Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea in Matematica

INVARIANTI POLINOMIALI SOTTO L'AZIONE DI GRUPPI FINITI

Tesi di Algebra

Relatore:
Chiar.mo Prof.
CASELLI
FABRIZIO

Presentata da:
MORETTI
GIADA

I Sessione
Anno Accademico 2014/2015

Introduzione

Il teorema di Chevalley-Shephard-Todd è un importante risultato del 1954/1955 nella teoria degli invarianti polinomiali sotto l'azione del gruppo delle matrici invertibili. Lo scopo di questa tesi è di presentare e dimostrare il teorema nella versione in cui l'anello dei polinomi ha come campo base $\mathbb{R}$ e di vedere alcuni esempi concreti di applicazione del teorema. Questa dimostrazione può essere generalizzata facilmente avendo come campo base un qualsiasi campo K di caratteristica 0 .
Nel primo capitolo viene descritto il gruppo simmetrico di ordine n e si definisce la sua azione sull'anello dei polinomi in n variabili; si trovano poi tutti i polinomi che restano invariati sotto questa azione, chiamati polinomi simmetrici, e si studia la struttura del sottinsieme composto da questi elementi.
Nel secondo capitolo vengono introdotte brevemente le riflessioni e i gruppi finiti che generano; si definiscono poi le azioni di gruppo e si dimostrano alcuni risultati preliminari che valgono per le azioni di gruppo in generale e per le azioni di gruppi finiti di riflessioni in particolare.
Nel terzo capitolo viene dimostrato invece il risultato principale della tesi dividendolo in due teoremi: il primo teorema dimostra che l'algebra degli invarianti polinomiali sotto l'azione di un gruppo finito di riflessioni è generata da un numero finito di elementi algebricamente indipendenti mentre il secondo mostra che se l'algebra degli invarianti polinomiali è generata da un numero finito di elementi algebricamente indipendenti allora il gruppo che agisce è generato da riflessioni. Fra la prima e la seconda parte vengono introdotte altre nozioni necessarie alla dimostrazione del teorema: in particolare si studiano i gradi degli invarianti polinomiali che generano il sottoanello dei polinomi e per fare ciò si analizzano somma

e prodotto dei gradi e viene sviluppato un criterio per l'indipendenza algebrica che sfrutta lo Jacobiano.

Infine il quarto capitolo è composto da esempi di applicazioni del teorema di Chevalley: si presentano i gruppi finiti di riflessioni di tipo B_n, D_n e $I_2(m)$, si descrivono gli invarianti polinomiali sotto l'azione di questi gruppi e si trova un insieme di generatori.

Indice

Capitolo 1

Polinomi simmetrici

In questo capitolo descriviamo l'azione di S_n su $\mathbb{R}[x_1, \ldots, x_n]$.
Per iniziare introduciamo alcune notazioni che verrano usate in questa tesi.

Definizione 1.1. Sia $[n] = \{x \in \mathbb{N} \text{ tale che } 1 \leq x \leq n\}$.

Definizione 1.2. Sia $n \geq 1$. Chiameremo gruppo simmetrico il gruppo $(S_n, \circ)$ dove $S_n = \{\tau : [n] \to [n]\}$ è l'insieme delle biezioni di $[n]$. Chiameremo gli elementi di S_n anche permutazioni.

Useremo la classica notazione di prodotto di cicli per scrivere esplicitamente un elemento di S_n.

Definizione 1.3. Sia $\tau \in S_n$, $\tau = (i, j)$ con $1 \leq i, j \leq n$. Chiameremo tutte le permutazioni di questo tipo trasposizioni.

Facciamo agire ora S_n su $\mathbb{R}[x_1, \ldots, x_n]$ in questo modo:

$$\tau f(x_1, \ldots, x_n) = f(x_{\tau(1)}, \ldots, x_{\tau(n)}).$$

Vedremo che questa azione rispetta la definizione che daremo nel secondo capitolo.

Esempio 1.1. Sia $n = 5$, $\tau = (12)(435)$, $f(x_1, \ldots, x_5) = x_1^3 + x_1x_4 + x_2x_3 + x_2 + 3x_5$. Allora $\tau f = x_2^3 + x_2x_3 + x_1x_5 + x_1 + 3x_4$.

In generale $\tau f \neq f$.

Definizione 1.4. Sia $f \in \mathbb{R}[x_1, \ldots, x_n]$ tale che $\tau f = f \ \forall \tau \in S_n$. Chiameremo tutti gli f per cui vale questa proprietà S_n-invarianti. Se è chiaro quale gruppo agisce su $\mathbb{R}[x_1, \ldots, x_n]$ diremo anche solamente invarianti.

Questi elementi formano una sottoalgebra di $\mathbb{R}[x_1, \ldots, x_n]$ che chiameremo sottoalgebra invariante e denoteremo come $\mathbb{R}[x_1, \ldots, x_n]^{S_n}$.

Definizione 1.5. Sia

$$\sigma_i = \sum_{j_1<j_2<\ldots<j_i} x_{j_1} x_{j_2} \cdots x_{j_i} \in \mathbb{R}[x_1, \ldots, x_n].$$

Chiameremo queste funzioni polinomi simmetrici elementari.

Vogliamo far vedere che ogni σ_i è in $\mathbb{R}[x_1, \ldots, x_n]^{S_n}$. Sia quindi T un'indeterminata su $\mathbb{R}[x_1, \ldots, x_n]$ e consideriamo $g = (T - x_1) \cdots (T - x_n) = T^n - \sigma_1 T^{n-1} + \sigma_2 T^{n-2} + \ldots + (-1)^n \sigma_n$. Sia inoltre $\tau \in S_n$: τ agisce su g scambiando gli x_i e lasciando fisso T. Avremo che $g(T, x_{\tau(1)}, \ldots, x_{\tau n}) = g$ poichè abbiamo solo cambiato l'ordine dei fattori nella fattorizzazione di g e quindi i coefficienti di g sono fissati da ogni $\tau \in S_n$ ovvero $\sigma_1, \ldots, \sigma_n$ sono fissati da ogni $\tau \in S_n$ come volevamo.

Teorema 1.0.1 (Newton)**.** *Ogni elemento di* $\mathbb{R}[x_1, \ldots, x_n]^{S_n}$ *si può scrivere come polinomio in* $\sigma_1, \ldots, \sigma_n$*.*

Esempio 1.2. Sia $n = 2$ allora $x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = \sigma_1^2 - 2\sigma_2$ è fissato da S_2.

Dimostrazione. Introduciamo innanzitutto un ordine totale nell'insieme dei monomi con coefficiente direttore 1: $x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n}$ se $\sum a_i > \sum b_i$ oppure se $\sum a_i = \sum b_i$ ed $\exists j$ tale che $a_1 = b_1, \ldots, a_j = b_j, a_{j+1} > b_{j+1}$. A questo punto dato un qualsiasi polinomio in $x_1, \ldots, x_n$ è ben individuato il monomio di grado massimo che chiameremo monomio direttivo. Inoltre se $f, g \in \mathbb{R}[x_1, \ldots, x_n]$ allora il monomio direttivo di fg è il prodotto dei monomi direttivi di f e g. Sia allora $f \in \mathbb{R}[x_1, \ldots, x_n]^{S_n}$ e sia $cx_1^{a_1} \cdots x_n^{a_n}$ il monomio direttivo di f. Osserviamo innanzitutto che $a_1 \geq \ldots \geq a_n$. Infatti se esistesse j tale che $a_j < a_{j+1}$,

considerando la trasposizione $(j, j+1)$, si avrà $(j, j+1)f = f$ e di conseguenza $(j, j+1)cx_1^{a_1} \cdots x_n^{a_n} = cx_1^{a_1} \cdots x_j^{a_{j+1}} x_{j+1}^{a_j} \ldots x_n^{a_n}$ che ha grado maggiore del monomio direttivo e ciò è assurdo.
Consideriamo ora $h = \sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3} \cdots \sigma_n^{a_n}$. Il monomio direttivo di h sarà $x_1^{a_1-a_2}(x_1x_2)^{a_2-a_3}(x_1x_2x_3$
$x_1^{a_1} \cdots x_n^{a_n}$. Quindi $f - ch$ avrà monomio direttivo minore di quello di f. Iterando il procedimento si giunge ad un polinomio di grado 0 cioè possiamo scrivere f come polinomio nei σ_i. □

Esempio 1.3. Riprendendo l'esempio precedente applichiamo il procedimento usato nella dimostrazione per vedere come scrivere $x_1^2 + x_2^2$ come combinazione algebrica di σ_1 e σ_2. Il monomio direttivo di $x_1^2 + x_2^2$ è $x_1^2x_2^0$ quindi avremo $a_1 = 2$ e $a_2 = 0$. Sarà allora

$$x_1^2 + x_2^2 - \sigma_1^{a_1-a_2}\sigma_2^{a_2} = x_1^2 + x_2^2 - (x_1 + x_2)^2 = -2x_1x_2 = -2\sigma_2.$$

Abbiamo quindi che quando S_n agisce su $\mathbb{R}[x_1, \ldots, x_n]$ il sottoanello fisso è isomorfo a $\mathbb{R}[x_1, \ldots, x_n]$: infatti i σ_i possono essere presi come un insieme di generatori per $\mathbb{R}[x_1, \ldots, x_n]^{S_n}$ perchè ogni polinomio nel sottoanello fisso si può scrivere come combinazione algebrica dei σ_i. Inoltre vale il seguente teorema.

Teorema 1.0.2. *I σ_i sono algebricamente indipendenti.*

Per una dimostrazione di questo teorema si veda il teorema 7.4.4 di [3].
Come vedremo nei prossimi capitoli, l'esistenza di un isomorfismo fra il sottoanello fisso e l'anello dei polinomi non è una prerogativa dell'azione di S_n su $\mathbb{R}[x_1, \ldots, x_n]$ ma caratterizza tutti i sottogruppi finiti di $GL(\mathbb{R}^n)$ generati da riflessioni.

Capitolo 2

Gruppi finiti di riflessioni

In questo capitolo descriviamo in generale i gruppi finiti di riflessioni. Introduciamo anche alcuni risultati generali che verranno usati nel prossimo capitolo. Assumiamo sempre, se non diversamente indicato, che V sia uno spazio euclideo di dimensione n su $\mathbb{R}$. Indicheremo inoltre con $GL(V)$ il gruppo degli automorfismi di V e con W un sottogruppo finito di $GL(V)$.

2.1 Riflessioni

Definizione 2.1. Sia α un vettore di V, H_α l'iperpiano di V ortogonale a α. Allora la riflessione associata ad α è un operatore lineare φ su V definito da

$$\varphi(v) = v - 2\frac{v \cdot \alpha}{\alpha \cdot \alpha}\alpha$$

dove con $v \cdot \alpha$ indichiamo il prodotto scalare di V.

Denoteremo φ anche come φ_α. Notiamo subito che $\varphi_\alpha = \varphi_{c\alpha} \forall c \in \mathbb{R}$.

Osservazione 2.1. Si può facilmente vedere che $\varphi_\alpha(v) = v$ se $v \in H_\alpha$ mentre $\varphi_\alpha(v) = -v$ quando $v \in \langle\alpha\rangle$. Abbiamo così descritto come agisce φ_α su ogni $v \in V$: infatti $V = H_\alpha \bigoplus \langle\alpha\rangle$.

Osservazione 2.2. E' anche possibile verificare che φ_α è una trasformazione ortogonale cioè $(\varphi_\alpha(v), \varphi_\alpha(w)) = (v, w)$. Infatti $(\varphi_\alpha(v), \varphi_\alpha(w)) = (v, w)$ banalmente

se $v, w \in H_\alpha$ mentre $(\varphi_\alpha(v), \varphi_\alpha(w)) = (-v, -w) = (v, w)$ se $v, w \in \langle\alpha\rangle$. Quando invece $v \in \langle\alpha\rangle$ e $w \in H_\alpha$ allora $(v, w) = 0$ e allo stesso modo $(\varphi(v), \varphi(w)) = (-v, w) = 0$.

Osservazione 2.3. Abbiamo che φ_α ha ordine 2 come elemento di $GL(V)$. Infatti se $v \in H_\alpha$ allora $\varphi_\alpha(v) = v$ mentre se $v \in \langle(\alpha)\rangle$ allora $\varphi_\alpha(v) = -v$ ma $\varphi_\alpha(\varphi_\alpha(v)) = v$.

Definizione 2.2. Sia W un sottogruppo di $GL(V)$. Se W è finito ed è generato da riflessioni viene detto gruppo finito di riflessioni.

Esempio 2.1. Consideriamo S_n. Sappiamo che S_n è generato dalle trasposizioni: possiamo infatti scrivere ogni α di S_n come prodotto di cicli disgiunti e ogni ciclo può essere scritto come prodotto di trasposizioni. In generale la scrittura di α come prodotto di trasposizioni non è unica.
Come trasposizioni che generano S_n possiamo scegliere, ad esempio, $(1, 2)$, $(2, 3)$, ..., $(n-1, n)$. Dobbiamo vedere quindi che S_n è generato da riflessioni. Infatti possiamo vederlo come un sottogruppo delle matrici ortogonali $O(\mathbb{R}^n)$ nel seguente modo: sia $\alpha \in S_n$, allora α agisce su $\mathbb{R}^n$ permutando i vettori della base canonica $e_1, \ldots, e_n$. Avremo che $\alpha(e_1, \ldots, e_n) = e_{\alpha(1)}, \ldots, e_{\alpha(n)}$. Così ogni trasposizione (ij) è una riflessione: fissa puntualmente l'iperpiano H di $\mathbb{R}^n$ formato da tutti i vettori $v = (v_1, ..., v_n)$ tali che $v_i = v_j$ e manda e_i in e_j e il vettore $e_i - e_j$ nel suo opposto $e_j - e_i$. S_n può quindi essere pensato come gruppo finito di riflessioni.

Definizione 2.3. Sia G un gruppo e R un anello. Diremo che G agisce su R se esiste un omomorfismo di gruppi

$$\begin{array}{rccc} \eta: & G & \to & Aut(R) \\ & g & \mapsto & \eta_g \end{array}$$

con η_g:$R \to R$ tale che valgano le seguenti proprietà $\forall x, y \in R$ e $\forall g, h \in G$:

- $\eta_g(x + y) = \eta_g(x) + \eta_g(y)$;
- $\eta_g(xy) = \eta_g(x)\eta_g(y)$;
- $\eta_h\eta_g(x) = \eta_{hg}(x)$.

Con abuso di notazione scriveremo anche $g(x)$ per indicare $\eta_g(x)$.

Definizione 2.4. Sia G un gruppo e R un anello. Se G agisce su R allora

$$R^G = \{x \in R | gx = x \ \forall \, g \in G\}$$

è un sottoanello di R che viene detto sottoanello fisso.

Osservazione 2.4. R^G è effettivamente un sottoanello: infatti siano x,$y \in R^G$ e $g \in G$. Abbiamo che $x + y = g(x) + g(y) = g(x + y)$ e $xy = g(x)g(y) = g(xy)$ cioè R^G è chiuso sia rispetto alla somma che al prodotto. Inoltre sia $-x$ l'opposto di x avremo allora che $-x = -g(x) = g(-x)$ cioè per ogni elemento di R^G anche il suo opposto è in R^G.

Esempio 2.2. Quando S_n agisce su $\mathbb{R}[x_1, \ldots, x_n]$ come definito nel primo capitolo si ha effettivamente un'azione di gruppo per come l'abbiamo appena definita. Infatti

$$\begin{aligned}\eta_\alpha(f+g) &= (f+g)(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) = \\ &= f(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) + g(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) = \eta_\alpha(f) + \eta_\alpha(g),\end{aligned}$$

$$\begin{aligned}\eta_\alpha(fg) &= (fg)(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) = \\ &= f(x_{\alpha(1)}, \ldots, x_{\alpha(n)})g(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) = \eta_\alpha(f)\eta_\alpha(g)\end{aligned}$$

e

$$\eta_\alpha\eta_\beta(f) = f(x_{\alpha(\beta(1))}, \ldots, x_{\alpha(\beta(n))} = \eta_{\alpha\beta}(f).$$

Ci concentriamo ora sull'anello degli invarianti di $\mathbb{R}[x_1, \ldots, x_n]$ rispetto all'azione di un sottogruppo finito W di $GL(V)$.
Sia S l'algebra $S(V^*) = \{f : V \to V \text{polinomiale}\}$. Se fissiamo una base su V, S può essere identificato con $\mathbb{R}[x_1, \ldots, x_n]$. C'è quindi un'azione naturale di W su S che viene dall'azione di contragradiente di W su V^*:

$$(g \cdot f)(v) = f(g^{-1}(v))$$

dove $g \in W$, $v \in V$, ed $f \in V^*$.
Vogliamo dare ora una prima idea della struttura di R. Indichiamo con $Q(A)$ il campo dei quozienti di un dominio A.

Proposizione 2.1.1. *Sia V uno spazio vettoriale finito di dimensione n su $\mathbb{R}$. Sia W un sottogruppo finito di $GL(V)$ che agisce su $S(V^*)$ in modo naturale e sia $R = S^W$. Allora $Q(R)$ coincide con il sottocampo di W-invarianti nel campo di $Q(S)$. In particolare ha grado di trascendenza n su $\mathbb{R}$.*

Dimostrazione. Sia $L = Q(S) \cong \mathbb{R}(x_1, \ldots, x_n)$. L è un'estensione puramente trascendente di $\mathbb{R}$ di grado n. Sappiamo che L è un'estensione finita di Galois di L^W con gruppo di Galois W. Ne segue che anche L^W ha grado di trascendenza n su $\mathbb{R}$. Naturalmente $Q(R) \subseteq L^W$. Vogliamo vedere che $L^W \subseteq Q(R)$ e quindi che $L^W = Q(R)$. Sia $\frac{p}{q} \in L^W$ con p, $q \in S$. Possiamo moltiplicare sia p che q per $\prod gp$ dove la produttoria è su ogni $g \in W$,$g \neq 1$. Il nuovo numeratore è chiaramente W-invariante e quindi lo deve essere anche il denominatore. Ciò prova che $L^W = Q(R)$. □

Vogliamo vedere ora che l'anello degli invarianti R è finitamente generato come $\mathbb{R}$-algebra. Per il teorema della base di Hilbert sappiamo che gli ideali di S sono finitamente generati. Ne segue che possiamo estrarre un insieme finito di generatori da qualsiasi insieme di generatori. Consideriamo quindi l'ideale $I = SR^+$ di S generato da R^+ ideale di R che contiene tutti gli elementi con costante nulla. Vogliamo vedere che un qualsiasi insieme finito di generatori di I scelto in R^+ che siano omogenei, insieme ad 1, genera R come $\mathbb{R}$-algebra.
Per fare ciò definiamo l'operatore $^\#$ per gli elementi di S come segue:

$$f^\# = \frac{1}{|W|} \sum_{g \in W} g \cdot f.$$

Avremo che $^\# : f \mapsto f^\#$ è lineare da S a R, conserva il grado e lascia fissati gli elementi di R. Vale inoltre la seguente proprietà:

$$(pq)^\# = p^\# q \quad \forall p \in S, \forall q \in R.$$

Proposizione 2.1.2. *Siano $f_1, \ldots, f_r$ elementi omogenei di R^+ che generano $I = SR^+ \subseteq S$. Allora R è generato come $\mathbb{R}$-algebra da questi elementi e 1.*

Dimostrazione. Dobbiamo vedere che ogni $f \in R$ è un polinomio in $f_1, \ldots, f_r$. Ci basterà mostrarlo per i polinomi omogenei. Procediamo per induzione su $deg(f)$:

il caso in cui $deg(f) = 0$ è ovvio. Se $deg(f) > 0$ abbiamo $f \in I$ e possiamo scrivere

$$f = s_1 f_1 + \ldots + s_r f_r \tag{2.1}$$

con $s_i \in S$. Dato che gli f_i sono omogenei possiamo assumere che anche gli s_i lo siano e abbiano gradi $deg(s_i) = deg(f) + deg(f_i) \quad \forall i$. Usiamo allora $^{\#}$ sull'espressione (2.1) e otteniamo:

$$f = f^{\#} = s_1^{\#} f_1 + \ldots + s_r^{\#} f_r.$$

Ora gli $s_i^{\#}$ sono elementi omogenei di R di grado minore di $deg(f)$ quindi per ipotesi induttiva sono polinomi negli f_i e quindi lo è anche f. □

Lemma 2.1.3. *Sia l un polinomio omogeneo di grado 1 nelle indeterminate $x_1, \ldots, x_n$ e supponiamo che f si annulli su tutti gli zeri di l. Allora l divide f nell'anello $\mathbb{R}[x] = \mathbb{R}[x_1, \ldots, x_n]$.*

Dimostrazione. Supponiamo che x_n abbia coefficiente $a_n \neq 0$ nella scrittura di l. Allora usando la divisione in una variabile avremo $f = lq + r$ dove $q \in \mathbb{R}[x]$ e r ha grado 0 rispetto a x_k. Supponiamo che esistano $a_1, \ldots, a_{n-1}$ in $\mathbb{R}$ per cui $r(a_1, \ldots, a_{n-1}) \neq 0$. Calcolando $l(a_1, \ldots, a_{n-1}, x_n)$ possiamo trovare un a_n per cui $l(a_1, \ldots, a_{n-1}, a_n) = 0$. Ma, per ipotesi, $f(a_1, \ldots, a_{n-1}, a_n) \neq 0$. Quindi $r = 0$ e ciò dimostra l'enunciato. □

Capitolo 3

Il teorema di Chevalley

Il nostro interesse si sposta sulla sottoalgebra R di $\mathbb{R}[x_1, \ldots, x_n]$ formato da W-invarianti quando W è un sottogruppo finitamente generato di $GL(\mathbb{R}^n)$ generato da riflessioni. E' infatti questo l'unico caso in cui possiamo trovare un isomorfismo fra R e $\mathbb{R}[x_1, \ldots, x_n]$.
Introduciamo innanzittutto la notazione che useremo nel resto del capitolo: W è un sottogruppo di $GL(\mathbb{R}^n)$ generato da riflessioni che agisce su uno spazio euclideo n-dimensionale V su $\mathbb{R}$ che identificheremo con $\mathbb{R}^n$. Quindi avremo che W agisce naturalmente anche su S che è l'anello dei polinomi di V e che possiamo quindi identificare con $\mathbb{R}[x_1, \ldots, x_n]$. Inoltre $R \subset S$ sarà l'anello dei W-invarianti di S, I l'ideale di S generato da $R^+ = \{f \in R \text{ tale che } f_0 = 0\}$ dove f_i indica la componente omogenea di grado i di f.

Lemma 3.0.4. *Siano $f_1, \ldots, f_r \in R$ con f_1 non appartenente all'ideale di R generato da $f_2, \ldots, f_r$. Supponiamo che $g_1, \ldots, g_r$ siano elementi omogenei di S che soddisfano $f_1 g_1 + \ldots + f_r g_r = 0$. Allora $g_1 \in I$.*

Dimostrazione. Osserviamo innanzitutto che f_1 non può essere nell'ideale di S generato da $f_2, \ldots, f_r$. Altrimenti avremmo che:

$$f_1 = f_2 h_2 + \ldots + f_r h_r$$

per certi $h_i \in S$. Applicando $^{\#}$ avremmo:

$$f_1 = f_1^{\#} = f_2 h_2^{\#} + \ldots + f_r h_r^{\#}.$$

Dato che $h_i^{\#} \in R$ allora f_1 è nell'ideale di R generato da $f_2, \ldots, f_r$ contro l'ipotesi. Ora, per provare che $g_1 \in I$ procediamo per induzione su $deg(g_1)$. Se g_1 è costante deve essere nullo e quindi è in I altrimenti contraddirebbe l'ipotesi sugli f_i. Sia ora $deg(g_1) > 0$. Consideriamo una tipica riflessione $s = s_\alpha$ in W e sia l un polinomio lineare il cui insieme di zeri sia l'iperpiano H_α in $\mathbb{R}^n$ fissato da s. E' immediato vedere che $sg_i - g_i$ si annulla in tutti i punti di H_α dato che s fissa quei punti. Possiamo usare quindi il lemma precedente per trovare polinomi h_i per cui $sg_i - g_i = lh_i$. Sia g_i che sg_i sono omogenei e di grado uguale quindi gli h_i devono essere omogenei e di grado inferiore a g_i. Applichiamo s a $f_1 g_1 + \ldots + f_r g_r = 0$ e otteniamo che

$$f_1(sg_1) + \ldots f_r(sg_r) = 0. \tag{3.1}$$

Sottraendo (3.1) dall'equazione precedente otteniamo che $l(f_1 h_1 + \ldots f_r h_r) = 0$. Siccome l non è identicamente nullo ciò implica che $f_1 h_1 + \ldots f_r h_r$ sia nullo. Per induzione, dato che $deg(h_i) < deg(g_i)$, otteniamo $h_1 \in I$. Quindi $sg_1 - g_1 \in I$ cioè $sg_1 \equiv g_1 (mod I)$. Dato che W stabilizza R^+ e, quindi, anche I, W agisce naturalmente su R/I. Abbiamo appena visto che ogni riflessione s agisce banalmente sull'immagine di g_1. Dato che W è generato da riflessioni ciò implica che $wg_1 \equiv g_1 (mod I) \forall w \in W$. Di conseguenza $g_1^{\#} \equiv g_1 (mod I)$. Ma $g_1^{\#}$ è in R^+ quindi in I e perciò $g_1 \in I$ come voluto. □

Lavoreremo con le derivate parziali di questi polinomi. E' utile ricordare alcune regole di derivazione.

Osservazione 3.1. Vale l'identità di Eulero. Sia $f(x_1, \ldots, x_n)$ un polinomio omogeneo. Allora

$$\sum_{i=1}^{n} x_i \frac{\partial f}{\partial x_i} = deg(f) f.$$

Osservazione 3.2. Vale la regola della catena. Siano $z(y)$ e $y(x)$ due funzioni. Allora

$$\frac{\partial z}{\partial x}(x) = \frac{\partial z}{\partial y}(y(x)) \frac{\partial y}{\partial x}(x).$$

Teorema 3.0.5. *Sia R la sottoalgebra di $\mathbb{R}[x_1, \ldots, x_n]$ costituita da W-invarianti. Allora R è generata come algebra da n elementi di grado positivo, omogenei ed algebricamente indipendenti (insieme a 1).*

Dimostrazione. Consideriamo $I \subset S$ l'ideale generato dagli invarianti omogenei con grado positivo. Possiamo scegliere un insieme di generatori $f_1, \ldots, f_r$ per I di cardinalità minima. Dobbiamo vedere che sono algebricamente indipendenti. Dopo aver dimostrato l'indipendenza algebrica, il risultato segue dalla proposizione (2.1.2). Ne seguirà che $r = n$ in quanto $Q(R)$ deve avere grado di trascendenza n su $\mathbb{R}$. Supponiamo allora che $f_1, \ldots, f_r$ siano algebricamente dipendenti cioè che esista un polinomio $h(y_1, \ldots, y_r)$ non identicamente nullo tale che $h(f_1, \ldots, f_r) = 0$. Raffiniamo la nostra scelta di h: sia $ay_1^{l_1} \ldots y_r^{l_r}$ un qualsiasi monomio di h. Se $d_i = deg(f_i)$ sia $d = \sum d_i l_i$ il grado di $af_1^{l_1} \ldots f_r^{l_r}$ in $x_1, \ldots, x_n$. Possiamo quindi sommare i vari monomi di h che hanno lo stesso grado d per ottenere un polinomio che ha la stessa proprietà di h: è chiaro quindi che tutti gli altri monomi di h possono essere scartati. Chiameremo comunque il nuovo polinomio così ottenuto h. Ora dato $h(f_1, \ldots, f_r) = 0$ è ragionevole derivare entrambi i lati rispetto a $x_k \forall k$ usando opportunamente la regola della catena. Avremo quindi che

$$\sum_{i=1}^{n} h_i \frac{\partial f_i}{\partial x_k} = 0 \tag{3.2}$$

dove $h_i = \frac{\partial h}{\partial y_i}(f_1, \ldots, f_n)$. Notiamo che ogni h_i è omogeneo in R di grado $d - d_i$ mentre $\frac{\partial f_i}{\partial x_k}$ sono omogenei in S. Vorremmo applicare il lemma (3.0.4) ma non sappiamo se gli h_i soddisfano le ipotesi del teorema. Rinumeriamo gli h_i se necessario in modo che $h_1, \ldots, h_m$ sia un insieme di generatori di cardinalità minima per l'ideale di R generato da tutti gli h_i. Avremo che $1 \leq m \leq r$. Allora per ogni $i > m$ scriviamo

$$h_i = \sum_{j=1}^{m} g_{ij} h_j$$

dove $g_{ij} \in R$. Come polinomi in $x_1, \ldots, x_n$ gli h_i sono omogenei di grado $d - d_i$ quindi dopo aver eventualmente scartato i termini inutili possiamo assumere che ogni g_{ij} sia omogeneo di grado $d_j - d_i = deg(h_i) - deg(h_j)$. Sostituendo

nell'equazione (3.2) otterremo allora che

$$\sum_{i=1}^{m} h_i \left(\frac{\partial f_i}{\partial x_k} + \sum_{j=m+1}^{r} g_{ij} \frac{\partial f_j}{\partial x_k} \right) = 0 \tag{3.3}$$

per ogni k. Chiameremo l'espressione fra parentesi $p_i \; \forall 1 \leq i \leq m$. Notiamo che ogni p_i è omogeneo in $x_1, \ldots, x_n$ di grado $d_i - 1$. Ora possiamo finalmente applicare il lemma precedente e concludere che $p_1 \in I$. Quindi

$$\frac{\partial f_1}{\partial x_k} + \sum_{j=m+1}^{r} g_{1j} \frac{\partial f_j}{\partial x_k} = \sum_{i=1}^{m} f_i q_i$$

con $q_i \in S$. Se moltiplichiamo entrambi i membri dell'equazione (3.3) per x_k e sommiamo su k possiamo usare la formula di Eulero e avremo

$$d_1 f_1 + \sum_{j=m+1}^{r} d_j g_{1j} f_j = \sum_{i=1}^{m} f_i r_i$$

dove $deg(r_i) > 0$. I termini del membro di sinistra di quest'ultima equazione sono omogenei di grado d_i quindi il termine $f_1 r_1$ nel membro di destra deve annullarsi con gli altri termini di grado diverso da d_1. Dopo aver scartato tutto tranne i termini di grado d_1 vediamo che l'equazione precedente esprime f_1 come un elemento dell'ideale di S generato da $f_2, \ldots, f_r$ che va contro la scelta iniziale degli f_i come insieme di cardinalità minima di generatori. □

Definizione 3.1. Sia $f_1, \ldots, f_n$ un insieme di generatori di R omogenei e algebricamente indipendenti. Allora chiameremo $f_1, \ldots, f_n$ base di invarianti di R.

E' evidente che la base di invarianti di R non è unicamente determinata.

Esempio 3.1. Consideriamo il caso $n = 2$. Vedremo che $f_1 = x_1 + x_2$ e $f_2 = x_1^2 + x_2^2$ possono essere presi come base di invarianti per R. Consideriamo ora $g_1 = x_1 + x_2$ e $g_2 = x_1 x_2$. Abbiamo che $f_1 = g_1$ e $f_2 = g_1^2 - g_2$ cioè possiamo scrivere f_1 e f_2 come combinazione algebrica di g_1 e g_2. Quindi anche g_1 e g_2 sono una base di invarianti per R.

Vogliamo allora vedere quale proprietà hanno in comune i polinomi di basi di invarianti diverse.

Proposizione 3.0.6. *Supponiamo che $f_1, \dots, f_n$ e $g_1, \dots, g_n$ siano due insiemi di generatori omogenei algebricamente indipendenti dell'anello R dei W-invarianti. Denotiamo i gradi dei vari polinomi con $d_i = deg(f_i)$ e $e_i = deg(g_i)$ per ogni $1 \leq i \leq n$. Supponiamo inoltre che i polinomi siano numerati in modo che $d_i \leq d_{i+1}$ e analogamente $e_i \leq e_{i+1}$ per ogni $1 \leq i \leq n$. Allora sarà $d_i = e_i \forall\ i = 1, \dots, n$.*

Dimostrazione. I polinomi g_i possono essere scritti come polinomi negli f_i e viceversa. Per ogni coppia di indici i, j possiamo usare la regola della catena per valutare la derivata parziale $\frac{\partial f_i}{\partial f_j}$:

$$\sum_{k=1}^{m} \frac{\partial f_i}{\partial g_k} \frac{\partial g_k}{\partial f_j} = \delta_{ij}.$$

Questo mostra che le matrici $\left(\frac{\partial f_i}{\partial g_j}\right)$ e $\left(\frac{\partial g_i}{\partial f_j}\right)$ sono una l'inversa dell'altra e quindi entrambe hanno determinante non nullo. L'espansione del primo determinante come somma di prodotti con segno deve coinvolgere un prodotto non nullo del tipo

$$\prod_{i=1}^{n} \frac{\partial f_i}{\partial g_{\sigma(i)}}$$

per una certa $\sigma \in S_n$. Dopo aver eventualmente riordinato i g_i possiamo assumere che $\sigma = id$. Perciò quando f_i è scritto come un polinomio nei $g_1, \dots, g_n$ allora ogni g_i deve effettivamente apparire nella scrittura di f_i. Dopo aver scartato eventuali termini sovrabbondanti possiamo assumere che ogni monomio $g_1^{k_1} \dots g_n^{k_n}$ che occorre nella scrittura di f_i soddisfa $d_i = \sum e_j k_j$. Quindi $d_i \geq e_i$ e quindi anche

$$\sum_{i=1}^{n} d_i \geq \sum_{i=1}^{n} e_i.$$

Scambiando il ruolo di f_i e g_i e ripetendo lo stesso ragionamento possiamo ottenere

$$\sum_{i=1}^{n} d_i \leq \sum_{i=1}^{n} e_i$$

e $d_i \leq e_i$. Possiamo quindi concludere che $d_i = e_i \forall\ i = 1, \dots, n$. □

Definizione 3.2. Sia $f_1, \ldots, f_n$ una base di invarianti di R. Per ogni $i = 1, \ldots, n$ sia $d_i = deg(f_i)$. Chiameremo $d_1, \ldots, d_n$ gradi di W e li scriveremo, per convenzione, in ordine crescente.

A questo punto, per meglio comprendere gli invarianti polinomiali in questione, facciamo un passo indietro e consideriamo gli invarianti di uno spazio vettoriale sotto l'azione di un gruppo qualsiasi. Possiamo vedere l'insieme degli invarianti come l'autospazio di alcuni operatori lineari per l'autovalore 1. Ci servirà però considerare tutti gli autovalori, in particolare la traccia e il determinante della matrice associata all'operatore lineare in questione. Vediamo innanzitutto una descrizione della dimensione dello spazio dei W-invarianti in una rappresentazione lineare arbitraria.

Lemma 3.0.7. *Sia E un qualsiasi W-modulo di dimensione finita su un campo di caratteristica 0. Allora la dimensione dello spazio dei W-invarianti in E è data dalla traccia dell'operatore lineare su E definito da*

$$z = \frac{1}{|W|} \sum_{w \in W} w.$$

Dimostrazione. Notiamo innanzitutto che $wz = z \quad \forall w \in W$. Usando questo fatto possiamo vedere subito che z è idempotente ed è quindi diagonalizzabile con possibili autovalori 0 oppure 1 dato che il suo polinomio minimo divide $x^2 - x$ ed ha quindi radici distinte. Sia ora $E = E_0 \bigoplus E_1$ la decomposizione di E in autospazi. E' chiaro che la traccia di z è $dim(E_1)$. Basterà quindi verificare che E_1 è lo spazio di tutti i W-invarianti in E. Infatti, sia $e \in E_1$, allora

$$e = z \times e = wz \times e = w \times e \quad \forall \quad w \in W.$$

Viceversa se e è W-invariante allora

$$z \times e = \frac{1}{|W|} \sum w \times e = \frac{1}{|W|} \sum e = e$$

quindi $e \in E_1$. □

Possiamo ora sviluppare un'identità di tipo somma-prodotto che si ha spesso quando parliamo di matrici e che coinvolge i gradi di W per quanto riguarda la

parte del prodotto. Per la somma avremo invece una serie di potenze formali che coinvolge l'azione di W su S. Per poter lavorare esplicitamente sugli autovalori estendiamo il campo base da $\mathbb{R}$ a $\mathbb{C}$. Come elemento di ordine finito in $GL(V)$ ogni $w \in W$ agisce tramite una matrice che sarà diagonale in un'adeguata base di $V_{\mathbb{C}}$. Inoltre gli autovalori di w sono radici dell'unità quindi possono essere reali oppure apparire in coppie di complessi coniugati. Ora, se t è un numero complesso, ha senso scrivere:

$$det(1 - tw) = (1 - c_1 t)(1 - c_2 t) \cdots (1 - c_n t) \tag{3.4}$$

dove w ha autovalori $c_1, \ldots, c_n$. Possiamo anche considerare t come un'indeterminata estendendo quindi formalmente il campo base a $\mathbb{C}(t)$. Il reciproco di (3.4) ha un'espressione come serie formale di potenze:

$$\frac{1}{det(1 - tw)} = (1 + c_1 t + c_1^2 t^2 + \ldots) \cdots (1 + c_n t + c_n^2 t^2 + \ldots) =$$

$$\sum_{k \geq 0} \left(\sum_{k = k_1 + \ldots + k_n} c_1^{k_1} \cdots c_n^{k_n} \right) t^k.$$

Proposizione 3.0.8 (Formula di Molien)**.** *Vedendo entrambi i membri dell'equazione come serie formali di potenze in t abbiamo:*

$$\frac{1}{|W|} \sum_{w \in W} \frac{1}{det(1 - tw)} = \prod_{i=1}^{n} \frac{1}{1 - t^{d_i}}. \tag{3.5}$$

Dimostrazione. Fissiamo $w \in W$ con autovalori c_i come prima. Abbiamo visto in precedenza S come l'algebra dei polinomi in $x_1, \ldots, x_n$ che consideriamo come base per V^*. Dopo aver esteso il campo base di V a $\mathbb{C}$ possiamo ora lavorare con una base $z_1, \ldots, z_n$ di V^* dove però V viene inteso come spazio vettoriale su $\mathbb{C}$. Per trovare gli autovalori di w sulle componenti omogenee S_k di S possiamo usare la base dello spazio complesso che consiste di monomi $z_1^{k_1} \cdots z_n^{k_n}$ tali che $k_1 + \ldots + k_n = k$. Questi sono autovettori per w che corrispondono agli autovalori $c_1^{k_1} \ldots c_n^{k_n}$. La somma di questi autovalori è la traccia di w su S_k e ha lo stesso segno del coefficiente di t^k nella prima serie di potenze che abbiamo visto. Considerando questa interpretazione il coefficiente di t^k a sinistra della seconda equazione è la

traccia di

$$\frac{1}{|W|}\sum_{w\in W} w$$

su S_k. Per il lemma precedente questa è precisamente la dimensione di R_k dove con R_k indichiamo lo spazio degli invarianti omogenei di grado k. Ma la dimensione di questo spazio può essere calcolata in un altro modo: se $f_1, \ldots, f_n$ è una base di invarianti di gradi $d_1, \ldots, d_n$ allora i monomi $f_1^{e_1} \cdots f_n^{e_n}$ con $\sum d_i e_i = k$ sono una base di R_k. Il numero di n-uple $(e_1, \ldots, e_n)$ è evidentemente il coefficiente di t^k nella serie di potenze formali

$$(1 + t^{d_1} + t^{2d_1} + \ldots) \cdots (1 + t^{d_n} + t^{2d_n} + \ldots)$$

che è lo stesso del membro di destra. □

A questo punto abbiamo tutti gli strumenti necessari per derivare espressioni che servono a calcolare facilmente somma e prodotto dei gradi di W.
Notiamo innanzitutto che la traccia di ogni $w \in W$ è reale. Avremo quindi che i soli elementi di W con $n-1$ autovalori uguali a 1 saranno l'identità e le N riflessioni. Quindi il polinomio $det(1 - tw)$ è uguale a $(1-t)^n$ se w è l'identità oppure a $(1-t)^{n-1}(1+t)$ se w è una riflessione. In tutti gli altri casi $det(1-tw)$ non è divisibile per $(1-t)^{n-1}$.

Teorema 3.0.9. *Siano $d_1, \ldots, d_n$ i gradi di W. Allora*

$$d_1 d_2 \cdots d_n = |W|$$

e

$$d_1 + d_2 + \ldots d_n = N + n.$$

Dimostrazione. Moltiplicando entrambi i membri di (3.5) per $(1 - t^n)$ otteniamo:

$$\frac{1}{|W|}\left(1 + N\frac{1-t}{1+t} + (1-t)^2 g(t)\right) = \prod_{i=1}^{n} \frac{1}{1 + t + \ldots + t^{d_i - 1}}$$

dove $g(t)$ è una funzione razionale con il denominatore non divisibile per $1-t$. Sia $t = 1$ allora avremo

$$\frac{1}{|W|} = \frac{1}{d_1 \cdots d_n}$$

cioè

$$|W| = d_1 \cdots d_n.$$

Se, invece, formalmente differenziamo entrambi i membri di (3.5) moltiplicati per $(1-t)^n$ otteniamo:

$$-\frac{2N}{|W|}\frac{1}{(1+t)^2} + h\,(t) =$$

$$\left(\prod_{i=1}^{n}\frac{1}{1+t+\ldots+t^{d_i-1}}\right)\left(\sum_{i=1}^{n}-\frac{1+2t+\ldots+(d_i-1)\,t^{d_i-2}}{1+t+\ldots+t^{d_i-1}}\right)$$

dove $h(t)$ è una funzione razionale con denominatore non divisibile per $1-t$. Per $t=1$ abbiamo quindi

$$-\frac{N}{2|W|} = -\frac{1}{2}\frac{1}{d_1\cdots d_n}\sum_{i=1}^{n}(d_i-1).$$

Sostituendo a $|W|$ il prodotto dei gradi avremo l'espressione desiderata per la somma dei gradi di W. □

Per poter lavorare con esempi un po' più complicati dobbiamo sviluppare un modo efficiente per vedere se un insieme di polinomi è algebricamente indipendente. Sia quindi $J(f_1,\ldots,f_n)$ la matrice $n\times n$ che ha nel posto (i,j) la derivata parziale $\frac{\partial f_i}{\partial x_j}$. Indicheremo con $J = det(J(f_1,\ldots,f_n))$.

Proposizione 3.0.10. *I polinomi $f_1,\ldots,f_n$ nelle variabili $x_1,\ldots,x_n$ sono algebricamente indipendenti su un campo K di caratteristica 0 se e solo se $J(f_1,\ldots,f_n)\neq 0$.*

Dimostrazione. Supponiamo che i polinomi siano algebricamente dipendenti cioè che esista un polinomio $h(y_1,\ldots,y_n)\neq 0$ tale che $h(f_1,\ldots,f_n)=0$. Possiamo assumere che h sia il polinomio di grado minore per cui vale questa proprietà. Per ogni j differenziamo questa condizione rispetto a x_j e usando la regola della catena otteniamo:

$$\sum_{i=1}^{n}\frac{\partial h}{\partial y_i}(f_1,\ldots,f_n)\frac{\partial f_i}{\partial y_j} = 0.$$

Queste equazioni formano un sistema di equazioni lineari su $\mathbb{R}(x_1,\ldots,x_n)$ con matrice dei coefficienti $J(f_1,\ldots,f_n)$ e incognite $\frac{\partial h}{\partial y_i}(f_1,\ldots,f_n)$. Dato che h non è

costante, non tutte le derivate $\frac{\partial h}{\partial y_i}$ possono annullarsi. Ognuna di queste derivate però ha grado minore di h e, per come abbiamo scelto h, tutte le derivate parziali devono essere non nulle. Quindi il sistema lineare ha una soluzione non banale e quindi $J = 0$.

Viceversa supponiamo che $f_1, \dots, f_n$ siano algebricamente indipendenti. Dato che $\mathbb{R}(x_1, \dots, x_n)$ ha grado di trascendenza n su $\mathbb{R}$ i polinomi $x_i, f_1, \dots, f_n$ sono algebricamente dipendenti per ogni $i = 1, \dots, n$. Sia allora $h_i(y_0, \dots, y_n)$ un polinomio non identicamente nullo tale che $h_i(x_i, f_1, \dots, f_n) = 0 \ \forall \ i = 1, \dots, n$. Scegliamo gli h_i in modo che siano quelli di grado minore per cui vale questa proprietà. Differenziando rispetto a x_k otteniamo:

$$\frac{\partial h_i}{\partial x_k}(x_i, f_1, \dots, f_n) = \sum_{i=1}^{n} \frac{\partial h_i}{\partial y_j}(x_i, f_1, \dots, f_n)\frac{\partial f_j}{\partial x_k} + \frac{\partial h_i}{\partial y_0}(x_i, f_1, \dots, f_n)\delta_{ik} = 0.$$

Siccome gli f_i sono algebricamente indipendenti, gli h_i devono avere gradi positivi in y_0. Quindi $\frac{\partial h_i}{\partial y_0}$ è non nullo e di grado minore di h_i: dovrà essere che $\frac{\partial h_i}{\partial y_0}(x_i, f_1, \dots, f_n) \neq 0$. Spostando questi termini non zero a destra per $1 \leq i, k \leq n$ e scrivendo le equazioni in forma matriciale come

$$\left(\frac{\partial h_i}{\partial y_j}\right)\left(\frac{\partial f_i}{\partial x_j}\right) = \left(-\delta_{ij}\frac{\partial h_i}{\partial y_0}\right)$$

otterremo che la matrice a destra è diagonale con determinante non nullo e quindi anche il determinante delle matrici a sinistra deve essere non nullo. □

Corollario 3.0.11. *Supponiamo che $f_1, \dots, f_n$ siano algebricamente indipendenti e omogenei di grado rispettivamente $d_1, \dots, d_n$.*
Allora $J = det(J(f_1, \dots, f_n))$ è omogeneo di grado N dato dall'espressione

$$\sum_{i=1}^{n} (d_i - 1) = N.$$

Dimostrazione. Sappiamo dal teorema precedente che J è non nullo. Possiamo quindi esprimerlo come somma di prodotti con segno e ogni prodotto sarà della forma

$$\frac{\partial f_1}{\partial x_{\sigma(1)}} \cdots \frac{\partial f_n}{\partial x_{\sigma(n)}}$$

per una certa $\sigma \in S_n$. Per ogni prodotto non nullo di questo tipo i termini individuali $\frac{\partial f_i}{\partial x_{\pi(i)}}$ sono non nulli ed omogenei di grado $d_i - 1$ per ogni i quindi ogni prodotto avrà grado

$$\sum_{i=1}^{n} (d_i - 1)$$

che è uguale a N per il teorema precedente. □

A questo punto abbiamo tutto quello che ci serve per dimostrare la seconda implicazione del teorema di Chevalley.

Teorema 3.0.12. *Sia V uno spazio euclideo su $\mathbb{R}$ di dimensione n e W un sottogruppo finito di $GL(V)$ che agisce naturalmente su $S = \mathbb{R}[x_1, \ldots, x_n]$. Supponiamo che l'anello degli invarianti S^W sia generato da n polinomi omogenei algebricamente indipendenti $g_1, \ldots, g_n$. Allora W è generato dalle riflessioni che contiene.*

Dimostrazione. Sia H il sottogruppo di W generato dalle riflessioni di W. Sappiamo che S^H è generato da n polinomi omogenei algebricamente indipendenti $f_1, \ldots, f_n$. Siano $d_i = deg(f_i)$ e $e_i = deg(g_i)$ per ogni $i = 1, \ldots, n$. Evidentemente $S^W \subseteq S^H$, possiamo quindi scrivere i g_i come polinomi negli f_i. Dopo aver eventualmente scartato i termini in eccesso possiamo assumere che ogni monomio $f_1^{k_1} \cdots f_n^{k_n}$ che appare in g_i soddisfi $e_i = \sum d_j k_j$. Usiamo la regola della catena per derivare g_i rispetto a x_k:

$$\frac{\partial g_i}{\partial x_k} = \sum_j \frac{\partial g_i}{\partial f_j} \frac{\partial f_j}{\partial x_k}.$$

Sappiamo che il determinante dello Jacobiano di $\left(\frac{\partial g_i}{\partial x_k}\right)$ non è nullo quindi non lo sarà neanche il determinante dello Jacobiano corrispondente di $\left(\frac{\partial g_i}{\partial f_j}\right)$. Dopo aver eventualmente riordinato gli indici possiamo assumere che il prodotto della forma $\frac{\partial g_1}{\partial f_1} \cdots \frac{\partial g_n}{\partial f_n}$ è non nullo. Questo obbliga $e_i \geq d_i \quad \forall i = 1, \ldots, n$. Possiamo ora applicare il corollario (3.0.11) sia ad H che a W ed avremo che

$$\sum_{i=1}^{n} (d_i - 1) = N = \sum_{i=1}^{n} (e_i - 1)$$

dove N è il numero di riflessioni in H che è anche il numero di riflessioni in W. Quindi $e_i = d_i \quad \forall i$ e $|G| = \prod e_i, |H| = \prod d_i$ cioè $|W| = |H|$. Quindi $W = H$. $\square$

Capitolo 4

Esempi

Vediamo ora la teoria del terzo capitolo applicata in particolare ad alcuni gruppi finiti generati da riflessioni.

4.1 Gruppi di tipo B_n

Definizione 4.1. Sia $n \geq 2$. Definiamo $[\pm n] = \{x \in \mathbb{Z} | 1 \leq |x| \leq n\}$.

Definizione 4.2. Sia $n \geq 2$. Allora $B_n = \{\tau \in S([\pm n]) | \tau(-i) = -\tau(i) \forall i \in [\pm n]\}$ dove con $S([\pm n])$ si intende il gruppo delle biezioni di $[\pm n]$ in se stesso con la composizione come operazione interna.

Se $\alpha \in B_n$ scriviamo $\alpha = [a_1, \ldots, a_n]$ per indicare che $\alpha(i) = a_i \forall i = 1, \ldots, n$. A causa di questa notazione B_n è chiamato gruppo delle permutazioni segnate di $[n]$. Possiamo quindi identificare S_n come sottogruppo di B_n nella maniera naturale. Vogliamo vedere che B_n è generato da riflessioni.

Proposizione 4.1.1. *Sia* $S_B = \{s_1, \ldots, s_{n-1}, s_0\}$ *dove* $s_i = [1, \ldots, i-1, i+1, i, i+2, \ldots, n] \forall i = 1, \ldots, n-1$ *e* $s_0 = [-1, 2, \ldots, n]$. *Allora* S_B *è un insieme di generatori per* B_n.

Dimostrazione. Sia $A \subseteq B_n$ il sottogruppo generato dagli elementi di S_B, vedremo che $B_n \subseteq A$. Supponiamo per assurdo che esista $\tau = [\tau(1), \ldots, \tau(n)] \in B_n$ tale

che $\tau \notin A$. Notiamo innanzitutto che gli s_i per $1 \leq i \leq n-1$ sono i generatori di S_n quindi $\tau \notin A$ implica che τ non sia neanche in S_n: esiste quindi almeno un indice $i \in [n]$ tale che $\tau(i) < 0$. Non è restrittivo assumere che $i = 1$: se così non fosse moltiplichiamo τ per gli $s_i, 1 \leq i \leq n-1$ finchè $\tau(1) < 0$. A questo punto possiamo moltiplicare τ per s_0 e ottenere $(s_0\tau)(1) > 0$. Se τ aveva un solo segno meno allora abbiamo $s_0\tau \in S_n$ e quindi possiamo scrivere

$$s_0\tau = \prod_{i=1}^{n} s_i^{a_i}$$

dove gli $a_i \in \mathbb{N}$. Moltiplicando entrambi i membri per $s_0^{-1} = s_0$ possiamo scrivere τ come prodotto degli elementi di S_B. Se τ avesse altri segni meno allora dopo averlo moltiplicato per s_0 l'avremmo potuto moltiplicare per $s_i, 1 \leq i \leq n$ in modo da avere il segno meno al primo posto per poi ripetere il procedimento appena descritto. Moltiplicando poi per $s_i^{-1} = s_i$ riusciamo di nuovo a scrivere τ come prodotto di elementi di S_B. Cioè $\tau \in A$ e ciò è assurdo. □

Notiamo che questi generatori per B_n sono effettivamente riflessioni: ogni s_i per $i = 1, \ldots, n-1$ è una delle trasposizioni che generano S_n e sappiamo già che queste sono riflessioni mentre s_0 fissa l'iperpiano H di $\mathbb{R}^n$ composto da tutti i vettori $v = (v_1, \ldots, v_n)$ tali che $v_1 = 0$ e manda il vettore e_1 nel suo opposto. Quindi B_n è effettivamente generato da riflessioni.

4.1.1 Invarianti polinomiali

Vediamo come agisce B_n su $\mathbb{R}[x_1, \ldots, x_n]$.

Definizione 4.3. Sia $\alpha \in B_n$, $f(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$. Allora α agisce su f in questo modo:

$$\alpha(f(x_1, \ldots, x_n)) = f(\alpha(x_1), \ldots, \alpha(x_n))$$

dove $\alpha(x_i) = x_{\alpha(i)}$ se $\alpha \in S_n$ mentre $\alpha(x_i) = -x_{-\alpha(i)}$ se $\alpha \in B_n \setminus S_n$.

Osservazione 4.1. Quella appena definita è effettivamente un'azione di gruppo per come l'abbiamo definita nel secondo capitolo. Infatti: definiamo $\eta_B : B_n \to$

$Aut(\mathbb{R}[x_1,\dots,x_n])$ come la funzione che manda $\alpha \in B_n$ in $\alpha(f)$ come definito sopra. Valgono così le tre proprietà dell'azione di gruppo: siano α, $\beta \in B_n$ e f,$g \in \mathbb{R}[x_1,\dots,x_n]$ allora

$$\begin{aligned}\alpha(f+g) &= (f+g)(\alpha(x_1),\dots,\alpha(x_n)) = \\ &= f(\alpha(x_1),\dots,\alpha(x_n)) + g(\alpha(x_1),\dots,\alpha(x_n)) = \alpha(f)+\alpha(g);\end{aligned}$$

$$\begin{aligned}\alpha(fg) &= (fg)(\alpha(x_1),\dots,\alpha(x_n)) = \\ &= f(\alpha(x_1),\dots,\alpha(x_n))g(\alpha(x_1),\dots,\alpha(x_n)) = \alpha(f)\alpha(g);\end{aligned}$$

$$\alpha(\beta(f)) = \alpha(f(\beta(x_1),\dots,\beta(x_n))) = f(\alpha(\beta(x_1)),\dots,\alpha(\beta(x_n))) = (\alpha\circ\beta)(f).$$

Notiamo che, siccome $S_n \subset B_n$, avremo $\mathbb{R}[x_1,\dots,x_n]^{B_n} \subset \mathbb{R}[x_1,\dots,x_n]^{S_n}$. I due anelli fissi non possono chiaramente essere uguali. Sia, ad esempio,

$$\sigma_1 = \sum_{i=1}^{n} x_i$$

e $\alpha \in B_n, \alpha = [-1,\dots,-n]$. Avremo che

$$\begin{aligned}\alpha(\sigma_1(x_1,\dots,x_n)) &= \sigma_1(-x_1,\dots,-x_n) = \\ &= -x_1 + \dots - x_n = -\sigma_1(x_1,\dots,x_n).\end{aligned}$$

Vogliamo usare quello che abbiamo visto nel primo capitolo sui polinomi simmetrici elementari per trovare gli invarianti polinomiali di B_n.

Proposizione 4.1.2. *Sia $f \in \mathbb{R}[x_1,\dots,x_n]^{B_n}$. Allora $f \in \mathbb{R}[x_1^2,\dots,x_n^2]$.*

Dimostrazione. Sia $f \in \mathbb{R}[x_1,\dots,x_n]^{B_n}$. Allora dovrà essere $\alpha f = f$ per ogni $\alpha \in B_n$.
Supponiamo per assurdo che nella scrittura di f esista un monomio f_i in cui x_i ha esponente $2k+1, k \in \mathbb{N}$. Sia allora $\alpha \in B_n$ tale che $\alpha(j) = j\ \forall\, j \neq \pm i$ e $\alpha(i) = -i$. Avremo allora che $\alpha f \neq f$: infatti $\alpha f_i = -f_i$ poichè $\alpha x_i^{2k+1} = (-x_i)^{2k+1} = -x_i^{2k+1}$. Questo però contraddice l'ipotesi che $f \in \mathbb{R}[x_1,\dots,x_n]^{B_n}$. □

L'idea a questo punto è quella di usare come base di invarianti per $\mathbb{R}[x_1,\dots,x_n]^{B_n}$ i polinomi simmetrici elementari nei quadrati delle variabili ovvero $\sigma_i(x_1^2,\dots,x_n^2)$.

Naturalmente, usando i quadrati delle variabili, questi polinomi hanno solo esponenti pari nella loro espressione e quindi non contraddicono la proposizione dimostrata in precedenza. Inoltre facendo agire una qualsiasi $\alpha \in B_n \backslash S_n$ su un qualsiasi polinomio nei quadrati delle variabili questa avrà solo l'effetto di scambiare le variabili quindi B_n agisce come S_n quando abbiamo polinomi con esponenti solo pari. Per avere una base di invarianti per B_n ci basterà quindi scegliere i polinomi simmetrici elementari nei quadrati delle variabili.

4.2 Gruppi di tipo D_n

Definizione 4.4. Sia D_n il sottogruppo di B_n di tutte le permutazioni segnate con un numero pari di meno. Più precisamente $D_n = \{\alpha \in B_n$ tale che $neg(\alpha(1), \ldots, \alpha(n)) \equiv 0(mod 2)\}$ dove $neg(a_1, \ldots, a_n)$ è la funzione che conta gli a_i negativi.

Mostriamo che anche D_n è generato da riflessioni.

Proposizione 4.2.1. *Sia $S_D = \{t_0, \ldots, t_{n-1}\}$ tali che $t_i = s_i$ per ogni $i = 1, \ldots, n-1$ dove s_i sono i generatori di B_n e $t_0 = [-2, -1, 3, \ldots, n] = (1, -2)(2, -1)$. Allora S_D genera D_n.*

Dimostrazione. Sia $A \subseteq D_n$ il sottogruppo di D_n generato dagli elementi di S_D, vogliamo vedere che $D_n \subseteq A$. Supponiamo, per assurdo, che esista $\alpha = [\alpha(1), \ldots, \alpha(n)] \in D_n$ tale che $\alpha \notin A$. Notiamo innanzitutto che i t_i per $i = 1, \ldots, n-1$ sono i generatori di S_n quindi $\alpha \notin A$ implica che $\alpha \notin S_n$: esiste quindi almeno una coppia di indici $i, j \in [n]$ tali che $\alpha(i) < 0$, $\alpha(j) < 0$. Non è restrittivo assumere che $i = 1$, $j = 2$: se così non fosse, moltiplicando α per t_i,$1 \leq i \leq n-1$ potremmo avere la coppia di segni meno nei primi due posti della notazione di α. Così, moltiplicando α per t_0 otteniamo $(t_0\alpha)(1) > 0$ e $(t_0\alpha)(2) > 0$. Se α aveva solo una coppia di segni meno allora avremo che $t_0\alpha \in S_n$ e potremo quindi scrivere

$$t_0\alpha = \prod_{i=1}^{n} t_i^{a_i}$$

dove $a_i \in \mathbb{N}$. Moltiplicando entrambi i membri per $t_0^{-1} = t_0$ possiamo scrivere α come prodotto di elementi di S_D. Se α avesse avuto altre coppie di segni meno allora ripetendo più volte il procedimento appena descritto saremmo comunque arrivati a scrivere α come prodotto di elementi di S_D cioè avremmo visto che $\alpha \in A$ e ciò è assurdo. □

4.2.1 Invarianti polinomiali

L'azione di D_n su $\mathbb{R}[x_1, \ldots, x_n]$ è già stata definita nel paragrafo precedente poichè $D_n \subset B_n$ quindi basterà restringere la funzione η_B a D_n: avremo ancora un'azione di gruppo per cui valgono le proprietà che abbiamo visto nel secondo capitolo in quanto valgono in B_n e D_n, essendo sottogruppo di B_n, è chiuso rispetto alla composizione.
Notiamo che $S_n \subset D_n \subset B_n$ quindi $\mathbb{R}[x_1, \ldots, x_n]^{B_n} \subseteq \mathbb{R}[x_1, \ldots, x_n]^{D_n} \subseteq \mathbb{R}[x_1, \ldots, x_n]^{S_n}$. Vedremo che $\mathbb{R}[x_1, \ldots, x_n]^{D_n} \neq \mathbb{R}[x_1, \ldots, x_n]^{B_n}$ e anche che $\mathbb{R}[x_1, \ldots, x_n]^{D_n} \neq \mathbb{R}[x_1, \ldots, x_n]^{S_n}$.

Proposizione 4.2.2. *Sia $l_d = x_1 x_2 \cdots x_n \in \mathbb{R}[x_1, \ldots, x_n]$. Allora $l_d \in \mathbb{R}[x_1, \ldots, x_n]^{D_n}$.*

Dimostrazione. Sia $t_i \in S_D, 1 \leq i \leq n-1$ allora $t_i l_d = l_d$ perchè $l_d = \sigma_n$ è in $\mathbb{R}[x_1, \ldots, x_n]^{S_n}$ e i t_i sono generatori di S_n. Sia invece $t_0 \in S_D$ allora $t_0 l_d = (-x_2)(-x_1)x_3 \cdots x_n = x_2 x_1 x_3 \cdots x_n = l_d$. Quindi l_d è effettivamente in $\mathbb{R}[x_1, \ldots, x_n]^{D_n}$. □

Questo ci mostra che $\mathbb{R}[x_1, \ldots, x_n]^{D_n} \neq \mathbb{R}[x_1, \ldots, x_n]^{B_n}$ in quanto gli invarianti polinomiali di B_n hanno solo variabili con esponenti pari mentre l_d ha solo esponenti dispari.

Proposizione 4.2.3. *Sia $f \in \mathbb{R}[x_1, \ldots, x_n]^{D_n}$. Allora in ogni monomio di f ogni x_i, $i = 1, \ldots, n$ ha grado pari oppure dispari; non esistono quindi monomi di f in cui appaiono x_i con esponente pari e contemporaneamente x_j con esponente dispari.*

Dimostrazione. Sia f un invariante per D_n: se f è un invariante anche per B_n allora sappiamo già che i monomi che lo compongono hanno variabili solo con

esponenti pari. Notiamo che moltiplicando un qualsiasi f invariante per B_n per l_d il polinomio che otteniamo ha le variabili con esponenti solamente dispari. Vogliamo vedere allora che un monomio che ha una variabile con esponente dispari e una con esponente pari non è D_n-invariante. Possiamo limitarci a dimostrare che un monomio dato dal prodotto di sole due variabili x_i con esponente pari e x_j con esponente dispari non è D_n-invariante: infatti se in un polinomio avessimo un monomio di questo tipo allora avremmo che il coefficiente di questo monomio cambia segno e quindi il polinomio non sarebbe D_n-invariante. Sia quindi $g = x_i^{2m+1}x_j^{2n}$ dove n,$m \in \mathbb{N}$. Sia inoltre $\tau \in D_n$, $\tau = [1, \ldots, -j, \ldots, -i, \ldots, n]$ cioè τ è la permutazione segnata che manda i in $-j$ e j in $-i$. Avremo allora che

$$\tau(g) = (-x_i)^{2m+1}(-x_j)^{2n} = -x_i^{2m+1}x_n^{2n} \neq g.$$

Abbiamo così dimostrato l'enunciato. □

Con questa ultima proposizione abbiamo anche trovato una base di invarianti per $\mathbb{R}[x_1, \ldots, x_n]^{D_n}$. Infatti abbiamo visto nella dimostrazione che per scrivere i D_n-invarianti possiamo moltiplicare o sommare fra di loro i σ_i nei quadrati delle variabili di B_n e l_d. Questi polinomi sono però $n+1$: notiamo che $\sigma_n(x_1^2, \ldots, x_n^2)$ è però l_d^2 e non è quindi algebricamente indipendente rispetto agli altri. Prendendo però $\sigma_1(x_1^2, \ldots, x_n^2)$, …, $\sigma_{n-1}(x_1^2, \ldots, x_n^2)$, $\sigma_1(x_1, \ldots, x_n)$ avremo n polinomi algebricamente indipendenti e quindi una base di invarianti per $\mathbb{R}[x_1, \ldots, x_n]^{D_n}$.

4.3 Gruppi diedrali $I_2(m)$

Vediamo ora un esempio nel caso in cui il campo base dell'anello dei polinomi è $\mathbb{C}$ ovvero un campo K con caratteristica 0.

Definizione 4.5. Sia $m \geq 3$. Allora definiamo $I_2(m) = \{A_k, B_k, k = 0, \ldots, m-1\}$ dove

$$A_k = \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix},$$

$$B_k = \begin{pmatrix} 0 & \zeta^k \\ \zeta^{-k} & 0 \end{pmatrix}$$

e $\zeta = e^{\frac{2\pi i}{m}}$ è una radice m-esima dell'unità.

$I_2(m)$ è così un sottinsieme di $GL(\mathbb{C}^2)$ delle matrici di ordine 2 con elementi in $\mathbb{C}$, con il prodotto matriciale come operazione interna è anche un sottogruppo di $GL(\mathbb{C}^2)$.
Vediamo ora quali possono essere due generatori per $I_2(m)$: siano $A_k = \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix}$ e $B_i = \begin{pmatrix} 0 & \zeta^i \\ \zeta^{-i} & 0 \end{pmatrix}$. Avremo allora che:

$$A_k^l = \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix}^l = \begin{pmatrix} \zeta^{lk} & 0 \\ 0 & \zeta^{-lk} \end{pmatrix} = A_{lk}$$

e $A_{lk} \neq Id_2$ a meno che lk non sia un multiplo di m.
Inoltre

$$B_i \times A_k = \begin{pmatrix} 0 & \zeta^i \\ \zeta^{-i} & 0 \end{pmatrix} \times \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix} = \begin{pmatrix} 0 & \zeta^{ik} \\ \zeta^{-ik} & 0 \end{pmatrix} = B_{ik}$$

ovvero moltiplicando una matrice di tipo A_k per una di tipo B_i otteniamo una matrice di tipo B_i. Infine

$$B_i \times B_j = \begin{pmatrix} 0 & \zeta^i \\ \zeta^{-i} & 0 \end{pmatrix} \times \begin{pmatrix} 0 & \zeta^j \\ \zeta^{-j} & 0 \end{pmatrix} = \begin{pmatrix} \zeta^{ij} & 0 \\ 0 & \zeta^{-ij} \end{pmatrix} = A_{ij}$$

cioè moltiplicando due matrici di tipo B_i otteniamo una matrice di tipo A_k. Quindi prendendo A_1 e B_1 potremo scrivere una matrice di $I_2(m)$ come prodotto di queste due matrici.

4.3.1 Invarianti polinomiali

Ci interessano ora gli invarianti polinomiali di $\mathbb{R}[x, y]$ sotto l'azione di $I_2(m)$. Vediamo prima come agisce $I_2(m)$ su $\mathbb{R}[x, y]$.

Definizione 4.6. Siano $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $f \in \mathbb{R}[x, y]$ allora A agisce su f in questo modo:

$$A(f(x, y)) = f(ax + by, cx + dy).$$

Osservazione 4.2. Sia $\eta_I : I_2(m) \to Aut(\mathbb{R}[x,y]$ la funzione che manda $A \in I_2(m)$ in $A(f) \in \mathbb{R}[x,y]$ come sopra descritto. Abbiamo effettivamente un'azione di gruppo che rispetta la definizione data nel secondo capitolo: valgono infatti le tre proprietà dell'azione di gruppo. Siano

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad B = \begin{pmatrix} m & n \\ o & p \end{pmatrix}$$

e f,$g \in \mathbb{R}[x,y]$ allora

$$\begin{aligned} A(f+g) &= (f+g)(ax+by, cx+dy) = \\ &= f(ax+by, cx+dy) + g(ax+by, cx+dy) = \\ &= A(f) + A(g); \end{aligned}$$

$$\begin{aligned} A(fg) &= (fg)(ax+by, cx+dy) = \\ &= f(ax+by, cx+dy)g(ax+by, cx+dy) = A(f)A(g); \end{aligned}$$

$$\begin{aligned} A(B(f)) &= A(f(mx+ny, ox+py)) = \\ &= f(a(mx+ny)+b(ox+py), c(mx+ny)+d(ox+py)) = \\ &= f(x(am+bo)+y(an+bp), x(cm+do)+y(cn+dp)) = \\ &= (A \times B)(f). \end{aligned}$$

Vediamo che $f(x,y) = xy$ e $g(x,y) = x^m + y^m$ sono invarianti. Proveremo in seguito che sono una base di invarianti. Siano $A_k = \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix}$ e $B_k = \begin{pmatrix} 0 & \zeta^k \\ \zeta^{-k} & 0 \end{pmatrix}$ allora:

$$A_k(f(x,y)) = f(\zeta^k x, \zeta^{-k} y) = \zeta^k x \zeta^{-k} y = xy = f(x,y)$$

e

$$B_k(f(x,y)) = f(\zeta^k y, \zeta^{-k} x) = \zeta^k y \zeta^{-k} x = xy = f(x,y)$$

cioè f è un invariante. Mostriamolo anche per g:

$$\begin{aligned} A_k(g(x,y)) &= g(\zeta^k x, \zeta^{-k} y) = (\zeta^k x)^m + (\zeta^{-k} y)^m = \\ &= \zeta^{km} x^m + \zeta^{-km} y^m = x^m + y^m = g(x,y) \end{aligned}$$

e

$$B_k(g(x,y)) = g(\zeta^k y, \zeta^{-k} x) = (\zeta^k y)^m + (\zeta^{-k} x)^m = \\ = \zeta^{km} y^m + \zeta^{-km} x^m = x^m + y^m = g(x,y)$$

in quanto ζ è una radice m-esima dell'unità quindi $\zeta^{km} = 1$.
Vogliamo ora vedere che un qualsiasi invariante sotto l'azione di $I_2(m)$ si può scrivere come polinomio in f e g.

Proposizione 4.3.1. *Sia $h \in \mathbb{R}[x,y]$ omogeneo di grado l. Supponiamo che in ogni monomio di h appaiano sia x che y con grado positivo. Allora $h \in \mathbb{R}[x,y]^{I_2(m)}$ se e solo se h si scrive come somma di potenze di $f(x,y) = xy$.*

Dimostrazione. L'espressione di h come somma di potenze di xy sarà

$$h(x,y) = \sum_{i=0}^{m} (xy)^i$$

dove $m = l/2$.Per vedere che h è un invariante procediamo per induzione sul suo grado. Il caso $l = 0, 1$ è banale. Sia $l \geq 2$ e A una matrice di $I_2(m)$. Avremo allora:

$$A(h) = A\left(\sum_{i=0}^{m} (xy)^i\right) = A((xy)^l) + A\left(\sum_{i=0}^{m-1} (xy)^i\right) = \\ = (A(xy))^l + \sum_{i=0}^{m-1} (xy)^i = (xy)^l + \sum_{i=0}^{m-1} (xy)^i = h$$

cioè h è un invariante.
Viceversa sia h un invariante che abbia sia x che y con grado positivo in ogni monomio. Supponiamo che h non si possa scrivere come somma di potenze di xy: avremo allora che almeno in un monomio di h, x o y ha grado maggiore dell'altra variabile. In particolare avremo che questo monomio può essere scritto come $x^i y^j$ con $i \neq j$. Se $A_k \in I_2(m)$ avremo allora:

$$A_k(x^i y^j) = (\zeta^k x)^i (\zeta^{-k} y)^j = x^i y^j \zeta^{k(i-j)} \neq x^i y^j$$

e analogamente con $B_k \in I_2(m)$ cioè h non è un invariante. Ciò va contro l'ipotesi quindi h si deve scrivere come somma di potenze di xy. □

Proposizione 4.3.2. *Sia $h \in \mathbb{R}[x,y]$ omogeneo di grado l. Supponiamo che in ogni monomio di h appaiano solo la x oppure solo la y. Allora $h \in \mathbb{R}[x,y]^{I_2(m)}$ se e solo se h si scrive come somma di potenze di $g(x,y) = x^m + y^m$.*

Dimostrazione. Sia h scritto come somma di potenze di $x^m + y^m$: sarà

$$h(x,y) = \sum_{i=0}^{n} (x^m + y^m)^i$$

dove n è tale che il grado del polinomio che si ottiene dalla sommatoria sia l. Procediamo per induzione sul grado di h per vedere che è un invariante. Il caso $l = 0, 1$ è banale. Sia $l \geq 2$ e $A \in I_2(m)$. Avremo che:

$$A(h) = A\left(\sum_{i=0}^{n} (x^m + y^m)^i\right) = A((x^m + y^m)^l) + A\left(\sum_{i=0}^{n-1} (x^m + y^m)^i\right) =$$
$$= (A(x^m + y^m))^l + \sum_{i=0}^{n-1} (x^m + y^m)^i = (x^m + y^m)^l + \sum_{i=0}^{n} (x^m + y^m)^i = h$$

cioè h è un invariante.
Viceversa sia h un invariante che abbia monomi in cui compare solo x oppure solo y con grado positivo. Supponiamo che h non si possa scrivere come somma di potenze di $x^m + y^m$: avremo allora che almeno in un monomio di h, x o y ha grado non multiplo di m. Non è restrittivo supporre che ciò accada per un monomio in cui appare solo x: allora in particolare avremo che questo monomio può essere scritto come x^i con $i \neq km$,$k \in \mathbb{N}$. Se $A_k \in I_2(m)$ avremo allora:

$$A_k(x^i) = (\zeta^k x)^i = x^i \zeta^{ki} \neq x^i$$

poichè non essendo nè k nè i multipli di m allora ki non è multiplo di m. Quindi h non è un invariante. Ciò va contro l'ipotesi quindi h si deve scrivere come somma di potenze di $x^m + y^m$. □

Sia ora un polinomio $h \in \mathbb{R}[x,y]^{I_2(m)}$ qualsiasi. Possiamo supporre che $h = h_1 + h_2$ dove h_1 è composto da monomi dove appaiono sia x che y con grado positivo mentre h_2 è composto dai monomi dove appare solamente x o solamente y. Allora sappiamo già che possiamo scrivere h come somma di potenze di $f(x,y) = xy$ e

$g(x, y) = x^m + y^m$ in quanto h_1 si può scrivere come somma di potenze di f e h_2 di g. Inoltre se h si può scrivere come somma di h_1 e h_2 dove h_1 è una somma di potenze di f e h_2 è una somma di potenze di g, allora sicuramente h sarà un invariante.

Abbiamo quindi visto che $f(x, y) = xy$ e $g(x, y) = x^m + y^m$ sono una base di invarianti per $\mathbb{R}[x, y]^{I_2(m)}$.

Bibliografia

[1] Bjorner, Brenti - Combinatorics of Coxeter Groups - Springer - 2005

[2] Humphreys - Reflection Groups and Coxeter Groups - Cambridge University Press -1990

[3] Stanley - Enumerative Combinatorics Volume 2 - Cambridge University Press -1999