Corso di Algebra 1

A. Machì

a.a. 2006–2007

Dispensa II

Piccolo teorema di Fermat. *Sia a un intero, p un numero primo e sia a primo con p : $(a,p)=1$. Allora*:

$$a^{p-1} \equiv 1 \bmod p.$$

Dim. Siano

$$[1],[2],\dots,[p-1] \tag{1}$$

le classi resto non nulle mod$p$. Poiché, per ipotesi, $(a,p)=1$, a appartiene a una di queste classi. Moltiplichiamo allora le classi precedenti per $[a]$; si ha:

$$[a],[2a],\dots,[(n-1)a]. \tag{2}$$

Queste classi mod$p$ sono a due a due distinte. Infatti, se $[ha]=[ka]$, allora $[0]=[ha]-[ka]=[(h-k)a]$, cioè p divide $(h-k)a$, ed essendo primo con a deve dividere $h-k$. Se $h \neq k$ ciò è impossibile perché h e k sono minori di p e perciò anche la loro differenza lo è. Allora $h=k$, come si voleva. Le classi (2) sono allora le stesse di (1), eventualmente in un altro ordine. Il prodotto di tutte le classi (1) è allora uguale al prodotto di tutte le (2):

$$[1]\cdot[2]\cdots[p-1]=[a]\cdot[2a]\cdots[(n-1)a].$$

Ma il secondo membro è uguale a

$$[1][a]\cdot[2][a]\cdots[n-1][a]=[1]\cdot[2]\cdots[p-1][a]^{p-1},$$

e perciò abbiamo

$$[1]\cdot[2]\cdots[p-1][a]^{p-1}=[1]\cdot[2]\cdots[p-1]$$

cioè $[1\cdot 2\cdots(p-1)][a]^{p-1}=[1\cdot 2\cdots(p-1)]$ ovvero $[(p-1)!][a]^{p-1}=[(p-1)!]$, o ancora

$$(p-1)!a^{p-1} \equiv (p-1)! \bmod p.$$

Avendosi $((p-1)!,p)=1$ è possibile dividere entrambi i membri per $(p-1)!$ e ottenere $a^{p-1}\equiv 1 \bmod p$. □

In questa dimostrazione abbiamo sfruttato le seguenti proprietà dell'operazione di prodotto nell'insieme delle classi resto modulo un intero:

i) l'operazione è associativa (si riporta all'associatività del prodotto degli interi);

ii) esiste un elemento neutro (la classe [1]): $[a] \cdot [1] = [a]$;

iii) ogni elemento ammette un inverso (l'inversa della classe $[a]$ è la classe $[h]$: $[a][h] = [1]$ dove $ha + kp = 1$ (si scrive $[h] = [a]^{-1}$;

iv) l'operazione è commutativa.

Un insieme G nel quale sia definita un'operazione che soddisfi:

i) l'operazione è associativa;

ii) esiste un elemento e tale che $ae = ea = a$, per ogni $a \in G$ (elemento *neutro* o *unità* o *identità*);

iii) ogni elemento ammette un inverso: dato $a \in G$, esiste $b \in G$ tale che $ab = ba = e$,

si chiama *gruppo*; se è soddisfatta anche la

iv) l'operazione è commutativa $ab = ba$, per ogni $a, b \in G$,

il gruppo si dice *commutativo* o *abeliano*. La cardinalità dell'insieme G è l'*ordine* del gruppo G.

L'insieme delle classi resto modulo n è dunque un gruppo abeliano rispetto alla somma tra classi. Se $n = p$ è primo, le classi viste sopra in (1) formano un gruppo di ordine $p-1$ rispetto al prodotto tra classi (l'ipotesi che p sia un numero primo è necessaria per garantire la *iii*), cioè che *ogni* elemento abbia un inverso). Nel teorema di Fermat si dimostra che in quest'ultimo gruppo, ogni classe, elevata al numero di elementi dell'insieme, dà la classe [1]. Per dimostrarlo, si sono sfruttate le proprietà $i), \ldots, iv)$ di sopra, cioè quelle che definiscono un gruppo abeliano. Vediamo allora se un teorema analogo esiste per un qualunque gruppo abeliano. Ci chiediamo cioè: elevando un qualunque elemento di un gruppo abeliano all'intero che dà l'ordine del gruppo si ottiene l'unità? La risposta è positiva.

Teorema 1. *Sia G un gruppo abeliano di ordine n. Allora $a^n = 1$, per ogni $a \in G$.*

Dim. La dimostrazione procede in modo analogo al teorema precedente. Siano

$$a_1, a_2, \ldots, a_n, \tag{3}$$

gli elementi di G, e sia $a \in G$. Moltiplichiamo gli elementi di G per a:

$$a_1 \cdot a, a_2 \cdot a, \ldots, a_n \cdot a. \tag{4}$$

Questi elementi sono a due a due distinti: infatti, se $a_i a = a_j a$, allora moltiplicando entrambi i membri a destra per a^{-1} (che esiste per la *iii*) della definizione di gruppo), si ha $(a_i a)a^{-1} = (a_j a)a^{-1}$, e applicando la proprietà associativa *i*), $a_i(aa^{-1}) = a_j(aa^{-1})$, cioè $a_i e = a_j e$ e per la *ii*), $a_i = a_j$. In altre parole, se a_i e a_j sono distinti, anche $a_i a$ e $a_j a$ lo sono. Gli elementi (4), non potendo essere in numero maggiore di n (perché si sono fatte n moltiplicazioni) sono allora gli stessi di (3), eventualmente in un altro ordine. Il prodotto di tutti gli elementi (3) è allora uguale al prodotto di tutti gli elementi (4) (l'ordine in cui si effettua il prodotto non conta perché il gruppo è commutativo):

$$a_1 \cdot a_2 \cdots a_n = a_1 a \cdot a_2 a \cdots a_n a.$$

Sfruttando ancora la commutatività, a secondo membro possiamo scrivere $a \cdot a_2 = a_2 \cdot a$, e facendo lo stesso con $a_3, \ldots, a_n$, portare a in fondo:

$$a_1 \cdot a_2 \cdots a_n = a_1 \cdot a_2 \cdots a_n a^n.$$

Il prodotto $a_1 \cdot a_2 \cdots a_n$ è un ben determinato elemento del gruppo, e sia b: Ne segue $b = ba^n$, e moltiplicando per b^{-1} a sinistra si ottiene $a^n = 1$, come si voleva. □

In un gruppo G, si definisce *periodo* o *ordine* di un elemento a il più piccolo intero positivo m tale che $a^m = 1$.

Teorema 2. *Sia a un elemento di periodo m in un gruppo G, e sia $a^n = 1$. Allora m è un divisore di n.*

Dim. Sia $n > 0$; allora $n > m$ per la minimalità di m. Dividiamo n per m: $n = mq + r$ con $0 \leq r < m$. Ne segue:

$$1 = a^n = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r = 1 \cdot a^r = a^r.$$

Se $r > 0$, $a^r = 1$ contraddice la minimalità di m. Allora $r = 0$, da cui $n = mq$, cioè m è un divisore di n, come si voleva. Se $n < 0$, si proceda come sopra con $n = m(-q) + r$ e $0 \leq r < m$. □

In un gruppo, un elemento di periodo m ha m potenze distinte. Infatti, sia $o(a) = m$, e siano $a, a^2, \ldots a^{m-1}, a^m = 1$ le potenze di a. Se due di queste sono uguali, $a^h = a^k$ con $h > k$, allora moltiplicando entrambi i membri per $(a^k)^{-1} = a^{m-k}$ abbiamo $a^h a^{m-k} = 1$. Ma $a^h a^{m-k} = a^{m+h-k} = a^m a^{h-k} = a^{h-k}$, e dunque si avrebbe $a^{h-k} = 1$ con $h - k < m$, contro la minimalità di m. Le m potenze di a sono allora tutte distinte.

Unicità dell'elemento neutro in un gruppo. L'elemento e tale che $ea = a = ae$ è unico. Se anche e' è tale che $e'a = a = ae'$, per ogni elemento a di G, allora con $a = e$ si ha $e'e = e$ perché e è neutro, ed $e'e = e'$ perché e' è neutro. Ne segue $e = e'$ perché alla coppia (e', e) non possono essere associati due elementi diversi (l'operazione è una funzione).

Unicità dell'inverso di ogni elemento in un gruppo. Sia $ab = 1 = ba$, e $ab' = 1 = b'a$. Moltiplichiamo $ab = 1$ per b' a sinistra; si ha:

$$b' = b' \cdot 1 = b'(ab) \Rightarrow (b'a)b = b' \Rightarrow 1 \cdot b = b' \Rightarrow b = b'.$$

Teorema 3. *Un gruppo di ordine* 4 *è abeliano. Vi sono soltanto due gruppi di ordine* 4*: il gruppo ciclico e il gruppo di Klein.*

Dim. Sia $G = \{1, a, b, c\}$ il gruppo. Il prodotto ab deve appartere a G, e dunque è uno dei quattro elementi:

$$ab = 1, a, b, c.$$

Non può essere $ab = a$ o $ab = b$ (che darebbero $b = 1$ e $a = 1$). Ne segue che il prodotto di due elementi distinti o è 1, oppure è uguale al terzo. Consideriamo allora i due casi $ab = 1$ e $ab = c$. I due casi daranno luogo ciscuno a uno dei due gruppi dell'enunciato del teorema.

1. $ab = 1$; allora a e b sono inversi uno dell'altro: $b = a^{-1}$ e $a = b^{-1}$. Consideriamo allora ac; come prima $ac = 1$ oppure $ac = b$. Ma $ac = 1$ implica che c è l'inverso di a, mentre abbiamo visto che l'inverso di a è b. Dunque $ac = b$, e per gli stessi motivi $ca = b$. A questo punto abbiamo che a e b permutano ($ab = ba = 1$), e anche a e c ($ac = ca$ perché entrambi uguali a b). Vediamo b e c. Al solito, $bc = 1$ oppure $bc = a$. Ma $bc = 1$ significa $c = b^{-1}$, impossibile perché $b^{-1} = a$. Allora $bc = a$, e analogamente $cb = a$. Gli elementi sono dunque a due a due permutabili, e G è abeliano. Inoltre, $a^2 = c$. Se infatti $a^2 = 1$, allora $a^{-1} = a$; ma siamo nell'ipotesi $ab = 1$, e dunque $a^{-1} = b$, e si avrebbe $a = b$, escluso. Se poi $a^2 = a$, allora $a = 1$, escluso, e se $a^2 = b$, allora, moltiplicando per a, si avrebbe $a^3 = ab = 1$. Dunque l'ordine di a sarebbe un divisore di 3, ma ciò è escluso perché $a^4 = 1$ (Teorema 2), e dunque l'ordine di a divide 4. Con lo stesso argomento si ha $b^2 = c$. Inoltre, $a^3 = a^2 \cdot a = ca$, e abbiamo visto sopra che $ca = b$. Ne segue che i quattro elementi sono

$$a, c = a^2, b = a^3, a^4 = 1,$$

e siamo pertanto in presenza del gruppo ciclico generato da a:

	1	a	a^2	a^3
a	a	a^2	a^3	1
a^2	a^2	a^3	1	a
a^3	a^3	1	a	a^2

2. Il prodotto di due qualunque elementi distinti e diversi da 1, in qualunque ordine, è uguale al terzo: $ab = c$, $ba = c$, e dunque $ab = ba$. Lo stesso per le coppie a, c, b, c e a, c, e anche in questo caso il gruppo è abeliano. Si osservi che in questo secondo caso il quadrato di ogni elemento è 1: infatti, se fosse $a^2 = b$, essendo $b = ac$ si avrebbe $a^2 = ac$ e $a = c$, escluso, e così per gli altri elementi. La tavola di moltiplicazione dunque:

	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

dove si riconosce il gruppo di Klein. □

Tra i modelli del gruppo ciclico vi sono:

– $Z_4(+) = \{[0], [1], [2], [3]\}$ ($a = [1]$);
– $Z_5^*(\cdot) = \{[1], [2], [3], [4]\}$ ($a =$[2] o [3]);
– le quattro potenze del numero complesso i: $\{i, -1, -i, 1\}$ ($a = i$ o $-i$);
– le rotazioni di $90, 180, 270$ e $360 = 0$ gradi ($a =$rotazione di 90 gradi);
– le quattro permutazioni I, (1,2,3,4),(1,3)(2,4), (1,4,3,2) (si pensi ai vertici del quadrato numerati 1,2,3,4).

ecc.

Tra i modelli del gruppo di Klein vi sono:

–le simmetrie rispetto agli assi coordinati e rispetto all'origine del piano cartesiano (più l'identità);
– $Z_8^*(\cdot) = \{1, 3, 5, 7\}$;
– $Z_{12}^*(\cdot) = \{1, 5, 7, 11\}$
– due simmetrie assiali del quadrato rispetto ad assi perpendicolari più la rotazione di 180 gradi;
– le quattro permutazioni I, (1,2)(3,4),(1,3)(2,4),(1,4)(2,3) (si pensi alle quattro simmetrie del quadrato precedenti;
– ecc. □ Ora che sappiamo che un gruppo di ordine 4 è necessariamente abeliano, possiama dimostrare:

Teorema 4. *Per $n = 1, 2, 3$ esiste un solo gruppo di ordine n.*

Dim. Se $n = 1$, poiché l'identità ci deve essere, il gruppo consta solo di questa. Se $n = 2$, e gli elementi sono 1 e a, allora è necessariamente $a^2 = 1$, e dunque il gruppo è ciclico di ordine 2. Se $n = 3$, e $1, a, b$ sono i tre elementi, allora è necessariamente $ab = 1$, e b è l'inverso di a. Ne segue $a^2 = b$ (se $a^2 = 1$, allora $a = a^{-1}$, mentre l'inverso di a è b). Dunque i tre elementi sono $1, a, a^2$, e il gruppo è ciclico. Modelli sono $Z_4^*(\cdot)$, la rotazione di 120 gradi e le sue potenze, ecc. □

Gruppi diedrali

Una *isometria* è una corrispondenza biunivoca tra i punti del piano che conserva le distanze. Le isometrie formano gruppo rispetto al solito prodotto di trasformazioni (prima una poi l'altra). I gruppi diedrali sono i gruppi delle isometrie (dette anche simmetrie) dei poligoni regolari. Esse si dividono in simmetrie assiali e simmetrie rotatorie.

Consideriamo ora un poligono con n lati, e distinguiamo due casi.

1. n pari. In questo caso vi sono due tipi di assi di simmetria: quelli passanti per i punti di mezzo di lati opposti (e sono $n/2$), e quelli passanti per coppie di punti diagonalmente opposti (altri $n/2$). Vi sono poi n rotazioni (di gradi $2\pi/n, 4\pi/n, \ldots, 2(n-1)\pi/n, 2n\pi/n$ =identità) attorno a un asse perpendicolare al piano e passante per il baricentro del poligono. In tutto $n/2 + n/2 + n = 2n$ simmetrie.

2. n dispari. In questo caso gli assi di simmetria sono di un solo tipo: passano per un vertice e per il punto di mezzo del lato opposto al vertice. Sono quindi tanti quanti sono i vertici, cioè n. Vi sono poi le n rotazioni viste sopra. In tutto $n + n = 2n$ simmetrie.

In ogni caso, *un gruppo diedrale ha ordine* $2n$. Si denota con D_n.

Numerando i vertici del triangolo in senso orario con 1,2 e 3, i tre assi di simmetria a, b e c fissano uno dei tre vertici. Consideriamo le seguenti composizioni di simmetrie:

– a: simmetria rispetto all'asse verticale seguita da una rotazione di 120 gradi;

– r: rotazione di 120 gradi seguita da una simmetria rispetto all'asse verticale.

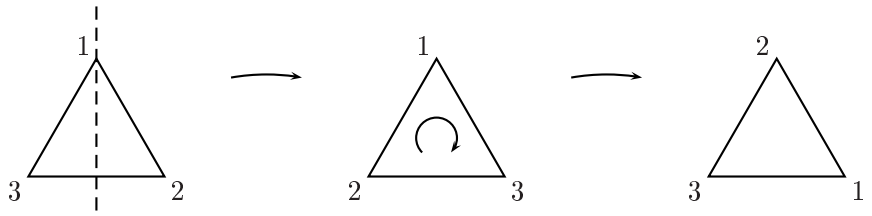

Fig. 1: prima la simmetria assiale a e poi la rotazione r

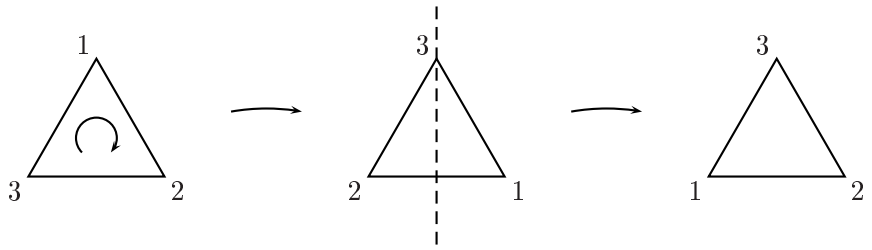

Fig. 2: prima la rotazione r e poi la simmetria assiale a

operando prima a e poi r si ottiene un risultato (Fig. 1), operando prima r e poi a se ne ottiene un altro (Fig. 2): *la composizione di simmetrie non è commutativa*. Abbiamo così un primo esempio di gruppo non commutativo. Poiché una simmetria induce una permutazione dei vertici (ad esempio, la simmetria rispetto all'asse passante per il vertice 1 induce la permutazione *ciclica* $1 \to 1, 2 \to 3, 3 \to 2$, che scriviamo $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, cioè mettendo uno sopra l'altro un elemento e la sua immagine. Avremmo anche potuto scrivere $\begin{pmatrix} 2 & 1 & 3 \\ 3 & 1 & 2 \end{pmatrix}$(o in un altro qualunque dei sei modi possibili). La rotazione di 120 gradi induce la permutazione *ciclica* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, e componendo le due simmetrie:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

come si vede anche dalla Fig. 1. Se si effettua prima la rotazione e poi la simmetria rispetto all'asse passante per il vertice 1:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

che è la simmetria rispetto all'asse passante per il vertice 2 (Fig. 2).

Sia ora r la rotazione di 120 gradi, e a una simmetria assiale. Le sei simmetrie:

$$1, r, r^2, a, ra, r^2,$$

sono a due a due distinte (ogni uguaglianza porta a una contraddizione), e dunque sono le sei simmetrie del triangolo. In generale, per un poligono di n lati, se r è la rotazione di $2\pi/n$, e a una simmetria assiale, i $2n$ elementi

$$1, r, \ldots, r^{n-1}, a, ra, \ldots, r^{n-1}a,$$

sono tutti distinti, e perciò esauriscono le $2n$ simmetrie del poligono. Si osservi inoltre l'uguaglianza:

$$ara = r^{-1}$$

(si ricordi che $r^{-1} = r^{n-1}$), il cui significato geometrico è chiaro: operare una simmetria assiale, seguita da una rotazione di $2\pi/n$, e poi ancora dalla stessa simmetria assiale, equivale a operare una rotazione in senso inverso alla precedente.

Azione

Definizione. Dati un insieme $\Omega = \{\alpha, \beta, \gamma, \ldots\}$ e un gruppo G, si dice che G *agisce* su Ω (o che G *opera* su Ω, o che Ω è un $G-$*insieme*) quando è assegnata una funzione $\Omega \times G \to \Omega$, tale che, denotando con α^g l'immagine della coppia (α, g), si abbia:

i) $\alpha^{gh} = (\alpha^g)^h$, $\alpha \in \Omega$, $g \in G$.

ii) $\alpha^1 = \alpha$, dove 1 è l'elemento neutro di G.

La funzione assegnata si chiama *azione* di G su Ω, e la cardinalità di Ω *grado* del gruppo. Con linguaggio geometrico, chiameremo spesso *punti* gli elementi di Ω. Scriveremo anche (G, Ω) per indicare che G agisce su Ω. Si osservi che se H è un sottogruppo di G e G agisce su Ω anche H agisce su Ω. Questa azione di H è la *restrizione* dell'azione di G.

La nozione di gruppo che agisce su un insieme generalizza quella di gruppo di permutazioni di un insieme nel senso che può ben accadere che esista qualche elemento $1 \neq g \in G$ tale che $\alpha^g = \alpha$ per ogni $\alpha \in \Omega$ (se G è un gruppo di permutazioni questo fatto implica $g = 1$). È quanto ora vediamo.

Teorema. *Se un gruppo G agisce su un insieme Ω, ogni elemento di G dà luogo a una permutazione di Ω. Più precisamente, la corrispondenza $\Omega \to \Omega$ data da $\varphi_g : \alpha \to \alpha^g$ è, per ogni fissato $g \in G$, una permutazione di Ω.*

Dim. La φ_g è iniettiva: $\alpha^g = \beta^g \Rightarrow (\alpha^g)^{g^{-1}} = (\beta^g)^{g^{-1}} \Rightarrow \alpha^{gg^{-1}} = \beta^{gg^{-1}} \Rightarrow \alpha^1 = \beta^1$, e dunque $\alpha = \beta$. Si noti che abbiamo usato sia la *i*) che la *ii*) della Def. 3.1. È surgettiva: se $\alpha \in \Omega$, sia $\beta = \alpha^{g^{-1}}$; allora: $\beta^g = (\alpha^{g^{-1}})^g = \alpha^{g^{-1}g} = \alpha^1 = \alpha$, e quindi α proviene da β. $\diamondsuit$

Sia ora S^Ω il gruppo di tutte le permutazioni di Ω (gruppo simmetrico su Ω), e G un gruppo che agisce su Ω. In base al teorema precedente possiamo considerare l'applicazione $\varphi : G \to S^\Omega$ ottenuta associando a ogni $g \in G$ la permutazione φ_g di Ω che esso induce: $g \to \varphi_g$. Tale corrispondenza è subito visto essere un omomorfismo. In questo modo si ottiene una *rappresentazione* degli elementi di G per mezzo di permutazioni. Al prodotto di due elementi di G corrisponde il prodotto delle due permutazioni che li rappresentano. Il nucleo di φ è dato da

$$K = \{g \in G \mid \alpha^g = \alpha,\ \forall \alpha \in \Omega\},$$

cioè dagli elementi di G che lasciano fisso ogni elemento di Ω. Il sottogruppo K si chiama *nucleo dell'azione*. Se esso si riduce al solo elemento neutro, l'azione si dice *fedele*, e in tal caso G è isomorfo a un sottogruppo di S^Ω; si dirà allora che G è un gruppo di permutazioni di Ω. In ogni caso, il quoziente G/K è un gruppo di permutazioni di Ω, con l'azione definita da:

$$(\alpha, Kg) \to \alpha^g, \text{ cioè } \alpha^{Kg} = \alpha^g,$$

che è ben definita in quanto se h è un altro rappresentante del laterale Kg, allora $h = kg$, $k \in K$, e dunque $\alpha^{(kg)} = (\alpha^k)^g = \alpha^g$, essendo $\alpha^k = \alpha$, per ogni $k \in K$ e $\alpha \in \Omega$. Se $K = G$, gli elementi di G fissano tutti i punti di Ω: l'azione è *banale*.

Un elemento α di Ω determina due sottoinsiemi, uno in Ω (l'orbita di α e l'altro in G (lo stabilizzatore di α).

Definizione. L'*orbita* di α sotto l'azione di G è il sottoinsieme

$$\alpha^G = \{\alpha^g,\ g \in G\},$$

cioè l'insieme degli elementi di Ω in cui è portato α dai vari elementi di G.

Due orbite o coincidono o sono disgiunte. Infatti, com'è subito visto, le orbite altro non sono che le classi della relazione di equivalenza ρ così definita:

$$\alpha \rho \beta \text{ se esiste } g \in G \text{ tale che } \alpha^g = \beta.$$

In particolare, Ω è unione disgiunta di orbite:

$$\Omega = \bigcup_{\alpha \in T} \alpha^G,$$

dove α varia in un insieme T di rappresentanti per le orbite. Se Ω è finito si ha allora

$$|\Omega| = \sum_{\alpha \in T} |\alpha^G|.$$

Se $H \leq G$, le orbite di G sono unioni di orbite di H. Se g è una permutazione, le orbite del sottogruppo generato da g sono i sottoinsiemi che danno i cicli di g. Le orbite si chiamano anche *sistemi di transitività*.

Definizione. G si dice *transitivo* se esiste una sola orbita.

In altri termini, G è transitivo se dati comunque $\alpha, \beta \in \Omega$ esiste almeno un elemento di G che porta α su β.

Definizione. Lo *stabilizzatore di α è il sottoinsieme di G:*

$$G_\alpha = \{g \in G \mid \alpha^g = \alpha\},$$

cioè l'insieme degli elementi di G che lasciano fisso α.

G_α è un sottogruppo di G. Infatti, $1 \in G_\alpha$; se $x, y \in G_\alpha$, allora $\alpha^{xy} = (\alpha^x)^y = \alpha^y = \alpha$, e dunque $xy \in G_\alpha$. Inoltre, se $x \in G_\alpha$, $\alpha = \alpha^1 = \alpha^{xx^{-1}} = (\alpha^x)^{x^{-1}} = \alpha^{x^{-1}}$, e dunque anche $x^{-1} \in G_\alpha$. Lo stabilizzatore di un elemento si chiama anche *gruppo di isotropia* dell'elemento.

Se un elemento di G appartiene allo stabilizzatore di ogni elemento di Ω, allora appartiene al nucleo dell'azione, e viceversa. Pertanto, il nucleo dell'azione è l'intersezione degli stabilizzatori di tutti gli elementi di Ω:

$$K = \bigcap_{\alpha \in \Omega} G_\alpha.$$

La relazione tra orbite e stabilizzatori è messa in luce dal seguente teorema.

Teorema. *i) La cardinalità dell'orbita di un elemento α è uguale all'indice dello stabilizzatore di α*:

$$|\alpha^G| = [G : G_\alpha]; \tag{5}$$

in particolare, se G è finito:

$$|G| = |G_\alpha||\alpha^G|, \tag{6}$$

e quindi la cardinalità di un'orbita divide l'ordine del gruppo.

ii) Se β appartiene all'orbita di α, allora gli stabilizzatori di β e α sono coniugati. Più precisamente, se $\beta = \alpha^g$ allora $G_\beta = (G_\alpha)^g$, cioè

$$G_{\alpha^g} = (G_\alpha)^g.$$

Dim. i) Può ben accadere che per due elementi distinti $g, h \in G$ si abbia $\alpha^g = \alpha^h$. Per sapere quanti elementi α^g (distinti) si ottengono al variare di g in G dobbiamo dunque poter stabilire quante volte è ripetuto uno stesso elemento. Ora $\alpha^g = \alpha^h \Leftrightarrow \alpha^{gh^{-1}} = \alpha \Leftrightarrow gh^{-1} \in G_\alpha$, e dunque α^g e α^h sono lo stesso elemento se e solo se g e h appartengono allo stesso laterale (destro) dello stabilizzatore di α, cioè se e solo se $g = xh$, con $x \in G_\alpha$. In altri termini, un elemento α^g è ripetuto tante volte quant'è la cardinalità del laterale $G_\alpha g$ (per ogni $x \in G_\alpha$ si ha infatti $\alpha^{xg} = (\alpha^x)^g = \alpha^g$). Due elementi g e h appartenenti a laterali distinti danno quindi luogo a elementi α^g e α^h distinti, e perciò abbiamo tanti elementi nell'orbita α^G quanti sono i laterali di G_α.

ii) Se $x \in G_\alpha$, allora $(\alpha^g)^{g^{-1}xg} = (\alpha^x)^g = \alpha^g$, cioè $g^{-1}xg$ stabilizza $\alpha^g = \beta$. Dunque $(G_\alpha)^g \subseteq G_{\alpha^g} = G_\beta$. Viceversa, se $x \in G_{\alpha^g}$, allora $(\alpha^g)^x = \alpha^g$, ovvero $gxg^{-1} \in G_\alpha$ e quindi $x \in (G_\alpha)^g$ e $G_{\alpha^g} = G_\beta \subseteq (G_\alpha)^g$. ♢

Se α e β appartengono alla stessa orbita, $\alpha^G = \beta^G$, e dunque, per la *i)* del teorema precedente, $[G : G_\alpha] = |\alpha^G| = |\beta^G| = [G : G_\beta]$, cioè i due stabilizzatori hanno lo stesso indice. La parte *ii)* del teorema dice che, in più, essi sono coniugati.

Corollario. *Se G è transitivo, $|\Omega| = [G : G_\alpha]$. Se G è finito e transitivo, allora anche Ω è finito e $|\Omega|$ divide $|G|$.* ♢

Per utilizzare l'azione al fine di scoprire proprietà di un gruppo G occorre trovare un opportuno insieme su cui fare agire G, insieme suggerito di volta in volta dalla natura del problema. Spesso questo insieme si troverà all'interno del gruppo. Alcuni risultati ottenuti in precedenza si possono ritrovare assumendo il punto di vista dell'azione.

Esempi. 1. Prendiamo per Ω l'insieme sostegno di G, e facciamo agire G per moltiplicazione a destra: $a^x = ax$. Si tratta di un'azione perché $a \cdot 1 = a$, e il fatto che si abbia $a^{xy} = (a^x)^y$ è dovuto semplicemente alla proprietà associativa di G: $a^{xy} = a(xy) = (ax)y = (a^x)^y$. G è transitivo in quanto dati due elementi $a, b \in G$, esiste sempre $x \in G$ tale che $ax = b$ (assioma dei quozienti: $x = a^{-1}b$). Inoltre lo stabilizzatore di un elemento è l'identità: se $ax = a$ allora $x = 1$; il nucleo dell'azione è dunque, a fortiori, l'identità,

per cui l'omomorfismo $G \to S^\Omega$ è un isomorfismo tra G e un sottogruppo di S^Ω. Si ottiene così la *rappresentazione regolare destra* di G. Analogamente definendo $a^x = x^{-1}a$ si ha la rappresentazione regolare sinistra.

Se G è finito, $G = \{x_1, x_2, \ldots, x_n\}$, l'immagine di un elemento $x \in G$ nella rappresentazione regolare (destra) è la permutazione

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_1x & x_2x & \ldots & x_nx \end{pmatrix}.$$

L'elemento x_1x sarà un certo x_i, e dunque $x_ix = x_1x^2$; analogamente, $x_1x^2 = x_j$ e $x_jx = x_1x^3$, ecc. Se k è l'ordine di x, si ha $x_1x^{k-1}x = x_1x^k = x_1$, e pertanto il ciclo cui appartiene x_1 è $(x_1, x_1^2, \ldots, x_1^{k-1})$ (se $x_1x^h = x_1$ allora $x^h = 1$, e perciò h non può essere minore di k). Lo stesso accade per gli altri cicli. Dunque, l'immagine di un elemento x di G nella rappresentazione regolare è una permutazione che ha tutti i cicli della stessa lunghezza, (permutazioni di questo tipo si dicono *regolari*

2. Un gruppo di trasformazioni lineari di uno spazio vettoriale V agisce su V. L'intero gruppo $GL(V)$ è transitivo sui sottospazi aventi una stessa dimensione. Se infatti W_1 e W_2 hanno la stessa dimensione e B_1 e B_2 sono due rispettive basi, sia φ una corrispondenza biunivoca tra queste due basi. B_1 e B_2 si possono estendere a due basi di V, e la φ a una corrispondenza biunivoca φ' tra queste. La φ' determina allora una trasformazione lineare invertibile di V che porta W_1 su W_2. Allo stesso modo si vede che lo stabilizzatore G_v di un vettore v è transitivo sui vettori che non sono multipli di v. Se infatti u e w non appartengono al sottospazio generato da v, allora v, u e v, w sono due coppie di vettori indipendenti che possono estendersi a due basi di V. Una corrispondenza biunivoca tra queste che porti v in v e u in w si estende a una trasformazione lineare invertibile che fissa v, e dunque appartiene a G_v e porta u in w.