A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
ESERCITAZIONI. FOGLIO 3.

Definizione. Sia $(A, +, \cdot)$ un anello (associativo) unitario. Diremo che un elemento $a \in A$ è invertibile a sinistra se esiste un elemento $b \in A$ tale che $b \cdot a = 1$. Diremo che $a \in A$ è invertibile a destra se esiste un elemento $b \in A$ tale che $a \cdot b = 1$. Diremo che a è invertibile se a è invertibile sia a sinistra che a destra.
Diremo che $a \in (A, +, \cdot)$ è un divisore dello zero se esiste un elemento $b \in A \setminus \{0\}$ tale che $a \cdot b = 0$ oppure $b \cdot a = 0$; se inoltre $a \neq 0$ diremo che esso è un divisore dello zero non banale.

Esercizio 3.1. Sia $(A, +, \cdot)$ un anello (associativo) unitario.
(A) Mostrare che se $a \in A$ è invertibile allora l'inverso sinistro e l'inverso destro coincidono.
(B) Dimostrare che se $a \in A$ è un divisore dello zero non banale allora a non è invertibile.
(C) Assumiamo che $(A, +, \cdot)$ sia anche commutativo. Mostrare che l'insieme dei divisori dello zero è chiuso rispetto al prodotto.

Esercizio 3. 2. [1] Sia G un gruppo nel quale sia verificata per ogni coppia di elementi $a, b \in G$ l'uguaglianza: $(ab)^2 = a^2b^2$. Mostrare che il gruppo G è abeliano.

Esercizio 3.3. [2] Siano $a, b, x \in \mathbb{Z}$. Supponiamo che $a \,|\, x$, $b \,|\, x$ e $\mathrm{MCD}(a, b) = 1$. Mostrare che $ab \,|\, x$.

Esercizio 3. 4. Utilizzando l'algoritmo delle divisioni successive determinare l' MCD e una Identità di Bézout per la seguente coppia di numeri interi: 334 e 219. (*Invito. Allenatevi a casa a fare questo stesso tipo di esercizio con altre coppie di numeri*)

Esercizio 3. 5. Siano p e q due numeri primi distinti. Mostrare che $\{k\,p \mid k \in \mathbb{Z}\} \setminus \{k\,q \mid k \in \mathbb{Z}\}$ e $\{k\,q \mid k \in \mathbb{Z}\} \setminus \{k\,p \mid k \in \mathbb{Z}\}$ sono sottoinsiemi di $\mathbb{Z}$ di cardinalità numerabile.

Esercizio 3.6. Sia G un gruppo ed a un elemento di G tale che $a^k = 1$ per qualche $k \in \mathbb{N}$. Sia m il più piccolo intero positivo per cui $a^m = 1$. Mostrare che se $a^k = 1$ allora $m \,|\, k$. (*Suggerimento. Usare la minimalità di $m \in \mathbb{N}$ e la divisione con resto*)
Sia G un gruppo abeliano e siano $a, b \in G$ due elementi il cui prodotto in G è non banale e tali che $a^p = 1$ e $b^q = 1$ per $p, q \in \mathbb{N}$ due numeri primi distinti. Mostrare che il più piccolo $k \in \mathbb{N}$ per cui $(ab)^k = 1$ è $k = p\,q$. (*Suggerimento. Usare il Lemma di Euclide*)

[1] Tratto dal libro Algebra di I.N. Herstein, Esercizio 3, Sezione 2.3
[2] Tratto dal libro Algebra di I.N. Herstein, Esercizio 4, Sezione 1.3

ESERCIZI PER CASA

Esercizio 3.7. Consideriamo l'insieme $\mathfrak{M}_{2,2}(\mathbb{Z})$ delle matrici 2×2 a coefficienti in $\mathbb{Z}$. Consideriamo le due operazioni seguenti:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

(A) Verificare che $(\mathfrak{M}_{2,2}(\mathbb{Z}), +)$ è un gruppo abeliano.
(B) Verificare che $(\mathfrak{M}_{2,2}(\mathbb{Z}), +, \cdot)$ è un anello (associativo) unitario. E' commutativo?
(C) Esistono divisori dello zero non banali? In caso affermativo esibirne uno.
(D) Richiamiamo il seguente fatto di algebra lineare: sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{M}_{2,2}(\mathbb{R})$ l'inversa di A è data dalla formula seguente:

$$A^{-1} = \frac{1}{\det(A)} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Definiamo $\mathrm{SL}_2(\mathbb{Z}) = \{A \in \mathfrak{M}_{2,2}(\mathbb{Z}) \mid \det(A) = 1\}$. Mostrare che tale insieme è un gruppo rispetto al prodotto. (*Suggerimento. Osservare che l'inversa di un elemento $A \in \mathrm{SL}_2(\mathbb{Z})$ è ancora in* $\mathrm{SL}_2(\mathbb{Z})$).
(E) Mostrare che la matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ commuta con tutte le matrici in tale insieme se e solo se $A = \pm Id = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. (*Suggerimento. Utilizzare la condizione sul determinante e quella di commutazione con le matrici* $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *per ottenere equazioni per i coefficienti*).
(F) Qual è l'ordine del gruppo generato dalle potenze dalla matrice $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$?
(G) Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ e supponiamo che i coefficienti di A siano tutti non nulli. Mostrare che $\mathrm{MCD}(a, b) = 1$. (*Suggerimento. Sfruttare l'identità di Bézout*)
(H) Mostrare che se $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ allora $\begin{pmatrix} a & b \\ c+ka & d+kb \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ per ogni $k \in \mathbb{Z}$.