Algebra I - Soluzione Esercizi

Primo Foglio

Esercizio 1. Vogliamo dimostrare che $\exists \sigma \in S_n : g = \sigma g^k \sigma^{-1}$; nei gruppi simmetrici ciò è equivalente a dimostrare che g e g^k hanno la stessa decomposizione in cicli, per una nota caratterizzazione. L'ipotesi $< g >=< g^k >$ ci dice che k è coprimo con l'ordine di g, che denotiamo con m. Questo è vero perché $< g >$ è isomorfo a $\mathbb{Z}/m\mathbb{Z}$, e gli interi invertibili modulo m sono esattamente i numeri coprimi con m. Scriviamo g in cicli:

$$g = (a_1^1 \dots a_1^{t_1})(a_2^1 \dots a_2^{t_2}) \dots (a_\ell^1 \dots a_\ell^{t_\ell})$$

Nella decomposizione i cicli sono disgiunti tra di loro, dunque commutano, e quindi per ogni intero r si ha

$$g^k = (a_1^1 \dots a_1^{t_1})^r (a_2^1 \dots a_2^{t_2})^r \dots (a_\ell^1 \dots a_\ell^{t_\ell})^r$$

Il punto chiave è il seguente: k coprimo con m implica che è coprimo anche con gli ordini di tutti i cicli di g, perché m è proprio il loro minimo comune multiplo. Dunque ogni ciclo di $(a_2^1 \dots a_2^{t_2})^k$ di g ha ancora la stessa lunghezza del corrispondente ciclo $(a_2^1 \dots a_2^{t_2})$ in g. Dunque g e g^k hanno la stessa struttura in cicli.

Esercizio 2. La risposta è SÌ, esibiamo un paio di strutture.

1. Possiamo rendere l'insieme un gruppo isomorfo a $\mathbb{C}^*$ guardando le singole componenti, ovvero:

$$\begin{pmatrix} z & z \\ z & z \end{pmatrix} \begin{pmatrix} w & w \\ w & w \end{pmatrix} = \begin{pmatrix} z \cdot w & z \cdot w \\ z \cdot w & z \cdot w \end{pmatrix}.$$

   con identità

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

2. L'insieme può essere dotato di una struttura di gruppo equipaggiandolo con il prodotto riga per colonna, ovvero:

$$\begin{pmatrix} z & z \\ z & z \end{pmatrix} \begin{pmatrix} w & w \\ w & w \end{pmatrix} = \begin{pmatrix} 2z \cdot w & 2z \cdot w \\ 2z \cdot w & 2z \cdot w \end{pmatrix}.$$

   L'elemento neutro è:

$$e = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Si ricordi che, in generale, se due insiemi A e B hanno la stessa cardinalità allora esiste una biezione:

$$A \xrightarrow{f} B$$

Se B ha un'operazione interna $\diamond_B$, allora si può dotare A di un'operazione $\diamond_A$ tale che f sia un "isomorfismo":

$$a \diamond_A a' := f^{-1}(f(a) \diamond_B f(a')) \qquad \forall\, a, a' \in A$$

Nel caso dei gruppi, l'inverso dell'elemento neutro di B è proprio l'elemento neutro di A.

Esercizio 3. Richiamiamo qualche definizione:

- L'indice di un sottogruppo $H \leq G$ per gruppi finiti è il rapporto tra gli ordini del gruppo G e del gruppo H:

$$[G : H] = \frac{|G|}{|H|};$$

- Inoltre si ricordi che H è un sottogruppo normale di G se $\forall\, g \in G$, $\forall\, h \in H$ si ha che $ghg^{-1} \in H$;

- Un gruppo G è semplice se non possiede sottogruppi normali.

Dunque utilizzando l'ultima affermazione, per dimostrare che G non è semplice troviamo un suo sottogruppo normale. Se H ha indice 2 allora è normale, perché ha una sola classe laterale destra e una sola classe laterale sinistra, che coincidono entrambe con il complementare in G. Procediamo con il caso in cui H ha indice 3. L'insieme delle classi laterali sinistre di H ha cardinalità 3, e G agisce su questo insieme per moltiplicazione sinistra:

$$g_1 \cdot (g_2 H) = g_1 g_2 H$$

Un'azione di G su un insieme di 3 elementi fornisce un morfismo non banale di gruppi

$$G \xrightarrow{\varphi} S_3 \,.$$

Se φ ha nucleo non banale K, questo è un sottogruppo normale e proprio di G, che quindi è non semplice. Se invece φ ha nucleo banale, deve essere iniettivo e G è quindi isomorfo ad un sottogruppo di S_3 di ordine maggiore di 3. L'unico tale sottogruppo è proprio S_3, che non è semplice.

Esercizio 4. Per la risoluzione dell'esercizio ricordiamo i Teoremi di Sylow:

1. Se p è primo e p^α divide l'ordine di G allora esiste un sottogruppo di G di ordine p^α. Un p-sottogruppo di Sylow è un tale sottogruppo, con α massimale per questa proprieta;
2. Tutti i p-sottogruppi di Sylow sono coniugati. In particolare se c'è un solo p-Sylow, questo è normale;
3. Se $|G| = p^\alpha m$ con $p \not| m$, il numero di p-Sylow n_p è congruo ad 1 modulo p e divide m.

Nel nostro caso l'ordine del gruppo G è $405 = 3^4 5$; calcoliamo n_3:

$$\begin{cases} n_3 \equiv 1 \mod 3 \\ n_3 \,|\, 5 \end{cases}$$

Dunque n_3 deve essere 1 oppure 5, e tra questi soltanto 1 verifica la prima condizione. Concludiamo per il secondo teorema di Sylow. Se $|G| = 588 = 2^2 \cdot 3 \cdot 7^2$, calcoliamo n_7:

$$\begin{cases} n_7 \equiv 1 \mod 7 \\ n_7 \,|\, 12 \end{cases}$$

Anche in questo caso l'unica soluzione è $n_7 = 1$.

Esercizio 5. Per risolvere

$$\begin{cases} 8x \equiv 1 & (33) \\ x \equiv k & (21) \end{cases}$$

cerchiamo prima l'inverso moltiplicativo di 8 modulo 33. Siccome $4 \cdot 8 = 32 \equiv -1$, l'inverso di 8 è $-4 \equiv 29$. Otteniamo il sistema

$$\begin{cases} x \equiv 29 & (33) \\ x \equiv k & (21) \end{cases}$$

che è equivalente a

$$\begin{cases} x \equiv 29 \equiv 2 & (3) \\ x \equiv 29 \equiv 7 & (11) \\ x \equiv k & (7) \\ x \equiv k & (3) \end{cases}$$

Abbiamo trovato che k deve essere congruo a 2 modulo 3. Utilizziamo il teorema cinese dei resti sulle 3 equazioni rimanenti:

$$\begin{cases} x \equiv 2 & (3) \\ x \equiv 7 & (11) \\ x \equiv k & (7) \end{cases}$$

una soluzione è data da $77x_1 + 21x_2 + 33x_3$. dove

$$\begin{cases} 77x_1 \equiv 2 & (3) \\ 21x_2 \equiv 7 & (11) \\ 33x_3 \equiv k & (7) \end{cases}$$

Delle soluzioni per questo sistema sono $x_1 = 1$, $x_2 = 4$, $x_3 = 3k$, quindi $x = 161 + 99k$ risolve il nostro sistema. Per $k = -1$ abbiamo $x = 62$, e per $k = 2$ abbiamo $x = 359$.

Esercizio 6.

- $\mathbb{C}[t]$ è un dominio euclideo, in quanto è ben definita la la divisione con resto tra polinomi, e una funzione di valutazione è data dal grado.
- Contrariamente al caso precedente, in $\mathbb{Z}[t]$ non sempre c'è la divisione con resto. Si noti ad esempio che $(t+1)$ non si può scrivere come $a(t)\cdot 2t+r$ con r costante. Inoltre $\mathbb{Z}[t]$ non è un P.I.D., e dimostriamo questo fatto esibendo un ideale non principale, ad esempio $(2, t+1)$. Tuttavia $\mathbb{Z}[t]$ è un dominio a fattorizzazione unica, in virtù del seguente risultato visto in classe: "Se R è un U.F.D. lo è anche $R[x]$."
- $\mathbb{C}[t]/(t^2)$ non è un dominio d'integrità in quanto è possibile prendere due elementi non nulli con prodotto nullo: $0 = t^2 = t \cdot t$.
- Come nel caso precedente si possono esibire due elementi di $\mathbb{Z}[x, y]/(x^2 - y^2)$ non nulli con prodotto nullo:

$$(x + y) \cdot (x - y) = 0$$

Esercizio 7. Sia M un ideale massimale (dunque proprio) di A e sia $x \in M$; allora x non è invertibile, perché altrimenti avremmo $1 \in M$. Viceversa, se un generico elemento $x \neq 0$ di A non è invertibile, l'ideale generato da x, ovvero $(x) = A \cdot x$, non contiene 1, dunque è proprio. Segue che (x) è contenuto in un ideale massimale, per il lemma di Zorn.
Denotiamo con J l'intersezione di tutti gli ideali massimali di A (che prende il nome di Radicale di Jacobson). Per dimostrare la seconda equivalenza di affermazioni, dimostriamo l'equivalenza tra le loro negazioni: ciò che vogliamo è

$$x \notin J \iff \exists\, y \in A \text{ tale che } xy - 1 \text{ non è invertibile in } A$$

La dimostriamo tramite la seguente catena di equivalenze:

$$\begin{gathered} x \notin J \\ \iff \exists\, M \text{ massimale in } A \text{ tale che } x \notin M \\ \iff \exists\, M \text{ massimale in } A \text{ tale che } x \neq 0 \text{ in } A/M \\ \iff \exists\, M \text{ massimale in } A,\ \exists\, y \in A \text{ tali che } xy = 1 \text{ in } A/M \\ \iff \exists\, M \text{ massimale in } A,\ \exists\, y \in A \text{ tali che } xy - 1 = 0 \text{ in } A/M \\ \iff \exists\, M \text{ massimale in } A,\ \exists\, y \in A \text{ tali che } xy - 1 \in M \\ \iff \exists\, y \in A \text{ tale che } xy - 1 \text{ non è invertibile in } A \end{gathered}$$

La terza affermazione segue direttamente dall'equivalenza delle negazioni appena dimostrata, mentre l'ultima osservazione segue dal primo punto.

Esercizio 8. Si ricordi che $\mathfrak{A}$ è un sottoanello di A se è chiuso per somma e prodotto, ed è un ideale destro (risp. sinistro) di A se è chiuso anche per prodotto a destra (risp. a sinistra) con elementi di A.
Il primo sottoinsieme è un sottoanello:

$$\begin{pmatrix} 0 & 0 & z \\ 0 & 0 & z \\ 0 & 0 & z \end{pmatrix} + \begin{pmatrix} 0 & 0 & w \\ 0 & 0 & w \\ 0 & 0 & w \end{pmatrix} = \begin{pmatrix} 0 & 0 & z+w \\ 0 & 0 & z+w \\ 0 & 0 & z+w \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & z \\ 0 & 0 & z \\ 0 & 0 & z \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & w \\ 0 & 0 & w \\ 0 & 0 & w \end{pmatrix} = \begin{pmatrix} 0 & 0 & zw \\ 0 & 0 & zw \\ 0 & 0 & zw \end{pmatrix}$$

ma non è un ideale nè destro nè sinistro: se consideriamo la matrice

$$\begin{pmatrix} a & 0 & 0 \\ b & 0 & 0 \\ c & 0 & 0 \end{pmatrix}$$

si ha:

$$\begin{pmatrix}0&0&z\\0&0&z\\0&0&z\end{pmatrix}\cdot\begin{pmatrix}a&0&0\\b&0&0\\c&0&0\end{pmatrix}=\begin{pmatrix}cz&0&0\\cz&0&0\\cz&0&0\end{pmatrix}\qquad\begin{pmatrix}a&0&0\\b&0&0\\c&0&0\end{pmatrix}\cdot\begin{pmatrix}0&0&z\\0&0&z\\0&0&z\end{pmatrix}=\begin{pmatrix}0&0&az\\0&0&bz\\0&0&cz\end{pmatrix}$$

i quali non vi appartengono. Analogamente si dimostra che il secondo insieme è un sottoanello di $M^{3\text{x}3}(\mathbb{C})$ ed anche un un ideale sinistro. Infatti:

$$\begin{pmatrix}a&b&c\\d&e&f\\g&h&j\end{pmatrix}\cdot\begin{pmatrix}0&0&z\\0&0&w\\0&0&u\end{pmatrix}=\begin{pmatrix}0&0&az+bw+cu\\0&0&dz+ew+fu\\0&0&gz+hw+ju\end{pmatrix}$$

L'ultimo sottoinsieme non è neanche un sottoanello, perché non è chiuso per la somma:

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}+\begin{pmatrix}0&0&0\\0&0&0\\0&0&1\end{pmatrix}=\mathrm{Id}_3$$

Esercizio 9. I due anelli in questione sono domini d'integrità perché sono sottoanelli di $\mathbb{C}$ ed ereditano la proprietà da $\mathbb{C}$, ma non sono a fattorizzazione unica perchè:

- In $\mathbb{Z}[\sqrt{-3}]$ l'elemento 4 si può scrivere sia come $4 = 2 \cdot 2$, sia come $4 = (1+\sqrt{-3})\cdot(1-\sqrt{-3})$;
- In $\mathbb{Z}[\sqrt{-5}]$ l'elemento 6 si può scrivere sia come $6 = 2 \cdot 3$, sia come $6 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$.

Definiamo una notazione per l'ultimo punto: chiamiamo ω l'elemento $\frac{1+\sqrt{-3}}{2}$; allora ω verifica

$$\omega^6 = 1, \quad \omega^3 = 1, \quad \omega^2 = \omega - 1$$

Dunque ogni elemento x di $\mathbb{Z}[\omega]$ si può scrivere come $a+b\omega$, con a, $b \in \mathbb{Z}$, e quindi $x = a+b\omega = \big(a+\frac{b}{2}\big)+\big(i\frac{b}{2}\sqrt{3}\big)$. Associamo ad x la valutazione

$$v(x) := \big(a+\frac{b}{2}\big)^2+\big(\frac{b\sqrt{3}}{2}\big)^2 = a^2+b^2+ab$$

La divisione con resto è analoga a quella nell'anello degli interi di Gauss $\mathbb{Z}[i]$.

Esercizio 10. $\mathbb{C}[x,y]/(x^3,y^2)$ è noetheriano perché è quoziente di $\mathbb{C}[x,y]$, che a sua volta è noetheriano per il Teorema della Base di Hilbert. $\mathbb{C}[x^3,y^2]$ è isomorfo all'anello dei polinomi in due variabili $\mathbb{C}[s,t]$ tramite

$$\begin{aligned} s &\longmapsto x^3\\ t &\longmapsto y^2 \end{aligned}$$

quindi è noetheriano. Infine $\mathbb{Z}\times\mathbb{Z}$ è anch'esso noetheriano perché ogni ideale I di $\mathbb{Z}\times\mathbb{Z}$ è della forma I_1+I_2, con $I_1 = I\cap\mathbb{Z}\times\{0\}$ e $I_2 = I\cap\{0\}\times\mathbb{Z}$ sono naturalmente isomorfi ad ideali di $\mathbb{Z}$; infatti, $(a,b)\in I$ si può scrivere come

$$(a,b) = (a,b)\cdot(1,1) = (a,b)\cdot[(1,0)+(0,1)] = (a,0)+(0,b)\in I_1+I_2\,.$$

Inoltre, se $I\subseteq J$, allora $I_1\subseteq J_1$ e $I_2\subseteq J_2$; ciò implica che data una catena ascendente di ideali $\big\{I^{(n)}\big\}_{n\in\mathbb{N}}$ di $\mathbb{Z}\times\mathbb{Z}$, le componenti $I_1^{(n)}$ e $I_2^{(n)}$ costituiscono catene ascendenti di ideali di $\mathbb{Z}$, che quindi stazionano dopo certi valori n_1 ed n_2. Ciò implica che la catena $\big\{I^{(n)}\big\}_{n\in\mathbb{N}}$ staziona dopo il valore $\max\{n_1,n_2\}$.