caratteristica non sia positiva, $p$ poniamo, ed esistano due $a_i$ e $a_j$ che differiscono solo per una potenza di $p$.

## 6.3 Il problema in due variabili

In questa sezione ci restringeremo al caso in due variabili $x, y$, e studieremo i sottocampi delle funzioni di simmetriche generati da polinomi di Newton in $x, y$. Vedremo come già questo in caso le soluzioni del problema siano tutt'altro che scontate, e come siano necessari strumenti moderatamente avanzati per ricavare tali soluzioni.

Iniziamo considerando il campo generato da due polinomi di Newton, seguendo [MS98]. Abbiamo allora la seguente proposizione, di cui proponiamo una dimostrazione leggeremente diversa da quella in [MS98] che non si adatta al caso in caratteristica positiva.

**Proposizione 6.3.1.** *Supponiamo che $a > b$ siano interi positivi primi fra loro. Se la caratteristica del campo base $k$ è positiva, $p$ poniamo, supponiamo anche che siano entrambi primi con $p$. Allora l'estensione $S/\mathcal{N}_{a,b}$ è separabile e ha grado*

$$[S : \mathcal{N}_{a,b}] \;=\; \begin{cases} \frac{ab}{2} & \text{se } ab \text{ è pari,} \\ \frac{(a-1)b}{2} & \text{se } ab \text{ è dispari.} \end{cases}$$

*Dimostrazione.* Calcoliamo il grado di $F/\mathcal{N}_{a,b}$. Se aggiungiamo $x$ al campo $\mathcal{N}_{a,b}$, allora possiamo ottenere

$$y^m \;=\; N_m - x^m, \qquad \text{per } m = a, b,$$

e quindi anche $y$ visto che $a$ e $b$ sono primi fra loro (infatti, se $as + bt = 1$ per qualche $s, t$ interi, abbiamo $y = (y^a)^s(y^b)^t$).

Abbiamo quindi dimostrato che $x$ è un elemento primitivo per l'estensione, ovvero $F = \mathcal{N}_{a,b}(x)$, e ci basta quindi calcolare il grado di $x$ su $\mathcal{N}_{a,b}$.

Ma $x$ soddisfa il polinomio

$$f(X) \;=\; (N_a - X^a)^b - (N_b - X^b)^a \in \mathcal{N}_{a,b}[X]$$

che è omogeneo di peso $ab$ (dove per peso intendiamo il grado pesato secondo cui $N_r$ ha grado $r$ per ogni $r \geq 1$, e $X$ ha grado 1). Inoltre $N_a$ e $N_b$ sono trascendenti indipendenti su $k$, e $\mathcal{N}_{a,b} = k(N_a, N_b)$ è il campo delle frazioni dell'anello di polinomi $k[N_a, N_b]$, che è un dominio a fattorizzazione unica.

Possiamo quindi applicare il lemma di Gauss ([Lan02, teo. 2.1 e 2.3, cap. IV]), e se dimostriamo che $f(X)$ è irriducibile in $k[N_a, N_b, X]$ avremo una relazione di dipendenza algebrica minimale per $x$ su $\mathcal{N}_{a,b}$, e il grado di $x$ sarà uguale al grado di $X$ in $f(X)$.

Ma il termine noto di $f(X)$ è $N_a^b - N_b^a$, che è omogeneo di peso $ab$. Esso è irriducibile perché un suo fattore dovrebbe essere omogeneo (secondo il peso sopra definito) e monico sia in $N_a$ che in $N_b$, e quindi dovrebbe avere peso che è multiplo sia di $a$ che di $b$, e di conseguenza di $ab$ essendo $a$ e $b$ primi fra loro. Quindi anche $f(X)$ è irriducibile essendo omogeneo, e il grado con cui compare $X$ è $ab$ se uno fra $a$ e $b$ è pari (e di conseguenza la caratteristica è $\neq 2$), e $(a-1)b$ altrimenti. Il grado di $S/\mathcal{N}_{a,b}$ è esattamente metà del grado di $F/\mathcal{N}_{a,b}$.

La separabilità è conseguenza diretta della prop. 6.2.5. □

Dalla dimostrazione si ricava che l'anello delle funzioni simmetriche in due variabili $\Lambda_{2,\mathbb{Q}}$ è un'estensione intera di $\mathbb{Q}[N_a, N_b]$, con $(a,b) = 1$, precisamente quando $a$ o $b$ è pari (e questo è vero in ogni caratteristica purché diversa da 2).

Dalla proposizione è possibile ottenere il grado anche quando $a$ e $b$, con $a > b$, non sono primi fra loro. Infatti se $d = (a,b)$, e $a = da', b = db'$, abbiamo applicando la prop. 6.2.1 che tale grado è

$$[S : \mathcal{N}_{a,b}] \;=\; \begin{cases} \frac{ab}{2} & \text{se } a'b' \text{ è pari,} \\ \frac{(a-d)b}{2} & \text{se } a'b' \text{ è dispari.} \end{cases}$$

Si noti che questa formula è valida in caratteristica $p$ anche se $p$ divide $d$, purché $p$ non divida $a'$ e $b'$ e si possa quindi applicare la prop. 6.3.1.

Se invece la potenza con cui $p$ divide gli $a, b$ è diversa, e supponiamo che $a = \tilde{a}a^*, a = \tilde{b}b^*$, con $\tilde{a}$ e $\tilde{b}$ le massime potenze di $p$ che dividono $a$ e $b$, allora possiamo comunque ricondurci alla formula qua sopra osservando che $\mathcal{N}_{a^*,b^*}$ è un'estensione puramente inseparabile di grado $\tilde{a}\tilde{b}$ di $\mathcal{N}_{a,b}$, visto che in caratteristica $p$ abbiamo sempre che $N_{pm} = N_m^p$ per ogni $m \geq 1$. Il grado di $S/\mathcal{N}_{a^*,b^*}$ si può calcolare usando la formula (si noti che il caso non simmetrico in $a$ e $b$ non dipende più da quale sia il maggiore fra $a$ e $b$, ma da quale sia il numero maggiore fra $a^*$ e $b^*$).

Un'altra conseguenza che possiamo trarre dalla proposizione 6.3.1 è che in caratteristica zero due polinomi di Newton generano l'intero campo simmetrico in due variabili se e solo se essi sono $N_1, N_2$ oppure $N_1, N_3$ (questo è vero anche in caratteristica positiva, purché diversa da 2 e 3). Vedremo più avanti delle condizioni sufficienti perché $n$ polinomi di Newton in $n$ variabili generino l'intero campo simmetrico che includono questo caso.

### 6.3.2 Soluzione in caratteristica zero

Questa sezione è principalmente dedicata a dimostrare il seguente risultato ([DZ03, teo. 1]). Sempre supponendo di star lavorando in due variabili, abbiamo:

**Teorema 6.3.3.** *Siano $a > b > c$ interi positivi tali che $(a,b,c) = 1$. Allora se $k$ è un campo di caratteristica zero e $S$ il campo delle funzioni simmetriche in due variabili su $k$ abbiamo che*

$$S \;=\; \mathcal{N}_{a,b,c} \;=\; k(N_a, N_b, N_c).$$

*Dimostrazione.* Grazie alla prop. 6.2.1 possiamo suppore che $k = \mathbb{C}$, i numeri complessi. Dimostreremo che il grado dell'estensione $F/\mathcal{N}_{a,b,c}$ è 2, e questo equivale a dimostrare che in una chiusura algebrica $\bar{F}$ di $F$ il sistema

$$X^m + Y^m \;=\; N_m, \qquad \text{per } m = a, b, c$$

nelle incognite $X, Y$ determina univocamente la coppia $(x, y)$ a meno di permutazione.

Supponiamo quindi per assurdo che esista una coppia di elementi $z, w \in \bar{F}$ tali che $\{z, w\} \neq \{x, y\}$ e tali che

$$x^m + y^m \;=\; z^m + w^m, \qquad \text{per } m = a, b, c. \tag{6.2}$$

Dimostriamo a beneficio di riferimenti futuri che non possono esistere due elementi fra $x, y, z, w$ che differiscano per una costante. Infatti $x, y$ sono trascendenti indipendenti per definizione, e quindi anche $z, w$ devono esserlo visto che $\mathbb{C}(z, w)$ contiene $\mathcal{N}_{a,b,c}$, che ha grado di trascendenza 2 su $\mathbb{C}$. Supponiamo ora per assurdo che $z = \mu x$. Abbiamo allora che sostituendo $\mu x$ per $z$ e eliminando $w$ dalle (6.2)

$$\begin{aligned}\big((1-\mu^a)x^a + y^a\big)^b &= \big((1-\mu^b)x^b + y^b\big)^a,\\ \big((1-\mu^a)x^a + y^a\big)^c &= \big((1-\mu^c)x^c + y^c\big)^a,\end{aligned}$$

che sono relazioni di dipendenza algebrica di $x$ e $y$, che sono trascendenti indipendenti. Esse devono quindi essere banali, e osservando i coefficienti dei termini in $x^b, x^c, x^a$ deduciamo che questo si verifica se e solo se $\mu^a = \mu^b = \mu^c = 1$, cioè $\mu = 1$ essendo $(a, b, c) = 1$. Abbiamo allora che $x = z$, assurdo perché stavamo supponendo le coppie $(x, y)$ e $(z, w)$ distinte. La dimostrazione di questo fatto funziona senza problemi anche in caratteristica positiva $p$, purché $a, b, c$ siano primi con $p$.

Se ora poniamo $t = y/x$, $u = z/x$ e $v = w/x$ e disomogeneizziamo le (6.2) dividendo per $x^m$ abbiamo che le nuove variabili devono soddisfare

$$1 + t^m \;=\; u^m + v^m, \qquad \text{per } m = a, b, c. \tag{6.3}$$

Inoltre il discorso appena fatto mostra che nessuna fra le $t, u, v$ è costante, e i rapporti $t/u, t/v, u/v$ non possono allo stesso modo essere costanti.

Estendiamo a $\bar{F}$ la derivazione naturale $\partial/\partial t$ di $\mathbb{C}(t)$, che indicheremo con un apice. Derivando le (6.3), e dividendo per $m$ abbiamo che

$$t^{m-1} - u^{m-1}u' - v^{m-1}v' \;=\; 0, \qquad \text{per } m = a, b, c,$$

che possiamo anche scrivere in come

$$\begin{pmatrix} t^a & u^a & v^a \\ t^b & u^b & v^b \\ t^c & u^c & v^c \end{pmatrix} \cdot \begin{pmatrix} 1/t \\ -u'/u \\ -v'/v \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

In particolare la matrice che compare al primo membro deve avere determinante zero. Sottraendo la prima colonna e sommando la seconda alla terza, abbiamo tenendo conto delle (6.3) che

$$\det \begin{pmatrix} t^a & u^a & 1 \\ t^b & u^b & 1 \\ t^c & u^c & 1 \end{pmatrix} \;=\; 0.$$

Dividendo la prima e seconda colonna rispettivamente per $t^c$ e $u^c$ ed espandendo il determinante abbiamo che

$$(t^{a-c}-1)(u^{b-c}-1)-(t^{b-c}-1)(u^{a-c}-1)=0.$$

Siccome possiamo ripetere lo stesso procedimento con $t,v$ al posto di $t,u$, otteniamo che

$$\frac{t^{a-c}-1}{t^{b-c}-1} \;=\; \frac{u^{a-c}-1}{u^{b-c}-1} \;=\; \frac{v^{a-c}-1}{v^{b-c}-1}. \tag{6.4}$$

Poniamo ora $d=(a-c,b-c)$, e $a-c=Ad, b-c=Bd$, e sia

$$R(X) \;=\; \frac{X^A-1}{X^B-1} \;=\; \frac{X^{A-1}+\cdots+X+1}{X^{B-1}+\cdots+X+1}.$$

Siccome $A\geq B$ e $A,B$ sono coprimi, il grado della mappa algebrica definita da $R$ è $A-1$. Osserviamo che la (6.4) si può riscrivere come

$$R(t^d) \;=\; R(u^d) \;=\; R(v^d). \tag{6.5}$$

Questa relazione fra $t,u,v$ motiva lo studio dell'equazione

$$R(X) \;=\; \zeta, \tag{6.6}$$

e in particolare mireremo a determinare il gruppo di Galois di questa equazione su $\mathbb{C}(\zeta)$. Come prima cosa calcoliamo la ramificazione del rivestimento della $\zeta$-sfera dato dall'equazione $R(\xi)=\zeta$.

I punti della $\xi$-sfera sopra $\zeta=\infty$ sono dati da $\xi=\infty$ e da

$$\xi^{B-1}+\cdots+\xi+1=0,$$

e siccome quest'equazione non ha radici multiple, può esserci ramificazione solo in corrispondenza di $\xi=\infty$, e l'indice di ramificazione è $A-B$.

Gli altri punti di branch corrispondo ai valori di $\zeta=R(\xi)$ in cui si abbia $R'(\xi)=0$. Quest'ultima equazione è verificata se e solo se

$$A\xi^{A-1}(\xi^B-1)-B\xi^{B-1}(\xi^A-1) \;=\; 0, \qquad \xi\neq 1, \tag{6.7}$$

dove abbiamo escluso le soluzioni $\xi=1$ perché $R'(1)=\frac{(A-B)A}{2B}$, come è possibile verificare facilmente dalla definizione.

Mostriamo ora che $R'(X)$ non ha radici multiple eccetto eventualmente la radice $X=0$. Infatti siccome possiamo equivalentemente studiare la (6.7), abbiamo che dividendo per $\xi^{B-1}$ e differenziando si ottiene

$$A(A-B)\xi^{A-B-1}(\xi^B-1),$$

e, essendo $A,B$ coprimi, questo polinomio non ha nessuna radice in comune con il primo membro della (6.7), eccetto eventualmente $\xi=0,1$.

Se $B>1$, allora $\xi=0$ è una soluzione della (6.7). Essa corrisponde al valore $R(0)=1$, e ha indice di ramificazione $B$.

Per quanto riguarda le altre soluzioni della (6.7), mostreremo che di fatto esse danno luogo a valori di $R(\xi)$ tutti distinti, eccetto eventualmente per il valore $R(\xi) = 1$. Supponiamo infatti che $\xi_1$ e $\xi_2$ siano due soluzioni distinte e non nulle della (6.7), con $R(\xi_1) = R(\xi_2)$. La (6.7) può essere riscritta come

$$\frac{A}{B}\xi^{A-B} = R(\xi),$$

e si dovrebbe quindi avere che $\xi_1^{A-B} = \xi_2^{A-B}$. D'altra parte l'uguaglianza $R(\xi_1) = R(\xi_2)$ si può scrivere come

$$\xi_1^{A-B} + \frac{\xi_1^{A-B} - 1}{\xi_1^B - 1} \;=\; \xi_2^{A-B} + \frac{\xi_2^{A-B} - 1}{\xi_2^B - 1}.$$

Sostituiamo nell'equazione le occorrenze di $\xi_2^{A-B}$ con $\xi_1^{A-B}$. Può succedere che $\xi_1^{A-B} = 1$, nel qual caso $\xi_1^A = \xi_1^B$, e quindi $R(\xi_1) = 1$. In caso contrario l'equazione ci dice che $\xi_1^B = \xi_2^B$, e siccome $\xi_1^{A-B} = \xi_2^{A-B}$ segue che $\xi_1 = \xi_2$, visto che $(B, A - B) = 1$.

Abbiamo quindi ottenuto che gli indici di ramificazione sui punti di branch diversi da $\zeta = 1, \infty$ sono dati dalla successione $2, 1, 1, \ldots, 1$, mentre la ramificazione sopra $\zeta = \infty$ è data da $A - B, 1, 1, \ldots, 1$. Se $B = 1$, abbiamo anche che $R(\xi) - 1 = \xi(\xi^{A-2} + \cdots + \xi + 1)$, e non c'è ramificazione sopra $\zeta = 1$.

Ricordiamo che il gruppo di Galois $\Gamma$ della (6.6), come gruppo delle permutazioni di $A - 1$ elementi, può essere generato da permutazioni le cui decomposizioni in cicli sono dello stesso tipo delle successioni di ramificazione. È possibile scegliere precisamente una permutazione per punto di branch in modo che il prodotto di tutti gli elementi scelti sia l'identità. Possiamo in particolare ignorare una singola permutazione e gli elementi rimanenti generano ancora $\Gamma$ (vedasi [Völ96, sec. 2.2, pag. 32-37, in particolare il Remark 4.33]).

Se $B = 1$, possiamo buttare via la permutazione associata a $\zeta = \infty$ ricavando che $\Gamma$ è generato da trasposizioni. Se $B \neq 1$, buttiamo via la permutazione corrispondente a $\zeta = 1$, ottenendo che $\Gamma \subseteq S_{A-1}$ è generato da trasposizioni e da un ciclo di lunghezza $A - B \lneqq A - 1$. Inoltre $\Gamma$ è transitivo, essendo $R(X) - \zeta$ irriducibile.

Questa caratterizzazione implica che $\Gamma = S_{A-1}$, grazie al seguente

**Lemma 6.3.4.** *Sia $\Gamma$ un sottogruppo transitivo di $S_n$ generato da trasposizioni e da un ciclo di lunghezza $\lneqq n$. Allora $\Gamma = S_{A-1}$.*

*Dimostrazione.* A meno di riordinamento possiamo supporre che il ciclo, di ordine $k-1$ poniamo, sia $\sigma = (2, 3, \ldots, k)$, e che una trasposizione sia $\tau = (1, 2)$. Abbiamo allora che $(1, i) = \sigma^{i-2}\tau\sigma^{2-i}$ per $i = 2, 3, \ldots, k$, e queste trasposizioni $(1, i)$ generano l'intero gruppo delle permutazioni di $1, 2, \ldots, k$.

A meno di riordinare gli elementi rimanenti $k+1, \ldots, n-1, n$, per transitività dobbiamo avere una trasposizione della forma $(j, k + 1)$ per qualche $1 \leq j \leq k$. Essa insieme a tutte le permutazioni di $1, 2, \ldots, k$ genera tutte le permutazioni di $1, 2, \ldots, k + 1$, ed è chiaro che possiamo ripetere questo ragionamento fino ad ottenere l'intero gruppo simmetrico $S_n$. □

Tornando alla dimostrazione del teorema, ricordiamo che non esistono due fra le $t, u, v$ che soddisfano la (6.3) con rapporto costante. In particolare, le loro potenze $d$-esime sono tutte distinte.

Sia ora $\Omega$ il campo di spezzamento di $R(X) - \zeta = 0$ su $\mathbb{C}(\zeta)$, dove $\zeta = R(t^d)$. Per la (6.5) abbiamo che $t^d, u^d, v^d \in \Omega$, e il gruppo di Galois dell'estensione $\Omega/\mathbb{C}(\zeta)$ è $\Gamma \cong S_{A-1}$.

Per trattare con $t, u, v$ invece che con le loro potenze $d$-esime abbiamo ancora bisogno di osservare quanto segue. Siccome la ramificazione di $\mathbb{C}(u^d)$ su $\mathbb{C}(\zeta)$ sopra $\zeta = \infty$ ha per indici $A - B, 1, 1, \ldots, 1$, l'estensione $\Omega/\mathbb{C}(\zeta)$ è ramificata sopra $\infty$ con indici tutti uguali a $A-B$. Quindi $\Omega/\mathbb{C}(u^d)$ non è ramificata sopra $\infty$. D'altra parte $\mathbb{C}(u)/\mathbb{C}(u^d)$ è totalmente ramificata sopra $\infty$, e quindi $u$ ha grado $d$ su $\Omega$.

Siccome $\Gamma$ è l'intero gruppo simmetrico, tenendo conto della (6.5) possiamo scegliere un $\sigma \in \Gamma$ tale che

$$\sigma(u^d) = u^d, \qquad \sigma(v^d) = t^d, \qquad \sigma(t^d) = v^d.$$

Sia $\psi$ una arbitraria radice $d$-esima primitiva dell'unità. Avendo $u$ grado $d$ su $\Omega$ possiamo sollevare $\sigma$ alla chiusura algebrica di $\mathbb{C}(\zeta)$ in modo che si abbia anche che

$$\sigma(u) = \psi u.$$

Inoltre per ogni tale estensione si avrà anche che $\sigma(v) = \alpha t$ e $\sigma(t) = \beta v$, dove $\alpha, \beta$ sono opportune radici $d$-esime dell'unità. Se applichiamo $\sigma$ alle equazioni (6.3), che riscriviamo come

$$u^m + v^m - t^m \;=\; 1, \qquad \text{per } m = a, b, c, \tag{6.8}$$

otteniamo che

$$\psi^m u^m + \alpha^m t^m - \beta^m v^m \;=\; 1, \qquad \text{per } m = a, b, c. \tag{6.9}$$

Supponiamo ora che la (6.9) sia identica alla (6.8), per $m = a, b, c$, e quindi che $\psi^m = 1, \alpha^m = \beta^m = -1$. Allora $\psi = 1$, e questo può succedere solo se $d = 1$. Abbiamo quindi per la scelta di $\sigma$ che $\sigma(t) = v, \sigma(v) = t$, e di conseguenza $\alpha = \beta = 1$, ma questo è assurdo.

Possiamo quindi assumere che le (6.8) e (6.9) siano differenti per qualche $m \in \{a, b, c\}$. Eliminando una delle $t, u, v$, otteniamo un'equazione del tipo

$$c_1 w_1^m + c_2 w_2^m \;=\; c_3,$$

dove $\{w_1, w_2, w_3\} = \{t, u, v\}$, e $c_1, c_2, c_3$ sono costanti non tutte nulle, e che anzi devono essere tutte diverse da zero, essendo i $w_i$ non costanti e non essendo costante nessun rapporto fra essi.

Prendiamo quindi un $\sigma \in \Gamma$ tale che $\sigma(w_1^d) = w_3^d$ e $\sigma(w_2^d) = w_2^d$, ragionando come sopra possiamo estendere $\sigma$ alla chiusura algebrica di $\mathbb{C}(\zeta)$ in modo che $\sigma(w_2) = w_2$. Applicando $\sigma$ a quest'ultima equazione otteniamo che il rapporto $w_1/w_3$ deve essere una costante, e questa è una contraddizione che conclude la dimostrazione del teorema. □

### 6.3.5 Risultati in caratteristica positiva

Ci proponiamo in questa sezione di studiare il campo generato da tre polinomi di Newton distinti $N_a, N_b, N_c$ su un campo a caratteristica positiva, $p$ poniamo, che supponiamo per comodità essere la chiusura algebrica $\bar{\mathbb{F}}_p$ di $\mathbb{F}_p$.

Iniziamo osservando che richiedere $(a, b, c) = 1$ non è più sufficiente perché il campo generato sia l'intero campo simmetrico $S$. Abbiamo infatti che

**Proposizione 6.3.6.** *Siano $a, b, c$ interi positivi distinti. Se almeno due fra gli $a, b, c$ sono divisibili per $p$, allora il campo $\mathcal{N}_{a,b,c}$ non può essere tutto $S$.*

*Dimostrazione.* Supponiamo infatti che $a, b$ siano divisibili per $p$. Allora

$$\mathcal{N}_{a,b,pc} \subseteq S^{(p)},$$

dove $S^{(p)}$ è il campo simmetrico nelle potenze $x^p, y^p$. Inoltre siccome $N_c^p = N_{pc}$, il grado $[\mathcal{N}_{a,b,c} : \mathcal{N}_{a,b,pc}]$ è al più $p$. Ma il grado di $[S : S^{(p)}]$ è $p^2$, e quindi $\mathcal{N}_{a,b,c}$ non può essere uguale a $S$. □

Per contro, abbiamo anche il seguente risultato che permette di ricondursi al caso in cui $a, b, c$ sono tutti primi con $p$.

**Proposizione 6.3.7.** *Siano $a, b, c$ interi positivi distinti tutti primi con $p$, e supponiamo anche che si abbia $\mathcal{N}_{a,b,c} = S$. Allora abbiamo anche che per ogni $k \geq 1$*

$$\mathcal{N}_{a,b,p^k c} = S.$$

*Dimostrazione.* Infatti $N_c$ soddisfa su $\mathcal{N}_{a,b,p^k c}$ la relazione di dipendenza algebrica

$$X^{p^k} - N_{p^k c} = 0,$$

che è un polinomio eventualmente riducibile, ma puramente inseparabile, ovvero con le radici tutte uguali. Abbiamo quindi che $\mathcal{N}_{a,b,p^k c}(N_c) = \mathcal{N}_{a,b,c} = S$ è un'estensione puramente inseparabile di $\mathcal{N}_{a,b,p^k c}$. Ma noi già sappiamo grazie alla 6.2.5 che $S/\mathcal{N}_{a,b}$ è un'estensione algebrica separabile, e quindi anche $S/\mathcal{N}_{a,b,p^k c}$ è algebrica separabile. Essendo sia separabile che puramente inseparabile tale estensione deve quindi essere banale. □

Questa proposizione permette quindi di suppore che $a, b, c$ siano tutti primi con $p$ senza perdita di generalità.

Vediamo ora il risultato principale di questa sezione, che fornisce condizioni abbastanza generali su $a, b, c$ perché si abbia $\mathcal{N}_{a,b,c} = S$.

**Proposizione 6.3.8.** *Siano $a > b > c$ interi positivi primi con la caratteristica $p$, e supponiamo inoltre che $a-c, a-b, b-c$ siano anch'essi primi con $p$. Allora*

$$\mathcal{N}_{a,b,c} = S.$$

*Dimostrazione.* Supponiamo, come nella dimostrazione del teo. 6.3.3, che il grado di $F/\mathcal{N}_{a,b,c}$ sia $\gneqq 2$. Sia quindi $\bar{F}^{\text{sep}}$ la chiusura algebrica separabile del campo delle funzioni razionali $F$, e supponiamo che esistano $z, w \in \bar{F}^{\text{sep}}$ distinti da $x, y$ tali che

$$x^m + y^m \;=\; z^m + w^m, \qquad \text{per } m = a, b, c. \tag{6.10}$$

Infatti $x, y$ sono separabili su $\mathcal{N}_{a,b,c}$, e quindi anche gli $z, w$ che sono loro coniugati su $\mathcal{N}_{a,b,c}$ devono esserlo.

Osserviamo che è possibile ripetere senza alcun problema il passo della dimostrazione in caratteristica zero con cui abbiamo stabilito che non possono esistere due fra gli $x, y, z, w$ che hanno rapporto costante.

Estendiamo ora a $\bar{F}^{\text{sep}}$ la derivazione $\partial/\partial z$ del campo $\bar{\mathbb{F}}(z, w)$ (ricordiamo che $w, z$ sono algebricamente indipendenti), che indichiamo con un apice. Derivando le (6.10) otteniamo le relazioni non banali

$$x^{m-1}x' + y^{m-1}y' \;=\; z^{m-1}, \qquad \text{per } m = a, b, c, \tag{6.11}$$

avendo scelto $a, b, c$ tutti primi con $p$.

Ragionando come nel caso in caratteristica zero si deve quindi annullare il determinante $R(x, y, z)$ definito come

$$R(X, Y, Z) \;=\; \det \begin{pmatrix} X^{a-c} & Y^{a-c} & Z^{a-c} \\ X^{b-c} & Y^{b-c} & Z^{b-c} \\ 1 & 1 & 1 \end{pmatrix} \;= \tag{6.12}$$
$$Z^A(X^B - Y^B) - Z^B(X^A - Y^A) + X^B Y^B (X^{A-B} - Y^{A-B}),$$

in cui $A = a - c$, $B = b - c$, e che vedremo come polinomio in $Z$ su $\bar{\mathbb{F}}[X, Y]$.

Sia $V(X, Y, Z) = (X - Y)(Z - X)(Z - Y)$, il determinante della matrice di Vandermonde in $X, Y, Z$. Se $d = (A, B)$, $R(X, Y, Z)$ è chiaramente divisibile per $V(X^d, Y^d, Z^d)$, il quale non si annulla su $(x, y, z)$ visto che non esistono due fra $x, y, z$ con rapporto costante.

Quindi $(x, y, z)$ devono annullare il quoziente

$$T(X, Y, Z) \;=\; T_{A,B}(X, Y, Z) \;=\; \frac{R(X, Y, Z)}{V(X^d, Y^d, Z^d)},$$

che mostreremo ora essere irriducibile. Osserviamo che $T(X, Y, Z)$ è simmetrico, esso è anche il polinomio di Schur $s_\lambda(X^d, Y^d, Z^d)$ nelle variabili $X^d, Y^d, Z^d$ relativo alla partizione $\lambda = (A/d - 2, B/d - 1, 0)$.

Dimostriamo ora l'irriducibilità di $T(X, Y, Z)$ in $\bar{\mathbb{F}}[X, Y, Z]$. Consideriamo il polinomio

$$I(X, Y, Z) \;=\; \frac{R(X, Y, Z)}{(X^d - Y^d)},$$

che ha una forma intermedia fra quella di $R(X, Y, Z)$ e $T(X, Y, Z)$ che useremo per estrarre informazione su $T(X, Y, Z)$, e che possiamo scrivere come

$$Z^A \prod_{\substack{\zeta^B = 1 \\ \zeta^d \neq 1}} (X - \zeta Y) - Z^B \prod_{\substack{\xi^A = 1 \\ \xi^d \neq 1}} (X - \xi Y) + X^B Y^B \prod_{\substack{\vartheta^{A-B} = 1 \\ \vartheta^d \neq 1}} (X - \vartheta Y). \tag{6.13}$$

Le $\zeta, \xi, \vartheta$ nella (6.13) sono quindi le radici $A$-esime, $B$-esime e $(A-B)$-esime dell'unità tranne quelle $d$-esime. Esse sono tutte distinte perché $p$ non divide $A, B, A-B$, e il massimo comun divisore fra due qualunque fra $A, B, A-B$ è precisamente $d$.

**Irriducibilità di $T(X,Y,Z)$.** La strategia che useremo per dimostrare l'irriducibilità di $T(X,Y,Z)$ è in un certo senso simile al criterio di irriducibilità di Eisenstein: sia infatti dato un polinomio $f(U) = \sum_{i=0}^{s} f_i U^i \in A[U]$ nell'indeterminata $U$ sull'anello $A$ di grado $s \geq r$ per qualche $r \geq 1$, tale che $f_r \notin P$ per un certo ideale primo $P \subset A$, $f_j \in P$ per $j < r$ e $f_0 \in P \setminus P^2$

$$f(U) \;=\; f_s U^s + \cdots + \underset{\not\in P}{f_r} U^r + \underset{\in P}{f_{r-1}} U^{r-1} + \cdots + \underset{\in P}{f_1} U + \underset{\in P\setminus P^2}{f_0}\ .$$

Allora se esso si fattorizza come $f(U) = g(U)h(U)$, uno dei suoi fattori, $g(U) = \sum g_i U^i$ poniamo, deve ereditare questa 'segnatura', e soddisfare $g_r \notin P$, $g_j \in P$ per $j < r$, e $g_0 \in P \setminus P^2$, e in particolare ha grado almeno $r$. Se $r$ è uguale al grado $s$ di $f$, allora questo fatto forza $h(U)$ ad avere grado zero, e questo è precisamente il criterio di Eisenstein. Il polinomio che studieremo non soddisfa le ipotesi per applicare il criterio Eisenstein, ma abbiamo in più che è simmetrico.

Chiameremo per comodità questa proprietà del polinomio $f(U)$ *segnatura di lunghezza $r$ relativa all'ideale $P$*, e siccome analogamente possiamo avere una tale segnatura nei primi $r$ coefficienti dei termini di grado alto invece che in quelli di grado basso

$$f(U) \;=\; \underset{\in P\setminus P^2}{f_s}\ U^s + \underset{\in P}{f_{s-1}} U^{s-1} + \cdots + \underset{\in P}{f_{s-r+1}} U^{s-r+1} + \underset{\not\in P}{f_{s-r}} U^{s-r} + \cdots + f_0,$$

parleremo rispettivamente di *segnatura alta* e *segnatura bassa*.

Supponiamo quindi che $T(X,Y,Z)$ si fattorizzi in $k > 1$ fattori irriducibili come $\prod_{i=1}^{k} G_i(X,Y,Z)$. Osservando la scrittura di

$$I(X,Y,Z) = T(X,Y,Z)(Z^d - X^d)(Z^d - Y^d)$$

nella (6.13), possiamo notare che i termini di grado $< B$ in $Z$ sono divisibili per $(X - \vartheta Y)$ per ogni $\vartheta^{A-B} = 1, \vartheta^d \neq 1$, e il termine noto è divisibile esattamente, mentre il coefficiente del termine in $Z^B$ non è divisibile. Esso possiede quindi una segnatura bassa di lunghezza $B$ relativa all'ideale $P_\vartheta = \langle X - \vartheta Y \rangle$ per ogni $\vartheta^{A-B} = 1, \vartheta^d \neq 1$, e possiamo osservare che analogamente possiede una segnatura alta di lunghezza $A - B$ relativa all'ideale $Q_\zeta = \langle X - \zeta Y \rangle$ per ogni $\zeta^B = 1, \zeta^d \neq 1$.

Gli unici casi in cui il polinomio non ha almeno una segnatura alta e una bassa si verifica quando o $d = B$ o $d = A - B$, e tratteremo a parte questi casi.

**Caso 1 (con $B \neq d$ e $A-B \neq d$).** I fattori che ereditano una segnatura bassa o alta devono avere grado in $Z$ rispettivamente almeno $B$ e $A-B$, e devono trovarsi fra i fattori di $T(X,Y,Z)$. Quindi siccome $T(X,Y,Z)$ ha grado in $Z$ pari a $A-2d$ deve trattarsi di un unico fattore 'grande', $G_1(X,Y,Z)$ poniamo, perché altrimenti il grado in $Z$ di $T(X,Y,Z)$ dovrebbe essere $\geq A$. Per lo stesso motivo questo fattore grande $G_1(X,Y,Z)$ deve ereditare *tutte* le segnature di $I(X,Y,Z)$ relative ai $P_\vartheta$ e $Q_\zeta$.

Abbiamo quindi che un qualunque prodotto non banale dei fattori rimanenti

$$\prod_{i\in I} G_i(X,Y,Z), \qquad \text{con } I \subseteq \{2,3,\dots,k\},\ I \neq \emptyset,$$

deve essere monico in $Z$, il temine noto deve essere della forma $X^rY^s$ per qualche $r,s \geq 0$, e in particolare non può essere simmetrico. Da questa osservazione segue che $T(X,Y,Z)$ non si può fattorizzare come prodotto di polinomi simmetrici, in altre parole l'azione del gruppo simmetrico $S_3$ come permutazione di $X,Y,Z$ sui fattori irridicibili $G_i(X,Y,Z)$ è transitiva.

L'azione del gruppo simmetrico non conserva il grado in $Z$, ma conserva però il grado totale, e i $G_i(X,Y,Z)$ devono quindi avere lo stesso grado totale. Abbiamo visto che il polinomio $G_1(X,Y,Z)$ ha grado in $Z$ almeno $A-B$, e il coefficiente di testa è divisibile per $B-d$ fattori in $X,Y$, gli $(X-\zeta Y)$. Esso ha quindi grado totale almeno $A-d$, mentre il grado totale di $T(X,Y,Z)$ è precisamente $A+B-3d$. Ma se ci fosse più di un fattore il grado si ritroverebbe ad essere almeno

$$2(A-d) \gneqq A+B-3d,$$

essendo $A > B$ e $d > 0$. Ma questo è assurdo, e quindi $G_1(X,Y,Z)$ deve essere l'unico fattore, e $T(X,Y,Z)$ è irriducibile.

**Caso 2 (con $B = d$ o $A-B = d$).** Mostriamo come prima cosa che il caso con $A-B=d$ si può ricondurre a quello con $B=d$. Siccome

$$\frac{\det\begin{pmatrix} X^A & Y^A & Z^A \\ X^d & Y^d & Z^d \\ 1 & 1 & 1 \end{pmatrix}}{\det\begin{pmatrix} X^{2d} & Y^{2d} & Z^{2d} \\ X^d & Y^d & Z^d \\ 1 & 1 & 1 \end{pmatrix}} = \frac{(XYZ)^A \cdot \det\begin{pmatrix} 1 & 1 & 1 \\ X^{-A+d} & Y^{-A+d} & Z^{-A+d} \\ X^{-A} & Y^{-A} & Z^{-A} \end{pmatrix}}{(XYZ)^{2d} \cdot \det\begin{pmatrix} 1 & 1 & 1 \\ X^{-d} & Y^{-d} & Z^{-d} \\ X^{-2d} & Y^{-2d} & Z^{-2d} \end{pmatrix}},$$

abbiamo che

$$T_{A,d}(X,Y,Z) \;=\; (XYZ)^{A-2d} \cdot T_{A,A-d}(X^{-1},Y^{-1},Z^{-1}),$$

e quindi una fattorizzazione di $T_{A,A-d}(X^{-1},Y^{-1},Z^{-1}) \in \bar{\mathbb{F}}[X^{-1},Y^{-1},Z^{-1}]$ permette di ricavare una fattorizzazione di $T_{A,d}(X,Y,Z)$ moltiplicando i fattori per fattori opportuni di $(XYZ)^{A-2d}$. L'unico caso in cui una fattorizzazione

non banale può diventare una fattorizzazione banale si ha quando uno dei fattori di $T_{A,A-d}(X^{-1}, Y^{-1}, Z^{-1})$ è un monomio $X^{-r}Y^{-s}Z^{-t}$ con $r, s, t$ non tutti nulli, ma questo è impossibile data la definizione di $T_{A,A-d}(X, Y, Z)$.

Ci basta quindi dimostrare l'irriducibilità di $T_{A,d}(X, Y, Z)$, e procederemo dimostrando che la varietà che esso definisce in $\mathbb{P}^2(\bar{\mathbb{F}})$ è non-singolare. Da questo segue immediatamente l'irriducibilità, perché altrimenti dei fattori non banali definirebbero varietà proiettive con intersezione non vuota (per il teorema di Bézout, si veda ad esempio [Har77]), e su un punto di tale intersezione le derivate del prodotto dei fattori dovrebbero forzatamente annullarsi.

Consideriamo come prima cosa il caso con $d = 1$, e poniamo per comodità di notazione $A = k$ per qualche intero $k \geq 2$. Se $k = 2$ allora $T_{k,1}(X, Y, Z) = 1$ e non c'è nulla da dimostrare, per cui possiamo supporre $k > 2$. È facile osservare con un conto diretto, o ad esempio grazie all'identità di Jacobi-Trudi nella (3.3), che $T_{k,1}(X, Y, Z)$ è la funzione simmetrica completa $h_{k-2}(X, Y, Z)$, cioè la somma di tutti i mononomi di grado $k - 2$. Abbiamo quindi che

$$\left(\frac{\partial}{\partial X} + \frac{\partial}{\partial Y} + \frac{\partial}{\partial Z}\right) T_{k,1}(X, Y, Z) \;=\; k \cdot T_{k-1,1}(X, Y, Z)$$

è uguale a $k$ volte la somma dei monomi di grado $k - 3$, perché il contributo al monomio $X^r Y^s Z^t$, con $r, s, t \geq 0, r + s + t = k - 3$, è dato da

$$\frac{\partial}{\partial X} X^{r+1} Y^s Z^t + \frac{\partial}{\partial Y} X^r Y^{s+1} Z^t + \frac{\partial}{\partial Z} X^r Y^s Z^{t+1} \;=\; k \cdot X^r Y^s Z^t.$$

Supponiamo quindi che esista un punto con coordinate omogenee $(x, y, z)$ in cui sia soddisfatto il sistema

$$\begin{cases} T_{k,1}(X, Y, Z) \;=\; 0, \\ \frac{\partial}{\partial X} T_{k,1}(X, Y, Z) \;=\; 0, \\ \frac{\partial}{\partial Y} T_{k,1}(X, Y, Z) \;=\; 0, \\ \frac{\partial}{\partial Z} T_{k,1}(X, Y, Z) \;=\; 0. \end{cases}$$

Deve allora anche annullarsi (ricordiamo che $k$ è primo con la caratteristica per ipotesi)

$$\begin{aligned} T_{k,1}(X, Y, Z) - \frac{X}{k} \cdot \left(\frac{\partial}{\partial X} + \frac{\partial}{\partial Y} + \frac{\partial}{\partial Z}\right) T_{k,1}(X, Y, Z) \\ = \sum_{i=0}^{k-2} Y^i Z^{k-2-i} \;=\; \prod_{\substack{\varphi^{k-1}=1 \\ \varphi \neq 1}} (Y - \varphi Z). \end{aligned}$$

Ricordando che per ipotesi anche $k - 1$ è primo con la caratteristica, in un tale punto si deve quindi avere $y = \varphi z$ per qualche $\varphi^{k-1} = 1, \varphi \neq 1$. Siccome possiamo ripetere il conto con $Y, Z$ al posto di $X$, abbiamo che $x, y, z$ differiscono tutti per radici $(k - 1)$-esime dell'unità diverse 1.

Un tale punto è quindi della forma $(\varphi t, \psi t, t) \in \mathbb{P}^2\bar{\mathbb{F}}$, con $\varphi^{k-1} = \psi^{k-1} = 1$ e $\varphi, \psi, 1$ distinti, e $t \neq 0$. Ma poiché

$$\frac{\partial}{\partial Z} T_{k,1}(X,Y,Z) \;=\; \frac{\partial}{\partial Z} \frac{R(X,Y,Z)}{V(X,Y,Z)} \;=$$
$$\frac{kZ^{k-1}(X-Y) - (X^k - Y^k)}{V(X,Y,Z)} - R(X,Y,Z)\frac{\frac{\partial}{\partial Z}V(X,Y,Z)}{V(X,Y,Z)^2},$$

dove abbiamo chiamato come al solito $V(X,Y,Z)$ il determinante di Vandermonde e $R(X,Y,Z)$ il determinante della (6.12) con $A = k, B = 1$, otteniamo valutando nel nostro punto $(\varphi t, \psi t, t)$ che, tenendo conto che $R(\varphi t, \psi t, t) = 0$,

$$\left.\frac{\partial}{\partial Z} T_{k,1}(X,Y,Z)\right|_{(\varphi t, \psi t, t)} \;=\; (k-1)\frac{t^{k-3}}{(1-\varphi)(1-\psi)} \;\neq\; 0.$$

Consideriamo ora il caso in cui $d > 1$, e se poniamo $A = kd$ questo vuol dire dimostrare l'irriducibilità di $T_{kd,d}(X,Y,Z) \;=\; T_{k,1}(X^d, Y^d, Z^d)$, e vedremo che anch'esso definisce una varietà proiettiva non-singolare. Consideriamo quindi il sistema

$$\begin{cases} T_{k,1}(X^d, Y^d, Z^d) \;=\; 0, \\ dX^{d-1} \cdot \frac{\partial}{\partial X} T_{k,1}(X^d, Y^d, Z^d) \;=\; 0, \\ dY^{d-1} \cdot \frac{\partial}{\partial Y} T_{k,1}(X^d, Y^d, Z^d) \;=\; 0, \\ dZ^{d-1} \cdot \frac{\partial}{\partial Z} T_{k,1}(X^d, Y^d, Z^d) \;=\; 0. \end{cases}$$

È ora chiaro che in un punto $(x,y,z)$ con $x,y,z$ tutti $\neq 0$ questo sistema non può essere soddisfatto, altrimenti $(x^d, y^d, z^d)$ dovrebbe essere un punto singolare della varietà definita da $T(X,Y,Z)$.

Supponiamo quindi che esso sia soddisfatto in un punto di coordinate omogenee $(x,y,z)$ con $y = 0$, poniamo. Ma in un tale punto si deve anche annullare

$$T_{k,1}(X^d, 0, Z^d) \;=\; \prod_{\substack{\varphi^{k-1}=1 \\ \varphi \neq 1}} (X^d - \varphi Z^d),$$

e quindi le potenze $x^d$ e $z^d$ differiscono per una radice $(k-1)$-esima dell'unità diversa da 1. Questa osservazione ci dice che $(x^d, y^d, z^d)$ è della forma $(\varphi t, 0, t)$ per $\varphi^{k-1} = 1, \varphi \neq 1$ e $t \neq 0$, e ci basta quindi vedere che

$$\left.\frac{\partial}{\partial Z} T_{k,1}(X,Y,Z)\right|_{(\varphi t, 0, t)} \;=\; (k-1)\frac{t^{k-3}}{1-\varphi} \;\neq\; 0.$$

**Conclusione della dimostrazione.** Mostriamo ora come dall'irriducibilità del polinomio $T(X,Y,Z)$, che è una relazione di dipendenza algebrica per $x,y,z$, segua la soluzione del problema. Ricordiamo che stavamo supponendo di avere soddisfatte le relazioni

$$x^m + y^m - z^m \;=\; w^m, \qquad \text{per } m = a, b, c \tag{6.14}$$

per qualche $w, z$ distinti da $x, y$.

Iniziamo osservando che $z$ deve essere trascendente su $\bar{\mathbb{F}}(x)$. Supponiamo infatti il contrario: $y$ annulla il polinomio $R(x, U, z)$ visto come polinomio in $U$ su $\bar{\mathbb{F}}(x, z)$, e quindi $T(x, U, z)$ dato che $x, y, z$ non hanno rapporto costante. Ma $T(x, U, z)$ non può essere identicamente nullo perché il termine noto in $U$ è della forma $\prod(x - \vartheta_i z)$, e $x, z$ non differiscono per una costante.

Abbiamo allora ottenuto una relazione di dipendenza algebrica non banale di $y$ su $\bar{\mathbb{F}}(x, z)$, il quale sarebbe quindi anche algebrico su $\bar{\mathbb{F}}(x)$, e questo è assurdo dato che $x, y$ sono indipendenti per ipotesi. Si noti a beneficio di riferimenti futuri che allo stesso modo anche $w$ deve essere trascendente su $\bar{\mathbb{F}}(x)$.

Possiamo ora definire un isomorfismo $\varepsilon : \bar{\mathbb{F}}(x, y) \to \bar{\mathbb{F}}(x, z)$ come l'unico isomorfismo che fissa le costanti e tale che

$$x \mapsto x, \qquad y \mapsto z.$$

Dato che $z$ è una radice del polinomio irriducibile $T(x, y, U)$ in $U$, possiamo estendere $\varepsilon$ a $\bar{\mathbb{F}}(x, y, z)$ mandando $z$ in una qualunque radice di

$$\varepsilon T(x, y, U) \;=\; T(\varepsilon x, \varepsilon y, U) \;=\; T(x, z, U) \;=\; T(x, U, z),$$

grazie al fatto che $T(X, Y, Z)$ è un polinomio simmetrico. Possiamo in particolare definire $\varepsilon(z) = y$.

Estendiamo quindi $\varepsilon$ alla chiusura algebrica di $\bar{\mathbb{F}}(x, y, z)$, e sia $u = \varepsilon(w)$ (di fatto $w \in \bar{\mathbb{F}}(x, y, z)$, quindi l'estensione non è realmente necessaria). Applicando $\varepsilon$ alle (6.14) abbiamo quindi che

$$x^m + z^m - y^m \;=\; u^m, \qquad \text{per } m = a, b, c. \tag{6.15}$$

Sommando le (6.14) e (6.15) otteniamo

$$2x^m \;=\; w^m + u^m, \qquad \text{per } m = a, b, c \tag{6.16}$$

(ricordiamo che le ipotesi escludono la possibilità che la caratteristica sia 2), e eliminando $u$ dalle prime due delle 6.16 abbiamo che

$$(2x^a - w^a)^b - (2x^b - w^b)^a \;=\; 0. \tag{6.17}$$

Questa è una relazione di dipendenza algebrica non banale di $w$ su $\bar{\mathbb{F}}(x)$, che avevamo però detto essere trascendente su $\bar{\mathbb{F}}(x)$, e questo assurdo conclude la dimostrazione. □

Una riflessione sulle ipotesi richieste nella proposizione 6.3.8 è d'obbligo. Consideriamo solo casi in cui $a, b, c$ sono tutti primi con $p$, a cui la 6.3.7 permette di ricondursi. Esperimenti al computer mostrano che in molte delle situazioni in cui $p$ divide le differenze $a - c, a - b, b - c$ i polinomi di Newton $N_a, N_b, N_c$ riescono comunque a generare l'intero campo simmetrico.

Un'analisi attenta della dimostrazione mostra che ad esempio nel *Caso 1* della dimostrazione non è realmente necessaria l'ipotesi che $A = a - c$ sia primo con

$p$ (nel *Caso 2* quest'ipotesi è invece importante e necessaria, come mostreremo più avanti con dei controesempi), abbiamo rinunciato a inserire questo leggero indebolimento delle ipotesi nella proposizione per non complicare eccessivamente l'enunciato.

Inoltre nel passo conclusivo non è realmente necessario che $T(X, Y, Z)$ sia irriducibile, lo stesso discorso si può tranquillamente ripetere sapendo che esso si fattorizza in fattori irriducibili *tutti simmetrici*. Si possono trovare esempi in cui precisamente questo succede (ad esempio $T_{7,3}(X, Y, Z)$ in caratteristica 2), ma sembra complicato dimostrare questo fatto per qualche classe di polinomi.

Cionondimeno se non si richiede che $a-c, a-b, b-c$ siano primi con $p$ esistono esempi in cui $N_a, N_b, N_c$ non generano l'intero campo simmetrico. Una famiglia di casi in cui questo succede che ora esibiamo è collegata alla fattorizzazione di $T_{p^r,1}(X, Y, Z)$, per $r \geq 1$. Abbiamo infatti che

$$T_{p^r,1}(X, Y, Z) \;=\; \prod_{\substack{\alpha \in \mathbb{F}_{p^r} \\ \alpha \neq 0,1}} (Z - \alpha X + (\alpha - 1)Y),$$

come mostreremo successivamente insieme ad altri esempi di fattorizzazioni dei polinomi $T_{A,B}(X, Y, Z)$, con $A, B, A - B$ non tutti primi con $p$.

**Una famiglia di controesempi.** Sia $p$ un primo diverso da 2, e per ogni $\eta \in \mathbb{F}_p$ consideriamo il polinomio

$$P_\eta(X) \;=\; X^2 - 2\eta X + \eta. \tag{6.18}$$

Si noti che una radice di $P_\eta(X)$ non può essere radice di $P_\kappa(X)$ per $\eta \neq \kappa$, perché l'equazione

$$X^2 - 2\eta X + \eta \;=\; 0$$

vista come un'equazione in $\eta$ per $X$ fissato determina univocamente $\eta$, eccetto che per $X = 1/2$, che non è mai soluzione perché $P_\eta(1/2) = 1/4 \neq 0$ per ogni $\eta \in \mathbb{F}_p$. Inoltre ogni $P_\eta(X)$ ha radici distinte a meno che non si annulli il discriminante $4(\eta^2 - \eta)$, e questo può succedere solo per $\eta = 0, 1$.

Quindi al variare di $\eta \in \mathbb{F}_p$ i $P_\eta(X)$ hanno in totale precisamente $2p - 2$ radici distinte, e $2p - 2 > p$ per $p \geq 3$. Quindi in particolare siccome in $\mathbb{F}_p$ ci sono soltanto $p$ elementi una di queste radici apparterrà a $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$, e da questo segue che almeno un $P_\eta(X)$ deve essere irriducibile per qualche $\eta \in \mathbb{F}_p$.

Sia quindi $P_\eta(X)$ irriducibile, e $\alpha, \beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ le sue radici, le quali vengono scambiate dall'automorfismo di Frobenius $\mathscr{F}$

$$\mathscr{F} : \bar{\mathbb{F}} \to \bar{\mathbb{F}}, \qquad \tau \mapsto \tau^p.$$

In particolare esse vengono scambiate applicando $\mathscr{F}$ un numero dispari di volte, e quindi

$$\alpha^{p^{2k+1}} \;=\; \beta, \qquad \beta^{p^{2k+1}} \;=\; \alpha$$

per ogni intero $k$.

Si noti che per costruzione abbiamo che

$$2\alpha\beta \;=\; 2\eta \;=\; \alpha+\beta.$$

Se ora poniamo

$$z \;=\; \alpha x+(1-\alpha)y, \qquad w \;=\; (1-\alpha)x+\alpha y, \tag{6.19}$$

abbiamo che per ogni $k$ intero

$$\begin{aligned} z^{p^{2k+1}+1}+w^{p^{2k+1}+1} \;&=\; z^{p^{2k+1}}\cdot z + w^{p^{2k+1}}\cdot w \\ &= (\alpha x+(1-\alpha)y)^{p^{2k+1}}(\alpha x+(1-\alpha)y) \\ &\quad + ((1-\alpha)x+\alpha y)^{p^{2k+1}}((1-\alpha)x+\alpha y) \\ &= (\beta x^{p^{2k+1}}+(1-\beta)y^{p^{2k+1}})(\alpha x+(1-\alpha)y) \\ &\quad + ((1-\beta)x^{p^{2k+1}}+\beta y^{p^{2k+1}})((1-\alpha)x+\alpha y) \\ &= (2\alpha\beta-\alpha-\beta+1)(x^{p^{2k+1}+1}+y^{p^{2k+1}+1}) \\ &\quad + (\beta+\alpha-2\beta\alpha)(x^{p^{2k+1}}y+xy^{p^{2k+1}}) \\ &= x^{p^{2k+1}+1}+y^{p^{2k+1}+1}. \end{aligned}$$

Quindi se prendiamo ora $a,b,c$ uguali a $p^{2k+1}+1, p^{2\ell+1}+1, 1$ per $k>\ell\geq 0$, abbiamo trovato la coppia 'alternativa' degli $z,w$ nella (6.19) che soddisfa le (6.10), e quindi $N_a, N_b, N_c$ non possono generare l'intero campo simmetrico.

È anche possibile calcolare quanto è il grado del campo simmetrico sul campo generato da $N_{p^r+1}, N_{p^s+1}, N_1$ per $r>s\geq 0$: infatti basta contare gli $z$ distinti che insieme a un qualche $w$ soddisfano la (6.10), ed in particolare quelli diversi da $x,y$ vanno cercati fra le radici di $T_{p^{r-s},1}(x,y,U)^{p^s}$ visto come polinomio in $U$, che per la fattorizzazione di $T_{p^{r-s},1}(x,y,U)$ in termini di primo grado devono essere della forma $z=\alpha x+(1-\alpha)y$ per $\alpha\in\mathbb{F}_{p^{r-s}}$, $\alpha\neq 1,0$.

Inoltre siccome $w$ è univocamente determinato come $w=(1-\alpha)x+\alpha y$, se poniamo $\beta=\alpha^{p^r}$ allora $\alpha,\beta$ devono soddisfare $2\alpha\beta=\alpha+\beta$, e sono radici della (6.18) per qualche $\eta\in\bar{\mathbb{F}}_p$. Se $\alpha=\beta$, allora $\alpha=0,1$, per cui consideriamo i casi in cui $\alpha\neq\beta$. Siccome anche per $\gamma=\alpha^{p^s}$ dobbiamo avere $2\alpha\gamma=\alpha+\gamma$, segue che $\beta=\gamma=\alpha^{p^s}$

Ora, un'importante osservazione è la seguente: $\mathscr{F}^s$ (ovvero $\mathscr{F}$ applicato $s$ volte) manda $\alpha$ in $\beta$, e inoltre applicato ai coefficienti manda il polinomio $P_\eta(X)$ in un polinomio della stessa forma, $P_\kappa(X)$ poniamo. Siccome si deve avere $P_\eta(\beta)=P_\kappa(\beta)=0$, allora $\eta=\kappa$, e da questo segue che simmetricamente $\beta$ viene mandato in $\alpha$ da $\mathscr{F}^s$, mentre $\eta$ resta fisso. Siccome lo stesso vale per $r$, abbiamo che $\eta$ deve essere lasciato fisso da $\mathscr{F}^m$ per $m=(r,s)$, e quindi $\eta\in\mathbb{F}_{p^m}$, mentre $\alpha$ ha grado precisamente 2 su $\mathbb{F}_{p^m}$, in altre parole $\alpha\in\mathbb{F}_{p^{2m}}\setminus\mathbb{F}_{p^m}$.

Distinguiamo ora due casi: se $2m\nmid(r-s)$, allora $\mathbb{F}_{p^{2m}}\cap\mathbb{F}_{p^{r-s}}=\mathbb{F}_{p^m}$, e quindi gli unici $\alpha$ ammissibili sono $\alpha=0,1$, e $N_{p^r+1}, N_{p^s+1}, N_1$ generano l'intero campo simmetrico.

Se invece $2m \mid (r-s)$, allora $\mathbb{F}_{p^{2m}} \subset \mathbb{F}_{p^{r-s}}$, e ci basta contare le soluzioni di

$$X^2 - 2\eta X + \eta = 0, \qquad X \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$$

al variare di $\eta \in \mathbb{F}_{p^m}$. Un conto identico a quello svolto all'inizio del paragrafo mostra che il numero totale di soluzioni in $\mathbb{F}_{p^{2m}}$ è $2p^m - 2$, mentre ogni $X \in \mathbb{F}_{p^m}$ è soluzione eccetto che per $X = 1/2$ che non può esserlo, e tali soluzioni sono quindi $p^m - 1$. Quindi il numero di soluzioni in $\mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ è precisamente $p^m - 1$. Contando anche le soluzioni banali $\alpha = 0, 1$ e dividendo per due abbiamo il grado.

Concludendo, se $r > s \geq 1$ e $m = (r, s)$, il grado del campo simmetrico $S$ sul campo generato da $N_{p^r+1}, N_{p^s+1}, N_1$ è

$$[S : \mathcal{N}_{p^r+1, p^s+1, 1}] \;=\; \begin{cases} 1 & \text{se } 2m \nmid (r-s) \\ \frac{p^m+1}{2} & \text{se } 2m \mid (r-s) \end{cases}$$

È facile verificare che anche in caratteristica 2 è possibile costruire una famiglia analoga di controesempi grazie alla coppia

$$z \;=\; \alpha x + (1-\alpha) y, \qquad w \;=\; (1-\alpha) x + \alpha y,$$

dove $\alpha \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$ è una radice terza dell'unità, ma in questo caso è necessario prendere esponenti $a, b, c$ della forma $2^{2l} + 1, 2^{2k} + 1, 1$, in cui compaiono le potenze *pari* di 2.

Infatti si noti che la condizione $2\alpha\beta = \alpha + \beta$ in caratteristica 2 equivale a imporre $\alpha = \beta$ (cosa che in caratteristica $\neq 2$ non può mai succedere eccetto che per $\alpha = 0, 1$).

Per calcolare il grado di $S$ su $N_{2^r+1}, N_{2^s+1}, N_1$ osserviamo che ci basta contare gli $\alpha$ lasciati fissi da $\mathscr{F}^s$ e $\mathscr{F}^r$, che sono gli elementi di $\mathbb{F}_{2^m}$, per $m = (r, s)$. Dividendo per due il grado dell'estensione è quindi

$$[S : \mathcal{N}_{2^r+1, 2^s+1, 1}] \;=\; 2^{m-1}.$$

**Fattorizzazioni di alcune classi di $T(X, Y, Z)$.** Mostriamo ora che

$$T_{p^r,1}(X, Y, Z) \;=\; \prod_{\substack{\alpha \in \mathbb{F}_{p^r} \\ \alpha \neq 0,1}} (Z - \alpha X + (\alpha - 1) Y). \tag{6.20}$$

Per verificare l'uguaglianza, è sufficiente osservare che, se come al solito $V(X, Y, Z)$ è il determinante di Vandemonde, allora

$$T_{p^r,1}(X, Y, Z) \cdot V(X, Y, Z) \;=\; \det \begin{pmatrix} X^{p^r} & Y^{p^r} & Z^{p^r} \\ X & Y & Z \\ 1 & 1 & 1 \end{pmatrix},$$

e il determinante si annulla ponendo $Z = \alpha X - (\alpha - 1) Y$ per ogni $\alpha \in \mathbb{F}_{p^r}$. Bisogna escludere i fattori $(Z - \alpha X + (\alpha - 1) Y)$ con $\alpha = 0, 1$ che sono tutti e soli

quelli che dividono $V(X,Y,Z)$, e i rimanenti $p^r-2$ fattori corrispondono a dei fattori di $T_{p^r,1}(X,Y,Z)$ il quale ha grado precisamente $p^r-2$. Per concludere basta quindi verificare che la costante di cui differiscono i due membri della (6.20) è precisamente 1, e questo è vero perché essi sono entrambi monici in $Z$.

Un'altra interessante fattorizzazione è la seguente:

$$T_{p^{2r}-1,p^r-1}(X,Y,Z) \;=\; \prod_{\substack{\alpha,\beta\in\mathbb{F}_{p^r}\\ \alpha,\beta\neq 0}} (Z-\alpha X-\beta Y). \tag{6.21}$$

Infatti se sostituiamo $Z=\alpha X+\beta Y$, abbiamo che per ogni $\alpha,\beta\in\mathbb{F}_{p^r}$ si annulla

$$T_{p^{2r}-1,p^r-1}(X,Y,Z)\cdot V(X^{p^r-1},Y^{p^r-1},Z^{p^r-1})\cdot XYZ \;= \\ =\; \det\begin{pmatrix} X^{p^{2r}} & Y^{p^{2r}} & Z^{p^{2r}} \\ X^{p^r} & Y^{p^r} & Z^{p^r} \\ X & Y & Z \end{pmatrix},$$

e escludendo i fattori $(Z-\alpha X+\beta Y)$ in cui $\alpha=0$ o $\beta=0$ ci rimangono $p^{2r}-2p^r+1$ fattori, che è precisamente il grado di $T_{p^{2r}-1,p^r-1}(X,Y,Z)$. Per avere l'uguaglianza, ci basta quindi osservare come sopra che entrambi i fattori sono monici in $Z$.

Può essere interessante osservare che tutte queste sostituzioni $Z=\alpha X+\beta Y$, per $\alpha,\beta\in\mathbb{F}_{p^r}$, annullano anche il determinante

$$\det\begin{pmatrix} X^{p^s} & Y^{p^s} & Z^{p^s} \\ X^{p^t} & Y^{p^t} & Z^{p^t} \\ X & Y & Z \end{pmatrix}$$

per ogni $s>t\geq 1$ che siano entrambi multipli di $r$.

Questo determinante è un multiplo di $T_{p^s-1,p^t-1}(X,Y,Z)$, e differisce da esso per un fattore del tipo $V(X^{p^m-1},Y^{p^m-1},Z^{p^m-1})\cdot XYZ$, che può annullarsi solo se nella sostituzione abbiamo posto $\alpha$ o $\beta$ uguale a 0.

Abbiamo quindi che se $s>t\geq 1$ e sono entrambi multipli di $r$, allora

$$T_{p^{2r}-1,p^r-1}(X,Y,Z) \;\Big|\; T_{p^s-1,p^t-1}(X,Y,Z).$$

Siccome di fatto entrambi questi polinomi sono polinomi in $X^{p^r-1}$, $Y^{p^r-1}$, $Z^{p^r-1}$, abbiamo anche la seguente divisibilità

$$T_{p^r+1,1}(X,Y,Z) \;\Big|\; T_{\frac{p^s-1}{p^r-1},\frac{p^t-1}{p^r-1}}(X,Y,Z).$$

**Irriducibilità di $T_{p^r+1,1}(X,Y,Z)$.** Mostriamo ora che $T_{p^r+1,1}(X,Y,Z)$, che abbiamo scoperto essere un fattore di una famiglia di $T(X,Y,Z)$, è irriducibile per $r\geq 1$. Si noti che tali polinomi non rientrano nella famiglia di $T(X,Y,Z)$ che abbiamo visto essere irriducibili nel *Caso 2* della 6.3.8 dimostrando che la

varietà proiettiva da essi definita è non-singolare, infatti i punti di coordinate omogenee $(t,t,t)$ per $t \neq 0$ sono punti singolari per $T_{p^r+1,1}(X,Y,Z)$.

Useremo la seguente strategia[2]: sia

$$f(Z) \;=\; f_k Z^k + \cdots + f_1 Z + f_0 \;\in k[X_1,\ldots,X_n,Z]$$

un polinomio omogeneo in $X_1,\ldots,X_n,Z$, che vediamo come polinomio in $Z$ a coefficienti nell'anello $k[X_1,\ldots,X_n]$. Supponiamo che esista un polinomio irriducibile $P \in k[X_1,\ldots,X_n]$ tale che $f_0$ è una potenza di $P$, mentre $P \nmid f_1$. Allora $f(Z)$ è irriducibile in $k[X_1,\ldots,X_n,Z]$.

Sia infatti $f(Z) = a(Z)b(Z)$ una fattorizzazione, con $a(Z) = \sum_i a_i Z^i$, $b(Z) = \sum_i b_i Z^i$, entrambi di grado $\geq 1$ in $Z$. Abbiamo allora che

$$f_0 \;=\; a_0 b_0, \qquad f_1 \;=\; a_1 b_0 + a_0 b_1.$$

Siccome la fattorizzazione è non banale e i fattori sono omogenei, $a_0$ e $b_0$ devono essere potenze non banali di $P$, ma questo è assurdo perché avremmo allora che $P \mid f_1$. Quindi $f(Z)$ non può fattorizzarsi in fattori di grado $\geq 1$ in $Z$, e per vedere che non può fattorizzarsi in $k[X_1,\ldots,X_n,Z]$ basta vedere che è primitivo come polinomio in $Z$, ma questo è ovvio dato che $P \nmid f_1$.

Tornando a $T_{p^r+1,1}(X,Y,Z)$, sappiamo che esso è la somma dei monomi di grado $p^r-1$, quindi se visto come polinomio in $Z$ il termine noto è

$$\sum_{i=0}^{p^r-1} X^i Y^{p^r-1-i} \;=\; \frac{X^{p^r}-Y^{p^r}}{X-Y} \;=\; (X-Y)^{p^r-1}.$$

Il coefficiente del termine in $Z$ è invece

$$\sum_{i=0}^{p^r-2} X^i Y^{p^r-2-i} \;=\; \frac{X^{p^r-1}-Y^{p^r-1}}{X-Y} \;=\; \prod_{\substack{\zeta^{p^r-1}=1 \\ \zeta\neq 1}} (X-\zeta Y).$$

Abbiamo quindi che il termine noto è una potenza di $X-Y$, e questo è un fattore che non compare nel coefficiente di $Z$. Ne segue l'irriducibilità applicando la strategia sopra esposta.

## 6.4 Il problema in più variabili

In questa sezione proponiamo alcuni risultati relativi al caso in più variabili del problema che stiamo trattando.

[2]Siccome questa strategia richiede ipotesi pressoché opposte di quelle del criterio di Eisenstein, essa può forse meritare il nome di criterio di Nietsnesie.

### 6.4.1 Teorema di Kakeya

Il seguente risultato risale a Kakeya ([Kak25],[Kak27]) e fornisce una curiosa condizione sufficiente perché in $n$ variabili l'intero campo simmetrico sia generato da precisamente $n$ polinomi di Newton.

Una complicata costruzione esplicita fu elaborata da Nakamura ([Nak27]), presentiamo qua l'elegante dimostrazione di Foulkes ([Fou56]) che fornisce al tempo stesso una costruzione esplicita relativamente semplice, e che utilizza gli strumenti combinatori sviluppati nei capitoli precedenti.

Ritorniamo momentaneamente alla notazione usata precedentemente che meglio si adatta a questo risultato e alla sua dimostrazione soprattutto. Se $n$ è il numero di variabili e $r$ un intero, indichiamo quindi l'$r$-esimo polinomio di Newton, o somma di potenze, come

$$p_r \;=\; x_1^r + \cdots + x_n^r.$$

**Teorema 6.4.2** (Kakeya)**.** *Sia $\alpha = (\alpha_1, \ldots, \alpha_n)$ una tupla di interi positivi distinti tali che il complementare nei naturali positivi*

$$C_\alpha \;=\; \mathbb{N}^+ \setminus \{\alpha_1, \ldots, \alpha_n\}$$

*è chiuso rispetto all'addizione. Allora $p_{\alpha_1}, \ldots, p_{\alpha_n}$ generano l'intero campo delle funzioni simmetriche in $n$ variabili.*

*Dimostrazione.* Ricordiamo come si caratterizza la scrittura delle funzioni di Schur $s_\lambda$ in termini delle somme di potenze $p_\rho$. Abbiamo che

$$\langle s_\lambda, p_\rho \rangle \;=\; \chi_\rho^\lambda,$$

per ogni coppia di partizioni $\lambda, \rho$ di $m$, dove $\chi_\rho^\lambda$ è il valore del carattere irriducibile $\chi^\lambda$ del gruppo simmetrico $S_m$ associato a $\lambda$ valutato in un elemento che ha decomposizione in cicli di tipo $\rho$.

Siccome gli $s_\lambda$ sono ortonormali e i $p_\rho$ ortogonali rispetto al prodotto scalare, abbiamo tenendo conto della (3.13) che

$$\begin{aligned} p_\rho &= \sum_{|\lambda|=m} \chi_\rho^\lambda s_\lambda, \\ s_\lambda &= \sum_{|\rho|=m} z_\rho^{-1} \chi_\rho^\lambda p_\rho. \end{aligned} \tag{6.22}$$

Richiamiamo inoltre la caratterizzazione combinatoria dei $\chi_\rho^\lambda$ ricavata nella (3.8). Ricordiamo che l'altezza di una striscia di bordo, definita nella sezione 1.3, è il numero di righe occupate meno uno. Se $S = (\lambda^{(0)}, \lambda^{(1)}, \ldots, \lambda^{(k)})$ è una successione di partizioni tali che $\lambda^{(i)} \subset \lambda^{(i-1)}$ e $\lambda^{(i)}/\lambda^{(i-1)}$ è una striscia di bordo per ogni $i = 1, \ldots, k$, allora $ht(S)$ è definito come

$$ht(S) \;=\; \sum_i ht(\lambda^{(i)}/\lambda^{(i-1)}).$$

Sia $k = \ell(\rho)$. Abbiamo allora che

$$\chi^\lambda_\rho \;=\; \sum_S (-1)^{ht(S)}, \tag{6.23}$$

dove la somma è su tutte le successioni di partizioni $S = (\lambda^{(0)}, \lambda^{(1)}, \dots, \lambda^{(k)})$ tali che $0 = \lambda^{(0)} \subset \lambda^{(1)} \subset \cdots \subset \lambda^{(k)} = \lambda$, e in cui ciascun $\lambda^{(i)}/\lambda^{(i-1)}$ è una striscia di bordo di lunghezza $\rho_i$, per ogni $i = 1, \dots, k$.

Inoltre una conseguenza ricavata alla fine della sezione 3.1.4 fondamentale per questa dimostrazione è la seguente: nel valutare la (6.23) è possibile rimpiazzare la partizione $\rho$ con una qualunque sua permutazione $w(\rho)$, con $w \in S_k$.

In particolare siccome si richede che ogni tupla $S = (\lambda^{(0)}, \lambda^{(1)}, \dots, \lambda^{(k)})$ soddisfi $\lambda^{(k)} = \lambda$ e che $\lambda^{(k)}/\lambda^{(k-1)}$ sia una striscia di bordo di lunghezza $\rho_k$, abbiamo che tale somma deve essere zero se non è possibile staccare dalla partizione $\lambda$ una striscia di bordo di lunghezza $\rho_i$ per qualche $i = 1, \dots, k$.

Quindi, vedendo $p_\rho = p_{\rho_1} p_{\rho_2} \dots$ come un monomio nelle somme di potenze $p_r$, abbiamo che la scrittura di $s_\lambda$ nella (6.22) è un polinomio nei $p_r$ in cui compaiono *soltanto i $p_r$ tali che è possibile staccare una striscia di bordo di lunghezza $r$ dal diagramma $\lambda$*.

Come abbiamo visto nella sezione 1.7, se $\beta = \lambda + \delta$ è la partizione stretta ottenuta sommando $\delta = (\ell(\lambda) - 1, \dots, 1, 0)$ a $\lambda$, staccare una striscia di bordo lunga $r$ da $\lambda$ equivale a sottrarre $r$ da una parte di $\beta$, e riordinare la partizione *stretta* ottenuta in ordine decrescente. In particolare è possibile staccare una striscia di bordo lunga $r$ da $\lambda$ se e solo se esiste qualche $\beta_i$ per $1 \le i \le \ell(\beta)$ tale che $\beta_i - r \ge 0$, e $\beta_i - r$ non coincide con nessuna altra parte di $\beta$.

Ci serve inoltre osservare che in un numero finito di variabili la funzione di Schur $s_\lambda(x_1, \dots, x_n)$ si annulla se e solo se $\ell(\lambda) \ge n + 1$, come è possibile verificare con un conto diretto o usando la più forte prop. 3.3.1.

Possiamo ora dimostrare il teorema di Kakeya. Se $\alpha = (1, 2, \dots, n)$ non c'è nulla da dimostrare, in quanto le (2.9') mostrano che è possibile ottenere induttivamente le funzioni simmetriche elementari $e_1, \dots, e_n$, le quali generano il campo simmetrico in $n$ variabili.

In caso contrario, sia $t$ il minimo intero dell'insieme $\mathbb{N}^+ \setminus \{\alpha_1, \dots, \alpha_n\}$. Sia $\beta = \alpha \cup (t)$, e osserviamo che anche il complementare di $\beta$

$$C_\beta \;=\; \mathbb{N}^+ \setminus \{\beta_1, \dots, \beta_{n+1}\}$$

è chiuso rispetto all'addizione.

Se il complementare $C_\gamma$ di una qualunque partizione stretta $\gamma$ è chiuso rispetto all'addizione, gli unici interi positivi che è possibile sottrarre da una qualche parte di $\gamma$ ottenendo un tupla di interi non-negativi distinti (che una volta riordinata ritorna quindi ad essere una partizione stretta) sono precisamente le parti $\gamma_i$. Supponiamo infatti per assurdo che si possa sottrarre un intero positivo $r \notin \{\gamma_i\}$ da qualche $\gamma_j$, in modo che $\gamma_j - r$, che è $\ge 1$, non coincida con nessuna altra parte di $\gamma$. Avremmo allora trovato due interi (non necessariamente distinti) $r, \gamma_j - r$ in $C_\gamma$ la cui somma è $\gamma_j$, e quindi $C_\gamma$ non potrebbe essere chiuso

rispetto all'addizione. Possiamo interpretare questa proprietà di $\gamma$ in termini dei $t$-core: se $\mu$ è la partizione tale che $\mu + \delta = \gamma$, con $\delta = (\ell(\gamma) - 1, \ldots, 1, 0)$, allora $\lambda$ è un $t$-core per ogni $t \in C_\gamma$.

Sia ora $\lambda$ la partizione tale che $\lambda + \delta = \beta$, con $\delta = (n, n-1, \ldots, 1, 0)$. Allora $s_\lambda(x_1, \ldots, x_n) = 0$ dato che $\ell(\lambda) = n + 1$, e inoltre nella scrittura data dalla (6.22) gli unici $p_r$ che compaiono sono i $p_{\beta_i}$ per $i = 1, \ldots, n+1$, visto che $C_\beta$ è chiuso per addizione e i $\beta_i$ sono le uniche lunghezze delle striscie di bordo che è possibile staccare dal diagramma $\lambda$. Inoltre, poiché anche $C_\alpha$ è chiuso per addizione, è possibile sottarre $t$ da una parte di $\beta$ ottenendo una partizione stretta *soltanto una volta*, e tale parte sarà precisamente la parte di $\beta$ uguale a $t$. Abbiamo quindi scritto $s_\lambda$, che vale zero in $n$ variabili, come polinomio in $p_{\alpha_1}, \ldots, p_{\alpha_n}, p_t$, in cui $p_t$ compare con grado 1. Tale relazione corrisponde a una scrittura non banale di $p_t$ come frazione di polinomi in $p_{\alpha_1}, \ldots, p_{\alpha_n}$.

Prendiamo ora $\alpha' = (\beta_2, \ldots, \beta_{n+1})$ la partizione che si ottiene rimuovendo la parte più grande di $\beta$, e supponiamo che $\alpha' \neq (n, \ldots, 2, 1)$. Essendo $p_t$ una funzione razionale dei $p_{\alpha_i}$, e il complementare di $\alpha'$ a sua volta chiuso per addizione, possiamo ripetere il procedimento con $\alpha'$ al posto di $\alpha$.

Siccome la nuova tupla differisce da quella precedente per la rimozione dell'elemento più grande e per l'aggiunta del minimo intero nel complementare, iterando il procedimento ci ritroveremo prima o poi con la tupla $(n, \ldots, 2, 1)$, e quindi una scrittura di $p_1, \ldots, p_n$ come funzioni razionali di $p_{\alpha_1}, \ldots, p_{\alpha_n}$. □

È interessante interpretare la (6.22) secondo il formalismo dei $t$-core: per ogni $t$, il grado con cui compare $p_t$ nella scrittura di $s_\lambda$ come polinomio nei $p_r$ è precisamente il peso $|\lambda^*|$ del $t$-quoziente $\lambda^*$ di $\lambda$, che è anche il numero di $t$-striscie che è possibile staccare dalla partizione $\lambda$.

Il coefficiente di tale termine di grado massimo in $p_t$ è, a meno di una costante, la funzione di Schur $s_{\tilde{\lambda}}$ relativa al $t$-core $\tilde{\lambda}$ di $\lambda$, visto che nel valutare il coefficiente con cui compare $p_\rho$ in $s_\lambda$ possiamo considerare le tuple permutate $\rho$ le cui parti uguali a $t$ compaiono tutte alla fine della tupla. In altre parole possiamo prima staccare le striscie di bordo lunghe $t$, e poi le striscie di lunghezza differente, e nel caso in cui il numero di striscie di bordo lunghe $t$ staccate sia il più grande possibile la partizione intermedia ottenuta dopo la rimozione di tutte le $t$-striscie è sempre la stessa, ovvero il $t$-core di $\lambda$.

È anche possibile calcolare il coefficiente a meno del segno: sia $m = |\lambda^*|$, e per ogni partizione $\rho$ con precisamente $m$ parti uguali a $t$ sia $\tilde{\rho}$ la partizione ottenuta rimuovendo tutte tali parti. Allora

$$\frac{z_\rho}{z_{\tilde{\rho}}} \;=\; m! \cdot t^m.$$

Inoltre come dicevamo invece di considerare le possibili rimozioni di striscie lunghe $\rho_i$ da $\lambda$, possiamo considerare i modi in cui possiamo rimuovere $m$ striscie lunghe $t$, e poi striscie lunghe $\tilde{\rho}_i$.

Il segno dato dalle rimozioni delle striscie di lunghezza $t$ fino al $t$-core è sempre lo stesso, perché il segno di una rimozione equivale alla parità del numero di parti scavalcate sottraendo $t$ da una parte di $\lambda + \delta$, e se anziché a delle parti

pensiamo a delle palline con coordinate intere, ogni coppia di palline si scavalca un numero fissato di volte, visto che ogni pallina giungerà a una posizione prestabilita nel $t$-core.

D'altra parte per ogni classe di resto $r$ le sottrazioni di $t$ dalle parti di $\lambda+\delta$ che sono $\equiv r \pmod t$ si svolgono indipendentemente dalle altre, ed equivalgono al numero di tableau standard di forma $\lambda^{(r)}$, la $r$-esima parte del $t$-quoziente $\lambda^*$ (a meno di permutazione ciclica del $t$-quoziente). Siccome dobbiamo ancora contare le scelte delle classi di resto su cui operare, ricordando la (3.40) abbiamo infine che il coefficente di $p_t^m$ a meno del segno è

$$\frac{1}{m!\cdot t^m}\cdot\prod_i \frac{|\lambda^{(i)}|!}{h(\lambda^{(i)})}\cdot\frac{m!}{\prod_i|\lambda^{(i)}|!}\cdot s_{\tilde\lambda} \;=\; \frac{s_{\tilde\lambda}}{t^m\cdot\prod_i h(\lambda^*)},$$

dove abbiamo indicato con $h(\lambda^*)=\prod_i h(\lambda^{(i)})$.

In particolare esso è sempre diverso da zero. Quest'ultima caratterizzazione è originale, per quanto noto a chi scrive.

### 6.4.3 Il campo generato da $n+1$ polinomi di Newton

In questa sezione mostriamo che se $n$ è il numero di variabili e la caratteristica del campo base è zero $n+1$ polinomi di Newton $N_{a_1},\dots,N_{a_{n+1}}$, con $a_1,\dots,a_{n+1}$ coprimi, sono sempre sufficienti a generare l'intero campo simmetrico. Questo è un risultato di Dvornicich e Zannier esposto [DZ08], che è precisamente l'analogo in più variabili del risultato ottenuto in [DZ03].

Non forniremo tutti i dettagli della dimostrazione, in particolare daremo per buona la parte riguardante la fattorizzazione e il calcolo del gruppo di Galois dei polinomi di Schur. Diamo però una dimostrazione originale del passo conclusivio, che mostra che è sufficiente l'irriducibilità dei polinomi che compaiono nella dimostrazione (che differiscono di poco dai polinomi di Schur), in analogia con quanto fatto in caratteristica positiva con i $T(X,Y,Z)$. Quando possa essere conveniente, useremo un segno $\sim$ per marcare i campi, polinomi, etc. riguardanti solo le variabili $x_2,\dots,x_n$ invece che tutte le $x_1,\dots,x_n$.

Sia quindi $a=(a_1,\dots,a_{n+1})$ una tupla di interi coprimi, e supponiamo che $a_1>a_2>\cdots>a_{n+1}$. Come abbiamo fatto in due variabili, per ottenere che $S=\mathcal{N}_a$ mostriamo che il grado dell'intero campo $F$ delle funzioni razionali in $x_1,\dots,x_n$ su $\mathcal{N}_a$ è $n!$.

Supponendo la conclusione vera in $n-1$ variabili, sarà sufficiente verificare che il grado di $x_1$ su $\mathcal{N}_a$ è $n$. Infatti il campo $\mathcal{N}_a(x_1)$ contiene i polinomi

$$\tilde N_m \;=\; N_m - x_1^m \;=\; x_2^m+\cdots+x_n^m, \qquad \text{per } m=a_1,\dots,a_{n+1},$$

e ogni sottoinsieme di $n$ tali polinomi $\tilde N_m$ per $m=a_1,\dots,a_{i-1},a_{i+1},\dots,a_{n+1}$ genera il campo simmetrico $\tilde S^{(d_i)}$ nelle potenze $d_i$-esime $x_2^{d_i},\dots,x_n^{d_i}$, dove $d_i$ è il massimo comun divisore degli $a_1,\dots,a_{i-1},a_{i+1},\dots,a_{n+1}$.

I massimi comuni divisori parziali $d_i$ possono benissimo essere $\neq 1$, ma sicuramente $(d_1,\dots,d_{n+1})=1$, essendo gli $a_1,\dots,a_{n+1}$ coprimi.

Ricordiamo che il grado $[\tilde{S} : \tilde{S}^{(d_i)}]$ è precisamente $d_i^{n-1}$, essendo $n-1$ le variabili $x_2, \ldots, x_n$. Se $\hat{S}$ è il composto in $F$ di tutti gli $\tilde{S}^{(d_i)}$ per $i = 1, \ldots, n+1$, il grado $[\tilde{S} : \hat{S}]$ deve dividere $d_i^{n-1}$ per ogni $i = 1, \ldots, n+1$, e deve quindi essere 1 visto che $(d_1, \ldots, d_{n+1}) = 1$.

Segue che $\mathcal{N}_a(x_1) = S(x_1)$, cioè è il sottocampo di $F$ delle funzioni in $x_1, \ldots, x_n$ che sono simmetriche in $x_2, \ldots, x_n$, e quindi il grado $[F : \mathcal{N}_a(x_1)]$ è $(n-1)!$. Se riusciamo a dimostrare che il grado di $x_1$ su $\mathcal{N}_a$ è $n$, abbiamo quindi immediatamente che $[F : \mathcal{N}_a] = n!$, e $S = \mathcal{N}_a$.

La dimostrazione procederà supponendo di avere un $y_1$ nella chiusura algebrica di $\mathcal{N}_a$ distinto da $x_1, \ldots, x_n$ che soddisfa la stessa relazione di dipendenza algebrica degli $x_i$ su $\mathcal{N}_a$.

Una qualunque estensione a una chiusura algebrica di $\mathcal{N}_a$ dell'isomorfismo $\mathcal{N}_a(x_1) \to \mathcal{N}_a(y_1)$ che lascia fisso $\mathcal{N}_a$ e tale che $x_1 \mapsto y_1$ determina una tupla alternativa $y_1, \ldots, y_n$ che soddisfa le stesse relazioni degli $x_1, \ldots, x_n$, ovvero

$$x_1^m + \cdots + x_n^m \;=\; y_1^m + \cdots + y_n^m \qquad \text{per } m = a_1, \ldots, a_{n+1}. \tag{6.24}$$

Prima di enunciare e dimostrare il risultato principale della sezione, mostriamo che se una tale relazione è verificata non possono esistere due fra gli $x_1, \ldots, x_n, y_1, \ldots, y_n$ che abbiano rapporto costante, a meno che gli $y_i$ non siano una permutazione degli $x_i$. Gli $x_i$ sono fra loro addirittura algebricamente indipendenti per ipotesi, e lo stesso deve essere vero per gli $y_i$, perché grazie alla prop. 6.2.5 gli $N_{a_i}$ per $i = 1, \ldots, n$ sono algebricamente indipendenti, e questo implica che anche gli $y_i$ devono esserlo.

Supponiamo quindi che $x_1$ e $y_1$ differiscano per una costante, $y_1 = cx_1$ poniamo. Abbiamo allora che

$$(1 - c^m)x_1^m + \cdots + x_n^m \;=\; y_2^m + \cdots + y_n^m, \qquad \text{per } m = a_1, \ldots, a_{n+1},$$

e siccome nel secondo membro compaiono solo $n-1$ variabili, il grado di trascendenza generato da tali espressioni per $m = a_1, \ldots, a_{n+1}$ è al più $n-1$.

Se consideriamo il primo membro e il fatto che gli $x_1, \ldots, x_n$ sono algebricamente indipendenti, abbiamo trascurando l'equazione per $m = a_{n+1}$ che deve annullarsi il determinante dello jacobiano

$$\det \begin{pmatrix} a_1(1-c^{a_1})x_1^{a_1-1} & a_1 x_2^{a_1-1} & \ldots & a_1 x_n^{a_1-1} \\ a_2(1-c^{a_2})x_1^{a_2-1} & a_2 x_2^{a_2-1} & \ldots & a_2 x_n^{a_2-1} \\ \vdots & \vdots & & \vdots \\ a_n(1-c^{a_n})x_1^{a_n-1} & a_n x_2^{a_n-1} & \ldots & a_n x_n^{a_n-1} \end{pmatrix},$$

e siccome non ci sono relazioni fra gli $x_1, \ldots, x_n$ questo può succedere se e solo se $c^{a_i} = 1$ per $i = 1, \ldots, n$. Se trascuriamo un'altra delle $n+1$ equazioni, abbiamo che $c^{a_i} = 1$ per tutti gli $i = 1, \ldots, n, n+1$, e poiché gli $a_i$ sono coprimi questo implica che $c = 1$, e $x_1 = y_1$.

Ma allora $x_2, \ldots, x_n, y_2, \ldots, y_n$ soddisfano le stesse equazioni su $\mathcal{N}_a(x_1)$, e siccome il grado $[F : \mathcal{N}_a(x_1)]$ è $(n-1)!$ abbiamo che gli $y_2, \ldots, y_n$ devono essere una permutazione degli $x_2, \ldots, x_n$.

Possiamo ora procedere con la dimostrazione del

**Teorema 6.4.4.** *Sia $a = (a_1, \dots, a_{n+1})$ una tupla di interi positivi distinti e coprimi. Allora il campo $\mathcal{N}_a$ generato dai polinomi di Newton $N_{a_1}, \dots, N_{a_{n+1}}$ è l'intero campo simmetrico in $n$ variabili.*

*Dimostrazione.* Supponiamo che $a_1 > \cdots > a_{n+1}$, e estendiamo la derivazione ordinaria $\frac{\partial}{\partial y_1}$ su $\mathbb{C}(y_1, \dots, y_n)$ alla chiusura algebrica di $\mathcal{N}_a$, essa sarà indicata con un apice. Dalle (6.24) abbiamo, derivando e dividendo per $m$, che

$$x_1^{m-1}x_1' + \cdots + x_n^{m-1}x_n' - y_1^{m-1} \;=\; 0, \qquad \text{per } m = a_1, \dots, a_{n+1}.$$

Ragionando come nel caso in due variabili, possiamo vedere tali equazioni come

$$\begin{pmatrix} x_1^{b_1} & \dots & x_n^{b_1} & y_1^{b_1} \\ x_1^{b_2} & \dots & x_n^{b_2} & y_1^{b_2} \\ \vdots & & \vdots & \vdots \\ x_1^{b_n} & \dots & x_n^{b_n} & y_1^{b_n} \\ x_1^{b_{n+1}} & \dots & x_n^{b_{n+1}} & y_1^{b_{n+1}} \end{pmatrix} \cdot \begin{pmatrix} x_1^{a_{n+1}-1}x_1' \\ x_2^{a_{n+1}-1}x_2' \\ \vdots \\ x_n^{a_{n+1}-1}x_n' \\ -y_1^{a_{n+1}-1} \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$$

dove $b$ è la tupla delle differenze $(a_1 - a_{n+1}, \dots, a_n - a_{n+1}, 0)$. In particolare la matrice al primo membro deve avere determinante zero.

Per ogni tupla $b = (b_1, \dots, b_{n+1})$ definiamo quindi il polinomio delle $n+1$ variabili

$$R_b(X) \;=\; R_b(X_0, \dots, X_n) \;=\; \det(X_j^{b_i})_{0 \le i,j \le n}.$$

Se $d$ è il massimo comun divisore dei $b_i$, questo polinomio è chiaramente divisibile per il determinante di Vandermonde nelle potenze $d$-esime

$$V(X^d) \;=\; V(X_0^d, \dots, X_n^d) \;=\; \det(X_j^{d(n-i)})_{0 \le i,j \le n}.$$

Infine, come abbiamo fatto in due variabili chiamiamo $T$ il polinomio che si ottiene dividendo per tale fattore

$$T_b(X) \;=\; T_b(X_0, \dots, X_n) \;=\; \frac{R_b(X)}{V(X^d)}.$$

Faremo ora uso del seguente risultato

**Teorema 6.4.5** (Dvoricich, Zannier)**.** *Per ogni tupla $b = (b_1, \dots, b_{n+1})$ tale che $b_1 > \cdots > b_{n+1} = 0$, il polinomio $T_b(X)$ è irriducibile su $\mathbb{C}(X_0, \dots, X_n)$. Visto come polinomio in $X_0$ su $\mathbb{C}(X_1, \dots, X_n)$, ha gruppo di Galois isomorfo al* prodotto wreath

$$(\mathbb{Z}/d\mathbb{Z}) \wr S_{b_1/d-n},$$

*dove $d$ è il massimo comun divisore dei $b_1, \dots, b_{n+1}$.*

Come abbiamo già anticipato, non useremo questo risultato in tutta la sua potenza ma ci servirà soltanto l'irriducibilità di $T_b(X)$.

Rinomiamo $y_1$ come $z$ poiché essa svolgerà un ruolo particolare nella dimostrazione. Supponiamo quindi che

$$x_1^m + \cdots + x_n^m \;=\; z^m + y_2^m + \cdots + y_n^m, \qquad \text{per } m = a_1, \ldots, a_{n+1}, \tag{6.25}$$

e che nell'espressione $z, y_2, \ldots, y_n$ non siano una permutazione di $x_1, \ldots, x_n$.

Se $b = (a_1 - a_{n+1}, \ldots, a_n - a_{n+1}, 0)$, abbiamo che $R_b(x_1, \ldots, x_n, z) = 0$, e in particolare $T_b(x_1, \ldots, x_n, z) = 0$, visto che non esistono due fra $x_1, \ldots, x_n, z$ che differiscano per una costante.

Avremo bisogno del seguente fatto fondamentale: $n$ elementi qualunque fra $x_1, \ldots, x_n, z$ sono algebricamente indipendenti. Gli $x_1, \ldots, x_n$ sono indipendenti per definizione, quindi ci basta vedere che gli elementi che restano dopo aver rimosso uno degli $x_i$, $x_1$ poniamo, sono indipendenti.

Supponiamo quindi che $z$ sia algebrico su $x_2, \ldots, x_n$. Ma $x_1$ annulla il polinomio

$$T_b(U, x_2, \ldots, x_n, z),$$

visto come polinomio in $U$. Se tale polinomio non si annulla identicamente abbiamo ottenuto che $x_1$ è algebrico su $x_2, \ldots, x_n, z$, e quindi su $x_2, \ldots, x_n$ visto che $z$ è algebrico su $x_2, \ldots, x_n$, e questo è assurdo.

Esso deve quindi annullarsi identicamente, ovvero ciascun coefficiente delle potenze di $U$ in $T(U, X_2, \ldots, X_n, Z)$ è un polinomio in $X_2, \ldots, X_n, Z$ che si annulla su $x_2, \ldots, x_n, z$.

Sia $I$ l'ideale di $\mathbb{C}[X_2, \ldots, X_n, Z]$ determinato da $(x_2, \ldots, x_n, z)$, ovvero l'ideale degli elementi che si annullano su $(x_2, \ldots, x_n, z)$. Mostreremo che tale ideale è principale.

Sia infatti $P(X_2, \ldots, X_n, Z) \in I$. Dato che $x_2, \ldots, x_n$ sono indipendenti, abbiamo che $P(x_2, \ldots, x_n, Z)$ deve essere divisibile in $\mathbb{C}(x_2, \ldots, x_n)[Z]$ per il polinomio minimo di $z$ su $x_2, \ldots, x_n$, $F(x_2, \ldots, x_n, Z)$ poniamo. Se dividiamo $F(x_2, \ldots, x_n, Z)$ per il contenuto in $Z$ rispetto all'anello $\mathbb{C}[x_2, \ldots, x_n]$, otteniamo un polinomio $\hat{F}(x_2, \ldots, x_n, Z)$ in $\mathbb{C}[x_2, \ldots, x_n, Z]$ che per il lemma di Gauss deve ancora dividere $P(x_2, \ldots, x_n, Z)$. Dato che $\hat{F}(X_2, \ldots, X_n, Z) \in I$, abbiamo quindi che $I$ è principale.

Siccome $T(U, X_2, \ldots, X_n, Z)$ è un polinomio non nullo in $U$, abbiamo quindi trovato un fattore non banale in $\mathbb{C}[X_2, \ldots, X_n, Z]$, ma questo è assurdo visto che $T(X)$ è irriducibile.

Abbiamo quindi che $n$ elementi qualunque fra $x_1, \ldots, x_n, z$ devono essere algebricamente indipendenti.

Procediamo ora osservando che se deriviamo la (6.25) con un'estensione della derivazione $\frac{\partial}{\partial x_1}$ su $\mathbb{C}(x_1, \ldots, x_n)$ alla chiusura algebrica di $\mathcal{N}_a$, allora indicando tale derivazione con un apice otteniamo

$$x_1^{m-1} - z^{m-1}z' - y_2^{m-1}y_2' \cdots - y_n^{m-1}y_n' \;=\; 0, \qquad \text{per } m = a_1, \ldots, a_{n+1}.$$

Ragionando come quando abbiamo dimostrato che $T_b(x_1, \ldots, x_n, z) = 0$, abbiamo quindi analogamente che $T_b(x_1, z, y_2, \ldots, y_n) = 0$, visto che non esistono due fra le variabili in questione che differiscano per una costante.

Inoltre, poiché $x_2, \dots, x_n, z$ sono algebricamente indipendenti, riscrivendo la (6.25) come

$$-z^m + x_2^m + \cdots + x_n^m \;=\; -x_1^m + y_2^m + \cdots + y_n^m, \qquad \text{per } m = a_1, \dots, a_{n+1},$$

abbiamo che condiderando $n$ di tali equazioni e il fatto che per il criterio dello jacobiano gli $-z^m + x_2^m + \cdots + x_n^m$ per $m = a_1, \dots, a_n$ sono algebricamente indipendenti, allora $x_1, y_2, \dots, y_n$ devono giocoforza essere algebricamente indipendenti.

Possiamo quindi definire un isomorfismo che lascia fisse le costanti

$$\begin{aligned} \varepsilon : \mathbb{C}(x_1, \dots, x_n) &\to \mathbb{C}(x_1, y_2, \dots, y_n), \\ x_1 &\mapsto x_1, \\ x_i &\mapsto y_i, \qquad \text{per } i = 2, \dots, n. \end{aligned}$$

Inoltre, essendo $T_b(X)$ simmetrico e irriducibile, abbiamo che la relazione di dipendenza di $z$ su $\mathbb{C}(x_1, \dots, x_n)$ è la stessa di quella di $z$ su $\mathbb{C}(x_1, y_2, \dots, y_n)$, e quindi $\varepsilon$ può essere esteso ponendo

$$z \mapsto z.$$

Possiamo ora estendere $\varepsilon$ alla chiusura algebrica, e chiamiamo $w_2, \dots, w_n$ le immagini di $y_2, \dots, y_n$ (che potranno essere qualunque elemento della chiusura algebrica, a noi servirà soltanto che esistano). Applicando $\varepsilon$ alla (6.25) otteniamo quindi che

$$x_1^m + y_2^m + \cdots + y_n^m \;=\; z^m + w_2^m + \cdots + w_n^m, \qquad \text{per } m = a_1, \dots, a_{n+1}. \tag{6.26}$$

Sommando la (6.26) alla (6.25) abbiamo quindi che

$$2x_1^m + x_2^m + \cdots + x_n^m \;=\; 2z^m + w_2^m + \cdots + w_n^m, \qquad \text{per } m = a_1, \dots, a_{n+1}. \tag{6.27}$$

È possibile ora ripetere l'intero procedimento con $x_2, z, w_2, \dots, w_n$: possiamo infatti ottenere come prima cosa che $T(x_2, z, w_2, \dots, w_n) = 0$, e che $x_2, w_2, \dots, w_n$ devono essere algebricamente indipendenti. Osservando che la relazione di $z$ su $x_2, w_2, \dots, w_n$ è la stessa di quella di $z$ su $x_1, \dots, x_n$ possiamo nuovamente costruire un isomorfismo $\zeta$ tale che

$$\begin{aligned} \varepsilon : \mathbb{C}(x_1, \dots, x_n) &\to \mathbb{C}(x_2, w_2, \dots, w_n), \\ x_1 &\mapsto x_2, \\ x_i &\mapsto w_i, \qquad \text{per } i = 2, \dots, n, \end{aligned}$$

e estenderlo in modo che

$$z \mapsto z.$$

Estendiamo $\zeta$ alla chiusura algebrica, e chiamiamo $v_i$ le immagini degli $y_i$. Applicando $\zeta$ alla (6.25) otteniamo

$$x_2^m + w_2^m + \cdots + w_n^m \;=\; z^m + v_2^m + \cdots + v_n^m, \qquad \text{per } m = a_1, \dots, a_{n+1},$$

e sommando tale equazione alla (6.27) abbiamo che

$$2x_1^m + 2x_2^m + x_3^m + \cdots + x_n^m \;=\; 3z^m + v_2^m + \cdots + v_n^m, \qquad \text{per } m = a_1, \ldots, a_{n+1}.$$

È ora chiaro che possiamo procedere in questo modo fino ad ottenere un'equazione della forma

$$2x_1^m + 2x_2^m + \cdots + 2x_n^m \;=\; (n+1)z^m + q_2^m + \cdots + q_n^m, \qquad \text{per } m = a_1, \ldots, a_{n+1},$$

per degli opportuni $q_2, \ldots, q_n$ nella chiusura algebrica di $\mathcal{N}_a$. Sottraendo due volte la (6.25) da quest'ultima equazione, abbiamo quindi che

$$(1-n)z^m + 2y_2^m + \cdots + 2y_n^m \;=\; q_2^m + \cdots + q_n^m, \qquad \text{per } m = a_1, \ldots, a_{n+1},$$

e in particolare il grado di trscendenza del campo generato dalle espressioni al primo membro deve essere al più $n-1$, visto che al secondo membro compaiono solo le $n-1$ variabili $q_2, \ldots, q_n$.

Ma se $n > 1$ abbiamo applicando il criterio dello jacobiano che il grado di trascendenza del campo generato da $n$ espressioni della forma

$$(1-n)z^m + 2y_2^m + \cdots + 2y_n^m \qquad \text{per } m = a_1, \ldots, a_n,$$

è $n$ essendo $z, y_2, \ldots, y_n$ algebricamente indipendenti, e questo assurdo conclude la dimostrazione. □

# Bibliografia


[Com74] L. Comtet, *Advanced Combinatorics: The Art of Finite and Infinite Expansions*, D. Reidel Pub. Co., 1974.

[DZ03] R. Dvornicich and U. Zannier, *Solution of a Problem about Symmetric Functions*, Rocky Mountain J. of Mathematics **33** (2003), no. 4, 1279–1288.

[DZ08] ———, *Newton Functions Generating Symmetric Fields and Irreducibility of Schur Polynomials (unpublished)*, 2008.

[FH91] W. Fulton and J. Harris, *Representation Theory: A First Course*, Graduate Texts in Mathematics, no. 129, Springer, New York, 1991.

[Fou56] H.O. Foulkes, *Theorems of Pólya and Kakeya on power-sums*, Math. Zeitschr **65** (1956), 345–352.

[Har77] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, no. 52, Springer, 1977.

[Kak25] S. Kakeya, *On Fundamental Systems of Symmetric Functions I*, Japan J. of Math **2** (1925), 69–80.

[Kak27] ———, *On Fundamental Systems of Symmetric Functions II*, Japan J. of Math **4** (1927), 77–85.

[KC02] V. Kac and P. Cheung, *Quantum Calculus*, Universitext, Springer-Verlag, New York, 2002.

[Lan02] S. Lang, *Algebra*, Springer, 2002.

[Lew84] R.P. Lewis, *A combinatorial proof of the triple product identity*, Amer. Math. Monthly **91** (1984), no. 7, 420–423.

[Mac95] I.G. Macdonald, *Symmetric Functions and Hall Polynomials (2nd edition)*, Oxford University Press, New York, 1995.

[Mil08a] J. S. Milne, *Algebraic Geometry*, `www.math.lsa.umich.edu/~jmilne/`, 2008.

[Mil08b] ———, *Fields and Galois Theory*, `www.math.lsa.umich.edu/∼jmilne/`, 2008.

[MS98] D.G. Mead and S.K. Stein, *Some Algebra of Newton Polynomials*, Rocky Mountain J. of Mathematics **28** (1998), 303–310.

[Nak27] K. Nakamura, *On the Representation of Symmetric Functions by Power-Sums which form the Fundamental System*, Japan J. Math **4** (1927), 87–92.

[Ser77] J.P. Serre, *Linear Representations of Finite Groups*, Springer Verlag, 1977.

[Völ96] H. Völklein, *Groups as Galois Groups: An Introduction*, Cambridge University Press, Cambridge England, 1996.

# Indice analitico

**Per chi credeva che questa tesi non contenesse nulla di analitico...**