Lezione 1 Algebra

Federico De Sisti

2024-10-01

1 Cosa c'è su e-leaning 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. Hernstein: 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

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

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

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

Nomenclatura 1 (notazione)
$(G, \cdot)$ *dato* $g \in G$ *denotiamo con:*
1) $g^0 = e$
2)$g^1 = g$
3)$g^n = g \cdot \ldots \cdot g 4) g^{-n} = (g^{-1})^n$

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

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

Speciale Se $X = \{1, \ldots, n\}$
Allora chiamiamo
$$S_n = S_X.$$
(è i lgruppo di permutazioni su n elementi)
Si chiama gruppo simmetrico

Definizione 2 (Gruppo diedrale)
$n \geq 3$ Consideriamo l'n-agono regoalre 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)
$(G,)$ 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)
$L(G, \cdot)$ gruppo, l'ordine di G è $|G|$

Definizione 6 (Ordine di un elemento)
$ord(g) = \min\{n \in \mathbb{N} | g^n = e\}$
se $\nexists n \in \mathbb{N}$ tale che $g^n = e$ poniamo $ord(g) = +\infty$

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 cicliclo

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) Trvoare un'applicazione biunivoca $S_3 \to D_3$
2) Dimostrare che non esiste un'applicazione biunivoca $S_4 \to D_4$
3) Dimostrare che i seguenti nkn sono gruppi
$\cdot Mat_{n\times n}(\mathbb{K})$ con prodotto riche per colonne
$GL(\mathbb{K})$ con somma tra matrici
$\mathbb{Z}\mathbb{Q}\mathbb{R} conilprodotto$

Proposizione 1
$(G, \cdot)$ gruppi finito, Allora ogni elemento ah 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

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

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

Definizione 8 (Sottogruppo)
$(G, \cdot)$ gruppo $H \subseteq G$ sottosinsieme, si dice che H è un sottogruppo se $(H, \cdot)$ è un gruppo.
In tal caso scriveremo $H \leq G$

Osservazione
$(G, \cdot)$ gruppo, $G \subseteq G$ sottoinsieme allora $H \leq G$se H è chiuso rispettto a $\cdot$
e H è chiuso rispetto agli inversi
(se $g, h \in G \Rightarrow g \cdot h \in H$ 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 alĺ 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 $ord(h) < +\infty$

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

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

Esempi
1)$C_n \leq D_n$
2) $SL_n(\mathbb{K}) \leq GL_n(\mathbb{K})$
3) $(G, \cdot)$ gruppo $g \in G$

$$< g >= \{g^n \in G | n \in \mathbb{Z}\}.$$

Allora $< g > \leq G$

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

$$f \equiv g \quad mod \quad H.$$

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 $H \to gH \quad \forall g \in G$

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'insimee $\{1, 2, 3\}$
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

$$H_1 =< (1, 2) >= \{id, (1, 2)\}.$$

$$H_2 =< (3, 2, 1) >= \{id, (3, 2, 1), (2, 3, 1)\}.$$

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 $\phi : H \to gH$
$g \to g \cdot h$
Soluzione
ϕ è suriettiva per definizione di gH
è anche iniettiva infatti se $h_1, h_1 \in H$ soddisfano

$$gh_1 = gh_2 \quad .$$

allora $h_1 = h_2$ (per la legge di cancellazione)
Ossercazione
$(G, \cdot)$ 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 $H \trianglelefteq G$
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
$H \subseteq G \Rightarrow [G : H] = \dfrac{|G|}{|H|}$

Teorema 1 (Lagrange)
$(G, \cdot)$ gruppo $H \leq G$ Allora l'ordine di H divide l'ordine di G

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

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* $H = H$

$\square$

Corollario 2
$(G, \cdot)$ *gruppo (finito)*
Dato $g \in G$ *si ha* $ord(g)$ *divide l'ordine di* G

Dimostrazione
Dato $g \in G$ *considero*

$$< g >= \{e, g, g^2, \ldots, g^{n-1}\}$$
$$| < g > | = ord(g).$$

La tesi segue ora da Lagrange $\square$

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* $\square$

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.
$h_1k_1 \in HK$ e $h_2 \cdot k_2 \in HK$

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

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

$$< X >= \bigcap_{H \leq G, X \subseteq H} H.$$

Notazione 4
$\cdot H, K \leq G$

$$< H, K >:=< H \cup K > .$$

$\cdot g_1, , g_n \in G$

$$< g_1, \dots, g_n >:=< \{g_1, \dots, g_n\} > .$$

Caso Speciale
$(G, \cdot) = (\mathbb{Z}, +) \quad m \in \mathbb{Z}$
$(m) :=< m >$

4 Sottogruppi di 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 $H = (m)$ Sicureamente $(m) \subseteq H$ poich$H \leq \mathbb{Z}$
$Viceversasupponiamoche \exists n \in H x(n).$
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:
$1)(a) \cap (b) = (n)$ *dove* $m := mcm\{a, b\}$
$2)(a) + (b) = (d)$ *dove* $d := MCD\{a, b\}$

Osservazione
$(a) + (b)$ è della forma HK con $H = (a)$ e $K = (b)$
inoltre $(a) + (b) \leq \mathbb{Z}$ poich$(\mathbb{Z}, +)$ 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 $d' = d$

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

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

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

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

Allora $d = d'$ □

5 Gruppi D_n e C_n

Ricordo
$n \geq 3$
Fissiamo un $n - agono$
$D_n = \{$isometrie che preservano l'n-agono$\}$
$C_n = \{$isometrie che preserrvano 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
$$C_n =< \rho > .$$
dove ρ è la rotazione di angolo $\frac{2\pi}{n}$ attorno al centro dell'n-agono
Infatti $\rho \in C_n \Rightarrow < \rho > \subseteq C_n$ ma l'ordine di questa rotazione è n

$$| < \rho > | = ord(\rho) = n = |C_n| => C_n =< \rho > .$$

Osservazione
Dalla dimostrazione segue che D_n è costituito da n rotazioni
(della forma $\rho^i \quad i \in \{1, \ldots, n\}$
e n riflessioni

Proposizione 4
$n \geq 3$ *Allora:*
$1) D_n =< \rho, \sigma >$
Dove σ è una rotazione qualsiasi $(\sigma \in D_n \setminus C_n)$
$2) \rho^i \sigma = \sigma \rho^{n-i}$

Dimostrazione

1)Sicuramente $< \rho, \sigma > \subseteq D_n$
$H =< \rho >= \{Id, \rho, \rho^2, \dots, \rho^{n-1}\}$
$K =< \sigma >= \{Id, \sigma\}$
$H \cap K = \{Id\}$

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

$\Rightarrow HK \subseteq D_n$ *(In particolare HK è sottogruppo)* $\Rightarrow D_n = HK =< \rho, \sigma >$
$\rho\sigma$ *non preserva l'orientazione*
$\Rightarrow \rho^i\sigma$ *è riflessione*
$\Rightarrow ord(\rho^i\sigma) = 2$
$\Rightarrow \rho^i\sigma\rho^i\sigma = Id$
$\Rightarrow \rho^i\sigma\rho^i = \sigma$
$\Rightarrow \sigma\rho^i = \rho^{n-1}\sigma$ □

Lezione 3 Algebra I

Federico De Sisti

2024-10-08

1 Altra roba sui gruppi

Proposizione 1 (Caratterizazzione 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* $G/N \times G/N \to G/N$
è ben posta $\qquad (fN, gN) \to fgN$
o equivalentemente $N\backslash G \times n\backslash G \to n\backslash G$
$\qquad (Nf, Ng) \to Nfg$

Dimostrazione
$1 \to 2$
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)*
$2 \to 3$
$\forall g \in G \;\; \forall n \in N$
$gng^{-1} \in N$ *(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 $\to 4$
Datifeg$\in G$ *abbiamo*

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

$4 \to 1$
Per ipotesi 4 $(Nf)(Ng) = Nfg \;\; \forall f, g \in G$ *quindi*

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

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

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

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

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

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

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
<u>Non</u> 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
$\varphi : G_1 \to G_2$ 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

$$\begin{tikzcd} (g, f) \arrow[d] & G_1 \times G_1 \arrow[r, "\cdot"] \arrow[d, "\varphi \times \varphi"'] & G_1 \arrow[d, "\varphi"] & (g, f) \arrow[r] & g \cdot f \arrow[d] \\ (\varphi(g), \varphi(f)) & G_2 \times G_2 \arrow[r, "*"] & G_2 & & \varphi(g \cdot f) \end{tikzcd}$$

Esempi:
$(\mathbb{R},+)$ gruppo additivo reali
$(\mathbb{R}_{>0},\cdot)$ gruppo moltiplicativo reali positivi
Allora
$exp : \mathbb{R} \to \mathbb{R}_{>0}$
$x \to e^x$
è un omomorfismo infatti: $\forall x, y \in \mathbb{R}$

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

Esempio
$ln : \mathbb{R}_{>0} \to \mathbb{R}$
$x \to ln(x)$
è un omomorfismo, infatti $\ln(x \cdot y) = \ln(x) + \ln(y) \quad \forall x, y \in \mathbb{R}_{>0}$
Osservazione:
$l^0 = 1 \;\; ln(1) = 0$
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 invero di e^x in $(\mathbb{R}_{>0},\cdot)$
$\ln(\frac{1}{x}) = -\ln(x)$
Esercizio
$\varphi : G_1 \to G_2$ omomorfismo. Dimostrare
1)$\varphi(e_1) = e_2$
2)$\varphi(g^{-1}) = \varphi(g)^{-1} \;\; \forall g \in G_1$
Soluzione:
$\varphi(e_1) = \varphi(e_1 \cdot e_2) = \varphi(e_1) * \varphi(e_1)$
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
$\pi : G \to G/N$
$g \to gN$
è un omomorfismo
Esempio
$det : GL_n(\mathbb{K}) \to \mathbb{K}^*$
dove $\mathbb{K}$ campo
$\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ è un gruppo rispetto l prodotto
allora det è un omomorfismo
infatti:

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

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

Definizione 2
$\varphi : G_1 \to G_2$ omomorfismo
il nucleo di φ è $ker(\varphi) := \{g \in G_1 | \varphi(g) = e\}$
L'immagine di ϕ è
$Im(\varphi) = \{h \in H_2 | \exists g \in G_1 : \varphi(g) = h\}$

Esercizio:
$\varphi : G_1 \to G_2$ 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 $\varphi(g) = e_2$)
$\Rightarrow \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) =$ per esercizio $= \varphi(g)\varphi(h)\varphi(g)^{-1} = e_2$
$\Rightarrow ghg^{-1} \in H \forall h \in H, \forall g \in G \Rightarrow gHg^{-1} \subseteq H$
Osservazione
$(G, \cdot)$ gruppo, $H \leq G$. Allora HG se e solo se esiste $\varphi : G_1 \to G_2$ omomorfismo tale che $H = ker(\varphi)$

Dimostrazione
Resta solo l'implicazione $\Rightarrow$
Sia $H \trianglelefteq G$. considero l'omomorfismo
$\pi : G \to G/H$
$\quad g \to gH$
chi è $ker(\pi)$
$ker(\pi) = \{g \in G | gH = H\} = \{g \in G | g \in H\} = H$ □

Esempio
$det : GL_n(\mathbb{K}) \to K^*$
$ker(det) := \{A \in GL_n(\mathbb{K}) | det(A) = 1\} = SL_n(\mathbb{K})$
quindi
$\mathrm{SL}_n(\mathbb{K}) \trianglelefteq GL_n(\mathbb{K})$
Esercizio
$(G, \cdot)$ gruppo $g \in G$ fissato
$\varphi : \mathbb{Z} \to G$
$\quad n \to g^n$
è un omomorfismo
determinare $ker\varphi$ e $Im\varphi$
Esercizio
Sia $\varphi : G_1 \to G_2$ 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 $\varphi : G_1 \to G_2$ omomorfismo dei gruppi
$ker\varphi = \{g \in G_1 | \varphi(g) = e_2\}$
Dimostrare che
φ 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

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

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:

$$\psi : G_1 \underset{\varphi}{\to} G_2 \underset{\pi}{\to} G_2/H_2.$$

Studia il $\ker(\psi)$
$\ker(\psi) := \{g \in G_1 | \psi(g) = H_2\} = \{g \in G_1 | \varphi(g)H_2 = H_2\}$
$ker(\psi) = \{g \in G | \varphi(g) \in H_2\} = \varphi^{-1}(H_2)$
Quindi $\varphi^{-1}(H_2)$ è il nucleo di un omomorfismo $\psi : G_1 \to G_2/H_2$ e dunque $\varphi^{-1}(H_2) \trianglelefteq G_1$
Osservazione:
Se $\varphi : G_1 \to G_2$
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 $H_1 = G_1 \leq G_1$
$\Rightarrow Im(\varphi) = \varphi(G_1) \leq G_2$

2 Parte figa della lezione

Lemma 1
$(G, \cdot)$ gruppo
$N \trianglelefteq G, H \trianglelefteq G$ sottogruppi normali
$\pi : G \to G/N$
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:
$\forall h \in H \quad \forall n \in N$
$\pi(hn) = \pi(h)\pi(n)$ *(omomorfismo)*
$n \in N$
$\Rightarrow \pi(n) = N \to \pi(h)\pi(e) = \pi(ne)$
$\pi(e) = N \qquad = \pi(n) \in \pi H$ $\square$

Lemma 2
$(G, \cdot)$ *gruppo*
$\cdot H \trianglelefteq G$
$\cdot N \trianglelefteq G$
$\cdot \pi \to G/N$
Allora:
1)$\pi^{-1}(\pi(H)) = HN$
2) *se* $N \subseteq H \to \pi^{-1}(\pi(H)) = N$
3)$\bar{H} \leq G/N \to \pi(\pi^{-1}(\bar{H})) = \bar{H}$

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 $\pi^{-1}(\pi(H)) \subseteq HN$

$$\pi^{-1}(\pi(H)) := \{g \in G | \pi(g) \in \pi(H)\}$$
$$= \{g \in G | \exists g \in H : \pi(g) = \pi(h)\}$$
$$= \{g \in G | \exists h \in H : \pi(h)^{-1}\pi(g) = N\} \text{ } N\textit{= elemento neutro in } G$$
$$= \{g \in G | \exists h \in H : \pi(hg) = N\}$$
$$= \{g \in G | \exists h \in H : h^{-1}g \in N\}$$
$$= \{g \in G | \exists h \in H : g \in hN \acute{r}brace \subseteq HN$$

segue (1) □

Dimostrazione (2)
È un caso particolare del punto 1, infatti se

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

□

Dimostrazione (3)
Segue dal fatto che $\pi \grave{e} unomomorfismosuriettivo$

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

□

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

$$\{sottogruppi\ H \leq G \quad t.c. \quad N \supseteq H\} \to \{sottogruppi\ di\ G/N\}$$
$$H \to \pi(H)$$
$$\pi^{-1} \leftarrow \bar{H}$$
$$\{\ sottogruppi\ normali\ H \trianglelefteq G\ t.c\ N \subseteq H\} \to \{\ sottogruppi\ normali\ G/N\}$$
$$H \to \pi(H)$$
$$\pi^{-1}(\bar{H}) \to \bar{H}$$

Dimostrazione
Il lemma 2 (punti 2 e 3) garantisce che le due applicazioni $H \to \pi(H)$ $\pi^{-1}(H) \to \bar{H}$
sono una l'inversa dell'altra □

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

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

Teorema 2 (Teorema di omomorfismo)
$\varphi : G_1 \to G_2$ *omomorfismo*
$\cdot N \trianglelefteq G_1$
$\pi : G_1 \to G/N$
Allora:
1) esiste unico omomorfismo
$\bar{G}/N \to G_2$

t.c. $\bar{\varphi} \circ \pi = \varphi$
$$\begin{tikzcd} G_1 \arrow[r, "\varphi"] \arrow[d, "\pi"] & G_2 \\ G_1/N \arrow[ur, dashed, "\exists!\bar{\varphi}"] & \end{tikzcd}$$

2) $Im(\bar{\varphi}) = Im(\varphi)$
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* $\bar{\varphi} \cdot \pi = \varphi$*)*
$\cdot\bar{\varphi}$ *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:
$gN = fN \to g \equiv f mod N$
$\Rightarrow \exists n \in N$ *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* $Im(\bar{\varphi}) = Im(\varphi)$
3)$\bar{\varphi}$ *è iniettivo* $\Leftrightarrow ker\bar{\varphi} = \{N\}$
$ker\bar{\varphi} = \{gN \in G_1/N | \bar{\varphi}(gN) = e_2\}$
$= \{gN \in G_1/N | \varphi(g) = e_2\}$
$= \{gN \in G_1/N | g \in ker(\varphi)\}$ □

Corollario 1
$(G, \cdot)$, $N \trianglelefteq G$
Allora esiste una corrispondenza biunivoca

$$\{omomorfismi\ \varphi : G \to G'\ t.c.\ N \subseteq ker(\varphi)\} \to \{omomorfismi\ G/N \to G'\}$$
$$\varphi \to \bar{\varphi}$$
$$\pi \leftarrow \bar{\varphi}$$

Dimostrazione
basta osservare che
dato $\bar{\varphi} : G/N \to G'$ *la composizione*
$\bar{\varphi} \circ \pi : G \to G'$ *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
$\varphi : G_1 \to G_2$
omomorfismo si dice isomorfismo se è invertibile

Teorema 3 (Primo teorema di isomorfismo)
$\varphi : G_1 \to G_2$
Allora:
$Im(\varphi) \cong G_1/ker(\varphi)$
Dove $\cong$ *(isomorfo) significa che esiste un isomorfismo tra i due gruppi*

Dimostrazione

$$\begin{tikzcd}
G_1 \arrow[r, "\varphi"] \arrow[d, "\pi"] & G_2 \\
G_1/N \arrow[ur, "\exists ! \overline{\varphi}"] &
\end{tikzcd}$$

scelgo $N - ker\varphi$
il teorema di isomorfismo fornisce un omomorfismo iniettivo

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

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

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

la prima tramite $\bar{\varphi}$ *la seconda per il teorema di isomorfismo*
Applicazione:
det: $GL_n(\mathbb{K}) \to (\mathbb{K}^*, \cdot) = (\mathbb{K} \setminus \{0\}, \cdot)$
$\ker(det) = SL_n(\mathbb{K})$ *matrici con det 1*
$\Rightarrow GL_n(\mathbb{K})/SL_n(\mathbb{K}) \cong (\mathbb{K}^*, \cdot)$ $\square$

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

$$\begin{tikzcd} G \arrow[r, "\varphi=\pi_H"] \arrow[d, "\pi"] & G/H \\ G/N \arrow[ur, dashed, "\exists!\bar{\varphi}"] & \end{tikzcd}$$

π_H proiezione sul quoziente H

$N \subseteq H = ker(\varphi)$
Inoltre $Im(\bar{\varphi}) = Im(\varphi) = G/H$
Idea: *applicare il primo teorema di isomorfismo*
<u>suriettiva</u> $\bar{\varphi} : G/N \to G/H$
basta quindi dimostrare che $ker(\bar{\varphi}) = H/N$
Studiamo

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

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

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

□

Corollario 1
In $(\mathbb{Z}, +)$ gruppo abeliano
$a, n \in \mathbb{Z}$ interi non nulli
Denotiamo con

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

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

Nota:
se $MCD(n, a) = 1$ allora a genera il gruppo ciclico $\mathbb{Z}/(n)$
Dimostrazione
Consideriamo $G = \mathbb{Z} \quad H = (a) + (n) \quad N = (n)$
Dal II Teorema di isomorfismo

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

□

Confrontiamo le cardinalità

$$MCD(a,n) = |\mathbb{Z}/(MCD(a,n))|.$$
$$= |\mathbb{Z}/(n) \Big/ ([a])|$$

.

$$\frac{|Z/(n)|}{([a])} = \frac{n}{ord([a])}.$$
$$ord([a]) = \frac{n}{MCD(a,n)}.$$

Lemma 1
$a, bg \in Z$ 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 <u>*distinti*</u> *esistono*
Dati $t, s \in \mathbb{Z}$ tali che

$$ta + (b) = sa + (b).$$
$$\Leftrightarrow ta \equiv sa \; mod(b).$$
$$\Leftrightarrow -ta + sa \in (b).$$

Allora

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

□

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
$\pi_N : G \to G/N$
$g \to gN$
consideriamo la restrizione

$$\begin{gathered}\pi_N|_H : H \to G/H \\ h \to hN \\ ker(\pi_N|_H) = \{h \in H | \pi_N|_H(h) = N\} \\ = \{h \in H | hN = N\} \\ = \{h \in H | h \in N\} \\ = H \cap N\end{gathered}$$

Deduciamo che $H \cap N \trianglelefteq N$
Idea: Applicare il I teorema di isomorfismo all'omomorfismo

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

Avremo $Im(\varphi) \cong H/ker(\varphi) = H/H \cap N$
Studiamo $Im(\varphi)$

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

Il penultimo passaggio deriva da un lemma già visto a lezione □

Corollario 2
$a, b \in \mathbb{Z}$ *non nullli*
Allora $mcm(a, b) = \frac{ab}{MCD(a,b)}$

Dimostrazione
$G = \mathbb{Z}$
$H = (a)$
$N = (b)$
$H + N = (MCD(a, b))$

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

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

Confrontiamo la cardinalità
Per il lemma

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

Quindi

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

$\square$

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

Ordine 1
Se $|G| = 1 \quad \Rightarrow \quad G = \{e\}$
Ordine p primo:
Abbiamo mostrato che se $|G| = p$ allora G non ammette sottogruppi non banali
Sia $g \in G$ tale che $g \neq e \Rightarrow ord(g) = p \ \Rightarrow G =< g >$

$$\varphi : G \to G_p =< p >$$
$$g \to p$$

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 $K_4 =< \rho, \sigma >$
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 $H =< g, h >$
Per Lagrange
$H \geq 3$
$\Rightarrow H = H$
$\Rightarrow G = \{e, f, g, fg\}$
abeliano
Costruisco l'isomorfismo esplicito con K_4

$$\begin{gathered} \varphi : G \to K_4 =< \rho, \sigma > \\ e \to e \\ f \to \rho \\ g \to \sigma \\ fg \to \rho\sigma \end{gathered}$$

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. $ord(r) = 3$ e $ord(s) = 2$
Definisco:

$$G :=< r >= \{e, r, r^2\} \qquad k :=< s >= \{e, s\}.$$
$$H \cap K = \{e\}.$$
$$|HK| = \frac{|H||K|}{|H \cap K|} = 6 = |KH|.$$

$\Rightarrow HK = G = KH$
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 $ord(rs)$
$(rs)^2 = r^2s^2 = r^2 \neq e \Rightarrow ord(rs) \neq 2$
$(rs)^3 = r^3s^3 = s^3 = s \neq e$
Per Lagrange
necessariamente $ord(rs) = 6$
$\Rightarrow G$ *è cicliclo* $\Rightarrow$ *Assurdo*
II caso: $\begin{cases} rs = sr^2 \\ r^2s = sr \end{cases}$
Costruiamo l'isomorfismo

$$\begin{gathered} G \to D_3 :=< \rho, \sigma > \\ e \to Id \\ r \to \rho \\ r^2 \to \rho^2 \\ s \to \sigma \\ sr \to \sigma\rho \end{gathered}$$

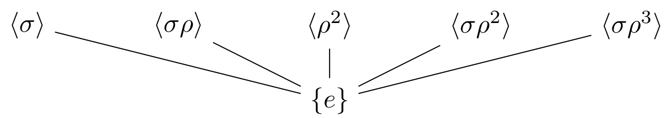
$\square$

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. $H_1 \subset K \subset H_2$

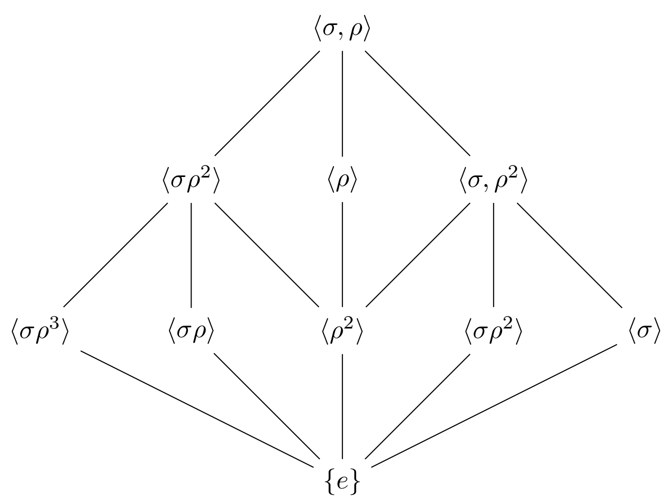
Esempio:
T_{D_4}
Ricordiamo che $D_4 =< \sigma, \rho > \quad |D_4| = 8$
studiamo i sottogruppi di D_4
ordine 1: L'unico sottogruppo è $H = \{e\}$
ordine 2: Sono tutti e soli quelli generati da un elemento di ordine 2 in D_4



ordine 4: per la classificazione sono ciclici (C_4) oppure di Klein (K_4) altre al ciclico $< p >$ esistono altri sottogruppi

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

Ordine 8: D_4



Esempio:
$G = D_4$
$N =< \rho^2 > \trianglelefteq G$
Vogliamo $T_{G/N}$
studiamo $G/N = D_4/ < rho^2 >$
$|G/N| = [G : N] = \dfrac{|G|}{|N|} = \dfrac{8}{2} = 4$
chi sono i laterali?
$IdN = N < \rho^2 >= \{Id, \rho^2\}$
$\rho N = \{\rho, \rho^3\}$
$\sigma N = \{\sigma, \sigma\rho^2\}$
$\sigma\rho N = \{\sigma\rho, \sigma\rho^3\}$
Ricordo:
Abbiamo una corrispondenza biunivoca tr ai sottogruppi di G/N e i sottogruppi di G contenenti N.

$$\begin{tikzcd}
 & G/N \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\begin{array}{c}\langle \sigma\rho N \rangle \\ \parallel \\ \{\sigma\rho N, N\}\end{array} \arrow[dr, dash] & \begin{array}{c}\langle \rho N \rangle \\ \parallel \\ \{\rho N, N\}\end{array} \arrow[d, dash] & \begin{array}{c}\langle \sigma N \rangle \\ \parallel \\ \{N, \sigma N\}\end{array} \arrow[dl, dash] \\
 & \{N\} &
\end{tikzcd}$$

Obiettivo: studiare S_n
Ricordo:
$X := \{1, \dots, n\}$
$S_n := S_X = \{$ applicazioni biunivoche $X \to X\}$
S_n gruppo di permutazioni
Osservazione:
$|S_n| = n!$
Osservazione:
se $n = 3 \to |S_3| = 6$
$\Rightarrow S_3 \cong D_3$
Osservazione
$S_n \cong D_n \quad \forall n \geq 4$
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 $i \sim j \Leftrightarrow \exists k \in \mathbb{Z}$ t.c. $\sigma^k(i) = j$
È una relazione d'equivalenza!
studiamo le classi di equivalenza
fissato $i \in X$
la sua clase

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

quindi $\exists\ \ k_1, k_2 \in \mathbb{Z}$ distinti t.c. $\sigma^{k_1}(i) = \sigma^{k_2}(i)$
$\Rightarrow i = \sigma^{k_2 - k_1}(i)$
$\Rightarrow m := min\{k \in \mathbb{Z}_{>0} | \sigma^k(i) = i\}$
$\Rightarrow X_i = \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{n-1}(i)\}$ $\square$

Proposizione 1
Data $\sigma \in S_n$, allora σ può essere rappresentata come composizione di cicli disgiunti

Obiettivo: Definire un omomorfismo

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

Questo ci permetterà di definire il sottogruppo alterno $A_n \trianglelefteq S_n$
$A_n := ker(sgn)$

Notazione 1
Dato un polinomio
$f \in \mathbb{Q}[x_1, \ldots, x_n]$
e data $\sigma \in S_n$
Definiamo

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

Ci sta un polinomio speciale:

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

Definizione 2
$\sigma \in S_n$
$sgn(\sigma) := \frac{\Delta^\sigma}{\Delta} \in \{\pm 1\}$

Osservazione
$sgn : S_n \to \{\pm 1\}$
è un omomorfismo

Dimostrazione
In generale
$(f^\sigma)^\tau = f^{\sigma\tau}$
$(fg)^\sigma = f^\sigma g^\sigma$
$sgn(\sigma\tau) = \dfrac{\Delta^{\delta\tau}}{\Delta} = \dfrac{(\Delta^\sigma)^\tau)}{\Delta} = \dfrac{\Delta^\sigma}{\Delta}\dfrac{(\Delta^\sigma)^\tau}{\Delta^\sigma} = sgn(\sigma)\dfrac{\Delta^\tau}{\Delta} = sgn(\delta)sgn(\tau)$ □

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:*

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

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

Proposizione 1
bold $(G_1 \times G_2, \cdot)$ *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 $K \trianglelefteq G_2$

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

Dimostrazione (4,5)

$$\begin{tikzcd}
G_1 \times G_2 \arrow[r, "\varphi"] \arrow[d] & \frac{G_1}{H} \times \frac{G_2}{K} \\
\frac{(G_1 \times G_2)}{ker\varphi} \arrow[ur, dotted, "\exists! \bar{\varphi}"] &
\end{tikzcd}$$

dove

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

Dal primo teorema di isomorfismo

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

$\cdot\varphi$ *suriettiva poichè* $\pi_H e \pi_K$ *sono suriettive*
$\cdot \ \ ker\varphi = \{(g_1, g_2) \in G_1 \times G_2 | \varphi(g_1, g_2) = (H, K)\}$
$= \{(g_1, g_2) | g_1 H = H \ \ e \ \ g_2 K = K\}$

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

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

□

Esercizio (importante)
$(G_1, \cdot)$ e $(G_2, *)$ gruppi
$H, K \trianglelefteq G_1 \times G_2$ 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

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

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

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) $H, K \trianglelefteq G$
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)
$\psi : H \times K \to G$
$(h, k) \to hk$
Dobbiamo verificare che ψ sia isomorfismo
1)ψ è suriettiva perchè ogni elemento di G si scrive come hk quindi $Im(\psi) = G$

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

$$\Rightarrow h_1k_1=h_2k_2$$
$$\Rightarrow h_2^{-1}h_1k_1=k_2$$
$$\Rightarrow h_2^{-1}h_1=k_2k_1^{-1}\in H\cap K=\{e\}$$
$$\Rightarrow \begin{cases} h_2^{-1}h_1=e \\ k_2k_1^{-1}=e \end{cases} \Rightarrow (h_1,k_1)=(h_2,k_2)$$
$$\Rightarrow \psi \textit{ iniettiva}$$

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

$$\psi(h_1h_2,k_1k_2)=\psi(h_1,k_1)\psi(h_2,k_2).$$

dunque

$$\psi(h_1h_2,k_1k_2)=h_1h_2k_1k_2=h_1(h_2k_1)k_2=h_1(k_1h_2)k_2=\psi(h_1,k_1)\psi(h_2,k_2).$$

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

Dimostrazione (2)
Per ipotesi esiste un isomorfismo $\varphi:G_1\times G_2\to G$
$(g_1,g_2)\to\varphi(g_1,g_2)$
considero
$H:=\varphi(G_1,\{e_2\})$
$K:=\varphi(\{e_1\}\times G_2)$
Abbiamo visto che
$\cdot G_1\times\{e_2\}\trianglelefteq G_1\times G_2\to H\trianglelefteq G$
$\cdot\{e_1\}\times G_2\trianglelefteq G_1\times G_2\to K\trianglelefteq G$

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

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

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.
$MCD(n,m)=1$
Consideriamo $C_{nm}=<p>$

dove $ord(p) = nm$
Considero
$$H =< \rho^m > \quad K =< \rho^n > .$$
$|H| = ord(\rho^m) = n$
$|K| = ord(\rho^n) = m$
Verifichiamo che
$$C_{nm} \cong H \times K.$$
Dobbiamo mostrare:

1. $H, K C_{nm}$

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

3. $HK = C_{nm}$

1) C_{nm} abeliano, quindi $H, K C_{nm}$
2) $H \cap K =?$
sia $\rho^h \in H \cap K$
Allora
$$\begin{cases} \rho^h = (\rho^m)^{t_1} \\ \rho^h = (\rho^h)^{t_2} \end{cases} \qquad \begin{cases} m|h \\ n|h \end{cases} .$$
Ma $h \geq mcm(m, n) = mn \Rightarrow h = mn \Rightarrow \rho^h = Id \Rightarrow H \cap K = \{Id\}$
$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{nm}{1}.$$
$\Rightarrow HK$ è tutto chiuso quindi è C_{nm}

Definizione 3 (Automorfismo)
$(G, \cdot)$ gruppo
Un automorfismo di G è un isomorfismo $\varphi : G \to G$

Osservazione
$(G, \cdot)$ gruppo
$\Rightarrow Aut(G) = \{$automorfismi di $G\}$
è un gruppo (rispetto alla composizione)
Esempio:
$(G, \cdot)$ gruppo
Fissato $g \in G$ definiamo
$I_g : G \to G$
$\quad f \to gfg^{-1}$
I_g si dice automorfismo interno
$Int(G) = \{$automorfismi interni di $G\}$

Proposizione 2
$Int(G) \trianglelefteq Aut(G)$

Dimostrazione
$If_G = I_e \in Int(G)$
$dato\ g \in G\ allora$

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

$I_{g_2} \cdot I_{g_1}(f) = g_3 g_2 f g_2^{-1} g_2^{-1} = (g_2 g_1) f (g_2 g_1)^{-1} = I_{g_2 g_1}(f)$
$I_{g_2} \cdot I_{g_1} = I_{g_2 g_1}$
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 $g \in G$

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

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

Definizione 4 (Centro di un gruppo)
$(G, \cdot)$ *gruppo*
Il centro di G *è*

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

Osservazione
$Z(G) \trianglelefteq G$
Osservazione:
$(G, \cdot)$ gruppo
Definiamo un omomorfismo
$\varphi : G \to Int(G)$
$\quad g \to I_g$
$\cdot$ φ è suriettiva
$\cdot$ 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 $ker(\varphi)$

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

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
$\phi : H \to Aut(N)$
$h \to \o_n$

Definizione 5 (Prodotto semidiretto)
il prodotto semidiretto di N e H tramite $\o$ è l'insieme $N \times H$ dotato dell'operazione

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

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

Notazione 1
Indichiamo il prodotto semidiretto tra N e H con il simbolo $N \rtimes_{\o} H$

Proposizione 3
$N \rtimes_{\o} H$ è un gruppo

Dimostrazione
Dato $(n, h) \in N \rtimes_{\o} H$
l'inverso è dato da $(\o_{h^{-1}}(n^{-1}), h^{-1})$ □

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
$D_n =< \rho, \sigma > \quad N =< \rho > \trianglelefteq D_n$
$H =< \sigma > \leq D_n$. 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 $\theta : H \to Aut(N)$ è l'insieme $N \times H$ dotato dell'operazione

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

Osservazione:
$h_1 \in H, \quad \o_{h_1} \in Aut(N) \quad \o_{h_1}(n_2) \in N$
Esempio
Scegliendo
$\o : H \to Aut(N)$
$\quad h \to \o_h$
con $\o_n := Id_N \quad \forall h \in H$
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 $\o : H \to Aut(N)$ un omomorfismo
Dimostrare:
1)$|N \rtimes_{\o} H| = |N||H|$
2)$N \rtimes_{\o} H$ è abeliano $\Leftrightarrow N, H$ abeliani
3)$\tilde{H} \leq H, \tilde{N} \leq N$ (sottogruppo caratteristico)

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

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

Definizione 2 (Sottogruppo caratteristico)
$\tilde{N} \leq N$ sottogruppo caratteristico se
$\varphi(n) \in \tilde{N} \quad \forall n \in N \quad \forall \varphi \in Aut(N)$

Teorema 1
Sia G un gruppo.
1) Se G è prodotto semidiretto di N e $H \leq G$, allora esiste un omomorfismo $\o : H \to Aut(N)$ tale che $G \cong N \rtimes_{\o} H$
2) Se $G \cong \tilde{N} \rtimes_{\o} \tilde{H}$ 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
$\o : H \to Aut(N)$
$h \to \o_n$
dove $\o_h(n) := (hnh^{-1}) \in hNh^{-1} = N \quad \forall n \in N$
Dato che abbiamo assunto N normale
Abbiamo verificato la volta scorsa che è un omomorfismo.
Definiamo l'applicazione
$\psi : N \rtimes_{\o} H \to G$
$(n, h) \to nh$
ψ è suriettiva poiché $N \cdot H = G$
ψ è iniettiva poichè

$$n_1h_1 = n_2h_2 \to n_2^{-1}h_1 = h_2h_1^{-1} \in H \cap N = \{e\}$$
$$\Rightarrow \begin{cases} n_2^{-1}n_1 = e \\ h_2h_1^{-1} = e \end{cases} \to (n_1, h_1) = (n_2, h_2)$$

ψ è omomorfismo:
$\psi((n_1, h_1) \cdot (n_2, h_2)) =$
$= \psi((n_1\o_{h_1}(n_2), h_1h_2))$
$= n_1\o_{h_1}(n_2)h_1h_2$
$= n_1h_1n_2h_1^{-1}h_1h_2 = \psi(n_1, h_1) \cdot \psi(n_2, h_2)$
Omomorfismo biunivoco $\square$

Dimostrazione (2)
Dato un isomorfismo
$\psi : \tilde{N} \rtimes_{\phi} \tilde{H} \to G$
definiamo:
$N := \psi(\tilde{N} \rtimes_{\phi} \{e_{\tilde{H}}\}) \trianglelefteq G$
$H := \psi(\{e_n\} \rtimes_{\phi} \tilde{H})$
Osserviamo che:
$\cdot\tilde{N} \cong \tilde{N} \rtimes_{\phi} \{e_{\tilde{H}}\} \cong N$
$\cdot\tilde{H} \cong \{e_{\tilde{H}\} \rtimes_{\phi} \tilde{H} \cong H}$
$\cdot N \cap H = \{e\}$
$\cdot NH = e$
(analogo alla dimostrazione per prodtto diretto) $\square$

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 $\forall a, b\mathbb{Z}$

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

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

$$n = \rho_1^{k_1} \cdot \ldots \cdot \rho_r^{k_r} \qquad \textit{(forma canonica)}$$

dove $k_i > 0 \;\; \forall i \in \{1, \ldots, r\}$
e $\rho_1 < \rho_2 < \ldots < \rho_r$
e ρ_i è primo $\forall i \in \{1, \ldots, r\}$

Teorema 2
ρ primo. Allora
$\sqrt{\rho}$ è irrazionale (ovvero $\sqrt{\rho} \ni \mathbb{Q}$)

Dimostrazione (Per assurdo)
$\exists a, b \in \mathbb{Z}$ *t.c.* $\sqrt{\rho} = \frac{a}{b}$ *con* $MCD(a, b) = 1$
Allora:
$(a) + (b) = (MCD(a, b)) = (1)$
$\to 1 \in (a)) + (b)$
$\exists r, s, \in$ *, t.c.* $1 = ra + sb$ *(identità di Bezout)*
ora: $\begin{cases} a = \sqrt{\rho} b \\ b\rho = a\sqrt{\rho} \end{cases}$
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* $1 < \sqrt{\rho} < \rho$ $\square$

Teorema 3 (Euclide)
Esistono infiniti numeri primi

Dimostrazione
Supponiamo per assurdo che $\exists$ *un numero finito di primi* $\rho_1, \ldots, \rho_r$
Definiamo: $N := (\rho_1 \cdot \ldots \cdot \rho_r) + 1 > 1$
$\Rightarrow \exists \rho_k$ *primo tale che* $\rho_k | N$
$\Rightarrow \begin{cases} \rho_k | N \\ \rho_k | N-1 \end{cases} \Rightarrow \rho_k | N - (N-1) \Rightarrow \rho_k | 1,$ *assurdo* $\square$

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

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

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

Lezione 11 Algebra I

Federico De Sisti

2024-11-05

1 Svolgimento esercizi

Ossercazione:
Quali sono gli elementi di oridne 21 in S_{13}?
Ricordo che in S_4, gli elementi $(12)(34), (13)(24), (14)(23)$ hanno ordine 2
gli elementi di ordine 21 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

$\phi : \mathbb{Z}_{>0} \to \mathbb{Z}$
$\quad n \to |U_n|$
Ricordo:
$\phi(1) = 1$
$\phi(\rho) = \rho - 1$
$\phi(\rho^k) = \rho^k - \rho^{k-1}$
$\phi(n \cdot m) = \phi(n)\phi(m) \quad$ se $MCD(n, m) = 1$

Lemma 1
$n > 1, a \in \mathbb{Z}$ t.c. $MCD(n, a) = 1$
sia $\{a_1, \ldots, a_{\phi(n)}\}$ l'insieme dei numeri positivi minori di n coprimi con n distinti fra loro.
Allora $\{[a_1], \ldots, [a_{\phi(n)}] = \{[aa_1], \ldots, [aa_{\phi(n)}]\}$ (Classi in $Z/(n)$)

Dimostrazione
Basta verificare che gli elementi delle classi $[aa_i] \ \ \forall\ 0 < i < \phi(n)$
Siano tutte distinte tra loro e aa_i sia coprimo con $n \ \forall\ 0 < i < \phi(n)$
Se per assurdo $[aa_i] = [aa_j] \quad i \neq j \Rightarrow aa_i \equiv aa_j \ mod(n) \Rightarrow a \equiv a_j \ mod(n)$
Assurdo perché $1 \leq a_i, a_j < n$ per ipotesi e dunque $a_i - a_j \notin (n)$

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

$\square$

Teorema 1 (Eulero 1760)
$n > 1, a \in \mathbb{Z}$ tale che $MCD(a, n) = 1$
Allora

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

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

$$a_1 \cdot \dots \cdot a_{\phi(n)} \equiv (aa_1) \cdot \dots \cdot (aa_{\phi(n)}) \ mod(n).$$

$$\equiv a^{\phi(n)} \cdot a_1 \cdot \dots \cdot a_{\phi(n)} \ mod(n).$$

Dal momento che $MCD(a_i, n) = 1$
abbiamo: $1 \equiv a^{\phi(n)} \ mod(n)$ □

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

$$x \equiv 2024^{2025} \ mod(1000)$$

È equivalente al sistema (Teorema cinese del resto):

$$\begin{cases} x \equiv 2024^{2025} \ mod(2^3) \\ x \equiv 2024^{2025} \ mod(5^3) \end{cases}$$

Alternativamente mi accorgo che la prima equazione è equivalente a

$$x \equiv 24^{2025} \ mod(1000).$$

$\phi(1000) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$
$\Rightarrow 24^{400} \equiv 1 mod(n)$
Ma questo implica che la congruenza che devo studiare è:

$$\Rightarrow x \equiv 24^{2025} mod(1000).$$

$$\Rightarrow \begin{cases} x \equiv 24^{2025} \ mod(8) \\ x \equiv 24^{2025} \ mod(125) \end{cases} \quad \Rightarrow \begin{cases} x \equiv 0 \ mod(8) \\ x \equiv 24^{2025} \ mod(125) \end{cases} .$$

Dove nell'ultimo passaggio abbiamo utilizzato il fatto che $8|24$ e $24^{\phi(125)} \equiv 24^{100} \equiv 1 \ mod(125)$
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
$$\begin{cases} x \equiv = a_1 \ mod(n_1) \\ \vdots \\ x \equiv = a_r \ mod(n_r) \end{cases}$$

con $MCD(n_i, n_j) = 1 \ \ \forall i \neq j$
Come ricostruire l'unica soluzione $[\bar{x}] \in \mathbb{Z}/(n_1 \cdot \ldots \cdot n_r)$
$\bar{x} \equiv a_i \ mod(n_i) \ \forall i \in \{1, \ldots, r\}$
Idea
Definiamo:
$n := n_1 \cdot n_r$
$N_i := \frac{n}{n_i}$
$\bar{x} := a_1 N_1^{\phi(n_1)} + \ldots + a_r N_r^{\phi(n_r)}$
Ora $\bar{x} \equiv a_i N^{\phi(n)} \ mod(n) \Rightarrow \bar{x} = a_i mod(n_i) \ \ \forall i$

Teorema 2 (TCR)
Damp il sistema
$\begin{cases} x \equiv a_1 \ mod(n) \\ \ldots x \equiv a_r \ mod(n_r) \end{cases}$
con $MCD(n_i, n_j) = 1 \ \ \forall i \neq j$
Allora esiste un'unica classe $[\bar{x}] \in \mathbb{Z}/(n_1 \cdot \ldots \cdot n_r)$ *tale che*
$\bar{x} \equiv a_i \ mod(n_i) \ \ \forall i \in \{1, \ldots, r\}$

Dimostrazione (Alternativa al teorema di Eulero)
$n := n_1 \ldots \cdot n_r$
$N_i = \frac{n}{n_i}$
$\bar{x} := a_1 N_1 m_1 + \ldots a_r N_r m_r$
dove gli m_i *sono univocamente determinati dalla condizione* $N_i m_i \equiv 1 mod(n_i)$
Infatti

$$\bar{x} \equiv a_i N_i m_i \ mod(n_i) \Rightarrow \bar{x} \equiv a_i mod(n_i).$$

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
$\{1, \ldots, n\} = \bigcup_d S_d$
$\Rightarrow n = \sum_{d|n} |S_d|$
$MCD(m, n) = d \ \Leftrightarrow MCD(\frac{m}{d}, \frac{n}{d}) = 1$
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 $a_1, \ldots, a_{\phi(n)}$ *tali interi:*
Studio $\sum_{i=1}^{\phi(n)} a_i$
Osserviamo che $MCD(a, n) = 1 \Leftrightarrow MCD(n - a_i, n) = 1$
Quindi
$\{a_1, \ldots, a_{\phi(n)}\} = \{n - a_1, \ldots n - a_{\phi(n)}\}$
$\Rightarrow \sum_{i=1}^{\phi(n)} a_i = \sum_{i=1}^{\phi(n)} (n - a_i) = n\phi(n) - \sum_{i=1}^{\phi(n)} a_i \Rightarrow 2\sum_{i=1}^{\phi(n)} a_i = n\phi(n)$ □

3.1 Teorema di Wilson/Lagrange

Ricordo

Teorema 3 (Wilson)
p primo. Allora
$(p - 1)! \equiv (p - 1) \ mod(p)$

Teorema 4 (Lagrange)
$m > 1$ *intero tale che*
$(m - 1)! \equiv (m - 1) \ mod(m)$
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

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

$\Rightarrow d|(m + 1)! + 1$
Quindi $\begin{cases} d|(m-1)! \\ d|(m-1)! + 1 \end{cases} => d|1$ *che è un assurdo* □
Esercizio
p primo dispari. Allora

$$p \equiv 1 \ mod(.$$

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
$\cdot a = qb + r$
$\cdot\ 0 \leq r < |b|$

Dimostrazione
Procediamo per passi
$1) a, b \in \mathbb{Z}_{>0}$

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

Osserviamo che $A \neq \emptyset$
Infatti $(a+1)b = ab + b > ab \geq a \Rightarrow a+ \in A$
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 $a < 0 \Rightarrow -a > 0$
$\Rightarrow -a = qb + r$ *con* $0 \leq r < b$
$\Rightarrow a = (-q)b - r$
Se $r = 0$ *abbiamo finito*
Se invece $0 < r < b$
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) $a \in \mathbb{Z}, b < 0$
$\Rightarrow -b > 0$
$a = q(-b) + r$ *con* $0 \leq r < -b$
$\Rightarrow a = (-q)b + r \quad 0 \leq r < |b|$ $\square$

2 Esercizi delle schede

$\begin{cases} x \equiv 50 \ mod(110) \\ x \equiv 47 mod(73) \end{cases}$

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

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

Bisogna determinare m_1, m_2
Idea: Sfruttare l´identità di Bezoit: $(n_1) + (n_2) = (MCD(n_1, n_2)) = (1)$
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 $110 \cdot r \equiv 1 \ mod(73)$
$73 \cdot s \equiv 1 \ mod(110)$
Il nuovo obiettivo è determinare r, s
Procedo con la divisione euclidea tra 110 e 73

$$110 = 73 + 37$$
$$73 = 2 \cdot 37 - 1$$
$$\Rightarrow 1 = 2 \cdot 37 - 73$$
$$\Rightarrow 2 \cdot (110 - 73) - 73 = 1$$
$$\Rightarrow 2 \cdot 110 - 3 \cdot 73$$

Quindi:
$1 = 2 \cdot 110 - 3 \cdot 73$
da cui

$$m_1 = -3$$
$$m_2 = 2$$

$$\bar{x} \equiv 5 - \cdot 73 \cdot (-3) + 47 \cdot 110 \cdot (2) \equiv -620 \ mod(8030).$$

8==D
Nuovo Esercizio
$\begin{cases} x \equiv_6 2 \\ x \equiv_{10} 3 \end{cases}$ Non possiamo sfruttare il teorema cinese del resto

$$x \equiv_6 2$$
$$\Updownarrow$$
$$x = 2 + 6k \quad k \in \mathbb{Z}$$
$$\Updownarrow$$
$$x = 2(1 + 3k)$$

$$x \equiv_{10} 3$$
$$\Updownarrow$$
$$x = 3 + 10h \quad h \in \mathbb{Z}$$
$$\Updownarrow$$
$$x = 2(5h + 1) + 1$$

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 $3x \equiv_{15} 6$

$$3x \equiv 6 + 15k$$
$$\Updownarrow$$
$$3x = 3(2 + 5k)$$
$$\Updownarrow$$
$$x = 2 + 5k$$

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

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

$$9 = 7 + 2$$
$$7 = 3 \cdot 2 + 1$$
$$\Rightarrow 1 = 7 - 3 \cdot 2$$
$$\Rightarrow 1 = 7 - 3 \cdot (9 - 7)$$
$$\Rightarrow 1 = 4 \cdot 7 - 3 \cdot 9$$

Quindi $s = 4$

$$7x \equiv_9 2$$
$$\Updownarrow$$
$$4 \cdot 7 \equiv_9 4 \cdot 2$$
$$\Updownarrow$$
$$x \equiv_9 8$$

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:

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

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

$$9 = 5 + 4$$
$$5 = 4 + 1$$
$$1 = 5 - 4$$
$$1 = 5 - (9 - 5)$$
$$1 = 2 \cdot 5 - 9$$

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

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

3 Azioni di gruppi

Definizione 1
Un'azione di un gruppo $(G, \cdot)$ *su un insieme* X *è un'applicazione*

$$G \times X \to X$$
$$(g, x) \to g.x$$

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

$$G \times X \to X$$
$$(g, x) = g \underset{\ast}{\ast} x$$

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

$$\mathrm{S}_n \times X \to X$$
$$(\sigma, x) \to \sigma(x)$$

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

$$G \times X \to X$$
$$(AB, C) \to BCA^{-1}$$

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

$$\mathrm{G} \times X \to X$$
$$(\mathrm{A,v}) \to Av$$

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

$$G \times X \to X$$
$$(A, C) \to ACA^{-1}$$

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

$$G \times X \to X$$
$$(g, x) \to g * x * g^{-1}$$

Definizione 2
Data un'azione di un gruppo G su un insieme X si dice transitiva se

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

Definizione 3
Un'azione si dice semplicemente transitiva se

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

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'inseme X

Definizione 4
$G \curvearrowright X$, Dato $x \in X$ definiamo:
· 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
$G \to O_x$
$g \to g.x$

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 $\forall g, f \in G$

$$g \equiv f mod(Stab_x)$$
$$\Updownarrow$$
$$g.x = f.x$$

> **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 $suXcomex\tilde{y} \Leftrightarrow g \in G$ tale che $g.x = y$.
Basta dimostrare che è una relazione d'equivalenza
2) $X = \{(g_1, \dots, g_n) \in G \times \dots \times G | g \cdot \dots \cdot g_p = e\}$
Vogliamo definire un'azione del gruppo ciclico $C_p =< p >$ su X

$$C_p \times X \to X$$
$$\rho.(g_1, \dots, g_p) \to (g_2, g_3, \dots, g_p, g_1)$$

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:
$\forall (g_1, \dots, g_{p-1}, g_p) \in X$ dove $_p = (g_1, \dots, g_{p-1})^{-1} \Rightarrow$ in particolare $p||X|$
4)Studiamo le orbite dell'azione $C_p \curvearrowright X$, Sappiamo che $|C_p| = |O_x||Stab_x|\ \forall x \in X$
Quindi $|O_x| = 1 \quad \vee \quad |O_x| = p$
5) Dato che X è unione disgiunta di orbite e $p||X|$
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

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

Quindi p divide $|\{g \in G | g^p = e\}|$
d'ora in poi $A = \{g \in G | g^p = e\}$

7)$A \neq \emptyset$ poiché $e \in A$

$$A = \{e\} \cup \{g \in G | ord(g) = p\}.$$

Quindi modulo (p) abbiamo

$$0 \equiv_p 1 + |\{g \in G | ord(g) = 1\}|.$$

Quindi l'insieme di elementi di ordine p in G è non uvoto e

$$|\{g | ord(g) = p\} \equiv_p p - 1.$$

Deduciamo

$$|\{g \in G | ord(g) = p\} = kp - 1 \geq p - 1.$$

con $k \in Z^+$

4 Torniamo alle schede

$\begin{cases} 3x \equiv_{15} 6 \\ 21x \equiv_{49} 13 \end{cases}$ 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 $MCD(a, n) \not| b$

allora $ax \equiv_n b$ non ammette soluzioni

Infatti: $d = MCD(a, n)$

con $d \not| b$ allora

con d divide il membro di sinistra ma non quello di destra

Esercizio

G gruppo $g \in G \quad ord(g) = n$

Allora, $g^h = g^k$ se e solo se $h \equiv_n k$

Soluzione

Assumiamo che $g^h = g^k$ Divisione Euclidea

$h - k = qn + r$ 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

$$2^n + 2^m \equiv_9 0$$
$$\Updownarrow 2^n \equiv_9 -2^m$$
$$\Updownarrow$$
$$2^{n-m} \equiv_9 -1$$
$$\Updownarrow$$
$$2^{n-m} \equiv_9 8$$
$$\Updownarrow$$
$$2^{n-m} \equiv_9 2^3$$

Sfruttiamo l'esercizio precedente con $G = U_9$
La congruenza è verificata se e solo se

$$n - m \equiv 3 \ mod(ord_{U_9}([2])).$$

Lezione 15 Algebra I

Federico De Sisti

2024-11-19

1 Nella lezione precedente..

Teorema 1 (1^o Teorema di Sylow)
p primo che divide $|G|$ Allora $Syl_p(G) \neq \emptyset$

Teorema 2 (2^o Teorema di Sylow)
p primo divide $|G|$ allora:

$$\forall H, K \in Syk_p(G) \;\; \exists g \in G \text{ tale che } H = gKg^{-1}.$$

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^o 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

$$C(S) = \{g \in G | gs = sg \quad \forall s \in S\}.$$

2) Il normalizzatore di S in G è

$$N_G(S) = \{g \in G | gS = Sg\}.$$

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
$G \times Syl_p(G) \to Syl_p(G)$
$(g, H) \to g.H := gHg^{-1}$
Allora $\forall H \in Syl_p(G)$
$p^r m = |G| = [G : Stab_H] \cdot |Stab_H|$
$= [G : N_G(H)] \cdot |N_G(H)|$ *(dato che $Stab_h = N_G(H)$)*
$= [G : B_G(H)][N_G(H) : H]|H|$ *(dato che $H \leq N_G(H)$)*
Deduciamo che $m = [G : N_G(H)] \cdot [N_G(H) : H]$
Ora:
$n_p = |Syl_p(G)| = |O_H^G|$ *(II Teorema di Sylow)*
$= [G : Stab_H]$
Quindi abbiamo dimostrato (1) *e* (2)
Resta da dimostrare (3)
di un fissato $K \in Syl_p(G)$

$$K \times Syl_p(G) \to Syl_p(G).$$
$$(k, H) \to k.H := kHk^{-1}.$$

Questa azione avrà $r + 1$ orbite (con $r \geq 0$)
$O_K^K, O_{H_1}^K, \ldots, O_{H_r}^K$
Abbiamo una decomposizione in orbite disgiunte

$$Syl_p(G) = O_K^K \cup O_{H_1}^K \cup \ldots \cup O_{H_r}^K.$$

$$\Rightarrow n_p = |Syl_p(G)| = |O_K^K| + \sum_{j=1}^{r} |O_{H_j}^K|$$

$$= |O_K^K| + \sum_{j=1}^{r} [K : Syl_{H_j}^K].$$

$$= |O_K^K| + \sum_{j=1}^{r} [K : N_K(H_j)].$$

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 $K \in Syl_p(G)$
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 $p^{2r-s_j} \not| \, p^r m$ *da cui l'assurdo per Lagrange* $\square$

3 Applicazioni di Sylow

Possiamo (ri)-dimostrare un vecchio risultato

Teorema 4 (Cauchy)
G gruppo finito, p primo che divide $|G|$ *allora*

$$g \in G \text{ tale che}$$

$ord(g) = p$.

Dimostrazione
Da Sylow I segue che esiste $H \in Syl_p(G)$
Scegliamo $h \in H$ *tale che* $h \neq e$
Ora $ord(h) = p^s$ *per qualche* $s > 0$
Definiamo $f = h^{p^{s-1}}$
$f = h^{p^{s-1}} \neq e \Rightarrow ord(h) \neq 1$
$f^p = (h^{p^{s-1}})^p = h^{p^s} = e \Rightarrow ord(f) = p$ $\square$

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*
$\cdot$ *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
$\Rightarrow (p-2)! = n_p \equiv_p 1 \quad \Rightarrow \quad (p-1)! \equiv_p p-1$ $\square$

Teorema 6 (Classificazione dei gruppi pq)
G gruppo finito, $p, q > 1$ tali che
$\cdot p, q$ primi
$\cdot p < 1$
$\cdot |G| = pq$
Allora
1) Se $p \not| \, q-1$ allora $G \cong C_{pq}$
2) Se $p | q-1$ allora $G \cong C_q \rtimes_\phi C_p$

Dimostrazione
Studio n_p
$$\begin{cases} p = m \equiv_{nq} 0 \\ n_q \equiv_q 1 \end{cases}$$
$$\Rightarrow \begin{cases} n_q = 1 \text{ oppure } m_q = p \\ \text{ seconda esclude } n_q = p \text{ perchè } p < q \end{cases}$$
$\Rightarrow n_q = 1$
$\Rightarrow \exists! Q \in Syl_p(G)$
$\Rightarrow Q \trianglelefteq G$ *e* $|G| = q \Rightarrow Q \cong C_q$
Studio n_p nel caso $p \not| q-1$
$$\begin{cases} q\text{-}m \equiv_{n_p} 0 \\ n_p \equiv_p 1 \end{cases} \quad \Rightarrow n_p = 1 \text{ oppure } n_p = q$$
$\Rightarrow n_p \neq q$ *perché*
$q \not\equiv_p 1$ *per ipotesi*
$n_p = 1 \Rightarrow \exists! P \in Syl_p(G)$
$\Rightarrow PG$ *e* $|P| = p \Rightarrow P \cong C_p$
Ora abbiamo due sottogruppi normali $P, Q \trianglelefteq G$
tali che

$\cdot P \cap Q = \{e\}$ *perchè* $|P \cap Q|$ *divide sia* $|P| = p$ *che* $|Q| = q$
$\cdot PQ| = \frac{|P||Q|}{|P|} = pq = |G|$
$\Rightarrow G \cong P \times Q \cong C_p \times C_q \cong C_{pq}$

Resta il caso $p|q-1$
$\cdot \exists! Q \in Syl_p(G) \rightsquigarrow Q \trianglelefteq G$
$\cdot \exists P \in Syl_p(G) \rightsquigarrow P \leq G$
Ora
$\cdot P \cap Q = \{e\}$ *come prima*
$PQ = G$ *come prima*
Quindi G *prodotto semidiretto interno*
$\Rightarrow G \cong Q \rtimes_{\emptyset} P \Rightarrow C_q \rtimes_{\emptyset} C_p$
per qualche omomorfismo $\phi : C_p \to Aut(C_q)$ $\square$
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 $p \not| q+1$ allora $G \cong C_{pq}$
· se $p|q+1$ allora $G \cong C_q \rtimes_\phi C_p$

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 omomorfisimi

$$\begin{aligned} \phi : & C_2 \to Aut(G) \\ & s \to (\phi_s : r \to s) \end{aligned}$$

Affinchè ϕ sia un omomorfismo, dato che $ord_{C_2}(s) = 2$
dobbiamo imporre che $ord_{Aut(G)}(\phi_s) \in \{1, 2\}$
Se è uguale a 1 $\phi_s = Id \Rightarrow \phi$ omomorfismo banale
$\Rightarrow$ il prodotto è diretto
$\Rightarrow G \cong C_q \times C_2 \cong C_{2q}$
Nell'altro caso $ord_{Aut(G)}(\phi_s) = 2$
$\Rightarrow \phi_s \circ \phi_s = Id_{C_q} \Rightarrow \phi_s(\phi_s(r)) = r$
$\phi_s(r^k) = r$
$\Rightarrow k^2 \equiv_{ord_{C_1}(r)} 1 \Rightarrow k^2 \equiv_q 1$
$\Rightarrow (k-1)(k+1) \equiv_q 0$
$\Rightarrow k \equiv_q \pm 1$
Se $k \equiv_q 1$
$\Rightarrow \phi_s = Id_{C_q} \Rightarrow G \equiv C_{2q}$
Se $k \equiv_q -1$
$\Rightarrow \phi_s(r) = r^{-1}$
$\Rightarrow G \cong C_q \rtimes_\phi C_2 \cong D_q$ *(già visto)*

$\square$

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* $\square$
Esercizio:
Se $|G| = 12$ e $n_3 = 4$ allora esiste un omomorfismo iniettivo $G \to S_4$
Nota
Da questo segue che $G \cong A_4$ perchè A_4 è l'unico sottogruppo di ordine 12 in S_4
Dimostrazione
$G \times Syl_3(G) \to Syl_3(G)$
$(g, H) \to gHg^{-1}$
$n_3 = 4$
$\Rightarrow Syl_3(G) = \{H_1, H_2, H_3, H_4\}$
Definiamo
$\psi : G \to S_4$
$g \to \tau_g$
$\tau_g(i) = j \Leftrightarrow gHg^{-1} = H_j$ *con* $i \in \{1, 2, 3, 4\}$ *(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*

$$\psi(gf) = \psi(g)\psi(f).$$

$\tau_{gf}(i) = j$
$\Leftrightarrow (gf)H(gf)^{-1} = H_j$
$\Leftrightarrow g(fHf^{-1})g^{-1} = H_j$
$\Leftrightarrow \tau_g(\tau_f(i)) = j$
3) ψ iniettiva
supponiamo che $\tau_g = \tau_f$
$gHg^{-1} = fHf^{-1} \quad \forall H \in Syl_3(G)$
$\Rightarrow (f^{-1}g)H(f^{-1}g)^{-1} = H \quad \forall H \in Syl_3(G)$
$\Rightarrow f^{-1}g \in N_G(H) \quad \forall H \in Syl_3(G)$
$\Rightarrow f^{-1}g \in \bigcap_{H \in Syl_3(G)} N_G(H)$
$\Rightarrow f^{-1}g \in \bigcap_{H \in Syl_3(G)} H = \{e\} \Rightarrow f^{-1}g = 3 \Rightarrow f = g$
Resta da verificare che $H = N_G(H)$
$4 = n_3 = [G : N_G(H)] = \dfrac{|G|}{|N_G(H)|} = \dfrac{12}{N_G(H)} \Rightarrow |N_G(H)| = 3$
Ma $H \leq N_G(H) \Rightarrow H = N_G(H)$ $\square$

3.1 Studiare gruppi di ordine 12 in cui $n_3 = 1$

Da Sylow III Segue che $\exists! Q \in Syl_3(G) \Rightarrow Q \trianglelefteq G$
Esiste in G almeno un 2-Sylow $P \leq G$
Ora:
$\cdot G \trianglelefteq G, \quad P \leq G$
$\cdot Q \cap P = \{e\}$ (perchè l' $MCD(|Q|, |P|) = 1$
$\cdot |QP| = \dfrac{|Q||P|}{|Q \cap P|} = \dfrac{3 \cdot 4}{1} = 12$
$\Rightarrow QP = G$
Allora $G \cong Q \rtimes_\phi P$ per qualche
$\phi : P \to Aut(Q) \cong C_2$
Quindi studiamo i possibili omomorfismi
$\phi : P \to Aut(C_3)$ se $P \cong C_4$
$C_4 =< \gamma > \quad C_3 =< r >$
$\phi :<\gamma>\to Aut(C_3)$
$\gamma \to (\phi_\gamma : r \to r^k$ con k $\pm$ 1) nel csao $k = 1$ abbiamo ϕ banale
$\Rightarrow$ prodotto diretto
$\Rightarrow G \cong C_3 \times C_4 \cong C_{12}$
nel caso $k = -1$
abbiamo $G \cong C_3 \rtimes_\phi C_4 \cong Dic_3$
dove
$\phi : C_4 \to Aut(C_3)$
$\gamma \to (\phi_\gamma : r \to r^{-1})$

$P \cong K_4$
$\phi : K_4 \to Aut(C_3)$

$\{Id, a, b, ab\}$

$a \to (\phi_a : r \to r^{\pm 1})$

$b \to (\phi_b : r \to r^{\pm 1})$

$ab \to (\phi_{ab} : r \to r^{\pm 1})$
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

$\phi_a r \to r$

$\phi_b r \to r^{-1}$ Grazie (!) a Esercizio 1 di scheda 7 tutti i restanti prodotti

$\phi_{ab} r \to r^{-1}$
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 $ord_{U_n}([a]) = \phi(n)$

Osservzaione:
Per teorema di Eulero

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

$\Rightarrow ord_{U_n}([a]) = \phi(n)$
Osservazione
a radice primitiva mod (n) significa che $U_n =< [a] >$
Obiettivo (Scheda 7)
Dimostrare che se $p > 1$ primo allora $\exists$ radice primitiva modulo (p)
Esempi
Non esistono radici primitive mod(8)
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
$Aut(C_p) \cong C_{p-1}$
Soluzione
Sappiamo che
$Aut(C_p) \cong U_p \cong C_{\phi(p)} \cong C_{p-1}$
Esercizio
p primo
$f(x) = a_n x^n + \ldots + a_1 x + a_0$
$f(x) \equiv_p 0$ ammette al più p soluzioni distinte in $\mathbb{Z}/(p)$

Dimostrazione
per induzione su n
se $n = 1 \Rightarrow a_1 x \equiv_p -a_0$
$\Rightarrow x \equiv_p = -a \cdot a_1^{-1}$ $\quad$ a_1 *invertibile in* $\mathbb{Z}/(p)$ *per ipotesi*
$n > 1$
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*:*
$\Rightarrow 0 \equiv_p f(a) \equiv_p (a-a)q(a) + r$
$\Rightarrow f(x) \equiv_p (x-a)q(x)$
Sia $b \not\equiv_p a$ *tale che* $f(b) \equiv_p 0$
$0 \equiv_p f(b) \equiv_p (b-a)q(b)$
$\mathbb{Z}/(p)$ *dominio d'integrità*
$q(b)_p 0$

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*

$\square$

Lezione 17 Algebra I

Federico De Sisti

2024-11-26

1 Ricordo (Lagrange)

$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ 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 $1, 2, \ldots, p-1$
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 $x^d - 1 \equiv_p$ 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. □

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 $S_d = \{k \in \mathbb{Z} | ord_{U_p}([k]) = d, \quad 1 \leq k \leq p-1\}$
La tesi è equivalente a dimostrare che $|S_d| = \phi(d)$
Abbiamo una partizione $\{1, \ldots, p-1\} = \bigcup_{d|p-1} S_d$
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 $S_d \neq \emptyset \Rightarrow \exists a \in S_d$
$\Rightarrow \{a, a^2, a^3, \ldots, a^d\}$ *sono tutti distinti mod(p) infatti*

$$a^i \equiv_p a^k$$
$$\Updownarrow$$
$$i \equiv_d j$$

Quindi $a, a^2, \ldots, a^n$ 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 $j \in \{1, \ldots, j\}$
Ma $ord([a^j]) = \frac{d}{MCD(j,d)}$ (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 $Aut(C_p) \cong C_{p-1}$
Soluzione:
Sappiamo che $Aut(C_p) \cong U_p \cong C_{p-1}$
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 $ord_{U_p}([a] \neq p - 1$
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:

$\cdot P \cap Q = \{e\}$

$\cdot |PQ| = |G| \Rightarrow PQ = G$

$\Rightarrow G \cong Q \rtimes_{\phi} P \cong C_q \rtimes_{\phi} C_p$