COMPITO DI ALGEBRA 1

10 luglio 2018

Esercizio 1. Siano p e q due numeri primi distinti.

1. Determinare in funzione di p e di q il minimo intero positivo n tale che S_n ammette un sottogruppo abeliano di ordine pq.

2. Determinare in funzione di p e di q il minimo intero positivo n tale che S_n ammette un sottogruppo di ordine pq.

Soluzione:

1. Un gruppo abeliano di ordine pq è necessariamente ciclico (lo sono tutti e gruppi abeliani di ordine squarefree), quindi S_n contiene un gruppo di ordine pq se e solo se contiene una permutazione σ di ordine pq. Visto che l'ordine di una permutazione è l'mcm degli ordini dei suoi cicli nella sua scrittura come prodotto di cicli disguinti, si ha che se $\mathrm{ord}(\sigma) = pq$ allora σ contiene almeno un p ciclo e almeno un q ciclo, oppure contiene un ciclo di lunghezza pq. Dato che $p+q < pq$ per ogni p, q primi distinti, si ha che $n \geq p+q$. D'altra parte in S_{p+q} la permutazione $\sigma = (1, \dots, p)(p+1, \dots, p+q)$ ha ordine pq e quindi genera il gruppo cercato.

2. Supponiamo $p > q$. Sappiamo che se $q \nmid p-1$ un gruppo di ordine pq è necessariamente ciclico. Abbiamo visto nel punto precedente che il minimo n in questo caso è $p+q$.
   Consideriamo quindi il caso in cui $q \mid p-1$. In questo caso oltre al gruppo ciclico esiste solo un altro gruppo G che è isomorfo al prodotto semidiretto $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ (sappiamo anche che i possibili prodotti semidiretti sono tutti isomorfi tra loro). Se $G \subseteq S_n$ allora S_n contiene elementi di ordine p, quindi $n \geq p$. Mostriamo che S_p contiene un sottogruppo isomorfo a G. Sia $\gamma = (1, 2, \dots, p) \in S_p$; sappiamo $|Z_{S_p}(\gamma)| = p!/(p-1)! = p$ quindi $Z_{S_p}(\gamma) = \langle\gamma\rangle$ e $|N_{S_p}(\langle\gamma\rangle)| = |Z_{S_p}(\gamma)|\phi(p) = p(p-1)$, quindi, dato che $q|p-1$, per Cauchy esiste un $\rho \in N_{S_p}(\langle\gamma\rangle)$ di ordine q. Dato che ρ normalizza $\langle\gamma\rangle$, il prodotto dei due gruppi $\langle\gamma\rangle$ e $\langle\rho\rangle$ è un gruppo che chiaramente ha cardinalità pq (è evidente che tale gruppo è isomorfo a G in quanto ρ non commuta con γ perché non appartiene al suo centralizzatore). Per quanto detto possiamo quindi concludere che se $q|p-1$ allora il minimo n tale che S_n ammette un sottogruppo di ordine pq è p.

Esercizio 2. Sia G un gruppo di ordine $20825 = 5^2 \cdot 7^2 \cdot 17$.

1. Mostrare che G contiene un sottogruppo di ordine $1225 = 5^2 \cdot 7^2$.

2. Mostrare che G è abeliano.

Soluzione:

1. Indichiamo con P, Q, R rispettivamente il 5, il 7 e l'11-Sylow di G; questi Sylow sono tutto abeliani per questioni di cardinalià. Osserviamo che P è un sottogruppo normale di G, infatti il numero n_5 dei 5-Sylow di G è congruo a 1 modulo 5 e divide $7^2 \cdot 17$, quindi $n_5 = 1$. Da questo segue che $H = PQ$ è un sottogruppo di G di ordine 1225.

2. Il sottogruppo H è abeliano in quanto Q, che è anche un 7-Sylow di H, è normale in H (il numero dei 7-Sylow di H è congruo a 1 modulo 7 e divide 5^2, quindi è 1), quindi $H \cong P \times Q$ e P e Q commutano elemento per elemento. In particolare sia P che Q sono contenuti nel normalizzatore in G di Q, che denotiamo con $N_G(Q)$, che quindi ha ordine almeno $5^2 \cdot 7^2$. Ora il numero dei 7-Sylow di G è $n_7 = [G : N_G(Q)]$ e questo numero è un divisore di 17 congruo a 1 modulo 7, quindi $n_7 = 1$.

   Consideriamo ora il gruppo $K = PR$: numero dei 17-Sylow di K, è un divisore di 5^2 congruo a 1 modulo 17, quindi R è un sottogruppo normale di K. Questo assicura che $K \cong P \times R$ e che gli elementi di P e R commutano tra loro. Da questa quanto osservato fin qui abbiamo che P è contenuto nel centro di G perché è abeliano e i suoi elementi commutano con quelli di Q e di R e quindi commutano con tutto G poiché P, Q e R generano G. Consideriamo ora il numero dei 17-Sylow di G, $n_{17} = [G : N_G(R)]$. Dato che sia R che P appartengono a $N_G(R)$ si ha che $n_{17} \mid 7^2$ e poiché $n_{17} \equiv 1 \pmod{17}$ si ottiene $n_{17} = 1$.

   Infine, posto $L = QR$ abbiamo $L \cong R \times Q$. Questo mostra che gli elementi di P, Q e R commutano tra loro e quindi sono tutti e tre contenuti nel centro di G. Ne segue che G è abeliano.

Esercizio 3. Sia A un anello commutativo con identità e sia x un'indeterminata su A.

1. Sia $f(x) = \sum_{j=0}^{n} a_j x^j \in A[x]$. Mostrare che $f(x)$ è nilpotente se e solo se $a_0, \ldots, a_n$ sono nilpotenti.

2. Per ogni I ideale di A consideriamo l'insieme $I[x]$ dei polinomi di $A[x]$ con tutti i coefficienti in I. Mostare che $I[x]$ è un ideale di $A[x]$ e che $A[x]/I[x] \cong (A/I)[x]$.

3. Dimostare che $\sqrt{I[x]} = \sqrt{I}[x]$.

Soluzione:

1. Poiché il nilradicale è un ideale, se $a_0, \ldots, a_n$ sono nilpotenti allora $f(x) = \sum_{j=0}^{n} a_j x^j$ è nilpotente. Dimostro il viceversa per induzione sul grado n di $f(x)$. Se $n = 0$ allora $f(x) = a_0$ e l'affermazione è ovvia. Supponiamo che la tesi sia vera per polinomi di grado minore di n, e che $f(x)^d = (\sum_{j=0}^{n} a_j x^j)^d = 0$. Ora $0 = f(x)^d = a_n^d x^{nd} +$ termini di grado inferiore, quindi chiaramente $a_n^d = 0$, cioè a_n è nilpotente. D'altra parte anche il polinomio $g(x) = f(x) - a_n x^n = \sum_{j=0}^{n-1} a_j x^j$ è nilpotente perché differenza di nilpotenti e ha grado minore o uguale a $n-1$, quindi, per ipotesi induttiva, i suoi coefficienti $a_0, \ldots, a_{n-1}$ sono nilpotenti. Questo conclude perché abbiamo già detto che a_n è nilpotente.

2. Consideriamo l'omomorfismo di proiezione $\pi\colon A \to A/I$ e sia $\varphi\colon A[x] \to (A/I)[x]$ l'unico omomorfismo di anelli che estende la proiezione π e tale che $\varphi(x) = x$. Chiaramente φ è surgettivo e $\ker(\varphi) = I[x]$. Questo mostra che $I[x]$ è un ideale e il teorema di omomorfismo dà l'isomorfismo richiesto.

3. Ricordiamo che se R è un anello e J un suo ideale, allora nella corrispondenza tra gli ideali di R che contengono J e gli ideali di R/J, l'ideale $\sqrt{J}$ corrisponde al nilradicale di R/J. In particolare, $\sqrt{I[x]}$ corrisponde al radicale di $A[x]/I[x]$. D'altra parte, per il punto (1), in $(A/I)[x]$ gli elementi nilpotenti sono quelli con coefficienti nilpotenti. Possimo quindi concludere che:
   $f(x) = \sum_{j=0}^{n} a_j x^j \in \sqrt{I[x]} \iff \bar{f}(x)$ è nilpotente in $A[x]/I[x] \iff \varphi(f(x)) = \sum_{j=0}^{n} \pi(a_j) x^j$ è nilpotente in $(A/I)[x] \iff \pi(a_j)$ sono nilpotent in $A/I\ \forall j \iff a_j \in \sqrt{I}\ \forall j \iff f(x) \in \sqrt{I}[x]$.

Esercizio 4. Sia $\mathbb{K}$ il campo $\mathbb{Q}(t)$ ed $f(X)$ il polinomio $X^4 - 2(t^2+1)X^2 + t^2(t^2+1)$.

1. Mostrare che $f(X)$ è irriducibile su $\mathbb{K}$ e descrivere con un insieme di generatori il suo campo di spezzamento L.

2. Calcolare il gruppo di Galois di L su $\mathbb{K}$.

3. Descrivere le estensioni intermedie $\mathbb{K} \subset E \subset L$ e per ciascuna determinare, se esiste, un polinomio $g(X) \in \mathbb{K}[X]$ di cui E è campo di spezzamento.

Soluzione.

1. Il polinomio $t^2 + 1$ è irriducibile e quindi primo in $\mathbb{Q}[t]$. Poiché divide tutti i coefficienti di $f(X)$ a parte quello del termine di grado massimo, ma il suo quadrato non divide il termine costante, per Eisenstein $f(X)$ è irriducibile.

Le radici di $f(X)$ sono

$$\pm\alpha = \pm\sqrt{t^2+1+\sqrt{t^2+1}} \qquad \pm\beta = \pm\sqrt{t^2+1-\sqrt{t^2+1}}$$

e generano $\mathbb{K}$.

2. Le radici α e β soddisfano l'uguaglianza

$$(X^2-\alpha^2)(X^2-\beta^2) = f(X).$$

In particolare $\alpha^2+\beta^2 = 2(t^2+1)$ e $\alpha^2\beta^2 = t^2(t^2+1)$. Dunque $(\alpha^2-\beta^2)^2 = (\alpha^2+\beta^2)^2 - 4\alpha^2\beta^2 = 4[(t^2+1)^2 - t^2(t^2+1)] = 4(t^2+1)$.

Poiché $f(X)$ è irriducibile il gruppo di Galois G agisce transitivamente sull'insieme delle radici. Inoltre l'ordine di G è almeno 4.

Preso un elemento $\sigma \in G$ chiaramente vale $\sigma(-\alpha) = -\sigma(\alpha)$ e $\sigma(-\beta) = -\sigma(\beta)$. Gli elementi di $G \subset S_4$ che soddisfano questa relazione sono un sottogruppo H di ordine 8 isomorfo a D_4. Come permutazioni dell'insieme $\{\alpha, -\alpha, \beta, -\beta\}$ possiamo descrivere così gli elementi di H:

$$\begin{aligned} H = \{&\mathrm{id}, (\alpha,-\alpha)(\beta,-\beta), (\alpha,\beta)(-\alpha,-\beta), (\alpha,-\beta)(-\alpha,\beta),\\ &(\alpha,\beta,-\alpha,-\beta), (\alpha,-\beta,-\alpha,\beta), (\alpha,-\alpha), (\beta,-\beta)\}. \end{aligned}$$

Poiché $(\alpha\beta(\alpha^2-\beta^2))^2 = 4t^2(t^2+1)^2$ è un quadrato in K, $\gamma = \alpha\beta(\alpha^2-\beta^2)$ è in $\mathbb{K}$ e deve essere quindi fissato da ogni elemento di G. Le permutazioni $(\alpha,\beta)(-\alpha,-\beta)$, $(\alpha,-\beta)(-\alpha,\beta)$, $(\alpha,-\alpha)$, $(\beta,-\beta)$, mandano γ in $-\gamma$ e dunque non appartengono a G. Ne segue che G è un gruppo ciclico di ordine 4.

3. G è isomorfo a $\mathbb{Z}_4$ e dunque contiene un solo sottogruppo proprio, che ha ordine 2. Inoltre è facile vedere che L contiene la sottoestensione $E = \mathbb{K}(\sqrt{t^2+1})$. Quindi E è l'unica sottoestensione propria di L. Si vede immediatamente che E è il campo di spezzamento di $X^2 - t^2 - 1$.