Algebra I

martedì 6 ottobre 2020 11:18

Osservazioni sull'ultima lezione.

D dominio di integrità: anello commutativo (con unità) in cui vale la legge di annullamento del prodotto

$ab = 0 \Rightarrow a = 0$ opp. $b = 0$.

$\mathbb{Z}$ ✓ $\mathbb{Q}$ ✓ $\mathbb{R}$ ✓

Da questa proprietà segue una proprietà di cancellazione.

$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0 \Rightarrow b - c = 0$

$a \neq 0$ ($a \neq 0$)

In un dominio d'integrità posso cancellare da entrambi i membri i fattori comuni NON NULLI

$\Downarrow$

$b = c$

Sulla definizione di gruppo.

G — insieme con moto $\circ : G \times G \to G$ operazione su G.

~~$\circ(a,b)$~~ $a \circ b$

associativa.

$a \circ (b \circ c) = (a \circ b) \circ c$ "Si possono rimuovere le parentesi senza danni".

Esiste un elemento neutro $e \in G$ (a seconda dei casi 0, 1, ...)

$a \circ e = e \circ a = a \quad \forall a \in G$.

Ogni elemento possiede un inverso rispetto a $\circ$.

$\forall a \in G$ posso trovare $\bar{a} \in G$ tale che

$a \circ \bar{a} = \bar{a} \circ a = e$.

---

① L'elemento neutro in un gruppo è unico

Dim. se e, u sono entrambi elementi neutri, allora

Dim:

$$e = e \circ u = u$$

(2) Ogni elemento possiede un solo inverso.

Dim: se $\bar{a}, a'$ sono entrambi inversi di a, allora

$$\begin{array}{ccc} \bar{a} \circ (a \circ a') & = & (\bar{a} \circ a) \circ a' \\ \| & & \| \\ \bar{a} = \bar{a} \circ e & & e \circ a' = a' \end{array}$$

(3a) Se $\bar{a}$ è l'inverso di a, allora a è l'inverso di $\bar{a}$

Compattamente: $\bar{\bar{a}} = a$ $\quad (a^{-1})^{-1} = a$ $\quad -(-a) = a$

($(a^{-1})^{-1} = a$: notazione moltiplicativa; $-(-a) = a$: notazione additiva.)

(3b) $\overline{ab} = \bar{b}\,\bar{a}$

$$(ab)(\bar{b}\,\bar{a}) = a(b\bar{b})\bar{a} = ae\bar{a} = a\bar{a} = e$$

$$(\bar{b}\,\bar{a})(ab) = \bar{b}(\bar{a}a)b = \bar{b}eb = \bar{b}b = e$$

$$(ab)^{-1} = b^{-1}a^{-1}$$

$$-(a+b) = -a - b$$

← La notazione additiva si usa solo quando il gruppo è abeliano

(4) Se in un gruppo un elemento si comporta come l'identità, ANCHE RISPETTO SOLO A UN ELEMENTO, allora è l'identità.

$$u \circ x = x \implies \begin{array}{ccc} (u \circ x) \circ \bar{x} & = & x \circ \bar{x} \\ \| & & \| \\ u \circ (x \circ \bar{x}) & & e \\ \| & & \\ u \circ e = u & & \end{array}$$

funziona anche dall'altro lato.

(destro)

(5) in un gruppo un inverso sinistro di un elemento è automaticamente l'inverso

$$y \circ x = e \Longrightarrow (y \circ x) \circ \bar{x} = e \circ \bar{x} = \bar{x}$$

$$\| \quad y \circ (x \circ \bar{x})$$

$$\| \quad y \circ e = y$$

$(\mathbb{Z}, +)$ $\quad \circ = +$, $e = 0$, $\bar{a} = -a$

Aritmetica = Proprietà algebriche dell'anello $\mathbb{Z}$.

Divisione euclidea ← divisione con resto.

$17 = 3 \cdot 5 + 2$ divisione euclidea

- Se $a, b \in \mathbb{N}$ e $b \neq 0$ allora esistono $q, r \in \mathbb{N}$ tali che

$$a = qb + r, \quad 0 \leq r < b.$$

Dim: $X = \{ n \in \mathbb{N} \mid nb > a \} \subseteq \mathbb{N}$

Oss: X è non vuoto. $b \neq 0$ $b \geq 1$

$0 \in X$? no

$(a+1)b \geq (a+1) \cdot 1 = a + 1 > a$ $\Leftrightarrow$ $0 = 0 \cdot b > a$

$a + 1 \in X$.

Per il principio di buon ordinamento X possiede un minimo elemento, che non è 0. Lo indico con $q+1$. $\boxed{q \in \mathbb{N}}$.

$$q+1 \in X \qquad (q+1)b > a$$
$$q \notin X \qquad qb \neq a \iff qb \leq a$$

$$qb \leq a < (q+1)b$$
$$qb \leq (a-qb) + qb < b + qb$$
$$0 \leq a - qb < b$$
$$\Rightarrow r$$

$$a - qb = r \iff \boxed{a = qb + r}$$

Divagazione (gruppale) $G, \circ, e \ldots$

Un **sottogruppo** del gruppo G è un sottoinsieme $X \subseteq G$ che è un gruppo rispetto all'operazione di G.

ϕ *

- L'associatività è l'unica cosa che non serve controllare.
- Deve esserci in X un elemento neutro che fuziona con tutti gli elementi di X

$u \in X \qquad u \circ x = x \circ u = x \quad \forall x \in X.$

$\Rightarrow u = e.$

$\boxed{e \in X}$

X [illegible] un inverso

- Ogni elemento di X deve possedere un inverso in X $\quad x \circ \bar{x} = \bar{x} \circ x = e$.

↑ che è sicuramente l'inverso di x nel gruppo G.

$$x \in X \Longrightarrow \bar{x} \in X$$

- Se $x, y \in X$ il risultato $x \circ y$ deve ancora essere un elemento di X

ALTRIMENTI NON È UN'OPERAZIONE

$$x, y \in X \Longrightarrow x \circ y \in X$$

$e \circ e = e \Longrightarrow \bar{e} = e$

Definizione alternativa: G gruppo. $X \subseteq G$ si dice sottogruppo se

- $e \in X$
- $x \in X \Longrightarrow \bar{x} \in X$
- $x, y \in X \Longrightarrow x \circ y \in X$.

Sottogruppi banali

Esempi: • G è un sottogruppo di G.

• $\{e\}$ è un sottogruppo di G.

$(\mathbb{Z}, +)$

Quindi, che cos'è un sottogruppo del gruppo $\mathbb{Z}$?

È un sottoinsieme $X \subseteq \mathbb{Z}$

$0 \in X$

$x \in X \Longrightarrow -x \in X$

$x, y \in X \Longrightarrow x + y \in X$

Struttura dei sottogruppi di $(\mathbb{Z}, +)$

Esempi: • $\mathbb{Z}$ è un sottogruppo $= (1)$

• $2\mathbb{Z}$ è un sottogruppo $= (0)$

- $X = \{\text{numeri pari}\} = \{2k \mid k \in \mathbb{Z}\}$
$= \{0, \pm 2, \pm 4, \pm 6, \pm 8, \dots\} = (2)$

$2 \cdot h + 2 \cdot k = 2(h+k)$. è un sottogruppo

- $d \in \mathbb{Z}$ $\quad X = \{dk \mid k \in \mathbb{Z}\}$.

$0 \in X \qquad 0 = d \cdot 0$

$x \in X \Rightarrow -x \in X \qquad -dk = d \cdot (-k)$

$x, y \in X \Rightarrow x+y \in X \qquad \underset{x}{dh} + \underset{y}{dk} = \underset{x+y}{d(h+k)}$

$\{dk \mid k \in \mathbb{Z}\} = (d) \leftarrow$ "sottogruppo generato da d"

In generale, cosa posso dire dei sottogruppi di $\mathbb{Z}$?

$0 \in X$

$x \in X \qquad \underset{2x}{x+x} \in X \qquad \underset{3x}{x+2x} \in X \qquad nx \in X$

$-x, -2x, -3x \dots \in X$.

$x \in X \Leftrightarrow (x) \subseteq X$ (con $x \in (x)$) $\qquad$ Se X è un sottogruppo di $(\mathbb{Z}, +)$

- Se X è un sottogruppo di $(\mathbb{Z}, +)$ allora è necessariamente della forma $X = (d)$ per qualche $d \in \mathbb{Z}$.

Dim: (Idea) utilizzo la divisione euclidea.

. .

$X \subset \mathbb{Z}$ sottogruppo. $0 \in X$.

2 possibilità:

- 0 è l'unico elemento di $X \Longrightarrow X = (0)$
- ci sono altri elementi positivi

$X \cap (\mathbb{N} - \{0\}) \neq \emptyset$ è un sottoinsieme non vuoto di $\mathbb{N}$, che deve avere elemento minimo $d > 0$

$d \in X$

$d \in X \Longrightarrow (d) \subseteq X$.

Voglio mostrare che X non contiene altri elementi.

$a \in X$ ($\leftarrow$ per comodità, se $a < 0$ lo cambio con $-a$) $\quad a \geq 0$, $a \in \mathbb{N}$

$$a = qd + r \qquad 0 \leq r < d$$

$$r = a - qd = a + (-q)d \in X$$

($a \in X$, $qd \in X$, $(-q)d \in X$)

Poiché d è il più piccolo elemento positivo del sottogruppo X, l'unico modo di non ottenere un assurdo è che sia $r = 0$. $\Longrightarrow \quad a = qd$

In conclusione, gli elementi di X sono tutti multipli di d

$$\left.\begin{array}{l} X \subseteq (d) \\ (d) \subseteq X \end{array}\right\} \Longrightarrow X = (d)$$

Divisione euclidea in $\mathbb{Z}$.

- Se $a, b \in \mathbb{Z}$, $b \neq 0$ allora esistono $q, r \in \mathbb{Z}$ tali che

$$a = qb + r, \qquad 0 \leq r < |b|.$$

Dim: esercizio

Es: $-7 = q \cdot 3 + r$ (è neg!)

$7 = 2 \cdot 3 + 1$

$-7 = (-2) \cdot 3 - 1$

$= (-3)3 + 2$ (-3, $+3$)

$0 \leq r < 3$

In prospettiva futura

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

$r = 0$ opp $|r| < |b|$ ← IGNORARE!

Divisibilità in $\mathbb{Z}$ (Multipli e divisori)

$(d) = \{nd \mid n \in \mathbb{Z}\}$ multipli di d.

$x \in (d) \iff x$ è multiplo di $d \iff d$ divide x

$\Updownarrow$

$(x) \subseteq (d)$

$d \mid x$

$d \nmid x$ d non divide x

Proprietà dei concetti di multiplo e divisore

- a divide 0 $\forall a \in \mathbb{Z}$ $0 \in (a)$
- a divide a $\forall a \in \mathbb{Z}$ $a \in (a)$ $a = a \cdot 1$
- a divide b, c $\Rightarrow$ a divide $b \pm c$ $b, c \in (a)$ $b \pm c \in (a)$
- a divide b, b divide c $\Rightarrow$ a divide c TRANSITIVITÀ

$(b) \subseteq (a)$ $(c) \subseteq (b)$ $(c) \subseteq (b) \subseteq (a)$

- a divide b $\Rightarrow$ a divide ogni multiplo di b.

- 1 divide a $\forall a \in \mathbb{Z}$.
- 0 divide a $\Rightarrow a = 0$
- a divide 1 $\Rightarrow a = \pm 1$
- a divide b, b divide a $\Rightarrow a = \pm b$.

INVERTIBILI

INVERTIBILI

ANTISIMMETRIA A MENO DI

Tutti i sottogruppi di $\mathbb{Z}$ sono della forma (d)

$(2) = (-2)$ $\quad (3) = (-3)$

Se $d > 0$, d è il più piccolo elemento positivo di (d)

Se $d < 0$, $-d$ è il più piccolo elemento positivo di (d)

$(a) = (b) \Rightarrow$ a e b sono uguali a meno del segno.

$a, b \neq 0$. $\quad (a) = (b)$ $\quad a = bx$ $\quad b = ay$

$a \neq 0$ $\quad d = xy\,d$ $\quad xy = 1$ $\quad x = y = \pm 1$

Se a divide b, c allora a divide $hb \pm kc$

$\forall h, k \in \mathbb{Z}$

Divagazione 2 (sempre gruppale)

X, Y sottogruppi di G ← gruppo.

- $X \cap Y$ è ancora un sottogruppo di G.

Dim: Sappiamo che $e \in X$, $x \in X \Rightarrow \bar{x} \in X$, $x, y \in X \Rightarrow x \circ y \in X$

$e \in Y$, $x \in Y \Rightarrow \bar{x} \in Y$, $x, y \in Y \Rightarrow x \circ y \in Y$

$e \in X \cap Y$ ✓ $\quad x \in X \cap Y \Rightarrow \bar{x} \in X \cap Y$ ✓

$x, y \in X \cap Y \Rightarrow x \circ y \in X \cap Y$ ✓

$X, Y \subset G$ sottogruppi

- $(G,+)$ gruppo abeliano

$X+Y = \{ x+y \mid x \in X, y \in Y \}$ ← somma dei sottogruppi.

è ancora un sottogruppo.

$0 = 0+0$ ($0 \in X$, $0 \in Y$)

$a \in X+Y \Rightarrow -a \in X+Y$

$a = x+y \Rightarrow -a = -x+(-y)$ ($x \in X$, $y \in Y$)

$a, b \in X+Y \Rightarrow a+b \in X+Y$

$a = x+y$, $b = x'+y'$

$x+y+x'+y' = (x+x')+(y+y') \in X+Y.$ ($x+x' \in X$, $y+y' \in Y$)

$(\mathbb{Z},+)$ $\quad (4) \cap (6) = \{$ multipli comuni di 4 e 6 $\} = (12)$

$(a) \cap (b) = (m)$ Def. $\quad (12)$

Dico che m è ~~il~~ un minimo comune multiplo di a e b.

Def: (← possibile traduzione di quanto appena detto).

m è un minimo comune multiplo di a e b se

① m è un multiplo comune di a e b

② ogni altro multiplo comune di a e b ne è multiplo.

① $m \in (a) \cap (b)$ $\quad (m) \subseteq (a) \cap (b)$

② $x \in (a) \cap (b) \Rightarrow x \in (m)$ $\quad (a) \cap (b) \subseteq (m)$

$\Big\} (a) \cap (b) = (m)$

Somma di sottogruppi di $(\mathbb{Z},+)$.

$X = (21)$ $\quad Y = (35)$

$X = \{ \ldots, -63, -42, -21, 0, 21, 42, 63, 84, 105, 126, \ldots \}$

$Y = \{\ldots, -105, -70, \boxed{-35}, 0, (35), 70, 105, 140, 175, \ldots\}$

$X+Y = \{$ 0 21 42 63 84 105 126 147 / 14 35 70 140 / 7 56 77 91 112

$X = (21) \quad Y = (35) \qquad X+Y \stackrel{?}{=} (7)$

$7 = 2\cdot 21 + (-1)35 = \underline{42 - 35}$ ← sottogruppo

$7 \in X+Y$

$(7) \subseteq X+Y$ ✓

$X+Y \stackrel{?}{\subseteq} (7)$ ✓

$21h + 35k = 7(3h+5k)$

$(a)+(b) = (d)$ vorrà mica dire che d è il MCD di a e b?

$a = a + 0 \in (a)+(b) = (d)$ d divide a

$b = 0 + b \in (a)+(b) = (d)$ d divide b

d è un divisore comune di a e b.

Sia e un divisore comune di a e b

e divide a
e divide b $\Longrightarrow$ e divide ogni numero della forma $ha \pm kb$

e divide d. $\Longrightarrow |e| \leq |d|$

$(a)+(b) = (d) \ni d$

↑ multipli di a ↑ multipli di b

d è della forma $ha+kb$

Def: d è un MCD di a e b se

(1) è un divisore comune di a e b

(2) ogni altro divisore comune di a e b lo divide

se $d = MCD(a,b)$, allora d è il più grande divisore comune positivo di a e b.

Osservazione: $MCD(a,b)$ è automaticamente della forma $ha+kb$ per una scelta opportuna di $h,k \in \mathbb{Z}$.

$MCD(a,b)$ = il più grande divisore comune di a e b

IDENTITÀ DI BÉZOUT.

$MCD(a,0) = a$

$MCD(a,b) = MCD(b,a)$

$(a)+(0) = (a)$

$(a)+(b) = (b)+(a)$

$MCD(a,b) = MCD(a+b,b)$ ⟵ (*)

$d|a$, $d|b$ $\Longrightarrow$ $d|a+b$, $d|b$ $\Longrightarrow$ $d|(a+b)-b = a$, $d|b$

L'insieme dei divisori comuni di a e b coincide con l'insieme dei divisori comuni di $a+b$ e b.

Di conseguenza coincidono anche quei divisori comuni che sono divisi dagli altri divisori comuni a meno di invertibili.

Si può iterare (*) ⟵

$MCD(a,b) = MCD(a+b,b) = MCD(a+2b,b) - - -$

$MCD(a,b) = MCD(a \pm qb, b)$

... l'idea per il calcolo del MCD

Algoritmo euclideo per il

MCD(1001, 345) // 690

$$1001 = 2 \cdot 345 + 311$$
$$345 = 1 \cdot 311 + 34$$
$$311 = 9 \cdot 34 + 5$$
$$34 = 6 \cdot 5 + 4$$
$$5 = 1 \cdot 4 + 1 \leftarrow \text{MCD}$$
$$4 = 4 \cdot 1 + 0$$

$34 \cdot 9 = 306$

$MCD(a,b) = MCD(a - 5q, b)$ // $MCD(1001, 345) = MCD(311, 345)$

$= MCD(345, 311) = MCD(34, 311) = MCD(311, 34)$

$= MCD(34, 5) = MCD(5, 4) = MCD(4, 1) = MCD(1, 0) = 1.$