

Lezione 1 Algebra

Federico De Sisti

2024-10-01

1 Cosa c'è su e-learning di Francesco Mazzini

Date appelli

Esercizi settimanali

All'esame ti chiedono due esercizi delle schede scelti a caso

Ci sono 2 esoneri (primo 17 dicembre) (secondo ?? maggio)

Libri

M. Artin Algebra

IN. Herstein: Algebra (difficile)

2 Gruppi

Definizione 1 (Gruppo)

Un gruppo è un dato di un insieme G con un'operazione \cdot tali che:

1) L'operazione è associativa

$$f \cdot (gh) = (f \cdot g) \cdot h \quad \forall f, g, h \in G$$

2) Esistenza elemento neutro

$$\exists e \in G \text{ tale che } g \cdot e = e \cdot g = g \quad \forall g \in G.$$

3) esistenza degli inversi

$$\forall g \in G \quad \exists \quad g^{-1} \in G \quad \text{tale che } g^{-1} \cdot g = g \cdot g^{-1} = e.$$

Nomenclatura 1 (notazione)

(G, \cdot) dato $g \in G$ denotiamo con:

1) $g^0 = e$

2) $g^1 = g$

3) $g^n = g \cdot \dots \cdot g$ $g^{-n} = (g^{-1})^n$

Osservazione:

Con questa notazione:

$$(g^n)^m = g^{nm}$$

$$g^n \cdot g^m = g^{n+m}$$

Esempi

1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$

2) $GL_n(\mathbb{K}) = \{A \in Mat_{n \times n}(\mathbb{K}) | \det(A) \neq 0\}$ con prodotto

3) $SL_n(\mathbb{K}) = \{A \in Mat_{nn}(\mathbb{K}) | \det(A) = 1\}$

4) X insieme

$$S_X = \{ \text{funzioni } X \rightarrow X \text{ invertibili} \}$$

Speciale Se $X = \{1, \dots, n\}$

Allora chiamiamo

$$S_n = S_X.$$

(è il gruppo di permutazioni su n elementi)

Si chiama gruppo simmetrico

Definizione 2 (Gruppo diedrale)

$n \geq 3$ Consideriamo l' n -agono regolare nel piano (3-agono, triangolo)

D_n è l'insieme delle simmetrie del piano che preservano l' n -agono

Si chiama gruppo diedrale, l'operazione è la composizione

Esempio:

Per $n = 3$ abbiamo D_3

TODO INSERISCI DISEGNO gruppo diedrale

Esercizio

Determina gli inversi e tutti i possibili prodotti degli elementi di D_3

Definizione 3 (Gruppo Abeliano)

(G, \cdot) gruppo si dice Abeliano se l'operazione è commutativa

$$f \cdot g = g \cdot f$$

Definizione 4 (Gruppo finito)

(G, \cdot) gruppo si dice finito se la sua cardinalità è finita

$$|G| < +\infty$$

Definizione 5 (Ordine del gruppo)

(G, \cdot) gruppo, l'ordine di G è $|G|$

Definizione 6 (Ordine di un elemento)

$$\text{ord}(g) = \min\{n \in \mathbb{N} \mid g^n = e\}$$

se $\nexists n \in \mathbb{N}$ tale che $g^n = e$ poniamo $\text{ord}(g) = +\infty$

Definizione 7 (Gruppo ciclico)

$n \geq 3$ consideriamo C_n l'insieme delle isometrie del piano che preservano

l' n -agono e preservano l'orientazione, questo si chiama gruppo ciclico

Esempio

Nel caso di $n = 3$ abbiamo solamente 3 elementi: identità, e le due rotazioni (ordine dispari) **Esercizi**

1) si dimostri che l'elemento neutro in un gruppo è unico

2) si dimostri che ogni elemento in un gruppo ammette un unico elemento inverso

per casa

1) Trovare un'applicazione biunivoca $S_3 \rightarrow D_3$

2) Dimostrare che non esiste un'applicazione biunivoca $S_4 \rightarrow D_4$

3) Dimostrare che i seguenti non sono gruppi

$\cdot Mat_{n \times n}(\mathbb{K})$ con prodotto righe per colonne

$GL(\mathbb{K})$ con somma tra matrici

$\mathbb{Z} \oplus \mathbb{Q}$ con il prodotto

Proposizione 1

(G, \cdot) gruppo finito, Allora ogni elemento ha ordine finito

Dimostrazione

$g \in G$ Considero il sottoinsieme

$$A = \{g, g^2, g^3, \dots\} \subseteq G.$$

quindi $|A| < +\infty \Rightarrow \exists s, t \in \mathbb{N}, s > t$ tali che

$$g^s = g^t.$$

Moltiplico per g^{-t} a destra

$$g^s = g^t \Rightarrow g^s \cdot g^{-t} = g^t \cdot g^{-t} \Rightarrow g^{s-t} = e.$$

Quindi $n = s - t \geq 1$ e $g^n = e \Rightarrow \text{ord}(g) \leq n < +\infty$ □

Definizione 8 (Sottogruppo)

(G, \cdot) gruppo $H \subseteq G$ sottoinsieme, si dice che H è un sottogruppo se (H, \cdot) è un gruppo.

In tal caso scriveremo $H \leq G$

Osservazione

(G, \cdot) gruppo, $H \subseteq G$ sottoinsieme allora $H \leq G$ se H è chiuso rispetto a \cdot e H è chiuso rispetto agli inversi

(se $g, h \in H \Rightarrow g \cdot h \in H$ e se $h \in H \Rightarrow h^{-1} \in H$)

Proposizione 2

(G, \cdot) gruppo $H \subseteq G$ sottoinsieme con $|H| < +\infty$ Allora:

1) $H \leq G$ se e solo se H è chiuso rispetto a \cdot

Dimostrazione

(\Rightarrow) ovvia

(\Leftarrow) basta dimostrare che H è chiuso rispetto all'inverso ovvero

se $|H| < +\infty$

e H chiuso rispetto a \cdot

Allora H è chiuso rispetto agli inversi

Sia $h \in H$

$$A = \{h, h^2, h^3, \dots\} \subseteq H$$

Allora $|A| < \infty$

Ragionando come prima deduciamo $\text{ord}(h) < +\infty$

$$h \cdot h^{\text{ord}(h)-1} = h^{\text{ord}(h)-1} \cdot h = e.$$

Quindi $h^{-1} = h^{\text{ord}(h)-1} = h \cdot \dots \cdot h \in H \Rightarrow h^{-1} \in H$

□

Esempi

1) $C_n \leq D_n$

2) $SL_n(\mathbb{K}) \leq GL_n(\mathbb{K})$

3) (G, \cdot) gruppo $g \in G$

$$\langle g \rangle = \{g^n \in G | n \in \mathbb{Z}\}.$$

Allora $\langle g \rangle \leq G$

Congruenze

(G, \cdot) gruppo $H \leq G$

Definizione 9

$f, g \in G$ si dicono congruenti modulo H se

$$f^{-1}g \in H.$$

In tal caso scriveremo

$$f \equiv g \pmod{H}.$$

Esercizio

Dimostrare che al congruenza modulo H definisce una relazione di equivalenza su G

Suggerimento

$$(f^{-1} \cdot g)^{-1} = g^{-1} \cdot (f^{-1})^{-1} = g^{-1} \cdot f$$

e H è chiuso rispetto agli inversi

Esercizi:

(G, \cdot) è un gruppo $H \leq G$ Allora la classe di equivalenza di $g \in G$ modulo H è il sottoinsieme

$$gH = \{g \cdot h | h \in H\}.$$

C'è una classe di equivalenza speciale in G data da

$$e \cdot H = H.$$

l'unica ad essere un sottogruppo

Dimostrare che esiste un'applicazione biunivoca tra $H \rightarrow gH \quad \forall g \in G$

Lezione 2 Algebra 1

Federico De Sisti

2024-10-03

1 Nelle lezioni precedenti...

Definizione 1

(G, \cdot) gruppo $H \leq G$ $f, g \in G$ si dicono congruenti modulo H se $f^{-1} \cdot g \in H$

2 Classi di equivalenza

Notazione 1

classi di equivalenza:

$$G/H.$$

Esempi importanti

$(G, \cdot) = (\mathbb{Z}, +)$ $H = (m) = \{am | a \in \mathbb{Z}\}$ con m fissato

$G/H = \mathbb{Z}/(m)$

Attenzione

potete definire $f = g \bmod H$ tramite la condizione $f \cdot g^{-1}$

Le due definizioni non sono equivalenti [La chiameremo congruenza destra]

Notazione 2

L'insieme delle classi di equivalenza destra si indica con

$$H \backslash G.$$

Definizione 2

Gli elementi di G/H si chiamano laterali sinistri, quelli di $H \backslash G$ si chiamano laterali destri

Esercizio:

(G, \cdot) gruppo

$H \leq G$ $g \in G$ fissato

Allora il laterale sinistro a cui appartiene g è

$$gH = \{g \cdot h | h \in H\}.$$

Soluzione

fisso $f \in G$ e osserviamo che

$$g \equiv f \bmod H.$$

Se e solo se $g^{-1} \cdot f \in H$.

Questo è equivalente a

$$\exists h \in H \text{ tale che } g^{-1} \cdot f = h.$$

ovvero

$$\exists h \in H \text{ tale che } f = g \cdot h.$$

Esercizio

$$H \leq G$$

Allora $|G/H| = |H \backslash G|$

Soluzione

Basta eseguire un'applicazione biunivoca tra i due insiemi

Definizione 3

(G, \cdot) gruppo $H \leq G$ si dice sottogruppo normale se $gH = Hg \quad \forall g \in G$

Esempio

$G = S_3$ ricordo che S_3 è il gruppo di permutazioni dell'insieme $\{1, 2, 3\}$

Quali sono gli elementi di S_3 ?

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

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

scambio il 3 con l'uno, il 2 con il 2

$(2, 3, 1)$

$(1, 3)$

$(1, 2)$

Id

$$H_1 = \langle (1, 2) \rangle = \{id, (1, 2)\}.$$

$$H_2 = \langle (3, 2, 1) \rangle = \{id, (3, 2, 1), (2, 3, 1)\}.$$

Esercizio— Dimostrare che $H_1 \leq S_3$ non è normale, mentre $H_2 \leq S_3$ è normale

Notazione 3

Se $H \leq G$ è normale scriveremo

$$H \trianglelefteq G.$$

Esercizio

$H \leq G$ sottogruppo dimostrare che l'applicazione $\phi : H \rightarrow gH$

$$g \rightarrow g \cdot h$$

Soluzione

ϕ è suriettiva per definizione di gH

è anche iniettiva infatti se $h_1, h_2 \in H$ soddisfano

$$gh_1 = gh_2 \quad .$$

allora $h_1 = h_2$ (per la legge di cancellazione)

Osservazione

(G, \cdot) gruppo

$H \leq G$ Allora

$$|gH| = |Hg| \quad \forall g \in G.$$

anche se $gH \neq Hg$ poiché hanno entrambi la stessa cardinalità di H

Inoltre tutti i laterali sinistri (e destri) hanno la stessa cardinalità

Definizione 4

(G, \cdot) gruppo, $H \leq G$ l'indice di H in G è

$$[G : H] = |G/H|.$$

dove $|G/H|$ è il numero di classi laterali sinistre

Osservazione

$H \leq G$ sottogruppo

Se G è abeliano allora $H \leq G$

Il viceversa è falso! Possono esistere sottogruppi normali in gruppi non abeliani

Proposizione 1

(G, \cdot) gruppo $H \leq G$ allora

$$|G| = [G : H]|H|.$$

Dimostrazione

Basta ricordare che la cardinalità di ciascun laterale sinistro è pari a $|H|$ \square

Osservazione

$$H \subseteq G \Rightarrow [G : H] = \frac{|G|}{|H|}$$

Teorema 1 (Lagrange)

(G, \cdot) gruppo $H \leq G$ Allora l'ordine di H divide l'ordine di G

Dimostrazione

Dall'osservazione segue $\frac{|G|}{|H|} = [G : H] \in \mathbb{N}$ \square

Corollario 1

(G, \cdot) gruppo di ordine primo (ovvero $|G| = p$ con p primo)

Allora G non contiene sottogruppi non banali (tutto il gruppo o il gruppo minimale)

Dimostrazione

Sia $H \leq G$ allora per Lagrange abbiamo

$$|H| \text{ divide } p.$$

$\Rightarrow |H| = 1$ quindi $H = \{e\}$
oppure $\Rightarrow |H| = p$ quindi $H = H$

□

Corollario 2

(G, \cdot) gruppo (finito)

Dato $g \in G$ si ha $\text{ord}(g)$ divide l'ordine di G

Dimostrazione

Dato $g \in G$ considero

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$$

$$|\langle g \rangle| = \text{ord}(g).$$

La tesi segue ora da Lagrange

□

3 Operazioni fra sottogruppi

Proposizione 2

(G, \cdot) gruppo $H, K \leq G$

Allora $H \cap K \leq G$

Dimostrazione

$H \cap K$ è chiuso rispetto all'operazione e agli inversi poiché sia H che K che lo sono

□

Esercizio

Esibire due sottogruppi $H, J \leq G$ tali che $H \cup K$ non è un gruppo

Definizione 5

Dati $H, K \leq G$ definiamo il sottoinsieme

$$HK = \{h \cdot k | h \in H, k \in K\}.$$

Attenzione non è necessariamente un sottogruppo

Esercizio

Dimostrare che HK è un sottogruppo, di G se e solo se

$$HK = KH.$$

Soluzione

Supponiamo che HK sia un sottogruppo

$$HK = (HK)^{-1} = \{(h \cdot k)^{-1} | h \in H, k \in K\} = K^{-1}H^{-1} = KH.$$

Viceversa supponiamo che $HK = KH$

1) Dimostro che KH è chiuso rispetto all'operazione.

$h_1 k_1 \in HK$ e $h_2 \cdot k_2 \in HK$

$$(h_1 \cdot k_1) \cdot (h_2 \cdot k_2) = h_1 \cdot (k_1 \cdot h_2) \cdot k_2 = h_1 \cdot h_3 \cdot k_3 \cdot k_2 = (h_1 \cdot h_3) \cdot (k_3 \cdot k_2).$$

2) HK è chiuso rispetto agli inversi

$$h \cdot k \in HK \rightsquigarrow (h \cdot k)^{-1} = k^{-1} \cdot h^{-1} = h_4 \cdot k_4 \in HK.$$

Definizione 6 (Sottogruppo generato da un sottoinsieme)

(G, \cdot) gruppo $X \subseteq G$ sottoinsieme

Il sottogruppo generato da X è

$$\langle X \rangle = \bigcap_{H \leq G, X \subseteq H} H.$$

Notazione 4

$\cdot H, K \leq G$

$$\langle H, K \rangle := \langle H \cup K \rangle.$$

$\cdot g_1, \dots, g_n \in G$

$$\langle g_1, \dots, g_n \rangle := \langle \{g_1, \dots, g_n\} \rangle.$$

Caso Speciale

$(G, \cdot) = (\mathbb{Z}, +) \quad m \in \mathbb{Z}$

$(m) := \langle m \rangle$

4 Sottogruppi di \mathbb{Z}

Ricordo

dato $a \in \mathbb{Z}$ si ha $(a) \leq \mathbb{Z}$

Obbiettivo

non esisotno altri sottogruppi

Teorema 2

$H \leq \mathbb{Z}$ allora esiste $m \in \mathbb{Z}$ tale che $H = (m)$

Dimostrazione

Distinguiamo due casi:

1) $H = (0)$ finito

2) $H \neq (0)$ allora H contiene (almeno) un intero positivo, Definiamo

$$m := \min\{n \in \mathbb{Z} | n \geq 1, n \in H\}.$$

Vogliamo verificare che $H = (m)$ Sicuramente $(m) \subseteq H$ poichè $H \leq \mathbb{Z}$
Viceversa supponiamo che $\exists n \in H$ con $n \notin (m)$.

Allora

$$n = qm - r \text{ per qualche } q \in \mathbb{Z} \quad 0 < r < m.$$

$$\rightarrow r = n - qm \in H$$

Ma $r > 0, r < m$ quindi otteniamo l'assurdo per minimalità di m

□

Proposizione 3

$a, b \in \mathbb{Z}$, Allora:

1) $(a) \cap (b) = (m)$ dove $m := \text{mcm}\{a, b\}$

2) $(a) + (b) = (d)$ dove $d := \text{MCD}\{a, b\}$

Osservazione

$(a) + (b)$ è della forma HK con $H = (a)$ e $K = (b)$

inoltre $(a) + (b) \leq \mathbb{Z}$ poichè $(\mathbb{Z}, +)$ è abeliano

Dimostrazione

1) $(a) \cap (b)$ è il sottogruppo dei multipli di a e di b

Dunque $(a) \cap (b) = (m)$

2) $a + b \leq \mathbb{Z} \Rightarrow (a) + (b) = (d')$ per teorema

Dobbiamo verificare che $d' = d$

$$(d) = (a) + (b) \supseteq (a) \Rightarrow d' | a \text{ (} d' \text{ divide } a \text{)}.$$

$$\Rightarrow \begin{cases} d' | a \\ d' | b \end{cases} \Rightarrow d' \leq d$$

$$d' \in (a) + (b) \Rightarrow \exists h, k \in \mathbb{Z} \text{ tale che } d' = ha + kb$$

Dunque:

$$\begin{cases} d | a \\ d | b \end{cases} \Rightarrow d | d' \Rightarrow d \leq d'$$

Allora $d = d'$

□

5 Gruppi D_n e C_n

Ricordo

$$n \geq 3$$

Fissiamo un n -agono

$D_n = \{\text{isometrie che preservano l'n-agono}\}$

$C_n = \{\text{isometrie che preservano l'n-agono e l'orientazione}\}$

Teorema 3

$n \geq 3$ Allora

$$|D_n| = 2n$$

$$|C_n| = n$$

Dimostrazione

Fissiamo un lato l dell' n -agono. Un'isometria $\varphi \in D_n$ è univocamente determinata dall'immagine di $\varphi(l)$

Ho n scelte per il lato e per ogniuna di queste ho 2 scelte per le orientazione (mando il lato in se stesso? in quello dopo? in quello dopo ancora?, posso anche invertire la sua orientazione, i successivi lati vengono definiti da dove viene mandato il primo)

se non scegliamo l'orientazione, ci rimane il gruppo ciclico, e ciò conclude la dimostrazione \square

Osservazione

La dimostrazione prova che

$$C_n = \langle \rho \rangle .$$

dove ρ è la rotazione di angolo $\frac{2\pi}{n}$ attorno al centro dell' n -agono

Infatti $\rho \in C_n \Rightarrow \langle \rho \rangle \subseteq C_n$ ma l'ordine di questa rotazione è n

$$|\langle \rho \rangle| = \text{ord}(\rho) = n = |C_n| \Rightarrow C_n = \langle \rho \rangle .$$

Osservazione

Dalla dimostrazione segue che D_n è costituito da n rotazioni

(della forma ρ^i $i \in \{1, \dots, n\}$)

e n riflessioni

Proposizione 4

$n \geq 3$ Allora:

1) $D_n = \langle \rho, \sigma \rangle$

Dove σ è una rotazione qualsiasi ($\sigma \in D_n \setminus C_n$)

2) $\rho^i \sigma = \sigma \rho^{n-i}$

Dimostrazione

1) Sicuramente $\langle \rho, \sigma \rangle \subseteq D_n$

$$H = \langle \rho \rangle = \{Id, \rho, \rho^2, \dots, \rho^{n-1}\}$$

$$K = \langle \sigma \rangle = \{Id, \sigma\}$$

$$H \cap K = \{Id\}$$

$$|KH| = \frac{|H||K|}{|H \cap K|} = 2n.$$

$\Rightarrow HK \subseteq D_n$ (In particolare HK è sottogruppo) $\Rightarrow D_n = HK = \langle \rho, \sigma \rangle$

$\rho\sigma$ non preserva l'orientazione

$\Rightarrow \rho^i\sigma$ è riflessione

$$\Rightarrow \text{ord}(\rho^i\sigma) = 2$$

$$\Rightarrow \rho^i\sigma\rho^i\sigma = Id$$

$$\Rightarrow \rho^i\sigma\rho^i = \sigma$$

$$\Rightarrow \sigma\rho^i = \rho^{n-1}\sigma$$

□

Lezione 3 Algebra I

Federico De Sisti

2024-10-08

1 Altra roba sui gruppi

Proposizione 1 (Caratterizzazione dei sottogruppi normali)

(G, \cdot) gruppo, $N \leq G$

Le seguenti sono equivalenti:

1) $gNg^{-1} \subseteq N \quad \forall g \in G$

2) $gNg^{-1} = N \quad \forall g \in G$

3) $N \trianglelefteq G$

4) L'operazione $G/N \times G/N \rightarrow G/N$

è ben posta $(fN, gN) \rightarrow fgN$

o equivalentemente $N \backslash G \times n \backslash G \rightarrow n \backslash G$

$(Nf, Ng) \rightarrow Nfg$

Dimostrazione

1 \rightarrow 2

Verifichiamo che $N \subseteq gNg^{-1}$

Dato che $n \in N \Rightarrow n = g(g^{-1}ng)g^{-1}$ basta dimostrare che $g^{-1}ng \in N$

D'altra parte $g^{-1}ng \in g^{-1}Ng \subseteq N$ (per ipotesi 1)

2 \rightarrow 3

$\forall g \in G \quad \forall n \in N$

$gng^{-1} \in N$ (per ipotesi 2)

$$\begin{cases} gn \in Ng \\ ng^{-1} \in g^{-1}N \end{cases} \Rightarrow \begin{cases} gN \subseteq Ng(1) \\ Ng^{-1} \subseteq g^{-1}N(2) \end{cases} .$$

Il che è equivalente a dire che $gN = Ng$ la prima condizione mi dice $G/N \subseteq$

G/N e la seconda dell'arbitrarietà di g

$G/N \subseteq G/N$

3 \rightarrow 4

Dati $f, g \in G$ abbiamo

$$(Nf)(Ng) = (fN)(Ng) = fNg = (fN)g = (Nf)g = Nfg.$$

4 \rightarrow 1

Per ipotesi 4 $(Nf)(Ng) = Nfg \quad \forall f, g \in G$ quindi

$$nfn'g \in Nfg \quad \forall n, n' \in N.$$

dall'arbitrarietà di g , scelgo $g = f^{-1}$, quindi

$$nfn'f^{-1} \in N \quad \forall f \in G.$$

Moltiplico (a sinistra) per n^{-1} e ottengo

$$fn'f^{-1} \in N \quad \forall f \in G.$$

Dall'arbitrarietà di n' otteniamo $fNf^{-1} \subseteq N \quad \forall f \in G$ che è la condizione (1)

□

Osservazione

(G, \cdot) gruppo, la proposizione ci dice che un sottogruppo H è normale se e solo se l'operazione indotta su G/H è ben definita

Teorema 1

(G, \cdot) gruppo $N \trianglelefteq G$

Allora $(G/N, \cdot)$ è un gruppo (detto gruppo quoziente)

Dimostrazione

Associatività, ovvia

elemento neutro : $N = Ne$

elemento inverso di Ng è $Ng^{-1} \quad \forall g \in G$ □

Osservazione

(G, \cdot) gruppo e $H \leq G$ t.c. $[G : H] = 2$ Allora $H \trianglelefteq G$

Infatti esistono solo due laterali sinistri o destri: $H, G/H$

Osservazione

(G, \cdot) gruppo abeliano \Rightarrow ogni sottogruppo è normale

Non vale sempre il viceversa

Esempio

Dimostrare che $Q = \{\pm 1, \pm i, \pm j, \pm k\}$

è un gruppo (rispetto al prodotto) non abeliano in cui però tutti i sottogruppi sono normali

Prodotti:

$$i^2 = k^2 = j^2 = -1$$

$$ij = k \quad jk = i \quad ki = j$$

$$ji = -k \quad kh = -i \quad ik = -j$$

Definizione 1

Siano (G_1, \cdot) e $(G_2, *)$ gruppi

Sia φ un'applicazione

$\varphi : G_1 \rightarrow G_2$ si dice omomorfismo se:

$$\varphi(g \cdot f) = \varphi(g) * \varphi(f) \quad \forall g, f \in G_1.$$

Osservazione

Graficamente φ è un omomorfismo se

$$\begin{array}{ccc} (g, f) & G_1 \times G_1 \xrightarrow{\quad \cdot \quad} G_1 & (g, f) \xrightarrow{\quad \quad} g \cdot f \\ \downarrow & \varphi \times \varphi \downarrow & \downarrow \\ (\varphi(g), \varphi(f)) & G_2 \times G_2 \xrightarrow{\quad * \quad} G_2 & \varphi(g \cdot f) \end{array}$$

Esempi:

$(\mathbb{R}, +)$ gruppo additivo reali

$(\mathbb{R}_{>0}, \cdot)$ gruppo moltiplicativo reali positivi

Allora

$\exp : \mathbb{R} \rightarrow \mathbb{R}_{>0}$

$$x \rightarrow e^x$$

è un omomorfismo infatti: $\forall x, y \in \mathbb{R}$

$$e^{x+y} = e^x \cdot e^y.$$

Esempio

$\ln : \mathbb{R}_{>0} \rightarrow \mathbb{R}$

$$x \rightarrow \ln(x)$$

è un omomorfismo, infatti $\ln(x \cdot y) = \ln(x) + \ln(y) \quad \forall x, y \in \mathbb{R}_{>0}$

Osservazione:

$$l^0 = 1 \quad \ln(1) = 0$$

0 è l'elemento neutro in $(\mathbb{R}, +)$

1 è l'elemento neutro in $(\mathbb{R}_{>0}, \cdot)$

Osservazione:

$$e^{-x} = \frac{1}{e^x}$$

Inverso di x in $(\mathbb{R}, +)$

è inverso di e^x in $(\mathbb{R}_{>0}, \cdot)$

$$\ln\left(\frac{1}{x}\right) = -\ln(x)$$

Esercizio

$\varphi : G_1 \rightarrow G_2$ omomorfismo. Dimostrare

$$1) \varphi(e_1) = e_2$$

$$2) \varphi(g^{-1}) = \varphi(g)^{-1} \quad \forall g \in G_1$$

Soluzione:

$$\varphi(e_1) = \varphi(e_1 \cdot e_2) = \varphi(e_1) * \varphi(e_2)$$

moltiplico per $\varphi(e_1)^{-1}$

$$\Rightarrow e_2 = \varphi(e_1)^{-1} * \varphi(e_1) = \varphi(e_1)^{-1} * (\varphi(e_1) * \varphi(e_1)) = \varphi(e_1)$$

Esempio: (G, \cdot) gruppo, $N \trianglelefteq G$

Allora

$$\pi : G \rightarrow G/N$$

$$g \rightarrow gN$$

è un omomorfismo

Esempio

$$\det : GL_n(\mathbb{K}) \rightarrow \mathbb{K}^*$$

dove \mathbb{K} campo

$\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ è un gruppo rispetto al prodotto

allora \det è un omomorfismo

infatti:

$$\forall A, B \in GL_n(\mathbb{K}) \quad \det(AB) = \det(A)\det(B).$$

in particolare:

$$\det(Id) = 1$$

$$\det(A^{-1}) = \frac{1}{\det(A)} \quad \forall A \in GL_n(\mathbb{K})$$

Definizione 2

$\varphi : G_1 \rightarrow G_2$ omomorfismo

il nucleo di φ è $\ker(\varphi) := \{g \in G_1 \mid \varphi(g) = e\}$

L'immagine di ϕ è

$\text{Im}(\varphi) = \{h \in G_2 \mid \exists g \in G_1 : \varphi(g) = h\}$

Esercizio:

$\varphi : G_1 \rightarrow G_2$ omomorfismo

Allora $\ker(\varphi) \trianglelefteq G_1$

Soluzione

Chiamo $H = \ker(\varphi)$

vorrei verificare che $gHg^{-1} \subseteq H \quad \forall g \in G_1$

scegliamo $h \in H$ (ovvero $\varphi(h) = e_2$)

$\Rightarrow \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \text{per esercizio} = \varphi(g)\varphi(h)\varphi(g)^{-1} = e_2$

$\Rightarrow ghg^{-1} \in H \quad \forall h \in H, \forall g \in G \Rightarrow gHg^{-1} \subseteq H$

Osservazione

(G, \cdot) gruppo, $H \leq G$. Allora $H \trianglelefteq G$ se e solo se esiste $\varphi : G_1 \rightarrow G_2$ omomorfismo tale che $H = \ker(\varphi)$

Dimostrazione

Resta solo l'implicazione \Rightarrow

Sia $H \trianglelefteq G$. considero l'omomorfismo

$\pi : G \rightarrow G/H$

$g \mapsto gH$

chi è $\ker(\pi)$

$\ker(\pi) = \{g \in G \mid gH = H\} = \{g \in G \mid g \in H\} = H$

□

Esempio

$\det : GL_n(\mathbb{K}) \rightarrow K^*$

$\ker(\det) := \{A \in GL_n(\mathbb{K}) \mid \det(A) = 1\} = SL_n(\mathbb{K})$

quindi

$SL_n(\mathbb{K}) \trianglelefteq GL_n(\mathbb{K})$

Esercizio

(G, \cdot) gruppo $g \in G$ fissato

$\varphi : \mathbb{Z} \rightarrow G$

$n \mapsto g^n$

è un omomorfismo

determinare $\ker \varphi$ e $\text{Im} \varphi$

Esercizio

Sia $\varphi : G_1 \rightarrow G_2$ omomorfismo

1) Se $H_1 \leq G_1 \Rightarrow \varphi(H_1) \leq G_2$

se $H_1 \trianglelefteq G_1 \Rightarrow \varphi(H_1) \trianglelefteq \varphi(G_1)$

1) Se $H_2 \leq G_2 \Rightarrow \varphi^{-1}(H_2) \leq G_1$

se $H_1 \trianglelefteq G_2 \Rightarrow \varphi^{-1}(H_2) \trianglelefteq \varphi(G_1)$

Lezione 4 Algebra I

Federico De Sisti

2024-10-10

1 Altre informazioni sugli omomorfismi

Esercizio

Sia $\varphi : G_1 \rightarrow G_2$ omomorfismo dei gruppi

$$\ker \varphi = \{g \in G_1 \mid \varphi(g) = e_2\}$$

Dimostrare che

$$\varphi \text{ è iniettivo} \Leftrightarrow \ker(\varphi) = \{e_1\}$$

soluzione:

supponiamo che $\ker(\varphi) = \{e_1\}$

Allora dati $g, h \in G_1$ t.c $\varphi(g) = \varphi(h)$

dobbiamo mostrare che $g = h$

moltiplico per $\varphi(h)^{-1}$

$$\Rightarrow \varphi(h)^{-1} * \varphi(g) = e_2$$

$$\Rightarrow \varphi(h^{-1}) * \varphi(g) = e_2$$

$$\Rightarrow \varphi(h^{-1} \cdot g) = e_2$$

$$\Rightarrow h^{-1} \cdot g \in \ker \varphi$$

$$\Rightarrow h^{-1} \cdot g = e_1$$

$$\Rightarrow g = h$$

Il viceversa è lasciato al lettore come esercizio

Soluzione di un esercizio passato

1) Se $H_1 \subseteq G_1$ dimostriamo che $\varphi(H_1) \trianglelefteq \varphi(G_1)$

Verifichiamo che

$$f\varphi(H_1)f^{-1} \subseteq \varphi(H_1) \quad \forall f \in (G_1).$$

Quindi basta dimostrare che

$\forall h \in H_1 \quad \forall g \in G_1$ abbiamo

$$\varphi(g)\varphi(h)\varphi(g)^{-1} \in \varphi(H_1)$$

Questo è equivalente a richiedere che

$$\varphi(g \cdot h \cdot g^{-1}) \in \varphi(H_1).$$

Ma $ghg^{-1} \in gH_1g^{-1} = H_1$ dato che $H_1 \trianglelefteq G_1$

$$\exists \tilde{h} \in H_1 \text{ t.c } g \cdot h \cdot g^{-1} = \tilde{h}$$

$$\varphi(ghg^{-1}) = \varphi(\tilde{h}) \in \varphi(H_1)$$

2) Se $H_2 \trianglelefteq G_2$ dimostriamo che $\varphi^{-1}(H_2) \trianglelefteq G_1$

Ho due omomorfismi,

li compongo:

$$\psi : G_1 \xrightarrow[\varphi]{} G_2 \xrightarrow[\pi]{} G_2/H_2.$$

Studia il $\ker(\psi)$

$$\ker(\psi) := \{g \in G_1 \mid \psi(g) = H_2\} = \{g \in G_1 \mid \varphi(g)H_2 = H_2\}$$

$$\ker(\psi) = \{g \in G \mid \varphi(g) \in H_2\} = \varphi^{-1}(H_2)$$

Quindi $\varphi^{-1}(H_2)$ è il nucleo di un omomorfismo $\psi : G_1 \rightarrow G_2/H_2$ e dunque

$$\varphi^{-1}(H_2) \trianglelefteq G_1$$

Osservazione:

Se $\varphi : G_1 \rightarrow G_2$

omomorfismo di gruppi

$$H_2 = \{e_2\} \trianglelefteq G_2$$

l'esercizio (2) ci dice che $\ker(\varphi) = \varphi^{-1}(\{e_2\}) \trianglelefteq G_1$

Osservazione

Dalla parte (1) segue che

$$H_1 \leq G_1 \Rightarrow \varphi(H_1) \leq G_2$$

Quindi se scelgo $H_1 = G_1 \leq G_1$

$$\Rightarrow \text{Im}(\varphi) = \varphi(G_1) \leq G_2$$

2 Parte figa della lezione

Lemma 1

(G, \cdot) gruppo

$N \trianglelefteq G, H \trianglelefteq G$ sottogruppi normali

$\pi : G \rightarrow G/N$

Allora $\pi(H) = \pi(HN)$

Dimostrazione

$H \subseteq HN$ poiché $e \in N$ ogni elemento di H lo scrivo come lui stesso e \Rightarrow

$$\pi(H) \subseteq \pi(HN)$$

Viceversa dimostriamo che $\pi(HN) \subseteq \pi(H)$

infatti:

$$\forall h \in H \quad \forall n \in N$$

$$\pi(hn) = \pi(h)\pi(n) \text{ (omomorfismo)}$$

$$n \in N$$

$$\Rightarrow \pi(n) = N \rightarrow \pi(h)\pi(n) = \pi(ne)$$

$$\pi(e) = N = \pi(n) \in \pi H$$

□

Lemma 2 (G, \cdot) gruppo $H \trianglelefteq G$ $N \trianglelefteq G$ $\pi \rightarrow G/N$

Allora:

1) $\pi^{-1}(\pi(H)) = HN$ 2) se $N \subseteq H \rightarrow \pi^{-1}(\pi(H)) = H$ 3) $\bar{H} \leq G/N \rightarrow \pi(\pi^{-1}(\bar{H})) = \bar{H}$ **Dimostrazione (1)** $\pi^{-1}(\pi(H)) = ?$

osserviamo che dal lemma 1

 $\pi(H) = \pi(HN) = HN$ dato che $\pi(hn) = \pi(h)\pi(n) = hn$ $\Rightarrow \pi^{-1}(\pi(H)) = \pi^{-1}(\pi(HN)) = \pi^{-1}(HN) \supseteq HN$ Resta da verificare che $\pi^{-1}(\pi(H)) \subseteq HN$

$$\begin{aligned}
\pi^{-1}(\pi(H)) &:= \{g \in G \mid \pi(g) \in \pi(H)\} \\
&= \{g \in G \mid \exists h \in H : \pi(g) = \pi(h)\} \\
&= \{g \in G \mid \exists h \in H : \pi(h)^{-1}\pi(g) = N\} \quad N = \text{elemento neutro in } G \\
&= \{g \in G \mid \exists h \in H : \pi(hg) = N\} \\
&= \{g \in G \mid \exists h \in H : h^{-1}g \in N\} \\
&= \{g \in G \mid \exists h \in H : g \in hN\} \subseteq HN
\end{aligned}$$

segue (1)

□

Dimostrazione (2)

È un caso particolare del punto 1, infatti se

$$N \subseteq H \Rightarrow HN = H.$$

□

Dimostrazione (3)Segue dal fatto che π è un omomorfismo suriettivo

$$\pi(\pi^{-1}(\bar{H})) = \pi(G) \cap \bar{H} = \bar{H}.$$

□

Teorema 1 $(G, \cdot), n \trianglelefteq G$ *Allora esistono due corrispondenze biunivoche*

$$\begin{aligned}
& \{\text{sottogruppi } H \leq G \text{ t.c. } N \supseteq H\} \rightarrow \{\text{sottogruppi di } G/N\} \\
& \quad H \mapsto \pi(H) \\
& \quad \pi^{-1} \leftarrow \bar{H} \\
& \{\text{sottogruppi normali } H \trianglelefteq G \text{ t.c. } N \subseteq H\} \rightarrow \{\text{sottogruppi normali } G/N\} \\
& \quad H \mapsto \pi(H) \\
& \quad \pi^{-1}(\bar{H}) \mapsto \bar{H}
\end{aligned}$$

Dimostrazione

Il lemma 2 (punti 2 e 3) garantisce che le due applicazioni $H \mapsto \pi(H)$ $\pi^{-1}(H) \mapsto \bar{H}$

sono una l'inversa dell'altra □

Osservazione:

Per la seconda corrispondenza osserviamo che per la suriettività di π e l'esercizio di oggi

$$H \trianglelefteq G \mapsto \pi(H) \trianglelefteq G/N.$$

Teorema 2 (Teorema di omomorfismo) $\varphi : G_1 \rightarrow G_2$ omomorfismo $N \trianglelefteq G_1$ $\pi : G_1 \rightarrow G_1/N$ *Allora:*

1) esiste unico omomorfismo

 $\bar{\varphi} : G_1/N \rightarrow G_2$

$$\begin{array}{ccc}
G_1 & \xrightarrow{\varphi} & G_2 \\
\downarrow \pi & \searrow \exists! \bar{\varphi} & \\
G_1/N & &
\end{array}$$

t.c. $\bar{\varphi} \circ \pi = \varphi$

2) $\text{Im}(\bar{\varphi}) = \text{Im}(\varphi)$ 3) $\bar{\varphi}$ è iniettivo $\Leftrightarrow \ker \varphi = N$ **Dimostrazione**La condizione $\bar{\varphi} \cdot \pi = \varphi$ *Significa* $\forall g \in G_1$ si ha

$$\bar{\varphi} \cdot \pi(g) = \varphi(g)$$

ovvero

$$\bar{\varphi}(gN) = \varphi(g)$$

Dobbiamo verificare:· Unicità (segue da $\bar{\varphi} \cdot \pi = \varphi$)· $\bar{\varphi}$ è ben definita

$\cdot \bar{\varphi}$ è un omomorfismo

significa che se $gN = fN$ per qualche $g, f \in G_1$, allora $\varphi(g) = \varphi(f)$

Verifichiamo:

$$gN = fN \rightarrow g \equiv f \text{ mod } N$$

$$\Rightarrow \exists n \in N \text{ t.c. } g^{-1}f = n$$

$$\Rightarrow f = gn \Rightarrow \varphi(f) = \varphi(gn)$$

$$\Rightarrow \varphi(f) = \varphi(g)\varphi(n) = \varphi(g)$$

dato che $\varphi(n) = e_2$ ovvero $N \subseteq \ker \varphi$

Mostriamo adesso che $\bar{\varphi}$ è un omomorfismo

Significa che $\forall f, g \in G$

$$\bar{\varphi}((fN) \cdot (gN)) = \bar{\varphi}(fN) \cdot \bar{\varphi}(gN).$$

Per definizione

$$\bar{\varphi}((fN)(gN)) = \bar{\varphi}(fgN) = \varphi(fg) = \varphi(f)\varphi(g).$$

$$2) \bar{\varphi} \circ \pi = \varphi$$

dalla suriettività del π segue che $\text{Im}(\bar{\varphi}) = \text{Im}(\varphi)$

$$3) \bar{\varphi} \text{ è iniettivo} \Leftrightarrow \ker \bar{\varphi} = \{N\}$$

$$\ker \bar{\varphi} = \{gN \in G_1/N \mid \bar{\varphi}(gN) = e_2\}$$

$$= \{gN \in G_1/N \mid \varphi(g) = e_2\}$$

$$= \{gN \in G_1/N \mid g \in \ker(\varphi)\}$$

□

Corollario 1

$(G, \cdot), N \trianglelefteq G$

Allora esiste una corrispondenza biunivoca

$$\begin{aligned} \{\text{omomorfismi } \varphi : G \rightarrow G' \text{ t.c. } N \subseteq \ker(\varphi)\} &\rightarrow \{\text{omomorfismi } G/N \rightarrow G'\} \\ \varphi &\rightarrow \bar{\varphi} \\ \pi &\leftarrow \bar{\varphi} \end{aligned}$$

Dimostrazione

basta osservare che

dato $\bar{\varphi} : G/N \rightarrow G'$ la composizione

$\bar{\varphi} \circ \pi : G \rightarrow G'$ è un omomorfismo

tale che $\ker(\bar{\varphi} \circ \pi) \supseteq N$

segue $\pi(N) = N$ che è l'elemento neutro di G/N

$\Rightarrow \bar{\varphi} \circ \pi(N) = e'$ che è l'elemento neutro di G'

□

Definizione 1

$$\varphi : G_1 \rightarrow G_2$$

omomorfismo si dice isomorfismo se è invertibile

Teorema 3 (Primo teorema di isomorfismo)

$$\varphi : G_1 \rightarrow G_2$$

Allora:

$$\text{Im}(\varphi) \cong G_1/\ker(\varphi)$$

Dove \cong (isomorfo) significa che esiste un isomorfismo tra i due gruppi

Dimostrazione

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ \downarrow \pi & \nearrow \exists! \bar{\varphi} & \\ G_1/N & & \end{array}$$

scelgo $N = \ker \varphi$

il teorema di isomorfismo fornisce un omomorfismo iniettivo

$$\bar{\varphi} : G_1/\ker \varphi \rightarrow G_2.$$

Allora mi restringo all'immagine di $\bar{\varphi}$ così diventa suriettiva

$$G/\ker \varphi \cong \text{Im}(\bar{\varphi}) \cong \text{Im}(\varphi).$$

la prima tramite $\bar{\varphi}$ la seconda per il teorema di isomorfismo

Applicazione:

$$\det: GL_n(\mathbb{K}) \rightarrow (\mathbb{K}^*, \cdot) = (\mathbb{K} \setminus \{0\}, \cdot)$$

$$\ker(\det) = SL_n(\mathbb{K}) \text{ matrici con } \det 1$$

$$\Rightarrow GL_n(\mathbb{K})/SL_n(\mathbb{K}) \cong (\mathbb{K}^*, \cdot)$$

□

Lezione 5 Algebra I

Federico De Sisti

2024-10-15

1 Teoremi di isomorfismo

Teorema 1 (Secondo teorema di isomorfismo)

(G, \cdot) gruppo

$H, N \trianglelefteq G$ tali che $N \subseteq H$ Allora

1. $H/M \trianglelefteq G/N$
2. $G/N/H/N \cong G/H$

Dimostrazione

$$\begin{array}{ccc} G & \xrightarrow{\varphi=\pi_H} & G/H \\ \downarrow \pi & \nearrow \exists! \bar{\varphi} & \\ G/N & & \end{array} \quad \pi_H \text{ proiezione sul quoziente } H$$

$N \subseteq H = \ker(\varphi)$

Inoltre $\text{Im}(\bar{\varphi}) = \text{Im}(\varphi) = G/H$

Idea: applicare il primo teorema di isomorfismo

suriettiva $\bar{\varphi} : G/N \rightarrow G/H$

basta quindi dimostrare che $\ker(\bar{\varphi}) = H/N$

Studiamo

$$\ker(\bar{\varphi}) = \{gN \in G/N \mid \bar{\varphi}(gN) = H\}.$$

$$\{gN \in G/N \mid gH = H\}.$$

$$\{gN \in G/N \mid g \in H\} = H/N.$$

□

Corollario 1

In $(\mathbb{Z}, +)$ gruppo abeliano

$a, n \in \mathbb{Z}$ interi non nulli

Denotiamo con

$$[a] = a + (n) \in \mathbb{Z}/(n) = \{[0], [1], [2], \dots, [n-1]\}.$$

$$\text{Allora } \text{ord}_{\mathbb{Z}/(n)}([a]) = \frac{n}{\text{MCD}(a, n)}$$

Nota:

se $\text{MCD}(n, a) = 1$ allora a genera il gruppo ciclico $\mathbb{Z}/(n)$

Dimostrazione

Consideriamo $G = \mathbb{Z}$ $H = (a) + (n)$ $N = (n)$

Dal II Teorema di isomorfismo

$$\mathbb{Z}/(n) \Big/ ([a]) \cong \mathbb{Z}/(n) \Big/ (a) + (n)/(n) \cong G/N \Big/ H/N \cong G/N \cong \mathbb{Z}/(\text{MCD}(a, n)).$$

□

Confrontiamo le cardinalità

$$\begin{aligned} MCD(a, n) &= |\mathbb{Z}/(MCD(a, n))|. \\ &= |\mathbb{Z}/(n) / ([a])|. \end{aligned}$$

$$\begin{aligned} \frac{|\mathbb{Z}/(n)|}{|[a]|} &= \frac{n}{ord([a])}. \\ ord([a]) &= \frac{n}{MCD(a, n)}. \end{aligned}$$

Lemma 1

$a, b \in \mathbb{Z}$ non nulli

tali che $a|b$ (allora $(b) \subseteq (a)$)

Allora

$$|(a)/(b)| = \frac{b}{a}.$$

Dimostrazione

Studiamo $(a)/(b)$

Per definizione è l'insieme dei laterali

$$(a)/(b) = \{ta + (b) | t \in \mathbb{Z}\}.$$

dobbiamo capire quanti laterali distinti esistono

Dati $t, s \in \mathbb{Z}$ tali che

$$ta + (b) = sa + (b).$$

$$\Leftrightarrow ta \equiv sa \pmod{b}.$$

$$\Leftrightarrow -ta + sa \in (b).$$

Allora

$$(a)/(b) = \{ta + (b) | t \in \{1, \dots, \frac{b}{a}\}\}.$$

□

Teorema 2 (III teorema di isomorfismo)

(G, \cdot) gruppo

- $N \trianglelefteq G$

- $H \leq G$

Allora

1. $H \cap N \trianglelefteq H$

2. $H / H \cap N \cong HN / N$

Dimostrazione

$$\pi_N : G \rightarrow G/N$$

$$g \rightarrow gN$$

consideriamo la restrizione

$$\begin{aligned} \pi_N|_H : H &\rightarrow G/N \\ h &\rightarrow hN \\ \ker(\pi_N|_H) &= \{h \in H \mid \pi_N|_H(h) = N\} \\ &= \{h \in H \mid hN = N\} \\ &= \{h \in H \mid h \in N\} \\ &= H \cap N \end{aligned}$$

Deduciamo che $H \cap N \trianglelefteq N$

Idea: Applicare il I teorema di isomorfismo all'omomorfismo

$$\varphi = \pi_N|_H : H \rightarrow G/N.$$

$$\text{Avremo } \text{Im}(\varphi) \cong H / \ker(\varphi) = H / H \cap N$$

Studiamo $\text{Im}(\varphi)$

$$\text{Im}(\varphi) = \text{Im}(\pi_N|_H) = \pi_N(H) = \pi_N(HN) = HN/N.$$

Il penultimo passaggio deriva da un lemma già visto a lezione

□

Corollario 2

$a, b \in \mathbb{Z}$ non nulli

$$\text{Allora } \text{mcm}(a, b) = \frac{ab}{\text{MCD}(a, b)}$$

Dimostrazione

$$G = \mathbb{Z}$$

$$H = (a)$$

$$N = (b)$$

$$H + N = (\text{MCD}(a, b))$$

$H \cap N = (mcm(a, b))$
 Dal III teorema di isomorfismo

$$(a) / (mcm(a, b)) \cong H / H \cap N \cong HN / N \cong (MCD(a, b)) / (b).$$

Confrontiamo la cardinalità
 Per il lemma

$$\frac{mcm(a, b)}{a} = |(a)(mcm(a, b))| = |(MCD(a, b)) / (b)| = \frac{b}{MCD(a, b)}.$$

Quindi

$$mcm(a, b) = \frac{ab}{MCD(a, b)}.$$

□

2 Classificazione di gruppi di ordine "piccolo" a meno di isomorfismo

Ordine 1

Se $|G| = 1 \Rightarrow G = \{e\}$

Ordine p primo:

Abbiamo mostrato che se $|G| = p$ allora G non ammette sottogruppi non banali
 Sia $g \in G$ tale che $g \neq e \Rightarrow ord(g) = p \Rightarrow G = \langle g \rangle$

$$\begin{aligned} \varphi : G &\rightarrow G_p = \langle p \rangle \\ g &\rightarrow p \end{aligned}$$

Obiettivo: classificare a meno di isomorfismo i gruppi di ordine 4 e di ordine 6

Definizione 1 (Klein, 1884)

Il gruppo di Klein, K_4 è il gruppo delle isometrie del piano che preservano un rettangolo fissato.

Esercizio

Verificare che $K_4 = \{id, \rho, \sigma, \rho\sigma\}$

dove ρ = rotazione di angolo π

e dove σ = riflessione rispetto ad un lato **Osservazione**

tutti gli elementi in K_4 hanno ordine ≤ 2 Quindi $K_4 \neq C_4$

Dato che $K_4 = \langle \rho, \sigma \rangle$

denoteremo anche

$$K_4 = D_2 \text{ (gruppo diedrale).}$$

Esercizio

(G, \cdot) gruppo in cui ogni elemento ha ordine ≤ 2 (equivalentemente ogni elemento è inverso di se stesso)

1) Dimostrare che G è abeliano

2) Se $|G| = 4$ dimostrare che $G \cong K_4$ **Svolgimento** 1) Dati $f, g \in G$

$$fg = (fg)^{-1} = g^{-1}f^{-1} = gf$$

2) Sia $|G| = 4$

Scelgo $g, f \in G$ distinti tali che $\begin{cases} g \neq e \\ f \neq e \end{cases}$

Considero $H = \langle g, h \rangle$

Per Lagrange

$$|H| \geq 3$$

$$\Rightarrow H = G$$

$$\Rightarrow G = \{e, f, g, fg\}$$

abeliano

Costruisco l'isomorfismo esplicito con K_4

$$\varphi : G \rightarrow K_4 = \langle \rho, \sigma \rangle$$

$$e \rightarrow e$$

$$f \rightarrow \rho$$

$$g \rightarrow \sigma$$

$$fg \rightarrow \rho\sigma$$

che è chiaramente biunivoca ed è un omomorfismo $\Rightarrow \varphi$ è un isomorfismo

Lezione 6 Algebra I

Federico De Sisti

2024-10-21

1 Teoremi sulla cardinalità dei gruppi

Teorema 1

(G, \cdot) gruppo. Se $|G| = 6$ allora
 $G \cong C_6$ (abeliano) oppure $G \cong D_3$ (non abeliano)

Dimostrazione

Se G contiene un elemento di ordine 6 allora $G \cong C_6$

Se invece G non contiene elementi di ordine 6, per l'esercizio (2) esistono elementi $r, s \in G$ t.c. $\text{ord}(r) = 3$ e $\text{ord}(s) = 2$

Definisco:

$$G := \langle r \rangle = \{e, r, r^2\} \quad k := \langle s \rangle = \{e, s\}.$$

$$H \cap K = \{e\}.$$

$$|HK| = \frac{|H||K|}{|H \cap K|} = 6 = |KH|.$$

$$\Rightarrow HK = G = KH$$

Esplicitamente:

$$HK = \{e, r, r^2, s, rs, r^2s\}$$

$$KH = \{e, r, r^2, s, sr, sr^2\}$$

Dobbiamo considerare 2 casi:

I caso: $rs = sr$

studiamo $\text{ord}(rs)$

$$(rs)^2 = r^2s^2 = r^2 \neq e \Rightarrow \text{ord}(rs) \neq 2$$

$$(rs)^3 = r^3s^3 = s^3 = s \neq e$$

Per Lagrange

necessariamente $\text{ord}(rs) = 6$

$\Rightarrow G$ è ciclico \Rightarrow Assurdo

$$\text{II caso: } \begin{cases} rs = sr^2 \\ r^2s = sr \end{cases}$$

Costruiamo l'isomorfismo

$$G \rightarrow D_3 := \langle \rho, \sigma \rangle$$

$$e \rightarrow Id$$

$$r \rightarrow \rho$$

$$r^2 \rightarrow \rho^2$$

$$s \rightarrow \sigma$$

$$sr \rightarrow \sigma\rho$$

□

Definizione 1

Dato un gruppo (G, \cdot) il reticolo dei sottogruppi T_G è un grafo definito come

- esiste un vertice in T_G per ogni sottogruppo $H \leq G$
- esiste un lato $H_1 - H_2$ se e solo se $H_1 \subseteq H_2$
e $\nexists K \leq G$ t.c. $H_1 \subset K \subset H_2$

Esempio:

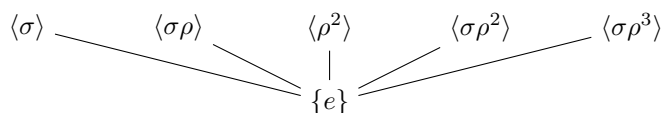
T_{D_4}

Ricordiamo che $D_4 = \langle \sigma, \rho \rangle$ $|D_4| = 8$

studiamo i sottogruppi di D_4

ordine 1: L'unico sottogruppo è $H = \{e\}$

ordine 2: Sono tutti e soli quelli generati da un elemento di ordine 2 in D_4

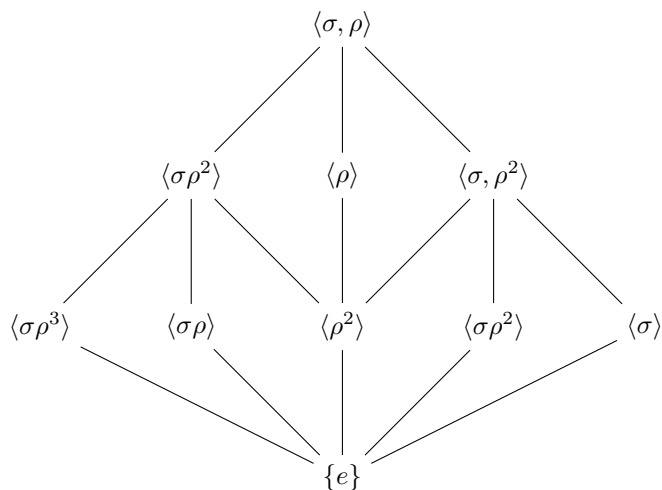


ordine 4: per la classificazione sono ciclici (C_4) oppure di Klein (K_4) oltre al ciclico $\langle p \rangle$ esistono altri sottogruppi

$$\langle \rho^2, \sigma \rangle = \{e, \sigma, \rho^2, \sigma \rho^2\}.$$

$$\langle \rho^2, \sigma \rho \rangle = \{e, \sigma \rho, \rho^2, \sigma \rho^3\}.$$

Ordine 8: D_4



Esempio:

$$G = D_4$$

$$N = \langle \rho^2 \rangle \trianglelefteq G$$

Vogliamo $T_{G/N}$

studiamo $G/N = D_4 / \langle \rho^2 \rangle$

$$|G/N| = [G : N] = \frac{|G|}{|N|} = \frac{8}{2} = 4$$

chi sono i laterali?

$$IdN = N \cap \langle \rho^2 \rangle = \{Id, \rho^2\}$$

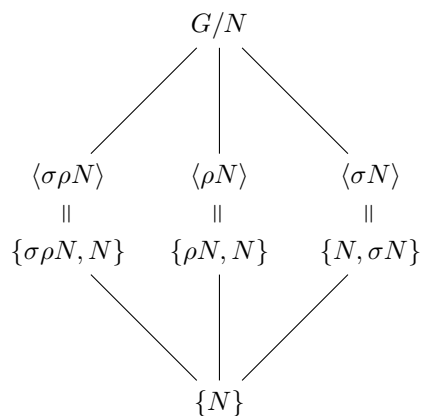
$$\rho N = \{\rho, \rho^3\}$$

$$\sigma N = \{\sigma, \sigma\rho^2\}$$

$$\sigma\rho N = \{\sigma\rho, \sigma\rho^3\}$$

Ricordo:

Abbiamo una corrispondenza biunivoca tra i sottogruppi di G/N e i sottogruppi di G contenenti N .



Obiettivo: studiare S_n

Ricordo:

$$X := \{1, \dots, n\}$$

$$S_n := S_X = \{ \text{applicazioni biunivoche } X \rightarrow X \}$$

S_n gruppo di permutazioni

Osservazione:

$$|S_n| = n!$$

Osservazione:

$$\text{se } n = 3 \rightarrow |S_3| = 6$$

$$\Rightarrow S_3 \cong D_3$$

Osservazione

$$S_n \cong D_n \quad \forall n \geq 4$$

$$\text{Infatti } n! > 2n \quad \forall n \geq 4$$

2 Notazioni in S_n

$$\sigma = (123)(47)$$

$$\tau = (23456)$$

$$\sigma\tau = \sigma \circ \tau = (123)(46)(23456)(12)(36)(45)$$

$$\tau \circ \sigma = (23456)(123)(46) = (13)(24)(56)$$

Lemma 1

Data $\sigma \in S_n$ allora σ partizione $X = \{1, \dots, n\}$ in sottoinsiemi permutati ciclicamente e disgiunti tra loro

Dimostrazione

Definiamo la relazione d'equivalenza $i \sim j \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } \sigma^k(i) = j$

È una relazione d'equivalenza!

studiamo le classi di equivalenza

fissato $i \in X$

la sua classe

$$X_i = \{\sigma^k(i) | k \in \mathbb{Z}\} \subseteq X.$$

quindi $\exists k_1, k_2 \in \mathbb{Z}$ distinti t.c. $\sigma^{k_1}(i) = \sigma^{k_2}(i)$

$$\Rightarrow i = \sigma^{k_2 - k_1}(i)$$

$$\Rightarrow m := \min\{k \in \mathbb{Z}_{>0} | \sigma^k(i) = i\}$$

$$\Rightarrow X_i = \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{m-1}(i)\}$$

□

Proposizione 1

Data $\sigma \in S_n$, allora σ può essere rappresentata come composizione di cicli disgiunti

Obiettivo: Definire un omomorfismo

$$\text{sgn} : S_n \rightarrow (\{\pm 1\}, \cdot).$$

Questo ci permetterà di definire il sottogruppo alterno $A_n \trianglelefteq S_n$

$$A_n := \ker(\text{sgn})$$

Notazione 1

Dato un polinomio

$$f \in \mathbb{Q}[x_1, \dots, x_n]$$

e data $\sigma \in S_n$

Definiamo

$$f^\sigma(x_1, \dots, x_n) := f(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Ci sta un polinomio speciale:

- $\Delta(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$
- $\Delta^\sigma(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$

Definizione 2

$$\sigma \in S_n$$

$$\text{sgn}(\sigma) := \frac{\Delta^\sigma}{\Delta} \in \{\pm 1\}$$

Osservazione

$$\text{sgn} : S_n \rightarrow \{\pm 1\}$$

è un omomorfismo

Dimostrazione

In generale

$$(f^\sigma)^\tau = f^{\sigma\tau}$$

$$(fg)^\sigma = f^\sigma g^\sigma$$

$$\text{sgn}(\sigma\tau) = \frac{\Delta^{\sigma\tau}}{\Delta} = \frac{(\Delta^\sigma)^\tau}{\Delta} = \frac{\Delta^\sigma}{\Delta} \frac{(\Delta^\sigma)^\tau}{\Delta^\sigma} = \text{sgn}(\sigma) \frac{\Delta^\tau}{\Delta} = \text{sgn}(\sigma) \text{sgn}(\tau) \quad \square$$

Lezione 7 Algebra I

Federico De Sisti

2024-10-22

1 parte da recuperare

2 Seconda ora

Lezione 8 Algebra I

Federico De Sisti

2024-10-26

1 Prodotti tra gruppi

1.1 Prodotto diretto di gruppi

Definizione 1

Siano (G_1, \cdot) , $(G_2, *)$ gruppi il loro prodotto diretto risulta l'insieme $(G_1 \times G_2)$ dotato dell'operazione:

$$(g_1, g_2) \cdot (f_1, f_2) = (g_1 \cdot f_1, g_2 * f_2) \quad \forall g_1, f_1 \in G_1, \quad \forall g_2, f_2 \in G_2.$$

e lo indichiamo con $(G_1 \times G_2)$

Proposizione 1

$(G_1 \times G_2, \cdot)$ è un gruppo

Dimostrazione

L'associatività segue da quella di \cdot e $*$ l'elemento neutro è (e_1, e_2)

l'inverso di (g, f) con $g \in G_1$ e $f \in G_2$ risulta (g^{-1}, f^{-1})

□

Esercizio

(G_1, \cdot) e $(G_2, *)$ gruppi

Dimostrare: 1) $|G_1 \times G_2| = |G_1| |G_2|$

2) $G_1 \times G_2$ è abeliano se e solo se G_1 e G_2 sono entrambi abeliani

3) Dati due sottogruppi $H \leq G_1$ e $K \leq G_2 \Rightarrow H \times K \leq G_1 \times G_2$

4) Dati $H \trianglelefteq G_1$ e $K \trianglelefteq G_2 \Rightarrow H \times K \trianglelefteq G_1 \times G_2$

5) Dati $H \trianglelefteq G_1$ e $K \trianglelefteq G_2$

$$G_1/H \times G_2/K \cong G_1 \times G_2 / H \times K.$$

Dimostrazione (4,5)

$$\begin{array}{ccc} G_1 \times G_2 & \xrightarrow{\varphi} & \frac{G_1}{H} \times \frac{G_2}{K} \\ \downarrow & \exists! \bar{\varphi} \nearrow & \\ \frac{(G_1 \times G_2)}{\ker \varphi} & & \end{array}$$

dove

$$\varphi(g_1, g_2) = (g_1 H, g_2 K)$$

Dal primo teorema di isomorfismo

$$\text{Im} \varphi \cong \frac{G_1 \times G_2}{\ker \varphi}.$$

φ suriettiva poichè $\pi_H \pi_K$ sono suriettive

$\ker \varphi = \{(g_1, g_2) \in G_1 \times G_2 \mid \varphi(g_1, g_2) = (H, K)\}$

$= \{(g_1, g_2) \mid g_1 H = H \text{ e } g_2 K = K\}$

$\{(g_1, g_2) | g_1 \in H, g_2 \in K\} = H \times K$
 quindi $H \times K \leq G_1 \times G_2$

$$\frac{G_1 \times G_2}{H \times K} \cong G_1/H \times G_2/K.$$

□

Esercizio (importante)

(G_1, \cdot) e $(G_2, *)$ gruppi

$H, K \leq G_1 \times G_2$ tali che $H \cap K = \{\tilde{e}\}$ dove $\tilde{e} = (e_1, e_2)$

Dimostrare che ogni elemento di H commuta con ogni elemento di K . **dimo** Consideriamo

$h \in H, k \in K$ e verifichiamo che $hk = kh$

Idea:

Dimostrare che $hkh^{-1}k^{-1} = e$

Data l'ipotesi $H \cap K = \{e\}$ è sufficiente dimostrare che $hkh^{-1}k^{-1} \in H \cap K$

Sfruttare la normalità di H e K

Per l'esercizio sotto chiedi a Marco

Esercizio

$(G_1, \cdot), (G_2, *)$ gruppi

$$H := G_1 \times \{e_2\} = \{(g, e_2) | g \in G_1\} \leq G_1 \times G_2.$$

$$K := \{e_1\} \times G_2 = \{(e_1, g) | g \in G_2\} \leq G_1 \times G_2.$$

Verificare che H e K soddisfano le ipotesi dell'esercizio precedente

Definizione 2

(G, \cdot) gruppo $H, K \leq G$

Diremo che G è

Prodotto diretto interno di H e K se:

- 1) $H, K \leq G$
- 2) $H \cap K = \{e\}$
- 3) $HK = G$

Teorema 1

(G, \cdot) gruppo

1) Se G è un prodotto diretto interno di $H, K \leq G$ allora $G \cong H \times K$

2) Se $G \cong G_1 \times G_2$ allora esistono $H, K \leq G$ tali che G sia prodotto diretto interno di H e K e inoltre $H \cong G_1, K \cong G_2$

Dimostrazione (1)

$\psi : H \times K \rightarrow G$

$(h, k) \rightarrow hk$

Dobbiamo verificare che ψ sia isomorfismo

1) ψ è suriettiva perchè ogni elemento di G si scrive come hk quindi $\text{Im}(\psi) = G$

2) È anche iniettiva infatti se $\psi(g_1, k_1) = \psi(h_2, k_1)$

$$\begin{aligned} &\Rightarrow h_1 k_1 = h_2 k_1 \\ &\Rightarrow h_2^{-1} h_1 k_1 = k_1 \\ &\Rightarrow h_2^{-1} h_1 = k_1 k_1^{-1} \in H \cap K = \{e\} \\ &\Rightarrow \begin{cases} h_2^{-1} h_1 = e \\ k_1 k_1^{-1} = e \end{cases} \Rightarrow (h_1, k_1) = (h_2, k_2) \\ &\Rightarrow \psi \text{ iniettiva} \end{aligned}$$

Bisogna in fine dimostrare che ψ è un omomorfismo, ovvero che

$$\psi(h_1 h_2, k_1 k_2) = \psi(h_1, k_1) \psi(h_2, k_2).$$

dunque

$$\psi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2 = h_1 (h_2 k_1) k_2 = h_1 (k_1 h_2) k_2 = \psi(h_1, k_1) \psi(h_2, k_2).$$

Ricordando che tutti gli elementi di H commutano con quelli di K □

Dimostrazione (2)

Per ipotesi esiste un isomorfismo $\varphi : G_1 \times G_2 \rightarrow G$

$$(g_1, g_2) \rightarrow \varphi(g_1, g_2)$$

considero

$$H := \varphi(G_1, \{e_2\})$$

$$K := \varphi(\{e_1\} \times G_2)$$

Abbiamo visto che

$$\cdot G_1 \times \{e_2\} \trianglelefteq G_1 \times G_2 \rightarrow H \trianglelefteq G$$

$$\cdot \{e_1\} \times G_2 \trianglelefteq G_1 \times G_2 \rightarrow K \trianglelefteq G$$

$$H \cap K = \varphi((G_1 \times \{e_2\}) \cap (\{e_1\} \times G_2)) = \{e\}.$$

$$HK = \varphi((G_1 \times \{e_2\})(\{e_1\} \times G_2)) = G.$$

Le opportune restrizioni di φ forniscono gli isomorfismi

$$H \cong G_1 \times \{e_2\} \cong G_1.$$

$$K \cong \{e_1\} \times G_2 \cong G_2.$$

□

Esempio:

Siano $n, m \in \mathbb{Z}_{>0}$ t.c.

$$\text{MCD}(n, m) = 1$$

Consideriamo $C_{nm} = \langle p \rangle$

dove $\text{ord}(p) = nm$

Considero

$$H = \langle \rho^m \rangle \quad K = \langle \rho^n \rangle .$$

$$|H| = \text{ord}(\rho^m) = n$$

$$|K| = \text{ord}(\rho^n) = m$$

Verifichiamo che

$$C_{nm} \cong H \times K.$$

Dobbiamo mostrare:

1. H, KC_{nm}

2. $H \cap K = \{Id\}$

3. $HK = C_{nm}$

1) C_{nm} abeliano, quindi H, KC_{nm}

2) $H \cap K = ?$

sia $\rho^h \in H \cap K$

Allora

$$\begin{cases} \rho^h = (\rho^m)^{t_1} \\ \rho^h = (\rho^n)^{t_2} \end{cases} \quad \begin{cases} m|h \\ n|h \end{cases} .$$

Ma $h \geq \text{mcm}(m, n) = mn \Rightarrow h = mn \Rightarrow \rho^h = Id \Rightarrow H \cap K = \{Id\}$

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{nm}{1}.$$

$\Rightarrow HK$ è tutto chiuso quindi è C_{nm}

Definizione 3 (Automorfismo)

(G, \cdot) gruppo

Un automorfismo di G è un isomorfismo $\varphi : G \rightarrow G$

Osservazione

(G, \cdot) gruppo

$\Rightarrow \text{Aut}(G) = \{\text{automorfismi di } G\}$

è un gruppo (rispetto alla composizione)

Esempio:

(G, \cdot) gruppo

Fissato $g \in G$ definiamo

$I_g : G \rightarrow G$

$$f \rightarrow gfg^{-1}$$

I_g si dice automorfismo interno

$\text{Int}(G) = \{\text{automorfismi interni di } G\}$

Proposizione 2
 $Int(G) \trianglelefteq Aut(G)$
Dimostrazione
 $I_f \in Int(G)$

dato $g \in G$ allora

$$I_{g^{-1}} = I_g^{-1} \rightarrow \begin{cases} I_g \in Aut(G) \\ Int(G) \text{ è chiuso rispetto agli inversi} \end{cases}.$$

$$I_{g_2} \cdot I_{g_1}(f) = g_2 g_1 f g_1^{-1} g_2^{-1} = (g_2 g_1) f (g_2 g_1)^{-1} = I_{g_2 g_1}(f)$$

$$I_{g_2} \cdot I_{g_1} = I_{g_2 g_1}$$

quindi $Int(G)$ è chiuso rispetto alla composizione

Quindi $Int(G) \leq Aut(G)$

Basta verificare che:

$$\varphi \circ Int(G) \circ \varphi^{-1} \subseteq Int(G) \quad \forall \varphi \in Aut(G)$$

ovvero dato $g \in G$

$$\varphi \circ I_g \circ \varphi^{-1} \in Int(G).$$

$$\forall f \in G$$

$$\varphi \circ I_g \circ \varphi^{-1}(f) = \varphi(g \varphi^{-1}(f) g^{-1}) =$$

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

$$= \varphi(g) f \varphi(g) =$$

$$= I_{\varphi(g)}(f)$$

$$\Rightarrow \varphi \circ I_g \circ \varphi^{-1} = I_{\varphi(g)} \in Int(G)$$

□

Definizione 4 (Centro di un gruppo)

(G, \cdot) gruppo

Il centro di G è

$$Z(G) := \{g \in G \mid gf = fg \quad \forall f \in G\}.$$

Osservazione

$$Z(G) \trianglelefteq G$$

Osservazione:

(G, \cdot) gruppo

Definiamo un omomorfismo

$$\varphi : G \rightarrow Int(G)$$

$$g \mapsto I_g$$

· φ è suriettiva

· φ è omomorfismo

$$\varphi(g_2 g_1) = \varphi(g_2) \varphi(g_1)$$

$$I_{g_2 g_1} = I_{g_2} \circ I_{g_1}$$

Chi è il $\ker(\varphi)$

$$\begin{aligned}
\ker(\varphi) &= \{g \in G \mid \varphi(g) = Id\} = \\
&= \{g \in G \mid I_g = Id\} = \\
&= \{g \in G \mid \forall f \in G : I_g(f) = Id(f)\} = \\
&= \{g \in G \mid \forall f \in G : gfg^{-1} = f\} = Z(G)
\end{aligned}$$

Dal I teorema di isomorfismo si ha che

$$Int(G) \cong G/Z(G).$$

1.2 Prodotto semidiretto

Consideriamo due gruppi

(N, \cdot) e $(H, *)$

Fissiamo un omomorfismo

$\phi : H \rightarrow Aut(N)$

$$h \rightarrow \phi_h$$

Definizione 5 (Prodotto semidiretto)

il prodotto semidiretto di N e H tramite ϕ è l'insieme $N \times H$ dotato dell'operazione

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \phi_{h_1}(n_2), h_1 * h_2).$$

$$\forall n_1, n_2 \in N \quad \forall h_1, h_2 \in H$$

Notazione 1

Indichiamo il prodotto semidiretto tra N e H con il simbolo $N \rtimes_{\phi} H$

Proposizione 3

$N \rtimes_{\phi} H$ è un gruppo

Dimostrazione

Dato $(n, h) \in N \rtimes_{\phi} H$

l'inverso è dato da $(\phi_{h^{-1}}(n^{-1}), h^{-1})$

□

Definizione 6

(G, \cdot) gruppo

$N, H \leq G$ Diremo che

G è prodotto semidiretto interno di N e H se

- $N \trianglelefteq G$
- $N \cap H = \{e\}$
- $NH = G$

Esempio

$D_n = \langle \rho, \sigma \rangle$ $N = \langle \rho \rangle \trianglelefteq D_n$

$H = \langle \sigma \rangle \leq D_n$. Allora D_n è prodotto semidiretto interno di N e H

Lezione 9 Algebra I

Federico De Sisti

2024-10-30

1 Ricapitolando

Siano $(N, \cdot), (H, *)$ gruppi.

Definizione 1

Il prodotto semidiretto di N e H tramite un omomorfismo $\theta : H \rightarrow \text{Aut}(N)$ è l'insieme $N \times H$ dotato dell'operazione

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \theta_{h_1}(n_2), h_1 * h_2).$$

Osservazione:

$h_1 \in H, \theta_{h_1} \in \text{Aut}(N) \quad \theta_{h_1}(n_2) \in N$

Esempio

Scegliendo

$\emptyset : H \rightarrow \text{Aut}(N)$

$h \rightarrow \emptyset_h$

con $\emptyset_n := \text{Id}_N \quad \forall h \in H$

Abbiamo:

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot n_2, h_1 * h_2).$$

Quindi il prodotto diretto è un caso particolare del prodotto semidiretto

2 Prodotto semidiretto interno:

Un gruppo G si dice *prodotto semidiretto interno* di N e $H \leq G$ se:

1. $N \trianglelefteq G$,
2. $N \cap H = \{e\}$,
3. $NH = G$.

Esercizio

Sia $\emptyset : H \rightarrow \text{Aut}(N)$ un omomorfismo

Dimostrare:

- 1) $|N \rtimes_{\emptyset} H| = |N||H|$
- 2) $N \rtimes_{\emptyset} H$ è abeliano $\Leftrightarrow N, H$ abeliani
- 3) $\tilde{H} \leq H, \tilde{N} \leq N$ (sottogruppo caratteristico)

$$\tilde{N} \rtimes_{\emptyset} \tilde{H} := \{(n, h) \in N \rtimes_{\emptyset} H \mid n \in \tilde{N}, h \in \tilde{H}\}.$$

è un sottogruppo di $N \rtimes_{\emptyset} H$

Definizione 2 (Sottogruppo caratteristico)

$\tilde{N} \leq N$ sottogruppo caratteristico se

$\varphi(n) \in \tilde{N} \quad \forall n \in N \quad \forall \varphi \in \text{Aut}(N)$

Teorema 1

Sia G un gruppo.

- 1) Se G è prodotto semidiretto di N e $H \leq G$, allora esiste un omomorfismo $\phi : H \rightarrow \text{Aut}(N)$ tale che $G \cong N \rtimes_{\phi} H$
 2) Se $G \cong \tilde{N} \rtimes_{\phi} \tilde{H}$ allora esistono $N, H \leq G$ t.c.

- G sia prodotto semidiretto interno di N e H
- $N \cong \tilde{N}, H \cong \tilde{H}$

Dimostrazione (1)

Definiamo l'applicazione

$$\phi : H \rightarrow \text{Aut}(N)$$

$$h \rightarrow \phi_h$$

$$\text{dove } \phi_h(n) := (hnh^{-1}) \in hNh^{-1} = N \quad \forall n \in N$$

Dato che abbiamo assunto N normale

Abbiamo verificato la volta scorsa che è un omomorfismo.

Definiamo l'applicazione

$$\psi : N \rtimes_{\phi} H \rightarrow G$$

$$(n, h) \rightarrow nh$$

ψ è suriettiva poiché $N \cdot H = G$

ψ è iniettiva poichè

$$\begin{aligned} n_1 h_1 = n_2 h_2 &\rightarrow n_2^{-1} h_1 = h_2 h_1^{-1} \in H \cap N = \{e\} \\ \Rightarrow \begin{cases} n_2^{-1} n_1 = e \\ h_2 h_1^{-1} = e \end{cases} &\rightarrow (n_1, h_1) = (n_2, h_2) \end{aligned}$$

ψ è **omomorfismo**:

$$\psi((n_1, h_1) \cdot (n_2, h_2)) =$$

$$= \psi((n_1 \phi_{h_1}(n_2), h_1 h_2))$$

$$= n_1 \phi_{h_1}(n_2) h_1 h_2$$

$$= n_1 h_1 n_2 h_1^{-1} h_1 h_2 = \psi(n_1, h_1) \cdot \psi(n_2, h_2)$$

Omomorfismo biunivoco

□

Dimostrazione (2)*Dato un isomorfismo*

$$\psi : \tilde{N} \rtimes_{\phi} \tilde{H} \rightarrow G$$

definiamo:

$$N := \psi(\tilde{N} \rtimes_{\phi} \{e_{\tilde{H}}\}) \trianglelefteq G$$

$$H := \psi(\{e_{\tilde{N}}\} \rtimes_{\phi} \tilde{H})$$

Osserviamo che:

$$\cdot \tilde{N} \cong \tilde{N} \rtimes_{\phi} \{e_{\tilde{H}}\} \cong N$$

$$\cdot \tilde{H} \cong \{e_{\tilde{N}}\} \rtimes_{\phi} \tilde{H} \cong H$$

$$\cdot N \cap H = \{e\}$$

$$\cdot NH = e$$

(analogo alla dimostrazione per prodotto diretto)

□

Lezione 10 Algebra I

Federico De Sisti

2024-11-02

1 Numeri primi e aritmetica

Definizione 1 (Numero primo)

Un intero $\rho > 1$ si dice primo se $\forall a, b \in \mathbb{Z}$

$$\rho | ab \rightarrow \rho | a \text{ oppure } \rho | b.$$

Definizione 2 (Numero irriducibile)

Un intero $\rho > 1$ si dice irriducibile se i suoi unici divisori positivi sono 1 e ρ

Esercizio:

Dimostrare che ρ è primo \Leftrightarrow è irriducibile

Teorema 1 (Fondamentale dell'aritmetica)

$n > 1$ intero. Allora n si scrive in modo unico come

$$n = \rho_1^{k_1} \cdot \dots \cdot \rho_r^{k_r} \quad (\text{forma canonica})$$

dove $k_i > 0 \quad \forall i \in \{1, \dots, r\}$

e $\rho_1 < \rho_2 < \dots < \rho_r$

e ρ_i è primo $\forall i \in \{1, \dots, r\}$

Teorema 2

ρ primo. Allora

$\sqrt{\rho}$ è irrazionale (ovvero $\sqrt{\rho} \notin \mathbb{Q}$)

Dimostrazione (Per assurdo)

$\exists a, b \in \mathbb{Z}$ t.c. $\sqrt{\rho} = \frac{a}{b}$ con $MCD(a, b) = 1$

Allora:

$$(a) + (b) = (MCD(a, b)) = (1)$$

$$\rightarrow 1 \in (a) + (b)$$

$\exists r, s \in \mathbb{Z}$ t.c. $1 = ra + sb$ (identità di Bezout)

$$\text{ora: } \begin{cases} a = \sqrt{\rho}b \\ b\rho = a\sqrt{\rho} \end{cases}$$

$$\text{Quindi: } \sqrt{\rho} = \rho \cdot 1 = \sqrt{\rho} \cdot (ra + sb)$$

$$(\sqrt{\rho}a)r + (\sqrt{\rho}b)s$$

$$= \rho br + as \in \mathbb{Z}$$

$\Rightarrow \sqrt{\rho} \in \mathbb{Z}$ quindi $\sqrt{\rho}$ è un intero che divide ρ e $1 < \sqrt{\rho} < \rho$

□

Teorema 3 (Euclide)*Esistono infiniti numeri primi***Dimostrazione***Supponiamo per assurdo che \exists un numero finito di primi ρ_1, \dots, ρ_r* *Definiamo: $N := (\rho_1 \cdot \dots \cdot \rho_r) + 1 > 1$* *$\Rightarrow \exists \rho_k$ primo tale che $\rho_k | N$*

$$\Rightarrow \begin{cases} \rho_k | N \\ \rho_k | N - 1 \end{cases} \Rightarrow \rho_k | N - (N - 1) \Rightarrow \rho_k | 1, \text{ assurdo}$$

□

Definizione 3 (Numero di Euclide)*Sia ρ primo*

$$\rho^\# := \left(\prod_{q \in \rho, q \text{ primo}} q \right) + 1.$$

 $\rho^\# + 1$ si dice numero di Euclide

Lezione 11 Algebra I

Federico De Sisti

2024-11-05

1 Svolgimento esercizi

Ossercazione:

Quali sono gli elementi di ordine 21 in S_{13} ?

Ricordo che in S_4 , gli elementi $(12)(34)$, $(13)(24)$, $(14)(23)$ hanno ordine 2

gli elementi di ordine 3 sono $(3 - ciclo)(7 - ciclo)$ sono $\frac{13!}{126}$

$(3 - ciclo)(3 - ciclo)(7 - ciclo)$ sono $\frac{13!}{126}$

Nelle note del corso trovi soluzioni degli esercizi

2 Funzione di Eulero

$$\begin{aligned}\phi : \mathbb{Z}_{>0} &\rightarrow \mathbb{Z} \\ n &\rightarrow |U_n|\end{aligned}$$

Ricordo:

$$\phi(1) = 1$$

$$\phi(p) = p - 1$$

$$\phi(p^k) = p^k - p^{k-1}$$

$$\phi(n \cdot m) = \phi(n)\phi(m) \quad \text{se } MCD(n, m) = 1$$

Lemma 1

$n > 1, a \in \mathbb{Z}$ t.c. $MCD(n, a) = 1$

sia $\{a_1, \dots, a_{\phi(n)}\}$ l'insieme dei numeri positivi minori di n coprimi con n distinti fra loro.

Allora $\{[a_1], \dots, [a_{\phi(n)}]\} = \{[aa_1], \dots, [aa_{\phi(n)}]\}$ (Classi in $\mathbb{Z}/(n)$)

Dimostrazione

Basta verificare che gli elementi delle classi $[aa_i] \quad \forall 0 < i < \phi(n)$

Siano tutte distinte tra loro e aa_i sia coprimo con $n \quad \forall 0 < i < \phi(n)$

Se per assurdo $[aa_i] = [aa_j] \quad i \neq j \Rightarrow aa_i \equiv aa_j \pmod{n} \Rightarrow a \equiv a_j \pmod{n}$

Assurdo perché $1 \leq a_i, a_j < n$ per ipotesi e dunque $a_i - a_j \notin (n)$

$$\begin{cases} MCD(a, n) = 1 \\ MCD(a_i, n) = 1 \end{cases} \Rightarrow MCD(a, a_i) = 1$$

□

Teorema 1 (Eulero 1760)

$n > 1, a \in \mathbb{Z}$ tale che $MCD(a, n) = 1$

Allora

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Nota

Se n è primo ritroviamo il piccolo teorema di Fermat

Dimostrazione

Considero la situazione del lemma:

$$A = \{a_1, \dots, a_{\phi(n)}\}$$

Insieme degli interi positivi minori di n e coprimi con n distinti tra loro

Dal lemma segue che

$$\begin{aligned} a_1 \cdot \dots \cdot a_{\phi(n)} &\equiv (aa_1) \cdot \dots \cdot (aa_{\phi(n)}) \pmod{n}. \\ &\equiv a^{\phi(n)} \cdot a_1 \cdot \dots \cdot a_{\phi(n)} \pmod{n}. \end{aligned}$$

Dal momento che $MCD(a_i, n) = 1$

abbiamo: $1 \equiv a^{\phi(n)} \pmod{n}$

□

Esempio

Se volessi calcolare le ultime 3 cifre di 2024^{2025} Studiamo la congruenza

$$x \equiv 2024^{2025} \pmod{1000}$$

È equivalente al sistema (Teorema cinese del resto):

$$\begin{cases} x \equiv 2024^{2025} \pmod{2^3} \\ x \equiv 2024^{2025} \pmod{5^3} \end{cases}$$

Alternativamente mi accorgo che la prima equazione è equivalente a

$$x \equiv 24^{2025} \pmod{1000}.$$

$$\phi(1000) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$$

$$\Rightarrow 24^{400} \equiv 1 \pmod{n}$$

Ma questo implica che la congruenza che devo studiare è:

$$\Rightarrow x \equiv 24^{2025} \pmod{1000}.$$

$$\Rightarrow \begin{cases} x \equiv 24^{2025} \pmod{8} \\ x \equiv 24^{2025} \pmod{125} \end{cases} \Rightarrow \begin{cases} x \equiv 0 \pmod{8} \\ x \equiv 24^{2025} \pmod{125} \end{cases}.$$

Dove nell'ultimo passaggio abbiamo utilizzato il fatto che $8|24$ e $24^{\phi(125)} \equiv 24^{100} \equiv 1 \pmod{125}$

Alla fine dovremmo ricostruire la soluzione in $\mathbb{Z}/(1000)$ che sarà unica per il teorema cinese del resto

3 Teorema cinese del resto

Problema

Dato un sistema di congruenze

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

con $MCD(n_i, n_j) = 1 \quad \forall i \neq j$

Come ricostruire l'unica soluzione $[\bar{x}] \in \mathbb{Z}/(n_1 \cdot \dots \cdot n_r)$

$$\bar{x} \equiv a_i \pmod{n_i} \quad \forall i \in \{1, \dots, r\}$$

Idea

Definiamo:

$$n := n_1 \cdot n_r$$

$$N_i := \frac{n}{n_i}$$

$$\bar{x} := a_1 N_1^{\phi(n_1)} + \dots + a_r N_r^{\phi(n_r)}$$

$$\text{Ora } \bar{x} \equiv a_i N^{\phi(n)} \pmod{n} \Rightarrow \bar{x} \equiv a_i \pmod{n_i} \quad \forall i$$

Teorema 2 (TCR)

Damp il sistema

$$\begin{cases} x \equiv a_1 \pmod{n} \\ \dots x \equiv a_r \pmod{n_r} \end{cases}$$

con $MCD(n_i, n_j) = 1 \quad \forall i \neq j$

Allora esiste un'unica classe $[\bar{x}] \in \mathbb{Z}/(n_1 \cdot \dots \cdot n_r)$ tale che

$$\bar{x} \equiv a_i \pmod{n_i} \quad \forall i \in \{1, \dots, r\}$$

Dimostrazione (Alternativa al teorema di Eulero)

$$n := n_1 \cdot \dots \cdot n_r$$

$$N_i = \frac{n}{n_i}$$

$$\bar{x} := a_1 N_1 m_1 + \dots + a_r N_r m_r$$

dove gli m_i sono univocamente determinati dalla condizione $N_i m_i \equiv 1 \pmod{n_i}$

Infatti

$$\bar{x} \equiv a_i N_i m_i \pmod{n_i} \Rightarrow \bar{x} \equiv a_i \pmod{n_i}.$$

Osserviamo che $MCD(N_i, n_i) = 1$ Per ipotesi

Quindi $[N_i] \in U_{n_i}$ e $[m_i]$ è l'unico inverso di $[N_i]$ in U_{n_i}

□

Osservazione

Per risolvere i sistemi di congruenze "basta" saper trovare gli inversi degli elementi in gruppi U_{n_i}

Esercizi dalle schede

Esercizio (Gauss)

Dato un intero $n > 1$ dimostrare che $n = \sum_{d|n} \phi(d)$ (somma di tutti i divisori positivi di n)

Dimostrazione

$$S_d := \{m \in \mathbb{Z} | MCD(m, n) = d, 1 \leq m \leq n\}$$

Osserviamo che

$$\{1, \dots, n\} = \bigcup_d S_d$$

$$\Rightarrow n = \sum_{d|n} |S_d|$$

$$MCD(m, n) = d \Leftrightarrow MCD(\frac{m}{d}, \frac{n}{d}) = 1$$

$$\text{Quindi } |S_d| = \phi(\frac{n}{d})$$

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} \phi(d)$$

□

Esempio

$n = 15$

Voglio ripetere la dimostrazione per ottenere $15 = \sum_{d|15} \phi(d)$

$$S_1 = \{1, 2, 4, 7, 8, 11, 13, 14\} \Rightarrow \phi(15/1) = 8$$

$$S_3 = \{3, 6, 9, 12\} \Rightarrow \phi(15/3) = 4$$

$$S_5 = \{5, 10\} \Rightarrow \phi(15/5) = 2$$

$$S_{15} = \{15\} \Rightarrow \phi(15/15) = 1$$

Esempio

n.1 Allora la somma di tutti gli interi positivi minori di n coprimi con n vale

$$\frac{1}{2}n\phi(n) \in \mathbb{Z}$$

Dimostrazione

Chiamiamo $a_1, \dots, a_{\phi(n)}$ tali interi:

$$\text{Studio } \sum_{i=1}^{\phi(n)} a_i$$

$$\text{Osserviamo che } MCD(a, n) = 1 \Leftrightarrow MCD(n - a_i, n) = 1$$

Quindi

$$\{a_1, \dots, a_{\phi(n)}\} = \{n - a_1, \dots, n - a_{\phi(n)}\}$$

$$\Rightarrow \sum_{i=1}^{\phi(n)} a_i = \sum_{i=1}^{\phi(n)} (n - a_i) = n\phi(n) - \sum_{i=1}^{\phi(n)} a_i \Rightarrow 2 \sum_{i=1}^{\phi(n)} a_i = n\phi(n) \quad \square$$

3.1 Teorema di Wilson/Lagrange

Ricordo

Teorema 3 (Wilson)

p primo. Allora

$$(p-1)! \equiv (p-1) \pmod{p}$$

Teorema 4 (Lagrange)

$m > 1$ intero tale che

$$(m-1)! \equiv (m-1) \pmod{m}$$

Allora m è primo

Dimostrazione

Per assurdo, se m non è primo allora esiste un intero $d|m$ tale che $1 < d < m$

Osserviamo che:

$$d < m \Rightarrow d|(m-1)!$$

dall'ipotesi segue che

$$m|(m-1)! + 1.$$

$$\Rightarrow d|(m-1)! + 1$$

$$\text{Quindi } \begin{cases} d|(m-1)! \\ d|(m-1)! + 1 \end{cases} \Rightarrow d|1 \text{ che è un assurdo} \quad \square$$

Esercizio

p primo dispari. Allora

$$p \equiv 1 \pmod{2}.$$

Lezione 12 Algebra I

Federico De Sisti

2024-11-07

1 Divisione Euclidea

Teorema 1

$a, b \in \mathbb{Z}$ con $b \neq 0$ allora $\exists q, r \in \mathbb{Z}$ tale che

$$a = qb + r$$

$$0 \leq r < |b|$$

Dimostrazione

Procediamo per passi

1) $a, b \in \mathbb{Z}_{>0}$

$$A = \{k \in \mathbb{Z} | kb > a\}.$$

Osserviamo che $A \neq \emptyset$

Infatti $(a+1)b = ab + b > ab \geq a \Rightarrow a+1 \in A$

Per il principio del buon ordinamento di \mathbb{N}

$$\Rightarrow \exists m := \min\{k\} \in \mathbb{Z}^+.$$

Definiamo

$$q := m - 1 \in \mathbb{Z}^+.$$

$q \notin A$ e $q+1 \in A$

$$qb \leq a < (q+1)b = qb + b$$

$$\Rightarrow 0 \leq a - qb < b$$

Definiamo $r = a - qb$ e otteniamo:

$$0 \leq r < b$$

$$a = qb + r$$

2) $a \in \mathbb{Z}$ $b > 0$

Se $a \geq 0$ (ok per 1)

Se $a < 0 \Rightarrow -a > 0$

$$\Rightarrow -a = qb + r \text{ con } 0 \leq r < b$$

$$\Rightarrow a = (-q)b - r$$

Se $r = 0$ abbiamo finito

Se invece $0 < r < b$

$$\text{definiamo } r' = b - r \Rightarrow 0 < r' < b$$

$$a = (-q)b - b + \frac{b-r}{r'}$$

$$\Rightarrow a = (-q-1)b + r' = q'b + r'$$

3) $a \in \mathbb{Z}$, $b < 0$

$$\Rightarrow -b > 0$$

$$a = q(-b) + r \text{ con } 0 \leq r < -b$$

$$\Rightarrow a = (-q)b + r \quad 0 \leq r < |b|$$

□

2 Esercizi delle schede

$$\begin{cases} x \equiv 50 \pmod{110} \\ x \equiv 47 \pmod{73} \end{cases}$$

Dal teorema cinese del resto sappiamo che esiste un'unica soluzione modulo il prodotto $\text{mod}(110 * 73) = \text{mod}(8030)$

Come lo costruisco?

$$\bar{x} = 50 \cdot 73 \cdot m_1 + 47 \cdot 110 \cdot m_2$$

L'idea è di infilare al posto di m_1 l'inverso di $73 \pmod{110}$

$$\begin{cases} 73 \cdot m_1 \equiv 1 \pmod{110} \\ 110 \cdot m_2 \equiv 1 \pmod{73} \end{cases}.$$

Bisogna determinare m_1, m_2

Idea: Sfruttare l'identità di Bezout: $(n_1) + (n_2) = (\text{MCD}(n_1, n_2)) = (1)$

obiettivo: $n_1 \cdot e + n_2 \cdot s = 1$

Nel nostro caso cerco $110 \cdot r + 73 \cdot s = 1 \quad r, s \in \mathbb{Z}$

Perché è importante $110 \cdot r \equiv 1 \pmod{73}$

$$73 \cdot s \equiv 1 \pmod{110}$$

Il nuovo obiettivo è determinare r, s

Procedo con la divisione euclidea tra 110 e 73

$$\begin{aligned} 110 &= 73 + 37 \\ 73 &= 2 \cdot 37 - 1 \\ \Rightarrow 1 &= 2 \cdot 37 - 73 \\ \Rightarrow 2 \cdot (110 - 73) - 73 &= 1 \\ \Rightarrow 2 \cdot 110 - 3 \cdot 73 &= 1 \end{aligned}$$

Quindi:

$$1 = 2 \cdot 110 - 3 \cdot 73$$

da cui

$$m_1 = -3$$

$$m_2 = 2$$

$$\bar{x} \equiv 50 \cdot 73 \cdot (-3) + 47 \cdot 110 \cdot (2) \equiv -620 \pmod{8030}.$$

8=====D

Nuovo Esercizio

$$\begin{cases} x \equiv_6 2 \\ x \equiv_{10} 3 \end{cases} \quad \text{Non possiamo sfruttare il teorema cinese del resto}$$

$$\begin{aligned}
x &\equiv_6 2 \\
&\Downarrow \\
x &= 2 + 6k \quad k \in \mathbb{Z} \\
&\Downarrow \\
x &= 2(1 + 3k)
\end{aligned}$$

$$\begin{aligned}
x &\equiv_{10} 3 \\
&\Downarrow \\
x &= 3 + 10h \quad h \in \mathbb{Z} \\
&\Downarrow \\
x &= 2(5h + 1) + 1
\end{aligned}$$

Dunque dalla prima congruenza segue

$$x \equiv_2 0.$$

dalla seconda

$$x \equiv_2 1.$$

8=====D

Nuovo Esercizio

$$\begin{cases} 3x \equiv_{15} 6 \\ 7x \equiv_9 2 \end{cases}$$

Non posso usare *TCB* studio $3x \equiv_{15} 6$

$$\begin{aligned}
3x &\equiv 6 + 15k \\
&\Downarrow \\
3x &= 3(2 + 5k) \\
&\Downarrow \\
x &= 2 + 5k
\end{aligned}$$

$$\begin{cases} x \equiv_5 2 \\ 7x \equiv_9 2 \end{cases}$$

Ora $MCD(3, 9) = 1$ Vorrei sfruttare TCR, per farlo dobbiamo eliminare i coefficienti

Noto che 7 e 9 sono coprimi $\Rightarrow [7] \in U_9$ (invertibili modulo 9)

Cerchiamo l'inverso moltiplicativo di $[7] \in U_9$

ovvero cerco $s \in \mathbb{Z}$ tale che $7s \equiv_9 1$

Utilizzo la divisione euclidea

$$\begin{aligned}
 9 &= 7 + 2 \\
 7 &= 3 \cdot 2 + 1 \\
 \Rightarrow 1 &= 7 - 3 \cdot 2 \\
 \Rightarrow 1 &= 7 - 3 \cdot (9 - 7) \\
 \Rightarrow 1 &= 4 \cdot 7 - 3 \cdot 9
 \end{aligned}$$

Quindi $s = 4$

$$\begin{aligned}
 7x &\equiv_9 2 \\
 \Updownarrow \\
 4 \cdot 7 &\equiv_9 4 \cdot 2 \\
 \Updownarrow \\
 x &\equiv_9 8
 \end{aligned}$$

Il sistema è quindi equivalente a

$$\begin{cases} x \equiv_5 2 \\ x \equiv_9 8 \end{cases}$$

Applico TCR

La soluzione esiste ed è unica modulo (45)

Soluzione:

$$\bar{x} \equiv_{45} 2 \cdot 9 \cdot m_1 - 1 \cdot 5 \cdot m_2.$$

$$\text{Dove : } \begin{cases} 5m_2 \equiv_9 1 \\ 9m_1 \equiv_5 1 \end{cases} \quad \text{Divisione euclidea}$$

$$\begin{aligned}
 9 &= 5 + 4 \\
 5 &= 4 + 1 \\
 1 &= 5 - 4 \\
 1 &= 5 - (9 - 5) \\
 1 &= 2 \cdot 5 - 9
 \end{aligned}$$

$$\Rightarrow m_2 = 2 \quad m_1 = -1$$

$$\bar{x} \equiv_{45} -18 - 10 \equiv_{45} -28.$$

3 Azioni di gruppi

Definizione 1

Un'azione di un gruppo (G, \cdot) su un insieme X è un'applicazione

$$\begin{aligned} G \times X &\rightarrow X \\ (g, x) &\rightarrow g.x \end{aligned}$$

tale che

- 1) $e.x = x$
- 2) $(f \cdot g).x = f(g.x) \quad \forall f, g \in G \quad \forall x \in X$

Esempi:

- 1) $(G, *)$ gruppo scelgo $X = G$ agisce per moltiplicazione sinistra

$$\begin{aligned} G \times X &\rightarrow X \\ (g, x) &\rightarrow g^*x \end{aligned}$$

- 2) $G = S_n \quad X = \{1, \dots, n\}$

$$\begin{aligned} S_n \times X &\rightarrow X \\ (\sigma, x) &\rightarrow \sigma(x) \end{aligned}$$

- 3) $n, m \in \mathbb{Z}^+$
 $G := GL_n(\mathbb{R}) \times GL_m(\mathbb{R})$
 $X = Mat_{n,m}(\mathbb{R})$

$$\begin{aligned} G \times X &\rightarrow X \\ (AB, C) &\rightarrow BCA^{-1} \end{aligned}$$

- 4) $G = GL_n(\mathbb{R}) \quad X = \mathbb{R}^n$

$$\begin{aligned} G \times X &\rightarrow X \\ (A, v) &\rightarrow Av \end{aligned}$$

- 5) $G = GL_n(\mathbb{R}) \quad X = Mat_{n,m}(\mathbb{R})$

$$\begin{aligned} G \times X &\rightarrow X \\ (A, C) &\rightarrow ACA^{-1} \end{aligned}$$

- 6) (G, \cdot) gruppo $X = G$

$$G \times X \rightarrow X$$

$$(g, x) \rightarrow g * x * g^{-1}$$

Definizione 2

Data un'azione di un gruppo G su un insieme X si dice transitiva se

$$\forall x, y \in X \quad \exists g \in G \text{ tale che } g.x = y.$$

Definizione 3

Un'azione si dice semplicemente transitiva se

$$\forall x, y \in X \quad \exists g \in G \text{ tale che } g.x = y.$$

Esercizio:

- 1) Dimostrare che gli esempi dati sono azioni
- 2) stabilire quali degli esempi sono semplicemente transitivi, transitivi o nessuna delle due

Notazione 1

Scriveremo $G \curvearrowright X$ per indicare che il gruppo G agisce sull'insieme X

Definizione 4

$G \curvearrowright X$, Dato $x \in X$ definiamo:
 \cdot l'orbita di x come il sottoinsieme

$$O_x = \{g.x | g \in G\} \subseteq X.$$

lo stabilizzatore di x il sottogruppo:

$$Stab_x = \{g \in G | g.x = x\} \subseteq G.$$

Esercizio:

Dimostra che lo stabilizzatore di ogni elemento è sempre un sottogruppo (non necessariamente normale)

Esercizio:

Sia G gruppo finito ($|G| < +\infty$) con $G \curvearrowright X$, per ogni $x \in X$ si ha:

- 1) $|Stab_x| < +\infty$ (banale)
- 2) $|O_x| < +\infty$
- 3) $|G| = |O_x| |Stab_x|$

Suggerimento:

- 2) Abbiamo un'applicazione suriettiva

$$G \rightarrow O_x$$

$$g \rightarrow g.x$$

3) L'idea è di dimostrare che esiste una corrispondenza biunivoca fra gli elementi dell'orbita e i laterali sinistri dello stabilizzatore, poi concludete ricordando che $[G : Stab_x] = \frac{|G|}{|Stab_x|}$ (numero di laterali sinistri)

Idea(per la corrispondenza biunivoca)

Verificare che $\forall g, f \in G$

$$g \equiv f \text{ mod}(Stab_x)$$

$$\Updownarrow$$

$$g.x = f.x$$

Teorema 2 (Cauchy)

Sia G un gruppo finito, Sia p primo tale che $p \mid |G|$

Allora esistono (almeno) $p - 1$ elementi di ordine p in G

Dimostrazione

1) In generale se $G \curvearrowright X$ allora X è unione disgiunta di orbite

Definiamo la relazione di equivalenza su X come $x \sim y \Leftrightarrow \exists g \in G \text{ tale che } g.x = y$.

Basta dimostrare che è una relazione d'equivalenza

2) $X = \{(g_1, \dots, g_n) \in G \times \dots \times G \mid g_1 \cdot \dots \cdot g_n = e\}$

Vogliamo definire un'azione del gruppo ciclico $C_p = \langle p \rangle$ su X

$$C_p \times X \rightarrow X$$

$$\rho.(g_1, \dots, g_p) \rightarrow (g_2, g_3, \dots, g_p, g_1)$$

Verifichiamo che l'azione sia ben definita ovvero che

$$\rho.(g_1, \dots, g_p) \in X \quad \forall (g_1, \dots, g_p) \in X$$

$$g_2 \cdot \dots \cdot g_p g_1 = (g_1^{-1} g_1)(g_2 \cdot \dots \cdot g_p) g_1 = g_1^{-1} (g_1 \cdot \dots \cdot g_p) g_1 = g_1^{-1} g_1 = e.$$

3) Studio $|X|$ abbiamo $|X| = |G|^{p-1}$ infatti:

$$\forall (g_1, \dots, g_{p-1}, g_p) \in X \text{ dove } g_p = (g_1, \dots, g_{p-1})^{-1} \Rightarrow \text{in particolare } p \mid |X|$$

4) Studiamo le orbite dell'azione $C_p \curvearrowright X$, Sappiamo che $|C_p| = |O_x| |Stab_x| \quad \forall x \in X$

$$\text{Quindi } |O_x| = 1 \quad \vee \quad |O_x| = p$$

5) Dato che X è unione disgiunta di orbite e $p \mid |X|$

Allora il numero di orbite formate da (x) unico elemento è un multiplo di p

6) Studio tali orbite

L'orbita $O_{(g_1, \dots, g_p)}$ è formata da un singolo elemento se e solo se

$$g_1 = g_2 = \dots = g_p$$

□

Dunque abbiamo una corrispondenza biunivoca

$$\{O_x : |O_x| = 1\} \leftrightarrow \{g \in G \mid g^p = e\}.$$

Quindi p divide $|\{g \in G \mid g^p = e\}|$

d'ora in poi $A = \{g \in G \mid g^p = e\}$

7) $A \neq \emptyset$ poiché $e \in A$

$$A = \{e\} \cup \{g \in G \mid \text{ord}(g) = p\}.$$

Quindi modulo (p) abbiamo

$$0 \equiv_p 1 + |\{g \in G \mid \text{ord}(g) = 1\}|.$$

Quindi l'insieme di elementi di ordine p in G è non vuoto e

$$|\{g \mid \text{ord}(g) = p\}| \equiv_p p - 1.$$

Deduciamo

$$|\{g \in G \mid \text{ord}(g) = p\}| = kp - 1 \geq p - 1.$$

con $k \in \mathbb{Z}^+$

4 Torniamo alle schede

$$\begin{cases} 3x \equiv_{15} 6 \\ 21x \equiv_{49} 13 \end{cases} \quad \text{La prima congruenza è equivalente a } x \equiv_5 2$$

$$MCD(21, 49) = 7$$

La seconda congruenza significa

$$21x = 13 + 49k \quad k \in \mathbb{Z}.$$

$$21x - 49k = 13$$

$$7(3x - 7k) = 13$$

Osservazione:

Se $MCD(a, n) \nmid b$

allora $ax \equiv_n b$ non ammette soluzioni

Infatti: $d = MCD(a, n)$

con $d \nmid b$ allora

con d divide il membro di sinistra ma non quello di destra

Esercizio

G gruppo $g \in G \quad \text{ord}(g) = n$

Allora, $g^h = g^k$ se e solo se $h \equiv_n k$

Soluzione

Assumiamo che $g^h = g^k$ Divisione Euclidea

$$h - k = qn + r \quad \text{con } 0 \leq r < n$$

Assurdo se $0 < r < n \quad r = 0$

$$h - k = qn \Rightarrow h \equiv_n k$$

Esercizio

per quali $n, m \in \mathbb{Z}$ si ha $2^n + 2^m$ divisibile per 9 **Soluzione**
Studio

$$2^n + 2^m \equiv_9 0$$

$$\Downarrow 2^n \equiv_9 -2^m$$

$$\Downarrow$$

$$2^{n-m} \equiv_9 -1$$

$$\Downarrow$$

$$2^{n-m} \equiv_9 8$$

$$\Downarrow$$

$$2^{n-m} \equiv_9 2^3$$

Sfruttiamo l'esercizio precedente con $G = U_9$
La congruenza è verificata se e solo se

$$n - m \equiv 3 \pmod{\text{ord}_{U_9}([2])}.$$

Lezione 13 Algebra I

Federico De Sisti

2024-11-12

1 Azione di coniugio

Definizione 1

Se G gruppo e $a, b, g \in G$ tali che:

$$a = gbg^{-1}.$$

diremo che a, b sono coniugati

Definizione 2

G gruppo. Allora G agisce su se stesso tramite l'azione di coniugio

$$G \times G \rightarrow G$$

$$g \cdot f = gfg^{-1}$$

Esercizio

Verificare che è un'azione

Teorema 1

G gruppo

1) elementi coniugati hanno lo stesso ordine

2) $|O_a| = [G : C(a)]$ dove

$C(a) := \{g \in G | ga = ag\} \leq G$ (centralizzatore di a) 3) equazione delle classi

$$|G| = |Z(G)| + \sum_{O_a \not\subseteq Z(G)} \frac{|G|}{|C(a)|}$$

Dimostrazione

1) Siano $a, b, g \in G$ tali che $a = gbg^{-1}$ supponiamo che $b^k = e \quad k \in \mathbb{Z}$

Allora $a^k = (gbg^{-1}) \cdot \dots \cdot (gbg^{-1}) = gb^k g^{-1} = e$

Quindi $\text{ord}(a) \leq \text{ord}(b)$.

Per simmetria $b = g^{-1}ag \Rightarrow \text{ord}(b) \leq \text{ord}(a)$

Allora $\text{ord}(a) = \text{ord}(b)$

2) Osserviamo che

$$C(a) = \{g \in G | ga = ag\}$$

$$= \{g \in G | gag^{-1} = a\} \text{ Ricordiamo che :}$$

$$= \text{Stab}_a$$

$$|O_a| \cdot |\text{Stab}_a| = |G|$$

$$\Rightarrow |O_a| = \frac{|G|}{|\text{Stab}_a|} = [G : C(a)]$$

3) se $a \in Z(G)$ allora $O_a = \{a\}$ poiché

$$\forall g \in G \text{ si ha } ga = gag^{-1} = agg^{-1} = a$$

Ricordiamo che G ammette una partizione in G -orbite

$$|G| = |Z(G)| + \sum_{O_a \not\subseteq Z(G)} |O_a|.$$

Dal punto (2) $\Rightarrow |O_a| = \frac{|G|}{|C(a)|}$

$$|G| = |Z(G)| + \sum_{O_a \not\subseteq Z(G)} \frac{|G|}{|C(a)|}.$$

Esempio (dalla nuova scheda)

$n \geq 3$ intero dispari $G = D_n$

$Z(D_n) = \{Id\}$ infatti $\rho^i \sigma = \sigma \rho^{n-i}$

Quindi

1) $O_\sigma = \{Id\}$

2) $O_{\rho^i} = ?$

Idea $|O_{\rho^i}| = [D_n : C(\rho^i)]$

$C(\rho^i) = \{\rho^i | i = 0, \dots, n-1\}$

$\Rightarrow |C(\rho^i)| \geq n$

Dato che $C(\rho^i) \leq D_n$ allora $|C(\rho^i)| = n$ oppure $|C(\rho^i)| = 2n$

Ma $\sigma \rho^i = \rho^{n-i} \sigma \neq \rho^i \sigma \quad \forall 0 < i < n$

$\Rightarrow |O(\rho^i)| = n$

Quindi

$O_{\rho^i} = [D_n : C(\rho^i)] = \frac{2n}{n} = 2$

Basta ora trovare un altro elemento coniugato a ρ^i ($0 < i < n$)

$$\sigma \rho^i \sigma^{-1} = \rho^{n-i} \sigma \sigma^{-1} = \rho^{n-i}.$$

quindi $O_{\rho^i} = \{\rho^i, \rho^{n-i}\} \quad \forall 0 < i < n$

3) $O_\sigma = \{\sigma, ?\}$

Studiamo $C(\sigma)$

σ non commuta con $\rho^i \quad \forall 0 < i < n$

Se σ commuta con $\sigma \rho^i$ con $0 < i < n$

Allora σ commuta anche con il prodotto $\sigma(\sigma \rho^i) = \rho^i$ assurdo

$C(\sigma) = \{Id, \sigma\}$

Quindi $|O|_\sigma = [D_n : C(\sigma)] = \frac{2n}{2} = n$

$\Rightarrow O_\sigma = \{\sigma \rho^i | 0 \leq i < n\}$

Equazione delle classi.

$$|D_n| = |Z(D_n)| + \sum_{O_a \not\subseteq Z(D_n)} |O_a|$$

$$2n = 1 + 2 + \dots + 2 + n.$$

□

Teorema 2

G gruppo tale che $|G| = p^k$ p primo $k > 0$.

Allora:

1) $Z(G) \neq \{e\}$

2) $[G : Z(G)] \neq p$

Dimostrazione

1) **IDEA** equazioni delle classi

$$|G| - |Z(G)| = \sum_{O_a \not\subseteq Z(G)} \frac{|G|}{|C(a)|}.$$

modulo (p) avremmo

$$|Z(G)| \equiv_p 0.$$

$$|Z(G)| \neq 1 \Rightarrow Z(G) \neq \{e\}$$

$$\text{Attenzione, } \frac{|G|}{|C(a)|} = 1 \Rightarrow C(a) = G \Rightarrow a \in Z(G) \Rightarrow O_a = \{a\} \subseteq Z(G)$$

Supponiamo per assurdo che

$$[G : Z(G)] = p$$

$$\Rightarrow \frac{|G|}{|Z(G)|} = p \Rightarrow |Z(G)| = p^{k-1}$$

Consideriamo $g \notin Z(G)$

$$\Rightarrow C(g) \supseteq Z(G) \cup \{g\}$$

$$\Rightarrow \Rightarrow |C(g)| = p^{k-1} + 1$$

$$\Rightarrow |C(g)| = p^k \Rightarrow C(g) = G$$

$$\Rightarrow g \in Z(G) \text{ assurdo}$$

□

Corollario 1 (Classificazione dei gruppi di ordine p^2)

G gruppo tale che $|G| = p^2$ con p primo.

Allora $G \cong C_{p^2}$ oppure $G \cong C_p \times C_p$

Dimostrazione

IDEA CHIAVE Se $|G| = p^2$ allora G è abeliano.

Infatti dal teorema:

$$\cdot Z(G) \neq \{e\}$$

$$\cdot |Z(G)| \neq p \text{ perché avremmo } [G : Z(G)] = p$$

allora per Lagrange

$$|Z(G)| = p^2 \Rightarrow Z(G) = G \Rightarrow G \text{ abeliano}$$

Ora se $\exists g \in G$ tale che $\text{ord}(g) = p^2$ allora $G \cong C_{p^2}$

Se invece non esistono elementi di ordine p^2 allora tutti gli elementi ($\neq e$) in G hanno ordine p

Sia $h \in G$ tale che $h \neq e \Rightarrow H := \langle h \rangle$ con $|H| = p$

Sia $k \in G \setminus H$

$$\Rightarrow K := \langle k \rangle \text{ con } |K| = p$$

Verifichiamo che G è prodotto diretto interno di H e K

$\cdot H \trianglelefteq G$ e $K \trianglelefteq G$ (poiché G abeliano)

$H \cap K = \{e\}$ Infatti:

$$\begin{cases} H \cap K = K \\ H \cap K \neq K \end{cases} \Rightarrow |H \cap K| = 1.$$

$HK = ?$

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

$$\Rightarrow HK = G$$

Allora $G \cong H \times K \cong C_p \times C_p$

□

Osservazione (per $p = 2$)

$G = C_4$ oppure $G \cong K_4 \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$

Osservazione

$p = 3$ $|G| = 9$ allora

$G \cong C_9$ oppure $G \cong C_3 \times C_3$

Esempio(Classi di coniugio in S_n)

Due permutazioni in S_n sono coniugate se e solo se hanno stessa struttura ciclica

Dimostrazione

1) $\tau = (a_1, \dots, a_n) \in S_n$ un k -ciclo $\sigma \in S_n$

Studio ora $\sigma\tau\sigma^{-1}$ e la sua azione sull'insieme $\{\sigma(1), \dots, \sigma(n)\}$

Se $\tau(j) = j$

$$\Rightarrow \sigma\tau\sigma^{-1}(\sigma(j)) = \sigma\tau(j) = \sigma(j)$$

Se $j = a_i$ per qualche $1 \leq i \leq k \Rightarrow \tau(j) = \tau(a_i) = a_{i+1 \text{ mod}(k)}$

$$\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma\tau(a_i) = \sigma(a_{i+1 \text{ mod}(k)})$$

Allora

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

2) Se $\tau = \tau_1 \cdot \dots \cdot \tau_h$ con τ_i k_i -ciclo

Allora

$$\sigma\tau\sigma^{-1} = \sigma\tau_1 \cdot \dots \cdot \tau_h\sigma^{-1} = (\sigma\tau_1\sigma^{-1}) \dots (\sigma\tau_h\sigma^{-1})$$

□

Lezione 15 Algebra I

Federico De Sisti

2024-11-19

1 Nella lezione precedente..

Teorema 1 (1° Teorema di Sylow)
 p primo che divide $|G|$ Allora $Syl_p(G) \neq \emptyset$

Teorema 2 (2° Teorema di Sylow)
 p primo divide $|G|$ allora:

$$\forall H, K \in Syl_p(G) \quad \exists g \in G \text{ tale che } H = gKg^{-1}.$$

2 Roba nuova

Corollario 1
 p primo che divide $|G|$ allora $H \in Syl(G)$ è normale se e solo se $n_p = |Syl_p(G)| = 1$

Osservazione

è importante sapere se $n_p = 1$ perché l'esistenza di sottogruppi normali spesso permette di realizzare un gruppo come prodotto semidiretto

Teorema 3 (3° teorema di Sylow)
 G gruppo finito

- $|G| = p^r m$
- $r, p, m \in \mathbb{Z}_{>0}$
- p primo
- $MCD(p, m) = 1$

Allora:

- 1) $n_p = [G : N_G(H)]$ dove $H \in Syl_p(G)$
- 2) $m \equiv_{n_p} 0$
- 3) $n_p \equiv_p 1$

Prima della dimostrazione vogliamo estendere la nozione di centralizzatore (o centralizzante)

Definizione 1 (Normalizzatore)

G gruppo $S \subseteq G$ sottoinsieme

1) Il centralizzatore di S in G è

$$C(S) = \{g \in G \mid gs = sg \quad \forall s \in S\}.$$

2) Il normalizzatore di S in G è

$$N_G(S) = \{g \in G \mid gS = Sg\}.$$

Esercizio:

Dimostrare che

1) Se $S \subseteq G \Rightarrow C(S) \leq G$

2) $S \subseteq G \Rightarrow N_G(S) \leq G$

3) $S \leq G \Rightarrow S \leq N_G(S)$

Dimostrazione

Considero l'azione

$$G \times \text{Syl}_p(G) \rightarrow \text{Syl}_p(G)$$

$$(g, H) \rightarrow g.H := gHg^{-1}$$

Allora $\forall H \in \text{Syl}_p(G)$

$$p^r m = |G| = [G : \text{Stab}_H] \cdot |\text{Stab}_H|$$

$$= [G : N_G(H)] \cdot |N_G(H)| \quad (\text{dato che } \text{Stab}_H = N_G(H))$$

$$= [G : B_G(H)] [N_G(H) : H] |H| \quad (\text{dato che } H \leq N_G(H))$$

$$\text{Deduciamo che } m = [G : N_G(H)] \cdot [N_G(H) : H]$$

Ora:

$$n_p = |\text{Syl}_p(G)| = |O_H^G| \quad (\text{II Teorema di Sylow})$$

$$= [G : \text{Stab}_H]$$

Quindi abbiamo dimostrato (1) e (2)

Resta da dimostrare (3)

di un fissato $K \in \text{Syl}_p(G)$

$$K \times \text{Syl}_p(G) \rightarrow \text{Syl}_p(G).$$

$$(k, H) \rightarrow k.H := kHk^{-1}.$$

Questa azione avrà $r + 1$ orbite (con $r \geq 0$)

$$O_K^K, O_{H_1}^K, \dots, O_{H_r}^K$$

Abbiamo una decomposizione in orbite disgiunte

$$\text{Syl}_p(G) = O_K^K \cup O_{H_1}^K \cup \dots \cup O_{H_r}^K.$$

$$\Rightarrow n_p = |\text{Syl}_p(G)| = |O_K^K| + \sum_{j=1}^r |O_{H_j}^K|$$

$$= |O_K^K| + \sum_{j=1}^r [K : \text{Syl}_{H_j}^K].$$

$$= |O_K^K| + \sum_{j=1}^r [K : N_K(H_j)].$$

Idea

Basta ora verificare che

- $|O_K^K| = 1$
- $O_{H_j}^K \equiv_p 0 \quad \forall 1 \leq j \leq r$

Abbiamo:

$$O_K^K = [K : N_K(K)] = 1.$$

Dato che $H \leq N_G(H) \leq G \Rightarrow N_K(K) = K$

$$|O_{H_j}^K| = [K : N_K(H_j)] = \frac{|K|}{|N_K(H_j)|} = \frac{p^r}{|N_K(H_j)|}.$$

dato che $K \in \text{Syl}_p(G)$

Quindi resta da escludere il caso $N_K(H_j) = K$

Ma questo è equivalente a $KH_j = H_jK$

$$\Rightarrow \begin{cases} KH_j \leq G \\ |KH_j| = \frac{|K||H_j|}{|K \cap H_j|} = \frac{p^{2r}}{p^{s_j}} \end{cases}.$$

dove $0 \leq s_j < r$ dato che $H_j \neq K_j$

Ma $p^{2r-s_j} \nmid p^r m$ da cui l'assurdo per Lagrange

□

3 Applicazioni di Sylow

Possiamo (ri)-dimostrare un vecchio risultato

Teorema 4 (Cauchy)

G gruppo finito, p primo che divide $|G|$ allora

$g \in G$ tale che

$$\text{ord}(g) = p.$$

Dimostrazione

Da Sylow I segue che esiste $H \in \text{Syl}_p(G)$

Scegliamo $h \in H$ tale che $h \neq e$

Ora $\text{ord}(h) = p^s$ per qualche $s > 0$

Definiamo $f = h^{p^{s-1}}$

$$f = h^{p^{s-1}} \neq e \Rightarrow \text{ord}(h) \neq 1$$

$$f^p = (h^{p^{s-1}})^p = h^{p^s} = e \Rightarrow \text{ord}(f) = p$$

□

Teorema 5 (Wilson)

p primo allora $(p-1)! \equiv_p p-1$

Dimostrazione

Scelgo $G = S_p$ Studio n_p

I p -Sylow in S_p hanno ordine p

\Rightarrow sono tutti i sottogruppi ciclici di ordine p in S_p

· Gli unici elementi di ordine p in S_p sono i p -cicli.

fissato il primo elemento, abbiamo $p-1$ scelte per il secondo, $p-2$ per il terzo e così via

quindi i p -cicli sono $(p-1)!$

Quindi i sottogruppi di S_p di ordine p sono $\frac{(p-1)!}{(p-1)} = (p-2)!$ perché in ogni tale sottogruppo appaiono $p-1$ p -cicli

$\Rightarrow (p-2)! = n_p \equiv_p 1 \Rightarrow (p-1)! \equiv_p p-1$

□

Teorema 6 (Classificazione dei gruppi pq)

G gruppo finito, $p, q > 1$ tali che

· p, q primi

· $p < q$

· $|G| = pq$

Allora

1) Se $p \nmid q-1$ allora $G \cong C_{pq}$

2) Se $p \mid q-1$ allora $G \cong C_q \rtimes C_p$

Dimostrazione

Studio n_p

$$\begin{cases} p = m \equiv_{n_q} 0 \\ n_q \equiv_q 1 \end{cases}$$

$$\Rightarrow \begin{cases} n_q = 1 \text{ oppure } m_q = p \\ \text{seconda esclude } n_q = p \text{ perchè } p < q \end{cases}$$

$\Rightarrow n_q = 1$

$\Rightarrow \exists! Q \in \text{Syl}_p(G)$

$\Rightarrow Q \trianglelefteq G$ e $|G| = q \Rightarrow Q \cong C_q$

Studio n_p nel caso $p \nmid q-1$

$$\begin{cases} q \cdot m \equiv_{n_p} 0 \\ n_p \equiv_p 1 \end{cases} \Rightarrow n_p = 1 \text{ oppure } n_p = q$$

$\Rightarrow n_p \neq q$ perché

$q \not\equiv_p 1$ per ipotesi

$n_p = 1 \Rightarrow \exists! P \in \text{Syl}_p(G)$

$\Rightarrow PG$ e $|P| = p \Rightarrow P \cong C_p$

Ora abbiamo due sottogruppi normali $P, Q \trianglelefteq G$ tali che

· $P \cap Q = \{e\}$ perchè $|P \cap Q|$ divide sia $|P| = p$ che $|Q| = q$

· $|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq = |G|$

$\Rightarrow G \cong P \times Q \cong C_p \times C_q \cong C_{pq}$

Resta il caso $p|q-1$

· $\exists! Q \in \text{Syl}_p(G) \rightsquigarrow Q \trianglelefteq G$

· $\exists P \in \text{Syl}_p(G) \rightsquigarrow P \leq G$

Ora

· $P \cap Q = \{e\}$ come prima

$PQ = G$ come prima

Quindi G prodotto semidiretto interno

$\Rightarrow G \cong Q \rtimes_{\phi} P \Rightarrow C_q \rtimes_{\phi} C_p$

per qualche omomorfismo $\phi : C_p \rightarrow \text{Aut}(C_q)$

□

Esercizio:

Classificare i gruppi di ordine $2q$ con $q > 2$ primo

Lezione 16 Algebra I

Federico De Sisti

2024-11-21

1 OPIS

il codice opis del corso è

7K817KGS.

2 Cazzi e mazzi

2.1 Ricordo:

Teorema 1

$p < q$ primi G gruppo finito di ordine pq

Allora:

- se $p \nmid q+1$ allora $G \cong C_{pq}$
- se $p \mid q+1$ allora $G \cong C_q \rtimes C_p$

Inserisci tabella fino ad ordine 9

Corollario 1

$q > 2$ primo, G gruppo di ordine $2q$

Allora $G \cong C_{2q}$ oppure $G \cong D_q$

Dimostrazione

Dal teorema basta studiare gli omomorfismi

$$\begin{aligned}\phi : C_2 &\rightarrow \text{Aut}(G) \\ s &\rightarrow (\phi_s : r \rightarrow s)\end{aligned}$$

Affinchè ϕ sia un omomorfismo, dato che $\text{ord}_{C_2}(s) = 2$

dobbiamo imporre che $\text{ord}_{\text{Aut}(G)}(\phi_s) \in \{1, 2\}$

Se è uguale a 1 $\phi_s = \text{Id} \Rightarrow \phi$ omomorfismo banale

\Rightarrow il prodotto è diretto

$\Rightarrow G \cong C_q \times C_2 \cong C_{2q}$

Nell'altro caso $\text{ord}_{\text{Aut}(G)}(\phi_s) = 2$

$\Rightarrow \phi_s \circ \phi_s = \text{Id}_{C_q} \Rightarrow \phi_s(\phi_s(r)) = r$

$\phi_s(r^k) = r$

$\Rightarrow k^2 \equiv_{\text{ord}_{C_1}(r)} 1 \Rightarrow k^2 \equiv_q 1$

$\Rightarrow (k-1)(k+1) \equiv_q 0$

$\Rightarrow k \equiv_q \pm 1$

Se $k \equiv_q 1$

$\Rightarrow \phi_s = \text{Id}_{C_q} \Rightarrow G \cong C_{2q}$

Se $k \equiv_q -1$

$\Rightarrow \phi_s(r) = r^{-1}$

$\Rightarrow G \cong C_q \rtimes C_2 \cong D_q$ (già visto)

□

3 Gruppi di ordine 12

Studiamo G tramite i teoremi di Sylow

$$\cdot Syl_2(G) \neq \emptyset$$

$$\cdot Syl_3(G) \neq \emptyset$$

Dal Sylow III abbiamo

$$\begin{cases} n_2 \equiv_2 1 \\ 3 \equiv_{n_2} 0 \end{cases}.$$

$\Rightarrow n_2 = 1$ oppure $n_2 = 3$

Dal Sylow II

$$\begin{cases} n_3 \equiv_3 1 \\ 4 \equiv_{n_3} 0 \end{cases}.$$

$n_3 = 1$ oppure $n_3 = 4$

Osservazione:

Esiste un sottogruppo normale in G

Dimostrazione

se $n_3 = 4$

Allora in G esistono 4 sottogruppi di ordine 3

Ognuno dei quali contenente due elementi di ordine 3.

Quindi G contiene 8 elementi di ordine 3.

Quindi i restanti 3 elementi di ordine diverso da 3 formano necessariamente l'unico 2-Sylow □

Esercizio:

Se $|G| = 12$ e $n_3 = 4$ allora esiste un omomorfismo iniettivo $G \rightarrow S_4$

Nota

Da questo segue che $G \cong A_4$ perchè A_4 è l'unico sottogruppo di ordine 12 in S_4

Dimostrazione

$$G \times Syl_3(G) \rightarrow Syl_3(G)$$

$$(g, H) \rightarrow gHg^{-1}$$

$$n_3 = 4$$

$$\Rightarrow Syl_3(G) = \{H_1, H_2, H_3, H_4\}$$

Definiamo

$$\psi : G \rightarrow S_4$$

$$g \rightarrow \tau_g$$

$$\tau_g(i) = j \Leftrightarrow gHg^{-1} = H_j \text{ con } i \in \{1, 2, 3, 4\} \text{ (Questa è l'idea da utilizzare negli esercizi delle schede)}$$

Verifiche:

1) ψ è ben definita, Infatti τ_g è invertibile con inversa $\tau_{G^{-1}}$

2) ψ è un omomorfismo, ovvero

$$\psi(gf) = \psi(g)\psi(f).$$

$$\begin{aligned}
& \tau_{gf}(i) = j \\
& \Leftrightarrow (gf)H(gf)^{-1} = H_j \\
& \Leftrightarrow g(fHf^{-1})g^{-1} = H_j \\
& \Leftrightarrow \tau_g(\tau_f(i)) = j \\
& 3) \psi \text{ iniettiva} \\
& \text{supponiamo che } \tau_g = \tau_f \\
& gHg^{-1} = fHf^{-1} \quad \forall H \in \text{Syl}_3(G) \\
& \Rightarrow (f^{-1}g)H(f^{-1}g)^{-1} = H \quad \forall H \in \text{Syl}_3(G) \\
& \Rightarrow f^{-1}g \in N_G(H) \quad \forall H \in \text{Syl}_3(G) \\
& \Rightarrow f^{-1}g \in \bigcap_{H \in \text{Syl}_3(G)} N_G(H) \\
& \Rightarrow f^{-1}g \in \bigcap_{H \in \text{Syl}_3(G)} H = \{e\} \Rightarrow f^{-1}g = e \Rightarrow f = g \\
& \text{Resta da verificare che } H = N_G(H) \\
& 4 = n_3 = [G : N_G(H)] = \frac{|G|}{|N_G(H)|} = \frac{12}{|N_G(H)|} \Rightarrow |N_G(H)| = 3 \\
& \text{Ma } H \leq N_G(H) \Rightarrow H = N_G(H)
\end{aligned}$$

□

3.1 Studiare gruppi di ordine 12 in cui $n_3 = 1$

Da Sylow III Segue che $\exists! Q \in \text{Syl}_3(G) \Rightarrow Q \trianglelefteq G$

Esiste in G almeno un 2-Sylow $P \leq G$

Ora:

$$G \trianglelefteq G, \quad P \leq G$$

$$Q \cap P = \{e\} \quad (\text{perch\`e } \text{MCD}(|Q|, |P|) = 1)$$

$$|QP| = \frac{|Q||P|}{|Q \cap P|} = \frac{3 \cdot 4}{1} = 12$$

$$\Rightarrow QP = G$$

Allora $G \cong Q \rtimes_{\phi} P$ per qualche

$$\phi : P \rightarrow \text{Aut}(Q) \cong C_2$$

Quindi studiamo i possibili omomorfismi

$$\phi : P \rightarrow \text{Aut}(C_3)$$

se $P \cong C_4$

$$C_4 = \langle \gamma \rangle \quad C_3 = \langle r \rangle$$

$$\phi : \langle \gamma \rangle \rightarrow \text{Aut}(C_3)$$

$\gamma \rightarrow (\phi_{\gamma} : r \rightarrow r^k \text{ con } k \pm 1)$ nel caso $k = 1$ abbiamo ϕ banale

\Rightarrow prodotto diretto

$$\Rightarrow G \cong C_3 \times C_4 \cong C_{12}$$

nel caso $k = -1$

$$\text{abbiamo } G \cong C_3 \rtimes_{\phi} C_4 \cong \text{Dic}_3$$

dove

$$\phi : C_4 \rightarrow \text{Aut}(C_3)$$

$$\gamma \rightarrow (\phi_{\gamma} : r \rightarrow r^{-1})$$

$$\begin{aligned}
P &\cong K_4 \\
\phi : K_4 &\rightarrow \text{Aut}(C_3) \\
&\{Id, a, b, ab\} \\
a &\rightarrow (\phi_a : r \rightarrow r^{\pm 1}) \\
b &\rightarrow (\phi_b : r \rightarrow r^{\pm 1}) \\
ab &\rightarrow (\phi_{ab} : r \rightarrow r^{\pm 1})
\end{aligned}$$

Se ϕ è banale

\Rightarrow prodotto diretto

$$\Rightarrow G \cong C_3 \times K_4$$

$$\cong C_3 \times C_2 \times C_2$$

$$\cong C_6 \times C_2$$

Se ϕ è non banale, a meno di rinominare gli elementi $\{a, b, ab\}$ avremo che

$$\phi_a r \rightarrow r$$

$$\phi_b r \rightarrow r^{-1} \text{ Grazie (!) a Esercizio 1 di scheda 7 tutti i restanti prodotti}$$

$$\phi_{ab} r \rightarrow r^{-1}$$

semidiretti sono isomorfi

$$G \cong C_3 \rtimes_{\phi} K_4 \cong D_6$$

Infatti $|D_6| = 12$

D_6 non è isomorfo ad alcuno dei precedenti casi

1) C_2 è ciclico

2) $C_6 \times C_2$ è abeliano, ma non ciclico

3) A_4 unico caso in cui $n_3 = 4$

4) Dic_3 non è abeliano e contiene elementi di ordine 4

5) D_6 non è abeliano e non contiene elementi di ordine 4 (C_4)

Definizione 1 (Radice primitiva modulo (n))

Un intero a si definisce radice primitiva modulo (n) se $\text{ord}_{U_n}([a]) = \phi(n)$

Osservazione:

Per teorema di Eulero

$$a^{\phi(n)} \equiv_n 1.$$

$$\Rightarrow \text{ord}_{U_n}([a]) = \phi(n)$$

Osservazione

a radice primitiva mod (n) significa che $U_n = \langle [a] \rangle$

Obiettivo (Scheda 7)

Dimostrare che se $p > 1$ primo allora \exists radice primitiva modulo (p)

Esempi

Non esistono radici primitive mod(8)

$$\text{Studio } U_8 = \{[1], [3], [5], [7]\}$$

$$\phi(8) = 2^3 - 2^2 = 4.$$

$$1^2 \equiv_8 1$$

$$3^2 \equiv_8 1$$

$$5^2 \equiv_8 1$$

$$7^2 \equiv_8 1$$

Es(ercizio esempio)

3 è radice primitiva mod(7)

Svolgimento:

$$3^1 \equiv_7 3$$

$$3^2 \equiv_7 2$$

$$3^3 \equiv_7 1$$

$$3^4 \equiv_7 3$$

$$3^5 \equiv_7 2$$

$$3^6 \equiv_7 1$$

2 è radice primitiva mod(9)

Da fare

Esercizio(Scheda 7)

Dimostrare che

$$\text{Aut}(C_p) \cong C_{p-1}$$

Soluzione

Sappiamo che

$$\text{Aut}(C_p) \cong U_p \cong C_{\phi(p)} \cong C_{p-1}$$

Esercizio

p primo

$$f(x) = a_n x^n + \dots + a_1 x + a_0$$

$f(x) \equiv_p 0$ ammette al più p soluzioni distinte in $\mathbb{Z}/(p)$

Dimostrazione

per induzione su n

$$\text{se } n = 1 \Rightarrow a_1 x \equiv_p -a_0$$

$$\Rightarrow x \equiv_p -a \cdot a_1^{-1}$$

$n > 1$

$$\text{Se } f(x) \equiv_p 0$$

non ammette soluzioni ok

Se invece a è soluzione dividiamo

$$f(x) = (x - a)q(x) + r$$

$$\Rightarrow f(x) \equiv_p (x - a)q(x) + r$$

Valuto in a :

$$\Rightarrow 0 \equiv_p f(a) \equiv_p (a - a)q(a) + r$$

$$\Rightarrow f(x) \equiv_p (x - a)q(x)$$

$$\text{Sia } b \not\equiv_p a \text{ tale che } f(b) \equiv_p 0$$

$$0 \equiv_p f(b) \equiv_p (b - a)q(b)$$

$\mathbb{Z}/(p)$ dominio d'integrità

$$q(b)_p 0$$

a_1 invertibile in $\mathbb{Z}/(p)$ per ipotesi

*Ma per induzione $q(x) \equiv_p 0$
ammette al più $n - 1$ soluzioni distinte
 $\Rightarrow f(x) \equiv_p 0$ ammette al più n soluzioni*

□

Lezione 17 Algebra I

Federico De Sisti

2024-11-26

1 Ricordo (Lagrange)

$f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ tale che $a_n \not\equiv_p 0$ con $p > 1$ primo
Allora $f(x) \equiv_p 0$ ammette al più n soluzioni

Corollario 1 (Esercizio)

Dimostrare che se p primo e $d|(p-1)$ allora $x^d - 1 \equiv_p 0$ ammette esattamente d soluzioni

Dimostrazione (Soluzione)

Abbiamo che se $d|(p-1)$ allora $(x^d - 1)|(x^{p-1} - 1)$

$\Rightarrow x^{p-1} = (x^d - 1)f(x)$

dove f è di grado $(p-1-d)$

Ora $x^{p-1} \equiv_p 1$ ammette $p-1$ soluzioni distinte per il piccolo teorema di Fermat.

Le soluzioni sono $1, 2, \dots, p-1$

Se una di tali soluzioni non risolve $f(x) \equiv_p 0$ allora risolve $x^d - 1 \equiv_p 0$ (Sto usando il fatto che $\mathbb{Z}/(p)$ è un dominio d'integrità [prodotto commutativo e se il prodotto tra due numeri è 0 allora o uno o l'altro sono 0])

Dato che $f(x) \equiv_p 0$ ammette al più $p-1-d$ soluzioni distinte deduciamo che $x^d - 1 \equiv_p 0$ ammette almeno $d = (p-1) - (p-1-d)$ soluzioni distinte in $\mathbb{Z}/(p)$.

D'altra parte per l'esercizio precedente ne ammette al più d , e quindi segue la tesi. \square

Corollario 2 (Esercizio)

$p > 1$ primo, $d|(p-1)$ Allora, esistono esattamente $\phi(d)$ interi, distinti in U_p , di ordine d in U_p

Dimostrazione (Soluzione)

Introduco $S_d = \{k \in \mathbb{Z} | \text{ord}_{U_p}([k]) = d, \quad 1 \leq k \leq p-1\}$

La tesi è equivalente a dimostrare che $|S_d| = \phi(d)$

Abbiamo una partizione $\{1, \dots, p-1\} = \bigcup_{d|p-1} S_d$

Quindi $p-1 = \sum_{d|(p-1)} |S_d|$

Ricordo:

$n = \sum_{d|n} \phi(d)$ (esercizio delle vecchie schede)

Scegliendo $n = p-1$ deduciamo

$\sum_{d|p-1} |S_d| = \sum_{d|p-1} \phi(d)$

Basta allora dimostrare che $|S_d| \leq \phi(d) \quad \forall d|p-1$

Se $S_d = \emptyset \Rightarrow |S_d| = 0 \leq \phi(d)$

Se $S_d \neq \emptyset \Rightarrow \exists a \in S_d$

$\Rightarrow \{a, a^2, a^3, \dots, a^d\}$ sono tutti distinti mod(p) infatti

$$a^i \equiv_p a^k$$

$$\Downarrow$$

$$i \equiv_d j$$

Quindi a, a^2, \dots, a^n sono tutte e sole le soluzioni di $x^d - 1 \equiv_p 0$. Quindi gli elementi di ordine d in U_p sono della forma a^j per qualche $j \in \{1, \dots, j\}$

Ma $\text{ord}([a^j]) = \frac{d}{\text{MCD}(j,d)}$ (esercizio di una riga)

Quindi $|S_d| = \phi(d)$

□

Corollario 3

Esercizio $p > 1$ primo:

Allora esistono esattamente $\phi(p-1)$ radici primitive distinte

Dimostrazione (Soluzione)

Basta applicare l'esercizio precedente, scegliendo $d = p-1$

□

Esercizio

$p > 1$ primo

dimostrare che $\text{Aut}(C_p) \cong C_{p-1}$

Soluzione:

Sappiamo che $\text{Aut}(C_p) \cong U_p \cong C_{p-1}$

Dove la prima congruenza la sappiamo da teoremi precedenti, la seconda viene data dal precedente corollario

Congettura 1 (Gauss, 1801)

Esistono infiniti primi per cui 10 è una radice primitiva

Congettura 2 (E. Artin, 1927)

$a \in \mathbb{Z}$, $a \neq \pm 1$

Assumiamo che a non sia un quadrato perfetto, Allora esistono infiniti primi per cui a è una radice prima

Osservazione

Oggi sappiamo che la congettura di Artin è vera per infiniti interi a , ma non è noto quali

Esercizio: $p > 1$ primo

Sia $a = x^2$ con $x \in \mathbb{Z}$

Dimostrare che se $[a] \in U_p$

allora $\text{ord}_{U_p}([a]) \neq p-1$

Esercizio [classificazione dei gruppi di ordine pq]

Dimostrare che tutti i gruppi non ciclici di ordine pq con $p \neq q$ primi, sono fra

loro isomorfi e non abeliani

Soluzione

Dato G tale che $|G| = pq$ Avevamo dimostrato che $\exists! Q \in Syl_q(G) \Rightarrow Q \trianglelefteq G$

Inoltre $\exists P \in Syl_p(G) \Rightarrow P \leq G$

Abbiamo verificato che:

$$P \cap Q = \{e\}$$

$$|PQ| = |G| \Rightarrow PQ = G$$

$$\Rightarrow G \cong Q \rtimes P \cong C_q \rtimes C_p$$