ALGEBRA 1 - Quinto appello scritto

8 settembre 2021

soluzioni

1. Determinare tutte le soluzioni, se esistono, dell'equazione

$$x^{100} + 556x^{66} + 1000x^{10} \equiv 1 \mod 15.$$

Soluzione: Se la congruenza è valida modulo 15, deve essere valida anche modulo 3. Ad ogni modo

$$x^{100} + 556x^{66} + 1000x^{10} \equiv 1 \mod 3$$

non ha alcuna soluzione intera. In effetti, se $x \equiv 0 \mod 3$, il primo membro è anch'esso congruo a 0 modulo 3, e quindi l'equazione non è soddisfatta. Se invece $x \not\equiv 0 \mod 3$, allora $x^2 \equiv 1 \mod 3$ per il Teorema di Eulero. Ma allora $x^{100} \equiv x^{66} \equiv x^{10} \equiv 1 \mod 3$ e il primo membro è congruo a $1 + 556 + 1000 \equiv 0 \mod 3$.

L'equazione data, pertanto, non ammette soluzioni intere.

2. Si descrivano tutti gli ideali dell'anello quoziente $\mathbb{Z}[i]/(13)$ e si spieghi se si tratta di un campo.

   Soluzione: Sappiamo che la fattorizzazione in primi (di Gauss) di 13 è $13 = (3+2i)(3-2i)$. Gli ideali di un anello quoziente A/I sono in corrispondenza biunivoca con gli ideali di A che contengono I. Nel caso in cui A sia un dominio a ideali principali, $(a) \subset (b)$ è equivalente a dire che b divide a.

   Gli ideali di $\mathbb{Z}[i]$ che contengono (13) sono allora $(1), (3+2i), (3-2i), (13)$ e le loro proiezioni al quoziente sono i quattro ideali di $\mathbb{Z}[i]/(13)$. Dal momento che tale anello quoziente è un anello commutativo con unità i cui ideali non sono esclusivamente i due ideali banali, non può trattarsi di un campo.[1]

[1] In effetti, non è nemmeno un dominio d'integrità, in quanto $[3+2i][3-2i] = [0]$.

3. Sia A un dominio a ideali principali e $f : A \to A$ un omomorfismo suriettivo di anelli con unità. Si dimostri che f è allora anche iniettivo.

   Soluzione: Sia $K \subset A$ il nucleo di f. Poiché f è suriettivo, si avrà $A \simeq A/K$. Sappiamo che A è un dominio d'integrità e quindi anche A/K lo è. Equivalentemente K è un ideale primo di A.

   Se $K \neq (0)$, allora l'ideale primo K sarebbe necessariamente massimale e $A/K \simeq A$ sarebbe un campo. Ma ogni omomorfismo tra campi (che mandi 1 in 1) è necessariamente iniettivo, il che contraddice $K \neq (0)$. In conclusione, $K = (0)$ ed f è iniettivo.

4. Sia E il campo di spezzamento sul campo F del polinomio $x^3 - 3 \in F[x]$. Si determini il grado $[E : F]$ quando $F = \mathbb{Q}, \mathbb{F}_5$ rispettivamente.

   Soluzione:

   - Iniziamo con il caso $F = \mathbb{Q}$. Sappiamo già che il campo di spezzamento di un polinomio di grado n è al più $n!$, e quindi $[F : E] \leq 6$.
     Il campo di spezzamento E, visto come sottocampo di $\mathbb{C}$, contiene la radice $\sqrt[3]{3}$ ma anche le altre due radici complesse coniugate

     $$\sqrt[3]{3} \cdot \left(\frac{-1 \pm \sqrt{3}}{2} \right).$$

     Il polinomio $x^3 - 3$ è irriducibile in $\mathbb{Z}[x]$ per il criterio di Eisenstein, e quindi anche in $\mathbb{Q}[x]$ per il Lemma di Gauss, ed è quindi il polinomio minimo di $\sqrt[3]{3}$. Pertanto $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ e quindi $[E : F]$ è un multiplo di 3. Inoltre $\mathbb{Q}(\sqrt[3]{3}) \subsetneq E$ poiché E contiene elementi non reali. Pertanto $[E : F]$ è un multiplo di 3, superiore a 3 e minore o uguale a 6; in conclusione, $[E : F] = 6$.
   - Passiamo ora al caso $F = \mathbb{F}_5$. Si vede subito che il polinomio $x^3 - 3$ ammette la radice 2 in F e si fattorizza quindi come

     $$x^3 - 3 = (x - 2)(x^2 + 2x + 4).$$

     E' facile vedere che il polinomio $x^2 + 2x + 4 \in \mathbb{F}_5[x]$ è irriducibile in quanto di grado due e privo di radici in F. L'estensione E è allora il campo di spezzamento del polinomio $x^2 + 2x + 4$, ed ha pertanto grado 2 su F (dopo aver aggiunto una radice, che ha grado due, si ottiene un'estensione in cui il polinomio si spezza).

5. Determinare quanti siano, a meno di isomorfimo, i gruppi di ordine 91.

   Soluzione: Abbiamo visto durante il corso che se $p < q$ sono numeri primi e p non divide $q - 1$, allora un gruppo di ordine pq è necessariamente abeliano.

   I gruppi di ordine 91 sono quindi tutti abeliani. Per la classificazione dei gruppi abeliani finitamente generati, ogni tale gruppo è isomorfo a C_{91}. In conclusione, vi è un unico gruppo di ordine 91, a meno di isomorfismo.