ALGEBRA I: SOLUZIONI DECIMA ESERCITAZIONE
6 giugno 2011

Esercizio 1.

i) Elencare tutti i possibili gruppi abeliani di cardinalità 140 a meno di isomorfismo.

ii) Elencare tutti i possibili gruppi abeliani di cardinalità 2310 a meno di isomorfismo.

Soluzione. Dal teorema di classificazione, ogni gruppo abeliano finito G si decompone come prodotto diretto di gruppi ciclici come segue

$$G \simeq \mathbb{Z}/(d_1) \times \mathbb{Z}/(d_2) \times \ldots \times \mathbb{Z}/(d_r),$$

dove d_i divide d_{i+1} per ogni $i < r$. Mostriamo che gli interi $d_1, \ldots, d_r$ sono univocamente determinati dalla struttura di gruppo di G.

Definizione. Sia G un gruppo abeliano (in notazione additiva) e sia $g \in G$ un elemento. L'*ordine* di g è il minimo intero $n \in \mathbb{N}$ tale che $ng = 0$.

Proposizione. *Siano $a_1, \ldots, a_s$ e $b_1, \ldots, b_t$ interi positivi tali che a_i divide a_{i+1} e b_j divide b_{j+1} per ogni $i < s$ e $j < t$. Allora*

$$\mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \ldots \times \mathbb{Z}/(a_s) \simeq \mathbb{Z}/(b_1) \times \mathbb{Z}/(b_2) \times \ldots \times \mathbb{Z}/(b_t)$$

se e solo se $s = t$ e $a_i = b_i$ per ogni $i < s$.

Dimostrazione. Procediamo per induzione su s. Poniamo $G = \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \ldots \times \mathbb{Z}/(a_s)$ e $H = \mathbb{Z}/(b_1) \times \mathbb{Z}/(b_2) \times \ldots \times \mathbb{Z}/(b_t)$. Si osservi che l'ipotesi sugli a_i implica che l'ordine di qualsiasi elemento di G divide a_s, e similmente l'ipotesi sui b_i implica che l'ordine di qualsiasi elemento di H divide b_t. D'altra parte G possiede un elemento di ordine a_s, mentre H possiede un elemento di ordine b_t: pertanto $a_s = b_t$. Dunque H e G possiedono degli $\mathbb{Z}$-sottomoduli $G_1 \subset G$ e $H_1 \subset H$ entrambi isomorfi a $\mathbb{Z}/(a_s)$ e dall'isomorfismo $G \simeq H$ otteniamo un isomorfismo dei moduli quoziente $G/G_1 \simeq H/H_1$. D'altra parte

$$G/G_1 \simeq \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \ldots \times \mathbb{Z}/(a_{s-1}) \qquad \text{e} \qquad H/H_1 \simeq \mathbb{Z}/(b_1) \times \mathbb{Z}/(b_2) \times \ldots \times \mathbb{Z}/(b_{t-1}) :$$

pertanto per induzione otteniamo $s - 1 = t - 1$ e $a_i = b_i$ per ogni $i < s$ e la dimostrazione è conclusa. □

Corollario. *Se $n > 1$ è un numero intero, i gruppi abeliani finiti di cardinalità n sono in corrispondenza biunivoca con le fattorizzazioni di n della forma*

$$n = d_1 d_2 \cdots d_k$$

dove d_i divide d_{i+1} per ogni $i < k$ e dove $d_1 \neq 1$.

Nel seguito chiameremo *ammissibili* quelle fattorizzazioni di un intero n che soddisfano la proprietà enunciate nel precedente corollario.

i) Supponiamo che G abbia cardinalità $140 = 2^2 \cdot 5 \cdot 7$. Poiché l'unico numero naturale il cui quadrato divide 140 è 2, le uniche fattorizzazioni ammissibili di 140 sono 140 e $2 \cdot 70$. Dunque gli unici due gruppi abeliani di ordine 140 sono $\mathbb{Z}/(140)$ e $\mathbb{Z}/(2) \times \mathbb{Z}/(70)$.
ii) Supponiamo che G abbia cardinalità $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Essendo privo di quadrati, l'unica fattorizzazione ammissibile di 2310 è 2310 stesso. Pertanto l'unico gruppo abeliano di ordine 3210 è $\mathbb{Z}/(3210)$.

Un modo più generale di procedere per determinare tutti i gruppi abeliani finiti il cui ordine è un fissato intero n è il seguente.

Definizione. Una *partizione* di un intero n è una scrittura di n della forma $n = a_1 + a_2 + \ldots + a_h$, dove $a_1, a_2, \ldots, a_h$ sono interi positivi tali che $a_1 \leq a_2 \leq \ldots \leq a_h$: l'intero h è detto *lunghezza* della partizione. Indichiamo con

$$\mathcal{P} : \mathbb{N} \longrightarrow \mathbb{N}$$

la *funzione di partizione*, che associa a un intero positivo n il numero delle sue partizioni.

Proposizione. *Sia $n > 1$ un numero intero e sia $n = p_1^{n_1} p_2^{n_2} \cdots p_h^{n_h}$ la sua fattorizzazione in numeri primi. Allora il numero di fattorizzazioni ammissibili di n è*

$$\mathcal{P}(n_1)\mathcal{P}(n_2)\cdots\mathcal{P}(n_h).$$

Dimostrazione. Indichiamo con $\Pi(n_i)$ l'insieme delle partizioni di n_i e costruiamo un'applicazione biunivoca come segue:

$$\{\text{fattorizzazioni ammissibili di } n\} \quad \longleftrightarrow \quad \Pi(n_1) \times \ldots \times \Pi(n_h)$$

Sia $n = d_1 d_2 \cdots d_k$ una fattorizzazione ammissibile, associamogli h partizioni rispettivamente di n_1, di n_2, ..., di n_h. Scriviamo

$$d_i = p_1^{n_{i,1}} \cdots p_h^{n_{i,h}} \qquad \text{per } i = 1, \ldots, k.$$

Poiché d_i divide d_{i+1} per ogni $i < k$, deve essere $n_{i,j} \leq n_{i+1,j}$ per ogni $i < k$. D'altra parte l'uguaglianza

$$p_1^{n_1} p_2^{n_2} \cdots p_h^{n_h} = d_1 d_2 \cdots d_k$$

implica che

$$n_j = n_{1,j} + n_{2,j} + \ldots + n_{k,j} \qquad \text{per } j = 1, \ldots, h :$$

dunque la fattorizzazione $n = d_1 d_2 \cdots d_k$ determina una partizione di n_j per ogni $j \leq h$ (dove ammettiamo che i primi addendi della partizione possano essere nulli).

Viceversa supponiamo di avere data una partizione di n_j per ogni $j \leq h$. Sia k la lunghezza della partizione più lunga: a patto di aggiungere degli addendi nulli all'inizio delle altre partizioni, possiamo assumere che tutte le partizioni date abbiano lunghezza k. Siano dunque

$$n_j = n_{1,j} + n_{2,j} + \ldots + n_{k,j} \qquad \text{per } j = 1, \ldots, h$$

le partizioni date e poniamo

$$d_i = p_1^{n_{i,1}} \cdots p_h^{n_{i,h}} \qquad \text{per } i = 1, \ldots, k.$$

Allora per costruzione $n = d_1 d_2 \cdots d_k$ e d_i divide d_{i+1} per ogni $i < k$: dunque abbiamo determinato una fattorizzazione ammissibile di n.

E' facile vedere che le due applicazioni costruite tra fattorizzazioni ammissibili di n e partizioni di $n_1, \ldots n_h$ sono l'una inversa dell'altra: pertanto l'enunciato segue. □

Esercizio 2. Se $M \subset V$ sono $\mathbb{Z}$-moduli, si definisca l'*indice* di M in V (denotato con $[V : M]$) come la cardinalità del modulo quoziente V/M.

i) Sia $M \subset \mathbb{Z}^n$ uno $\mathbb{Z}$-sottomodulo di rango n con base $v_1, \ldots, v_n$ e si consideri il parallelogramma $P \subset \mathbb{R}^n$ generato da $v_1, \ldots, v_n$:

$$P = \left\{ \sum_{i=1}^{n} a_i v_i \ : \ a_i \in \mathbb{R},\ 0 \leq a_i < 1 \right\}.$$

Mostare che l'indice di M in $\mathbb{Z}^n$ coincide con la cardinalità dell'intersezione $P \cap \mathbb{Z}^n$.

ii) Sia A una matrice intera quadrata di ordine n con determinante diverso da zero. Mostrare che l'indice dell'immagine di A in $\mathbb{Z}^n$ coincide con il modulo del determinante di A.

Soluzione. i) Mostriamo che $P \cap \mathbb{Z}^n$ è un insieme di rappresentanti per il modulo quoziente $\mathbb{Z}^n/M$: ciò equivale a dire che per ogni vettore $w \in \mathbb{Z}^n$ esiste un vettore $v \in M$ tale che

$$w - v \in P \cap \mathbb{Z}^n.$$

Poiché P è un parallelogramma di dimensione n in $\mathbb{R}^n$, l'insieme dei traslati $P+v$ con $v \in M$ ricopre tutto quanto $\mathbb{R}^n$. Pertanto esiste $v_0 \in M$ tale che il traslato $P + v_0$ contiene w, dunque $w - v_0 \in P$.

ii) Sia $A' = Q^{-1}AP$ la forma diagonale di A, dove Q e P sono matrici quadrate il cui determinante ha modulo 1. Allora $\mathbb{Z}^n/\mathrm{Im}(A) \simeq \mathbb{Z}^n/\mathrm{Im}(A')$ e $\det(A') = |\det(A)|$, pertanto ci siamo risotti a mostrare l'enunciato per A'. Supponiamo

$$A' = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & d_n \end{pmatrix}:$$

allora una base di $\mathrm{Im}(A')$ è costituita dalle colonne di A'. Sia $P_{A'}$ il parallelogramma associato a tale base come nel punto i): poiché A' è diagonale, segue che $P_{A'} \cap \mathbb{Z}^n$ contiene $d_1 d_2 \cdots d_n = |\det(A)|$ elementi. Pertanto per il punto i)

$$[\mathbb{Z}^n : \mathrm{Im}(A)] = [\mathbb{Z}^n : \mathrm{Im}(A')] = |P_{A'} \cap \mathbb{Z}^n| = |\det(A)|.$$

Esercizio 3. Mostrare che il concetto di $\mathbb{Z}[i]$-modulo è equivalente al seguente:

- gruppo abeliano M dotato di un endomorfismo $\phi : M \longrightarrow M$ tale che $\phi^2 = -\mathrm{id}$.

Soluzione. Sia M uno $\mathbb{Z}[i]$-modulo. In particolare, la restrizione a $\mathbb{Z}$ (identificato con gli interi di Gauss con parte immaginaria nulla) induce una struttura di $\mathbb{Z}$-modulo su M, dunque di gruppo abeliano. Denotiamo $\phi : M \to M$ l'omomorfismo definito dalla moltiplicazione per i: allora per ogni $v \in M$ vale

$$\phi^2(v) = \phi(\phi(v)) = i(i \cdot v) = i^2 \cdot v = -v,$$

pertanto $\phi^2 = -\mathrm{id}$.

Sia ora M un gruppo abeliano dotato di un endomorfismo $\phi : M \longrightarrow M$ tale che $\phi^2 = -\mathrm{id}$ e definiamo su di esso una struttura di $\mathbb{Z}[i]$-modulo. Essendo un gruppo abeliano, in particolare M è uno $\mathbb{Z}$-modulo, dunque è lecito moltiplicare elementi di v per numeri interi. Se $v \in M$ e se $a, b \in \mathbb{Z}$, poniamo

$$(a + bi) \cdot v = av + b\phi(v) :$$

si lascia per esercizio di verificare che tale definizione induce una struttura di $\mathbb{Z}[i]$-modulo su M.

Esercizio 4. Mostrare che il gruppo abeliano moltiplicativo $\mathbb{Q}^+$ dei numeri razionali positivi è uno $\mathbb{Z}$-modulo libero e determinarne una base.

Soluzione. Ogni intero $n > 0$ può essere scritto in modo unico (a meno di riordinare i fattori) come prodotto di numeri primi come segue

$$n = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_r^{a_r},$$

dove $a_1, \dots, a_r$ sono numeri interi positivi. Dunque ogni numero razionale $n/m > 0$ può essere scritto in modo unico (a meno di riordinare i fattori) come prodotto di numeri primi come segue

$$n/m = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_r^{a_r},$$

dove $a_1, \dots, a_r$ sono numeri interi, possibilmente negativi. L'unicità di tale scrittura equivale a dire che, come $\mathbb{Z}$-modulo rispetto alla moltiplicazione, $\mathbb{Q}^+$ è uno $\mathbb{Z}$-modulo libero con base l'insieme $\mathcal{P}$ dei numeri primi.

Esercizio 5. Sia R un anello commutativo unitario e sia $I \subset R$ un ideale. Confutare o dimostrare le seguenti affermazioni:

i) Il quoziente R/I è un R-modulo libero se e solo se $I = R$ oppure $I = 0$.

ii) L'ideale I è un R-modulo libero se e solo se è principale.

Soluzione. i) L'affermazione è vera. Supponiamo infatti che R/I sia uno $\mathbb{Z}$-modulo libero: poiché esso è dotato di un'applicazione suriettiva $R \longrightarrow R/I$, il suo rango deve essere minore o uguale al rango di R come R-modulo, vale a dire 1. Pertanto o R/I ha rango 1, nel qual caso $R/I \simeq R$ e $I = 0$, o R/I ha rango 0, nel qual caso $R/I \simeq 0$ e $I = R$.

ii) L'affermazione è falsa. Consideriamo infatti l'ideale I generato da 2 in $\mathbb{Z}/(4)$: allora I contiene due elementi, mentre la cardinalità di ogni $\mathbb{Z}/(4)$-modulo libero di rango finito è un multiplo di 4. Dunque I non può essere uno $\mathbb{Z}/(4)$-modulo libero.

Però è vero il seguente fatto:

- L'ideale I è un R-modulo libero se e solo se è principale, generato da un elemento $\alpha \in R$ che non è un divisore dello zero.

Supponiamo infatti che $I \subset R$ sia un R-modulo libero. Allora, essendo dotato di un'applicazione iniettiva $I \subset R$, il rango di I come R-modulo deve essere minore uguale del rango di R come R-modulo, vale a dire 1. Pertanto o I ha rango 0, nel qual caso $I = 0$, oppure I ha rango 1, nel qual caso è generato da un elemento $\alpha \in R$ che lo genera anche come ideale. Dunque abbiamo mostrato che se I è un R-modulo libero, allora esso è un ideale principale.

Supponiamo ora che $\alpha \in R$ non sia un divisore dello zero e consideriamo l'ideale (α). Allora l'omomorfismo di moduli $\phi : R \longrightarrow (\alpha)$ definito da $\phi(a) = a\alpha$ è suriettivo per definizione ed è iniettivo in quanto α non è un divisore dello zero: pertanto $(\alpha) \simeq R$ come R-moduli e l'ideale (α) è un R-modulo libero.

Si osservi che nel caso di un anello finito R, allora $\alpha \in R$ non è un divisore dello zero se e solo se è invertibile se e solo se $(\alpha) = R$ (cfr. soluzione Esercizio 7 dell'11 Aprile 2011). Ciò è falso nel caso di anelli infiniti: per esempio $\mathbb{Z}$ e l'ideale I costituito dai numeri pari sono isomorfi come $\mathbb{Z}$-moduli, ma chiaramente $I \neq \mathbb{Z}$.

Esercizio 6. Dimostrare che un anello commutativo unitario R tale che ogni modulo finitamente generato è libero è un campo.

Soluzione. Sia $I \subset R$ un ideale e consideriamo il quoziente R/I come R-modulo: esso è finitamente generato, dunque per ipotesi è libero e dal punto i) dell'Esercizio 5 otteniamo che $I = 0$ oppure $I = R$. Pertanto R è privo di ideali non banali e dunque è un campo.