Algebra n. 3 - NOTE ALLA LEZIONE 1

Esercizio 1.3

Sono utili i seguenti richiami di aritmetica elementare.

Definizione: Siano $m_1, \dots, m_r$ numeri interi. Allora un numero intero d si dice un *massimo comune divisore* di $m_1, \dots, m_r$ se sono verificate le seguenti condizioni:
a) $d|m_i$ per ogni $i \in \{1, \dots, r\}$;
b) per ogni intero e tale che $e|m_i$ per ogni $i \in \{1, \dots, r\}$ si ha che $e|d$.

Proposizione: Siano $m_1, \dots, m_r$ numeri interi. Allora esiste un massimo comune divisore d di $m_1, \dots, m_r$. Inoltre i loro massimi comuni divisori sono d e $-d$.

Dimostrazione: Procediamo per induzione su $r \geq 2$ per provare che, se ∂ è un massimo comune divisore di $m_1, \dots, m_{r-1}$, allora detto d un massimo comune divisore di ∂ e m_r, si ha che d è un massimo comune divisore di $m_1, \dots, m_r$. In tal modo dimostreremo l'esistenza a partire dal caso particolare in cui $r = 2$, per il quale la proprietà è stata precedentemente stabilita, e che costituisce la base dell'induzione. Per il passo induttivo sia dunque $r > 2$, e supponiamo che esista un massimo comune divisore ∂ di $m_1, \dots, m_{r-1}$. Sia d come sopra. Allora $d|\partial$ e $d|m_r$. Poiché $\partial|m_i$ per ogni $i \in \{1, \dots, r-1\}$, per transitività segue che $d|m_i$ per ogni $i \in \{1, \dots, r-1\}$. Ciò prova a). Sia ora e un intero tale che $e|m_i$ per ogni $i \in \{1, \dots, r\}$. Allora, poiché, in particolare, $e|m_i$ per ogni $i \in \{1, \dots, r-1\}$, si avrà che $e|\partial$. Poiché si ha anche $e|m_r$, segue che $e|d$. Ciò prova b) e conclude la dimostrazione dell'esistenza.
Per la seconda parte dell'enunciato è sufficiente osservare che due massimi comuni divisori di $m_1, \dots, m_r$ si dividono reciprocamente, ossia sono associati, e, inoltre, due elementi associati hanno gli stessi divisori e gli stessi multipli.

Osservazione: Se $m_1, \dots, m_r$ non sono tutti nulli, si definisce $\mathrm{MCD}(m_1, \dots, m_r)$ come il loro massimo comune divisore positivo. Dalla dimostrazione precedente si ricava la seguente formula ricorsiva:

$$\mathrm{MCD}(m_1, \dots, m_r) = \mathrm{MCD}(\mathrm{MCD}(m_1, \dots, m_{r-1}), m_r).$$

In modo del tutto analogo si tratta la nozione di minimo comune multiplo di $m_1, \dots, m_r$.

Lemma di Bézout generalizzato
Siano $m_1, \dots, m_r$ numeri interi. Sia $d = \mathrm{MCD}(m_1, \dots, m_r)$. Allora esistono numeri interi $a_1, \dots, a_r$ tali che $a_1 m_1 + \cdots a_r m_r = d$.

Dimostrazione: Procediamo per induzione su r, considerando banale il caso $r = 1$ ed acquisito il caso $r = 2$ dalla versione del Lemma di Bézout già nota. Sia dunque $r > 2$ e supponiamo l'enunciato provato per $r-1$ interi. Posto $\partial = \mathrm{MCD}(m_1, \dots, m_{r-1})$, per l'ipotesi induttiva esistono numeri interi $a'_1, \dots, a'_{r-1}$ tali che $a'_1 m_1 + \cdots a'_{r-1} m_{r-1} = \partial$. Ora, sapendo che $d = \mathrm{MCD}(\partial, m_r)$, ed applicando la base dell'induzione per $r = 2$, si deduce che esistono numeri interi s, t tali che $s\partial + t m_r = d$. Ciò prova che gli interi $a_1 = s a'_1, \dots, a_{r-1} = s a'_{r-1}, a_r = t$ verificano l'uguaglianza richiesta.

Corollario
Nelle precedenti ipotesi, il sottogruppo di $\mathbb{Z}$ generato da $\{m_1, \dots, m_r\}$ è $\langle d \rangle$.

Dimostrazione: Dal Lemma segue immediatamente l'inclusione $\langle m_1, \dots, m_r \rangle \supset \langle d \rangle$. Per l'inclusione $\langle m_1, \dots, m_r \rangle \subset \langle d \rangle$ basta osservare che ogni combinazione lineare intera di $m_1, \dots, m_r$ è multipla di d, poiché tale è ogni m_i.