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* □

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 $f = h^{p^{s-1}}$
$f = h^{p^{s-1}} \neq e \Rightarrow ord(h) \neq 1$
$f^p = (h^{p^{s-1}})^p = h^{p^s} = e \Rightarrow ord(f) = p$ □

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 $\phi : C_p \rightarrow Aut(C_q)$ $\square$

Esercizio:
Classificare i gruppi di ordine $2q$ con $q > 2$ primo