COMPITO DI ALGEBRA 1

7 settembre 2015

Esercizio 1.

Diciamo che un gruppo finito G è iperciclico se tutti i suoi sottogruppi di Sylow sono ciclici. Supponiamo che G sia iperciclico. Mostrare i seguenti fatti:

a) tutti i sottogruppi e i quozienti di G sono iperciclici;

b) per un primo p e un intero r fissati, tutti i sottogruppi di G di ordine p^r sono coniugati;

c) se N è un sottogruppo normale di G e H è un p-sottogruppo di G allora

$$|N \cap H| = \mathrm{MCD}(|N|, |H|).$$

d) ogni sottogruppo normale di G è caratteristico.

Soluzione Esercizio 1.

a) Sia H un sottogruppo di G e sia P un sottogruppo di Sylow di H. P è contenuto in un sottogruppo di Sylow di G e dunque è ciclico in quanto sottogruppo di un sottogruppo ciclico. Dunque H è iperciclico.

Sia K un quoziente di G e sia Q un q-sottogruppo di Sylow di K. Detta $\pi : G \to K$ la mappa di proiezione, $\widetilde{Q} := \pi^{-1}(Q)$ è un sottogruppo di G che contiene un q-sottogruppo di Sylow di G, che chiameremo Q'. Inoltre $\pi(Q') = Q$ e dunque Q, essendo immagine di sottogruppo ciclico, è a sua volta ciclico. Dunque K è iperciclico.

b) Siano H_1 e H_2 due sottogruppi di G di ordine p^r. Essi sono rispettivamente contenuti in due p-Sylow, $H_1 < P_1$, $H_2 < P_2$. I sottogruppi P_1 e P_2, essendo dei p-Sylow, sono tra loro coniugati. Inoltre, essendo ciclici, ciascuno contiene un unico sottogruppo di ordine p^r. Dunque un coniugio che manda P_1 in P_2 deve anche mandare H_1 in H_2.

c) L'equazione vale se e solo se $N \cap H$ è un p-sottogruppo di Sylow di N. Dimostriamo che questo è sempre verificato. Sia K un p-sottogruppo di Sylow di N. Per il punto b) K è coniugato ad un sottogruppo $K' < H$. Poiché N è normale, anche K' è un sottogruppo di N e dunque $N \cap H > K'$. L'inclusione opposta vale perchè K' è un p-Sylow di N e H è un p-sottogruppo, e dunque anche $H \cap N$ deve esserlo.

d) Sia N un sottogruppo normale di G e sia H un p-sottogruppo di Sylow di G. Sia p^r l'ordine di $N \cap H$, poichè H è ciclico, $N \cap H$ è l'unico sottogruppo di H di ordine p^r. Sia φ un automorfismo di G. Il sottogruppo $\varphi(N \cap H)$ è l'unico sottogruppo ciclico di ordine p^r del p-Sylow $\varphi(H) := H'$. Dunque per il punto c) $\varphi(N \cap H) = N \cap H' < N$. Ne segue che l'insieme dei p-Sylow di N è invariante per automorfismi di G e poichè N è generato dai suoi sottogruppi di Sylow ne segue che N è caratteristico.

Esercizio 2.
Sia $G = D_{15}$ il gruppo diedrale di ordine 30 (cioè il gruppo delle isometrie di un poligono regolare di 15 lati).
a) Provare che, per ogni divisore d di 30, G possiede almeno un sottogruppo di ordine d;
b) determinare tutti i divisori d di 30 per i quali G possiede un unico sottogruppo di ordine d.

Soluzione Esercizio 2.
a) I divisori propri di 30 sono $2, 3, 5, 6, 10, 15$. Dunque per il teorema di Cauchy D_{15} ha sottogrupppi di ordine $2, 3, 5$.
Notiamo che $D_{15} = \mathbb{Z}/15 \rtimes \mathbb{Z}_2 = (\mathbb{Z}/3 \times \mathbb{Z}/5) \rtimes \mathbb{Z}/2$, dove il generatore di $\mathbb{Z}/2$ agisce per coniugio tramite l'unico automorfismo non banale sia su $\mathbb{Z}/3$, sia su $\mathbb{Z}/5$.
Rispetto alla decomposizione di D_{15} come prodotto semidiretto $(\mathbb{Z}/3 \times \mathbb{Z}/5) \rtimes \mathbb{Z}/2$, abbiamo, per ciascun divisore proprio di 30 che non sia primo, i seguenti sottogruppi: $H_6 = (\mathbb{Z}/3 \times \{0\}) \rtimes \mathbb{Z}/2 \simeq D_3$, $H_{10} = (\{0\} \times \mathbb{Z}/5) \rtimes \mathbb{Z}/2 \simeq D_5$, $H_{15} = (\mathbb{Z}/3 \times \mathbb{Z}/5) \rtimes \{0\} \simeq \mathbb{Z}/15$.
b) Ovviamente $G = D_{15}$ possiede un unico sottogruppo di ordine 1 ed un unico sottogruppo di ordine 30.
Inoltre G contiene 1 elemento di ordine 1, 2 elementi di ordine 3, 4 elementi di ordine 5, 8 elementi di ordine 15 e 15 elementi di ordine 2. Di conseguenza G contiene un unico sottogruppo di ordine 3, un unico sottogruppo di ordine 5 ed un unico sottogruppo di ordine 15. Sia s un qualsiasi elemento di G di ordine 2, il suo centralizzatore ha anch'esso ordine 2 perché s non commuta con nessun elemento di ordine 3 o 5. Dunque il normalizzatore di $< s >$ ha ordine 2 e tutti gli elementi di ordine 2 sono tra loro coniugati. Ora, se un sottogruppo proprio $H < G$ ha ordine pari, esso contiene un elemento di ordine 2. Dunque per ogni elemento di ordine 2 esiste un opportuno coniugato di H che lo contiene. Poiché gli elementi di ordine 2 generano G, H essendo proprio non può contenerli tutti. Dunque esiste un suo coniugato disgiunto da lui. Segue che i divisori d per i quali G contiene un unico sottogruppo di ordine d sono $1, 3, 5, 15, 30$.

Esercizio 3.
a)Dimostrare che non esistono omomorfismi surgettivi da $\mathbb{Z}[x]$ in $\mathbb{Q}$.
b) Sia $\varphi : \mathbb{Z}[x] \to \mathbb{Q}$ l'omomorfismo definito da $\varphi(f(x)) = f(\frac{1}{10})$. Determinare gli elementi invertibili e gli ideali primi di $\varphi(\mathbb{Z}[x])$.

Soluzione Esercizio 3.

a) Sia φ un omomorfismo da $\mathbb{Z}[x]$. Chiaramente $\varphi(1) = 1$ e l'omomorfismo è determinato dall'immagine di x. Sia dunque $\varphi(x) = \frac{a}{b}$ con a e b interi coprimi e b positivo. L'immagine di un qualsiasi polinomio $f(x)$ di grado n può essere espressa come frazione con denominatore b^n. Sia dunque p un primo che non divide b, il razionale $\frac{1}{p}$ non può essere espresso

nella forma $\frac{m}{b^n}$ per nessun n (perché non si può avere $m \cdot p = b^n$). Ne segue che φ non è suriettivo.
b) L'immagine di φ è isomorfa a $S^{-1}\mathbb{Z}$ dove $S = \{(10)^n, n \in \mathbb{N}\}$. Gli ideali primi di $S^{-1}\mathbb{Z}$ sono in corrispondenza con gli ideali primi di $\mathbb{Z}$ che non intersecano S. Poiché $10 = 2 \cdot 5$ gli ideali primi di $\varphi(\mathbb{Z}[x])$ sono dunque quelli generati dai primi di $\mathbb{Z}$ distinti da 2 e 5.
Sia $t = \frac{m}{(10^n)} \in S^{-1}\mathbb{Z}$, se m è diviso da un primo p di $\mathbb{Z}$ diverso da 2 o 5 allora t è contenuto nell'ideale primo $S^{-1}(p)$ e dunque non è invertibile. Se gli unici primi che dividono m sono 2 e 5 allora possiamo scrivere $m = (-1)^\epsilon 2^a 5^b$ e quindi $t \cdot \frac{(-1)^\epsilon (10)^n}{1} \in S$ e dunque t è invertibile.

Esercizio 4.
Per ogni $n \in \mathbb{N}$ indichiamo con ζ_n una radice n-esima primitiva dell'unità.
a) Determinare le sottoestensioni del campo $\mathbb{Q}(\zeta_7)$.
b) Sia $L = \mathbb{Q}(\zeta_7, \zeta_5)$. Determinare tutte le sottoestensioni $K \subseteq L$ tali che $[L : K] = 2$.

Soluzione Esercizio 4.
a) Sappiamo che $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \phi(7) = 6$, che $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ è di Galois e che gli automorfismi di $\mathbb{Q}(\zeta_7)$ che fissano $\mathbb{Q}$ sono $\{\sigma_i\}_{i=1}^6$ dove $\sigma_i(\zeta_7) = \zeta_7^i$. Da questo segue che $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})\langle\sigma_3\rangle \cong (\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$. L'estensione $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ ha quindi, oltre alle due sottoestensioni banali $\mathbb{Q}$ e $\mathbb{Q}(\zeta_7)$, due sottoestensioni proprie, una di grado 2 e una di grado 3 su $\mathbb{Q}$. Tali sottoestensioni sono fissate rispettivamente dai sottogruppi $\langle\sigma_2\rangle$ (che ha ordine 3) e $\langle\sigma_6\rangle$ (che ha ordine 2). È noto che σ_6 è il coniugio e fissa la massima sottoestensione reale di $\mathbb{Q}(\zeta_7)$ cioè $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Per quanto riguarda la sottoestensione di grado 2, osserviamo che l'elemento $\zeta_7 + \zeta_7^2 + \zeta_7^4$ è fissato da σ_2 e quindi è contenuto nella sottoestensione F di grado 2. Inoltre tale elemento non appartiene a $\mathbb{Q}$, altrimenti esisterebbe un numero razionale q tale che $\zeta_7^4 + \zeta_7^2 + \zeta_7 = q$ mentre ζ_7 ha grado 6 su $\mathbb{Q}$. Ne segue che $F = \mathbb{Q}(\zeta_7^4 + \zeta_7^2 + \zeta_7)$.
b) Ricordiamo che $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \phi(5)$ e che il suo gruppo di Galois è isomorfo a $\mathbb{Z}/4\mathbb{Z}$. Calcoliamo il grado di L su $\mathbb{Q}$. Osserviamo che $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \phi(7) = 6$ e $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \phi(5) = 4$, quindi confrontando i gradi delle due estensioni si ha che $\mathbb{Q}(\zeta_7) \cap \mathbb{Q}(\zeta_5)$ ha al più grado 2 su $\mathbb{Q}$. D'altra parte l'unica sottoestensione di grado 2 su $\mathbb{Q}$ di $\mathbb{Q}(\zeta_5)$ è quella reale, mentre la sottoestensione di grado 2 su $\mathbb{Q}$ di $\mathbb{Q}(\zeta_7)$ è non reale (la sottoestensione reale ha grado 3), e quindi $\mathbb{Q}(\zeta_7) \cap \mathbb{Q}(\zeta_5) = \mathbb{Q}$. Da questo segue che $[\mathbb{Q}(\zeta_7, \zeta_5) : \mathbb{Q}] = [\mathbb{Q}(\zeta_7) : \mathbb{Q}][\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 6 \cdot 4 = 24$ e che $\mathrm{Gal}(\mathbb{Q}(\zeta_7, \zeta_5)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_7) : \mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_5) : \mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
Osserviamo che questa prima parte poteva essere semplificata usando l'osservazione $L = \mathbb{Q}(\zeta_{35})$ e il risultato generale $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ e $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ (che però non è stato dimostrato a lezione).
Le sottoestensioni K tali che $[L : K] = 2$ sono quelle fissate dai sottogruppi di ordine 2

del gruppo di Galois. È semplice vedere che ce ne sono 3 e che quindi le sottoestensioni cercate sono 3. D'altra parte le 3 sottoestensioni $K_1 = \mathbb{Q}(\zeta_{35} + \zeta_{35}^{-1})$, $K_2 = \mathbb{Q}(\zeta_7, \zeta_5 + \zeta_5^{-1})$ e $K_3 = \mathbb{Q}(\zeta_5, \zeta_7 + \zeta_7^{-1})$, sono distinte e $[L : K_i] = 2$ per $i = 1, 2, 3$, quindi sono le sottoestensioni cercate. Il calcolo del grado è elementare e dipende da osservazioni già fatte. Inoltre $K_1 \neq K_2$ e $K_1 \neq K_3$, perché K_1 è reale mentre K_2 e K_3 no, e $K_2 \neq K_3$ perché hanno gruppi di Galois distinti su $\mathbb{Q}$.