DOMANDE ORALI DI ARITMETICA

12 giugno 2015

SESSIONE GENNAIO 2015

1. Un polinomio $p \in \mathbb{Z}[x]$ può essere riducibile o irriducibile. Lo stesso polinomio, preso con coefficienti in $\mathbb{Z}/p\mathbb{Z}[x]$ può essere riducibile o irriducibile. Che relazione c'è tra queste due cose?
   (Attenzione se su $\mathbb{Z}/p\mathbb{Z}$ la scoposizione diventa banale)
2. Capire se -1 è residuo quadratico modulo p (**Hint:** si può dare per scontato che esista un generatore)
3. Sia $q \in \mathbb{Z}[x]$ un polinomio irriducible. Si chiede se $\exists p \in \mathbb{P}$ tale che q modulo p è riducibile?
4. G gruppo abeliano finito, $H \lhd G$. Sappiamo che sia H che G/H sono ciclici. Si può dedurre che G è ciclico? Se no, c'è una qualche altra ipotesi che mi permette di dedurlo? (**Hint:** pensare agli ordini di H e G/H)
5. Fai un esempio di due anelli isomorfi come spazi vettoriali ma non come anelli
6. Consideriamo $\sigma : \mathbb{N}^+ \to \mathbb{N}^+$ definita come $\sigma(n) = \sum_{d|n} d$. Dimostrarne la moltiplicatività, ovvero che $\sigma(mn) = \sigma(m) \cdot \sigma(n) \quad$ se $(n,m) = 1$
7. Si consideri in $\mathcal{M}(\mathbb{K}, n, n)$ l'insieme delle matrici quadrate invertibili di ordine n a coefficienti nel campo $\mathbb{K}$. Dimostrare che è un gruppo.
   Consideriamo $\mathcal{M}(\mathbb{F}_{11}, 2, 2)$. Non è un gruppo abeliano ma mostriamo che esiste un sottogruppo normale. (**Hint:** prendiamo l'insieme delle matrici il cui determinante $\dots$)
   Sappiamo che ogni sottogruppo normale di un gruppo è $\mathcal{K}$er di un omomorfismo. Sai trovare un omomorfismo $\varphi : \mathcal{M}(\mathbb{F}_{11}, 2, 2) \to \mathbb{F}_{11}$ che abbia come $\mathcal{K}$er il sottogruppo delle matrici con determinante che è un quadrato in $\mathbb{F}_{11}$?
8. Quanti sono i polinomi irriducibili di grado n su $\mathbb{F}_p$? (**Hint:** può essere utile provare prima il caso dei polinomi di secondo grado. **Hint:** in alternativa si possono contare i polinomi riducibili.) **Hint:** Altrimenti dimostrate che
$$\prod_{\substack{p(x) \text{ irriducibile} \\ \deg(p(x)) \mid n}} p(x) = x^{p^n} - x$$
9. Sia $G = \langle x_1, x_2 \rangle$ un gruppo e $H < G$ un sottogruppo. È vero che anche H è generato da al più due elementi? Se è falso trovare un controesempio. (Provare prima il caso $H \lhd G$, poi il caso generale) (**Hint:** una volta è vero, l'altra è falso)
10. Descrivere i sottogruppi di $G = \mathbb{Z}_{10} \times \mathbb{Z}_5$ e contare i sottogruppi $H \lhd V$ tali che $\mid H \mid = 1000$ e $V = \mathbb{Z}_{1000} \times \mathbb{Z}_{500}$. E quanti sono i sottogruppi $H \lhd V$ tali che $\mid H \mid = 5$?

11. Considera l'insieme $W = \{p(x) \in \mathbb{Z}_5[x]\}$. Ogni polinomio $p \in W$ lo posso vedere come funzione $f_p : \mathbb{Z}_5 \to \mathbb{Z}_5$ associando ad ogni polinomio la funzione valutazione sui suoi elementi.
Esistono polinomi distinti la cui funzione associata è la stessa?
Sia φ l'omomorfismo che ad un polinomio associa la sua funzione polinomiale in $\mathbb{Z}/p\mathbb{Z}$. Qual'è il $\mathcal{K}$er di questa funzione? E l'immagine di φ quanti elementi ha?

12. Siano $\alpha, \boldsymbol{\eta}$ algebrici su $\mathbb{Q}$ tali che $\deg(\alpha) = m$ e $\deg(\boldsymbol{\eta}) = n$. Quali sono i possibili valori per $\deg(\alpha + \boldsymbol{\eta})$? Qual è il minimo $\deg(\alpha + \boldsymbol{\eta})$ fissati m ed n?

13. $(\mathbb{Q}, +)$ è ciclico? Quanti generatori ha?
(**Hint:** considera le frazioni con numeratore uno e denominatore potenza di un primo) Dimostra che quelli che hai trovato generano.

14. Sia $H < G$, con G gruppo ciclico finito. Dimostra che anche H è ciclico. Vale anche nel caso $\mid G \mid = +\infty$?

15. $\forall n \in \mathbb{N}$ sia $z_n = e^{i\frac{2\pi}{n}}$. Che cosa ottengo se aggiungo z_n a $\mathbb{Q}$? E se aggiungo z_n e z_m con $m \neq n$?
Calcola il grado dell'estensione di campo $[\mathbb{Q}(z_n, z_m) : \mathbb{Q}]$ (**Hint:** $[\mathbb{Q}(z_n) : \mathbb{Q}] = \varphi(n)$)
Dimostra che se ho $(n,m) = 1$ allora $\mathbb{Q}(z_{nm}) = \mathbb{Q}(z_n, z_m)$.
Dimostra che $\sum_{j=0}^{p-1} x^j$ è irriducibile su $\mathbb{Q}[x]$.

16. Trova un $\mathbb{Z}/n\mathbb{Z}[x]$ in cui esiste un polinomio $p(x)$ tale che $\exists k \in \mathbb{N} \quad p^k = 0$. Esistono polinomi invertibili in $\mathbb{Z}/6\mathbb{Z}[x]$?
Sia $p(x) = \sum_{i=0}^{n} a_i x^i$ t.c. $\exists k \in \mathbb{N} \quad p^k = 0$. Dimostra che allora a_i è nilpotente $\forall 0 \geq i \leq n$

17. Sia $f(x) = x^{14} + 2 \in \mathbb{F}_{13}[x]$. Trovane il campo di spezzamento.

18. Sia $G = (\mathbb{Z}/m\mathbb{Z})^*$ un gruppo e $f : G \to G$ definita come $f(x) = x^5$ una funzione. È un morfismo? Quando è iniettiva e quando e suriettiva (al variare di m)?
Mostra che $\mathcal{K}\text{er}\varphi \simeq \underbrace{\mathbb{Z}_5 \times \mathbb{Z}_5 \times \ldots \times \mathbb{Z}_5}_{\text{un po' di volte}}$.
Trova un G tale che $\mathcal{K}\text{er}\varphi \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$.

19. Dimostrare che $\forall p \in \mathbb{P} \qquad x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Q}[x]$ è irriducibile. Dimostra che $f(x)$ è irriducibile in $\mathbb{Q} \Leftrightarrow f(x + a)$ è irriducibile, con $a \in \mathbb{Q}$
Per quali $n \in \mathbb{N}$ si ha $x^n + x^{n-1} + \ldots + x + 1$ irriducibile?

20. Quand'è che esiste $(3x + 5)^{-1}$ in $\mathbb{Z}_{100}$? (con x parametro).
So che $x^2 \equiv a \quad (p)$. Quando $\exists y$ t.c. $y^2 \equiv (p^2)$?
(**Hint:** provare $y = x + bp$)
$\sqrt{2} + \sqrt{3} + \sqrt{5}$ è algebrico sui razionali? Trova un polinomio su cui si annulla e trova una base di $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$
Sia $\mathbb{K}$ un campo che contiene $\mathbb{Q}$. Quando $\mathbb{K}(\sqrt{a}) = \mathbb{K}(\sqrt{b})$?