Algebra I

Esercizi

Anno accademico 2018-2019

1 26.09.2018

1.1 Qualche proprietà del gruppo diedrale

Si ricorda che il gruppo diedrale D_n è il gruppo delle isometrie del piano che preservano un poligono regolare ad n lati centrato nell'origine. La sua cardinalità è $2n$.

- Determinare quante classi di coniugio di simmetrie ci sono in D_n (la risposta dipende dalla parità di n).
- Descrivere tutti i sottogruppi di D_n. Quali di questi sottogruppi sono normali?
- Dimostrare che, dato un gruppo G e un elemento $g \in G$, l'insieme $C_G(g) = \{x \in G : xg = gx\}$ è un sottogruppo di G.
- Determinare il centro di D_n.
- Dimostrare che se d è un numero dispari si ha $D_{2d} \cong D_d \times \mathbb{Z}/2\mathbb{Z}$. Dimostrare che invece i gruppi D_{4m} e $D_{2m} \times \mathbb{Z}/2\mathbb{Z}$ non sono isomorfi per alcun $m \geq 1$.
- ($\star$) Siano m, n due interi positivi. Determinare tutti gli omomorfismi da D_m a D_n.

2 03.10.2018

2.1 Sul gruppo simmetrico

- Esprimere $(1,2)(1,3)(1,4)(1,5)$ come prodotto di cicli. Qual è l'ordine di questa permutazione?
- Dato un ciclo σ di S_n, determinare la decomposizione in cicli di σ^2.
- Esibire un esempio di un gruppo G e di un elemento $g \in G$ tali che lo stabilizzatore di g per l'azione di coniugio (altrimenti detto il normalizzatore di g) non sia un sottogruppo normale di G.
- Dimostrare che ogni permutazione si può esprimere come prodotto di trasposizioni.
- Siano $\sigma = (1,2,3,4,5,6,7)$ e $\tau = (1,3,5)$. Determinare $\sigma\tau\sigma^{-1}$. In generale, dimostrare che se σ, τ sono due permutazioni in S_n e $\tau = (c_{1,1}, \dots, c_{1,l_1}) \cdots (c_{k,1}, \dots, c_{k,l_k})$, allora
$$\sigma\tau\sigma^{-1} = (\sigma(c_{1,1}), \dots, \sigma(c_{1,l_1})) \cdots (\sigma(c_{k,1}), \dots, \sigma(c_{k,l_k})).$$
- Caratterizzare le classi di coniugio nei gruppi S_n.
- Quali sono gli ordini degli elementi di S_5? Per ogni possibile ordine d, determinare il numero degli elementi di S_5 di ordine esattamente d e quanti di questi sono permutazioni pari/dispari.
- Qual è il massimo ordine di un elemento di S_6? Qual è l'esponente di S_6?

  Nota. L'*esponente* di un gruppo G è il minimo intero positivo n, se esiste, tale che $g^n = \mathrm{id}$ per ogni $g \in G$. Quando G è finito, il teorema di Lagrange implica che l'esponente di G divide $|G|$.
- Consideriamo le permutazioni $(1,2,3,4,5)$ e $(2,5)(3,4)$ di S_5. Che ordine ha il sottogruppo di S_5 da esse generato? Questo gruppo è ciclico?

2.2 Azioni di gruppo

- (Teorema di Cayley) Sia G un gruppo di ordine finito n. Dimostrare che esiste un omomorfismo iniettivo $\varphi : G \hookrightarrow S_n$.
- Sia G un gruppo finito e H un sottogruppo di G di indice p primo. Supponiamo che p sia il più piccolo primo che divide l'ordine di G: allora H è normale in G.

3 05.10.2018

3.1 Azioni di gruppo II

- Abbiamo visto in classe una dimostrazione del seguente fatto:

  Sia G un gruppo finito e H un sottogruppo di G di indice p primo. Supponiamo che p sia il più piccolo primo che divide l'ordine di G: allora H è normale in G.

  La dimostrazione passava dal considerare l'azione di moltiplicazione a sinistra di G sull'insieme G/H. Si era detto che non sarebbe stato irragionevole anche considerare l'azione di coniugio sull'insieme $\{K : K \text{ sottogruppo di } G\}$. Trovare una dimostrazione che sfrutti questa azione.

- Dimostrare che per ogni numero primo p esistono solo due gruppi di ordine p^2 a meno di isomorfismo.

  Indicazione: se g, h sono due elementi di G di ordine p che non sono uno una potenza dell'altro, si dimostri prima che $ghg^{-1} = h^k$ per qualche $k \in \mathbb{N}$ e poi che $k = 1$. In alternativa, l'esercizio è anche una conseguenza facile del fatto che ogni p-gruppo finito ha centro non banale.

- Sia G un gruppo di cardinalità $2d$, dove d è dispari. Dimostrare che G possiede un sottogruppo (necessariamente normale) di indice 2.

  Indicazione. Applicare il teorema di Cayley (e ripensare alla sua dimostrazione).

3.2 Ancora su S_n

- Consideriamo l'elemento $\sigma = (1, 2, 3, 4)(5, 6, 7)(8, 9)$ di S_9. Sia H il centralizzatore di σ in S_9. Determinare la cardinalità di H. Dimostrare che H è abeliano. Dimostrare che in effetti $H \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- Sia G il sottogruppo di S_7 generato da $(1, 2, 3, 4, 5, 6, 7)$. Determinare la cardinalità del normalizzatore di G.

- Determinare gli interi positivi n per cui S_n possiede un sottogruppo di ordine 21.

  Indicazione. Può essere utile osservare che se G è un gruppo di ordine 21 e $g \in G$ è un elemento di ordine 7, allora $\langle g \rangle$ è normale in G (perché?). Combinare questo, l'esercizio precedente, e un altro esercizio di oggi (un gruppo di ordine $2d$ contiene un sottogruppo di ordine d).

4 16.10.2018

4.1 Azioni di gruppo III

- Dare una nuova dimostrazione del teorema di Cauchy tramite il seguente approccio. Sia G un gruppo finito di cardinalità divisibile per un numero primo p. Consideriamo l'insieme

$$X = \{(g_1, \dots, g_p) \in G^p : g_1 \cdots g_p = e\}.$$

  Qual è la cardinalità di X? C'è un'azione di $\mathbb{Z}/p\mathbb{Z}$ su X (quale? Data una p-upla $(g_1, \dots, g_p)$ in X, anche $(g_p, g_1, g_2, \dots, g_{p-1})$ è in X...). Le orbite possono essere solo di lunghezza 1 o p (perché?). Come sono fatte le orbite di lunghezza 1? Si osserverà che c'è almeno un'orbita "evidente" di lunghezza 1 (quale?). Dimostrare che il numero delle orbite di lunghezza 1 è divisibile per p. Dedurne il teorema di Cauchy.

4.2 Gruppo simmetrico III

- Consideriamo $\sigma = (1,2,3)(4,5,6)(7,8,9)$ in S_9. Sia H il suo centralizzatore. Qual è la cardinalità di H? H è abeliano? Trovare un insieme di generatori di H. Dimostrare che H ha un sottogruppo normale isomorfo a $(\mathbb{Z}/3\mathbb{Z})^3$.

- Abbiamo visto che la classe di coniugio di $(1,2,3,4,5)$ in S_5 contiene $24 = 5!/5$ elementi, ovvero tutti i 5-cicli. D'altro canto, $(1,2,3,4,5)$ è anche un elemento di A_5 (il sottogruppo delle permutazioni pari): qual è la cardinalità della classe di coniugio di $(1,2,3,4,5)$ in A_5?

- Più generalmente, determinare per quali elementi σ di A_n si ha che la classe di coniugio di σ in A_n è diversa dalla cardinalità della classe di coniugio di σ nel gruppo ambiente S_n.

- Determinare per quali primi p l'equazione

$$\sigma^p = (1, \dots, p)(p+1, \dots, 2p), \quad \sigma \in S_{2p}$$

  ammette soluzione. Per tali primi determinare tutte le soluzioni di questa equazione.

- Dimostrare che il gruppo A_5 è semplice.

  Nota. Si ricorda che un gruppo G è detto semplice se gli unici sottogruppi normali di G sono $\{e\}$ e G stesso.

- ($\star$) Dimostrare che A_n è semplice per $n \geq 5$.

  Indicazione. Si può procedere per induzione, considerando l'intersezione di un (eventuale) sottogruppo normale $H < A_{n+1}$ con i sottogruppi $G_i = \{\sigma \in A_{n+1} : \sigma(i) = i\}$. Si osserverà che ogni G_i è isomorfo ad A_n, dunque semplice per ipotesi induttiva...

4.3 Struttura di qualche gruppo

- Dimostrare che un gruppo di ordine p^n (dove p è primo) possiede un sottogruppo di ordine p^k per ogni k fra 0 e n.

- Dimostrare che un gruppo di ordine p^n (dove p è primo) possiede un sottogruppo **normale** di ordine p^k per ogni k fra 0 e n.

  Nota. Questi ultimi due esercizi non saranno svolti ad esercitazione in quanto visti a lezione.

5 17.10.2018

- Dimostrare che per ogni n le permutazioni $(1,2)$ e $(1,2,\cdots,n)$ generano S_n.

5.1 Prodotti semidiretti

- Motivazione: il gruppo delle sostituzioni lineari. Dimostrare che l'insieme $\{ax+b \mid a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p\}$ ha una struttura naturale di gruppo con la quale è isomorfo a $\mathbb{F}_p \rtimes \mathbb{F}_p^\times$.

  In particolare, questo descrive un gruppo non-abeliano di ordine $p(p-1)$ per ogni $p \geq 3$.

- Descrivere il gruppo diedrale D_n come prodotto semidiretto di $\mathbb{Z}/n\mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z}$.

- Sia p un primo e q un primo che divide $p-1$. Costruire un gruppo non-abeliano di ordine pq. Dimostrare che questo gruppo è unico a meno di isomorfismo. Cosa succede se invece q è un primo che **non** divide $p-1$?

- Approfondiamo un esercizio visto il 05/10. Sia $G = S_7$ e $H = \langle(1,2,3,4,5,6,7)\rangle$ un suo sottogruppo ciclico di ordine 7. Abbiamo visto che il normalizzatore $N = N_G(H)$ è di ordine 42.

  1. Determinare se N/H sia o meno un gruppo abeliano. A quale gruppo astratto è isomorfo N/H?
  2. Descrivere N come prodotto semidiretto di due opportuni sottogruppi (quali?)

6 24.10.2018

6.1 Prodotti semidiretti II

- Determinare quanti elementi di ogni ordine ci siano nell'unico gruppo non abeliano di ordine 21.

6.2 Struttura di qualche gruppo II

- Durante l'esercitazione del 17/10 è stato affermato (senza dimostrazione) che il sottogruppo di S_6 generato da $(1,2,3,4,5,6)$ e $(1,4)$ non è l'intero S_6. In questo esercizio dimostreremo questo fatto (e molto di più). Sia $H = \langle (1,2,3,4,5,6), (1,4) \rangle < S_6$ il sottogruppo di S_6 in questione.

  1. Dimostrare che $24 \mid \#H$.
  2. Sia $\tau = (1,4)(2,5)(3,6)$. Dimostrare che τ è un elemento di H. Dimostrare che in effetti τ è contenuto nel centro di H.
  3. Dedurre che $H \subseteq Z_{S_6}((1,4)(2,5)(3,6))$. Sia $K = Z_{S_6}((1,4)(2,5)(3,6))$.
  4. Mostrare che $\#K = 48$. Dedurne in particolare che $\#H \in \{24, 48\}$ e che $H \neq S_6$.
  5. Dimostrare che K è isomorfo a $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$.

     Indicazione. Questo esercizio è praticamente identico all'analogo esercizio, visto in classe, che riguardava il centralizzatore di $(1,2,3)(4,5,6)(7,8,9)$ in S_9.
  6. Osservare che c'è un omomorfismo naturale $\pi : K \to S_3$. Determinare $\pi(H)$ e dedurre che $\#H = 24$, e anzi più precisamente che $H \cong (\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathbb{Z}/3\mathbb{Z}$.

6.3 Gruppi abeliani finitamente generati

- Sia G un gruppo abeliano (non necessariamente finito) che si può generare con 2 elementi x e y. Vogliamo dimostrare che esistono un intero $r \in \{0,1,2\}$ ed un gruppo finito T tale che $G \cong \mathbb{Z}^r \oplus T$, e che T è il gruppo banale se $r = 2$. Questo è un caso particolare del teorema di struttura per gruppi abeliani finitamente generati.

  1. Costruire un omomorfismo surgettivo $\mathbb{Z}^2 \to G$. Sia K il nucleo di questo omomorfismo.
  2. Siano $\pi_1, \pi_2 : \mathbb{Z}^2 \to \mathbb{Z}$ le proiezioni sulle due coordinate. Definiamo $K_1 = \pi(K)$ e $K_2 = \pi(K)$. Dimostrare la tesi nel caso speciale $K_1 = K_2 = (0)$.
  3. Possiamo quindi supporre che almeno uno fra K_1 e K_2 sia non banale. Per simmetria supponiamo $K_1 \neq (0)$. Siccome K_1 è un sottogruppo di $\mathbb{Z}$ è ciclico, quindi $K_1 = \langle a \rangle$ per un certo $a \in \mathbb{Z}$, $a \neq 0$.
  4. ($\star$) Consideriamo ora
     $$H = K \cap \ker \pi_1$$
     e $\pi_2(H) < \mathbb{Z}$. Dimostrare la tesi nel caso particolare $\pi_2(H) = (0)$.
  5. Se $\pi_2(H) \neq (0)$, allora $\pi_2(H) = \langle d \rangle$ per un certo $d \in \mathbb{Z}$, $d \neq 0$. Dimostrare che K è generato da due elementi, e che questi due elementi possono essere presi della forma (a,b) e $(0,d)$. Dedurre che G è finito.

7 31.10.2018

7.1 Un fatto utile: il teorema di Poincaré

- Sia G un gruppo finito e sia H un sottogruppo di G di indice n. Allora esiste un sottogruppo N di G con le seguenti proprietà:

  1. N è normale in G;
  2. N è contenuto in H;
  3. $n \mid [G : N] \mid n!$.

  In particolare, se un gruppo G contiene un sottogruppo H di indice n e $n! < \#G$, allora G non è semplice.

7.2 Gruppi abeliani finitamente generati

- Determinare il numero di (classi di isomorfismo di) gruppi abeliani di cardinalità $16 \cdot 9$.

7.3 Applicazioni dei teoremi di Sylow

- In questo esercizio dimostreremo che ogni gruppo G di ordine $3{\cdot}5{\cdot}17$ è isomorfo a $\mathbb{Z}/(3{\cdot}5{\cdot}17)\mathbb{Z}$.

  1. Dimostrare che il 17-Sylow H di G è normale.
  2. Dimostrare che in effetti $H \subseteq Z(G)$.
  3. Dedurre che $G/Z(G)$ è ciclico e concludere.

  Nota. Questo esercizio si fa anche senza i teoremi di Sylow, ma ormai...

- Trovare per quali n fra 1 e 100 esiste un gruppo semplice non-abeliano di ordine n (per i più pigri: le cardinalità più interessanti da considerare sono 56, 72, 80; 84 sembra difficile ma non lo è).

- Dimostrare che A_5 è l'unico gruppo semplice di ordine 60. Una possibile strategia è la seguente:

  1. Sia G un gruppo semplice di ordine 60. Dimostrare che il numero n_2 di 2-Sylow di G è 1, 3, 5 o 15.
  2. Dimostrare che il numero di 5-Sylow di G è 6.
  3. Escludere i casi $n_2 = 1$ (facile) e $n_2 = 3$ (considerare l'azione di G sui 2-Sylow).
  4. Dimostrare che se $n_2 = 5$ allora $G \cong A_5$.
  5. Supporre ora $n_2 = 15$. Confrontando 2-Sylow e 5-Sylow, dedurre che ci sono due 2-Sylow S_1 e S_2 tali che $|S_1 \cap S_2| = 2$.
  6. Posto $H = S_1 \cap S_2$ e $N = N_G(H)$, dimostrare che $4 \mid \#N$, che $\#N > 4$, e che $\#N \mid 60$. Dedurre che $\#N \geq 12$. Concludere.

- Dimostrare che un gruppo di ordine 112 non può essere semplice.

7.4 Automorfismi

- Sia m un intero positivo dispari. Determinare il gruppo degli automorfismi del gruppo $D_m \times D_m$, dove D_m indica il gruppo diedrale di ordine $2m$.

8 06.11.2018

- Determinare il gruppo degli automorfismi di S_3 e di S_4.
- Ricordando che il gruppo A_n è semplice per ogni $n \geq 5$, dimostrare che per $n \geq 5$ il gruppo A_n è l'unico sottogruppo normale non banale di S_n (con *non banale* si intende naturalmente *diverso da* $\{e\}$ *e da* S_n *stesso*)

  Dimostrare poi che A_4 è l'unico sottogruppo di S_4 di indice 2.
- ($\star$) Sia H un sottogruppo di S_n di indice n. Dimostrare che H è isomorfo a S_{n-1}.
- Fornire una dimostrazione del primo teorema di Sylow modellata sulla dimostrazione del teorema di Cauchy (ovvero per induzione sulla cardinalità del gruppo, sfruttando la formula delle classi).
- Dimostrare che ogni gruppo di ordine 45 è abeliano.
- Dimostrare che un gruppo di ordine 144 non può essere semplice.
- Dimostrare che – a meno di isomorfismo – esistono esattamente due gruppi di cardinalità 105.
- Dimostrare che $S_4 \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_3$. Qual è l'azione di S_3 su $(\mathbb{Z}/2\mathbb{Z})^2$?
- Sia $G = \mathrm{GL}_2(\mathbb{F}_3)$.
  1. Ricordare perché il determinante $\det : G \to \mathbb{F}_3^\times$ è un omomorfismo di gruppi.
  2. Il nucleo dell'applicazione det è detto il gruppo *speciale lineare* $\mathrm{SL}_2(\mathbb{F}_3)$. Determinare la cardinalità di $H := \mathrm{SL}_2(\mathbb{F}_3)$.
  3. Determinare $Z(G)$ e mostrare in particolare che è un sottogruppo di H.
  4. Dimostrare che il quoziente $H/Z(G)$ è isomorfo ad A_4.
  5. Dimostrare che H contiene un unico 2-Sylow, che chiameremo J.
  6. Mostrare che J non è abeliano. A quale gruppo 'famoso' è isomorfo?
  7. ($\star$) Dimostrare che J coincide con il sottogruppo derivato di H.

9 Esercizi sui gruppi che non ho avuto il tempo di trattare in classe

9.1 Prodotti semidiretti III

- Consideriamo le matrici 2×2 a coefficienti in $\mathbb{F}_2$ che siano invertibili. Dimostrare che questo insieme è un gruppo, determinarne la cardinalità, e dimostrare che è isomorfo ad un certo gruppo "ben noto".

  Essenzialmente visto; questo gruppo, denotato $\mathrm{GL}_2(\mathbb{F}_2)$*, ha cardinalità* $(2^2-1)(2^2-2) = 6$*, e siccome non è abeliano è isomorfo a* S_3*.*

- Costruire un gruppo di ordine 8 non abeliano che non sia il prodotto semidiretto di due dei suoi sottogruppi. *Risolto nella lezione di Dvornicich del 26 ottobre.*

9.2 Struttura di qualche gruppo III

- 1. Descrivere le classi di coniugio di $S_4 \times \mathbb{Z}/3\mathbb{Z}$.
  2. Descrivere tutti i possibili omomorfismi da $S_4 \times \mathbb{Z}/3\mathbb{Z}$ in $\mathbb{Z}/6\mathbb{Z}$.

9.3 Una curiosità

- Ricordiamo che in un gruppo abeliano ogni sottogruppo è normale. Vale il viceversa? Ovvero: sia G un gruppo tale che ogni sottogruppo di G sia normale. Il gruppo G è allora abeliano?

Indicazione. No, il viceversa non vale, e un controesempio è fornito dal gruppo Q_8 delle unità dei quaternioni.

10 14.11.2018

- Qualche operazione fra ideali:
  1. $A = \mathbb{F}_5[x]$, $I = (x^2 + 1)$, $J = (x^3 - 1)$. Descrivere $I + J$.
  2. $A = \mathbb{Q}[x, y]$. Dimostrare che $I = (x - 1, y - 1)$ contiene $J = (1 - xy)$. Mostrare che I è massimale ma J non lo è. J è primo?
  3. $A = \mathbb{Z}$, $I = (100)$. Descrivere $\sqrt{I}$.
  4. A anello qualunque (commutativo con identità). Dimostrare che:
     (a) $I \cdot J \subseteq I \cap J$
     (b) $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
     (c) $\sqrt{\sqrt{I}} = \sqrt{I}$
     (d) Sia D l'insieme dei divisori di 0 in A. Dimostrare che $\sqrt{D} = D$.
  5. Due ideali I, J di un anello (commutativo con identità) A sono detti *coprimi* se $I + J = A$.
     (a) Verificare che questa nozione riproduce la nozione di coprimalità che ci è familiare negli interi.
     (b) Dimostrare che se I e J sono coprimi allora $IJ = I \cap J$.
  6. Siano I, J, K tre ideali di A. Dimostrare che:
     (a) se $I + J + K = A$, allora $I^n + J^n + K^n = A$ per ogni $n \geq 1$.
     (b) se $I + J = J + K = K + I = A$, allora $IJ + JK + KI = A$.
- Utilizzando il teorema cinese del resto per polinomi, dimostrare il seguente risultato di interpolazione: per ogni $n \geq 1$ e per ogni scelta di due n-uple di numeri razionali $a_1 < a_2 < \ldots < a_n$ e $b_1, \ldots, b_n$, esiste un unico polinomio $p(x) \in \mathbb{Q}[x]$ di grado al più $n - 1$ tale che $p(a_i) = b_i$.

11 21.11.2018

- ($\star$) Descrivere gli ideali massimali di $\mathbb{Z}[x]$.
- Ritorno su un esercizio del 14.11: dimostrare che $\mathbb{Q}[x,y]/(xy-1)$ è isomorfo alla localizzazione $S^{-1}A$, dove $A = \mathbb{Q}[x]$ e $S = \{x^n : n \geq 0\}$.
- Descrivere gli ideali dell'anello $S^{-1}A$, dove $A = \mathbb{Z}$ e $S = \mathbb{Z} \setminus 2\mathbb{Z}$. Quali di questi ideali sono primi? Quali sono massimali?

  Sia poi $S = \{n \in \mathbb{Z} : (n, 6) = 1\}$. Quanti ideali primi ha $S^{-1}\mathbb{Z}$?

  Infine sia $S = \{2^n : n \in \mathbb{N}\}$: quali sono gli ideali primi di $S^{-1}\mathbb{Z}$?
- Sia $S^{-1}A$ una localizzazione di un anello A ad ideali principali. Dimostrare che $S^{-1}A$ è ancora ad ideali principali.

  Trovare un esempio di un anello A integro ma *non* ad ideali principali e di una localizzazione $S^{-1}A$ che invece sia ad ideali principali.
- Sia A un dominio ad ideali principali. Dimostrare che se B è un dominio d'integrità e $\varphi : A \to B$ è un omomorfismo suriettivo, allora o φ è un isomorfismo oppure B è un campo.
- Siano $A = \mathbb{Z}[x]/(x^2+1)$, $I = (5)$, $J = (1+2x)$. Descrivere $J : I$ e $I : J$.

12 23.11.2018

- ($\star$) Descrivere gli ideali primi di $\mathbb{Z}[i]$. Più precisamente, mostrare che se p è un primo $\equiv 3 \pmod 4$, allora p è irriducibile anche in $\mathbb{Z}[i]$. Cosa succede per $p \equiv 1 \pmod 4$ (pensate al caso di $p = 5$, visto in classe il 21.11)? E per $p = 2$?

- ($\star$) Dimostrare che $A := \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ non è un anello euclideo.

  Indicazione. Supponiamo per assurdo che d sia una funzione grado su A.

  1. Determinare $A^\times$.
  2. Detto x un elemento di A con $d(x)$ minimo fra gli $x \notin A^\times \cup \{0\}$, dimostrare che $A^\times \cup \{0\} \twoheadrightarrow A/(x)$ (pensare alla divisione con resto).
  3. Dedurre che $|A/(x)| \leq 3$.
  4. Determinare il polinomio minimo $f(x)$ di $\frac{1+\sqrt{-19}}{2}$.
  5. Osservare che $f(x)$ è irriducibile modulo 2 e modulo 3, e ottenere una contraddizione.

13 28.11.2018

- Dedurre da quanto fatto il 23/11 una descrizione di tutti i primi di $\mathbb{Z}[i]$.
- ($\star$) Dimostrare che $A := \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ è un PID. Questo anello mostra quindi che esistono PID che non sono euclidei.

  Indicazione. Pensando A come sottoanello di $\mathbb{C}$, denotiamo con $|\cdot|$ l'usuale valore assoluto complesso. Denotiamo ω l'elemento $\frac{1+\sqrt{-19}}{2}$.

  Sia I un ideale non nullo di A e sia $b \in I \setminus \{0\}$ un elemento di valore assoluto minimo. Vogliamo mostrare che $I = (b)$.

  1. Supponiamo per assurdo che $I \neq (b)$, e fissiamo $a \in I \setminus (b)$. Dimostrare che $|pa+qb| \geq |b|$ per ogni scelta di $p, q \in A$ tali che $pa + qb \neq 0$.
  2. Consideriamo ora $a/b \in \mathbb{Q}(\sqrt{-19})$. Dimostrare che esiste $r \in A$ tale che la parte immaginaria di $\frac{a}{b} - r$ si trovi nell'intervallo $\left[-\frac{\sqrt{19}}{4}, \frac{\sqrt{19}}{4}\right]$.
  3. Supponiamo ora che la parte immaginaria di $\frac{a}{b} - r$ sia nell'intervallo aperto $\left(-\frac{\sqrt{3}}{2}, \frac{\sqrt{3}}{2}\right)$. Dimostrare che esiste un intero n tale che $|\frac{a}{b} - r - n| < 1$. Dedurne che $|a-(r+n)b| < |b|$ e trovare una contraddizione.
  4. Supponiamo invece che la parte immaginaria di $\frac{a}{b} - r$ sia nell'intervallo $\left[\frac{\sqrt{3}}{2}, \frac{\sqrt{19}}{4}\right]$ (oppure $\left[-\frac{\sqrt{19}}{4}, -\frac{\sqrt{3}}{2}\right]$). Supponendo di essere nel primo caso, dimostrare che esiste un intero m tale che
  $$\left|\frac{2a}{b} - 2r - \omega - m\right| < 1.$$
  Dedurne allora che uno fra $\frac{\omega b}{2}$ e $\frac{(\omega-1)b}{2}$ appartiene ad I, mostrare che questo implica che $\frac{5b}{2}$ appartiene ad I, ed infine per differenza ottenere che $\frac{b}{2}$ appartiene ad I, contraddizione.
- Sia A un PID e $I = (p)$ un ideale tale che $A/(p)$ sia finito. Dimostrare che $|A/I^n| = |A/I|^n$.

  Indicazione. Considerando l'omomorfismo *di gruppi abeliani*
  $$\begin{array}{ccccc} A & \to & A & \to & A/I^2 \\ x & \mapsto & px & \mapsto & \overline{px} \end{array}$$
  costruire un isomorfismo (di gruppi) $\dfrac{A}{I} \to \dfrac{I}{I^2}$. Generalizzare questa costruzione per ottenere un isomorfismo di gruppi $\dfrac{A}{I} \cong \dfrac{I^k}{I^{k+1}}$ per ogni $k \geq 1$. Osservare infine che $\dfrac{A}{I} \cong \dfrac{A/I^2}{I/I^2}$, e che in generale $\dfrac{A}{I^k} \cong \dfrac{A/I^{k+1}}{I^k/I^{k+1}}$.
- ($\star$) Sia $\alpha = a + bi \in \mathbb{Z}[i]$ un elemento diverso da zero. Dimostrare che $\mathbb{Z}[i]/(\alpha)$ è un anello finito, di cardinalità uguale a $\alpha\overline{\alpha} = a^2 + b^2$.

  Indicazione. Dimostrare l'enunciato quando $b = 0$ e quando $a^2 + b^2$ è un numero primo. Dedurre l'enunciato generale dal Teorema Cinese del Resto e dall'esercizio precedente.
- Trovare tutte le coppie di interi positivi a, b tali che $a^2 + b^2 = 65$.
- Fattorizzare il polinomio $x^4 + x^2y^2 + y^4$.
- Sia A un anello e sia $A[x]$ l'anello dei polinomi con coefficienti in A in una indeterminata. Dimostrare che se $A[x]$ è un dominio ad ideali principali, allora A è un campo.

14 05.11.2018

14.1 Anelli

- Questo non è un esercizio, semplicemente una formulazione del lemma di Gauss che mi preme sottolineare. Sia A un UFD e sia $p(x) = a_n x^n + \cdots + a_0 \in A[x]$. Sia inoltre K il campo delle frazioni di A. Allora sono equivalenti:
  - $p(x)$ è irriducibile in $A[x]$;
  - $p(x)$ è irriducibile in $K[x]$ ed è *primitivo*, ovvero il massimo comun divisore (calcolato in A) degli elementi $a_0, \ldots, a_n$ è 1 (equivalentemente, in termini di ideali, vale l'uguaglianza $(a_0, \ldots, a_n) = (1)$).
- Trovare una seconda dimostrazione del fatto che se $A[x]$ è un PID, allora A è un campo.
- Sia A un anello commutativo con unità. Dimostrare che $\sqrt{(0)} = \bigcap_{\mathcal{P} \text{ primo}} \mathcal{P}$. Dedurne che se I è un qualunque ideale, $\sqrt{I}$ è l'intersezione dei primi che contengono I.

  Nota. L'insieme $\sqrt{(0)}$ è a volte detto il *nilradicale* di A; è uguale all'insieme di tutti gli elementi nilpotenti. Si ricorda che un elemento $a \in A$ è detto *nilpotente* se esiste $n > 0$ tale che $a^n = 0$.
- Sia A un anello commutativo con identità. Supponiamo che per ogni $x \in A$ esista un intero n (eventualmente dipendente da x) tale che $x^n = x$. Dimostrare che allora un ideale di A è primo se e solo se è massimale.
- Consideriamo l'anello $A = \mathbb{Z}[x]/(x^2 + 5)$. Dimostrare che A è un dominio d'integrità. Dimostrare che $2 \in A$ è irriducibile ma non è primo. Dedurre che l'ideale (2) in A è massimale fra gli ideali principali, ma non è primo (e quindi in particolare non è massimale nella famiglia di tutti gli ideali di A). Trovare un ideale primo che contiene (2). Tale primo è massimale?
- Sia $p(x, y) \in \mathbb{Q}[x, y]$ un polinomio tale che $p(x, y_0)$ è irriducibile per ogni $y_0 \in \mathbb{Q}$. È vero che $p(x, y)$ è necessariamente irriducibile?

14.2 Campi

- Per definizione, un *isomorfismo* tra i campi K e L è un omorfismo *di anelli* $K \to L$ che sia iniettivo e surgettivo. Quando $L = K$ si parla di *automorfismo*.

  Sia K un campo. Dimostrare che un omomorfismo di anelli $\phi : K \to K$ è un automorfismo se e solo se è surgettivo. Dimostrare inoltre che esistono campi K e omomorfismi $K \to K$ iniettivi che non sono automorfismi.
- Sia p un numero primo. Determinare tutti gli automorfismi del campo $\mathbb{F}_{p^2}$.

15 Esercizi sugli anelli non trattati in classe

- Siano I, J due ideali di un anello I. Vale sempre l'uguaglianza $I(J+K) = IJ + IK$?

  Indicazione. Sì, e non è difficile dimostrarlo: verifichiamo la doppia inclusione. Certamente $IJ \subseteq I(J+K)$ e $IK \subseteq I(J+K)$, da cui $IJ + IK \subseteq I(J+K)$. Viceversa, un elemento di $I(J+K)$ è della forma $\sum_h i_h(j_h + k_h) = \sum_h (i_h j_h) + \sum_h (i_h k_h)$ (con $i_h \in I, j_h \in J, k_h \in K$), e quindi appartiene a $IJ + IK$.

- Dato un intero positivo m consideriamo le parti moltiplicative $S = \left\{m^k \;\middle|\; k \in \mathbb{N}\right\}$ e $T = \left\{a \in \mathbb{Z} \;\middle|\; (a, m) = 1\right\}$ di $\mathbb{Z}[x]$.

  1. Dimostrare che non esiste un omomorfismo suriettivo $S^{-1}\mathbb{Z}[x] \to \mathbb{Q}$.
  2. Determinare un omomorfismo suriettivo $T^{-1}\mathbb{Z}[x] \to \mathbb{Q}$.

  Indicazione. Per il punto 1, detto ϕ un qualunque omomorfismo da $A := S^{-1}\mathbb{Z}[x]$ a $\mathbb{Q}$, osservare che c'è solo un numero finito di primi che possono comparire nella fattorizzazione del denominatore di $\phi(a)$, indipendentemente dalla scelta di $a \in A$ (questi primi sono i divisori di m e i divisori del denominatore di $\phi(x)$).

  Per il punto 2, invertendo T si sono già invertiti tutti i numeri primi che *non* dividono m; allora ponendo $\psi(x) = \frac{1}{m}$ si avrà che ψ è un omomorfismo, ed inoltre l'immagine di ψ contiene $\frac{1}{p}$ per ogni primo p. Questo implica (perché?) che ψ è suriettivo.

- ($\star$) Sia $I = (x_1, \ldots, x_n)$, visto come ideale dell'anello $A = \mathbb{Q}[x_1, \ldots, x_n]$. È possibile trovare $n-1$ polinomi $p_1(x_1, \ldots, x_n), \ldots, p_{n-1}(x_1, \ldots, x_n) \in A$ tali che $I = (p_1, \ldots, p_{n-1})$? (In altre parole: è possibile generare I con meno di n elementi?)

  Indicazione. Questo esercizio può essere molto difficile, se non si prende la strada giusta. L'idea cruciale è che I/I^2 è uno spazio vettoriale su $A/I = \mathbb{Q}$. Non è difficile vedere che le classi di $x_1, \ldots, x_n$ in I/I^2 sono una base di questo spazio vettoriale. Infine, se $p_1, \ldots, p_k$ generano I, allora le loro classi in I/I^2 generano I/I^2 (essenzialmente ovvio). Segue da fatti base di algebra lineare che $k \geq n$.

16 07.12.2018

- Sia $K := \mathbb{F}_2(x, y)$ il campo delle funzioni razionali in due variabili su $\mathbb{F}_2$, ovvero il campo dei quozienti di $\mathbb{F}_2[x, y]$. Sia poi $L \subset K$ il campo $\mathbb{F}_2(x^2, y^2)$. Dimostrare che:

  1. il polinomio minimo di x su L ha radici multiple in K (si dice che non è *separabile*);
  2. $[K : L] = 4$;
  3. per ogni elemento $f \in K$ si ha $[L(f) : L] \leq 2$.

  Dedurne che l'estensione K/L non è *semplice*, ovvero non è generata da un singolo elemento.

  Dimostrare infine che esistono infinite estensioni intermedie distinte $K/F/L$ con $[K : F] = [F : L] = 2$.

- Sia K un campo, $f(x) \in K[x]$ un polinomio irriducibile, e L il campo di spezzamento di $f(x)$ su K. Supponendo che le radici di $f(x)$ in L siano tutte distinte, dimostrare che $\#\operatorname{Gal}(L/K) = [L : K]$.

- Siano L_1, L_2 due estensioni normali finite di un campo K. Supponiamo K, L_1, L_2 tutti immersi in una certa chiusura algebrica E di K. Dimostrare che:

  - L_1L_2 è un'estensione normale di K;
  - il gruppo di Galois $\operatorname{Gal}(L_1L_2/K)$ si immerge in $\operatorname{Gal}(L_1/K) \times \operatorname{Gal}(L_2/K)$.

- Siano $a, b \in \mathbb{Q}$ tali che $K_1 = \mathbb{Q}(\sqrt{a})$ e $K_2 = \mathbb{Q}(\sqrt{b})$ siano estensioni quadratiche *distinte* di $\mathbb{Q}$. Dimostrare che $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ è un'estensione normale e determinarne il gruppo di Galois.

- Sia ζ_7 una radice primitiva settima dell'unità in $\mathbb{C}$ e sia $K := \mathbb{Q}(\zeta_7)$. Sia poi $\alpha := \zeta_7 + \zeta_7^{-1}$ e $L = \mathbb{Q}(\alpha)$. Dimostrare che l'estensione $L/\mathbb{Q}$ è normale e che il suo gruppo di Galois è $\mathbb{Z}/3\mathbb{Z}$.

  Sia inoltre $m(x)$ il polinomio minimo di α su $\mathbb{Q}$. Determinare $m(x)$ e dimostrare che le sue tre radici sono $\zeta_7 + \zeta_7^{-1}$, $\zeta_7^2 + \zeta_7^{-2}$, $\zeta_7^3 + \zeta_7^{-3}$.

  Indicazione.

  1. Dimostrare che $[L : \mathbb{Q}] = 3$.
  2. Dimostrare che $L_i := \mathbb{Q}(\zeta_7^i + \zeta_7^{-i})$ è contenuto in L per ogni i positivo (se così non fosse, L e L_i genererebbero K; ma questo è impossibile, perché?).
  3. Sia ora $\psi : L \to \mathbb{C}$ un omomorfismo non nullo. Dimostrare che $\psi(L) \subseteq K$. Dimostrare inoltre che esiste un omomorfismo non nullo $\phi : K \to \mathbb{C}$ tale che $\phi|_L = \psi$.
  4. Dedurre che $\psi(\zeta_7 + \zeta_7^{-1}) = \zeta_7^i + \zeta_7^{-i}$ per qualche i.
  5. Concludere che $L/\mathbb{Q}$ è normale e che il suo gruppo di Galois è $\mathbb{Z}/3\mathbb{Z}$.
  6. Il metodo più comodo per determinare il polinomio minimo di α è probabilmente quello di partire dall'identità $\zeta_7^6 + \cdots + 1 = 0$, dividere tutto per ζ_7^3, e tentare di esprimere il risultato in funzione di α. L'affermazione relativa alle radici segue da quanto già dimostrato: perché?

- Sia $f(x) = x^3 + ax + b$ un polinomio irriducibile di terzo grado a coefficienti in un certo campo K (di caratteristica diversa da 2 e da 3, per semplificare la discussione). Sia α una radice di $f(x)$ in una opportuna chiusura algebrica, sia $F = K(\alpha)$, e sia L il campo di spezzamento di $f(x)$ su K. Infine, siano $\alpha_1 = \alpha, \alpha_2, \alpha_3$ le radici di $f(x)$ in L, e consideriamo $\Delta := ((\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1))^2$; questa quantità è detta il *discriminante* del polinomio. Dimostrare che:

  1. $\Delta \in K$.
  2. Il grado $[L : K(\sqrt{\Delta})]$ è 3.

3. Il gruppo di Galois di L/K è isomorfo a S_3 o ad A_3, e il secondo caso si verifica se e solo se Δ è un quadrato in K.
4. Se $K = \mathbb{Q}$, si ha $\Delta > 0$ se e solo se le tre radici di $f(x)$ sono tutte reali, e $\Delta < 0$ altrimenti. In particolare, il gruppo di Galois di L su $\mathbb{Q}$ può essere A_3 solo quando tutte le radici sono reali.

Determinare infine il gruppo di Galois su $\mathbb{Q}$ del campo di spezzamento dei polinomi x^3-3x-1 e $x^3 - 4x - 1$.

Indicazione. Dimostrare che il discriminante di $f(x) = x^3 + ax + b$ è $-4a^3 - 27b^2$. Questo si può fare o tramite un calcolo piuttosto noioso, oppure osservando che, dette $\alpha_1, \alpha_2, \alpha_3$ le radici del polinomio $x^3 + ax + b$, si ha

$$\begin{aligned}\operatorname{disc}(f(x)) &= \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}^2 = \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix} \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix}, \\ &= \det \begin{pmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{pmatrix}\end{aligned}$$

dove $s_j = \alpha_1^j + \alpha_2^j + \alpha_3^j$. Un calcolo meno noioso del precedente mostra ora $s_0 = 3$, $s_1 = 0$, $s_2 = -2a$, $s_3 = -3b$, $s_4 = 2a^2$.

17 12.12.2018

- Dimostrare che (per ogni primo p, ogni m e ogni n con $m \mid n$) l'estensione $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ è semplice e normale. Qual è il corrispondente gruppo di Galois?

  Nota. Questo esercizio non sarà svolto in classe, in quanto l'argomento è già stato affrontato a lezione l'11 dicembre.

- Determinare tutte le sottoestensioni di $\mathbb{Q}(\zeta_7)$. Quali di queste sono normali?

- Sia $p(x) = x^4 + ax^2 + b$ un polinomio irriducibile a coefficienti razionali, e sia K il suo campo di spezzamento. Dimostrare che il gruppo di Galois $G = \mathrm{Gal}(K/\mathbb{Q})$ è dato da:

  1. $(\mathbb{Z}/2\mathbb{Z})^2$ se e solo se b è un quadrato in $\mathbb{Q}$;
  2. $\mathbb{Z}/4\mathbb{Z}$ se e solo se b non è un quadrato in $\mathbb{Q}$, ma $b(a^2 - 4b)$ lo è;
  3. D_4, se né b né $b(a^2 - 4b)$ è un quadrato in $\mathbb{Q}$.

- Dimostrare che l'unica sottoestensione non banale di $\mathbb{Q}(\sqrt[4]{2})$ è $\mathbb{Q}(\sqrt{2})$.

- Siano $p_1, \dots, p_k$ primi distinti. Determinare il grado ed il gruppo di Galois dell'estensione $K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k})$ di $\mathbb{Q}$ (come prima cosa dimostrare che $K/\mathbb{Q}$ è effettivamente normale!)

- Sia N/K un'estensione di Galois e F/K un'estensione qualsiasi. Dire se l'estensione FN/F è necessariamente normale e in tal caso studiare il suo gruppo di Galois.

- ($\star$) Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado p primo. Supponiamo che le radici reali di $f(x)$ siano esattamente $p-2$ (mentre le altre due sono complesse coniugate). Dimostrare che il gruppo di Galois del campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è isomorfo a S_p.

  Indicazione. Ricordare (o dimostrare) che S_p è generato da un qualunque p-ciclo e da una qualunque trasposizione. Usando il teorema di Cauchy, dimostrare che il gruppo di Galois contiene un p-ciclo. E la trasposizione?

- ($\star$) Dimostrare che per ogni primo p esiste un polinomio irriducibile $f(x) \in \mathbb{Q}[x]$ con la seguente proprietà: detto K il campo di spezzamento di $f(x)$ su $\mathbb{Q}$, il gruppo di Galois di K su $\mathbb{Q}$ è isomorfo a S_p.

  Indicazione. Usare l'esercizio precedente. Un possibile esempio per $p > 2$ è il seguente (ma bisogna dimostrare che funziona!). Poniamo $h = \frac{p-3}{2}$. Allora il polinomio

  $$q_d(x) = dx(x^2 - 2^2)(x^2 - 4^2) \cdots (x^2 - (2h)^2)(x^2 + 4) + 2,$$

  dove d è un intero dispari, è irriducibile e (se d è sufficientemente grande) ha il gruppo di Galois richiesto.

18 19.12.2018

- Sia N/K un'estensione di Galois e F/K un'estensione qualunque. Supponiamo che $F \cap N = K$. Dimostrare che $[FN : K] = [F : K][N : K]$. Vale la medesima conclusione se si toglie l'ipotesi che N/K sia di Galois?

- Applicando il teorema di corrispondenza di Galois, descrivere tutte le sottoestensioni del campo di spezzamento su $\mathbb{Q}$ del polinomio $x^3 - 2$. Quali di queste sono fra loro isomorfe? Quali di queste sono normali su $\mathbb{Q}$?

- Sia $p(x) = x^6 + 3 \in \mathbb{Q}[x]$ e sia K il suo campo di spezzamento su $\mathbb{Q}$. Determinare il gruppo $\mathrm{Gal}(K/\mathbb{Q})$.

- Sia $p(x) = x^5 - 3 \in \mathbb{Q}[x]$ e sia K il suo campo di spezzamento su $\mathbb{Q}$. Determinare il gruppo di Galois di K su $\mathbb{Q}$. Determinare tutte le sottoestensioni F di K; per ognuna di esse, determinare un elemento $\alpha \in F$ tale che $F = \mathbb{Q}(\alpha)$.

- Sia K un campo di caratteristica diversa da 3 che contenga le radici primitive terze dell'unità. Sia poi F un'estensione di Galois di K con gruppo di Galois $\mathbb{Z}/3\mathbb{Z}$.

  1. Dimostrare che esiste $a \in K^\times$ tale che $L = K(\sqrt[3]{a})$.
  2. Dimostrare che per due elementi $a, b \in K^\times$ vale l'uguaglianza $K(\sqrt[3]{a}) = K(\sqrt[3]{b})$ se e soltanto se vale una delle seguenti: a/b è un cubo in K oppure a^2/b è un cubo in K.
  3. Trovare un esempio di un campo K che non contiene le radici terze dell'unità e di una sua estensione di Galois L con gruppo $\mathbb{Z}/3\mathbb{Z}$ tali che L non si possa scrivere nella forma $K(\sqrt[3]{a})$ per alcun $a \in K^\times$.

- ($\star\star$) Trovare una formula risolutiva per l'equazione di terzo grado $x^3+px+q = 0$. Dare un'interpretazione di questa formula in termini di teoria di Galois. Si ricorda che il discriminante di $x^3 + px + q$ è $-4p^3 - 27q^2$.

19 Qualche complemento

- (Teorema fondamentale delle funzioni simmetriche, versione per funzioni razionali) Sia K un campo e $f(x_1, \dots, x_n) \in K(x_1, \dots, x_n)$ una funzione razionale in n variabili *simmetrica*, ovvero tale che per qualunque permutazione $\sigma \in S_n$ si abbia

$$f(x_1, \dots, x_n) = f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right).$$

  Siano poi $e_1, \dots, e_n$ le cosiddette *funzioni simmetriche elementari*, ovvero

$$e_i := \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I|=i}} \prod_{j \in I} x_j$$

  (A titolo di esempio, $e_1 = x_1 + x_2 + \cdots + x_n$ è la somma delle variabili, $e_2 = \sum_{i \neq j} x_i x_j$ è la somma dei prodotti due a due, ed $e_n = \prod_{j=1}^{n} x_j$ è il prodotto di tutte le variabili.) Dimostrare che esiste una funzione razionale $g \in K(e_1, \dots, e_n)$ tale che $f(x_1, \dots, x_n) = g(e_1, \dots, e_n)$.

- ($\star\star$) Siano α, β numeri algebrici di grado rispettivamente m, n. Dimostrare che se $(m, n) = 1$, allora $\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha, \beta)$.

  Indicazione. Quest'esercizio è *estremamente* difficile senza qualche aiutino. L'idea chiave (un po' miracolosa) è la seguente: sul campo $\mathbb{C}$ c'è un ordinamento compatibile con la somma. Considerare il massimo degli elementi $\alpha_i + \beta_j$ rispetto a questo ordinamento, dove α_i sono i coniugati di α e β_j sono i coniugati di β.

- (Il teorema fondamentale dell'algebra, $\star$) Dimostrare che $\mathbb{C}$ è algebricamente chiuso.

  Indicazione.

  - Mostrare che è sufficiente far vedere che ogni polinomio a coefficienti *reali* ha tutte le sue radici in $\mathbb{C}$.
  - Sia $p(x) \in \mathbb{R}[x]$ un polinomio irriducibile di grado dispari. Dimostrare che $p(x)$ è di grado 1 (hint: sarà necessario usare un minimo di analisi, nella forma del teorema dei valori intermedi. Questo è inevitabile: la definizione di $\mathbb{R}$ è analitica e non algebrica)
  - Sia ora $q(x) \in \mathbb{R}[x]$ un polinomio irriducibile qualsiasi, e sia K il suo campo di spezzamento su $\mathbb{R}$. Vogliamo mostrare che $K = \mathbb{R}$ o $K = \mathbb{C}$. Sia $[K : \mathbb{R}] = 2^k d$ con d dispari. Dimostrare che esiste una sottoestensione $F/\mathbb{R}$ di $K/\mathbb{R}$ con $[F : \mathbb{R}] = d$ (hint: usare il teorema di corrispondenza di Galois e un opportuno teorema di Sylow).
  - Dimostrare che $d = 1$.
  - Dedurre che esiste una torre di estensioni intermedie

$$\mathbb{R} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n = K$$

    tale che $[K_{i+1} : K_i] = 2$.
  - Dimostrare che ogni estensione quadratica di $\mathbb{R}$ è isomorfa a $\mathbb{C}$, e che $\mathbb{C}$ non ammette estensioni quadratiche.
  - Concludere.

- (Teorema di Abel-Ruffini, $\star\star\star$) Dare un senso preciso al seguente enunciato e poi dimostrarlo: esistono equazioni polinomiali di grado 5 le cui soluzioni non si possono esprimere tramite le operazioni di campo combinate con l'estrazione di radicali.

  Indicazione. Andare a leggere su Wikipedia la definizione di gruppo risolubile, e tentare di connetterla al concetto di risolubilità per radicali.

- (Due dei tre grandi problemi dell'antichità, $\star\star\star$) Dare un senso preciso al seguente enunciato e poi dimostrarlo: la duplicazione del cubo e la trisezione dell'angolo sono impossibili con riga e compasso.