Facoltà di Scienze MFN- Corso di laurea in Matematica

ALGEBRA 2 - G.M. Piacentini Cattaneo -

RIEPILOGO SUI GRUPPI

SOLUZIONI

(1) Sia G l'insieme di tutte le matrici reali della forma

$$\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

rispetto al prodotto.

(a) Verificare che si tratta di un gruppo.

(b) Provare che si tratta di un gruppo risolubile.

SOLUZIONE.

Osserviamo che

$$\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a' & b' & c' \\ 0 & 1 & 0 & d' \\ 0 & 0 & 1 & e' \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b' & c+c'+be'+ad'+ \\ 0 & 1 & 0 & d+d' \\ 0 & 0 & 1 & e+e' \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

e quindi il prodotto sta ancora in G. Inoltre, se

$$X = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

allora

$$X^{-1} = \begin{pmatrix} 1 & -a & -b & -c+be+ad \\ 0 & 1 & 0 & -d \\ 0 & 0 & 1 & -e \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Quindi si tratta di un gruppo.

Posto

$$A := \{ \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid c \in \mathbb{R} \}$$

si verifica facilmente che A è un sottogruppo di G e che si tratta di un sottogruppo normale in G. Il quoziente

$$G/A = \{ \begin{pmatrix} 1 & a & b & 0 \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} A, \ a, b, d, e \in \mathbb{R}\}$$

è abeliano (facile da verificare) . Ne segue che il derivato G' di G è contenuto in A. Allora due casi possono presentarsi: $G' = A$ o $G' = \{e\}$. Nell'ultimo caso il gruppo G è risolubile perché esiste un indice $k(= 1)$ tale che $G^{(k)} = \{e\}$. Nel primo caso risulta invece, come è facile controllare, $G^{(2)} = \{e\}$. In ogni caso G è risolubile.

(2) Siano H e K due gruppi risolubili. Provare che il loro prodotto diretto $H \times K$ è risolubile.

SOLUZIONE H è risolubile se e solo se esiste una successione finita di sottogruppi $H_0 = H, H_1, H_m$ tali che

$$H = H_0 \supset H_1 \supset \dots H_m = \{e\}$$

tali che H_{i+1} sia normale in H_i e H_i/H_{i+1} sia abeliano.

K è risolubile se e solo se esiste una successione finita di sottogruppi $K_0 = K \supset K_1, \dots K_r$ tali che

$$K = K_0 \supset K_1 \supset \dots K_r = \{e\}$$

tali che K_{i+1} sia normale in K_i e K_i/K_{i+1} sia abeliano.

Per provare che $H \times K$ è risolubile basta esibire una catena analoga. Consideriamo la catena

$$H \times K \supset H_1 \times \{e\} \supset \dots \{e\} \times K \supset \{e\} \times K_1 \supset \{e\} \times K_2 \supset \dots \{e\} \times \{e\}.$$

Dato che

$$\frac{H_i \times K}{H_{i+1} \times K} \simeq \frac{H_i}{H_{i+1}}, \quad \text{e} \quad \frac{\{e\} \times K_j}{\{e\} \times K_{j+1}} \simeq \frac{K_i}{K_{j+1}}$$

si deduce che il prodotto è risolubile.

(3) Provare che ogni gruppo di ordine 30 possiede un sottogruppo ciclico normale in G di ordine 15.

SOLUZIONE

$30 = 2 \cdot 3 \cdot 5$.

$N_3 | 10, \qquad N_3 \equiv 1 \pmod 3$, quindi $\mathbb{N}_3 \in \{1, 10\}$;

$N_5 | 6, \qquad N_5 \equiv 1 \pmod 5$, quindi $\mathbb{N}_5 \in \{1, 6\}$;

(a) Supponiamo $N_3 = 1$, e quindi che esista un unico 3-Sylow normale P. In tal caso possiamo fare il gruppo quoziente G/P che ha ordine 10. Ora, un gruppo di ordine 10 ha sempre un $5-$Sylow normale che ha 5 elementi. Quindi G/P ha un 5-Sylow normale, diciamo N/P. Per il teorema di corrispondenza, N è normale in G e N ha 15 elementi (infatti $\frac{|N|}{|P|} = \frac{|N|}{3} = 5$, da cui $|N| = 15$).
Quindi N è il gruppo di ordine 15 ciclico e normale richiesto.

(b) Supponiamo invece $N_3 = 10$, cioè che G abbia 10 3-Sylow distinti, P_1, $P_2, \dots P_{10}$. Allora G possiede $10 \cdot 2 = 20$ elementi distinti di ordine 3. Allora G avrà solamente

$$30 - (1 + 20) = 9$$

elementi di ordine $\neq 1, 3$.
Se G avesse 6 5-Sylow, un ragionamento analogo a quello appena fatto mostrerebbe che avrebbe 24 elementi di ordine 5: assurdo perché abbiamo appena detto che di questi ce ne possono essere al più 9.
Quindi se G ha 10 3-Sylow, *deve* avere *un solo* 5-Sylow: chiamiamolo Q.
Il quoziente G/Q ha 6 elementi. Ora un gruppo con 6 elementi o è ciclico, oppure è isomorfo a $\mathcal{S}_3$, quindi in ogni caso contiene un sottogruppo normale di ordine 3, N/Q. Per il teorema di corrispondenza N è normale in G e $\frac{|N|}{|Q|} = 3$ da cui $|N| = 15$. Quindi ancora G contiene un sottogruppo normale di 15 elementi (ciclico).

(4) Sia G un sottogruppo di $\mathcal{S}_4$, e si consideri l'azione naturale di G sull'insieme $\{1, 2, 3, 4\}$. Per ciascuna delle seguenti scelte di G scrivere le orbite dell'azione e trovare lo stabilizzatore. Verificare la formula

$$|G| = |\mathcal{O}(x)||St_x|.$$

(a) $G = \langle(1, 2, 3)\rangle$;
(b) $G = \langle(1, 2, 3, 4)\rangle$;
(c) $G = \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$;
(d) $G = \{id, (1, 2), (3, 4), (1, 2)(3, 4)\}$;
(e) $G = A_4$.

(5) Data la permutazione $(1, 2) \in \mathcal{S}_n$, quante sono le permutazioni che commutano con $(1, 2)$?
SOLUZIONE

Si tratta di calcolare $|C((1,2))|$. Tra le permutazioni che commutano con $(1,2)$ ci sono certamente le permutazioni di $\mathcal{S}_n$ che fissano 1 e 2: sono in tutto $(n-2)!$. Inoltre c'è $(1,2)$ stessa. Allora le $2(n-2)!$ permutazioni del sottogruppo generato da $(1,2)$ e da quelle che fissano 1 e 2 commutano con $(1,2)$. Dico che sono tutte: infatti, indicato con $c_{(1,2)}$ il numero di coniugati di $(1,2)$,

$$c_{(1,2)} = \frac{|\mathcal{S}_n|}{|C((1,2))|} = \frac{n!}{x}$$

Essendo $c_{(1,2)} = \frac{n(n-1)}{2}$, segue che $x = |C((1,2)) = 2(n-2)!$, come avevamo stabilito.

(6) Quante sono le permutazioni che commutano con $(1,2,3,4,\dots n)$?

SOLUZIONE Di sicuro $(1,2,3,\dots nn)$ permuta con le sue potenze, che sono in numero di n. Dico che sono tutte. Infatti

$$(n-1)! = c_{(1,2,\dots n)} = \frac{|\mathcal{S}_n|}{|C((1,2,\dots,n))} = \frac{n!}{x}$$

da cui $x = n$.

(7) Quanti sono e quali sono i gruppi abeliani non isomorfi di ordine 144?

SOLUZIONE

$144 = 2^4 \cdot 3^2$.

Le partizioni di 4 sono 5 : $\quad 4, 3+1, 2+2, 2+1+1, 1+1+1+1$, ossia $p(4) = 5$

Le partizioni di 2 sono 2, ossia $p(2) = 2$.

Quindi i gruppi di ordine 144 e abeliani sono in numero di $p(4) \cdot p(2) = 5 \cdot 2 = 10$.

I gruppi abeliani non isomorfi di ordine 144 sono i seguenti:

$$\mathbb{Z}_{2^4} \times \mathbb{Z}_{3^2} = \mathbb{Z}_{16} \times \mathbb{Z}_9 : \qquad \text{ciclico}$$

$$\mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$$

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$$

$$\mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$\mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

(8) Determinare l'ordine massimo tra gli elementi dei seguenti gruppi:

(a) $\mathbb{Z}_4 \times \mathbb{Z}_6$
(b) $\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_{21}$
(c) $\mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$

SOLUZIONE

(a) 12
(b) 210
(c) 30

(9) Determinare i p-Sylow dei gruppi dell'esercizio precedente e la decomposizione in prodotto di gruppi ciclici del teorema fondamentale dei gruppi abeliani finiti.

Verificare il risultato dell'esercizio precedente.

SOLUZIONE

(a) La decomposizione del teorema fondamentale sui gruppi abeliani è :
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$
Il 2-Sylow è $\mathbb{Z}_4 \times \mathbb{Z}_2$. il 3-Sylow è $\mathbb{Z}_3$.

(b)
$$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3\mathbb{Z}_5 \times \mathbb{Z}_7$$
Il 2-Sylow è $\mathbb{Z}_2$, il 3-Sylow è $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, il 5-Sylow è $\mathbb{Z}_5$ e il 7-Sylow è $\mathbb{Z}_7$.

(c)

(10) Provare che ogni gruppo di ordine p^2q, p, q primi distinti, non è semplice.

SOLUZIONE

Proveremo che G ha o un p-Sylow o un q-Sylow normale.

N_q può essere: 1, p o p^2. Esamineremo separatamente i 3 casi:

(a) Se $N_q = 1$ il gruppo contiene un unico q-Sylow, che è quindi normale.
(b) Supponiamo $N_q = p$. Allora $N_q = p \equiv 1 \pmod q$ e in particolare $p > q$. Quindi $q \not\equiv 1 \pmod p$ e non si può avere $N_p = q$. Quindi $N_p = 1$ e pertanto esiste un sottogruppo normale.
(c) Supponiamo infine $N_q = p^2$. Contiamo gli elementi: Se P_1 e P_2 sono due $q-$Sylow ($P_1 \neq P_2$) allora $P_1 \cap P_2 = \{1\}$. Ci sono in tutto p^2 q-Sylow, ciascuno con $q - 1$ elementi diversi dall'identità , per cui in tutto ci sono $p^2(q-1)$ elementi elementi di ordine q diversi dalll'identità . Sia X l'insieme degli elementi che non abbiamo contato ancora.
$$|X| = |G| - p^2(q-1) = p^2$$

e ogni elemento di G con ordine diverso da q sta in X. Se quindi S è un p-Sylow, i suoi elementi non hanno ordine q, per cui $S \subseteq X$. Dato che $|S| = p^2 = |X|$, segue che $S = X$ da cui segue che S è l'unico p-Sylow, per cui è normale.

(11) Provare che ogni gruppo di ordine p^2q è risolubile.
SOLUZIONE
Se G contiene un p-Sylow normale, P, allora

$$G \supset P \supset \{e\}$$

è una catena tale che ogni sottogruppo è normale nel precedente e G/P avendo q elementi (q primo) è abeliano, e $P/\{e\}$ anche, avendo cardinalità p^2.
Se invece G contiene un q-Sylow normale, Q, la catena

$$G \supset Q \supset \{e\}$$

è ancora tale che G/Q è abeliano, avendo p^2 elementi e così $Q/\{e\}$.

(12) Sia G un gruppo tale che $|G| = p^3 \cdot q$, p, q primi. Provare che G possiede o un p-Sylow normale o un q-Sylow normale, oppure $p = 2$, $q = 3$ e $|G| = 24$.
SOLUZIONE
Si può supporre $p \neq q$ $N_q > 1$ e $N_p > 1$. Le possibilità per N_q sono pertanto $N_q = p, p^2, p^3$.
(a) $N_q = p$: dato che possiamo supporre $N_p > 1$ segue che $N_p = q$ e $q \equiv 1 \pmod p$ da cui $q > p$ e *non* si può avere $p \equiv 1 \pmod q$. Questo esclude che possa essere $N_q = p$.
(b) $N_q = p^3$: contiamo gli elementi. Ci sono $p^3(q-1)$ elementi di ordine q. Esiste quindi un insieme X contenente tutti gli elementi di ordine diverso da q, e $|X| = p^3$. Ne segue che un p-Sylow S arbitrario coincide con X , ossia c'è un unico p-Sylow ed è pertanto normale. Questo contraddice che sia $N_p > 1$.
(c) $N_q = p^2$. Si ha allora $p^2 \equiv 1 \pmod q$, da cui $q|p^2 - 1$, ossia $p|(p-1)(p+1)$. Essendo p primo $q|p-1$ o $q|p+1$. essendo $q > p$ non può essere $q|(p-1)$ da cui $q|(p+1)$ e quindi $p < q \leq p+1$. Ne segue che $q = p + 1$. Dato che 2 e 3 sono gli unici primi consecutivi, si ha $p = 2$ e $q = 3$, e quindi $|G| = 24$.

(13) Sia G un gruppo finito e sia S un $p-$ Sylow, (p divisore primo di $|G|$). Provare che se P è un p-sottogruppo di $N_G(S)$, allora $P \subseteq S$.
SOLUZIONE

Ricordiamo che $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$. Dato che $P \leq N_G(S)$ ne segue che PS è un sottogruppo di G. Si ha

$$|PS| = \frac{|P||S|}{|P \cap S|}$$

quindi PS è ancora un p-gruppo. Ma $PS \supseteq S$. Dato che S è un p-Sylow, *deve* essere $PS = S$ da cui $|P| = |P \cap S|$ cioè $P \subseteq S$.

(14) Determinare tutti i gruppi di ordine 177.

SOLUZIONE

$177 = 3 \cdot 59$. Ora, un gruppo di ordine pq, $q > p$ contiene sempre un sottogruppo normale di ordine q e, se $q \not\equiv 1 \pmod p$, allora il gruppo è ciclico (perché diventa prodotto diretto di due gruppi di ordini coprimi). In questo caso $q - 1 = 58$ non è multiplo di $p = 3$ quindi c'è un solo gruppo di ordine 177 ed è il gruppo ciclico di quell'ordine.

(15) Sia G un gruppo abeliano finito. Provare l'equivalenza delle seguenti affermazioni:

(a) G possiede un p-Sylow *ciclico* per ogni p divisore di $|G|$;
(b) G è ciclico
(c) G possiede un unico sottogruppo di ordine p per ogni p divisore primo di $|G|$.

SOLUZIONE

a) $\Longrightarrow$ *b*) Sia $|G = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$. Indichiamo con x_{p_i} un generatore di ogni p_i-Sylow di G al variare di p_i tra i divisori primi di $|G|$. Sia $n = \frac{|G|}{p_i}$: per ogni $p_j \neq p_i$ si ha $x_{p_j}^n = 1$ essendo n un multiplo dell'ordine di x_{p_j}, $(i \neq j)$. Posto $g = \Pi x_{p_i}$, risulta (il gruppo è abeliano) $g^n = \Pi(x_{p_k})^n = x_{p_i}^n$ e questo non è uguale ad 1, dato che il periodo di x_{p_i} è $p_i^{h_i}$, mentre $n = p_1^{h_1} \cdots p_i^{h_i - 1} \cdots p_r^{h_r}$ (cioè n non è un multiplo del periodo). Ne segue che il periodo di g non può essere un divisore *proprio* di $|G|$. Ne segue che il periodo di g deve coincidere con $|G|$, ossia g è un generatore di G e G è pertanto ciclico.

$b \Longrightarrow c$

Questa è una proprietà che ben conosciamo dei gruppi ciclici finiti: un gruppo ciclico ha uno e un solo sottogruppo per ogni divisore del suo ordine, e quindi in particolare per ogni divisore primo.

$c \Longrightarrow a$) Per ogni divisore primo p di $|G|$, in base al teorema fondamentale sui gruppi abeliani finiti, ogni p-Sylow Σ_p è prodotto diretto di p-gruppi ciclici,

$$\Sigma_p \simeq \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \ldots \mathbb{Z}_{p^{\alpha_n}}$$

Ogni $\mathbb{Z}_{p^{\alpha_i}}$, per $i = 1, \dots n$ contiene un sottogruppo di ordine p e per $i \neq j$ questi saranno distinti. In base a c) segue che deve necessariamente essere $n = 1$, ossia Σ è ciclico.

(16) Sia G un gruppo che possiede un sottogruppo normale N risolubile tale che anche il quoziente G/N sia risolubile. Provare che G è risolubile.

(17) In quanti modi diversi si possono disporre due chiavi rosse e due chiavi verdi in un portachiavi circolare? Dare una spiegazione in termini di azioni e orbite.

SOLUZIONE

Le quattro chiavi (due rosse e due verdi) si possono disporre in $\binom{4}{2} = 6$ modi. Ma non tutti questi modi danno luogo a configurazioni effettivamente distinauibili. Sono distinguibili solo quelle che appartengono ad orbite diverse rispetto all'azione di D_4 sull'insieme S di tutte le 6 configurazioni. Contare il numero di configurazioni diverse equivale quindi a contare le orbite di S rispetto all'azione di D_4. In base al teorema di Burnside, tale numero n è

$$n = \frac{1}{|G|} \sum_{g \in G} X_g, \qquad X_g = \{x \in G \mid gx = x\}$$

Nel nostro caso

$$n = \frac{1}{8}[6 + 0 + 2 + 0 + 2 + 2 + 2 + 2] = 2$$

avendo fatto variare gli elementi $g \in D_4$ nel seguente ordine: $id, r, r^2, r^3, s, rs, r^2s, r^3s$

(18) Sia G un gruppo di ordine 117. Decidere se è sempre risolubile. In caso positivo, costruire una catena.

SOLUZIONE

$117 = 3^2 \cdot 13$. Quindi ogni gruppo di quest'ordine è risolubile, in virtù dell'esercizio 11.

In questo caso $N_{13} = 1$ quindi esiste un q-Sylow normale Q. Una catena sarà :

$$G \supset Q \supset \{e\}.$$

(19) (a) Dare un esempio di gruppo semplice;
(b) dare un esempio di gruppo non semplice;
(c) dare un esempio di gruppo risolubile;

(d) dare un esempio di gruppo non risolubile.

(20) Sia G un gruppo di ordine 319.
(a) provare che G è ciclico;
(b) determinare tutti i possibili ordini degli elementi di G e per ogni ordine m il numero di elementi di G aventi ordine m.
SOLUZIONE
(a) $319 = 11 \cdot 29$. Esiste un unico 29-Sylow, che è quindi normale. Essendo poi $q - 1 = 28 \not\equiv 1 \pmod{11}$ si ha che il gruppo è necessariamente ciclico.
(b) Possibili ordini: tutti i divisori di 319, ossia 1, 11, 29, 319.
Elementi di ordine 1: uno solo, l'identità : $\{(e, e)\}$
Elementi di ordine 11: quelli di tipo (a, e), con $a \neq e$: sono in tutto 10
Elementi di ordine 29: quelli di tipo (e, b) con $b \neq e$: sono in tutto 28
Tutti gli altri $(319 - (10 + 28 + 1) = 280)$ sono generatori, e sono del tipo (a, b), $a, b \neq e$.
Dato che i generatori di un gruppo ciclico di ordine n sono in numero di $\varphi(n)$, φ funzione di Eulero, verifichiamolo:

$$\varphi(319) = \varphi(11)\varphi(29) = 10 \cdot 28 = 280.$$

(21) Determinare tutti i gruppi di ordine 289.
SOLUZIONE
$289 = 17^2$. Dato che l'ordine è il quadrato di un numero primo, ogni gruppo di ordine 289 è abeliano. Quindi i gruppi di ordine 289 sono i seguenti:

$$\mathbb{Z}_{289} \simeq \mathbb{Z}_{17^2} \qquad \text{ciclico}$$

$$\mathbb{Z}_{17} \times \mathbb{Z}_{17}$$

(22) (a) Determinare quanti gruppi abeliani non isomorfi ci sono di ordine 2800 e 13270.
(b) Per ciascun tipo determinarne uno.

(23) (a) Quali dei seguenti gruppi sono isomorfi tra di loro?

$$\mathbb{Z}_{209} \times \mathbb{Z}_{211}, \qquad \mathbb{Z}_{46189}, \qquad \mathbb{Z}_{143} \times \mathbb{Z}_{323}.$$

(b) Per ciascuno dei precedenti gruppi determinare i periodi dei suoi elementi.
SOLUZIONE

(a) Sono tutti isomorfi tra di loro. Infatti, essendo $209 = 11 \cdot 19$, $211 = 13 \cdot 17$, $143 = 11 \cdot 13$ e $323 = 17 \cdot 19$ e $46189 = 11 \cdot 13 \cdot 17 \cdot 19$, si ha

$$\mathbb{Z}_{209} \times \mathbb{Z}_{211} \simeq \mathbb{Z}_{11} \times \mathbb{Z}_{13} \times \mathbb{Z}_{17} \times \mathbb{Z}_{19} \simeq \mathbb{Z}46189 \simeq \mathbb{Z}_{143} \times \mathbb{Z}323$$

(b) I periodi degli elementi di un gruppo ciclico sono tutti e soli i divisori dell'ordine del gruppo ciclico, ossia

$$11^i \cdot 13^j \cdot 17^k \cdot 19^l, \qquad i, j, k, l \in \{0, 1\}$$

(24) Determinare tutti i gruppi abeliani semplici.

SOLUZIONE

Si tratta di determinare ttuti i gruppi privi di sottogruppi normali, ossia, essendo i gruppi abeliani, tutti i sottogruppi privi di sottogruppi (non banali). Quindi si tratta di tutti i gruppi ciclici di ordine un numero primo.