Algebra I

Paolo Bettelini

Contents

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

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

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

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

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

e

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

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 ho 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 mulitpli 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 quando b è un maggiorante). Abbiamo quindi che $a = b$.

Definizione Massimale

Un elemento $a \in A$ con A insieme partzialmente 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 partzialmente 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 irriflessiva

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 irriflessiva.

4 Funzioni

Una funzione $\phi\colon A \to B$ 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 $\phi\colon \mathbb{R} \to \mathbb{R}$ 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 $D\phi^{-1} = \{y \in A \,|\, y\phi \in D\}$. Dunque $Cy\phi = \{y \in A \,|\, y\phi \in C\phi\}$. 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 $D\phi^{-1} = \{y \,|\, y\phi \in D\}$. 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 $\phi\colon A \to B$, $\psi\colon B \to C$ e $\theta\colon C \to D$ funzioni. allora

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

Proof

Notiamo che $\phi\psi\colon A \to C$ e $\theta\colon C \to D$. Dunque $\phi\psi\colon A \to D$. Analogamente $\phi\colon A \to B$, $\psi\theta\colon B \to D$ e quindi $\phi(\psi\theta)\colon A \to D$. Per mostrare l'uguaglianua 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 $\phi\colon A \to B$, $\psi\colon B \to C$ 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 $\phi\colon A \to A$ e $\psi\colon A \to A$. 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 $\mathrm{Id}_A\colon A \to A$ definita come $a\mathrm{Id}_A \triangleq a$.

Proposition

Sia $\phi\colon A \to B$, allora $\phi\mathrm{Id}_B = \phi$ e $\mathrm{Id}_A\phi = \phi$. 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 $f\colon A \to B$ data $f(a) = b$ e $g\colon B \to C$ 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 $f\colon A \to B$, allora f è invertibile se esiste $g\colon B \to A$ 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 $h\colon B \to A$ tale che $h(f(a)) = a$ e $f(h(b)) = b$. Allora $g = g\mathrm{Id}_A = g(fh) = (gf)h = \mathrm{Id}_B h = h$ e quindi è la funzione identità.

Proposition

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

Proposition

Se $f\colon A \to B$ e $g\colon B \to C$ 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

($\Longrightarrow$) 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.

($\Longleftarrow$) Sia f biettiva. Dobbiamo costruire $g\colon B \to A$ 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'emenento di posto (i,j).

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

Una matrice uguale alla sua trasporta è detta simmetrica.

Definizione

Dato un anello commutativo R diciamo $M_{m,n}(R)$ l'insieme delle matricii $m \times n$ 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

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

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

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

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

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

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

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

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 $B \in B_{n,p}(R)$ 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 $S\colon \mathbb{N} \to \mathbb{N}$ e di un elemento fissato 0 tali che:

- la funzione S è iniettiva;
- $0 \notin \mathrm{Im}_S$;
- 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 $f\colon \mathbb{N} \to \mathbb{N}'$ tale che $f(0) = 0'$ e $nfs' = nsf$

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

Questo può essere fatto con un procedimento cosidetto 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 $m + S(n) = S(m + n)$.

Usango gli assiomi posso dimsotrare 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:** $mn = mp \land m \neq 0 \implies n = p$;
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. $a \leq b \land c \geq 0 \implies ac \leq bc$;
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 o 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 risutato 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 $X^X = \{\mathrm{Id}_X\}$, in questo caso è quindi commutativa. Supponiamo ora $|X| = 2$ e quindi $X = \{a, b\}$. Allora abbiamo le seguenti funzioni $X^X = \{\mathrm{Id}_A, \mathrm{Id}_B, \mathrm{Inv}_A, \mathrm{Inv}_B\}$, che sono 4 possibilità. Per vedere se è commutatia, 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

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

Nella tabella di Caley: l'operazione è commutative 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 solzione si interpreta dicendo che sulla riga di a appaiono tutti gli elementi del gruppo una sola volta (analogamente per el 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 $(P, \mathrm{Id}) \to P$ per ogni P, $(P, \sigma) \to Q$ e $(Q, \tau) \to R$, allora $(P, \tau(\sigma)) \to R$.

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, $(H, g) \to H^g$. 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

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

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 $H^n = n$;
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

   $$H \leq K \leq K_G(H)$$

6. In particoalre $H \trianglelefteq N_G(H)$, 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,

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

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

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

Riassumento, 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 $h^g k^g \in K$. Allora, $x^g \in HK$ come volevamo.

Corollario

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

Si dimostra per induzione su r.

12.1 classi di coniugio nel simmetrico

Lemma

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

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

Proof

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

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

oppure

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

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

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

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
$$a_1(a_1\ \cdots\ a_r)\tau = a_2\tau$$
e
$$a_1\tau(a_1\tau\ \cdots\ a_r\tau) = a_2\tau$$
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 $\sigma = \gamma_1\gamma_2 \cdot \gamma_t$ con γ_i cicli disgiunti di lunghezze $r_1 \geq r_2 \cdots$ e sia $\tau \in \mathrm{Sym}_n$. 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 $\tau \in \mathrm{Sym}_8$ 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.
$$\{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$
Unione di tre classi: abbiamo $1 + 8 + 3 = 12$
$$\{\mathrm{Id}\} \cup (1\ 2\ 3)^G \cup (1\ 2)(3\ 4)^G = A_4$$
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 $\sigma\sigma = \mathrm{Id}$. Allora rimangono 6 casi:

- $(1\ 2)(3\ 4) \circ (1\ 3)(2\ 4) = (1\ 4)(2\ 4) \in T$;
- 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 $\mathrm{Id}, T, A_4, \mathrm{Sym}_4$ come sottogruppi.

Problema: siano $H \trianglelefteq K$ e $K \trianglelefteq G$. È vero che $H \trianglelefteq G$? Per esempio $G = \mathrm{Sym}_4$ 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

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

Si potrebbe dimostrare che che per ogni $n \geq 5$, i sottogruppi normali di Sym_n sono questi 3. Questo è legato al fatto che none sistano soluzioni di polinomi del grado quinto in poi.

Classi di coniugio nell'alterno. Sappiamo che $A_n \trianglelefteq \mathrm{Sym}_n$. 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 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 $H \cap Kk_1$, $H \cap Kk_2$, $\cdots$, $H \cap Kk_{n+1}$ laterali di $H \cap K$ in K (cioè siano $k_1, k_2, \cdots, k_{n+1}$ di K). Consideri questi laterali (destri) di H in G

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

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 $h = k_2 k_1^{-1} \in K$, 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 $C_G(x) \cap H = \{x \in H \,|\, xg = gx\} = C_H(x)$. 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 $x^G = x^H$.

Questo teorema, in particolare, vale per la classe di coniugio dell'alterno.

Sia $\varphi\colon G \to H$ un omomorfismo.

12.2 Omomorfismi di sottogruppi normali

Se $K \trianglelefteq G$, allora $K\varphi \trianglelefteq H$? Non sempre. Sappiamo che $K\varphi = \{k\varphi \,|\, k \in K\}$. Per mostrare che è un sottogruppo normale dobbiamo mostrare che $(k\varphi)^h = k\varphi$ per tutti $h \in H, k \in K$, cioè che

$$h^{-1}(K\varphi)h = k'\varphi$$

per qualche $k' \in K$. Se sapessimo che $h = g\varphi$ per qualche $g \in G$, allora avremmo

$$g\varphi^{-1}(k\varphi)(g\varphi) = (g^{-1}\varphi)(k\varphi)(g\varphi) = (g^{-1}kg)\varphi$$

che appartiene a $K\varphi$ perché $g^{-1}kg = k^g \in K$. Quindi, $K\varphi \trianglelefteq \mathrm{Im}\{\varphi\}$ necessariamente solamente per quella condizione. Prendiamo un esempio per mostrare che in generale la proposizione non è vera. Sia $\varphi\colon C_2 \to \mathrm{Sym}_3$ con $c_2 = \langle g \rangle$ tale che

$$\varphi(g) = (1\ 2)$$

Siccome lo scambio ha periodo 2 che divide il periodo di G (sono uguali), questo omomorfismo è ben definito. Ora $C_2 \trianglelefteq C_2$, ma l'immagine di $\varphi(C_2) = \langle (1\ 2) \rangle$ non è normale nel simmetrico su 3 lettere.

Se $L \trianglelefteq H$, allora $L\varphi^{-1} \trianglelefteq G$? Sì. Ricordiamo che

$$L\varphi^{-1} = \{x \in G \,|\, x\varphi \in L\}$$

Bisogna verificare se per ogni $x \in L\varphi^{-1}$ e ogni $g \in G$ risulta $x^g \in L\varphi^{-1}$ cioè $(x^g)\varphi \in L$.

$$(x^g)\varphi = (g^{-1}xg)\varphi = (g\varphi)^{-1}x\varphi(g\varphi) = (x\varphi)^{(g\varphi)} \in L^{g\varphi} = L$$

Proposition

Sia $\varphi\colon G \to H$ un omomorfismo di gruppi, allora:
1. se $K \trianglelefteq G$, allora $K\varphi \trianglelefteq \mathrm{Im}\varphi$;
2. se $L \trianglelefteq H$, allora $L\varphi^{-1} \trianglelefteq G$.

12.3 A cosa servono i sottogruppi normali

Proprietà che vengono preservate nelle congruenze in X (relazioni di equivalenza che sono compatibili rispetto ad un operazione). Quindi se $x \sim x'$ e $y \sim y'$, allora $x \circ y \sim x' \circ y'$.

1. se $\circ$ in X è associativa, allora l'operazione in $X/\sim$ è associativa.
$$([x]_\sim [y]_\sim)[z]_\sim = [x]_\sim([y]_\sim [z]_\sim)$$
2. se $\circ$ in X è commutativa, allora l'operazione in $X/\sim$ è commutativa;
3. se $\circ$ in X ha elemento neutro 1, allora $[1]_\sim$ è elemento neutro in $X/\sim$;
4. se x è invertibile in X, allora $[x]_\sim$ è invertibile in $X/\sim$.
5. se M è un monoide e $\sim$ è una congruenza in M, allora $M/\sim$ è un monoide. Se è commutativo allora $M/\sim$ è commutativo.
6. se G è un gruppo e $\sim$ è una congruenza in G, allora $G/\sim$ è un gruppo chaimato *gruppo quoziente*. Se è abeliano allora $G/\sim$ è abeliano.

Esempio

Consider $(\mathbb{N}, +)$ and let $n \in \mathbb{N}$ and defined $\sim$ such that $a \sim a'$ if $a = a'$ or $(a > n) \wedge (a' > n)$.
- è una relazione di equivalenza;
- è una congruenza.

Teorema

Sia G un gruppo e sia $\sim$ una congruenza. Risulta allora:
1. $[1]_\sim$ è un sottogruppo normale H di G;
2. le classi di equivalenza sono esattamente i laterali di H in G.
3. Viceversa, se $H \trianglelefteq G$ allora la relazione di equivalenza le cui classi sono i laterali di H in G è una congruenza; Dunque, dare una congruenza in G o un sottogruppo normale H è la stessa informazione.

Dato $H \trianglelefteq G$ scriviamo G/H per indicare il gruppo quoziente.

La medesima classificazione con i sottogruppi normali non funzione bene nei monoidi (come nell'esempio precedente).

Proof

($\Longrightarrow$) Data ua congruenza, allora la la classe dell'identità è un sottogruppo normale e le classi sono i laterali.
1. $[1]_\sim = H \neq \emptyset$ perché $1_G \in H$;
2. se $x \in H$ e $y \in H$, cioè $x \sim 1_G$ e $y \sim 1_G$, allora $xy \sim 1_G 1_G = 1_G$, cioè $xy \in H$;
3. se $x \in H$, cioè $x \sim 1$. Siccome $x^{-1} \sim x^{-1}$, abbiamo che $x^{-1}x \sim x^{-1}1_G$, cioè $x^{-1} \in H$.

Per mostrare che il sottogruppo è normale mosrtriamo che se $x \in H$ e $g \in G$, cioè $x \sim 1_G$, allora $x^g = g^{-1}xg \sim g^{-1}g = 1_G$. Quindi, $x^g \in H$ e allora è normale in G. Mostriamo ora che le classi di equivalenza sono i laterali di H in G. Dobbiamo mostrare una per ogni $g \in G$, risulta $[g]_\sim = Hg$.
1. $[g]_\sim \subseteq Hg$: sia $x \sim g$. Abbiamo $x = (xg^{-1})g$ ovviamente. Basta mostrare che $xg^{-1} \in H$. Ora $xg^{-1} \sim gg^{-1} = 1_G$ cioè $xg^{-1} \in H$;
2. $[g]_\sim \supseteq Hg$: sia $x \sim Hg$ cioè $x = hg$ con $h \in H$, vale a dire $h \sim 1_G$. Ma allora $x = hg \sim 1_G g = g$, cioè $x \in [g]_\sim$.

($\Longleftarrow$) sia $H \trianglelefteq G$ e sia $\sim$ la relazione di equivalenza le cui classi sono i laterali di H in G. Mostriamo che $\sim$ è una congruenza: se $x \sim x'$ e $y \sim y'$, allora $xy \sim x'y'$. Sappiamo che $x \in Hx'$ e $y \in Hy'$ e dobbiamo mostrare che $xy \in Hx'y'$. Allora $x = h_x x'$ con $h \in H$ e $y = h_y y'$. Allora, $xy = h_x x' h_y y'$. Concentriamoci sul termine $x'h_y$: $x'h_y \in xH = Hx'$, cioè $x'h' = \overline{h}x$. Dunque,

$$xy = h_x \overline{h} x' y' \in Hx'y'$$

Dunque se $H \trianglelefteq G$, l'operazione nel gruppo quoziente G/H è così definita

$$Hx \cdot Hy \triangleq Hxy$$

Se H non è normale, l'operazione non è ben-definita (se lo fosse avrei una congruenza la cui classe di $[1]_\sim$ dovrebbe essere un sottogruppo normale).

Proposition Alcune proprietà

1. se G è abeliano, allora G/H è abeliano;
2. se G è ciclico di generatore g, allora G/H è ciclico con generatore Hg (infatti, per ogni $x \in G$ si ha $x = g^n$ per $n \in \mathbb{N}$ e quindi $Hx = (Hg)^n$). Non vale necessariamente il viceversa.

Proposition

Sia G un gruppo e $H \trianglelefteq G$, la funzione $\varphi\colon G \to G/H$ che manda x in Hx, è un omomorfismo suriettivo di nucleo H. Tale omomorfismo è detto omomorfismo canonico.

Proof

Chiaramente φ è suriettivo (ogni laterale proviene dai suoi elementi). Se x, y sono elementi di G si ha che $(xy)\varphi = Hxy = Hx \cdot Hy = x\varphi \cdot y\varphi$. Abbiamo anche

$$\ker_\varphi = \{x \in G \,|\, x\varphi = 1_{G/H}\} = \{x \in G \,|\, Hx = H\} = H$$

Quindi, dato un sottogruppo normale c'è almeno un omomorfismo di cui lui è il nucleo: l'omomorfismo canonico sul quoziente.

I sottogruppi normali di G sono tutti e soli i nuclei di omomorfismi da G in qualche gruppo.

Proposition

Se G è un gruppo non-abeliano, allora $G/Z(G)$ non è ciclico.

Proof

Per assurdo sia $G/Z(G)$ ciclico, generato da un centro $Z(G)g$. Per ogni $x \in G$, si ha allora

$$Z(G)x = (Z(G)g)^n$$

per qualche $n \in \mathbb{N}$, cioè $x \in (Z(G)g)^n = Z(g)g^n$, cioè $x = zg^n$ per qualche $z \in Z(G)$ e $n \in \mathbb{N}$. Se ora y è un altro elemento di G, abbiamo che $y = z'g^m$ per qualche $z' \in Z(G)$ e $m \in \mathbb{N}$. Ora $xy = zg^n z'g^m = zz'g^{n+m}$ e $yx = z'g^m zg^n = zz'g^{n+m}$ quindi $xy = xy$. Quindi G è abeliano lightning.

Corollario

Dato un gruppo G, l'indice $|G : Z(G)|$ non è primo.

Proof

Se l'indice fosse primo, il quoziente $G/Z(G)$ avrebbe ordine primo e sarebbe dunque ciclico. Allora, G sarebbe abeliano e $|G : Z(G)|$ sarebbe 1.

Corollario

Sia G di ordine qudrato di un primo p. Allora, G è abeliano.

Proof

Sappiamo che $Z(G)$ ha ordine che divide $|G| = p^2$. Le possibilità sarebbero $|Z(G)| = 1, p, p^2$. Tuttavia, abbiamo dimostrato che in un p-gruppo non banale il centro non è banale. Dunque, non è 1. Se fosse $|Z(G)| = p$, avremmo allora

$$|G : Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$$

contro il corollario precedente. Allora, $|Z(G)| = p^2$ cioè $G = Z(G)$ cioè G è abeliano.

12.4 Classificazione dei gruppi di ordine primo quadro

Abbiamo già visto che sono tutti abeliani. Gli elementi di un tale gruppo possono avere periodo $1, p, p^2$. (Solo uno ha periodo 1)-

Se $|G| = p^2$ ed esiste almeno un elemento di periodo p^2, allora G è ciclico di ordine p^2. Se $|G| = p^2$ e non esistono elementi di periodo p^2, allora tutti gli elementi non banali di G hanno periodo p. Sia x un tale elemento e sia $H = \langle x \rangle$. Allora, H è ciclico di ordine p ed è normale in G, in quanto G è abeliano. Sia ora $y \in G \backslash H$. Anche $K = \langle y \rangle$ è ciclico di ordine p ed è normale in G. Ora $|H \cap K|$ è un divisore di $|H|$ e $|K|$ cioè di p. Tuttavia, non può essere p in quanto altrimenti sarebbero uguali, e quindi $H \cap K = 1$. Ora,

$$|HK| = \frac{|K||H|}{|H \cap K|} = \frac{p^2}{1} = p^2$$

Quindi, $HK = G$. Riassumento G è prodotto di due ciclici normali di periodo p con intersezione banale, cioè G è il prodotto diretto di due ciclici di ordine p.

12.5 Prodotto semidiretto

Esempio

Consideriamo Sym_n con $n \geq 2$ e sia $H = \langle (1\ 2) \rangle$ e $N = A_n$. Ora $A_n \trianglelefteq \mathrm{Sym}_n$, $H \cap N = \mathrm{Id}$: infatti $H = \{\mathrm{Id}\}$ e $(1\ 2) \notin A_n$. Inoltre

$$|HA_n| = \frac{|H||A_n|}{|H \cap A_n|} = \frac{2 \cdot \frac{n!}{2}}{1}$$

cioè $HA_n = \mathrm{Sym}_n$.
Notiamo che se $n \geq 3$, allora H non è normale nel simmetrico, perché i coniugati dello scambio di $(1\ 2)$ sono tutti e soli gli scambi $(i\ j)$ e questi non stanno tutti in H. Vogliamo costruire un gruppo non abeliano da due gruppo abeliani (addirittura anche ciclici).

Qual'è la differenza fra prodotto diretto e semidiretto? Se $G = H \times N$ allora il prodotto di due elementi di G è semplice. Se $g_1 = h_1 n_1$ e $g_2 = h_2 n_2$, allora $g_1 g_2 = h_1 h_2 n_1 n_2$. Se $G = H \ltimes N$, allora ho comunque una decomposizione unica per ogni elemento di G, cioè per ogni $g \in G$ esistono e sono unici $h \in H$ e $n \in N$ tale che $g = hn$ (qui non serve la normalità ma solo intersezione banale e prodotto uguale al gruppo). Se però $g_1 = h_1 n_1$ e $g_2 = h_2 n_2$ non posso più garantire che $g_1 g_2 = h_1 h_2 n_1 n_2$. Questo fatto

è ciò che mi dà più libertà nella costruzione. La conoscenza dei prodotto in H e N non è sufficiente a descrivere il prodotto in G.

Esempio

Abbiamo visto che

$$\mathrm{Sym}_3 = \langle (1\ 2) \rangle \ltimes A_3 \cong C_2 \ltimes C_3$$

Ma $C_6 = C_2 \times C_3$ che è un caso particolare di $C_2 \ltimes C_3$. Quindi a partire dagli stessi strumenti possiamo arrivare a due cose differenti.

Nel caso generale, so che $g_2 g_2 = hn$ per $h \in H$ e $n \in N$. Come calcolo h e n? Non è detto che $h = h_1 h_2$ e $n = n_1 n_2$ (ciò vale per tutti se il prodotto è diretto). Abbiamo

$$g_1 g_2 = h_1 n_1 h_2 n_2 = hn$$

Questo prodotto è unico anche se uno dei due sottogruppi non è normale, ma in questo caso uno dei due lo è e possiamo usare questa informazione. Scriviamo infatti

$$h_1 n_1 h_2 n_2 = h_1 h_2 h_2^{-1} n_1 h_2 n_2 = h_1 h_2 n_1^{h_2} n_2$$

abbiamo allora un prodotto di un elemento in H e uno in N. Quindi $h = h_1 h_2$ e $n = n_1^{h_2} n_2$. Pertando, conosco comde moltiplicare in G se so come moltiplicare in H e N e so come coniugare elementi di N tramite elementi di H. Nel caso particolare del prodotto diretto, questo coniugio è banale. Quindi, cosa vuol dire dare questa il coniugio di elementi di N traimite elementi di H?

Ricordiamo che in un gruppo G il coniugio tramite un elemento $g \in G$ definisce un automorfismo di G e chese $N \trianglelefteq G$, il coniugio tramite g definisce un'automorfismo di N. Ho cioè una funzione che manda elementi di g in automorfismi di N. Precisamente,

$$g \to (n \to n^g)$$

Inoltre, se $h \in G$ è un altro elemento, abbiamo $h \to (n \to n^h)$. Abbiamo allora

$$gh \to (n \to n^{gh})$$

Se indichiamo con φ_g l'automorfismo di N che manca n in n^g

$$n \xrightarrow{\varphi g} n^g \xrightarrow{\varphi h} (n^g)^h \qquad n \xrightarrow{\varphi_{gh}} (n^g)^h$$

ma questo è equivalente a

$$h^{-1} n^g h = h^{-1} g^{-1} n g h = n^{gh}$$

Dunque $\varphi_g \varphi_n = \varphi_{gh}$: abbiamo cioè un omomorfismo di gruppi da G in $\mathrm{Aut}(N)$. Nel caso $G = H \ltimes N$ per dire come gli elementi di N sono coniugati da elementi di H mi basta conoscere la restrizione di questo omomorfismo ad H. Cioè, abbiamo un omomorfismo di gruppi da H in $\mathrm{Aut}(N)$. Se chiamiamo φ tale isomorfismo, abbiamo

$$h_1 n_1 h_2 n_2 = h_1 h_2 n_1^{h_2} n_2 = h_1 h_2 n_1 (h_2 \varphi) n_2$$

Il termine $h_2 \varphi$ è un automorfismo.

Notiamo che nel caso di prodotto diretto $h_2 \varphi = \mathrm{Id}_n$ per ogni $h_2 \in H$. Vediamo come fare il viceversa

Definizione Prodotto semidiretto esterno

Siano H e N due gruppi e sia $\varphi \colon H \to \mathrm{Aut}(N)$ un omomorfismo di gruppi. Nel prodotto cartesiano $H \times N$ definiamo l'operazione nel modo seguente:

$$(h_1, n_1)(h_2, n_2) \triangleq (h_1 h_2, n_1 (h_2 \varphi) n_2)$$

Il prodotto semidiretto esterno è denotato

$$H \ltimes_\varphi N$$

Dagli stessi gruppi di partenza potrei avere φ diverse e ottenere prodotti diversi, anche non isomorfi fra di loro.

Teorema Il prodotto semidiretto esterno è un gruppo

Il prodotto semidiretto esterno è un gruppo $H \ltimes_\varphi N$ è un gruppo G. Inoltre, G contiene un sottogruppo $H' \cong H$ e un sottogruppo normale $N' \cong N$ tale che $G = H' \ltimes N'$ (prodotto semidiretto interno)

Proof Il prodotto semidiretto esterno è un gruppo

Per semplicità scriviamo φ_h per indicare l'automorfismo di N immagine di h tramite φ. Quindi

$$\varphi_{h_1}\varphi_{h_2} = (h_1\varphi)(h_2\varphi) = (h_1h_2)\varphi_{h_1h_2}$$

allora

$$(h_1, n_1)(h_2, n_1) = (h_1h_2, n_1\varphi_{n_2}n_2)$$

Verifichiamo le proprietà

1. *associativà:* prendere dal libro;
2. *associativà:* prendere dal libro

13 Teorema di Sylow

Se $|G| = n$ e d divide n, esiste un sottogruppo di ordine d? Nei gruppi ciclici sì: per ogni d che divide $|G|$ esiste un unico sottogruppo di ordine d. In generale no, il più piccolo esempio è A_4 dove non esistono sottogruppi di ordine 6. Infatti, se esistesse $H \leq A_4$ con $|H| = 6$, avremmo $|A_4 : H| = 2$ e H dovrebbe essere normale, ed essere unione di classi di coniugio di A_4. Ma in A_4 c'è una classe di ordine 1, 2 classi di ordine 4, e una classe di ordine 3. Non è possibile far uscire 6, non ci sono nemmeno candidati.

Teorema

Sia G un gruppo abeliano finito di ordine n e sia d un divisore di n. Allora, in G esiste un sottogruppo di ordine d (non necessariamente unico).

Infatti, se per ogni divisore ce n'è esattamente uno, allora il gruppo è ciclico. Esercizio.

Proof

Consideriamo prima il caso in cui d è primo p, e procediamo per induzione su $\frac{n}{p}$:

- la base è $\frac{n}{p} = 1$ cioè $n = p$, G stesso ha ordine p.
- sia ora $\frac{n}{p} > 1$ cioè $n > p$. Prendiamo un elemento non banale $y \in G$ e consideriamone il periodo $|y| = m$. Distinguiamo due casi: se p divide m, abbiamo finito perché l'elemento $y^{\frac{m}{p}}$ ha periodo p e quindi genera un sottogruppo di ordine p. Se p non divide m, considero il quoziente

$$\frac{G}{\langle y \rangle}$$

(qui usiamo il fatto che G è abeliano e quindi il sottogruppo è normale). Ora, questo quoziente ha ordine $\frac{n}{m} < n$ in quanto $m > 1$. Tuttavia, tale ordine è multiplo di p. Per ipotesi induttiva, tale quoziente contiene un elemento $x\langle y \rangle$ di periodo p. Ora consideriamo $x^m = z$. Poiché p non divide m,

$$z\langle y \rangle = x^m \langle y \rangle = (x\langle y \rangle)^m \neq 1_{G/\langle y \rangle}$$

(se dividesse m farebbe 1). In particolare, $z \neq 1$. Ora $z^p = (x^m)^p = (x^p)^m$. Ma $|x\langle y \rangle| = p$ segue che $x^p \in \langle y \rangle$. Poiché $|\langle y \rangle| = m$, segue che tutti i suoi elementi elevati alla m danno 1, quindi $z^p = 1$. Ma siccome $z \neq 1$, allora $|z| = p$.

Consideriamo ora il caso generale e procediamo per induzione completa su d. Il caso in cui $d = 1$ è banale. Se $d > 1$, sia p un divisore di d, e sia H un sottogruppo di G di ordine p. Consderiamo il quoziente G/H che posso fare in quanto è abeliano. Allora l'ordine di tale quoziente è n/p e d/p divide n/p. Per ipotesi induttiva, G/H contiene un sottogruppo K/H (per il teorema di isomorfismo) di ordine d/p. Ma allora, K è un sottogruppo di G di ordine d (teorema di isomorfismo).

Teorema

Sia G un p-gruppo di ordine p^n. Per ogni $0 \leq k \leq n$, esiste un sottogruppo normale in G di ordine p^k.

Proof

Procediamo per induzione su k

1. il caso banale è $k = 0$ e $|1| = 1 = p^0$ e $1 \trianglelefteq G$;
2. se $k > 0$, allora anche $n > 0$. Sappiamo che $Z(G) \neq 1$. Se $|Z(G)| = p^t$ con $t \geq k$, poiché $Z(G)$ è abeliano, sappiamo che $Z(G)$ contiene un sottogruppo di ordine p^k. Ma i sottogruppi del centro sono normali in G, quindi abbiamo un sottogruppo normale in G di oridne p^k. Se

invece $|Z(G)| = p^t$ con $t < k$, considero il quoziente

$$\frac{G}{Z(G)}$$

che ha ordine p^{n-t}. Questo contiene un sottogruppo normale

$$\frac{N}{Z(G)}$$

di ordine p^{k-t} e $0 < k - t \leq n - t$, dove uso l'ipotesi induttiva. Per uno dei teoremi di isomorfismo, il terzo, $N \trianglelefteq G$ e

$$|N| = \left|\frac{N}{Z(G)}\right| \cdot |Z(G)| = p^{k-t} \cdot p^t = p^k$$

14 Esercizi

Esercizio

Sia $G = C_{p^3} \times C_{p^2}$ con p primo.

1. quanti sottogruppi di ordine p ha G?
2. quanti sottogruppi ciclici di ordine p^2 ha G?
3. quanti sottogruppi non ciclici di ordine p^2 ha G?

Proof

1. ciascun gruppo di ordine p ciclico contiene $p-1$ elementi di periodo p e ognuno di questi elementi appartiene ad un unico sottogruppo di ordine p. Per contare i sottogruppi di ordine p posso allorare contare gli elementi di periodo p e dividere per $p-1$. Un elemento (x, y) nel prodotto diretto esterno ha periodo pari al minimo comune multiplo dei due periodi. Quindi, per far sì che il periodo sia p, o entrambi sono p o uno è 1 e l'altro è p. In C_{p^3} c'è un unico sottogruppo di ordine p che è formato da tutti gli elementi di periodo che divide p. Dunque, abbiamo p possibilità per x in modo tale che $|x|$ divide p. Lo stesso vale per C_{p^2}. Ma allora, ci sono $p \cdot p$ coppie $(x, y) \in G$ tale che $|x|$ e $|y|$ dividano p. Siccome almeno uno deve avere periodo p, bisogna togliere il caso $|x| = 1$ e $|y| = 1$, cioè $(1, 1)$, quindi il risultato è $p^2 - 1$ elementi di periodo p, e quindi vi sono
$$\frac{p^2-1}{p-1} = p+1$$
sottogruppi di oridne p.
2. ci sono $\varphi(p^2) = p^2 - p$ elementi di periodo p^2, ciascuno in un unico elemento di ordine p^2. Quindi sia $|x|$ e $|y|$ devono dividere p^2 e almeno uno di essi è esattamente p^2. Nel C_{p^3} c'è un unico sottogruppo di ordine p^2 che contiene tutti gli elementi di periodo che divide p^2. Analogamente nell'altro. Quindi ho $p^2 \cdot p^2$ elementi (x, y) con $|x|$ e $|y|$ che divide p^2. Di questi ne togliamo p^2, cioè quelli per cui $|x|$ e $|x|$ dividono$p$. Otteniamo
$$\frac{p^4-p^2}{p^2-p} = p^2+p$$
gruppi ciclici di ordine p^2.
3. Un gruppo di ordine p^2 non ciclico contiene $p^2 - 1$ elementi di periodo p e un elemento di periodo 1. Poiché ho esattamente $p^2 - 1$ elementi di periodo p in G, ho un'unica possibilità, cioè ho al massimo un sottogruppo non ciclico di ordine p^2. Ma un sottogruppo siffatto esiste. Prendo l'unico sottogruppo H di C_{p^3} di ordine p e l'unico sottogruppo K di C_{p^2} di oridne p. Ora $H \cap K = 1$. Quindi,
$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = p^2$$
e HK è un sottogruppo di ordine p^2 non ciclico (perché contiene gli elementi (x, y) con $x \in H$ e $y \in K$, cioè $|x|$ e $|y|$ dividono p).

Esercizio

Sia $G = \langle a \rangle$ con $|G| = 120$. Siano $H = \langle a^{33} \rangle$ e $K = \langle a^{28} \rangle$ sottogruppi.

1. trova $|H|$
2. trova $|H \cap K|$
3. esiste $L \leq G$ tale che $G = H \times L$?
4. esiste $M \leq G$ tale che $G = K \times M$?

Proof

1. L'ordinato è dato da
$$|H| = |a^{33}| = \frac{120}{\gcd(120, 33)} = 40$$
e
$$|K| = |a^{28}| = \frac{120}{\gcd(120, 28)} = 30$$
2. L'ordine deve dividere sia 40 che 30 quindi 10. Vi è solamente un sottogruppo in G di ordine 10 e H e K contengono ciascuno un sottogruppo di oridne 10 (tutti e 3 sono il medesimo).
3. Se esistesse L come cercato, dovrei avere $|G| = 120 = |H| \cdot |L|$, quindi $|L| = 3$. In G vi è un unico sottogruppo di ordine 3, ossia $L = \langle a^{\frac{120}{3}} \rangle$. Vediamo se $G = H \times L$: la normalità è soddisfatta in quanto siamo in un gruppo ciclico quindi abeliano. L'intersezione è banale in quanto $H \cap L$ ha ordine che divide $|H| = 40$ e $|L| = 3$. Dunque, è 1. Per vedere se il prodotto funziona, calcoliamo l'oridne del prodotto
$$|HL| = \frac{|H| \cdot |L|}{|H \cap L|} = \frac{40 \cdot 3}{1} = 120$$
Dunque $G = H \times L$.
4. M dovrebbe avere ordine 4. L'unico candidato è $M = \langle a^{30} \rangle$. L'intersezione non è banale in quanto 30 e 4 non sono coprimi, quindi non vi è soluzione.