Lezione 05 - 10/10/2022

Esercizio operazioni ben poste

$$\begin{aligned} \mathbb{R} \quad & x \sim_1 y \text{ se } [x] = [y] \\ & x \sim_2 y \text{ se } \{x\} = \{y\} \end{aligned}$$

Dove con:

- $[x] = \text{parte intera } \leq x$
- $\{x\} = \text{parte frazionaria } x - [x]$

$\sim_1$ e $\sim_2$ sono relazioni di equivalenza in quanto sono definite in **termini di uguaglianza**.

Chiamiamo:

- $\bar{x} = x \mod \sim_1 \quad (\bar{x} = \{y \in \mathbb{R} : y \sim_1 x\})$
- $\tilde{x} = x \mod \sim_2$

Definiamo

$$\begin{aligned} \bar{x} +_1 \bar{y} = \overline{x+y} \\ \tilde{x} +_2 \tilde{y} = \widetilde{x+y} \end{aligned}$$

Sono ben poste?

$+_1$ **non è ben posta**. Vengano presi $\overline{0.2} = \overline{0.8}$

$$\begin{aligned} \overline{0.2} + \overline{0.2} = \overline{0.2 + 0.2} = \overline{0.4} = 0 \\ \overline{0.8} + \overline{0.8} = \overline{0.8 + 0.8} = 1.6 \end{aligned}$$

Ma $0 \neq 1.6$ anche se abbiamo posto $\overline{0.2} = \overline{0.8}$. Questo significa che l'operazione **dipende** dai rappresentanti che vengono scelti.

$+_2$ invece è **ben posta**. Per dimostrarlo si osserva che

$$x \sim_2 y \Leftrightarrow x - y \in \mathbb{Z} \quad \text{(differiscono per un intero)}$$

È facile vedere che $+_2$ è ben posta:

$$\widetilde{x} = \widetilde{x_1}, \tilde{y} = \widetilde{y_1} \text{ allora } \widetilde{x+y} = \widetilde{x_1 + y_1}$$

<u>Ipotesi</u>:

$$x - x_1 = n, y - y_1 = m$$
$$x + y - (x_1 + y_1) = x - x_1 + y - y_1 = n + m \in \mathbb{Z}$$

Definizioni: divisore dello zero, dominio di integrità, elemento invertibile, elementi associati, elemento irriducibile, elemento primo

Sia A un **anello commutativo con unità**:

1. Un elemento $a \in A, a \neq 0$ si dice **divisore dello zero** se esiste $b \in A, b \neq 0 : ab = 0$
2. Un **dominio di intregrità** è un anello commutativo con unità **privo** di divisori dello 0
3. Se $a, b \in A$ diciamo che $a \mid b$ se $\exists c \in A : b = ac$
4. Un elemento $a \in A : a \mid 1$ si dice **invertibile**
5. Due elementi $a, b \in A : a \mid b \wedge b \mid a$ si dicono **associati**
6. Un elemento $a \in A, a \neq 0, a$ non invertibile si dice **irriducibile** se

$$a = bc \Rightarrow b \text{ invertibile o } c \text{ invertibile}$$

7. Un elmento $a \in A, a \neq 0, a$ non invertibile si dice **primo** se

$$a \mid bc \Leftrightarrow a \mid b \text{ oppure } a \mid c$$

Commenti ed esempi

- In $\mathbb{Z}_6, \overline{2} \cdot \overline{3} = \overline{0}$

  Per lo stesso motivo, se $n = ab \text{ con } a, b \neq 1$ allora $\mathbb{Z}_n$ non è un domino di integrità

- È stato già dimostrato che $\mathbb{Z}$ è un dominio di integrità

- Dire che $a \mid 1$ significa dire che $\exists b \in A : ab = 1$

- È immediato osservare che in $\mathbb{Z}$ gli unici elementi invertibili sono ± 1 perchè la relazione in $\mathbb{Z}$

  $$ab = 1$$

  è possibile solo quando $a = b = 1$ oppure $a = b = -1$

Proposizione

In un dominio di integrità

$$a \text{ primo} \Rightarrow a \text{ riducibile}$$

Dimostrazione: Supponiamo a primo e facciamo vedere che se $a = bc$ allora b è invertibile o c è invertibile.

Se $a = bc$, in particolare $a \mid bc$, quindi per ipotesi $a \mid b$ oppure $a \mid c$.

Se $a \mid b$ significa che $b = ad$, quindi $a = bc$ diventa

$$\begin{gathered} a = adc \\ a(1 - dc) = 0 \end{gathered}$$

Poichè $a \neq 0$ per l'ipotesi, $1 - dc = 0$ ovvero $dc = 1$ ovvero c è **invertibile**.

Se $a \mid c$ si procede allo stesso modo: $c = af$, allora

$$\begin{aligned} a &= bc \\ a &= baf \\ a(1{-}bf) &= 0 \\ \Rightarrow bf = 1 &\Leftrightarrow b \text{ è invertibile} \end{aligned}$$

MCD e algoritmo euclideo in Z

Definizione: $a, b \in \mathbb{Z}$. Un numero $d \in \mathbb{Z}$ si dice un MCD(Massimo Comun Divisore) tra a e b se:

1. $d \mid a, \quad d \mid b$
2. $d' \mid a, \quad d' \mid b \Rightarrow d' \mid d$ (d è il più grande)

Nomenclatura: due interi a, b tali che $\mathrm{MCD}(a, b) = 1$ si dicono **coprimi**, ovvero non hanno divisori comuni.

Proposizione

Dati $a, b \in \mathbb{Z}, b \neq 0\ \exists! q, r \in \mathbb{Z} : a = bq + r,\ 0 \leq r < |b|$.

Esempi:

$$
\begin{aligned}
29, 7 &\rightsquigarrow 29 = 7 \cdot 4 + 1 \\
-29, 7 &\rightsquigarrow -29 = 7 \cdot (-5) + 6 \\
29, -7 &\rightsquigarrow 29 = (-7) \cdot (-4) + 1 \\
-29, -7 &\rightsquigarrow -29 = (-7) \cdot 5 + 6 \\
6, 7 &\rightsquigarrow 6 = 7 \cdot 0 + 6
\end{aligned}
$$

Dimostrazione: Ricordiamo che dati a, b dobbiamo trovare q, r tali che

$$a = bq + r, \quad 0 \leq r < |b|$$

Vanno dimostrate **esistenza** e **unicità** di questi due elementi

- **Esistenza**:

  Sia $a > 0$. Procediamo per induzione su a.

  Se $a = 0$, poniamo $q = 0$ e $r = 0$ (base)

  Se $|b| > a$, posso porre $q = 0$ e $r = a$

  Quindi posso supporre $|b| \leq a$, cioè $a - |b| \geq 0$ e $a > a - |b|$, per induzione esistono q' e r' tali che

$$
\begin{aligned}
a - |b| &= q'b + r', \quad 0 \leq r' < |b| \\
a &= |b| + q'b + r'
\end{aligned}
$$

Se $b > 0$

$$a = \underbrace{b(1+q')}_{=q} + \underbrace{r'}_{=r} \quad 0 \leq r < |b|$$

Se $b < 0$

$$\begin{aligned} a &= -b + q'b + r' \\ &= \underbrace{b(q'-1)}_{=q} + \underbrace{r'}_{=r} \quad 0 \leq r < |b| \end{aligned}$$

Se $a < 0,\ -a > 0$ posso quindi usare la prima parte con $-a$. Per i dettagli, vedere sul libro di testo.

- **Unicità**

$$a = \overbrace{bq + r}^{(1)} = \overbrace{bq' + r'}^{(2)} \quad \begin{aligned} 0 &\leq r < |b| \\ 0 &\leq r' < |b| \end{aligned}$$

Possiamo assumere $r' \geq r$. Sottraiamo (1) da (2)

$$\begin{aligned} &0 \leq r' - r = b(q-q') \\ &|b||q-q'| = |r'-r| = r'-r \leq r' < |b| \end{aligned}$$

Siccome $b \neq 0$, da $|b||q-q'| < |b|$ segue che $|q-q'| < 1 \Rightarrow q = q'$.
Ma se $q = q'$

$$bq + r = bq' + r' = bq + r'$$

Quindi bq ha come resti sia r che r', che deve significare che $r = r'$.

Teorema - Identità di Bezout

Dati $a, b \in \mathbb{Z}$ non entrambi 0, esiste $d = \mathrm{MCD}(a,b)$. Inoltre esistono interi $s, t \in \mathbb{Z}$ tali che:

$$d = sa + tb$$

tale espressione viene chiamata **identità di Bezout** e ne esistono infinite.

Dimostrazione: ricordiamo che il principio di induzione è equivalente al principio del minimo: ogni sottoinsieme $S \neq \emptyset, S \subseteq \mathbb{N}$, ha minimo.

Poniamo $S = \{xa + yb > 0 | x, y \in \mathbb{Z}\}$:

- $S \neq \emptyset$: supponiamo $a \neq 0$. Se $a > 0, a \in S$. Se $a < 0, -a \in S$. Per costruzione $S \subseteq \mathbb{N}$.

  Per il principio del minimo esiste $d = \min S$. Dico che $d = \mathrm{MCD}(a, b)$. Dimostro che $d \mid a$ facendo la divisione con resto di a per d e mostrando che il resto è 0.

  $$\begin{gathered} a = qd + r, \quad 0 \leq r < d \\ 0 \leq r = a - qd \overset{*}{=} a - q(x_0 a + y_0 b) = \\ = (1 - x_0 q)a - q y_0 b \leq d \end{gathered}$$

  $*$: $d = x_0 a + y_0 b$ in quanto $d \in S$ siccome abbiamo detto che $d = \min S$ e gli elementi di S sono della forma $xa + yb$.

  Se $r \neq 0$, ho dimostrato che $r \in S$, $r < d = \min S$ (contraddizione, in quanto risulta che r è minore di d).

  Questo significa che $r = 0$ e quindi abbiamo dimostrato che $d \mid a$ e similmente $d \mid b$. Inoltre è chiaro che se $d' \mid a$ e $d' \mid b$ allora $d' \mid d$.

  Infatti se $a = hd', b = kd'$ allora

  $$d = x_0 a + y_0 b = x_0 h d' + y_0 k d' = (x_0 h + y_0 k) d'$$

  e qunque $d' \mid d$.