Lezione 18

Prerequisiti: Lezioni 4, 17.

Orbite e cicli di una permutazione.

In questa lezione introduciamo, per un'arbitraria permutazione, la cosiddetta *decomposizione in cicli disgiunti*, che ne rivela la struttura, agevolando la determinazione del suo periodo e della sua classe di parità.

Sia n un intero positivo.

Definizione 18.1 Si dice *ciclo* (o *permutazione ciclica*) ogni $\sigma \in S_n$ per cui esistono un intero positivo ℓ e $a_1,\dots,a_\ell \in \{1,\dots,n\}$ a due a due distinti tali che
i) $\sigma(a_1)=a_2, \sigma(a_2)=a_3,\dots,\sigma(a_{\ell-1})=a_\ell, \sigma(a_\ell)=a_1$;
ii) $\sigma(k)=k$ per ogni $k \in \{1,\dots,n\} \setminus \{a_1,\dots,a_\ell\}$.

Il numero ℓ si dice *lunghezza* di σ. Una permutazione ciclica di lunghezza ℓ si dice anche un ℓ-ciclo.

Nota Per il ciclo σ della Definizione 18.1 esiste, oltre alla notazione matriciale, la scrittura *ciclica*

$$(a_1,a_2,\dots,a_\ell).$$

Esempio 18.2 (a) Il solo ciclo di lunghezza 1 è la permutazione identica. Infatti, in base alla Definizione 18.1, per ogni $a_1 \in \{1,2,\dots,n\}$, la permutazione $\sigma=(a_1)$ è tale che $\sigma(a_1)=a_1$ (condizione i)) e, per ogni $k \in \{1,\dots,n\}$, $k \neq a_1$, $\sigma(k)=k$ (condizione ii)). Quindi σ lascia fisso ogni elemento, e dunque $\sigma = id$.
(b) La permutazione $\alpha \in S_n$ dell'Esercizio 4.18 è il 2-ciclo $(1,2)$.
(c) In S_3,

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

(d) In S_4,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1,3,2,4).$$

Osservazione 18.3 La scrittura ciclica di un $\ell -$ciclo non è unica. Se $\ell > 1$, il ciclo della precedente Nota ammette esattamente ℓ scritture cicliche distinte, ottenute tramite rotazioni successive degli indici verso sinistra:

$$(a_1,a_2,\dots,a_{\ell-2},a_{\ell-1},a_\ell), \quad (a_2,a_3,\dots a_{\ell-1},a_\ell,a_1), \quad (a_3,a_4,\dots a_\ell,a_1,a_2), \quad \dots, \quad (a_\ell,a_1,a_2,\dots,a_{\ell-2},a_{\ell-1}).$$

In particolare, la permutazione dell'Esempio 18.2 (d) ammette le seguenti 4 scritture cicliche:

$$(1,3,2,4), \quad (3,2,4,1), \quad (2,4,1,3), \quad (4,1,3,2).$$

Proposizione 18.4 *(ℓ-cicli in S_n)* Sia ℓ un intero maggiore di 1 e non maggiore di *n*. In S_n vi sono esattamente

$$\frac{1}{\ell}\frac{n!}{(n-\ell)!}$$

cicli di lunghezza ℓ.

Dimostrazione: Il più generale ciclo di lunghezza ℓ in S_n è $\sigma=(a_1,...,a_\ell)$. L'insieme $\{a_1,...,a_\ell\}\subset\{1,...,n\}$ può essere scelto in esattamente $\binom{n}{\ell}=\frac{n!}{(n-\ell)!\ell!}$ modi distinti. D'altra parte, gli elementi $a_1,...,a_\ell$ possono essere disposti in esattamente $\ell!$ modi distinti. Pertanto esistono esattamente $\binom{n}{\ell}\ell!=\frac{n!}{(n-\ell)!}$ sequenze $a_1,...,a_\ell$ di ℓ elementi scelti in $\{1,...,n\}$. Questo è quindi il numero delle scritture cicliche di lunghezza ℓ. In base all'Osservazione 18.3, queste rappresentano, prese a ℓ a ℓ, lo stesso ℓ - ciclo. □

Esempio 18.5 In S_4 vi sono

- un solo ciclo di lunghezza 1;
- $\frac{1}{2}\frac{4!}{(4-2)!}=6$ cicli di lunghezza 2;
- $\frac{1}{3}\frac{4!}{(4-3)!}=8$ cicli di lunghezza 3;
- $\frac{1}{4}\frac{4!}{(4-4)!}=6$ cicli di lunghezza 4.

Quindi le permutazioni cicliche di S_4 sono complessivamente $1+6+8+6=21$.

Esercizio 18.6* Trovare tutti i 3-cicli di S_5.

Osservazione 18.7 Poiché il gruppo S_4 ha ordine $4!=24$, dall'Esempio 18.5 segue che non tutte le permutazioni di S_4 sono cicliche. Precisamente, ne esistono 3 non cicliche. Si tratta delle seguenti:

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(1,2)(3,4)$$
$$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(1,3)(2,4)$$
$$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(1,4)(2,3)$$

Ognuna di esse è prodotto di due 2-cicli. Ciò è dovuto ad una importante proprietà generale, che ci apprestiamo a dimostrare.

Fissiamo una permutazione $\sigma \in S_n$. Consideriamo, sull'insieme $X = \{1, ..., n\}$, la relazione binaria $\sim_\sigma$ così definita: per ogni $a, b \in X$ poniamo $a \sim_\sigma b$ se esiste un intero i tale che $\sigma^i(a) = b$.

Proposizione 18.8 La relazione $\sim_\sigma$ è una relazione di equivalenza.

Dimostrazione: Per ogni $a \in X$, $\sigma^0(a) = id(a) = a$, quindi $a \sim_\sigma a$. Ciò prova la proprietà riflessiva.
Siano $a, b \in X$ tali che $a \sim_\sigma b$. Allora esiste un intero i tale che $\sigma^i(a) = b$. Ma allora $a = (\sigma^i)^{-1}(b) = \sigma^{-i}(b)$, quindi $b \sim_\sigma a$. Ciò prova la proprietà simmetrica.
Siano $a, b, c \in X$ tali che $a \sim_\sigma b$ e $b \sim_\sigma c$. Allora esistono interi i, j tali che $\sigma^i(a) = b$, $\sigma^j(b) = c$. Segue che $c = \sigma^j(\sigma^i(a)) = \sigma^j\sigma^i(a) = \sigma^{j+i}(a)$, quindi $a \sim_\sigma c$. Ciò prova la proprietà transitiva. □

Definizione 18.9 Per ogni $a \in X$, la classe di equivalenza di a rispetto alla relazione $\sim_\sigma$ si dice *orbita di a sotto l'azione di* σ. La si denota con $\Omega_\sigma(a)$. Gli insiemi $\Omega_\sigma(a)$, al variare di a in X, si dicono le *orbite* di σ. Si ha $\Omega_\sigma(a) = \{\sigma^i(a) \mid i \in \mathbb{Z}\}$.

Proposizione 18.10 Sia $a \in X$. Allora esiste un intero positivo ℓ tale che

$$\Omega_\sigma(a) = \{\sigma^0(a), \sigma^1(a), ..., \sigma^{\ell-1}(a)\},$$

ove gli elementi elencati sono a due a due distinti.

Dimostrazione: Essendo $\Omega_\sigma(a) \subset X$, l'insieme $\Omega_\sigma(a)$ è finito. Quindi esistono $i, j \in \mathbb{Z}, i > j$, tali che $\sigma^i(a) = \sigma^j(a)$. Pertanto $\sigma^{-j+i}(a) = \sigma^{-j}(\sigma^i(a)) = a$. Poiché $i - j > 0$, l'insieme

$$\{n \in \mathbb{Z}, n > 0 \mid \sigma^n(a) = a\}$$

è non vuoto, e quindi, per l'assioma di buon ordinamento, possiede un minimo ℓ. Sia $i \in \mathbb{Z}$. Siano q, r il quoziente ed il resto della divisione di i per ℓ. Allora

$$\sigma^i(a) = \sigma^{\ell q + r}(a) = \sigma^r\left(\sigma^\ell\right)^q(a) = \sigma^r(a),$$

poiché $\sigma^\ell(a) = a$. Siccome $0 \leq r \leq \ell - 1$, ciò prova che $\Omega_\sigma(a) \subset \{\sigma^0(a), \sigma^1(a), ..., \sigma^{\ell-1}(a)\}$. L'altra inclusione è ovvia. Ciò prova l'uguaglianza voluta. La dimostrazione della seconda parte dell'enunciato è lasciata per esercizio. □

Nota Il numero ℓ della Proposizione 18.10 è la cardinalità dell'insieme $\Omega_\sigma(a)$. Per questo lo si dice *lunghezza* dell'orbita $\Omega_\sigma(a)$.

Definizione 18.11 La permutazione ciclica $(\sigma^0(a), \sigma^1(a), ..., \sigma^{\ell-1}(a))$ si dice *ciclo associato all'orbita* di a sotto l'azione di σ. Al variare di a in X, i cicli associati alle orbite di a sotto l'azione di σ si dicono i *cicli di* σ.

Osservazione 18.12 (a) Il ciclo associato ad ogni orbita di lunghezza 1 *(orbita banale)* è la permutazione identica.
(b) Sia $\gamma = (\sigma^0(a), \sigma^1(a), ..., \sigma^{\ell-1}(a))$ il ciclo associato a $\Omega_\sigma(a)$. Allora $\gamma = (a, \gamma(a), ..., \gamma^{\ell-1}(a))$ e, in particolare, $\sigma(a) = \gamma(a)$. Inoltre, $\Omega_\sigma(a) = \Omega_\gamma(a)$.

Esercizio 18.13 Determinare le orbite ed i cicli della permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 5 & 7 & 12 & 2 & 9 & 1 & 6 & 8 & 10 & 11 & 3 \end{pmatrix}.$$

<u>Svolgimento</u>: Le orbite di σ sono

$\Omega_\sigma(1) = \{1, 4, 12, 3, 7\} = \Omega_\sigma(4) = \Omega_\sigma(12) = \Omega_\sigma(3) = \Omega_\sigma(7),$
$\Omega_\sigma(2) = \{2, 5\} = \Omega_\sigma(5),$
$\Omega_\sigma(6) = \{6, 9, 8\} = \Omega_\sigma(6) = \Omega_\sigma(9) = \Omega_\sigma(8),$
$\Omega_\sigma(10) = \{10\},$
$\Omega_\sigma(11) = \{11\}.$

Quindi i cicli di σ sono:

$$(1, 4, 12, 3, 7), \quad (2, 5), \quad (6, 9, 8), \quad (10), \quad (11).$$

I cicli (10) e (11) coincidono con la permutazione identica.

Il nostro prossimo obiettivo è stabilire il modo in cui una permutazione può essere ricostruita a partire dai suoi cicli.

Definizione 18.14 Si dice *supporto* di una permutazione l'insieme degli elementi che essa non lascia fissi.

Esempio 18.15 (a) La permutazione identica è l'unica permutazione avente supporto vuoto.
(b) Se ℓ è un intero maggiore di 1, il supporto del ciclo $(a_1, a_2, ..., a_\ell)$ è $\{a_1, a_2, ..., a_\ell\}$, che è anche la sua unica orbita non banale.
(c) Più in generale, il supporto di una permutazione è l'unione delle sue orbite non banali.

Definizione 18.16 Due permutazioni di S_n si dicono *disgiunte* se i loro supporti sono insiemi disgiunti.

Osservazione 18.17 I cicli associati ad una permutazione sono a due a due disgiunti. Infatti i loro supporti non vuoti sono le orbite della permutazione, che, in quanto classi di equivalenza, sono insiemi a due a due disgiunti.

Lemma 18.18 Il prodotto tra permutazioni disgiunte è commutativo.

Dimostrazione: Siano $\sigma_1, \sigma_2 \in S_n$ permutazioni disgiunte. Sia $a \in X$. Allora a non appartiene al supporto di σ_1 oppure non appartiene al supporto di σ_2. Possiamo supporre, senza ledere la generalità, che valga il secondo caso. Allora a viene lasciato fisso da σ_2, quindi $\sigma_1\sigma_2(a) = \sigma_1(a)$. Se $\sigma_1(a) = a$ allora $\sigma_1\sigma_2(a) = \sigma_1(a) = a = \sigma_2\sigma_1(a)$. Altrimenti l'orbita $\Omega_{\sigma_1}(a)$ non è banale, ed è quindi contenuta nel supporto di σ_1. Poiché $\sigma_1(a) \in \Omega_{\sigma_1}(a)$, segue che $\sigma_1(a)$ appartiene al supporto di σ_1. Ma allora $\sigma_1(a)$ non appartiene al supporto di σ_2, quindi viene lasciato fisso da σ_2. Pertanto $\sigma_2\sigma_1(a) = \sigma_1(a)$. Abbiamo così provato che, anche in questo caso, $\sigma_1\sigma_2(a) = \sigma_2\sigma_1(a)$. Stante l'arbitrarietà di a, segue che $\sigma_1\sigma_2 = \sigma_2\sigma_1$. □

Proposizione 18.19 *(Decomposizione in cicli disgiunti)* Ogni permutazione è uguale al prodotto dei suoi cicli.

Dimostrazione: Sia $\sigma \in S_n$, e siano $\gamma_1, ..., \gamma_r$ i suoi cicli diversi dalla permutazione identica. Siano $\Omega_1, ..., \Omega_r$ le corrispondenti orbite, tutte non banali. In base all'Osservazione 18.17, queste sono a due a due disgiunte. Sia $a \in X$. Allora, se a viene lasciato fisso da σ, non appartiene al suo supporto, e quindi non appartiene ad alcuna delle orbite $\Omega_1, ..., \Omega_r$, che sono i supporti dei cicli $\gamma_1, ..., \gamma_r$ (v. Esempio 18.15 (b)). Pertanto a viene lasciato fisso da ciascuno dei cicli $\gamma_1, ..., \gamma_r$. Segue che $\gamma_1 \cdots \gamma_r(a) = a = \sigma(a)$. Supponiamo allora che a non venga lasciato fisso da σ. In tal caso a appartiene ad una delle orbite $\Omega_1, ..., \Omega_r$. Supponiamo, senza ledere la generalità, che appartenga all'orbita Ω_r, associata al ciclo γ_r. Allora, in base all'Osservazione 18.12 (b), $\Omega_r = \Omega_\sigma(a)$ e, quindi, $\gamma_r(a) = \sigma(a)$. Inoltre quest'ultimo elemento, che appartiene a $\Omega_r = \Omega_\sigma(a)$, non appartiene a nessuna delle orbite $\Omega_1, ..., \Omega_{r-1}$, ossia non appartiene ai supporti di $\gamma_1, ..., \gamma_{r-1}$, e quindi viene lasciato fisso da tutti i cicli $\gamma_1, ..., \gamma_{r-1}$. Pertanto viene lasciato fisso anche dal prodotto $\gamma_1 \cdots \gamma_{r-1}$. Segue che $\gamma_1 \cdots \gamma_r(a) = (\gamma_1 \cdots \gamma_{r-1})\gamma_r(a) = \gamma_r(a) = \sigma(a)$. Abbiamo così provato che, per ogni $a \in X$, $\gamma_1 \cdots \gamma_r(a) = \sigma(a)$, ossia che $\sigma = \gamma_1 \cdots \gamma_r$. □

Osservazione 18.20 Alla luce del Lemma 18.18, nella scrittura $\sigma = \gamma_1 \cdots \gamma_r$ è indifferente l'ordine dei fattori a secondo membro.

Nota Ogni rappresentazione di una permutazione come prodotto dei suoi cicli si dice *decomposizione in cicli disgiunti.* In essa possono essere, indifferentemente, inclusi oppure omessi i cicli di lunghezza 1, che coincidono con la permutazione identica.

Definizione 18.21 Siano $\gamma_1, ..., \gamma_r$ i cicli della permutazione $\sigma \in S_n$, ivi compresi tutti quelli di lunghezza 1. Sia, per ogni $i = 1, ..., r$, ℓ_i la lunghezza di γ_i. Possiamo supporre che i cicli siano stati ordinati in modo che $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_r$. Allora $(\ell_1, \ell_2, ..., \ell_r)$ si dice la *struttura ciclica* di σ.

Chiaramente si avrà $\ell_1 + \ell_2 + \cdots + \ell_r = n$, poiché $\ell_1, \ell_2, ..., \ell_r$ sono le lunghezze delle orbite di σ, che formano una partizione dell'insieme X.

Esempio 18.22 (a) In base all'Esercizio 18.13,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 5 & 7 & 12 & 2 & 9 & 1 & 6 & 8 & 10 & 11 & 3 \end{pmatrix} = (1,4,12,3,7)(2,5)(6,9,8)\cancel{(10)}\,\cancel{(11)}.$$

Questa è una decomposizione di σ in cicli disgiunti. Pertanto la struttura ciclica di σ è

$$(5,3,2,1,1).$$

(b) Le decomposizioni presentate nell'Osservazione 18.7 sono le decomposizioni in cicli disgiunti delle tre permutazioni non cicliche di S_4.

Osservazione 18.23 L'enunciato del Lemma 18.18 non si estende alle permutazioni non disgiunte. Ad esempio, in S_3 i cicli $(1,2)$ e (2,3) non sono disgiunti, e si ha

$$(1,2)(2,3) = (1,2,3), \qquad (2,3)(1,2) = (1,3,2).$$

Esercizio 18.24 Calcolare $(1,3,7,2,4)(6,8,1,4,7,5) \in S_8$.

Svolgimento: Si ha $(1,3,7,2,4)(6,8,1,4,7,5) = \cancel{(1)}(2,4)(3,7,5,6,8)$.

La struttura ciclica è utile ai fini della determinazione del periodo di una permutazione e, come vedremo più avanti, della sua classe di parità.

Dalla dimostrazione della Proposizione 18.10 si deduce facilmente il seguente risultato ausiliario, la cui dimostrazione è lasciata per esercizio al lettore.

Lemma 18.25 Sia $\sigma \in S_n$. Sia $a \in X$, e sia ℓ la lunghezza di $\Omega_\sigma(a)$. Allora, per ogni $i \in \mathbb{Z}$, $\sigma^i(a) = a$ se e solo se ℓ divide i.

Proposizione 18.26 Sia $\sigma \in S_n$, e sia $(\ell_1, \ell_2, ..., \ell_r)$ la sua struttura ciclica. Allora

$$o(\sigma) = \mathrm{mcm}(\ell_1, \ell_2, ..., \ell_r).$$

Dimostrazione: Siano $\gamma_1, ..., \gamma_r$ i cicli (non banali) di σ, di lunghezze $\ell_1, \ell_2, ..., \ell_r$. Sia $a \in X$, e sia γ_r il ciclo associato all'orbita $\Omega_\sigma(a)$, che, in base all'Osservazione 18.12 (b), è uguale a $\Omega_{\gamma_r}(a)$ ed è il supporto di γ_r. In tal caso, per ogni $i \in \mathbb{Z}$, $\gamma_r^{\,i}(a) \in \Omega_{\gamma_r}(a)$, e quindi $\gamma_r^{\,i}(a)$ è lasciato fisso da $\gamma_1, ..., \gamma_{r-1}$, i cui supporti sono disgiunti da $\Omega_{\gamma_r}(a)$. Pertanto $\gamma_r^{\,i}(a)$ è anche lasciato fisso dal prodotto $\gamma_1 \cdots \gamma_{r-1}$ e da tutte le sue potenze. Quindi, per ogni $i \in \mathbb{Z}$,

$$\sigma^i(a) = (\gamma_1 \cdots \gamma_r)^i(a) = (\gamma_1 \cdots \gamma_{r-1})^i \gamma_r^{\,i}(a) = \gamma_r^{\,i}(a), \tag{1}$$

dove abbiamo utilizzato, nell'ordine, il Lemma 18.18 e la Proposizione 17.6 (d). Ora, in base al Lemma 18.25, $\gamma_r^{\,i}(a) = a$ se e solo se ℓ_r divide i. Ora, al variare di a in X, all'indice r si sostituiscono tutti gli indici $k = 1, 2, ..., r$. Quindi, in base alla (1), si ha $\sigma^i(a) = a$ per ogni a se e solo se ℓ_k divide i per ogni $k = 1, 2, ..., r$. Il più piccolo intero positivo siffatto è $i = \mathrm{mcm}(\ell_1, \ell_2, ..., \ell_r)$. □

Corollario 18.27 Il periodo di un ciclo è uguale alla sua lunghezza.

Dimostrazione: Se $\sigma \in S_n$ è un ciclo di lunghezza ℓ, allora la sua struttura ciclica è

$$(\ell, \underbrace{1,\ldots,1}_{n-\ell}).$$

La tesi segue allora immediatamente dalla Proposizione 18.26. □

Esempio 18.28 La permutazione σ dell'Esempio 18.22 (a) ha periodo uguale a $\text{mcm}(2,3,5)=30$.

I protagonisti del resto di questa lezione saranno i 2-cicli. Essi vengono detti anche *trasposizioni* o *scambi*, poiché, per ogni intero $n \geq 2$, il ciclo $(a_1, a_2) \in S_n$ è la permutazione che invia a_1 in a_2 e viceversa, mentre lascia fisso ogni altro elemento.
Le trasposizioni non solo sono le permutazioni più semplici dopo la permutazione identica, ma sono anche i costituenti fondamentali dell'insieme delle permutazioni, poiché, a partire da esse, si può costruire ogni permutazione, nel modo che ora indicheremo.

Proposizione 18.29 *(Cicli e trasposizioni)* Sia ℓ un intero maggiore di 1. Ogni $\ell-$ciclo è prodotto di $\ell-1$ trasposizioni.

Dimostrazione: Sia σ un $\ell-$ciclo. A meno di ridenominare gli elementi, possiamo supporre che $\sigma = (1,2,\ldots,\ell)$. Si verifica facilmente che

$$(1,2,\ldots,\ell) = (1,2)(2,3)\cdots(\ell-1,\ell). \quad \square$$

Osservazione 18.30 L'enunciato della Proposizione 18.29 non ha senso per $\ell = 1$. Tuttavia, anche la permutazione identica di S_n $(n \geq 2)$ si scrive come prodotto di trasposizioni: $id = (1,2)(1,2)$.

Dalla Proposizione 18.19 e dalla Proposizione 18.29 segue subito il

Corollario 18.31 *(Permutazioni e trasposizioni)* Sia n un intero maggiore di 1. Allora ogni permutazione di S_n si scrive come prodotto di trasposizioni.

Abbiamo provato, nell'Esercizio 4.18 (a), che la trasposizione $(1,2)$ è dispari. Ciò si può generalizzare.

Proposizione 18.32 *(Disparità delle trasposizioni)* Ogni trasposizione è una permutazione dispari.

Dimostrazione: Sia n un intero maggiore di 1, e sia σ una trasposizione di S_n. Allora $\sigma = (a,b)$ ove $a,b \in \{1,2,\ldots,n\}, a \neq b$. Se $\sigma = (1,2)$ il risultato è noto. Altrimenti uno tra 1 e 2 non appartiene all'insieme $\{a,b\}$. Supponiamo dapprima che i cicli (a,b) ed (1,2) non siano disgiunti. Senza ledere la generalità possiamo allora supporre che $a=1, b \neq 2$. In tal caso $(2,b)\sigma(2,b) = (2,b)(1,b)(2,b) = (1,2)$. Dalle regole di moltiplicazione date nell'Osservazione 4.15, segue che σ ed (1,2) hanno la stessa parità, quindi σ è dispari. Supponiamo ora che i cicli (a,b) ed (1,2) siano disgiunti. Allora

$$(2,b)(1,a)\sigma(1,a)(2,b) = (2,b)(1,a)(a,b)(1,a)(2,b) = (1,2).$$

Segue nuovamente che σ ed (1,2) hanno la stessa parità, quindi σ è dispari anche in questo caso. □

Dalla Proposizione 18.32 e dalle regole di moltiplicazione segue immediatamente il seguente:

Corollario 18.33 *(Classe di parità di una permutazione)* Sia *n* un intero maggiore di 1. Allora una permutazione di S_n è pari se e solo se è prodotto di un numero pari di trasposizioni.

Corollario 18.34 *(Classe di parità di un ciclo)* Un ciclo è pari se e solo se è di lunghezza dispari.

Dimostrazione: L'unico ciclo di lunghezza 1 è l'identità ed è quindi pari. Sia σ un ciclo di lunghezza $\ell > 1$. Allora, in base alla Proposizione 18.29, esso è prodotto di $\ell - 1$ trasposizioni. In base al Corollario 18.33 segue che σ è pari se e solo se $\ell - 1$ è pari, cioè se e solo se ℓ è dispari. □

Il Corollario 18.34, insieme alla decomposizione in cicli disgiunti, consente di determinare la classe di parità di una permutazione in maniera molto più agevole rispetto ai procedimenti seguiti nella Lezione 4 ed, in particolare, nell'Esercizio 4.22.

Esercizio 18.35 Dire se la permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 7 & 6 & 12 & 11 & 3 & 9 & 10 & 2 & 4 & 1 & 8 \end{pmatrix} \in S_{12}$$

è pari o dispari.

Svolgimento: La decomposizione di σ in cicli disgiunti è

$$\sigma = \underbrace{(1,5,11)}_{\text{pari}}\underbrace{(2,7,9)}_{\text{pari}}\underbrace{(3,6)}_{\text{dispari}}\underbrace{(4,12,8,10)}_{\text{dispari}}$$

Quindi σ è pari.

La classe di parità di una permutazione è quindi determinata dalla sua struttura ciclica, che, nell'Esercizio 18.35, è $(4,3,3,2)$. In generale una permutazione è pari se e solo se, nella sua struttura ciclica, il numero di lunghezze pari è pari.

Esercizio 18.36* Determinare tutti gli elementi di A_3 ed A_4 utilizzando le strutture cicliche.