TRUCCHI DI ALGEBRA 1

13 aprile 2016

Abbiamo cercato di raccogliere tutti i trucchi che ci è capitato di vedere più di una volta negli esercizi dei compiti d'esame di Algebra 1 e ne abbiamo fatto uno studio sistematico ed un po' più approfondito siccome al corso spiegano solo la teoria, mentre per fare gli esercizi serve una serie infinita di trucchetti vari.

GRUPPI

TEOREMA DI SYLOW ESPANSO

Versione "potenziata" del teorema di Sylow, con tutte le conseguenze che esso ha:

-

LEMMA DEL PIÙ PICCOLO PRIMO

Se $H \sqsubseteq G$, con G finito, è tale che $[G : H] = p$, dove p è il più piccolo primo che compare nella fattorizzazione di $\mid G \mid$ allora H è normale in G (basta usare il teorema dell'indice fattoriale e notare che il sottogruppo normale che ci restituisce è proprio H)

CONTEGGIO NUMERO DI SOTTOGRUPPI CICLICI

Supponiamo di contare il numero di sottogruppi ciclici di ordine n del gruppo G. Basterà allora contare il numero di elementi di ordine n in G (solitamente molto più agevole) e poi dividere questo numero per $\phi(n)$ (dove la ϕ è quella di Eulero): infatti siamo interessati al numero di sottogruppi, ciascuno dei quali ha esattamente $\phi(n)$ generatori.

CONTEGGIO NUMERO DI SOTTOGRUPPI ISOMORFI A $\mathbb{Z}_p \times \mathbb{Z}_p$

PARTICOLARI SOTTOGRUPPI CARATTERISTICI (IN UN ABELIANO)

Ricordiamo che nei gruppi abeliani l'elevamento a potenza è un morfismo: $\phi_k : G \to G$ definito da $\phi_k(g) = g^k$. Allora in particolare si può osservare che, $\forall k$, Ker ϕ_k e $\Im\phi_k$ sono sottogruppi caratteristici, sono infatti rispettivamente tutti gli elementi ad avere ordine divisore di k e tutti gli elementi ad ottenersi come potenza k-esima di un qualche elemento in G

MODI PER DIRE CHE UN SOTTOGRUPPO È CARATTERISTICO

Per dire che un certo sottogruppo è caratteristico va caratterizzato in maniera quasi letteraria, con espressioni astratte di cui diamo qualche esempio (conta molto la fantasia):

- É il generato da tutti gli elementi di ordine due.
- É il normalizzatore del generato da tutti gli elementi di ordine quattro e cinque.
- É il centro del sottogruppo dei commutatori.
- É il più grande sottogruppo ad avere intersezione banale con il sottogruppo generato dagli elementi di ordine tre.

Trucchi per gruppi semplici

Dualità ordine-indice per i gruppi abeliani

Centralizzatore e Normalizzatore in S_n ed in A_n

Immersioni minime in S_n ed A_n

Equazione $\sigma^k = \tau$ in S_n

p-Sylow di S_n

Scriviamo n in base p: $n = k_0 + k_1 p + k_2 p^2 + \ldots + k_r p^r$. Allora i p-Sylow di S_n (Li indichiamo con $Q_{p,n}$) sono isomorfi a

$$Q_{p,n} \cong \underbrace{Q_{p,p} \times \ldots \times Q_{p,p}}_{k_1 \text{volte}} \times \underbrace{Q_{p,p^2} \times \ldots \times Q_{p,p^2}}_{k_2 \text{volte}} \times \ldots \times \underbrace{Q_{p,p^r} \times \ldots \times Q_{p,p^r}}_{k_r \text{volte}}$$

Questo si vede abbastanza bene appena si capisce come sono fatti quelli di S_{p^k}: In pratica sono costituiti da tutti i p-cicli disgiunti possibili, uniti a p a p con un'altra azione di scambio tra di loro. [DA INSERIRE DISEGNO DEI P-SYLOW] Per mostrare che sono effettivamente fatti così, si calcola la cardinalità di questi sottogruppi di S_n e si nota che è uguale a quella attesa da un p-Sylow di S_n

Lemmi noti sui p-gruppi

Sia P un p-gruppo, ovvero $\mid P \mid = p^k$. Allora si ha:

- P ha centro non banale, ovvero $Z(P) \neq (e)$
- P contiene almeno un sottogruppo di ogni ordine possibile e contiene almeno un sottogruppo normale di ogni ordine possibile
- Se ho $H \lhd P$ allora $H \cap Z(P) \neq (e)$, ovvero ogni sottogruppo normale interseca il centro in maniera non banale

Numero di sottogruppi (normali e non) di un p-gruppo

Automorfismi di $\mathbb{Z}_{p^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p^{\alpha_n}}$

Centro di un prodotto diretto e semidiretto

Siano H, K due gruppi finiti e $G = H \times K$ allora $Z(G) = Z(H) \times Z(K)$ (segue banalmente impostando il conto).
Se invece $G = H \rtimes_\phi K$ allora [INSERIRE FORMULA PER IL CENTRO]

Quozientare $H \rtimes_\phi K$ per H

Esempio: Siano p un numero primo, $\phi : \mathbb{Z}_{p-1} \to \text{Aut}\, \mathbb{Z}_p$ un omomorfismo iniettivo, $G = \mathbb{Z}_p \rtimes_\phi \mathbb{Z}_{p-1}$ e d un divisore di $p-1$. Dimostrare allora che ogni sottogruppo di G di ordine d è ciclico e che, se H e K sono due sottogruppi distinti di G di ordine d, allora $H \cap K = \{e\}$

p-Sylow di gruppi abeliani

Se G è un gruppo abeliano finito, ricordiamo che i p-Sylow esistono e sono unici (perché essendo sottogruppi sono normali) e sono tali che, detto $G_p = \{x \in G \mid \text{Ord}\,(x) = p^k\}$ allora si ha $G = \prod_{p \in \mathbb{P}} G_p$.
Inoltre se $H \sqsubseteq G$ allora, definiti H_p come sopra si ha $H = \prod_{p \in \mathbb{P}} H_p$ e inoltre $H_p \sqsubseteq G_p$.

FORMULA DELLE CARDINALITÀ DI HK

Utile in molti contesti:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

dove per HK si intende il sottoinsieme (in generale non è un sottogruppo) $HK := \{hk \mid h \in H, k \in K\}$

SOTTOGRUPPI DI INDICE k IN S_n

Per $k \neq 2$, $n \geq 5$ e $k < n$ non ci sono sottogruppi di questo indice (corollario dell'indice fattoriale e poi usare che A_n è l'unico sottogruppo normale), mentre per $k = n$ tutti i sottogruppi di indice n sono isomorfi a S_{n-1} (basta considerare l'azione di traslazione sulle loro classi laterali)

ANELLI

CONTEGGIO DI ZERO-DIVISORI, INVERTIBILI E NILPOTENTI IN UN ANELLO POLINOMIALE QUOZIENTE

FATTI SUGLI INTERI DI GAUSS

VERSIONE POTENZIATA DI EISENSTEIN

Sia $f(x) \in A[x]$ un polinomio. Allora sia $P \subseteq A$ un ideale primo di A. Se scrivendo $f(x) = \sum_i a_i x^i$ si ha che $a_0, a_1, \ldots, a_{n-1} \in P$ e $a_n \notin P$ e $a_0 \notin P^2$ allora ogni fattorizzazione di f in $A[x]$ è tale che uno dei due polinomi è una costante.
Supponiamo infatti che si scriva $f(x) = g(x)h(x)$. Riduciamo allora tutti i coefficienti di f, g, h modulo P ed otteniamo $\bar{f}(x) = \bar{g}(x)\bar{h}(x) \in \frac{A}{P}[x]$. Notiamo che deg $\bar{f} =$ deg f poiché $a_n \notin P$. Inoltre ora si deve avere che $\bar{f}(x) = \bar{a_n}x^n$. Ma $\bar{g}$ e $\bar{h}$ adesso devono essere entrambi della forma λx^k e μx^h (basta immergere $\frac{A}{P}$ nel suo campo delle frazioni e sappiamo che $K[x]$ è UFD). Quindi se $h, k > 0$ allora abbiamo vinto perché otterremmo che $a_0 \in P^2$, altrimenti otteniamo che uno dei due è semplicemente una costante.

INVERTIBILI DI $S^{-1}A$ E PROPRIETÀ DI $S^{-1}A$

(Dovrebbe starci scritto quando è che è un PID, etc.)

IDEALE DI JACOBSON E NILRADICALE

POSSIBILE GRADO SU $\mathbb{Z}[\gamma]$ CON γ DI SECONDO GRADO

Ad esempio $\mathbb{Z}[\frac{1+i\sqrt{7}}{2}]$ è un anello euclideo con il grado dato da $d(m+n\gamma) = m^2 + mn + 2n^2$

TEOREMA CINESE

Riportiamo l'enunciato solo perché spesso ce ne si dimentica ed in alcuni esercizi invece è l'unico modo per risolverli. Siano $I, J \subseteq A$ due ideali. Se $I + J = A$ allora $\frac{A}{IJ} \cong \frac{A}{I \cap J} \cong \frac{A}{I} \times \frac{A}{J}$

Ideali primi di $\mathbb{Z}[x]$

Campi

Sottoestensioni quadratiche di $\mathbb{Q}(\zeta_m)$

Polinomi di gradi 2, 3 e 4 biquadratici

Confronto tra estensioni quadratiche

$K(\alpha), K(\beta)$ due estensioni quadratiche di K. Allora $K(\alpha) = K(\beta) \Leftrightarrow \alpha\beta \in K^2$. [DIMOSTRAZIONE DA METTERE]

Estensioni quadratiche sono sempre normali

Sia L su K un'estensione di grado due. Allora si prenda $\alpha \in L \setminus K$ è tale che $L = K(\alpha)$. Quindi si prenda il polinomio minimo di α su K: $\mu(x) = (x-\alpha)(x-\beta) = x^2 + rx + s$. Allora per le formule di Viète si ha $\alpha\beta = s \in K$ e quindi ogni estensione di K che contiene α deve contenere anche β.

Galois del Campo di spezzamento di $x^n - a$ su $\mathbb{Q}$

Il campo di spezzamento di $x^n - a$ è ovviamente $L = \mathbb{Q}(\sqrt[n]{a}, \zeta_n)$, che è il composto di $E = \mathbb{Q}(\sqrt[n]{a})$ e $F = \mathbb{Q}(\zeta_n)$ e quindi si ha Gal $(L/\mathbb{Q}) \hookrightarrow$ Gal $(L/E) \rtimes$Gal (L/F) tramite la funzione $\sigma \mapsto (\sigma\mid_E, \sigma\mid_F)$. Quindi supponiamo di sapere chi è il campo $K = \mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n)$ (problema che viene comunque risolto in questo file perché trattiamo il problema di quali sono le sottoestensioni di entrambi). Allora Gal $(L/E) \cong$ Gal (F/K) per teoria generale e Gal (F/K) è noto per la teoria delle estensioni ciclotomiche. [DA FINIRE]

Campo di spezzamento di $x^n - a$ su $\mathbb{F}_p$

$\sqrt[n]{b} \in \mathbb{Q}(\sqrt[n]{a})$?

Fattorizzazione di un irriducibile in un'estensione normale

Sia f irriducibile in $K[x]$ e sia L/K normale. Allora $f = f_1 \cdot \ldots \cdot f_r$ con f_i irriducibile in $L[x]$. Allora deg $f_i =$ deg f_j. Infatti presi gli automorfismi $\sigma_k \in$ Aut $_K(L)$, se α_i radice di f è anche radice di f_i, si ha che $\sigma_k(f_i)$ è un polinomio irriducibile che ha $\sigma_k(\alpha_i) = \alpha_j$ come radice e coincide quindi a meno di un fattore moltiplicativo con il polinomio minimo di α_j su L. Quindi σ_k applicato ai polinomi deve mandare f_i in λf_j con $\lambda \in L$, ovvero deg $f_i =$ deg f_j.

Estensione $\mathbb{Q}(\sqrt[3]{a + \sqrt[2]{b}})$

Estensione $\mathbb{Q}(\sqrt[2]{a + \sqrt[2]{b}})$

Metodi per dire che un polinomio è irriducibile

Per i gradi bassi si ha: Un polinomio $f(x)$ di grado minore o uguale a 3 è irriducibile su $K[x]$ se e solo se non ha radici in K.
Per cose di grado più grande o in più variabili si può cercare di usare Eisenstein nella seguente forma: [DA METTERE]
Se si cerca di sollevare l'irriducibilità può essere utile tenere presente il lemma che dice che un polinomio irriducibile $f(x) \in K[x]$ si scompone nel prodotto di r fattori dello

stesso grado in $L[x]$ (se L/K è normale). In questo modo ad esempio, se so che $x^p - a$ è irriducibile in $\mathbb{Q}[x]$ (E se $a \in \mathbb{Z}, a \neq 0, 1, -1$ lo è per Eisenstein) con p primo, allora su una generica estensione normale di $\mathbb{Q}$ è irriducibile se e solo se non ha radici (che è in generale una condizione più semplice da verificare).

Fatti sui campi finiti

Fatti sulle estensioni di Galois

Sottoestensioni di $\mathbb{Q}(\sqrt[n]{a})$

$\sqrt[n]{a} \in \mathbb{Q}(\zeta_m)$?

Sappiamo che Gal $\left(\frac{\mathbb{Q}(\zeta_m)}{\mathbb{Q}}\right) \cong \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$ ed è quindi abeliano. Ma allora tutti i suoi sottogruppi (e quindi tutti i suoi sottocampi) sono normali, e quindi necessariamente $n = 2$. E questo caso è già stato trattato.