ALGEBRA 1 - Terzo appello scritto

22 giugno 2021

1. Calcolare l'inverso moltiplicativo, se esiste, di 1357 modulo 5432.

   Soluzione: L'inverso moltiplicativo di a modulo n esiste esattamente quando $\mathrm{MCD}(a, n) = 1$; calcoliamo allora $\mathrm{MCD}(1357, 5432)$ con l'algoritmo euclideo. Si ha:

   $$5432 = 4 \cdot 1357 + 4$$
   $$1357 = 339 \cdot 4 + 1,$$

   e quindi 1357 è effettivamente invertibile. Si ha inoltre $1 = 1357 - 339 \cdot 4$, e sostituendo $5432 - 4 \cdot 1357$ al posto di 4 si ottiene

   $$1 = 1357 - 339(5432 - 4 \cdot 1357) = 1357 \cdot 1357 - 339 \cdot 5432.$$

   Pertanto $1357 \cdot 1357 \equiv 1 \mod 5432$ e $[1357] \in \mathbb{Z}/(5432)$ coincide con il proprio inverso moltiplicativo.

2. Quante sono le permutazioni dispari di ordine 4 contenute in S_6?

   Soluzione: Ricordiamo che l'ordine di una permutazione è il minimo comune multiplo delle lunghezze delle permutazioni cicliche disgiunte di cui è prodotto; una permutazione ha quindi ordine 4 se almeno una di tali permutazioni cicliche ha lunghezza 4 e le altre (non banali) hanno lunghezza 2. Gli elementi di ordine 4 in S_6 sono allora i 4-cicli e i prodotti disgiunti di un 4-ciclo con una trasposizione. Poiché sia le trasposizioni che i 4-cicli sono permutazioni dispari, le permutazioni dispari di ordine 4 in S_6 sono tutti e soli i 4-cicli.

   Il conteggio dei 4-cicli è ora facile: dobbiamo decidere quali elementi compaiono nel 4-ciclo, e vi sono $\binom{6}{4} = 15$ scelte diverse possibili. Una volta scritto per primo l'elemento minimo, gli altri tre possono essere posizionati in $3! = 6$ modi diversi, dando quindi origine a $15 \cdot 6 = 90$ permutazioni diverse.

3. Siano I_1, I_2, P ideali dell'anello commutativo con unità A, e supponiamo che P sia primo. Mostrare che:

   - Se $I_1 \cap I_2 \subset P$, allora $I_1 \subset P$ oppure $I_2 \subset P$;
   - Se A è un dominio a ideali principali, e $(0) \neq P \subset I_1 + I_2$ allora $I_1 + I_2 = A$ oppure $I_1 + I_2 = P$.

   Soluzione:

   - Supponiamo, senza perdere di generalità, che $I_1 \not\subset P$. Allora esiste $x \in I_1$ che non appartiene a P. Per ogni scelta di $y \in I_2$, il prodotto xy appartiene a $I_1 I_2 \subset I_1 \cap I_2 \subset P$ e quindi $x \in P$ oppure $y \in P$ per primalità di P. Ma allora $y \in P$ e quindi $I_2 \subset P$.
   - Un ideale primo non nullo in un dominio a ideali principali è necessariamente massimale, e quindi da $(0) \neq P \subset I_1 + I_2$ segue $I_1 + I_2 = A$ oppure $I_1 + I_2 = P$.

4. Calcolare l'identità di Bézout per gli elementi $2+3i, 3+5i$ in $\mathbb{Z}[i]$.

   Soluzione: Come nel primo esercizio, eseguiamo l'algoritmo euclideo in $\mathbb{Z}[i]$. Ricordate che un modo efficiente di procedere è quello di effettuare la divisione complessa tra i due interi di Gauss e arrotondare il risultato complesso all'intero di Gauss più vicino. Si ottiene:

$$\begin{aligned} 3+5i &= 2\cdot(2+3i) - (1+i) \\ 2+3i &= 2\cdot(1+i) + i, \end{aligned}$$

   e poiché i è invertibile, si ha $\mathrm{MCD}(2+3i, 3+5i) = 1$, o anche i, dal momento che il Massimo Comun Divisore è definito solo a meno di moltiplicazione per invertibili.

   Per il calcolo dell'identità di Bézout si procede come nel primo esercizio, e si ottiene

$$i = (2+3i) - 2(1+i) = (2+3i) + 2((3+5i) - 2(2+3i)) = 2(3+5i) - 3(2+3i).$$

   Se si vuole ottenere 1, basta moltiplicare tutto per $-i$, da cui

$$1 = 3i(2+3i) - 2i(3+5i).$$

5. Calcolare il campo di spezzamento, e la struttura del corrispondente gruppo di Galois, del polinomio $x^4 - x^2 + 1 \in \mathbb{Q}[x]$.

   Soluzione: Il polinomio $x^4 - x^2 + 1 \in \mathbb{Q}[x]$ si spezza sui numeri complessi per il Teorema Fondamentale dell'Algebra, e possiamo quindi descrivere il (o meglio un) suo campo di spezzamento come sottocampo di $\mathbb{C}$.

   Le soluzioni complesse dell'equazione $x^4 - x^2 + 1 = 0$ soddisfano

$$x^2 = \frac{1 \pm \sqrt{-3}}{2} = e^{\pm i\pi/3}$$

   e sono quindi $e^{\pm i\pi/6}, e^{\pm 7i\pi/6}$. Il campo di spezzamento è allora $\mathbb{Q}(e^{\pm i\pi/6}, e^{\pm 7i\pi/6})$ che coincide con $\mathbb{Q}(e^{i\pi/6})$ in quanto tutte le radici sono potenze di $e^{i\pi/6}$ e quindi già contenute in $\mathbb{Q}(e^{i\pi/6})$. In altre parole, il campo di spezzamento di $x^4 - x^2 + 1$ è la dodicesima estensione ciclotomica di $\mathbb{Q}$, anche se non avremo bisogno di questo fatto.

   Il polinomio $x^4 - x^2 + 1$ è comunque irriducibile in $\mathbb{Q}[x]$, come si può vedere in tanti modi. Un possibile modo di procedere (ma ve ne sono di più furbi) è per forza bruta: da

$$x^4 - x^2 + 1 = (x^2 + ax + b)(x^2 - ax + c)$$

   si ottiene

$$\begin{cases} b + c - a^2 = -1 \\ a(c - b) = 0 \\ bc = 1, \end{cases}$$

   di cui vanno cercate le soluzioni intere, per il Lemma di Gauss.

   Da $bc = 1$ si ottiene $b = c = \pm 1$, e la seconda equazione è automaticamente soddisfatta. Sostituendo nella prima, si ottiene $a^2 = 1 \pm 2 = 3$ oppure -1 che non ha soluzioni intere. L'estensione $\mathbb{Q} \subset \mathbb{Q}(e^{i\pi/6})$ ha quindi grado 4, ed è di Galois in quanto campo di spezzamento di un polinomio separabile (siamo in caratteristica zero!!!).

   Indichiamo ora con $\omega = e^{i\pi/6}, \omega^5, \omega^7, \omega^{11}$ le quattro radici di $x^4 - x^2 + 1$. Notiamo che $\omega^7 = \omega^{-5}, \omega^{11} = \omega^{-1}$ in quanto $\omega^{12} = e^{2\pi i} = 1$.

   Il gruppo di Galois $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ possiede $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ elementi, che permutano tra loro le quattro radici e sono determinati dalle possibili immagini di ω, scelte tra le radici del suo polinomio minimo:

   Si ottengono le permutazioni

$$(\omega, \omega^5)(\omega^7, \omega^{11}), \qquad (\omega, \omega^7)(\omega^5, \omega^{11}), \qquad (\omega, \omega^{11})(\omega^5, \omega^7),$$

   oltre naturalmente all'identità. Le permutazioni hanno tutte ordine due e pertanto il gruppo di Galois è un gruppo non ciclico di ordine 4, necessariamente isomorfo a $\mathrm{C}_2 \times \mathrm{C}_2$.