

Algebra I

Paolo Bettelini

Contents

1	Richiami di teoria degli insiemi	1
2	Classi di equivalenza	2
3	Esempi di maggiorante etc.	3
3.1	Relazioni irreflessiva	4
4	Funzioni	4
4.1	Proprietà	4
4.2	Iniettività suriettività	6
4.3	Composizione	6
4.4	Definizione di invertibilità	6
5	Matrici	8
6	Numeri naturali	10
7	Numeri interi	11
7.1	Divisione con resto	11
7.2	Massimo comun divisore	11
8	Classi di resto	11
9	Monoidi e gruppi	12
10	Gruppi geometrici	13
11	Altro	13
12	Sottogruppi normali	13
12.1	classi di coniugio nel simmetrico	14

1 Richiami di teoria degli insiemi

Data una famiglia finita o infinite di insiemi $\{A_i\}_{i \in I}$, la loro intersection

$$\bigcap_{i \in I} A_i$$

è l'insieme degli elementi che stanno in tutti gli insiemi A_i , mentre la loro unione

$$\bigcup_{i \in I} A_i$$

è l'insieme degli elementi che stanno in almeno uno degli insiemi A_i .

2 Classi di equivalenza

Esempio insieme quoziente \sim su \mathbb{Z} dove $a \sim b \iff |a| = |b|$ è dato da

$$\{\{0\}, \{1, -1\}, \{2, -2\}, \dots\}$$

L'unica relazione di equivalenza che è un ordine è l'uguaglianza.

3 Esempi di maggiorante etc.

In \mathbb{R} consideriamo l'usuale ordinamento. Consideriamo i sottoinsiemi

$$A = \{x \in \mathbb{R} \mid x > 0\}$$

$$B = \{x \in \mathbb{R} \mid x \geq 0\}$$

e

$$C = \{x \in \mathbb{R} \mid 0 < x \leq 2\}$$

Il sottoinsieme A non ha maggioranti. Ogni numero non-positivo è minorante di A . A non ha nè massimo nè minimo.

Il sottoinsieme B non ha maggioranti. Ogni numero non-positivo è minorante di B . B ha 0 come minimo.

Il sottoinsieme C ha minoranti e maggioranti ma non minimo e ha 2 come massimo.

Consideriamo ora la relazione di divisibilità in \mathbb{N} . L'unico maggiorante è 0 in quanto tutti dividono zero, ed è un massimo. Il numero 1 è minorante, ed è un minimo.

Se ora prendiamo l'insieme $\{2, 3, 4, 5\}$, i maggioranti sono multipli del minimo comune multiplo (60), i minoranti sono i divisori comuni. Non ci sono massimo e minimo.

Proposition Il massimo è unico

Il massimo, se esiste, è unico.

Proof Il massimo è unico

Diciamo che a, b sono due massimi di A , cioè maggioranti di A che appartiene ad A . Abbiamo allora $a \geq b$ (in quanto a è un maggiorante) e $b \geq a$ (in quanto b è un maggiorante). Abbiamo quindi che $a = b$.

Definizione Massimale

Un elemento $a \in A$ con A insieme parzialmente ordinato è detto massimale in A se non esiste alcun $b \in A$ tale che $a \leq b$ dove $a \neq b$.

Definizione Minimale

Un elemento $a \in A$ con A insieme parzialmente ordinato è detto minimale in A se non esiste alcun $b \in A$ tale che $a \geq b$ dove $a \neq b$.

Ogni massimo è massimale, ogni minimo è minimale.

Esempio in cui i massimali non sono massimi: in \mathbb{N} , rispetto alla divisibilità, consideriamo l'insieme $A = \{2, 3, 4, 5, 6\}$.

- Il numero 2 è minimale ma non massimale.
- Il numero 3 è minimale ma non massimale.
- Il numero 4 è massimale perché non divide nient'altro, ma non minimale.
- Il numero 5 è sia massimale che minimale.
- Il numero 6 è massimale ma non minimale.

In una relazione d'ordine totale un eventuale elemento massimale è massimo. Infatti, se a è massimale per A , preso un qualsiasi elemento $b \in A$, sappiamo che vale almeno una tra $a \leq b$ e $b \leq a$. Se vale la prima, per la definizione di massimalità di a , non può essere $a \neq b$. Nel secondo caso, $b \leq a$ e quindi a è un massimo. Analogamente per i minimali.

3.1 Relazioni irreflessiva

Data una relazione d'ordine \leq , possiamo ottenere la relazione d'ordine stretta $<$ dicendo che $a < b$ se $a \leq b$ e $a \neq b$.

Si può definire l'ordine stretto rimpiazzando la proprietà riflessiva con quella irreflessiva.

4 Funzioni

Una funzione $\phi: A \rightarrow B$ dove A è il dominio mentre B è il codominio, preso un elemento $a \in A$, la sua immagine viene denotata $\phi(a)$ oppure af .

Se $C \subseteq A$, la sua immagine tramite ϕ è indicata come $C\phi$ che è un sottoinsieme di B .

$$C\phi = \{c\phi \mid c \in C\}$$

Se D è un sottoinsieme di B , la sua immagine inversa tramite ϕ è il sottoinsieme $D\phi^{-1}$ di A degli elementi la cui immagine appartiene a D .

$$D\phi^{-1} = \{a \in A \mid a\phi \in D\}$$

Esempio Funzione

Sia $\phi: \mathbb{R} \rightarrow \mathbb{R}$ definita ponendo $\phi x \triangleq x^2$.

Consideriamo ora $A = \{-1, 0, 1, 2\}$. Abbiamo allora $A\phi = \{1, 0, 4\}$. Consideriamo poi $B = \{-1, 0, 2, 9\}$. Abbiamo allora $B\phi^{-1} = \{0, \sqrt{2}, 3, -3\}$.

L'immagine di una funzione è chiaramente l'immagine per il suo dominio come insieme considerato.

4.1 Proprietà

Proposition

Se $C \subseteq D \subseteq A$, abbiamo $C\phi \subseteq D\phi$.

Proof

Abbiamo che

$$C\phi = \{c\phi \mid c \in C\}$$

Dunque $x \in C\phi$ se e solo se esiste $c \in C$ tale che $x = c\phi$. Ma $C \subseteq D$, dunque $c \in D$. Quindi, $x = c\phi \in D\phi$.

Non è detto che se $C \subset D$ allora $C\phi \subset D\phi$. Mostriamo un esempio in cui $C \subset D$ ma $C\phi = D\phi$. Prendiamo $C = \{1\} \subset D = \{1, -1\}$. Se prendiamo la funzione del quadrato, in ambo caso trovo la stessa immagine per via di ambo gli insiemi.

Ciò non avviene nel caso in cui la funzione fosse iniettiva.

Proposition

Se $E \subseteq F \subseteq B$, abbiamo che $E\phi^{-1} \subseteq F\phi^{-1}$.

TODO: esercizio proof.

Anche qui la medesima proposizione ma con l'inclusione stretta non è assicurata.

Proposition

Se $C \subseteq A$, allora $C\phi\phi^{-1} \supseteq C$.

Proof

Sia $x \in C$. Bisogna mostrare $x \in C\phi\phi^{-1}$. Ricordiamo che $D\phi^{-1} = \{y \in A \mid y\phi \in D\}$. Dunque $Cy\phi = \{y \in A \mid y\phi \in C\phi\}$. Ma ora $x\phi \in C\phi$, perché $x \in C$. Dunque $x \in C\phi\phi^{-1}$.

Nel solito esempio

$$\{1, -1\}\phi\phi^{-1} = \{1, -1\}$$

e

$$\{1\}\phi\phi^{-1} = \{1, -1\}$$

Proposition

Se $D \subseteq B$ allora $D\phi^{-1}\phi \subseteq D$. L'inclusione può essere stretta.

Proof

Sia $x \in D\phi^{-1}\phi$. Ciò significa che $x = z\phi$ per qualche $z \in D\phi^{-1}$. Ma $D\phi^{-1} = \{y \mid y\phi \in D\}$. Dunque, $z \in D\phi^{-1}$, allora $z\phi \in D$, cioè $x \in D$.

Con il solito esempio

$$\{1, 2\}\phi^{-1}\phi = \{1\}$$

$$\{-1\}\phi^{-1}\phi = \emptyset$$

Proposition

Siano $\phi: A \rightarrow B$, $\psi: B \rightarrow C$ e $\theta: C \rightarrow D$ funzioni. allora

$$(\phi\psi)\theta = \phi(\psi\theta)$$

Proof

Notiamo che $\phi\psi: A \rightarrow C$ e $\theta: C \rightarrow D$. Dunque $\phi\psi\theta: A \rightarrow D$. Analogamente $\phi: A \rightarrow B$, $\psi\theta: B \rightarrow D$ e quindi $\phi(\psi\theta): A \rightarrow D$. Per mostrare l'uguaglianza devo mostrare che per ogni $x \in A$ risulta

$$a((\phi\psi)\theta) = a(\phi(\psi\theta))$$

Abbiamo infatti $a((\phi\psi)\theta) = (a(\phi\psi\theta)) = ((a\phi)\psi)\theta$ e $a(\phi(\psi\theta)) = (a\phi)(\psi\theta) = ((a\phi)\psi)\theta$.

Dunque possiamo scrivere semplicemente $\phi\psi\theta$ senza ambiguità.

Siano $\phi: A \rightarrow B$, $\psi: B \rightarrow C$ funzioni. Ci chiediamo ora che $\psi\phi = \phi\psi$. Chiaramente, non è detto che $\phi\psi$ esista. Possiamo confrontarle solo che $A = B$.

Allora guardiamo $\phi: A \rightarrow A$ e $\psi: A \rightarrow A$. Non è comunque detto che $\psi\phi = \phi\psi$ siano uguali.

Definizione Funzione identità

Dato un insieme A , la *funzione identica* di A è la funzione $\text{Id}_A: A \rightarrow A$ definita come $a\text{Id}_A \triangleq a$.

Proposition

Sia $\phi: A \rightarrow B$, allora $\phi\text{Id}_B = \phi$ e $\text{Id}_A\phi = \phi$. TODO: dimostrazione.

4.2 Iniettività suriettività

La definizione di iniettività è equivalente a dire che $b\phi^{-1}$ contiene solo un elemento.

La definizione di suriettività è equivalente a dire che $b\phi^{-1}$ contiene almeno un elemento.

La definizione di suriettività è equivalente a dire che $b\phi^{-1}$ e $b\phi$ contengono solo un elemento.

4.3 Composizione

Date f e g cosa possiamo dire di f e g sapendo che $g(f)$ è suriettiva o iniettiva?

Supponiamo che $g(f)$ sia suriettiva. Dunque, per ogni $c \in C$ esiste a tale che $c = g(f(a))$. In particolare, posto $b = f(a) \in B$, abbiamo che $g(b) = c$ cioè g è suriettiva.

Supponiamo che $g(f)$ sia iniettiva. Dunque, per ogni $a_1, a_2 \in A$ dove $a_1 \neq a_2$, risulta che $g(f(a_1)) \neq g(f(a_2))$. Sicuramente la prima funzione non può fare convergere i due elementi, in quando non potrebbero uscire separati dopo la seconda funzione. In particolare, $f(a_1) \neq f(a_2)$. Quindi, f è iniettiva.

Esempio

Siano $A = \{a\}$ e $B = \{b, b'\}$ con $b \neq b'$, $C = \{c\}$ e $f: A \rightarrow B$ data $f(a) = b$ e $g: B \rightarrow C$ data $g(b) = c$ e $g(b') = c$. Allora $g(f)$ è biettiva. f è iniettiva e g non è iniettiva. f non è suriettiva e g è suriettiva.

4.4 Definizione di invertibilità

Data $f: A \rightarrow B$, allora f è invertibile se esiste $g: B \rightarrow A$ tale che $g(f)$ è la funzione identità su A e $f(g)$ è la funzione identità su B .

Proposition

Se f è invertibile, allora g è unica.

Proof

Prendiamo $h: B \rightarrow A$ tale che $h(f(a)) = a$ e $f(h(b)) = b$. Allora $g = g\text{Id}_A = g(fh) = (gf)h = \text{Id}_B h = h$ e quindi è la funzione identità.

Proposition

Ogni inverso è anch'esso invertibile f^{-1-1} .

Proposition

Se $f: A \rightarrow B$ e $g: B \rightarrow C$ sono invertibili, allora $g(f)$ è invertibile e $(g(f))^{-1} = f^{-1}(g^{-1})$.

Proof

Sappiamo che esistono f^{-1} e g^{-1} . Dunque esiste $f^{-1}(g^{-1})$. Mostriamo che componendo le due in maniera simmetrica si trovano le identità di A e di B .

Proof Invertibilità è equivalente a biettività

(\Rightarrow) Sia f invertibile. Allora sappiamo che $f(f^{-1})$ è la funzione identità di A e $f^{-1}(f)$ è la funzione identità di B . Ora, l'identità di A è iniettiva (anche biettiva), dunque f è iniettiva e l'identità di B è suriettiva (dalle due proposizioni di prima), dunque f è suriettiva.

(\Leftarrow) Sia f biettiva. Dobbiamo costruire $g: B \rightarrow A$ tale che $f(g)$ è l'identità di A e $f(g)$ è l'identità di B . Sappiamo che per ogni $b \in B$ esiste un unico $a \in A$ tale che $f(a) = b$. Poniamo allora $g(b) = a$. Se $b \in B$, allora $f(g(b)) = f(a) = b$. Se $a \in A$, abbiamo che $g(f(a))$ è per definizione di g l'unico elemento $a' \in A$ tale che $f(a') = f(a)$. Siccome f è iniettiva, $a' = a$, e quindi $g(f(a)) = a$ e quindi $g = f^{-1}$.

5 Matrici

Data una matrice A indichiamo con $A_{i,j}$ l'elemento di posto (i, j) .

La trasposta di una triangolare inferiore è triangolare superiore, e viceversa. La trasposta di una matrice diagonale rimane uguale.

Una matrice uguale alla sua trasposta è detta simmetrica.

Definizione

Dato un anello commutativo R diciamo $M_{m,n}(R)$ l'insieme delle matrici $m \times n$ a coefficienti in R .

L'addizione è associativa e commutativa (come nell'anello commutativo). Esiste l'elemento neutro (matrice nulla $0_{m,n}$). Esiste l'elemento inverso $-A = -1 \cdot A$. Si dovrebbe dimostrare l'unicità dell'elemento inverso e del neutro.

Proposition

Date matrici A e B della stessa dimensione, si ha

$$(A + B)^t = A^t + B^t$$

Teorema Moltiplicazione associativa

Se $A \in M_{m,n}(R)$ e $B \in M_{n,p}(R)$ e $C \in M_{p,r}(R)$, allora

$$(AB)C = A(BC)$$

Proof Moltiplicazione associativa

AB è di tipo $m \times p$. L'elemento di posto (i, j) è

$$\sum_{k=1}^n A_{i,k} B_{k,j} = D_{i,j}$$

La matrice $(AB)C$ ha dimensione $m \times r$. L'elemento di posto (i, l) è

$$\begin{aligned} \sum_{j=1}^p D_{i,j} C_{j,l} &= \sum_{j=1}^p \left(\sum_{k=1}^n A_{i,k} B_{k,j} \right) C_{j,l} \\ &= \sum_{j=1}^p \sum_{k=1}^n A_{i,k} B_{k,j} C_{j,l} \end{aligned}$$

BC ha dimensione $n \times r$. L'elemento di posto (k, l) è

$$\sum_{j=1}^p B_{k,j} C_{j,l} = E_{k,l}$$

$A(BC)$ ha dimensione $m \times r$. L'elemento di posto (i, l) è

$$\begin{aligned} \sum_{k=1}^n A_{i,k} E_{k,l} &= \sum_{k=1}^n A_{i,k} \left(\sum_{j=1}^p B_{k,j} C_{j,l} \right) \\ &= \sum_{k=1}^n \sum_{j=1}^p A_{i,k} B_{k,j} C_{j,l} \end{aligned}$$

Proposition Distributività destra

Con $A, B \in M_{m,n}(R)$ e $C \in M_{n,p}(R)$

$$(A + B)C = AC + BC$$

Proposition Distributività sinistra

Con $A, B \in M_{m,n}(R)$ e $C \in M_{n,p}(R)$

$$A(B + C) = AB + AC$$

In generale non vale $AB = BA$. Ambo le operazioni sono definite solo se ambo le matrici sono quadrate con dimensione $n \times n$. In tal caso, non è comunque detto che la proprietà valga. Nel caso in cui $n = 1$ la proprietà commutativa vale necessariamente.

Il principio di annullamento del prodotto non vale.

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

In questo caso il risultato è la matrice nulla ma nessuno dei due era nulla.

Proposition

Se A e B sono invertibili e dello stesso ordine, allora AB è invertibile e $(AB)^{-1} = B^{-1}A^{-1}$.

Esempio Matrice non invertibile

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} x + 2z & y + 2w \\ 2x + 4z & 2y + 4w \end{bmatrix}$$

Notiamo che i punti dove dovrebbe esserci uno 0 sono il doppio di quelli con 1, quindi non vi è soluzione e non è invertibile.

Se A e B sono due matrici quadrate della stessa dimensione tali che $AB = I_n$ allora anche $BA = I_n$ (La dimostrazione non è banale).

Proposition

Se $A \in M_{m,n}(R)$ e $B \in M_{n,p}(R)$ allora $B^t A^t \in M_{p,m}(R)$. Abbiamo quindi che

$$B^t A^t = (AB)^t$$

Proposition

Se A è invertibile, allora

$$(A^t)^{-1} = (A^{-1})^t$$

6 Numeri naturali

Definizione Assiomi di Peano

I numeri naturali sono un insieme \mathbb{N} dotati di una funzione successore $S: \mathbb{N} \rightarrow \mathbb{N}$ e di un elemento fissato 0 tali che:

- la funzione S è iniettiva;
- $0 \notin \text{Im}_S$;
- se $A \subseteq \mathbb{N}$ tale che $0 \in A$ e $As \subseteq A$, allora $A = \mathbb{N}$;

L'esistenza di un tale insieme è garantita dalla teoria assiomatica. Tuttavia, dobbiamo garantire che i modelli degli assiomi di Peano siano isomorfi, quindi trovare una funzione biettiva fra tutti i modelli. Quindi, dati due modelli $(\mathbb{N}, S, 0)$ e $(\mathbb{N}', S', 0')$ bisogna trovare una funzione biettiva $f: \mathbb{N} \rightarrow \mathbb{N}'$ tale che $f(0) = 0'$ e $nf s' = ns f$

$$\begin{array}{ccc} n & \xrightarrow{f} & n' \\ s \downarrow & & \downarrow s' \\ ns & \xrightarrow{f} & n's' \end{array}$$

Questo può essere fatto con un procedimento cosiddetto per ricorrenza, dipende fortemente dall'assioma 3. In generale gli assiomi di Peano mi permettono di definire successioni di oggetti per ricorrenza, cioè assegnando un oggetto associato a 0 e il modo di costruire l'oggetto associato (come per esempio il fattoriale o l'addizione nei naturali).

La somma è definita nel seguente modo ricorrente: $m + n = 0$ e $m + S(n) = S(m + n)$.

Usando gli assiomi posso dimostrare varie proprietà dell'addizione, detta moltiplicazione (da definire anch'esso per ricorrenza) e dell'ordine (anch'esso da definire per ricorrenza).

L'ordine è definito solamente da $n \leq S(n)$.

Le proprietà per $m, n, p \in \mathbb{N}$ sono:

1. **somma associativa:** $(m + n) + p = m + (n + p)$;
2. **somma distributiva:** $m + n = n + m$;
3. **somma nulla:** $m + 0 = m$;
4. **prodotto associativo:** $(mn)p = m(np)$;
5. **prodotto distributivo:** $mn = nm$;
6. **prodotto nullo:** $mS(0) = m$;
7. **distributiva:** $(m + n)p = mp + np$;
8. **cancellazione somma:** $m + n = m + p \implies n = p$;
9. **cancellazione prodotto:** $mn = mp \wedge m \neq 0 \implies n = p$;
10. **compatibilità tra somma e ordine:** $m \leq n \implies m + p \leq n + p$;
11. **compatibilità tra prodotto e ordine:** $m \leq n \implies mp \leq np$;

Detto 1 il numero $S(0)$ risulterà che $S(n) = n + 1$.

Assioma 3:

Proposition

Un altro modo per dire l'assioma 3 è che ogni sottoinsieme non vuoto di \mathbb{N} ammette un minimo.

Proof

Per dimostrarlo sia $A \subseteq B$ l'insieme di tutti i minoranti. L'insieme A contiene sicuramente 0. Infatti, $0 \leq n$ per ogni $n \in \mathbb{N}$. L'insieme A è diverso da \mathbb{N} . Infatti, preso un $n \in B$, sappiamo che $B \neq \emptyset$, abbiamo che $n + 1$ non è minore o uguale di n , quindi non è un minorante di B . Pertanto $n + 1 \notin A$. Sappiamo per gli assiomi di Peano che un sottoinsieme di \mathbb{N} che contiene 0 e contiene il successore di ogni elemento, coincide con \mathbb{N} . Poiché $0 \in A$ e $A \neq \mathbb{N}$, possiamo concludere che esiste $k \in A$ tale che $k + 1 \notin A$, cioè k è minorante di B ma $k + 1$ no. Ma allora esiste $i \in A$ tale che $k + 1 \not\leq i$. Poiché l'ordine è totale, ciò significa che $i < k + 1$. D'altra parte k è minorante di B . In particolare, $k \leq i$, che è minore di $k + 1$. Per la proprietà dell'ordine dei naturali, si ha che $k = 1$, cioè $k \in B$. Dunque, k è minorante di B che appartiene a B come volevamo (è il nostro minimo).

Non è necessario l'assioma della scelta per prendere $n \in B$ in quando B è ben definito e sappiamo come sceglierlo.

7 Numeri interi

Fatto l'anello commutativo degli interi si possono dimostrare delle proprietà come ad esempio $n \cdot 0 = 0$ per ogni n .

Per dimostrare invece il principio di annullamento del prodotto, cioè che $mn = 0$ se e solo se almeno uno tra m e n è 0. In alcuni anelli commutativi il principio di annullamento del prodotto non vale.

Si dimostra poi che dato $n \in \mathbb{Z}$, si ha che $n \in \mathbb{Z}$ oppure $0 - nn \in \mathbb{Z}$ per ogni n intero. Si pone allora

$$|n| = \begin{cases} n & \text{è un naturale} \\ -n & \text{altrimenti} \end{cases}$$

Una volta introdotto l'ordine negli interi (compatibile con quello dei naturali), si dimostrano queste proprietà:

1. $a \leq b \implies a + c \leq b + c$;
2. $a \leq b \wedge c \geq 0 \implies ac \leq bc$;
3. $|a + b| \leq |a| + |b|$;
4. $|a \cdot b| \leq |a| \cdot |b|$.

7.1 Divisione con resto

Estendiamo l'mcd a valori tutti nulli. Dati due interi il loro mcd è il numero naturali d che divide entrambi ed è multiplo di tutti i divisori comuni. Se almeno uno tra questi è nullo, questo coincide con la definizione precedente. Se tutti sono zero, definiamo l'mcd come zero, in quanto zero è un multiplo di zero.

7.2 Massimo comun divisore

Dimostrare l'esistenza di un massimo comune divisore su più interi per induzione: il caso base è quello in cui il numero di interi è 2. Usare l'esistenza del membro a destra e verificare che soddisfa la definizione.

8 Classi di resto

Consideriamo i non-multipli di 3. La differenza fra un non-multiplo di 3 e quello dopo è 0 1 o 2. Dividiamo allora i non-multipli di 3 saltando 2 a 2, ossia

$$-5, -2, +1, +4, +7, +10$$

e

$$-4, -1, +2, +5, +8, +11$$

La somma di due numeri corrispondenti è sempre un numero di 3. In generale, se considero le tre liste

$$\begin{aligned} -6, -3, +0, +3, +6, +9 &- 5, -2, +1, +4, +7, +10 \\ &-4, -1, +2, +5, +8, +11 \end{aligned}$$

Se facciamo la somma di due termini, la lista in cui è il risultato è dato solamente dalle liste dei due addenti.

9 Monoidi e gruppi

La moltiplicazione in matrici quadrate è associativa ma non commutativa.

La composizione X^X è associativa ma non commutativa. Studiamo la commutatività: diciamo che se $|X| = 1$, allora abbiamo solo l'identità $X^X = \{\text{Id}_X\}$, in questo caso è quindi commutativa. Supponiamo ora $|X| = 2$ e quindi $X = \{a, b\}$. Allora abbiamo le seguenti funzioni $X^X = \{\text{Id}_A, \text{Id}_B, \text{Inv}_A, \text{Inv}_B\}$, che sono 4 possibilità. Per vedere se è commutativa, dovrei considerare tutte le possibili coppie ordinate $(f, g) \in X^X \times X^X$ (sono 16) e vedere se $fg = gf$. Chiaramente, se facciamo la composizione della funzione che manda sempre in a con quella che manda sempre b , non commuta.

Se AB è l'identità delle matrici, allora lo è anche BA . Se ho un inverso a destra e uno a sinistra sono uguali.

Il *gruppo lineare generale* è dato da

$$GL_n(R) = (\text{Inv}(M_n(R)), \cdot)$$

Nella tabella di Caley: l'operazione è commutativa se la tabella è specchiata sulla diagonale. L'associatività non è facile da vedere. Vi è un elemento neutro se la riga e la colonna dell'elemento neutro ripetono le etichette. Un elemento è invertibile nella sua riga e colonna vi è un 1. Il fatto che l'equazione $ax = b$ abbia una sola soluzione si interpreta dicendo che sulla riga di a appaiono tutti gli elementi del gruppo una sola volta (analogamente per le colonne). Su ogni riga e colonna ogni elemento può comparire una volta sola.

Esiste un gruppo di ogni ordine n , per esempio $(\mathbb{Z}/n, +)$ ha ordine n .

10 Gruppi geometrici

Altro: un gruppo generato è abeliano se e solo se gli elementi del sottogruppo commutano fra di loro.

Esercizio

Dimostra

$$\langle g^h \rangle \cap \langle g^k \rangle = \langle g^m \rangle$$

con m minimo comune multiplo di h e k .

11 Altro

Prendiamo un punto P del piano e una trasformazione σ del nostro gruppo. Consideriamo allora $\sigma(P)$. Questo modo di associare una coppia $(P, \sigma) \in \pi \times G$ ha alcune regole. Per esempio $(P, \text{Id}) \rightarrow P$ per ogni P , $(P, \sigma) \rightarrow Q$ e $(Q, \tau) \rightarrow R$, allora $(P, \tau(\sigma)) \rightarrow R$.

12 Sottogruppi normali

Vogliamo contare il numero di coniugati di H in G . Dato H elemento di X , cioè sottogruppo in G , e $g \in G$, consideriamo l'azione di G per coniugio. Ossia, $(H, g) \rightarrow H^g$. Chiaramente questa è un'azione in quanto $H^1 = H$ e $(H^{g_1})^{g_2} = H^{g_1 g_2}$. La sua orbita è l'insieme dei coniugati di H . Lo stabilizzatore sono gli elementi di G tali che $H^g = H$.

Definizione Normalizzante

Il *normalizzante* in G di H è il sottoinsieme di G così definito

$$N_G(H) \triangleq \{g \in G \mid H^g = H\}$$

Alcune proprietà:

1. $N_G(H) \leq G$ (è un particolare stabilizzatore rispetto ad un'azione, quindi sottogruppo);
2. $H \leq N_G(H)$ infatti se $h \in H$, ovviamente $H^h = H$;
3. il numero dei coniugati di H è uguale all'indice dello stabilizzatore, cioè del normalizzante in G .

$$|G : N_G(H)|$$

Infatti la cardinalità di un'orbita è uguale all'indice nel gruppo dello stabilizzante di un elemento.

4. In particolare, se l'indice $|G : H|$ è finito, che avviene almeno sicuramente se G è finito, allora abbiamo che

$$|G : H| = |G : N_G(H)| \cdot |N_G(H) : H|$$

Ma allora ciò mi dice che il numero di coniugati è finito e divide l'indice $|G : H|$.

5. Se $H \leq K \leq G$, allora $H \trianglelefteq K$ se e solo se $K \leq N_G(H)$. In altri termini, i sottogruppi K in cui H è normale, sono tutti e soli quelli per cui

$$H \leq K \leq N_G(H)$$

6. In particolare $H \trianglelefteq N_G(H)$, cioè il normalizzante di H è il più grande sottogruppo di G in cui H è normale. Si ha $H \trianglelefteq G$ se e solo se $N_G(H) = G$.

Ricordiamo che dati due sottogruppi H e K di un gruppo G , si ha che $HK \leq G$ in particolare se e solo se $HK = KH$. Inoltre, $H \trianglelefteq G$ se e solo se $Hg = gH$ per ogni $g \in G$. Ora,

$$HK = \{hk \mid h \in H, k \in K\} = \bigcup_{k \in K} Hk$$

e

$$KH = \{kh \mid h \in H, k \in K\} = \bigcup_{k \in K} kH$$

Quindi, se $H \trianglelefteq G$, allora $Hg = gH$ per ogni $g \in G$. In particolare, ciò è vero per ogni $k \in K$, cioè $Hk = kH$ per ogni $k \in K$, e quindi

$$\bigcup_{k \in K} Kh = \bigcup_{k \in K} kH \iff HK = KH$$

Riassunto, se $H \trianglelefteq G$ e $K \leq G$, allora $HK = KH$, cioè $HK \leq G$. Se anche $K \trianglelefteq G$, possiamo dire che $HK \trianglelefteq G$.

Proposition

Se $H \trianglelefteq G$ e $K \trianglelefteq G$, allora $HK \trianglelefteq G$.

Proof

Sappiamo già che HK è un sottogruppo, siccome almeno uno dei due è normale, allora usiamo la proprietà che $x^g \in HK$ per ogni $x \in HK$. Ora, $x = hk$ per qualche $h \in H$ e $k \in K$. Ma allora $x^g = h^g k^g$. Poiché $H \trianglelefteq G$, si ha che $h^g \in H$ e analogamente $k^g \in K$. Allora, $x^g \in HK$ come volevamo.

Corollario

Se H_1, H_2, \dots, H_r sono sottogruppi normali di G , allora $H_1 H_2 \dots H_r \trianglelefteq G$.

Si dimostra per induzione su r .

12.1 classi di coniugio nel simmetrico

Lemma

Sia $\sigma = (a_1 a_2 \dots a_r)$ e τ una permutazione qualunque n lettere. Allora,

$$\sigma^\tau = (\tau(a_1) \tau(a_2) \dots \tau(a_r))$$

Proof

Dobbiamo mostrare che $\tau^{-1} \sigma \tau^{-1}$ è uguale all'espressione data, cioè che

$$\sigma \tau = \tau(a_1 \tau a_2 \tau \dots)$$

oppure

$$(a_1 a_2 \dots) \tau = \tau(a_1 \tau a_2 \tau \dots)$$

Questo è equivalente a dire che per ogni lettera i si ha che

$$i(a_1 \dots a_r) \tau = i \tau(a_1 \tau \dots)$$

Distinguiamo due casi:

1. i è una degli a_j . Senza perdita di generalità supponiamo $i = a_1$ (al massimo riordiniamo il ciclo). Allora abbiamo

$$a_1(a_1 \dots a_r) \tau = a_2 \tau$$

e

$$a_1 \tau(a_1 \tau \dots a_r \tau) = a_2 \tau$$

e quindi coincidono.

2. i non è nessuno degli a_j , allora

$$i(a_1 \cdots a_r)\tau = i\tau$$

e

$$i\tau(a_1\tau \cdots a_r\tau) = i\tau$$

perché $i\tau \neq a_j\tau$ per ogni j . Infatti, $i \neq j$ per ogni j , e τ è iniettiva. Dunque, il coniugato di un r -ciclo è un r -ciclo.

Tutti gli r -cicli sono coniugati tra di loro. Infatti, dati $a_1 \cdots a_r$ e $b_1 \cdots b_r$, basta prendere τ tale che $a_j\tau = b_j$ per ogni j da 1 a r e completare τ in modo che sia biettiva, cioè dando valori arbitrari a $i\tau$ per ogni i che non sia uno degli a_j .

Teorema

Due elementi di Sym_n sono coniugati se e solo se hanno lo stesso tipo.

Proof

Sia $\sigma = \gamma_1\gamma_2 \cdots \gamma_t$ con γ_i cicli disgiunti di lunghezze $r_1 \geq r_2 \cdots$ e sia $\tau \in \text{Sym}_n$. Allora,

$$\sigma^\tau = (\gamma_1 \gamma_2 \cdots \gamma_t)^\tau = \gamma_1^\tau \gamma_2^\tau \cdots \gamma_t^\tau$$

e dal lemma precedente segue immediatamente che γ_i^τ sono disgiunti e di lunghezze rispettivamente $r_i \geq r_2 \cdots$. Viceversa, se abbiamo 2 permutazioni dello stesso tipo, completando come per il lemma, si mostra che sono coniugati.

Esercizio

Trovare un $\tau \in \text{Sym}_8$ tale che

$$((1\ 2)(3\ 5\ 6\ 7))^\tau = (2\ 8)(1\ 4\ 3\ 5)$$

Basta prendere τ tale che $1\tau = 2$, $2\tau = 8$ etc. e completare, quindi per esempio $4\tau = 6$ e $8\tau = 7$. Quindi $\tau = (1\ 2\ 8\ 7\ 6\ 4\ 6\ 3)$

Esempio

Calcolo delle classi di coniugio di Sym_n con $n = 1 \cdots 5$ (e calcolo dei centralizzanti).

Abbiamo visto che le due permutazioni in Sym_n sono coniugate se e solo se hanno lo stesso tipo, dunque le classi di coniugio sono formate dagli elementi di tipo assegnato

Un sottogruppo normale è unione di classi di coniugio tra cui perlomeno la classe di identità. Tali unioni, se sottogruppi, sono normali.

Abbiamo sicuramente il sottogruppo normale identità e tutto il simmetrico Sym_4 . **Unione di due classi:** abbiamo possibilmente $1 + 6 = 7$ elementi. Notiamo che 7 non divide 24 e quindi non può essere un sottogruppo. Allo stesso modo $1 + 6$ di nuovo. Possiamo anche scartare $1 + 9$. Rimane $1 + 3 = 4$, che potrebbe essere sottogruppo.

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

Unione di tre classi: abbiamo $1 + 8 + 3 = 12$

$$\{\text{Id}\} \cup (1\ 2\ 3)^G \cup (1\ 2)(3\ 4)^G = A_4$$

che è normale in Sym_4 .

Unione di quattro classi: non ci sono divisori.

Abbiamo quindi trovato 3 sottogruppi normali e 1 candidato T . Controlliamo se T è sottogruppo. Dobbiamo verificare che $\sigma\tau$ con $\sigma\tau \in T$ rimangano in T . Se uno dei due è l'identità, ciò è banale. Quindi rimangono le altre 9 operazioni. Se $\sigma = \tau$, abbiamo sempre $\sigma\sigma = \text{Id}$. Allora rimangono 6 casi:

- $(1\ 2)(3\ 4) \circ (1\ 3)(2\ 4) = (1\ 4)(2\ 3) \in T$;
- gli altri sono analoghi;

Dunque T è un sottogruppo ed è quindi normale. Siccome T ha 4 elementi è isomorfo a C_3 oppure al gruppo di Klein. Tuttavia, T non è ciclico (non contiene elementi di periodo 4) quindi è il gruppo trirettangolo. Abbiamo quindi $\text{Id}, T, A_4, \text{Sym}_4$ come sottogruppi.

Problema: siano $H \trianglelefteq K$ e $K \trianglelefteq G$. È vero che $H \trianglelefteq G$? Per esempio $G = \text{Sym}_4$ e $K = T$ e $H = \langle (1\ 2)(3\ 4) \rangle$. Ora, $H \trianglelefteq K$ perché K è abeliano e $K \trianglelefteq G$, H non è normale in G perché non è unione di classi di coniugio come visto.

Guardiamo ora il caso $n = 5$.

Notiamo che il centralizzante $C_G((1\ 2\ 3\ 4)) \geq \langle (1\ 2\ 3\ 4) \rangle$. Inoltre sappiamo che entrambi hanno ordine 4. Quindi, il centralizzante è esattamente $C_G((1\ 2\ 3\ 4)) = \langle (1\ 2\ 3\ 4) \rangle$. Analogamente per $(1\ 2\ 3\ 4\ 5)$. Lo stesso vale per i cicli 3 per 2 che hanno ordine 6. Facendo i calcoli estensivi si trova che i sottogruppi normali sono

$$\text{Id}, A_5, \text{Sym}_5$$

Si potrebbe dimostrare che per ogni $n \geq 5$, i sottogruppi normali di Sym_n sono questi 3. Questo è legato al fatto che non esistono soluzioni di polinomi del grado quinto in poi.

Classi di coniugio nell'alterno. Sappiamo che $A_n \trianglelefteq \text{Sym}_n$. Gli elementi $(1\ 2\ 3)$ e $(1\ 3\ 2)$ sono coniugate nel simmetrico 3 lettere ma non nell'alterno a 3 lettere.

Lemma

Sia H un sottogruppo di un gruppo G di indice finito e sia K un sottogruppo di G qualsiasi. Allora $H \cap K$ ha indice finito in K e

$$|K : H \cap K| \leq |G : H|$$

Proof

Supponiamo che $|G : H| = n$. Devo mostrare che se prendo $n+1$ laterali (destri) di $H \cap K$ in K , questi non sono tutti diversi. Siano allora $H \cap Kk_1, H \cap Kk_2, \dots, H \cap Kk_{n+1}$ laterali di $H \cap K$ in K (cioè siano k_1, k_2, \dots, k_{n+1} di K). Consideri questi laterali (destri) di H in G

$$HK_1, HK_2 \dots HK_{n+1}$$

Poiché $|G : H| = n$, almeno due di questi coincidono. Ad esempio, $Hk_1 = Hk_2$, cioè $k_1 = hk_2$ per qualche $h \in H$. Ma allora $h = k_2k_1^{-1} \in K$, cioè $h \in H \cap K$. Ma allora $H \cap Kk_1 = H \cap Kk_2$.

Teorema

Sia G un gruppo finito e sia H un suo sottogruppo di indice 2 (dunque $H \trianglelefteq G$). Se $x \in H$, vale una e una sola delle seguenti:

1. $x^H = x^G$ e $|C_G(x)| = 2|C_H(x)|$;
2. $x^G = x^H \cup (x')^H$ con x', x non coniugati in H ,

$$|x^H| = |(x')^H| = \frac{1}{2}|x^G|$$

quindi la classe si separa in due con lo stesso numero di elementi, e $C_G(x) = C_H(x)$.

Proof

Applichiamo il lemma prendendo come $K = C_G(x)$. Abbiamo allora,

$$|C_G(x) : C_G(x) \cap H| \leq |G : H| = 2$$

Ora $C_G(x) \cap H = \{x \in H \mid xg = gx\} = C_H(x)$. Duque $|C_G(x) : C_H(x)| \leq 2$. Sappiamo poi che $|x^G||C_G(x)| = |G|$ e che $|x^H||C_H(x)| = |H|$. ma $|G| = 2|H|$, quindi otteniamo

$$|x^G||C_G(x)| = 2|x^H||C_H(x)|$$

Ma $|C_G(x) : C_H(x)| \leq 2$. Abbiamo 2 possibilità:

1. $|C_G(x)| = |C_H(x)|$ cioè $C_G(x) = C_H(x)$;
2. $|C_G(x)| = 2|C_H(x)|$

nel primo caso

$$|x^G||C_G(x)| = 2|x^H||C_H(x)|$$

diventa $|x^G| = 2|x^H|$, nel secondo caso $|x^G| = |x^H|$, cioè $x^G = x^H$.