TRENTO, A.A. 2021/22
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 5

Esercizio 5.1.
Siano A, C insiemi, e $f : A \to C$ una funzione.

(1) Mostrate che f è iniettiva se e solo se $|\, f^{-1}(\{\, c\,\})\,| \le 1$ 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 $f^{-1}(\{\, c\,\}) \ne \emptyset$ 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 5.2 (Precisazione). Enunciate e dimostrate la forma quantitativa del Lemma dei Cassetti.

Esercizio 5.3. Sia A un anello.

(1) Mostrate che valgono le *regole dei segni*
$$a(-b) = (-a)b = -ab, (-a)(-b) = ab.$$
Qui "$-$" indica l'*opposto*, cioè $-a$ è quell'unico elemento tale che $a+(-a) = 0$.

(Suggerimento: Ad esempio, per mostrare che $a(-b) = -ab$ dovete notare che)
$$ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0.$$
(2) Per $a, b \in A$, definiamo la *differenza*
$$a - b = a + (-b).$$
Dunque, attenzione, a sinistra "$-$" indica la differenza che sto definendo, a destra "$-$" indica l'*opposto*
   (a) Mostrate che valgono le proprietà distributive
$$(a - b)c = ac - bc \qquad c(a - b) = ca - cb.$$
   (Suggerimento: $(a-b)c = (a+(-b))c = ac+(-b)c = ac+(-bc) = ac - bc$, dove ho usato le regole dei segni.)
   (b) La differenza è una operazione associativa?

   (Suggerimento: Fornite una dimostrazione o un controesempio.)

Esercizio 5.4. Sia A un anello commutativo, $a, x, y \in A$. Si mostri che se a non è uno 0-divisore, allora $ax = ay$ implica $x = y$, ovvero si può semplificare per a.

Esercizio 5.5. Sia $A \neq \{ 0 \}$ un anello commutativo con unità.
Si mostri che se A è finito, allora per ogni $a \in A$ si ha

(1) o a è invertibile,
(2) o a è uno 0-divisore.

Esercizio 5.6. Si mostri che per un anello commutativo $A \neq \{ 0 \}$ sono equivalenti

(1) l'unico 0-divisore è 0,
(2) in A vale la legge di annullamento del prodotto.

Esercizio 5.7.

(1) Si dia la definizione di dominio e di campo.
(2) Sia A un anello commutativo con unità.
    (a) Si mostri che se A è un campo, allora A è un dominio.
    (b) Si dia un esempio di un dominio che non è un campo.
    (c) Si mostri se A è finito, allora equivalenti:
        (i) A è un dominio,
        (ii) A è un campo.

Esercizio 5.8 (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 5.9.

(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 invertibile in un monoide.
(6) Fate vedere che se un elemento di un monoide è invertibile allora l'elemento inverso è unico.

Esercizio 5.10.

(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 5.11. 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 5.12. 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 5.13. Enunciate la definizione della funzione di Eulero.

Esercizio 5.14. Mostrate che se p è un numero primo, ed $e \geq 1$, allora

$$\varphi(p^e) = (p-1)p^{e-1}.$$