COMPITO DI ALGEBRA 1

5 febbraio 2021

Esercizio 1.
Sia G un gruppo finito, N un sottogruppo normale e $x \in N$. Sia A la classe di coniugio di x in G e C il centralizzatore di x in G. Dimostrare che l'azione di coniugio di N su A ha $[G : NC]$ orbite, tutte con lo stesso numero di elementi.

Soluzione. Dimostriamo innanzitutto che due qualsiasi orbite di questa azione hanno lo stesso numero di elementi. Siano $a, a' \in A$: per ipotesi a, a' sono coniugati in G, ovvero esiste $g \in G$ tale che $a' = gag^{-1}$. Siano rispettivamente X e X' le orbite di a e a' sotto l'azione di N: affermiamo che la funzione $f : x \mapsto gxg^{-1}$ è una bigezione fra X e X'. Verifichiamo innanzitutto f è ben definita, cioè che per ogni $x \in X$ l'elemento gxg^{-1} appartiene ad X'. Per definizione di orbita di a esiste $n \in N$ tale che $x = nan^{-1}$, dunque $f(x) = gnan^{-1}g^{-1} = (gng^{-1})(gag^{-1})(gng^{-1})^{-1} = (gng^{-1})a'(gng^{-1})^{-1}$. Dato che N è normale in G, l'elemento gng^{-1} appartiene ad N, e quindi $f(x)$ è effettivamente nell'orbita per coniugio di a'. Inoltre f è iniettiva, in quanto è la restrizione ad X dell'automorfismo di G dato dal coniugio per g. Questo dimostra che $|X| \leq |X'|$, e data l'evidente simmetria della situazione si ha anche $|X'| \leq |X|$, da cui $|X'| = |X|$ come voluto (e in particolare f è una bigezione).
Per determinare la cardinalità comune di tutte le orbite calcoliamo ora la cardinalità dell'orbita di x. Grazie al lemma orbita-stabilizzatore questa può essere scritta come $|N|/|\operatorname{Stab}(x)|$, dove $\operatorname{Stab}(x)$ è lo stabilizzatore di x per l'azione considerata. Siccome si tratta dell'azione di coniugio, $\operatorname{Stab}(x)$ non è altro che il centralizzatore di x in N, ovvero $C \cap N$. Otteniamo allora che l'orbita di x, e quindi ogni orbita, ha $|N|/|C \cap N|$ elementi. Il numero di orbite è il rapporto fra $|A|$ (la cardinalità dell'insieme su cui avviene l'azione) e $|N|/|C \cap N|$ (la cardinalità di ogni orbita). Nuovamente per il lemma orbita-stabilizzatore abbiamo anche $|A| = |G|/|C|$, da cui il numero delle orbite è

$$\frac{|G|/|C|}{|N|/|C \cap N|} = \frac{|G|}{|N| \cdot |C|/|N \cap C|} = \frac{|G|}{|NC|} = [G : NC],$$

dove si è usata la ben nota formula $|NC| = \frac{|N| \cdot |C|}{|N \cap C|}$.

Esercizio 2.
Consideriamo il gruppo $G = \mathbb{Z}/9\mathbb{Z} \rtimes_\phi \mathbb{Z}/3\mathbb{Z}$ dove $\phi\colon \mathbb{Z}/3\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/9\mathbb{Z})$ è l'unico omomorfismo tale che $\phi(\bar{1})$ sia l'automorfismo $a \mapsto 4a$ di $\mathbb{Z}/9\mathbb{Z}$.

1. Dimostrare che G ha un sottogruppo caratteristico isomorfo a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
2. Determinare tutti i sottogruppi normali e non caratteristici di G.

Soluzione.

1. Usando la notazione moltiplicativa una presentazione del gruppo G è data da
$$\{x, y \mid x^9 = 1, y^3 = 1, yxy^{-1} = x^4\}.$$
Osserviamo che il centro di G ha ordine 3: infatti, il centro non è tutto il gruppo perché G non è abeliano, è non banale perché G è un p-gruppo e non può avere ordine 9 perché in questo caso si avrebbe che $G/Z(G)$ avrebbe ordine 3 e quindi sarebbe ciclico, cosa non possibile in un gruppo non abeliano.

   Dalla regola di commutazione si ricava
$$yx^iy^{-1} = (yxy^{-1})^i = x^{4i},$$
quindi l'elemento x^3 commuta con y e quindi genera il centro. Inoltre $\langle x^3\rangle\langle y\rangle$ è un sottogruppo di G perché i due sottogruppi commutano e ha ordine 9 perché i due gruppi hanno ordine 3 e si intersecano banalmente, quindi $H = \langle x^3\rangle\langle y\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Mostriamo che H contiene tutti gli elementi di ordine 3 di G: questo ci dirà che H è caratteristico, cioè che $f(H) = H$ per ogni $f \in \mathrm{Aut}(G)$ in quanto gli automorfismi conservano l'ordine degli elementi.

   Un elemento generico di G è della forma x^iy^j con $0 \leq i < 9$ e $j = 0, 1, 2$:
   - per $j = 0$ abbiamo le potenze di x e tra queste quelle di ordine che divide 3 sono le potenze di x^3;
   - per $j = 1$ si ha $(x^iy)^3 = x^{i(1+4+4^2)}y^3 = x^{3i} = 1$ se e solo se $i \equiv 0 \pmod 3$;
   - per $j = 2$ si ha $(x^iy^2)^3 = x^{i(1+4^2+4^4)}y^3 = x^{3i} = 1$ se e solo se $i \equiv 0 \pmod 3$.

   Concludiamo che x^iy^j ha ordine 1 o 3 se e solo se $i \equiv 0 \pmod 3$, quindi se e solo se appartiene ad H. Tutti gli altri elementi, cioè gli elementi del tipo x^iy^j con $(i, 3) = 1$, hanno ordine 9.

2. Chiaramente i sottogruppi banali sono caratteristici.

   Di ordine 3 abbiamo il centro del gruppo che è caratteristico. Gli elementi di ordine 3 fuori da $\langle x\rangle$ non sono normali (e quindi neppure caratteristici), altrimenti il gruppo G sarebbe abeliano perché isomorfo al prodotto diretto di due sottogruppi ciclici.

   I sottogruppi di ordine 9 di G hanno indice 3, che è il più piccolo primo che divide l'ordine del gruppo, quindi sono tutti normali. Il sottogruppo H del punto precedente è anche caratteristico ed è l'unico abeliano elementare. Gli altri sottogruppi di ordine 9 sono ciclici: dato che gli elementi di ordine 9 sono in tutto $3 \cdot \varphi(9)$, il gruppo G contiene 3 sottogruppi di ordine 9, ed è immediato vedere che sono $\langle x \rangle$, $\langle xy \rangle$ e $\langle x^2 y \rangle$. Vediamo che nessuno di questi è caratteristico. Consideriamo l'assegnamento $f(x) = xy$ e $f(y) = y$: vediamo che questo si estende ad un automorfismo di G. Dalla teoria sappiamo che f si estende ad un omomorfismo di G se gli assegnamenti fatti rispettano le relazioni del gruppo, cioè se

$$\begin{cases} f(x)^9 = 1 \\ f(y)^3 = 1 \\ f(y)f(x)f(y)^{-1} = f(x)^4. \end{cases}$$

Le prime due relazioni sono verificate perché $f(x) = xy$ ha ordine 9 e $f(y) = y$ ha ordine 3. Quanto alla terza relazione osserviamo che $f(y)f(x)f(y)^{-1} = yxyy^{-1} = yx = x^4 y$ e $f(x)^4 = (xy)^4 = x^{(1+4+4^2+4^3)} y = x^4 y$, quindi vale anche questa, e f si estende ad un omomorfismo di G. Inoltre f è anche surgettivo perché $\mathrm{Im}(f) = \langle xy, y \rangle = \langle x, y \rangle = G$, ed essendo G un gruppo finito otteniamo che $f \in \mathrm{Aut}(G)$. Verifichiamo ora che nessuno dei tre sottogruppi di ordine 9 viene fissato da f. Infatti è chiaro che $f(x) = xy \notin \langle x \rangle$ e di conseguenza, dato che f è iniettivo, $f(xy) \notin \langle xy \rangle$. Infine $f(x^2 y) = f(x)^2 f(y) = (xy)^2 y = x^5 \notin \langle x^2 y \rangle$.

In conclusione, i sottogruppi normali e non caratteristici di G sono i sottogruppi ciclici di ordine 9, che sono $\langle x \rangle$, $\langle xy \rangle$ e $\langle x^2 y \rangle$.

Esercizio 3.

1. Sia A un anello commutativo con unità. Dimostrare che A è isomorfo al prodotto di due anelli (non banali, commutativi, con identità) se e solo se esiste $\varepsilon \in A \setminus \{0, 1\}$ tale che $\varepsilon^2 = \varepsilon$.

2. Sia $A = \mathbb{Q}[x, y]/(x^2 - y^2)$. Dimostrare che A **non** è isomorfo al prodotto di due anelli (non banali, commutativi, con identità).

Soluzione.

1. Supponiamo che A sia isomorfo al prodotto diretto $B \times C$ tramite l'isomorfismo φ. Allora posto $\varepsilon := \varphi^{-1}(1, 0)$ si ha $\varepsilon^2 = \varphi^{-1}(1^2, 0^2) = \varphi^{-1}(1, 0) = \varepsilon$, e d'altro canto ε è diverso sia da 0 che da 1 dato che φ è una bigezione e $(1, 0) \neq (0, 0), (1, 1)$ (che sono rispettivamente lo 0 e l'unità dell'anello $B \times C$). Viceversa, supponiamo dato $\varepsilon \in A \setminus \{0, 1\}$ tale che $\varepsilon^2 = \varepsilon$. Osserviamo che ε non può essere un'unità, in quanto in tal caso potremmo moltiplicare per ε^{-1} e ottenere $\varepsilon = 1$, assurdo. In

particolare, l'ideale $I = (\varepsilon)$ non è l'ideale (1). Similmente, $1-\varepsilon$ non può essere un'unità, altrimenti da $\varepsilon(1-\varepsilon) = 0$ otterremmo $\varepsilon = 0$ (nuovamente assurdo): ne segue che $J = (1-\varepsilon)$ non è l'ideale (1). Inoltre $I + J$ contiene $\varepsilon + (1-\varepsilon) = 1$, e quindi si ha $I + J = (1)$. Infine abbiamo $IJ = (\varepsilon)(1-\varepsilon) = (\varepsilon(1-\varepsilon)) = (0)$. Siamo allora nelle condizioni di poter applicare il teorema cinese del resto per ottenere

$$A \cong \frac{A}{(0)} = \frac{A}{IJ} \cong \frac{A}{I} \times \frac{A}{J},$$

e siccome abbiamo già dimostrato che gli anelli A/I e A/J sono non banali abbiamo così ottenuto che A è isomorfo a un prodotto diretto del tipo voluto.

2. Visto il punto precedente si tratta di stabilire se esista $\varepsilon \in A$ tale che $\varepsilon^2 = \varepsilon$. Dal momento che nel quoziente A si ha $\overline{y}^{2k} = \overline{x}^{2k}$ e $\overline{y}^{2k+1} = \overline{y} \cdot \overline{x}^{2k}$, ogni elemento di A è rappresentato da un polinomio $a(x) + yb(x)$ avente grado al massimo 1 in y. Inoltre questa rappresentazione è unica: la differenza di due polinomio di questo tipo non può essere divisibile per $y^2 - x^2$ (che ha grado 2 in y) a meno che non sia nulla. Sia allora $a(x) + yb(y) \in \mathbb{Q}[x, y]$ un rappresentante di ε: ci chiediamo se si possa risolvere
$$(a(x) + yb(x))^2 \equiv a(x) + yb(x) \pmod{(x^2 - y^2)},$$
o equivalentemente, sviluppando e sostituendo y^2 con x^2, vorremmo studiare $a(x)^2 + x^2b(x)^2 + 2a(x)b(x)y \equiv a(x) + yb(x) \pmod{(x^2 - y^2)}$. I due lati della congruenza sono polinomi di grado al massimo 1 in y, e quindi come già osservato sono congrui modulo $x^2 - y^2$ se e solo se sono uguali. Confrontando i termini con lo stesso grado in y otteniamo quindi il sistema

$$\begin{cases} a(x)^2 + x^2b(x)^2 = a(x) \\ 2a(x)b(x) = b(x). \end{cases}$$

Dalla seconda equazione otteniamo $b(x)(2a(x) - 1) = 0$, cioè $b(x) = 0$ oppure $a(x) = 1/2$. Nel primo caso la prima equazione fornisce $a(x)^2 = a(x)$, che per ragioni di grado è possibile solo se $a(x)$ è una costante, e tale costante deve essere uguale a 0 o 1. Le uniche soluzioni in questo caso sono quindi $\varepsilon = 0, 1$. Nel caso $a(x) = 1/2$, invece, la prima equazione fornisce $x^2b(x)^2 = \frac{1}{2} - \frac{1}{4} = \frac{1}{4}$, che è evidentemente impossibile per questioni di grado (il membro sinistro è o 0 o di grado ≥ 2). Concludiamo che l'equazione $\varepsilon^2 = \varepsilon$ in A ha solo le soluzioni banali $\varepsilon = 0, 1$, e quindi che A non si decompone come prodotto diretto.

Seconda soluzione. Vogliamo risolvere $\varepsilon^2 = \varepsilon$ in A, ovvero (detto $q(x, y) \in \mathbb{Q}[x, y]$ un rappresentante di ε) vorremmo $x^2 - y^2 \mid q^2 - q = q(q-1)$. Stiamo ora lavorando nell'UFD $\mathbb{Q}[x,y]$, in cui $x-y$ e $x+y$ sono primi (in quanto irriducibili). Se entrambi questi fattori dividono q, oppure entrambi dividono $q-1$, allora $\varepsilon = q+(x^2-y^2) = 0+(x^2-y^2)$ o $1-\varepsilon = 1-q+(x^2-y^2) = 0+(x^2-y^2)$, e quindi abbiamo le soluzioni banali $\varepsilon = 0,1$. In caso invece $x-y$ divida q e $x+y$ divida $q-1$ (o viceversa: la situazione è simmetrica) possiamo scrivere $q(x,y) = (x-y)c(x,y)$ e $1-q(x,y) = (x+y)d(x,y)$. Otteniamo allora $1 = q(x,y)+(1-q(x,y)) = (x-y)c(x,y)+(x+y)d(x,y)$, e valutando in $x=y=0$ otteniamo $1=0$, assurdo. Le uniche soluzioni dell'equazione $\varepsilon^2=\varepsilon$ in A sono quindi $\varepsilon=0$ e $\varepsilon=1$.

Esercizio 4. Sia M in campo di spezzamento del polinomio $f(x) = (x^4-3)(x^3-5)$.

1. Determinare il grado di $M/\mathbb{Q}$.

2. Descrivere il gruppo di Galois di $M/\mathbb{Q}$ come prodotto semidiretto di sottogruppi non banali.

Soluzione.

Anche se non è strettamente necessario, studiamo dapprima separatamente i campi di spezzamento su $\mathbb{Q}$ dei polinomi $g(x) = x^3-5$ e di $h(x) = x^4-3$.

Le radici del polinomio $g(x)$ sono $\zeta_3^k\sqrt[3]{5}$ dove $k=0,1,2$, quindi il suo campo di spezzamento su $\mathbb{Q}$ è $F = \mathbb{Q}(\sqrt[3]{5},\zeta_3) = \mathbb{Q}(\sqrt[3]{5}, i\sqrt{3})$.

Ora, $[\mathbb{Q}(\sqrt[3]{5}):\mathbb{Q}] = 3$ perché il polinomio x^3-5 è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein e il Lemma di Gauss; inoltre $\zeta_3 \notin \mathbb{Q}(\sqrt[3]{5})$ in quanto questa è un sottocampo di $\mathbb{R}$, per cui $[F:\mathbb{Q}] = 6$. Il gruppo di Galois del polinomio x^3-5 è quindi un sottogruppo di ordine 6 di S_3, quindi $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

Le radici del polinomio $h(x) = x^4-3$ sono $i^k\sqrt[4]{3}$ dove $k=0,1,2,3$, quindi un calcolo immediato mostra che il suo campo di spezzamento K è $\mathbb{Q}(\sqrt[4]{3},i)$. Abbiamo $[K:\mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{3})(i):\mathbb{Q}(\sqrt[4]{3})][\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}] = 2\cdot 4 = 8$: infatti $[\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}] = 4$ perché x^4-3 è il polinomio minimo di $\sqrt[4]{3}$ su $\mathbb{Q}$, in quanto su tale campo è irriducibile (anche in questo caso per il criterio di Eisenstein e il Lemma di Gauss), e $[\mathbb{Q}(\sqrt[4]{3})(i):\mathbb{Q}(\sqrt[4]{3})] = 2$ perché i ha grado 2 sul campo reale $\mathbb{Q}(\sqrt[4]{3})$. Il gruppo di Galois di K su $\mathbb{Q}$ è quindi un sottogruppo di ordine 8 di S_4, cioè un suo 2-Sylow; sappiamo quindi che $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$.

1. Da quanto detto sopra segue che $M = K(\sqrt[3]{5},\zeta_3) = K(\sqrt[3]{5})$, dato che $\zeta_3 = \frac{-1+i\sqrt{3}}{2} \in K$, quindi $[M:\mathbb{Q}] = [K(\sqrt[3]{5}):K][K:\mathbb{Q}]$. Abbiamo già mostrato che $[K:\mathbb{Q}] = 8$. Inoltre $[K(\sqrt[3]{5}):K] = 3$ in quanto il polinomio $g(x) = x^3-5$ è irriducibile su K: infatti, è irriducibile su $\mathbb{Q}$ e le sue radici non possono appartenere a K in quanto $3 \nmid [K:\mathbb{Q}]$; poiché $g(x)$ ha grado 3 e non ha radici in K, è irriducibile su K. Ne segue che $[M:\mathbb{Q}] = 24$.

2. Per calcolare il gruppo di Galois di $M/\mathbb{Q}$ possiamo vedere M come il composto delle sue sottoestensioni K e $L = \mathbb{Q}(\sqrt[3]{5})$. L'estensione $K/\mathbb{Q}$ è normale ed è fissata da $\mathrm{Gal}(M/K)$ che è quindi un sottogruppo normale di $\mathrm{Gal}(M/\mathbb{Q})$ e ha ordine $[M : K] = 3$: questo assicura che il polinomio $g(x)$ rimane irriducibile su K (il campo generato da una sua radice ha grado 3), quindi l'assegnamento $\alpha(\sqrt[3]{5}) = \zeta_3\sqrt[3]{5}$ definisce un elemento non banale del gruppo di Galois di M/K e quindi ne è un generatore.

   D'altra parte M/L è il traslato dell'estensione $K/\mathbb{Q}$, quindi $\mathrm{Gal}(M/L)$ è isomorfo ad un sottogruppo di $\mathrm{Gal}(K/\mathbb{Q})$ e dato che hanno lo stesso grado abbiamo $\mathrm{Gal}(M/L) \cong D_4$.

   Ora $K \cap L = \mathbb{Q}$ (questo segue ad esempio dal fatto che $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$), quindi dalla teoria di Galois otteniamo $\mathrm{Gal}(M/L)\mathrm{Gal}(M/K) = \mathrm{Gal}(M/\mathbb{Q})$ e $\mathrm{Gal}(M/L) \cap \mathrm{Gal}(M/K) = \{id\}$. Questo dimostra che

$$\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{Gal}(M/K) \rtimes_\phi \mathrm{Gal}(M/L) \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi D_4,$$

   dove $\phi\colon D_4 \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^*$. Per descrivere ϕ dobbiamo individuare l'azione di $\mathrm{Gal}(M/L)$ su $\mathrm{Gal}(M/K)$. Il gruppo $\mathrm{Gal}(M/K)$ è isomorfo a D_4 ed è generato da

$$\rho\colon \begin{cases} \sqrt[4]{3} \mapsto i\sqrt[4]{3} \\ i \mapsto i \end{cases} \qquad \sigma\colon \begin{cases} \sqrt[4]{3} \mapsto \sqrt[4]{3} \\ i \mapsto -1 \end{cases}$$

   che hanno rispettivamente ordine 4 e 2.

   Si verifica che $\rho\alpha\rho^{-1} = \alpha^2$ e $\sigma\alpha\sigma^{-1} = \alpha^2$(per verificare le uguaglianze basta valutare i due membri su $\sqrt[3]{5}$). Questo mostra che

$$\phi\colon \mathrm{Gal}(M/L) \to \mathrm{Aut}(\mathrm{Gal}(M/F))$$

   è l'omomorfismo definito da

$$\phi(\rho) = \phi(\sigma) : \alpha \mapsto \alpha^2.$$

   Osserviamo che avremmo potuto fare un discorso analogo invertendo K con F. In. tal caso avremmo ottenuto

$$\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{Gal}(M/F) \rtimes_\psi \mathrm{Gal}(M/L) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\psi S_3$$

   per un opportuno ψ che si può determinare come nel caso precedente.