UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Algebra

Alessandro D'Andrea

8. La relazione di coniugio

Richiami

- Gruppo additivo $\mathbb{Z}/n$
- Gruppo moltiplicativo $(\mathbb{Z}/n)^\times$
- C_n, D_n, S_n, A_n
- Posso contare gli elementi di un gruppo ripartendoli in classi laterali (Teorema di Lagrange)
- Oggi: **Relazione di coniugio**
  - Ripartisco gli elementi in classi coniugate
  - Le classi coniugate non hanno tutte lo stesso numero di elementi
  - I gruppi di ordine p^n hanno centro non banale
  - I gruppi di ordine p^2 sono abeliani

Elementi coniugati

Due elementi $a, b \in G$ si dicono coniugati se esiste $g \in G$ tale che $b = gag^{-1}$. Scriveremo $a \sim b$ per indicare che a, b sono coniugati.

Vedremo più avanti nel corso che matrici coniugate vengono fuori in modo naturale dai cambiamenti di base.

Due elementi coniugati hanno necessariamente lo stesso ordine. In effetti $(gag^{-1})^n = ga^ng^{-1}$, quindi $a^n = 1$ se e solo se $(gag^{-1})^n = 1$.

Ogni elemento è coniugato a se stesso. L'elemento $a \in G$ è coniugato solo a se stesso esattamente quando $ag = ga$ per ogni $g \in G$: questi elementi sono detti centrali e formano un sottogruppo $Z(G)$, detto centro di G. L'identità è sempre centrale.

In un gruppo abeliano, ogni elemento è centrale.

Relazione di coniugio

La relazione di coniugio è una relazione di equivalenza.

- Riflessività: $a \sim a$
  - $a = 1 \cdot a \cdot 1^{-1}$.
- Simmetria: $a \sim b \implies b \sim a$
  - Se $b = gag^{-1}$, allora $a = g^{-1}bg = g^{-1}b(g^{-1})^{-1}$.
- Transitività: $a \sim b, b \sim c \implies a \sim c$
  - Se $b = gag^{-1}$ e $c = hbh^{-1}$, allora $c = h(gag^{-1})h^{-1} = (hg)a(hg)^{-1}$.

Come accade per ogni relazione di equivalenza, il gruppo G risulta ripartito nell'unione disgiunta di classi di equivalenza, dette classi di coniugio o classi coniugate. Indicheremo la classe di coniugio di a con il simbolo $[a]$.

Classi di coniugio in S_3

Gli elementi di S_3 sono

- Ordine 1: l'identità Id.
- Ordine 2: le trasposizioni $(1\,2), (1\,3), (2\,3)$.
- Ordine 3: i 3-cicli $(1\,2\,3)$ e $(1\,3\,2)$.

Ogni trasposizione commuta solo con l'identità e se stessa. Questo mostra che l'unico elemento centrale di S_3 è l'identità. Di conseguenza, l'unica classe di coniugio costituita da un solo elemento è quella di Id.
Le altre classi devono tutte contenere strettamente più di un elemento; inoltre ciascuna classe deve contenere elementi tutti dello stesso ordine.

L'unica possibilità è:

$$[\mathrm{Id}] = \{\mathrm{Id}\}, \quad [(1\,2)] = \{(1\,2), (1\,3), (2\,3)\}, \quad [(1\,2\,3)] = \{(1\,2\,3), (1\,3\,2)\}.$$

Quanti elementi in una classe?

Quanti e quali elementi di G sono coniugati all'elemento $a \in G$?

Sicuramente, se $g \in G$ commuta con a, allora $gag^{-1} = agg^{-1} = a$. Gli elementi che commutano con a costituiscono il centralizzatore $C(a)$ di a, che è un sottogruppo di G.

I coniugati $gag^{-1} = hah^{-1}$ coincidono se e solo se $(g^{-1}h)a = a(g^{-1}h)$, cioè quando $g^{-1}h \in C(a)$. Questo è un altro modo di dire che $g \equiv h \mod C(a)$.

In altre parole, g e h inducono lo stesso coniugato di a se e solo se $g \equiv h \mod C(a)$, cioè se e solo se g, h appartengono allo stesso laterale sinistro di $C(a)$ in G. Questo mostra che a possiede tanti coniugati quante sono le classi laterali di $C(a)$ in G. In altre parole

$$|[a]| = [G : C(a)].$$

Il numero di coniugati di a in G è un divisore di $|G|$.

L'equazione delle classi - I

Ogni gruppo G è unione disgiunta delle sue classi coniugate.

Pertanto, l'ordine di G si può ricavare sommando il numero di elementi di tutte le sue classi coniugate.

Ad esempio, in S_3

$$S_3 = [\mathrm{Id}] \cup [(1\,2)] \cup [(1\,2\,3)] \implies 6 = 1 + 2 + 3.$$

L'equazione delle classi - II

Supponiamo che G sia un gruppo con p^n elementi, dove p è un numero primo. L'equazione delle classi diventa

$$p^n = |Z(G)| + \text{ potenze di } p.$$

Questo mostra che $|Z(G)|$ è un multiplo di p, e quindi $Z(G)$ non può essere limitato alla sola identità, ma deve contenere anche altri elementi.

Gruppi di ordine p^2

Se $|G| = p^n$, allora $|Z(G)|$ non può essere uguale a p^{n-1}.
Se così fosse, un elemento $a \notin Z(G)$ dovrebbe commutare sicuramente con se stesso e con tutti gli elementi di $Z(G)$. Ma l'unico divisore di p^n strettamente più grande di p^{n-1} è proprio p^n, e quindi a dovrebbe commutare con tutto G. Questo mostrerebbe che $a \in Z(G)$, un assurdo.

- $|G| = p \implies G$ è ciclico
- $|G| = p^2 \implies |Z(G)| = p^2$, e quindi G è abeliano
- $|G| = p^3 \implies |Z(G)| = p$ oppure p^3
- $|G| = p^4 \implies |Z(G)| = p, p^2$ oppure p^4
- ...

Coniugio in S_n

Se $\tau \in S_n$, allora

$$\tau(a_1\ a_2\ \dots\ a_k)\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \dots\ \tau(a_k)).$$

Allo stesso modo, due permutazioni coniugate in S_n hanno la stessa struttura ciclica, ed è vero anche il viceversa!

Ad esempio, la permutazione $(1\,2\,3\,4\,5)$ viene coniugata in $(1\,4\,2\,3\,5)$ dalla permutazione

$$\sigma = \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 4 \\ 3 \mapsto 2 \\ 4 \mapsto 3 \\ 5 \mapsto 5. \end{cases}$$

Si ha in effetti $(1\,4\,2\,3\,5) = \sigma(1\,2\,3\,4\,5)\sigma^{-1}$.

Sottogruppi normali

Un sottogruppo $N < G$ è normale se $gNg^{-1} \subset N$. Equivalentemente, se N contiene i coniugati di ogni suo elemento.

Un sottogruppo normale è unione di classi di coniugio.

Le classi di coniugio di S_5 sono

- L'identità: 1 elemento
- $[(1\,2)]$: 10 elementi
- $[(1\,2\,3)]$: 20 elementi
- $[(1\,2\,3\,4)]$: 30 elementi
- $[(1\,2\,3\,4\,5)]$: 24 elementi
- $[(1\,2)(3\,4)]$: 15 elementi
- $[(1\,2\,3)(4\,5)]$: 20 elementi.

Un sottogruppo di S_5 contiene Id e il suo ordine divide $120 = |\,S_5\,|$. Le uniche unioni di classi di coniugio con queste proprietà sono 1, 120, $40 = 1 + 15 + 24$, $60 = 1 + 15 + 20 + 24$.

Sottogruppi normali di S_5

- L'identità: 1 elemento
- $[(1\,2)]$: 10 elementi
- $[(1\,2\,3)]$: 20 elementi
- $[(1\,2\,3\,4)]$: 30 elementi
- $[(1\,2\,3\,4\,5)]$: 24 elementi
- $[(1\,2)(3\,4)]$: 15 elementi
- $[(1\,2\,3)(4\,5)]$: 20 elementi.

$40 = 1 + 15 + 24$ fornisce $[\mathrm{Id}] \cup [(1\,2)(3\,4)] \cup [(1\,2\,3\,4\,5)]$. Se fosse un sottogruppo di S_5, sarebbe tutto contenuto in A_5, e dovrebbe dividere 60 per il teorema di Lagrange.

$60 = 1 + 15 + 20 + 24$ dà due possibilità. Una è A_5, che è un sottogruppo normale. Se l'altra unione fosse un sottogruppo, allora la sua intersezione con A_5 sarebbe il sottogruppo di ordine 40 del caso precedente, che abbiamo visto non esistere.

Sottogruppi normali di A_4

Proviamo ad eseguire lo stesso conto per A_4. Le strutture cicliche degli elementi sono:

- L'identità: 1 elemento
- I 3-cicli: 8 elementi
- I prodotti di due trasposizioni disgiunte: 3 elementi

Anche nei gruppi alterni, gli elementi coniugati hanno la stessa struttura ciclica. Tuttavia, due elementi con la stessa struttura ciclica non sono necessariamente coniugati. Le classi coniugate in A_4 sono

- $[\mathrm{Id}]$: 1 elemento
- $[(1\,2\,3)] = \{(1\,2\,3), (1\,4\,2), (1\,3\,4), (2\,4\,3)\}$: 4 elementi
- $[(1\,3\,2)] = \{(1\,3\,2), (1\,2\,4), (1\,4\,3), (2\,3\,4)\}$: 4 elementi
- $[(1\,2)(3\,4)] = \{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$: 3 elementi

Le uniche possibilità per i sottogruppi normali sono $\{\mathrm{Id}\}$, A_4 e $V_4 = [\mathrm{Id}] \cup [(1\,2)(3\,4)]$, che è effettivamente un sottogruppo.