ALGEBRA 1 - Secondo esame scritto

16 febbraio 2021

Soluzioni

1. • Calcolare l'inverso di $[27]$ nel gruppo moltiplicativo $\mathbb{Z}/(91)^\times$.
   • Calcolare l'ordine di $[26]$ nel gruppo additivo $\mathbb{Z}/(91)$.

   Soluzione:

   • Innanzitutto, $[27]$ è moltiplicativamente invertibile nell'anello $\mathbb{Z}/(91)$ in quanto $\mathrm{MCD}(27, 91) = 1$, come si vede facilmente osservando che $27 = 3^3$ mentre $91 = 7 \cdot 13$.
   Per trovare l'inverso, si può calcolare l'identità di Bézout con l'algoritmo euclideo. Si ottiene rapidamente

   $$\begin{aligned} 91 &= 3 \cdot 27 + 10 \\ 27 &= 2 \cdot 10 + 7 \\ 10 &= 1 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1, \end{aligned}$$

   da cui, procedendo a ritroso, si ricava

   $$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2(10 - 7) = 3 \cdot 7 - 2 \cdot 10 \\ &= 3(27 - 2 \cdot 10) - 2 \cdot 10 = 3 \cdot 27 - 8 \cdot 10 \\ &= 3 \cdot 27 - 8(91 - 3 \cdot 27) = 27 \cdot 27 - 8 \cdot 91. \end{aligned}$$

   Pertanto $27 \cdot 27 \equiv 1 \mod 91$ e $[27][27] = [1]$ in $\mathbb{Z}/(91)$. L'inverso di $[27]$ è quindi $[27]$ stesso.
   Un metodo alternativo è quello di inviduare l'inverso di 27 modulo 7 e 13 e rimettere tutto insieme col Teorema cinese dei resti. Poiché $27 \equiv -1 \mod 7$ e $27 \equiv 1 \mod 13$, si vede che anche l'inverso di 27 soddisfa le stesse congruenze, e quindi che $[27]$ inverte se stesso.

   • Sappiamo che l'ordine additivo di $[a]$ in $\mathbb{Z}/(n)$ è $n/\mathrm{MCD}(a, n)$. In questo caso si ottiene rapidamente che l'ordine è $91/\mathrm{MCD}(26, 91) = 91/13 = 7$.
   Non ricordando questo fatto, si può procedere osservando che l'ordine additivo di $[26]$ è il minimo k naturale diverso da 0 tale che $26k \equiv 0 \mod 91$. Questa congruenza è equivalente a $2k \equiv 0 \mod 7$ da cui, ricordando che 2 è invertibile modulo 7, si ottiene $k \equiv 0 \mod 7$. Ma allora il minimo valore positivo di k cercato è 7, e quindi l'ordine di $[26]$ è 7.

2. Sia G un gruppo, H un suo sottogruppo e N un sottogruppo normale di G. Mostrare che se N è abeliano e $G = NH$ allora $N \cap H$ è un sottogruppo normale di G.

   Soluzione: L'esercizio si fa anche con le mani, ma possiamo provare a farlo in modo un po' più sofisticato, individuando il normalizzatore di $N \cap H$ in G e mostrando che è tutto il gruppo.

   Innanzitutto, poiché N è abeliano, ogni suo sottogruppo è normale, e quindi N normalizza $N \cap H$. Inoltre, poiché N è normale in G, H normalizza $N \cap H$. Ma allora il normalizzatore di $N \cap H$ in G contiene sia H che N, e quindi contiene i prodotti $NH = G$.

3. Poniamo
$$I = \{f(x) \in \mathbb{Q}[x] \mid f(3) = f(4/5) = f(\sqrt{3}) = 0\}.$$

- Mostrare che I è un ideale di $\mathbb{Q}[x]$.
- Determinare gli ideali massimali di $\mathbb{Q}[x]$ che contengono I.

Soluzione:

- Abbiamo visto a lezione che se $K \subset L$ sono campi e $\alpha \in L$, allora l'applicazione di valutazione
$$E_\alpha : K[x] \ni p(x) \mapsto p(\alpha) \in L$$
è un omomorfismo di anelli, e il suo nucleo è quindi un ideale. Se scegliamo $K = \mathbb{Q}$, $L = \mathbb{C}$, il sottoinsieme I è per definizione l'intersezione $\ker E_3 \cap \ker E_{4/5} \cap \ker E_{\sqrt{3}}$ ed è quindi un ideale in quanto intersezione di ideali. Ovviamente, si può fare anche tutto con le mani, ma ricordate che dovete anche mostrare che I è un sottogruppo additivo!!!
- L'ideale $I \subset \mathbb{Q}[x]$ contiene il prodotto di polinomi irriducibili
$$(x-3)(x-4/5)(x^2-3).$$
Se $M = (q(x))$ è un ideale massimale di $\mathbb{Q}[x]$ che contiene I, allora $q(x)$ è un polinomio irriducibile che divide questo prodotto. Pertanto le uniche possibilità sono $(x-3), (x-4/5), (x^2-3)$, ma va ancora mostrato che questi tre ideali massimali effettivamente contengono I.
Questo è però più o meno immediato, perché tali ideali sono $\ker E_3, \ker_{4/5}, \ker_{\sqrt{3}}$, dei quali I è intersezione!

4. G è un gruppo di ordine $598 = 2 \cdot 13 \cdot 23$ che agisce su un insieme X che possiede 16 elementi.

   - Mostrare che l'azione di G su X ha almeno tre orbite.
   - Mostrare che se l'azione di G su X non ha punti fissi, allora vi sono esattamente 8 orbite.

   Soluzione:

   - Se $x \in X$, sappiamo che la cardinalità dell'orbita $G.x$ coincide con l'indice dello stabilizzatore di x e quindi divide l'ordine di G. Sappiamo inoltre che X è unione disgiunta delle G-orbite. Se X avesse una singola orbita, 16 dovrebbe dividere $|G|$, ma questo non succede. Se ne avesse due, 16 dovrebbe essere somma di due divisori (positivi) di $|G|$ e anche questo non accade. Pertanto l'azione di G su X ha almeno tre orbite. Per la cronaca, questo può effettivamente accadere, in quanto $16 = 1 + 2 + 13$.
   - Se non ci sono orbite costituite da un solo elemento, allora $|X| = 16$ deve essere somma di divisori positivi di 16 diversi da 1, e gli unici tali divisori sono 2 e 13. Tuttavia, sia 16 che 2 sono pari, e quindi in tale somma deve comparire un numero pari di 13. Poiché $2 \cdot 13 = 26 > 16$, 13 non compare affatto, e tutti gli addendi sono uguali a 2. Ma allora abbiamo esattamente 8 addendi, e l'esercizio è concluso.

     Qualche studente ha supposto che *non ha punti fissi* significasse in questo esercizio *è libera*. Però è stato detto esplicitamente durante la prova cosa intendessimo, e inoltre si vede facilmente che gli elementi di G di ordine 23, che esistono per il Teorema di Cauchy, non possono agire su un insieme di cardinalità 16 senza punti fissi. L'azione non poteva quindi essere libera e questo chiariva immediatamente il significato della domanda.

5. Sia $\alpha = \sqrt{5} + i \in \mathbb{C}$.

   - Individuare il polinomio minimo di α su $\mathbb{Q}$.
   - Dimostrare che l'estensione $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ è di Galois.
   - Usando la corrispondenza di Galois, descrivere tutte le sottoestensioni di grado 2 dell'estensione $\mathbb{Q} \subset \mathbb{Q}(\alpha)$.

   Soluzione:

   - Si vede subito che $\alpha^2 = 4 + 2i\sqrt{5}$ e quindi che $(\alpha^2 - 4)^2 = -20$, da cui $\alpha^4 - 8\alpha^2 + 16 + 20 = 0$. L'algebrico α soddisfa quindi il polinomio $x^4 - 8x^2 + 36 \in \mathbb{Q}[x]$, che scopriamo essere il polinomio minimo una volta dimostrata la sua irriducibilità in $\mathbb{Q}[x]$, o anche in $\mathbb{Z}[x]$ grazie al Lemma di Gauss.

     L'irriducibilità può essere ottenuta direttamente o indirettamente. Intanto si vede subito che le radici del polinomio soddisfano $x^2 = 4 \pm \sqrt{-20}$ e quindi non sono razionali. L'eventualità che il polinomio si decomponga nel prodotto di due polinomi di secondo grado si può escludere per forza bruta. Infatti, se $x^4 - 8x^2 + 36 = (x^2 + ax + b)(x^2 - ax + c)$, allora

     $$\begin{cases} b + c - a^2 = -8 \\ a(c - b) = 0 \\ bc = 36. \end{cases}$$

     Se $a = 0$, allora $b + c = -8$ e $bc = 36$. Ma allora b, c soddisfano l'equazione $t^2 + 8t + 36 = 0$, che non ha soluzioni intere (né tantomeno razionali). Se invece $b = c$, allora $b = c = \pm 6$ e si ottiene $a^2 = -4$ oppure -20, che sono entrambe impossibili.

     Se si vuole procedere indirettamente, si vede che $\alpha \in \mathbb{Q}(i, \sqrt{5})$, che, analogamente a quanto fatto più volte a lezione, è un'estensione di $\mathbb{Q}$ di grado 4 della quale conosciamo esplicitamente una $\mathbb{Q}$-base: $1, i, \sqrt{5}, i\sqrt{5}$. Il grado di α divide allora 4 e si vede che $1, \alpha, \alpha^2$ sono $\mathbb{Q}$-linearmente indipendenti; di conseguenza il grado di α è proprio 4 e ogni polinomio di grado 4 che lo annulla ne è il polinomio minimo.

     Un'altra possibilità è notare che se α soddisfacesse un polinomio (diciamo monico senza perdere di generalità) a coefficienti razionali, e quindi reali, di grado 2, le sue radici sarebbero α e $\overline{\alpha} = \sqrt{5} - i$. Ma allora il polinomio sarebbe $x^2 - 2x\sqrt{5} + 6$ che però non ha coefficienti razionali. Pertanto il polinomio minimo su $\mathbb{Q}$ di α non ha grado 2, e quindi α ha grado 4 e $x^4 - 8x^2 + 36$ deve esserne il polinomio minimo.

   - Siamo in caratteristica 0, quindi va mostrata solo la normalità dell'estensione, ovvero il fatto che $\mathbb{Q}(\alpha)$ è il campo di spezzamento su $\mathbb{Q}$ di un polinomio a coefficienti in $\mathbb{Q}$.

     Da un lato, è sufficiente mostrare che $\mathbb{Q}(\alpha)$ contiene le quattro radici del polinomio $x^4 - 8x^2 + 36$. Ma noi queste quattro radici le conosciamo esplicitamente: sono $\pm\alpha, \pm\overline{\alpha}$. Che $\pm\alpha \in \mathbb{Q}(\alpha)$ è chiaro, mentre da $\alpha\overline{\alpha} = 6$ segue $\overline{\alpha} = 6/\alpha$ e quindi $\pm\overline{\alpha} \in \mathbb{Q}(\alpha)$.

     Alternativamente, abbiamo già visto nel punto precedente che $\mathbb{Q}(\alpha) = \mathbb{Q}(i, \sqrt{5})$, che è chiaramente (mostratelo!) il campo di spezzamento di $(x^2 + 1)(x^2 - 5)$.

   - Essendo $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ un'estensione di Galois di grado 4, il suo gruppo di Galois ha ordine 4 e quindi possiede un sottogruppo di indice 2 se è ciclico, o tre sottogruppi di indice due altrimenti. Le sottoestensioni di $\mathbb{Q}(\alpha)$ di grado 2 su $\mathbb{Q}$ sono quindi una oppure tre.

     Però due di tali sottoestensioni si vedono ad occhio: sono $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{5})$. La terza non può che essere $\mathbb{Q}(i\sqrt{5})$. Se volete fare i conti esplicitamente, calcolate l'azione del gruppo di Galois sulla $\mathbb{Q}$-base di $\mathbb{Q}(\alpha) = \mathbb{Q}(i, \sqrt{5})$ trovata nel primo punto.