A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
SOLUZIONE ESERCIZI FOGLIO 8.

Esercizio 8.1. Siano n, $m \in \mathbb{N}$ due numeri naturali tali che $\mathrm{MCD}(n,m) = 1$; dimostrare che il gruppo $\mathbb{Z}_n \times \mathbb{Z}_m$ è un gruppo ciclico.

Soluzione. Per l'esercizio è sufficiente ragionare come nel caso dell'esercizio 3.6. Siano m, $n \in \mathbb{N}$. Sia G un gruppo e siano g, $h \in G$, $\langle g\rangle \cap \langle h\rangle = 1_G$ due elementi tali che $o(g) = n$, $o(h) = m$ e $g\,h = h\,g$. Mostriamo che $o(g\,h) = \mathrm{mcm}(m,n)$. Da un lato è chiaro che $o(g\,h) \,|\, \mathrm{mcm}(m,n)$ infatti

$$(g\,h)^{\mathrm{mcm}(m,n)} = g^{\mathrm{mcm}(m,n)} h^{\mathrm{mcm}(m,n)} = 1_G$$

Facciamo ora vedere che $\mathrm{mcm}(m,n) \,|\, o(g\,h)$. Osserviamo che $1_G = (g\,h)^{o(g\,h)} = g^{o(g\,h)} h^{o(g\,h)}$, in particolare deve risultare $g^{o(g\,h)} = 1_G$ e $h^{o(g\,h)} = 1_G$ che $n \,|\, o(g\,h)$ e $m \,|\, o(g\,h)$; ma allora $\mathrm{mcm}(n,m) \,|\, o(g\,h)$.

A questo punto risolvere l'esercizio è molto semplice. Abbiamo un gruppo $\mathbb{Z}_n \times \mathbb{Z}_m$ abeliano. Prendiamo $(\overline{1},\overline{0})$ e $(\overline{0},\overline{1})$. Il primo elemento è un generatore di $\mathbb{Z}_n$ ed ha ordine n, mentre il secondo è un generatore di $\mathbb{Z}_m$ ed ha ordine m. Osserviamo inoltre che $\langle(\overline{1},\overline{0})\rangle \cap \langle(\overline{0},\overline{1})\rangle = (\overline{0},\overline{0})$ e dunque ne deduciamo che $o((\overline{1},\overline{1})) = \mathrm{mcm}(m,n)$; ma stiamo supponendo $\mathrm{MCD}(m,n) = 1$ e pertanto $\mathrm{mcm}(m,n) = m \cdot n$. D'altra parte il gruppo $\mathbb{Z}_n \times \mathbb{Z}_m$ ha cardinalità $n \cdot m$ e poiché $\langle(\overline{1},\overline{1})\rangle < \mathbb{Z}_n \times \_m$ è un sottogruppo della stessa cardinalità del gruppo esso deve coincidere con il gruppo stesso, che pertanto è ciclico generato da $(\overline{1},\overline{1})$. □

Esercizio 8.2. Determinare le possibili strutture cicliche ed i possibili ordini degli elementi di S_7.

Soluzione. Ricordiamo la definizione di struttura ciclica. Sia $\gamma \in S_7$. Sappiamo che γ può essere scritta come prodotto di cicli disgiunti. La struttura ciclica di γ è semplicemente un vettore con le lunghezze in ordine crescente delle lunghezze della sua scomposizione in cicli disgiunti (contate con le molteplicità i.e. $(1\,2)(3\,4)$ ha struttura ciclica $(2,2)$). Si osservi che se $(k_1,..,k_m)$ è la struttura ciclica di un elemento di S_n allora necessariamente $k_1 + \cdots + k_m \leq n$.
Tenendo a mente queste cose ecco le possibili strutture cicliche di S_7:
Identità.
(1)
Strutture cicliche contenenti almeno una trasposizione.
(2) ; $(2,2)$; $(2,2,2)$; $(2,3)$; $(2,2,3)$; $(2,4)$; $(2,5)$;
Strutture cicliche senza trasposizioni ma contenenti almeno un 3-ciclo.
(3) ; $(3,3)$; $(3,4)$;
Strutture cicliche contenenti solo k-cicli con $k \geq 4$.
(4) ; (5) ; (6) ; (7) .
Calcoliamo gli ordini degli elementi corrispondenti ad una data struttura ciclica; impropriamente scriverò $o((k_1,..,k_m))$ per indicare l'ordine di un generico elemento $\gamma \in S_7$ che ha $(k_1,..,k_m)$ come struttura ciclica: $o((k)) = k$, $o((2,2)) = 2$, $o((2,2,2)) = 2$, $o((2,3)) = 6$, $o((2,2,3)) = 6$, $o((2,4)) = 4$, $o((2,5)) = 10$, $o((3,3)) = 3$, $o((3,4)) = 12$. Notare che per calcolare gli ordini degli elementi abbiamo usato il fatto che cicli disgiunti commutano ed il fatto preliminare dimostrato nell'esercizio 8.1. □

Esercizio 8.3. Consideriamo il gruppo diedrale D_n. Numeriamo da 1 ad n i vertici (che chiameremo dunque v_1,...,v_n) dell'n-gono regolare, $\mathcal{P}_n$, procedendo in senso antiorario e denotiamo con ℓ_i il lato dell' n-gono regolare compreso tra v_i e v_{i+1} per $i = 1,..,n-1$ ed ℓ_n il lato compreso tra v_n e v_1.
Denotiamo con $\rho_{\frac{2\pi}{n}}$ la rotazione di $\frac{2\pi}{n}$ intorno all'origine e denotiamo con $\sigma_{\ell,\,i}$ e $\sigma_{v,\,i}$ rispettivamente le

riflessioni rispetto agli assi dei lati ℓ_i e rispetto alle rette contenenti $\overline{ov_i}$ (o è l'origine del piano euclideo).

(A) Dimostrare che se n è dispari allora per $j(i,n)$ uguale ad un rappresentante compreso tra 1 ed n della classe resto modulo n di $\frac{n-1}{2}+i$ si ha: $\sigma_{v,\,i}=\sigma_{\ell,\,j(i,n)}$.
(B) Dimostrare che se n è dispari allora $\sigma_{v,\,j(i,n)}\circ\sigma_{v,\,i}=\rho_{\frac{2\pi}{n}}$ mentre $\sigma_{v,\,i+1}\circ\sigma_{v,\,i}=\rho_{\frac{4\pi}{n}}$.
(C) Dimostrare che se n è pari ogni $\{\sigma_{v,\,i},\,\sigma_{\ell,j}\}_{i,j=1}^{\frac{n}{2}}$ costituisce un insieme di isometrie di $\mathcal{P}_n$ a due a due distinte. Dimostrare che $\sigma_{\ell,\,i}\circ\sigma_{v,\,i}=\rho_{\frac{2\pi}{n}}$.

Soluzione. Cominciamo con il punto (A). Si osservi che per n dispari dato l'n-gono regolare, $\mathcal{P}_n$, la bisettrice dell'angolo relativo ad un vertice v coincide con la mediana del lato opposto. L'unica cosa da verificare dunque è che, numerati vertici e lati di $\mathcal{P}_n$ come specificato nel testo dell'esercizio, si ha $\ell_{j(i,n)}$ è effettivamente il lato opposto al vertice v_i. Notiamo quindi che dato il vertice v_i il lato opposto è l' $(\frac{n-1}{2}+1)$-simo lato dopo v_i (percorrendo il poligono in senso antiorario). Poiché la numerazione dei lati va da 1 ad n risulta che l'indice da assegnare al lato è un rappresentante compreso tra 1 ed n del numero $i+\frac{n-1}{2}$, ovvero l'indice $j(i,n)$. Dato che l'asse del segmento $\ell_{j(i,n)}$ coincide con la bisettrice di $\mathcal{P}_n$ nel vertice v_i ne ricaviamo che $\sigma_{\ell,\,j(i,n)}=\sigma_{v_i}$.

Per quanto riguarda (B) notiamo che $\sigma_{v,j(i,n)}$ è la riflessione rispetto al vertice iniziale del lato $\ell_{j(i,n)}$; d'altra parte abbiamo dimostrato nel punto (A) che $\sigma_{\ell,j(i,n)}=\sigma_{v,i}$, pertanto la composizione $\sigma_{v,j(i,n)}\circ\sigma_{v,i}$ può anche essere scritta come la composizione $\sigma_{v,j(i,n)}\circ\sigma_{\ell,j(i,n)}$. Per dimostrare che quest'ultima è uguale a $\rho_{-\frac{2\pi}{n}}$ ci è sufficiente provare che la coppia di vertici $(v_{j(i,n)},v_{j(i,n)+1})$ viene inviata dalla nostra trasformazione in $(v_{j(i,n)-1},v_{j(i,n)})$, infatti trattandosi di isometrie che fissano l'origine è sufficiente sapere dove viene inviata una coppia di vertici. Ora $\sigma_{\ell,j(i,n)}(v_{j(i,n)})=v_{j(i,n)+1}$ e $\sigma_{\ell,j(i,n)}(v_{j(i,n)+1})=v_{j(i,n)}$, componendo quindi con $\sigma_{v,j(i,n)}$ abbiamo che: $(\sigma_{v,j(i,n)}\circ\sigma_{\ell,j(i,n)})(v_{j(i,n)})=\sigma_{v,j(i,n)}(v_{j(i,n)+1})=v_{j(i,n)-1}$ mentre $(\sigma_{v,j(i,n)}\circ\sigma_{\ell,j(i,n)})(v_{j(i,n)+1})=\sigma_{v,j(i,n)}(v_{j(i,n)})=v_{j(i,n)}$. Dunque l'azione di tale elemento sulla coppia coincide con quella della trasformazione $\rho_{-\frac{2\pi}{n}}$ in particolare le due trasformazioni coincidono sulla terna di punti non allineati $(o,v_{j(i,n)},v_{j(i,n)+1})$; due isometrie del piano che coincidono su tre punti non allineati sono la stessa isometria. Analogamente si osserva che la trasformazione $\sigma_{v,i+1}\circ\sigma_{v,i}$ invia la coppia (v_i,v_{i+1}) nella coppia (v_{i+2},v_{i+3}) (verificate) e dunque tale trasformazione deve coincidere con la rotazione di angolo $\frac{4\pi}{n}$.

Per quanto riguarda (C) si osservi preliminarmente che simmetrie relative a rette distinte sono distinte. Siccome per n pari gli assi dei lati e le diagonali dei vertici sono distinte si ha la prima affermazione. Per quanto riguarda la seconda basta osservare che la coppia di punti (v_i,v_{i+1}) viene inviata nella coppia (v_{i+1},v_{i+2}) (verificate).

Esercizio 8. 4. Consideriamo l'insieme $\mathcal{F}(\mathbb{R},\mathbb{R})$ l'insieme delle funzioni da $\mathbb{R}$ in $\mathbb{R}$. Sia $C^0(\mathbb{R},\mathbb{R})$ il sottoinsieme delle funzioni continue da $\mathbb{R}$ in $\mathbb{R}$. Denotiamo con $+$ e $\circ$ le seguenti operazioni:

$$(f+g)(x)=f(x)+g(x)\,,\qquad f,g\in\mathcal{F}(\mathbb{R},\mathbb{R})$$
$$(f\circ g)(x)=f(g(x))\,,\qquad f,g\in\mathcal{F}(\mathbb{R},\mathbb{R})$$

(A) Dimostrare che su $\mathcal{F}(\mathbb{R},\mathbb{R})$ l'operazione $\circ$ non è distributiva rispetto alla somma . Verificare che esiste un'unità in $\mathcal{F}(\mathbb{R},\mathbb{R})$ rispetto a tale prodotto.
(B) Determinare l'insieme degli invertibili di $\mathcal{F}(\mathbb{R},\mathbb{R})$.
(C) Verificare che $C^0(\mathbb{R},\mathbb{R})$ è un sottogruppo additivo chiuso rispetto al prodotto.
(D) Verificare che l'insieme $\mathcal{F}^+$ delle funzioni di $\mathcal{F}(\mathbb{R},\mathbb{R})$ a valori in $\mathbb{R}^+$ è tale che $\mathcal{F}^+\circ\mathcal{F}(\mathbb{R},\mathbb{R})\subseteq\mathcal{F}^+$ ma che non è un sottogruppo rispetto alla somma.
(E) Verificare che $\mathcal{C}\simeq\mathbb{R}$, l'insieme delle funzioni costanti è un sottogruppo rispetto alla somma tale che $\mathcal{C}\circ\mathcal{F}(\mathbb{R},\mathbb{R})=\mathcal{F}(\mathbb{R},\mathbb{R})\circ\mathcal{C}=\mathcal{C}$.

Soluzione. Nel punto (A) si chiede di verificare che l'operazione $\circ$ non è distributiva rispetto alla somma in $\mathcal{F}(\mathbb{R},\mathbb{R})$ ma che tale operazione ammette un'unità. Cominciamo dalla prima affermazione:

$$[f\circ(g+h)](x)=f(g(x)+h(x))\neq f(g(x))+f(h(x))$$

a meno che la funzione f non sia lineare. Si osservi che la composizione invece è distributiva a destra:

$$[(f+g)\circ h](x) = f(h(x)) + g(h(x))$$

L'operazione $\circ$ è chiaramente associativa su $\mathcal{F}(\mathbb{R},\mathbb{R})$ (verficate). Osserviamo infine che la funzione $1_{\mathcal{F}} : \mathbb{R} \to \mathbb{R}$, $1_{\mathcal{F}}(x) = x$ è l'identità di $\mathcal{F}(\mathbb{R},\mathbb{R})$ rispetto alla composizione:

$$(f \circ 1_{\mathcal{F}})(x) = f(1_{\mathcal{F}}(x)) = f(x) = 1_{\mathcal{F}}(f(x)) = (1_{\mathcal{F}} \circ f)(x)$$

Nel punto (B) si chiede di determinare l'insieme degli invertibili in $\mathcal{F}(\mathbb{R},\mathbb{R})$ rispetto all'operazione $\circ$. Una funzione $f \in \mathcal{F}(\mathbb{R},\mathbb{R})$ è invertibile rispetto a $\circ$ se esiste una funzione $g \in \mathcal{F}(\mathbb{R},\mathbb{R})$ tale che $(f\circ g) = (g \circ f) = 1_{\mathcal{F}}$ ovvero tale che $f(g(x)) = g(f(x)) = x$. Una tale funzione esiste se e soltanto se f è biettiva ed è precisamente l'inversa f^{-1}. Dunque l'insieme degli invertibili di $\mathcal{F}(\mathbb{R},\mathbb{R})$ rispetto a $\circ$ è esattamente l'insieme delle funzioni biettive in $\mathcal{F}(\mathbb{R},\mathbb{R})$.

Nel punto (C) viene chiesto di mostrare che $C^0(\mathbb{R},\mathbb{R})$ è un sottogruppo additivo chiuso rispetto alla composizione. Ci vengono in aiuto le nostre conoscenze di calcolo. Sappiamo infatti che se $f, g \in C^0(\mathbb{R},\mathbb{R})$ sono funzioni continue allora $f+g$ è una funzione continua così come $-f$; in particolare $c_0 : \mathbb{R} \to \mathbb{R}$, $c_0(x) \equiv 0$, ovvero l'elemento neutro di $(\mathcal{F}(\mathbb{R},\mathbb{R}),+)$ è in $C^0(\mathbb{R},\mathbb{R})$. Ne concludiamo che $C^0(\mathbb{R},\mathbb{R})$ è un sottogruppo additivo di $(\mathcal{F}(\mathbb{R},\mathbb{R}),+)$. Osserviamo che anche $1_{\mathcal{F}}$ è in $C^0(\mathbb{R},\mathbb{R})$ ed inoltre $f, g \in C^0(\mathbb{R},\mathbb{R})$ implica che $(f\circ g) \in C^0(\mathbb{R},\mathbb{R})$ (ci viene qui in soccorso qualche nozione elementare di Calcolo 1). Ne segue che l'insieme $C^0(\mathbb{R},\mathbb{R})$ è chiuso rispetto alla composizione. Inoltre per quanto detto fino ad ora risulta chiaro che gli elementi invertibili di $\mathcal{F}(\mathbb{R},\mathbb{R})$ in $C^0(\mathbb{R},\mathbb{R})$ formano un sottogruppo moltiplicativo del gruppo degli invertibili di $\mathcal{F}(\mathbb{R},\mathbb{R})$.

Nel punto (D) si chiede di verificare che vale la seguente inclusione $\mathcal{F}^+ \circ \mathcal{F}(\mathbb{R},\mathbb{R}) \subseteq \mathcal{F}(\mathbb{R},\mathbb{R})$ ma che $\mathcal{F}^+$ non è un sottogruppo rispetto alla somma. Questa seconda affermazione è banalmente verificata: sia infatti $f \in \mathcal{F}^+$ una funzione a valori positivi, allora $-f$ è una funzione a valori negativi o nulli e pertanto non è in $\mathcal{F}^+$. Osserviamo invece che vale l'inclusione precedentemente citata: sia $f \in \mathcal{F}^+$ e $g \in \mathcal{F}(\mathbb{R},\mathbb{R})$, allora $(f\circ g)(x) = f(g(x)) > 0$ perché $f(x) > 0$ per ogni $x \in \mathbb{R}$. In realtà vale proprio l'uguaglianza come si può vedere componendo con l'elemento $1_{\mathcal{F}}$.

Punto (E). Si denota con $\mathcal{C}$ l'insieme delle funzioni costanti:

$$\mathcal{C} = \{c_\alpha \mid c_\alpha(x) \equiv \alpha,\ \alpha \in \mathbb{R}\}$$

Osserviamo che $(c_\alpha + c_\beta)(x) = c_\alpha(x) + c_\beta(x) \equiv \alpha+\beta = c_{\alpha+\beta}(x)$ e dunque $\mathcal{C}$ è chiuso rispetto alla somma. Inoltre contiene l'elemento neutro ovvero $c_0(x) \equiv 0$ e dunque è un sottogruppo di $(\mathcal{F}(\mathbb{R},\mathbb{R}),+)$. Infine si osservi che per ogni $f \in \mathcal{F}(\mathbb{R},\mathbb{R})$ si ha: $f \circ c_\alpha = c_{f(\alpha)}$, $c_\alpha \circ f = c_\alpha$. Questo conclude l'esercizio. □

Esercizio 8. 5. Sia A un anello (unitario). Siano I, $J \subset A$ due ideali e K_1, $K_2 \subset A$ due sottoanelli (ma non ideali).
(A) Verificare che $(I + K_1)$ è un sottoanello;
(B) Dimostrare che $K_1 + K_2$ è un sottoanello se e soltanto se $(K_1\, K_2 + K_2\, K_1) \subset K_1 + K_2$;
(C) Sia ora $J \subset K_1$ e supponiamo che $(I + K_1)/J = (I + J)/J$. Dimostrare che allora K_1/J è un sottoanello di I/J.

Soluzione. Cominciamo dal punto (A). Proviamo che $I+K$ è un sottoanello; dalla teoria sappiamo che è un sottogruppo in quanto somma di sottogruppi. Inoltre, $I+K$ è chiuso rispetto alla moltiplicazione: infatti, sia $a \in (I + K)$, dunque $a = i' + k'$ per opportuni $i' \in I$ e $k' \in K$, e sia $i + k \in I + K$ un generico elemento, dove $i \in I$ e $k \in K$. Se $i' \in I$, allora $i' \cdot (i + k) = i'i + ik \in I$ perché I è ideale, dunque in particolare $i' \cdot (i+k) = i'i + ik \in I \subseteq I + K$ è un elemento in $I + K$. Supponiamo invece che $k' \in K$; allora $k' \cdot (i+k) = k'i + k'k \in I + K$, perché $k'i \in I$ essendo I un ideale, mentre $k'k \in K$ perché K è un sottoanello. La proprietà distributiva della somma rispetto alla moltiplicazione permette di concludere che

$$a \cdot (i + k) = (i' + k') \cdot (i + k) = i' \cdot (i + k) + k' \cdot (i + k) \in I + K,$$

da cui segue la tesi.

Passiamo alla dimostrazione del punto (B). Supponiamo che K_1+K_2 sia un sottoanello; allora è chiuso per prodotto, dunque per ogni $k_1, k_1' \in K_1$, $k_2, k_2' \in K_2$ si ha

$$(k_1' + k_2') \cdot (k_1 + k_2) = k_1'k_1 + k_1'k_2 + k_2'k_1 + k_2'k_2 \in K_1 + K_2,$$

da cui segue che $k_1'k_2 + k_2'k_1 \in K_1 + K_2$. Dall'arbitrarietà della scelta di k_1, k_1', k_2, k_2' segue che $K_1K_2 + K_2K_1 \subseteq K_1 + K_2$. Dimostriamo il viceversa per assurdo, ovvero supponiamo che $K_1K_2 + K_2K_1 \nsubseteq K_1 + K_2$ e dimostriamo che in tal caso $K_1 + K_2$ non è un sottoanello. Se $K_1K_2 + K_2K_1 \nsubseteq K_1 + K_2$, allora esistono elementi $k_1, k_1' \in K_1$ e $k_2, k_2' \in K_2$ tali che $k_1k_2' + k_2k_1' \notin K_1 + K_2$. In tal caso, un calcolo analogo a quello svolto nel punto (A) mostra che gli elementi $k_1 + k_2$ e $k_1' + k_2' \in K_1 + K_2$ sono tali che il loro prodotto non appartiene a $K_1 + K_2$, che dunque non essendo chiuso rispetto a tale operazione non è un sottoanello.

Per quanto riguarda il punto (C) osserviamo preliminarmente che, per come sono definite le operazioni nel quoziente A/J, l'insieme K_1/J è un sottoanello di A/J. Dunque l'unica cosa da verificare è che $K_1/J \subseteq I/J$. Dalla relazione $(I + K_1)/J = (I + J)/J$ segue che per ogni $k_1 \in K_1$, $i \in I$ esistono $i' \in I$ e $j, j' \in J$ tali che $i + k_1 = i' + j + j'$. Da questa relazione segue che $k_1 = i' - i + j + j'$, dunque $\overline{k \equiv i' - i} \mod (J)$, da cui per l'arbitrarietà di $k_1 \in K_1$ si ha $K_1/J \subseteq I/J$. □

Esercizio 8. 6. Sia A un anello (unitario). Sia $K \subset A$ un sottoanello e siano $I, J \subseteq A$ due ideali. Supponiamo che:

(1) $J \leq K$;
(2) $(I + K)/I = (I + J)/I$;
(3) $I \cap K = I \cap J$;

Dimostrare che allora $K = J$.

Soluzione. Poiché per il punto (1) si ha $J \subseteq K$, per avere la tesi è sufficiente dimostrare l'inclusione $K \subseteq J$. Sia dunque $k \in K$; dalla condizione (2) segue che per ogni $i_1 \in I$ esistono $j \in J$ e $i_2 \in I$ tali che

$$k + i_1 \equiv j + i_2 \mod I,$$

ovvero esiste $i \in I$ tale che $k + i_1 = j + i_2 + i$. Equivalentemente, $k - j = i_2 - i_1 + i$, dunque $k - j \in I$. D'altra parte, $k \in K$ e $j \in J \subseteq K$, quindi $k - j \in K$. Si deduce pertanto che $k - j \in K \cap I = I \cap J \subseteq J$, in virtù dell'ipotesi (3). Dunque esiste $j' \in J$ tale che $k - j = j'$, da cui $k = j' - j \in J$. Dall'arbitrarietà di $k \in K$ si conclude che $K \subseteq J$. □

Esercizio 8. 7. Consideriamo S_6. Definiamo il seguente sottoinsieme di S_6:

$$T_3 = \{\gamma \in S_6 \mid \gamma = (i_1\, j_1)\,(i_2\, j_2)\,(i_3\, j_3) \text{ con } \{(i_k\, j_k)\}_{k=1}^{3} \text{ 2-cicli disgiunti}\}$$

(A) Mostrare che ogni trasposizione di S_6 può essere scritta come prodotto di 3 elementi di T_3 ; [*Suggerimento. Sfruttare un ragionamento analogo a quello dell'esercizio 7.4. (B)*]
(B) Utilizzare il punto (A) per dedurre che $\langle T_3 \rangle = S_6$.

Soluzione. Il suggerimento era quello di sfruttare l'esercizio 7.4. (B). In quell'esercizio veniva chiesto di dimostrare che vi era un sottogruppo normale di S_4 isomorfo al gruppo di Klein; esso era individuato dai prodotti di trasposizioni disgiunte: $(1\,2)\,(3\,4)$, $(1\,3)\,(2\,4)$, $(1\,4)\,(2\,3)$. Per quanto riguarda il punto (A) possiamo osservare la cosa seguente: siano a, b, c, d, e, f numeri distinti compresi tra 1 e 6 allora vale la seguente:

$$(a\,d)\,(b\,c)\,(e\,f) \cdot (a\,b)\,(c\,d)\,(e\,f) \cdot (a\,c)\,(b\,d)\,(e\,f) = (e\,f)$$

In particolare è possibile ottenere ogni trasposizione come prodotto di tre elementi ciascuno prodotto di tre trasposizioni disgiunte, che era ciò che ci veniva chiesto di dimostrare nel punto (A).

Il punto (B) a questo punto è di facile soluzione. Sappiamo infatti dalla teoria che S_n è generato dai suoi 2-cicli (le trasposizioni). Poiché ogni trasposizione può essere scritta come prodotto di elementi di T_3 ne deduciamo che l'insieme T_3 genera S_6. □

N.B. Si osservi che tale argomento funziona per S_n in generale: è infatti ancora possibile definire T_3 ed analogamente a quanto fatto nell'esercizio si può dimostrare che ogni trasposizione di S_n può essere ottenuta come prodotto di 3 elementi in T_3.

Esercizio 8. 8. Sia A un anello (unitario). Ricordiamo che $a \in A$ è detto *nilpotente* se esiste $n \in \mathbb{N}$ tale che $a^n = 0_A$. Dimostrare che se $a \in A$ è nilpotente allora $(1_A + a) \in A$ è invertibile.
[*Suggerimento. Come può essere espressa la somma di due potenze n-sime?*]

Soluzione. Supponiamo che $a \in A$ sia nilpotente; allora esiste $n \in \mathbb{N}$ tale che $a^n = 0_A$. Ricordando la formula del binomio di Newton, possiamo scrivere:

$$1_A = 1_A + 0_A = 1_A + a^n = (1_A + a) \cdot \left(\sum_{i=0}^{n-1} (-1)^i a^i \right)$$

Ciò prova che l'elemento $\sum_{i=0}^{n-1}(-1)^i a^i$ è l'inverso di $(1_A + a)$. □

Definizione. Sia A un anello e sia $K \subset A$ un sottoanello di A. Il radicale di K in A, $\sqrt[A]{K}$, è definito come l'insieme degli elementi $a \in A$ per cui esiste $m \in \mathbb{N}$ tale che $a^m \in K$.

Esercizio 8. 9. Siano A, B due anelli e sia $\varphi : A \to B$ un omomorfismo di anelli. Sia K un sottoanello di B. Mostrare che $\sqrt[A]{\varphi^{-1}(K)} = \varphi^{-1}\left(\sqrt[B]{K}\right)$.

Soluzione. Sia $a \in \sqrt[A]{\varphi^{-1}(J)}$; dalla definizione di radicale segue che esiste $m \in \mathbb{N}$ tale che:

$$a^m \in \varphi^{-1}(J) \Leftrightarrow \varphi(a^m) \in J \Leftrightarrow (\varphi(a))^m \in J \Leftrightarrow \varphi(a) \in \sqrt[B]{J}. \ \square$$

Esercizio 8. 10. Sia A un anello (unitario) commutativo. Sia J un ideale di A. Dimostrare che $\sqrt[A]{J}$ è ancora un ideale. Dimostrare che $\sqrt[A]{\sqrt[A]{J}} = \sqrt[A]{J}$.

Soluzione. Cominciamo dimostrando che $\sqrt[A]{J}$ è un ideale di A. Consideriamo quindi un elemento $a \in A$ ed un elemento $a' \in \sqrt[A]{J}$ tale che $(a')^m = j \in J$: $(a \cdot a')^m = a^m \cdot (a')^m = a^m \cdot j \in J$, pertanto $a\,a' \in \sqrt[A]{J}$; per arbitrarietà dell'elemento $a \in A$ ed $a' \in \sqrt[A]{J}$ ne segue che $(A \cdot \sqrt[A]{J}) \subseteq \sqrt[A]{J}$. Essendo l'anello A commutativo vale anche $(\sqrt[A]{J} \cdot A) \subseteq \sqrt[A]{J}$. Rimane solo da verificare che $\sqrt[A]{J}$ è un sottogruppo additivo di A. Osserviamo che $0_A \in J \subseteq \sqrt[A]{J}$. Ora siano a'_1, $a'_2 \in \sqrt[A]{J}$, e siano $m_1, m_2 \in N$ tali che $(a'_1)^{m_1} \in \sqrt[A]{J}$, $(a'_2)^{m_2} \in \sqrt[A]{J}$. Sia $M = \max\{m_1, m_2\}$ allora

$$(a'_1 + a'_2)^{2M} = \sum_{j=0}^{2M} \binom{2M}{j} (a'_1)^j \, (a'_2)^{2M-j}$$

Per definizione di M risulta che, qualsiasi sia j risulta $\max\{j\,;\ 2M - j\} \geq \max\{m_1,\, m_2\}$ e dunque per ogni addendo della sommatoria si ha che uno tra $(a'_1)^j$ e $(a'_2)^{2M-j}$ è in J. Essendo J un ideale ne deduciamo che $(a'_1)^j \, (a'_2)^{2M-j} \in J$ e dunque $\sum_{j=0}^{2M} \binom{2M}{j} (a'_1)^j \, (a'_2)^{2M-j} \in J$, ovvero $(a'_1 + a'_2)^{2M} \in J$ e quindi $(a'_1 + a'_2) \in \sqrt[A]{J}$.
Infine se $a' \in \sqrt[A]{J}$ si osservi che $-a' \in \sqrt[A]{J}$. Infatti se $(a')^m \in J$ allora $(-a')^m = \pm(a')^m \in J$. Questo conclude la dimostrazione del fatto che $\sqrt[A]{J}$ è un ideale.

Per quanto riguarda l'identità $\sqrt[A]{\sqrt[A]{J}} = \sqrt[A]{J}$ abbiamo invece: $a \in \sqrt[A]{\sqrt[A]{J}}$ se e soltanto se esiste $m \in \mathbb{N}$ tale che $a^m \in \sqrt[A]{J}$ se e soltanto se esiste $n \in \mathbb{N}$ tale che $(a^m)^n \in J$ se e soltanto se $a^{n\,m} \in J$ se e soltanto se $a \in \sqrt[A]{J}$. □