COMPITO DI ALGEBRA 1

22 gennaio 2019

Soluzioni

1. Un sottogruppo K di S_n è detto *transitivo* se per ogni coppia i, j di interi in $\{1, \dots, n\}$ esiste $\sigma \in K$ tale che $\sigma(i) = j$.

(a) Sia p un numero primo e G un sottogruppo di S_p. Dimostrare che G è transitivo se e solo se $p \mid \#G$.

(b) Sia G un sottogruppo transitivo di S_p (con p primo) e H un sottogruppo normale di G diverso dalla sola identità. Dimostrare che H è un sottogruppo transitivo di S_p.

SOLUZIONE:

(a) Consideriamo l'azione naturale di $G < S_p$ sull'insieme $X = \{1, \dots, p\}$. Se G è transitivo, allora l'orbita di $1 \in X$ è tutto X, dunque il lemma orbita-stabilizzatore fornisce

$$\#G = \#\operatorname{Orb}(1) \cdot \#\operatorname{Stab}(1) = p \cdot \#\operatorname{Stab}(1),$$

da cui $p \mid \#G$ come voluto. Viceversa, se $p \mid \#G$, allora per il teorema di Cauchy G contiene un elemento di ordine p, che – essendo in particolare un elemento di S_p – è necessariamente un p-ciclo. D'altro canto l'azione di un p-ciclo su $\{1, \dots, p\}$ è per definizione transitiva, quindi a maggior ragione G è transitivo.

(b) Dal punto precedente sappiamo che G contiene un p-ciclo; a meno di un automorfismo di S_p, possiamo supporre che $g = (1, 2, \dots, p) \in G$. Identifichiamo per semplicità l'insieme $\{1, \dots, p\}$ all'insieme dei possibili resti modulo p e notiamo che l'azione delle potenze di g su un elemento i è data da $g^r(i) = i + r$, dove l'uguaglianza va intesa come congruenza modulo p.

Sia $h \in H$ un qualunque elemento non banale (che esiste per ipotesi): siccome h è diverso dall'identità, c'è almeno un intero in $\{1, \dots, p\}$ che non è fissato da h, ovvero esiste $a \in \{1, \dots, p\}$ tale che $h(a) = a + k$ con $k \not\equiv 0 \pmod{p}$. Sia ora b un qualunque elemento di $\{1, \dots, p\}$. Siccome H è un sottogruppo normale di G, esso contiene anche $g^{b-a} h g^{a-b}$, la cui azione su b è data da

$$g^{b-a} h g^{a-b}(b) = g^{b-a}(h(b + (a - b))) = g^{b-a}(h(a)) = g^{b-a}(a + k) = b + k.$$

Ne segue che per ogni $b \in \{1, \dots, p\}$ i numeri b e $b + k$ sono nella stessa orbita per l'azione di H. Un'induzione immediata mostra quindi che $1, 1 + k, 1 + 2k, \dots$ sono

tutti nella stessa orbita; ma siccome $(k,p)=1$, queste sono tutte le classi di resto modulo p, ovvero l'azione di H su $\{1,\dots,p\}$ è transitiva.

Seconda soluzione:

(b) Consideriamo l'azione di H su X. Dimostriamo che tutte le orbite hanno la stessa cardinalità. Siano infatti $a,b\in X$ due elementi qualunque: allora per ipotesi esiste $g\in G$ tale che $b=g(a)$. Consideriamo inoltre i sottogruppi $\mathrm{Stab}_H(a)=\{h\in H : h\cdot a=a\}$ e $\mathrm{Stab}_H(b)=\{h\in H : h\cdot b=b\}$ di H. Mostriamo che si ha

$$h\in \mathrm{Stab}_H(a) \Leftrightarrow ghg^{-1}\in \mathrm{Stab}_H(b).$$

In effetti, se $h\in \mathrm{Stab}_H(a)$ si ha $(ghg^{-1})(b)=g(h(a))=g(a)=b$, dunque la permutazione ghg^{-1} stabilizza b; l'ipotesi che H sia normale in G garantisce inoltre che ghg^{-1} sia un elemento di H, e dunque un elemento di $\mathrm{Stab}_H(b)$. L'altra implicazione si dimostra in maniera del tutto analoga.

Questo dimostra che $\mathrm{Stab}_H(a)$ e $\mathrm{Stab}_H(b)$ sono coniugati (in G), e quindi in particolare hanno la stessa cardinalità. D'altro canto, dal lemma orbita-stabilizzatore segue

$$\#H=\#\,\mathrm{Orb}(a)\cdot\#\,\mathrm{Stab}_H(a)=\#\,\mathrm{Orb}(b)\cdot\#\,\mathrm{Stab}_H(b),$$

da cui (siccome $\#\,\mathrm{Stab}_H(a)=\#\,\mathrm{Stab}_H(b)$) si ottiene come voluto $\#\,\mathrm{Orb}(a)=\#\,\mathrm{Orb}(b)$. Sia allora ℓ la lunghezza di un'orbita e r il numero di orbite: si ha $r\ell=\#X=p$, da cui $r=1$ o $r=p$. Se $r=1$ c'è una sola orbita, che è la tesi. Se invece $r=p$ ogni orbita ha lunghezza $\ell=1$, ovvero per ogni $i\in\{1,\dots,p\}$ e ogni $h\in H$ si ha $h(i)=i$: ma in tal caso h è necessariamente l'identità, e quindi H è il sottogruppo banale, escluso per ipotesi.

2. Sia G un gruppo finito, sia P un suo sottogruppo di Sylow, e siano $a,b\in Z(P)$ e $g\in G$ elementi che soddisfano la relazione $b=gag^{-1}$.

Dimostrare che:

(a) P e gPg^{-1} sono contenuti in $Z(b)$;

(b) esiste un elemento $u\in N(P)$ tale che $uau^{-1}=b$.

Nota: Per ogni sottoinsieme S di G indichiamo con $Z(S)$ il suo centralizzatore, ossia $Z(S)=\{x\in G \mid xs=sx\ \forall s\in S\}$ e con $N(S)$ il suo normalizzatore, ossia $N(S)=\{x\in G \mid xsx^{-1}\in S\ \forall s\in S\}$.

Soluzione: (a) Osserviamo che, in generale, per ogni $g\in G$ e per ogni sottogruppo H di G, si ha $gZ(H)g^{-1}=Z(gHg^{-1})$, facendo vedere la doppia inclusione.

Se $x\in Z(H)$, allora, per ogni $h\in H$ si ha $gxg^{-1}\cdot ghg^{-1}=gxhg^{-1}=ghxg^{-1}=ghg^{-1}\cdot gxg^{-1}$, e quindi $gxg^{-1}\in Z(ghg^{-1})$ per ogni $h\in H$.

Viceversa, se $x \in Z(ghg^{-1})$ per ogni $h \in H$, allora $g^{-1}xg \cdot h = g^{-1}(x \cdot ghg^{-1})g = g^{-1}(ghg^{-1} \cdot x)g = h \cdot g^{-1}xg$, e quindi $g^{-1}xg \in Z(h)$, ossia $x \in gZ(h)g^{-1}$, per ogni $h \in H$.

Per concludere, il fatto che $b \in Z(P)$ significa che $P \subseteq Z(b)$, e il fatto che $a \in Z(P)$ significa che $b = gag^{-1} \subseteq gZ(P)g^{-1} = Z(gPg^{-1})$, ossia $gPg^{-1} \subseteq Z(b)$.

(b) Poiché P e gPg^{-1} sono sottogruppi di Sylow di G e sono contenuti in $Z(b)$, essi sono anche sottogruppi di Sylow di $Z(b)$. Per i teoremi di Sylow, essi sono coniugati in $Z(b)$, ossia esiste $y \in Z(b)$ tale che $yPy^{-1} = gPg^{-1}$. Altrimenti detto, $y^{-1}gP(y^{-1}g)^{-1} = P$. Consideriamo l'elemento $u = y^{-1}g$. L'equazione precedente dice che $u \in N(P)$. D'altra parte,

$$uau^{-1} = y^{-1}gag^{-1}y = y^{-1}by = b\,,$$

come richiesto.

3. Sia $p > 2$ un numero primo e sia

$$A = \left\{ \frac{a + b\sqrt{-p}}{2^m} \mid a, b \in \mathbb{Z},\ m \in \mathbb{N} \right\}.$$

(a) Dimostrare che A^* è l'insieme degli elementi $\frac{a+b\sqrt{-p}}{2^m} \in A$ per cui $a^2 + b^2p = 2^k$ per qualche $k \in \mathbb{N}$.

(b) Dimostrare che, se $\alpha = a + b\sqrt{-p}$ è un elemento di A tale che $a^2 + b^2p$ è un numero primo di $\mathbb{Z}$, allora α è un elemento primo di A.

Soluzione (a) Supponiamo che $a^2+b^2p = 2^k$. Poiché $\frac{a-b\sqrt{p}}{2^{m-k}} \in A$ e $\frac{a+b\sqrt{p}}{2^m} \cdot \frac{a-b\sqrt{p}}{2^{k-m}} = 1$, si ha che $\frac{a+b\sqrt{-p}}{2^m} \in A^*$.

Viceversa, supponiamo che $\frac{a+b\sqrt{-p}}{2^m} \in A^*$. Siccome 2 è invertibile in A, ci possiamo ricondurre al caso in cui $m = 0$ e a, b non siano entrambi pari. Se (a, b) è un numero dispari $d > 1$, allora anche d è invertibile, cioè $\frac{1}{d} \in A$, assurdo. Analogamente, (a, p) non può essere uguale a p, perchè altrimenti $\sqrt{-p}$ sarebbe invertibile (di nuovo assurdo). Quindi $(a, b) = (a, p) = 1$ e l'inverso di $a + b\sqrt{-p}$ in $\mathbb{C}$, cioè $\frac{a-b\sqrt{-p}}{a^2+b^2p}$, è una frazione ridotta ai minimi termini. Perché l'inverso di $a + b\sqrt{-p}$ appartenga ad A è dunque necessario che $a^2 + b^2p$ sia una potenza di 2.

(b) Trattiamo separatamente il caso $a = 0$. In tal caso, se $a^2 + b^2p = b^2p$ è un numero primo, si ha necessariamente $b = \pm 1$, e vogliamo allora dimostrare che l'ideale $(\sqrt{-p})$ è primo. Sia $B = S^{-1}\mathbb{Z}$ con $S = \{2^m : m \in \mathbb{N}\}$. È allora chiaro che $A = B[x]/(x^2 + p)$ (con x che corrisponde a $\sqrt{-p}$), da cui

$$\frac{A}{(\sqrt{-p})} \cong \frac{B[x]}{(x^2 + p, x)} = \frac{B[x]}{(p, x)} \cong \frac{B}{(p)}.$$

Siccome p è un primo *dispari*, l'ideale (p) di $\mathbb{Z}$ non incontra l'insieme S, e quindi $S^{-1}(p)$ è un ideale primo di B: questo implica che $\frac{B}{(p)}$ è un dominio, quindi lo stesso vale per $\frac{A}{(\sqrt{-p})}$, e quindi $(\sqrt{-p})$ è un ideale primo come voluto.

Nel caso $b = 0$ il numero $a^2 + pb^2 = a^2$ non è mai un numero primo, quindi possiamo ora supporre $a \neq 0, b \neq 0$. Supponiamo ancora che $a^2 + b^2 p = q$ sia un numero primo. Ovviamente si ha $(a, b) = 1$: mostriamo che in effetti $(a, pb) = 1$. Per quanto già osservato è sufficiente dimostrare che p non divide a; se per assurdo p dividesse a, si otterrebbe $p \mid a^2 + b^2 p = q$, quindi $q = p$, da cui $p = a^2 + b^2 p \geq 1 + 1 \cdot p > p$, assurdo. Consideriamo gli ideali $I = (a + b\sqrt{-p})$ e $J = (a - b\sqrt{-p})$. L'ideale $I + J$ contiene $(2a, 2b\sqrt{-p})$ e, poiché 2 è invertibile, contiene $(a, b\sqrt{-p})$. Ma allora $I + J$ contiene anche a e $pb = -b\sqrt{-p} \cdot \sqrt{-p}$, e per quanto visto sopra questo implica $1 \in I + J$, cioè $I + J = A$. Applicando il teorema cinese per anelli abbiamo

$$A/IJ = A/(q) \cong A/I \times A/J\,.$$

Ora $A/(q)$ ha q^2 elementi e, siccome A/I ed A/J sono evidentemente isomorfi, essi hanno entrambi q elementi. Ne segue che $A/I \cong \mathbb{Z}/q\mathbb{Z}$ è un dominio di integrità e quindi I è un ideale primo di A (anzi è massimale).

4. Sia $p(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado $n \geq 3$ e sia K il suo campo di spezzamento su $\mathbb{Q}$. Supponiamo che $\mathrm{Gal}(K/\mathbb{Q})$ sia isomorfo a S_n. Sia poi $m \geq 3$ un intero ed $L = K \cap \mathbb{Q}(\zeta_m)$.

(a) Dimostrare che $[L : \mathbb{Q}] \leq 2$.

(b) Dimostrare che $p(x)$ è irriducibile in $L[x]$.

(c) Dimostrare che $p(x)$ è irriducibile in $\mathbb{Q}(\zeta_m)[x]$.

Soluzione:

(a) In quanto intersezione di estensioni di Galois, L è un'estensione di Galois di $\mathbb{Q}$, e dal teorema di corrispondenza di Galois sappiamo che $H = \mathrm{Gal}(L/\mathbb{Q})$ è un quoziente sia di $\mathrm{Gal}(K/\mathbb{Q}) \cong S_n$, sia di $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. In particolare, H è un gruppo abeliano, il che vuol dire che il nucleo dell'omomorfismo $\varphi : S_n \to H$ contiene il sottogruppo derivato di S_n, che come noto è A_n. Ne segue che l'indice di $\ker\varphi$ in S_n è al massimo 2 (dato che $[S_n : A_n] = 2$) e quindi $|H| = |\frac{S_n}{\ker\phi}| \leq 2$. Siccome $|H| = [L : \mathbb{Q}]$ questo dimostra la tesi.

(b) Il campo di spezzamento di $p(x)$ su L è ancora K; dall'analisi del punto precedente sappiamo che $\mathrm{Gal}(K/L) \cong S_n$ o A_n. Si può allora procedere in due modi:

- o si ricorda il criterio che afferma che, data una sottoestensione $L/\mathbb{Q}$ del campo di spezzamento di $p(x) \in \mathbb{Q}[x]$, il polinomio $p(x) \in L[x]$ è irriducibile se e solo se

$\mathrm{Gal}(K/L)$ agisce transitivamente sulle radici di $p(x)$ (cosa che è ovvia nel nostro caso, sia per A_n che per S_n);

- oppure si osserva che se $p(x) \in L[x]$ si fattorizzasse come $p_1(x)p_2(x)$ con $\deg p_1(x) = a \geq 1$, $\deg p_2(x) = b \geq 1$, allora il campo di spezzamento di $p(x)$ su L avrebbe grado al più $a!b!$, che è strettamente minore di $\#A_n = \frac{n!}{2} = \frac{(a+b)!}{2}$. Per mostrare questa disuguaglianza basta osservare che essa è equivalente a $2 < \binom{a+b}{a}$, che è essenzialmente ovvia (ad esempio perché $\binom{a+b}{a} \geq \binom{a+b}{1} = a + b = n > 2$).

(c) Il campo di spezzamento di $p(x)$ su $\mathbb{Q}(\zeta_m)$ è $K\mathbb{Q}(\zeta_m)$; osservando che l'estensione $K\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)$ è uno shift di $K/\mathbb{Q}$ si ha

$$\mathrm{Gal}(K\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)) \cong \mathrm{Gal}(K/K \cap \mathbb{Q}(\zeta_m)) = \mathrm{Gal}(K/L),$$

quindi si applicano i medesimi argomenti del punto (b).