Azioni permutazionali di gruppi

Appunti per il corso di Algebra Superiore
tenuto da
Giovanni Cutolo

Università degli Studi di Salerno
Anno Accademico 1997/98

1. Rappresentazioni ed azioni permutazionali

Sia G un gruppo. Una *rappresentazione permutazionale* di G su un insieme X è, per definizione, un omomorfismo $G \longrightarrow Sym\, X$, dove $Sym\, X$ indica il gruppo simmetrico su X.

Una nozione equivalente è quella di *azione permutazionale destra*. Un'azione permutazionale destra (o, più brevemente, azione permutazionale) del gruppo G sull'insieme X è un'operazione esterna $* : X \times G \longrightarrow X$ che verifichi le condizioni:

$$x * 1 = x \qquad \text{e} \qquad (x * g) * h = x * (gh)$$

per ogni $x \in X$ e per ogni g, $h \in G$ (come di consueto, trattandosi di operazioni, la scrittura $x * g$ indica $(x, g)*$, l'immagine di (x, g) mediante $*$).

In che senso le due nozioni siano equivalenti, di fatto interscambiabili, è spiegato in [Rob], pp. 33–34: alla rappresentazione permutazionale $\rho : G \to Sym\, X$ si può associare l'azione permutazionale $(x, g) \in X \times G \mapsto xg^\rho \in X$,(†) inversamente, all'azione permutazionale $* : X \times G \longrightarrow X$ si può associare la rappresentazione permutazionale $g \in G \mapsto \binom{x}{x*g} \in Sym\, X$;(‡) le applicazioni così definite, dall'insieme delle rappresentazioni permutazionali a quello delle azioni permutazionali di G su X e viceversa, sono l'una inversa dell'altra, in particolare sono biettive.

Per questo motivo si usa spesso la dizione "azione di G su X" in luogo di "rappresentazione permutazionale di G su X". Con le notazioni usate sopra, se $x \in X$ e $g \in G$, scriveremo xg per xg^ρ, ovvero per $x * g$ se $*$ è l'azione determinata dalla rappresentazione permutazionale ρ. Va notato che la seconda delle proprietà che definiscono le azioni permutazionali rende non necessario l'uso di parentesi in espressioni come xgh (dove anche h è un elemento di G), che può essere indifferentemente letta come $(x*g)*h$ o come $x*(gh)$. È chiaro che utilizziamo queste espressioni solo quando è possibile sottintendere un esplicito riferimento a ρ o a $*$ senza incorrere in ambiguità.

Per dire che è definita un'azione permutazionale di G su X si usano anche le locuzioni 'G agisce su X', 'G opera su X', 'X è un G-insieme', 'X è un G-spazio'.

Terminologia e notazioni

Sia fissata una rappresentazione permutazionale $\rho : G \longrightarrow Sym\, X$. Definiamo:

- $\deg \rho = |X|$, il *grado* di ρ.
- Per ogni $x \in X$, lo *stabilizzante* (o stabilizzatore) di x (rispetto a ρ) è $\mathrm{St}_\rho(x) = \{g \in G \mid xg = x\}$. Questo è un sottogruppo di G. Se $Y \subseteq X$, poniamo $\mathrm{St}_\rho(Y) = \bigcap_{x \in Y} \mathrm{St}_\rho(x) = \{g \in G \mid (\forall x \in Y)(xg = x)\}$.
- Per ogni $x \in X$, la *ρ-orbita* di x è l'insieme $\mathrm{Orb}_\rho(x) = \{xg \mid g \in G\}$. La relazione binaria $\sim_\rho$ in X, definita ponendo, per ogni x, $y \in X$,
$$x \sim_\rho y \iff (\exists g \in G)(y = xg)$$
è una relazione di equivalenza, che prende il nome di *ρ-equivalenza*. È ovvio che, per ogni $x \in X$, $\mathrm{Orb}_\rho(x)$ è precisamente la $\sim_\rho$-classe di equivalenza a cui appartiene x. Pertanto le ρ-orbite costituiscono una partizione di X.
- ρ è *transitiva* se e solo se la relazione di equivalenza definita al punto precedente è quella totale, cioè se e solo se X ha una sola orbita oppure $X = \varnothing$, ovvero se e solo se, scelti comunque x, $y \in X$, esiste $g \in G$ tale che $xg = y$.
- ρ è *fedele* se e solo se è un monomorfismo. In generale, il nucleo di ρ coincide con $\mathrm{St}_\rho(X) = \bigcap_{x \in X} \mathrm{St}_\rho(x)$, quindi ρ è fedele precisamente quando questa intersezione è il sottogruppo identico.
- ρ è *semiregolare* se e solo se $X \neq \varnothing$ e $\mathrm{St}_\rho(x) = 1$ per ogni $x \in X$; ρ è *regolare* se e solo se è semiregolare e transitiva. Da quanto osservato sopra segue che una rappresentazione semiregolare è necessariamente fedele.
- Per ogni $g \in G$, poniamo $\mathrm{Fix}_\rho(g) = \{x \in X \mid xg = x\}$, l'insieme dei *punti fissati* da ρ (in contesto di rappresentazioni permutazionali ci si riferisce spesso agli elementi dell'insieme su cui si opera come a 'punti'). Il *supporto* di g è $\mathrm{supp}_\rho(g) = X \setminus \mathrm{Fix}_\rho(g) = \{x \in X \mid xg \neq x\}$. Se $K \subseteq G$, si pone anche $\mathrm{Fix}_\rho(K) = \bigcap_{g \in K} \mathrm{Fix}_\rho(g)$ e $\mathrm{supp}_\rho(K) = X \setminus \mathrm{Fix}_\rho(K) = \bigcup_{g \in K} \mathrm{supp}_\rho(g)$.

Altre definizioni importanti sono contenute tra gli esercizi (ad esempio, p. 3, nr. 14 e nota precedente il nr. 17). Verifichiamo in dettaglio alcune delle affermazioni inserite tra le definizioni appena date:

(†) Per indicare l'immagine b di un elemento a mediante un'applicazione α si userà la notazione destra: $b = a\alpha$ o la notazione esponenziale: $b = a^\alpha$. Pur essendo queste due notazioni interscambiabili, useremo di preferenza la notazione esponenziale quando l'applicazione è un omomorfismo di gruppi, e quindi, in particolare, per rappresentazioni permutazionali, e la notazione destra altrimenti. Quindi xg^ρ è l'immagine di x mediante la permutazione g^ρ, che a sua volta è l'immagine di g mediante ρ. L'uso di queste notazioni è conforme alla notazione usata per la composizione di applicazioni: se $\alpha : A \to B$ e $\beta : B \to C$ sono applicazioni, $\alpha\beta$ è l'applicazione $a \in A \mapsto (a\alpha)\beta \in C$.

(‡) dove il contesto renda inutile specificare dominio e codominio, un simbolo come $\binom{x}{x'}$, se riferito ad applicazioni, indica l'applicazione che manda un generico elemento x in x'.

⋆ $\mathrm{St}_\rho(x)$ *e* $\mathrm{St}_\rho(Y)$ *sono sottogruppi di* G*, per ogni* $x \in X$ *e* $Y \subseteq X$*.*
Infatti $1 \in \mathrm{St}_\rho(x)$, che è così non vuoto. Se g, $h \in \mathrm{St}_\rho(x)$, allora $xg = x = xh$ e quindi $x(gh^{-1}) = (xg)h^{-1} = (xh)h^{-1} = x(hh^{-1}) = x1 = x$. Dunque $gh^{-1} \in \mathrm{St}_\rho(x)$, e $\mathrm{St}_\rho(x)$ è un sottogruppo. Se $\varnothing \neq Y \subseteq X$, allora, per definizione, $\mathrm{St}_\rho(Y)$ è una intersezione di sottogruppi di G, quindi un sottogruppo; infine $\mathrm{St}_\rho(\varnothing) = G \leq G$. L'asserzione è così dimostrata.

⋆ *La relazione* $\sim_\rho$ *di* ρ*-equivalenza è effettivamente una relazione di equivalenza.*
Infatti $\sim_\rho$ è *riflessiva:* per ogni $x \in X$ si ha $x1 = x$, quindi $x \sim_\rho x$; *simmetrica:* se $x \sim_\rho y$ esiste $g \in G$ tale che $y = xg$, ma allora $x = yg^{-1}$ e $y \sim_\rho x$; *transitiva:* se $x \sim_\rho y$ e $y \sim_\rho z$, allora $y = xg$ e $z = yh$ per opportuni g, $h \in G$, dunque $z = (xg)h = x(gh)$ e $x \sim_\rho z$. Pertanto $\sim_\rho$ è una relazione di equivalenza.

Un comune abuso di notazione e di linguaggio consiste nell'omettere il riferimento a ρ nelle espressioni definite sopra, o di sostituirlo con un riferimento a G. Ad esempio, può capitare di leggere $\mathrm{St}_G(x)$ per $\mathrm{St}_\rho(x)$, o l'espressione 'G-orbita' per 'ρ-orbita', o $\mathrm{supp}(g)$ e $\mathrm{Fix}(g)$ per $\mathrm{supp}_\rho(g)$ e $\mathrm{Fix}_\rho(g)$. Ovviamente è lecito praticare questo abuso solo quando il contesto chiarisca quale sia la rappresentazione permutazionale ρ (di dominio G) considerata.

Un caso particolarmente importante è quello dei *gruppi di permutazioni*, cioè dei sottogruppi dei gruppi simmetrici su un insieme. Se $\Gamma \leq Sym\, X$ allora, a meno di esplicita indicazione in senso contrario, si useranno per Γ ed i suoi elementi le espressioni 'stabilizzante', 'orbita', 'supporto' etc. in riferimento all'ovvia rappresentazione permutazionale di Γ: l'immersione $\iota_\Gamma : \Gamma \hookrightarrow Sym\, X$. Diremo, ad esempio, che Γ è transitivo se e solo se lo è ι_Γ. In generale, se $\mathcal{P}$ è una proprietà che pertiene a rappresentazioni permutazionali, diremo che Γ verifica $\mathcal{P}$ se e solo se ι_Γ verifica $\mathcal{P}$. (Va notato che X è il dominio degli elementi di Γ, pertanto X, e quindi ι_Γ, è determinato da Γ. Già che ci siamo, notiamo anche che, se $x \in X$ e $g \in \Gamma$, allora $x * g = xg^{\iota_\Gamma}$ è proprio l'immagine di x mediante g, il che ci permette di usare l'espressione xg in modo non ambiguo.)

In effetti molte proprietà relative a rappresentazioni permutazionali possono essere equivalentemente espresse in termini di gruppi di permutazioni, nel senso che sono verificate da una rappresentazione permutazionale $\rho : G \longrightarrow X$ se e solo se sono verificate dal gruppo di permutazioni $\mathrm{im}\,\rho \leq Sym\, X$. Ad esempio, le ρ-orbite coincidono con le $(\mathrm{im}\,\rho)$-orbite, e, in particolare, ρ è transitiva se e solo se lo è $\mathrm{im}\,\rho$. Inoltre, per ogni $g \in G$, si ha $\mathrm{supp}_\rho(g) = \mathrm{supp}(g^\rho)$ e $\mathrm{Fix}_\rho(g) = \mathrm{Fix}(g^\rho)$.

Se $\rho : G \longrightarrow Sym\, X$ è una rappresentazione permutazionale e H è un sottogruppo di G, si usano espressioni come $\mathrm{St}_H(x)$ o 'H-orbita' per indicare stabilizzanti ed orbite rispetto alla restrizione di ρ ad H, cioè alla rappresentazione permutazionale $\rho_{|H} : h \in H \mapsto h^\rho \in Sym\, X$ (che si dice indotta per restrizione da ρ su H). Quindi, ad esempio, due elementi x e y di X sono H-equivalenti se e solo se $y = xh$ $(= xh^\rho)$ per un opportuno $h \in H$, e per esprimere questo fatto useremo la notazione $x \sim_H y$. Sono molto frequenti espressioni come 'H è transitivo' oppure 'H è transitivo su Y' per indicare rispettivamente che la restrizione di ρ ad H è transitiva oppure che Y è una H-orbita o $Y = \varnothing$. Anche in questo caso l'uso di questa terminologia presuppone che sia individuata dal contesto la rappresentazione ρ. Infine, se $g \in G$, si usa anche la locuzione 'g-orbita' intendendo $\langle g \rangle$-orbita.

Notazioni alternative (frequentemente usate, ad esempio in [DM], in [W] e in [P]) per orbite e stabilizzanti sono: G_x per $\mathrm{St}_G(x)$ e x^G per $\mathrm{Orb}_G(x)$.

La terminologia sin qui introdotta è in accordo con quella abitualmente usata in letteratura, ad esempio in [DM], con l'eccezione del fatto che la maggior parte degli autori non considera rappresentazioni permutazionali sull'insieme vuoto. Rispetto alla terminologia di [Rob], sezione 1.6, va segnalato che lì alcune nozioni sono definite per gruppi di permutazioni e solo dopo estese (cfr. pag. 34) a rappresentazioni permutazionali arbitrarie, e che la nozione di regolarità come qui definita coincide con quella data in [Rob] solo nel caso delle rappresentazioni fedeli.

Esercizi.

1. Dimostrare la correttezza di tutte le osservazioni non giustificate che accompagnano le definizioni date sopra.
2. Sia X il piano euclideo, sia $O \in X$ e sia Γ il gruppo delle rotazioni di X con centro O. Se $P \in X$, qual è la Γ-orbita di P? (Questo esempio dovrebbe suggerire il motivo per il quale si usa, in questo contesto, il termine 'orbita'.)
3. Per ogni insieme X, il gruppo $Sym\, X$ è transitivo.
4. Per ogni intero $n > 2$, il gruppo $\mathbb{A}_n$ è transitivo.
5. Determinare supporto ed orbita dell'elemento $(123)(84)$ di $\mathbb{S}_8$.

Sia data una rappresentazione permutazionale $\rho : G \longrightarrow Sym\, X$.

6. Se ρ è regolare, per ogni $x \in X$ l'applicazione $g \in G \mapsto xg \in X$ è biettiva.
7. Per ogni $x \in X$, il nucleo di ρ è $\mathrm{St}_\rho(X \smallsetminus \{x\})$.
8. In nessun caso il supporto di una permutazione è un singleton.
9. Per ogni $x \in X$ la G-orbita di x è l'intersezione (ovvero il minimo) tra le parti Y di X tali che $x \in Y = Yg$ per ogni $g \in G$. (Yg denota $\{yg \mid y \in Y\}$, l'immagine di Y mediante g^ρ.)
10. Se $g \in G$ e $x \in X$ la g-orbita di x è $\{xg^n \mid n \in \mathbb{Z}\}$.
11. Se $(Y_i)_{i \in I}$ è una famiglia di parti di X si ha

$$\mathrm{St}_\rho\Big(\bigcup_{i \in I} Y_i\Big) = \bigcap_{i \in I} \mathrm{St}_\rho(Y_i) \qquad \text{e} \qquad \mathrm{St}_\rho\Big(\bigcap_{i \in I} Y_i\Big) \geq \big\langle\, \mathrm{St}_\rho(Y_i) \mid i \in I \,\big\rangle.$$

Nella seconda formula l'inclusione può essere propria.

12. L'azione $(Y,g)\mapsto Yg$ (cfr. esercizio 9) determina una rappresentazione permutazionale $G\to Sym\big(\mathcal{P}(X)\big)$, dove $\mathcal{P}(X)$ è l'insieme delle parti di X.

13. Date due rappresentazioni permutazionali $\rho: G\to Sym\,X$ e $\varphi: G\to Sym\,Y$ dello stesso gruppo G, verificare che le posizioni $f*g=\big(g^\rho\big)^{-1}f$ e $f\star g=fg^\varphi$ per ogni $g\in G$ e $f\in Y^X$ definiscono due azioni permutazionali $*$ e $\star$ di G su Y^X.

14. Se $Y\subseteq X$, l'insieme $\mathrm{St}^*_\rho(Y)=\{g\in G\mid Yg=Y\}$ è un sottogruppo di G (è lo stabilizzante di Y rispetto all'azione definita nell'esercizio precedente). Per ogni $g\in G$ si ha $\mathrm{St}^*_\rho(Yg)=\big(\mathrm{St}^*_\rho(Y)\big)^g$. Nella letteratura in lingua inglese (ad esempio, in [DM]), $\mathrm{St}^*_\rho(Y)$ prende il nome di *setwise stabilizer* di Y, in italiano, talvolta, si chiama *stabilizzante globale* di Y (rispetto a ρ).

15. Per ogni $g,h\in G$ si ha $\mathrm{supp}(g^h)=\big(\mathrm{supp}(g)\big)h$. Inoltre $\mathrm{supp}(g^{-1})=\mathrm{supp}(g)$ e $\mathrm{supp}(gh)\subseteq\mathrm{supp}(g)\cup\mathrm{supp}(h)$.

16. Due permutazioni σ e τ si dicono *disgiunte* se e solo se $\mathrm{supp}(\sigma)$ e $\mathrm{supp}(\tau)$ sono disgiunti. Verificare che in questo caso $\sigma\tau=\tau\sigma$.

Una permutazione σ su un insieme X si dice *finitaria* se e solo se $\mathrm{supp}(\sigma)$ è finito. Sia $FSymX$ l'insieme delle permutazioni finitarie di X.

17. $FSymX$ è un sottogruppo normale di $Sym\,X$.

18. $FSymX$ è transitivo.

19. $FSymX=Sym\,X$ se e solo se X è finito.

Risultati elementari

Consideriamo fissata una rappresentazione permutazionale $\rho: G\longrightarrow Sym\,X$. Alcuni importanti legami tra orbite e stabilizzanti rispetto a questa azione sono espressi dall'enunciato che segue.

1.1. *Sia $x\in X$. Detto $\mathcal{L}$ l'insieme dei laterali destri di $\mathrm{St}_\rho(x)$ in G, l'applicazione:*

$$\mathrm{St}_\rho(x)g\in\mathcal{L}\longmapsto xg\in\mathrm{Orb}_\rho(x)$$

è ben posta e biettiva. In particolare,

(i) per ogni $g,h\in G$ si ha: $xg=xh\iff\mathrm{St}_\rho(x)g=\mathrm{St}_\rho(x)h$;
(ii) $|\,\mathrm{Orb}_\rho(x)|=|G:\mathrm{St}_\rho(x)|$;
(iii) $|G|=|\,\mathrm{Orb}_\rho(x)|\cdot|\,\mathrm{St}_\rho(x)|$;
(iv) se ρ è transitiva $\deg\rho=|X|=|G:\mathrm{St}_\rho(x)|$; se ρ è regolare $\deg\rho=|X|=|G|$;
(v) se G è finito le ρ-orbite hanno ordine finito divisore di $|G|$;
(vi) se G è finito e ρ è transitiva, il grado $|X|$ di ρ è finito e divide $|G|$ se $X\neq\varnothing$, e ρ è regolare se e solo se $|X|=|G|$.

Dimostrazione — Se $g,h\in G$, allora $xg=xh\iff xgh^{-1}=x\iff gh^{-1}\in\mathrm{St}_\rho(x)\iff\mathrm{St}_\rho(x)g=\mathrm{St}_\rho(x)h$, e con questo è provata la (i). Ne è ovvia conseguenza che l'applicazione definita nell'enunciato è ben posta e iniettiva; essendo ovviamente anche suriettiva essa è biettiva. Il resto dell'enunciato consiste di conseguenze banali di questo fatto. ❑

Le dimostrazioni dei prossimi due enunciati sono strettamente analoghe a quelle svolte in [Rob], p. 31 per gruppi di permutazioni. Si noti che in 1.3 è necessaria l'ipotesi che la rappresentazione sia fedele.

Stabilizzanti di punti appartenenti alla stessa orbita sono tra loro coniugati in G. Infatti:

1.2. *Per ogni $x\in X$ si ha $\mathrm{St}_\rho(xg)=\big(\mathrm{St}_\rho(x)\big)^g$.*

Quindi, se ρ è transitiva, gli stabilizzanti degli elementi di X costituiscono una classe di coniugio di sottogruppi di G.

1.3. *Ogni rappresentazione permutazionale fedele e transitiva di un gruppo abeliano su un insieme non vuoto è regolare.*

Chiamiamo *classe completa di rappresentanti* delle orbite di ρ una parte di X a cui appartenga esattamente un elemento di ciascuna ρ-orbita. Di frequentissimo uso è la seguente:

1.4. (Equazione delle classi generalizzata). *Se X e G sono finiti e T è una classe completa di rappresentanti delle orbite di ρ si ha:*

$$|X|=\sum_{x\in T}\frac{|G|}{|\,\mathrm{St}_\rho(x)|}.$$

Dimostrazione — La partizione di X costituita dalle ρ-orbite è $X/{\sim_\rho}=\{\mathrm{Orb}_\rho(x)\mid x\in T\}$. Inoltre, se x ed y sono elementi distinti di T si ha $\mathrm{Orb}_\rho(x)\neq\mathrm{Orb}_\rho(y)$. Allora dalla parte (ii) di 1.1 segue $|X|=\sum_{x\in T}|\,\mathrm{Orb}_\rho(x)|=\sum_{x\in T}\frac{|G|}{|\,\mathrm{St}_\rho(x)|}$. ❑

Un'altra formula utile in questioni di tipo combinatorio è:

1.5. *Se X e G sono finiti, il numero delle ρ-orbite è* $\dfrac{1}{|G|}\sum_{g\in G}\big|\operatorname{Fix}_\rho(g)\big|$.

Dimostrazione — La dimostrazione consiste essenzialmente nel contare in due modi diversi l'ordine dell'insieme (finito) $S=\{(x,g)\in X\times G \mid xg=x\}$. Per ogni $g\in G$ sia S_g l'insieme degli elementi di S di seconda coordinata g. Chiaramente $S_g=\operatorname{Fix}_\rho(g)\times\{g\}$, quindi $|S_g|=|\operatorname{Fix}_\rho(g)|$. Poiché poi $\{S_g \mid g\in G\}$ è una partizione di S e $S_g\neq S_h$ se $g\neq h$, abbiamo

$$|S|=\sum_{g\in G}|S_g|=\sum_{g\in G}\big|\operatorname{Fix}_\rho(g)\big|. \tag{♮}$$

D'altra parte, per ogni $x\in X$ l'insieme ${}_xS$ degli elementi di S di prima coordinata x coincide con $\{x\}\times\operatorname{St}_\rho(x)$, quindi $|{}_xS|=|\operatorname{St}_\rho(x)|$. Essendo anche gli ${}_xS$ a due a due distinti, e formando essi una partizione di S, si ha $|S|=\sum_{x\in X}|{}_xS|=\sum_{x\in X}|\operatorname{St}_\rho(x)|$. Posto $\mathcal{Q}=X/{\sim_\rho}$, l'insieme delle ρ-orbite, possiamo allora scrivere $|S|=\sum_{Y\in\mathcal{Q}}\sum_{x\in Y}|\operatorname{St}_\rho(x)|$. Fissata un'orbita Y, per ogni elemento $x\in Y$ si ha $|\operatorname{St}_\rho(x)|=|G|/|Y|$ per 1.1 (*iii*). Allora $\sum_{x\in Y}|\operatorname{St}_\rho(x)|=\sum_{x\in Y}|G|/|Y|=|Y|\big(|G|/|Y|\big)=|G|$ e quindi $|S|=\sum_{Y\in\mathcal{Q}}\sum_{x\in Y}|\operatorname{St}_\rho(x)|=\sum_{Y\in\mathcal{Q}}|G|=|\mathcal{Q}|\cdot|G|$. Confrontando con la (♮) otteniamo in questo modo $|\mathcal{Q}|\cdot|G|=\sum_{g\in G}|\operatorname{Fix}_\rho(g)|$, da cui segue l'asserto. ❑

È bene soffermarsi su un caso particolare della formula appena provata: se, in aggiunta alle altre ipotesi, ρ è transitiva e $X\neq\varnothing$, allora esiste esattamente una ρ-orbita e quindi $|G|=\sum_{g\in G}|\operatorname{Fix}_\rho(g)|$.

Esercizio. Se il gruppo finito G agisce in modo transitivo su un insieme non vuoto X di n elementi, esistono almeno $n-1$ elementi di G *senza punti fissi* (cioè elementi g tali che $\operatorname{Fix}(g)=\varnothing$).

Se Y è una parte di X fissata da ρ, cioè tale che $Yg=Y$ per ogni $g\in G$, si definisce l'azione di G indotta da ρ su Y come la rappresentazione di G su $SymY$ definita da $g\mapsto\binom{y}{yg^\rho}$. È di facile verifica che la definizione è ben posta. Chiaramente ogni ρ-orbita è fissata, quindi ρ induce una rappresentazione permutazionale di G su ogni ρ-orbita; ciascuna di queste rappresentazioni è, ovviamente, transitiva.

Esercizi. Come al solito, fissiamo una rappresentazione permutazionale $\rho: G\longrightarrow Sym\,X$.

1. Sia $Y\subseteq X$. Allora Y è fissato da G se e solo se Y è unione di ρ-orbite.
2. $\operatorname{supp}(G)$ è fissato da G e coincide con l'unione delle ρ-orbite di cardinalità maggiore di 1.
3. Per ogni $Y\subseteq X$, l'azione indotta da ρ per restrizione su $\operatorname{St}^*_\rho(Y)$ (si veda l'esercizio 14 di p. 3) fissa Y, ed induce quindi, a sua volta, una rappresentazione $\operatorname{St}^*_\rho(Y)\longrightarrow SymY$ di nucleo $\operatorname{St}_\rho(Y)$. Pertanto $\operatorname{St}_\rho(Y)\lhd\operatorname{St}^*_\rho(Y)$ e il quoziente $\operatorname{St}^*_\rho(Y)/\operatorname{St}_\rho(Y)$ è isomorfo ad un sottogruppo di $Sym(Y)$.

Lo stabilizzante di una parte Y di X ha (oltre a quella indotta per restrizione da ρ, a valori in $Sym\,X$) un'ovvia rappresentazione a valori in $Sym(X\smallsetminus Y)$:

1.6. *Sia Y una parte di X e sia $Y'=X\smallsetminus Y$. Allora, per ogni $g\in\operatorname{St}_\rho(Y')$, è ben definita la permutazione $g^{\bar\rho}: x\mapsto xg$ di Y e l'applicazione $g\in\operatorname{St}_\rho(Y')\mapsto g^{\bar\rho}\in SymY$ è una rappresentazione permutazionale di nucleo* $\ker\rho$.

Dimostrazione — Per ogni $g\in\operatorname{St}_\rho(Y')$, si ha $Yg^\rho=(X\smallsetminus Y')g^\rho=Xg^\rho\smallsetminus Y'g^\rho=X\smallsetminus Y'=Y$, perché g^ρ è una permutazione, quindi Y è fissato da $\operatorname{St}_\rho(Y')$. La rappresentazione indicata all'enunciato non è altro che quella indotta su Y dalla restrizione di ρ a $\operatorname{St}_\rho(Y')$. Il suo nucleo è $\operatorname{St}_{\operatorname{St}_\rho(Y')}\big(\operatorname{St}_\rho(Y)\big)=\operatorname{St}_\rho(Y)\cap\operatorname{St}_\rho(Y')=\operatorname{St}_\rho(Y\cup Y')=\operatorname{St}_\rho(X)=\ker\rho$. ❑

1.7. *Se Y è una parte dell'insieme X, allora $SymY$ è isomorfo a* $\operatorname{St}_{Sym\,X}(X\smallsetminus Y)$.

Dimostrazione — Sia $H=\operatorname{St}_{Sym\,X}(Y')$ dove $Y'=X\smallsetminus Y$. Applichiamo 1.6 al gruppo di permutazioni $Sym\,X$, scegliendo cioè per ρ l'identità in $Sym\,X$. Allora la rappresentazione $\varphi: H\longrightarrow SymY$, che ad ogni $h\in H$ associa $h^\varphi: x\in Y\mapsto xh\in Y$, è ben definita ed è un monomorfismo. Essa è anche suriettiva: per ogni $\alpha\in SymY$ l'applicazione $\bar\alpha$ di X in sé definita da $x^{\bar\alpha}=x$ se $x\in Y'$ e $x^{\bar\alpha}=x^\alpha$ se $x\in Y$ è una permutazione appartenente ad H e $\alpha=\bar\alpha^\varphi$. Dunque φ è un isomorfismo. ❑

In altri termini, se Y è una parte di X allora $SymY$ si immerge in $Sym\,X$; nelle notazioni della dimostrazione di 1.7 un monomorfismo è $\alpha\mapsto\bar\alpha$. Questo viene detto *monomorfismo canonico* di $SymY$ in $Sym\,X$.

1.8. Esempi. Alcune importanti azioni di un gruppo su se stesso o sull'insieme delle sue parti sono descritte ad esempio in [Rob], pp. 34–37 e [DM], p. 6: la rappresentazione regolare destra, l'azione per coniugio su elementi ed altre azioni da queste dedotte.

La *rappresentazione regolare destra* (o *rappresentazione di Cayley*) di un gruppo G è la rappresentazione permutazionale corrispondente alla più ovvia delle azioni permutazionali di G sul suo supporto: l'operazione interna del gruppo: $(x,g)\in G\times G\mapsto xg\in G$; è immediato verificare che questa è effettivamente un'azione permutazionale. La rappresentazione regolare destra è dunque l'applicazione $\delta_{_G}: g\in G\mapsto\binom{x}{xg}\in SymG$. In particolare $\delta_{_G}$ è un

omomorfismo. Come il nome suggerisce, questa è effettivamente una rappresentazione regolare, quindi fedele, cioè un monomorfismo. Si ritrova così il teorema di Cayley, che nella sua formulazione completa garantisce che:

ogni gruppo è isomorfo ad un gruppo regolare di permutazioni sul suo supporto.

Il gruppo regolare in questione è naturalmente $\operatorname{im}\delta_G$ (l'insieme delle traslazioni destre in G), che si chiama *cayleyano destro* di G.

La rappresentazione regolare destra determina, nel senso dell'esercizio 12 di p. 3, un'azione di G su $\mathcal{P}(G)$ per moltiplicazione destra, che a $g \in G$ associa la permutazione $X \in \mathcal{P}(G) \mapsto Xg \in \mathcal{P}(G)$. Se H è un sottogruppo di G, l'orbita di H rispetto a questa azione è l'insieme dei laterali destri di H. Come ogni orbita, questo insieme è fissato da G, che agisce così su di esso, in modo transitivo. Otteniamo in questo modo l'*azione di G su laterali destri di H*, cioè la rappresentazione $\rho_H : g \mapsto \binom{Hx}{Hxg}$, che ha grande importanza nella teoria generale delle rappresentazioni permutazionali. È facile calcolare gli stabilizzanti dei punti (cioè dei laterali di H) rispetto a questa azione. Lo stabilizzante del laterale banale H è $\{g \in G \mid Hg = H\} = H$, quindi per ogni $g \in G$ si ha $\operatorname{St}_{\rho_H}(Hg) = \big(\operatorname{St}_{\rho_H}(H)\big)^g = H^g$, per 1.2. Pertanto il nucleo di ρ_H è $\operatorname{St}_{\rho_H}\big(\{Hg \mid g \in G\}\big) = \bigcap_{g\in G} H^g = H_G$, il core (o nocciolo) di H in G. Osserviamo anche che l'esistenza dell'azione sui laterali destri di un sottogruppo, unitamente a 1.1 (iv), prova che *se κ è un numero cardinale diverso da 0, un gruppo G ha una rappresentazione permutazionale transitiva di grado κ se e solo se G ha un sottogruppo di indice κ.*

Per ogni cardinale κ, l'azione di G per moltiplicazione destra su $\mathcal{P}(G)$ fissa anche l'insieme delle parti di G di cardinalità κ, determinando così un'azione di G su questo insieme. Un esempio di applicazione di questa azione permutazionale è la dimostrazione di 1.9.

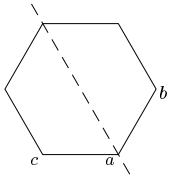
Anche l'azione di coniugio $g \mapsto \binom{x}{x^g}$ di G su se stesso induce un'azione (ancora detta di coniugio) sulle parti di G. Quest'azione fissa l'insieme dei sottogruppi di G, dando così luogo all'azione di coniugio di G sui suoi sottogruppi. Più in generale, se G ed H sono sottogruppi di un gruppo K e $G \leq N_K(H)$, allora l'azione di coniugio di K su se stesso induce per restrizione un'azione su G che fissa H, e quindi un'azione (ancora detta di coniugio) di G su H ([DM], Example 1.3.5).

L'applicazione dei risultati sin qui ottenuti (in particolare 1.1 e 1.4) a queste azioni porta a numerose conseguenze, di frequente uso in teoria dei gruppi. Oltre al teorema di Cayley, si vedano in [Rob], sezione 1.6, gli enunciati 9 e 10, e quanto concerne classi di coniugio, centralizzanti e normalizzanti (pp. 37 e 38). Si confronti 1.6.13 con l'esercizio 3 a p. 4 di questi appunti. Applicando 1.2 (e l'esercizio 14 di p. 3) alle azioni di coniugio in un gruppo si ricavano le seguenti identità: se x e g sono elementi di un gruppo G, allora $C_G(x^g) = \big(C_G(x)\big)^g$, se $H \leq G$ poi $C_G(H^g) = \big(C_G(H)\big)^g$ e $N_G(H^g) = \big(N_G(H)\big)^g$.

Altri Esempi. Sia V uno spazio vettoriale non nullo sul corpo K. Allora il gruppo Γ degli automorfismi di V agisce in modo ovvio su V (è un sottogruppo di $Sym\, V$). Le orbite sono esattamente due: il sottospazio nullo $\{0\}$ e $V^\# := V \smallsetminus \{0\}$. Quindi Γ agisce transitivamente su $V^\#$. Quest'azione induce (in modo simile a quanto fatto sopra) azioni di Γ sull'insieme dei sottospazi di V e sull'insieme dei sottospazi di V di dimensione fissata. È particolarmente importante l'azione di Γ sull'insieme dei sottospazi di dimensione 1, cioè sullo spazio proiettivo associato a V.

Si possono interpretare con il linguaggio delle azioni permutazionali molte nozioni fondamentali della teoria di Galois. Se F/K è un'estensione di Galois (tra campi), il gruppo di Galois G di F/K è lo stabilizzante di K rispetto all'ovvia azione di $\operatorname{Aut} F$ su F. Se $H \leq G$ e L è un sottocampo di F contenente K, hanno molta importanza $H^* = \operatorname{Fix}_G(H)$ e $L^* = \operatorname{St}_G(L)$, che è il gruppo di Galois di F/L. Ad esempio, i sottocampi coniugati a L (cioè quelli della forma L^g per qualche $g \in G$) sono tanti quanto è $|G : L^*|$, per 1.1. Se inoltre assumiamo che F sia il campo di spezzamento di un polinomio irriducibile f a coefficienti in K, allora G opera in modo transitivo e fedele sull'insieme delle radici di f in F.

Sia G il gruppo delle isometrie del piano (euclideo, analogo discorso vale per parti dello spazio tridimensionale euclideo). Se F è una parte del piano, per l'esercizio 3 di p. 4 il quoziente $\operatorname{St}^*_G(F)/\operatorname{St}_G(F)$ agisce in modo fedele su F. Vediamo quali informazioni possiamo ottenere a proposito di questo gruppo da semplici applicazioni dei risultati finora ottenuti. Innanzitutto, sappiamo dalla geometria elementare che l'unica isometria del piano che fissi tre punti non allineati è l'identità, quindi, se F contiene almeno tre punti non allineati, $\operatorname{St}_G(F) = 1$ e $\Gamma := \operatorname{St}^*_G(F)$ agisce in modo fedele su F. Questo gruppo (o anche la sua immagine in $Sym\, F$) si chiama *gruppo delle isometrie di F*. Se ci limitiamo al caso in cui F sia un poligono (non degenere), possiamo descrivere l'azione di Γ su F come azione sui vertici di F. Più precisamente, l'insieme V dei vertici di F è fissato da Γ, quindi l'azione di Γ su F induce una rappresentazione permutazionale $\Gamma \longrightarrow Sym\, V$ che risulta ancora fedele (sempre per lo stesso motivo: tra i vertici di F ci sono almeno tre punti non allineati). Per fissare un esempio concreto, supponiamo che F sia un esagono regolare, come quello disegnato a fianco. È chiaro che Γ agisce transitivamente su V (basta considerare le rotazioni intorno al centro dell'esagono). Quindi $\Gamma_a := \operatorname{St}_\Gamma(a)$ ha indice $|V| = 6$ in Γ, per 1.1. Calcoliamo l'orbita di b rispetto all'azione di Γ_a. Se $\gamma \in \Gamma_a$, certamente $b\gamma$ è un vertice adiacente a $a\gamma = a$, quindi $b\gamma \in \{b, c\}$. Dunque $\operatorname{Orb}_{\Gamma_a}(b) \subseteq \{b, c\}$. D'altra parte, ovviamente $b \in \operatorname{Orb}_{\Gamma_a}(b)$ e anche $c \in \operatorname{Orb}_{\Gamma_a}(b)$, dal momento che c è l'immagine di b mediante la simmetria assiale di asse la retta per a ed il centro di F (tratteggiata nella figura accanto), e questa simmetria appartiene a Γ_a. Pertanto $\operatorname{Orb}_{\Gamma_a}(b) = \{b, c\}$ ha ordine 2, quindi, posto $\Gamma_{ab} = \operatorname{St}_{\Gamma_a}(b)$, si ha $|\Gamma_a : \Gamma_{ab}| = 2$ e dunque $|\Gamma : \Gamma_{ab}| = 12$. Ora, ogni elemento di Γ_{ab} fissa c, perché fissando a deve fissare l'insieme $\{b, c\}$ dei vertici adiacenti ad a e fissa anche b. Questo significa che Γ_{ab} stabilizza tre punti non allineati del piano, dunque $\Gamma_{ab} = 1$. È così provato che Γ ha ordine 12 (come



ben noto, Γ è il gruppo diedrale di ordine 12). In modo strettamente analogo si può ragionare per provare, più in generale che il gruppo delle isometrie di un poligono regolare di n lati (dove n è un intero maggiore di 2) ha ordine $2n$ (anche in questo caso si ottiene, come noto, un gruppo diedrale). Può anche essere interessante considerare il caso di altre figure piane: se R è un rettangolo non quadrato si riconosce facilmente che il gruppo Δ delle isometrie di R opera in modo regolare sui vertici di R, quindi ha ordine 4 (la transitività è ovvia, inoltre, se a è un vertice e $\sigma \in \mathrm{St}_\Delta(a)$, allora σ fissa (globalmente) l'insieme $\{b, c\}$ costituito dai due vertici adiacenti ad a; questi non possono essere tra loro scambiati da σ, perché hanno distanze diverse da a, dunque $\mathrm{St}_\Delta(a)$ fissa anche b e c, sicché $\mathrm{St}_\Delta(a) = 1$. Se poi Λ è il gruppo delle isometrie di un rombo non quadrato, è facile verificare che l'azione di Λ sull'insieme dei vertici del rombo non è transitiva: ogni orbita ha ordine 2. Quindi lo stabilizzante di un vertice ha indice 2 in Λ, e, come si verifica subito, ordine 2. Pertanto anche Λ ha ordine 4. Di fatto sia che Δ che Λ sono isomorfi al gruppo quadrinomio V_4 (ad esempio, perché ciascuno di essi ha più di un elemento di ordine 2). Otteniamo così due rappresentazioni permutazionali fedeli di V_4, entrambe di grado 4: una, regolare, sull'insieme dei vertici del rettangolo R, l'altra, non transitiva, sull'insieme dei vertici del rombo.

Altre Applicazioni

Diverse dimostrazioni dei teoremi di Sylow (vedi [Rob], 1.6.16) utilizzano, in un modo o nell'altro, la nozione di azione permutazionale. Una generalizzazione degli enunciati in [Rob], 1.6.16 è, sempre in [Rob], in 14.3.2. Modificando leggermente la dimostrazione di 1.6.16 (i) (il primo teorema di Sylow) si ottiene la seguente estensione di 1.6.16 (iii) a p-sottogruppi di ordine arbitrario:

1.9. Teorema (cfr. [H], Satz 7.2). *Siano p un numero primo, $a \in \mathbb{N}_0$ e G un gruppo finito di ordine divisibile per p^a. Allora il numero dei sottogruppi di G di ordine p^a è congruo a 1 modulo p.*

Dimostrazione — Sia X l'insieme delle parti di G di ordine p^a. Come osservato in 1.8 si può far agire G su X per moltiplicazione destra. Fissiamo questa azione. Ovviamente $|X| = \binom{|G|}{p^a}$ è la somma degli ordini delle G-orbite in X. Vogliamo calcolare $|X|$ modulo pn, dove n è l'intero $|G|/p^a$, per farlo basterà sommare gli ordini delle G-orbite di ordine non divisibile per pn.

Se $Y \in X$ e $S = \mathrm{St}_G(Y)$, allora $Y = YS = \bigcup_{y \in Y} yS$, una unione di laterali sinistri di S, sicché Y ha una partizione costituita da insiemi equipotenti a S e quindi l'ordine di S divide l'ordine p^a di Y. Pertanto $|S| = p^b$ per un intero non negativo $b \leq a$. Se $b < a$ allora $|\mathrm{Orb}_G(Y)| = |G : S| = np^{a-b}$ è multiplo di pn; se invece $b = a$ allora $|\mathrm{Orb}_G(Y)| = n$ e $|S| = p^a = |Y|$. In questo caso Y (che è unione di laterali sinistri di S) è quindi un laterale sinistro di S, poniamo $Y = yS$. Ma allora $Y = (S^{y^{-1}})y$, un laterale destro del sottogruppo $S^{y^{-1}}$ di G, per cui $\mathrm{Orb}_G(Y)$ non è altro che l'insieme dei laterali destri di un sottogruppo di G di ordine p^a. Viceversa è ovvio che, per ogni sottogruppo H di G di ordine p^a, l'insieme dei laterali destri di H in G è una G-orbita in X di ordine n. In definitiva abbiamo due tipi di G-orbite: quelle il cui ordine è multiplo di pn (che non ci interessano ai fini del calcolo di $|X|$ modulo pn) e quelle di ordine n, che sono precisamente le orbite dei sottogruppi di G di ordine p^a, ovvero gli insiemi dei laterali destri di questi. Allora $|X|$ è congruo modulo pn a n volte il numero delle orbite di questo secondo tipo. Poiché sottogruppi distinti dànno luogo a orbite distinte (un sottogruppo non può essere laterale di un altro sottogruppo), il numero di queste orbite è pari al numero N_{G,p^a} dei sottogruppi di G di ordine p^a. Pertanto

$$\binom{np^a}{p^a} = |X| \equiv nN_{G,p^a} \pmod{pn}. \qquad (*)$$

Quanto appena stabilito vale per ogni gruppo finito di ordine np^a, in particolare vale sostituendo a G un gruppo ciclico C di ordine np^a. Un tale gruppo ha un unico sottogruppo di ordine p^a, quindi $N_{C,p^a} = 1$. Applicando $(*)$ al gruppo C si ha allora $\binom{np^a}{p^a} \equiv n \pmod{pn}$. Ritornando al caso generale possiamo allora sostituire n a $\binom{np^a}{p^a}$ in $(*)$, ottenendo così $n \equiv nN_{G,p^a} \pmod{pn}$, ovvero $N_{G,p^a} \equiv 1 \pmod{p}$, il risultato desiderato. ❑

Val la pena di notare come, nel corso di questa dimostrazione, abbiamo anche provato la seguente formula aritmetica:

$$\binom{np^a}{p^a} \equiv n \pmod{pn}$$

per ogni primo p e per ogni $n \in \mathbb{N}$.

La seguente semplicissima osservazione ha molte eleganti applicazioni in teoria dei gruppi.

1.10. (Argomento di Frattini Generalizzato). *Supponiamo che il gruppo G agisca in modo transitivo sull'insieme X, siano $H \leq G$ e $x \in X$. Allora H è transitivo se e solo se $G = \mathrm{St}_G(x)H$.*

Dimostrazione — Una delle due implicazioni è banale. Supponiamo infatti $G = \mathrm{St}_G(x)H$. Poiché G è transitivo, $X = \mathrm{Orb}_G(x) = \{xgh \mid g \in \mathrm{St}_G(x) \wedge h \in H\}$. D'altra parte $xg = x$ se $g \in \mathrm{St}_G(x)$, quindi $X = \{xh \mid h \in H\} = \mathrm{Orb}_H(x)$, cioè H è transitivo.

Viceversa, se H è transitivo, per ogni $y \in X$ esiste $h \in H$ tale che $y = xh$. Pertanto, per ogni $g \in G$ si ha $xg = xh$ per un opportuno $h \in H$. Allora $gh^{-1} \in \mathrm{St}_G(x)$, dunque $g = (gh^{-1})h \in \mathrm{St}_G(x)H$. Quindi $G \subseteq \mathrm{St}_G(x)H$. L'inclusione opposta è ovvia, dunque $G = \mathrm{St}_G(x)H$, come si voleva. ❑

Come noto dai corsi di algebra, se H e K sono sottogruppi di un gruppo G, il loro prodotto HK è un sottogruppo di G se e solo se $HK = KH$. Dunque la condizione $G = \mathrm{St}_G(x)H$ nell'enunciato di 1.10 può essere equivalentemente espressa come $G = H\,\mathrm{St}_G(x)$.

La più classica delle applicazioni di 1.10 è:

1.11. (Argomento di Frattini). *Sia H un sottogruppo normale finito del gruppo G. Se P è un p-sottogruppo di Sylow di H allora $G = HN_G(P)$.*

Dimostrazione — Sia X l'insieme dei p-sottogruppi di Sylow di H. Poiché $H \lhd G$, per ogni $g \in G$ e per ogni $Q \in X$ si ha $Q^g \in X$; dunque G agisce su X per coniugio. Chiaramente $P \in X$ e $\mathrm{St}_G(P) = N_G(P)$. Il secondo teorema di Sylow assicura che H è transitivo (rispetto a questa azione), pertanto 1.10 implica l'asserto. ❑

L'implicazione interessante (quella non banale) di 1.10 fornisce un metodo per costruire sottogruppi H e K di un gruppo G tali che il loro prodotto sia ancora un sottogruppo. Come ben noto ciò accade sempre purché almeno uno tra H o K sia normale in G, non accade sempre altrimenti. Può essere interessante notare che vale anche il viceversa, ovvero: ogni volta che il prodotto di due sottogruppi di un gruppo è un sottogruppo è possibile interpretare questa circostanza nei termini dell'enunciato di 1.10. Infatti si ha:

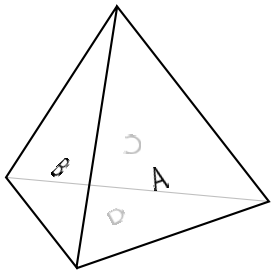
1.12. *Sia G un gruppo e siano H e K due sottogruppi di G. Allora $G = KH$ se e solo se esistono un insieme X ed un'azione permutazionale di G su X tali che, rispetto a questa azione, H sia un sottogruppo transitivo di G e $K = \mathrm{St}_G(x)$ per un opportuno $x \in X$.*

Dimostrazione — La sufficienza della condizione è già espressa in 1.10; è da provarne la necessità. Sia $G = KH$, e consideriamo l'azione di G sui laterali destri di K, come definita in 1.8. Rispetto a quest'azione $K = \mathrm{St}_G(K)$. Inoltre, poiché $G = KH$, ogni laterale destro di K in G si può scrivere come Kh per un opportuno $h \in H$, quindi appartiene alla H-orbita di K. Pertanto H è transitivo e l'asserto è provato. ❑

Esercizio. Si osservi come l'enunciato 1.6.18 (i) in [Rob] è un caso particolare di 1.11.

Concludiamo con un esempio di uso del linguaggio delle rappresentazioni permutazionali di genere completamente diverso.

1.13. Esempio. Supponiamo di voler dipingere le quattro facce di un tetraedro avendo a disposizione k colori. In quanti modi possiamo farlo a meno di rotazioni o di arbitrarie simmetrie del tetraedro stesso? Per poter rispondere, dobbiamo innanzitutto precisare meglio la domanda: stabilire come vogliamo interpretare la clausola 'a meno di rotazioni o di arbitrarie simmetrie'.



Una *colorazione* del nostro tetraedro T è una applicazione dall'insieme $\mathcal{F} = \{A, B, C, D\}$ delle facce di T all'insieme $\mathcal{C}$ dei colori a nostra disposizione. Ad esempio, se $\mathcal{C}$ ha elementi r, b e g, la colorazione definita da $\begin{pmatrix} A & B & C & D \\ r & b & g & b \end{pmatrix}$ esprime la scelta di dipingere A di rosso, B e D di blu e C di giallo. Possiamo ruotare T applicando la rotazione γ intorno all'asse perpendicolare a D e passante per il vertice opposto, che agisce su $\mathcal{F}$ come il 3-ciclo $(A\,B\,C)$. Avendo effettuato questa rotazione, al posto delle faccia A troviamo la faccia $C = A\gamma^{-1}$, di colore giallo; al posto di B abbiamo $A = B\gamma^{-1}$ di colore rosso, al posto di C e D troviamo infine $B = C\gamma^{-1}$ e $D = D\gamma^{-1}$ entrambe di colore blu. La colorazione da cui eravamo partiti è allora indistinguibile, a meno della rotazione γ, dalla colorazione $\begin{pmatrix} A & B & C & D \\ g & r & b & b \end{pmatrix}$, che possiamo indicare, con ovvio abuso di notazione, come $\gamma^{-1}f$. Questo esempio suggerisce come si può precisare la domanda da cui siamo partiti. Definiamo un'azione permutazionale del gruppo Γ delle isometrie di T sull'insieme $\mathcal{C}^{\mathcal{F}}$ delle colorazioni ponendo $f * \gamma = \gamma^{-1}f$ per ogni $f \in \mathcal{C}^{\mathcal{F}}$ e $\gamma \in \Gamma$ (si verifica immediatamente che queste posizioni definiscono un'azione destra, cfr. esercizio 13, p. 3) e diciamo che due colorazioni sono indistinguibili a meno di elementi di Γ se e solo se esse appartengono alla stessa Γ-orbita. Quindi il problema che ci siamo posti diventa: quante sono le orbite rispetto all'azione di Γ su $\mathcal{C}^{\mathcal{F}}$?

Iniziamo a descrivere Γ. Questo gruppo agisce in modo ovvio su $\mathcal{F}$ (esercizio 12, p. 3), e la rappresentazione così ottenuta è fedele. Infatti il suo nucleo K è costituito dalle isometrie che fissano ciascuna delle facce, ma una isometria di T che fissi una faccia fisserà anche il vertice opposto ad essa, quindi ogni elemento di K fissa ciascuno dei vertici del tetraedro e dunque è l'identità. Inoltre, come si vede subito considerando opportune rotazioni, Γ è transitivo su $\mathcal{F}$. Allora, per 1.1 (*iv*), lo stabilizzante Γ_D della faccia D ha indice 4 in Γ. A sua volta Γ_D agisce (cfr. 1.6) su $\{A, B, C\}$, in modo chiaramente transitivo. Dunque $\Gamma_{CD} := \mathrm{St}_{\Gamma_D}(C) = \mathrm{St}_{\Gamma}(\{C, D\})$ ha indice 3 in Γ_D e quindi 12 in Γ. Infine, consideriamo l'azione di Γ_{CD} su $\{A, B\}$. Anche questa è transitiva, infatti la simmetria rispetto al piano per lo spigolo comune a A e B e perpendicolare allo spigolo comune a C e D appartiene a Γ_{CD} e scambia tra loro A e B. Allora lo stabilizzante di A in Γ_{CD} ha ivi indice 2. D'altra parte, questo stabilizzante fissa necessariamente anche B (esercizio 7, p. 2), quindi è il sottogruppo identico, perché l'azione di Γ su $\mathcal{F}$ è fedele. Pertanto $|\Gamma_{CD}| = 2$ e $|\Gamma| = |\Gamma : \Gamma_{CD}| \cdot |\Gamma_{CD}| = 24$. Ora, la rappresentazione permutazionale che stiamo considerando è un monomorfismo $\rho : \Gamma \to Sym\mathcal{F}$, e $Sym\,\mathcal{F}$ ha ordine $4! = 24$. Quindi ρ è un isomorfismo.

Calcoliamo ora, per ogni $k \in \mathbb{N}$, il numero N_k delle colorazioni diverse di T a meno di simmetrie se $k = |\mathcal{C}|$, cioè avendo k colori a disposizione. Per quanto sopra, N_k è il numero di orbite dell'azione di Γ su $\mathcal{C}^{\mathcal{F}}$, cioè, per 1.5, $N_k = \frac{1}{24}\sum_{\gamma\in\Gamma} |\operatorname{Fix}(\gamma)|$. Ora, per ogni $f \in \mathcal{C}^{\mathcal{F}}$ e per ogni $\gamma \in \Gamma$, è chiaro che $f \in \operatorname{Fix}(\gamma)$ se e solo se f è costante su ciascuna orbita di γ in $\mathcal{F}$, cioè se e solo se, scelta comunque una γ-orbita Y in $\mathcal{F}$, tutte le facce appartenenti a Y hanno lo stesso colore. Da ciò si ricava facilmente che $|\operatorname{Fix}(\gamma)|$ è uguale a k elevato al numero delle γ-orbite di $\mathcal{F}$. Per ottenere N_k basterà dunque calcolare il numero delle orbite in $\mathcal{F}$ di ciascun elemento di Γ. Ricordando che ρ è una biezione da Γ a $Sym\,\mathcal{F}$ e che, per ogni $\gamma \in \Gamma$, le γ-orbite coincidono con le γ^ρ-orbite, basta considerare le orbite degli elementi di $Sym\,\mathcal{F}$ su $\mathcal{F}$, che possiamo facilmente descrivere. $Sym\,\mathcal{F}$, gruppo simmetrico su quattro oggetti, consiste di una permutazione identica, 6 trasposizioni, 8 tre-cicli, 3 prodotti di due trasposizioni disgiunte e 6 quattro-cicli, come schematizzato nella tabella:

classe	$(\cdot)$	$(\cdot\cdot)$	$(\cdot\cdot\cdot)$	$(\cdot\cdot)(\cdot\cdot)$	$(\cdot\cdot\cdot\cdot)$
nr. elementi	1	6	8	3	6
nr. orbite	4	3	2	2	1

in cui l'ultima riga riporta il numero delle orbite di ciascun elemento appartenente alla classe di coniugio indicata nella prima riga. Quindi in Γ ci sono: un elemento con quattro orbite, sei con tre orbite, $8 + 3 = 11$ con due orbite e sei con una sola orbita. Allora otteniamo:

$$N_k = \frac{k^4 + 6k^3 + 11k^2 + 6k}{24}.$$

Ad esempio, come è ovvio, $N_1 = 1$: avendo un solo colore a disposizione possiamo colorare T in un solo modo; $N_2 = (16 + 48 + 44 + 12)/24 = 5$. Se $\mathcal{C} = \{r, b\}$ abbiamo le cinque colorazioni:

$$\begin{pmatrix} A & B & C & D \\ r & r & r & r \end{pmatrix} \quad \begin{pmatrix} A & B & C & D \\ r & r & r & b \end{pmatrix} \quad \begin{pmatrix} A & B & C & D \\ r & r & b & b \end{pmatrix} \quad \begin{pmatrix} A & B & C & D \\ r & b & b & b \end{pmatrix} \quad \begin{pmatrix} A & B & C & D \\ b & b & b & b \end{pmatrix},$$

che sono effettivamente a due a due diverse anche a meno di trasformazioni per elementi di Γ, in quanto tra loro differenziate per il numero di facce 'rosse' (o 'blu'). Il fatto che ciascuna Γ-orbita sia caratterizzata proprio dal numero delle facce di ciascun colore (cioè due colorazioni con lo stesso numero di facce rosse siano Γ-equivalenti) è una peculiarità di questo esempio, non una proprietà generale,(*) essa dipende da una importante proprietà (transitività multipla) dell'azione di Γ su $\mathcal{F}$, sulla quale si tornerà più avanti.

Accenniamo anche ad una variazione (che si potrebbe considerare più sensata, in fondo) del problema appena risolto. Con le definizioni date abbiamo considerati indistinguibili due colorazioni simmetriche rispetto ad un piano, come ad esempio $\begin{pmatrix} A & B & C & D \\ r & b & v & g \end{pmatrix}$ e $\begin{pmatrix} A & B & C & D \\ r & b & g & v \end{pmatrix}$. Queste due colorazioni sono ottenibili l'una dall'altra tramite una isometria del tetraedro, ma non tramite un movimento (cioè una isometria associata ad una matrice di determinante 1; più concretamente: una isometria effettivamente realizzabile nello spazio fisico tridimensionale). Se siamo interessati a sapere quante sono le colorazioni possibili di T con k colori disponibili a meno di *movimenti* (cioè di rotazioni) di T possiamo risolvere il problema in modo analogo a quanto fatto per le isometrie. Detto Γ^+ il sottogruppo di Γ costituito dai movimenti che fissano T, possiamo fare agire Γ^+ in modo fedele su $\mathcal{F}$, l'insieme delle facce di T, e, ragionando come sopra, otteniamo che lo stabilizzante Γ^+_{CD} in Γ^+ di $\{C, D\}$ ha indice 12 in Γ^+. Ora però si ha $\Gamma^+_{CD} = 1$, per ovvie considerazioni geometriche, quindi $|\Gamma^+| = 12$. Se ne ricava che $(\Gamma^+)^\rho$, isomorfo a Γ^+, è il gruppo alterno su $\mathcal{F}$, isomorfo dunque ad $\mathbb{A}_4$ (si sarebbe potuto ricavare ciò anche in modo più diretto: osservando che Γ^+ deve avere indice 2 in Γ). Dalla tabella che fornisce il numero delle orbite ricaviamo che in Γ^+ ci sono un elemento con quattro orbite e 11 con 2 orbite, quindi il numero delle colorazioni di T a meno di rotazioni e con k colori a disposizione è

$$N^*_k = \frac{k^4 + 11k^2}{12}.$$

Quindi $N^*_1 = 1 = N_1$, $N^*_2 = 5 = N_2$, $N^*_3 = 15 = N_3$, ma $N^*_4 = 36 \neq 35 = N_4$. Anche il fatto che per $k \leq 3$ si ha $N^*_k = N_k$ non è casuale ma si può ricavare da proprietà di transitività multipla di Γ e Γ^+.

Esercizi.

1. Svolgere in dettaglio il calcolo di N^*_k. Osservare che 1, 2 e 3 sono gli unici interi positivi k per i quali si abbia $N^*_k = N_k$.
2. Calcolare il numero delle terne di elementi (a, b, c) del gruppo D_8 tali che a e b abbiano periodo 2 e c abbia periodo 4, a meno di automorfismi interni di D_8. [*Il risultato è* 13.]

(*) Ad esempio, al posto del tetraedro T consideriamo un cubo. La colorazione del cubo con due facce opposte rosse e le altre blu, e quella con due facce adiacenti rosse e le altre blu non sono indistinguibili, cioè non sono equivalenti rispetto all'azione del gruppo delle isometrie del cubo. Il problema della colorazione del cubo e problemi analoghi sono discussi in [DM], Example 1.4.1 e sezione 1.7.

2. Componenti transitive

In un certo senso lo studio delle rappresentazioni permutazionali si riduce allo studio delle rappresentazioni transitive. Infatti ogni rappresentazione permutazionale di un gruppo G si può scomporre in 'prodotto' (in un senso da specificare) di rappresentazioni transitive di G. Un caso particolare di questo procedimento è già essenzialmente noto: la decomposizione di una permutazione a supporto finito in prodotto di cicli disgiunti.

Sia I una classe completa di rappresentanti delle orbite di una rappresentazione permutazionale ρ. Per ogni $i \in I$ sia X_i l'orbita cui appartiene i e sia ρ_i la rappresentazione permutazionale $G \to Sym\, X_i$ indotta da ρ su X_i (cfr. p. 4). Più esplicitamente, per ogni $g \in G$ e per ogni $x \in X_i$ poniamo $xg^{\rho_i} = xg^{\rho}$. Le rappresentazioni ρ_i si chiamano *componenti transitive* di ρ; è infatti evidente che ciascuna delle ρ_i è transitiva. Si dice anche che ρ è la *somma disgiunta* delle sue componenti transitive ρ_i. Questa terminologia è giustificata dal fatto che le ρ_i determinano ρ, infatti dalle ρ_i si costruisce ρ con una procedura nota come 'incollamento' (forse già incontrata in corsi di topologia): per ogni $g \in G$ il dominio X di g^{ρ} è l'unione (in questo caso disgiunta) dei domini X_i delle permutazioni g^{ρ_i} e ogni $x \in X$ viene mandato da g^{ρ} in xg^{ρ_i}, dove i è l'unico indice tale che $x \in X_i$ (in termini più sintetici: g^{ρ} è l'applicazione di X in sé il cui grafico è l'unione dei grafici delle ρ_i).

Da un punto di vista più astratto, si può descrivere il rapporto tra una rappresentazione permutazionale e le sue componenti transitive in termini puramente categoriali, come si vedrà più avanti (3.5).

Esempio. Consideriamo l'azione ρ del gruppo additivo di $\mathbb{R}$ su $X = \mathbb{R} \times \mathbb{Z}$ definita da $(x, n)a^{\rho} = (x + a, n)$ per ogni $(x, n) \in X$ e $a \in \mathbb{R}$. Dunque a^{ρ} è la traslazione di ampiezza $(a, 0)$ su X, che è a sua volta l'unione delle rette r_n di equazione $y = n$, al variare di n in $\mathbb{Z}$. Ciascuna di queste rette è una ρ-orbita, quindi ogni $n \in \mathbb{Z}$ individua una componente transitiva ρ_n, che ad ogni $a \in \mathbb{R}$ associa la traslazione di ampiezza a sulla retta (orientata) r_n. Ciascuna delle ρ_n è una rappresentazione regolare, quindi ρ si può descrivere come somma disgiunta di una famiglia numerabile di rappresentazioni regolari di $\mathbb{R}$. In un senso che verrà specificato nella prossima sezione, questa descrizione essenzialmente caratterizza ρ, intendendo con ciò che tutte le proprietà di ρ che riguardino la teoria delle rappresentazioni permutazionali sono ricavabili da essa.

Il *prodotto cartesiano* $\prod_{i \in I} G_i$ di una famiglia $(G_i)_{i \in I}$ di gruppi è il gruppo che ha per sostegno il prodotto cartesiano (insiemistico) dei sostegni dei G_i ed operazione definita componente per componente: $(g_i)_{i \in I}(h_i)_{i \in I} = (g_i h_i)_{i \in I}$ per ogni $(g_i)_{i \in I}, (h_i)_{i \in I} \in \prod_{i \in I} G_i$. Questo, munito delle ovvie proiezioni canoniche $pr_i : (g_j)_{j \in I} \in \prod_{j \in I} G_j \mapsto g_i \in G_i$, è il prodotto della famiglia $(G_i)_{i \in I}$ nella categoria dei gruppi.

Si dice poi che un gruppo G è *prodotto subcartesiano* di $(G_i)_{i \in I}$ se e solo se esiste un monomorfismo $\mu : G \rightarrowtail \prod_{i \in I} G_i$ tale che $\mu\, pr_i$ sia suriettivo per ogni $i \in I$. Pur non determinando univocamente il tipo di isomorfismo di G a partire da quelli dei gruppi G_i, questa condizione restringe fortemente la struttura di G: equivale infatti a richiedere che G abbia una famiglia di sottogruppi normali $(N_i)_{i \in I}$ tali che G/N_i sia isomorfo a G_i per ogni $i \in I$ (si veda [Rob], p. 57).

2.1. *Sia $\rho : G \to Sym\, X$ una rappresentazione permutazionale. Se I e, per ogni $i \in I$, le componenti transitive ρ_i sono definite come sopra,* $\operatorname{im}\rho$ *è prodotto subcartesiano di* $(\operatorname{im}\rho_i)_{i \in I}$.

Dimostrazione — L'applicazione $\nu : g \in G \mapsto (g^{\rho_i})_{i \in I} \in \prod_{i \in I} \operatorname{im}\rho_i$ è evidentemente un omomorfismo di nucleo $\ker\rho$. Sia ν' il monomorfismo $G/\ker\rho \rightarrowtail \prod_{i \in I} \operatorname{im}\rho_i$ da essa indotto. Componendo con ν' l'isomorfismo da $\operatorname{im}\rho$ a $G/\ker\rho$ indotto da ρ si ottiene un monomorfismo $\mu : \operatorname{im}\rho \rightarrowtail \prod_{i \in I} \operatorname{im}\rho_i$. Per ogni $i \in I$ si ha $\operatorname{im}\mu\, pr_i = \operatorname{im}\nu'\, pr_i = \operatorname{im}\nu\, pr_i = \operatorname{im}\rho_i$, dalla qual cosa segue l'asserto. ❑

Almeno nel caso delle rappresentazioni permutazionali su insiemi finiti, le componenti transitive di una rappresentazione permutazionale ρ dànno luogo ad una utilissima decomposizione degli elementi di $\operatorname{im}\rho$. Per poter esprimere questa decomposizione nel caso generale abbiamo bisogno di definire un 'prodotto infinito' tra permutazioni, prodotto definito solo per particolari famiglie di permutazioni. Sia $(\sigma_i)_{i \in I}$ una famiglia di permutazioni a due a due disgiunte di un insieme X. Indichiamo con $\prod_{i \in I} \sigma_i$ e chiamiamo prodotto della famiglia $(\sigma_i)_{i \in I}$ la permutazione di X che fissa ogni elemento di $X \setminus \bigcup_{i \in I} \operatorname{supp}(\sigma_i)$ e manda ogni altro elemento x di X in $x\sigma_i$, dove i è l'unico elemento di I tale che $x \in \operatorname{supp}(\sigma_i)$. Se I è finito $\prod_{i \in I} \sigma_i$ coincide con l'ordinario prodotto tra le permutazioni σ_i, dove, essendo queste ultime permutabili tra loro in quanto disgiunte, l'ordine dei fattori è irrilevante.

Siano ora ρ un'arbitraria rappresentazione permutazionale, I una classe completa di rappresentanti delle ρ-orbite e ρ_i, al variare di $i \in I$, le componenti transitive di ρ. Per ogni $i \in I$ poniamo $\hat{\rho}_i := \rho_i \mu_i$, dove μ_i è il monomorfismo canonico $Sym\, X_i \rightarrowtail Sym\, X$ (quello definito a p. 4, nell'osservazione successiva a 1.7). Quindi $g^{\hat{\rho}_i} \in \mathrm{St}_{\rho}(X \setminus X_i)$ e $xg^{\hat{\rho}_i} = xg^{\rho}$ per ogni $g \in G$ e $x \in X_i$. In termini meno formali, $\hat{\rho}_i$ è la rappresentazione transitiva di G su X che fa operare ogni $g \in G$ come g^{ρ} sugli elementi dell'orbita X_i e come l'identità sugli altri elementi di G. Ovviamente, se i e j sono elementi distinti di I e $g, h \in G$, allora $g^{\hat{\rho}_i}$ e $h^{\hat{\rho}_j}$ sono permutazioni disgiunte, e si ha $g^{\rho} = \prod_{i \in I} g^{\hat{\rho}_i}$. Questa fattorizzazione di g^{ρ} si chiama decomposizione di g^{ρ} rispetto alle ρ-orbite.

Il caso particolare più importante è la decomposizione di una permutazione in cicli disgiunti, che verrà presto discussa.

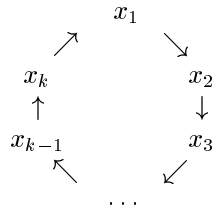
Esercizio. Sia π una partizione dell'insieme X. Per ogni $Y \in \pi$ sia ι_Y il monomorfismo canonico $Sym Y \rightarrowtail Sym X$. Allora l'applicazione

$$(\sigma_Y)_{Y\in\pi} \in \prod_{Y\in\pi} Sym Y \longmapsto \prod_{Y\in\pi} (\sigma_Y)^{\iota_Y} \in \bigcap_{Y\in\pi} \mathrm{St}^*_{Sym X}(Y)$$

è un isomorfismo. Esso induce un isomorfismo dal prodotto diretto $\mathrm{Dr}_{Y\in\pi} Sym Y$ a $\langle \mathrm{St}_{Sym X}(X \smallsetminus Y) \mid Y \in \pi\rangle$.

Cicli

Chiamiamo *ciclo* una permutazione transitiva sul suo supporto, cioè una permutazione γ tale che $\mathrm{supp}(\gamma)$ sia o l'insieme vuoto (nel qual caso $\gamma = 1$) oppure una γ-orbita. Equivalentemente, un ciclo è una permutazione che ha al più una orbita contenente più di un elemento. La *lunghezza* del ciclo γ è, per definizione, 1 se γ è la permutazione identica, $|\mathrm{supp}(\gamma)|$ altrimenti. I cicli di lunghezza finita k si chiamano anche k-cicli, i 2-cicli anche *trasposizioni*. Verifichiamo che i cicli di lunghezza finita hanno la familiare descrizione nota dai corsi di algebra. Come segue dall'esercizio 8 di p. 2, l'identità è l'unico ciclo di lunghezza 1. Sia poi γ un ciclo di lunghezza finita maggiore di 1, e sia x un qualsiasi elemento del suo supporto. Posto $x_i = x\gamma^{i-1}$ per ogni $i \in \mathbb{Z}$, l'insieme $\{x_i \mid i \in \mathbb{Z}\}$, essendo la γ-orbita di x, ossia il supporto di γ, è finito e si ha $x_{k+1} \in S = \{x_1, \dots, x_k\}$ per qualche $k \in \mathbb{N}$. Scegliamo il minimo k con questa proprietà. È chiaro che $S = S\gamma$ e che quindi S è la γ-orbita di $x = x_1$, dunque $S = \mathrm{supp}(\gamma)$. Per la minimalità di k gli elementi $x_1, \dots, x_k$ sono a due a due distinti (e quindi k è proprio la lunghezza di γ) e, per l'iniettività di γ, se $1 < i \leq k$ si ha $x_k\gamma \neq x_{i-1}\gamma = x_i$. Pertanto, poiché $x_k\gamma = x_{k+1} \in S$, deve essere $x_k\gamma = x_1$. L'azione di γ si può dunque descrivere con il diagramma in figura: $x = x_1$ viene mandato in x_2, questo in x_3, questo in x_4 e così via, sino ad arrivare ad x_k, che viene mandato in x_1. Tutti gli altri elementi di X (cioè quelli di $X \smallsetminus \{x_1, x_2, \dots, x_k\}$) sono fissati da γ. Come ben noto, per indicare il ciclo γ appena descritto si utilizza la notazione $(x_1\, x_2 \cdots x_k)$. In termini più espliciti, se a_1, $a_2, \dots, a_k$ sono elementi *distinti* di X, con la scrittura $(a_1\, a_2 \cdots a_k)$ si indica la permutazione di X che manda a_i in a_{i+1} per $1 \leq i < k$ e a_k in a_1 (più brevemente: la permutazione in questione manda ciascun a_i in a_{i+1}, dove gli indici vanno letti modulo k) e fissa tutti gli altri elementi di X. Questa permutazione risulta appunto essere un ciclo, di supporto $\{a_1, \dots, a_k\}$, e quanto sopra assicura che ogni k-ciclo ha questa forma.



Per quanto riguarda invece i cicli infiniti (cioè di lunghezza infinita), osserviamo innanzitutto che essi hanno tutti lunghezza numerabile. Infatti, se γ è un ciclo infinito, allora $\mathrm{supp}\,\gamma$, essendo una $\langle\gamma\rangle$-orbita, ha cardinalità minore o uguale a quella di $\langle\gamma\rangle$ per 1.1 (*ii*). Una descrizione di un ciclo infinito γ analoga al diagramma disegnato per cicli di lunghezza finita sarà, come si verifica subito, della forma

$$\cdots \mapsto x_{-(n+1)} \mapsto x_{-n} \mapsto \cdots \mapsto x_{-2} \mapsto x_{-1} \mapsto x_0 \mapsto x_1 \mapsto x_2 \mapsto \cdots \mapsto x_n \mapsto x_{n+1} \mapsto \cdots,$$

dove $x = x_0$ è un qualsiasi elemento di $\mathrm{supp}(\gamma)$ e $x_i = x\gamma^i$ per ogni $i \in \mathbb{Z}$. Un tale ciclo viene talvolta indicato come $(\cdots x_{-n} \cdots x_{-2}\, x_{-1}\, x_0\, x_1\, x_2 \cdots x_n \cdots)$. Un esempio di ciclo infinito è la permutazione $n \mapsto n+1$ di $\mathbb{Z}$, che si può informalmente scrivere come $(\cdots -n \cdots -2\ -1\ 0\ 1\ 2 \cdots n \cdots)$.

Esercizi. Per cicli di lunghezza finita i seguenti fatti di importanza essenziale dovrebbero essere ben noti dal corso di algebra.

1. Il periodo di ogni ciclo coincide con la sua lunghezza. (In particolare, i cicli di lunghezza infinita sono aperiodici).

Con riferimento al k-ciclo γ descritto sopra:

2. Le k-uple $(a_1, \dots, a_k)$ di elementi distinti di X tali che $\gamma = (a_1 \cdots a_k)$ sono precisamente k. Quali sono?
3. Se $k \leq n$ sono interi positivi, il numero dei k-cicli appartenenti a $\mathbb{S}_n$ è $n!/k(n-k)!$.
4. γ è prodotto delle $k-1$ trasposizioni $(x_1\, x_2)(x_1\, x_3)\cdots(x_1\, x_k)$.
5. Vale la regola di calcolo $(x_1\, x_2 \cdots x_k)^\sigma = (x_1^\sigma\, x_2^\sigma \cdots x_k^\sigma)$ per ogni $\sigma \in Sym X$. Analogamente, per cicli infiniti vale $(\cdots x_{-n} \cdots x_{-1}\, x_0\, x_1 \cdots x_n \cdots)^\sigma = (\cdots x_{-n}^\sigma \cdots x_{-1}^\sigma\, x_0^\sigma\, x_1^\sigma \cdots x_n^\sigma \cdots)$.

A proposito della notazione utilizzata per scrivere i cicli su un insieme X, è bene osservare l'ambiguità derivante dal fatto che questa notazione non fa riferimento all'insieme X stesso. Ad esempio, il ciclo $\pi = (1\,2\,3) \in \mathbb{S}_4$ ed il ciclo $\pi' = (1\,2\,3) \in \mathbb{S}_5$, pur scrivendosi nello stesso modo, sono due oggetti distinti, essendo applicazioni con distinti domini e codomini. D'altra parte π' è l'immagine di π tramite il monomorfismo canonico di $\mathbb{S}_4$ in $\mathbb{S}_5$ (vedi p. 4), il che rende più sopportabile questa ambiguità notazionale (si veda anche 3.3).

2.2. *Siano σ e τ due cicli sull'insieme X. Allora σ e τ sono coniugati in $Sym X$ se e solo se hanno la stessa lunghezza e $|\mathrm{Fix}(\sigma)| = |\mathrm{Fix}(\tau)|$. In particolare due qualunque cicli su X della stessa lunghezza finita sono coniugati in $Sym X$.*

Dimostrazione — Se $\tau = \sigma^\pi$ per un $\pi \in Sym X$, allora $\mathrm{supp}(\tau) = \mathrm{supp}(\sigma)\pi$ per l'esercizio 15 a p. 3, dunque anche $\mathrm{Fix}(\tau) = \mathrm{Fix}(\sigma)\pi$. Quindi le lunghezze di σ e τ (cioè $|\mathrm{supp}(\sigma)|$ e $|\mathrm{supp}(\tau)|$ se σ non è identica, 1 altrimenti) coincidono e $|\mathrm{Fix}(\sigma)| = |\mathrm{Fix}(\tau)|$. Viceversa, siano $\mathrm{Fix}(\sigma)$ e $\mathrm{Fix}(\tau)$ equipotenti ed abbiano σ e τ la stessa lunghezza. Se questa lunghezza è 1, allora $\sigma = \tau$ (è la permutazione identica), possiamo dunque supporre che la lunghezza sia maggiore di 1, cioè che σ e τ siano entrambi non identici. Esiste un'applicazione biettiva $f : \mathrm{Fix}(\sigma) \to \mathrm{Fix}(\tau)$. Inoltre, scrivendo

σ e τ rispettivamente come $(x_1\, x_2 \cdots x_k)$ e $(y_1\, y_2 \cdots y_k)$ se di lunghezza finita, o come $(\cdots x_{-n} \cdots x_{-1}\, x_0\, x_1 \cdots x_n \cdots)$ e $(\cdots y_{-n} \cdots y_{-1}\, y_0\, y_1 \cdots y_n \cdots)$ se infiniti, poiché sia gli elementi x_i che gli elementi y_i sono a due a due distinti, la posizione $x_i \mapsto y_i$, al variare di i nell'opportuno insieme di indici, definisce un'applicazione biettiva g da $\mathrm{supp}(\sigma)$ a $\mathrm{supp}(\tau)$. Ora l'applicazione

$$h : x \in X \longmapsto \begin{cases} xf, & \text{se } x \in \mathrm{Fix}(\sigma) \\ xg, & \text{se } x \in \mathrm{supp}(\sigma) \end{cases} \in X$$

è una permutazione di X tale che $\sigma^h = \tau$. Dunque la condizione enunciata è sufficiente affinché σ e τ siano coniugati.

Infine dimostriamo l'ultima affermazione. Se σ e τ hanno la stessa lunghezza finita, anche $\mathrm{Fix}(\sigma) = X \smallsetminus \mathrm{supp}(\sigma)$ e $\mathrm{Fix}(\tau) = X \smallsetminus \mathrm{supp}(\tau)$ saranno equipotenti, quindi, per quanto appena provato, σ e τ sono coniugati in $Sym\, X$. ❑

Mostriamo con un esempio che cicli infiniti possono non essere coniugati tra loro (pur avendo necessariamente la stessa lunghezza), a differenza di quanto accade per cicli finiti. Sia $\sigma : n \mapsto n+1$ il già menzionato ciclo in $\mathbb{Z}$, e sia τ il ciclo in $\mathbb{Z}$ che fissa ogni intero dispari e manda ciascun intero pari n in $n+2$, cioè $(\cdots -2n \cdots -4\ -2\ 0\ 2\ 4 \cdots 2n \cdots)$. Poiché $\mathrm{Fix}(\sigma) = \varnothing$ e $\mathrm{Fix}(\tau) \neq \varnothing$, certamente σ e τ non sono coniugati in $Sym\, \mathbb{Z}$.

Decomposizione in cicli disgiunti

Vediamo ora in quale modo i cicli appaiono come componenti transitive di permutazioni.

Se σ è un'arbitraria permutazione sull'insieme X, possiamo ragionare su σ facendo riferimento alla ovvia rappresentazione permutazionale $\rho : \langle\sigma\rangle \hookrightarrow Sym\, X$. Sia I una classe completa di rappresentanti delle σ-orbite e indichiamo con X_i la σ-orbita cui appartiene l'elemento i di I. Se ripetiamo la costruzione effettuata per le componenti transitive ρ_i e per le rappresentazioni $\hat{\rho}_i$ otteniamo che $\sigma_i := \sigma^{\hat{\rho}_i}$ è la permutazione di X che opera come σ sugli elementi di X_i e stabilizza $X \smallsetminus X_i$. Evidentemente σ_i è un ciclo, identico se e solo se $|X_i| = 1$, cioè se e solo se i è fissato da σ, di supporto X_i altrimenti. Inoltre, per quanto osservato nel caso generale, i cicli σ_i sono a due a due disgiunti e $\sigma = \sigma^\rho = \prod_{i\in I} \sigma_i$; ovviamente da questo prodotto possiamo espungere tutte le occorrenze della permutazione identica, ottenendo così una decomposizione di σ come prodotto di cicli non identici a due a due disgiunti: $\sigma = \prod_{i\in J} \sigma_i$, dove $J = I \smallsetminus \mathrm{Fix}(\sigma)$. Viceversa, se $\sigma = \prod_{a\in A} \tau_a$ è una decomposizione di σ come prodotto di cicli non identici a due a due disgiunti, è evidente che i supporti dei cicli τ_a sono precisamente le σ-orbite contenute in $\mathrm{supp}(\sigma)$, vale a dire $\{\mathrm{supp}(\tau_a) \mid a \in A\} = \{X_i \mid i \in J\} = \{\mathrm{supp}(\sigma_i) \mid i \in J\}$. Inoltre, se $a \in A$ e i è l'elemento (necessariamente unico) di J tale che $\mathrm{supp}(\tau_a) = \mathrm{supp}(\sigma_i)$, si ha $x\tau_a = x\sigma = x\sigma_i$ per ogni $x \in X_i$, dunque $\tau_a = \sigma_i$. Ciò prova $\{\tau_a \mid a \in A\} = \{\sigma_i \mid i \in J\}$. Esprimiamo questo fatto dicendo che le due decomposizioni sono essenzialmente la stessa (in parole povere: vi appaiono gli stessi fattori). In conclusione:

2.3. *Ogni permutazione non identica ha una ed essenzialmente una sola decomposizione in prodotto di cicli non identici a due a due disgiunti.*

Come visto, la decomposizione in prodotto di cicli disgiunti di una permutazione esprime la partizione in orbite del suo dominio, per questo capita frequentemente di leggere espressioni come 'σ ha un ciclo di lunghezza n' per indicare il fatto che la permutazione σ ha un'orbita di cardinalità n. Osserviamo anche che una permutazione è finitaria se e solo se nella sua decomposizione in cicli disgiunti non identici appare solo un numero finito di fattori e questi hanno tutti lunghezza finita.

Esempio. Se σ è la permutazione $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 6 & 5 & 4 & 7 \end{pmatrix} \in \mathbb{S}_7$, le σ-orbite sono $X_1 = \{1,2,3\}$, $X_6 = \{4,6\}$, $X_5 = \{5\}$ e $X_7 = \{7\}$, dove i pedici sono stati scelti in accordo alle notazioni usate sopra partendo dall'insieme $I = \{1,5,6,7\}$ di rappresentanti delle σ-orbite. Con notazioni ancora conformi, $\sigma_1 = (1\,2\,3)$ e $\sigma_6 = (4\,6)$ corrispondono alle orbite contenute in $\mathrm{supp}(\sigma)$ e dànno quindi luogo alla fattorizzazione $\sigma = \sigma_1\sigma_6$ in prodotto di cicli disgiunti, mentre $\sigma_5 = \sigma_7$ è la permutazione identica in $\mathbb{S}_7$.

Dato un numero intero $n \neq 0$, sia ora τ la permutazione $x \mapsto x+n$ di $\mathbb{Z}$ (cioè l'immagine di n nella rappresentazione regolare destra del gruppo additivo di $\mathbb{Z}$). Le orbite di τ sono i laterali $n\mathbb{Z}+i$, cioè le n classi di coniugio modulo n, la scomposizione di τ in cicli disgiunti è $\tau = \tau_0\tau_1 \cdots \tau_{n-1}$, dove ciascuno dei τ_i è il ciclo in $Sym\, \mathbb{Z}$ che manda il generico elemento $nk+i$ di $n\mathbb{Z}+i$ in $n(k+1)+i$ e fissa tutti gli elementi di $\mathbb{Z} \smallsetminus (n\mathbb{Z}+i)$.

La permutazione $n \mapsto -n$ di $\mathbb{Z}$ ha invece infinite orbite di ordine 2 e un'orbita ($\{0\}$) di ordine 1. Essa si decompone in prodotto di cicli non identici a due a due disgiunti come $\prod_{n\in\mathbb{N}} t_n$, dove, per ogni $n \in \mathbb{N}$, t_n è la trasposizione $(-n\ \ n)$.

Esercizi. Generalizzando quanto noto nel caso finito, verificare:

1. Se $\sigma = \prod_{i\in I} \sigma_i$ è una decomposizione della permutazione σ come prodotto di cicli a due a due disgiunti, si ha $\sigma^n = \prod_{i\in I} \sigma_i^n$ per ogni $n \in \mathbb{Z}$. Dedurne che il periodo di σ è il minimo comune multiplo delle lunghezze dei cicli σ_i, qualora queste lunghezze siano tutto finite ed abbiano minimo comune multiplo in $\mathbb{N}$, infinito altrimenti.
2. Due permutazioni σ e τ di uno stesso insieme X sono coniugate in $Sym\, X$ se e solo se hanno la stessa struttura ciclica, dove quest'ultima locuzione vuol dire che esiste una biezione tra l'insieme delle σ-orbite e quello delle τ-orbite tale che orbite corrispondenti siano equipotenti. Alternativamente questa condizione si può esprimere così: se $\sigma = \prod_{i\in I} \sigma_i$ e $\tau = \prod_{i\in J} \tau_i$ sono decomposizioni di σ e τ come prodotti di cicli non identici a due a due

disgiunti, allora esiste una biezione tra I e J tale che, per ogni $i \in I$ il ciclo σ_i abbia la stessa lunghezza di τ_j, dove j è l'immagine di i mediante questa biezione, ed inoltre $|\mathrm{Fix}(\sigma)| = |\mathrm{Fix}(\tau)|$. (Quando σ è finitaria la condizione sugli insiemi dei punti fissi è conseguenza della condizione precedente; a questo proposito si veda 2.2).

3. Se σ appartiene ad un gruppo semiregolare di permutazioni i fattori della decomposizione di σ in prodotto di cicli disgiunti hanno tutti la stessa lunghezza.

Parità — Il gruppo alterno

Il contenuto di questa sottosezione è riferito esclusivamente alle permutazioni finitarie (cioè a supporto finito), introdotte tra gli esercizi a p. 3. Tra queste sono ovviamente comprese *tutte* le permutazioni su un insieme finito.

Come segue dall'esercizio 4 di p. 10 e da 2.3, ogni permutazione finitaria è prodotto (finito) di cicli di lunghezza finita, ciascuno dei quali è a sua volta prodotto di trasposizioni. Quindi ogni permutazione finitaria è prodotto di (un numero finito di) trasposizioni. In altri termini:

2.4. *Sia X un insieme. Allora $FSymX$ è il sottogruppo generato dalle trasposizioni in X.*

Più precisamente, si può provare che una permutazione finitaria σ si può scrivere o come prodotto di un numero pari o come prodotto di un numero dispari di trasposizioni, ma non è possibile che si verifichino entrambe le eventualità. Si dice che σ è pari nel primo caso, dispari nel secondo. Ovviamente la buona posizione di questa definizione dipende dall'averne dimostrato la premessa. Per aggirare questa difficoltà formuliamo diversamente la definizione, dimostreremo poi che la nuova è equivalente alla prima formulazione data.

Sia σ una permutazione finitaria. Indicato con N_σ il numero delle σ-orbite di ordine maggiore di 1 (cioè contenute in $\mathrm{supp}(\sigma)$; ovviamente $N_\sigma \in \mathbb{N}_0$), diciamo che σ è una *permutazione pari* se la differenza $|\mathrm{supp}(\sigma)| - N_\sigma$ è pari, una *permutazione dispari* altrimenti. Diciamo anche che la classe di resto modulo 2 di $|\mathrm{supp}(\sigma)| - N_\sigma$ è la *parità* di σ. Osserviamo che N_σ è il numero dei fattori nella decomposizione di σ in prodotto di cicli disgiunti non identici. Se γ è un k-ciclo, la parità di γ è facile da calcolare: se γ è identico allora $|\mathrm{supp}(\gamma)| = 0 = N_\sigma$, quindi γ è pari; altrimenti $|\mathrm{supp}(\gamma)| = k$ e $N_\sigma = 1$, quindi la parità di γ è la stessa di $k-1$. Pertanto, in ciascun caso, γ è pari se k è dispari, dispari se k è pari. In particolare le trasposizioni sono permutazioni dispari. Notiamo anche che se σ e τ sono due permutazioni finitarie disgiunte, allora $|\mathrm{supp}(\sigma\tau)| = |\mathrm{supp}(\sigma)| + |\mathrm{supp}(\tau)|$ e $N_{\sigma\tau} = N_\sigma + N_\tau$, sicché la parità di $\sigma\tau$ è la somma delle parità di σ e τ. Questo permette di calcolare agevolmente la parità di una permutazione finitaria una volta che ne sia nota la decomposizione in cicli disgiunti (o in orbite).

Due fatti molto importanti: che le permutazioni pari costituiscono un sottogruppo e che la definizione di parità data equivale a quella proposta per prima sono conseguenze di questa proposizione:

2.5. Proposizione. *Sia X un insieme. L'applicazione che ad ogni $\sigma \in FSymX$ associa la parità di σ è un omomorfismo da $FSymX$ al gruppo additivo di $\mathbb{Z}_2$.*

Dimostrazione — Sia f l'applicazione definita nell'enunciato. Per provare $(\sigma\tau)f = \sigma f + \tau f$ per ogni $\sigma, \tau \in FSymX$ basta limitarsi al caso in cui il secondo fattore (τ) sia una trasposizione. Infatti, assumiamo di aver dimostrato che vale $(\alpha t)f = \alpha f + tf$ per ogni $\alpha \in FSymX$ e per ogni trasposizione t su X. Sappiamo che τ è prodotto di un numero n di trasposizioni; ragioniamo per induzione su n per provare $(\sigma\tau)f = \sigma f + \tau f$. Se $n = 0$, ovvero $\tau = 1$, quanto desiderato segue dal fatto che la permutazione identica è pari. Se $n > 0$, allora $\tau = \tau_1 t$, dove τ_1 è prodotto di $n-1$ trasposizioni. L'assunzione fatta assicura che $(\sigma\tau)f = \big((\sigma\tau_1)t\big)f = (\sigma\tau_1)f + tf$ e $\tau f = (\tau_1 t)f = \tau_1 f + tf$, l'ipotesi di induzione che $(\sigma\tau_1)f = \sigma f + \tau_1 f$. Pertanto $(\sigma\tau)f = (\sigma\tau_1)f + tf = \sigma f + \tau_1 f + tf = \sigma f + \tau f$, come si voleva.

Possiamo dunque supporre che τ sia una trasposizione, poniamo $\tau = (x\,y)$. Dal momento che τ è una permutazione dispari ciò che dobbiamo provare è che $\sigma\tau$ e σ hanno parità diverse. Iniziamo con l'osservare che, scelti comunque $r, s \in \mathbb{N}_0$ e $a_1, \dots, a_r, b_1, \dots, b_s$, elementi di X a due a due distinti tra loro e distinti da x e y, vale l'identità

$$(x\,a_1\,a_2 \cdots a_r\,y\,b_1\,b_2 \cdots b_s)(x\,y) = (x\,a_1\,a_2 \cdots a_r)(y\,b_1\,b_2 \cdots b_s), \qquad (*)$$

dove i simboli (x) e (y), che appaiono nel caso in cui $r = 0$ o $s = 0$, rappresentano l'identità in X. La verifica è diretta e immediata. Per concludere la dimostrazione distinguiamo ora due casi:

— Se x e y appartengono ad una stessa σ-orbita, nella decomposizione di σ in prodotto di cicli disgiunti non identici apparirà un ciclo della forma $\gamma = (x\,a_1\,a_2 \cdots a_r\,y\,b_1\,b_2 \cdots b_s)$. Se σ_1 è il prodotto dei rimanenti cicli, $\sigma = \sigma_1\gamma$ e la parità di σ è $\sigma f = \sigma_1 f + \gamma f$ perché σ_1 e γ sono disgiunte; analogamente $(\sigma\tau)f = \sigma_1 f + (\gamma\tau)f$. La parità γf di γ è quella di $(r+s+2)-1 = r+s+1$, quella di $\gamma\tau$ è, per $(*)$, la parità di $(r+1)-1+(s+1)-1 = r+s$, quindi $\gamma f \neq (\gamma\tau)f$ e $\sigma f \neq (\sigma\tau)f$, come desiderato.

— Se x e y non appartengono ad una stessa σ-orbita, detti $\gamma_x = (x\,a_1\,a_2 \cdots a_r)$ e $\gamma_y = (y\,b_1\,b_2 \cdots b_s)$ i cicli corrispondenti alle σ-orbite di x e y rispettivamente, poiché $\tau^{-1} = \tau$ segue da $(*)$ che $\gamma_x\gamma_y\tau$ è un ciclo non identico e quindi che x e y appartengono alla stessa $(\sigma\tau)$-orbita. Per quanto al caso precedente, $\sigma\tau$ ha parità diversa da quella di $\sigma\tau\tau = \sigma$. ❑

L'omomorfismo f definito nella proposizione precedente ha per nucleo l'insieme delle permutazioni pari, che è così un sottogruppo normale di $FSymX$ —anzi, come si verifica subito, di $Sym\,X$— detto *gruppo alterno* di X e denotato con $AltX$. Per il primo teorema di omomorfismo $FSymX\,/\,AltX$ è isomorfo all'immagine di f, quindi

$|FSymX\,/\,AltX| \leq 2$. Se $|X| \leq 1$, allora $SymX = FSymX = AltX$ è un gruppo identico, se $|X| > 1$ invece $AltX < FSymX$ e quindi $|FSymX\,/\,AltX| = 2$, perché in questo caso esiste almeno una trasposizione, e quindi una permutazione dispari, in $FSymX$.

2.6. *Sia X un insieme. Allora $AltX$ è il sottogruppo generato dai 3-cicli in X.*

Dimostrazione — Gli elementi di $AltX$ sono i prodotti di un numero (finito) pari di trasposizioni, dunque $AltX$ è generato dagli elementi di $SymX$ che si esprimano come prodotto di due trasposizioni. Quindi, tenendo presente che ogni 3-ciclo appartiene ad $AltX$, basterà verificare che il prodotto di due arbitrarie trasposizioni t_1 e t_2 è anche prodotto di 3-cicli. Se $t_1 = t_2$ ciò è banalmente vero: $t_1t_2 = 1$. Altrimenti, se t_1 e t_2 non sono disgiunte possiamo scriverle come $(a\,b)$ e $(a\,c)$ per opportuni elementi distinti a, b e c di X, e si ha $t_1t_2 = (a\,b\,c)$. Se infine t_1 e t_2 sono disgiunte, poniamo $t_1 = (a\,b)$ e $t_2 = (c\,d)$, allora $t_1t_2 = (a\,b\,c)(c\,a\,d)$. ❑

3. Categorie di rappresentazioni permutazionali

Per lo studio dei gruppi di permutazione e delle rappresentazioni permutazionali è necessario stabilire dei criteri di confronto che permettano di esprimere il fatto che due rappresentazioni permutazionali siano equivalenti dal punto di vista della determinazione delle loro proprietà —di quelle a cui siamo interessati— nello stesso senso in cui lo sono, in teoria dei gruppi, due gruppi tra loro isomorfi o, in topologia, due spazi topologici tra loro omeomorfi. Ad esempio, tutti converremo che l'azione del gruppo

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

su $\{1,2,3,4\}$ è in qualche senso identificabile con quella di

$$W = \{1, (56)(78), (57)(68), (58)(67)\}$$

su $\{5,6,7,8\}$, ma è tutt'altra cosa rispetto all'azione data dall'omomorfismo nullo $v \in V \mapsto 1 \in \mathbb{S}_4$.

Per precisare queste idee introduciamo la categoria $\mathcal{RP}$ delle rappresentazioni permutazionali. Gli oggetti di questa categoria sono appunto le rappresentazioni permutazionali di gruppi. Se $\rho : G \longrightarrow SymX$ e $\varphi : H \longrightarrow SymY$ sono rappresentazioni permutazionali, definiamo come $\mathcal{RP}$-*morfismi* da ρ a φ le quaterne $(\rho, \varphi, \alpha, f)$ dove α è un omomorfismo di gruppi da G ad H e f è un'applicazione da X ad Y tali che, per ogni $g \in G$, sia commutativo il diagramma:

$$\begin{array}{ccc} X & \xrightarrow{\;g^\rho\;} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{\;(g^\alpha)^\varphi\;} & Y \end{array} \quad , \qquad (*)$$

cioè valga $g^\rho f = f g^{\alpha\varphi}$. Ove siano intese le rappresentazioni permutazionali ρ e φ, chiameremo $(\rho, \varphi, \alpha, f)$ *l'$\mathcal{RP}$-morfismo determinato da* (α, f). È facile verificare che, definendo il prodotto tra morfismi (componibili) secondo la regola $(\rho, \varphi, \alpha_1, f_1)\cdot(\varphi, \psi, \alpha_2, f_2) = (\rho, \psi, \alpha_1\alpha_2, f_1f_2)$, si determina, appunto, una categoria. L'identità di una rappresentazione $\rho : G \longrightarrow X$ è la quaterna di prime due coordinate ρ e ultime due coordinate le identità di G e di X rispettivamente, gli $\mathcal{RP}$-isomorfismi (detti anche *similitudini*) sono precisamente i morfismi del tipo $(\rho, \varphi, \alpha, f)$ con α e f biettive, come è facile verificare.

Due rappresentazioni permutazionali $\rho : G \longrightarrow SymX$ e $\varphi : H \longrightarrow SymY$ sono dunque $\mathcal{RP}$-isomorfe (o, come si dice, *simili*) se e solo se esistono un isomorfismo $\alpha : G \xrightarrow{\sim} H$ ed una biezione $f : X \to Y$ tali che $(*)$ sia un diagramma commutativo per ogni $g \in G$ (in particolare, se ciò accade, allora $G \simeq H$ e $|X| = |Y|$).

Ritornando all'esempio di sopra, con la terminologia ora introdotta, il fatto che le azioni di V ed W siano 'identificabili' si può esprimere osservando che esse (cioè le immersioni $V \hookrightarrow \mathbb{S}_4$ e $W \hookrightarrow Sym(\{5,6,7,8\})$) sono simili. Un $\mathcal{RP}$-isomorfismo è determinato dalla coppia (α, f), dove $f : n \in \{1,2,3,4\} \mapsto n+4 \in \{5,6,7,8\}$ e α è definito da $(12)(34) \mapsto (56)(78)$ e $(13)(24) \mapsto (57)(68)$.

La nozione di similitudine così introdotta estende quella nota dai corsi di algebra per elementi dei gruppi finiti di permutazione. Infatti:

3.1. *Siano X un insieme, Γ e Δ due sottogruppi di $SymX$. Allora Γ e Δ sono simili se e solo se sono coniugati in $SymX$.*

Dimostrazione — La coppia (α, f) determini un $\mathcal{RP}$-isomorfismo da Γ a Δ (come sempre intendiamo: tra le immersioni di Γ e Δ in $SymX$). Allora $f \in SymX$ e, per ogni $g \in \Gamma$, il diagramma

$$\begin{array}{ccc} X & \xrightarrow{\;g\;} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ X & \xrightarrow{\;g^\alpha\;} & X \end{array}$$

è commutativo, cioè $g^\alpha = f^{-1}gf = g^f$. Pertanto $\Delta = \Gamma^\alpha = \Gamma^f$ è un coniugato di Γ in $Sym\, X$. Viceversa, se $\Delta = \Gamma^f$ per un opportuno $f \in Sym\, X$, allora, detto α l'isomorfismo $g \mapsto g^f$ da Γ a Δ, è evidente che (α, f) determina un $\mathcal{RP}$-isomorfismo da Γ a Δ. ❑

Possiamo allora subito osservare che i due sottogruppi $\langle (1\,2) \rangle$ e $\langle (1\,2)(3\,4) \rangle$ di $\mathbb{S}_4$ sono isomorfi ma non simili tra loro.

Le similitudini conservano le proprietà delle azioni permutazionali definite sinora. Infatti:

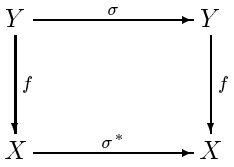
3.2. *Sia $(\rho, \varphi, \alpha, f)$ un $\mathcal{RP}$-morfismo dalla rappresentazione permutazionale $\rho : G \to Sym\, X$ a $\varphi : H \to Sym\, Y$. Allora, per ogni $x \in X$ e per ogni $g \in G$ si ha:*

$$\big(\mathrm{St}_\rho(x)\big)^\alpha \leq \mathrm{St}_\varphi(xf) \qquad \big(\mathrm{Orb}_\rho(x)\big)f \subseteq \mathrm{Orb}_\varphi(xf) \qquad \big(\mathrm{Fix}_\rho(g)\big)f \subseteq \mathrm{Fix}_\varphi(g^\alpha).$$

Se $(\rho, \varphi, \alpha, f)$ è un isomorfismo queste relazioni valgono con i segni di uguaglianza e si ha anche $\deg(\rho) = \deg(\varphi)$ e $\big(\mathrm{supp}_\rho(g)\big)f = \mathrm{supp}_\varphi(g^\alpha)$, *inoltre φ è transitiva (risp. semiregolare, regolare) se e solo se lo è ρ.*

Dimostrazione — Le dimostrazioni sono dirette; svolgiamo quella per gli stabilizzanti a titolo di esempio. Se $g \in \mathrm{St}_\rho(x)$, allora $xg^\rho = x$, quindi $xfg^{\alpha\varphi} = xg^\rho f = xf$ (abbiamo usato il fatto che $g^\rho f = fg^{\alpha\varphi}$), cioè $g^\alpha \in \mathrm{St}_\varphi(xf)$. Pertanto $\big(\mathrm{St}_\rho(x)\big)^\alpha \leq \mathrm{St}_\varphi(xf)$, come si voleva. Se poi $(\rho, \varphi, \alpha, f)$ è un isomorfismo, allora (α^{-1}, f^{-1}) determina un $\mathcal{RP}$-morfismo da φ a ρ ed otteniamo anche $\big(\mathrm{St}_\varphi(xf)\big)^{\alpha^{-1}} \leq \mathrm{St}_\rho((xf)f^{-1}) = \mathrm{St}_\rho(x)$, ovvero $\mathrm{St}_\varphi(xf) \leq \big(\mathrm{St}_\rho(x)\big)^\alpha$. Concludiamo quindi $\big(\mathrm{St}_\rho(x)\big)^\alpha = \mathrm{St}_\varphi(xf)$. ❑

3.3. Esempi. Se $f : Y \to X$ è un'applicazione iniettiva, ogni permutazione σ dell'insieme Y definisce, come già osservato in alcuni casi particolari, una permutazione σ^* di X che fissa ciascun elemento di $X \smallsetminus \mathrm{im}\, f$ e manda ogni $yf \in \mathrm{im}\, f$ in $y\sigma f$. Indicando con $\tilde{f}$ l'applicazione $\sigma \in Sym\, Y \mapsto \sigma^* \in Sym\, X$, si verifica agevolmente che $(\tilde{f}, f)$ determina un $\mathcal{RP}$-monomorfismo da $Sym\, Y$ a $Sym\, X$, in quanto il diagramma a destra è commutativo e sia f che $\tilde{f}$ sono iniettive. Se f è biettiva $(\tilde{f}, f)$ determina un $\mathcal{RP}$-isomorfismo. In particolare:



— se X e Y sono due insiemi equipotenti, allora $Sym\, X$ e $Sym\, Y$ sono simili (quindi anche isomorfi; vedi 7.7 per l'inverso).

— Se $Y \subseteq X$ ed f è l'immersione di Y in X, allora $\tilde{f}$ è il monomorfismo canonico $Sym\, Y \rightarrowtail Sym\, X$, quindi a quest'ultimo corrisponde un $\mathcal{RP}$-monomorfismo. Questa osservazione migliora l'enunciato 1.7 e giustifica il fatto che, talvolta, $Sym\, Y$ venga identificato con lo stabilizzante in $Sym\, X$ di $X \smallsetminus Y$, l'immagine di $\tilde{f}$.

— Similmente, se $Y \subseteq X$ e ρ è una rappresentazione permutazionale del gruppo G su X rispetto alla quale Y sia fissato, allora, ponendo ancora $f : Y \hookrightarrow X$ si verifica subito che l'identità di G e f determinano un $\mathcal{RP}$-monomorfismo dalla rappresentazione permutazionale di G indotta da ρ su Y a ρ. Un caso particolarmente importante è quello in cui Y è una ρ-orbita e quindi la rappresentazione indotta è la relativa componente transitiva di ρ.

— Se $\rho : G \to Sym\, X$ è una rappresentazione permutazionale e $H \leq G$, allora l'immersione di H in G e l'identità in X descrivono un $\mathcal{RP}$-monomorfismo da $\rho_{|H}$ a ρ.

— Dualmente, se $N = \ker \rho$, per il primo teorema di omomorfismo ρ determina una rappresentazione permutazionale $\bar{\rho} : G/N \to Sym\, X$; allora l'epimorfismo canonico $G \twoheadrightarrow G/N$ e l'identità in X descrivono un $\mathcal{RP}$-epimorfismo da ρ a $\bar{\rho}$.

Esercizi.

1. Completare la dimostrazione di 3.2.
2. Se $(\rho, \varphi, \alpha, f)$ è un $\mathcal{RP}$-morfismo, allora $\mathrm{im}\, f$ è φ-invariante.
3. Con le notazioni di 3.2 provare che:
   — $\big(\mathrm{Orb}_\rho(x)\big)f = \mathrm{Orb}_{G^{\alpha\varphi}}(xf)$ per ogni $x \in X$. Se f è suriettiva, ρ è transitiva e $X \neq \varnothing$, allora φ è transitiva; se α è suriettiva f manda ρ-orbite in φ-orbite.
   — $\big(\mathrm{supp}_\rho(g)\big)f \supseteq \mathrm{supp}_\varphi(g^\alpha) \cap \mathrm{im}\, f$ per ogni $g \in G$. Vale l'uguaglianza se f è iniettiva.
   — Sempre se f è iniettiva, vale $\big(\mathrm{St}_\rho(x)\big)^\alpha = \mathrm{St}_\varphi(xf) \cap \mathrm{im}\, \alpha$ per ogni $x \in X$.
   — Se f è biettiva, g^ρ e $g^{\alpha\varphi}$ hanno la stessa struttura ciclica, per ogni $g \in G$. In particolare, se g^ρ è finitaria anche $g^{\alpha\rho}$ è finitaria e della stessa parità di g^ρ.

   Cercare controesempi per le inclusioni non dimostrate in 3.2 o in questo esercizio.
4. Data una qualsiasi rappresentazione permutazionale ρ di un gruppo G, ad ogni elemento $g \in G$ possiamo associare l'$\mathcal{RP}$-isomorfismo $(\rho, \rho, \tilde{g}, g^\rho)$, dove $\tilde{g} : h \mapsto h^g$ è l'automorfismo interno di G determinato da g. Unitamente a 3.2 quest'osservazione permette di ritrovare alcuni tra gli enunciati precedenti (come 1.2 o l'esercizio 15 a p. 3).
5. Sia $\rho : G \to Sym\, X$ una rappresentazione permutazionale. Per ogni $x \in X$ indichiamo con ρ_x l'azione di $\mathrm{St}_\rho(x)$ indotta da ρ su $X \smallsetminus \{x\}$. Utilizzando l'esercizio precedente, verificare che se x e y sono elementi della stessa ρ-orbita, allora ρ_x e ρ_y sono simili.

Quando si è interessati a rappresentazioni permutazionali di un fissato gruppo G, è utile considerare la sottocategoria $\mathcal{RP}_G$ di $\mathcal{RP}$ costituita da:

— Oggetti: le rappresentazioni permutazionali di G;

— Morfismi: i morfismi di $\mathcal{RP}$ della forma (ρ, φ, id_G, f) dove id_G è l'applicazione identica in G (un tale morfismo si dice *determinato da* f).

Due rappresentazioni permutazionali $\rho : G \to Sym X$ e $\varphi : G \to Sym Y$ di G sono quindi $\mathcal{RP}_G$-isomorfe, o *equivalenti*, esattamente quando esiste un'applicazione biettiva $f : X \to Y$ tale che, per ogni $g \in G$ valga $g^\rho f = f g^\varphi$, cioè il diagramma

$$\begin{array}{ccc} X & \xrightarrow{g^\rho} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{g^\varphi} & Y \end{array}$$

sia commutativo. Lo studio degli $\mathcal{RP}$-morfismi è riconducibile a quello degli $\mathcal{RP}_G$-morfismi, nel senso che, con le notazioni usate per il diagramma $(*)$, è evidente che (α, f) determina un $\mathcal{RP}$-morfismo da ρ a φ se e solo se f determina un $\mathcal{RP}_G$-morfismo da ρ alla rappresentazione permutazionale $\alpha\varphi : G \to Sym Y$.

La categoria $\mathcal{RP}_G$ è in un certo senso analoga alla categoria dei moduli destri su un fissato anello. I morfismi in $\mathcal{RP}_G$ si possono infatti descrivere con il consueto linguaggio algebrico riferendosi alle azioni permutazionali (che sono, lo ricordiamo, particolari operazioni esterne).

3.4. *Siano ρ e φ due rappresentazioni permutazionali di un gruppo G, a valori rispettivamente in $Sym X$ e $Sym Y$. Indicate con $* : X \times G \to X$ e $\star : Y \times G \to Y$ le azioni permutazionali da esse definite, un'applicazione $f : X \to Y$ determina un $\mathcal{RP}_G$-morfismo (risp. $\mathcal{RP}_G$-isomorfismo) da ρ a φ se e solo se f è un morfismo (risp. isomorfismo) da $(X, *)$ a $(Y, \star)$.*

Dimostrazione — La condizione affinché f sia un morfismo da $(X, *)$ a $(Y, \star)$ è che valga $(x*g)f = xf \star g$ per ogni $x \in X$ e per ogni $g \in G$. Poiché $x * g = xg^\rho$ e $xf \star g = xfg^\varphi$, questa condizione equivale all'essere $g^\rho f = f g^\varphi$ per ogni $g \in G$, cioè al fatto che f determini un $\mathcal{RP}_G$-morfismo. Se la condizione è verificata, quest'ultimo è un $\mathcal{RP}_G$-isomorfismo se e solo se f è biettiva, quindi un isomorfismo. ❑

Quanto abbiamo visto nella sezione 2 suggerisce che, per molti scopi, lo studio delle rappresentazioni permutazionali di un fissato gruppo si riduca allo studio delle sue rappresentazioni transitive. Queste ultime, come visto, determinano la rappresentazione permutazionale che le definisce e, come anticipato, sono legate ad essa da una relazione che possiamo esprimere ora in linguaggio categoriale. Data la rappresentazione permutazionale $\rho : G \to Sym X$, per una delle osservazioni in 3.3, l'immersione di una ρ-orbita X_i in X determina un $\mathcal{RP}_G$-monomorfismo dalla corrispondente componente transitiva ρ_i di ρ in ρ stesso.

3.5. *Sia I una classe completa di rappresentanti delle orbite di una rappresentazione permutazionale ρ; per ogni $i \in I$ siano X_i la ρ-orbita cui appartiene i e ρ_i la relativa componente transitiva di ρ, e sia ι_i l'immersione $X_i \hookrightarrow X$. Allora ρ è il coprodotto nella categoria $\mathcal{RP}_G$ della famiglia $(\rho_i)_{i\in I}$, con immersioni $\big((\rho_i, \rho, id_G, \iota_i)\big)_{i\in I}$.*

Dimostrazione — Sappiamo che le $(\rho_i, \rho, id_G, \iota_i)$ sono $\mathcal{RP}_G$-morfismi (vedi 3.3). Dobbiamo provare che, data un rappresentazione permutazionale φ e, per ogni $i \in I$, un $\mathcal{RP}_G$-morfismo $(\rho_i, \varphi, id_G, f_i) : \rho_i \to \varphi$, esiste un unico $\mathcal{RP}_G$-morfismo $(\rho, \varphi, id_G, f) : \rho \to \varphi$ tale che $\iota_i f = f_i$ per ogni i. L'unicità è ovvia: f deve necessariamente essere l'applicazione definita in X per incollamento dalle f_i (cioè: per ogni $x \in X$ si ha $xf = xf_i$ dove i è l'unico elemento di I tale che $x \in X_i$). D'altra parte, avendo definito f in questo modo, è chiaro che $\iota_i f = f_i$ per ogni $i \in I$ e che (ρ, φ, id_G, f) è un $\mathcal{RP}_G$-morfismo. ❑

Una conseguenza di quest'ultimo risultato è il fatto, verificabile comunque direttamente senza difficoltà, che due rappresentazioni permutazionali di uno stesso gruppo che abbiano componenti transitive a due a due equivalenti sono tra loro equivalenti.

Quanto sopra ci spinge a concentrare la discussione sulle rappresentazioni permutazionali transitive. Tra i risultati elementari della teoria delle rappresentazioni permutazionali dei gruppi uno dei più fondamentali è che le rappresentazioni transitive di un fissato gruppo G su un insieme non vuoto si possono sempre identificare, a meno di equivalenze (cioè di $\mathcal{RP}_G$-isomorfismi), con le rappresentazioni sui laterali destri di un sottogruppo.

3.6. Teorema. *Sia ρ una rappresentazione permutazionale transitiva del gruppo G su un insieme X, e sia $x \in X$. Posto $H = \mathrm{St}_G(x)$, allora ρ è equivalente alla rappresentazione ρ_H di G sui laterali destri di H.*

Più precisamente, l'applicazione $f : Hg \mapsto xg^\rho$ di dominio l'insieme dei laterali destri di H in G e codominio X determina un $\mathcal{RP}_G$-isomorfismo da ρ_H a ρ.

Dimostrazione — L'applicazione f è ben definita e biettiva, come visto in 1.1. Resta da verificare $g^{\rho_H} f = f g^\rho$ per ogni $g \in G$. Per ogni laterale destro Ha di H in G si ha $(Ha)g^{\rho_H} f = (Hag)f = x(ag)^\rho = (xa^\rho)g^\rho = (Ha)fg^\rho$; l'asserto è così provato. ❑

3.7. Corollario. *Per ogni numero cardinale $\kappa > 0$, un gruppo G ha una rappresentazione permutazionale transitiva e fedele di grado κ se e solo se G ha un sottogruppo H di indice κ tale che $H_G = 1$.*

Dimostrazione — Se G ha sottogruppo H di indice κ tale che $H_G = 1$, allora l'azione di G sui laterali destri di H definisce una rappresentazione permutazionale transitiva che è anche fedele perché il suo nucleo è $H_G = 1$. Viceversa, se G opera in modo fedele e transitivo su un insieme X di cardinalità κ, detto H lo stabilizzante di un punto, l'azione di G su X è simile a quella di G sui laterali destri di H, per 3.6, dunque quest'ultima è fedele, vale a dire $H_G = 1$. ❑

Il Teorema 3.6 (unitamente a 3.2 ed enunciati simili) ci dice che per studiare proprietà di arbitrarie azioni transitive è sempre possibile ridursi al caso delle azioni su laterali destri di sottogruppi. Naturalmente la sua importanza è ulteriormente accresciuta dalle considerazioni svolte sopra, che indicano come le rappresentazioni transitive di un gruppo essenzialmente ne descrivano tutte le rappresentazioni permutazionali.

Vediamo un'altra utile conseguenza del Teorema 3.6. Come già osservato, da 1.2 segue che ogni azione transitiva individua una classe di coniugio di sottogruppi di G, gli stabilizzanti dei punti. Ebbene, questa classe di coniugio caratterizza le classi di equivalenza delle rappresentazioni transitive di un fissato gruppo.

3.8. Proposizione. *Siano ρ e φ due rappresentazioni transitive di un gruppo G su insiemi non vuoti X e Y, rispettivamente. Sono allora equivalenti le asserzioni:*

(*a*) *ρ e φ sono rappresentazioni equivalenti;*

(*b*) *esistono $x \in X$ e $y \in Y$ tali che $\mathrm{St}_\rho(x) = \mathrm{St}_\varphi(y)$;*

(*c*) *la classe di coniugio degli stabilizzanti dei punti di X rispetto a ρ coincide con quella degli stabilizzanti dei punti di Y rispetto a φ.*

Dimostrazione — (*a*) $\Rightarrow$ (*b*): Se f determina un $\mathcal{RP}_G$-isomorfismo da ρ a φ, scelto comunque $x \in X$ e posto $y = xf$, si ha $\mathrm{St}_\rho(x) = \mathrm{St}_\varphi(y)$ per 3.2.

Che (*b*) implichi (*c*) è ovvio.

(*c*) $\Rightarrow$ (*a*): Siano $x \in X$ e $y \in Y$. Allora, per un opportuno $g \in G$, si ha $\mathrm{St}_\rho(x) = \big(\mathrm{St}_\varphi(y)\big)^g = \mathrm{St}_\varphi(yg)$. Dunque vale (*b*), e quindi 3.6 implica che sia ρ che φ sono equivalenti alla rappresentazione di G sui laterali destri di $\mathrm{St}_\rho(x)$, in particolare esse sono equivalenti tra loro. ❑

Ad esempio, *ogni rappresentazione permutazionale regolare di G è equivalente alla rappresentazione regolare destra.*

Riassumendo: possiamo descrivere ogni rappresentazione permutazionale di un gruppo G, a meno di equivalenze, come somma disgiunta (ovvero coprodotto in $\mathcal{RP}_G$) di rappresentazioni permutazionali transitive; queste ultime sono determinate (sempre a meno di equivalenze) dalla classe di coniugio degli stabilizzanti dei punti. Ad esempio, la rappresentazione permutazionale di $\mathbb{R}$ descritta nell'esempio a pagina 9 è, a meno di equivalenze, la somma disgiunta di un insieme numerabile di copie della rappresentazione regolare destra di $(\mathbb{R}, +)$.

Esercizio. Determinare, prima a meno di equivalenze, poi a meno di similitudini, tutte le rappresentazioni permutazionali fedeli di grado 4 del gruppo quadrinomio V_4. Tra esse identificare quelle simili alle rappresentazioni di V_4 sull'insieme dei vertici di un rettangolo o di un rombo non quadrati presentati a pagina 6.

Esercizi. Per chi è interessato ad una descrizione più dettagliata delle categorie $\mathcal{RP}$ e $\mathcal{RP}_G$.

1. Sia $(\rho_i)_{i\in I}$ un'arbitraria famiglia di rappresentazioni permutazionali del gruppo G. Si può costruire il coprodotto di questa famiglia in $\mathcal{RP}_G$ come segue. Per ogni $i \in I$ sia X_i l'insieme su cui agisce G tramite ρ_i, cioè supponiamo $\rho_i : G \to Sym\, X_i$; sia poi $\bar{X}_i = \{i\} \times X_i$. Per ogni $i \in I$, l'azione di G su $\bar{X}_i$ definita da $(i, x) * g = (i, xg^{\rho_i})$ dà luogo ad una rappresentazione permutazionale $\bar{\rho}_i$, evidentemente equivalente a ρ_i. Essendo gli insiemi $\bar{X}_i$ a due a due disgiunti, partendo appunto dalle rappresentazioni $\bar{\rho}_i$ possiamo definire per incollamento una rappresentazione permutazionale ρ di G su $X := \bigcup_{i\in I} \bar{X}_i$ le cui componenti transitive sono quelle delle $\bar{\rho}_i$. Da 3.5 segue che ρ è il coprodotto delle $\bar{\rho}_i$ e quindi delle ρ_i.
2. Per ogni gruppo G è possibile immergere la categoria Set degli insiemi in $\mathcal{RP}_G$. Infatti Set è isomorfa alla sottocategoria piena di $\mathcal{RP}_G$ costituita dalle rappresentazioni permutazionali di G che sono omomorfismi nulli.
3. Si può anche immergere la categoria Grp dei gruppi in $\mathcal{RP}$. Infatti Grp è isomorfa alla sottocategoria piena di $\mathcal{RP}$ costituita da rappresentazioni permutazionali di gruppi sull'insieme vuoto.
4. Un morfismo in $\mathcal{RP}$ è epi (risp. mono) se e solo se le sue due ultime componenti sono entrambe suriettive (risp. iniettive). Descrizione analoga si ha per gli epi- (risp. mono-) morfismi in $\mathcal{RP}_G$, per ogni gruppo G.

4. Transitività multipla

Sia $\rho : G \longrightarrow Sym\, X$ una rappresentazione permutazionale. Per ogni intero positivo k si definisce una rappresentazione $\rho_{[k]} : G \longrightarrow Sym\, X^{[k]}$, dove $X^{[k]}$ è l'insieme delle k-uple di elementi distinti di X, ponendo $(x_1, \dots, x_k)g^{\rho_{[k]}} = (x_1 g^\rho, \dots, x_k g^\rho)$ per ogni $g \in G$ e $(x_1, \dots, x_k) \in X^{[k]}$. Si dice che ρ è *k-transitiva* se e solo se $k \leq \deg\rho = |X|$ e $\rho_{[k]}$ è transitiva (qui la limitazione $k \leq |X|$ serve ad escludere il caso banale in cui $X^{[k]}$ è vuoto). In termini più espliciti, ρ è k-transitiva quando X contiene almeno k punti distinti x_1, $x_2, \dots, x_k$ e, scelti comunque k punti di X tra loro distinti y_1, $y_2, \dots, y_k$, esiste $g \in G$ tale che $x_i g^\rho = y_i$ per ogni $i \in \{1, \dots, k\}$. Ad esempio, il gruppo simmetrico su X è k-transitivo per ogni intero positivo $k \leq |X|$. Invece il gruppo alterno $\mathbb{A}_3$ non è 2-transitivo, perché non esiste in $\mathbb{A}_3$ alcuna permutazione che mandi 1 in 1 e 2 in 3, sicché la condizione di 2-transitività fallisce per le coppie $(x_1, x_2) = (1, 2)$ e $(y_1, y_2) = (1, 3)$. Dalla seconda formulazione della definizione segue subito che *se ρ è k-transitiva allora ρ è anche k'-transitiva per ogni intero positivo k' minore di k*. Inoltre, escluso il caso che X sia l'insieme vuoto, la proprietà di 1-transitività coincide con la transitività, quindi, per ogni intero $k > 1$, la proprietà di essere una rappresentazione permutazionale k-transitiva è un più forte della proprietà di essere transitiva, ed è tanto più forte quanto maggiore è k. Se ρ è k-transitiva per ogni $k \in \mathbb{N}$, si dice che ρ è *altamente transitiva*. Ovviamente, affinché ciò accada è necessario che X sia infinito. Facili esempi di gruppi altamente transitivi sono il gruppo finitario ed il gruppo alterno su un insieme infinito. Osserviamo anche che una rappresentazione permutazionale ρ è k-transitiva (o altamente transitiva) se e solo se lo è $\operatorname{im}\rho$.

Con le notazioni di sopra, si dice poi che ρ è *strettamente k-transitiva* se e solo se $k \leq \deg\rho$ e $\rho_{[k]}$ è regolare.[♯] Quindi ρ è strettamente 1-transitiva precisamente quando è regolare. Possiamo anche dire che ρ è strettamente k-transitiva esattamente quando è k-transitiva e, scelti comunque elementi x_i e y_i come sopra, è unico l'elemento $g \in G$ tale che $y_i = x_i g^\rho$ per ogni indice i. Ad esempio, $\mathbb{S}_4$ è strettamente 4-transitivo, ma non strettamente 2-transitivo (sia (1 2 3) che (1 2 3 4) mandano 1 in 2 e 2 in 3). Questo esempio mostra che, a differenza di quanto osservato per la molteplice transitività (cioè k-transitività per un imprecisato $k > 1$), la proprietà di essere strettamente k-transitivo non implica la k'-transitività per interi positivi $k' < k$. La situazione è chiarita completamente da questa osservazione:

4.1. *Siano k un intero positivo e $\rho : G \longrightarrow Sym\, X$ una rappresentazione permutazionale k-transitiva. Se (X e) G sono finiti, posto $n = |X|$ si ha:*
(i) $n!/(n-k)! = n(n-1)\cdots(n-k+1)$ *divide* $|G|$;
(ii) $n!/(n-k)! = |G|$ *se e solo se ρ è strettamente k-transitiva.*

Dimostrazione — L'asserto segue direttamente da 1.1 (*vi*), una volta osservato che $\left|X^{[k]}\right| = n!/(n-k)!$. ❑

Di conseguenza è possibile che ρ sia k- e, contemporaneamente, k'-transitiva per un qualche $k' < k$ soltanto nel caso in cui $k = n = \deg\rho$ e $k' = n - 1$; come è chiaro, ciò non accade mai se ρ ha grado infinito. Ciò implica che non esistono rappresentazioni permutazionali 'altamente strettamente transitive', in un senso analogo alla definizione data sopra di alta transitività.

Va infine osservato che, per ogni intero positivo k, ogni rappresentazione permutazionale strettamente k-transitiva è necessariamente fedele. Unitamente al fatto che una rappresentazione permutazionale ρ è k-transitiva (o altamente transitiva) se e solo se lo è $\operatorname{im}\rho$, questo vuol dire che la teoria delle rappresentazioni strettamente k-transitive si riduce allo studio dei gruppi strettamente k-transitivi di permutazioni.

Molto spesso la maniera più semplice di provare che una rappresentazione permutazionale è (strettamente) k-transitiva per qualche k è utilizzare questo lemma, particolarmente utile per ragionamenti induttivi (cfr. anche esercizio 5, p. 14):

4.2. *Sia ρ una rappresentazione permutazionale transitiva su un insieme non vuoto X. Sia k un intero maggiore di* 1 *e sia G_x lo stabilizzante di un punto $x \in X$. Allora ρ è k-transitiva (risp. strettamente transitiva) se e solo se l'azione di G_x su $X \setminus \{x\}$ è $(k-1)$-transitiva (risp. strettamente transitiva).*

Dimostrazione — La dimostrazione è svolta in [Rob], 7.1.1, per la transitività. La dimostrazione per la stretta transitività si ottiene aggiungendo l'osservazione che, posto $Y = X \setminus \{x\}$, lo stabilizzante di un elemento $a = (x_1, \dots, x_{k-1})$ di $Y^{[k-1]}$ rispetto all'azione di G_x coincide con lo stabilizzante rispetto a $\rho_{[k]}$ di un elemento di $X^{[k]}$, avendosi $\mathrm{St}_{G^x}(a) = \mathrm{St}_\rho\big(\{x_1, \dots, x_{k-1}, x\}\big) = \mathrm{St}_{\rho_{[k]}}\big((x_1, \dots, x_{k-1}, x)\big)$. ❑

Più generalmente, se G opera in modo (strettamente) k-transitivo su un insieme X e Y è una parte di X di ordine $m < k$, allora $\mathrm{St}_G(Y)$ opera in modo (strettamente) $(k-m)$-transitivo su $X \setminus Y$. Ovviamente, per ciascun $m \leq k$ gli stabilizzanti delle parti di X di ordine m costituiscono una classe di coniugio in G.

Sin dall'inizio della teoria dei gruppi di permutazione molta attenzione è stata rivolta alla determinazione di gruppi 'molte volte' transitivi. Gli esempi più ovvi sono i gruppi simmetrici (come già osservato) e quelli alterni.

[♯] Piuttosto che 'strettamente transitiva' è molto usata l'espressione 'sottilmente transitiva'. Sia 'strettamente transitiva' che 'sottilmente transitiva' traducono l'inglese 'sharply transitive'.

4.3. *Sia X un insieme finito di ordine $n > 2$. Allora $Sym\,X$ e $Alt X$ sono gli unici sottogruppi $(n-2)$-transitivi di $Sym\,X$. Inoltre $Sym\,X$ è strettamente n- e $(n-1)$-transitivo, $Alt X$ è strettamente $(n-2)$-transitivo.*

Dimostrazione — Per 4.1 ogni sottogruppo $(n-2)$-transitivo Γ di $Sym\,X$ ha ordine maggiore o uguale a $n!/2$, quindi o $\Gamma = Alt X$ o $\Gamma = Sym\,X$.[♮] È ovvio (e lo abbiamo anche già osservato) che $Sym\,X$ è n- e quindi anche $(n-1)$-transitivo. Per 4.1 (ii) sia la n- che la $(n-1)$-transitività sono strette. Per provare la stretta $(n-2)$-transitività di $Alt X$ si può procedere in almeno due modi, entrambi molto semplici. Uno è quello di ragionare per induzione su $|X|$, osservando che il gruppo alterno su tre oggetti è regolare (cioè strettamente 1-transitivo) e utilizzando poi 4.2 (vedi [Rob], 7.1.4 (ii)). Un altro modo è questo: se $(x_1, \dots, x_{n-2})$ e $(y_1, \dots, y_{n-2})$ sono due $(n-2)$-uple di elementi distinti di X, esiste $g \in Sym\,X$ tale che $y_i = x_i g$ per ogni $i \in \{1, \dots, n-2\}$. Se t è la trasposizione che scambia tra loro i due elementi di $X \setminus \{x_1, \dots, x_{n-2}\}$, allora anche tg ha la stessa proprietà di g (quella di mandare ciascun x_i in y_i), e uno tra g e tg appartiene a $Alt X$. Quindi $Alt X$ è $(n-2)$-transitivo. Da 4.1 segue che $Alt X$ è strettamente $(n-2)$-transitivo. ❑

Esempio. Ritorniamo sull'esempio delle colorazioni delle facce di un tetraedro discusso in 1.13. Con le notazioni lì utilizzate, si era osservato che:

(i) con due colori a disposizione, due colorazioni f e f' sono indistinguibili se e solo se ogni colore appare sullo stesso numero di facce in f ed in f';

(ii) $N_k = N_k^*$ se $k \leq 3$.

Entrambe queste circostanze si possono facilmente giustificare utilizzando le nozioni introdotte in questa sezione. La prima dipende dalla 4-transitività dell'azione del gruppo Γ delle isometrie del tetraedro sull'insieme $\mathcal{F}$ delle sue facce e non dipende dal fatto di avere a disposizione due soli colori. Infatti, qualsiasi sia il numero k dei colori a disposizione, siano date due colorazioni f e f' del tetraedro tali che ciascun colore appaia lo stesso numero di volte nella colorazione f e nella colorazione f'. Questa condizione assicura che possiamo scrivere i quattro elementi di $\mathcal{F}$ come x_1, x_2, x_3, x_4 e anche, riordinandoli, come y_1, y_2, y_3, y_4 in modo che $x_i f = y_i f'$ per ogni $i \in \{1, 2, 3, 4\}$. Per la 4-transitività di Γ, esiste $\gamma \in \Gamma$ tale che $x_i \gamma = y_i$ per ogni i. Allora $f * \gamma = f'$; infatti $y_i(f * \gamma) = y_i \gamma^{-1} f = x_i f = y_i f'$ per ogni i. Pertanto f e f' sono indistinguibili rispetto all'azione di Γ. Questo spiega (i). Per giustificare (ii), lasciando f, f' e le facce x_i e y_i scelte come sopra, sia $k \leq 3$. Almeno due facce, possiamo supporre che siano x_1 e x_2, hanno lo stesso colore rispetto alla colorazione f. Poiché l'azione di Γ^+ su $\mathcal{F}$ è 2-transitiva, in quanto simile a quella naturale di $\mathbb{A}_4$, esiste $\gamma \in \Gamma^+$ tale che $x_3 \gamma = y_3$ e $x_4 \gamma = y_4$. Da una verifica analoga alla precedente si ricava $f * \gamma = f'$, dunque, se $k \leq 3$, due colorazioni indistinguibili rispetto all'azione di Γ lo sono anche rispetto all'azione di Γ^+, il che spiega (ii).

Come evidenziato da 4.2, gli stabilizzanti dei punti forniscono informazioni essenziali per la descrizione delle rappresentazioni permutazionali transitive. La nozione di rango è per questo di uso molto frequente. Il *rango* di una rappresentazione permutazionale transitiva su un insieme non vuoto è, per definizione, il numero di orbite dello stabilizzante di un punto. Per 1.2 (o, più precisamente, per l'esercizio 4 di p. 14) il rango è indipendente dalla scelta del punto di cui consideriamo lo stabilizzante. Le rappresentazioni permutazionali (transitive) di rango 1 sono precisamente quelle sui singletons; quelle di rango 2 sono invece, per 4.2, le 2-transitive.

4.4. *Sia $\rho : G \longrightarrow Sym\,X$ una rappresentazione permutazionale transitiva. Se G è finito e $X \neq \varnothing$, il rango di ρ è $\frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_\rho(g)|^2$.*

Dimostrazione — Come l'enunciato, anche la dimostrazione ricorda da vicino quella di 1.5. Si consideri infatti l'insieme $S = \{(x, y, g) \mid g \in G \wedge x, y \in \operatorname{Fix}(g)\}$. Per ogni $g \in G$ l'insieme degli elementi di S di terza coordinata g è $\operatorname{Fix}(g) \times \operatorname{Fix}(g) \times \{g\}$, quindi $|S| = \sum_{g \in G} |\operatorname{Fix}(g)|^2$. Sia r il rango di ρ. Per ogni $x \in X$ l'insieme degli elementi di S di prima coordinata x è equipotente a $S'_x = \{(y, g) \in X \times G_x \mid yg = g\}$, dove $G_x = \operatorname{St}_G(x)$. La cardinalità di S'_x è stata calcolata nel corso della dimostrazione di 1.5: poiché r è il numero delle G_x-orbite in X si ha $|S'_x| = r|G_x| = r|G| \,/\, |X|$. Allora

$$|S| = \sum_{x \in X} |S'_x| = \sum_{x \in X} \frac{r|G|}{|X|} = r|G|.$$

Confrontando con l'uguaglianza $|S| = \sum_{g \in G} |\operatorname{Fix}(g)|^2$ ottenuta sopra si arriva alla conclusione. ❑

[♮] $Alt X$ è l'unico sottogruppo di indice 2 in $Sym\,X$. Questo fatto segue subito dalla semplicità dei gruppi alterni di grado maggiore di 4 (Teorema 7.3), che non abbiamo però ancora provato. Non volendo fare riferimento a questo teorema si può ottenere la stessa conclusione come conseguenza di 2.6. Sia infatti H un sottogruppo di indice 2 in $Sym\,X$. Allora $H \lhd Sym\,X$ e ad H appartiene il quadrato di ogni elemento di $Sym\,X$; in particolare, se t è un 3-ciclo, $t^{-1} = t^2 \in H$, quindi $t \in H$. Allora $Alt X \leq H$ per 2.6. Poiché X è finito di ordine maggiore di 1, anche $Alt X$ ha indice 2 in $Sym\,X$, quindi $H = Alt X$.

4.5. Corollario. *Con le stesse notazioni, ρ è 2-transitiva se e solo se* $\frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix}(g)|^2 = 2$.

Va evidenziato che mentre, per il teorema di Cayley, ogni gruppo può essere rappresentato fedelmente come (vale a dire: è isomorfo a) un gruppo regolare di permutazioni, quindi niente può essere detto in generale sulla struttura (gruppale) di un gruppo transitivo o, appunto, regolare, lo stesso non accade per le proprietà di transitività multipla. Ad esempio, 4.1 implica che un gruppo finito G di ordine dispari non ha alcuna rappresentazione fedele 2-transitiva. Infatti, se n fosse il grado di una tale rappresentazione, $|G|$ dovrebbe essere divisibile per $n(n-1)$, ma questo è un numero pari.

Teoremi di classificazione per gruppi di permutazione k-transitivi o k-strettamente transitivi per $k \geq 2$ verranno discussi nella sezione 6. È un fatto notevole, e per niente elementare, che non esistono gruppi finiti 6-transitivi a parte i gruppi alterni e simmetrici.

Esercizi.

1. Per ogni $n \in \mathbb{N}$ il gruppo delle isometrie di $\mathbb{R}^n$ è transitivo ma non 2-transitivo.
2. Il gruppo degli omeomorfismi di $\mathbb{R}$ dotato della topologia usuale è 2-transitivo ma non 3-transitivo. Il gruppo degli omeomorfismi di $\mathbb{Q}$ è invece altamente transitivo.
3. Sia definita un'azione transitiva del gruppo G e sia H lo stabilizzante di un punto. Utilizzando 3.6 dimostrare che l'azione di G è 2-transitiva se e solo se esiste $g \in G$ tale che $G \smallsetminus H = HgH$ e che, in questo caso, ciò accade per ogni $g \in G \smallsetminus H$.
4. Siano X un insieme di cardinalità finita n e ρ un'azione permutazionale k-transitiva del gruppo G su X, dove k è un intero positivo minore o uguale a n. Per ogni intero non negativo $i \leq n$ sia P_i l'insieme delle parti di X di cardinalità i. Se $i \leq k$, verificare che sia P_i che P_{n-i} sono orbite rispetto all'azione di G su $\mathcal{P}(X)$ indotta da ρ.

5. Rappresentazioni primitive

È stato visto come ogni rappresentazione permutazionale si decomponga nelle sue componenti transitive. In questo senso le rappresentazioni permutazionali transitive si possono considerare come costituenti elementari tramite le quali si possono descrivere tutte le rappresentazioni permutazionali. Di fatto è possibile definire una classe di rappresentazioni transitive più 'elementari' delle altre: le rappresentazioni primitive.

Si perviene in modo rapido a definire la primitività considerando, dal punto di vista strettamente algebrico, le azioni destre. Sia $* : X \times G \to X$ un'azione permutazionale. Allora, conformemente al linguaggio usato per ogni struttura algebrica, una *$*$-congruenza* è una relazione di equivalenza $\sim$ in X compatibile con l'operazione $*$, cioè tale che

$$\forall g \in G,\ \forall x, y \in X, \qquad \big(x \sim y \Longrightarrow xg \sim yg\big)$$

(continuiamo a scrivere xg e yg per $x * g$ e $y * g$). L'importanza delle congruenze consiste nel fatto che esse sono precisamente le relazioni di equivalenza che permettono di definire in modo naturale un'azione sul quoziente.

5.1. *Sia $*$ un'azione permutazionale del gruppo G sull'insieme X e sia $\sim$ una $*$-congruenza. Per ogni $x \in X$ indichiamo con $[x]$ la $\sim$-classe di equivalenza a cui appartiene x. Allora la posizione $[x]g = [xg]$, per ogni $x \in X$ e $g \in G$, definsce un'azione permutazionale di G su $X/\sim$. Se $*$ è transitiva, anche l'azione così ottenuta è transitiva.*

Dimostrazione — Si tratta di innanzitutto di verificare che l'applicazione $\big([x], g\big) \in (X/\sim) \times G \longmapsto [xg] \in X/\sim$ è ben definita, cioè che, scelti comunque $g \in G$ e x, y elementi di X tali che $[x] = [y]$ (ovvero $x \sim y$), si ha $[xg] = [yg]$. Ciò è immediata conseguenza della definizione di congruenza. È poi chiaro che $[x]1 = [x1] = [x]$ e $([x]g)h = [xgh] = [x](gh)$ per ogni $x \in X$ e $g, h \in G$, dunque l'applicazione considerata effettivamente è un'azione permutazionale. Infine, supponiamo che $*$ sia transitiva. Se $[x]$ e $[y]$ sono elementi di $X/\sim$, esiste $g \in G$ tale che $y = xg$. Allora $[y] = [x]g$. Ciò prova che l'azione di G su $X/\sim$ è transitiva. ❑

Sono ovvi esempi di congruenze la relazione di uguaglianza e la relazione totale in X, che chiamiamo congruenze banali. Una rappresentazione permutazionale transitiva si dice *primitiva* se e solo se quelle banali sono le uniche congruenze da essa ammesse (le congruenze di una rappresentazione permutazionale sono le congruenze relative all'azione permutazionale ad essa associata). È chiaro che le congruenze rispetto ad una rappresentazione permutazionale ρ sono precisamente le congruenze rispetto a $\operatorname{im}\rho$, quindi ρ è primitiva se e solo se lo è $\operatorname{im}\rho$. Va evidenziato che la nozione di primitività viene definita esclusivamente per rappresentazioni transitive.

I sottogruppi normali determinano congruenze. Infatti:

5.2. *Sia fissata un'azione permutazionale $*$ del gruppo G sull'insieme X, e sia $N \lhd G$. Allora la relazione $\sim_N$ di N-equivalenza è una $*$-congruenza.*

Dimostrazione — Sia $x \sim_N y$, cioè esista $a \in N$ tale che $y = xa$. Allora, per ogni $g \in G$, si ha $yg = xag = (xg)a^{g^{-1}}$ e dunque $xg \sim_N yg$, dal momento che $a^{g^{-1}} \in N$. ❑

Le congruenze banali sono determinate dai sottogruppi (normali) banali di G. Infatti, se $N = G$, allora $\sim_N$ è la relazione totale in X, se $N = 1$, allora $\sim_N$ è la relazione di uguaglianza in X.

Un'importante conseguenza di 5.2 è:

5.3. *Se il gruppo G opera in modo fedele e primitivo su un insieme X, ogni sottogruppo normale non identico di G è transitivo.*

Dimostrazione — Sia $N \lhd G$. Per 5.2 la relazione $\sim_N$ è una congruenza. Poiché G è primitivo, allora $\sim_N$ è o la relazione totale o la relazione di uguaglianza in X. Nel primo caso N è transitivo. Nel secondo caso N fissa ogni elemento di X, quindi $N = 1$. ❑

Un'altra dimostrazione di 5.3 sarà ottenuta più avanti.

Si può definire in modo equivalente la nozione di primitività a partire da quella di *blocco di imprimitività*. Sia data una rappresentazione permutazionale transitiva del gruppo G sull'insieme X e sia Y una parte non vuota di X. Si dice che Y è un *blocco di imprimitività* (rispetto all'azione di G specificata) se e solo se, per ogni $g \in G$, si ha o $Yg = Y$ o $Yg \cap Y = \varnothing$. Si usa chiamare *traslati* di Y gli insiemi della forma Yg con $g \in G$; dunque Y è un blocco di imprimitività se e solo se è disgiunto da ogni suo traslato distinto da se stesso. Ad esempio, sono ovvi blocchi di imprimitività i singletons degli elementi di X e X stesso (se non vuoto). Questi vengono detti blocchi banali.

5.4. *Supponiamo che il gruppo agisca in modo transitivo su X. Una parte Y di X è un blocco di imprimitività rispetto all'azione di G se e solo se $\{Yg \mid g \in G\}$ è una partizione di X.*

Dimostrazione — Se $\{Yg \mid g \in G\}$ è una partizione di X e $g \in G$, allora Yg è o uguale a Y o disgiunto da Y, quindi Y è un blocco di imprimitività. Viceversa, se Y è un blocco di imprimitività allora $\{Yg \mid g \in G\}$ è una partizione. Infatti, poiché G è transitivo e Y non è vuoto, $\bigcup_{g\in G} Yg = \{yg \mid y \in Y \wedge g \in G\} = X$; inoltre, se $g, h \in G$, si ha $Yg \neq \varnothing$ (altrimenti $Y = (Yg)g^{-1} = \varnothing$) e, se $Yg \neq Yh$, allora $Y = (Yg)g^{-1} \neq Yhg^{-1}$, sicché per ipotesi $Y \cap Yhg^{-1} = \varnothing$ e quindi $Yg \cap Yh = (Y \cap Yhg^{-1})g = \varnothing g = \varnothing$. ❑

Verifichiamo ora che i blocchi di imprimitività sono tutte e sole le classi di equivalenza modulo congruenze. Se Y è un blocco di imprimitività, chiameremo *sistema di imprimitività* determinato da Y la partizione $\mathcal{S}(Y) = \{Yg \mid g \in G\}$ (che è l'orbita di Y rispetto all'azione di G su $\mathcal{P}(X)$ indotta da quella di G su X). Come ogni partizione, $\mathcal{S}(Y)$ definisce una relazione di equivalenza $\overset{Y}{\sim}$ in X: due elementi di X sono equivalenti modulo $\overset{Y}{\sim}$ se e solo se appartengono allo stesso elemento di $\mathcal{S}(Y)$, cioè allo stesso traslato di Y. Le relazioni di equivalenza così definite partendo da blocchi di imprimitività sono tutte e sole le congruenze in X:

5.5. *Sia fissata un'azione permutazionale transitiva del gruppo G sull'insieme X. Allora:*

(*i*) *se Y è un blocco di imprimitività $\overset{Y}{\sim}$ è una congruenza, non banale se e solo se Y è un blocco non banale;*

(*ii*) *viceversa, se $\sim$ è una congruenza ogni elemento Y di $X/\sim$ è un blocco di imprimitività tale che $\overset{Y}{\sim} = \sim$, ovvero $\mathcal{S}(Y) = X/\sim$.*

Pertanto l'azione di G su X è primitiva se e solo se gli unici blocchi di imprimitività in X sono quelli banali.

Dimostrazione — (*i*) Verifichiamo che $\overset{Y}{\sim}$ è una congruenza. Se $x \overset{Y}{\sim} y$, esiste $h \in G$ tale che $x, y \in Yh$. Allora per ogni $g \in G$ si avrà $xg, yg \in Yhg$ e quindi $xg \overset{Y}{\sim} yg$. Risulta poi chiaro che $\overset{Y}{\sim}$ è la relazione di uguaglianza (risp. la relazione totale) se e solo se $\mathcal{S}(Y)$ è l'insieme dei singletons degli elementi di X (risp. $\mathcal{S}(Y) = \{X\}$), cioè se e solo se Y è un singleton (risp. $Y = X$). Ciò prova (*i*).

(*ii*) Questa affermazione è una riformulazione di 5.1. Infatti 5.1 assicura che, se $Y = [x] \in X/\sim$, allora l'insieme dei traslati di Y è $\{Yg \mid g \in G\} = \{[xg] \mid g \in G\} = X/\sim$, una partizione, quindi Y è un blocco di imprimitività per 5.4 e $X/\sim = \mathcal{S}(Y)$, vale a dire $\sim = \overset{Y}{\sim}$. ❑

L'enunciato appena provato definisce implicitamente un'applicazione biettiva tra l'insieme delle congruenze in X a quello dei sistemi di imprimitività di X (rispetto, ovviamente, all'azione fissata). In effetti questi due insiemi costituiscono due sottoreticoli del reticolo delle equivalenze in X e del reticolo delle partizioni di X rispettivamente. Una volta osservato ciò, si può rendere più preciso l'enunciato di 5.5: *fissata un'azione permutazionale su X, l'isomorfismo canonico tra il reticolo delle equivalenze e quello delle partizioni di X induce un isomorfismo tra i reticoli delle congruenze e quello dei blocchi di imprimitività di X.*

Condizioni di primitività

Se il gruppo G agisce sull'insieme finito X e Y è un blocco di imprimitività, allora $\deg G = |X| = |\mathcal{S}(Y)| \cdot |Y|$, perché tutti gli elementi di $|\mathcal{S}(Y)|$ hanno ordine $|Y|$. Quindi $|Y|$ è un blocco non banale se e solo se $|Y|$ è un divisore proprio di $|X|$. In particolare:

5.6. *Ogni rappresentazione permutazionale transitiva di grado primo è primitiva.*

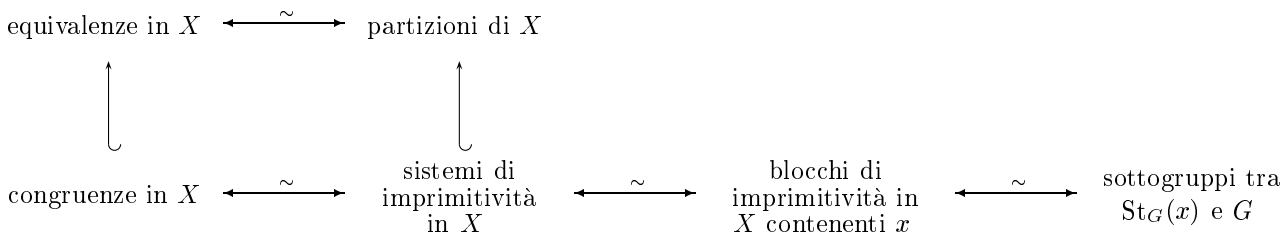
Sono poi banalmente primitive le rappresentazioni permutazionali di grado al più 1. Un'altra condizione sufficiente per la primitività è:

5.7. *Ogni rappresentazione permutazionale 2-transitiva è primitiva.*

Dimostrazione — Il gruppo G agisca in modo 2-transitivo su un insieme X e, per assurdo, sia Y un blocco di imprimitività non banale in X. Allora Y possiede almeno due elementi distinti x e y, ed esiste $z \in X \setminus Y$, perché $Y \neq X$. Poiché l'azione è 2-transitiva, esiste $g \in \mathrm{St}_G(x)$ tale che $yg = z$. Allora $x = xg \in Y \cap Yg \neq \varnothing$ e $Yg \neq Y$ perché $z \in Yg$, contraddicendo la definizione di blocco di imprimitività. ❑

Come visto in 3.8, le rappresentazioni permutazionali transitive di un gruppo G sono determinate (a meno di equivalenze) dalla classe di coniugio degli stabilizzanti dei punti. Ha senso dunque cercare di caratterizzare le rappresentazioni primitive (tra quelle transitive) in termini degli stessi stabilizzanti.

In effetti si ottiene facilmente un risultato ancora più preciso: una descrizione completa dei blocchi di imprimitività di una arbitraria rappresentazione transitiva. Tralasciamo il caso, ovvio, delle rappresentazioni sull'insieme vuoto. Se G opera in modo transitivo su X e $x \in X$, indichiamo con $\mathcal{B}$ l'insieme dei blocchi di imprimitività in X a cui appartiene x. Una volta noti tutti gli elementi di $\mathcal{B}$ sono noti tutti blocchi di imprimitività in X, perché ciascuno di essi è un traslato di un blocco al quale appartiene x (infatti se Y è un blocco qualsiasi, allora x apparterrà ad un elemento $Y' = Yg$ della partizione $\delta(Y)$ e $Y = Y'g^{-1}$). In altri termini, l'applicazione che ad un elemento di $\mathcal{B}$ associa il sistema di imprimitività da esso determinato è biettiva. È anche evidente che $\mathcal{B}$ è chiuso per intersezioni, quindi, ordinato per inclusione, costituisce un reticolo. L'applicazione appena considerata è di fatto un isomorfismo di reticoli tra $\mathcal{B}$ e il reticolo dei sistemi di imprimitività di X. Quindi sia quest'ultimo reticolo che quello delle congruenze in X sono reticoli isomorfi a $\mathcal{B}$. Ciò che è più interessante è questi reticoli sono isomorfi all'intervallo $\{K \leq G \mid \mathrm{St}_G(x) \leq K\}$ del reticolo dei sottogruppi di G, come stabilito nella prossima proposizione; abbiamo quindi un diagramma commutativo tra reticoli:



5.8. Proposizione. *Sia definita un'azione permutazionale transitiva del gruppo G sull'insieme non vuoto X. Siano $x \in X$ e $H = \mathrm{St}_G(x)$. Siano poi $\mathcal{L}$ l'insieme dei sottogruppi di G contenenti H e $\mathcal{B}$ l'insieme dei blocchi di imprimitività in X a cui appartiene x. Allora $K \mapsto \mathrm{Orb}_K(x)$ definisce un isomorfismo di reticoli da $\mathcal{L}$ ad $\mathcal{B}$ di inverso $Y \mapsto \mathrm{St}^*_G(Y)$. Inoltre, ogni elemento $Y \in \mathcal{B}$ ha per cardinalità l'indice di H nel sottogruppo $St^*_G(Y)$ corrispondente a Y.*

Dimostrazione — Iniziamo col provare che, per ogni $K \in \mathcal{L}$, se $g \in G$ è tale che $\mathrm{Orb}_K(x) \cap \mathrm{Orb}_K(x)g \neq \varnothing$, allora $g \in K$. Sia $y \in \mathrm{Orb}_K(x) \cap \mathrm{Orb}_K(x)g$. Allora $y = xk = xk'g$ per opportuni $k, k' \in K$. Dunque $x = xk'gk^{-1}$, cioè $k'gk^{-1} \in H \leq K$. Da ciò segue, come si voleva, $g \in K$. Questa prima osservazione ha due conseguenze. In primo luogo $\mathrm{Orb}_K(x)$ è un blocco di imprimitività a cui, ovviamente, appartiene x; infatti $\mathrm{Orb}_K(x) = \mathrm{Orb}_K(x)g$ per ogni $g \in K$. Dunque l'applicazione $\alpha : K \in \mathcal{L} \mapsto \mathrm{Orb}_K(x) \in \mathcal{B}$ è ben definita. In secondo luogo $\mathrm{St}^*_G(K^\alpha) = K$ per ogni $K \in \mathcal{L}$.

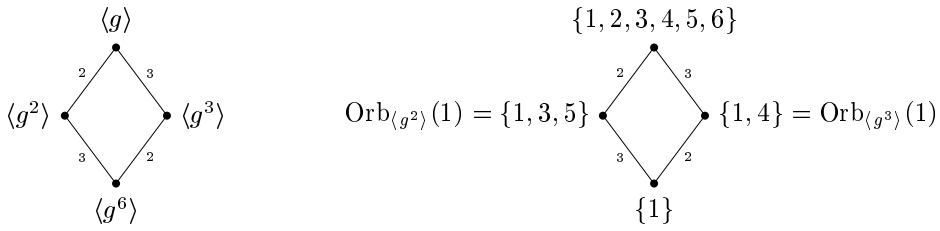
Per ogni $Y \in \mathcal{B}$ proviamo ora $\mathrm{St}^*_G(Y) = \{g \in G \mid xg \in Y\}$. L'inclusione da sinistra verso destra è banale: se $g \in \mathrm{St}^*_G(Y)$ allora $xg \in Yg = Y$. Anche l'inclusione opposta si verifica facilmente: se $g \in G$ e $xg \in Y$ allora $xg \in Y \cap Yg$, quindi $Y = Yg$ (perché Y è un blocco di imprimitività), cioè $g \in \mathrm{St}^*_G(Y)$. Anche in questo caso ricaviamo due conseguenze. La prima è che per ogni $Y \in \mathcal{B}$ si ha $H = \mathrm{St}_G(x) \leq \{g \in G \mid xg \in Y\} = \mathrm{St}^*_G(Y)$, quindi $\mathrm{St}^*_G(Y) \in \mathcal{L}$ ed è ben definita l'applicazione $\beta : Y \in \mathcal{B} \mapsto \mathrm{St}^*_G(Y) \in \mathcal{L}$. L'altra è che, sempre per ogni $Y \in \mathcal{B}$, si ha $Y^{\beta\alpha} = \mathrm{Orb}_{Y^\beta}(x) = \{xg \mid g \in \mathrm{St}^*_G(Y)\} = \{xg \mid g \in G \wedge xg \in Y\} = Y$.

Abbiamo così provato $\alpha\beta = 1_{\mathcal{L}}$ nel primo capoverso, $\beta\alpha = 1_{\mathcal{B}}$ nel secondo, quindi α e β sono biettive ed una inversa dell'altra. Per provare che α e β sono isomorfismi reticolari basta osservare che esse sono entrambe crescenti. Ciò è ovvio nel caso di α; lo è anche per β se si ricorda che $Y^\beta = \{g \in G \mid xg \in Y\}$ per ogni $Y \in \mathcal{B}$.

Se infine $Y \in \mathcal{B}$ e $K = Y^\beta$, allora $Y = K^\alpha = \mathrm{Orb}_K(x)$ e quindi $|Y| = |K : \mathrm{St}_K(x)| = |K : H|$, provando così l'ultima parte dell'enunciato. ❑

La parte conclusiva della proposizione appena dimostrata fornisce un analogo del teorema di Lagrange per i blocchi di imprimitività: se Y e Y' sono due blocchi (relativi alla stessa rappresentazione permutazionale transitiva) e $Y \subseteq Y'$, allora $|Y|$ divide $|Y'|$ (ed entrambi dividono $|X|$). Più precisamente, è facile vedere che Y' ha una partizione costituita da traslati di Y. Ritroviamo così, come caso particolare, 5.6.

Esempio. Sia $\langle g\rangle$ un gruppo ciclico infinito e sia ρ la sua rappresentazione permutazionale (transitiva) definita da $g^\rho = (1\,2\,3\,4\,5\,6) \in \mathbb{S}_6$. Lo stabilizzante del punto 1 è $\mathrm{St}_\rho(1) = \langle g^6\rangle$. I reticoli $\mathcal{L}$ e $\mathcal{B}$ di cui a 5.8 sono in questo caso:



Dunque ρ non è primitiva. Otteniamo infatti due sistemi di imprimitività non banali, uno determinato dal blocco $U := \{1,3,5\}$, di elementi U e $Ug = \{2,4,6\}$, l'altro determinato dal blocco $V = \{1,4\}$ e di elementi V, $Vg = \{2,5\}$ e $Vg^2 = \{3,6\}$.

Con le notazioni di 5.8 e delle sua dimostrazione, i blocchi banali appartenenti a $\mathcal{B}$ (cioè quelli a cui appartiene x) sono precisamente $\{x\} = H^\alpha$ e $X = G^\alpha$. L'azione di G è primitiva se e solo se non esistono altri elementi in $\mathcal{B}$, quindi, per 5.8, se e solo se $\mathcal{L} = \{H, G\}$. Questo equivale a dire che non esistono sottogruppi K di G tali che $H < K < G$, cioè che H è massimale in G oppure $H = G$, nel qual caso, ovviamente, $X = \{x\}$. Abbiamo così provato:

5.9. Corollario. *Se il gruppo G agisce in modo transitivo su un insieme X, l'azione di G è primitiva se e solo se $|X| \leq 1$ oppure lo stabilizzante in G di un punto di X è un sottogruppo massimale di G.*

Ad esempio, la rappresentazione regolare destra di un gruppo G è primitiva se e solo se G è identico o di ordine primo.

5.10. Corollario. *Un gruppo G ammette una rappresentazione permutazionale fedele e primitiva se e solo se possiede un sottogruppo massimale H tale che $H_G = 1$.*

Dimostrazione — Si ragiona come per 3.7. Se G ha un sottogruppo massimale H come all'enunciato, allora l'azione di G sui laterali destri di H definisce una rappresentazione permutazionale fedele e primitiva. Viceversa, se G opera in modo fedele e primitivo su un insieme, lo stabilizzante H di un punto è un sottogruppo massimale di G. Inoltre, per 3.6, l'azione di G è simile a quella di G sui laterali destri di H, dunque quest'ultima è fedele, cioè $H_G = 1$. ❑

Il Corollario 5.9 permette di dedurre risultati su gruppi primitivi da osservazioni sull'immersione di sottogruppi massimali. Ad esempio, una dimostrazione molto rapida di 5.3 è questa: se $1 \neq N \lhd G$ e G è un gruppo primitivo, allora, detto H lo stabilizzante di un punto si ha $N \not\leq H$ (altrimenti $N \leq H_G$ e quindi $H_G \neq 1$) sicché $G = NH$ per la massimalità di H. Dunque N è transitivo per 1.10.

In alcuni casi può essere preferibile, allo scopo di determinare la primitività o meno di una rappresentazione permutazionale (transitiva), ricorrere al metodo più diretto: cercare blocchi di imprimitività non banali (o dimostrare che non ne esistono). Come già osservato è sufficiente limitarsi a considerare i blocchi a cui appartiene un qualsiasi prefissato punto. La seguente osservazione può essere molto utile:

5.11. *Il gruppo G agisca transitivamente sull'insieme X; siano $x \in X$ e $H = \mathrm{St}_G(x)$. Allora ogni blocco di imprimitività a cui appartenga x è unione di H-orbite.*

Dimostrazione — Per 5.8 ogni blocco di imprimitività cui appartiene x è la K-orbita di x per un sottogruppo K di G contenente H. Quest'orbita è fissata da K e quindi da H, dunque è unione di H-orbite. ❑

Esempio. Utilizziamo l'osservazione appena fatta per provare che, per ogni intero $n > 1$, il gruppo delle isometrie dello spazio euclideo n-dimensionale $\mathbb{R}^n$ è primitivo.

Fissiamo un punto O. Basterà verificare che non esistono blocchi non banali ai quali appartenga O, cioè che se Y è un blocco di imprimitività a cui appartengono O ed almeno un altro punto di $\mathbb{R}^n$, allora necessariamente $Y = \mathbb{R}^n$. Sia Y un tale blocco. Sia poi G lo stabilizzante di O nel gruppo delle isometrie di $\mathbb{R}^n$. Per ogni numero reale non negativo r sia S_r la superficie sferica di centro O e raggio r (cioè l'insieme dei punti di $\mathbb{R}^n$ a distanza r da O). Poiché ogni rotazione di centro O appartiene a G, è facile vedere che le S_r sono precisamente le G-orbite in $\mathbb{R}^n$, dunque, per 5.11, Y sarà unione di alcune di queste superfici sferiche. In altri termini, per ogni r appartenente all'insieme $\mathbb{R}_0^+$ dei numeri reali non negativi, si ha $S_r \cap Y = \varnothing$ o $S_r \subseteq Y$. Sia $R := \{r \in \mathbb{R}_0^+ \mid S_r \subseteq Y\}$. Abbiamo assunto $Y \smallsetminus \{O\} \neq \varnothing$; se $P \in Y \smallsetminus \{O\}$, detta r la distanza (positiva) tra O e P, allora $S_r \subseteq Y$. Ragionando per P come per O si ricava che Y è anche unione di superfici sferiche di centro P, perché $P \in Y$. Allora la superficie sferica S' di centro P e raggio r è contenuta in Y. Per ogni numero reale $s \in [0, 2r]$ esiste un punto $P_s \in S' \cap S_s$ (ad esempio, perché S' è connessa e la funzione distanza è continua), quindi $Y \cap S_s \neq \varnothing$ e $s \in R$. È così provato che per ogni $r \in R$ si ha $[0, 2r] \subseteq R$. Da ciò segue subito che R è un intervallo non superiormente limitato di minimo 0, dunque $R = \mathbb{R}_0^+$. Pertanto $Y = \bigcup_{r\in R} S_r = \mathbb{R}^n$, come si voleva. ❑

Il gruppo delle isometrie dello spazio euclideo di dimensione finita maggiore di 1 fornisce così un esempio di gruppo primitivo non 2-transitivo (vedi esercizio 1 di p. 19).

Il gruppo G che appare nell'esempio appena discusso si chiama *gruppo ortogonale* (reale, n-dimensionale). Quanto appena visto assicura, per 5.9, che il gruppo ortogonale è un sottogruppo massimale del gruppo delle isometrie dello spazio euclideo n-dimensionale, se $n > 1$. Naturalmente si sarebbe anche potuto procedere inversamente: dimostrare per via algebrica la massimalità del gruppo ortogonale nel gruppo delle isometrie dello spazio euclideo e dedurne la primitività di quest'ultimo.

Esercizi.

1. Il gruppo delle isometrie della retta reale non è primitivo (quindi nell'esempio appena discusso è essenziale supporre $n > 1$).
2. Osservare che dall'esercizio 3 di p. 19 e da 5.9 segue un'altra dimostrazione di 5.7.
3. Siano X un insieme e G un sottogruppo di $Sym\, X$. Osservare che la relazione binaria $\sim$ in X definita ponendo $x \sim y$ se e solo se la trasposizione $(x\, y)$ appartiene a G è una congruenza rispetto all'azione di G. Dedurne che se G è primitivo e contiene una trasposizione allora G contiene $FSymX$. [*Se X è infinito vale, più in generale, questo teorema: ogni sottogruppo primitivo di $Sym\, X$ a cui appartenga almeno una permutazione finitaria non identica contiene $AltX$.*]
4. Rispetto all'azione naturale del gruppo delle traslazioni del piano euclideo, ogni retta è un blocco di imprimitività e la sua direzione (classe di parallelismo) è il corrispondente sistema di imprimitività.
5. Sia G un gruppo primitivo di permutazioni. Se G è un gruppo abeliano oppure un p-gruppo finito allora G è o identico oppure di ordine primo.
6. Se H è un sottogruppo di un gruppo G, rispetto alla rappresentazione di G sui laterali destri di H i blocchi di imprimitività a cui appartiene H sono tutti e soli gli insiemi dei laterali destri di H in K al variare di K tra i sottogruppi di G contenenti H.

Riduzione a rappresentazioni primitive

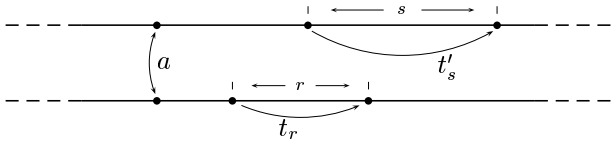
In un certo senso, l'imprimitività (cioè non-primitività) di una rappresentazione permutazionale $\rho : G \to Sym\, X$ su un insieme non vuoto permette di descriverne l'azione in termini di G-rappresentazioni permutazionali più semplici (nel caso finito: di grado minore). Infatti, sia $\sim$ una congruenza rispetto a ρ, determinata da un blocco di imprimitività Y. Posto $\bar{X} := X/\!\sim$, ovvero $\bar{X} = \mathcal{S}(Y)$, sappiamo da 5.1 che ρ induce un'azione permutazionale transitiva $\rho_1 : G \to Sym\, \bar{X}$. Si ha $L := \mathrm{St}_{\rho_1}(Y) = \mathrm{St}^*_\rho(Y)$, quindi, per 3.6, ρ_1 è equivalente all'azione di G sui laterali destri di L, in particolare il suo nucleo è L_G. Un'altra rappresentazione permutazionale indotta da ρ è quella ovvia di L su Y, indichiamola con ρ_2. Anche ρ_2 è transitiva, infatti se x e y sono elementi di Y si ha $y = xg^\rho$ per un opportuno $g \in G$, perché ρ è transitiva. Allora $Y \cap Yg^\rho \neq \varnothing$, quindi $Y = Yg^\rho$ e $g \in L$. Raccogliamo queste osservazioni nel prossimo enunciato, la seconda parte del quale garantisce che il tipo di similitudine di ρ_2 non dipende dalla scelta del blocco di imprimitività Y tra quelli che determinano la fissata congruenza $\sim$.

5.12. *Sia $\rho : G \longrightarrow Sym\, X$ una rappresentazione permutazionale transitiva e sia Y un blocco di imprimitività. Allora ρ dà luogo a due rappresentazioni transitive, $\rho_1 : G \longrightarrow Sym\, \bar{X}$ di nucleo L_G e $\rho_2 : L \longrightarrow Sym\, Y$ di nucleo $\mathrm{St}_\rho(Y)$, dove $\bar{X} = \mathcal{S}(Y)$ e $L = \mathrm{St}^*_\rho(Y)$. La rappresentazione ρ_2 è, per ogni $g \in G$, simile all'azione indotta da ρ di $L^g = \mathrm{St}^*_\rho(Yg)$ su Yg, tramite l'$\mathcal{RP}$-isomorfismo determinato dalle applicazioni $a \in L \mapsto a^g \in L^g$ e $y \in Y \mapsto yg \in Yg$.*

Dimostrazione — È solo da verificare la seconda parte dell'enunciato, cioè che le applicazioni indicate determinano un $\mathcal{RP}$-isomorfismo. La verifica è diretta; l'isomorfismo indicato è indotto da quello descritto nell'esercizio 4, p. 14. ❑

Si può riguardare il procedimento appena descritto come una 'decomposizione' della rappresentazione transitiva ρ nelle due rappresentazioni transitive ρ_1 e ρ_2. Visualizziamo ciò interpretando ρ, ρ_1 e ρ_2 come azioni su laterali di sottogruppi di G: se H è lo stabilizzante di un punto rispetto a ρ, allora ρ è simile all'azione di G sui laterali destri di H, mentre ρ_1 e ρ_2 sono simili rispettivamente all'azione di G sui laterali destri di L e all'azione di L sui laterali destri di H (in L; ciò ha senso perché $H \leq L$). Va però tenuto ben presente che se da una parte è vero, come mostreremo (si veda quanto segue 5.17), che date due rappresentazioni transitive φ_1 e φ_2 su insiemi non vuoti è sempre possibile costruire una rappresentazione permutazionale ρ tale che φ_1 e φ_2 siano rispettivamente simili a rappresentazioni con la stessa immagine delle ρ_1 e ρ_2 costruite come in 5.12, una tale ρ non è in generale univocamente determinata da φ_1 e φ_2 (neanche a meno di similitudini o del nucleo), e una sua descrizione esplicita partendo da φ_1 e φ_2 può essere piuttosto complicata (cfr. 5.18). In alcuni casi, comunque, questo procedimento di 'decomposizione' di ρ è particolarmente trasparente. Vediamo un esempio.

5.13. Esempio. Nel piano cartesiano $\mathbb{R}^2$, sia $X = \mathbb{R} \times \{0, 1\}$, l'unione (disgiunta) dell'asse delle ascisse e della retta di equazione $y = 1$. Sono permutazioni di X l'applicazione $a : (u, v) \in X \longmapsto (u, 1 - v) \in X$, che scambia le due rette tra loro e, per ogni $r \in \mathbb{R}$, l'applicazione t_r che opera come la traslazione di ampiezza r sull'asse delle ascisse (lungo la direzione e verso dell'asse stesso) e fissa ogni punto della retta di equazione $y = 1$; più esplicitamente, t_r è definita da $(u, 0) \mapsto (u + r, 0)$ e $(u, 1) \mapsto (u, 1)$ per ogni $u \in \mathbb{R}$. In modo analogo, per ogni $r \in \mathbb{R}$ possiamo



anche considerare la permutazione t'_r di X che fissa tutti i punti dell'asse delle ascisse e agisce sulla retta di equazione $y = 1$ come la traslazione di ampiezza r: $(u, 1) \mapsto (u + r, 1)$; si verifica subito $t'_r = t^a_r$. È chiaro che $T := \{t_r \mid r \in \mathbb{R}\}$ è un sottogruppo di $Sym\, X$, isomorfo a $(\mathbb{R}, +)$ tramite l'isomorfismo $r \in \mathbb{R} \mapsto t_r \in T$. Inoltre T commuta con $T^a = \{t'_r \mid r \in \mathbb{R}\}$ e, ovviamente, $T \cap T^a = 1$; quindi $\langle T, T^a\rangle = T \times T^a$. Infine, TT^a è normalizzato da a, perché a ha periodo 2. Allora il sottogruppo G di $Sym\, X$ generato da T e a è $(T \times T^a) \rtimes \langle a\rangle$, quindi ogni elemento di G si esprime (in modo unico) in una delle forme $t_r t'_s$ oppure $t_r t'_s a$, con $r, s \in \mathbb{R}$. È evidente che G è transitivo, e che rispetto all'azione di G le due rette costituiscono un sistema di imprimitività non banale; la corrispondente congruenza è la relazione $\sim$ definita in X da $(u, v) \sim (u', v') \iff v = v'$. Il sottogruppo TT^a di G svolge il ruolo svolto da L in 5.12: è lo stabilizzante globale di uno dei blocchi di imprimitività —di fatto di entrambi, perché $TT^a \lhd G$. Il quoziente $X/\!\sim$ ha ordine 2 (i suoi elementi sono le due rette), su di esso G agisce nell'unico modo possibile con nucleo TT^a: gli elementi di $G \setminus TT^a$ scambiano tra loro le rette. Invece TT^a agisce su ciascuna delle rette con un'azione transitiva (sull'asse delle ascisse con nucleo T^a, sull'altra retta con nucleo T; le due azioni sono simili tra loro). ❑

Facendo di nuovo riferimento alle notazioni di 5.12, se il blocco Y (ovvero la congruenza $\sim$) da cui si parte non è banale e $|X|$ è finito, allora ρ_1 e ρ_2 hanno grado minore di quello di ρ. Questa osservazione può essere di aiuto per ragionamenti di tipo induttivo, e suggerisce un metodo di riduzione per affrontare problemi relativi a rappresentazioni permutazionali su insiemi finiti.

Un esempio di applicazione è il prossimo teorema, che permette di fare una stima sul numero di generatori di un gruppo finito di permutazioni. Premettiamo un semplicissimo lemma.

5.14. Lemma. *Siano G un gruppo ed N un suo sottogruppo normale. Se S e T sono due parti di G tali che $N \leq \langle S\rangle$ e $G/N = \langle gN \mid g \in T\rangle$, allora $G = \langle S \cup T\rangle$.*

Dimostrazione — Sia $H = \langle S \cup T\rangle$. Allora $N \leq \langle S\rangle \leq H$. Inoltre $H/N \geq \langle gN \mid g \in T\rangle = G/N$, quindi $H/N = G/N$ e $H = G$. ❑

5.15. Teorema. *Sia G un gruppo di permutazioni di grado finito n. Se G ha r orbite allora G è generato da un insieme di al più $n - r$ elementi. In particolare, per ogni $n \in \mathbb{N}$, ogni sottogruppo di $\mathbb{S}_n$ è generato da al più $n - 1$ suoi elementi.*

Dimostrazione — Si procede per successive riduzioni del problema al caso in cui G sia primitivo, ragionando per induzione su $|G| + n$, dove n è il grado di G. Se $n \leq 1$, allora $r = n$ e G è il gruppo identico (generato da 0 elementi, come richiesto in questo caso dall'enunciato), il che fornisce la base di induzione e ci permette di assumere $n > 1$.
— *Riduzione al caso transitivo.* Supponiamo G non transitivo. Sia Y una G-orbita. Ovviamente $m := |Y| < n$. Poiché Y è fissata da G, dall'esercizio 3 di p. 4 segue $N := \mathrm{St}_G(Y) \lhd G$, e G/N opera fedelmente su Y. Quindi, per ipotesi induttiva, G/N è generato da un insieme $\{g_1 N, \ldots, g_{m-1} N\}$ di al più $m - 1$ elementi. Inoltre N opera, anch'esso fedelmente, su $X \setminus Y$, nel modo ovvio stabilito in 1.6. Chiaramente N ha almeno $r - 1$ orbite in $X \setminus Y$, ciascuna contenuta in una delle G-orbite distinte da Y. Quindi, sempre per ipotesi induttiva, N è generato da un insieme S di ordine al più $|X \setminus Y| - (r - 1) = (n - m) - (r - 1)$. Il Lemma 5.14 garantisce che G è generato da $S \cup \{g_1, \ldots, g_{m-1}\}$, il quale ha ordine al più $(n - m) - (r - 1) + (m - 1) = n - r$. È pertanto sufficiente provare il teorema nel caso in cui G sia transitivo.
— *Riduzione al caso primitivo.* Supponiamo G transitivo ma non primitivo, sia Y un G-blocco di imprimitività non banale e sia $L = \mathrm{St}^*_G(Y)$. Da 5.12 sappiamo che G/L_G opera fedelmente su $\mathcal{S}(Y)$, quindi, per induzione, G/L_G è generato da al più $t - 1$ elementi, dove $t = |\mathcal{S}(Y)| < n$. Inoltre L_G è un sottogruppo proprio di G ed opera fedelmente su X, con azione indotta per restrizione da quella di G. Rispetto a quest'azione L_G ha almeno t orbite, perché ogni elemento di $\mathcal{S}(Y)$ è fissato da L_G, quindi è unione di L_G-orbite. Dunque, ancora per induzione, L_G è generato da una sua parte di ordine al più $n - t$, e, per il lemma, G è generato da al più $(n - t) + (t - 1) = n - 1$ elementi. Pertanto possiamo supporre che G sia primitivo.
— *Conclusione.* Supponiamo G primitivo, e sia H lo stabilizzante in G di un punto x di X. Ovviamente H agisce fedelmente su $X \setminus \{x\}$ (non vuoto perché $n > 1$), quindi H è generato da al più $(n - 1) - 1 = n - 2$ elementi, per ipotesi di induzione. Inoltre, poiché H è massimale in G (vedi 5.9), $G = \langle H, g\rangle$ per ogni $g \in G \setminus H$. Da ciò segue l'asserto. ❑

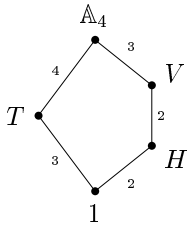
Un teorema di dimostrazione molto più complessa di questo, dovuto a A. McIver e P.M. Neumann (1987) mostra che, con la sola eccezione del gruppo $\mathbb{S}_3$, per ogni numero naturale n ogni sottogruppo di $\mathbb{S}_n$ è generato da un insieme di al più $n/2$ suoi elementi.

Esercizio. Per ogni intero $n > 2$ ciascuno dei seguenti insiemi è un sistema di generatori per $\mathbb{S}_n$:
— $T_1 = \{(1\ 2), (1\ 3), \ldots, (1\ n)\} = \{(1\ i) \mid i \in \mathbb{N} \wedge 1 < i \leq n\}$;
— $T_2 = \{(1\ 2), (2\ 3), \ldots, (n-1\ \ n)\} = \{(i\ \ i+1) \mid i \in \mathbb{N} \wedge 1 \leq i < n\}$;
— $T_3 = \{(1\ 2), (2\ 3\ \cdots\ n)\}$;

— $T_4 = \{(1\ 2), (1\ 2\ \cdots\ n)\}$.
[*Suggerimento: ogni trasposizione in $\mathbb{S}_n$ si ottiene coniugando tra loro due opportuni elementi di T_1; ogni elemento di T_1 è uguale a $(1\ 2)^\sigma$ dove σ è prodotto di elementi di T_2, ciascun elemento di T_1 (risp. T_2) è un coniugato di $(1\ 2)$ mediante una potenza di $(2\ 3\ \cdots\ n)$ (risp. di $(1\ 2\ \cdots\ n)$).*] Come si vede T_1 e T_2 sono insiemi di generatori di ordine $n-1$, la cui esistenza è prevista da 5.15, ma $\mathbb{S}_n$ è anche generato da un insieme di ordine 2. Verificare che, T_1, T_2, T_3 e T_4 sono sistemi minimali di generatori, cioè nessuna loro parte propria genera $\mathbb{S}_n$.

Osserviamo infine che iterando il procedimento di 'decomposizione' presentato in 5.12, da una rappresentazione permutazionale transitiva di grado finito si ottiene una sequenza finita di rappresentazione primitive. A differenza di quanto si potrebbe sperare, però, il numero di queste rappresentazioni ed il loro tipo dipende dal modo in cui la decomposizione è stata effettuata (cioè dai sistemi di imprimitività utilizzati), come mostra il prossimo esempio (a titolo di confronto, una situazione più fortunata è quella che si verifica per i fattori di composizione di un gruppo finito: per il teorema di Jordan-Hölder, a meno dell'ordine in cui appaiono e di isomorfismi, essi non dipendono dalla serie di composizione con cui sono stati calcolati).

Esempio. Consideriamo la rappresentazione regolare destra δ del gruppo $\mathbb{A}_4$. Sia T un sottogruppo di ordine 3 in $\mathbb{A}_4$, ad esempio $T = \langle(1\ 2\ 3)\rangle$. Osservato che T è un blocco di imprimitività rispetto a δ, possiamo applicare 5.12 a δ, con T in luogo di Y, ottenendo così una rappresentazione permutazionale ρ_1 di $\mathbb{A}_4$ sul sistema di imprimitività determinato da T ed una rappresentazione ρ_2 dello stabilizzante globale di T (cioè, ovviamente, T stesso) su T. Come sappiamo, possiamo facilmente identificare queste due rappresentazioni. Chiaramente ρ_2 è la rappresentazione regolare destra di T (primitiva perché di grado 3). Per quanto riguarda ρ_1, il sistema di imprimitività determinato da T è l'insieme dei laterali destri di questo in $\mathbb{A}_4$, quindi ρ_1 è la rappresentazione di $\mathbb{A}_4$ sui laterali destri di T; dal fatto che T è anche lo stabilizzante di un punto rispetto alla rappresentazione naturale di $\mathbb{A}_4$ segue subito (Proposizione 3.8) che ρ_1 è simile a quest'ultima, anch'essa primitiva in quanto 2-transitiva (ovvero: perché T è massimale in $\mathbb{A}_4$). Abbiamo così ottenuto due rappresentazioni primitive 'decomponendo' δ a partire da T, una di grado 4 ed una di grado 3, entrambe fedeli.

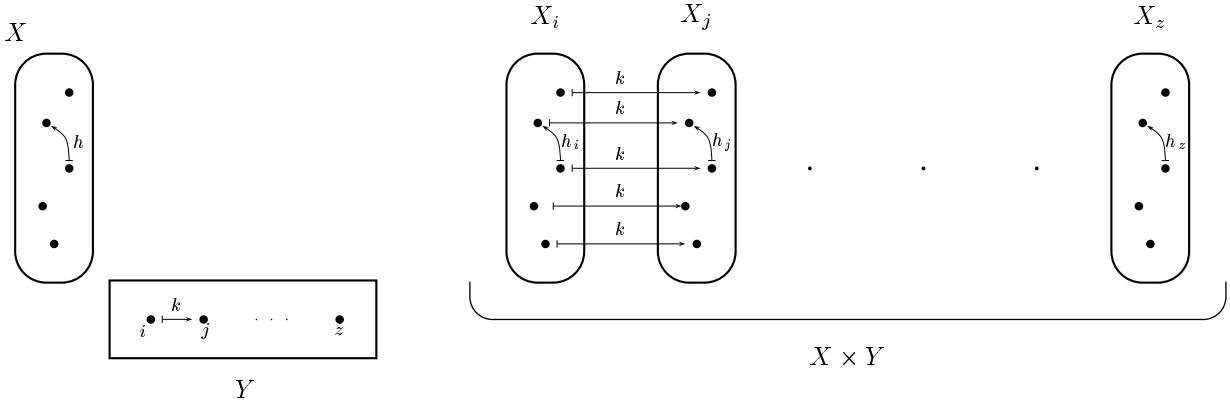


Consideriamo ora $V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, il sottogruppo di ordine 4 in $\mathbb{A}_4$. Se partiamo da V (visto come blocco di imprimitività) otteniamo da δ l'azione di $\mathbb{A}_4$ sui laterali destri di V, che ha grado 3 (quindi è primitiva), nucleo V e per immagine il cayleyano destro di $\mathbb{A}_4/V$, e poi la rappresentazione regolare destra di V. Questa seconda rappresentazione non è primitiva, ma, ancora per 5.12, un suo blocco non banale, cioè un sottogruppo H di ordine 2 in V, dà luogo a due rappresentazioni (primitive) di grado 2: quella di V sui laterali di H (con nucleo H) e quella regolare di H. Come si vede, le tre rappresentazioni primitive ottenute per questa via non si possono ricondurre a ρ_1 e ρ_2.

Prodotto intrecciato

Concludiamo questa sezione accennando brevemente ad una importante costruzione, il prodotto intrecciato, che in qualche modo inverte il procedimento di scomposizione presentato in 5.12.

Siano date due rappresentazioni permutazionali di gruppi, $\rho : H \longrightarrow Sym\, X$ e $\varphi : K \longrightarrow Sym\, Y$, con $X \neq \varnothing \neq Y$. Sia poi $B = \prod_{i\in Y} H_i$ il prodotto cartesiano di $|Y|$ copie del gruppo H. Si definisce una rappresentazione permutazionale ρ_* di B su $\Omega := X \times Y$ facendo agire ciascuna componente H_y di B sulla y-esima sezione $X_y := X \times \{y\}$ di Ω, poniamo cioè $(x,y)\big((h_i)_{i\in Y}\big)^{\rho_*} = (xh_y^\rho, y)$ per ogni $(x,y) \in \Omega$ e $(h_i)_{i\in Y} \in B$. È facile verificare che ρ_* è effettivamente una rappresentazione permutazionale. Definiamo poi una rappresentazione permutazionale φ_* di K su Ω, ponendo $(x,y)k^{\varphi_*} = (x, yk^\varphi)$ per ogni $(x,y) \in \Omega$ e $k \in K$. Le azioni su Ω appena definite possono essere così schematizzate:



Un agevole calcolo diretto mostra che, scelti comunque $k \in K$ e $h = (h_i)_{i\in Y} \in B$, si ha $(h^{\rho_*})^{k^{\varphi_*}} = \big((h_{ik^{-\varphi}})_{i\in Y}\big)^{\rho_*}$, dove, come di consueto, $k^{-\varphi}$ indica $(k^\varphi)^{-1}$, ovvero $(k^{-1})^\varphi$. In particolare $\operatorname{im}\varphi_*$ normalizza $\operatorname{im}\rho_*$. Poiché, come è chiaro, $\operatorname{im}\varphi_*$ e $\operatorname{im}\rho_*$ hanno intersezione identica, il sottogruppo di $Sym\,\Omega$ da essi generato è $\operatorname{im}\rho_* \rtimes \operatorname{im}\varphi_*$.

Consideriamo per un momento un caso particolare, sostituendo a ρ la rappresentazione regolare destra δ di H. Allora δ_* è un monomorfismo e $B \simeq \operatorname{im}\delta_*$. L'azione di coniugio di $\operatorname{im}\varphi_*$ su $\operatorname{im}\delta_*$ determina un omomorfismo da $\operatorname{im}\varphi_*$ a $\operatorname{Aut}(\operatorname{im}\delta_*)$ e quindi, a meno dell'identificazione degli elementi di B con quelli di $\operatorname{im}\delta_*$ tramite δ_*, un omomorfismo $\operatorname{im}\varphi_* \to \operatorname{Aut} B$. Componendo questo con l'epimorfismo $k \in K \mapsto k^{\varphi_*} \in \operatorname{im}\varphi_*$ otteniamo l'omomorfismo di K in $\operatorname{Aut} B$

$$\theta : K \longrightarrow \operatorname{im}\varphi_* \longrightarrow \operatorname{Aut}(\operatorname{im}\delta_*) \xrightarrow{\sim} \operatorname{Aut} B.$$

Utilizzando θ si definisce il prodotto semidiretto $B \rtimes_\theta K$, in cui, quindi, l'azione di coniugio di K su B è definita da

$$\big((h_i)_{i\in Y}\big)^k = (h_{ik^{-\varphi}})_{i\in Y}.$$

Come si vede, l'azione di coniugio di $k \in K$ su un elemento $h \in B$ si può descrivere in questo modo: la componente h_i di posto i in h diventa la componente di posto ik^φ in h^k.

Questo prodotto semidiretto si chiama si chiama *prodotto intrecciato* di H e K rispetto a φ, in simboli $H \operatorname{Wr} K$, ed il suo fattore normale B viene detto *gruppo base* di $H \operatorname{Wr} K$ (ovviamente, essendo φ rilevante nella definizione del prodotto intrecciato, utilizzando questa notazione è importante che il contesto chiarisca quale sia la rappresentazione φ).

Esempi. Se $K = \langle k\rangle$ è un gruppo ciclico di ordine multiplo di 4 e $\varphi : K \to \mathbb{S}_4$ è la sua rappresentazione permutazionale definita da $k^\varphi = (1\ 2\ 3\ 4)$, allora B si può identificare con $H \times H \times H \times H$, e $H \operatorname{Wr} K$ è $B \rtimes K$, dove per ogni $(h_1, h_2, h_3, h_4) \in B$ si ha $(h_1, h_2, h_3, h_4)^k = (h_4, h_1, h_2, h_3)$. Se invece $|K|$ è multiplo di 6 e $\varphi : K \to \mathbb{S}_7$ è definita da $k^\varphi = (1\ 3)(2\ 5\ 6)$, allora B è identificabile col prodotto diretto di sette copie di H e per ogni suo elemento $(h_1, \dots, h_7)$ in $H \operatorname{Wr} K$ si ha $(h_1, \dots, h_7)^k = (h_3, h_6, h_1, h_4, h_2, h_5, h_7)$.

Tornando al caso generale, passiamo ora a definire la rappresentazione permutazionale prodotto intrecciato $\rho \operatorname{Wr} \varphi$. Questa rappresentazione si ottiene estendendo in modo ovvio ρ_* e φ_* a $H \operatorname{Wr} K$, è definita infatti così:

$$\rho \operatorname{Wr} \varphi : (h_i)_{i\in Y}\, k \in H \operatorname{Wr} K \longmapsto \big((h_i)_{i\in Y}\big)^{\rho_*} k^{\varphi_*} \in Sym(X \times Y).$$

Il fatto che questa applicazione sia un omomorfismo si verifica in modo diretto applicando la seguente osservazione.

5.16. *Sia $G = N \rtimes H$ un prodotto semidiretto di gruppi. Dati due omomorfismi $\alpha : N \to G_1$ e $\beta : H \to G_1$ di codominio lo stesso gruppo G_1, esiste un omomorfismo $G \to G_1$ che prolunga sia α che β se e solo se $\big(a^h\big)^\alpha = \big(a^\alpha\big)^{h^\beta}$ per ogni $a \in N$ e $h \in H$.*

Dimostrazione — È chiaro che l'unico possibile omomorfismo che prolunghi sia α che β è l'applicazione φ che all'elemento $ah \in G$ (con $a \in N$ e $h \in H$) associa $a^\alpha h^\beta \in G_1$. Che φ sia ben definita come applicazione è evidente: ogni elemento di G ha un'unica espressione come prodotto di un elemento di N per un elemento di H. Ciò che va provato è dunque che φ è un omomorfismo se e solo se vale la condizione indicata all'enunciato. Affinché φ sia un omomorfismo occorre e basta che valga $(aha_1h_1)^\varphi = (ah)^\varphi (a_1h_1)^\varphi$ per ogni $a, a_1 \in N$ e $h, h_1 \in H$. Si ha

$$(aha_1h_1)^\varphi = \big(aa_1^{h^{-1}}hh_1\big)^\varphi = \big(aa_1^{h^{-1}}\big)^\alpha (hh_1)^\beta = a^\alpha \big(a_1^{h^{-1}}\big)^\alpha h^\beta h_1^\beta,$$
$$(ah)^\varphi (a_1h_1)^\varphi = a^\alpha h^\beta a_1^\alpha h_1^\beta = a^\alpha \big(a_1^\alpha\big)^{h^{-\beta}} h^\beta h_1^\beta,$$

e questi sono uguali se e solo se $\big(a_1^{h^{-1}}\big)^\alpha = \big(a_1^\alpha\big)^{h^{-\beta}}$. Da ciò segue immediatamente l'asserto. ❑

Avendosi $\Big(\big((h_i)_{i\in Y}\big)^k\Big)^{\rho_*} = \big((h_{ik^{-\varphi}})_{i\in Y}\big)^{\rho_*} = \Big(\big((h_i)_{i\in Y}\big)^{\rho_*}\Big)^{k^{\varphi_*}}$ per ogni $(h_i)_{i\in Y} \in B$ e $k \in K$ abbiamo così che $\rho \operatorname{Wr} \varphi$ è un omomorfismo, dunque una rappresentazione permutazionale. Naturalmente la sua immagine è $\operatorname{im}\rho_* \rtimes \operatorname{im}\varphi_*$.

Se $(x, y) \in X \times Y$ e $w = (h_i)_{i\in Y}\, k \in H \operatorname{Wr} K$, con ovvie notazioni, allora $(x, y)w^{\rho \operatorname{Wr} \varphi} = \big(xh_y^\rho, yk^\varphi\big)$. Evidentemente $\rho \operatorname{Wr} \varphi$ è *fedele se e solo se sia ρ che φ sono fedeli*. Pertanto, se ρ e φ sono fedeli (in particolare, se H e K sono gruppi di permutazioni e ρ e φ ne sono le rappresentazioni naturali) $H \operatorname{Wr} K$ è identificabile col sottogruppo $\operatorname{im}\rho_* \rtimes \operatorname{im}\varphi_*$ di $Sym(X \times Y)$. Un caso particolarmente importante in cui ciò si verifica è il *prodotto intrecciato standard*, cioè il prodotto intrecciato tra due gruppi H e K ottenuto partendo dalle loro rappresentazioni regolari destre.

Esclusi casi banali, se ρ e φ sono transitive $\rho \operatorname{Wr} \varphi$ è transitiva ma imprimitiva:

5.17. *Con le notazioni finora usate, $\rho \operatorname{Wr} \varphi$ è transitiva se e solo se ρ e φ sono entrambe transitive. Se ciò accade, per ogni $y \in Y$ la sezione $X_y = X \times \{y\}$ è un blocco di imprimitività rispetto a $\rho \operatorname{Wr} \varphi$, non banale se $|X|$ e $|Y|$ sono maggiori di 1.*

Dimostrazione — Poniamo, per brevità, $\psi = \rho \operatorname{Wr} \varphi$. Sia ψ transitiva. Se $x, x' \in X$ e $y \in Y$, esiste $w \in H \operatorname{Wr} K$ tale che $(x, y)w^\psi = (x', y)$. Allora, se $w = hk$ con $h \in B$ e $k \in K$, detta h_y la componente di h di posto y si ha $x' = xh_y^\rho$. Ciò prova che ρ è transitiva (si noti che è stata usata l'ipotesi $Y \neq \varnothing$). Analogamente si prova che φ è transitiva.

Supponiamo viceversa ρ e φ transitive. Per ogni (x, y) e (x', y') in $X \times Y$ esistono $h \in H$ e $k \in K$ tali che $x' = xh^\rho$ e $y' = yk^\rho$. Se b è un qualsiasi elemento di B la cui componente di posto y è h, allora $(x', y') = (x, y)(bk)^\psi$. Dunque ψ è transitiva. Infine $X_y(bk)^\psi = X_{yk^\varphi}$ per ogni elemento bk (con $b \in B$ e $k \in K$) di $H \operatorname{Wr} K$; essendo $X_y \cap X_{y'} = \varnothing$ se $y \neq y'$, ciò mostra che X_y è un blocco di imprimitività. Chiaramente $|X_y| = 1$ se e solo se $|X| = 1$, e X_y è l'unico traslato di se stesso se e solo se $Y = \{y\}$. Quest'ultima osservazione completa la dimostrazione. ❑

Mantenendo le stesse notazioni dell'ultima dimostrazione, nell'ipotesi che ψ sia transitiva, possiamo applicare 5.12 a ψ ed al suo blocco di imprimitività X_y. Detta ψ_1 la rappresentazione indotta da ψ su $\overline{Y} := \delta(X_y) = \{X_i \mid i \in Y\}$, è chiaro che il gruppo base B è contenuto nel nucleo di ψ_1 e quindi, tramite il primo teorema di omomorfismo, ψ_1 induce una rappresentazione permutazionale $(H \operatorname{Wr} K)/B \longrightarrow Sym\,\overline{Y}$. Questa è simile a φ: una similitudine è determinata dall'isomorfismo $k \in K \mapsto kB \in (H \operatorname{Wr} K)/B$ e dalla biezione $i \in Y \mapsto X_i \in \overline{Y}$.

L'altra delle due rappresentazioni permutazionali in cui, nel senso di 5.12, si decompone ψ, chiamiamola ψ_2, è quella dello stabilizzante globale di X_y — che è $L := B\,\mathrm{St}_\varphi(y)$ — su X_y stesso. Detto $\hat{H}_y$ il sottogruppo di B costituito dalle famiglie $(h_i)_{i\in Y}$ per le quali $h_y = 1$ (cioè il nucleo della proiezione canonica di B sulla componente di posto y), si verifica che $N := \hat{H}_y\,\mathrm{St}_\varphi(y)$ è contenuto in $\ker\psi_2 = \mathrm{St}_\psi(X_y)$. Inoltre N è un sottogruppo normale di L. Per provare ciò osserviamo in primo luogo che $\hat{H}_y$ è normalizzato da $\mathrm{St}_\varphi(y)$ (oltre che, ovviamente, da B). Inoltre $B/\hat{H}_y$ e $N/\hat{H}_y$ si centralizzano. Infatti ogni elemento di $B/\hat{H}_y$ si può scrivere come $\tilde{h}_y\hat{H}_y$, dove, per $h \in H$, indichiamo con $\tilde{h}_y$ l'elemento $(h_i)_{i\in Y}$ di B definito da $h_y = h$ e $h_i = 1$ per $i \neq y$; ed è chiaro che $\tilde{h}_y$ è centralizzato da N. Pertanto $N/\hat{H}_y$ è normale in $BN/\hat{H}_y = L/N$, quindi, come si voleva, $N \lhd L$. Allora, analogamente a quanto fatto per ψ_1, otteniamo che ρ è simile alla rappresentazione $L/N \longrightarrow Sym\,X_y$ indotta da ψ_2; una similitudine è determinata dall'isomorfismo $h \in H \mapsto \tilde{h}_yN \in L/N$ e dalla biezione $x \in X \mapsto (x, y) \in X_y$.

Abbiamo in particolare così stabilito che, date comunque due rappresentazioni permutazionali transitive ρ e φ, esiste una rappresentazione permutazionale ψ tale che ρ e φ siano simili a rappresentazioni ottenute da ψ mediante la decomposizione definita in 5.12 ed un'applicazione del primo teorema di omomorfismo. Ciò chiarisce anche l'osservazione fatta dopo la dimostrazione di 5.12 che non era stata ancora giustificata.

In accordo con 5.17 possiamo dire che il prodotto intrecciato fornisce un metodo generale per la costruzione di rappresentazioni imprimitive. In un certo senso questa costruzione è la più generale possibile: se G agisce su un insieme X in modo imprimitivo tramite una rappresentazione permutazionale transitiva ρ, allora, a meno di similitudini, si può identificare G con un sottogruppo del prodotto intrecciato costruito a partire da due rappresentazioni permutazionali in cui ρ si 'decompone' nel senso di 5.12.

5.18. Teorema. *Sia $\rho : G \longrightarrow Sym\,X$ una rappresentazione permutazionale transitiva, e sia Y un blocco di imprimitività rispetto a ρ. Scelto comunque un sottogruppo normale N di G contenuto in $L := \mathrm{St}^*_\rho(Y)$ e detto $\bar{X}$ il sistema di imprimitività determinato da Y, si considerino le rappresentazioni permutazionali indotte da ρ:*

$$\rho_1 : G/N \longrightarrow Sym\,\bar{X} \qquad \text{e} \qquad \rho_2 : L \longrightarrow Sym\,Y.$$

Allora ρ è simile all'azione indotta per restrizione da $\rho_2 \operatorname{Wr} \rho_1$ su un un sottogruppo di $L \operatorname{Wr} (G/N)$.

Dimostrazione — Indichiamo con $\bar{G}$ il quoziente G/N e, per ogni $g \in G$, poniamo $\bar{g} = gN$. Sia T un trasversale destro di L in G. Per ogni $t \in T$ e $g \in G$, indichiamo con t_{g^*} l'unico elemento di T appartenente al laterale Ltg, quindi $Ltg = Lt_{g^*}$. Come segue da 1.1, l'applicazione $t \in T \mapsto Yt \in \bar{X}$ è biettiva, ogni elemento di $\bar{X}$ si rappresenta dunque in unico modo nella forma Yt con $t \in T$. Per ciascuno di questi elementi ed ogni $g \in G$, si ha $Yt\bar{g}^{\rho_1} = Ytg = Yt_{g^*}$. Inoltre $tg = l_{g,t}t_{g^*}$, dove $l_{g,t} = tg(t_{g^*})^{-1} \in L$. Con queste notazioni, e indicando con W il prodotto intrecciato $L \operatorname{Wr} \bar{G}$ effettuato rispetto a ρ_1, verifichiamo che

$$\mu : g \in G \longmapsto \big(l_{g,t}\big)_{Yt\in\bar{X}} \cdot \bar{g} \in W$$

è un monomorfismo. A questo scopo osserviamo che per ogni $g, h \in G$ e $t \in T$ vale $t_{(gh)^*} = t_{g^*h^*}$, perché $Lt_{(gh)^*} = Ltgh = Lt_{g^*}h = Lt_{g^*h^*}$. Quindi:

$$l_{gh,t} = tgh(t_{(gh)^*})^{-1} = l_{g,t}t_{g^*}h(t_{g^*h^*})^{-1} = l_{g,t}l_{h,t_{g^*}}.$$

Allora

$$\begin{aligned}(gh)^\mu &= \big(l_{gh,t}\big)_{Yt\in\bar{X}} \cdot \bar{g}\bar{h} = \big(l_{g,t}\big)_{Yt\in\bar{X}}\big(l_{h,t_{g^*}}\big)_{Yt\in\bar{X}} \cdot \bar{g}\bar{h}\\ &= \big(l_{g,t}\big)_{Yt\in\bar{X}}\,\bar{g}\left(\big(l_{h,t_{g^*}}\big)_{Yt\in\bar{X}}\right)^{\bar{g}}\bar{h} = \big(l_{g,t}\big)_{Yt\in\bar{X}}\,\bar{g}\,\big(l_{h,t_{(g^{-1})^*g^*}}\big)_{Yt\in\bar{X}}\,\bar{h} = g^\mu h^\mu.\end{aligned}$$

Quindi μ è un omomorfismo. Sia ora $g \in \ker\mu$. Allora $\big(l_{g,t}\big)_{Yt\in\bar{X}} \cdot \bar{g} = 1$, quindi $\bar{g} = 1$, cioè $g \in N \leq L$, e $l_{g,t} = 1$ per ogni $t \in T$. Se t è l'elemento di T appartenente a L, allora $tg \in L$, quindi $t_{g^*} = t$ e da $tg = l_{g,t}t_{g^*} = t_{g^*}$ segue $g = 1$. È così provato che μ è un monomorfismo.

Vogliamo ora provare che ρ è simile alla rappresentazione permutazionale indotta per restrizione da $\rho_2 \operatorname{Wr} \rho_1$ sull'immagine G^μ di μ. L'insieme su cui G^μ agisce tramite $\rho_2 \operatorname{Wr} \rho_1$ è $\Omega := Y \times \bar{X}$. Definiamo un'applicazione $f : X \longrightarrow \Omega$ come segue: ad ogni $x \in X$ associamo (xt^{-1}, Yt), dove t è l'unico elemento di T tale che $x \in Yt$. Si verifica subito che f è una biezione: l'inversa di f è l'applicazione $(y, Yt) \in \Omega \mapsto yt \in X$. Ovviamente $\alpha : g \in G \mapsto g^\mu \in G^\mu$ è un isomorfismo; per verificare che (α, f) determina una similitudine basta dunque provare $g^\rho f = fg^{\mu(\rho_2 \operatorname{Wr}\rho_1)}$ per ogni $g \in G$. A questo scopo, sia $x \in X$. Allora, posto $(y, Yt) = xf$ (quindi $x = yt$), abbiamo

$$xfg^{\mu(\rho_2 \operatorname{Wr}\rho_1)} = (y, Yt)\big((l_{g,i})_{Yi\in\bar{X}}\,\bar{g}\big)^{\rho_2 \operatorname{Wr}\rho_1} = (yl_{g,t}, Ytg) = (yl_{g,t}, Yt_{g^*}).$$

D'altro canto $xg^\rho \in Ytg = Yt_{g^*}$ e quindi $xg^\rho f = (xg(t_{g^*})^{-1}, Yt_{g^*}) = (ytg(t_{g^*})^{-1}, Yt_{g^*}) = (yl_{g,t}, Yt_{g^*})$. Otteniamo così l'asserto. ❑

I casi più interessanti del teorema appena provato sono quelli in cui $N = 1$ oppure $N = L_G$. Applicando il teorema con $N = 1$ otteniamo infatti questo elegante risultato: se si 'decompone' una rappresentazione permutazionale transitiva ρ (nel senso di 5.12) e si effettua poi il prodotto intrecciato tra le rappresentazioni ottenute, ciò che si ricava è, a meno di similitudini, un prolungamento di ρ. La scelta $N = L_G$ è invece quella (generalmente) più conveniente se il Teorema 5.18 viene utilizzato per ottenere informazioni dirette su ρ o su G (come nel caso del prossimo corollario), infatti in questo caso il prodotto intrecciato $L \operatorname{Wr} (G/N)$, con un sottogruppo del quale G si può identificare, è il più 'piccolo' possibile.

5.19. Corollario. *Siano G un gruppo e H un sottogruppo di G. Allora G è isomorfo ad un sottogruppo del prodotto intrecciato $H \operatorname{Wr} (G/H_G)$ rispetto all'azione di G/H_G sui laterali destri di H.*

Dimostrazione — Si consideri la rappresentazione regolare destra δ di G. Rispetto ad essa H è un blocco di imprimitività (cfr. esercizio 6 a p. 23). Ovviamente $\mathrm{St}^*_\delta(G) = H$. Il sistema di imprimitività determinato da H è l'insieme dei laterali destri di H in G, e l'azione indotta da δ su esso è, come si verifica immediatamente, la consueta azione per moltiplicazione destra. L'asserto segue ora da 5.18, applicato ponendo $N = H_G$. ❑

Nell'ipotesi aggiuntiva che H sia normale in G, il precedente corollario ci dice che G è isomorfo ad un sottogruppo del prodotto intrecciato standard tra H e G/H.

Esercizi. Con le notazioni adottate nelle pagine precedenti:

1. Calcolare il nucleo di $\rho \operatorname{Wr} \varphi$.
2. Se $|Y| = 1$ allora $\rho \operatorname{Wr} \varphi$ è simile a ρ. Se $|X| = 1$ è necessariamente $\rho \operatorname{Wr} \varphi$ simile a φ?
3. $\rho \operatorname{Wr} \varphi$ è semiregolare se e solo se o $|Y| = 1$ e ρ è semiregolare oppure $|H| = 1$ e φ è semiregolare.
4. Provare che il prodotto intrecciato standard tra due gruppi di ordine 2 è isomorfo al gruppo diedrale di ordine 8.
5. Il gruppo G di permutazioni su due rette parallele presentato nell'Esempio 5.13 è simile al prodotto intrecciato standard di $(\mathbb{R}, +)$ per il gruppo di ordine 2.

6. Teoremi di classificazione

In questa sezione vengono riportati teoremi che descrivono la struttura di alcuni tipi di gruppi di permutazione. Iniziamo col raccogliere alcuni risultati elementari dalla teoria dei gruppi abeliani.

Gruppi additivi di spazi vettoriali

Come è ben noto dai corsi di algebra, il gruppo additivo di uno spazio vettoriale è isomorfo ad una somma diretta di copie del gruppo additivo razionale $\mathbb{Q}$ se il campo degli scalari ha caratteristica 0, ad una somma diretta di gruppi di ordine p se invece la caratteristica del campo degli scalari è il numero primo p. Viceversa, ogni somma diretta del tipo indicato è isomorfo al gruppo additivo di uno spazio vettoriale o sul campo razionale o sul campo di ordine p, a seconda del caso. Una somma diretta di gruppi di ordine primo p si chiama anche *p-gruppo abeliano elementare*. I gruppi additivi degli spazi vettoriali svolgono un ruolo importante nelle descrizione di alcuni tipi di rappresentazioni permutazionali; lo scopo di questa sottosezione è quello di discuterne alcune proprietà e di individuare condizioni sufficienti affinché un gruppo abeliano sia di questo genere.

Sia A un gruppo abeliano (indicato con notazione additiva). Per ogni $n \in \mathbb{Z}$ l'applicazione $\varepsilon_n : a \in A \mapsto na \in A$ è un endomorfismo di A. Allora

$$A[n] := \ker \varepsilon_n = \{a \in A \mid na = 0\} \qquad \text{e} \qquad nA := \operatorname{im} \varepsilon_n = \{na \mid a \in A\}$$

sono due sottogruppi di A. Si tratta, come è piuttosto evidente, di sottogruppi caratteristici di A. Se vale $nA = A$ per ogni intero n diverso da 0 si dice che A è un gruppo *divisibile*. Questo significa che, per ogni $a \in A$ e per ogni $n \in \mathbb{Z}$ tale che $n \neq 0$ esiste $b \in A$ tale che $a = nb$ (il che giustifica il nome dato a tali gruppi). Ricordiamo anche che un gruppo è *senza torsione* se e solo se ogni suo elemento non identico è aperiodico.

6.1. *Siano A un gruppo abeliano e p un numero primo. Allora:*
(i) A è un p-gruppo abeliano elementare se e solo se $A[p] = 0$ (cioè: se e solo se $pa = 0$ per ogni $a \in A$).
(ii) A è isomorfo ad una somma diretta di copie di $\mathbb{Q}$ se e solo se A è divisibile e senza torsione.

Dimostrazione — Il fatto che $A[p] = 0$ se A è un p-gruppo abeliano elementare è del tutto ovvio. Viceversa, supponiamo che A sia un gruppo abeliano tale che $A[p] = 0$. Per ogni $a \in A$, se n e m sono due numeri interi congrui modulo p si ha $na = ma$, quindi è possibile definire in modo non ambiguo il prodotto $\bar{n}a := na$ dove $\bar{n}$ indica la classe di resto di n modulo p. Una facile verifica diretta mostra che il prodotto esterno così definito dà luogo ad una struttura di $\mathbb{Z}_p$-spazio vettoriale su A. Ciò prova (i).

Veniamo a (ii). Sia $A = \bigoplus_{i\in I} \mathbb{Q}$ una somma diretta di copie del gruppo additivo razionale. Allora possiamo rappresentare ogni elemento a di A come una famiglia di numeri razionali: $a = (a_i)_{i\in I}$. Per ogni intero non nullo n si ha $na = (na_i)_{i\in I}$, che è zero se e solo se $a = 0$ (dunque ogni elemento non identico di A è aperiodico, ovvero: A è senza torsione) e $a = nb$ dove $b = (a_i/n)_{i\in I} \in A$, il che prova che A è divisibile. Viceversa, se A è un gruppo abeliano divisibile senza torsione, si può dotare A di una struttura di spazio vettoriale sul campo razionale. Per fare ciò verifichiamo che, per ogni $a \in A$ e per ogni $q \in \mathbb{Q}$, scritto q come r/s con r e s interi, esiste un unico $b \in A$ tale che $ra = sb$ (e tale b non dipende dalla scelta degli interi r e s il rapporto tra i quali è q). L'esistenza di b è rapidamente verificata: poiché A è divisibile $sA = A$, quindi $ra \in sA$. Per quanto riguarda l'unicità, supponiamo $ra = sb$ e $r'a = s'b'$ con $b' \in A$, $r', s' \in \mathbb{Z}$, $s' \neq 0$ e $q = r'/s'$. Allora $rr'a = sr'b$ (come segue da $ra = sb$) e $rr'a = rs'b'$ (come segue da $r'a = s'b'$), dunque $sr'b = rs'b'$. Dal momento che $sr' = rs'$ ciò implica $sr'(b - b') = 0$. Poiché A è senza torsione, o $sr' = 0$ oppure $b - b' = 0$. Nel secondo caso $b = b'$; nel primo caso $r' = 0$ (perché $s \neq 0$) e quindi anche $r = q = 0$, sicché $s'b' = sb = 0$ e quindi $b' = 0 = b$, ancora perché A è senza torsione. Essendo così provata l'unicità di b possiamo definire un prodotto esterno $\mathbb{Q} \times A \to A$: per ogni $q \in \mathbb{Q}$ e $a \in A$ poniamo $qa = b$ dove b è l'elemento di A determinato come sopra. Questo prodotto definisce una struttura di $\mathbb{Q}$-spazio vettoriale su A. Infatti, se $a \in A$ è chiaro che $1a = a$. Verifichiamo poi che se $q_1, q_2 \in \mathbb{Q}$ si ha $(q_1 + q_2)a = q_1a + q_2a$. Per opportuni $r_1, r_2, s \in \mathbb{Z}$ abbiamo $q_1 = r_1/s$ e $q_2 = r_2/s$, quindi $q_1 + q_2 = (r_1 + r_2)/s$ e $b := (q_1 + q_2)a$ è definito dall'essere $sb = (r_1 + r_2)a$. La definizione dei prodotti q_ia fornisce $s(q_ia) = r_ia$, quindi $s(q_1a + q_2a) = s(q_1a) + s(q_2a) = r_1a + r_2a = (r_1 + r_2)a$, sicché $b = q_1a + q_2a$, come si voleva. In modo analogo si dimostrano le uguaglianze $q_1(a_1 + a_2) = q_1a_1 + q_1a_2$ e $q_1(q_2a_1) = (q_1q_2)a_1$ per ogni $a_1, a_2 \in A$ e $q_1, q_2 \in \mathbb{Q}$. Pertanto A è il gruppo additivo di un $\mathbb{Q}$-spazio vettoriale, dunque A è somma diretta di copie del gruppo additivo di $\mathbb{Q}$. ❑

Endomorfismi ed automorfismi dei gruppi descritti nel precedente teorema coincidono con quelli dei corrispondenti spazi vettoriali.

6.2. *Sia V_+ il gruppo additivo di uno spazio vettoriale V su campo K, dove $K = \mathbb{Z}_p$ o $K = \mathbb{Q}$. Allora gli endomorfismi (risp. automorfismi) di V_+ sono precisamente gli endomorfismi (risp. automorfismi) dello spazio vettoriale V.*

Dimostrazione — Gli endomorfismi (risp. automorfismi) di V sono precisamente gli endomorfismi (risp. automorfismi) di V_+ che sono anche compatibili con il prodotto esterno per elementi di K. Si tratta quindi di verificare che ogni endomorfismo di V_+ è K-lineare, cioè $(ka)^\varepsilon = ka^\varepsilon$ per ogni $k \in K$, $a \in A$ e $\varepsilon \in \operatorname{End} V_+$. Se $K = \mathbb{Z}_p$, allora $k = \bar{n} = n + p\mathbb{Z}$ per un opportuno intero n, e $(\bar{n}a)^\varepsilon = (na)^\varepsilon = na^\varepsilon = \bar{n}a^\varepsilon$, come si voleva. Se invece $K = \mathbb{Q}$, allora $k = n/m$ per opportuni interi n ed m, allora $m(ka)^\varepsilon = (mka)^\varepsilon = (na)^\varepsilon = na^\varepsilon$ da cui segue $(ka)^\varepsilon = (1/m)na^\varepsilon = ka^\varepsilon$. ❑

Ci sarà utile il fatto che i gruppi additivi degli spazi vettoriali non nulli sono precisamente i gruppi abeliani che appaiono come sottogruppo normale minimale di qualche gruppo. Se G è un gruppo e N è un suo sottogruppo normale minimale, allora $(1 \neq) N$ non ha sottogruppi caratteristici non banali, vale a dire, N è *caratteristicamente semplice* (infatti, se M è un sottogruppo caratteristico di N allora $M \lhd G$, quindi $M = 1$ o $M = N$). Il prossimo esercizio 2 mostra come questa affermazione si può invertire. Basta allora descrivere i gruppi abeliani caratteristicamente semplici.

6.3. *Un gruppo abeliano A è caratteristicamente semplice se e solo se è isomorfo al gruppo additivo di uno spazio vettoriale non nullo.*

Dimostrazione — Sia A caratteristicamente semplice, quindi, in particolare, $A \neq 0$. Per determinare la struttura di A distinguiamo due casi. Se A è senza torsione, allora $nA \neq 0$ per ogni intero $n \neq 0$. Essendo ciascun nA un sottogruppo caratteristico di A da ciò segue $nA = A$ per ogni $n \neq 0$, sicché A è divisibile. Per 6.1 (ii) allora A è isomorfo al gruppo additivo di uno spazio vettoriale su $\mathbb{Q}$. Se invece A non è senza torsione, allora A possiede un elemento periodico diverso da zero, e quindi un elemento di periodo un numero primo p, dunque $A[p] \neq 0$. Poiché $A[p]$ è caratteristico in A, questo significa $A[p] = A$, quindi A è un p-gruppo abeliano elementare, per 6.1 (i). Concludiamo così che, in ciascuno dei due casi, A è isomorfo al gruppo additivo di uno spazio vettoriale.

Viceversa, il gruppo additivo di uno spazio vettoriale non nullo V è sempre caratteristicamente semplice. Sia infatti H un sottogruppo non banale di V_+, il gruppo additivo di V. Allora esistono $a \in H \smallsetminus \{0\}$ e $b \in V \smallsetminus H$. Sappiamo dall'algebra lineare elementare che l'automorfo di V agisce in modo transitivo su $V \smallsetminus \{0\}$, dunque esiste un automorfismo α di V tale che $a^\alpha = b$, sicché $H^\alpha \neq H$. Ma α è anche un automorfismo di V_+, quindi H non è caratteristico in V. ❑

6.4. Corollario. *Sia N un sottogruppo normale minimale abeliano di un gruppo G. Allora N è o un p-gruppo abeliano elementare per un primo p oppure una somma diretta di copie del gruppo additivo razionale.*

Esercizi.

1. Sia A un gruppo abeliano. Provare che A è divisibile se e solo se $pA = A$ per ogni numero primo p. Per un fissato primo p, provare che A è un p-gruppo abeliano elementare se e solo se $pA = 0$.
2. Ogni gruppo caratteristicamente semplice N è un sottogruppo normale minimale di un gruppo. [*Suggerimento: si consideri l'olomorfo di N, che viene definito nelle prossime pagine.*]

Sottogruppi normali regolari

Lo studio dei gruppi di permutazione e delle rappresentazioni permutazionali è semplificato dalla eventuale presenza di sottogruppi regolari, particolarmente se normali. Questi permettono una efficace descrizione sia della struttura del gruppo stesso che della sua azione permutazionale, descrizione basata su una decomposizione del gruppo in prodotto semidiretto e sull'azione permutazionale che andiamo a definire.

Sia dato un prodotto semidiretto di gruppi $G = N \rtimes H$. Conosciamo una rappresentazione permutazionale di H su N: quella per coniugio, chiamiamola θ, ed una di N su N: quella regolare destra, chiamiamola δ. È possibile definire una rappresentazione permutazionale di G che prolunghi simultaneamente δ e θ.

6.5. *Con le notazioni appena stabilite, l'applicazione φ che all'elemento ah di G (con $a \in N$ e $h \in H$) associa $a^\delta h^\theta \in Sym\, N$ è una rappresentazione permutazionale rispetto alla quale N è un sottogruppo normale regolare.*

Dimostrazione — Siano $a \in N$ e $h \in H$. Per ogni $x \in N$, l'immagine di x mediante $(a^\delta)^{h^\theta} = (h^\theta)^{-1} a^\delta h^\theta$ è $\left(x^{h^{-1}} a\right)^h = xa^h = x(a^h)^\delta$, dunque $(a^\delta)^{h^\theta} = (a^h)^\delta$. Allora φ è un omomorfismo per 5.16. La restrizione di φ a N è δ, dunque N è normale regolare rispetto a φ. ❑

Più esplicitamente, l'azione di G su N è data da $x*(ah) = (xa)^h$ (o, se si preferisce questa forma, da $x*(ha) = x^h a$) per ogni $x, a \in N$ e $h \in H$. Chiamiamo (N,H)-*rappresentazione* di G la rappresentazione permutazionale così definita. Il prossimo teorema mostra che, a meno di equivalenze, ogni rappresentazione permutazionale rispetto alla quale esista un sottogruppo normale regolare è di questo tipo.

6.6. Teorema. *Sia data una rappresentazione permutazionale ρ del gruppo G su un insieme X. Sia N un sottogruppo normale regolare di G e sia $H = \mathrm{St}_\rho(x)$ per un elemento $x \in X$. Allora $G = N \rtimes H$ e ρ è equivalente alla (N,H)-rappresentazione di G. Il nucleo di ρ è $C_H(N)$.*

Dimostrazione — La transitività di N implica $G = NH$ per 1.10; poiché poi N è regolare $N \cap H = \mathrm{St}_N(x) = 1$, sicché $G = N \rtimes H$. La regolarità di N assicura che l'applicazione $f : a \in N \mapsto xa^\rho \in X$ è biettiva (esercizio 6, p. 2). Verifichiamo che f determina una equivalenza da φ, la (N,H)-rappresentazione di G, a ρ. Dobbiamo provare $g^\varphi f = f g^\rho$ per ogni $g \in G$. Posto $g = ah$, con $a \in N$ e $h \in H$, per ogni $n \in N$ si ha

$$ng^\varphi f = x\left(ng^\varphi\right)^\rho = x\left((na)^h\right)^\rho = x(h^{-1}nah)^\rho = x(nah)^\rho = xn^\rho g^\rho = nfg^\rho,$$

avendo sfruttato il fatto che $h^{-\rho}$ fissa x. Dunque $g^\varphi f = fg^\rho$, come desiderato, e ρ e φ sono equivalenti.

Infine $\ker\rho = \mathrm{St}_\rho(X)$ è certamente contenuto in $H = \mathrm{St}_\rho(x)$, quindi $\ker\rho$ è lo stabilizzante di X in H (rispetto all'azione indotta da ρ). Per quanto appena provato questo è lo stabilizzante di N rispetto all'azione per coniugio di H, cioè $C_H(N)$. ❑

Un esempio di gruppo di permutazioni con la struttura descritta in 6.6 è $\mathbb{S}_4$. Infatti $\mathbb{S}_4$ ha un sottogruppo normale regolare $V = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$; lo stabilizzante di 4 è il sottogruppo $H = \langle (1\,2), (1\,2\,3)\rangle \simeq \mathbb{S}_3$ e $\mathbb{S}_4 = V \rtimes H$, dove H agisce per coniugio sugli elementi di V permutando tra loro i tre elementi non identici e fissando l'identità (di fatto $H \simeq \mathrm{Aut}\, V$).

Interpretiamo quanto provato in 6.6 nel caso particolare dei gruppi di permutazioni (o, che è lo stesso, delle rappresentazioni permutazionali fedeli). Se un gruppo G agisce in modo fedele su un insieme X e N ne è un sottogruppo normale regolare, allora $G = N \rtimes H$, dove H è lo stabilizzante di un punto e, a meno di similitudini, possiamo identificare X con N e G con l'immagine in $Sym\, N$ della (N,H)-rappresentazione di G, cioè con $N^\delta \rtimes H^\theta$, nelle notazioni di 6.5. Definiamo l'*olomorfo* di N come il prodotto semidiretto $\mathrm{Hol}\, N := N \rtimes \mathrm{Aut}\, N$ (con ovvia azione di coniugio di $\mathrm{Aut}\, N$ su N). L'azione di $\mathrm{Hol}\, N$ su N (cioè la sua $(N, \mathrm{Aut}\, N)$-rappresentazione) è fedele per 6.6 (infatti il centralizzante in $\mathrm{Aut}\, N$ di N è il sottogruppo identico), dunque, per quanto appena detto, $\mathrm{Hol}\, N$ è simile al sottogruppo $N^\delta \rtimes \mathrm{Aut}\, N$ di $Sym\, N$, che contiene $N^\delta \rtimes \Gamma$. Pertanto l'azione di G su X si può identificare, a meno di similitudini, con l'azione su N di un sottogruppo di $\mathrm{Hol}\, N$ della forma $N \rtimes \Gamma$, per un opportuno $\Gamma \leq \mathrm{Aut}\, N$. Isoliamo un caso particolarmente rilevante.

6.7. Esempio. Un importante esempio di gruppo di permutazioni con sottogruppo normale regolare abeliano non identico è il *gruppo affine* su uno spazio vettoriale. Sia V uno spazio vettoriale su un campo K. Detto V_+ il gruppo additivo di V, possiamo considerare il sottogruppo $V_+ \rtimes \mathrm{Aut}\, V$ di $\mathrm{Hol}\, V_+$, dove $\mathrm{Aut}\, V$ è il gruppo degli automorfismi dello spazio vettoriale V (ovviamente $\mathrm{Aut}\, V \leq \mathrm{Aut}\, V_+$). Se δ è la rappresentazione regolare destra di V_+, l'immagine della rappresentazione di $V \rtimes \mathrm{Aut}\, V$ su V è $V^\delta \rtimes \mathrm{Aut}\, V$, che prende il nome di *gruppo affine* su V e viene indicato con $\mathrm{Aff}(V)$. È evidente la connessione geometrica: gli elementi di $\mathrm{Aff}(V)$ sono precisamente le affinità dello spazio affine su V. Queste formano un sottogruppo (eventualmente proprio) del gruppo degli automorfismi (o collineazioni) affini su V. Per ogni $v \in V$ l'affinità v^δ è la traslazione di ampiezza v, dunque V^δ, il cayleyano di V_+, è il gruppo $T(V)$ delle traslazioni di V e $\mathrm{Aff}(V) = T(V) \rtimes \mathrm{Aut}\, V$.

Ovviamente $\mathrm{Aff}(V)$ è un gruppo 2-transitivo, in quanto $T(V)$ è transitivo e lo stabilizzante di 0 in $\mathrm{Aff}(V)$ è $\mathrm{Aut}\, V$, che agisce transitivamente su $V^\# = V \setminus \{0\}$. Se V ha dimensione 1 (e solo in questo caso), allora $\mathrm{Aff}(V)$ è strettamente 2-transitivo, dal momento che $\mathrm{Aut}\, V$ consiste delle applicazioni $\sigma_k : v \in V \mapsto vk \in V$ al variare di k in $K^* = K \setminus \{0\}$ ed opera quindi in modo regolare su $V^\#$.

Come si vedrà, i gruppi affini costituiscono un importante riferimento per la classificazione di alcuni tipi di gruppi di permutazioni. Raccogliamo alcune semplici ma utili osservazioni che mostrano in quale modo i gruppi affini possono apparire in tali contesti.

6.8. Osservazione. Come abbiamo visto, se N è o un p-gruppo abeliano elementare per un primo p oppure una somma diretta di copie del gruppo additivo razionale, è possibile dotare N di una struttura di spazio vettoriale, diciamolo V, rispettivamente sul campo $\mathbb{Z}_p$ o su $\mathbb{Q}$, e si ha $\operatorname{Aut} V = \operatorname{Aut} N$ (vedi 6.2). Da ciò segue subito che la rappresentazione permutazionale di $\operatorname{Hol} N$ su N è simile a quella naturale di $\operatorname{Aff}(V)$.

Per brevità diremo che un gruppo di permutazioni G è *di tipo affine su* N se e solo se G è simile ad un sottogruppo di $\operatorname{Aff}(V)$ contenente il gruppo delle traslazioni. I sottogruppi di questo tipo sono precisamente quelli della forma $T(V) \rtimes \Gamma$ con $\Gamma \leq \operatorname{Aut} V$. Infatti la legge modulare di Dedekind (cfr. [Rob], 1.3.14) implica che se $T(V) \leq H \leq \operatorname{Aff}(V)$ allora $H = T(V) \operatorname{Aut} V \cap H = T(V) \rtimes (\operatorname{Aut} V \cap H)$. Un tale sottogruppo è necessariamente transitivo, dal momento che $T(V)$ è transitivo.

In conclusione, sempre nell'ipotesi che N sia o un p-gruppo abeliano elementare per un primo p oppure una somma diretta di copie del gruppo additivo razionale, se N è un sottogruppo normale regolare di un gruppo G di permutazioni 6.6 e le considerazioni che seguono assicurano che G è di tipo affine su N. In particolare, se N è finito allora G avrà grado finito potenza del primo p.

Tornando al caso generale, il Teorema 6.6 mostra quanto sia rilevante la descrizione dei gruppi di automorfismi come gruppi di permutazioni per lo studio delle rappresentazioni permutazionali con sottogruppi normali regolari. Dal momento che $\operatorname{Aut} N$ stabilizza $1 \in N$, per ogni gruppo N, siamo particolarmente interessati all'azione di $\operatorname{Aut} N$ su $N \smallsetminus \{1\}$. Nel caso finito, per quanto concerne la transitività, e la transitività multipla in particolare, abbiamo questo risultato, per dimostrazione del quale si rimanda a [Rob], 7.2.8. Per una sua inversione si veda il prossimo esercizio 3.

6.9. *Siano N un gruppo finito e $k \in \mathbb{N}$. Supponiamo che l'azione di $\operatorname{Aut} N$ su $N \smallsetminus \{1\}$ sia k-transitiva. Allora $k \leq 3$ e:*
(*i*) *se $k = 1$, allora N è un p-gruppo abeliano elementare, per qualche numero primo p;*
(*ii*) *se $k = 2$, allora $|N| = 3$ oppure N è un 2-gruppo abeliano elementare;*
(*iii*) *se $k = 3$, allora N è isomorfo al gruppo quadrinomio V_4.*

La parte (*i*) di questo enunciato non si estende ad arbitrari gruppi infiniti. Ad esempio, esistono gruppi infiniti dalla struttura molto complicata (sembra un gioco di parole, ma ovviamente si tratta di gruppi semplici) in cui il gruppo degli automorfismi interni opera transitivamente sull'insieme degli elementi non identici. Sono invece generalizzabili a gruppi arbitrari le parti (*ii*) e (*iii*) (vedi il prossimo esercizio 4).

6.10. Corollario. *Siano k un intero maggiore di 1 e ρ una rappresentazione permutazionale k-transitiva di un gruppo G su un insieme finito X. Supponiamo che G abbia un sottogruppo normale regolare N. Allora $k \leq 4$ e:*
(*i*) *se $k = 2$, allora N è un p-gruppo abeliano elementare per qualche numero primo p e $|X| = |N|$ è una potenza di p;*
(*ii*) *se $k = 3$, allora $|N| = 3$ oppure N è un 2-gruppo abeliano elementare, dunque o $|X| = 3$ e $\operatorname{im}\rho = Sym\, X$ oppure $|X|$ è una potenza di 2;*
(*iii*) *se $k = 4$, allora $|X| = 4$, $\operatorname{im}\rho = Sym\, X$ e N è isomorfo al gruppo quadrinomio V_4.*

Dimostrazione — Dall'ipotesi e da 6.6 segue $\operatorname{im}\rho = N^\delta \rtimes \Gamma$ (dove N^δ è il cayleyano destro di N) per un opportuno $\Gamma \leq \operatorname{Aut} G$, la cui azione è $(k-1)$-transitiva su $N \smallsetminus \{1\}$ dal momento che $\Gamma = \operatorname{St}_{\operatorname{im}\rho}(1)$. Allora il risultato segue da 6.9, tenendo in conto che $|X| = |N|$ per 1.1 (*iv*) e che, se $k = |X|$, allora $\operatorname{im}\rho = Sym\, X$ per 4.3. ❑

Esercizi.

1. Se il gruppo di permutazioni G possiede un sottogruppo regolare R (non necessariamente normale), allora $G = HR = RH$ e $R \cap H = 1$ per ogni H stabilizzante di un punto.
2. I gruppi $\mathbb{S}_3$ e $\mathbb{S}_4$ sono simili rispettivamente all'olomorfo del gruppo di ordine 3 ed all'olomorfo del gruppo quadrinomio V_4.
3. Siano p un numero primo ed N un p-gruppo abeliano elementare (non necessariamente finito). Allora $\operatorname{Aut} N$ opera in modo transitivo su $N \smallsetminus \{1\}$. Se $|N| = 3$ oppure $p = 2 < |N|$ questa azione di $\operatorname{Aut} N$ è 2-transitiva; se $N \simeq V_4$ allora $\operatorname{Aut} N$ è 3-transitivo.
4. Se N è un gruppo e $\operatorname{Aut} N$ agisce in modo primitivo su $N \smallsetminus \{1\}$, allora $|G| = 3$ oppure G è un 2-gruppo abeliano elementare. [*Suggerimento: per ogni $a \in N \smallsetminus \{1\}$ l'insieme $\{a, a^{-1}\}$ è un blocco di imprimitività.*] Osservare come ciò implichi la validità della parte (*ii*), e quindi della (*iii*), di 6.9 anche per gruppi infiniti.
5. Sia N un gruppo e sia N^δ il cayleyano destro di N. Il centralizzante in $Sym\, N$ di N^δ è l'immagine della rappresentazione regolare sinistra di N, (detto *cayleyano sinistro* di N, cfr. [Rob], p. 35). Inoltre il normalizzante di N^δ in $Sym\, N$ è $N^\delta \rtimes \operatorname{Aut} N$, gruppo simile a $\operatorname{Hol} N$.

Alcuni gruppi primitivi

Iniziamo con una utile conseguenza della legge modulare di Dedekind.

6.11. *Sia G un gruppo e sia $H \leq K \leq G$. Fissato un sottogruppo $L \leq G$ si ha $H = K$ se e solo se $HL = KL$ e $H \cap L = K \cap L$.*

Dimostrazione — Per la legge modulare di Dedekind da $HL = KL$ e $H \cap L = K \cap L$ segue $K = KL \cap K = HL \cap K = H(L \cap K) = H(L \cap H) = H$. L'altra implicazione è ovvia. ❑

6.12. *Sia $G = N \rtimes H$ un gruppo, e si supponga N abeliano. Allora H è un sottogruppo massimale di G se e solo se N ne è un sottogruppo normale minimale.*

Dimostrazione — Sia H massimale in G e sia M un sottogruppo normale di G tale che $1 \neq M \leq N$. Allora $M \cap H = 1$ e quindi $M \not\leq H$. Per la massimalità di H e poiché $M \lhd G$ si ha $G = \langle M, H \rangle = MH$ e quindi $MH = NH$, oltre che $M \cap H = N \cap H$, dunque $M = N$ per 6.11. Pertanto N è normale minimale. Sia, viceversa, N normale minimale in G e sia $H \leq K \leq G$. Ovviamente $NK = NH = G$; inoltre $N \cap K \lhd K$ e $N \cap K \lhd N$ perché N è abeliano. Allora $N \cap K$ è normale in $G = NK$ e, per la minimalità di N, si ha $N \cap K = 1$ oppure $N \cap K = N$. Nel primo caso $N \cap K = N \cap H$ e quindi $K = H$ per 6.11. Nel secondo caso $K \geq N \cup H$, quindi $K = G$. Ciò prova che H è massimale in G. ❑

6.13. Teorema. *Sia G un gruppo primitivo di permutazioni su un insieme X. Se G contiene un sottogruppo abeliano normale $N \neq 1$, allora N è regolare nonché normale minimale in G, e G è di tipo affine su N. Se G è finito il suo grado $|N|$ è potenza di un primo.*

Dimostrazione — Sappiamo da 5.3 che N è transitivo, dunque regolare per 1.3. Allora, per 6.6, si ha $G = N \rtimes H$ dove H è lo stabilizzante di un elemento di X; da 5.9 segue che H è massimale in G e quindi N è normale minimale per 6.12. L'asserto segue ora 6.4 e dalle osservazioni svolte in 6.8. ❑

6.14. Corollario. *Ogni gruppo risolubile primitivo di permutazioni è di tipo affine su un suo sottogruppo normale minimale.*

Inversamente, se V è uno spazio vettoriale e $\Gamma \leq \operatorname{Aut} V$, allora il sottogruppo $G = T(V) \rtimes \Gamma$ di $\operatorname{Aff}(V)$, ovviamente transitivo, è primitivo se e solo se Γ, che è $\operatorname{St}_G(0)$, è un sottogruppo massimale di G (per 5.9) ovvero (per 6.12) se e solo se $T(V)$ è normale minimale. Inoltre G è 2-transitivo se e solo se Γ agisce in modo transitivo su $V \smallsetminus \{0\}$. Ciò permette di costruire facili esempi di gruppi primitivi che non sono 2-transitivi.

Esercizi.

1. Il gruppo diedrale di ordine 10 è isomorfo ad un sottogruppo primitivo non 2-transitivo di $\operatorname{Aff}(V)$, dove V è uno spazio vettoriale di dimensione 1 su $\mathbb{Z}_5$.
2. Per una delle due implicazioni in 6.12 (quella utilizzata in 6.13) non è necessario supporre che N sia abeliano: se H è massimale nel prodotto semidiretto $N \rtimes H$ allora N è ivi normale minimale.

Lo zoccolo di un gruppo primitivo

Se G è un gruppo si chiama *zoccolo* di G (e si scrive $\operatorname{Soc}(G)$) il sottogruppo generato dai sottogruppi normali minimali di G. Lo zoccolo di G può essere il sottogruppo identico anche se G stesso non è identico (ad esempio, quando G è ciclico infinito), ma ciò non accade se G è finito. Se infatti G è finito e non identico allora l'insieme dei sottogruppi normali non identici di G è un insieme finito non vuoto, dunque (ordinato per inclusione) ha elementi minimali; vale a dire: G possiede sottogruppi normali minimali e quindi $\operatorname{Soc}(G) \neq 1$.

Se (e solo se) l'intersezione dei sottogruppi normali non identici di un gruppo G non è identico, allora questa è il *minimo* sottogruppo normale non identico di G. Nel caso esista, quest'ultimo si chiama *monolite* di G, e coincide anche con $\operatorname{Soc}(G)$. Ad esempio, se G è un p-gruppo ciclico non identico il sottogruppo di ordine p in G è il monolite di G; il centro del gruppo diedrale D_8 di ordine 8 è il monolite di D_8; invece V_4 non possiede monolite.

Le nozioni di zoccolo e monolite sono rilevanti per la teoria generale dei gruppi primitivi (specialmente di quelli finiti). Ad esempio, l'enunciato del Teorema 6.13 può essere completato osservando che, valendo le ipotesi, N è il monolite di G (come segue da 6.17 o anche dal prossimo esercizio 3). In effetti la teoria dei gruppi primitivi finiti è in larga parte basata sulla descrizione del loro zoccolo (che è abbastanza facile) e, viceversa, su come si possa esplicitare la struttura e (almeno parzialmente) l'azione del gruppo in termini del suo zoccolo (il che è molto più complicato).

Due facili lemmi vengono usati nella dimostrazione del primo risultato, che mostra in particolare che un gruppo primitivo contiene al più due sottogruppi normali minimali.

6.15. *Sia Γ un gruppo transitivo di permutazioni su un insieme non vuoto X. Allora $C_{Sym\, X}(\Gamma)$ è semiregolare.*

Dimostrazione — Siano $x \in X$ e $c \in C_{Sym\, X}(\Gamma)$. Se c stabilizza x, per ogni $\gamma \in \Gamma$ si ha $(x\gamma)c = x(\gamma c) = x(c\gamma) = (xc)\gamma = x\gamma$, dunque c stabilizza la Γ-orbita di x, cioè X. Allora $c = 1$. Ciò prova che $C_{Sym\, X}(\Gamma)$ è semiregolare. ❑

6.16. *Sia Γ un gruppo regolare di permutazioni. Allora Γ non ha sottogruppi propri transitivi.*

Dimostrazione — Sia Δ un sottogruppo transitivo di Γ. Allora, per 1.10, si ha $\Gamma = \Delta H$ dove H è lo stabilizzante di un punto in Γ. Ma $H = 1$ perché Γ è regolare, dunque $\Gamma = \Delta$. ❑

6.17. *Sia N un sottogruppo normale minimale del gruppo primitivo di permutazioni G. Allora o N è il monolite di G oppure G ha esattamente un sottogruppo normale non identico M non contenente N e si ha:*

(*i*) *N e M sono i soli sottogruppi normali minimali di G, dunque* $\mathrm{Soc}(G) = N \times M$;

(*ii*) *esiste una similitudine tra G ed un gruppo di permutazioni su N, tramite la quale ad N e M corrispondono rispettivamente il cayleyano destro ed il cayleyano sinistro di N;*

(*iii*) *N e M sono regolari e isomorfi tra loro, il loro centro è identico e $M = C_G(N)$.*

Dimostrazione — Se N non è il monolite di G esiste in G un sottogruppo normale $M \neq 1$ tale che $N \not\leq M$. Allora $M \cap N$ è un sottogruppo normale di G propriamente contenuto in N, quindi il sottogruppo identico. Da ciò segue $NM = N \times M$, sicché M ed N si centralizzano. Essendo M transitivo per 5.3, da 6.15 si deduce che N è regolare. Esiste allora una similitudine tra G ed un gruppo di permutazioni su N tramite la quale ad N corrisponde il cayleyano destro N^δ di N. Poiché $M \leq C_G(N)$, ad M corrisponde un sottogruppo del centralizzante di N^δ, che è il cayleyano sinistro N^λ di N (vedi esercizio 5 a p. 31). Siccome N^λ non contiene sottogruppi propri transitivi per 6.16, allora ad M corrisponde proprio N^λ, sicché $M = C_G(N)$. Ciò prova (*ii*) nonché il fatto che M è l'unico sottogruppo normale non identico di G in cui N non sia contenuto, dalla qual cosa segue (*i*). Inoltre sia N che M sono regolari; essendo $N \simeq N^\lambda$ certamente $N \simeq M$. Infine $Z(N) = N \cap C_G(N) = N \cap M = 1$. Con questo è completata la dimostrazione dell'enunciato. ❑

Con le notazioni del precedente enunciato, se N è abeliano N è il monolite di G, non potendo valere nel caso opposto la condizione (*iii*). Ciò completa, come si diceva sopra, l'enunciato del Teorema 6.13.

È noto che un gruppo finito caratteristicamente semplice è prodotto diretto di gruppi semplici tra loro isomorfi. Quindi, se G è un gruppo finito primitivo non identico, $\mathrm{Soc}(G)$, che è o un sottogruppo normale minimale o il prodotto diretto di due sottogruppi normali minimali tra loro isomorfi, è il prodotto diretto di un certo numero di copie di un gruppo semplice finito.

Come già accennato, un importante teorema, il Teorema di O'Nan-Scott permette, viceversa, di ottenere forti informazioni sulla struttura (algebrica) e, parzialmente, sull'azione (permutazionale) di un gruppo finito primitivo in termini del suo zoccolo. Il solo enunciato del Teorema di O'Nan-Scott richiede definizioni che impegnerebbero per la loro esposizione più di quanto non sembra appropriato in queste note, e viene quindi tralasciato (un riferimento bibliografico è il quarto capitolo di [DM]). Ciò che si vuole evidenziare è, comunque, il fatto che questo risultato permette di stabilire uno stretto nesso tra lo studio dei gruppi primitivi e quello dei gruppi semplici finiti. Ciò è tanto più vero nel caso particolare dei gruppi 2-transitivi. Infatti il corrispondente caso speciale del Teorema di O'Nan-Scott (di molto precedente: il Teorema di O'Nan-Scott risale al 1979, questo di Burnside al 1911) lega molto direttamente la struttura di un gruppo 2-transitivo non di tipo affine a quella di un gruppo semplice non abeliano:

6.18. Teorema (Burnside). *Sia G un gruppo finito 2-transitivo di permutazioni. Allora* $\mathrm{Soc}(G)$ *è o abeliano (e quindi G è di tipo affine su esso) oppure semplice non abeliano e primitivo.*

Ad esempio, se $G = \mathbb{S}_n$ con n intero maggiore di 4, allora $\mathrm{Soc}(G) = \mathbb{A}_n$, semplice e primitivo. Nella situazione del Teorema 6.18 è chiaro che se $S = \mathrm{Soc}(G)$ è semplice allora S è l'unico sottogruppo normale minimale di G, quindi S è il monolite di G. Nel caso in cui S non sia abeliano (cioè quando G non è di tipo affine) consideriamo l'applicazione $\varphi : G \to \mathrm{Aut}\, S$ che a $g \in G$ associa l'automorfismo indotto per coniugio da g su S (cioè: $s \in S \mapsto s^g \in S$). Come sappiamo, φ è un omomorfismo di nucleo $C = C_G(S)$. Poiché $C \lhd G$ e S è il monolite di G, si ha $C = 1$ oppure $S \leq C$; quest'ultima possibilità è esclusa perché S non è abeliano, quindi $C = 1$ e φ è un monomorfismo. In questo caso, dunque, G è isomorfo a G^φ, un sottogruppo di $\mathrm{Aut}\, S$ contenente $S^\varphi = \mathrm{Inn}\, S$. In questo modo ad ogni gruppo finito 2-transitivo non di tipo affine viene associato un gruppo semplice finito (il suo zoccolo) e, viceversa, dato un gruppo semplice finito S, ogni gruppo finito 2-transitivo con zoccolo isomorfo a S è contenuto, a meno di isomorfismi, tra i sottogruppi dell'automorfo di S contenenti $\mathrm{Inn}\, S$. Allora, se sono noti tutti i gruppi semplici finiti ed i loro gruppi di automorfismi queste informazioni forniscono un metodo per elencare tutti i gruppi finiti 2-transitivi non di tipo affine. Ad esempio, sapendo che $\mathbb{A}_5$ è un gruppo semplice e che il suo automorfo è isomorfo a $\mathbb{S}_5$ (queste proprietà saranno discusse più avanti), se G è un gruppo 2-transitivo il cui zoccolo è isomorfo a $\mathbb{A}_5$ allora G è isomorfo a $\mathbb{A}_5$ oppure a $\mathbb{S}_5$, gli unici sottogruppi di $\mathbb{S}_5$ contenenti un sottogruppo isomorfo a $\mathbb{A}_5$. Si sta parlando qui di isomorfismi piuttosto che di similitudini perché le considerazioni appena svolte dànno informazioni sulla struttura algebrica di G ma non sulla sua azione permutazionale, che va descritta con argomentazioni ulteriori.

Il progetto di classificare i gruppi semplici finiti risale almeno all'ultimo decennio del secolo scorso, quando Otto Hölder, dopo aver dimostrato quello che ora è noto come Teorema di Jordan-Hölder, osserva come la conoscenza di tutti i gruppi semplici finiti, unitamente allo studio dettagliato di come la struttura di un gruppo G si possa descrivere in termini di un sottogruppo normale N e del relativo quoziente G/N (il cosiddetto problema dell'estensione) può, in linea di principio, fornire un metodo per la descrizione di tutti i gruppi finiti. Il programma di Hölder è stato portato a compimento, grazie alla congiunzione degli sforzi di un gran numero di matematici, con il teorema di classificazione dei gruppi semplici finiti, annunciato per la prima volta nel 1979, che appare essere se non *il più* certamente *uno dei più* notevoli (e complessi) risultati della matematica contemporanea.(*)

(*) va detto che la dimostrazione di questo teorema è tuttora troppo lunga e, appunto, complessa perché sia stato

Per le argomentazioni riportate sopra, il teorema di classificazione dei gruppi semplici finiti, fornendo una lista di tali gruppi, ha anche reso possibile elencare tutti i gruppi 2-transitivi di permutazioni su insiemi finiti (a meno di similitudini); ovviamente tra essi sono compresi tutti i gruppi finiti di permutazioni k-transitivi o strettamente k-transitivi per qualche intero $k > 1$. Non è qui possibile neanche dare una descrizione di questa lista: nella definizione di alcune delle famiglie in cui sono suddivisi tali gruppi sono coinvolte costruzioni piuttosto tecniche (un riferimento bibliografico è ancora [DM]). Quello che si può però enunciare è la seguente conseguenza delle informazioni fornite dalla lista:

6.19. Teorema. *Ammettendo la validità del teorema di classificazione dei gruppi semplici finiti, non esistono gruppi finiti di permutazioni k-transitivi per alcun intero $k > 5$, ad eccezione dei gruppi alterni o simmetrici.*

Esercizi.

1. Sia N un sottogruppo normale minimale del gruppo finito G. Allora N è il monolite di G se e solo se N è l'unico sottogruppo normale minimale di G, ovvero se e solo se $N = \mathrm{Soc}(G)$.
2. Sia N un sottogruppo normale minimale del gruppo G. Se $C_G(N) \leq N$ allora N è il monolite di G. Se N non è abeliano, $Z(N) = 1$ e N è il monolite di G se e solo se $C_G(N) = 1$.
3. Siano G un gruppo primitivo e N un suo sottogruppo normale minimale abeliano (quindi G ed N sono come nel Teorema 6.13). Allora $N = C_G(N)$. Dedurne che N è il monolite di G senza utilizzare 6.17. [*Suggerimento: osservare preliminarmente che $C_G(N) = N \rtimes C_H(N)$, dove H è lo stabilizzante di un punto.*]
4. Sia N un sottogruppo normale regolare di un gruppo primitivo G. Utilizzando 6.16 provare che N è normale minimale. Verificare che non vale il viceversa: esistono gruppi primitivi G con sottogruppi normali minimali non regolari. Osservare che il risultato provato permette di evitare il ricorso a 6.12 nella dimostrazione di 6.13.
5. Una interessante conseguenza del teorema di classificazione dei gruppi semplici finiti è la validità della cosiddetta congettura di Schreier: *per ogni gruppo semplice finito S il quoziente* $\mathrm{Aut}\, S \,/\, \mathrm{Inn}\, S$ *è un gruppo risolubile.* Utilizzando ciò, provare che se S è lo zoccolo di un gruppo finito 2-transitivo G non di tipo affine allora G/S è risolubile.

Gruppi più volte (strettamente) transitivi

La ricerca sistematica di esempi di gruppi molte volte transitivi, o molte volte strettamente transitivi, esclusi i casi ovvi dei gruppi simmetrici o alterni (vedi 4.3), è stato uno dei principali obiettivi della teoria dei gruppi finiti di permutazione sin dai suoi inizi, nel secolo scorso, quindi ben prima che i rapporti con la teoria dei gruppi semplici finiti a cui abbiamo accennato sopra fossero formulati. Ad esempio il caso particolare del Teorema 6.19 per gruppi k-strettamente transitivi (cioè la non esistenza di gruppi k-strettamente transitivi per $k > 5$, esclusi gruppi simmetrici e alterni) era noto da tempo e non dipende dal teorema di classificazione. Almeno in parte, infatti, la descrizione dei gruppi k-strettamente transitivi (per $k > 1$) è sufficientemente elementare da poter essere qui affrontata.

Tali gruppi, essendo 2-transitivi, sono come sappiamo particolari gruppi primitivi, quindi sono di tipo affine se dotati di un sottogruppo normale regolare abeliano. Questo è ciò che accade, nel caso finito, per tutti i gruppi strettamente 2-transitivi:

6.20. Teorema. *Sia G un gruppo di permutazioni strettamente 2-transitivo su un insieme finito X. Allora G possiede un sottogruppo normale regolare N; questo è un p-gruppo abeliano elementare, per un numero primo p, ed è l'unico p-sottogruppo di Sylow di G. Infine G è di tipo affine su N ed il suo grado è potenza di p.*

Dimostrazione — Sia $n = |X|$ il grado di G, allora $n > 1$ e $|G| = n(n-1)$ per 4.1. Per ipotesi, l'unico elemento di G che fissa più di un punto di X è l'identità, dunque, posto

$$N = \{g \in G \mid \mathrm{Fix}(g) = \varnothing\} \cup \{1\},$$

$G \smallsetminus N$ è costituito dagli elementi di G che fissano esattamente un punto. Da 1.5 segue allora

$$1 = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}(g)| = \frac{1}{|G|}\left(|\,\mathrm{Fix}(1)| + \sum_{g \in G \smallsetminus N} 1\right) = \frac{1}{|G|}\big(n + |G \smallsetminus N|\big),$$

sicché $n + |G \smallsetminus N| = |G|$ e $|N| = n$. È chiaro (dall'esercizio 15 di p. 3, ovvero dal nr. 4 di p. 14) che N è una parte normale di G (cioè è fissata da ogni automorfismo interno di G), bisogna verificare che si tratta di un sottogruppo.

---

possibile per la comunità matematica verificarla nella sua interezza. Per rendere l'idea: da alcuni anni è in corso di pubblicazione una serie di volumi dedicata esclusivamente all'esposizione di una dimostrazione del teorema, di molto semplificata rispetto all'originale; il piano dell'opera prevede una dozzina di volumi! Per questi motivi, il teorema di classificazione dei gruppi semplici finiti, pur essendo ormai generalmente accettato, non ha raggiunto lo status di indiscussa certezza che si considera prerogativa dei risultati della matematica. Pertanto è abitudine indicare esplicitamente la dipendenza dal teorema di classificazione nell'esporre risultati per i quali non si conoscano dimostrazioni che del teorema di classificazione non facciano uso.

Siano $a \in N \smallsetminus 1$ e sia $C = C_G(a)$. Poiché ogni coniugato di a in G è contenuto in $N \smallsetminus 1$, che ha ordine $n-1$, certamente $|G : C| \leq n-1$, quindi $|C| \geq |G|/(n-1) = n$. D'altra parte $C \subseteq N$, infatti, se esistesse $c \in C \smallsetminus N$, allora $c \in \mathrm{St}_G(x)$ per un opportuno $x \in X$ (per la definizione di N), quindi $c \in \mathrm{St}_G(x) \cap \big(\mathrm{St}_G(x)\big)^a = \mathrm{St}_G(x) \cap \mathrm{St}_G(xa)$, contro l'essere $\mathrm{St}_G(x) \cap \mathrm{St}_G(xa) = 1$ perché $x \neq xa$ dal momento che $\mathrm{Fix}(a) = \varnothing$. Dunque $C \subseteq N$, e da $|C| \geq n = |N|$ segue $C = N$. Pertanto N coincide col centralizzante in G di ogni suo elemento ed è dunque un sottogruppo abeliano (normale) di G. Poiché G è primitivo per 5.7, segue da 6.13 che N è regolare e G è di tipo affine su N, in particolare N è un p-gruppo abeliano elementare per un certo primo p e $n = \deg G$ è una potenza di p. Infine N è un sottogruppo di Sylow di G, dal momento che $|G : N| = n-1$ è primo con p, unico in quanto normale in G. ❑

In modo più preciso, i gruppi finiti strettamente 2-transitivi sono caratterizzati, a meno di similitudini, come gruppi affini su particolari strutture algebriche chiamate quasi-corpi (cfr. [DM], p. 236).

La situazione pare essere più complicata per quanto riguarda la descrizione dei gruppi infiniti strettamente 2-transitivi. Infatti non è noto se un tale gruppo debba o meno possedere necessariamente un sottogruppo normale regolare.

Esercizio. Dimostrare il Teorema 6.20 senza utilizzare 6.13 ma sostituendo il ricorso a questo teorema con argomenti diretti per provare la transitività del sottogruppo N e applicando 6.10 e 6.8.

Il contenuto essenziale del Teorema 6.20 consiste nel fatto che i gruppi finiti strettamente 2-transitivi contengono un sottogruppo normale regolare abeliano. Da questo punto di vista 6.20 è un caso particolare (e particolarmente semplice) del seguente

6.21. Teorema (Frobenius). *Sia G un gruppo transitivo di permutazioni sull'insieme finito non vuoto X. Se $\mathrm{St}_G(Y) = 1$ per ogni parte Y di X di ordine 2, allora G possiede un sottogruppo normale regolare,*

completato dall'informazione (Teorema di Thompson) che, se G stesso non è regolare, il sottogruppo normale regolare N di G verifica una certa condizione (si chiama nilpotenza) che implica in particolare $Z(N) \neq 1$. Se G è anche primitivo allora il Teorema 6.13 implica che $Z(N)$ è regolare, quindi $N = Z(N)$ è abeliano, e questo spiega come effettivamente 6.20 si possa ricavare da 6.21.

I gruppi che ammettono una rappresentazione permutazionale fedele non regolare del tipo richiesto nell'enunciato del Teorema 6.21 sono noti come gruppi di Frobenius. Più precisamente, un *gruppo di Frobenius* è per definizione un gruppo G dotato di un sottogruppo non banale H tale che $H \cap H^g = 1$ per ogni $g \in G \smallsetminus H$. Un tale H si chiama complemento di Frobenius di G. Per tali G e H si ha chiaramente $H_G = 1$, quindi la rappresentazione di G sui laterali destri di H è, oltre che transitiva, fedele, ma non regolare perché $H \neq 1$, e rispetto ad essa lo stabilizzante di ciascun sottoinsieme di ordine 2 è identico (essendo l'intersezione tra due coniugati distinti di H). Dal Teorema 6.21 segue dunque che G possiede un sottogruppo normale regolare N, quindi $G = N \rtimes H$.

Esercizi.

1. Verificare che un gruppo è di Frobenius se e solo se ammette una rappresentazione permutazionale transitiva non regolare di grado maggiore di 1 rispetto alla quale ogni parte di ordine 2 abbia stabilizzante identico (una delle due implicazioni è stata appena provata).
2. Sia ρ una rappresentazione permutazionale. Osservare che ρ è strettamente 2-transitiva se e solo se o ρ è simile alla rappresentazione naturale di $\mathbb{S}_2$ oppure ρ è 2-transitiva e verifica le proprietà elencate all'esercizio precedente (non è regolare e ogni parte di ordine 2 ha stabilizzante identico; ρ ha automaticamente grado maggiore di 1 per definizione di 2-transitività). Detto in altri termini: escluso il caso della rappresentazione naturale di $\mathbb{S}_2$, i gruppi strettamente 2-transitivi sono precisamente quelli 2-transitivi che sono anche di Frobenius con lo stabilizzante di un punto come complemento.

Passiamo ora a considerare gruppi strettamente 3-transitivi. Un'importante famiglia di gruppi di permutazione strettamente 3-transitivi è fornita dai gruppi proiettivi lineari su spazi vettoriali di dimensione 2.

Esempio. Sia V lo spazio vettoriale numerico di dimensione 2 su un campo K. La retta proiettiva $P_1(K)$ è l'insieme dei sottospazi di V di dimensione 1. È ben noto (e del tutto elementare) che ogni elemento di $P_1(K)$ ha una (unica) rappresentazione nella forma $[1, 0]$ o $[a, 1]$ con $a \in K$, dove la notazione $[a, b]$ (con a e b elementi di K non entrambi nulli) è usata per indicare il sottospazio $(a, b)K$ di V generato da (a, b) (quindi, se $a', b' \in K$ non sono entrambi nulli, si ha $[a, b] = [a', b']$ se e solo se (a, b) e (a', b') sono proporzionali). Ogni automorfismo di V manda sottospazi in sottospazi della stessa dimensione, quindi il gruppo $\mathrm{Aut}\, V$ ha un'ovvia azione transitiva su $P_1(K)$: quella definita ponendo $W\alpha$ uguale all'immagine di W mediante α, per ogni $W \in P_1(K)$ e $\alpha \in \mathrm{Aut}\, V$. È ben noto che gli elementi di $\mathrm{Aut}\, V$ possono essere rappresentati come matrici invertibili su K: detto $\mathrm{GL}(V)$ il gruppo delle matrici invertibili di tipo 2×2 su K, associando ad ogni $A \in \mathrm{GL}(V)$ l'automorfismo $v \in V \mapsto vA \in V$ si definisce un isomorfismo da $\mathrm{GL}(V)$ a $\mathrm{Aut}(V)$. Componendo questo isomorfismo con la rappresentazione permutazionale di $\mathrm{Aut}\, V$ su $P_1(K)$ già descritta si definisce un'azione di $\mathrm{GL}(V)$ su $P_1(K)$, ovviamente simile alla precedente. È facile verificare che il

nucleo di questa azione è il gruppo delle matrici scalari non nulle $Z = \{kI \mid k \in K^*\}$, dove I è la matrice identica e $K^* = K \setminus \{0\}$. Infatti, per ogni $k \in K^*$ si ha $[a,b](kI) = [ak, bk] = [a,b]$, il che prova che Z è contenuto nel nucleo N della rappresentazione. Viceversa, se $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in N$, allora $[1,0] = [1,0]A = [a,b]$, quindi $b = 0$, analogamente $c = 0$ perché A stabilizza $[0,1]$ e quindi $[1,1] = [1,1]A = [a,d]$ da cui segue $a = d$ e $A = aI \in Z$.

Per definizione, il *gruppo proiettivo lineare* su V è il quoziente $\mathrm{PGL}(V) := \mathrm{GL}(V)/Z$. Naturalmente, per il primo teorema di omomorfismo, l'azione di $\mathrm{GL}(V)$ su $P_1(K)$ induce una rappresentazione fedele e transitiva di $\mathrm{PGL}(V)$ su $P_1(K)$.

Per studiare questa azione partiamo dallo stabilizzante di un punto. Sia $\Gamma = \mathrm{St}_{\mathrm{PGL}(V)}([1,0])$. Chiaramente $\Gamma = \{gZ \mid g \in \mathrm{St}_{\mathrm{GL}(V)}([1,0])\}$. Come già osservato, ogni elemento di $\mathrm{St}_{\mathrm{GL}(V)}([1,0])$ ha la forma $\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right)$ dove $a, b, c \in K$ e, dovendo la matrice essere invertibile, $ac \neq 0$. Viceversa, ogni matrice di questa forma stabilizza $[1,0]$. Inoltre il laterale modulo Z di una tale matrice è $\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right)Z = \left\{\left(\begin{smallmatrix} ak & 0 \\ bk & ck \end{smallmatrix}\right) \mid k \in K^*\right\}$; poiché $c \neq 0$ ad esso appartiene una ed una sola matrice in cui appaia 1 al posto $(2,2)$. Pertanto, ponendo $M_{a,b} := \left(\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right)Z$ per ogni $a, b \in K$ con $a \neq 0$, si ha:

$$\Gamma = \{M_{a,b} \mid a \in K^* \wedge b \in K\} \qquad \text{e} \qquad M_{a,b} = M_{a',b'} \iff (a,b) = (a',b').$$

Vogliamo provare che l'azione di Γ su $X := P_1(K) \setminus \{[0,1]\}$ è simile all'azione di $\mathrm{Aff}(K)$, dove K è visto come spazio vettoriale su se stesso. $\mathrm{Aut}_K(K)$ consiste delle applicazioni $x \in K \mapsto xa \in K$, al variare di $a \in K^*$. Allora $\mathrm{Aff}(K) = \mathrm{Aut}_K(K)\, T(K) = \{A_{a,b} \mid a \in K^* \wedge b \in K\}$, dove $A_{a,b}$ è l'affinità $x \in K \mapsto xa + b \in K$. Le applicazioni

$$\alpha : A_{a,b} \in \mathrm{Aff}(K) \longmapsto M_{a,b} \in \Gamma \qquad \text{e} \qquad f : a \in K \longmapsto [a,1] \in X$$

dànno luogo ad una similitudine tra l'azione di $\mathrm{Aff}(K)$ e quella di Γ su X. Infatti è facile verificare che f è biettiva, inoltre α è biettiva dal momento che ogni elemento di $\mathrm{Aff}(K)$ (risp. di Γ) si scrive in uno ed un solo modo come $A_{a,b}$ (risp. $M_{a,b}$) con $a \in K^*$ e $b \in K$. Scelti comunque $a, a' \in K^*$ e $b, b' \in K$ si ha

$$A_{a,b}A_{a',b'} : x \in K \longmapsto (xa+b)a' + b' = xaa' + (ba' + b') \in K, \quad \text{ovvero} \quad A_{a,b}A_{a',b'} = A_{aa',ba'+b'},$$

$$M_{a,b}M_{a',b'} = \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}\begin{pmatrix} a' & 0 \\ b' & 1 \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ba' + b' & 1 \end{pmatrix} = M_{aa',ba'+b'},$$

il che mostra che α è un isomorfismo. Resta da verificare che, per ogni $a \in K^*$ e $b \in K$ il diagramma

$$\begin{array}{ccc} K & \xrightarrow{A_{a,b}} & K \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ X & \xrightarrow{M_{a,b}} & X \end{array}$$

è commutativo. Per ogni $x \in K$ si ha $xA_{a,b}f = (xa+b)f = [xa+b, 1]$ e $xfM_{a,b} = [x,1]M_{a,b} = [xa+b, 1]$, dunque il diagramma è commutativo e l'azione di Γ è simile a quella di $\mathrm{Aff}(K)$.

Abbiamo osservato in 6.7 che $\mathrm{Aff}(K)$ è strettamente 2-transitivo, utilizzando 4.2 concludiamo allora che $\mathrm{PGL}(V)$ opera in modo (fedele e) strettamente 3-transitivo su $P_1(K)$. ❑

Il gruppo $\mathrm{PGL}(V)$ viene anche indicato come $\mathrm{PGL}(2,K)$, oppure, se K è finito, con $\mathrm{PGL}(2,|K|)$, la qual cosa ha senso perché i campi finiti sono determinati (a meno di isomorfismi) dal loro ordine.

Il fatto che lo stabilizzante di un punto in $\mathrm{PGL}(V)$ sia identificabile con il gruppo affine su K ha una chiara interpretazione geometrica. Infatti $\mathrm{PGL}(V)$ agisce sulla retta proiettiva su K; un punto fissato di quest'ultima si può riguardare come punto all'infinito e il suo complemento come retta affine. Allora lo stabilizzante considerato consiste delle proiettività della retta proiettiva che fissano il punto all'infinito, e queste sono identificate con le affinità della retta affine.

Modificando leggermente la costruzione precedente, si può ottenere un'altra famiglia di gruppi strettamente 3-transitivi. Per semplicità ci limitiamo al caso finito.

Esempio. Sia K un campo finito di ordine $q = p^{2n}$, dove p è un primo dispari e n è un intero positivo. Il gruppo moltiplicativo K^* di K è ciclico di ordine pari $q-1$, quindi i quadrati non nulli costituiscono un sottogruppo proprio $Q = \{a^2 \mid a \in K^*\}$ di indice 2 in K^*. Inoltre K ha un automorfismo di ordine 2, precisamente $\theta : x \in K \mapsto x^{p^n} \in K$ (come è noto, l'automorfo di K è un gruppo ciclico, generato dall'automorfismo di Frobenius $x \mapsto x^p$ che ha ordine $2n$, quindi θ è l'unico automorfismo di K di ordine 2). Chiaramente $Q^\theta = Q$.

Definiamo V e $P_1(K)$ come per la costruzione precedente, e continuiamo ad adottare le notazioni lì introdotte. L'automorfismo θ induce un automorfismo di $\mathrm{GL}(V)$ ed una permutazione su $P_1(K)$, che continuiamo a denotare con θ, definiti rispettivamente da $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a^\theta & b^\theta \\ c^\theta & d^\theta \end{smallmatrix}\right)$ e $[a,b] \mapsto [a^\theta, b^\theta]$ (si verifica subito che questa è ben posta). Definiamo poi un omomorfismo η da $\mathrm{GL}(V)$ al sottogruppo $\langle\theta\rangle$ di $Sym\left(P_1(K)\right)$ componendo l'omomorfismo determinante $A \in \mathrm{GL}(V) \mapsto \det A \in K^*$ con l'epimorfismo canonico $K^* \twoheadrightarrow K^*/Q$ e infine con l'unico isomorfismo da K^*/Q a $\langle\theta\rangle$ (si tratta di due gruppi di ordine 2); l'omomorfismo così ottenuto è quindi:

$$\eta : A \in \mathrm{GL}(V) \longmapsto \begin{cases} 1, & \text{se } \det A \in Q \\ \theta, & \text{se } \det A \notin Q \end{cases} \in Sym\left(P_1(K)\right).$$

Per ogni $A \in \mathrm{GL}(V)$ sia $\Phi_A = A^\eta A^*$, dove $A^* \in Sym\big(P_1(K)\big)$ è la permutazione $W \mapsto WA$, dunque

$$\Phi_A : W \in P_1(K) \longmapsto W^{A^\eta} A \in P_1(K),$$

una permutazione di $P_1(K)$. Verifichiamo che $M(K) := \{\Phi_A \mid A \in \mathrm{GL}(V)\}$ costituisce un sottogruppo di $Sym\big(P_1(K)\big)$. Poiché $Sym\big(P_1(K)\big)$ è finito basterà verificare che $M(K)$ è stabile rispetto al prodotto. A questo scopo, siano $A, B \in \mathrm{GL}(V)$. Per ogni $W \in P_1(K)$ si ha $W(\Phi_A\Phi_B) = \big(W^{A^\eta}A\big)\Phi_B = W^{A^\eta B^\eta}(A^{B^\eta}B)$. Inoltre $\big(A^{B^\eta}\big)^\eta = A^\eta$, dal momento che $Q^{B^\eta} = Q$ e quindi $\det\big(A^{B^\eta}\big) = (\det A)^{B^\eta} \in Q$ se e solo se $\det A \in Q$. Dunque $\big(A^{B^\eta}B\big)^\eta = A^\eta B^\eta$ e $W(\Phi_A\Phi_B) = W\Phi_{A^{B^\eta}B}$. Ne segue $\Phi_A\Phi_B = \Phi_{A^{B^\eta}B}$ e, in particolare, $\Phi_A\Phi_B \in M(K)$, come richiesto. Stabilito che $M(K)$ è un un sottogruppo di $Sym\big(P_1(K)\big)$, studiamone l'azione su $P_1(K)$. Se W è uno tra $[1,0]$, $[0,1]$, $[1,1]$ vale $W^\theta = W$, quindi $W\Phi_A = W^{A^\eta}A = WA$ per ogni $A \in \mathrm{GL}(V)$. Siccome l'azione di $\mathrm{GL}(V)$ su $P_1(K)$ è 3-transitiva per quanto all'esempio precedente, si ricava che $M(K)$ è 3-transitivo (se W_1, W_2 e W_3 sono tre elementi distinti di $P_1(K)$ esiste $A \in \mathrm{GL}(V)$ tale che $W_1 = [1,0]A = [1,0]\Phi_A$, $W_2 = [0,1]A = [0,1]\Phi_A$ e $W_3 = [1,1]A = [1,1]\Phi_A$). Inoltre, ancora dall'esempio precedente ricaviamo che se Φ_A appartiene lo stabilizzante in $M(Q)$ di $\{[1,0],[0,1],[1,1]\}$ allora A è una matrice scalare, cioè $A = aI$ per un opportuno $a \in K^*$. Dunque $\det A = a^2 \in Q$ e quindi $A^\eta = 1$; anche la permutazione $A^* : W \mapsto WA$ di $P_1(K)$ è l'identità, per cui $\Phi_A = A^\eta A^* = 1$. Pertanto $M(K)$ è strettamente 3-transitivo.

L'ultimo passo della dimostrazione svolta implica anche che, se $A \in \mathrm{GL}(V)$ e $a \in K^*$, allora $\Phi_{A(aI)} = \Phi_A$. Infatti $\Phi_A = \Phi_A\Phi_{aI} = \Phi_{A^{(aI)^\eta}(aI)} = \Phi_{A(aI)}$, avendo usato l'identità $\Phi_{AB} = \Phi_{A^{B^\eta}B}$ dimostrata sopra. Allora due elementi di $\mathrm{GL}(V)$ determinano la stessa permutazione se sono congrui modulo Z; in altri termini è ben definita l'applicazione $f : AZ \in \mathrm{PGL}(V) \mapsto \Phi_A \in M(K)$. Ovviamente f è suriettiva. Inoltre, per 4.1, sia $M(K)$ che $\mathrm{PGL}(V)$ hanno ordine $q(q+1)(q-1)$ (infatti l'ordine di $P_1(K)$ è $q+1$), quindi f è biettiva. Va però tenuto ben presente che f *non è un isomorfismo*, anzi, $\mathrm{PGL}(V)$ e $M(K)$ non sono in nessun caso isomorfi (ed in particolare non sono simili), sicché i gruppi $M(K)$ costituiscono effettivamente una nuova famiglia di gruppi strettamente 3-transitivi.

Il fatto che l'azione di $M(K)$ non sia simile a quella di un gruppo proiettivo (2-dimensionale) si può provare osservando che, qualsiasi sia il campo L, lo stabilizzante in $\mathrm{PGL}(2,L)$ di un insieme di ordine 2 (ovvero lo stabilizzante di un punto in $\mathrm{Aff}(L)$) è isomorfo al gruppo moltiplicativo di L ed è quindi abeliano, mentre, come stiamo per provare, non è abeliano lo stabilizzante Δ di $\{[1,0],[0,1]\}$ in $M(K)$. Infatti calcoli precedentemente svolti mostrano che Δ è costituito dalle permutazioni Φ_A con A matrice diagonale, ovvero $\Delta = \{\Phi_{D_a} \mid a \in K^*\}$ dove $D_a = \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$ per ogni $a \in K^*$. L'insieme degli elementi di K fissati da θ (cioè delle radici del polinomio $x^{p^n} - x$) costituisce il sottocampo di ordine p^n di K, chiamiamolo F. È chiaro che Q, che ha ordine $(p^{2n}-1)/2 > p^n - 1$, non è contenuto in F^*, quindi esiste $a \in Q \smallsetminus F^*$. Sia poi $b \in K^* \smallsetminus Q$. Allora D_a e D_b hanno determinanti rispettivamente a e b, quindi ${D_a}^\eta = 1$ e ${D_b}^\eta = \theta$, sicché $[1,1]\Phi_{D_b}\Phi_{D_a} = [b,1]\Phi_{D_a} = [ba,1]$ e $[1,1]\Phi_{D_a}\Phi_{D_b} = [a,1]\Phi_{D_b} = [a^\theta b,1] \neq [ba,1]$, dunque $\Phi_{D_a}\Phi_{D_b} \neq \Phi_{D_b}\Phi_{D_a}$ e Δ non è abeliano.

Come suggerito nel prossimo esercizio 3, si può usare quanto appena visto per provare che $M(K)$ non è neanche isomorfo come gruppo astratto a $\mathrm{PGL}(2,L)$. ❑

La lista dei gruppi finiti di permutazioni strettamente 3-transitivi è esaurita dai due esempi appena costruiti, come assicurato dal teorema che segue, del quale è omessa la dimostrazione. Il prossimo esercizio 1 chiarisce come mai i casi ovvi (gruppi simmetrici o alterni: $\mathbb{S}_3$, $\mathbb{S}_4$, $\mathbb{A}_5$) di gruppi strettamente 3-transitivi sono (apparentemente) omessi dalla lista.

6.22. Teorema (Zassenhaus). *A meno di similitudini gli unici gruppi finiti di permutazioni strettamente* 3*-transitivi sono i gruppi* $\mathrm{PGL}(2,K)$*, dove* K *è un campo finito, ed i gruppi* $M(K)$*, dove* K *è un campo finito di ordine potenza di un primo dispari con esponente pari. In particolare, ogni gruppo finito strettamente* 3*-transitivo ha grado* $p^n + 1$ *per opportuni* $n \in \mathbb{N}$ *e* p *numero primo.*

Esercizi.

1. Utilizzando 4.3, provare che $\mathbb{S}_3$, $\mathbb{S}_4$ e $\mathbb{A}_5$ sono rispettivamente simili (e quindi isomorfi) a $\mathrm{PGL}(2,2)$, $\mathrm{PGL}(2,3)$ e $\mathrm{PGL}(2,4)$.
2. Sia K un campo finito. Mostrare che, se K ammette un automorfismo di periodo 2 ed il sottogruppo dei quadrati degli elementi di K^* è distinto da K^*, allora $|K| = p^{2n}$ dove p è un primo dispari e $n \in \mathbb{N}$. Ciò spiega perché la costruzione di $M(K)$ è stata effettuata solo in queste ipotesi.
3. Provare che, dati comunque due campi K e L, con K finito di ordine potenza di un primo dispari con esponente pari, $\mathrm{PGL}(2,L)$ e $M(K)$ non sono isomorfi, procedendo come segue:
   — se $|\mathrm{PGL}(2,L)| = |M(K)|$ allora $|L| = |K|$, quindi L e K sono isomorfi e possiamo assumere $L = K$.
   — Sia $q = p^n$ l'ordine di K e L, con p primo e $n \in \mathbb{N}$. Se G è uno tra $\mathrm{PGL}(2,K)$ e $M(K)$, detto H lo stabilizzante in G di un punto, allora H, rispetto all'azione sul suo supporto, contiene un sottogruppo normale regolare N, il quale è un p-sottogruppo di Sylow di G. Dal fatto che G è primitivo dedurre che H è massimale in G e quindi $H = N_G(N)$. Il quoziente H/N è isomorfo allo stabilizzante in G di un insieme di ordine 2.
   — Se P è un qualsiasi p-sottogruppo di Sylow di G allora $N_G(P)/P$ è abeliano se $G = \mathrm{PGL}(2,K)$, non abeliano se $G = M(K)$. Concludere $\mathrm{PGL}(2,K) \not\cong M(K)$.

Per interi $k > 3$ sono molto più rari gli esempi di gruppi k-strettamente transitivi, in particolare non ne esistono esempi infiniti. Allo scopo classificare i gruppi 4-strettamente transitivi iniziamo con:

6.23. *Siano p un numero primo e c un p-ciclo in $\mathbb{S}_{p+2}$. Allora $C_{\mathbb{S}_{p+2}} = \langle c\rangle \times \langle t\rangle$, dove t è la trasposizione che scambia tra loro i due elementi di* $\mathrm{Fix}(c)$.

Dimostrazione — Sia $C = C_{\mathbb{S}_{p+2}}(c)$. L'indice di C in $\mathbb{S}_{p+2}$ uguaglia il numero dei coniugati in $\mathbb{S}_{p+2}$ di c, cioè il numero dei p-cicli in $\mathbb{S}_{p+2}$; questo numero è $(p+2)!/2p$ (vedi esercizio 3 a p. 10). Dunque $|\mathbb{S}_{p+2} : C| = (p+2)!/2p$ e quindi $|C| = 2p$. D'altra parte $\langle c, t\rangle = \langle c\rangle \times \langle t\rangle$ ha anch'esso ordine $2p$ ed è contenuto in C, quindi $C = \langle c\rangle \times \langle t\rangle$. ❑

6.24. *Sia G un sottogruppo strettamente 4-transitivo di $\mathbb{S}_{p+2}$, dove p è un numero primo dispari. Allora $p = 3$ e $G = \mathbb{S}_5$.*

Dimostrazione — Sia H lo stabilizzante in G di una parte di ordine 2. Allora H agisce in modo strettamente 2-transitivo sui p punti rimanenti ed ha quindi un sottogruppo normale regolare N, di ordine p, per 6.20. Gli elementi di ordine p in $\mathbb{S}_{p+2}$ sono precisamente i p-cicli, quindi $N = \langle c\rangle$ per un p-ciclo c. Sia t la trasposizione di $\mathbb{S}_{p+2}$ che scambia tra loro i due punti fissati da c; supponiamo per assurdo $t \notin G$. Per 6.23 si ha allora $C_G(N) = \big(N \times \langle t\rangle\big) \cap G = N$. Dunque, da [Rob], 1.6.13, si deduce che $N_G(N)/N$ è isomorfo ad un sottogruppo di $\mathrm{Aut}\, N$, che ha ordine $p-1$. Poiché $H \leq N_G(N)$ e $|H/N| = p-1$, ne segue $H = N_G(N)$. D'altra parte p non divide $|G : H| = (p+1)(p+2)$, quindi N è un p-sottogruppo di Sylow di G e $|G : H| \not\equiv 1 \pmod p$, in contraddizione col terzo teorema di Sylow (1.9). Pertanto $t \in G$. Essendo G primitivo, l'esercizio 3 di p. 23 implica $G = \mathbb{S}_{p+2}$. Ora, $\mathbb{S}_n$ è strettamente 4-transitivo se e solo se $n = 4$ (caso escluso dall'ipotesi) o $n = 5$. (Alternativamente: t fissa p punti, quindi, essendo G strettamente 4-transitivo, necessariamente $p < 4$, sicché $p = 3$ e $G = \mathbb{S}_5$ per 4.3.) Otteniamo così l'asserto. ❑

6.25. Teorema (Jordan, Tits). *Siano X un insieme e G un sottogruppo strettamente 4-transitivo di $\mathrm{Sym}\, X$. Allora, se G non è né $\mathrm{Sym}\, X$ né $\mathrm{Alt}X$ si ha $|X| = 11$. In particolare, non esistono gruppi infiniti strettamente k-transitivi per alcun intero $k > 3$.*

Dimostrazione — Osserviamo innanzitutto che se Y è una parte di X di ordine 4, allora ciascun elemento di G è determinato dalla sua azione sugli elementi di Y. Più precisamente, se $\sigma, \tau \in G$ e $y\sigma = y\tau$ per ogni ogni $y \in Y$, allora $\sigma = \tau$, perché $\sigma\tau^{-1}$ appartiene a $\mathrm{St}_G(Y)$, che è identico per la stretta 4-transitività di G.

Sia $Y = \{a, b, c, d\}$ una parte di X di ordine 4. Ancora per la stretta 4-transitività di G esiste un (unico) elemento $\sigma \in G$ che agisce su Y come $(a\,b)$, cioè tale che $a^\sigma = b$, $b^\sigma = a$ e sia c che d siano fissati da σ. Poiché σ^2 stabilizza Y, certamente $\sigma^2 = 1$ e σ ha periodo 2. Ne segue che ogni σ-orbita ha ordine 1 o 2. Sia Ω l'insieme delle σ-orbite di ordine 2 distinte da $\{a, b\}$. Sia poi $F = \mathrm{Fix}(\sigma)$; per ipotesi $|F| < 4$, d'altra parte c, $d \in F$, quindi $|F|$ vale 2 o 3. Ogni elemento $\tau \in C_G(\sigma)$ fissa F, infatti $F\tau = \mathrm{Fix}(\sigma^\tau) = \mathrm{Fix}(\sigma) = F$. Allora l'azione di G su X induce una rappresentazione permutazionale $\rho : H \to \mathit{Sym}\, F$, dove $H = \mathrm{St}_G(a) \cap C_G(\sigma)$. Questa rappresentazione è fedele, infatti se $h \in \ker\rho$ allora h stabilizza gli elementi di F, ma anche a, e quindi b perché $b = a\sigma \in \mathrm{Fix}(h^\sigma) = \mathrm{Fix}(h)$; dunque $h \in \mathrm{St}_G(Y) = 1$. Pertanto H è isomorfo ad un sottogruppo di $\mathit{Sym}\, F$, in particolare è finito.

Inoltre H agisce su Ω: se $\{i, j\}$ è una σ orbita e $h \in H$ allora $\{i, j\}h = \{ih, jh\}$ è ancora una σ-orbita in quanto $ih\sigma = i\sigma h = jh$; e se $\{i, j\}$ ha ordine 2 ed è diverso da $\{a, b\}$ lo stesso accade per $\{ih, jh\}$, dal momento che h fissa a. Proviamo ora che l'azione di H su Ω è transitiva. Siano $\{i, j\}$ e $\{u, v\}$ elementi di Ω. Poiché l'insieme $\{a, b, i, j\}$ ha certamente ordine 4 dal momento che le σ-orbite $\{a, b\}$ e $\{i, j\}$ sono disgiunte, la 4-transitività di G assicura l'esistenza di un elemento τ di G tale che $a, b \in \mathrm{St}_G(\tau)$, $i\tau = u$ e $j\tau = v$. Possiamo calcolare l'azione di $\tau\sigma$ e quella di $\sigma\tau$ sugli elementi di $\{a, b, i, j\}$. Si ha $a\tau\sigma = a\sigma = b$ e $b\tau\sigma = a$, poi $i\tau\sigma = u\sigma = v$ e, allo stesso modo, $j\tau\sigma = u$. L'analogo calcolo per $\sigma\tau$ porta agli stessi risultati, quindi $\tau\sigma$ e $\sigma\tau$ agiscono allo stesso modo sugli elementi di $\{a, b, i, j\}$. Pertanto $\sigma\tau = \tau\sigma$ e $\tau \in H$. Ovviamente $\{i, j\}\tau = \{u, v\}$, ed è così provata la transitività di H nella sua azione su Ω. Questa azione non è regolare: se infatti $\Omega \neq \varnothing$, definito τ come sopra ponendo $i = v$ e $j = u$, si ha $\{i, j\}\tau = \{i, j\}$ e $\tau \neq 1$. Dunque $\Omega = \varnothing$ o $|\Omega| = |H : H_1|$, dove H_1 è lo stabilizzante, non identico, di un elemento di Ω; poiché H è finito e $|H_1| \geq 2$ concludiamo $|\Omega| \leq |H|/2$. Ricordiamo ora che H si immerge in $\mathit{Sym}\, F$ e $|F| \in \{2, 3\}$. Assumiamo $|F| = 2$. Allora $|H| \leq |\mathit{Sym}\, F| = 2$ e quindi $|\Omega| \leq 1$. Inoltre $F = \{c, d\}$, quindi tutti gli elementi di $X \smallsetminus Y$ sono spostati da σ ed appartengono ad un elemento di Ω. Ne segue $|X| = |Y| + 2|\Omega|$, uguale a 4 o 6 a seconda che $|\Omega|$ sia 0 o 1. Da 4.3 ricaviamo $G = \mathit{Sym}\, X$ nel primo caso, $G = \mathit{Alt}X$ nel secondo. Supponiamo invece $|F| = 3$. Allora $|H| \leq |\mathit{Sym}\, F| = 6$ e $|\Omega| \leq 3$. Gli elementi di X sono: i quattro elementi di Y, l'elemento di $F \smallsetminus Y$ ed i $2|\Omega| \leq 6$ elementi appartenenti ad una orbita appartenente a Ω. Allora $|X| = 4 + 1 + 2|\Omega| \leq 5 + 6 = 11$, inoltre $|X|$ è dispari (e maggiore di 3). Se $|X| = 5$ allora $G = \mathit{Sym}\, X$. I casi $|X| = 7$ e $|X| = 9$ rientrano (a meno di similitudini) tra i casi esclusi in 6.24, non si possono quindi verificare. L'unica possibilità rimasta è $|X| = 11$, come si voleva dimostrare.

Abbiamo in particolare provato che non esistono gruppi strettamente 4-transitivi di grado infinito, ovvero gruppi strettamente 4-transitivi infiniti. Sia k un intero maggiore di 4 e sia, per assurdo, Γ un gruppo strettamente k-transitivo su un insieme infinito I. Lo stabilizzante in Γ di una parte J di I di ordine $k-4$ agisce in modo (fedele e) strettamente 4-transitivo su $I \smallsetminus J$. Per quanto sopra $I \smallsetminus J$ deve essere finito, in contraddizione con l'ipotesi che I sia infinito. Il teorema è così dimostrato. ❑

Il Teorema 6.25 conduce quasi ad una caratterizzazione completa dei gruppi strettamente 4-transitivi di permutazioni, dicendoci che tali gruppi sono, a meno di similitudini, tutti e soli i seguenti: $\mathbb{S}_4$, $\mathbb{S}_5$, $\mathbb{A}_6$ e eventuali altri gruppi di grado 11. Resta ovviamente da decidere se esistano gruppi strettamente 4-transitivi di grado 11, e quanti essi siano a meno di similitudini. La risposta è che ne esiste esattamente uno. Questo gruppo è noto come M_{11} e fa parte di una notevole serie di 5 gruppi scoperti tra il 1861 e il 1873 dal matematico francese Emile Mathieu.(*)

I cinque *gruppi di Mathieu* sono M_{11}, M_{12}, M_{22}, M_{23} e M_{24}, ciascuno dei quali ha per grado il numero posto a pedice. Questi gruppi sono tra loro legati: M_{11} è simile allo stabilizzante di un punto in M_{12} (nell'azione di questo sul suo supporto), analogamente M_{22} è simile allo stabilizzante di un punto in M_{23} e M_{23} allo stabilizzante di un punto in M_{24}. Come detto, M_{11} è strettamente 4-transitivo, quindi M_{12} è strettamente 5-transitivo, per 4.2. Questi due sono, a meno di similitudini, gli unici gruppi strettamente k-transitivi per qualche intero $k > 3$, esclusi i gruppi simmetrici o alterni. Pertanto il Teorema 6.25 si completa in questo modo:

6.26. Teorema. *I gruppi di permutazione strettamente k-transitivi sono, a meno di similitudini:*
(*i*) *per $k = 4$ tutti e soli $\mathbb{S}_4$, $\mathbb{S}_5$, $\mathbb{A}_6$ e M_{11};*
(*ii*) *per $k = 5$ tutti e soli $\mathbb{S}_5$, $\mathbb{S}_6$, $\mathbb{A}_7$ e M_{12};*
(*iii*) *per $k > 5$ tutti e soli $\mathbb{S}_k$, $\mathbb{S}_{k+1}$ e $\mathbb{A}_{k+2}$.*

Questo teorema è stato dimostrato da Jordan nel 1873 per gruppi finiti, la sua estensione al caso generale è dovuta a Tits (1952). Limitatamente al caso infinito, una generalizzazione di 6.25 è:

6.27. Teorema (Yoshizawa, 1979). *Non esistono gruppi infiniti di permutazioni 4-transitivi in cui lo stabilizzante di un insieme di ordine 4 sia finito.*

Tornando ai gruppi di Mathieu, va ancora detto che M_{22} è 3-transitivo, quindi M_{23} e M_{24} sono rispettivamente 4- e 5-transitivi. Conseguenza della classificazione dei gruppi semplici finiti è, oltre alla non esistenza di gruppi finiti 6-transitivi non simmetrici o alterni, già enunciata come Teorema 6.19, il fatto che i gruppi di Mathieu esauriscono tutti i casi non banali di 4-transitività:

6.28. Teorema. *I gruppi finiti di permutazione k-transitivi che non siano né simmetrici né alterni sono, a meno di similitudini:*
(*i*) *per $k = 4$ tutti e soli M_{11}, M_{12}, M_{23} e M_{24}.*
(*ii*) *per $k = 5$ tutti e soli M_{12} e M_{24}.*

Infine la proprietà forse più importante dei gruppi di Mathieu: ciascuno di essi è semplice.
A titolo di curiosità, questi sono gli ordini dei gruppi di Mathieu:

$$|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7.920 \qquad |M_{12}| = |M_{11}| \cdot 12 = 95.040$$
$$|M_{22}| = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 443.520 \qquad |M_{23}| = |M_{22}| \cdot 23 = 10.200.960 \qquad |M_{24}| = |M_{23}| \cdot 24 = 244.823.040.$$

Esercizio. Senza usare quanto è stato riportato senza dimostrazione, provare che da 6.25 e 4.2 segue che ogni gruppo di permutazioni strettamente 5-transitivo che non sia né simmetrico né alterno deve avere grado 12.

Gruppi transitivi di grado primo

I gruppi di cui al titolo costituiscono un'altra classe di gruppi primitivi, come visto in 5.6. Una loro semplice ma notevole proprietà è che ciascuno di essi possiede un sottogruppo regolare. Siano infatti p un numero primo e G un gruppo transitivo di permutazioni di grado p. Il gruppo simmetrico su p oggetti ha ordine $p!$, e la massima potenza di p che divide $p!$ è p stesso. Poiché G è transitivo, p divide $|G|$ e quindi p è proprio l'ordine di un p-sottogruppo di Sylow P di G. Gli unici elementi di ordine p in $\mathbb{S}_p$ sono i p-cicli, dunque P è generato da un p-ciclo, ed è quindi, ovviamente, regolare.

Se P è normale in G la struttura di G si ottiene molto facilmente. Infatti è possibile in questo caso applicare 6.13 per concludere che G è di tipo affine su P. Allora G si può identificare con un sottogruppo di $\mathrm{Hol}\, P$ (ovvero, di $\mathrm{Aff}(V)$, dove V è uno spazio vettoriale di ordine p; si veda 6.8), dunque G è simile a $P \rtimes \Gamma$, per un opportuno $\Gamma \leq \mathrm{Aut}\, P$. Ora, l'automorfo di un gruppo di ordine p è, notoriamente, un gruppo ciclico di ordine $p - 1$, quindi Γ è ciclico di ordine divisore di $p - 1$. In particolare, G è risolubile. Viceversa ogni gruppo transitivo di permutazioni di grado primo e risolubile ha la struttura indicata, come segue da 6.14.

(*) è interessante notare come queste costruzioni siano molto precoci nello sviluppo storico della teoria dei gruppi, che in quegli anni era appena agli inizi. A titolo di paragone si consideri che il lavoro di Evariste Galois che, introducendo quella che oggi chiamiamo teoria di Galois, dà inizio allo studio sistematico della teoria dei gruppi di permutazione è del 1832 e fu pubblicato solo nel 1846, il primo tentativo di definizione 'astratta' della nozione di gruppo, dovuto a Cayley, risale al 1854; i teoremi di Sylow, forse il risultato elementare più fondamentale della teoria dei gruppi finiti, furono dimostrati solo nel 1872, undici anni più tardi della costruzione di M_{11} e M_{12}.

Dunque, tra i gruppi transitivi di grado primo quelli risolubili sono precisamente quelli dotati di p-sottogruppo di Sylow normale; inoltre ciascuno di essi si può identificare con un sottogruppo (contenente le traslazioni) del gruppo affine su uno spazio vettoriale di ordine primo. Come già notato (in 6.7), quest'ultimo gruppo è strettamente 2-transitivo. Ciò ovviamente non implica che tutti i gruppi transitivi di grado primo risolubili siano strettamente 2-transitivi (possono non essere 2-transitivi), ma certamente implica che in ciascuno di essi lo stabilizzante di due punti è il sottogruppo identico (cioè che il gruppo è esso stesso regolare oppure di Frobenius, con lo stabilizzante di un punto come complemento). Questa condizione caratterizza i gruppi transitivi di grado primo risolubili.

6.29. Lemma (Galois). *Sia G un gruppo transitivo di permutazioni su un insieme X di ordine primo p. Sono equivalenti:*
(a) *G è risolubile;*
(b) *G ha un p-sottogruppo di Sylow normale;*
(c) *G è di tipo affine su un gruppo di ordine p;*
(d) *per ogni parte Y di X di ordine 2 si ha $\mathrm{St}_G(Y) = 1$.*

Dimostrazione — L'equivalenza tra (a), (b) e (c), nonché il fatto che queste implicano (d) è stata provata sopra. Resta da provare che (d) implica (b); la dimostrazione è simile a quella di 6.20.

Valga (d). Allora ciascun elemento non identico g di G fissa al più un punto di X. Come per 6.20, posto $N = \{g \in G \mid \mathrm{Fix}(g) = \varnothing\} \cup \{1\}$, da 1.5 segue $|G| = p + |G \smallsetminus N|$, quindi $|N| = p$. D'altra parte, come osservato sopra, G ha un sottogruppo P di ordine p (quindi di Sylow) regolare, e quest'ultima proprietà implica $P \subseteq N$. Per ragioni d'ordine, $P = N$. Pertanto $P \lhd G$, perché la definizione di N implica che N è fissato da ogni automorfismo interno di G. È così provata (b). ❑

Naturalmente l'implicazione (d) $\Rightarrow$ (b) del precedente Lemma è ancora un caso particolare del Teorema di Frobenius 6.21.

La motivazione principale per il lemma precedente è la connessione tra la risolubilità per radicali di una equazione algebrica e la risolubilità del gruppo di Galois del corrispondente polinomio. Come esempio di applicazione alla teoria di Galois della teoria dei gruppi di permutazioni dimostriamo il seguente:

6.30. Teorema. *Sia $f \in F[x]$ un polinomio irriducibile di grado primo su un campo F di caratteristica 0, e sia L il campo di riducibilità completa di f rispetto a F. Allora l'equazione $f(x) = 0$ è risolubile per radicali se e solo se, scelte comunque due radici distinte α e β di f in L, si ha $L = F(\alpha, \beta)$.*

Dimostrazione — Sia G il gruppo di Galois di L su F; sappiamo che $f(x) = 0$ è risolubile per radicali se e solo se G è risolubile. Sappiamo anche che G agisce in modo fedele e transitivo sull'insieme X delle radici di f in L, e che $|X|$ è pari al grado di f, un numero primo. Possiamo quindi applicare il Lemma 6.29; otteniamo che $f(x) = 0$ è risolubile per radicali se e solo se, scelti comunque due elementi distinti α e β di X, si ha $\mathrm{St}_G\big(\{\alpha, \beta\}\big) = 1$. Ora, lo stabilizzante in G di una parte Y di X coincide con lo stabilizzante in G del campo $F(Y)$, e questo è il gruppo di Galois di L su $F(Y)$. Per il teorema fondamentale della teoria di Galois quest'ultimo è identico se e solo se $F(Y) = L$. Pertanto, per ogni α, $\beta \in X$, vale $\mathrm{St}_G\big(\{\alpha, \beta\}\big) = 1$ se e solo se $L = F(\alpha, \beta)$. L'asserto è ora ovvio. ❑

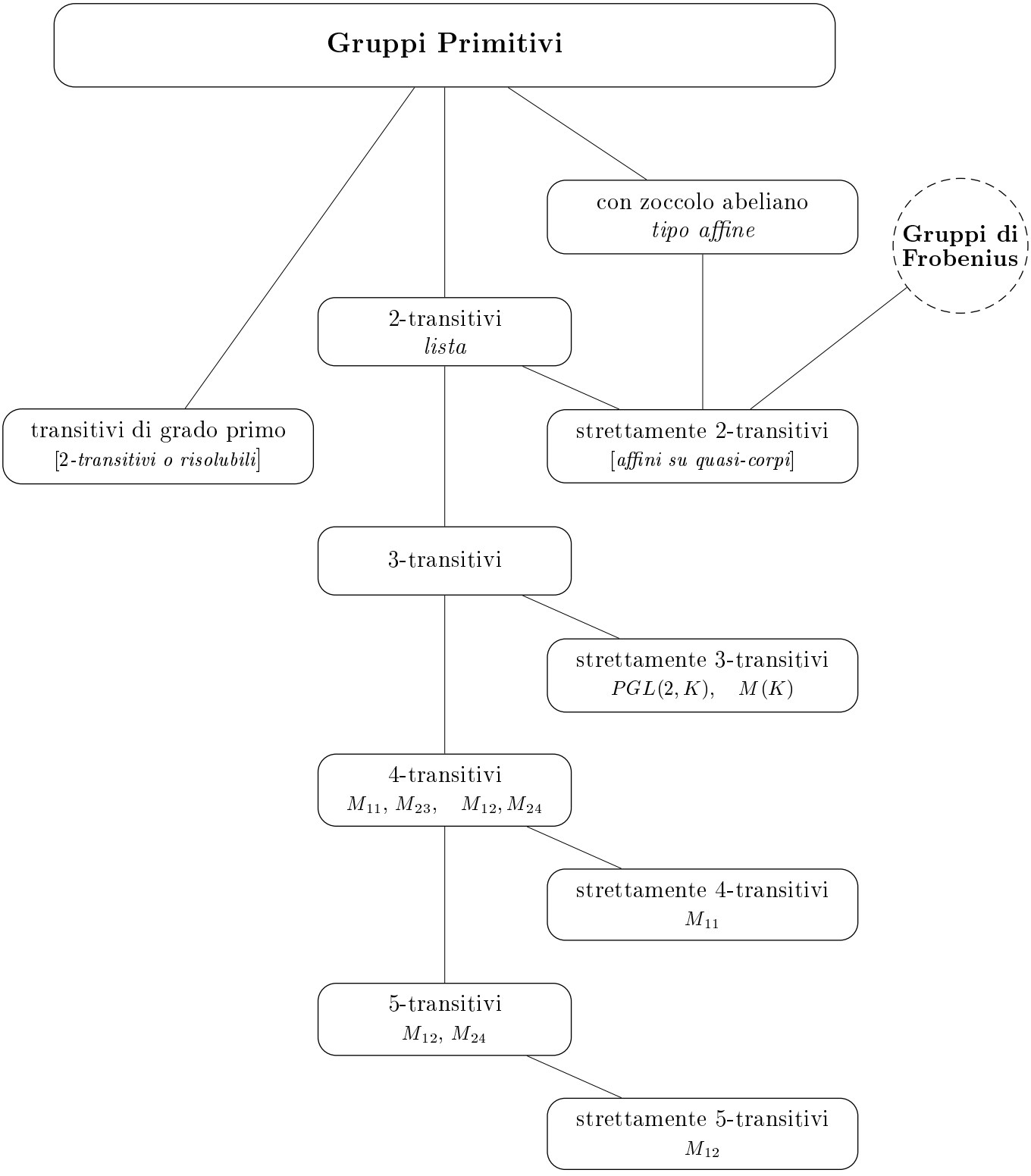
Per i gruppi transitivi di grado primo non risolubili (cioè non di tipo affine) vale:

6.31. Teorema (Burnside). *Ogni gruppo transitivo di permutazioni di grado primo che non sia risolubile è 2-transitivo.*

Esercizio. Verificare che, a meno di similitudini, se p è un numero primo l'unico gruppo risolubile di permutazioni 2-transitivo di grado p è il gruppo affine su uno spazio vettoriale di ordine p.

Lo schema nella pagina seguente riassume la classificazione ottenuta per alcuni tipi di gruppi finiti di permutazioni, con l'esclusione di quelli simmetrici o alterni, le cui proprietà di transitività multipla sono note da 4.3.

Classificazione di gruppi finiti di permutazioni, esclusi simmetrici e alterni



7. Struttura dei gruppi simmetrici

In questa sezione sono raccolti alcuni teoremi che descrivono la struttura gruppale del gruppo simmetrico, il gruppo di *tutte* le permutazioni su un dato insieme.

La prima, ovvia, domanda è: quanti elementi ha $Sym\, X$? Se X è finito di ordine n, la risposta è ben nota: $|Sym\, X| = n!$. Nel caso infinito si ha invece:

7.1. *Sia X un insieme infinito. Allora $|Sym\, X| = 2^{|X|}$.*

Dimostrazione — L'applicazione che ad un elemento di $Sym\, X$ associa il suo grafico è un'applicazione iniettiva da $Sym\, X$ a $\mathcal{P}(X \times X)$. Poiché X è infinito $|X \times X| = |X|$, quindi $|\mathcal{P}(X \times X)| = 2^{|X|}$ e $|Sym\, X| \leq 2^{|X|}$. Per provare la disuguaglianza opposta, sia $\mathcal{P}^*$ l'insieme delle parti di X che non sono singletons. Chiaramente $|\mathcal{P}^*| = |\mathcal{P}(X)| = 2^{|X|}$ (infatti $\mathcal{P}(X) = \mathcal{P}^* \cup S$, dove S, l'insieme dei singletons degli elementi di X, è equipotente a X). Per ogni $Y \in \mathcal{P}^*$ esiste una permutazione $\sigma \in Sym\, X$ tale che $\mathrm{supp}(\sigma) = Y$. Infatti, se Y è finito basta scegliere come σ un ciclo di supporto Y, se Y è infinito si può, ad esempio, ripartire Y nell'unione disgiunta di due insiemi Y_1 e Y_2 entrambi equipotenti ad Y; esiste allora una biezione $f : Y_1 \to Y_2$ e si può porre $\sigma = \prod_{y \in Y_1} (y\ yf)$. Allora l'applicazione $\sigma \in Sym\, X \mapsto \mathrm{supp}(\sigma) \in \mathcal{P}^*$, ben definita per l'esercizio 8 di p. 2, è suriettiva, sicché $|Sym\, X| \geq |\mathcal{P}^*| = 2^{|X|}$, il che prova l'asserto. ❑

Notiamo di passaggio che la dimostrazione appena fornita prova anche che $\left|X^X\right| = 2^{|X|} = |Sym\, X|$ per ogni insieme infinito X. Verrà di nuovo utile il fatto, provato nel corso della dimostrazione stessa, che ogni parte di X che non sia un singleton è il supporto di una permutazione di X.

Ben sappiamo (cfr. 3.3) che due insiemi equipotenti X e Y dànno luogo a gruppi simmetrici $Sym\, X$ e $Sym\, Y$ tra loro isomorfi. Escludendo il caso banale dell'insieme vuoto vale anche l'inverso: se X e Y sono insiemi tali che $Sym\, X \simeq Sym\, Y$, allora $|X| = |Y|$. Questo è del tutto ovvio nel caso degli insiemi finiti. Infatti, se X è un insieme di ordine finito $n > 0$ e Y è un altro insieme non vuoto tale che $Sym\, X \simeq Sym\, Y$, allora $|Sym\, Y| = |Sym\, X| = n!$; in particolare anche Y è finito, e $n! = |Y|!$. Poiché n e $|Y|$ sono entrambi diversi da zero si ha $|Y| = n$, come desiderato. L'ipotesi che X e Y non siano vuoti è naturalmente necessaria: i gruppi simmetrici del vuoto e dei singletons sono gruppi identici, quindi isomorfi tra loro. È meno immediato dimostrare lo stesso enunciato nel caso che X sia infinito, lo faremo in 7.7 utilizzando i prossimi risultati sulla struttura normale dei gruppi simmetrici.(*)

Iniziamo con il famoso teorema, dovuto per il caso finito a Galois, secondo il quale il gruppo alterno su un insieme con più di quattro elementi è sempre semplice. Alla dimostrazione di questo premettiamo un lemma che, in gruppi di permutazioni, lega proprietà relative all'azione permutazionale alla proprietà gruppale di essere un gruppo semplice.

7.2. Lemma. *Sia G un gruppo primitivo di permutazioni non identico privo di sottogruppi normali regolari e sia H lo stabilizzante in G di un punto. Se H è semplice allora anche G è semplice.*

Dimostrazione — Sia N un sottogruppo normale non identico di G. Certamente N è transitivo per 5.3, allora $G = NH$ per 1.10. Essendo $N \cap H \lhd H$ e H semplice, si ha $N \cap H = 1$ o $N \cap H = H$. Nel primo caso N è regolare, la qual cosa è esclusa dall'ipotesi. Si verifica allora la seconda eventualità, dunque $H \leq N$, ma allora da $G = HN$ segue $N = G$. È così provato che gli unici sottogruppi normali di G sono quelli banali, cioè G è semplice. ❑

7.3. Teorema (Galois). *Sia X un insieme. Se $|X| \geq 5$ oppure $|X| = 3$ allora $AltX$ è semplice.*

Dimostrazione — Consideriamo in primo luogo il caso in cui $n = |X|$ sia finito. Allora $AltX \simeq \mathbb{A}_n$. Il caso $n = 3$ è banale: sappiamo che $\mathbb{A}_3$ ha ordine 3, quindi è semplice. Sia ora $n = 5$ e sia $1 \neq N \lhd \mathbb{A}_5$; dobbiamo provare $N = \mathbb{A}_5$. Sappiamo da 4.3 e 5.7 che $\mathbb{A}_5$ è 3-transitivo e quindi primitivo, dunque N è transitivo e $|N|$ è multiplo di 5 per 1.1 (*vi*). Sia P un 5-sottogruppo di Sylow di N. Allora, poiché 5 è la massima potenza di 5 che divide $60 = |\mathbb{A}_5|$, certamente P è anche un 5-sottogruppo di Sylow di $\mathbb{A}_5$. Sia $L = N_{\mathbb{A}_5}(P)$. L'indice di L in $\mathbb{A}_5$ è pari al numero dei 5-sottogruppi di Sylow di $\mathbb{A}_5$, i quali sono 6: lo si verifica contando i 5-cicli in $\mathbb{S}_5$, oppure come semplice applicazione del terzo teorema di Sylow. Inoltre $\mathbb{A}_5 = NL$ per 1.11, sicché $|N : N \cap L| = |NL : L| = |\mathbb{A}_5 : L| = 6$. Allora 6 divide $|N|$,(♮) quindi $|N|$ è multiplo di 30 e $|\mathbb{A}_5/N| \leq 2$. Sia t un 3-ciclo in $\mathbb{A}_5$. Allora $t^{-1} = t^2 \in N$, sicché $t \in N$. Pertanto N contiene tutti i 3-cicli di $\mathbb{A}_5$ e quindi $N = \mathbb{A}_5$ per 2.6, come si voleva (si è qui ripetuto il ragionamento già svolto nella nota di p. 18).

Supponiamo ora $n > 5$. Possiamo ragionare per induzione su n, assumendo il teorema dimostrato per il gruppo alterno su $n-1$ oggetti. Utilizzando ancora 4.3 e 5.7 ricaviamo che $\mathbb{A}_n$ è un gruppo primitivo $(n-2)$-transitivo, quindi per lo meno 4-transitivo, e dunque, per 6.10, privo di sottogruppi normali regolari (nel caso $n = 6$ ciò dipende dal

(*) se valesse l'implicazione '$2^\kappa = 2^\lambda \Longrightarrow \kappa = \lambda$', per ogni coppia di cardinali infiniti κ e λ, allora sarebbe immediata la dimostrazione di 7.7 anche nel caso di insiemi infiniti: basterebbe ragionare come nel caso finito utilizzando 7.1. Purtroppo non è possibile dimostrare tale implicazione, a meno di non adottare una teoria degli insiemi con assiomi molto forti, come l'ipotesi generalizzata del continuo.

(♮) dimostrazione alternativa: i 5-sottogruppi di Sylow di $\mathbb{A}_5$ sono 6 e sono tutti contenuti in N, perché sono tra loro coniugati in $\mathbb{A}_5$ e $N \lhd \mathbb{A}_5$; allora i 5-sottogruppi di Sylow di N sono 6, dunque 6 divide $|N|$.

fatto che, essendo $\mathbb{A}_6 \not\simeq \mathbb{S}_4$, il caso (*iii*) di 6.10 non si può verificare). Lo stabilizzante di un punto in $\mathbb{A}_n$ è ovviamente isomorfo a $\mathbb{A}_{n-1}$, che è semplice per ipotesi di induzione, dunque 7.2 prova che $\mathbb{A}_n$ è semplice.

È così provato che $AltX$ è semplice se X è finito, purché sia verificata la condizione su $|X|$ di cui all'enunciato. Supponiamo ora X infinito. Sia $1 \neq N \lhd AltX$; dobbiamo provare che N coincide con $AltX$. Indichiamo con $\mathcal{F}$ l'insieme delle parti finite di X di cardinalità maggiore di 4. Per ogni $Y \in \mathcal{F}$ sia $A_Y := \mathrm{St}_{AltX}(X \smallsetminus Y)$. L'isomorfismo da $\mathrm{St}_{Sym\,X}(X \smallsetminus Y)$ a $Sym\,Y$ introdotto in 1.7 induce un isomorfismo da A_Y a $AltY$, quindi A_Y è semplice, per ogni $Y \in \mathcal{F}$. Inoltre, come è facile verificare, $AltX = \bigcup_{Y\in\mathcal{F}} A_Y$. Essendo $N \neq 1$, esiste $Y_0 \in \mathcal{F}$ tale che $N \cap A_{Y_0} \neq 1$. Per ogni $Y \in \mathcal{F}$ si ha, ovviamente, $A_{Y\cup Y_0} \geq A_{Y_0}$, quindi $N \cap A_{Y\cup Y_0} \neq 1$. Poiché $N \cap A_{Y\cup Y_0} \lhd A_{Y\cup Y_0}$ e $A_{Y\cup Y_0}$ è semplice, allora $N \cap A_{Y\cup Y_0} = A_{Y\cup Y_0}$, cioè $N \supseteq A_{Y\cup Y_0}$; inoltre $A_{Y\cup Y_0} \geq A_Y$, sicché $N \supseteq A_Y$. Allora $N \supseteq \bigcup_{Y\in\mathcal{F}} A_Y = AltX$, cioè $N = AltX$, come si voleva dimostrare. ❑

Esercizio. È stato riportato, ma non dimostrato, il fatto che i cinque gruppi di Mathieu sono semplici. Assumendo la semplicità dei soli M_{11} e M_{22} (e le altre proprietà di questi gruppi esposte), provare che anche gli altri tre gruppi di Mathieu sono semplici.

Il risultato ottenuto in 7.3 si completa osservando che, nei casi indicati nell'enunciato, il gruppo alterno è il minimo sottogruppo normale non identico di $Sym\,X$. Infatti si ha:

7.4. *Se X è un insieme e $|X| > 2$, il centralizzante in $Sym\,X$ di $FSymX$ è il sottogruppo identico. In particolare $Z(Sym\,X) = Z(FSymX) = 1$. Se poi $|X| > 3$, anche il centralizzante in $Sym\,X$ di $AltX$ è il sottogruppo identico, e $Z(AltX) = 1$.*

Dimostrazione — Sia f una permutazione non identica su X. Esiste $x \in X$ tale che $xf \neq x$; poiché $|X| > 2$, esiste $y \in X \smallsetminus \{x, xf\}$. Sia σ la trasposizione $(x\,y)$. Allora $\sigma^f = (xf\ yf)$ e $\sigma \neq \sigma^f$, perché xf è diverso sia da x che da y. Dunque σ non commuta con f, quindi $f \notin C_{Sym\,X}(FSymX)$. Se poi $|X| > 3$, possiamo scegliere in X un elemento $z \notin \{x, xf, y\}$. Allora, ragionando come sopra, si verifica che il 3-ciclo $(x\,y\,z)$ non commuta con f, quindi $f \notin C_{AltX}(FSymX)$. L'ovvia osservazione che $C_{Sym\,X}(FSymX)$ contiene $Z(Sym\,X)$ e $Z(FSymX)$, e $Z(AltX) \leq C_{AltX}(FSymX)$ completa la dimostrazione. ❑

7.5. Corollario. *Sia X un insieme. Se $|X| \geq 5$ oppure $|X| = 3$ allora $AltX$ è il monolite di $Sym\,X$ ed è l'unico sottogruppo normale non banale di $FSymX$.*

Dimostrazione — Poiché $AltX$ è semplice, siamo certi che $AltX$ è un sottogruppo normale minimale sia in $Sym\,X$ che in $FSymX$. Se $|X| \geq 5$ allora 7.4 mostra che il centralizzante di $AltX$ in $Sym\,X$ (e quindi, a maggior ragione, il centralizzante di $AltX$ in $FSymX$) è identico; se $|X| = 3$ la struttura di $\mathbb{S}_3$ mostra che questo centralizzante è $AltX$ stesso. Allora, in ciascun caso, $C_{Sym\,X}(AltX) = C_{FSym\,X}(AltX) \leq AltX$. Per l'esercizio 2 di p. 34 ciò implica che $AltX$ è il monolite sia di $Sym\,X$ che di $FSymX$. Il fatto che $AltX$ è l'unico sottogruppo normale non banale di $FSymX$ è una facile conseguenza. Infatti $|\,FSymX : AltX\,| = 2$ e quindi $AltX$ è un sottogruppo massimale di $FSymX$. Allora, se $1 \neq N \lhd FSymX$ da $AltX \leq N$ segue $N = AltX$ o $N = FSymX$. ❑

Ovviamente 7.5 dice, nel caso in cui X sia finito, che $\mathbb{A}_n$ è l'unico sottogruppo normale non banale di $\mathbb{S}_n$, con le sole eccezioni dei casi $n \leq 2$ (per i quali $\mathbb{A}_n = 1$) e $n = 4$, (come è noto, i sottogruppi normali non banali di $\mathbb{S}_4$ sono due: $\mathbb{A}_4$ ed il 2-sottogruppo di Sylow di quest'ultimo, isomorfo a V_4). Osserviamo anche che, in ogni caso, $AltX$ è un sottogruppo caratteristico di $Sym\,X$.

Si può utilizzare il Corollario 7.5 per risolvere la questione lasciata in sospeso all'inizio di questa sezione. Osserviamo che:

7.6. *Sia X un insieme infinito. Allora $|\,AltX\,| = |\,FSymX\,| = |X|$.*

Dimostrazione — Analogamente a quanto fatto nella parte conclusiva della dimostrazione di 7.3, poniamo $S_Y := \mathrm{St}_{Sym\,X}(X \smallsetminus Y)$ per ogni Y appartenente all'insieme $\mathcal{P}_{\mathrm{f}}(X)$ delle parti finite di X. Ovviamente $FSymX = \bigcup_{Y\in\mathcal{P}_{\mathrm{f}}(X)} S_Y$ e ciascuno dei sottogruppi S_Y è finito. Pertanto $FSymX$ è unione di una famiglia di insiemi finiti indiciata in $\mathcal{P}_{\mathrm{f}}(X)$. Essendo $\mathcal{P}_{\mathrm{f}}(X)$ equipotente a X si ha $|\,FSymX\,| \leq |X|$. La disuguaglianza opposta è ovvia (perché?), dunque $|\,FSymX\,| = |X|$. Infine, da $|\,FSymX : AltX\,| = 2$ segue $|\,AltX\,| = |\,FSymX\,|$. ❑

7.7. *Dati comunque due insiemi non vuoti X e Y si ha: $Sym\,X \simeq Sym\,Y \iff |X| = |Y|$.*

Dimostrazione — Essendo il resto dell'enunciato già chiarito, è da provare che se X e Y sono insiemi infiniti ed esiste un isomorfismo $\alpha : Sym\,X \xrightarrow{\sim} Sym\,Y$ allora $|X| = |Y|$. Per 7.5 l'immagine mediante α di $AltX$, l'intersezione dei sottogruppi normali non identici di $Sym\,X$, è $AltY$, l'intersezione dei sottogruppi normali non identici di $Sym\,Y$. Dunque $AltX$ e $AltY$ sono isomorfi. Per 7.6 si ha allora $|X| = |\,AltX\,| = |\,AltY\,| = |Y|$. ❑

Sottogruppi normali

Nel caso infinito, la prima parte dell'enunciato del Corollario 7.5 è un caso particolare di un teorema di Reinhold Baer (1902–1979) che descrive completamente la struttura normale dei gruppi simmetrici su infiniti. Se X è un insieme infinito, oltre ai sottogruppi banali ed a $Alt X$ già conosciamo un sottogruppo normale di $Sym\, X$: il gruppo finitario $FSym X$. Si ottengono altri sottogruppi normali generalizzando la definizione di $FSym X$. Infatti, per ogni cardinale infinito κ,

$$Sym_\kappa X := \{\sigma \in Sym\, X \;\big|\; |\operatorname{supp}(\sigma)| < \kappa\}$$

è un sottogruppo normale di $Sym\, X$. Chiaramente $Sym_{\aleph_0} X = FSym X$ e, supponendo sempre κ infinito, se $\kappa < \lambda \leq |X|$ allora $Sym_\kappa X < Sym_\lambda X$, perché ogni permutazione di X il cui supporto abbia cardinalità κ (ne esistono certamente; si veda l'osservazione che segue la dimostrazione di 7.1) appartiene a $Sym_\lambda X$ ma non a $Sym_\kappa X$. Per motivi analoghi, $Sym_\kappa X = Sym\, X$ se e solo se $\kappa > |X|$.

7.8. Teorema (Baer, 1934). *Se X è un insieme infinito, i sottogruppi normali non banali di $Sym\, X$ sono tutti e soli $Alt X$ ed i sottogruppi $Sym_\kappa X$ con κ cardinale infinito minore o uguale a $|X|$.*

Si ricava da questo teorema che i sottogruppi normali di $Sym\, X$ costituiscono una catena ben ordinata e sono tutti caratteristici in $Sym\, X$ (notare che ciò è vero anche nel caso in cui X sia finito).

La dimostrazione del Teorema di Baer è in parte basata sui prossimi due lemmi, piuttosto interessanti anche per proprio conto.

7.9. *Siano σ e τ due permutazioni sullo stesso insieme, tali che $\big|\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau)\big| = 1$. Allora il commutatore $[\sigma,\tau] = \sigma^{-1}\sigma^\tau$ è un 3-ciclo.*

Dimostrazione — Si ponga $S_\sigma = \operatorname{supp}(\sigma)$, $S_\tau = \operatorname{supp}(\tau)$ e $S_\sigma \cap S_\tau = \{a\}$. Sia poi $\Sigma = \operatorname{supp}\big([\sigma,\tau]\big)$. Da momento che $\operatorname{supp}(\sigma^{-1}) = S_\sigma$ e $\operatorname{supp}(\sigma^\tau) = S_\sigma\tau$, da $[\sigma,\tau] = \sigma^{-1}\sigma^\tau$ segue $\Sigma \subseteq S_\sigma \cup S_\sigma\tau$. Analogamente, poiché $[\sigma,\tau] = (\tau^{-1})^\sigma\tau$, si ha $\Sigma \subseteq S_\tau\sigma \cup S_\tau$. Pertanto

$$\Sigma \subseteq (S_\sigma \cup S_\sigma\tau) \cap (S_\tau\sigma \cup S_\tau) = (S_\sigma \cap S_\tau) \cup (S_\sigma\tau \cap S_\tau) \cup (S_\sigma \cap S_\tau\sigma) \cup (S_\sigma\tau \cap S_\tau\sigma). \qquad (\star)$$

Ora, $S_\tau^* := S_\tau \smallsetminus \{a\} \subseteq \operatorname{Fix}(\sigma)$. Quindi $S_\tau\sigma = S_\tau^* \cup \{a\sigma\}$ e $S_\sigma \cap S_\tau^* = \varnothing$, dunque $S_\sigma \cap S_\tau\sigma = \{a\sigma\}$. Analogamente $S_\sigma\tau \cap S_\tau = \{a\tau\}$. Inoltre $S_\sigma\tau \cap S_\tau\sigma = (S_\sigma^* \cup \{a\tau\}) \cap (S_\tau^* \cup \{a\sigma\}) = \{a\sigma, a\tau\}$, dove $S_\sigma^* = S_\sigma \smallsetminus \{a\}$ è definito similmente a S_τ^*. La $(\star)$ fornisce allora $\operatorname{supp}\big([\sigma,\tau]\big) = \Sigma \subseteq \{a, a^\sigma, a^\tau\}$. Da $a\sigma^{-1} \notin S_\tau$ segue $a[\sigma,\tau] = (a\sigma^{-1})\tau^{-1}\sigma\tau = (a\sigma^{-1})\sigma\tau = a\tau$; poiché $a\tau \notin S_\sigma$ si ha poi $a\tau[\sigma,\tau] = (a\tau)\sigma^{-1}\tau^{-1}\sigma\tau = a\tau\tau^{-1}\sigma\tau = a\sigma\tau = a\sigma$, avendo usato anche $a\sigma \notin S_\tau$. Di conseguenza $a, a\sigma, a\tau \in \operatorname{supp}\big([\sigma,\tau]\big)$, quindi $\operatorname{supp}\big([\sigma,\tau]\big) = \{a, a^\sigma, a^\tau\}$ e $a\sigma[\sigma,\tau] = a$, sicché $[\sigma,\tau] = (a\ a\sigma\ a\tau)$ è un 3-ciclo. ❑

7.10. *Ogni permutazione σ si può scrivere come il prodotto di due permutazioni α e β tali che $\alpha^2 = \beta^2 = 1$ e $\operatorname{supp}(\sigma) = \operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$.*

Dimostrazione — È chiaro che σ e σ^{-1} hanno la stessa struttura ciclica e quindi sono coniugate (cfr. esercizio 2, p. 11). Si ha dunque $\sigma^\alpha = \sigma^{-1}$ per un opportuna permutazione α. È possibile scegliere α in modo che $\operatorname{supp}(\alpha) \subseteq \operatorname{supp}(\sigma)$ e $\alpha^2 = 1$. Infatti, se la decomposizione di σ in cicli disgiunti non identici è $\sigma = \prod_{i\in I} \sigma_i$ basta porre $\alpha = \prod_{i\in I} \alpha_i$, dove ciascun α_i è definito come segue: scritto σ_i come

$$\begin{aligned}
&(\cdots\ x_{-n}\ \cdots\ x_{-2}\ x_{-1}\ x_0\ x_1\ x_2\ \cdots\ x_n\ \cdots), && \text{se di lunghezza infinita,}\\
&(x_{-n}\ \cdots\ x_{-2}\ x_{-1}\ x_0\ x_1\ x_2\ \cdots\ x_n), && \text{se di lunghezza finita dispari,}\\
&(x_{-n}\ \cdots\ x_{-2}\ x_{-1}\ x_1\ x_2\ \cdots\ x_n), && \text{se di lunghezza finita pari,}
\end{aligned}$$

α_i è la permutazione che manda ciascun x_j in x_{-j} e lascia fissati i punti di $\operatorname{Fix}(\sigma_i)$. È chiaro che in questo modo si ha $\sigma_i^{\alpha_i} = \sigma_i^{-1}$ per ogni $i \in I$, e quindi $\sigma^\alpha = \sigma^{-1}$, e che $\alpha^2 = 1$ e $\operatorname{supp}(\alpha) \subseteq \operatorname{supp}(\sigma)$. Sia ora $\beta = \alpha\sigma$. Allora $\alpha\beta = \alpha(\alpha\sigma) = \alpha^2\sigma = \sigma$ e $\beta^2 = (\alpha\sigma\alpha)\sigma = \sigma^\alpha\sigma = \sigma^{-1}\sigma = 1$. Inoltre $\operatorname{supp}(\beta) \subseteq \operatorname{supp}(\alpha) \cup \operatorname{supp}(\sigma) = \operatorname{supp}(\sigma)$, sicché $\operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta) \subseteq \operatorname{supp}(\sigma)$; d'altra parte da $\sigma = \alpha\beta$ segue $\operatorname{supp}(\sigma) \subseteq \operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$, e con questo la dimostrazione è completa. ❑

7.11. *Siano X un insieme e κ un cardinale infinito minore o uguale a $|X|$. Allora $Sym_{\kappa^+} X$ è generato dagli elementi σ di $Sym\, X$ di periodo 2 tali che $|\operatorname{supp}(\sigma)| = \kappa$ e $\operatorname{Fix}(\sigma) = |X|$.*[♮]

Dimostrazione — Da 7.10 segue subito che $Sym_{\kappa^+} X$ è il sottogruppo di $Sym\, X$ generato dalle permutazioni τ di periodo 2 tali che $|\operatorname{supp}(\tau)| \leq \kappa$. Basta dunque mostrare che ogni tale τ appartiene a

$$\Gamma := \big\langle\, \sigma \in Sym\, X \;\big|\; \sigma^2 = 1 \wedge |\operatorname{supp}(\sigma)| = \kappa \wedge |\operatorname{Fix}(\sigma)| = |X| \,\big\rangle.$$

[♮] Si indica con κ^+ il minimo cardinale maggiore di κ. Quindi $Sym_{\kappa^+} X$ è costituito da tutte e sole le permutazioni di X il cui supporto abbia cardinalità minore o uguale a κ. L'esistenza di κ^+ è garantita dal fatto che esistono cardinali maggiori di κ (ad esempio, 2^κ) e *ogni collezione non vuota di numeri cardinali ha minimo.*

Supponiamo in primo luogo $|\operatorname{Fix}(\tau)| = |X|$. Allora $\operatorname{Fix}(\tau)$ è unione disgiunta di due insiemi Y e Z tali che $|Y| = \kappa$ e $|Z| = |X|$. Come nella dimostrazione di 7.1, possiamo costruire una permutazione σ di periodo 2 e supporto Y. Chiaramente σ è disgiunta da τ, quindi $(\sigma\tau)^2 = 1$, e sia $\operatorname{supp}\sigma = Y$ che $\operatorname{supp}(\sigma\tau) = Y \cup \operatorname{supp}(\sigma)$ hanno cardinalità κ, mentre Z è contenuto sia in $\operatorname{Fix}(\sigma)$ che in $\operatorname{Fix}(\sigma\tau)$, i quali hanno così cardinalità $|X|$. Pertanto $\sigma, \sigma\tau \in \Gamma$. Inoltre $\tau = \sigma(\sigma\tau)$, dunque, in questo caso, $\tau \in \Gamma$. Supponiamo ora che si verifichi l'altra possibilità: $|\operatorname{Fix}(\tau)| < |X|$. Da $X = \operatorname{Fix}(\tau) \cup \operatorname{supp}(\tau)$ segue $|X| = |\operatorname{supp}(\tau)| = \kappa$. Allora, se $\tau = \prod_{i\in I} \tau_i$ è la decomposizione di τ in trasposizioni disgiunte non identiche, certamente $|I| = \kappa$ e I è unione disgiunta di due sue parti J e J' entrambe di cardinalità κ. Allora $\sigma := \prod_{i\in J} \sigma_i$ e $\sigma' := \prod_{i\in J'} \sigma_i$ appartengono a Γ (hanno periodo 2, supporto ed insieme dei punti fissi di cardinalità $\kappa = |X|$), quindi $\tau = \sigma\sigma' \in \Gamma$. ❑

7.12. *Siano X un insieme e σ una permutazione su X di supporto infinito. Posto $\kappa = |\operatorname{supp}(\sigma)|$, la chiusura normale di $\langle\sigma\rangle$ in $Sym_{\kappa^+} X$ è $Sym_{\kappa^+} X$.*

Dimostrazione — Osserviamo innanzitutto che $N := \langle\sigma\rangle^{Sym_{\kappa^+} X}$ è normale in $Sym X$. Infatti, in generale, come è immediato verificare, se α e β sono permutazioni di X con la stessa struttura ciclica, non solo α e β sono coniugate in $Sym X$, ma $\alpha^\gamma = \beta$ per un opportuna permutazione γ il cui supporto è contenuto in $\operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$. Quindi, se $\alpha \in N$ e $\gamma \in Sym X$, allora, avendo α e α^γ la stessa struttura ciclica ed essendo $|\operatorname{supp}(\alpha) \cup \operatorname{supp}(\alpha^\gamma)| \le \kappa$, si ha $\alpha^\gamma = \alpha^{\gamma_1}$ per un opportuno $\gamma_1 \in Sym_{\kappa^+} X$, dunque $a^\gamma \in N$ perché $N \lhd Sym_{\kappa^+} X$; pertanto $N \lhd Sym X$.

Allo scopo di provare l'enunciato (cioè: $N = Sym_{\kappa^+} X$), per 7.11 è sufficiente provare che N contiene tutte le permutazioni σ' di periodo 2 tali che $|\operatorname{supp}(\sigma')| = \kappa$ e $|\operatorname{Fix}(\sigma')| = |X|$. Ma queste permutazioni hanno tutte la stessa struttura ciclica e costituiscono quindi una classe di coniugio in $Sym X$; essendo $N \lhd Sym X$ basterà allora mostrare che N contiene almeno *una* tale permutazione σ'.

La dimostrazione è divisa in passi, in ciascuno dei quali viene costruita una permutazione appartenenete a N, sempre più vicina a verificare le proprietà richieste per σ'.

(1) *N contiene una permutazione σ' con κ orbite di lunghezza maggiore di* 1.

Sia Ω l'insieme delle σ-orbite di lunghezza maggiore di 1 (cioè contenute in $\operatorname{supp}(\sigma)$). Se Ω è infinito, poiché $\operatorname{supp}(\sigma) = \bigcup_{Y\in\Omega} Y$ e ciascun $Y \in \Omega$ è al più numerabile, si ha $\kappa = |\operatorname{supp}(\sigma)| = |\Omega|$, e basta quindi porre $\sigma' = \sigma$. Se invece Ω è finito, σ è prodotto di un numero finito di cicli a due a due disgiunti. Essendo $\operatorname{supp}(\sigma)$ infinito, almeno uno di questi cicli ha lunghezza infinita e $\kappa = \aleph_0$. Si ponga allora $\sigma = \alpha\gamma$ con $\gamma = (\cdots\ x_{-n}\ \cdots\ x_{-1}\ x_0\ x_1\ \cdots\ x_n\ \cdots)$ disgiunto da α. Sia $\gamma_1 = \gamma^\tau$ dove τ è la permutazione $\prod_{n\in\mathbb{N}}(x_{2n}\ x_{-2n})$, sicché

$$\gamma_1 = (\cdots\ x_{-(2n+1)}\ x_{2n}\ \cdots\ x_{-3}\ x_2\ x_{-1}\ x_0\ x_1\ x_{-2}\ x_3\ \cdots\ x_{-2n}\ x_{2n+1}\ \cdots)$$

manda x_{2n} in x_{-2n+1} e x_{2n-1} in x_{-2n} per ogni $n \in \mathbb{Z}$. Evidentemente $\sigma_1 := \alpha\gamma_1$ ha la stessa struttura ciclica di σ, quindi appartiene a N. Allora $\sigma' := \gamma^{-1}\gamma_1 = \sigma^{-1}\sigma_1 \in N$. Per ogni $n \in \mathbb{Z}$ si ha $x_{2n}\sigma' = x_{-2n}$, sicché $\{x_{2n}, x_{-2n}\}$ è una σ'-orbita. Allora N contiene un elemento, appunto σ', con κ (in questo caso pari a $\aleph_0$) orbite di lunghezza maggiore di 1.

Quanto dimostrato al passo (1) dice, in sostanza, che per dimostrare il nostro enunciato possiamo supporre che σ abbia κ orbite di lunghezza maggiore di 1. Infatti, supposto dimostrato l'enunciato in questo caso, si avrà $Sym_{\kappa^+} X = \langle\sigma'\rangle^{Sym_{\kappa^+} X}$, dove σ' è l'elemento scelto come in (1); ovviamente però $\langle\sigma'\rangle^{Sym_{\kappa^+} X} \le N$, quindi $N = Sym_{\kappa^+} X$. Analogo senso hanno le affermazioni che proveremo ai prossimi passi.

(2) *N contiene una permutazione σ' con κ orbite di lunghezza maggiore di* 1 *e tale che* $|\operatorname{Fix}(\sigma')| = |X|$.

Possiamo infatti supporre che σ abbia κ orbite di lunghezza maggiore di 1. Se $|\operatorname{Fix}(\sigma)| = |X|$ basta porre $\sigma' = \sigma$; supponiamo allora anche $|\operatorname{Fix}(\sigma)| < |X|$. Come nella dimostrazione di 7.11 ne deduciamo $|X| = \kappa$. Ora, σ si decompone nel prodotto di κ cicli disgiunti non identici; è possibile raggruppare a due a due le trasposizioni che appaiono tra questi cicli in modo da scrivere σ come prodotto di permutazioni disgiunte: $\sigma = \prod_{i\in I} \sigma_i$, dove ciascuno dei σ_i è o un ciclo non identico oppure il prodotto di due trasposizioni disgiunte e tra i σ_i che sono cicli al più uno è una trasposizione. Naturalmente $|I| = \kappa$. Esiste allora una parte J di I tale che $|J| = |I \setminus J| = \kappa$. Definiamo $\tau = \prod_{i\in I} \tau_i \in Sym X$ ponendo:

$$\tau_i = \sigma_i^{-1},\ \text{se } i \in I \setminus J \qquad \tau_i = \begin{cases} \sigma_i, & \text{se } \sigma_i \text{ è un ciclo;} \\ (a\,c)(b\,d), & \text{se } \sigma_i \text{ ha la forma } (a\,b)(c\,d); \end{cases} \quad \text{se } i \in I,$$

in modo che τ abbia la stessa struttura ciclica di σ e, così, appartenga a N. Allora $\sigma' := \sigma\tau \in N$. Si ha chiaramente $\sigma' = \prod_{i\in I} \sigma_i\tau_i = \prod_{i\in J} \sigma_i\tau_i$, dal momento che $\sigma_i\tau_i = 1$ se $i \in I \setminus J$. Quindi, essendo $|I \setminus J| = \kappa = |X|$, certamente $|\operatorname{Fix}(\sigma)| = |X|$. Se $i \in J$ si ha $\sigma_i\tau_i = \sigma_i^2$ se σ_i è un ciclo, $\sigma_i\tau_i = (a\,d)(b\,c)$ se $\sigma_i = (a\,b)(c\,d)$; in particolare $\sigma_i\tau_i = 1$ per al più un valore di $i \in J$, quello per il quale σ_i è una trasposizione. Allora σ' è prodotto di κ permutazioni a due a due disgiunte, quindi ha almeno κ orbite di lunghezza maggiore di 1; non potendo essere più di $|\operatorname{supp}(\sigma')| \le \kappa$ esse sono proprio κ. Anche il secondo passo è stato completato.

(3) *N contiene una permutazione σ', prodotto di κ 3-cicli a due a due disgiunti e tale che* $|\operatorname{Fix}(\sigma')| = |X|$.

Possiamo supporre che σ verifichi le proprietà richieste per σ' al passo (2). Sia T una classe completa di rappresentanti delle σ-orbite di lunghezza maggiore di 1. Come nella dimostrazione di 7.11, $\operatorname{Fix}(\sigma)$ è unione disgiunta di due sue

parti Y e Z tali che $|Y| = \kappa$ e $|Z| = |X|$. Poiché $|T| = \kappa$ esiste un'applicazione biettiva $f : T \to Y$. Le trasposizioni $\tau_t = (t\ tf)$ al variare di $t \in T$ sono a due a due disgiunte ed è quindi lecito considerarne il prodotto $\tau = \prod_{t\in T} \tau_t$. Chiaramente $\sigma' := [\sigma, \tau] = \sigma^{-1}\sigma^\tau \in N$. Per ogni $t \in T$, tra i cicli che appaiono nella decomposizione di σ in cicli disgiunti indichiamo con σ_t quello che sposta t. Gli insiemi $\operatorname{supp}([\sigma_t, \tau_t]) \subseteq \operatorname{supp}(\sigma_t) \cup \{tf\}$ al variare di $t \in T$ sono a due a due disgiunti; da ciò segue $\sigma' = \prod_{t\in T}[\sigma_t, \tau_t]$. Per 7.9 ciascuno dei fattori $[\sigma_t, \tau_t]$ è un 3-ciclo. Poiché $|T| = \kappa$ e $\operatorname{Fix}(\sigma')$ contiene Z, equipotente a $|X|$, abbiamo costruito la permutazione desiderata.

(4) *N contiene una permutazione σ' di periodo 2 tale che $|\operatorname{supp}(\sigma')| = \kappa$ e $|\operatorname{Fix}(\sigma')| = |X|$.*

Per il passo precedente possiamo assumere che $\sigma = \prod_{i\in I}(a_i\, b_i\, c_i)$ sia un prodotto di 3-cicli disgiunti, con $|I| = \kappa$ e $|\operatorname{Fix}(\sigma)| = |X|$. Similmente a quanto fatto sopra, possiamo costruire un'applicazione iniettiva f da $\operatorname{supp}(\sigma)$ a $\operatorname{Fix}(\sigma)$ tale che $|\operatorname{Fix}(\sigma) \setminus \operatorname{im} f| = |X|$. Ponendo $d_i = if$ per ogni $i \in I$, si ha $\tau := \prod_{i\in I}(a_i\, b_i\, d_i) \in N$ (τ ha la stessa struttura ciclica di σ) e, per l'identità $(a_i\, b_i\, c_i)(a_i\, b_i\, d_i) = (a_i\, d_i)(b_i\, c_i)$, vale $\sigma' := \sigma\tau = \prod_{i\in I}(a_i\, d_i)(b_i\, c_i)$, una permutazione di periodo 2 appartenente a N. Chiaramente $|\operatorname{supp}(\sigma')| = |I| = \kappa$ e $\operatorname{Fix}(\sigma')$, contenendo $\operatorname{Fix}(\sigma) \setminus \operatorname{im} f$, è equipotente a $|X|$, come richiesto.

Le considerazioni svolte nella parte iniziale della dimostrazione spiegano perché da quest'ultima affermazione segue $N = Sym_{\kappa^+} X$. ❑

Otteniamo a questo punto la dimostrazione del seguente teorema, che contiene il Teorema 7.8 come caso particolare (perché $Sym_\lambda X = Sym X$ per $\lambda > |X|$).

7.13. Teorema. *Siano X un insieme infinito e λ un numero cardinale infinito. Allora i sottogruppi normali non identici di $Sym_\lambda X$ sono tutti e soli $AltX$ ed i sottogruppi $Sym_\kappa X$ con κ cardinale infinito minore o uguale a λ.*

Dimostrazione — Sia infatti H un sottogruppo normale non identico di $Sym_\lambda X$. Se $H \le FSymX$ allora $H \lhd FSymX$ (perché $FSymX \le Sym_\lambda X$) e H è uno tra $AltX$ e $FSymX = Sym_{\aleph_0} X$, per 7.5. Altrimenti, H contiene elementi di supporto infinito. Esistono cardinali infiniti ν tali che $H \le Sym_\nu X$, ad esempio ciò vale per $\nu = \lambda$. Sia κ il minimo tra tali cardinali ν. Ovviamente $\kappa \le \lambda$ e $H \le Sym_\kappa X$. Verifichiamo che vale anche l'inclusione opposta. Sia $\sigma \in Sym_\kappa X$. Allora $\zeta := |\operatorname{supp}(\sigma)| < \kappa$. Anche se ζ è infinito $H \not\le Sym_\zeta X$, per la definizione di κ, quindi H contiene un elemento τ tale che $\xi := |\operatorname{supp}(\tau)|$ sia infinito e $\zeta \le \xi$. Poiché $H \le Sym_\lambda X$, si ha $\xi < \lambda$, quindi $\xi^+ \le \lambda$ e $Sym_{\xi^+} X \le Sym_\lambda X$. Allora la chiusura normale di $\langle\tau\rangle$ in $Sym_{\xi^+} X$, che è $Sym_{\xi^+} X$ per 7.12, è contenuta nella chiusura normale di $\langle\tau\rangle$ in $Sym_\lambda X$, che è contenuta in H perché $H \lhd Sym_\lambda X$. Dunque $Sym_{\xi^+} X \le H$. Ma $\sigma \in Sym_{\xi^+} X$, perché $|\operatorname{supp}(\sigma)| = \zeta \le \xi < \xi^+$, quindi $\sigma \in H$. Ciò prova $H = Sym_\kappa X$. ❑

Esercizi.

1. Verificare in dettaglio che $Sym_\kappa X$ è un sottogruppo normale di $Sym X$ per ogni insieme X ed ogni cardinale infinito κ. Cosa succede se κ è finito?
2. Per ogni insieme X tale che $|X| \ne 4$, se $H \lhd K \lhd Sym X$ allora $H \lhd Sym X$.
3. Calcolare il commutatore $[\sigma, \tau]$, dove $\sigma = (1\ 2\ 3\ 7)(9\ 5\ 111) \in Sym\,\mathbb{Z}$ e τ è la permutazione di $\mathbb{Z}$ che fissa ogni numero dispari e manda ogni intero pari n in $n + 2$.
4. Scrivere ciascuna delle permutazioni $(1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9) \in \mathbb{S}_9$ e $f : n \in \mathbb{Z} \mapsto n + 1 \in \mathbb{Z}$ come prodotto di due permutazioni di ordine 2.

Automorfismi

Un altro notevole teorema sulla struttura dei gruppi simmetrici riguarda i loro automorfismi. Con una sola eccezione ($Sym X$ quando $|X| = 6$) tali automorfismi sono tutti e soli gli automorfismi interni (e quindi $\operatorname{Aut}(Sym X) \simeq Sym X$ a meno che $|X|$ sia 2 o 6). Per poter esprimere questo risultato in una forma più generale, ricordiamo (cfr. 1.8 e [Rob], 1.6.13) che se H è un sottogruppo di un gruppo G, ad ogni elemento g di $N = N_G(H)$ si può associare l'automorfismo $\tilde{g} : h \mapsto h^g$ di H, detto l'*automorfismo indotto per coniugio* da g su H; l'applicazione $g \in N \mapsto \tilde{g} \in \operatorname{Aut} H$ è un omomorfismo di nucleo $C_G(H)$.

7.14. Teorema. *Sia X un insieme di cardinalità diversa da 6. Sia H un sottogruppo di $Sym X$ contenente $AltX$. Allora ogni automorfismo di H è indotto per coniugio da qualche elemento di $N = N_{Sym\,X}(H)$. In particolare* $\operatorname{Aut}(Sym X) = \operatorname{Inn}(Sym X)$.

L'applicazione che ad ogni elemento g di N associa l'automorfismo di H indotto per coniugio da g è un isomorfismo, a meno che non si abbia $|X| = 2$ oppure $|X| = 3$ e $H = AltX$.

Per ogni sottogruppo normale non identico K di $Sym X$ si ha $\operatorname{Aut} K \simeq Sym X$, ad eccezione dei casi $|X| = 2$, $|X| = 3$ e $K = AltX$, e $|X| = 4 = |K|$.

Una dimostrazione di questo teorema è nella sezione 8.2 di [DM]; ci limitiamo qui ad un paio di osservazioni. Il teorema consiste essenzialmente della sua prima parte, che si può riformulare richiedendo che l'omomorfismo $N \to \operatorname{Aut} H$ di cui all'enunciato, chiamiamolo φ, sia suriettivo. Le due affermazioni che seguono sono conseguenze pressoché immediate di questa. Infatti il nucleo di φ è $C_N(H)$, ovviamente contenuto in $C_N(AltX)$, quindi è identico per 7.4,

tranne che nei casi indicati come eccezione nella seconda parte di 7.14, sicché, esclusi questi, φ è un monomorfismo. La parte conclusiva dell'enunciato, a proposito dei sottogruppi normali non identici di $Sym\,X$ (escluse di nuovo le eccezioni lì indicate) segue dalla seconda parte e dal fatto che $Alt X$ contiene ciascuno di essi, per 7.5. In particolare va evidenziato che, come anticipato, $\mathrm{Aut}(Sym\,X) = \mathrm{Inn}(Sym\,X) \simeq Sym\,X$ se $|X| \neq 2$ (e $|X| \neq 6$, come richiesto dall'ipotesi di 7.14).

Una discussione più approfondita merita il caso dei gruppi simmetrici di grado 6, l'eccezione generale dichiarata alla validità di 7.14. Si può verificare che $\mathrm{Aut}\,\mathbb{S}_6$ contiene propriamente $\mathrm{Inn}\,\mathbb{S}_6$ (come sottogruppo di indice 2), dunque il caso $|X| = 6$ è effettivamente eccezionale. Ciò è collegato al fatto che $\mathbb{S}_6$ ha rappresentazioni permutazionali fedeli di grado 6 non equivalenti a quella naturale. Per chiarire il nesso, osserviamo che, come mostra la dimostrazione di 3.1, per ogni insieme X, un automorfismo α di $Sym\,X$ è interno se e solo se α (che può essere riguardato come rappresentazione permutazionale di $Sym\,X$ su X) è equivalente alla rappresentazione naturale (cioè all'automorfismo identico) di $Sym\,X$. Infatti α è l'automorfismo interno determinato da $f \in Sym\,X$ se e solo se f determina una equivalenza da $id_{Sym\,X}$ a α. Sia ora n è un intero positivo e $\rho : \mathbb{S}_n \rightarrowtail Sym\,F$ è una rappresentazione fedele di grado n. Per ragioni di ordine, ρ è necessariamente un isomorfismo. Detta f un'applicazione biettiva da F all'insieme $\{i \in \mathbb{N} \mid 1 \leq i \leq n\}$ su cui agisce $\mathbb{S}_n$, sappiamo da 3.3 che ad f è associata una similitudine da $Sym\,F$ a $\mathbb{S}_n$, quella determinata da $(\tilde{f}, f)$, dove $\tilde{f}$ è l'isomorfismo $\alpha \mapsto f^{-1}\alpha f$. Ovviamente $\rho\tilde{f}$ è un automorfismo di $\mathbb{S}_n$, ed è equivalente a ρ: un'equivalenza da ρ a $\rho\tilde{f}$ è determinata appunto da f. Per quanto detto sopra, $\rho\tilde{f}$ (ovvero ρ) è equivalente alla rappresentazione naturale di $\mathbb{S}_n$ se e solo se è un automorfismo interno. Se $n \neq 6$ ciò accade sempre, per il Teorema 7.14, quindi si ha:

7.15. *Sia n un intero positivo diverso da 6. Allora:*

(*i*) *a meno di equivalenze $\mathbb{S}_n$ ha un'unica rappresentazione permutazionale fedele di grado n, quella naturale;*

(*ii*) *$\mathbb{S}_n$ ha un'unica classe di coniugio di sottogruppi di indice n, quella costituita dagli stabilizzanti dei punti nell'azione naturale.*

Dimostrazione — La parte (*i*) è immediata conseguenza di quanto appena visto; la (*ii*) è una riformulazione equivalente della (*i*). Infatti, se H è un sottogruppo di indice n in $\mathbb{S}_n$ allora $H_G = 1$ per 7.5 (i casi in cui $n = 4$ o $n < 3$ vanno trattati a parte), quindi la rappresentazione ρ_H di $\mathbb{S}_n$ sui laterali destri di H è fedele. Dire che ρ_H è equivalente alla rappresentazione naturale $id_{\mathbb{S}_n}$ di $\mathbb{S}_n$ equivale, per 3.8, a dire che H è lo stabilizzante di un punto rispetto a $id_{\mathbb{S}_n}$. ❑

Per $n = 6$, invece, la situazione è diversa: appare un'altra classe di coniugio di sottogruppi di indice 6 in $\mathbb{S}_6$, dunque:

7.16. *Il gruppo $\mathbb{S}_6$ ha una rappresentazione permutazionale fedele di grado 6 non equivalente a quella naturale, quindi* $\mathrm{Aut}(\mathbb{S}_6) \neq \mathrm{Inn}(\mathbb{S}_6)$.

Dimostrazione — Sia S lo stabilizzante di un punto nella rappresentazione naturale di $\mathbb{S}_6$. Come sappiamo da 1.7, si ha $S \simeq \mathbb{S}_5$. Una semplice applicazione del terzo Teorema di Sylow (o un calcolo diretto) mostra che l'insieme X dei 5-sottogruppi di Sylow di S ha ordine 6. Possiamo considerare l'azione per coniugio di S su X, chiamiamola ρ; si tratta ovviamente di un'azione transitiva e quindi fedele, per 7.5, in quanto $\ker\rho$ ha indice maggiore di 2.

Si fissi un'applicazione biettiva f da X a $I := \{1, 2, 3, 4, 5, 6\}$; questa fornisce la similitudine $(\tilde{f}, f)$ da ρ a $Sym\,X$ definita in 3.3. Sia Γ l'immagine del monomorfismo $\rho\tilde{f} : S \rightarrowtail \mathbb{S}_6$. Allora Γ è un sottogruppo di $\mathbb{S}_6$ isomorfo a S (ovvero a $\mathbb{S}_5$), quindi di indice 6. Chiaramente Γ (nella sua azione naturale su I) è simile a ρ (l'isomorfismo $s \in S \mapsto s^{\rho\tilde{f}} \in \Gamma$ e f determinano una similitudine). Ma ρ è transitiva, quindi anche Γ deve essere transitivo, e per questo Γ non è lo stabilizzante in $\mathbb{S}_6$ di un punto. È così provato che $\mathbb{S}_6$ ha più di una classe di coniugio di sottogruppi di indice 6; detto in altro modo, $\mathbb{S}_6$ ha una rappresentazione permutazionale fedele di grado 6 non equivalente a quella naturale (quella sui laterali destri di Γ) o, ancora, $\mathbb{S}_6$ ha un automorfismo non interno: le considerazioni svolte sopra spiegano perché queste proprietà si equivalgono (ma si veda anche il prossimo esercizio 3). ❑

Esercizi.

1. Per ogni intero positivo n, verificare in modo diretto (senza usare 7.15) che ogni rappresentazione permutazionale fedele di grado n di $\mathbb{S}_n$ è transitiva. (Questo chiarisce del tutto l'affermazione contenuta nella dimostrazione di 7.15 che le parti (*i*) e (*ii*) dello stesso enunciato sono *a priori* equivalenti. Perché?)
2. Sia X un insieme infinito. Provare che $Sym\,X$ ha una rappresentazione fedele non transitiva su X, necessariamente non equivalente alla rappresentazione naturale di $Sym\,X$. [*Suggerimento: $Sym\,X$ è isomorfo allo stabilizzante in $Sym\,X$ di un punto ...*]

I prossimi esercizi forniscono alcune informazioni sugli automorfismi non interni di $\mathbb{S}_6$.

3. Con le notazioni della dimostrazione di 7.16, detta φ la rappresentazione di $\mathbb{S}_6$ sull'insieme F dei laterali destri di Γ in $\mathbb{S}_6$ e fissata una biezione $h : F \to I$, osservare che $\lambda := \varphi\tilde{h}$ è un automorfismo non interno di $\mathbb{S}_6$, facendo per questo riferimento alle osservazioni immediatamente precedenti 7.15.
4. Riprendendo le notazioni del precedente esercizio, notare che lo stabilizzante di un punto rispetto a ρ (cioè il normalizzante in S di un suo 5-sottogruppo di Sylow) ha ordine 20. Dedurne che ciascun elemento di periodo 3 in S agisce via ρ senza punti fissi e che quindi Γ non contiene 3-cicli. Utilizzando ciò, provare che λ non manda

3-cicli in 3-cicli. [*Suggerimento: Se t è un 3-ciclo in $\mathbb{S}_6$, t non è contenuto nello stabilizzante di alcun punto rispetto all'azione di φ, ovvero di λ, quindi t^λ non è un 3-ciclo.*] Qual è la struttura ciclica dell'immagine di un 3-ciclo mediante λ?

5. Sia λ un automorfismo di $\mathbb{S}_6$ che non fissa l'insieme T dei 3-cicli. Osservato che λ scambia tra loro le due classi di coniugio di elementi di periodo 3 in $\mathbb{S}_6$, dedurne che se anche λ' è un automorfismo di $\mathbb{S}_6$ che non fissa T, allora $\lambda\lambda'$ fissa T, e che quindi l'insieme degli automorfismi di $\mathbb{S}_6$ che fissano T costituisce un sottogruppo di indice 2 in $\mathrm{Aut}(\mathbb{S}_6)$ (si dimostra che questo sottogruppo è $\mathrm{Inn}(\mathbb{S}_6)$, il che spiega perché $\left|\mathrm{Aut}\,\mathbb{S}_6 \,/\, \mathrm{Inn}\,\mathbb{S}_6\right| = 2$).
6. Sia, di nuovo, λ un automorfismo di $\mathbb{S}_6$ che non fissa l'insieme dei 3-cicli. Allora λ non fissa neanche l'insieme delle trasposizioni. [*Suggerimento: i 3-cicli sono tutti e soli i prodotti di due trasposizioni che abbiano ordine* 3.]
7. Sia λ un automorfismo di $\mathbb{S}_6$ che non fissa l'insieme D delle trasposizioni. Calcolare in $\mathbb{S}_6$ le cardinalità delle classi di coniugio di elementi di ordine 2 e dedurne che λ scambia tra loro D e la classe di coniugio costituita dai prodotti di tre trasposizioni disgiunte. Come in 5, dedurne che l'insieme degli automorfismi di $\mathbb{S}_6$ che fissano D costituisce un sottogruppo di indice 2 in $\mathrm{Aut}(\mathbb{S}_6)$. Utilizzando poi l'esercizio precedente concludere che un automorfismo di $\mathbb{S}_6$ fissa l'insieme dei 3-cicli se e solo se fissa l'insieme delle trasposizioni.

Bibliografia

[B] M. Bhattacharjee - D. Macpherson - R.G. Möller - P.M. Neumann, "*Notes on Infinite Permutation Groups*", Hindustan Book Agency, New Delhi, 1997.

[DM] J.D. Dixon - B. Mortimer, "*Permutation Groups*", Springer, Berlin, 1996.

[H] B. Huppert, "*Endliche Gruppen*", vol. I, Springer, Berlin, 1967.

[Rob] D.J.S. Robinson, "*A Course in the Theory of Groups*", Springer, Berlin, 1982.

[P] D. Passman, "*Permutation Groups*", W.A. Benjamin, New York, 1968.

[W] H. Wielandt, "*Finite Permutation Groups*", Academic Press, New York, 1964.

Indice