ALGEBRA 1 - Primo esame scritto

25 gennaio 2021

soluzioni

1. Determinare per quali valori del parametro $a \in \mathbb{Z}$ il sistema di equazioni alle congruenze

$$\begin{cases} 2x \equiv 7 \mod (15)\,, \\ 3ax \equiv 12 \mod (21) \end{cases}$$

ammette soluzioni. Scelto un tale valore di a, calcolare tutte le soluzioni del sistema corrispondente.

Soluzione: La prima congruenza è equivalente a $x \equiv 11 \mod 15$, come si vede facilmente moltiplicando entrambi i membri per l'inverso di 2 modulo 15, che è 8. La seconda congruenza è invece equivalente a $ax \equiv 4 \mod 7$ e possiede soluzioni intere esattamente quando $\mathrm{MCD}(a, 7)$ divide 4, cioè quando a non è un multiplo di 7.

Quando a non è un multiplo di 7, il sistema si compone di una congruenza modulo 15 e di una modulo 7 e ammette sicuramente almeno una soluzione intera per il Teorema cinese dei resti, che ci garantisce l'unicità della soluzione modulo $15 \cdot 7 = 105$.

Per calcolare esplicitamente le soluzioni, indichiamo con b un inverso di a modulo 7. Il sistema da risolvere è

$$\begin{cases} x \equiv 11 \mod 15 \\ x \equiv 4b \mod 7. \end{cases}$$

Dalla prima congruenza, ricaviamo

$$x = 11 + 15k, \tag{1}$$

dove $k \in \mathbb{Z}$. Sostituendo nella seconda, otteniamo $11 + 15k \equiv 4b \mod 7$, cioè $k \equiv 4b - 4 \mod 7$. In altre parole, $k = 4b - 4 + 7t$, che sostituito in (1) fornisce

$$x = 60b - 49 + 105t.$$

Sono soluzioni del sistema dato, quindi, tutti e soli gli interi $x \equiv 60b - 49 \mod 105$.

2.
- Se G è un gruppo semplice di ordine $1365 = 3 \cdot 5 \cdot 7 \cdot 13$, calcolare il numero dei suoi 7-Sylow e dei suoi $13-$Sylow.
- Mostrare che non esistono gruppi semplici di ordine 1365.

Soluzione:

- Il numero dei p-sottogruppi di Sylow di un gruppo finito G è $\equiv 1 \mod p$ e divide $|G|$; inoltre un p-Sylow è normale se e solo se è l'unico del suo ordine. Dal momento che G non è semplice, per ogni p che divide $|G|$ deve esservi più di un p-Sylow.

  Ma allora il numero dei 13-Sylow di G è un numero diverso da 1, che divide $3 \cdot 5 \cdot 7$ ed è $\equiv 1 \mod 13$. Si vede rapidamente che i 13-Sylow sono $105 = 13 \cdot 8 + 1$. Allo stesso modo i 7-Sylow sono necessariamente 15.
- Per quanto visto nel primo punto, G contiene almeno $105 \cdot (13 - 1) = 1260$ elementi di ordine 13 e $15 \cdot (7 - 1) = 90$ elementi di ordine 7. Con un ragionamento analogo, si vede che il numero dei 5-Sylow che G contiene è 21 oppure 91 e quindi in G vi sono almeno $21 \cdot (5 - 1) = 84$ elementi. Abbiamo già contato almeno $1260 + 90 + 84 = 1434$ elementi distinti, che sono troppi per un gruppo di ordine 1365.

3. Ricordiamo che se g è un elemento del gruppo G, l'applicazione $G \ni x \mapsto gxg^{-1} \in G$ è l'*automorfismo interno* di G indotto da g. Gli automorfismi interni formano un sottogruppo $\mathrm{Int}(G)$ del gruppo $\mathrm{Aut}(G)$ costituito da tutti gli automorfismi del gruppo G.

   - Mostrare che $\mathrm{Int}(G) \simeq G/Z(G)$, dove $Z(G)$ è il centro di G.
   - Mostrare che se $\mathrm{Aut}(G)$ è ciclico, allora G è abeliano.

   Soluzione:

   - L'applicazione che associa a ciascun elemento $g \in G$ il corrispondente automorfismo interno $I_g(x) = gxg^{-1}$ è un omomorfismo di gruppi $G \to \mathrm{Aut}(G)$ la cui immagine è $\mathrm{Int}(G)$ e il cui nucleo è $Z(G)$. Pertanto $G/Z(G)$ è isomorfo a $\mathrm{Int}(G)$.
   - Abbiamo visto a lezione che ogni sottogruppo di un gruppo ciclico è ciclico; essendo $\mathrm{Int}(G)$ un sottogruppo di $\mathrm{Aut}(G)$, se $\mathrm{Aut}(G)$ è ciclico, allora $\mathrm{Int}(G)$ è ciclico, così come anche il quoziente $G/Z(G)$ che abbiamo visto essere isomorfo a $\mathrm{Int}(G)$.

     Scegliamo $a \in G$ in modo che $[a]$ sia un generatore ciclico di $G/Z(G)$. Questo vuol dire che ogni elemento di G è della forma $a^n z$, dove $n \in \mathbb{Z}$ e $z \in Z(G)$. In particolare a commuta con tutti gli elementi di G e quindi giace in $Z(G)$. Di conseguenza, $[a] = [1]$ e quindi $G/Z(G)$ è il gruppo banale o, equivalentemente, $G = Z(G)$. In conclusione, G è abeliano.

4. Nell'anello $\mathbb{Z}[i]$ degli interi di Gauss, consideriamo l'ideale $I = (6 + 8i, 8 - i)$.

   - Dire se $\mathbb{Z}[i]/I$ è un dominio d'integrità.
   - Dire se $\mathbb{Z}[i]/I$ è un campo.

Soluzione: L'anello $\mathbb{Z}[i]$ è un dominio a ideali principali e quindi l'ideale I è generato da $\mathrm{MCD}(6 + 8i, 8 - i)$. Questo elemento si calcola facilmente eseguendo l'algoritmo euclideo, e si ottiene:

$$\begin{aligned} 6 + 8i &= (1 + i)(8 - i) - (3 - i) \\ 8 - i &= 2(3 - i) + (2 + i) \\ 3 - i &= (1 - i)(2 + i) + 0, \end{aligned}$$

e possiamo concludere che $I = (2 + i)$. Poiché $2 + i$ è irriducibile in $\mathbb{Z}[i]$ — ha norma euclidea prima! — il quoziente $\mathbb{Z}[i]/I$ è sia un dominio d'integrità che un campo.

5. Il campo F è un'estensione del campo $\mathbb{Q}$ dei numeri razionali e contiene una radice α del polinomio $x^3 - 2x + 6$.

   - Determinare il grado su $\mathbb{Q}$ dell'elemento algebrico $\beta = \alpha^2 + 1 \in F$.
   - Trovare il polinomio minimo di β su $\mathbb{Q}$.
   - Trovare il polinomio minimo di α su $\mathbb{Q}(\beta)$.

Soluzione:

- Il polinomio $x^3 - 2x + 6$ è irriducibile in $\mathbb{Q}[x]$ per il Criterio di Eisenstein ed è pertanto il polinomio minimo di α su $\mathbb{Q}$.
  Poiché α ha polinomio minimo di grado 3 su $\mathbb{Q}$, sappiamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Inoltre $\beta \in \mathbb{Q}(\alpha)$ e quindi $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$. Il grado di β su $\mathbb{Q}$ divide allora 3 e può essere solo 1 oppure 3. Ma se $\beta = \alpha^2 + 1$ fosse razionale, α soddisferebbe un polinomio non nullo di grado 2 su $\mathbb{Q}$, mentre il suo polinomio minimo ha grado 3. Concludiamo che $\beta \notin \mathbb{Q}$ e quindi il grado su $\mathbb{Q}$ di β è 3.
  Questo permette di rispondere immediatamente anche alla terza domanda: poiché le estensioni $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$ hanno lo stesso grado su $\mathbb{Q}$, si ha $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$ e quindi $\alpha \in \mathbb{Q}(\beta)$. Ma allora il polinomio minimo di α su $\mathbb{Q}(\beta)$ è $x - \alpha$.
- Sappiamo che $\alpha^3 = 2\alpha - 6$. Di conseguenza $\alpha^4 = \alpha \cdot \alpha^3 = 2\alpha^2 - 6\alpha$. Le prime potenze di β si calcolano allora facilmente:

$$\begin{aligned}
\beta^0 = 1 &= 1 \\
\beta^1 = \beta &= \alpha^2 + 1 \\
\beta^2 = (\alpha^2+1)^2 &= \alpha^4 + 2\alpha^2 + 1 = 4\alpha^2 - 6\alpha + 1 \\
\beta^3 = \beta \cdot \beta^2 &= (\alpha^2+1)(4\alpha^2 - 6\alpha + 1) = 4\alpha^4 - 6\alpha^3 + 5\alpha^2 - 6\alpha + 1 \\
&= 13\alpha^2 - 42\alpha + 37.
\end{aligned}$$

  Si ricava facilmente $\beta^3 = 7\beta^2 - 15\beta + 45$ e quindi β soddisfa il polinomio $x^3 - 7x^2 + 15x - 45$. Questo **deve** essere il polinomio minimo di β su $\mathbb{Q}$ poiché abbiamo già visto che $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$.

PS: ci sono state soluzioni molto creative in questo esercizio. Qualcuno ha usato

$$(\alpha^2 - 2)\alpha + 6 = 0$$

per dedurre che $(\beta - 3)x + 6$ fosse un polinomio a coefficienti in $\mathbb{Q}(\beta)$ – necessariamente quello minimo!!! – annullato da α e quindi che $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

Nel calcolo del polinomio minimo di β su $\mathbb{Q}$, qualcun altro ha proceduto così: poiché $\alpha(\alpha^2 - 2) = -6$, allora $\alpha(\beta - 3) = -6$. Quadrando entrambi i membri, si ottiene

$$36 = \alpha^2(\beta - 3)^2 = (\beta - 1)(\beta^2 - 6\beta + 9) = \beta^3 - 7\beta^2 + 15\beta - 9,$$

e il calcolo di un polinomio a coefficienti razionali di grado 3 che annulli β è ora immediato.