DOMANDE DEGLI ORALI DI ALGEBRA 1

2 febbraio 2016

PREAPPELLO DI GENNAIO 2016

- Restiamo negli anelli commutativi unitari. Ce ne sono che hanno un numero finito di ideali massimali? Fai un po' di esempi. Posso trovare un anello che abbia m ideali massimali $\forall m \in \mathbb{N}$?
- Supponiamo ora di avere A un UFD e supponiamo che $\mid A \mid = +\infty$ e supponiamo che A^* sia finito. Dimostra che allora A contiene infiniti elementi primi. (Poi ci accontentiamo anche di Char $A = 0$ ma ci assicura che si fa anche in caratteristica p)
- Conosci un gruppo finito che abbia esattamente due sottogruppi di indice due? (Suggerimento: I commutatori) Quanti possono essere i sottogruppi di indice due di un gruppo finito, ovvero quali numeri si realizzano?
- Prendo i polinomi a coefficienti interi in infinite variabili $\mathbb{Z}[(x_\lambda)_{\lambda\in\Lambda}]$. Questo è un UFD?
  Ora al posto di infinite variabili mettiamo infiniti esponenti (razionali) $B = \cup_{n\geq 0}\mathbb{Z}[x^{\frac{1}{n}}]$. B è un UFD? (Suggerimento: ACCP non soddisfatta)
- G gruppo che non ha sottogruppi normali di indice finito. Sia $N \lhd G$ e N di ordine finito. Mostrare che $N \sqsubseteq Z(G)$ (Cioè N è sottogruppo del centro) (Suggerimento: Azioni furbe?)
- Consideriamo $\mathbb{Q} \subseteq K_1, \ldots, K_n$ estensioni distinte dei razionali tutte di grado tre su $\mathbb{Q}$. Se $n = 2$ quali sono i possibili gradi del composto K_1K_2? Voglio ora determinare il minimo n tale che, per ogni scelta di $K_1, \ldots, K_n$ si abbia $9 \mid [K_1 \ldots K_n : \mathbb{Q}]$
- Parliamo di p-gruppi. $\mid G \mid = p^3$, G non abeliano. Che dimensione ha il centro? Quante sono le classi di coniugio?
- Enuncia e dimostra il teorema di Cayley. $\mid G \mid = n$. Supponiamo ora $n = 2d$ con d dispari. Mostrare che G possiede un sottogruppo di ordine d. Supponiamo ora che d sia squarefree, quindi $\mid G \mid = 2p_1 \cdot \ldots \cdot p_k$ con i p_i tutti distinti. Quanti gruppi G di quest'ordine ci sono? (Quanti sono se $H \sqsubseteq G, \mid H \mid = d$, H è ciclico?)
- Prendiamo $p = 13$ un primo e consideriamo $\mathbb{Q}(\zeta_p)$. Quante sottoestensioni su $\mathbb{Q}$ di grado 2 ci sono? Dato un sottogruppo di indice m di $C_p^* \equiv$ Gal $(\frac{\mathbb{Q}(\zeta_p)}{\mathbb{Q}})$ vorrei trovare un sottocampo di grado m su $\mathbb{Q}$, espresso come $F = \mathbb{Q}(\alpha)$. Dimostrare che è proprio lui ciò che cerchiamo.
- Prendo p, q primi distinti e vorrei dire che ogni gruppo di ordine p^2q si scrive come prodotto semidiretto
- Prendo $\mathbb{Z}$ e vorrei trovare due sottoinsiemi moltiplicativamente chiusi distinti S_1, S_2 di $\mathbb{Z}$ tali che $S_1^{-1}\mathbb{Z} \equiv S_2^{-1}\mathbb{Z}$

- Prendo un ideale in $A = \mathbb{Z}[x]$. è vero che se non è massimale possono non bastare solo due generatori (al contrario di come invece avviene per quelli massimali)? (Riportiamo la soluzione integrale: Vero, notiamo che per $I = (4, 2x, x^2) = ((2, x))^2$ e $(2, x) = M$ è un ideale massimale. Quindi $\frac{M}{M^2}$ è uno spazio vettoriale di dimensione 2 su $\frac{A}{M}$, che è un campo. Se prendo invece $\frac{M^2}{M^3}$ e controllo che ha dimensione 3 concludo, perché il quoziente ha tre generatori quindi anche M^2 deve averne almeno tre.)
- Sia G un p-gruppo. $\mid G \mid = p^n$ e supponiamo che sia abeliano. Mostra che il numero di sottogruppi di ordine p è congruo a 1 modulo p. Vedere che ciò avviene anche per G non abeliano e per sottogruppi di ogni ordine.
- Consideriamo l'estensione ciclotomica $K = \mathbb{Q}(\zeta_p)$, con p primo diverso da due. Esso avrà quindi un'unica sottoestensione (su $\mathbb{Q}$) di grado 2 ed un'unica di grado $\frac{p-1}{2}$. Un'estensione quadratica di $\mathbb{Q}$ si può sempre esprimere come $\mathbb{Q}(\sqrt{a})$. Al variare di p stabilire se a è positivo o negativo.
- Com'è fatto un 2-Sylow di $S7$? (Suggerimento piccolissimo: 7 in base due si scrive come $1 * 2^2 + 1 * 2^1 + 1 * 2^0$)

SESSIONE DI FINE GENNAIO 2016

- Trova un esempio di anello commutativo unitario A nel quale esiste una catena ascendente infinita e non stazionaria di ideali $I_1 \subsetneq I_2 \subsetneq \dots$
- G gruppo finito e $H \sqsubseteq G$ un sottogruppo che interseca ogni classe di coniugio. Ovvero $\forall x \in G \exists g \in G \quad$ t.c. $gxg^{-1} \in H$. Dimostrare allora che $H = G$. (Suggerimenti: Considerare l'azione di coniugio di G sui sottogruppi coniugati di H e dimostrare che H è normale)
- Costruisci un'estensione di Galois con gruppo di Galois D_5 (puoi scegliere tu i campi)
- Come sono fatti i 2-Sylow ed i 3-Sylow di S_9. Che gruppi sono?
- L'unione di tre sottogruppi propri (tali che nessuno sia contenuto in qualcun'altro) può essere un sottogruppo? Se $G = C_p \times C_p$ si può fare (esistono tre sottogruppi tali che)? Qual è il minimo numero di sottogruppi propri tali che la loro unione sia tutto $C_p \times C_p$?
- A dominio euclideo. $B \subset A$ è un sottoanello (unitario). è vero o no che B è a sua volta un dominio euclideo? (Con una qualunque funzione grado)
- Prendiamo il campo di spezzamento di un polinomio di terzo grado su $\mathbb{Q}$. Quali radici dell'unità può contenere? (Ovvero ζ_n per quali n). E se prendiamo un polinomio di grado quattro? (Suggerimento: usando corrispondenza di Galois deve essere che il gruppo Gal $(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ si ottiene come quoziente di S_4)
- Supponiamo che G sia generato da n elementi $\langle x_1, x_2, \dots, x_n \rangle$. $H \sqsubseteq G$. Esistono per forza $\geq n$ elementi che generano H? E se G è abeliano finito?
- Ci sono anelli c.u. A tali che $(A^*, \cdot) \cong (\mathbb{Z}, +)$ come gruppo? (Suggerimento: $(\mathbb{Z}, +)$ ha solo elementi di ordine infinito. Può essere che $\mathbb{Z}_m$ si immerga in A (come sottoanello)? Che ordine ha $\{-1\}$? Se esiste deve avere $\mathbb{Z}_2$ come sottoanello fondamentale. A

questo punto posso considerare $S = \{1, x, x^2, \ldots\}$ e $B = \mathbb{F}_2[x]$ allora $A = S^{-1}B$ è un anello cercato.

- Classificare i gruppi di ordine $3 \cdot 5 \cdot 7$. Chi sono i sottogruppi normali di $\mathbb{Z}_{35} \rtimes_\phi \mathbb{Z}_3$?

- Considera $\mathbb{K}[x, y]$, per fissare le idee consideriamo $\mathbb{K} = \mathbb{Q}$. $I = (x^2y - 1)$ è primo? massimale? (Suggerimento: $A = \mathbb{Q}[x]$, $x^2y - 1 \in A[y]$ è di primo grado in y)

- $\mathbb{K}$ su $\mathbb{Q}$ estensione di Galois. $[\mathbb{K} : \mathbb{Q}] = n$. Quanti sono i morfismi di campi $\sigma : \mathbb{K} \to \mathbb{C}$? Devo aggiungere l'ipotesi $\sigma \mid_{\mathbb{Q}} \cong \text{id}$? Distinguo due categorie: $\sigma(\mathbb{K}) \subseteq \mathbb{R}$, $\sigma(\mathbb{K}) \subsetneq \mathbb{R}$. Possono esistere morfismi di entrambi i tipi? E se $\mathbb{K}$ su $\mathbb{Q}$ non è di Galois? Quanti sono i morfismi di immersione in $\mathbb{C}$ in questo caso?
  Inoltre è vero che se $\exists \sigma$ t.c. $\sigma(\mathbb{K}) \subseteq \mathbb{R}$ allora si ha che $\forall \sigma \quad \sigma(\mathbb{K}) \subseteq \mathbb{R}$? E è vero che se $\exists \sigma$ t.c. $\sigma(\mathbb{K}) \subsetneq \mathbb{R}$ allora $\forall \sigma \quad \sigma(\mathbb{K}) \subsetneq \mathbb{R}$? E se $\mathbb{K}$ su $\mathbb{Q}$ è di Galois?

- $\mathbb{K}[x^m, x^n]$, dove $\mathbb{K}$ è un campo, è un sottoanello di $\mathbb{K}[x]$. Che proprietà ha? É UFD, è PID?

- $\mid G \mid = p^n m$ e sia $P \sqsubseteq G$ con $\mid P \mid = p^n$ (un p-Sylow). Dimostra che $\mathrm{N}_G(P) = \mathrm{N}_G(\mathrm{N}_G(P))$

- $G = \frac{\mathbb{Z}}{p^\alpha \mathbb{Z}} \times \frac{\mathbb{Z}}{p^\beta \mathbb{Z}}$, cercane i sottogruppi massimali.

- A anello c.u. e siano $P, Q \subseteq A$ due ideali primi di A. $P \cap Q$ è un ideale primo?

- Che relazione c'è tra $\sqrt{I} + \sqrt{J}$ e $\sqrt{I + J}$? E con $\sqrt{\sqrt{I} + \sqrt{J}}$?

- Qual'è la classe di coniugio di $\sigma = (12345)$ dentro ad A_6?

- $[G : H] = p$, $H \sqsubseteq G$. Quali condizioni devo avere su p affinchè $H \lhd G$? Dimostra che se p è il più piccolo primo che divide l'ordine di G allora H è normale in G.

- $H \sqsubseteq S_n$. Può avere indice piccolo? (Suggerimento: usare il teorema dell'indice fattoriale. Risultato: può avere indice 2 (A_n), ma non può avere indice $3, 4, \ldots, n-1$) Sottogruppi di indice n ce ne sono? (Sì, ad esempio considero le permutazioni di S_n che lasciano fisso un numero $i \in \{1, \ldots, n\}$. Queste sono un sottogruppo isomorfo ad S_{n-1} e di questi sottogruppi ne trovo n). Sono tutti coniugati fra loro (i sottogruppi $\cong S_{n-1}$)?
  Supponiamo che G agisca su X e sia $x \in X$ ($\phi : G \to S(X)$). Quando è vero che $\phi_g(x) = \phi_h(x)$? (Suggerimento: centrano le classi laterali dello stabilizzatore)

- Consideriamo $\mathbb{C}$ e sia K un campo che contiene $\mathbb{C}$. Considero la dimensione di K come $\mathbb{C}$-spazio vettoriale. Quale può essere questa dimensione? Può essere finita? Può essere numerabile? (Suggerimento per quella numerabile: se $\exists x \in K \setminus \mathbb{C}$ allora $\mathbb{C}(x) \subseteq K$, ma allora basta mostrare che $\mathbb{C}(x)$ ha elementi linearmente indipendenti su $\mathbb{C}$ in cardinalità del continuo)

- Facciamo una leggera modifica all'azione di coniugio nei gruppi: $H \subseteq G$. Definiamo la seguente relazione tra elementi di G: $g \sim g' \Leftrightarrow \exists h \in H \quad hgh^{-1} = g'$. Verifica che è una relazione di equivalenza. C'è qualche relazione tra le classi di equivalenza di questa azione e quella di coniugio classica? (Suggerimento: le nuove orbite sono una partizione di quelle vecchie). Vale la divisibilità tra le cardinalità delle orbite nuove e di quelle vecchie? (Suggerimento: mostrare che se H è normale allora vale e trovare un controesempio in generale)

- Esiste un'estensione di campi $K \subseteq F$ che sia di Galois e tale che Gal $\left(\frac{F}{K}\right) \cong \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$? (Trucco: ogni estensione abeliana di $\mathbb{Q}$ sta dentro ad una estensione con le radici dell'unità. Quindi sapendo che se $n = \prod_i p_i^{e_i}$ si ha $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* = \times_i \left(\frac{\mathbb{Z}}{p_i^{e_i}\mathbb{Z}}\right)^* \cong \times_i \frac{\mathbb{Z}}{p_i^{e_i-1}(p_i-1)\mathbb{Z}}$ (Attenzione però a $p = 2$). Quindi basta trovarsi due primi congrui a 1 modulo 5 (ad esempio 11 e 31) e sappiamo che Gal $\left(\frac{\mathbb{Q}(\zeta_1 1,\zeta_3 1)}{\mathbb{Q}}\right)$ è un gruppo abeliano che ha due fattori $\frac{\mathbb{Z}}{5\mathbb{Z}}$ nella sua fattorizzazione. Quindi siccome sappiamo che i gruppi abeliani hanno sottogruppi di ogni ordine lecito sappiamo che esiste un campo fissato da questo sottogruppo e così troviamo l'estensione di campi cercata. Oppure potremmo anche ottenerla come quoziente di questa (in modo da avere un campo su $\mathbb{Q}$ e non su una estensione di $\mathbb{Q}$))
- A anello c.u. e considero $\ldots \subseteq P_2 \subseteq P_1$ catena di ideali primi discendente. Considero $I = \cap_i P_i$. I è un ideale primo?
- $G = H \rtimes_\phi K$. Vorrei sapere chi sono gli elementi nel centro di G.
- G gruppo abeliano finito. $\mid G \mid = n$ e sia $d \mid n$. $X = \{x \in G \mid dx = 0\}$. Dire che X è un sottogruppo. Qual è la cardinalità di X? Mostra che $d \mid\mid X \mid$.
- Quali sono i gruppi ciclici della forma $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$? (Va dimostrato che $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^*$ è ciclico)
- A anello c.u. tale che $\forall x \in A \quad x^2 = x$. Che caratteristica ha? (Può avere caratteristica arbitraria?) Che cardinalità può avere se è finito? (Suggerimento: è uno spazio vettoriale su ...) Supponiamo ora $P \subseteq A$ ideale primo, ma A non necessariamente di cardinalità finita. Allora che cardinalità può avere $\frac{A}{P}$ (dimostra che è finito e che ha cardinalità 2).