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)*

□

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 $H = N_G(H)$
$4 = n_3 = [G : N_G(H)] = \frac{|G|}{|N_G(H)|} = \frac{12}{N_G(H)} \Rightarrow |N_G(H)| = 3$
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' $MCD(|Q|, |P|) = 1$
$\cdot |QP| = \frac{|Q||P|}{|Q \cap P|} = \frac{3 \cdot 4}{1} = 12$
$\Rightarrow QP = G$
Allora $G \cong Q \rtimes_{\phi} P$ per qualche
$\phi : P \to Aut(Q) \cong C_2$
Quindi studiamo i possibili omomorfismi
$\phi : P \to Aut(C_3)$ se $P \cong C_4$
$C_4 =< \gamma > \qquad C_3 =< r >$
$\phi :< \gamma > \to Aut(C_3)$
$\quad \gamma \to (\phi_\gamma : r \to r^k$ 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
$\phi : C_4 \to Aut(C_3)$
$\quad \gamma \to (\phi_\gamma : r \to r^{-1})$

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

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

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

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

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

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 $n = 1 \Rightarrow a_1 x \equiv_p -a_0$
$\Rightarrow x \equiv_p = -a \cdot a_1^{-1}$ $\qquad$ 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*

$\square$