TRENTO, A.A. 2021/22
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 3

Esercizio 3.1. Si dimostri, per induzione o con il principio del minimo intero, il

Teorema. Siano $a, b \in \mathbf{Z}$ *con* $a \geq 0$ *e* $b > 0$. *Allora esistono* $q, r \in \mathbf{N}$ *tali che*

$$\begin{cases} a = bq + r \\ 0 \leq r < b. \end{cases}$$

Esercizio 3.2.

(1) Si definisca la relazione di congruenza modulo n.
(2) Si descrivano le relazioni di congruenza modulo 0 e modulo 1.
(3) Si dimostri, *usando direttamente la definizione* che la relazione di congruenza è una relazione di equivalenza.
(4) Si mostri che per $n > 0$ sono equivalenti
    (a) $a \equiv b \pmod{n}$, e
    (b) a e b divisi per n danno lo stesso resto.
(5) Si deduca dal punto (4) che la congruenza modulo n è una relazione di equivalenza.

Esercizio 3.3. Si mostri che sono equivalenti le affermazioni

- $a \equiv b \pmod{n}$, e
- $a \equiv b \pmod{-n}$.

Esercizio 3.4. Sia A un insieme non vuoto, e R una relazione di equivalenza su di esso.

- Si mostri che per ogni $a \in A$ si ha $a \in [a]$.
- Si mostri che per $a, b \in A$ sono equivalenti:
    (1) aRb,
    (2) $a \in [b]$,
    (3) $[a] \subseteq [b]$,
    (4) $[a] = [b]$,
    (5) $[a] \cap [b] \neq \emptyset$.

Esercizio 3.5. Sia $A \neq \emptyset$ un insieme, e $\mathcal{P}$ un insieme di sottoinsiemi non vuoti di A. Si mostri che sono equivalenti

(1) ogni $a \in A$ sta in uno e un solo elemento di $\mathcal{P}$, e
(2) A è unione disgiunta degli elementi di $\mathcal{P}$, ovvero $A = \bigcup \mathcal{P}$, e se $P \neq Q \in \mathcal{P}$, allora $P \cap Q = \emptyset$.

(Vi ricordo che $\bigcup \mathcal{P} = \{ x \in A : \text{esiste } P \in \mathcal{P} \text{ tale che } a \in P \}$.)

Esercizio 3.6. Si mostri che se A è un insieme non vuoto, R è una relazione di equivalenza su A, e per $a \in A$ definiamo la sua classe

$$[a] = \{ x \in A : xRa \},$$

allora

$$\{ [a] : a \in A \}$$

è una partizione di A.

Esercizio 3.7. Sia $n \geq 2$. Si mostri che la classe di congruenza modulo n di $a \in \mathbf{Z}$ è

$$[a] = \{ a + nt : t \in \mathbf{Z} \}.$$

Esercizio 3.8. Siano $x, n \in \mathbf{Z}$, con $n \neq 0$. Sia $[x]$ la classe di congruenza di x modulo n,

Si mostri che sono equivalenti

(1) n divide x,
(2) $x \equiv 0 \pmod{n}$,
(3) $[x] = [0]$.

Esercizio 3.9. Siano $a, r, n \in \mathbf{Z}$, con $n > 0$, e $0 \leq r < n$. Si mostri che sono equivalenti

(1) $a \in [r]$, e
(2) r è il resto della divisione di a per n.

Esercizio 3.10. Sia $n \geq 2$. Si mostri che le classi di congruenza modulo n sono n (distinte), e sono

$$[0], [1], [2], \dots, [n-1].$$

Esercizio 3.11. Si dia la definizione di gruppo, e si faccia vedere che elemento neutro e inversi sono unici.

Esercizio 3.12 (Facoltativo). Sia A un insieme non vuoto, su cui è definita una operazione $\cdot$. Supponiamo che $\cdot$ sia associativa, che cioè per $a, b, c \in A$ valga

$$a(bc) = (ab)c.$$

(Qui indichiamo l'operazione semplicemente con la giustapposizione, $ab = a \cdot b$.)

Siano $a_1, \dots, a_n \in A$. Si mostri che tutti i possibili prodotti di $a_1, \dots, a_n$ in quest'ordine coincidono.

Occorre per prima cosa precisare questa ultima espressione. Definiamo dunque, per ricorrenza su n, un *prodotto ammissibile* di $a_1, \dots, a_n$.

Se $n = 1$, l'unico prodotto ammissibile è a_1. Se $n = 2$, l'unico prodotto ammissibile è $a_1 a_2$. Se $n \geq 3$, i prodotti ammissibili si ottengono scrivendo $n = s + t$, con $s, t \geq 1$, e prendendo il prodotto di un prodotto ammissibile di $a_1, \dots, a_s$ con un prodotto ammissibile di $a_{s+1}, \dots, a_n$.

Adesso provate a dimostrare per induzione su n che tutti i prodotti ammissibili di $a_1, \dots, a_n$ coincidono col *prodotto normato a sinistra*

$$((\dots(a_1 a_2) a_3) \dots) a_n),$$

cioè col prodotto in cui prima calcolo $a_1 a_2$, poi moltiplico il risultato a destra per a_3, poi moltiplico il risultato a destra per a_4, ecc.

(Suggerimento: (Lascio però da parte qualche dettaglio.) Sia P un prodotto ammissibile di $a_1, \dots, a_n$. Per definizione sarà della forma $P = ST$, ove S è un prodotto ammissibile di $a_1, \dots, a_s$, e T è un prodotto ammissibile di $a_{s+1}, \dots, a_n$, con $s + t = n$.

Procedo a una doppia induzione, prima su n, e in subordine su t.

Se $t = 1$, per induzione su n si ha che S è un prodotto normato a sinistra, e dunque lo è anche P.

Se $t > 1$, allora posso scrivere $T = UV$, ove U, V sono due prodotti ammissibili. Per l'associatività (su tre termini) ho $P = ST = S(UV) = (SU)V$. Ora V è un prodotto di un numero di a_i minore di t, dunque per l'induzione su t, il prodotto $(SU)V$ si scrive come un prodotto normato a sinistra.)

Esercizio 3.13 (Facoltativo, magari lo espando). Il numero di modi per mettere le parentesi in un prodotto di $a_1, \dots, a_n$ è dato dal *numero di Catalan* C_{n-1}. Per questo al momento vi rimando alla Wikipedia