TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 4

Esercizio 4.1. Enunciate a dimostrate il Lemma dei Cassetti.

Esercizio 4.2. Si mostri che se A è un anello commutativo con unità, e A è finito, allora un elemento di A o è invertibile, o è uno 0-divisore.

Esercizio 4.3 (Del tutto facoltativo). Sia A un anello finito, non necessariamente commutativo. Supponiamo che in A ci sia un elemento a che non è uno 0-divisore, nel senso che per ogni $b \in A$ si ha che da $ab = 0$ segue $b = 0$ e da $ba = 0$ segue $b = 0$.

(1) Si mostri che le funzioni $A \to A$ definite da $x \mapsto ax$ e $y \mapsto ya$ sono iniettive e dunque suriettive. Dunque ogni elemento b di A si scrive nella forma $b = ax$ e anche nella forma $b = ya$, per opportuni $x, y \in A$.
(2) Si mostri che esistono elementi $e, f \in A$ tali che $ae = a = fa$.
(3) Si mostri che $be = b = fb$ per ogni $b \in A$.
(4) Si mostri che $e = f$, e che questo è l'elemento neutro 1 per il prodotto.
(5) Si mostri che esistono $b, c \in A$ tali che $ba = 1 = ac$.
(6) Si mostri che $b = c$, e che questo elemento è l'inverso di a.
(7) Si mostri che gli elementi di A che non sono 0-divisori (nel senso detto più sopra) sono invertibili.

Esercizio 4.4.

(1) Definite un elemento neutro per un insieme con una operazione (binaria).
(2) Si mostri che in un insieme con un'operazione, l'elemento neutro, se c'è, è unico.
(3) Definite un semigruppo.
(4) Definite un monoide.
(5) Definite un elemento simmetrizzabile, e un suo simmetrico, in un monoide.
(6) Fate vedere che se un elemento di un monoide è simmetrizzabile, allora l'elemento simmetrico è unico.

Esercizio 4.5.

(1) Sia $(M, \cdot, 1)$ un monoide, a $a, b \in M$ elementi invertibili.
   (a) Si mostri che 1 è invertibile, e $1^{-1} = 1$,
   (b) si mostri che a^{-1} è invertibile, e $(a^{-1})^{-1} = a$,
   (c) si mostri che ab è invertibile, e $(ab)^{-1} = b^{-1}a^{-1}$.
(2) Si mostri che se $(M, \cdot, 1)$ è un monoide, e G è l'insieme degli elementi invertibili di M, allora $(G, \cdot, 1)$ è un gruppo.

Esercizio 4.6. Rimosso, era un duplicato.

Esercizio 4.7. Rimosso, era un duplicato.

Esercizio 4.8.

(1) Si mostri che per calcolare il resto della divisione di x per $n = 2^a 5^b$ è sufficiente guardare le ultime c cifre decimali di x, ove $c = \max\{a, b\}$.

(SUGGERIMENTO: Visto che me l'avete chiesto in tanti, scrivo una soluzione. Notiamo subito che $n \mid 10^c$. E precisiamo la domanda, nel senso che vogliamo far vedere che il resto della divisione di un numero x per n (la notazione è quella della domanda) è lo stesso del resto della divisione per n del numero x' formato dalle ultime c cifre decimali di x. Ma per definizione di x' si ha $x = x' + 10^c y$ per qualche y, dunque $n \mid 10^c \mid x - x'$, sicché per un risultato precedente x e x' divisi per n danno lo stesso resto.)

(2) (Facoltativo) Supponiamo che per calcolare il resto della divisione per n di *ogni* numero x sia sufficiente guardare le ultime c cifre decimali di x. Si mostri che n è della forma $2^a 5^b$ (con $c \geq a, b$).

(SUGGERIMENTO: Dato un numero x, sia x' il numero formato dalle ultime c cifre decimali di x, sicché come sopra $x = x' + 10^c y$ per qualche y. Supponiamo che per ogni x, il resto della divisione di x e x' per n sia lo stesso. Allora, per il risultato citato sopra, si ha $x \equiv x' \pmod{n}$, dunque $n \mid x - x' = 10^c y$. Siccome questo deve valere *per ogni numero* x, in particolare vale per $y = 1$, e dunque...)

Esercizio 4.9 (Facoltativo al momento). Si dica quali e quanti sono gli elementi $[a] \in \mathbf{Z}/n\mathbf{Z}$ tali che

- $[a]^2 = [0]$.
- $[a]^k = [0]$ per qualche k.

Esercizio 4.10. Siano A, B insiemi, e $f : A \to B$ una funzione.

(1) Si mostri che f ha un'inversa sinistra se e solo se è iniettiva.
(2) Si mostri che f ha un'inversa destra se e solo se è suriettiva.
(3) Si mostri che se f ha sia un'inversa destra che sinistra, allora queste coincidono, e in tal caso la funzione è biiettiva.
(4) Si dia un esempio in cui f ha infinite inverse sinistre, e un altro in cui f ha infinite inverse destre.

Esercizio 4.11 (**Ho cambiato la notazione in questo esercizio, perché la versione precedente creava confusione, e l'ho espanso un pochino**).

Sia $f : A \to C$ una funzione.

Se $S \subseteq C$ si scrive

$$f^{-1}(S) = \{\, a \in A : f(a) \in S \,\} \subseteq A.$$

In particolare per $c \in C$, si ha

$$f^{-1}(\{\, c \,\}) = \{\, a \in A : f(a) \in \{\, c \,\} \,\} = \{\, a \in A : f(a) = c \,\}$$

è l'insieme di tutti gli elementi di a che sono mandati in c da f.

Attenzione! f è una funzione qualsiasi, dunque non è detto che abbia un'inversa. Il simbolo f^{-1}, in questo contesto, non denota dunque un'inversa: in generale,

se $S \subseteq C$,

$$f^{-1}(S) = \{\, a \in A : f(a) \in S \,\}$$

è un sottoinsieme di A, che potrebbe anche essere vuoto.

(1) Mostrate che f è iniettiva se e solo se $|\, f^{-1}(\{\, c \,\})\,| \leq 1$ per ogni $c \in C$. **Attenzione!** Qui $|\, f^{-1}(\{\, c \,\})\,|$ indica la cardinalità, ovvero il numero di elementi, dell'insieme $f^{-1}(\{\, c \,\})$.
(2) Mostrate che f è suriettiva se e solo se $f^{-1}(\{\, c \,\}) \neq \emptyset$ per ogni $c \in C$.
(3) Mostrate che f è biiettiva se e solo se $|\, f^{-1}(\{\, c \,\})\,| = 1$ per ogni $c \in C$. In questo caso f ha dunque un'inversa $f^{-1} : C \to A$, per cui vale

$$f^{-1}(\{\, c \,\}) = \left\{\, f^{-1}(c) \,\right\},$$

per ogni $c \in C$

Esercizio 4.12. Per ognuno dei monoidi M seguenti, si dica chi è il gruppo G degli elementi invertibili.

(1) $(\mathbf{Z}, \cdot, 1)$.
(2) $(M(n, F), \cdot, 1)$, ove $M(n, F)$ sono le matrici $n \times n$ a coefficienti nel campo F, "$\cdot$" è il prodotto fra matrici, e 1 è la matrice identica $n \times n$.
(3) $(M(n, \mathbf{Z}), \cdot, 1)$, ove $M(n, \mathbf{Z})$ sono le matrici $n \times n$ a coefficienti interi, "$\cdot$" è il prodotto fra matrici, e 1 è la matrice identica $n \times n$.
(4) $(M(A), \circ, 1_A)$, il monoide delle funzioni su A.

Esercizio 4.13. Enunciate la definizione della funzione di Eulero.

Esercizio 4.14.

(1) Mostrate che se p è un numero primo, e $e \geq 1$, allora
$$\varphi(p^e) = (p-1)p^{e-1}.$$
(2) (Facoltativo) Mostrate che se $a > 1$ è un intero, e $e \geq 1$, allora
$$\varphi(a^e) = \varphi(a)a^{e-1}.$$
(SUGGERIMENTO: Questo richiede la formula precedente, e la moltiplicatività della funzione di Eulero.)

Esercizio 4.15. Si mostri che se p, q sono numeri primi distinti, allora
$$\varphi(pq) = pq - p - q + 1.$$

Esercizio 4.16. Sia n un numero intero positivo, che conoscete. Sapete anche che n è il prodotto di due numeri primi distinti p, q, che però non conoscete.

- Mostrate che se qualcuno vi dice p, q, allora siete in grado di calcolare $\varphi(n)$.
- Mostrate che se qualcuno vi dice $\varphi(n)$, allora siete in grado di calcolare p, q, al solo prezzo di risolvere un'equazione di secondo grado.