Algebra 1

Proff. A. D'Andrea, A. De Sole, G. Mondello

Prova scritta del 7 settembre 2022

Nome: _____

Cognome: _____

Numero di matricola: _____

Docente: **D'Andrea \ De Sole - Mondello** (cerchiare il/i docente/i).

Esercizio	Punti totali	Punteggio
1	6	
2	6	
3	6	
4	6	
5	6	
Totale	30	

Esercizio 1. Sia G il gruppo delle matrici 3×3 triangolari superiori unipotenti, ovvero con tutti elementi 1 sulla diagonale principale, a coefficienti nel campo $\mathbb{F}_3$ con tre elementi.

(a) Calcolare l'ordine di G.

(b) Esibire elementi $a, b \in G$ che non commutano tra loro.

(c) Mostrare che ogni elemento $M \in G$ soddisfa $M^3 = \mathrm{Id}$.

(d) Calcolare il centro $Z(G)$ del gruppo G.

Soluzione:

(a) Ciascun elemento di G corrisponde alla scelta dei tre coefficienti al di sopra della diagonale principale, che vanno presi in $\mathbb{F}_3$. L'ordine di G è quindi $3^3 = 27$.

(b) Si vede facilmente che gli elementi

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

non commutano tra loro. Calcolate ad esempio l'ultimo coefficiente sulla prima riga di entrambi i prodotti!

(c) Si può fare anche con le mani, ma più brevemente ogni elemento di G è della forma $I + M$ dove M è una matrice triangolare superiore **stretta**, cioè con zeri sulla diagonale. Poiché ogni matrice commuta con l'identità, si ha

$$(I + M)^3 = I^3 + 3I^2M + 3IM^2 + M^3 = I + M^3,$$

dove i termini misti scompaiono poiché i coefficienti sono in $\mathbb{F}_3$. E' ora facilissimo notare che se M è triangolare superiore stretta, allora $M^3 = 0$.

(d) Prima di procedere, ricordiamo che G è un gruppo non abeliano di ordine 27 e abbiamo visto a lezione che un gruppo non abeliano di ordine p^3, con p primo, ha centro di ordine p. Stiamo quindi cercando tre elementi, uno dei quali è sicuramente l'identità.

La cosa più semplice è procedere con le mani. Si calcola facilmente che

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & b+y+az \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & b+y+cx \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}.$$

Affinché la matrice

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

commuti con tutte le altre, deve valere $az = cx$ per ogni scelta di $a, c \in \mathbb{F}_3$. Scegliendo $a = 1, c = 0$ si ottiene $z = 0$, mentre scegliendo $a = 0, c = 1$ si ottiene $x = 0$. Gli elementi centrali di G sono quindi tutti e soli quelli della forma

$$\begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

che sono proprio 3, dal momento che si ottengono scegliendo $y \in \mathbb{F}_3$.

Risposta:

(a) $|G| =$ [ ] (b) $a, b :$ [ ] (d) $Z(G) =$ [ ]

Esercizio 2. Sia G un gruppo di ordine $n = pqr$ con $p < q < r$ primi. Mostrare che G non è semplice.

Soluzione: Sia G un gruppo semplice di ordine pqr e cerchiamo di ottenere un assurdo.

Innanzitutto, l'r-Sylow non è unico (sarebbe normale) e il numero degli r-Sylow divide pq ed è $\equiv 1$ mod r. Gli unici divisori possibili di pq sono p, q, pq (abbiamo già escluso 1) ma p e q sono inferiori a r e non possono quindi essere $\equiv 1 \mod r$. In conclusione, abbiamo esattamente pq sottogruppi (ciclici!) di ordine r, che danno origine a $pq(r-1) = pqr - pq$ elementi di ordine r.

Passiamo a contare i q-Sylow. Anche qui, i possibili numeri di q-Sylow sono $1, p, r, pr$, ma dobbiamo escludere 1 (l'unico q-Sylow sarebbe normale) e p (non può essere congruo a 1 modulo q, poiché $1 \neq p < q$). In conclusione i q-Sylow sono almeno r. In modo simile si conclude che il numero dei p-Sylow è almeno q e quindi che ci sono almeno $q(p-1)$ elementi di ordine p.

Considerando anche l'identità, abbiamo già contato $(pqr - pq) + (rq - r) + (pq - q) + 1 = pqr + (r-1)(q-1) > pqr = |G|$ elementi. In conclusione, un gruppo semplice di ordine pqr dovrebbe possedere più di pqr elementi, il che è assurdo.

Esercizio 3. Sia I un ideale dell'anello A commutativo con unità. Il radicale di I è definito come

$$\sqrt{I} := \{a \in A \mid a^n \in I \text{ per qualche } n > 0\}.$$

(a) Mostrare che $\sqrt{I}$ è un ideale di A.

(b) Mostrare che, se P è un ideale primo, allora $\sqrt{P} = P$.

(c) Mostrare che, se P è un ideale primo che contiene I, allora $\sqrt{I} \subseteq P$.

(d) Calcolare $\sqrt{I}$ quando $A = \mathbb{Z}$ e $I = (72)$.

Soluzione:

(a) Che $\sqrt{I}$ contenga 0 è immediato. Inoltre, se $a^n \in I$ allora[1] $(ax)^n = a^n x^n$ e poiché I è un ideale, anche $a^n x^n \in I$.

Rimane da mostrare che I sia un sottogruppo additivo, cioè che sia additivamente chiuso. In effetti, se $a^m, b^n \in I$, allora[2]

$$(a+b)^{m+n-1} = \sum_{i+j=m+n-1} \binom{m+n-1}{i} a^i b^j,$$

e si vede subito che se $i + j = m + n - 1$, allora $i \geq m$ oppure $j \geq n$. In ogni caso, ciascun addendo a secondo membro appartiene ad I, e quindi anche la loro somma.

(b) Innanzitutto, $I \subset \sqrt{I}$ è vero sempre (ogni elemento di I, elevato alla prima potenza, sta ancora in I). Dobbiamo quindi dimostrare solo che $\sqrt{P} \subset P$.

Ma in effetti, se $a \in \sqrt{P}$, allora $a \cdot a \cdot \cdots \cdot a \in P$, e poiché P è un ideale primo, almeno uno dei fattori deve appartenere a P. In altre parole $a \in P$ e questo mostra $\sqrt{P} \subset P$.

(c) Se $a \in \sqrt{I}$, allora $a^n \in I \subset P$ per qualche $n \geq 1$. Procedendo come nel punto precedente, si ottiene $a \in P$, il che mostra che $\sqrt{I} \subset P$.

(d) Affinché a^n sia un multiplo di $72 = 2^3 \cdot 3^2$ per qualche $n \geq 1$ è necessario e sufficiente che a sia multiplo di 6. Pertanto $\sqrt{(72)} = (6)$.

Risposta: (d) $\sqrt{I} =$ 

[1] Qui stiamo utilizzando la commutatività del prodotto!!
[2] Anche qui sfruttiamo la commutatività!

Esercizio 4. Sia M in gruppo abeliano generato da tre elementi x, y, z, soggetti alle relazioni

$$\begin{cases} 2x + 3y + 4z = 0 \\ 3x + 3z = 0. \end{cases}$$

Descrivere M come somma diretta di gruppi ciclici.

Soluzione: Si procede come abbiamo visto tante volte. M è l'immagine dell'omomorfismo di $\mathbb{Z}$-moduli $f : \mathbb{Z}^3 \to M$ definito da $f(i, j, k) = ix + jy + kz$, il cui nucleo U è generato dagli elementi $(2, 3, 4), (3, 0, 3)$. Si tratta di capire come sia fatto il quoziente $\mathbb{Z}^3/U$.

Il procedimento per mettere in forma canonica di Smith è facile da eseguire, e porta a:

$$\begin{pmatrix} 2 & 3 \\ 3 & 0 \\ 4 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 3 \\ 1 & -3 \\ 0 & -3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -3 \\ 0 & -3 \\ 2 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -3 \\ 0 & -3 \\ 0 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & -3 \\ 0 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix},$$

indicando che $U \subset \mathbb{Z}^3$, dopo aver eseguito un automorfismo di $\mathbb{Z}^3$, è generato dalle colonne $(1, 0, 0)$, $(0, 3, 0)$. M è isomorfo a $\mathbb{Z}^3/U$ che è allora a sua volta isomorfo a $\mathbb{Z}/(1) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(0) \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}$.

Risposta: $M \simeq$ $\boxed{}$

Esercizio 5. Sia $\mathbb{K} \subset \mathbb{C}$ il campo generato su $\mathbb{Q}$ dalle cinque radici del polinomio $p(x) := x^5 - 9x + 3$.

(a) Determinare se $p(x) \in \mathbb{Q}[x]$ sia irriducibile.

(b) Determinare se $\mathbb{K}$ sia contenuto in $\mathbb{R}$.

(c) Determinare il gruppo di Galois di $\mathbb{K}$ su $\mathbb{Q}$.

(d) Determinare se $\mathbb{K} \cap \mathbb{R}$ sia un'estensione di Galois su $\mathbb{Q}$.

(e) Calcolare il grado di $\mathbb{K} \cap \mathbb{R}$ su $\mathbb{Q}$.

Soluzione:

(a) Si vede che il polinomio $p(x)$ è irriducibile in $\mathbb{Z}[x]$ applicando il Criterio di Eisenstein (per il primo 3). Dal Lemma di Gauss (e dalla monicità di $p(x)$ segue l'irriducibilità in $\mathbb{Q}[x]$.

(b) Bisogna decidere se le radici complesse di $p(x)$ siano tutte reali oppure no. Le radici reali della derivata $p'(x) = 5x^4 - 9$ sono solo due: $\pm\sqrt[4]{9/5}$. Si deduce facilmente (provate a disegnare il grafico) che le radici reali di $p(x)$ non possono essere più di 3.

In conclusione $\mathbb{K}$ non è contenuto in $\mathbb{R}$.

(c) Il gruppo di Galois G di $\mathbb{K}$ su $\mathbb{Q}$ agisce sulle cinque radici complesse (distinte!) di $p(x)$ permutandole transitivamente. E' quindi (isomorfo a) un sottogruppo del gruppo simmetrico S_5; contiene inoltre un 5-ciclo perché la cardinalità dell'orbita (che è 5) divide sempre l'ordine del gruppo che agisce (qui G) e il Teorema di Cauchy garantisce l'esistenza di un elemento di ordine 5, che non può che essere un 5-ciclo.

Se avete disegnato bene il grafico di $p(x)$, avete visto che possiede esattamente tre radici reali, e quindi due complesse non reali. La coniugazione complessa è un elemento del gruppo di Galois G e agisce trasponendo le sole due radici complesse non reali. Pertanto G contiene anche una trasposizione, che possiamo supporre essere $(1\,2)$ numerando le radici in modo che le prime due siano non reali. Numerando opportunamente le tre radici reali, una potenza del 5-ciclo sarà allora $(1\,2\,3\,4\,5)$ e G è allora un sottogruppo di S_5 che contiene queste due permutazioni. Coniugando $(1\,2)$ con le potenze di $(1\,2\,3\,4\,5)$ si ottiene che G contiene anche $(2\,3)$, $(3\,4)$, $(4\,5)$ e moltiplicando queste trasposizioni tra loro si possono ottenere tutti gli elementi di S_5. In conclusione, G è tutto S_5.

(d) L'estensione $\mathbb{K} \cap \mathbb{R}$ contiene tre delle radici di $p(x)$ (quelle reali!). Se fosse un'estensione di Galois di $\mathbb{Q}$ dovrebbe contenere anche le altre radici di $p(x)$, che sono però non reali. Pertanto l'estensione non è di Galois su $\mathbb{Q}$.

(e) Se H è un sottogruppo del gruppo di Galois $G = Gal(\mathbb{K}/\mathbb{Q})$, allora $[\mathbb{K}^H : \mathbb{Q}] = [G : H]$. Abbiamo visto nel punto precedente che $\mathbb{K} \cap \mathbb{R} = \mathbb{K}^H$ quando H è il sottogruppo di ordine 2 generato dalla coniugazione complessa. Pertanto $|H| = 2$, e poiché $|G| = |S_5| = 120$, si ha $[\mathbb{K}^H : \mathbb{Q}] = 120/2 = 60$.

Risposta:

(a) $p(x) \in \mathbb{Q}[x]$ è irriducibile? **SI** \ **NO**. (b) $\mathbb{K} \subset \mathbb{R}$? **SI** \ **NO**. (c) $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \simeq$ [ ]

(d) $\mathbb{K} \cap \mathbb{R} \,/\, \mathbb{Q}$ è di Galois? **SI** \ **NO**. (e) $\big[(\mathbb{K} \cap \mathbb{R}) : \mathbb{Q}\big] =$ [ ]

Foglio per la brutta copia

Foglio per la brutta copia

Foglio per la brutta copia