Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea Triennale in Matematica

GRUPPI DI PERMUTAZIONI

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa
Marta Morigi

Presentata da:
Francesco Bertozzi

II Sessione
Anno Accademico 2012/2013

Indice

Introduzione

Fino alla prima metà dell'Ottocento con il termine gruppo ci si riferiva ad un insieme di trasformazioni G su un insieme X chiuso rispetto alla composizione e contenente la trasformazione identica e l'inversa di ogni sua trasformazione. Una struttura così definita è ciò che noi oggi chiamiamo gruppo di permutazioni.

Nell'approccio moderno, infatti, un gruppo è un insieme G su cui è definita un'operazione binaria associativa rispetto alla quale esiste un elemento neutro in G e ogni elemento di G ha un inverso.

Questi due approcci sono essenzialmente equivalenti. Infatti ogni gruppo di permutazioni può essere visto come un gruppo astratto, mentre, per il teorema di Cayley, ogni gruppo astratto è in realtà isomorfo ad un gruppo di permutazioni.

In questa tesi si è cercato di sintetizzare i due punti di vista: partendo da un gruppo astratto è stata definita un'azione di tale gruppo su un insieme, ottenendo così un gruppo di permutazioni. Si sono poi studiate le proprietà dei gruppi di permutazioni, ma per quanto appena detto, tali proprietà si possono trasferire anche ad un gruppo astratto che agisce su un insieme.

Esistono tuttavia alcune ragioni per cui è conveniente distinguere i gruppi di permutazioni dai gruppi astratti: un gruppo astratto gode di talune proprietà note che valgono anche per il caso particolare di un gruppo di permutazioni, mentre le proprietà dei secondi sono strettamente legate agli insiemi su cui agiscono e a tali azioni. Vedremo nello specifico che due gruppi di permutazioni isomorfi potrebbero godere di proprietà diverse. Abbiamo introdotto allora la nozione di similarità di gruppi di permutazioni: oltre all'isomorfismo di gruppi, una similarità è costituita anche da una biezione tra gli insiemi su cui tali gruppi agiscono, che assicura che i due gruppi siano identificabili come gruppi di permutazioni.

Innanzittuto sono stati caratterizzati i gruppi intransitivi: si è visto infatti che la condizione di intransitività non è così limitante come potrebbe sembrare in prima analisi. Difatti vale che ogni gruppo intransitivo si immerge in un prodotto diretto di gruppi transitivi, per la precisione è isomorfo ad un prodotto subdiretto di tali gruppi.

Successivamente siamo passati ai gruppi transitivi, soffermandoci dapprima sui gruppi di permutazioni che godono di una proprietà più forte, la transitività multipla, e ne abbiamo dato qualche esempio. In particolare, abbiamo dimostrato che il gruppo delle

proiettività di una retta su un campo finito risulta essere un gruppo semplicemente 2-transitivo.

Una classe più generale di quella dei gruppi più volte transitivi è la classe dei gruppi primitivi, di cui ci siamo occupati in seguito. Abbiamo dimostrato che ogni gruppo primitivo contenente un sottogruppo normale minimale abeliano è isomorfo ad un sottogruppo del gruppo affine di uno spazio vettoriale costruito su un campo finito, il quale, a sua volta, può essere visto come un prodotto semidiretto di due gruppi di permutazioni.

Infine si sono studiati i gruppi imprimitivi. In primo luogo è stato mostrato che ogni prodotto intrecciato di due gruppi di permutazioni è imprimitivo e in seguito si è dimostrato un risultato ancora più forte: vale infatti che ogni gruppo imprimitivo è in realtà un sottogruppo di un prodotto intrecciato di gruppi di permutazioni. Come ultima cosa, sulla base del risultato appena citato, è stato costruito un esempio di gruppo non primitivo.

Capitolo 1

Nozioni Preliminari

In questo elaborato si presumono noti i contenuti dei corsi fondamentali di algebra della laurea triennale. Per eventuali chierimenti o approfondimenti su tali temi si rimanda a [1]. Ricordiamo qui di seguito alcune nozioni che verranno utilizzate spesso.

1.1 Alcuni Concetti Fondamentali della Teoria Dei Gruppi

Sia H un sottogruppo fissato di G, allora è definita in G una relazione $\sim_H$ come segue:

$$x \sim_H y \text{ se e solo se } yx^{-1} \in H.$$

Si verifica facilmente che quella appena definita è una relazione di equivalenza su G.

Definizione 1.1. La classe di quivalenza contenente x è il sottoinsieme

$$Hx = \{hx : h \in H\}$$

ed è detta laterale destro di H contenente x.

Definizione 1.2. Scegliamo ora un elemento da ogni laterale destro di H e definiamo T come l'insieme formato dai rappresentanti scelti per ogni laterale. T si dice trasversale destro di H in G.

Notiamo subito che $G = \bigcup_{\tau \in T} H\tau$. Inoltre $|T|$ è uguale al numero delle classi laterali destre di H. Generalmente come rappresentante di H si sceglie 1; così facendo $1 \in T$.

In maniera del tutto analoga si definiscono le classi laterali sinistre e i trasversali sinistri. Inoltre, se H è un sottogruppo fissato di G il numero di classi laterali destri di H in G è uguale al numero di classi laterali sinistre di H in G e si dice indice di H in G, in simboli $|G : H|$.

Generalizziamo ora la nozione di classi laterali.

Definizione 1.3. Siano X e Y arbitrari sottoinsiemi non vuoti di un gruppo G, definiamo il loro prodotto come il sottoinsieme

$$XY = \{xy : x \in X, y \in Y\}$$

e l'inverso di X come

$$X^{-1} = \{x^{-1} : x \in X\}.$$

Allora è evidente che $Hx = H\{x\}$ è un laterale destro di H e $xH = \{x\}H$ è un laterale sinistro di H se $H \leq G$. Naturalmente la definizione appena data è estendibile ad un numero finito k di sottoinsiemi. In tal caso

$$X_1X_2 \cdots X_k = \{x_1x_2 \cdots x_k : x_i \in X_i\}.$$

Teorema 1.1.1 (di Lagrange)**.** *Sia G un gruppo e $H \leq G$. Allora $|G| = |H| \cdot |G : H|$.*

Corollario 1.1.2. *Sia G un gruppo di ordine finito, allora ogni suo sottogruppo H ha ordine che divide $|G|$.*

Definizione 1.4. Siano G un gruppo e H e K due suoi sottogruppi. Si dice che H e K permutano se $HK = KH$.

Proposizione 1.1.3. *Siano H e K sottogruppi di un gruppo G. Allora*

$$HK \leq G \quad \textit{se e solo se } HK = KH.$$

In tal caso $KH = HK = \langle H, K\rangle$.

Dimostrazione. Supponiamo $HK \leq G$, allora $H \leq HK$ e $K \leq HK$, quindi $KH \subseteq HK$. Applicando gli inversi ad ambo i membri si ottiene $(KH)^{-1} \subseteq (HK)^{-1}$, da cui segue $H^{-1}K^{-1} \subseteq K^{-1}H^{-1}$, ma H e K, essendo sottogruppi, sono uguali ai propri inversi. Cocludiamo allora che $HK \subseteq KH$ e quindi $KH = HK$. Inoltre $\langle H, K\rangle \leq HK$ perché HK è un sottogruppo di G, mentre $HK \subseteq \langle H, K\rangle$ è sempre vera. Quindi $\langle H, K\rangle = HK$. Viceversa supponiamo $HK = KH$: siano $h_i \in H$ e $k_i \in K$ allora:

$$h_1k_1(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1}.$$

Ma $(k_1k_2^{-1})h_2^{-1} = h_3k_3$, con $h_3 \in H$ e $k_3 \in K$. Allora $h_1k_1(h_2k_2)^{-1} = (h_1h_3)k_3 \in HK$, quindi $HK \leq G$. □

Definizione 1.5. Un sottogruppo H di G si dice normale in G se $x^{-1}Hx = H$ per ogni $x \in G$. In tal caso si scrive $H \trianglelefteq G$.

Ovviamente il gruppo identico 1 e G sono sottogruppi normali di G. Notiamo anche che un gruppo abeliano ha solo sottogruppi normali. Infine segue dalla definizione che un sottogruppo normale è sempre permutabile. Allora il prodotto tra un sottogruppo e un sottogruppo normale è sempre un sottogruppo.

Definizione 1.6. Sia N un sottogruppo normale di G, definiamo il gruppo quoziente di N in G, in simboli G/N, come l'insieme di tutte le classi laterali di N in G con l'operazione $(NX)(Ny) = N(xy)$.

Si verifica facilmente che l'operazione è ben definita e associativa, che l'elemento inverso di Nx è Nx^{-1} e che l'elemento neutro è N. Chiaramente $|G/N| = |G : N|$.

Teorema 1.1.4 (Primo Teorema Fondamentale di Isomorfismo di Gruppi)**.**

1. *Sia $\alpha : G \to H$ un omomorfismo di gruppi, allora la mappa ϕ definita da $\phi : (Ker\ \alpha)x \to x^{\alpha}$ è un isomorfismo tra $G/Ker\ \alpha$ e $Im\ \alpha$.*

2. *Sia $N \trianglelefteq G$, allora la mappa π definita da $\pi : x \to Nx$ è un omomorfismo suriettivo di gruppi tra G e G/N. Si ha che $Ker\ \pi = N$ e π è detta proiezione canonica di G sul gruppo quoziente G/N.*

Teorema 1.1.5 (Secondo Teorema Fondamentale di Isomorfismo di Gruppi)**.** *Siano H un sottogruppo e N un sottogruppo normale di G. Allora $N \cap H \trianglelefteq H$ e la mappa definita da $(N \cap H)x \to Nx$ è un isomorfismo tra $H/N \cap H$ e NH/N.*

Teorema 1.1.6 (Terzo Teorema Fondametale di Isomorfismo di Gruppi)**.** *Siano M e N sottogruppi normali di G, con $N \leq M$. Allora $M/N \trianglelefteq G/N$ e $(G/N)/(M/N) \simeq G/M$.*

1.1.1 Automorfismi di Coniugio

Definizione 1.7. Sia G un gruppo e sia $a \in G$. Si dice automorfismo di coniugio indotto da a in G l'applicazione

$$\phi_a : G \to G$$
$$g \to a^{-1}ga.$$

L'elemento $a^{-1}ga$ è detto coniugato di g tramite a.
Indichiamo con $Inn\ G = \{\phi_a : a \in G\}$ l'insieme di tutti gli automorfismi di coniugio di G.

Osservazione 1. Sia G un gruppo e sia H un suo sottogruppo. Allora $H \trianglelefteq G$ se e solo se $H^{\phi_a} \subseteq H$ per ogni $a \in G$.

Proposizione 1.1.7. *Sia G un gruppo. L'applicazione*

$$\phi : G \to Aut\ G$$

$$g \to \phi_g$$

è un omomorfismo di gruppi che ha per immagine $Inn\ G$ e come nucleo il sottogruppo $Z(G) = \{x \in G : xg = gx \text{ per ogni } g \in G\}$, detto centro di G.

Definizione 1.8. Siano $x, y \in G$. Allora x e y si dicono coniugati se esiste $\phi_g \in Inn\ G$ tale che $x^{\phi_g} = y$.

Proposizione 1.1.8. *In un gruppo G la relazione definita da $x \sim y$ se e solo se x e y sono coniugati è una relazione di equivalenza.*

1.1.2 Prodotto diretto e semidiretto di gruppi

Definizione 1.9. Sia $\{G_k : k = 1, \dots, n\}$ una famiglia di gruppi. Definiamo il prodotto cartesiano o prodotto diretto esterno l'insieme:

$$Dr_{k=1,\dots,n} G_k := G_1 \times \cdots \times G_n = \{(g_1, \dots, g_n), \text{ con } g_k \in G_k \text{ per ogni } k = 1, \dots, n\}.$$

Proposizione 1.1.9. *Con l'operazione*

$$(x_1, \dots, x_n)(y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n)$$

si ha che $G_1 \times \cdots \times G_n$ è un gruppo. L'elemento neutro è $(1_{G_1}, \dots, 1_{G_n})$ e l'inverso di $(g_1, \dots, g_n)$ è $(g_1^{-1}, \dots, g_n^{-1})$.

Proposizione 1.1.10. *Per ogni $k = 1, \cdots, n$ consideriamo la funzione*

$$i_k : G_k \to G_1 \times \cdots \times G_n$$

$$g_k \to (1, \dots, 1, g_k, 1, \dots, 1).$$

Allora i_k è un omomorfismo iniettivo di gruppi, la cui immagine $\bar{G}_k$ è un sottogruppo normale di $G_1 \times \cdots \times G_n$ isomorfo a G_k. Inoltre $G_1 \times \cdots \times G_n = \langle \bar{G}_k : k = 1, \cdots, n \rangle$ e $\bar{G}_k \cap \langle \bar{G}_l : l \neq k \rangle = 1$ per ogni $k = 1, \dots, n$.

Dimostrazione. Che i_k sia un omomorfismo iniettivo di gruppi è chiaro dalla definizione. Mostriamo che $\bar{G}_k \trianglelefteq G_1 \times \cdots \times G_n$, supponendo per semplicità di notazione $k = 1$. La dimostrazione è analoga negli altri casi. Si ha che:

$$(x_1^{-1}, \dots, x_n^{-1})(g_1, 1, \dots, 1)(x_1, \dots, x_n) = (x_1^{-1} g_1 x_1, 1, \dots, 1).$$

Poiché $(x_1^{-1} g_1 x_1, 1, \dots, 1) \in \bar{G}_1$, segue che $\bar{G}_1 \trianglelefteq G_1 \times \cdots \times G_n$. Siccome i_k è un omomorfismo iniettivo e $Im\ i_k = \bar{G}_k$, i_k è un isomorfismo tra G_k e $\bar{G}_k$. Sia $(g_1, \dots, g_n) \in G_1 \times \cdots \times G_n$, allora $(g_1, \dots, g_n) = g_1^{i_1} \cdots g_n^{i_n}$, quindi $G_1 \times \cdots \times G_n = \langle \bar{G}_k : k = 1, \cdots, n \rangle$. Infine che $\bar{G}_k \cap \langle \bar{G}_l : l \neq k \rangle = 1$ per ogni $k = 1, \dots, n$ si vede direttamente dalla definizione di $\bar{G}_k$. □

Definizione 1.10. Sia H un gruppo e sia $\{H_k : k = 1, \dots, n\}$ una famiglia di suoi sottogruppi con le seguenti proprietà:

- $H_k \trianglelefteq H$ per ogni $k = 1, \dots, n$
- $H = \langle H_k : k = 1, \dots, n \rangle$
- $H_k \cap \langle H_l : l \neq k \rangle = 1$

Allora H è detto prodotto diretto interno dei suoi sottogruppi H_k.

Osservazione 2. Siano $h_l \in H_l, h_k \in H_k$, con $l \neq k$, allora $h_l h_k = h_k h_l$.

Dimostrazione. $h_l^{-1} h_k^{-1} h_l h_k = h_l^{-1}(h_k^{-1} h_l h_k) = (h_l^{-1} h_k^{-1} h_l) h_k \in H_l \cap H_k = 1$, allora $h_l h_k = h_k h_l$. □

Lemma 1.1.11. *Se H è prodotto interno di una famiglia di suoi sottogruppi normali H_k, con $k = 1, \dots, n$, allora ogni elemento $h \in H$ si scrive in modo unico nella forma $h = h_1 \cdots h_n$, con $h_k \in H_k$ per ogni $k = 1, \dots, n$.*

Dimostrazione. Per definizione di prodotto diretto interno $H = \langle H_k : k = 1, \dots, n \rangle = H_1 \cdots H_n$, allora ogni elemento di H è della forma $h = h_1 \cdots h_n$. Supponiamo che h si scriva anche nella forma $h = x_1 \cdots x_n$, con $x_k \in H_k$, allora $h_1 \cdots h_n = x_1 \cdots x_n$ e, visto che elementi appartenenti a sottogruppi diversi commutano si ottiene $h_k h_1 \cdots h_{k-1} h_{k+1} \cdots h_n = x_k x_1 \cdots x_{k-1} x_{k+1} \cdots x_n$, da cui otteniamo che $h_k x_k^{-1} = (x_1 \cdots x_{k-1} x_{k+1} \cdots x_n)$ $(h_1 \cdots h_{k-1} h_{k+1} \cdots h_n) \in H_k \cap \langle H_l : l \neq k \rangle = 1$. Ne segue $h_k = x_k$ per ogni $k = 1, \cdots, n$. □

Proposizione 1.1.12.

1. *Sia $\{G_k : k = 1, \dots, n\}$ una famiglia di gruppi. Allora il prodotto diretto esterno $Dr_{k=1,\dots,n} G_k$ è uguale al prodotto diretto interno dei suoi sottogruppi normali $\bar{G}_k$, dove $\bar{G}_k = G_k^{i_k}$.*
2. *Viceversa sia H prodotto diretto interno di una famiglia di suoi sottogruppi normali H_k, allora H è isomorfo al prodotto diretto esterno $Dr_{k=1,\dots,n} H_k$.*

Dimostrazione.

1. Grazie alla proposizione 1.1.10 si ha che $\bar{G}_k \trianglelefteq Dr_{k=1,\dots,n} G_k$ per ogni $k = 1, \dots, n$; inoltre $Dr_{k=1,\dots,n} G_k = \langle \bar{G}_k : k = 1, \dots, n \rangle$ e $\bar{G}_k \cap \langle \bar{G}_l : l \neq k \rangle = 1$ per ogni $k = 1, \dots, n$. Allora, per definizione, $Dr_{k=1,\dots,n} G_k$ è prodotto diretto interno dei suoi sottogruppi normali $\bar{G}_k$.

2. Si ha che $H = \langle H_k : k = 1, \dots, n\rangle = H_1 \dots H_n$, allora grazie a 1.1.11 ogni $h \in H$ si scrive in modo unico come $h = h_1 \cdots h_n$, ove $h_k \in H_k$. Allora la seguente funzione:

$$\tilde{i} : H \to Dr_{k=1,\cdots,n} H_k$$

$$h \to (h_1, \cdots, h_n)$$

è ben definita, iniettiva e suriettiva. Mostriamo che $\tilde{i}$ è un omomorfismo. Utilizzando l'osservazione *2* si ha che:

$$(xy)^{\tilde{i}} = (x_1 \cdots x_n y_1 \cdots y_n)^{\tilde{i}} = (x_1 y_1, \cdots x_n y_n)^{\tilde{i}} = (x_1 y_1, \cdots, x_n y_n) =$$

$$(x_1, \cdots, x_n)(y_1, \cdots y_n) = x^{\tilde{i}} y^{\tilde{i}}.$$

□

Grazie a questa proposizione, possiamo ora identificare G_k con $\bar{G}_k$ e il prodotto diretto interno con il prodotto diretto esterno e chiamarli entrambi prodotto diretto.

Proposizione 1.1.13. *Sia $\{G_k : k = 1, \dots, n\}$ una famiglia di sottogruppi normali di G. Allora G è prodotto diretto dei suoi sottogruppi G_k se e solo se:*

1. *dati $g_k \in G_k$ e $g_l \in G_l$, con $l \neq k$, allora $g_l g_k = g_k g_l$;*

2. *ogni $g \in G$ si scrive in modo unico come $g = g_1 \cdots g_n, g_k \in G_k$.*

Dimostrazione. Se G è prodotto diretto dei G_k abbiamo già dimostrato che vale *1.* Inoltre per il lemma 1.1.11 vale *2.* Viceversa se $g_k g_l = g_l g_k$ per ogni $l \neq k$ allora $g_l^{-1} g_k g_l = g_k \in G_k$, quindi $G_k \trianglelefteq G$ per ogni $k = 1, \dots, n$. Supponiamo infine che esista $\tilde{g} \in G_k \cap \langle G_l : l \neq k\rangle$, allora $\tilde{g} \in G$ e $\tilde{g} = 1 \cdots 1 \tilde{g}_k 1 \cdots 1 = \tilde{g} = g_1 \cdots 1_{G_k} \cdots g_n$, con $g_i \in G_i$ per ogni $i = 1, \dots, n$. Quindi, per l'unicità della scrittura, vale che $\tilde{g} = 1$. □

Definizione 1.11. Sia G un gruppo e siano $N \triangleleft G$ e $H < G$ tali che $G = HN$ e $H \cap N = 1$. Allora G è detto prodotto semidiretto interno di H e N e si indica con $H \ltimes N$ o $N \rtimes H$.

Osservazione 3. Ogni elemento di G si scrive in modo unico nella forma $g = hn$, con $h \in H$ e $n \in N$.

Proposizione 1.1.14. *Ogni elemento $h \in H$ induce per coniugio un automorfismo h^α di N e la mappa $\alpha : H \to AutN$ è un omomorfismo di gruppi.*

Dimostrazione. Sia $h^\alpha : N \to G$ definito da $n^{h^\alpha} = h^{-1} n h$. Sappiamo che h^α è un omomorfismo, inoltre, siccome $N \triangleleft G$, si ha che $Im(h^\alpha) = N$. Siano ora $h_1, h_2 \in H$ e $n \in N$, allora $n^{(h_1 h_2)^\alpha} = (h_2^{-1} h_1^{-1}) n (h_1 h_2) = h_2^{-1}(h_1^{-1} n h_1) h_2 = (n^{h_1^\alpha})^{h_2^\alpha}$ □

Proposizione 1.1.15. *Nelle condizioni precedenti, G è prodotto diretto di H e N se e solo se $\alpha = 1$.*

Dimostrazione. Ogni $g \in G$ è del tipo $g = hn$, dove $h \in H$ e $n \in N$. Allora G è prodotto diretto di H e $N \iff hn = nh \iff n = h^{-1}nh$ per ogni $h \in H$ e per ogni $n \in N \iff \alpha = 1$. □

Definizione 1.12. Siano H ed N due gruppi e sia $\alpha : H \to Aut\ N$ un omomorfismo di gruppi. Definiamo prodotto semidiretto esterno l'insieme

$$G = H \ltimes_\alpha N = \{(h, n), h \in H, n \in N\}.$$

Proposizione 1.1.16. *$H \ltimes_\alpha N$ è un gruppo con l'operazione*

$$(h_1, n_1)(h_2, n_2) = (h_1h_2, n_1^{h_2^\alpha} n_2).$$

L'elemento neutro è $(1_H, 1_N)$; inoltre $(h, n)^{-1} = (h^{-1}, (n^{-1})^{(h^\alpha)^{-1}})$.

Dimostrazione. Si ha che: $((h_1, n_1)(h_2, n_2))(h_3, n_3) = (h_1h_2, n_1^{h_2^\alpha} n_2)(h_3, n_3) = (h_1h_2h_3, (n_1^{h_2^\alpha} n_2)^{h_3^\alpha} n_3) = (h_1h_2h_3, (n_1^{h_2^\alpha})^{h_3^\alpha} n_2^{h_3^\alpha} n_3) = (h_1h_2h_3, n_1^{(h_2h_3)^\alpha} n_2^{h_3^\alpha} n_3) = (h_1, n_1)(h_2h_3, n_2^{h_3^\alpha} n_3) = (h_1, n_1)((h_2, n_2)(h_3, n_3))$ e questo prova l'associatività dell'operazione. Inoltre $(h, n)(1_H, 1_N) = (h1_H, n^{1_h} 1_N) = (n, h)$ e $(1_H, 1_N)(h, n) = (1_H, 1_N^{h^\alpha} n) = (h, n)$. Infine $(h, n)(h^{-1}, (n^{-1})^{(h^\alpha)^{-1}}) = (hh^{-1}, n^{(h^{-1})^\alpha}(n^{-1})^{(h^\alpha)^{-1}}) = (1_H, (1_N)^{(h^\alpha)^{-1}}) = (1_H, 1_N)$ e $(h^{-1}, (n^{-1})^{h^\alpha})(n, h) = (h^{-1}h, ((n^{-1})^{(h^\alpha)^{-1}})^{h^\alpha} n) = (h^{-1}h, n^{-1}n) = (1_H, 1_N)$. □

Osservazione 4. Consideriamo le funzioni $i : H \to G$ definita da $h^i = (h, 1_N)$ e $j : N \to G$ definita da $n^j = (1_H, n)$. Esse sono omomorfismi iniettivi da H in G e da N in G rispettivamente. Chiamando H^* e N^* le loro rispettive immagini otteniamo $H \simeq H^*$ e $H \simeq H^*$.

Sia $(h, n) \in G$. Siccome $(h, n) = (h, 1_N)(1_H, n)$ si ha che $G = H^*N^*$. Inoltre è ovvio che $H^* \cap N^* = 1$. Infine $(h, 1_N)^{-1}(1_H, n)(h, 1_N) = (1_H, n^{h^\alpha})$, da cui segue $(h, m)^{-1}(1_H, n)(h, m) = (h^{-1}, (m^{-1})^{(h^\alpha)^{-1}})(1_H, n)(h, m) = (h^{-1}, (m^{-1})^{(h^\alpha)^{-1}} n)(h, m) = (1_H, n^{h^\alpha}) \in N^*$ e quindi $N^* \trianglelefteq G$.

Allora G è prodotto semidiretto interno di H^* e N^*. Osserviamo che H^* agisce su N^* per coniugio esattamente come H agisce su N tramite α. Generalmente identifichiamo N con N^* e H con H^* e diciamo semplicemente che G è prodotto semidiretto di H e N.

1.2 Permutazioni

1.2.1 Il gruppo simmetrico

Definizione 1.13. Sia X un insieme non vuoto. Una biezione $\pi : X \to X$ si dice permutazione su X.

Definizione 1.14. Sia X un insieme non vuoto. L'insieme di tutte le permutazioni su X si dice gruppo simmetrico di X e si indica con $Sym\ X$. Se $X = \{1, 2, \dots, n\}$, $Sym\ X$ si indica con S_n ed è detto gruppo simmetrico su n lettere.

Proposizione 1.2.1. *Con l'operazione di composizione $Sym\ X$ è un gruppo. L'elemento neutro è la biezione identica, quindi l'elemento inverso è chiaramente la biezione inversa. Se $|X| = n$, allora $|Sym\ X| = n!$.*

Definizione 1.15. Sia $i_1, \dots\ i_l$ una successione di elementi distinti di $\{1, \dots, n\}$, tale che $2 \leq l \leq n$. La permutazione $\pi \in S_n$ definita da $i_k\pi = i_{k+1}$ se $k \leq l-1$ e da $i_l\pi = i_1$ e $j\pi = j$ se $j \neq i_1, \dots\ i_l$ si dice ciclo di lunghezza l e si indica con $\gamma = (i_1, \dots, i_l)$. Infine indichiamo con $l(\gamma)$ la lunghezza del ciclo γ.

Definizione 1.16. Due cicli $(i_1, \dots, i_l)$ e $(j_1, \dots, j_k)$ si dicono disgiunti se $\{i_1, \dots, i_l\}$ e $\{j_1, \dots, j_k\}$ sono insiemi disgiunti.

Osservazione 5. Siano $\gamma_1 = (i_1, \dots, i_l)$ e $\gamma_2 = (j_1, \dots, j_k)$ due cicli disgiunti. Allora $\gamma_1\gamma_2 = \gamma_2\gamma_1$.

Proposizione 1.2.2. *Ogni permutazione $1 \neq \pi \in S_n$ si scrive in modo unico, a meno dell'ordine, come prodotto di cicli disgiunti.*

Proposizione 1.2.3.

1. *Sia $\gamma = (i_1, \dots, i_l) \in S_n$ un ciclo di lunghezza l, allora $|\gamma| = l$, ove con $|\gamma|$ indichiamo l'ordine di γ.*
2. *Sia $1 \neq \pi \in S_n$ una permutazione, allora se $\pi = \gamma_1 \cdots \gamma_r$*

$$|\pi| = m.c.m(|\gamma_1|, \dots, |\gamma_r|),$$

ove con $m.c.m(|\gamma_1|, \dots, |\gamma_r|)$ indichiamo il minimo comune multiplo.

1.2.2 Segno di una Permutazione e Gruppo Alterno

Definizione 1.17. Una trasposizione è un ciclo di lunghezza 2, ossia una permutazione di S_n della forma (i, j), con $i, j \in \{1, \dots, n\}$ e $i \neq j$.

Osservazione 6. Sia $(i_1, \dots, i_l)$ un ciclo di lunghezza l. Allora

$$(i_1, \dots, i_l) = (i_1, i_2)(i_1, i_3) \cdots (i_1, i_l).$$

Pertanto ogni ciclo di lunghezza l è prodotto di $l-1$ trasposizioni.

Proposizione 1.2.4. *Sia $\pi \in S_n$ una permutazione. Allora*

$$\pi = \tau_1 \cdots \tau_r,$$

dove $\tau_1, \ldots, \tau_r$ sono trasposizioni.

Teorema 1.2.5. *Sia $\pi \in S_n$. Se π si decompone in prodotto di trasposizioni come $\pi = \tau_1 \cdots \tau_r$ e $\pi = \tau'_1 \cdots \tau'_s$, allora $r \equiv s \ (mod\ 2)$.*

Definizione 1.18. Sia $\pi \in S_n$ una permutazione. Il segno di π si indica con $sgn(\pi)$ e vale 1 se π è prodotto di un numero pari di trasposizioni e -1 se π è prodotto di un numero dispari di trasposizioni. Inoltre π si dice pari se $sgn(\pi) = 1$ e dispari se $sgn(\pi) = -1$.

Proposizione 1.2.6.

1. $sgn(1) = 1$.
2. $sgn(\pi\sigma) = sgn(\pi)sgn(\sigma)$ *per ogni* $\pi, \sigma \in S_n$.

In altri termini, la mappa $sgn : S_n \to (\{1, -1\}, \cdot)$ è un omomorfismo di gruppi.

Definizione 1.19. Definiamo

$$A_n = \{\pi \in S_n : sgn(\pi) = 1\}.$$

Con l'operazione indotta da S_n si verifica grazie a 1.2.6 che A_n è un sottogruppo di S_n. In più, ancora una volta per effetto di 1.2.6, si ha che A_n è normale in S_n.

Capitolo 2

Gruppi di Permutazioni e Azioni di Gruppo

2.1 Nozioni fondamentali

2.1.1 Gruppi di Permutazioni

Definizione 2.1. Sia X un insieme non vuoto, un sottogruppo G di $Sym\ X$ si dice gruppo di permutazioni su X. La cardinalità di X è detta grado del gruppo di permutazioni G.

Definizione 2.2. Due elementi $x, y \in X$ si dicono G-equivalenti se esiste $\pi \in G$ tale che $x\pi = y$.

Proposizione 2.1.1. *Essere G-equivalenti è una relazione di equivalenza.*

Dimostrazione. Sia $x \in X$, allora $x1 = x$. Siano $x, y \in X$ tali che $x\pi = y$, allora $y\pi^{-1} = x$. Siano $x, y, z \in X$ tali che $x\pi = y$ e $y\sigma = z$, allora $x\pi\sigma = z$. □

Definizione 2.3. Le classi di equivalenza della relazione di G-equivalenza sono dette G-orbite. L'orbita contenente x è $\{x\pi : \pi \in G\}$.

Osservazione 7. Le G-orbite formano una partizione di X.

Definizione 2.4. Un gruppo di permutazioni G si dice transitivo se per ogni $x, y \in X$ esiste $\pi \in G$ tale che $x\pi = y$.

Osservazione 8. Un gruppo di permutazioni G su X è transitivo se e solo se l'unica G-orbita è X.

Dimostrazione. G è transitivo $\iff$ per ogni $x, y \in X$esiste $\pi \in G$ tale che $x\pi = y$ $\iff$ per ogni $x, y \in X$ vale che $y \in \{x\pi : \pi \in G\}$ $\iff$ l'unica G-orbita è X. □

Esempio 2.1. Il gruppo $\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ è transitivo su $\{1,2,3,4\}$, mentre il suo sottogruppo $\{1, (1,2)\}$ non lo è.

Definizione 2.5. Sia $Y \subseteq X, Y \neq \emptyset$, definiamo stabilizzatore di Y in G l'insieme

$$St_G(Y) := \{\pi \in G : Y\pi = Y\}.$$

Indicheremo con $St_G(x)$ l'insieme $St_G(\{x\})$.

Definizione 2.6. Sia G un gruppo di permutazioni su X. Allora

1. G si dice semiregolare se $St_G(x) = 1$ per ogni $x \in X$.
2. G si dice regolare se è semiregolare e transitivo.

Proposizione 2.1.2. *$St_G(Y)$ è un sottogruppo di G.*

Dimostrazione. Siano $\pi, \sigma \in St_G(Y)$, allora per ogni $y \in Y$ si ha $y\sigma\pi^{-1} = y\pi^{-1} = y$. □

Proposizione 2.1.3. *Sia G un gruppo di permutazioni su X.*

1. *Sia $x \in X$. Allora la mappa $St_G(x)\pi \to x\pi$ è una biezione tra l'insieme dei laterali destri di $St_G(x)$ e l'orbita di x. Quindi quest'ultima ha cardinalità $|G : St_G(Y)|$.*
2. *Se G è transitivo allora $|G| = |X| \cdot |St_G(x)|$ per ogni $x \in X$.*
3. *Se G è regolare allora $|G| = |X|$.*

Dimostrazione. La mappa in *1* è ben definita e suriettiva per definizione di laterali destri e di orbite. Mostriamo ora l'iniettività: siano $\pi, \sigma \in G$ tali che $x\pi = x\sigma$, allora $\pi\sigma^{-1} \in St_G(x)$ e quindi $St_G(x)\pi = St_G(x)\sigma$. Per 1.1.1 $|G| = |G : St_G(x)| \cdot |St_G(x)|$, ma $|G : St_G(X)|$ coincide con con la cardinalità dell'orbita contenente x. Inoltre, siccome G è transitivo, l'unica G-orbita è l'insieme X e questo prova *2*. Infine da *2* segue immediatamente *3*. □

Proposizione 2.1.4. *Sia G un gruppo di permutazioni su X. Se $x \in X$ e $\pi \in G$, allora $St_G(x\pi) \equiv \pi^{-1}St_G(x)\pi$.*

Dimostrazione. $\sigma \in St_G(x\pi) \iff x\pi\sigma = x\pi \iff x\pi\sigma\pi^{-1} = x \iff \sigma \in \pi^{-1}St_G(x)\pi$. □

Corollario 2.1.5. *Sia G un gruppo di permutazioni transitivo su X. Se G è abeliano, allora G è regolare.*

Dimostrazione. Sia $x \in X$. Se $\pi \in G$ allora $\pi^{-1}St_G(x)\pi = St_G(x\pi)$. Ma $St_G(x) \trianglelefteq G$, perché G è abeliano. Allora $St_G(x) = St_G(x\pi)$ per ogni $\pi \in G$. Siccome G è transitivo una permutazione che fissa x fissa tutto X, quindi G è regolare. □

Definizione 2.7. Siano G un gruppo di permutazioni su X e H un gruppo di permutazioni su Y. Una similarità tra G e H è una coppia (α, β), dove $\alpha : G \to H$ è un isomorfismo e $\beta : X \to Y$ è una biezione, le quali soddisfano la seguente proprietà.

$$\pi\beta = \beta\pi^{\alpha} \text{ per ogni } \pi \in G.$$

Osservazione 9. Se $X = Y$ la regola appena descritta significa $\pi^{\alpha} = \beta^{-1}\pi\beta$, con $\beta \in SymX$. Allora due gruppi di permutazioni G e H sono simili se e solo se G è coniugato ad H in $Sym\ X$.

Esempio 2.2. Se $|X| = |Y|$ allora $SymX$ e $SymY$ sono simili.

Esempio 2.3. I gruppi $G = \langle (1,2)(3,4) \rangle$ e $H = \langle (1,2) \rangle$ sono isomorfi come gruppi, ma come gruppi di permutazioni su $\{1,2,3,4\}$ non sono simili, perché non sono coniugati. Questo esempio mostra che la similarità come gruppi di permutazioni è una condizione più forte dell'essere isomorfi come gruppi.

2.1.2 Azioni di Gruppo e Rappresentazione di Permutazioni

Definizione 2.8. Sia G un gruppo e sia X un insieme non vuoto. Una azione destra di G su X è una funzione $\rho : X \times G \to X$ tale che

- $(x, g_1g_2)\rho = ((x, g_1)\rho, g_2)\rho$ per ogni $x \in X$ e per ogni $g_1, g_2 \in G$
- $(x, 1_G)\rho = x$ per ogni $x \in X$.

Anziché $(x, g)\rho$, risulta più intuitivo scrivere xg, allora le equazioni sopra diventano:

- $x(g_1g_2) = (xg_1)g_2$ per ogni $x \in X, g_1, g_2 \in G$
- $x1_G = x$ per ogni $x \in X$.

Definizione 2.9. Analogamente si definisce azione sinistra di G su X una funzione $\lambda : G \times X \to X$ tale che $(g_1g_2, x)\lambda = (g_1, (g_2, x)\lambda)\lambda$ e $(1_G, x)\lambda = x$. Anche in questo caso preferiamo scrivere gx anziché $(g, x)\lambda$, ottenendo così $(g_1g_2)x = g_1(g_2x)$ e $1_Gx = x$.

Definizione 2.10. Sia G un gruppo e X un insieme non vuoto. Un omomorfismo di gruppi $\gamma : G \to SymX$ è detto rappresentazione di permutazione di G in X.

Osservazione 10. Consideriamo un'azione destra di G in X data da: $(x, g) \to xg$. Fissato $g \in G$, la mappa $x \to xg$ è una permutazione di X che ha come inversa la permutazione $x \to xg^{-1}$. Chiamiamo g^{γ} tale permutazione. Allora

$$x(g_1g_2)^{\gamma} = xg_1g_2 = (xg_1)g_2 = (xg_1^{\gamma})g_2^{\gamma}.$$

Allora l'azione destra di G su X definisce una rappresentazione di permutazione $\gamma : G \to SymX$.

Viceversa sia $\gamma : G \to SymX$ una qualsiasi rappresentazione di permutazione di G in X Allora la mappa $(x, g) \to xg^{\gamma}$ è un'azione di gruppo di G su X.

Osservazione 11. La stessa cosa si può fare con le azioni di gruppo sinistre: se $(g, x) \to gx$ è un'azione sinistra di G su X allora la corrispondente rappresentazione di permutazione è $\gamma : g^\gamma x \to g^{-1}x$. Senza inserire l'inverso γ non sarebbe un omomorfismo.

Queste due osservazioni conducono alla seguente

Proposizione 2.1.6.

1. *È definita una biezione tra le azioni destre di G su X e le rappresentazioni di permutazione di G in X. L'azione $(x, g) \to gx$ corrisponde alla rappresentazione di permutazione $g \to (x \to xg)$.*
2. *È definita una biezione tra le azioni sinistre di G su X e le rappresentazioni di permutazione di G in X. L'azione $(g, x) \to gx$ corrisponde alla rappresentazione di permutazione $g \to (x \to g^{-1}x)$.*

Grazie a questo risultato parleremo indifferentemente di azioni di gruppo e rappresentazioni di permutazione. In particolare le prossime definizioni saranno date sulle rappresentazioni di permutazione ma valgono anche per le azioni di gruppo.

Definizione 2.11. Sia $\gamma : G \to SymX$ una rappresentazione di permutazioni di G in X. La cardinalità di X è detta grado della rappresentazione.

Definizione 2.12. Una rappresentazione γ si dice fedele se $Ker\ \gamma = 1$.

Osservazione 12. Se γ è fedele G è isomorfo ad un gruppo di permutazioni di X.

Definizione 2.13. Una rappresentazione γ si dice transitiva se $Im\ \gamma$ è un gruppo di permutazioni transitivo su X.

Definizione 2.14. Un'orbita di γ è un'orbita di $Im\ \gamma$.

Definizione 2.15. Lo stabilizzatore di $x \in X$ in G è $St_G(x) = \{g \in G : xg^\gamma = x\}$.

Definizione 2.16. Una rappresentazione γ si dice regolare se è transitiva e $St_G(x) = 1$ per ogni $x \in X$.

Osservazione 13. La proposizione 2.1.3 è vera anche nel caso G sia un gruppo che agisce su X.

Teorema 2.1.7 (di Cayley)**.** *Ogni gruppo G è isomorfo ad un sottogruppo di Sym G.*

Definizione 2.17. Sia G un gruppo e siano $\gamma : G \to Sym\ X$ e $\delta : G \to Sym\ Y$ due rappresentazioni di permutazioni di G, allora γ e δ si dicono equivalenti se esiste una biezione $\beta : X \to Y$ tale che

$$\beta g^\delta = g^\gamma \beta \text{ per ogni } g \in G.$$

Se $X = Y$ l'equivalenza tra γ e δ si puo riscrivere nella forma $g^\delta = \beta^{-1} g^\gamma \beta$.

Proposizione 2.1.8. *Siano G un gruppo e $\gamma : G \to Sym\ X$ una rappresentazione di permutazione transitiva di G su X. Allora γ è equivalente alla rappresentazione di permutazione canonica δ di G sull'insieme dei laterali destri di un suo sottogruppo H.*

Dimostrazione. Fissiamo $x \in X$. Sia $H = St_G(x)$ e chiamiamo $\mathfrak{R}$ l'insieme dei laterali destri di H in G. Definiamo

$$\beta : \mathfrak{R} \to X$$

$$Hg \to xg^\gamma.$$

β è ben definita perché $x(hg)^\gamma = xg^\gamma$ se $h \in H$. Inoltre β è suriettiva perché γ è transitiva e β è suriettiva perché $xg^\gamma = xg_1^\gamma \implies gg_1^{-1} \in H \implies Hg = Hg_1$. Infine $(Hg)g_1^\delta\beta = (Hgg_1)\beta = x(gg_1)^\gamma = xg^\gamma g_1^\gamma = (Hg)\beta g_1^\gamma$. □

2.1.3 Classi di coniugio e centralizzatore

Oltre che per moltiplicazione destra e sinistra, è possibile rappresentare un gruppo G come gruppo di permutazioni sull'insieme dei suoi elementi tramite coniugio: se $g \in G$, l'applicazione $\phi_g : x \to g^{-1}xg$ è una permutazione di G e $\phi : G \to Sym\ G$ che a g associa ϕ_g è una rappresentazione di permutazioni. Chiaramente l'orbita di x è formata da tutti gli elementi di G coniugati ad x; quest'orbita si dice classe di coniugio di x. Inoltre risulta chiaro che lo stabilizzatore di x in questo caso è il centralizzatore di x:

$$C_G(x) = \{g \in G : gx = xg\}$$

Allora $|G : C_G(x)|$ coincide con la cardinalità dell'orbita di x e $\{x\}$ è una classe di coniugio se e solo se $x \in Z(G)$.

2.2 Gruppi di Permutazioni Semplici

2.2.1 Teorema di Jordan

Definizione 2.18. Un gruppo G si dice semplice se non è il gruppo identico 1 e i suoi unici sottogruppi normali sono 1 e G.

Teorema 2.2.1 (di Jordan)**.** *Il gruppo alterno A_n è semplice se e solo se $n \neq 1, 2, 4$.*

Dimostrazione. Per effettuare la dimostrazione usiamo il semplice

Lemma 2.2.2. *Se $n \geq 3$ A_n è generato da 3-cicli.*

Dimostrazione. Ogni permutazione pari è prodotto di un numero pari di trasposizioni. Siccome $(a.b)(c, d) = (a, b, c)(a, c, d)$ e $(a, b)(a, c) = (a, b, c)$, una permutazione pari è anche prodotto di 3-cicli. Infine i 3-cicli sono pari quindi si trovano in A_n. □

Innanzitutto notiamo che A_4 non è semplice perché il sottogruppo

$$\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

è normale in A_4. Inoltre A_1 e A_2 hanno ordine 1. Viceversa A_3 è banalmente semplice, poiché ha ordine 3.

Supponiamo ora $n \geq 5$ e supponiamo esista un sottogruppo N non banale e normale in A_n.

Supponiamo N contenga un 3-ciclo (a, b, c). Sia (a', b', c') un altro 3-ciclo e sia $\pi \in S_n$ una permutazione che manda a in a', b in b' e c in c'. Allora $\pi^{-1}(a, b, c)\pi = (a', b', c')$. Nel caso π sia dispari, basta considerare $\pi(e, f)$ che è pari e (e, f) non influisce sul coniugio. Allora $(a', b', c') \in N$ e per il lemma $N = A_n$.

Supponiamo ora che N contenga una permutazione π la cui decomposizione in cicli disgiunti ne contiene uno di lunghezza almeno 4. Sia $\pi = (a_1, a_2, a_3, a_4, ...)....$ Allora N contiene $\pi' = (a_1, a_2, a_3)^{-1}\pi(a_1, a_2, a_3) = (a_2, a_3, a_1, a_4, ...)...$, quindi contiene anche $\pi^{-1}\pi' = (a_1, a_2, a_4)$. Ma per quanto mostrato prima questo è impossibile, quindi gli elementi non banali di N decomposti in cicli disgiunti devono essere prodotto di cicli di lunghezza 2 e 3. Inoltre in questa decomposizione non può esserci un solo 3-ciclo, altrimenti elevando al quadrato si otterrebe che N contiene tale 3-ciclo e questo non è possibile.

Supponiamo ora N contenga $\pi = (a, b, c)(a', b', c')....$ Allora N contiene

$$\pi' = (a', b', c)^{-1}\pi(a', b', c) = (a, b, a')(c, c', b')...$$

e quindi N contiene anche $\pi\pi' = (a, a', c, b, c')...$, il che è impossibile. Allora ogni elemento di N deve essere prodotto di trasposizioni disgiunte.

Sia $\pi = (a, b)(a', b') \in N$, allora N contiene $\pi' = (a, c, b)^{-1}\pi(a, c, b) = (a, c)(a', b')$ per ogni c fissato da π. Quindi N contiene anche $\pi\pi' = (a, b, c)$. Ne segue che se $\pi \in N$ è un elemento non banale π deve essere prodotto di almeno quattro trasposizioni.

Sia $\pi = (a_1, b_1)(a_2, b_2)(a_3, b_3)(a_4, b_4)... \in N$, allora N contiene

$$\pi' = (a_3, b_2)(a_2, b_1)\pi(a_2, b_1)(a_3, b_2) = (a_1, a_2)(a_3, b_1)(b_2, b_3)(a_4, b_4)...,$$

quindi N contiene anche $\pi\pi' = (a_1, a_3, b_2)(a_2, b_3, b_1)$. Con questa contraddizione raggiunta è chiaro che $N = 1$ oppure $N = A_n$. □

Corollario 2.2.3. *Se $n \neq 4$ gli unici sottogruppi normali di S_n sono 1, A_n, e S_n.*

Dimostrazione. I casi $n = 1, 2$ sono banali. Supponiamo $n \geq 3$. Sia $N \trianglelefteq S_n$, allora $N \cap A_n \trianglelefteq A_n$, ma siccome A_n è semplice $A_n \cap N = 1$ o $A_n \leq N$. Nell'ultimo caso, siccome $|A_n| = \frac{1}{2}|S_n|$, si ha che $N = A_n$ oppure $N = S_n$.

Supponiamo $N \cap A_n = 1$, allora, escludendo la permutazione 1, N può contenere solo permutazioni dispari. Sia $\sigma \in N$, allora σ^2 è pari, quindi σ è prodotto di un numero

dispari di trasposizioni. Siccome $N \trianglelefteq S_n$, N contiene tutti i coniugati di σ che sono dispari. Sia β uno di questi coniugati, allora $\sigma\beta$ è pari. L'unica possibilità è quindi $N = 1$. □

Capitolo 3

Gruppi di Permutazioni Finiti

In questo capitolo, se G è un gruppo di permutazioni su X, si sottointende che G e X sono finiti. Tranne quando diversamente indicato, X sarà l'insieme $\{1, 2, ..., n\}$, sicché $G \leq Sym\ X = S_n$. Siccome in questo capitolo ci interessa studiare le proprietà dei gruppi di permutazioni finiti a meno di similarità, non c'è perdita di generalità in questa supposizione. Inoltre, se $Y \subseteq X$, per semplicità di notazione scriveremo lo stabilizzatore di Y in G, in precedenza indicato come $St_G(Y)$, come G_Y.

3.1 Gruppi Intransitivi e Prodotto Subdiretto

Osservazione 14. Sia G un gruppo di permutazioni su X e sia $I = \{xg : g \in G\}$ una G-orbita. Allora la mappa di restrizione

$$\Phi : G \to Sym\ I$$

$$\sigma \to \sigma|_I$$

è un omomorfismo di gruppi.

Inoltre, se $x \in I$ e $g \in G$, si ha per definizione che $xg = xg^{\Phi}$.

Definizione 3.1. Sia G un sottogruppo di un prodotto diretto $Dr_{i=1,...,n}H_i$ e sia

$$\pi_i : Dr_{i=1,...,n}H_i \to H_i$$

$$(h_1, \ldots, h_n) \to h_i$$

la proiezione i-esima. Allora G si dice prodotto subdiretto dei gruppi H_i, con $i = 1, \ldots, n$, se $G^{\pi_i} = H_i$.

Esempio 3.1. Un prodotto diretto di gruppi è in particolare un prodotto subddiretto.

Inoltre, se $G = H_1 \times \cdots \times H_n$, dove gli H_i sono tutti gruppi tra loro isomorfi, allora la diagonale D di G, $D = \{(h, \ldots, h) : h \in H\}$ è un prodotto subdiretto.

Definizione 3.2. Osserviamo che se $G_1, \ldots, G_n$ sono gruppi di permutazioni che agiscono sugli insiemi disgiunti $X_1, \ldots, X_n$ rispettivamente, allora il loro prodotto diretto $G_1 \times \cdots \times G_n$ è in modo naturale un gruppo di permutazioni sull'insieme $X_1 \cup \cdots \cup X_n$, dove l'azione è definita da $x\,(\sigma_1, \ldots, \sigma_n) = x\sigma_i$, con i tale che $x \in X_i$.

Teorema 3.1.1. *Sia G un gruppo di permutazioni intransitivo su X, allora G è simile ad un prodotto subdiretto di gruppi transitivi.*

Dimostrazione. Siano $I_1, \ldots, I_s$ le orbite di G. Per ogni $i = 1, \ldots, s$ sia Φ_i la mappa di restrizione

$$\Phi_i : G \to Sym\ I_i$$

$$\sigma \to \sigma|_{I_i}.$$

Allora Φ_i è un omomorfismo di gruppi per ogni $i = 1, \ldots, s$.

Si consideri $H = G^{\Phi_1} \times \cdots \times G^{\Phi_s}$. Definiamo la seguente mappa:

$$\tilde{\Phi} : G \to G^{\Phi_1} \times \cdots \times G^{\Phi_s}$$

$$\sigma \to (\sigma^{\Phi_1}, \ldots, \sigma^{\Phi_s}).$$

Si ha che $\tilde{\Phi}$ è un omomorfismo di gruppi perché Φ_i è un omomorfismo di gruppi per ogni $i = 1, \ldots, s$.

Osserviamo che se ι è l'applicazione identica di X in se, si ha che $x\iota\sigma^{\tilde{\Phi}} = x\sigma\iota$ per ogni $x \in X$ e per ogni $\sigma \in G$. Infatti se $x \in X$ allora $x \in I_i$ per qualche i, quindi $x\iota\sigma^{\tilde{\Phi}} = x(\sigma^{\Phi_1}, \ldots, \sigma^{\Phi_s}) = x\sigma^{\Phi_i} = x\sigma = x\sigma\iota$, ove abbiamo utilizzato l'osservazione 14.

Inoltre $\sigma \in Ker\ \tilde{\Phi} \iff \sigma|_{I_i}$ è l'identità per ogni $i = 1, \ldots, s \iff \sigma = 1$, in quanto X è unione delle G-orbite. Infine se $\pi_i : G \to G^{\Phi_1} \times \cdots \times G^{\Phi_s} \to G^{\Phi_i}$ è l'i-esima proiezione, si ha che $G^{\tilde{\Phi}\pi_i} = G^{\Phi_i}$, quindi $G^{\tilde{\Phi}}$ è un prodotto subdiretto.

Poichè la coppia $(\iota, \tilde{\Phi})$ è una similarità, si ha quanto voluto. □

3.2 Transitività Multipla

Definizione 3.3. Sia G un gruppo di permutazioni su un insieme X che contiene n elementi. Sia $1 \leq k \leq n$, allora

$$X^{[k]} = \{(a_1, a_2, \ldots, a_k) : a_i \in X \text{ per } i = 1, \ldots, k \text{ e } a_i \neq a_l \text{ se } i \neq l\}.$$

Il gruppo G agisce componente per componente su $X^{[k]}$: sia $\pi \in G$, allora

$$(a_1, \ldots, a_k)\pi = (a_1\pi, \ldots, a_k\pi).$$

Otteniamo così una rappresentazione di permutazioni di G su $X^{[k]}$.

Definizione 3.4. Se l'azione di G su $X^{[k]}$ è transitiva, il gruppo di permutazioni G si dice k-transitivo su X.

Osservazione 15. G è 1-transitivo su X se e solo se G è transitivo su X.

Osservazione 16. La definizione di k-transitività è valida anche nel caso in cui G sia un gruppo che agisce su X e non sia un gruppo di permutazioni.

Proposizione 3.2.1. *Sia G un gruppo di permutazioni transitivo su X. Sia $k > 1$ e sia $a \in X$ fissato. Allora G è k-transitivo se e solo se G_a è $(k-1)$-transititivo su $X \setminus \{a\}$.*

Dimostrazione. Supponiamo che G sia k-transitivo. Siano $(a_1, \dots, a_{k-1}), (a'_1, \dots, a'_{k-1}) \in Y^{[k-1]}$, dove $Y = X \setminus \{a\}$. Allora $a_i \neq a \neq a'_i$ per ogni $i = 1, \dots, k-1$ e per k-transitività esiste $\pi \in G$ tale che $(a_1, \dots, a_{k-1}, a)\pi = (a'_1, \dots, a'_{k-1}, a)$. Quindi $\pi \in G_a$ e $(a_1, \dots, a_{k-1})\pi = (a'_1, \dots, a'_{k-1})$, il che implica che G_a è $(k-1)$-transitivo.

Viceversa supponiamo che G_a sia $(k-1)$-transitivo su Y e prendiamo $(a_1, \dots, a_k)$ e $(\bar{a}_1, \dots, \bar{a}_k)$ in $X^{[k]}$. Siccome G è transitivo esistono π e $\bar{\pi}$ tali che $a_1\pi = a$ e $\bar{a}_1 = a\bar{\pi}$. Inoltre, per $(k-1)$-transitività di G_a, esiste $\sigma \in G_a$ tale che $(a_2\pi, \dots, a_k\pi)\sigma = (\bar{a}_2\bar{\pi}^{-1}, \dots, \bar{a}_k\bar{\pi}^{-1})$. Allora $a_i\pi\sigma\bar{\pi} = \bar{a}_i$ per ogni $i = 2, \dots, k$ e $a_1\pi\sigma\bar{\pi} = a\sigma\bar{\pi} = a\bar{\pi} = \bar{a}_1$ perché $\sigma \in G_a$. Allora $(a_1, \dots, a_k)\pi\sigma\bar{\pi} = (\bar{a}_1, \dots, \bar{a}_k)$ e G è k-transitivo su X. □

Corollario 3.2.2. *La $(k+1)$-transitività implica la k-transitività.*

Proposizione 3.2.3. *Sia G un gruppo di permutazioni k-transitivo di grado n. Allora $|G|$ è divisibile per $n(n-1)\cdots(n-k+1)$.*

Dimostrazione. Dal calcolo combinatorio sappiamo che la cardinalità di $X^{[k]}$ è uguale al numero di permutazioni possibili di k oggetti scelti fra un totale di n oggetti e questo è esattamente uguale a $n(n-1)\cdots(n-k+1)$. Ora il risultato segue direttamente da 2.1.3. □

3.2.1 Gruppi di Permutazioni Semplicemente k-Transitivi

Definizione 3.5. Sia G un gruppo di permutazioni su X. Se l'azione di G su $X^{[k]}$ è regolare G si dice gruppo di permutazioni semplicemente k-transitivo su X.

Osservazione 17. G è semplicemente k-transitivo su X se e solo se per ogni $(a_1, \dots, a_k)$, $(b_1, \dots, b_k) \in X^{[k]}$ esiste ed è unico $\sigma \in G$ tale che $(a_1, \dots, a_k)\sigma = (b_1, \dots, b_k)$.

Dimostrazione. Siano σ e γ tali che $(a_1, \dots, a_k)\sigma = (a_1, \dots, a_k)\gamma = (b_1, \dots, b_k)$. Allora $(a_1, \dots, a_k)\sigma\gamma^1 = (a_1, \dots, a_k)$ quindi $\sigma\gamma^{-1} = 1$ per regolarità dell'azione di G.

Il viceversa è ovvio. □

Proposizione 3.2.4. *Un gruppo di permutazioni k-transitivo G è semplicemente k-transitivo se e solo se $|G| = n(n-1)\cdots(n-k+1)$.*

Dimostrazione. Segue direttamente da 2.1.3. □

Proposizione 3.2.5.

1. *Il gruppo simmetrico S_n è semplicemente n-transitivo.*
2. *Se $n > 2$ il gruppo alterno A_n è semplicemente $(n-2)$-transitivo.*
3. *A meno di similarità A_n e S_n sono gli unici gruppi $(n-2)$-transitivi di grado n e S_n è l'unico gruppo $(n-1)$-transitivo di grado n.*

Dimostrazione.

1. È ovvio per definizione di S_n.
2. È evidente dalla definizione che A_n è transitivo. Siccome A_3 è generato da $(1,2,3)$, è regolare e quindi semplicemente 1-transitivo. Allora l'asserto è vero per $n = 3$. Sia $n > 3$ e sia H lo stabilizzatore di n in A_n. Allora H agisce su $\{1, 2, \cdots, n-1\}$ e contiene tutte e sole le permutazioni pari su $\{1, 2, \ldots, n-1\}$. Per ipotesi induttiva H è $(n-3)$-transitivo su $\{1, 2, \cdots, n-1\}$, quindi A_n è $(n-2)$-transitivo grazie a 3.2.1. Siccome $|A_n| = \frac{1}{2}(n!)$, si ha che A_n è semplicemente $(n-2)$-transitivo per 3.2.4.
3. Sia $G \leq S_n$. Se G è $(n-2)$-transitivo allora $n(n-1)\cdots 3 = \frac{1}{2}(n!)$ divide $|G|$ e $|S_n : G| = 1$ o 2. Allora $G \trianglelefteq S_n$, quindi da 2.2.3 segue $G = A_n$ o $G = S_n$, se $n \neq 4$. Se $n = 4$ bisogna considerare anche il sottogruppo

$$K = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \trianglelefteq S_n,$$

ma è evidente che K non è 2-transitivo: ad esempio non esiste $\sigma \in K$ tale che $(1,2)\sigma = (1,3)$. Infine è chiaro che se G è $(n-1)$-transitivo allora $G = S_n$.

□

3.2.2 Esempi di Gruppi Semplicemente 2- e 3- transitivi

Esempio 3.2. Sia $F = GF(q)$ un campo finito, ove $q = p^m$ e p è un numero primo. Aggiungiamo a F un punto che indicheremo con ∞ e poniamo $X = F \cup \{\infty\}$. Consideriamo l'insieme $L(q)$ formato da tutte le funzioni $\alpha : X \to X$ definite da:

$$x\alpha = \frac{ax + b}{cx + d},$$

ove $a, b, c, d \in F$ e vale $ad - bc \neq 0$. Definiamo $\infty\alpha = a/c$ e $-\frac{d}{c}\alpha = \infty$, così che ogni elemento di X abbia un'immagine tramite α.

Proposizione 3.2.6. *Con l'operazione di composizione $L(q)$ è un gruppo.*

Dimostrazione. Osserviamo innanzitutto che se α è la funzione definita da $x\alpha = \frac{ax+b}{cx+d}$ e sia β è la funzione di $L(q)$ definita da: $x\beta = \frac{dx-b}{-cx+a}$ si ha che:

$$x\alpha\beta = \frac{\frac{ax+b}{cx+d}d - b}{-\frac{ax+b}{cx+d}c - a} = \frac{\frac{adx+bd-bcx-bd}{cx+d}}{\frac{-acx-bc+acx+ad}{cx+d}} = \frac{(ad-bc)x}{ad-bc} = x$$

e analogamente $x\beta\alpha = x$. Allora β è la funzione inversa di α. Ne segue quindi che $L(q)$ è un sottoinsieme del gruppo delle biezioni da X in X ed è chiuso rispetto all'inverso. Inoltre la funzione identica appartiene chiaramente ad $L(q)$, infatti $x1 = \frac{1x+0}{0x+1}$. Rimane quindi da mostrare che $L(q)$ è chiuso rispetto all'operazione di composizione. Sia α la funzione definita da $x\alpha = \frac{ax+b}{cx+d}$ e sia β definita da $x\beta = \frac{ex+f}{gx+h}$, con $ad - bc \neq 0$ e $ef - gh \neq 0$. Si ha che:

$$x\alpha\beta = \frac{\frac{ax+b}{cx+d}e + f}{\frac{ax+b}{cx+d}g + h} = \frac{\frac{aex+be+cfx+df}{cx+d}}{\frac{agx+bg+chx+dh}{cx+d}} = \frac{(ae+cf)x + be + df}{(ag+ch)x + bg + dh}.$$

Per terminare la dimostrazione verifichiamo che $(ae+cf)(bg+dh)-(ag+ch)(be+df) \neq 0$. Ma sviluppando i calcoli si ottiene: $(ae+cf)(bg+dh)-(ag+ch)(be+df) = (ad-bc)(eh-fg) \neq 0$. In conclusione abbiamo ottenuto $\alpha\beta \in L(q)$, per cui $L(q)$ è un sottogruppo del gruppo delle biezioni da X in se. □

Consideriamo allora l'azione di gruppo di $L(q)$ su $F \cup \{\infty\}$: è evidente che lo stabilizzatore di ∞ in $L(q)$ è il sottogruppo $H(q)$ contenente tutte e sole le funzioni α definite da $x\alpha = ax + b$, con $a \neq 0$. Vale allora la seguente:

Proposizione 3.2.7. *Il gruppo $H(q)$ è semplicemente 2-transitivo su F di grado q. Il gruppo $L(q)$ è semplicemente 3-transitivo su $F \cup \{\infty\}$ di grado $q + 1$.*

Dimostrazione. In primo luogo, mostriamo che $H(q)$ è 2-transitivo su F. Siano $x, y, x', y' \in F$, con $x \neq y$ e $x' \neq y'$ allora esistono sempre $a, b \in F$, con $a \neq 0$, tali che $x' = ax + b$ e $y' = ay + b$. Infatti la condizione $x \neq y$ implica che il sistema costituito dalle equazioni nelle incognite a e b scritte in precedenza abbia sempre soluzione, mentre la condizione $x' \neq y'$ assicura che, se (a, b) è una soluzione del sistema, vale $a \neq 0$. Di conseguenza esiste $\pi \in H(q)$ tale che $(x, y)\pi = (x', y')$. Inoltre l'ordine di $H(q)$ è chiaramente $q(q-1)$ e per 3.2.4 concludiamo che $H(q)$ è semplicemente 2-transitivo su F.
Siccome $H(q)$ è 2-transitivo su F e la funzione $x \to 1/x$ manda ∞ in 0, per 3.2.1 otteniamo che $L(q)$ è 3-transitivo su $F \cup \{\infty\}$. Inoltre, per 2.1.3, si ha che $|L(q) : H(q)| = |X| = q + 1$. Si ha quindi che $|L(q)| = (q + 1)q(q - 1)$ e quindi, per 3.2.4, il gruppo $L(q)$ è semplicemente 3-transitivo su $F \cup \{\infty\}$. □

Mostriamo infine un'importante proprietà del gruppo $L(q)$. Sia $PGL(2,q)$ il gruppo delle proiettività della retta proiettiva $\mathbb{P}(F)$ formata da $q+1$ punti. Ricordiamo di seguito alcune fondamentali proprietà riguardanti la retta proiettiva e le sue proiettività; maggiori approfondimenti sull'argomento potranno essere trovati in [5]. Indichiamo con $[x,y]$ i punti della retta proiettiva, ricordando che tali punti sono classi di equivalenza della relazione di $F \times F \setminus \{(0,0)\}$ definita da: $v \sim w$ se e solo se esiste $\lambda \in F \setminus \{0\}$ tale che $v = \lambda w$; in altri termini vale la seguente proprietà: $[x,y] = \lambda[x,y]$, ove λ è un elemento non nullo del campo. Come è noto, fissato un sistema di coordinate omogenee di $\mathbb{P}(F)$, è possibile identificare una proiettività con una classe di equivalenza di matrici invertibili

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix},$$

per le quali rimane sempre valida la regola $A = \lambda A$. Risulta evidente allora che in questa notazione $PGL(2,q)$ agisce su $\mathbb{P}(F)$ tramite moltiplicazione a destra. Vale allora la seguente:

Proposizione 3.2.8. *Il gruppo di permutazioni $L(q)$ è simile a $PGL(2,q)$.*

Dimostrazione. L'applicazione $\varphi : \mathbb{P}(F) \to F \cup \{\infty\}$ definita da $[x,1]\varphi = x$ se $x \in F$ e $[1,0]\varphi = \infty$ è una biezione. Costruiamo l'applicazione $\Phi : PGL(2,q) \to L(q)$ che manda la matrice $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ nella funzione α definita da $x\alpha = \frac{ax+b}{cx+d}$ e osserviamo che Φ è ben definita: infatti $x(\lambda A)^\Phi = \frac{(\lambda a)x+\lambda b}{(\lambda c)x+\lambda d} = \frac{\lambda(ax+b)}{\lambda(cx+d)} = \frac{ax+b}{cx+d} = xA^\Phi$. In più Φ è un omomorfismo di gruppi: siano $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ e $B = \begin{bmatrix} e & g \\ f & h \end{bmatrix}$, allora ricordando che $x\alpha\beta = \frac{(ae+cf)x+be+df}{(ag+ch)x+bg+dh}$, si verifica immediatamente che $(AB)^\Phi = A^\Phi B^\Phi$. Quindi Φ è un omomorfismo di gruppi e che sia suriettivo è ovvio dalla definizione. Mostriamo che Φ è iniettivo. Sia $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$, tale che $xA^\Phi = x$, allora si ha che $xA^\Phi = \frac{\lambda x+0}{0+\lambda}$, da cui segue $A = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Mostriamo infine che (Φ, φ) è la similarità cercata, ovvero che per ogni $A \in PGL(2,q)$ vale $A\varphi = \varphi A^\Phi$: sia $[x,1] \in \mathbb{P}(F)$, allora $[x,1]A\varphi = [x,1]\begin{bmatrix} a & c \\ b & d \end{bmatrix}\varphi = [ax+b, cx+d]\varphi$. Abbiamo allora due possibilità: se $x \neq -d/c$ allora $[ax+b,cx+d]\varphi = [\frac{ax+b}{cx+d},1]\Phi = \frac{ax+b}{cx+d} = x\alpha = [x,1]\varphi A^\Phi$. Se invece $x = -d/c$ si ha: $[ax+b,cx+d]\varphi = [1,0]\varphi = \infty = x\alpha = [x,1]\varphi A^\Phi$. Prendiamo ora $[1,0] \in \mathbb{P}(F)$, allora $[1,0]A\varphi = [a,c]\varphi$ e analizzando entrambe le possibilità come nel caso precedente otteniamo: se $c \neq 0$ segue $[1,0]\varphi = a/c = \infty\alpha = [1,0]\varphi A^\Phi$, mentre se $c = 0$ segue invece $[1,0]\varphi = \infty = \infty\alpha = [1,0]\varphi A^\Phi$. □

Esempio 3.3. Sia $F = GF(q)$ un campo finito, ove $q = p^{2m}$ e p è un numero primo dispari. Come svolto nell'esempio precedente, aggiungiamo l'elemento ∞. La funzione

$\sigma : F \to F$ definita da $x^\sigma = x^{pm}$ è un automorfismo del campo F e ha ordine 2. Definiamo $\infty^\sigma = \infty$ per estendere σ a $X = F \cup \{\infty\}$. Definiamo allora $M(q)$ come l'insieme contentente tutte le funzioni $\alpha : X \to X$ della forma $x\alpha = \frac{ax+b}{cx+d}$ se $ad - bc$ è un quadrato non nullo di F e $x\alpha = \frac{ax^\sigma+b}{cx^\sigma+d}$ se $ad - bc$ non è un quadrato di F, con la condizione che $x\alpha = \infty$ se il denominatore è nullo. Definiamo infine $\infty\alpha = a/c$.

Anche in questo caso, si dimostra che $M(q)$ è un gruppo; allora $M(q)$ è un gruppo di permutazioni su X. Lo stabilizzatore di ∞ in $M(q)$ è il sottogruppo $S(q)$, contenente le funzioni α della forma $x\alpha = ax + b$ se a è un quadrato non nullo di F e $x\alpha = ax^\sigma + b$ se a non è un quadrato. Vale allora la seguente:

Proposizione 3.2.9. *Il gruppo $S(q)$ è semplicemente 2-transitivo su F e il gruppo $M(q)$ è semplicemente 3-transitivo su $F \cup \{\infty\}$.*

Dimostrazione. Sia $x\alpha = ax + b$ che $x\alpha = ax^\sigma + b$ mandano $(0, 1)$ in $(b, a + b)$ e una delle due appartiene a $S(q)$; sia τ definita da $x\tau = a'x^\sigma + b'$ se a non è un quadrato di F o $x\tau = a'x + b'$ se a è un quadrato in F, allora $\alpha^{-1}\tau$ manda $(b, a + b)$ in $(b', a' + b')$, quindi $S(q)$ è 2-transitivo su F. Consideriamo l'endomorfismo del gruppo moltiplicativo di F che manda x in x^2: siccome ha ordine 2, segue da 1.1.4 che in F ci sono esattamente $\frac{1}{2}(q-1)$ quadrati non nulli e ovviamente il numero dei quadrati è uguale a quello dei non quadrati. Allora $S(q)$ ha ordine $2(\frac{1}{2}(q - 1)q) = q(q - 1)$, per cui $S(q)$ è semplicemente 2-transitivo su F.
Siccome $S(q)$ è 2-transitivo e la funzione $x \to 1/x$ appartenente a $M(q)$ manda ∞ in 0 si ha da 3.2.1 che $M(q)$ è 3-transitivo. Infine per 2.1.3 $|M(q) : S(q)| = |X| = q + 1$, allora $|M(q)| = (q + 1)q(q - 1)$ e $M(q)$ è semplicemente 3-transitivo. □

3.3 Gruppi di Permutazioni Primitivi

Definizione 3.6. Sia G un gruppo di permutazioni transitivo su X. Un sottoinsieme proprio $Y \subset X$ contenente almeno due elementi si dice blocco di imprimitività di G se

$$Y = Y\pi \text{ oppure } Y \cap Y\pi = \emptyset \text{per ogni } \pi \in G.$$

Definizione 3.7. Se G non ha blocchi di imprimitività è detto primitivo.

Proposizione 3.3.1. *Sia G un gruppo di permutazioni transitivo su X. Sia Y un blocco di imprimitività di G e definiamo il sottogruppo $H = \{\pi \in G : Y\pi = Y\}$. Scegliamo un qualsiasi trasversale destro T di H in G, allora:*

1. *I sottoinsiemi $Y\tau$, con $\tau \in T$, partizionano X.*
2. *L'azione naturale di G permuta i sottoinsiemi $Y\tau$ nello stesso modo in cui permuta i laterali destri di H, ovvero tramite moltiplicazione a destra.*

3. $|X| = |Y| \cdot |T|$.

Dimostrazione. Fissiamo $b \in Y$ e sia $a \in X$. Per transitività di G esiste $\pi \in G$ tale che $a = b\pi$. Scriviamo $\pi = \sigma\tau$, con $\sigma \in H$ e $\tau \in T$, allora $a = (b\sigma)\tau$, allora $X = \bigcup_{\tau \in T} Y\tau$. Supponiamo ora $Y\tau \cap Y\tau' \neq \emptyset$, allora $Y \cap Y\tau'\tau^{-1} \neq \emptyset$, quindi $Y = Y\tau'\tau^{-1}$ perché Y è un blocco di imprimitività e $\tau'\tau^{-1} \in H$. Siccome τ e τ' sono in una trasversale $\tau = \tau'$ e questo prova *1.* Infine *3* segue direttamente da $|Y\tau| = |Y|$.

Siano $\tau \in T$ e $\pi \in G$ allora $H\tau\pi = H\tau'$, dove $H\tau \to H\tau'$ è una permutazione dei laterali destri di H. Ma $H\tau\pi = H\tau' \iff \tau\pi\tau'^{-1} \in H \iff Y\tau\pi\tau'^{-1} = Y \iff \tau\pi = \tau' \iff Y\tau\pi = Y\tau'$, il che prova *2.* □

Corollario 3.3.2. *Un gruppo di permutazioni transitivo di ordine primo è primitivo.*

Proposizione 3.3.3. *Sia G un gruppo di permutazioni transitivo su X. G è primitivo se e solo se per ogni $a \in X$ si ha che G_a è un sottogruppo massimale di G.*

Dimostrazione. Supponiamo che G_a non sia massimale, allora esiste H tale che $G_a < H < G$. Definiamo $Y = \{a\sigma : \sigma \in H\}$, allora $|Y| \geq 2$, perché $G_a < H$. Supponiamo $Y = X$, allora per ogni $\pi \in G$ esiste $\sigma \in H$ tale che $a\pi = a\sigma$. Da ciò segue $\pi\sigma^{-1} \in G_a$ da cui $\pi = \pi\sigma^{-1}\sigma \in H$, quindi $G = H$, il che è assurdo in quanto abbiamo supposto che $H < G$. Quindi si ha che $Y \subsetneq X$. Infine, se $Y \cap Y\pi \neq \emptyset$ e $a\sigma_1 = a\sigma_2\pi$, con $\sigma_1, \sigma_2 \in H$, segue $\sigma_2\pi\sigma_1^{-1} \in G_a$ che implica $\pi \in H$ e quindi $Y = Y\pi$. Allora Y è un blocco di imprimitività e G non è primitivo.

Vicecersa sia Y un blocco di imprimitività, per transitività di G possiamo suppore $a \in Y$. Definiamo $H = \{\pi \in G : Y\pi = Y\}$, allora H è un sottogruppo di G. Mostriamo che l'azione di H è transitiva su Y: siano $b, c \in Y$, allora esiste $\pi \in G$ tale che $b\pi = c$, ma questo implica $c \in Y \cap Y\pi$, quindi $Y = Y\pi$ e $\pi \in H$. Allora $|Y| = |H : H_a|$. Se $\pi \in G_a$ allora $a = a\pi \in Y \cap Y\pi$, quindi $Y = Y\pi$ e $\pi \in H$. In conclusione: $|X| = |G : G_a|$ e $|Y| = |H : H_a| = |H : G_a|$, così $G_a < H < G$. □

Proposizione 3.3.4. *Ogni gruppo di permutazioni 2-transitivo è primitivo.*

Dimostrazione. Sia G un gruppo di permutazioni 2-transitivo su X e supponiamo che Y sia un blocco di imprimitivià di G in X. Allora esistono $a, b \in Y$ distinti e $c \in X \setminus Y$. Per 2-transitività di G esiste $\pi \in G$ tale che $(a, b)\pi = (a, c)$. Allora $a \in Y \cap Y\pi$, quindi $Y = Y\pi$, ma questo implica $c = b\pi \in Y$ che è assurdo. □

3.3.1 Gruppi Primitivi Risolubili

Definizione 3.8. Un gruppo G si dice risolubile se esiste una catena di sottogruppi

$$1 = G_1 \leq \cdots \leq G_n = G$$

tali che $G_i \trianglelefteq G$ per ogni $i = 1, \ldots, n$ e G_i/G_{i-1} è abeliano per ogni $i = 2, \ldots, n$.

Esempio 3.4. I gruppi S_3 ed S_4 sono risolubili. Infatti per S_3 basta considerare la catena

$$1 \trianglelefteq A_3 \trianglelefteq S_3,$$

mentre per S_4 si considera

$$1 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4,$$

ove $K = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. I quozienti tra due termini successivi di ogni serie, escludendo il caso $K/1$, hanno ordine primo e quindi sono abeliani. Invece $K/1 = K$ è ovviamente abeliano.

Lemma 3.3.5. *Sia N un sottogruppo normale non banale di un gruppo di permutazioni primitivo G su X. Allora N è transitivo su X.*

Dimostrazione. Sia Y una N-orbita di X e prendiamo $a \in Y$. Allora $Y = \{a\sigma : \sigma \in N\}$. Siano $\pi \in G$ e $\sigma \in N$, allora $(a\sigma)\pi = (a\pi)\pi^{-1}\sigma\pi$ e $\pi^{-1}\sigma\pi \in N$, quindi $Y\pi = \{a\pi\sigma^\pi : \sigma \in N\}$, ove σ^π è il coniugato di σ tramite π e per normalità di N osserviamo che $Y\pi$ è esattamente l'N-orbita contenente $a\pi$. Siccome le orbite formano una partizione di X, segue che $Y = Y\pi$ oppure $Y \cap Y\pi = \emptyset$. Ma G è primitivo, allora Y non può essere un blocco di imprimitività e dunque $Y = X$ e N è transitivo oppure ogni N-orbita ha un solo elemento e $N = 1$, ma quest'ultima possibilità è assurda. □

Teorema 3.3.6. *Sia G un gruppo di permutazioni primitivo su un insieme X e supponiamo che G abbia un sottogruppo normale minimale N abeliano. Allora N è un p-gruppo abeliano elementare di ordine p^m per un qualche primo p. Inoltre $N = C_G(N)$ e N è l'unico sottogruppo abeliano minimale di G. Inoltre $G = G_a N$ e $G_a \cap N = 1$ per ogni $a \in X$. Il grado di G è p^m.*

Dimostrazione. Per il lemma precedente il gruppo N è transitivo, quindi per 2.1.5 N è regolare. In più, siccome N è abeliano e normale minimale in G, N è abeliano elementare. Mostriamo innanzitutto che N contiene almeno un elemento di ordine primo p: prendiamo quindi $y \in N$, con $y \neq 1$; se p divide $|y|$, vale $|y| = pm$, allora y^m ha ordine p. Sia quindi $N_p = \{x \in N : x^p = 1\}$: per quanto appena mostrato $N_p \neq 1$ e si vede facilmente che N_p è un sottogruppo di N. In più, per ogni elemento $\bar{n} \in N_p$ e per ogni automorfismo ϕ di G vale $\bar{n}^\phi \in N_p$. Considerando in particolare l'automorfismo di coniugio, risulta $N_p \trianglelefteq G$, allora $N_p = N$. Facciamo infine vedere che l'ordine di N è esattamente p^m per un certo intero m: supponiamo che esista un altro primo q tale che q divide l'ordine di N; siccome N è abeliano, si ha che $N = C_{n_1} \times \cdots C_{n_r}$, ove C_{n_i} è un gruppo ciclico di ordine n_i per ogni $i = 1, \ldots, r$. Segue allora $|N| = n_1 \cdots n_r$ e quindi q divide $n_1 \cdots n_r$. Ma, essendo q primo, questo implica che esiste i tale che q divide n_i. Concludiamo allora che $C_{n_i} = \langle z \rangle$, con z tale che $z^{qs} = 1$, ma questo implicherebbe che z^s ha ordine q, il che è assurdo perché $z^s \in N$ e tutti gli elementi di N hanno ordine p. Ne traiamo che N è abeliano elementare e da questo fatto aggiunto alla regolarità di N segue direttamente che $|X| = p^m$.

Inoltre la regolarità di N implica che $G_a \cap N = N_a = 1$. In più, siccome G è primitivo, G_a è massimale in G, da cui segue $G = G_a N$. Mostriamo ora che $C_G(N) = C_{G_a}(N)N$: sia $g \in C_G(N)$, allora vale $g^{-1}ng = n$. Scrivendo $g = \tilde{g}\tilde{n}$, con $\tilde{g} \in G_a$ e $\tilde{n} \in N$ si ha $(\tilde{g}\tilde{n})^{-1}n(\tilde{g}\tilde{n}) = \tilde{n}^{-1}\tilde{g}^{-1}n\tilde{g}\tilde{n} = n$. Ma N è normale in G, percui si ha che $\tilde{g}^{-1}n\tilde{g} = n'$, con $n' \in N$ e siccome N è abeliano otteniamo $\tilde{n}^{-1}n'\tilde{n} = n'\tilde{n}^{-1}\tilde{n} = n' = n$ da cui segue che $\tilde{g} \in C_{G_a}(N)$ e $g \in C_{G_a}(N)N$. Viceversa, se $\tilde{g}\tilde{n} \in C_{G_a}(N)N$ allora vale che $(\tilde{g}\tilde{n})^{-1}n(\tilde{g}\tilde{n}) = \tilde{n}^{-1}\tilde{g}^{-1}n\tilde{g}\tilde{n} = \tilde{n}^{-1}n\tilde{n} = n\tilde{n}^{-1}\tilde{n} = n$, dunque $\tilde{g}\tilde{n} \in C_G(N)$ e $C_G(N) = C_{G_a}(N)N$. Sia $\pi \in C_{G_a}(N)$ e $\sigma \in N$, vale $a\sigma\pi = a\pi\sigma = a\sigma$ e per transitività di N segue $\pi = 1$, dunque $C_{G_a}(N) = 1$ e $C_G(N) = N$. Sia ora $\bar{N}$ un altro sottogruppo normale minimale di G, allora $N \cap \bar{N} = 1$. Ma $[N, \bar{N}] \subseteq N \cap \bar{N} = 1$, allora $\bar{N} \leq C_G(N) = N$, il che è assurdo. □

Osservazione 18. Il teorema appena citato si applica al caso particolare dei gruppi risolubili. Vale infatti la seguente:

Proposizione 3.3.7. *Sia G un gruppo risolubile e sia N un suo sottogruppo normale minimale. Allora N è abeliano.*

Dimostrazione. Sia $1 = G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ una serie normale in G, tale che G_j/G_{j-1} è abeliano per ogni $j = 2, \ldots, n$. Allora esiste i tale che $G_{i-1} \cap N = 1$ e $G_i \cap N \neq 1$. Ma $G_i \cap N = N$, perché N è normale minimale. Consideriamo allora la proiezione canonica $\pi : G_i \to G_i/G_{i-1}$; è chiaro che $Ker\ \pi = G_{i-1}$. Prendendo $\pi|_N$, la restrizione di π ad N, risulta ovvio che $Ker\ \pi|_N = N \cap G_{i-1} = 1$, quindi $\pi|_N$ è iniettivo e N isomorfo ad un sottogruppo di G_i/G_{i-1}, quindi è abeliano. □

3.3.2 Gruppo Affine

Illustriamo qui di seguito le principali proprietà dello spazio affine e del gruppo delle affinità, maggiori approfondimenti potranno essere trovati in [5]

Definizione 3.9. Sia V uno spazio vettoriale su un campo K, si definisce spazio affine associato a V un insieme X con un'azione regolare del gruppo $(V, +)$.

Osservazione 19. Grazie a 2.1.3 si ha $|X| = |V|$. In particolare, fissato $P_0 \in X$, l'applicazione $\tau_v : V \to X$ che a v associa $P_0 + v$ è biunivoca.

Definizione 3.10. Si definisce dimensione dello spazio affine X la dimensione dello spazio vettoriale associato V.

Definizione 3.11. Una applicazione $F : X \to X$ si dice affinità di X se esiste $\tilde{F} : V \to V$ lineare e invertibile tale che $(P - P_0)^{\tilde{F}} = P^F - P_0^F$ per ogni$P, P_0 \in X$, ove $P - P_0$ è l'unico vettore $v \in V$ tale che $P = P_0 + v$ e analogamente $P^F - P_0^F$ è l'unico vettore w tale che $P^F = P_0^F + w$.

Esempio 3.5. Fissato $v \in V$, l'applicazione

$$v^* : X \to X$$

$$P \to P + v$$

è un'affinità che ha come applicazione lineare associata l'applicazione identica.

Esempio 3.6. Siano $L : V \to V$ un'applicazione lineare e invertibile e $P_0 \in X$. Allora l'applicazione

$$A_{L,P_0} : X \to X$$
$$P \to P_0 + (P - P_0)^L$$

è un'affinità che ha L come applicazione lineare associata. Inoltre $P_0^{A_{L,P_0}} = P_0$ e ogni affinità che lascia invariato P_0 è della forma A_{L,P_0} con L applicazione lineare.

Proposizione 3.3.8. *Sia $F : X \to X$ un'affinità. Allora esistono $P_0 \in X$, $v \in V$ e $L : V \to V$ lineare e invertibile tali che $F = v^* A_{L,P_0}$.*

Possiamo allora identificare un'affinità F con una coppia (A, b), dove A è una matrice invertibile a coefficienti in K e b un vettore di V. Allora per ogni $x \in X$ $x^F = xA + b$. Sia ora $x^G = xC + d$, risulterà quindi $(x^F)^G = xAC + bC + d$ e possiamo identificare l'affinità FG con la coppia $(CA, b\,C + d)$. Sono quindi evidenti le seguenti:

Proposizione 3.3.9. *Sia $Aff\ X$ l'insieme contenente tutte le affinità di X. Con l'operazione di composizione $Aff\ X$ è un gruppo, detto gruppo affine di X. L'elemento neutro è rappresentato dalla coppia $(1, 0)$ e l'inverso di (A, b) è l'elemento $(A^{-1}, -b)$.*

Proposizione 3.3.10. *Sia $GL(V)$ il gruppo di tutte le trasformazioni lineari invertibili, allora l'applicazione $\phi : Aff\ X \to GL(V)$ è un omomorfismo di gruppi.*
Inoltre $Ker\ \phi = V^* := \{v^* : v \in V\}$ è isomorfo a $(V, +)$.

Sia ora V uno spazio vettoriale, possiamo pensare a V come spazio affine che ha se stesso come spazio vettoriale associato. Sia $G = GL(V)$; allora G è un gruppo di permutazioni su V. Allo stesso modo, anche il gruppo delle traslazioni V^* può essere visto come un gruppo di permutazioni su X. Grazie a 3.3.8 abbiamo

$$A := Aff\ V = \langle G, V^* \rangle$$

e per 3.3.10 $V^* \trianglelefteq A$ e $A = GV^*$. È evidente inoltre che $A_{\{0\}} = G$, perché nessun elemento non banale di V^* può fissare il vettore nullo e quindi $G \cap V^* = 1$. In conclusione $A = G \ltimes V^*$.

Teorema 3.3.11. *Ogni gruppo G della forma descritta in 3.3.6 è simile ad un sottogruppo di $Aff\ V$ contenente il sottogruppo delle traslazioni, ove V è uno spazio vettoriale di dimensione m su $GF(p)$,.*

Dimostrazione. G agisce su un insieme X, con $|X| = p^m = |N|$.

Sia V uno spazio vettoriale di dimensione m su $GF(p)$ e $\psi : N \to V$ un qualsiasi isomorfismo di gruppi abeliani.

Se $b \in X$, per regolarità di N si può scrivere in modo unico come $b = a\sigma$, con $\sigma \in N$, allora possiamo definire una biezione $\varphi : X \to V$ tramite la regola $b\varphi = \sigma^\psi$.

Grazie a tale biezione è possibile produrre anche un omomorfismo $\Phi : G \to A = Aff\ V$ come segue: se $\sigma \in N$, allora $\sigma^\Phi = (1, \sigma^\psi)$; invece se $\pi \in G_a$, allora $\pi^\Phi = (\psi^{-1}\phi_\pi\psi, 0)$, dove ϕ_π è il coniugio in N tramite π. Infine definiamo $(\pi\sigma)^\Phi = \pi^\Phi\sigma^\Phi$.

Osserviamo che Φ è ben definita: a $\sigma \in N$ è associata evidentemente una traslazione e se $\psi^{-1}\phi_\pi\psi$ è lineare su V ad ogni elemento di G è associata un'affinità di V. Mostriamo quindi la linearità: $\psi^{-1}\phi_\pi\psi$ è un omomorfismo di gruppi perché composizione di omomorfismi di gruppi quindi è chiaro che $v_1\psi^{-1}\phi_\pi\psi + v_2\psi^{-1}\phi_\pi\psi = (v_1 + v_2)\psi^{-1}\phi_\pi\psi$. Inoltre V è uno spazio vettoriale costruito su $GF(p)$, il che implica $\lambda v = v + \cdots + v$, dove il numero degli addendi del termine a destra è esattamente λ. Ne segue $(\lambda v)\psi^{-1}\phi_\pi\psi = (v + \cdots + v)\psi^{-1}\phi_\pi\psi = v\psi^{-1}\phi_\pi\psi + \cdots + v\psi^{-1}\phi_\pi\psi = (\lambda v)\psi^{-1}\phi_\pi\psi$.
Mostriamo ora che Φ è un omomorfismo: siano $\sigma_1, \sigma_2 \in N$, allora $(\sigma_1\sigma_2)^\Phi = (1, (\sigma_1\sigma_2)^\psi) = (1, \sigma_1^\psi + \sigma_2^\psi) = (1, \sigma_1^\psi)(1, \sigma_2^\psi) = \sigma_1^\Phi\sigma_2^\Phi$. Siano invece $\pi_1, \pi_2 \in G_a$, allora $(\pi_1\pi_2)^\Phi = (\psi^{-1}\phi_{\pi_1\pi_2}\psi, 0) = (\psi^{-1}\phi_{\pi_1}\phi_{\pi_2}\psi, 0) = (\psi^{-1}\phi_{\pi_1}\psi\psi^{-1}\phi_{\pi_2}\psi, 0) = (\psi^{-1}\phi_{\pi_1}\psi, 0)(\psi^{-1}\phi_{\pi_2}\psi, 0) = \pi_1^\Phi\pi_2^\Phi$. Verifichiamo ora che le proprietà di omomorfismo sono rispettate anche per elementi di G generici: consideriamo $xn, ym \in G$, con $x, y \in G_a$ e $n, m \in N$ e verifichiamo che $(xnym)^\Phi = (xn)^\Phi(ym)^\Phi$. Per semplicità di notazione indichiamo con n^y, anziché n^{ϕ_y} il coniugio di n tramite y e osserviamo che $xnym = xyn^ym$, allora $(xnym)^\Phi = (xyn^ym)^\Phi = (xy)^\Phi(n^ym)^\Phi = x^\Phi y^\Phi n^{y\Phi}m^\Phi$. D'altra parte $(xn)^\Phi(ym)^\Phi = x^\Phi n^\Phi y^\Phi m^\Phi = x^\Phi y^\Phi (n^\Phi)^{y^\Phi} m^\Phi$, pertanto è sufficiente verificare $(n^y)^\Phi = n^{\Phi y^\Phi}$. Questo è vero, infatti $(n^\Phi)^{y^\Phi} = (\psi^{-1}\phi_y^{-1}\psi, 0)(1, n^\psi)(\psi^{-1}\phi_y\psi, 0) = (\psi^{-1}\phi_y^{-1}\psi, n^\psi)(\psi^{-1}\phi_y^\psi, 0) = (1, n^\psi\psi^{-1}\phi_y\psi) = (1, (n^y)^\psi) = (n^y)^\Phi$. Abbiamo quindi mostrato che Φ è un omomorfismo.

Inoltre Φ è iniettivo: siano $y \in G_a$ e $n \in N$ tali che $(yn)^\Phi = 1_A$, allora $(yn)^\Phi = y^\Phi n^\Phi = 1_A$, da cui otteniamo $y^\Phi = (n^\Phi)^{-1} \in G \cap V^* = 1$, quindi $y^\Phi = n^\Phi$ e siccome $\Phi|_{G_a}$ e $\Phi|_N$ sono iniettive per definizione ne segue che Φ è iniettivo.

Dunque Φ coristretto alla sua immagine è un isomorfismo e $Im\ \Phi$ contiene $N^\Phi = V^*$. In più la coppia (Φ, φ) è una similarità tra G e $Im\ \Phi$, ovvero vale $\pi\varphi = \varphi\pi^\Phi$ per ogni $\pi \in G$. Infatti sia $\pi \in N$ allora, ricordando che ogni $b \in X$ si scrive in modo unico come $a\sigma$ con $a \in X$ fissato e $\sigma \in N$ e $b\varphi = \sigma^\psi$, si ottiene: $b\pi\varphi = (\sigma\pi)^\psi = \sigma\psi + \pi^\psi = \sigma^\psi(1, \pi^\psi) = b\varphi\pi^\Phi$. Supponiamo invece $\pi \in G_a$, allora $b\pi = a\sigma\pi = a\pi\sigma^\pi = a\sigma^\pi$, da cui segue $b\pi\varphi = (\sigma^\pi)^\psi$, mentre $b\varphi\pi^\Phi = \sigma^\psi(\psi^{-1}\phi_\pi\psi, 0) = \sigma^{\psi\psi^{-1}\phi_\pi\psi} = (\sigma^\pi)^\psi$. Infine se $\pi = yn$, con $y \in G_a$ e $n \in N$ si ha $b\pi\varphi = byn\varphi = by\varphi n^\psi = b\varphi y^\Phi n^\Phi = b\varphi(yn)^\Phi = b\varphi\pi^\Phi$. □

Esempio 3.7. Consideriamo S_3 e il suo sottogruppo normale A_3. Siccome A_3 ha ordine 3, otteniamo che A_3 è abeliano e, siccome è semplice, è normale minimale. Allora grazie a 3.3.6 sappiamo che $S_3 = S_2A_3$, ove $S_2 = \{1, (1, 2)\}$. Inoltre, grazie a 3.3.11, si ottiene che S_3 è simile al gruppo delle affinità di $\mathbb{Z}_3$ che, usando la stessa notazione vista sinora,

indicheremo con A. Infatti, come visto in 3.3.8, le affinità di $\mathbb{Z}_3$ sono esattamente 6, ovvero tutte le possibili combinazioni (a, b), ove a è un elemento invertibile e b è un qualsiasi elemento di $\mathbb{Z}_3$. Vediamo esplicitamente questo risultato: innanzitutto costruiamo l'isomorfismo ψ da A_N in $\mathbb{Z}_3$.

$$\psi : A_n \to \mathbb{Z}_3$$
$$1 \to 0$$
$$(1,2,3) \to [1]$$
$$(1,3,2) \to [2].$$

Si verifica direttamente che questa applicazione è un omomorfismo di gruppi ed essendo definita termine per termine sono evidenti l'iniettività e la suriettività. Ora ogni elemento di $\{1,2,3\}$ si scrive come 1σ, con $\sigma \in A_3$; costruiamo dunque la biezione:

$$\varphi : \{1,2,3\} \to \mathbb{Z}_3$$
$$1 = 1(1) \to [0]$$
$$2 = 1(1,2,3) \to [1]$$
$$3 = 1(1,3,2) \to [2].$$

Infine definiamo l'isomorfismo $\Phi : S_3 \to A$, esattamente come abbiamo visto nella dimostrazione di 3.3.11. Osserviamo che $(1,3) = (1,2)(1,2,3)$ e $(2,3) = (1,2)(1,3,2)$, da cui si ottiene che Φ deve essere costruito come segue:

$$\Phi : S_3 \to A$$
$$1 \to ([1],[0])$$
$$(1,2,3) \to ([1],[1])$$
$$(1,3,2) \to ([1],[2])$$
$$(1,2) \to (\psi^{-1}\phi_{(1,2)}\psi, [0])$$
$$(1,3) \to (\psi^{-1}\phi_{(1,2)}\psi, [1])$$
$$(2,3) \to (\psi^{-1}\phi_{(1,2)}\psi, [2]).$$

Per descrivere meglio l'omomorfismo Φ, resta da determinare esplicitamente l'azione di $\psi^{-1}\phi_{(1,2)}\psi$ sui vettori di $\mathbb{Z}_3$. Scegliamo quindi $\{[1]\}$ come base di $\mathbb{Z}_3$ e vediamo come vi agisce $\psi^{-1}\phi_{(1,2)}\psi$. Allora $[1]\psi^{-1}\phi_{(1,2)}\psi = (1,2)(1,2,3)(1,2)\psi = (1,3,2)\psi = [2]$.

Quindi $\psi^{-1}\phi_{(1,2)}\psi$ è l'applicazione lineare definita dalla moltiplicazione per l'elemento $[2]$ del campo $\mathbb{Z}_3$. Ora è facile verificare direttamente che Φ è un isomorfismo di gruppi e che la coppia (Φ, φ) è una similarità tra S_3 e A.

Esempio 3.8. Consideriamo ora S_4 e il suo sottogruppo normale

$$K = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

L'applicazione

$$\begin{gathered}\psi : K \to \mathbb{Z}_2 \times \mathbb{Z}_2 \\ 1 \to ([0],[0]) \\ (1,2)(3,4) \to ([1],[0]) \\ (1,3)(2,4) \to ([0],[1]) \\ (1,4)(2,3) \to ([1],[1])\end{gathered}$$

è un isomorfismo di gruppi. Inoltre K è un sottogruppo normale minimale di S_4 ed è abeliano. Per 3.3.6 si ha che $S_4 = S_3K$, infatti S_3 è lo stabilizzatore di 4 in S_4.

In più, grazie a 3.3.11, si ottiene che S_4 è simile al gruppo delle affinità di $\mathbb{Z}_2 \times \mathbb{Z}_2$, che ancora sarà indicato con A. Infatti le matrici invertibili a coefficienti in $\mathbb{Z}_2$ sono sei, mentre i vettori di $\mathbb{Z}_2 \times \mathbb{Z}_2$ sono quattro, per cui concludiamo che $|A| = 24$ e perciò il sottogruppo di A simile ad S_4 è il gruppo A stesso.

La similarità cercata è la coppia (Φ, φ), dove $\varphi : \{1,2,3,4\} \to \mathbb{Z}_2 \times \mathbb{Z}_2$ è la biezione che, fissato un elemento $a \in \{1,2,3,4\}$, associa ad un qualsiasi elemento $b \in \{1,2,3,4\}$ l'elemento σ^ψ di $\mathbb{Z}_2 \times \mathbb{Z}_2$, ove σ è l'unica permutazione in K tale che $b = a\sigma$, mentre $\Phi : S_4 \to A$ è l'isomorfismo definito da $\sigma^\Phi = (1, \sigma^\psi)$ se $\sigma \in K$ e $\pi^\Phi = (\psi^{-1}\phi_\pi\psi, ([0],[0]))$ se $\pi \in S_3$.

Un altro sottogruppo importante di S_4 è il gruppo diedrale di ordine 8, indicato con D_8, ovvero il gruppo delle simmetrie del quadrato. Vale che $D_8 = \langle (1,2,3,4), \sigma \rangle$, ove $\sigma \in K \setminus \{1\}$. Osserviamo ora che $(2,4) = (1,3)(1,3)(2,4)$, $(1,2,3,4) = (1,3)(1,4)(2,3)$ e $(1,4,3,2) = (1,3)(1,2)(3,4)$ e determiniamo l'immagine di D_8 tramite Φ:

$$\begin{gathered}\Phi : D_8 \to A \\ 1 \to (1, ([0],[0])) \\ (2,4) \to (\psi^{-1}\phi_{(1,3)}\psi, ([0],[1])) \\ (1,3) \to (\psi^{-1}\phi_{(1,3)}\psi, ([0],[0])) \\ (1,2)(3,4) \to (1, ([1],[0])) \\ (1,3)(2,4) \to (1, ([0],[1])) \\ (1,4)(2,3) \to (1, ([1],[1])) \\ (1,2,3,4) \to (\psi^{-1}\phi_{(1,3)}\psi, ([1],[1])) \\ (1,4,3,2) \to (\psi^{-1}\phi_{(1,3)}\psi, ([1],[0])).\end{gathered}$$

Infine scegliamo $\{([1],[0]),([0],[1])\}$ come base di $\mathbb{Z}_2 \times \mathbb{Z}_2$ e facciamo agire su di essa l'applicazione lineare $\psi^{-1}\phi_{(1,3)}\psi$. Si ottiene: $([1],[0])\psi^{-1}\phi_{(1,3)}\psi = (1,3)(1,2)(3,4)(1,2)\psi = (1,4)(2,3)\psi = ([1],[1])$ e $([0],[1])\psi^{-1}\phi_{(1,3)}\psi = (1,3)(1,3)(2,4)(1,3)\psi = (1,3)(2,4)\psi = ([0],[1])$. Allora l'applicazione lineare $\psi^{-1}\phi_{(1,3)}\psi$ coincide con la moltiplicazione per la matrice $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

3.4 Gruppi Imprimitivi e Prodotto Intrecciato

Siano H e K due gruppi di permutazioni rispettivamente su X e Y. Costruiremo ora un nuovo gruppo di permutazioni sul prodotto cartesiano $Z = X \times Y$.

Sia $\gamma \in H$ una permutazione e $y \in Y$, definiamo allora la permutazione γ_y di Z che associa $(x\gamma, y)$ alla coppia (x, y), mentre lascia invariate tutte le coppie del tipo (x, y_1), con $y_1 \neq y$. Sia invece $\tau \in K$, definiamo la permutazione τ^* di Z costruita come segue: $\tau^* : (x, y) \to (x, y\tau)$. Si verifica immediatamente che γ_y ha per inverso l'elemento $(\gamma^{-1})_y$ e che τ^* ha per inverso $(\tau^{-1})^*$, allora le applicazioni appena definite sono effettivamente permutazioni. Inoltre la funzione definita da $\gamma \to \gamma_y$, con $y \in Y$ fissato, è un omomorfismo iniettivo da H a $Sym\ Z$ e la funzione definita da $\tau \to \tau^*$ è un omomorfismo inettivo da K in $Sym\ Z$. Chiamiamo H_y e K^* le loro rispettive immagini.

Definizione 3.12. Si dice prodotto intrecciato di H e K il gruppo di permutazioni su Z generato da K^* e da tutti gli H_y al variare di y in Y. In simboli scriviamo:

$$H \wr K = \langle H_y, K^* : y \in Y \rangle.$$

Osserviamo che $(x, y\tau)(\tau^*)^{-1}\gamma_y\tau^* = (x, y)\gamma_y\tau^* = (x\gamma, y\tau)$ e $(x_1, y_1)(\tau^*)^{-1}\gamma_y\tau^* = (x_1, y_1\tau^{-1})\gamma_y\tau^* = (x_1, y_1)$ se $y_1 \neq y\tau$. Segue quindi dalla definizione di γ_y che $(\tau^*)^{-1}\gamma_y\tau^* = \gamma_{y\tau}$ e $(\tau^*)^{-1}H_y\tau^* = H_{y\tau}$. Osserviamo che se $\tilde{\gamma} \in H_y$, allora $\tilde{\gamma}$ fissa tutte le coppie del tipo (x, k), con $k \neq y$. Mostriamo ora che i sottogruppi H_y generano il loro prodotto diretto, al variare di $y \in Y$.

È immediato verificare che H_y e H_w commutano tra loro, se $y \neq w$. Sia ora $\tilde{\gamma} \in H_y \cap \langle H_w : w \neq y \rangle$. Siccome $\tilde{\gamma} \in H_y$ si ha che $\tilde{\gamma}$ fissa tutte le coppie del tipo (x, k), con $k \neq y$, ma siccome $\tilde{\gamma} \in \langle H_w : w \neq y \rangle$ allora $\tilde{\gamma}$ fissa anche tutte le coppie del tipo (x, y). Ne segue che $\tilde{\gamma} = 1$.

La proprietà $(\tau^*)^{-1}H_y\tau^* = H_{y\tau}$ indica che il coniugio tramite elementi di K^* permuta i fattori H_y di B esattamente come τ permuta gli elementi y di Y. In più, siccome B agisce solo sulla componente X di Z e K^* sulla componente Y, è evidente che $K^* \cap B = 1$, inoltre vale che $B \trianglelefteq H \wr K$ e $H \wr K = K^*B$. Concludiamo quindi che $H \wr K$ è prodotto semidiretto di B e K^*, in cui l'automorfismo di B prodotto da un elemento di K^* è dato dalla proprietà $(\tau^*)^{-1}\gamma_y\tau^* = \gamma_{y\tau}$.

Proposizione 3.4.1. *Siano H e K due gruppi di permutazioni transitivi, rispettivamente su X e su Y. Allora $H \wr K$ è transitivo su $X \times Y$. Inoltre $H \wr K$ è imprimitivo su $X \times Y$.*

Dimostrazione. Siano (x, y) e (x', y') due elementi di $X \times Y$. Per transitività esistono $\gamma \in H$ e $\tau \in K$ tali che $x' = x\gamma$ e $y' = y\tau$. Allora la permutazione $\tau^*\gamma_{y'}$ manda (x, y) in $(x, y')\gamma_{y'} = (x', y')$.

Osserviamo che, al variare di y in Y, i sottoinsiemi $I_y = \{(x, y) : n \in X\}$ formano una partizione di $X \times Y$. Inoltre $H \wr K$ è generato da permutazioni della forma $\gamma_y \in H_y$, con $y \in Y$, e $\tau^* \in K^*$. Vale che $(x, y)\gamma_y \in I_y$, per ogni $\gamma \in H$ e per ogni $y \in Y$, e $(x, y)\tau^* \in I_{y\tau}$, per ogni $\tau^* \in K^*$. Pertanto ogni generatore di $H \wr K$ permuta gli insiemi I_y, allora ogni elemento $\sigma \in H \wr K$, essendo prodotto di generatori, permuta gli insiemi I_y. Quindi gli insiemi I_y, al variare di $y \in Y$, sono blocchi di imprimitività. □

Teorema 3.4.2. *Sia G un gruppo di permutazioni transitivo su W. Se G è non primitivo, allora G è simile ad un sottogruppo di un prodotto intrecciato di gruppi di permutazioni.*

Dimostrazione. Siano $I_1, \ldots, I_r$ i blocchi di imprimitività di G, con $I_j = \{a_{j1}, \ldots, a_{jr}\}$. Supponiamo $W = \{a_{11}, \ldots, a_{mr}\}$ e definiamo $Z = \{(u, v) : u = 1, \ldots, m \text{ e } v = 1, \ldots, r\}$. Costruiamo quindi la biezione $\varphi : W \to Z$ definita da $a_{uv}\varphi = (u, v)$. Sia $P = S_m \wr S_r$, allora P è un gruppo di permutazioni su Z e cerchiamo un omomorfismo iniettivo $\Phi : G \to P$ tale che $\sigma\varphi = \varphi\sigma^\Phi$ per ogni $\sigma \in G$. Siccome G è imprimitivo, per ogni $\sigma \in G$ e per ogni $i = 1, \ldots, r$ esiste $k \in \{1, \ldots, r\}$ tale che $I_i\sigma = I_k$. Definiamo allora l'omomorfismo $\psi : G \to S_r$ nel modo seguente: se $\sigma \in G$ e $i \in \{1, \ldots, r\}$, allora $\sigma\psi$ è l'apllicazione che manda i in k e la chiamiamo $\tilde{\sigma}$. Possiamo finalmente definire l'omomorfismo

$$\Phi : G \to P$$

$$\sigma \to \tilde{\sigma}^* \sigma_1 \cdots \sigma_r,$$

ove $(i,k)\tilde{\sigma}^* = (i, k\tilde{\sigma})$ e $(i,k)\sigma_j = (i,k)$ se $j \neq k$ e $(i,k)\sigma_k = (a_{ik\tilde{\sigma}^{-1}})\sigma\varphi$. Affinché Φ sia un'applicazione ben definita, occore verificare che σ_k sia effettivamente una permutazione. Se $j \neq k$ si ha che σ_k è la funzione identica sulle coppie del tipo (i,k); mostriamo allora che σ_k permuta tra loro le coppie dell'insieme $I_k\varphi = \{(i,k) : i = 1, \ldots, m\}$. Si ha che $(i,k)\sigma_k = a_{ik\tilde{\sigma}^{-1}}\sigma\varphi$, ma $a_{ik\tilde{\sigma}^{-1}} \in I_{k\tilde{\sigma}^{-1}}$, quindi $a_{ik\tilde{\sigma}^{-1}}\sigma \in I_k$ e dunque otteniamo che $(i,k)\sigma_k = a_{ik\tilde{\sigma}^{-1}}\sigma\varphi \in I_k\varphi$. Allora σ_k è una funzione da $I_k\varphi$ in se. Inoltre σ_k è iniettiva e suriettiva perché lo è σ ed è suriettiva perché $I_k\varphi$ è un insieme finito.

Mostriamo ora che $\varphi\sigma^\Phi = \sigma\varphi$ per ogni $\sigma \in G$. Sia $a_{ik} \in W$, allora $a_{ik}\varphi\sigma^\Phi = (i,k)(\tilde{\sigma}^*\sigma_1 \cdots \sigma_r) = (i, k\tilde{\sigma})\sigma_1 \cdots \sigma_r = (i, k\tilde{\sigma})\sigma_{k\tilde{\sigma}} = a_{ik\tilde{\sigma}\tilde{\sigma}^{-1}}\sigma\varphi = a_{ik}\sigma\varphi$.

Per concludere la dimostrazione rimane da fare vedere che Φ è un omomorfismo iniettivo: siano $\sigma, \tau \in G$, allora $(i,k)\sigma^\Phi\tau^\Phi = a_{ik}\varphi\sigma^\Phi\tau^\Phi = a_{ik}\sigma\varphi\tau^\Phi = a_{ik}\sigma\tau\varphi = a_{ik}\varphi(\sigma\tau)^\Phi = (i,k)(\sigma\tau)^\Phi$, quindi $\sigma^\Phi\tau^\Phi = (\sigma\tau)^\Phi$. Supponiamo infine che $(i,k)\sigma^\Phi = (i,k)$ per ogni coppia (i,k). Si ha che $(i,k)\sigma^\Phi = (i,k)(\tilde{\sigma}^*\sigma_1 \cdots \sigma_r) = (i,k\tilde{\sigma})\sigma_{k\tilde{\sigma}} = a_{ik\tilde{\sigma}\tilde{\sigma}^{-1}}\sigma\varphi = a_{ik}\sigma\varphi$, per cui $a_{ik}\sigma\varphi = (i,k) = a_{ik}\varphi$, da cui otteniamo che $\sigma = 1$, in quanto φ è iniettiva. □

Esempio 3.9. Sia $G = S_3 \wr S_4$ un gruppo di permutazioni su $Z = \{(i,k) : i = 1, \ldots, 3 \text{ e } k = 1, \ldots, 4\}$. Ricordiamo che ogni permutazione di G si scrive nella forma $\sigma = \tau^*\gamma_1 \cdots \gamma_4$, con τ^* tale che $(i,k)\tau^* = (i, k\tau)$, mentre $(i,k)\gamma_j = (i,k)$ se $j \neq k$ e $(i,k)\gamma_k = (i\gamma, k)$.

Consideriamo ora il sottogruppo di G

$$S = \langle (1,2,3,4)^*, (1,2)(3,4)^*, (1,2)_1(1,2)_2(1,2)_3(1,2)_4, (1,3)_1(1,3)_2(1,3)_3(1,3)_4 \rangle.$$

Allora S è transitivo; prendiamo infatti il sottogruppo di S

$$U = \langle (1,2,3,4)^*, (1,2)(3,4)^* \rangle$$

e $\Phi_1 : U \to D_8$ definito da $(\tau^*)^{\Phi_1} = \tau$. Si ha che Φ_1 è un isomorfismo. Inoltre la funzione $\varphi_1 : \{1,2,3\} \times \{1,2,3,4\} \to \{1,2,3,4\}$ definita da $(i,k)\varphi_1 = k$ è suriettiva. Allora, per ogni $i = 1,2,3$, la coppia $(\Phi_1, \varphi_1|_{\{i\}\times\{1,2,3,4\}})$ è una similarità tra U e D_8 e, siccome D_8 è transitivo, segue che U è transitivo su $\{i\} \times \{1,2,3,4\}$ per ogni $i = 1,2,3$. Prendiamo ora il sottogruppo di S

$$V = \langle (1,2)_1(1,2)_2(1,2)_3(1,2)_4, (1,3)_1(1,3)_2(1,3)_3(1,3)_4 \rangle$$

e osseviamo che $V = \{\gamma_1\gamma_2\gamma_3\gamma_4 : \gamma \in S_3\}$. Sia $\Phi_2 : V \to S_3$ l'isomorfismo definito da $(\gamma_1 \cdots \gamma_4)^{\Phi_2} = \gamma$. Sia inoltre $\varphi_2 : \{1,2,3\} \times \{1,2,3,4\} \to \{1,2,3\}$ definita da $(i,k)\varphi_2 = i$, allora la coppia $(\Phi_2, \varphi_2|_{\{1,2,3\}\times\{k\}})$ è una similarità tra V e S_3 per ogni $k = 1,2,3,4$. Ne

segue che V è transitivo su $\{1,2,3\} \times \{k\}$ per ogni $k = 1,2,3,4$. Dalla transitività di U e V segue facilmente la transitività di S su $\{1,2,3\} \times \{1,2,3,4\}$.

Per 3.4.1 si ha che G è transitivo e imprimitivo su $\{1,2,3\} \times \{1,2,3,4\}$. I suoi blocchi di imprimitività sono gli insiemi della forma $I_k = \{(i,k) : i = 1,2,3\}$, con $k = 1,2,3,4$. Per definizione di blocco di imprimitività, vale che $I_k\sigma = I_k$ oppure $I_k\sigma \cap I_k = \emptyset$ per ogni $\sigma \in G$, ma siccome S è un sottogruppo di G, ogni σ in S appartiene a G. Ne segue che anche S è un gruppo imprimitivo su $\{1,2,3\} \times \{1,2,3,4\}$ e i suoi blocchi di imprimitività sono gli stessi di G.

Bibliografia

[1] M. Artin, *Algebra*, Bollati Boringhieri, (1997).

[2] P.J. Cameron, *Permutation Groups*, Cambridge University Press, (1999).

[3] J.D. Dixon, B. Mortimer, *Permutation Groups*, Springer, (1996).

[4] D.J.S. Robinson, *A Course in the Theory of Groups*, Springer, (1996).

[5] E. Sernesi, *Geometria*, Bollati Boringhieri, (1989).