Algebra Gruppi (Unimib)

1 luglio 2022

wikitolearn
collaborative textbooks

This book is the result of a collaborative effort of a community of people like you, who believe that knowledge only grows if shared.
We are waiting for you!

Get in touch with the rest of the team by visiting http://join.wikitolearn.org

Capitolo 1

Gruppi

1.1 Semigruppi e Monoidi

1.1.1 Definizione ed esempi

Definizione (67 Semigruppo)

In generale, preso un insieme non vuoto X con un'operazione binaria $*$ associativa, esso si dice *semigruppo*.

Definizione (68 Monoide)

Se inoltre X ammette un'unità, allora la struttura $(X, *)$ viene detta *monoide*. Se si tratta di un'operazione additiva, l'unità si chiama 0 del monoide. Se l'operazione $*$ è un prodotto, l'unità si chiama 1 o unità del monoide.

Esempio (69)

Rispetto alla somma, l'insieme dei naturali escluso 0 forma un semigruppo, ma non un monoide perché non c'è l'unità.

Esempio (70)

Invece $(\mathbb{Z}_0, +)$ è un monoide rispetto alla somma.

Esempio (71)

$\mathbb{N}$ rispetto all'operazione di prodotto è un monoide.

Esempio (72)

Preso $P(U)$ e l'operazione intersezione o unione, queste operazioni sono associative quindi si ha a che fare con semigruppi. Si tratta anche di monoidi, perché U è l'unità rispetto all'intersezione e $\emptyset$ è l'unità rispetto all'unione.

Esempio (73)

Preso X^2 l'insieme di tutte le relazioni binarie, e la composizione come operazione $*$, è un semigruppo. L'identità funziona da elemento neutro, quindi ho un monoide.

1.1.2 Definizione di potenza

Supponiamo di avere un monoide e di chiamare $*$ l'operazione prodotto. L'unità si chiama 1_M . Se vale la proprietà associativa si può dare la definizione di potenza.

Definizione (74)

Sia a un elemento del monoide. Definiamo la *potenza n-esima* dell'elemento a di M per ogni $n \in \mathbb{N}_0$ ponendo: $a^0 = u$ per definizione, e $\forall n > 0$, usando il principio di induzione si definisce ricorsivamente $a^n = a^{n-1} * a$.

Proposizione (75)

In ogni monoide valgono le usuali proprietà delle potenze:

1. $$\forall m, n \in \mathbb{Z}_0 \, \forall a \in M, \text{allora} a^m * a^n = a^{m+n}$$
2. $$(a^m)^n = a^{m*n}$$

Fissato $m > 0$ arbitrario, le proprietà sono facilmente dimostrabili per induzione su n .

In un monoide, non si chiede a priori che il prodotto sia commutativo.

Ad esempio, preso l'insieme delle matrici quadrate con l'operazione di prodotto, sono un monoide. Il prodotto è associativo ma non commutativo.

Se $AB = BA$, allora si può avere $(AB)^n = A^n * b^n$, altrimenti questa proprietà non è soddisfatta.

1.2 Gruppi

1.2.1 Definizione

Definizione (76 Gruppo)

Sia G un insieme non vuoto e $*$ un'operazione. La coppia $(G, *)$ si dice *gruppo* se è un monoide, con unità u in cui per ogni $g \in G$ esiste $\bar{g} \in G$ tale che $g*\bar{g} = \bar{g}*g = u$.

Definizione (77 Gruppo abeliano)

Non si richiede che $*$ sia commutativa, ma se lo è, allora il gruppo si chiama *abeliano* (in onore di Abel, 1802-1829).

Definizione (78)

Notazione moltiplicativa: L'operazione $*$ viene chiamata *prodotto*, indicato con $\cdot$. L'unità si indica con 1_G . Per ogni $g \in G$, l'inverso $\bar{g}$ si indica con g^{-1} .

Definizione (79)

Notazione additiva: L'operazione $*$ si chiama somma, l'unità è 0_G . In questo caso l'inverso additivo di un elemento si indica con $-g$ e si chiama *opposto*.

Esercizio (80)

Gli assiomi di gruppo sono sovrabbondanti. Per definire un gruppo sarebbe sufficiente definire un semigruppo e richiedere che ogni elemento abbia un inverso sinistro.

1.2.2 Prime proprietà formali di calcolo

Sono le prime proprietà che derivano dagli assiomi di gruppo espressi nella definizione. Con la notazione moltiplicativa:

Proposizione (81 Prodotto di inverse)

$(AB)^{-1} = B^{-1} * A^{-1}$, questo è vero perché $(AB)^{-1} * B^{-1}A^{-1} = u$

Proposizione (82 Leggi di cancellazione)

Per tre elementi a, b, c comunque scelti, si ha che se vale l'uguaglianza $ab = ac$, questa implica necessariamente $b = c$ e si ha anche $ac = ab$ implica $c = b$ (il gruppo a priori non è commutativo).

Dimostrazione

Moltiplicando ambo i membri per l'inversa di a ottengo $a^{-1} * ab = a^{-1} * ac \longrightarrow uc = ub \longrightarrow c = b$. Queste leggi non valgono in generale in un monoide, perché lì non è richiesto che ogni elemento sia invertibile.

1.2.3 Definizione di potenza

In un gruppo si può definire per ogni elemento a la nozione di potenza con esponente relativo, mentre in un monoide si definisce solo la potenza con esponente positivo.

Definizione (83)

Se $a \in G$, allora a^0 è l'unità di G , per $n > 0$, $a^n = a^{n-1} * a$, e se $n < 0$, $(a^n)^{-1} = a^{-n}$

In notazione additiva, la nozione di potenza equivale alla nozione di multiplo.

Definizione (84)

Si definisce la nozione di *multiplo* secondo un intero relativo. Il multiplo secondo $n = 0$ di a è 0_G . Se $n > 0$ il multiplo è $a * (n-1) + a$ Se $n < 0$, $a * n = -a * (-n)$.

Proposizione (85)

Valgono le proprietà delle potenze: Con m, n sono numeri relativi e vale che

1. $\forall a \in G, a^n * a^m = a^{n+m}$
2. $(a^m)^n = a^{mn}$

Se m e n sono positivi il risultato si ricava dai monoidi.

Anche nei gruppi $a^n * b^n \neq (ab)^n$ e sono uguali solo se $*$ è commutativa.

1.3 Sottogruppo

1.3.1 Definizione

Proposizione (86)

Supponiamo di avere un gruppo $(G, \cdot)$. Se $H \subset G$ si dice che H è un *sottogruppo* del gruppo G se sono soddisfatte le tre condizioni seguenti:

1. $1_G \in H$
2. H è chiuso rispetto al prodotto definito su G (cioè il prodotto tra due elementi di H è ancora un elemento di H);
3. G è chiuso rispetto agli inversi, cioè per ogni $h \in H$, l'elemento h^{-1} , che esiste in G , è anch'esso un elemento di H .

Osservazione (87)

Un sottogruppo H è a sua volta un gruppo rispetto alla restrizione ad H del prodotto definito su G .

Inversamente ogni sottoinsieme di G che sia chiuso rispetto al prodotto soddisfa le tre condizioni della definizione di gruppo.

Osservazione (88)

Un gruppo ammette sempre dei sottogruppi, almeno i sottoinsiemi banali, infatti il sottoinsieme formato dalla sola unità e il gruppo G soddisfano la definizione di sottogruppo di G .

Inoltre, un gruppo ammette solo sottogruppi banali se e solo se il numero di elementi è un numero primo ed è finito.

Definizione (89)

L'ordine di un gruppo è la cardinalità dell'insieme G .

1.3.2 Criterio utile

Lemma (90)

Per verificare se un sottoinsieme non vuoto di G è un sottogruppo, è utile il seguente criterio: Sia H non vuoto un sottoinsieme di un gruppo G . H è un sottogruppo se e solo se per ogni $a, b \in H$, $a\dot{b}^{-1} \in H$.

Usando la notazione additiva, questa condizione diventa $a+(-b) \in H = a-b \in H$, cioè il sottogruppo è chiuso rispetto alla differenza.

Dimostrazione

Vale la doppia implicazione: Se H è un sottogruppo, per ogni elemento $b \in H$, $b^{-1} \in H$, ma per la proprietà 2 segue che comunque scelga un elemento $a \in H$ e $b \in H$, il loro prodotto sta ancora in H e quindi la condizione è soddisfatta.

Viceversa, supponiamo che H sia un sottoinsieme non vuoto di G , chiuso rispetto alla differenza. Devo mostrare che sono soddisfatte le condizioni della definizione di sottogruppo.

1. Supponiamo che per ogni $a, b \in H$, $a * b^{-1} \in H$. Per $a = b$ segue che $a * a^{-1} = u \in H$. (condizione 1)
2. Per $a = 1_G$, per ogni $b \in H$ questa condizione dice che $1_G * b^{-1} = b^{-1} \in H$, (condizione 3);
3. per ogni $a, b \in H$, poiché $b^{-1} \in H$, se $b = b^{-1}$, l'inverso dell'inverso appartiene ad H , quindi $a * (b^{-1})^{-1} = a * b \in H$ (condizione 2).

Esercizio (91)

Se considero un sottoinsieme H finito di un gruppo G e suppongo che H sia chiuso rispetto al prodotto, allora H è un sottogruppo di G .

Dimostrazione (Svolgimento dell'esercizio precedente)

Siccome H è non vuoto, sia a un elemento di H . Siccome per ipotesi il gruppo è chiuso rispetto al prodotto, tutte le potenze sono ancora elementi di H . Al variare dell'esponente m , la potenza è la funzione che a ogni elemento a associa a^m . Se questa applicazione fosse iniettiva, avrei infiniti elementi distinti che stanno in H . Poiché H è supposto finito, esistono $r < s$ interi positivi tali che $a^s = a^r$ (cioè esistono esponenti distinti per cui gli elementi rappresentabili con le potenze coincidono). Quindi, moltiplicando per a^{-r} ottengo $a^r * a^{-r} = a^s * a^{-r}$ e per le proprietà delle potense $a^{s-r} = u_G$. Ho due possibilità: $s - r = 1$, questo corrisponde al fatto che $s = r+1$, allora l'uguaglianza $a^1 = u_g$ dice che a è l'unità

di G , quindi H contiene l'unità. Sia $t = s - r > 1$, ovvero $a^t = 1_G$. Se $a^t = 1_G$, con $t > 1$, posso riscriverlo come $a * a^{t-1} = U_G$. Quindi $a^{-1} = a^{t-1} \in H$, quindi preso un elemento di H il suo inverso essendo una potenza di a sta ancora in H . Da cui infine, se a^{-1} sta in H allora il sottogruppo contiene l'unità.

1.4 Esempi di gruppi e sottogruppi

1.4.1 Gruppi numerici

Esempio (92)

$\mathbb{Z}$ è l'insieme dei numeri interi relativi. La coppia $(\mathbb{Z}, +)$ dove $+$ rappresenta la somma di interi, è un gruppo (abeliano) ed è chiamato *Gruppo additivo degli interi relativi.*

Esempio (93)

$(\mathbb{Q}, +)$ rispetto alla somma di numeri razionali è un gruppo, costruito a partire da quello degli interi. $\mathbb{Z}$ è un sottogruppo di $\mathbb{Q}$.

Esempio (94)

Il gruppo additivo dei razionali si può considerare come sottogruppo del gruppo additivo dei reali, contenuto a sua volta nel gruppo additivo dei numeri complessi.

Esempio (95)

Presa l'operazione di prodotto, $\mathbb{Z}$ non forma un gruppo, perché gli unici interi relativi che ammettono inverso nei numeri relativi sono 1 e -1 .

Esempio (96)

Tuttavia, i razionali rispetto al prodotto non formano un gruppo, perché 0 non ha l'inverso. Se chiamo $\mathbb{Q}_* = \mathbb{Q} \setminus (0)$, rispetto al prodotto questo costituisce il gruppo moltiplicativo dei razionali non nulli, sottoinsieme del sottogruppo moltiplicativo dei reali non nulli, sottogruppo del gruppo moltiplicativo dei complessi non nulli.

Tutti questi sono gruppi abeliani infiniti.

1.4.2 Gruppi non abeliani

Un gruppo di simmetria in genere non è commutativo. A parte i casi numerici classici, gli altri gruppi sono tipicamente non commutativi.

Definizione (97 Campo)

Sia F un campo. In breve un campo è un insieme con almeno due oggetti, che è un gruppo abeliano rispetto alla somma. Gli elementi diversi dallo 0 formano un gruppo rispetto al prodotto, di cui 1 è l'elemento neutro, e il prodotto è anch'esso commutativo.

Esempio (98)

Chiamiamo $Mat_n(F)$ l'insieme di tutte le matrici quadrate di ordine n a elementi in F . Possiamo definire tre operazioni: la somma di matrici, il prodotto righe per colonne e il prodotto di una matrice per uno scalare. Una matrice $A \in Mat_n(F)$ è invertibile rispetto al prodotto se e solo se $\det A \neq 0$. Denotiamo con $GL(n, F)$ il sottoinsieme di $Mat(n, F)$ costituito da tutte e sole le matrici invertibili rispetto al prodotto righe per colonne. Allora $GL(n, F)$ è chiuso rispetto al prodotto di matrici (il prodotto di matrici con determinante diverso da 0 è ancora una matrice con determinante diverso da 0). $mat(n, F)$ rispetto al prodotto è un monoide, ma non un gruppo. Per il teorema di Binet, per ogni $A, B \in Mat(n, F)$, $\det AB = \det A * \det B$. Quindi se A e B sono invertibili, anche AB è invertibile. Quindi se considero $GL(n, F)$ rispetto al prodotto esso è un gruppo: infatti il prodotto è un'operazione binaria che a due elementi dell'insieme associa una matrice dell'insieme. L'unità è la matrice identica.

Il prodotto di matrici qualsiasi è sempre associativo. Ogni matrice invertibile ha inversa rispetto al prodotto. Questo è un gruppo non abeliano per qualsiasi $n > 1$.

Questo gruppo $GL(n, F)$ si chiama *gruppo generale lineare* delle matrici di ordine n .

Esso ha sottogruppi di ordine inferiroe, ad esempio si può considerare il sottogruppo delle matrici con determinante 1 , denotato con $SL(n, F)$ *gruppo speciale lineare*. Anche le matrici diagonali invertibili formano un sottogruppo.

Si può anche considerare il sottogruppo delle matrici triangolari superiori invertibili.

Le matrici scalari (multipli delle identità) formano un sottogruppo fatto da tutte e sole le matrici che commutano e formano il *centro* di $Mat(n, F)$.

1.4.3 Anticipazione sugli anelli

Esempio (99 Prosegue l'esempio sulle matrici)

Presa una matrice A di ordine n , essa è invertibile in $Mat(n, R)$ se e solo se esiste una matrice $B = A^{-1}$ a elementi nell'anello $\mathbb{Z}$ tale che sia $AB = BA = id$. Se A è invertibile, valendo ancora il teorema di Binet, si ha $\det(AB) = \det A * \det B = \det(id) = 1$. Se A è invertibile il suo prodotto con l'inversa deve dare l'unità dell'anello. Il suo determinante deve avere un inverso nell'anello, quindi dev'essere invertibile in $\mathbb{Z}$ e dev'essere 1 o -1 .

Inversamente, se $\det A$ è invertibile in R , allora $(\det A)^{-1}$ è un elemento di R e allora A^{-1} è inversa di $A \in Mat(n, R)$.

Conclusione: Perché una matrice nell'anello abbia inversa, occorre solo che il suo determinante sia invertibile nell'anello. Ad esempio nel caso di $\mathbb{Z}$ le matrici invertibili sono quelle con determinate uguale a ± 1 .

1.5 Gruppi di trasformazioni

1.5.1 Definizione di permutazione

Definizione (100)

Sia X un insieme non vuoto e chiamiamo S_X l'insieme di tutte le applicazioni biettive (invertibili) di X in sé stesso, chiamate anche *permutazioni* o trasformazioni su X . Il prodotto di due applicazioni biettive è ancora un'applicazione biettiva, quindi la coppia $(S_X, \cdot)$ è un gruppo. Il prodotto di applicazioni ha una legge di composizione interna all'insieme, è associativo e l'unità è l'identità. Questo è il gruppo totale o simmetrico sull'insieme X .

Supponiamo che X sia finito e supponiamo che la sua cardinalità sia n allora il gruppo simmetrico ha ordine $n!$. In questo caso S_X si denota anche con S_n .

Se chiamo σ una permutazione di S_X , allora la indico con

$$\begin{array}{cccc} a_1 & a_2 & \dots & a_n \\ \downarrow & \downarrow & \downarrow & \downarrow \\ b_1 & b_2 & \dots & b_n \end{array}$$

o anche $\sigma(a_i) = b_i \, \forall i = 1, n$.

1.5.2 Cicli

Consideriamo un tipo particolare di permutazione dette *cicli*.

Definizione (101)

Per ogni $r \geq 2$, si dice *ciclo di lunghezza* r una permutazione su X del tipo

$$\begin{pmatrix} c_1 & c_2 & \dots & c_r & c_{r+1} & \dots & c_n \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ c_2 & c_3 & \dots & c_{r+1} & c_{r+2} & \dots & c_1 \end{pmatrix}$$

.

Esempio (102)

$1 \to 2, 2 \to 3, 3 \to 4, 4 \to 1, 5 \to 5$.

Se ho una permutazione $\sigma \in S_X$ e $a \in X$, ho due possibilità: $S(a) \neq a$ allora σ muove a , se $\sigma(a) = a$ allora σ fissa a .

1.5.3 Permutazioni disgiunte

Definizione (103)

Due permutazioni $\sigma, \tau \in S_X$ si dicono *disgiunte* se gli oggetti mossi da σ sono fissati da τ . In questo caso, $\sigma \circ \tau = \tau \circ \sigma$ (le due permutazioni non interferiscono sugli oggetti).

Proposizione (104)

Ogni permutazione $\sigma \in S_n$ diversa dall'identità si può scrivere come prodotto di un numero finito di cicli a due a due disgiunti, univocamente determinati dalla permutazione σ a meno dell'ordine dei fattori.

Dimostrazione

$\sigma \neq id$, prendo un oggetto c_1 mosso da σ . Se $\sigma(c_1) = c_2$, allora c_2 potrebbe avere come immagine c_1 e chiudere un ciclo di lunghezza 2 , altrimenti potrebbe andare in c_3 . Poi c_3 non può tornare in c_2 perché σ è biettiva. Allora $c_3 \to c_4$. Non posso proseguire all'infinito perché si ha solo un numero finito di oggetti. Non posso tornare in $c_2, c_3, \ldots, c_{n-1}$ per la biettività di σ , allora si torna in c_1 e si chiude un ciclo. Se tutti gli n oggetti sono terminati, la permutazione è un ciclo di lunghezza n . Se alcuni oggetti sono rimasti fuori, la permutazione potrebbe fissarli tutti. Quindi gli elementi fissati non compaiono. Se c'è un altro elemento che viene mosso, si ripete il ragionamento e si ha un ciclo disgiunto dal precedente. Posso considerare σ come il prodotto di cicli a due a due disgiunti, e gli elementi che non compaiono sono punti fissi.

Oltre alla scrittura in tabella, un ciclo di lunghezza r , si può indicare come (c_1, c_2, c_r) : questa scrittura indica che $\sigma(c_1) = c_2$, $\sigma(c_2) = c_r$, $\sigma(c_r) = c_1$, cioè a destra di ogni elemento si mette la sua immagine mediante σ , e l'immagine dell'ultimo elemento scritto è il primo (il ciclo si chiude).

Usando la prima notazione su più righe, è inessenziale l'ordinamento della prima riga, ma è essenziale che sotto a ciascun elemento ci sia l'immagine.

1.5.4 Esempi di permutazioni di X

Per ogni ciclo ci sono r scritture del tipo (c_1, c_2, c_r) .

Se X ha almeno due oggetti, le permutazioni sono l'identità id e la permutazione che scambia 1 con 2 (S_X ha ordine 2!).

Definizione (105)

Un ciclo di lunghezza 2 si chiama *scambio* o *trasposizione*.

Esempio (106)

S_3 ha 6 oggetti (3!): l'identità, tre scambi, un ciclo di lunghezzza 3 $(1, 2, 3)$ e il suo inverso $(1, 3, 2)$.

Esempio (107)

S_4 ha 24 permutazioni. La struttura ciclica di una permutazione è la decomposizione in cicli disgiunti. Possiamo avere l'identità, 6 scambi (si calcolano facendo

$3 * 4/2$, perché ogni scambio ha due scritture possibili), 8 cicli di lunghezza 3 , prodotti di due cicli disgiunti $(1,2) \circ (3,4)$ che sono 3 . Infine ci sono i cicli di lunghezza 4 che sono 6 . La somma è 24 .

Il risultato si può generalizzare con una formula complessiva.

1.5.5 Segno di una permutazione

Prendiamo una permutazione σ e la scriviamo nel modo iniziale:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \downarrow & \downarrow & \downarrow & \downarrow \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

e definiamo *segno di* σ la quantità $\delta_\sigma = \prod_{1 \le i < j \le n} \frac{b_i - b_j}{a_i - a_j}$ (faccio il prodotto di frazioni che hanno al numeratore $\sigma(a_i) - \sigma(a_j)$ e al denominatore $a_i - a_j$ per ogni coppia con $i < j$). Ciascuno dei numeratori compare anche al denominatore a meno di un segno (sia gli a_i che i b_i appartengono a X), quindi posso semplificare ciascun numeratore con il denominatore corrispondente a meno di un segno.

Definizione (108)

Chiamo δ_s il segno.

1.5.6 Permutazioni pari e dispari

Definizione (109)

σ è una permutazione *pari* se $\delta_\sigma = 1$ e si dice *dispari* se $\delta_\sigma = -1$.

Presa una qualsiasi permutazione τ , scritta come

$$\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ \downarrow & \downarrow & \downarrow & \downarrow \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

Se considero il prodotto $\tau \circ \sigma$, applico prima σ e poi τ , quindi $\tau \circ \sigma$ è la permutazione che manda $a_1, a_2, \dots, a_n$ in $c_1, c_2, \dots, c_n$. Il suo segno per definizione è uguale a $\prod_{1 \le i < j \le n} \frac{c_i - c_j}{a_i - a_j}$

Se calcolo $\delta_\tau * \delta_\sigma = (\prod_{1 \le i < j \le n} \frac{c_i - c_j}{b_i - b_j}) * (\prod_{1 \le i < j \le n} \frac{b_i - b_j}{a_i - a_j})$. Ciascun $b_i - b_j$ che compare in δ_τ si semplifica con il corrispondente denominatore in δ_σ e il risultato è lo stesso.

Quindi il segno del prodotto $\delta_{\tau * \sigma}$ è uguale al prodotto dei segni $\delta_\tau * \delta_s$.

1.5.7 Sottogruppo delle permutazioni pari

Si deduce immediatamente che l'insieme di tutte le permutazioni di segno 1 di S_n formano un sottogruppo. L'identità è pari, quindi l'insieme è non vuoto. L'insieme

delle permutazioni pari è chiuso rispetto al prodotto, perché il prodotto tra permutazioni pari è pari. L'inverso di σ , chiamata σ^{-1} è pari. Questo sottogruppo si chiama *gruppo alterno su n oggetti* e si denota con $\dashv_n$.

Il prodotto di due permutazioni dispari è pari, quindi le permutazioni dispari non formano un sottogruppo.

Il gruppo alterno $\dashv_n$ ha ordine $\frac{n!}{2}$ e anche le permutazioni dispari sono $\frac{n!}{2}$

1.5.8 Segno di cicli

Osservazione (110)

preso il ciclo di lunghezza 2 , (c_1, c_2) il segno è -1 , perché $\delta_C = \frac{c_1 - c_2}{c_2 - c_1}$.

Ogni ciclo di lunghezza 2 è dispari.

Sia $r \geq 2$, sia $C = (c_1, c_2, c_r)$. Posso scrivere questo ciclo come prodotto di scambi non disgiunti, cioè come $(c_1, c_r) \circ (c_1, c_{r-1}) \circ \circ \circ (c_1, c_3) \circ (c_1, c_2)$. Ogni termine compare in uno solo degli addendi.

Allora ogni ciclo di lunghezza r è prodotto di $r - 1$ scambi (non disgiunti) e con segno -1 . Se $r - 1$ è pari, il ciclo è pari (moltiplicando -1 per sé stesso per un numero pari di volte ottengo 1), altrimenti è dispari.

Osservazione (111)

$\delta_C = (-1)^{r_1 - 1}$ se $C = (1, r_1)$, cioè se il ciclo ha lunghezza R_1 .

Prendo una generica permutazione σ , un qualsiasi elemento di S_n . Allora $\sigma = \sigma_{r_1} \circ \sigma_{r_2} \circ \cdots \circ \sigma_{r_t}$ per un certo t . Sia questa la decomposizione di σ nel prodotto di t cicli disgiunti di lunghezza $r_1, r_2, \ldots, r_t$. Il segno conserva il prodotto, quindi $\delta_\sigma = \delta_{\sigma_{r_1}} * \cdots * \delta_{\sigma_{r_t}}$.

Ogni ciclo è prodotto di scambi e ogni scambio ha segno -1 . Il ciclo di lunghezza r_1 ha segno uguale a $(-1)^{r_1 - 1}$.

$$\delta_\sigma = (-1)^{(\sum_{i=1}^{t} r_i) - t}$$

L'esponente è il numero totale di scambi di cui σ è prodotto in base a questa formula.

$\delta_s = 1$ se l'esponente è pari, e quindi se è decomponibile in un numero pari di scambi non necessariamente disgiunti. σ è dispari se l'esponente è dispari e quindi se è decomponibile nel prodotto di un numero dispari di scambi, non necessariamente disgiunti.

Una permutazione pari si può decomporre in infiniti modi, ma qualunque sia il modo, il numero degli scambi è sempre pari.

Prese tutte le permutazioni pari, se ad ognuna aggiungiamo lo scambio $(1, 2)$ otteniamo tutte permutazioni dispari e se ne ottengono altrettante. Quindi l'ordine del gruppo alterno è $\frac{n!}{2}$

1.6 Congruenze

1.6.1 Definizione

Dato un insieme X si possono generare tante relazioni di equivalenza. Prendiamo un insieme X con un'operazione binaria $*$ e sia R una relazione di equivalenza definita su X .

Definizione (112)

Si dice che R è una *congruenza* rispetto all'operazione $*$, o anche che R è compatibile con $*$, se $\forall a, b, a', b' \in X$, e supponiamo aRa' e bRb' , questo implica necessariamente che $(a * b)R(a' * b')$.

Queste relazioni consentono di indurre sull'insieme quoziente un'operazione che ha quasi tutte le proprietà dell'operazione $*$.

Osservazione (113)

Se R è una congruenza rispetto a $*$, si induce un'operazione binaria chiamata $*_R$ sull'insieme quoziente X/R ponendo per ogni coppia $([a]_r, [b]_r) \in X/R$ l'uguaglianza $[a_r] *_r [b]_r = [a * b]_r$.

$*_R$ è un'operazione ben definita : $X/R \times X/R \to X/R$, perché R è una congruenza e quindi preso un elemento qualsiasi in $[a]_R$ e uno in $[b]_r$, il loro prodotto è associato a quello di altri due elementi presi rispettivamente in $[a]_R$ e $[b]_r$, cioè $a' * b'$ e $a * b$ appartengono alla stessa classe di equivalenza, che chiamo $[a * b]_R$.

Osservazione (114)

Si può esprimere $*_R$ in termini della proiezione canonica. Si chiama π_r la proiezione canonica da X a X/R . Allora si può anche scrivere:

$$[a]_r * [b]_r = \pi_r(a) * \pi_r(b) = \pi([a * b]_r) = \pi_R(a * b)$$

(la proiezione canonica conserva il prodotto). π_r in queste condizioni è un morfismo.

Osservazione (115)

L'operazione indotta sul quoziente eredita alcune proprietà di $*$. Le proprietà di $*_R$ esreditate da $*$ sono:

1. le proprietà di tipo equazionale (commutativa o associativa);
2. Se $*$ ammette unità sinistra u_s o unità destra u_d o unità bilatera u , allora le immagini mediante la proiezione canonica che contengono u_s, u_d, u funzionano da unità rispetto all'operazione indotta e si denotano con $[u_s], [u_d], [u]$.
3. Infine, se $x \in X$ e $*$ ammette unità u , e $x \in X$ ammette inverso sinistro $\bar{x}_s$ e inverso destro $\bar{x}_d$ o inverso bilatero $\bar{x}$, ispetto a $*$, allora l'immagine

$[x]_R$ ammette rispettivamente inverso sinistro $[\bar{x}_s]_r$, inverso destro $[\bar{x}_d]_r$ e inverso bilatero $[\bar{x}]$ rispetto all'unità u .

Proposizione (116)

[Proprietà di annullamento del prodotto] Il prodotto di due interi $m, n \neq 0$ è diverso da 0 .

Prese due matrici elementari, due matrici non nulle possono avere prodotto 0 .

Se questa proprietà vale per $(X, *)$, può non valere per l'operazione indotta.

1.6.2 Relazione di congruenza in Z

Definizione (117)

Sia n un fissato intero ≥ 1 . Due interi a e b si dicono *congrui modulo* n se la differenza $a - b$ è divisibile per n , cioè se $n \mid a - b$, ovvero esiste h tale che sia $a - b$ è esprimibile come $h * n$. Allora questa relazione su $\mathbb{Z}$ si dice congruenza modulo n e se a e $b \in \mathbb{Z}$ sono congrui mod n fra loro, scriviamo $a \equiv b \mod n$ (uguale con tre lineette).

Osservazione (118)

Per $n = 0$, $a \equiv b \mod n$ se e solo se $a = b$ e la relazione sarebbe l'identità.

Esempio (119)

Se $n = 1$, $a \equiv b \mod n$ per ogni b , ottengo la relazione universale, tutti gli interi sono nella stessa classe.

Esempio (120)

Presi i numeri relativi, si otengono le stesse classi di equivalenza che avevo ottenuto con i numeri positivi. Per questo si sceglie $n > 1$.

Esempio (121)

La relazione di equivalenza modulo 2 consiste delle classi dei pari e dei dispari.

Esempio (122)

Per $n = 6$, allora le classi sono $[0], [1], [2], [3], [4], [5]$.

Si possono definire una somma e un prodotto di classi, tali che $[a] + [b] = [a + b]$, e $[a] * [b] = [ab]$.

Se considero ad esempio $[2] * [3] = [6] = [0]$, perché $6 - 0/6$, si verifica che la proprietà dell'annullamento del prodotto non si eredita nel quoziente.

1.6.3 Congruenza modulo n come relazione di equivalenza

Nell'insieme $\mathbb{Z}$ degli interi relativi, fissato un intero positivo maggiore di 1 si può dare la definizione di congruenza modulo n : a è congruo a b modulo n ($a \equiv b \mod n$) se $n \mid a-b$, cioè esiste un intero h tale che $a-b=hn$.

Proposizione (123)

La relazione di congruenza è di equivalenza su $\mathbb{Z}$ e l'insieme quoziente è costituito da esattamente n classi, che sono indicate con $[0]_n, [1]_n, \ldots, [n-1]_n$. Ogni intero è contenuto in una di queste classi.

Dimostrazione

Dimostro che la relazione è di equivalenza:

1. Per ogni $a \in \mathbb{Z}$, $a \equiv a \mod n$ se pongo $h=0$ (riflessiva).
2. se $a \equiv b \mod n$, allora $a-b=h*n, h \in \mathbb{Z}$ quindi $b-a=-h*n$, (simmetrica);
3. se $a \equiv b \mod n$ e $b \equiv c \mod n$, allora esiste h per cui $a-b=h*n$, ed esiste k tale che $b-c=kn$. Sommando termine a termine ottengo $a-b+b-c=a-c=(h+k)*n$, ovvero $a \equiv c \mod n$ (transitiva)

Sia a un intero e mostriamo che la classe che lo contiene è una di quelle indicate. Usiamo l'algoritmo della divisione.

Se $a > n$, divido a per n e ottengo un quoziente e un resto, cioè scrivo $a=q*n+r$, con $r \geq 0$, $r < n$. $a-r=q*n$, quindi la differenza $a-r$ è divisibile per n e $a \equiv r \mod n$, cioè la classe che contiene a è quella che contiene il resto. Siccome il resto può andare da 0 a $n-1$, l'insieme delle classi di equivalenza consiste di n classi.

Dimostriamo che le n classi $[0]_n, [1]_n, [n-1]_n$ sono a due a due distinte. Supponiamo per assurdo che j_1, j_2 siano due interi fra 0 e $n-1$, e quindi supponiamo che $[j_1]=[j_2]$. Allora dev'essere j_1-j_2 un multiplo di n , ma $0 \leq j_1 < j_2 < n$, la differenza j_2-j_1 è strettamente compresa tra 0 e n . j_2-j_1 è un multiplo di n se e solo se $h=0$. Quindi $j_1 \equiv j_2 \mod n$ se e solo se coincidono, quindi l'insieme quoziente consiste esattamente di n classi.

Definizione (124)

L'insieme quoziente rispetto alla relazione di congruenza modulo n si denota con $\mathbb{Z}/(n\mathbb{Z})$ e prende il nome di *insieme delle* classi di resti modulo n .

Esempio (125)

Se $n=2$, l'insieme quoziente di $\mathbb{Z}$ consiste di due classi $[0], [1]$, dove $[0]$ è la classe dei numeri pari e $[1]=\{2h+1\}$ è quella dei numeri dispari.

Esempio (126)

Se $n = 3$ ho tre oggetti: $[0] = \{3h\}$ costituita dai multipli di 3 , $[1] = \{3h + 1\}$, $[2] = \{3h + 2\}$.

1.6.4 Compatibilità tra congruenza e operazioni

Per ogni fissato modulo $n > 1$, la relazione di congruenza modulo n è compatibile sia rispetto all'operazione di somma ordinaria, che rispetto a quella di prodotto fra interi.

Supponiamo che $a \equiv a' \mod n$ e $b \equiv b' \mod n$. Se la relazione è compatibile rispetto alla somma, allora $a+b \sim a'+b'$. Infatti, se $a \sim a'$ esiste un intero h tale che $a = a'+hn$. Invece $b \sim b'$ significa che esiste un intero k tale che $b = b'+kn$. Se sommo le uguaglianze termine a termine, $a+b = a'+hn+b'+kn = a'+b'+(h+k)n$, cioè $a+b \equiv a'+b' \mod n$ perché i due numeri differiscono di un intero multiplo di n .

Considerando la compatibilità rispetto al prodotto, $ab = (a' + hn)(b' + kn) = a'b' + (a'k + hb' + khn) * n$. quindi $a'b'$ e ab differiscono per un multiplo di n .

Pertanto la somma e il prodotto tra gli interi inducono sull'insieme quoziente $\mathbb{Z}/(n\mathbb{Z})$ due operazioni ben definite, che chiameremo somma e prodotto, tali che:

$$\text{somma} = [a]_n + [b]_n = [a + b]_n$$

$$\text{prodotto} = [a]_n * [b]_n = [ab]_n$$

Le operazioni sono ben definite perché non dipendono dalla scelta dei rappresentanti della classe di equivalenza.

Dati due interi a, b e un'incognita x , ci si chiede quando l'equazione $ax + b$ ha soluzioni intere.

Le congruenze lineari servono anche per risolvere le equazioni diofantee, della forma $ax + by + c = 0$, di cui si vuole capire quando le coppie x, y sono soluzioni intere.

1.6.5 Tavole di composizione

Siccome l'insieme quoziente per ogni n fissato è finito, allora si possono scrivere le tavole di composizione di queste operazioni.

Queste tavole sono matrici nxn e permettono di evidenziare alcune proprietà. La commutatività si vede dal fatto che la tavola è simmetrica. Non si riesce a vedere l'associatività.

Esempio (127)

Esempio di tavola della somma: scrivo sulla prima riga e sulla prima colonna le classi di equivalenza in ordine, poi nelle celle faccio le operazioni tra le classi di equivalenza (ad esempio $2 + 4 = 0$, perché mi sto riferendo alle classi di equivalenza e $[0] = [6]$). Nella cella a_{23} escluse la prima riga e la prima colonna, ad esempio c'è l'operazione $[1] + [2]$. Ad esempio, se $n = 6$.

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tavola del prodotto:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Dal fatto che nella tavola della somma la prima riga e la prima colonna rimangono invariate si capisce che l'operazione ha un elemento neutro.

Dal fatto che nella tavola del prodotto c'è una riga e una colonna di 0 si capisce che l'operazione ha un elemento annullatore.

Il prodotto di due classi di equivalenza diverse da 0 può essere 0.

1.7 Sottogruppo generato da un sottoinsieme

1.7.1 Unione e intersezione di sottogruppi

Sia G un gruppo, e consideriamo una collezione non vuota di sottogruppi di G : $\{h_i\}_{i\in I}$. L'intersezione insiemistica di sottogruppi è un sottogruppo, ma l'unione insiemistica no.

Proposizione (128)

Posto $H = \bigcap\{h_i\}_{i\in I}$, l'intersezione è un sottogruppo.

Dimostrazione

L'intersezione soddisfa la definizione di sottogruppo, infatti:

1. l'unità 1_g sta in ciascuno dei sottogruppi H_i , quindi sta nell'intersezione.
2. presi $a, b \in H$, devo garantire che ab sta in H . Se ab sta in H , deve stare in ciascuno degli H_i . ma ogni H_i è chiuso rispetto al prodotto, e a, b stanno in ciascuno degli H_i , quindi ab sta nell'intersezione.
3. lo stesso vale per la chiusura rispetto agli inversi: se $a \in H$, allora $a \in H_i, \forall i \in I$, quindi siccome ogni H_i è chiuso rispetto all'inversa si ha che $a^{-1} \in H_i$ e $a^{-1} \in H$.

L'unione insiemistica di sottogruppi può non essere un sottogruppo. Ad esempio, presi i sottogruppi dei multipli di 2 e dei multipli di 3 sottoinsiemi del gruppo $\mathbb{Z}$, l'unione insiemistica ($\{2, 3, 4, 6, 8, 9, \dots\}$), non è un sottogruppo. Se fosse un sottogruppo, essa dovrebbe essere chiusa rispetto alla somma e contenere anche $5 = 2 + 3$, ma questo non avviene. Il sottogruppo dato dall'unione dei due sottogruppi è il sottogruppo dei multipli di 1 , perché 1 è il massimo comun divisore tra 2 e 3 e quindi si può scrivere come combinazione lineare $1 = 2h+3k$. Il sottogruppo dei multipli di 1 è l'intero ed è quindi diverso dall'unione insiemistica dei due sottogruppi generati da 2 e da 3 .

1.7.2 Sottogruppo generato da un insieme

Consideriamo un qualsiasi sottoinsieme non vuoto A di G . Allora se considero la collezione di tutti e soli i sottoinsiemi di G che contengono A , questa collezione è non vuota perché di sicuro contiene G . L'intersezione di tutti i sottogruppi di G contenenti A è per la proposizione precedente un sottogruppo di G , che denotiamo con $\langle A \rangle$.

Osservazione (129)

Il sottogruppo $\langle A \rangle$ contiene l'insieme A .

Osservazione (130)

$\langle A \rangle$ è contenuto in ogni sottogruppo di G contenente l'insieme A .

Rispetto all'inclusione insiemistica, $\langle A \rangle$ è il "minimo" dei sottogruppi contenenti A .

Definizione (131)

Diremo che $\langle A \rangle$ è il sottogruppo di G generato dal sottoinsieme A .

Se in particolare $\langle A \rangle$ coincide con l'intero gruppo G , allora diremo che A è l'insieme di generatori di G .

Esercizio (132)

Caratterizzare il sottogruppo generato da A in base ai suoi elementi.

Il sottogruppo generato da A consiste di tutti e soli gli elementi di G che si possono esprimere come prodotto di un numero finito di elementi di A e di inversi di elementi di A . In formule, questo sottogruppo

$$< A >= \{g \in G \, t.c. g = \prod_{i=1}^{r} (a_i)^{\varepsilon_i}\}$$

,

dove $r \geq 1$ è il numero dei fattori, gli a_i sono elementi di A e ε_i vale 1 e -1 a seconda che sto considerando un elemento o il suo inverso.

Per far vedere che $< A >$ consiste solo di tutti gli elementi di questa forma, basta mostrare che l'insieme degli elementi scritti a destra è un sottogruppo di G che contiene A e che è contenuto in ogni sottogruppo di G che contiene A .

$< A >$ verifica la definizione di sottogruppo:

1. c'è l'unità, se pongo $g = a * a^{-1}$ e $r = 2$;
2. presi due elementi di questo tipo, il prodotto è ancora un prodotto dello stesso tipo (chiusura rispetto al prodotto)
3. L'inverso del prodotto è il prodotto degli inversi nell'ordine opposto ed è ancora un elemento g di questa forma.

Verifico che $< A >$ contiene A , perché per $r = 1$ g può essere uguale a un qualsiasi elemento di A .

Prendo un qualsiasi sottogruppo di G che contiene A , e che chiamo K . Allora K contiene tutti gli elementi di $< A >$, i loro prodotti e i loro inversi, perché è chiuso rispetto al prodotto e agli inversi.

1.7.3 Esempi

Esempio (133)

Prendiamo il gruppo additivo degli interi relativi: fissato $m \in \mathbb{Z}$, consideriamo il caso in cui A consista di un oggetto solo. Allora il sottogruppo generato da $A = \{n\}$, è dato da mh, $h \in \mathbb{Z}$ cioè mz .

Esempio (134)

Sia $A = \{4, 6\}$ allora consideriamo il sottogruppo generato da A , che consiste di tutti gli elementi della forma $6h + 4k, h, k \in Z$, cioè gli interi che si possono scrivere come combinazioni lineari di 4 e 6 con interi. Tutti questi oggetti sono multipli di 2 , quindi questo sottogruppo è contenuto nel sottogruppo degli elementi multipli di 2 .

2 è M.C.D. tra 4 e 6 e per l'identità di Bézout esistono interi h_1 e k_1 tali che $2 = 4h_1 + 6k_1$. Questo sottogruppo coincide col sottogruppo generato dal numero 2 .

In generale, le argomentazioni non dipendono da 4 e 6 . Quindi si può dimostrare che $\forall a, b \in \mathbb{Z}$ se considero il sottogruppo generato da a e da b , esso coincide con il sottogruppo generato dal massimo comun divisore fra a e b (usando l'identità di Bezout).

Esempio (135)

$\mathbb{Z}$ rispetto alla somma coincide con il gruppo generato da 1 e da -1 , questi sono gli unici generatori singoli di $\mathbb{Z}+$.

Ogni sottogruppo di $(\mathbb{Z}, +)$ è generabile da un solo elemento.

L'unione insiemistica di due sottogruppi è un sottogruppo se e solo se uno è contenuto nell'altro (e quindi si ottiene il più grande dei due sottogruppi).

1.7.4 Sottogruppi ciclici

Definizione (136 Sottogruppo ciclico)

Sia G un gruppo. Supponiamo che A sia un sottoinsieme di G che consiste del solo elemento a . In questo caso il sottogruppo generato da a si denota con $< a >$ e prende il nome di *sottogruppo ciclico* generato dall'elemento a .

Se il sottogruppo ciclico generato da a è l'intero gruppo, diremo che l'intero gruppo G è un gruppo ciclico generabile dal singolo elemento a .

Osservazione (137)

In notazione moltiplicativa, gli elementi di $< a >$ sono tutti gli elementi di G che si possono scrivere come potenze di a , cioè $\{x \in Gt.c.x = a^n,\ n \in \mathbb{Z}\}$.

In notazione additiva si ha $< a >= \{x \in Gt.c.na = x\}$.

1.7.5 Ordine o periodo di un elemento

Definizione (138 Ordine o periodo di un elemento)

Sia a un elemento di G . Se $< a >$ è finito di ordine n , si dice che n è l'*ordine* o *periodo* dell'elemento a e si scrive $o(a) = n$. Se invece il sottogruppo ciclico generato da a è infinito, si dice che a ha periodo infinito.

Osservazione (139)

In un qualsiasi gruppo l'unità ha periodo 1 , perché il sottogruppo generato dall'unità ha un solo elemento (l'unità ha come inverso sé stessa e moltiplicata per sé stessa è sempre l'unità).

Osservazione (140)

Consideriamo i gruppi additivi $(\mathbb{Z}, +)$ e $(\mathbb{Q}, +)$ e $(\mathbb{R}, +)$. L'unità è 0 , ogni altro elemento ha periodo infinito.

In un gruppo infinito, oltre all'unità può succedere che ogni elemento abbia periodo infinito, ma può anche avvenire che alcuni elementi abbiano periodo finito.

1.7.6 Esempi sul periodo

Esempio (141)

Preso il gruppo costituito dai numeri complessi non nulli che chiamo $\mathbb{C}* = \mathbb{C} \setminus (0)$, essi formano un gruppo moltiplicativo. Gli elementi di periodo finito sono le radici dell'unità mentre tutti gli altri elementi hanno periodo infinito.

Per ogni $n > 1$, gli elementi di periodo n sono i numeri complessi $e^{i*2k\pi/n}$ dove k è un intero relativo variabile tra 0 e $n-1$, cioè le radici n-esime dell'unità, ma solo quelle per cui k è primo con n , cioè $M.C.D.(k,n) = 1$.

Per $k = 1$, posso prendere tutte le potenze fino all' n -esima per ottenere 1 . Questo è un modello moltiplicativo per ogni gruppo ciclico di ordine n . In termini additivi, questo equivale al gruppo additivo delle classi di resti modulo n . Il gruppo delle radici n -esime dell'unità nei complessi e quello delle classi di resto modulo n sono isomorfi.

Esempio (142)

Se considero il gruppo moltiplicativo dei reali non nulli, gli elementi di periodo finito sono solo 1 e -1 , cioè le uniche radici n -esime dell'unità.

Esercizio (143)

Preso il gruppo simmetrico S_n e presa una permutazione di n oggetti, calcolarne il periodo.

Se chiamo σ un elemento di S_n , un modo per calcolarne il periodo è decomporla nel prodotto di cicli disgiunti, scriviamo quindi $\sigma = \gamma_1 \circ \gamma_2 \circ \gamma_s$. Supponiamo che i cicli abbiano rispettivamente lunghezze r_1, r_2, r_s . Si può provare che il periodo o ordine della permutazione σ è il minimo comune multiplo delle lunghezze di questi cicli r_1, r_2, r_n .

Definizione (144 Minimo comune multiplo)

Presi due o più interi si dice minimo comune multiplo M un intero che sia multiplo di tutti quanti e inoltre ogni altro intero che è multiplo di tutti quanti è divisibile per M .

1.7.7 Nozione di potenza

Con la nozione di periodo di un elemento intendiamo più precisamente parlare della nozione di potenza, cioè della funzione di dominio $\mathbb{Z}$ e di codominio G definita ricorsivamente associando a ogni $n \in \mathbb{Z}$ l'elemento $a^n \in G$, dove ricorsivamente significa che $a^0 = 1_G$ e per ogni $n > 0$ si ha $a^n = a^{n-1} * a$ e per $n < 0$, $a^n = (a^{-1})^{-n}$

Non ci si aspetta che questa funzione sia iniettiva, ma potrebbe avvenire che per due elementi m e n si abbia $a^n = a^m$.

Proposizione (145)

1. Supponiamo che a abbia periodo finito ($o(a) = n$). Allora n è il minimo intero positivo tale che $a^n = 1_g$ e gli elementi distinti del sottogruppo ciclico generato da a sono l'unità a^0 , a, a^2, a^{n-1}

mentre a^n coincide nuovamente con l'unità. Equivalentemente, $a^l = a^m$ se e solo se l è congruo a m modulo n .

1. $o(a) = +\infty$ se e solo se $l \neq m$ implica $a^l \neq a^m$ (cioè se e solo se la funzione potenza in base a è iniettiva).

Dimostrazione

Se $o(a) = n < \infty$ allora esistono sicuramente due interi $i, j \in \mathbb{Z}$ tali che $i > j$ e tali che $a^i = a^j$. Se moltiplico entrambi i membri di quest'uguaglianza per l'inverso di a^j ottengo $a^i * a^{-j} = a^{i-j} = a^0 = u$ con $i - j > 0$.

Considero il minimo intero positivo t tale che $a^t = 1_G$. Questo è possibile per il principio del buon ordinamento.

Principio del buon ordinamento per ogni fissato intero z_0 , ogni sottoinsieme non vuoto di tutti gli interi maggiori di z_0 ammette minimo.

Presi tutti gli interi tali che $a^n > 0$, C'è un minimo intero positivo con questa proprietà: sia t il minimo intero positivo tale che sia $a^t = 1_G$ (t è il minimo degli $i - j$ tali che $a^{i-j} = 1_G$). Prendo una qualsiasi potenza a^h che è un elemento di G . Dividiamo h per t .

$$h = q * t + r,\ 0 \leq r < t$$

Segue che

$$a^h = a^{qt+r} = a^{qt} * a^r = (a^t)^q * a^r = (1_G)^q * a^r = a^r$$

Preso un qualsiasi elemento di G che si scrive come a^h , esso può assumere solo t valori, compresi tra 0 e $t - 1$.

L'ordine del sottogruppo ciclico generato da a è minore o uguale di t .

D'altronde, supponiamo che $a^{h_1} = a^{h_2}$ con $h_1 < h_2 < t$. Allora $a^{h_2-h_1} = 1_G$ (ho moltiplicato entrambi i membri per a^{-h_1}). Questo è assurdo, perché $h_2 - h_1 > 0$ e $h_2 - h_1 < t$. Quindi ho un intero positivo minore di t tale che $a^{h_1-h_2} = 1_G$. Questo va contro la scelta minimale di t (t è il minimo intero per cui avviene che $a^t = 1_G$).

Si conclude che gli elementi della forma a^0, a, a^{t-1} sono a due a due distinti. Quindi sono esattamente t elementi distinti e $n = t$ è l'ordine del sottogruppo ciclico generato da a . Allora $< a >= a^0, a, a^{n-1}$.

Supponiamo dapprima che $a^l = a^m$, $m, l \in \mathbb{Z}$. Quindi $a^{l-m} = 1_G$. Dividiamo $l - m$ per il periodo n , quindi

$$l - m = n * q + r,\ 0 < r < n$$

.

Si ha

$$1_G = a^{l-m} = a^{nq+r} = a^{nq} * a^r = (1_G)^q * a^r = a^r$$

.

n è il minimo intero positivo tale che $a^n = 1_G$, quindi l'unica possibilità è che $r = 0$. Quindi $l - m$ è divisibile per n dunque si conclude che l è congruo a m modulo n .

Vale viceversa: se l è congruo a m modulo n , presi due interi generici allora esiste un intero h tale che $l-m = hn$ da cui $a^{l-m} = a^{hn} = (a^n)^h = (1_G)^h = 1_G$. Quindi se $l \equiv m \mod n$ si ha $a^l = a^m$.

Se la funzione potenza in base a è iniettiva, il gruppo ciclico generato da a consiste di infiniti elementi, quindi $o(a) = +\infty$.

Inversamente, supponiamo che l'ordine di a sia infinito e supponiamo per assurdo che $a^l = a^m$, con $l \neq m$. Possiamo supperre senza perdere generalità $l > m$. Se fosse $a^l = a^m$ si avrebbe $a^{l-m} = 1_G$, con $l - m > 0$. Ragionando come nel punto 1 si otterrebbe che il periodo di a è al più $l - m$, contro l'ipotesi che sia infinito.

Corollario (146)

Se ho un intero s tale che $a^s = 1_G$, $s \neq 0$, allora s è un multiplo del periodo di a .

Dimostrazione

Sia a un elemento di G e supponiamo che ci sia un intero s diverso da 0 tale che $a^s = 1_G$. Se questo è vero, la funzione potenza in base a non è iniettiva, perché s e 0 danno luogo allo stesso elemento. Allora l'ordine di a è $n < +\infty$.

Dividiamo s per n e scriviamo

$$s = nq + r, \, 0 \leq r < n$$

Allora riscrivo

$$1_G = a^s = a^{nq+r} = a^{nq} * a^r = a^r$$

e $a^r = 1_G$, ma n è il periodo di a , che è il minimo intero positivo tale che $a^n = 1_G$, siccome $r < n$, allora se $a^r = 1_G$, necessariamente $r = 0$ e $s = nq$, cioè $n \mid s$.

1.7.8 Osservazioni conclusive

Osservazione (147)

Se a è un elemento di periodo infinito e k è un intero diverso da 0 , la potenza a^k ha anch'essa periodo infinito (da dimostrare in seguto).

Osservazione (148)

Se invece $o(a) = n$, per ogni $k \neq 0$ il periodo di a^k è esattamente uguale al quoziente tra n e il massimo comun divisore tra k e n .

Osservazione (149)

In particolare, se a genera un sottogruppo finito di ordine n , allora i generatori del sottogruppo ciclico generato da a sono tutti e soli gli elementi che come potenze di a si esprimono nella forma a^k , ove il massimo comun divisore tra k e n è 1 .

1.7.9 Gruppo ciclico

Definizione (150 Gruppo ciclico)

Un gruppo si dice *ciclico* quando contiene un elemento a tale che il sottogruppo ciclico generato da a coincide con l'intero gruppo.

Osservazione (151)

Un gruppo ciclico infinito è isomorfo al gruppo degli interi mentre per ogni numero naturale n c'è un solo gruppo ciclico finito, dato dal gruppo additivo delle classi di resto modulo n .

Esempio (152)

Il gruppo di interi relativi è ciclico infinito e i suoi generatori sono 1 e -1 .

Preso un naturale maggiore di 1 , se considero $\mathbb{Z}/(n\mathbb{Z})$, con l'operazione di somma di classi, questo gruppo è ciclico. Presa la classe $[a]_n$ essa si può scrivere come il multiplo dell'intero a della classe $[1]_r$. Quindi la classe $[1]_r$ genera. Il gruppo è generato dalle classi $[x]_n$ dove x è primo con n .

Esempio (153)

Il gruppo delle classi della relazione di congruenza modulo 10 ha come generatori $[1], [3], [7], [9]$.

Infatti se considero ad esempio la classe di equivalenza $[7]_r$ considero i suoi multipli.

$$\{[7]_r, [14]_r = [4]_r, [21]_r = [1]_r, [28]_r = [8]_r, [35]_r = [5]_r, [42]_r = [2]_r, [49]_r = [9]_r, [56]_r = [6]_r, [63]_r = [3]_r,$$

Compaiono le 10 classi di equivalenza della relazione di congruenza modulo 10 (e quindi l'intero gruppo G) e poi ricompare l'unità.

Osservazione (154)

Preso un gruppo ciclico, ogni sottogruppo è ancora ciclico.

1.7.10 Teorema di Lagrange

Teorema (155 Teorema di Lagrange)

L'ordine di un sottogruppo di un gruppo finito dev'essere necessariamente un divisore dell'ordine del gruppo.

Nel caso di gruppi ciclici il teorema di Lagrange si inverte: per ogni divisore esiste ed è unico un sottogruppo che ha come ordine quel divisore.

1.8 Classi laterali di un sottogruppo

1.8.1 Relazioni di equivalenza associate ad H

Sia H un sottogruppo di G . Allora ad H sono associabili due relazioni di equivalenza:

1. D_H : Se a, b sono elementi di G , aD_Hb se esiste $h \in H$ tale che $b = h * a$
2. S_H : aS_Hb se esiste $h \in H$ tale che $b = a * h$

Se il gruppo è abeliano queste due relazioni sono sempre equivalenti.

Se in un gruppo non abeliano queste relazioni sono equivalenti, allora si ha un gruppo normale.

Lemma (156)

D_H e S_H sono relazioni di equivalenza su G .

Dimostrazione

Il fatto che queste relazioni sono di equivalenza dipende dal fatto che H è un sottogruppo.

1. Se $h = 1_g$, allora $a = 1_g * a$ e ho trovato un h per cui la proprietà riflessiva vale con $a = b$
2. se aD_Hb , allora esiste h tale che $b = h * a$, ma posso moltiplicare per l'inverso di h i termini di quest'uguaglianza e

ottengo $h^{-1} * b = a$, quindi ho trovato un elemento h^{-1} di H tale che vale la simmetria;

1. la transitività dipende dalla chiusura di H rispetto al prodotto: se aD_Hb e bD_Hc ,

allora esiste h tale che $b = ah$ ed esiste k tale che $c = bk$, quindi $c = (ah)k = a(hk)$ e a è associato a c .

1.8.2 Notazione

$[a]_{D_H}$ è la classe che contiene l'elemento a e consiste di tutti i soli i b in G che si possono scrivere come $h * a$, cioè

$$\{g \in Gt.c.\exists h \in H \text{ tale che } g = h * a\} = \{g = h * a, h \in H\}$$

,

ci sono tutti i prodotti degli elementi di H per a , quindi chiamo la classe di equivalenza di a con Ha .

In notazione additiva, $b = ha$ equivale a $b = h + a$ e il simbolo della classe di equivalenza che contiene a sarebbe $H + a$.

La classe che contiene a rispetto alla relazione S_H consiste di

$$\{g = a * h\}$$

,

e la classe di equivalenza che contiene a si denota col simbolo aH oppure in notazione additiva con $a + H$.

1.8.3 Definizioni

Definizione (157 Laterali)

Le classi di equivalenza della relazione D_H si dicono *laterali destri* del sottogruppo H in G , mentre le classi di equivalenza della relazione S_H si dicono *laterali sinistri* di H in G (equivalgono all'insieme quoziente della relazione S_H su G).

G è unione disgiunta dei laterali destri di H in G (è unione disgiunta delle classi di equivalenza).

Osservazione (158)

Non tutti i laterali sono sottogruppi: H è un laterale di sé stesso ed è l'unico laterale che contiene l'unità; quindi se ci sono altri laterali non possono essere sottogruppi.

1.8.4 Uguaglianza tra laterali

Prendo Ha e Hb laterali destri. Si ha che $Ha = Hb$ se e solo se $b * a^{-1} \in H$. Infatti in questo modo $b = Ha = b*a^{-1}*a = b$ quindi $b \in Ha$ e $h = b*a^{-1}$, allora anche l'inverso di h che è $h^{-1} = a*b^{-1} \in H$. Si ha anche $a = Hb = a*b^{-1}*b = a$ e quindi $a \in Hb$, quindi $Hb = Ha$

In notazione additiva due laterali coincidono se e solo se la differenza $b - a$ è un elemento di H .

Nel caso sinistro, $aH = bH$ se e solo se $a^{-1}b \in H$, quindi $-a + b \in H$.

1.8.5 Esempi sulle classi laterali

Ci sono due partizioni di G , quella dei laterali destri e quella dei laterali sinistri di $H \in G$. Se le due partizioni coincidono allora $D_H = S_H$.

Può succedere che D_H coincida con S_H oppure no. Il più piccolo gruppo non abeliano in cui le due relazioni non coincidono è il gruppo simmetrico di 3 oggetti.

Esempio (159)

Nel gruppo S_3 prendo il sottogruppo generato dallo scambio $(1,2)$ che consiste dell'identità e di $(1,2)$. Se calcolo D_H e S_H sono diverse, perché le partizioni dei laterali destri e sinistri di questi 6 elementi sono diverse.

Laterali destri di $(1,2) \in S_3$:

$$H * (1,2) = H * (id)$$
$$H * (1,2,3) = (1,2) * (1,2,3), id * (1,2,3)$$
$$H * (1,2,3) = (2,3), (1,2,3) = H * (2,3)$$
$$H * (1,3) = (1,2) * (1,3), id * (1,3)$$
$$H * (1,3) = (1,3,2), (1,3) = H * (1,3,2)$$

Per s_H si trova una partizione diversa di S_3 .

$$(1,2) * H = id * H = H$$
$$(1,3) * H = (1,3) * (1,2), (1,3) * id$$
$$(1,3) * H = (1,2,3), (1,3) = (1,2,3) * H$$
$$(2,3) * H = (2,3) * (1,2), (2,3) * id$$
$$(2,3) * H = (1,3,2)), (2,3) = (1,3,2) * H$$

Esempio (160)

Nel gruppo S_3 , se prendo come sottogruppo $H = A_3$, le due partizioni coincidono. Si ha $o(A_3) = 3!/2 = \frac{o(S_3)}{2}$.

In generale, in ogni gruppo finito in cui si prende un sottogruppo tale che il numero dei laterali ha indice 2 si ha che le due relazioni coincidono (cioè, ogni sottogruppo che ha la metà degli elementi del gruppo è normale (le due relazioni coincidono).

I laterali destri di A_4 sono due: H che è il laterale che contiene l'unità, e $H * \sigma$ dove σ è una permutazione dispari, non appartenente ad H .

I laterali sinistri sono H e $\sigma * H$, con $\sigma \notin H$.

La partizione consiste di due oggetti in entrambe le relazioni. Per ogni $\sigma \in S_n$ i due laterali destri sono disgiunti e la loro unione è uguale ad S_n .

Esempio (161)

Preso il gruppo S_4 con $o(S_4) = 4!$, allora $H = A_4$ è un sottogruppo normale. Anche il sottogruppo costituito da id e dai prodotti di due scambi disgiunti $(1,2)*(3,4)$, $(1,3)*(2,4)$, $(1,4)*(2,3)$ chiamato gruppo trirettangolo è un gruppo normale. Anche in questo caso si vede che le due relazioni D_h e S_h coincidono.

Esclusi questi due gruppi e i sottogruppi banali, non ci sono altri sottogruppi normali in S_4 .

1.8.6 Dimostrazione del teorema di Lagrange

Teorema (162)

Sia G un gruppo finito di ordine n e sia H un sottogruppo di G di ordine r . Allora r è un divisore dell'ordine del gruppo, cioè $r \mid n$.

Dimostrazione

Per ogni fissato elemento $a \in G$, consideriamo l'applicazione $f_a \colon H \to Ha$ che manda ogni $h \in H$ nel prodotto $h * a$. (non cambia niente se si considera il laterale sinistro, infatti il numero dei laterali destri e quello dei laterali sinistri è uguale)

Ogni elemento del laterale $H * a$ è della forma $h * a$ con $h \in H$, quindi f_a è suriettiva per definizione: preso un qualsiasi elemento $h * a$ esso ha una preimmagine mediante f .

Inoltre F_a è iniettiva, per la validità delle leggi di cancellazione del gruppo: presi due elementi $h_1, h_2 \in H$ che abbiano la stessa immagine si ha $h_1 * a = h_2 * a$ e cancellando a si ottiene $h_1 = h_2$.

Siccome l'applicazione è biettiva, allora per ogni fissato $a \in G$ la cardinalità di H coincide con quella di aH .

I laterali sono un numero finito s , allora $G = \bigcup\{H, H * a_2, \ldots, H * a_s\}$. Siccome tutti i laterali hanno la stessa cardinalità, allora $|G| = |H * 1_G| + |H * a_2| + \cdots + |H * a_s|$. Ci sono quindi s laterali con cardinalità r (uguale a quella di H), quindi $n = O(G) = r * s$, quindi $r \mid n$.

Abbiamo anche provato che l'ordine del gruppo è uguale all'ordine del sottogruppo per il numero dei laterali.

1.8.7 Corollari e osservazioni

Corollario (163)

Sia G come sopra e sia a un qualsiasi elemento di G . Allora il periodo di a è un divisore dell'ordine del gruppo (equivalentemente, $a^n = 1_G$).

Dimostrazione

Se a ha periodo r , allora il sottogruppo ciclico generato da a ha ordine r e si ha che $a^r = 1_G$. Allora per il teorema di Lagrange l'ordine r del sottogruppo ciclico generato da a divide n . Per il corollario sulla funzione potenza, se $r \mid n$ e $a^r = 1_G$, $a^n = 1_G$

Osservazione (164)

Il teorema di Lagrange non si inverte in generale. Il controesempio minimo è $G = A_4$. Infatti $o(A_4) = 12$ ma A_4 non contiene sottogruppi di ordine 6 . Se ci fosse un sottogruppo di ordine 6 , conterrebbe la metà degli elementi di A_4 e

sarebbe un sottogruppo normale in A_4 .

In alcune classi particolari di gruppi il teorema si inverte. Ad esempio, preso un gruppo ciclico finito, per ogni divisore dell'ordine del gruppo esiste un sottogruppo che ha come ordine quel divisore.

1.9 Congruenze in un gruppo

1.9.1 Classi rispetto a una congruenza

Dato un insieme G con un'operazione binaria, considero le relazioni compatibili con l'operazione $*$. Queste permettono di indurre in modo naturale un'operazione sul quoziente, che eredita parte delle proprietà di $*$.

In un gruppo le congruenze si possono caratterizzare in modo significativo. Conoscendo la classe che contiene l'unità, detta nucleo, si possono determinare le altre classi della congruenza.

Proposizione (165)

Sia R una congruenza in un gruppo $(G, *)$. Allora:

1. la classe d'equivalenza che contiene l'unità $[1_G]_R = N$ è un sottogruppo di G ;
2. per ogni $a \in G$, allora $[a]_R$ è il laterale destro $N * a$ che coincide con $a * N$ laterale sinistro

(i laterali si possono definire perché per il punto 1 N è un sottogruppo). In particolare $S_N = D_N$.

Dimostrazione

Dimostriamo che la classe che contiene l'unità è un sottogruppo, usando la definizione:

1. ovviamente la classe dell'unità contiene l'unità;
2. siano a, b due elementi entrambi associati all'unità cioè tali che $aR1_g$ e $bR1_g$.

Siccome R è una congruenza da questo segue che $abR1_G * 1_G = 1_G$. Con questo si dimostra che la classe dell'unità è chiusa rispetto al prodotto;

1. sia ora $a \in [1_G]_R$. Dal fatto che $aR1_G$ se considero a^{-1} che appartiene a G si può scrivere $a^{-1}Ra^{-1}$

(R è riflessiva), allora $a * a^{-1}R1_G * a^{-1}$ cioè 1_GRa^{-1} e per simmetria $a^{-1}R1_G$.

In conclusione N è un sottogruppo di G .

Proviamo che per ogni $a \in G$, $[a]_R$ coincide con il laterale destro Na del sottogruppo N . Dimostro la doppia inclusione.

Prendo un elemento $b \in [a]_R$. Se bRa , allora $a^{-1}Ra^{-1}$. Allora $b*a^{-1}Ra*a^{-1} = 1_G$ cioè $b * a^{-1} \in N$. Questo significa che esiste $n \in N$ tale che $b * a^{-1} = n$, cioè $b = na$, $n \in N$. Ogni $[a]_r \in Na$.

Inversamente, prendo un elemento a del laterale destro. Allora dal fatto che $nR1_g$ segue che $naRa$ (per la proprietà di contruenza e per il fatto che aRa). Ovvero $na \in [a]_R$ cioè $Na \in [a]_r$. Si concude che $[a]_R = Na$.

Ora si dimostra che il laterale destro e quello sinistro coincidono. Allora $[a]_r = aN$. Sia $b \in [a]_R$, allora bRa implica $a^{-1}bRa^{-1}a = 1_g$ ovvero $a^{-1}b \in N$. Allora $b = an$, $n \in N$. Dunque la classe di equivalenza $[a]_R$ è contenuta nel laterale sinistro aN . Viceversa, per ogni $n \in aN$, allora $nR1_g$ implica che $aNRa*1_G = a$, ovvero $aN \subset [a]_R$.

Dunque si conclude che $[a]_R = aN$ e $[a]_r = Na$. Abbiamo provato che $R = d_N = s_N$.

1.9.2 Nucleo

Definizione (166 Nucleo)

Il sottogruppo $N = [1_G]_R$ si dice *nucleo* della congruenza R . In un gruppo l'intera congruenza è completamente determinata dal suo nucleo, perché conoscendo N e volendo calcolare la classe che contiene a , basta calcolare il laterale Na .

1.9.3 Sottogruppo normale

Definizione (167 Sottogruppo normale)

Un sottogruppo H di un gruppo G si dice *normale* in G se $\forall a \in G$, $Ha = aH$, ovvero $D_H = S_H$.

Osservazione (168)

Un gruppo ha sempre almeno due sottogruppi normali, cioè quelli banali. Il sottogruppo ridotto alla sola unità e l'intero gruppo G sono ovviamente normali.

Un gruppo che ha come ordine un numero primo, non ha sottogruppi non banali: questo segue dal teorema di Lagrange, perché in questo caso $o(G)$ non ha divisori e quindi non può avere sottogruppi di ordine inferiore. In questo caso il gruppo è ciclico (il sottogruppo generato da ogni elemento deve coincidere necessariamente con il gruppo, perché non può avere ordine inferiore).

Un gruppo che non ha sottogruppi non banali ha come ordine un numero primo.

Osservazione (169)

Se G è abeliano, ogni sottogruppo di G è normale (gli elementi commutano e quindi necessariamente le relazioni coincidono).

Più in generale, in un gruppo abeliano ogni sottogruppo è normale. Non vale viceversa (esempio: gruppo dei quaternioni di ordine 8).

Esempio (170)

In S_4 abbiamo considerato il gruppo trirettangolo e quello alterno che sono normali, ma ad esempio il gruppo ciclico generato da $(1,2,3,4)$ non è normale.

$$< (1,2,3,4) >= (1,2,3,4), (1,3) * (2,4), (1,4,3,2), id$$

Definizione (171 Gruppo semplice)

In generale un gruppo in cui non ci siano sottogruppi normali non banali si dice *semplice*. Attraverso i gruppi semplici si possono costruire tutti i gruppi finiti.

Esempio (172)

Il gruppo alterno su n oggetti, se $n \geq 5$ è un gruppo semplice. Questo dipende dal fatto che l'equazione generale di grado 5 non ha una formula risolutiva.

Osservazione (173)

Abbiamo provato sopra che il nucleo di una congruenza in un gruppo G è normale in G , infatti $d_N = s_N$.

Questa osservazione si inverte, infatti siamo in grado di provare la seguente

Proposizione (174)

Sia N un sottogruppo normale di G e sia R la relazione tale che $R = d_N = s_N$. Allora R è una congruenza su G e il suo nucleo è il sottogruppo N .

Dimostrazione

Per la definizione di sottogruppo normale, poiché $d_N = s_N = R$, allora due elementi $x, y \in G$ sono associati nella R se e solo se $y d_N x$, cioè $\exists n \in N$ tale che $y = nx$, $n \in N$ e $y s_N x$, cioè esiste $\bar{n}$ tale che $y = x * \bar{n}$, per opportuni $n, \bar{n} \in N$.

Proviamo che R è compatibile con l'operazione di prodotto definita su G . Siano $a, a', b, b' \in G$ tali che aRa' e bRb' . Allora $a' = n_1 * a$, $n_1 \in N$ e $b' = n_2 * b\, n_2 \in N$.

Segue che $a' * b' = n_1 * a * n_2 * b = n_1 * (a * n_2) * b$. Con la proprietà associativa ho messo in evidenza l'elemento $a * n_2$ che sta in aN ma $aN = Na$. Allora posso spostare a a destra e scrivere $a * n_2 = n_3 * a$, con $n_3 \in N$, cioè $a' * b' = n_1 * n_3 * a * b$. Allora il prodotto $a' * b'$ è associato ad ab nella R , perché $a'b'$ appartiene ad Nab .

Il nucleo N è il laterale $N * 1_G = N$. Quindi il nucleo è N . Ogni sottogruppo normale è il nucleo di una congruenza.

Se considero una qualsiasi congruenza e associo il nucleo che la determina completamente, esso è un sottogruppo normale di G . Esiste quindi una biezione tra l'in-

sieme delle congruenze su G e l'insieme dei sottogruppi normali di G . Determinare i sottogruppi normali di un gruppo equivale a determinare le congruenze.

1.9.4 Criterio per i gruppi normali

La nozione di normalità di un sottogruppo si può stabilire in seguito al seguente criterio:

Proposizione (175 Criterio per i gruppi normali)

Un sottogruppo $H \in G$ è normale se e solo se $\forall g \in G, \forall h \in H$ allora $g^{-1} * h * g \in H$. (equivalentemente, non si esce da H coniugando un qualsiasi elemento di H con un qualsiasi elemento di G).

Dimostrazione

Supponiamo che H sia normale in G , allora per ogni $g \in G$ si ha $Hg = gH$. Allora per ogni $h \in H$, se considero $h * g$ è anche un elemento del laterale sinistro e deve poter essere scritto come $g * h'$. Allora moltiplicando per l'inverso di g ottengo $g^{-1} * h * g = g^{-1} * g * h' = h' \in H$.

Viceversa, supponiamo che $g^{-1} * h * g \in H$ (condizione 1) per ogni $g \in G$ e per ogni $h \in H$. Allora $g^{-1} * h * g \in H$ implica $(g^{-1})^{-1} * h * g^{-1} \in H$ (g^{-1} è un elemento di G). Dalla prima condizione segue subito che $hg \in gH$ (lo si verifica moltiplicando a sinistra per g l'uguaglianza), allora $Hg \in gH$. Siccome per un g generico si ha $(g^{-1})^{-1} * h * g^{-1} = g * h * g^{-1} \in H$ segue che $gh \in Hg$ (questa volta si moltiplica per g a destra), ovvero che il laterale sinistro $g * H$ è contenuto nel laterale destro. Le due inclusioni $gH \subset Hg$ e $Hg \subset gH$ implicano $gH = Hg$.

Esempio (176)

Prendo G_L gruppo di tutte le applicazioni lineari invertibili rispetto all'operazione di composizione. Uno dei sottogruppi notevoli è il sottogruppo speciale lineare delle applicazioni di determinante 1 . Questo sottogruppo è normale. Infatti il determinante di $g^{-1}hg = 1$ e quindi $g^{-1}hg \in H$.

1.10 Morfismi

1.10.1 Definizione e proprietà

Definizione (177 Morfismo)

Se G, H sono due gruppi, un *morfismo* (o omomorfismo) è un'applicazione $f \colon G \to H$ che conserva il prodotto, cioè tale che per ogni $a, b \in G$ l'immagine del prodotto ab mediante f coincide con il prodotto delle immagini, cioè $f(ab) = f(a) * f(b)$.

Dalla definizione discendono le due seguenti proprietà dei morfismi:

Proposizione (178)

1. $f(1_G) = 1_H$ (non vale nei monoidi, perché dipende dalle proprietà di gruppo).
2. $\forall g \in G$ si ha $f(g^{-1}) = (f(g))^{-1} \in H$.

Dimostrazione

Devo dimostrare che $f(1_G) = 1_h$. Siccome $1_G = 1_G * 1_G$ si ha $f(1_G) = f(1_G * 1_G) = f(1_G) * f(1_G) = f(1_G) * 1_G$. Valgono le leggi di cancellazione e semplifico per $f(1_G)$, quindi rimane $1_H = f(1_G)$.

Il secondo punto segue dal primo, perché $1_H = f(1_G)$, ma per ogni $g \in G$, $1_H = f(g * g^{-1})$. Ma f conserva il prodotto, quindi $f(g^{-1} * g) = 1_H = f(g^{-1}) * f(g)$, quindi $f(g^{-1})$ è inverso di $f(g)$.

1.10.2 Tipi di morfismo

Un morfismo di gruppi può essere iniettivo, biettivo, suriettivo.

Se ho un morfismo f che è iniettivo, esso prende il nome di *monomorfismo*. Ogni elemento di H , se ha una preimmagine, ne ha una sola.

Se f è suriettivo, allora si dice che è un *epimorfismo*.

Se f è biettivo, allora si dice *isomorfismo*. Se ho un isomorfismo da G ad H ed identifico ogni elemento di H con la sua preimmagine in G , allora non c'è nessuna distinzione sulle operazioni tra i due gruppi.

Presa la classe di tutti i gruppi e considerata la relazione che associa due gruppi se e solo se sono isomorfi, essa è una relazione di equivalenza.

1.10.3 Altre proprietà

Osservazione (179)

Dati due morfismi $f_1 \colon G \to H$ e $f_2 \colon H \to K$, allora posso considerare la composizione $f_2 \circ f_1 \colon G \to K$ che è a sua volta un morfismo.

Osservazione (180)

Se $f \colon G \to H$ è un isomorfismo, allora f è biettiva quindi esiste l'inversa $f^{-1} \colon H \to G$ che è a sua volta un isomorfismo.

Dimostrazione

Devo provare che f^{-1} conserva il prodotto. Per ogni $a, b \in H$, devo provare che $f^{-1}(a) * f^{-1}(b) = f^{-1}(ab)$.

$$f(f^{-1}(a) * f^{-1}(b)) = [f \circ f^{-1}(a)] * [f \circ f^{-1}(b)] = ab$$

(questo è possibile perché f è un morfismo e $g^{-1}(a), g^{-1}(b)$ sono elementi di G) Allora applico f^{-1} a entrambi i membri di questa uguaglianza e ottengo:

$$f^{-1}[f(f^{-1}(a) * f^{-1}(b))] = f^{-1}(ab)$$
$$f^{-1}(a) * f^{-1}(b) = f^{-1}(ab)$$

(si sa che l'inversa di un'applicazione biettiva è biettiva, quindi f^{-1} è un morfismo)

1.11 Gruppi quoziente

1.11.1 Notazione

Sia ora R una congruenza in un gruppo G con nucleo uguale al sottogruppo normale N . Sappiamo che il prodotto definito su G induce un prodotto sull'insieme quoziente delle classi di equivalenza G/R . G/R ha come elementi i laterali destri (o sinistri) di N in G .

Denotiamo l'insieme quoziente G/R con G/N (perché i suoi elementi sono esprimibili mediante N). Allora G/N si chiama gruppo quoziente di G rispetto al sottogruppo normale N .

Teorema (181)

1. L'insieme quoziente G/N è un gruppo rispetto all'operazione indotta definita su G chiamata *prodotto di laterali*:

presi due laterali Na e Nb , si definisce $Na * Nb = Nab$. Questo gruppo con l'operazione si chiama *gruppo quoziente* di G rispetto al sottogruppo normale N .

1. Se consideriamo la proiezione canonica $\pi\colon G \to G/N$, definita ponendo $\pi(a) = Na, \forall a \in G$,

essa è un epimorfismo da G a G/N . Allora π in questo contesto viene chiamata *epimorfismo canonico*.

Dimostrazione

L'operazione indotta è associativa, ammette unità (la classe di equivalenza dell'unità, cioè il laterale destro che contiene l'unità, che è N). Ogni laterale Na ammette come inverso il laterale Na^{-1} che contiene l'inverso di a . Quindi l'insieme quoziente con l'operazione indotta è un gruppo.

Presi due elementi a, b devo dimostrare che la proiezione canonica $\pi(ab)$ conserva il prodotto. $\pi(a) * \pi(b) = Na * Nb = Nab = \pi(ab)$ per definizione della proiezione canonica. Un elemento generico dell'insieme quoziente ha una preimmagine in G , data da tutti gli elementi contenuti nel laterale, quindi π è suriettiva.

Osservazione (182)

Se considero un gruppo G e un qualsiasi sottogruppo normale N , il quoziente G/N è epimorfo a G (l'epimorfismo è la proiezione canonica π).

Osservazione (183)

π non è l'unico morfismo di G su G/N , la proiezione canonica si può comporre con altri isomorfismi.

1.11.2 Teorema fondamentale di omomorfismo per i gruppi

Teorema (184)

Siano G, H due gruppi e $F\colon G \to H$ un morfismo di gruppi. Allora valgono le seguenti proprietà:

1. la relazione di equivalenza $R = R_f$ sul dominio G associata all'applicazione f è una congruenza.
2. supponendo vero il punto 1, sia N il nucleo di R e sia $\pi\colon G \to G/N$ la proiezione canonica di G su G/N . Allora esiste ed è unico un morfismo $\bar{f}\colon G/N \to H$ tale che sia $f = \bar{f} \circ \pi$, ovvero tale da rendere commutativo il diagramma:

$$G \to^{\pi} G/N \to^{\bar{f}} H = G \to^{f} H$$

(per la teoria degli insiemi una tale aplicazione esiste, bisogna verificare che esiste per i gruppi)

1. $\bar{f}$ è iniettiva, cioè $\bar{f}$ è un monomorfismo ed è un isomorfismo se e solo se f è un epimorfismo.

Dimostrazione

1. Supponiamo che aRa' e bRb' , quindi $f(a) = f(a')$ e $f(b) = f(b')$, da cui segue $f(a) * f(b) = f(a') * f(b')$. Ma f è un

morfismo. quindi $f(a)*f(b) = f(ab)$. Similmente $f(a')*f(b') = f(a'b')$, quindi ab e $a'b'$ hanno la stessa immagine, quindi $abRa'b'$ e R è una congruenza. (ricordare che $R = R_f$ è la relazione tale che $a \sim b$ se e solo se $f(a) = f(b)$)

1. Per il teorema di omomorfismo per gli insiemi, sappiamo che esiste ed è unica un'applicazione $\bar{f}\colon G/N \to H$ tale che $f = \bar{f} \circ \pi$. L'applicazione $\bar{F}$ manda un elemento dell'insieme quoziente Na nell'immagine del rappresentante a ,

ed è ben definita perché N è il nucleo di R e due elementi con la stessa immagine mediante f sono in relazione mediante R e appartengono allo stesso laterale Na

. $\bar{f}$ è la funzione cercata. Bisogna dimostrare che è un morfismo. $\bar{f}(Na) = f(a)$, e $\bar{f}(Nb) = f(b)$, $\bar{f}(Na) * \bar{f}(Nb) = f(a) * f(b)$, ma f è un morfismo e conserva il prodotto. Quindi $f(a) * f(b) = f(ab) = \bar{f}(Nab)$, quindi $\bar{f}(Na * Nb)$.

1. Segue dal teorema di omomorfismo per gli insiemi, in cui l'iniettività è verificata se $R = R_f$ come in questo caso.

In particolare, in questo caso se $f(G) = H$, allora $\bar{F}$ è un isomorfismo e H è isomorfo a G/N . Viceversa, tutti e soli i gruppi H che sono immagine epimorfa di un gruppo G coincidono a meno di isomorfismi con i gruppi quozienti rispetto ai sottogruppi normali di G .

1.11.3 Nucleo di una congruenza

Definizione (185 Nucleo di un morfismo)

Il nucleo N della congruenza $R = R_f$ associata al morfismo $f\colon G \to H$, si dice *nucleo del morfismo* F e si denota con $\ker F$. Per definizione $\ker F = \{g \in G \, t.c. \, f(g) = f(1_G)\}$, ma se f è un morfismo, $f(1_G) = 1_H$. Il nucleo è l'insieme di tutte le preimmagini dell'unità di H .

1.11.4 Esempi sui morfismi

Esempio (186)

Sia $G = S_n$ gruppo simmetrico delle biezioni, sia $H = \pm 1$ il sottogruppo di $(Q^*, \dot{})$. Se $F = \delta_\sigma$ (associa a σ 1 se è pari e -1 se è dispari), è un epimorfismo di S_n sul gruppo moltiplicativo ± 1 . La funzione segno conserva il prodotto, è un epimorfismo e il nucleo è l'insieme di tutte le permutazioni pari che hanno come immagine 1 . Il gruppo alterno, essendo il nucleo di un epimorfismo, è normale in S_n .

1.11.5 Riepilogo

Se G è un gruppo ed esiste un omomorfismo $f\colon G \to H$ allora si considera il quoziente di G rispetto al nucleo di F . La proiezione canonica $\pi\colon G \to G/N$ è la mappa che a ogni elemento di G associa il laterale Na . Per il teorema di morfismo degli insiemi esiste ed è unica l'applicazione $\bar{f}$ tale che $f = \bar{f} \circ \pi$. $\bar{f}\colon G/N \to H$ è iniettiva ed è un isomorfismo solo se f è un epimorfismo da G ad H . Il teorema universale del morfismo esprime la proprietà universale della proiezione canonica.

Ogni quoziente di G rispetto a un qualsiasi sottogruppo normale è epimorfo a G .

1.11.6 Gruppo additivo degli interi

Sia $(\mathbb{Z}, +)$ il gruppo additivo degli interi. Fissato un intero n , consideriamo il sottogruppo ciclico generato da n (normale) che chiamiamo N : esso consiste di tutti i multipli di n , cioè gli interi della forma

$$\{hn,\, h \in \mathbb{Z}\} = n\mathbb{Z}$$

.

Considero tre casi distinti:

1. Se $n = 0$, il sottogruppo N è ridotto alla sola unità di $(\mathbb{Z}, +)$. Quando considero il quoziente $\mathbb{Z}/(0 * \mathbb{Z})$

esso coincide con l'intero gruppo $\mathbb{Z}$. Questo quoziente è isomorfo a G . In generale, se prendo un qualsiasi gruppo G e ne faccio il quoziente rispetto al sottogruppo contenente solo l'unità, esso è isomorfo a G .

1. se $n = 1, -1$ allora $N = \mathbb{Z}$, il gruppo quoziente di $\mathbb{Z}$ rispetto a $\mathbb{Z}$ stesso è dato da un solo elemento ed è il gruppo banale.

E' isomorfo al sottogruppo generato dall'unità di $\mathbb{Z}$.

1. Se $n \neq 0, n \neq \pm 1$, siccome il sottogruppo ciclico generato da n coincide con quello generato da $-n$, considero $n > 0$.

In questo caso gli elementi del quoziente $\frac{\mathbb{Z}}{n*\mathbb{Z}}$ sono i laterali additivi della forma $n*h$. Il laterale $a+N$ che contiene a è dato dagli elementi della forma $\{a+hn,\, h \in \mathbb{Z}\}$ che è la classe di resti di $a \mod n$. Dunque $\frac{\mathbb{Z}}{N\mathbb{Z}}$ è l'insieme delle classi di resti modulo n e l'operazione indotta su $\frac{\mathbb{Z}}{n*\mathbb{Z}}$ è la somma di laterali. La somma di due laterali $N + a + N + b = N + a + b$ cioè la somma di classi di resti modulo n . Dunque si conclude che il gruppo quoziente $\frac{\mathbb{Z}}{n\mathbb{Z}}$ con l'operazione indotta da $\mathbb{Z}$ coincide con il gruppo additivo delle classi di resti modulo n .

Un gruppo ciclico infinito è sempre isomorfo al gruppo additivo degli interi. Se consideriamo un qualsiasi sottogruppo di $(\mathbb{Z}, +)$ esso dev'essere ciclico. I gruppi che ottengo quozientando il gruppo degli interi sono a meno di isomorfismi lo stesso $\mathbb{Z}$ (ottenuto quozientando rispetto al sottogruppo banale), il sottogruppo banale (ottenuto quozientando rispetto all'intero $\mathbb{Z}$) e i gruppi additivi delle classi di resto modulo n (ottenuti quozientando rispetto ai sottogruppi ciclici generati da n). In termini di congruenze, le uniche congruenze ammesse dal sottogruppo degli interi oltre a quelle banali (identità e relazione universale) sono le congruenze modulo n per ogni fissato $n > 1$.

1.11.7 Classificazione dei gruppi ciclici

Sia G un gruppo ciclico generato da un suo elemento a . Allora ogni elemento di G si può scrivere come una potenza di a . Consideriamo la mappa $f\colon (\mathbb{Z}, +) \to (G, \cdot)$ definita ponendo per ogni $r \in \mathbb{Z}$, $f(r) = a^r$.

F è un epimorfismo perché conserva le operazioni: presi due interi r, s se considero la loro somma e ne faccio l'immagine, si ottiene $f(r+s) = a^{r+s} = a^r * a^s$ (conserva il prodotto). Per costruzione, siccome G è ciclico, ogni elemento di G si può scrivere come una potenza e quindi ha una preimmagine (suriettività).

Se f è suriettivo, $\ker f = \{r \in \mathbb{Z}\, t.c. a^r = 1_G\}$. Ci sono due possibilità:

1. a ha periodo infinito; in questo caso la funzione potenza è iniettiva l'unico r per cui $a^r = 1_G$ è $r = 0$.

Allora il quoziente $\frac{\mathbb{Z}}{\ker f} = \mathbb{Z}/0$ è isomorfo al gruppo di arrivo, ovvero G è isomorfo a $\frac{\mathbb{Z}}{0}$. Ogni gruppo ciclico infinito è isomorfo al gruppo degli interi $(\mathbb{Z}, +)$.

1. il periodo di a è $n < +\infty$. Allora

$$\ker f = \{r t.c. a^r = 1_G\}$$

.

Se $o(a) = n$, per ogni $r \neq 0\, t.c. a^r = 1_g$, allora r è un multiplo di n . Allora il nucleo è il sottogruppo ciclico $n * \mathbb{Z}$ generato da n . Se $n = 1$ ho il gruppo banale. Se $n > 1$, usando il teorema di omomorfismo si ha che G è isomorfo al quoziente di $\mathbb{Z}$ rispetto al nucleo, cioè alla classe di resti modulo n (il teorema di omomorfismo è quello che afferma l'esistenza di un morfismo $\bar{f}\colon \mathbb{Z}/n \to G$). Ogni gruppo ciclico finito di ordine $n > 1$ è isomorfo al gruppo additivo delle classi di resto modulo n .

Osservazione (187)

$(\mathbb{Z}, +)$ è un sottogruppo di $(\mathbb{Q}, +)$. Nel quoziente $\frac{\mathbb{Q}}{\mathbb{Z}}$ ogni elemento ha periodo finito. Preso un laterale del tipo $z + m/n$, sommando n volte si ottiene l'unità del quoziente, infatti si ottiene $\mathbb{Z} + m = \mathbb{Z}$. Quindi l'ordine di ogni laterale divide n .

1.11.8 Prodotto di insiemi

L'unione insiemistica di due sottogruppi non è sempre un sottogruppo.

Definizione (188 Insieme prodotto)

Siano A, B sottogruppi di G . Chiamo l'insieme prodotto l'insieme di tutti i possibili prodotti ab . Questo non è in generale un sottogruppo.

Lemma (189)

Condizione necessaria e sufficiente affinché il prodotto sia un sottogruppo è che sia permutabile, cioè che ogni elemento ab si possa scrivere come $b'a'$.

Il prodotto non è sempre un sottogruppo.

Esempio (190 Controesempio)

Se considero infatti il gruppo S_3 , il prodotto generato dai sottogruppi di due scambi distinti ha ordine 4 e questo non può essere un sottogruppo di S_3 perché 4 non divide 6 .

Esercizio (191)

In generale, se G è un gruppo finito e se A e B sono finiti, allora il prodotto è finito e l'ordine del sottogruppo prodotto è dato dalla formula:

$$O(G) = \frac{o(A) * o(B)}{O(A \cap B)}.$$

Lemma (192)

Siano N, H sottogruppi di un gruppo G e supponiamo che N sia normale in G . Allora il prodotto NH è un sottogruppo. (Inoltre, il prodotto di due sottogruppi normali è ancora normale.)

Dimostrazione

unità Il prodotto contiene ovviamente l'unità, che è contenuta in ognuno dei due sottogruppi.

chiusura per prodotto siano n_1h_1 e n_2h_2 elementi del prodotto. Allora $(n_1 * h_1)(n_2 * h_2) = n_1 * (h_1 * n_2) * h_2$. Siccome

N è normale, il laterale sinistro $h_1 * N$ coincide con il laterale destro, quindi esiste $n_3 \in N$ tale che $h_1 * n_2 = n_3 * h_1$. $n_1 * (n_3 * h_1) * h_2 = (n_1 * n_3) * (h_1 * h_2)$ che appartiene ancora a NH .

chiusura per inversi sia nh un elemento di NH .

L'inverso $(nh)^{-1} = h^{-1} * n^{-1}$ appartiene al laterale $h^{-1}N$ che coincide con $N * h^{-1}$ e questo implica che l'inverso di nh è $\bar{n} * h^{-1}$ che appartiene a NH .

1.11.9 Conseguenze del teorema di omomomrfismo

Teorema (193)

Sia G un gruppo, siano N, H sottogruppi di G e supponiamo che N sia normale. Allora N è un sottogruppo normale del prodotto NH , e l'intersezione $H \cap N$ è un sottogruppo normale di H . Il gruppo quoziente $\frac{NH}{N}$ è isomorfo al gruppo quoziente $\frac{H}{H \cap N}$.

Dimostrazione

Consideriamo l'applicazione $F\colon H \to NH/N$ definita ponendo $f(h) = Nh$, cioè ad ogni h associa il laterale che lo contiene (*nota 1*). f è suriettiva, un generico

elemento del quoziente è Nh , che è un elemento di N , cioè coincide con il laterale Nh . Allora questo elemento ha preimmagine h mediante f .

f è un morfismo, perché presi due elementi $h_1, h_2 \in H$, se calcolo $f(h_1 + h_2) = Nh_1h_2$. Ma questo per definizione di prodotto di laterali è uguale al prodotto $Nh_1 * Nh_2$ (per l'operazione di prodotto di laterali).

Dunque f è un epimorfismo da H a NH/H . Il nucleo di f è l'insieme di tutti gli elementi di H che hanno come immagine l'unità nel gruppo di arrivo, cioè è l'insieme $\{h \in Ht.c.f(h) = Nh = N\}$. Cioè sono tutti e soli gli h che stanno anche in N (il nucleo è $H \cap N$), quindi segue dal teorema di omomorfismo che il quoziente $\frac{H}{H\cap N}$ è isomorfo al gruppo di arrivo $\frac{NH}{N}$ (tesi). (Infatti per il teorema di omomorfismo l'applicazione $\bar{f}\colon \frac{H}{H\cap N} \to \frac{NH}{H}$ è un omomorfismo).

Osservazione (194)

Se considero il quoziente $\frac{NH}{N}$ i laterali sono della forma Nnh , ma $n \in N$ quindi $Nnh = Nh$.

Teorema (195)

Sia G un gruppo e siano N, H entrambi sottogruppi normali di G . Supponiamo che $N \subset H$. Allora N è normale in H e si può considerare il quoziente H/N . Questo è un sottogruppo normale del gruppo quoziente G/N e il quoziente di G/N rispetto al sottogruppo normale H/N è isomorfo a G/H , (in simboli $\frac{G/N}{H/N}$ è isomorfo a G/H , cioè posso semplificare per N).

Dimostrazione

Consideriamo l'applicazione $f\colon G/N \to G/H$ che associa a un elemento di G/N Ng un elemento Hg di G/H . Questa corrispondenza sembra dipendere dalla scelta dei rappresentanti dei laterali, ma in realtà non è così. Se cambio rappresentante, f è ben definita.

Supponiamo di cambiare rappresentante del laterale. $f(Nx) = H * x$. Allora $Hx = Hnx$. Siccome $n \in H$ per ipotesi, $hn \in H$, $hng = hg$. Quindi f è ben definita perché $N \subset H$.

f è suriettiva, perché ogni elemento di G/H ha una preimmagine. L'applicazione inoltre conserva il prodotto ed è un epimorfismo.

Il nucleo di f è l'insieme dei laterali Ng tali che $f(Ng) = Hg = 1_{G/H} = H$. Quindi $\ker F = \{Ngt.c.Hg = H\}$. Questo avviene quando $g \in H$, quindi $\ker f = \{Nh\}$ laterali di N in G e costituiscono il gruppo quoziente H/N . Allora per il teorema di omomorfismo il gruppo di partenza G/N quozientato rispetto ad H/N (nucleo) dev'essere isomorfo al gruppo di arrivo G/H .

1.12 Azioni di gruppo

1.12.1 Definizione

Definizione (196 Azione di un gruppo)

Si dice *azione* di un gruppo G su un insieme X un'applicazione $\phi\colon G \times X \to X$ che alla coppia (g, x) associa un elemento $g \cdot x$, spesso indicato semplicemente gx . Attenzione, non si tratta di una moltiplicazione (se non in particolari casi).

L'applicazione soddisfa due condizioni:

1. $$\forall x \in X,\ 1_G \cdot x = x$$
   (l'unità del gruppo opera come l'identità)
2. $$\forall g, h \in G \forall x \in X,\ (gh) \cdot x = g \cdot (h \cdot x)$$

(il prodotto opera come la composizione di due applicazioni su X)

Assegnata un'azione di G su X si dice anche che X è un G -insieme (insieme su cui G opera).

L'azione di G su X si dice *banale* se per ogni $g \in G$, e per ogni $x \in X$, $g \cdot x = x$ (se ogni elemento di G agisce come l'identità su X).

1.12.2 Biiezione tra azione di un gruppo G e omomorfismi da G al gruppo simmetrico su X

Lemma (197 Biiezione tra azioni e omomorfismi di gruppi)

Esiste una biiezione tra l'insieme delle azioni di un gruppo G sull'insieme X e l'insieme degli omomorfismi α dal gruppo G al gruppo simmetrico su X , $\alpha\colon G \to S_X$ definiti da $g \mapsto (\sigma\colon x \mapsto g \cdot x)$ (gruppo di applicazioni biettive con l'operazione di composizione).

Dimostrazione

Corrispondenza azione $\to$ omomorfismo. Data un'azione, $\phi\colon G \times X \to X$, per ogni $g \in G$ resta definita un'applicazione, che chiamo σ_g di X in se stesso definita ponendo: $\sigma_g(x) = g \cdot x$. Si noti che σ è biettiva, cioè σ_g è un elemento di S_X .

Iniettività. Supponiamo che x_1, x_2 abbiano la stessa immagine mediante σ_g , cioè che $g \cdot x_1 = g \cdot x_2$. Allora posso far agire l'inversa g^{-1} sui due elementi e ottengo: $g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot (g \cdot x_2) \longrightarrow (g^{-1} \cdot g) \cdot x_1 = (g^{-1} * g) \cdot x_2 \longrightarrow (1_g) \cdot x_1 = (1_g) \cdot x_2$. Allora $1_g \cdot x_1 = 1_g \cdot x_2$ implica $x_1 = x_2$ (per la condizione 1), allora σ_g è iniettiva.

Suriettività: ogni elemento di X ha una preimmagine per σ_g , basta porre $x = g^{-1} \cdot x$. Infatti $g \cdot (g^{-1} \cdot x) = (g \cdot g^{-1}) \cdot x = 1_G \cdot x = x$ (deriva sempre dalle condizioni 1 e 2 della definizione).

In particolare σ_g è biettiva, ed è un elemento di S_X .

Omomorfismo: Possiamo definire l'applicazione σ che a ogni elemento di G associa la permutazione σ_g su X . Questa applicazione definita ponendo, per ogni $g \in G$, $\sigma(g) = \sigma_g$ è un omomorfismo di gruppi. In altre parole, data un'azione di G su X ad essa si può associare un morfismo σ tra G e S_x descritto sopra, tale che a ogni elemento di G associa σ_g .

Dobbiamo provare che comunque scelga due elementi $g_1, g_2 \in G$, allora $\sigma(g_1 * g_2) = \sigma(g_1) * \sigma(g_2) = \sigma_{g_1} \circ \sigma_{g_2}$ (il prodotto delle immagini eseguito nel gruppo simmetrico è la composizione).

$$\sigma(g_1 g_2) = \sigma_{g_1 g_2}(x) = (g_1 g_2) \cdot x$$

Per la proprietà 2 della nozione di azione valgono le seguenti equivalenze:

$$\sigma_{g_1 g_2}(x) = g_1 \cdot g_2 \cdot x = g_1 \cdot (g_2 \cdot x) = \sigma_{g_1}(g_2 \cdot x) = \sigma_{g_1}(\sigma_{g_2}(x)) = \sigma_{g_1} \circ \sigma_{g_2}(x)$$

Allora $\sigma_{g_1 g_2}(x) = \sigma_{g_1} \circ \sigma_{g_2}(x)$ e σ è un morfismo.

Corrispondenza omomorfismo $\rightarrow$ azione: sia $\alpha \colon G \rightarrow S_X$ un omomorfismo di gruppi. Allora ponendo per ogni $g \in G$ e per ogni $x \in X$, $g \cdot x = \alpha_g(x)$, resta definita un'azione di G su X .

α_g è biettiva. Verifichiamo le proprietà della definizione di azione:

1. Vale la proprietà 1: $1_G \cdot x = f_{1_g}(x) = x = id$. Quindi 1_g opera come l'identità su X .
2. Se prendo elementi $(gh), x$ ottengo $(gh) \cdot x = g \cdot (h \cdot x) = (g \cdot h) \cdot x = f_{gh}(x) = f_g \circ f_h(x)$.

Per costruzione le corrispondenze azione $\rightarrow$ morfismo e morfismo $\rightarrow$ azione descritte sono l'una l'inversa dell'altra.

Si realizza una biiezione tra l'insieme di tutte le azioni di un gruppo G su un insieme X e gli omomorfismi di G in S_X .

In conclusione, quindi, azioni di G su X e omomorfismi $\alpha \colon G \rightarrow S_X$ sono concetti equivalenti.

1.12.3 Rappresentazione di permutazioni

Definizione (198)

Un morfismo f da un gruppo G al gruppo S_X si dice *rappresentazione di permutazioni* di G su X .

Osservazione (199)

In generale, dato un morfismo da G a H , l'immagine $f(G)$ è un sottogruppo di H . Un monomorfismo è un morfismo iniettivo. In un monomorfismo il nucleo è ridotto all'unità di G .

Vale anche viceversa: se il nucleo è ridotto alla sola unità, il morfismo è iniettivo.

Definizione (200 Gruppo di permutazioni)

Ogni sottogruppo del gruppo simmetrico su X si dice gruppo di permutazioni.

Se f ha nucleo ridotto all'unità di G , ovvero f è un monomorfismo, allora G è isomorfo alla sua immagine per il teorema di omomorfismo (infatti il quoziente $\frac{G}{\ker f} = \frac{G}{0} = G$ ed è isomorfo a H).

Definizione (201 Rappresentazione fedele)

Un morfismo f è una *rappresentazione fedele* se ha nucleo ridotto all'unità di G , ossia se è monomorfismo.

Osservazione (202)

Se in generale ho un morfismo, H potrebbe perdere vari elementi rispetto al gruppo di partenza.

1.12.4 Azioni di G su se stesso

Nel caso in cui X è finito, si ha il teorema di Cayley.

Consideriamo l'azione di G sull'insieme $X = G$ che è $f\colon G \times G \to G$ definita ponendo, per ogni coppia $(g, h) \in G \times G$, $f(g, h) = g \cdot h$, che sta ancora in G .

Se fisso g e considero la permutazione σ_g , essa è la moltiplicazione a sinistra di ogni $h \in G$ per g . Si può verificare che f è un'azione:

1. $1_G \cdot h$ è il prodotto dell'unità per l'elemento di G , che è ancora uguale ad h .
2. Se prendo g_1, g_2 e calcolo $(g_1 g_2) \cdot h$ ottengo $(g_1 g_2) \cdot h \in G = g_1(g_2 h) = g_1 \cdot (g_2 \cdot h)$

Per ogni fissato g la permutazione σ_g manda ogni elemento $h \in G$ nel prodotto gh , cioè è la moltiplicazione a sinistra per g degli elementi $h \in G$. A ogni elemento di g viene associata la permutazione σ_g sugli elementi di G .

Definizione (203 Rappresentazione regolare sinistra)

Il morfismo $\sigma\colon G \to S_G$ si dice *rappresentazione regolare sinistra* di G .

1.12.5 Proprietà della rappresentazione regolare

σ è un monomorfismo, ed è una rappresentazione fedele del gruppo G nel gruppo simmetrico S_G infatti $\ker \sigma = 1_G$.

$$\ker \sigma = \{g \in G | \sigma(g) = \sigma_g = 1_{S_G} = id\}$$

Osserviamo che se σ_g è l'identità su G , deve essere $gh = h \forall h \in G$. Con le leggi di cancellazione si ha $g = 1_G$. Dunque $\ker \sigma = 1_G$ e si ha un monomorfismo. (se considero la permutazione σ_g , se g non è l'unità nessun elemento è fissato). Abbiamo provato che $\forall g \neq id$ la permutazione σ_g è priva di punti fissi.

1.12.6 Teorema di Cayley

Nel caso in cui G sia un gruppo finito si può enunciare il seguente teorema riguardante la rappresentazione regolare.

Teorema (204 Teorema di Cayley)

Sia G un gruppo finito di ordine n , allora esiste un momomorfismo σ da G al gruppo simmetrico S_n tale che il gruppo $\sigma(G)$ (che è isomorfo a G) risulta costituito da permutazioni $\sigma_g = \sigma(g)$ tali che siano prive di punti fissi e decomponibili nel prodotto di n/r cicli a due a due disgiunti di lunghezza r , dove $r = o(g)$.

Dimostrazione

Il morfismo cercato σ è la rappresentazione regolare sinistra; è iniettivo quindi l'immagine di G mediante σ è isomorfa a G o equivalentemente è una rappresentazione fedele di G .

Proviamo che $\sigma(g)$ è una permutazione priva di punti fissi e scrivo come agisce sugli elementi:

$$\sigma_g(h) = (h, gh, g^2h, g^3h, g^{r-1}h, g^r h)$$

infatti se r è il periodo di g , $g^r = 1_G$ e torno in h e il ciclo si chiude.

Questo è un ciclo di lunghezza r : l'immagine di un elemento si ottiene moltiplicandolo a sinistra per g . Se $n = r$ non ci sono altri cicli (il numero di cicli è $n/r = 1$).

Altrimenti prendo un nuovo elemento $h_1 \in G$ e scrivo il ciclo:

$$\sigma_g(h_1) = (h_1, gh_1, g^{r-1}h_1, g^r h_1)$$

Anche questo ciclo è di lunghezza r .

Esiste anche una rappresentazione regolare destra. Cerco un morfismo σ' da G al gruppo simmetrico S_G dove $\sigma' g$ è la permutazione sugli elementi di G che ottengo moltiplicando a destra gli elementi di G per g^{-1} . Solo in questo modo il morfismo è ben definito (deriva dal fatto di usare gli operatori a destra).

1.13 Classi di coniugio

1.13.1 Definizione e osservazioni

Definizione (205 Coniugato)

Si consideri l'azione $\phi\colon G \times G \to G$ definita associando alla coppia (g,h) di elementi di G l'elemento $h^g = ghg^{-1}$. Questo elemento si chiama il *coniugato* di h mediante g .

Verifico che ϕ sia un'azione e che sono soddisfatte le due proprietà:

1. $1_g \cdot h = 1_g h (1_g)^{-1} = h$
2. $$(g_1 g_2) \cdot h = (g_1 g_2) h (g_1 g_2)^{-1} = g_1 (g_2 h g_2^{-1}) g_1^{-1}$$ $$= g_1 (g_2 \cdot h) g^{-1} = g_1 \cdot (g_2 \cdot h)$$

Il morfismo associato in è definito, per ogni g in G , $in_g = in(g)$. E' la permutazione che a ogni elemento associa $g \cdot h$ uguale al coniugato mediante l'elemento g .

Ad h viene associata l'immagine ghg^{-1} . Se σ denota la rappresentazione regolare, questo equivale a fare $\sigma_g \circ \sigma'(g)$.

1.13.2 in_g come automorfismo

Osservazione (206)

La permutazione in_g è un isomorfismo di G in sé, perché conserva il prodotto.

$$in_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = (gag^{-1})(gbg^{-1}) = in_g(a) * in_g(b)$$

(moltiplicare per $g^{-1} * g$ equivale a moltiplicare per l'unità).

Rispetto alla composizione di morfismi, l'insieme di tutti gli automorfismi su un gruppo G è un gruppo. In altre parole, il morfismo che a ogni g associa σ_g con $\sigma_g\colon G \to G$ tale che $\sigma_g(h) = ghg^{-1}$ dà luogo a un sottogruppo del gruppo $autG$ degli automorfismi di G in sé.

Esercizio (207)

Provare che in_g è un sottogruppo normale di $autG$.

Definizione (208 Automorfismi interni)

Gli automorfismi in_g di G realizzati mediante coniugio si chiamano *interni*. In_G è un sottogruppo degli automorfismi interni di G .

Si può considerare il quoziente $\frac{autG}{in_G}$ l'automorfo esterno di G .

Teorema (209)

Preso il gruppo simmetrico S_n per ogni n fissato, esso non ha automorfismi esterni, tranne nel caso in cui $n = 6$.

1.13.3 Centro di in_g

Il nucleo del morfismo In che a g associa l'azione $\sigma_g = ghg^{-1}$ è l'insieme degli elementi $g \in G$ tali che $in_g = id$, cioè tali che $ghg^{-1} = h$ per ogni $h \in H$, che equivale a dire $gh = hg$ (h commuta con g).

Definizione (210 Centro di in_g)

Il nucleo del morfismo in_g è l'insieme di tutti e soli gli $h \in G$ che sono permutabili con ogni elemento di G . Questo è il *centro* di G che si indica con Z_g .

Osservazione (211)

Il centro, essendo un nucleo, è un gruppo normale.

$z_g = G$ se e solo se il gruppo è abeliano e in tal caso l'azione per coniugio è banale.

Esempio (212)

Considero il gruppo $GL(n, F)$ gruppo generale lineare di tutte le matrici invertibili. Il centro è ridotto ai multipli dell'identità.

In alcuni gruppi in_g è iniettivo.

Esempio (213)

In S_n con $n > 2$ il centro è ridotto all'identità. Si verifica calcolando le classi di coniugio.

Definizione (214 Sottogruppo coniugato)

Se prendo un sottogruppo H di un gruppo G , faccio agire gli elementi di G associando ad H il sottogruppo gHg^{-1} . Tale sottogruppo è chiamato *sottogruppo coniugato* di H mediante l'elemento g .

1.14 Orbite e stabilizzatori

1.14.1 Definizioni

Definizione (215 Orbita e stabilizzatore)

Data un'azione di un gruppo G su un insieme X , per ogni elemento $x \in X$ definiamo:

1. $Gx = \{g \cdot x | g \in G\}$.

Questo è l'insieme di tutte le immagini mediante σ_g del punto x al variare di g e si chiama *orbita* contenente x per il gruppo G . E' un sottoinsieme di X .

1. $G_x = \{g \in G | g \cdot x = x\}$. E' l'insieme di tutti e soli gli elementi di G tali che σ_g fissa x .

E' un sottoinsieme (e un sottogruppo) di G e si chiama *stabilizzatore* del punto x in G .

1.14.2 Stabilizzatore come sottogruppo

Osservazione (216)

Per ogni fissato $x \in X$ lo stabilizzatore G_x è un sottogruppo di G . Questo discende dagli assiomi di un'azione di gruppo.

1. $1_g \in G_x$, infatti $1_g \cdot x = x$ (per la proprietà 1 di azione di gruppo)
2. Dimostro che presi due elementi $a, b \in G_x$, allora $ab^{-1} \in G_x$, cioè se a, b fissano x , anche ab^{-1} fissa x .

$$ab^{-1} \cdot x = ab^{-1} \cdot (b \cdot x)$$

($b \cdot x$ è ancora uguale a x perché b in g_x)

$$= (ab^{-1}b) \cdot x = a \cdot x = x$$

(perché anche $a \in G_x$)

Quindi lo stabilizzatore di un punto di x in G è un sottogruppo per il criterio.

1.14.3 Orbite come classi di equivalenza

Osservazione (217)

Le orbite di G su X determinano una partizione di X , allora posso definire una relazione di equivalenza le cui classi sono le orbite.

Consideriamo sull'insieme X la relazione $\sim$ definita ponendo per $x, y \in X$, $x \sim y$ se e solo se esiste un elemento $g \in G$ tale che $y = g \cdot x$. Questo equivale a dire che gli elementi associati a x sono gli elementi dell'orbita.

Mostriamo che $\sim$ è una relazione di equivalenza su X :

Riflessività ogni x è associato a se stesso. L'elemento di g tale che $g \cdot x = x$ è l'unità.

Simmetria se $x \sim y$, allora $y \sim x$. Se $x \sim y$, esiste $y \in X$ tale che $y = g \cdot x$.

Allora $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x)$ e per le proprietà di azione di gruppo si ha $(g * g^{-1}) \cdot x = 1_g \cdot x = x$. Questo significa che $y \sim x$ se pongo $g = g^{-1}$.

Transitività se $x \sim y$, allora esiste g_1 tale che $y = g_1 \cdot x$. Se $y \sim z$, allora $y \cdot g_2 = z$.

Allora $g_2 \cdot y = g_2 g_1 \cdot x = (g_2 g_1) \cdot x$, ovvero vale la proprietà transitiva perché esiste $g_1 g_2 \in G$ tale che $g_1 g_2 \cdot x = z$.

La classe di equivalenza $[x]_\sim$ è l'orbita Gx per come $\sim$ è definita. Pertanto si può concludere che se considero l'insieme delle G -orbite sull'insieme X , esso costituisce una partizione dell'insieme dei punti di X . Sia $\{X_i,\, i \in I\}$ la partizione e in ciascuna orbita scegliamo un rappresentante. Sia $\{x_i,\, i \in I\}$ un insieme completo di rappresentanti per le G -orbite su X , cioè per $\{G_i\}$. Allora l'insieme $X = \bigcup\{X_i\}_{i\in I} = \bigcup_{i\in I} G.x_i$. La cardinalità di X è la somma delle cardinalità delle orbite.

Osservazione (218)

Se la cardinalità di I è 1, ovvero se c'è una sola G -orbita su X , allora presi due elementi $\alpha, \beta \in X$ esiste sempre un elemento g tale che $g \cdot \alpha = \beta$. Diremo che l'azione di G su X è *transitiva*. (per moltiplicazioni a sinistra si può passare da un elemento di G all'altro).

Nel caso della rappresentazione regolare lo stabilizzatore di un punto è ridotto all'unità di G .

1.14.4 Numero dei laterali

Osservazione (219)

Se ho un gruppo G e un suo sottogruppo H , allora possiamo considerare i laterali sinistri e destri di H in G . Se H è normale, le due partizioni coincidono. Se G è un gruppo finito, il numero dei laterali sinistri è uguale a quello dei laterali destri, anche se il sottogruppo non è normale (per il teorema di Lagrange).

Questo è vero in generale: dato un gruppo anche infinito G e un suo sottogruppo H (non necessariamente normale), l'insieme dei laterali sinistri $G|H$ e quello dei laterali destri $H|G$ in G hanno la stessa cardinalità.

Infatti se si considera la biezione di G in sé che associa al laterale sinistro gH il laterale destro Hg^{-1} è una biezione tra $G|H$ e $H|G$. Questa corrispondenza non dipende dalla scelta dei rappresentanti. Infatti si ha:

$$ghH \to Hh^{-1}g^{-1} = H(gh)^{-1}$$

L'applicazione è ben definita. Lo stesso non si può dire per la corrispondenza che a gH associa Hg .

Definizione (220 Indice)

La cardinalità comune a $G|H$ e $H|G$ si dice *indice* del sottogruppo H in G e si denota con $G : H$. (questo è ovvio nel caso in cui G è finito).

Osservazione (221)

Per il teorema di Lagrange, l'indice del sottogruppo H in G è uguale a $\frac{O(G)}{O(H)}$. (quoziente fra ordine del gruppo e ordine del sottogruppo)

1.14.5 Legame tra laterali e orbite

Proposizione (222)

Sia ϕ: $G \times X \to X$ un'azione di G sull'insieme X . Per ogni $x \in X$ vi è una bieziione fra l'insieme $G|G_x$ (insieme dei laterali sinistri dello stabilizzatore G_x in G) e l'orbita $G.x$. In altre parole la cardinalità $|Gx|$ dell'orbita è uguale alla cardinalità di $G|G_x$ che è l'indice $G : G_x$

Nel caso di G finito, l'ordine di un'orbita è uguale al quoziente tra l'ordine di G e l'ordine dello stabilizzatore G_x .

Dimostrazione

Sia $g \in G$ e supponiamo che $g \cdot x = h \cdot x$ per un altro elemento $h \in G$. Allora $g \cdot x = h \cdot x$ se e solo se $h^{-1} \cdot (g. \cdot x) = h^{-1} \cdot (h \cdot x)$ (faccio agire h^{-1} su entrambi i membri). Quindi $h^{-1} \cdot g \cdot x = (h^{-1} \cdot h) \cdot x = (h^{-1}h) \cdot x$ quindi $(h^{-1}g) \cdot x = x$ se e solo se $h^{-1}g \in G_x$. E questa condizione implica che $gG_x = hG_x$ per la condizione di uguaglianza tra i laterali.

In altre parole, l'applicazione da $G|G_x$ all'orbita $G.x$ definita associando a g l'elemento $g \cdot x$ induce una biezione fra $G|G_x$ e l'orbita Gx .

Quindi le immagini distinte $g \cdot x$ sono tante quante i laterali dello stabilizzatore G_x in G , perché se due elementi di un'orbita coincidono, anche i rispettivi laterali dello stabilizzatore coincidono.

1.14.6 Equazione delle orbite

Corollario (223 equazione delle orbite)

Supponiamo X un insieme di cardinalità finita n su cui G opera. Sia $X = \bigcup_{i=1}^{t} X_i$ la partizione di X nelle G -orbite X_i . Allora se scelgo $\{x_i, \}_{i=1}^{t}$ un insieme completo di rappresentanti per le G -orbite su X , allora l'ordine di x_n è uguale alla cardinalità di X e si ha

$$o(x_n) = |X| = \sum_{i=1}^{t} |G.x_i| = \sum_{i=1}^{t} (G : G_{x_i})$$

(l'ultima espressione corrisponde al numero dei laterali dello stabilizzatore).

1.14.7 Esempi: rappresentazione regolare sinistra

Consideriamo la rappresentazione regolare sinistra, cioè l'azione da $G \times G$ a G che a ogni coppia ordinata (g, h) associa $g.h = gh$ (per ogni $g \in G$, σ_g è data dalla moltiplicazione a sinistra per g). Se considero $h \in X$ e considero $G.h$, l'orbita è $G.h = \{gh = \sigma_g(h)\, g \in G\}$. In quest'azione c'è un'unica orbita che è G , l'azione è transitiva. Lo stabilizzante $G_h = \{g \in Gt.c.g.h = h\}$ quindi è ridotto all'unità di G .

Osservazione (224)

Posso considerare un elemento $g \in G$ e sia H il sottogruppo ciclico generato da g . Consideriamo la restrizione della rappresentazione regolare di G ad H , allora per ogni $x \in G$, l'orbita che contiene x è il laterale destro Hx . La cardinalità di questo laterale è uguale all'indice dello stabilizzante di x nel gruppo H .

Infatti, lo stabilizzante è ridotto all'unità di G e ha ordine 1 , quindi il quoziente $\frac{o(H)}{|H_x|} = o(H)$.

Se considero la rappresentazione regolare ristretta al sottogruppo H , ogni orbita ha cardinalità uguale all'ordine di H .

Se G è un gruppo finito, l'azione che g realizza per moltiplicazione a sinistra è decomponibile nel prodotto di cicli disgiunti e la loro lunghezza è uguale al periodo di g ,

Se $o(g) = r$, ogni orbita ha lunghezza $r = o(g)$.

In particolare, se G è un gruppo finito, la lunghezza di ogni G -orbita su X è uguale al quoziente fra l'ordine finito di G e l'ordine dello stabilizzatore di un punto.

1.14.8 Classi di coniugio e centralizzante

Definizione (225 Classe di coniugio)

Ho un'applicazione $f\colon G \times G \to G$ che alla coppia (g, h) associa $h^g = ghg^{-1}$, cioè il coniugato dell'elemento di H mediante g .

Se prendo un elemento h l'orbita Gh è l'insieme $\{ghg^{-1},\ g \in G\}$. Ogni orbita è una classe di equivalenza e viene definita *classe di coniugio* di $h \in G$.

Definizione (226 Centralizzante)

Lo stabilizzatore $G_h = \{g \in G | ghg^{-1} = h\} = \{g \in G | gh = hg\}$, cioè sono tutti e soli gli elementi di G che commutano con l'elemento h . Questo sottogruppo si denota con C_G e si chiama *centralizzante* di h in G . E' un sottogruppo essendo uno stabilizzatore.

La cardinalità di Gh è uguale all'indice del centralizzante di G in H . In particolare, se G è un gruppo finito, ogni classe di coniugio ha ordine $\frac{O(G)}{O(C)}$. L'ordine dello stabilizzatore è un divisore dell'ordine del gruppo. La cardinalità di Gh è uguale a 1 se e solo se il centralizzante in G dell'elemento h coincide con l'intero gruppo e quindi se h commuta con tutti gli elementi di G . In questo caso le orbite contengono un solo elemento, che è un elemento del centro di G , indicato con Z_G oppure con $Z(G)$.

1.14.9 Equazione delle classi

Proposizione (227 Equazione delle classi)

Sia G un gruppo finito e sia $\{x_1, x_2, x_s\}$ un insieme completo di rappresentanti per le classi di coniugio di G non centrali, cioè contenute in $G \setminus Z_G$ e sono $s \leq t$. (le classi di coniugio centrali sono quelle che sono costituite da un oggetto solo, perché in questo caso l'ordine dello stabilizzatore è uguale all'ordine del gruppo). Allora:

$$O(G) = O_{Z_G} + \sum_{i=1}^{s} \frac{O(G)}{O(G_{x_i})},$$

cioè l'ordine del gruppo è la somma degli ordini delle classi di coniugio non centrali e del numero di elementi del centro. Ogni classe ha lunghezza pari all'ordine di G diviso l'ordine del centralizzante di un rappresentante.

Riassumendo, il centro si può definire come l'insieme degli elementi $h \in G$ che commutano con tutti gli elementi di G . Invece il centralizzante, dato un elemento h , è l'insieme degli elementi di G che commutano con h .

Esercizio (228)

Supponiamo di avere un gruppo finito che ha potenza uguale a un numero primo (p -gruppo finito). In questo gruppo il centro è più grande della sola unità.

Il fatto che il centro non può essere ridotto a 1 si ricava dall'equazione delle classi. Infatti, per quest'equazione

$$O(Z_G) = O(G) - \sum_{i=1}^{s} \frac{O(G)}{O(G_{x_i})}$$

In ogni gruppo ciclico finito esiste per ogni divisore dell'ordine uno e un solo sottogruppo che ha come ordine quel divisore. Ma se G ha come ordine un numero primo, ha solo due sottogruppi banali. Quindi $\frac{o(G)}{o(G_{x_i})} = 1$. Allora necessariamente ci sono orbite con un elemento solo.

1.14.10 Azione per coniugio sui sottogruppi

Sia G un gruppo e sia X l'insieme dei sottogruppi di G . Allora possiamo definire un'azione $G \times X \to X$ ponendo $\forall g \in G$, $\forall H$ sottogruppo di G , $H^g = \{h^g, \forall h \in H\} = \{gHg^{-1}, \forall h \in H\}$ (è immediato verificare che gHg^{-1} è un sottogruppo di G).

Sono soddisfatti i due assiomi di azione:

1. $1_g \cdot H = 1_g H (1_g)^{-1} = H$
2. Siano $g_1, g_2 \in G$, allora $g_1 \cdot (g_2 \cdot h) = g_1 \cdot (g_2 h g_2^{-1}) = g_1 g_2 h g_2^{-1} g_1^{-1} = (g_1 g_2) H (g_1 g_2)^{-1} = (g_1 g_2) \cdot h, \quad \forall h \in H$ (operatorialità)

L'orbita GH è l'insieme $\{h^g\}$, cioè l'insieme dei coniugati di H mediante gli elementi di G , della forma $\{gHg^{-1}, g \in G\}$ (classe di coniugio del sottogruppo H).

Definizione (229 Normalizzante)

Lo stabilizzatore G_H è definito come $G_H = \{g \in G | H^g = H\} = \{g \in G | gHg^{-1} = H\}$. Questo stabilizzatore viene denotato con $N_G(H)$ e si chiama *normalizzante* del sottogruppo H in G . E' il più grande sottogruppo di G in cui H è normale.

Per l'equazione delle orbite sappiamo che la cardinalità dell'orbita che contiene H $G.H$ è uguale alla cardinalità dell'insieme dei laterali $G : N_G(H)$. La lunghezza dell'orbita è un divisore dell'ordine di G ed è uguale al quoziente tra l'ordine di G e l'ordine del normalizzante.

1.15 Teoremi di Sylow

1.15.1 Proposizione introduttiva

Proposizione (230)

Sia G un gruppo finito di ordine m e sia p un primo tale che $m = p^a * n$, per qualche $a > 0$ (sia p un divisore primo dell'ordine del gruppo). Denotiamo con $N(p^a)$ il numero dei sottogruppi di G di ordine p^a . Allora $N(p^a)$ è congruo a 1 modulo p ed è maggiore di 0 .

Dimostrazione

Cardinalità di X : Sia X l'insieme di tutti i sottoinsiemi $S \in G$ tali che $O(S) = p^a$. La cardinalità di X è data da $\binom{m}{p^a} = \binom{p^a * n}{p^a} = \binom{o(G)}{o(S)}$.

Consideriamo l'azione di G su X definita da $(g, S) \mapsto g.S = gS = \{gs,\ s \in S\}$.

Si può verificare che valgono le proprietà di azione.

Quest'azione dà luogo a una partizione in G -orbite dei sottoinsiemi. In ciascuna orbita si può scegliere un rappresentante.

Sia $\{S_i\}$ un insieme completo di rappresentanti per le G -orbite sull'insieme X . Allora per l'equazione delle orbite $|X| = \sum_i |G.S_i|$.

Stabilizzatore: Poniamo $G_i = G_{S_i}$ (lo stabilizzatore di S_i in G).

Allora poiché $G_i = \{g \in G t.c. g.S_i = S_i\}$, sicuramente S_i è unione insiemistica di laterali destri del sottogruppo $G_i \in G$, infatti:

$$S_i = \{s_{i1}, s_{ir_i}\} = G_i * S_i = \bigcup_{j=1}^{r_i} G_i * s_{ij}$$

Sia $S_i = \bigcup_{j=1}^{r_i} G_i * s_{ij}$, $s_{ij} \in S_i$. Ne segue che l'ordine di S_i che è p^a è uguale a $p^a = |S_i| = \sum_{j=1}^{r_i} |G_i * s_{ij}| = o(G_i) * r_i$, da cui $o(G_i)$ è un divisore di p^a ed è $p^{b_i} \leq p^a$.

Se $b_i < a$, allora la cardinalità dell'orbita è uguale al rapporto tra l'ordine di G e l'ordine dello stabilizzatore G_i . Quindi si ha:

$$|G.S_i| = \frac{|G|}{|G_i|} =$$

$$= (m)/(p^{b_i}) = \frac{n * p^a}{p^{b_i}} = p^{a-b_i} * n \equiv 0 \mod pn$$

. (è divisibile per pn).

Invece se $b_i = a$ si ha

$$\frac{p^a * n}{p^a} = n \not\equiv 0 \mod pn$$

Possiamo eliminare dalla 1 i termini congrui a 0 modulo pn ottenendo:

$$|X| \equiv \binom{p^a * n}{p^a} \equiv \sum_{|G.S_i|=n} |G.S_i| \mod pn$$

$$|X| \equiv |G.S_i| \mod pn$$

dove i sono le orbite di lunghezza n .

Osservazione (231)

Se prendo un'orbita di lunghezza $|G.S_i| = n$, allora $b_i = a$ e quindi l'ordine dello stabilizzatore G_i è p^a (lo stabilizzatore ha ordine uguale al numero delle orbite). Il sottogruppo G_i e il sottoinsieme S_i hanno lo stesso ordine.

Sottogruppo coniugato: $O(S_i) = O(G_i)$ e quindi $r_i = 1$ (deriva dalla relazione $|G.S_i| = |G_i| * r_i$). Quindi c'è un solo laterale e $S_i = G_i * s_i$. Segue che $(s_i)^{-1}S_i = (s_i)^{-1}G_i s_i$. Siccome G_i è un sottogruppo, questo è il coniugato di G_i mediante s_i . Ho un sottogruppo di G di ordine p^a contenuto nell'orbita $g.S_i$, che chiamo b_i .

Biezione tra orbite e laterali: Quindi $g.S_i = \bigcup\{g * b_i\}$ cioè l'orbita $g.S_i$ è unione dei laterali sinistri gb_i al variare di g in G . Quindi l'orbita può essere scritta come il sottoinsieme dei laterali del sottogruppo $b_i \in G$.

Inversamente, se suppongo che ci sia un sottogruppo U di ordine p^a e considero i suoi laterali sinistri che sono un'orbita per l'azione, ad esso corrisponde una G -orbita O data da $\{gU, g \in G\}$ di lunghezza n .

In conclusione: se ho un'orbita di lunghezza n , essa è costituita dai laterali sinistri del sottogruppo di ordine p^a di G . Se esiste un sottogruppo di ordine p^a , l'orbita ha lunghezza n .

Si può costruire una biezione tra i sottogruppi di G di ordine p^a e le orbite di lunghezza n .

Se immagino di avere un sottogruppo U di G di ordine p^a , posso associargli l'orbita di tutti i laterali sinistri.

Lemma (232)

Supponiamo che esistano due sottogruppi distinti U_1 e U_2 di ordine P^a , allora le orbite $O_1 = \{gU_1, g \in G\}$ e $O_2 = \{gU_2, g \in G\}$ associate sono distinte.

Dimostrazione

Supponiamo per assurdo che l'orbita sia la stessa. Allora U_1 sta in O_1 e deve essere uguale a un elemento di O_2 , quindi dev'essere $U_1 = gU_2$. Ma preso un laterale gH di un sottogruppo H , questo è un sottogruppo solo se coincide con H stesso. Allora l'unico elemento di O_2 che può essere uguale a U_1 è U_2 , e questa è una contraddizione perché per ipotesi $U_1 \neq U_2$.

Conseguenze: in forza di queste osservazioni, deduciamo che il numero delle G -orbite su X aventi lunghezza n è uguale al numero dei sottogruppi di G di ordine p^a . (le orbite distinte di lunghezza n corrispondono ai sottogruppi di ordine p^a e sono tutte disgiunte).

La cardinalità di X è congrua modulo pn alla somma delle cardinalità orbite di lunghezza n .

allora

$$|X| = \binom{p^a * n}{p^a} \equiv n * N(p^a) \mod pn$$

Gruppi ciclici: Questa formula dev'essere vera per ogni gruppo G , e quindi anche nel caso in cui G è un gruppo ciclico finito.

Per questi gruppi il teorema di lagrange si inverte: se G è ciclico, $N(p^a) = 1$, perché per ogni divisore del gruppo esiste un unico sottogruppo che ha come ordine quel divisore, e dunque si ottiene

$$|X| = \binom{p^a * n}{p^a} \equiv n \mod pn$$

Conclusione: Considero quindi le due disuguaglianze:

1. $$|X| = \binom{p^a * n}{p^a} \equiv n * N(p^a) \mod pn$$
2. $$|X| = \binom{p^a * n}{p^a} \equiv n \mod pn$$

quindi unendo le due congruenze per la proprietà transitiva:

$$n * N(p^a) \equiv n \mod pn$$

semplificando per n :

$$N(p^a) \equiv 1 \mod p$$

1.15.2 Primo teorema di Silow

Definizione (233 p-sottogruppo di Sylow)

Sia G un gruppo finito di ordine $p^a * n$ ove p è un primo e $p \nmid n$ (p^a è la massima potenza di p che divide l'ordine del gruppo). Un sottogruppo P di G di ordine p^a si dice *p -sottogruppo di Sylow* di G .

Dalla proposizione precedente segue come corollario il primo teorema di Sylow:

Corollario (234 Primo teorema di Sylow)

Per ogni primo p ogni gruppo finito contiene i sottogruppi di Sylow e il numero n_p dei p -sottogruppi di Sylow è congruo a 1 modulo p .

1.15.3 Corollario di Cauchy

Un'altra conseguenza della proposizione è il corollario di Cauchy.

Corollario (235 Corollario di Cauchy)

Se p è un primo che divide l'ordine del gruppo G , il gruppo G contiene elementi di periodo p (è il caso particolare in cui la potenza di p che divide G è $a = 1$).

Definizione (236 p-gruppo)

Sia p un primo. Un gruppo G non necessariamente finito si dice *p -gruppo* se ogni suo elemento ha come periodo una potenza di p .

Esercizio (237)

Nel caso finito, un gruppo G è un p -gruppo se e solo se ha come ordine una potenza di p .

Supponiamo che G abbia come ordine una potenza di p : allora G è un p -gruppo, perché ogni suo elemento ha come periodo un divisore dell'ordine di G , cioè una potenza di p .

Viceversa, se G è un p -gruppo, supponiamo che per assurdo non abbia come ordine una potenza di p . Allora il suo ordine deve essere divisibile per un altro primo $q \neq p$, ma per il corollario di Cauchy questo significa che G contiene elementi di periodo q diverso da una potenza di p e quindi non sarebbe un p -gruppo.

1.15.4 Secondo teorema di Sylow

Teorema (238 Secondo teorema di Sylow)

Sia G un gruppo finito e p un primo. Allora:

1. Se P è un p -gruppo di Sylow, e U è un qualsiasi p -sottogruppo di G con ordine una potenza di p , allora esiste un elemento

$g \in G$ tale che U sia contenuto nel coniugato gPg^{-1} . (ogni P -sottogruppo di G è contenuto in un P -sylow, inoltre si può considerare U come un sottogruppo del coniugato di P)

1. I p -sottogruppi di Sylow di G formano una classe di coniugio di sottogruppi di G (un'orbita), in

particolare $n_p \mid \frac{o(G)}{o(P)}$, dove n_p è il numero dei p -sottogruppi di Sylow.

Dimostrazione

1. Consideriamo l'azione di U per moltiplicazione a sinistra sui laterali sinistri di P , cioè l'azione di U sull'insieme $G|P$.

$\sigma \colon U \times G|p \to G|p$ definita ponendo per ogni $u \in U$, $u.gP = ugP$. In altre parole $\sigma_u(gP) = ugP$.

Si può verificare che è un'azione del p -sottogruppo U sui laterali sinistri di U in G .

Poiché U è un P -gruppo, la lunghezza di ogni u -orbita dev'essere un divisore dell'ordine di U e quindi una potenza di p . (perché ogni u ha periodo una potenza di p). D'altronde, poiché p è un P -Sylow di G , il numero dei laterali sinistri di P in G è coprimo con p (l'indice di un Sylow è uguale a $O(G)/o(p) = nt.c.p \nmid n$).

Ne segue che esiste almeno una u -orbita su $G|P$ di lunghezza 1 , ovvero esiste almeno un laterale sinistro gP di P in G tale che costituisca da solo un'orbita di lunghezza 1 . Quindi per ogni $u \in U$, $gp = ugp$ per ogni $u \in U$. Segue che $uP = ugP$ per ogni $u \in U$. e quindi ug appartiene a gP .

Moltiplicando a destra per l'inverso di g , u appartiene a gPg^{-1} , cioè Sta nel coniugati di P per ogni $u \in U$, quindi U è contenuto in gPg^{-1} .

1. Il punto 2 segue subito dall'1. Se prendo un sottogruppo dello stesso ordine di P , allora U è contenuto in qualche coniugato di P e quindi U è uguale a gPg^{-1} .

I P -Sylow costituiscono un'intera G -orbita.

Un p -sottogruppo di Sylow è unico del suo ordine se e solo se è normale in G .

1.15.5 Riepilogo

Se G è un gruppo finito il cui ordine è $o(G) = p^a * n$ dove p è un divisore primo di $o(G)$ e p è primo con n , allora esistono dei sottogruppi $P \in G$ di ordine p^a . Essi si chiamano P -sottogruppi di Sylow. Il numero n_p di questi sottogruppi è congruo a 1 modulo p e divide l'indice di un P-Sylow, cioè divide $\frac{O(G)}{O(P)}$.

Per il secondo teorema di Sylow, se U è un sottogruppo di G dove $O(U)$ è una potenza di P (U è un p-sottogruppo) allora esiste $g \in G$ tale che $U \in gPg^{-1}$ dove P è un P-Sylow di G .

In particolare, i P -sottogruppi di Sylow di G sono tutti tra loro coniugati e formano una classe completa di coniugio di G .

Se U è un P-Sylow, allora $U = gPg^{-1}$ perché ha ordine uguale a gPg^{-1} . Il numero esatto di sottogruppi di G è uguale all'indice del normalizzante di P in G .

Consideriamo il gruppo $Gl(n, F)$. Supponiamo che f sia finito. Si può provare che un campo finito ha necessariamente come ordine la potenza di un primo. Supponiamo che F abbia ordine p^a . Prendendo le matrici unitriangolari alte, esse formano un P-sottogruppo di Sylow.

Per determinare l'ordine di $Gl(n, F)$ basta prendere tutte le matrici lineari: esse sono determinate univocamente dal fatto che presa una base, si decide quali immagini hanno i vettori della base. Se $o(f) = p^q$, l'immagine del primo vettore di una base fissata può essere scelta tra q^{n-1} vettori (non il vettore nullo). Per il secondo si può scegliere tra q^{n-q} vettori (vanno scartati i vettori linearmente dipendenti agli altri).

$$q^{n*q^{n-1}}$$

si raccoglie la massima potenza di p che divide il prodotto e quello che si ottiene è uguale all'ordine del sottogruppo delle matrici triangolari.

Capitolo 2

Fonti per testo e immagini; autori; licenze

2.1 Testo

- **Corso:Algebra Gruppi (Unimib)/Gruppi/Semigruppi e Monoidi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Semigruppi_e_Monoidi?oldid=48171 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Gruppi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Gruppi?oldid=48170 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Sottogruppo** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Sottogruppo?oldid=48413 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Esempi di gruppi e sottogruppi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Esempi_di_gruppi_e_sottogruppi?oldid=48488 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Gruppi di trasformazioni** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Gruppi_di_trasformazioni?oldid=48080 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Congruenze** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Congruenze?oldid=48426 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Sottogruppo generato da un sottoinsieme** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Sottogruppo_generato_da_un_sottoinsieme?oldid=48201 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Classi laterali di un sottogruppo** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Classi_laterali_di_un_sottogruppo?oldid=48168 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Congruenze in un gruppo** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Congruenze_in_un_gruppo?oldid=48468 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Morfismi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Morfismi?oldid=48267 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Gruppi quoziente** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Gruppi_quoziente?oldid=48443 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Azioni di gruppo** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Azioni_di_gruppo?oldid=177142 *Contributori:* Toma.luca95, Mmontrasio e Giaco1975

- **Corso:Algebra Gruppi (Unimib)/Gruppi/Classi di coniugio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Classi_di_coniugio?oldid=177122 *Contributori:* Toma.luca95, Mmontrasio e Giaco1975
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Orbite e stabilizzatori** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Orbite_e_stabilizzatori?oldid=177129 *Contributori:* Toma.luca95, Mmontrasio e Giaco1975
- **Corso:Algebra Gruppi (Unimib)/Gruppi/Teoremi di Sylow** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Gruppi_(Unimib)/Gruppi/Teoremi_di_Sylow?oldid=48302 *Contributori:* Toma.luca95 e Mmontrasio

2.2 Immagini

2.3 Licenza dell'opera

- [Project:Copyright Creative Commons Attribution Share Alike 3.0 & GNU FDL]
- Creative Commons Attribution-Share Alike 3.0