COMPITO DI ALGEBRA 1

2 luglio 2019

Soluzioni

1. Sia G un gruppo di ordine $2^k d$, con d dispari e k positivo. Supponiamo che G contenga un unico sottogruppo di ordine 2^k e che questo sottogruppo, che denotiamo P, sia ciclico.

(a) Dimostrare che P è contenuto nel centro di G.

(b) Dimostrare che G contiene un sottogruppo di indice 2.

(c) Dimostrare che G è isomorfo al prodotto diretto $P \times H$ per un opportuno gruppo H di ordine d.

Nota. È possibile usare senza dimostrazione il fatto – visto in classe – che un gruppo di ordine $2d$ con d dispari possiede un sottogruppo di ordine d.

Soluzione: (a) Chiaramente P è l'unico 2-Sylow di G; siccome è unico, è anche normale, e quindi possiamo considerare l'omomorfismo che manda un elemento $g \in G$ nel coniugio per g ristretto a P:

$$\begin{array}{rccc} \Phi: & G & \to & \mathrm{Aut}(P) \\ & g & \mapsto & \begin{pmatrix} P & \to & P \\ p & \mapsto & gpg^{-1} \end{pmatrix} \end{array}$$

Siccome P è abeliano, esso è sicuramente contenuto nel nucleo di Φ, e quindi otteniamo un omomorfismo $G/P \to \mathrm{Aut}(P)$, dove $|G/P| = d$ è dispari. D'altro canto, $\mathrm{Aut}(P) \cong \mathrm{Aut}(\mathbb{Z}/2^k\mathbb{Z}) \cong \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$ ha ordine $\varphi(2^k) = 2^{k-1}$, che è una potenza di 2, quindi l'immagine di Φ ha ordine 1 (perché tale ordine è un divisore tanto di d quanto di 2^k). Questo significa che Φ è l'omomorfismo banale, ovvero che ogni coniugio agisce banalmente su P, e quindi che P è contenuto nel centro.

(b) Procediamo per induzione su k. Il caso $k = 1$ è stato dimostrato in classe. Supponiamo ora di aver dimostrato la tesi fino a k e mostriamola per $k+1$. Per il teorema di Cauchy, G contiene un elemento g di ordine 2. Tale elemento è certamente contenuto in P, dunque è centrale, e quindi possiamo considerare il quoziente $\pi : G \to G/\langle g \rangle =: K$. Il gruppo K ha ordine $|G|/2 = 2^k d$, dunque un suo 2-Sylow deve avere ordine 2^k, e d'altro canto $P/\langle g \rangle$ ha anch'esso ordine 2^k, quindi il 2-Sylow di K è l'immagine in K del 2-Sylow di G. Siccome l'immagine di un gruppo ciclico tramite un omomorfismo è ciclica, otteniamo che K soddisfa le ipotesi del problema (con esponente k) e quindi, per ipotesi induttiva, contiene un sottogruppo N di indice 2. Allora $\pi^{-1}(N)$ è un sottogruppo di G di indice 2, il che prova la tesi.

(c) Dal punto precedente, G contiene un sottogruppo G_1 di indice 2 (e quindi cardinalità $2^{k-1}d$). Il 2-Sylow di G_1 è contenuto nel 2-Sylow di G, dunque è ciclico, e siccome è contenuto nel centro di G è a maggior ragione contenuto nel centro di G_1. Possiamo quindi applicare nuovamente il punto precedente per ottenere un sottogruppo G_2 di indice 2 in G_1, e procedere induttivamente fino ad ottenere un sottogruppo H di G di ordine d.

Chiaramente $P \cap H$ è banale, perché il suo ordine divide sia $2^k = |P|$ che $d = |H|$, e P è normale come visto al punto (a). Ne segue che HP è un sottogruppo di G di ordine $|H| \cdot |P|/|H \cap P| = 2^k d = |G|$. Abbiamo quindi tutti gli ingredienti per dedurre che $G \cong P \rtimes H$; tuttavia, siccome P è contenuto nel centro, l'azione di coniugio di H su P è banale, e quindi questo è in realtà un prodotto diretto.

2. Sia G un gruppo di ordine $8p^2$, dove p è un numero primo. Dimostrare che G non è semplice.

SOLUZIONE: Se $p = 2$, allora G è un 2-gruppo, e quindi possiede sottogruppi normali per ogni ordine che divide l'ordine del gruppo.

Se $p \neq 2$ consideriamo un p-Sylow P, che quindi ha ordine p^2. Per i teoremi di Sylow, P può non essere un sottogruppo normale di G solo se esiste un divisore di 8 diverso da 1 e congruo a 1 modulo p, cioè se $p = 3, 7$.

$p = 7$: P è un sottogruppo di G di indice 8, quindi G agisce sulle 8 classi laterali sinistre di P tramite la moltiplicazione a sinistra, cioè tramite la mappa $G \ni x \mapsto (gP \to xgP)$. Questa azione è ovviamente transitiva, quindi il suo nucleo è diverso da G. D'altra parte la sua immagine è contenuta in $\mathcal{S}_8$ e, siccome $9 \cdot 7^2 \nmid 8!$, l'azione non può essere iniettiva. Ne segue che il nucleo dell'azione è un sottogruppo normale di G non banale, e quindi G non è semplice.

$p = 3$: se P non è un sottogruppo normale di G, allora, sempre per i teoremi di Sylow, P ha esattamente 4 sottogruppi coniugati. Questo significa che, detto $N = N(P)$ il normalizzatore di P in G, si ha $[G : N] = 4$. Consideriamo quindi, analogamente a prima, l'azione di G sulle 4 classi laterali di N: di nuovo il nucleo dell'azione non può essere tutto G e non può essere solo l'identità, in quanto $8 \cdot 3^2 \nmid 4!$.

3. Sia A un dominio ad ideali principali.

(a) Dimostrare che ogni ideale primo P di $A[X]$ tale che $P \cap A = \{0\}$ è principale.

(b) Sia I un ideale di $A[X]$ tale che $I \cap A = (m)$ dove $m \neq 0$ è "libero da quadrati", ossia prodotto di primi distinti. Dimostrare che I può essere generato da al più 2 elementi.

SOLUZIONE: Nel corso della soluzione useremo tacitamente il fatto che un dominio a ideali principali è anche un dominio a fattorizzazione unica.

(a) Se $P = \{0\}$ non c'è niente da dimostrare, Supponiamo dunque $P \neq \{0\}$, e sia $f(X) \in P \setminus \{0\}$ un polinomio in P diverso da zero di grado minimo. Scriviamo $f(X) = cf_1(X)$, dove c è il contenuto di $f(X)$ e $f_1(X)$ è un polinomio primitivo. Poiché P è primo e $c \notin P$, si ha $f_1(x) \in P$, e quindi possiamo supporre $f(X) = f_1(X)$ primitivo.

Sia ora $g(X)$ un altro polinomio appartenente a P e sia K il campo dei quozienti di A. Effettuando la divisione euclidea di $g(X)$ per $f(X)$ in $K[X]$ otteniamo due polinomi $q(X), r(X) \in k[X]$ tali che $g(x) = q(X)f(X) + r(X)$. Moltiplicando poi quest'uguaglianza per una costante opportuna in modo da eliminare i denominatori, otteniamo $G(X) = Q(X)f(x) + R(X)$ per opportuni polinomi $G, Q, R \in A[X]$ dello stesso grado, rispettivamente, di g, q, r. Poiché evidentemente $R(X) \in P$, per la nostra ipotesi sulla minimalità del grado di $f(X)$ otteniamo $R(X) = r(X) = 0$, ossia $f(X) \mid g(X)$ in $K[X]$. Ma poiché $f(X)$ è primitivo, per il lemma di Gauss otteniamo che $f(X) \mid g(X)$ in $A[X]$, ossia $g(X)$ appartiene all'ideale generato da $f(X)$, e quindi $P \subseteq (f(X))$. L'altra inclusione è ovvia.

(b) Sia $m = p_1 \cdots p_r$, dove $p_1, \dots p_r$ sono primi distinti. Gli ideali I contenenti (m) corrispondono in maniera biunivoca, tramite la proiezione canonica, agli ideali $\bar{I}$ di $A[X]/(m) \cong A/(m)[X]$ (quest'ultimo isomorfismo si ottiene facilmente considerando l'omomorfismo di proiezione $A[X] \to A/(m)[X]$ e verificando che il nucleo è proprio l'ideale generato da m).

Per il teorema cinese del resto $A/(m) \cong A/(p_1) \times \cdots A/(p_r)$ e, similmente,

$$A/(m)[X] \cong A/(p_1)[X] \times \cdots \times A/(p_r)[X]\,.$$

Ora ricordiamo che: (i) in un dominio a ideali principali ogni ideale primo diverso da zero è massimale, quindi $K_1 = A/(p_1), \dots, K_r = A/(p_r)$ sono campi e $K_1[X], \dots, K_r[X]$ sono domini ad ideali principali; (ii) nel prodotto di anelli ogni ideale è prodotto di ideali dei singoli fattori, quindi $A/(m)[X]$ è a ideali principali.

Sia dunque I un ideale di $A[X]$ contenente (m), e sia $\bar{f}(X)$ un generatore dell'ideale $\bar{I}$ che gli corrisponde. Detto $f(X)$ un polinomio di $A[X]$ la cui proiezione è $\bar{f}(X)$ si ha che $I = (m, f(X))$: infatti, se $g(X) \in I$ e $\bar{g}(X)$ è la sua proiezione si ha che esiste $\bar{h}(X) \in A/(m)[X]$ tale che $\bar{g}(X) = \bar{h}(X)\bar{f}(X)$ e quindi, detto $h(x) \in A[X]$ un polinomio la cui proiezione è $\bar{h}(X)$, esiste $l(X) \in A[X]$ tale che $g(x) = ml(x) + h(x)f(x)$. Ancora una volta, l'altra inclusione è ovvia.

4. Sia $g(x) \in \mathbb{F}_2[x]$ il polinomio $g(x) = x^4 + x + 1$ e sia β una radice di $g(x)$ in una opportuna estensione di $\mathbb{F}_2$. Determinare, per ogni $n \geq 1$, il grado di $\mathbb{F}_2(\beta^n)$ su $\mathbb{F}_2$.

Soluzione:

Osserviamo innanzitutto che $g(x)$ è irriducibile, in quanto non ha radici (verifica immediata) e non si può neppure scomporre come prodotto di due fattori irriducibili di grado 2: in effetti, l'unico polinomio irriducibile di grado 2 in $\mathbb{F}_2[x]$ è x^2+x+1, e $(x^2+x+1)^2 = x^4+x^2+1$ è diverso da $g(x)$. Ne segue che $\mathbb{F}_2(\beta)$ è un'estensione di grado 4 di $\mathbb{F}_2$, e per quanto sappiamo dalla teoria dei campi finiti si ha $\mathbb{F}_2(\beta) = \mathbb{F}_{2^4}$. In particolare, β è un elemento del gruppo moltiplicativo $\mathbb{F}_{2^4}^\times$, che è un gruppo ciclico con 15 elementi. Ne segue quindi che $\beta^{15} = 1$. Dimostriamo ora che l'ordine moltiplicativo di β è proprio 15. Certamente l'ordine di β è un divisore di 15, e non può essere né 1 né 3, perché in tal caso si avrebbe rispettivamente $\beta = 1$ (e quindi $\beta \in \mathbb{F}_2$) o $\beta^3 = 1 \Rightarrow \beta^4 = \beta$ (e quindi $\beta \in \mathbb{F}_4$). Infine, se si avesse $\beta^5 = 1$, l'elemento β sarebbe una radice tanto del polinomio $g(x)$ quanto del polinomio $x^5-1 = (x-1)(x^4+x^3+x^2+x+1)$. Siccome $\beta \neq 1$, i polinomi $x^4+x^3+x^2+x+1$ e x^4+x+1 avrebbero la radice β in comune, e β sarebbe quindi anche radice della loro differenza x^3+x^2. Ma questo è assurdo, perché tutte le radici di x^3+x^2 sono in $\mathbb{F}_2$ mentre β non lo è. Abbiamo così dimostrato che l'ordine di β è 15, ovvero che β è un generatore di $\mathbb{F}_{2^4}^\times$. Adesso:

(a) se $(n, 15) = 1$, allora β^n è ancora un generatore di $\mathbb{F}_{2^4}^\times$, e quindi $\mathbb{F}_2(\beta^n) = \mathbb{F}_{2^4}$ ha grado 4 su $\mathbb{F}_2$.

(b) se $15 \mid n$, allora $\beta^n = 1$ e $\mathbb{F}_2(\beta^n) = \mathbb{F}_2$ ha grado 1 su $\mathbb{F}_2$.

(c) se $5 \mid n$ ma $3 \nmid n$, allora $\alpha := \beta^n$ è un elemento di ordine esattamente 3, e come tale rispetta $\alpha^4 = \alpha$. Questo implica che $\alpha \in \mathbb{F}_4$, e viceversa $\alpha \notin \mathbb{F}_2$ perché $\mathbb{F}_2^\times$ non contiene elementi di ordine 3. Ne segue quindi che $\mathbb{F}_2(\beta^n) = \mathbb{F}_4$ ha grado 2 su $\mathbb{F}_2$.

(d) infine, se $3 \mid n$ ma $5 \nmid n$, allora β^n è un elemento di ordine esattamente 5, e quindi non può stare né in $\mathbb{F}_2$ né in $\mathbb{F}_4$ (i cui gruppi moltiplicativi hanno ordine rispettivamente 1 e 3). D'altro canto β^n appartiene certamente a $\mathbb{F}_{2^4}$, perché $\beta \in \mathbb{F}_{2^4}$, e quindi $\mathbb{F}_2(\beta^n) = \mathbb{F}_{2^4}$ ha grado 4 su $\mathbb{F}_2$.