ALGO

WWW.ALGORITMOSTEM.IT

SCIENCE TECHNOLOGY ENGINEERING MATHEMATICS

Appunti di Algebra1: Strutture algebriche

UNI - Matematica

rev.0.1 - 05 set 2023

Draft version

Appunti in formato bozza, intesi esclusivamente di ausilio alle lezioni, che le integrano nelle descrizioni e nei ragionamenti su quanto viene riportato in queste pagine.

STRUTTURE ALGEBRICHE

le operazioni sono funzioni
$A \times A \to A$
$(a,b) \mapsto a \circ b$

Insieme dotato di una o più operazioni che godono di particolari proprietà.

$(A, *, +)$

PROPRIETÀ
- elementi (risp. operazioni)
  - neutro
  - simmetrizzabili
  - cancellabili
- operazioni
  - commutatività
  - associatività
  - distributività
  - idempotenza

Proprietà delle strutture

* commutativa $\iff \forall a,b \in A \quad a*b = b*a$
* Associativa $\iff \forall a,b \in A \quad a*(b*c) = (a*b)*c$
* DISTRIBUTIVA risp. + $\iff \forall a,b,c \in A \quad a*(b+c) = a*b + a*c$
* IDEMPOTENZA $\iff \forall a \in A \iff a*a = a$

esempio di idempotenza: $(\mathcal{P}(A), \cup) \quad X \cup X = X$

insieme delle parti di A (insieme di sottoinsiemi)

operazione di unione tra insiemi

proprietà degli elementi delle strutture

Elemento neutro

el. neutro a DX — el. neutro a SX

$\varepsilon \in A$ è neutro risp. $* \iff \forall a \in A \quad a*\varepsilon = a*\varepsilon = a$

se α è neutro a DX e β è neutro a SX $\Rightarrow \alpha = \beta$

dim: $\alpha = \beta * \alpha = \beta \rightarrow \alpha = \beta$

se $\exists$ più elementi neutri a DX o SX $\rightarrow \nexists$ elemento neutro

Ricerca dell'elemento neutro:

1) se $*$ è commutativa $\begin{cases} \text{è sufficiente cercare il} \\ \text{neutro a dx o sx} \end{cases}$

2) caso generale $\begin{cases} \nexists \text{ neutro} \\ \exists \text{ più el. neutri} \rightarrow \nexists \text{ el. neutro} \\ \exists \text{ neutro DX} \rightarrow \text{verificare neutro SX} \end{cases}$

Esempio:

Struttura algebrica: $(\mathcal{P}(A), \setminus)$

operazione di differenza tra insiemi (non è commutativa)

cerchiamo il neutro DX, supponendo sia $\emptyset$ e verifichiamo se unico:

$$\forall X \in \mathcal{P}(A) \quad X \setminus \emptyset = X \qquad \text{neutro dx}$$

se $\exists$ neutro dx $\varepsilon \neq \emptyset \Rightarrow \varepsilon \setminus \varepsilon = \emptyset$ ma per essere neutro dovrebbe risultare $\varepsilon \setminus \varepsilon = \varepsilon$ quindi non è neutro dx e concludiamo che $\emptyset$ è neutro dx unico

verifichiamo l'esistenza del neutro sx:

$$\forall X \in \mathcal{P}(A) \qquad \emptyset \setminus X \neq X \text{ quindi } \emptyset \text{ non è neutro sx}$$

Elemento simmetrizzabile (o invertibile)

struttura algebrica $(A, *)$

el. neutro

$a \in A$ è simmetrizzabile (invertibile) $\Leftrightarrow \exists b \in A \mid a * b = b * a = \varepsilon$

b, simmetrico di a è unico

nella notazione additiva (operazione $+$) $(-a)$

nella notazione moltiplicativa (operazione $\cdot$) (a^{-1})

$\varepsilon * \varepsilon = \varepsilon$ l'elemento neutro è sempre invertibile e coincide con il suo simmetrico

Elemento cancellabile

struttura algebrica $(A, *)$

$a \in A$ è cancellabile $\Leftrightarrow \begin{cases} \forall x, y \in A \quad x * a = y * a \Rightarrow x = y & \text{cancellabile a DX} \\ \forall x, y \in A \quad a * x = a * y \Rightarrow x = y & \text{cancellabile a SX} \end{cases}$

Esempio:

struttura algebrica $(\wp(A), \cup)$ e $X \subseteq A$ con $X \neq \emptyset$

verifichiamo se X è cancellabile

A dx: deve essere $\forall A_1, A_2 \in \wp(A) \quad A_1 \cup X = A_2 \cup X \Rightarrow A_1 = A_2$

scegliendo $A_1 = \emptyset$ e $A_2 = X$,

diventa: $\emptyset \cup X = X \cup X \not\Rightarrow \emptyset \neq X$

$\emptyset$ diverso X

CLASSIFICAZIONE Delle strutture Algebriche

La classificazione è fatta sulla base delle proprietà che caratterizzano le operazioni e gli elementi della struttura

SEMIGRUPPO

struttura algebrica $(A, *)$
proprietà • associativa

MONOIDE (semigruppo con el. neutro)

proprietà • associativa
• $\exists$ el. neutro

GRUPPO (monoide con elementi invertibili)

• associativa
• $\exists$ el. neutro
• $\exists$ el. inverso $\forall a \in A$
• commutativa (GRUPPO ABELIANO)

$\boxed{\text{Teorema}}$ [1]

Hp $(A, *)$ monoide ; $a, x, y \in A$

Th Se A è invertibile $\Rightarrow$ A è cancellabile

$\cancel{\Leftarrow}$

Dim $a * x = a * y$

$a^{-1} * (a * x) = a^{-1} * (a * y)$

$(a^{-1} * a) * x = (a^{-1} * a) * y$ applichiamo le proprietà associative del monoide

$\varepsilon * x = \varepsilon * y \Rightarrow x = y$

Strutture algebriche con due operatori

ANELLO

$(A, +, \cdot)$

proprietà:
- $(A,+)$ gruppo abeliano
- $(A,\cdot)$ semigruppo ($\cdot$ associativa)
- $\cdot$ è distributiva risp. $+$

convenzioni:
0_A neutro risp. $+$ $\quad -a$ opposto di a
1_A neutro risp. $\cdot$ $\quad a^{-1}$ inverso di a

Estensioni:
- $(A,\cdot)$ commutativa $\to$ anello commutativo
- $(A,\cdot)$ monoide $\to$ anello unitario

esempio $(\mathbb{Z},+,\cdot)$ è un anello commutativo unitario.

	$(A,+)$	$(A,\cdot)$	$\cdot$
ANELLO	gruppo abeliano	semigruppo	distr. risp. $+$
ANELLO COMMUTATIVO	gruppo abeliano	semigruppo	distr. risp. $+$ commutativa
ANELLO UNITARIO	gruppo abeliano	monoide	distr. risp. $+$

CAMPO

Anello commutativo $\mid \forall$ elemento $\neq 0$ ha l'inverso rispetto all'operazione $\cdot$

proprietà di calcolo

anello $(A, +, \cdot)$ $\quad a, b \in A \quad 0_A$ unità anello

1) $0_A \cdot a = a \cdot 0_A = 0_A$

In un anello, $\cdot$ gode della proprietà distributiva rispetto a $+$

Dim

$$0_A \cdot a = (0_A + 0_A) \cdot a = 0_A \cdot a + 0_A \cdot a$$

$$0_A \cdot a = 0_A + (0_A \cdot a)$$

$$\Rightarrow 0_A \cdot a + \cancel{0_A \cdot a} = 0_A + \cancel{(0_A \cdot a)}$$

poichè $(A, +, \cdot)$ è un anello, $(A, +)$ è un gruppo abeliano e quindi tutti gli elementi sono invertibili e, per il teorema [1] sono anche cancellabili

Stessa dimostrazione si può fare a sx

2) $(-a) \cdot b = -(a \cdot b)$

Dim

applichiamo la prop. distributiva del prodotto risp. alla somma

$(-a) \cdot b + (a \cdot b) =$ ← se è vera la 2) deve risultare 0_A (el. neutro)

$= b(-a + a) = b \cdot 0_A = 0_A$

divisori dello zero

Sia A un Anello commutativo

in questo modo entrano le definizioni di divisore dx e sx perché vale la proprietà commutativa

$a \in A \setminus \{0\} \Leftrightarrow \exists b \in A \setminus \{0\} \,/\, a \cdot b = 0$

PROPOSIZIONE

a divisore dello zero $\Leftrightarrow$ a non è cancellabile

Dim $\Rightarrow$

Ap: a è cancellabile $\Leftrightarrow \forall x, y \in A \;\; xa = ya \Rightarrow x = y$

Hp: a è divisore dello zero $\Leftrightarrow \exists b \in A - \{0\} \,/\, a \cdot b = 0$

ma le due ipotesi sono incompatibili perché risulterebbe

$$b \cdot a = 0 \cdot a = 0 \;\wedge\; b \neq 0 \Rightarrow b \text{ non cancellabile}$$

non c'è bisogno della dimostrazione a sx poiché abbiamo considerato l'anello commutativo

Dim $\Leftarrow$

implicazione $a \Rightarrow b$ negazione $a \wedge \bar{b}$

Hp a non cancellabile $\Leftrightarrow \overline{\exists x, y \in A \;\; xa = ya \wedge x \neq y}$ non cancellabile

$x \cdot a = y \cdot a \Rightarrow xa - ya = ya - ya = 0 \Rightarrow (x - y) \cdot a = 0$

quindi a è un divisore dello zero.

ESEMPI

$(\mathbb{Z}, +, \cdot)$ è un anello unitario commutativo

Anello
$(X, +)$ gruppo abeliano
$\cdot$ associativo
distributive
$\exists$ el. neutro $\cdot$
vale commutative $\cdot$

non è un campo perché non tutti i numeri interi hanno l'inverso rispetto all'operazione $\cdot$, gli unici sono "1" e "-1"

GRUPPO
$(X, +)$ Associative
el. neutro
inverso algebrico
abeliano commutative

$(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ $(\mathbb{C}, +, \cdot)$ sono campi

$(M_N(\mathbb{R}), +, \cdot)$ è anello non commutativo

Matrici quadrate a coeff in $\mathbb{R}$

Detto un anello $(A,+,\cdot)$ è possibile determinare due gruppi:

1) $(A,+)$ GRUPPO ADDITIVO DI A

è gruppo commutativo per definizione di Anello

2) $(A^*, \cdot) = \{a \in A / \exists a^{-1}\}$ GRUPPO MOLTIPLICATIVO DI A

sottoinsieme degli elementi di A che hanno l'inverso risp. $\cdot$

OSS Se $A^* = A$ significa che $\exists$ l'inverso risp. $\cdot$ $\forall e$, allora $(A,+,\cdot)$ è un campo

es Anello $(\mathbb{Z},+,\cdot)$

GRUPPO ADDITIVO $(\mathbb{Z},+)$

GRUPPO MOLTIPLICATIVO $(\mathbb{Z}^* = \{1,-1\}, \cdot)$

l'inverso di 1 è 1 $\quad 1\cdot 1 = 1$

l'inverso di -1 è -1 $\quad (-1)\cdot(-1) = 1$

es Anello $(\mathbb{R},+,\cdot)$ anche campo

GRUPPO ADDITIVO $(\mathbb{R},+)$

GRUPPO MOLTIPLICATIVO $(\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}, \cdot)$

es Anello $(M_n(\mathbb{R}),+,\cdot)$

GRUPPO ADDITIVO $(M_n(\mathbb{R}),+)$

GRUPPO MOLTIPLICATIVO $M_n^*(\mathbb{R})$ Insieme delle matrici invertibili $(\det M_n \neq 0)$

es Anello $(\mathbb{Z}_n +, \cdot)$ commutativo

Insieme delle classi di congruenza mod n

$\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \dots \overline{n-1} \}$ $|\mathbb{Z}_n| = n$

tutti i possibili resti della div per n

NB $\forall$ elemento di $\mathbb{Z}_n$ posso scrivere qualsiasi elemento rappresentante la classe, per esempio al posto di $\bar{1}$ posso scrivere $\overline{1+n}$, $\overline{1+2n}$, $\overline{1-2n}$, ...

def $\bar{a} + \bar{b} \overset{def}{=} \overline{a+b}$ $\bar{a} \cdot \bar{b} \overset{def}{=} \overline{a \cdot b}$

le definizioni son ben definite perchè non dipendono dal rappresentante della classe

esempio in $\mathbb{Z}_5$: $\bar{3} + \bar{4} = \bar{7} = \bar{2}$ $\bar{3} \cdot \bar{4} = \overline{12} = \bar{2}$

$\overline{8} + \overline{9} = \overline{17} = \bar{2}$

- el. neutro per la somma è $\bar{0}$, per il prodotto è $\bar{1}$
- inverso di $\bar{a}$ rispetto alla somma è $\overline{-a}$ $\bar{a} + \overline{-a} = \bar{0}$
- GRUPPO MOLTIPLICATIVO $\mathbb{Z}_n^* = \{ \bar{a} \in \mathbb{Z}_n \mid \exists \bar{b} \in \mathbb{Z}_n \Rightarrow \bar{a} \cdot \bar{b} = \bar{1} \}$

ovvero $\mathbb{Z}_n^* = \{ \bar{a} \in \mathbb{Z}_n \mid \exists b \in \mathbb{Z} \Rightarrow ab \equiv 1 \pmod{n} \}$

quindi b è una soluzione dell'eq. $ax \equiv 1 \pmod{n}$

Proposizione:

$$\mathbb{Z}_n^* = \{ \bar{a} \in \mathbb{Z}_n \mid MCD(a, n) = 1 \}$$

$\exists$ l'inverso di $\bar{a} \in \mathbb{Z}_n$ se a e n sono coprimi

es

$$\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$$

1) $\bar{5} \in \mathbb{Z}_8^*$? $\quad MCD(5,8) = 1 \rightarrow$ SI, $\bar{5} \in \mathbb{Z}_8^*$

l'inverso di $\bar{5}$ in $\mathbb{Z}_8$ è la soluzione dell'eq.

$5x \equiv 1 \pmod 8 \longrightarrow 5 \cdot 5x \equiv 5 \cdot 1 \pmod 8 \rightarrow x \equiv 5 \pmod 8$

$$\bar{5}^{-1} = \bar{5} \text{ in } \mathbb{Z}_8$$

2) $\bar{4} \in \mathbb{Z}_8^*$? $\quad MCD(4,8) \neq 1 \rightarrow$ NO, $\bar{4} \notin \mathbb{Z}_8^*$

cioè l'eq. $4x \equiv 1 \pmod 8$ non ammette soluzione

es

$$\mathbb{Z}_{32} = \{\bar{0}, \bar{1}, \ldots, 31\}$$

$\overline{15} \in \mathbb{Z}_{32}^*$? $\quad MCD(15,32) = 1 \rightarrow$ SI, $\overline{15} \in \mathbb{Z}_{32}^*$

posso calcolare l'inverso con l'alg. euclideo

$32 = 15 \cdot 2 + 2 \qquad 2 = 32 - 15 \cdot 2$

$15 = 2 \cdot 7 + 1 \qquad 1 = 15 - 2 \cdot 7 = 15 - (32 - 15 \cdot 2) \cdot 7 =$

$2 = 1 \cdot 2 + 0 \qquad\qquad = 15 \cdot 15 - 7 \cdot 32$

soluzione

$15 \cdot 15x \equiv 15 \cdot 1 \pmod{32} \longrightarrow x \equiv 15 \pmod{32}$

PROPOSIZIONE

$\mathbb{Z}_n$ è un campo <u>sse</u> n è primo

<u>Dim</u> $\forall\, \bar{a} \in \mathbb{Z}_n \quad \bar{a} \neq 0$:

n primo $\rightarrow$ $MCD(a, n) = 1$ $\rightarrow$ a è invertibile

<u>OSS</u> i campi $\mathbb{Z}_n$ sono finiti (n. finito di elementi) quindi molto più vantaggiosi del campo dei reali $\mathbb{R}$ per certi calcoli. Sono più facili da descrivere

FUNZIONI NELLE STRUTTURE Algebriche

Siano $(G, \cdot)$ $(G, *)$ GRUPPI:

Omomorfismo (preserva le operazioni)

$$f : G \to G'$$

$$f(a \cdot b) = f(a) * f(b) \quad \forall\, a, b \in G$$

ESEMPIO: log

$(\mathbb{R}, \cdot) \to (\mathbb{R}, +)$

$x \mapsto \log x$

$\log(x \cdot y) = \log x + \log y$

epimorfismo

$f : G \to G'$ è suriettiva

isomorfismo

$f : G \to G'$ è biiezione

(G e G' isomorfi)

l'applicazione e le sue inverse sono omomorfismi

endomorfismo

se $f : G \to G$

isomorfismo + endomorfismo $\to$ **automorfismo**

se $f : G \to G$

è endomorfismo biettivo

ESEMPI

consideriamo le strutture $(N, +)$ e $(2^N, \cdot)$

e l'applicazione $N \to 2^N$

$$a \mapsto 2^a$$

$$f(a) = 2^a$$

$$f(b) = 2^b$$

$$\boxed{f(a) \cdot f(b) = f(a+b)}$$

$$f(a+b) = 2^{(a+b)} = 2^a \cdot 2^b$$

l'applicazione preserva le operazioni
quindi è omomorfismo

l'applicazione è iniettiva e suriettiva
quindi è un <u>isomorfismo</u>

ESERCIZIO

Sia G gruppo finito. Det. tutti i possibili omomorfismi di G in $\mathbb{Z}$

$\exists !$ omomorfismo banale $G \to \{0\}$

l'immagine di un omomorfismo è un sottogruppo $\to$ $\varphi : G \to \mathbb{Z}$ è un sottogruppo finito di $\mathbb{Z}$. L'unico sottogruppo finito di $\mathbb{Z}$ è $\emptyset$ (Ricordare le proprietà di un gruppo)

ESERCIZIO 1 pag 63

$M_2(\mathbb{Q})$ Gruppo Matrici quadrate invertibili ($\det \neq 0$) con coeff. in $\mathbb{Q}$. Verificare se l'applicazione $\det(M_2(\mathbb{Q})) \to \mathbb{Q}-\{0\}$, definita da

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad-bc$$ è omomorfismo tra gruppi moltiplicativi

---

bisogna verificare

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \det\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \stackrel{?}{=} \det\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right]$$

$$\begin{cases} \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad-bc \\ \det\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = a'd'-b'c' \end{cases} \Longrightarrow \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \det\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = (ad-bc)(a'd'-b'c')$$

$$\det\left|\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right| = \det\left|\begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}\right| =$$

$$= (aa'+bc')(cb'+dd') - (ab'+bd')(ca'+dc')$$

ESERCIZIO 3 pag. 64

$f: \mathbb{Z}_{18} \to \mathbb{Z}_6$ definita da $a_{18} \mapsto a_6$

1) è ben posta?

2) è omomorfismo tra gruppi additivi? $(\mathbb{Z}_{18},+)$ $(\mathbb{Z}_6,+)$

1) Una corrispondenza è ben posta se $a=b \to f(a)=f(b)$

Nel nostro caso deve essere: $a_{18} = b_{18} \to a_6 = b_6$

$$\overset{8_{18}}{a_{18}} = \overset{8_{18}}{b_{18}} \to \overset{8}{a} \equiv b \,(\text{mod } 18) \quad 8 \equiv 8 \,(\text{mod } 18)$$

poiché 6 divide 18 $\to a \equiv b \,(\text{mod } 6)$, cioè $a_6 = b_6$ $\quad a \equiv 8 \,(\text{mod } 6)$

quindi f è ben posta

$\mathbb{Z}_{18}$ $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \ldots$

$\mathbb{Z}_6$ $\{0, 1, 2, 3, 4, 5, 0, 1, 2, 3$

2) $f(a_{18}+b_{18}) = \left[f\,(a+b)_{18}\right] = (a+b)_6 = a_6+b_6 = f(a_{18}) + f(b_{18})$

è omomorfismo poiché preserva l'operazione

Esercizio 1 pag. 71

Provare che l'applicazione $f: \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$

$x \to 3x + \mathbb{Z}$

$x+y \qquad x+y$

1) è un omomorfismo tra gruppi.

2) Det $\ker(f)$ e, se possibile descrivere $\ker(f)/\mathbb{Z}$

1) $f(x+y) = f(x) + f(y)$

$3(x+y)+\mathbb{Z} \qquad f(x) \qquad f(y)$

$3x+3y+\mathbb{Z} = \underline{3x+\mathbb{Z}} + \underline{3y+\mathbb{Z}}$ con $\underset{\text{elemento}}{\mathbb{Z}+\mathbb{Z}} \in \mathbb{Z}$

2) $3x + \mathbb{Z} = 0 \to x = -\frac{\mathbb{Z}}{3}$

Descrizione: proprietà?

Potenze mod n

Teor di Lagrange ('800)

Hp $(G, \circ)$ gruppo commutativo finito $|G| = h$

Th $\forall g \in G \quad g^h = e$ ← el. neutro

g^h ← $g \circ g \circ g \dots g$ h volte

es $G = \mathbb{Z}_p^*$ con p numero primo

$\mathbb{Z}_p^*$ ← gruppo moltiplicativo di $\mathbb{Z}_p$

$|\mathbb{Z}_p^*| = p-1$ ← se p è primo, gli elementi di $\mathbb{Z}_p^*$ sono tutte le classi di $\mathbb{Z}_p$ diverse da "0"

corollario del teorema di Lagrange:

Teorema di Fermat ('600)

se $\begin{cases} p \text{ primo} \\ a, p \text{ coprimi} \end{cases}$ $\Rightarrow a^{p-1} \equiv 1 \pmod{p}$

a non è multiplo di p

cioè $\bar{a}^{p-1} = 1$ in $\mathbb{Z}_p$

Dim segue da Lagrange perché $|\mathbb{Z}_p^*| = p-1$

OSS Risultato: le potenze mod n sono periodiche

DOMINIO DI INTEGRITÀ

Teorema

K campo $\Rightarrow$ K dominio di integrità

Def Dominio di integrità

$\forall (a,b) \in K$, se $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$

Esempio $3 \cdot x = 0 \Rightarrow x = 0$

Se una struttura algebrica non è Dominio di integrità, allora si dice che "ammette divisori dello zero" ($a \cdot b = 0$ con $a, b \neq 0$) $\Rightarrow a = \frac{0}{b}$

Esempio: $\mathcal{F} = \{ f : [0,1] \to \mathbb{R} \text{ continue} \}$

$(\mathcal{F}, *)$ dove $f * g = \int_0^1 f(x)\, g(x)\, dx$

non è dominio di integrità

$f(x) = \frac{1}{2} - x \qquad g(x) = 1$

$$f * g = \int_0^1 1 \cdot \left(\frac{1}{2} - x\right) dx = \left.\frac{1}{2}x - \frac{1}{2}x^2\right]_0^1 = \frac{1}{2}\left[(1-1^2) - (0-0)\right] = 0$$

quindi $f * g = 0$ anche se $f \neq 0$ e $g \neq 0$

$$P(x) = Q(x)(x-a) + \cancel{R(x)}$$

$\downarrow$ radice

$Deg(P(x)) = n$

$Deg(Q(x)) = n-1$

$x = 1$

$$P(x) = \underline{x^3 + 5x^2 - 2x - 4} = 0 \rightarrow 1+5-2-4 = 0$$

$$\overset{!}{=} Q(x)(x-1) + \cancel{R(x)}$$

$$\overset{!}{=} (x^2+6x+4)(x-1)$$

	1	5	-2	-4
		+	+	+
1		1	6	4
	1	6	4	Ø

$Q(x) = x^2 + 6x + 4$

STRUTTURA $\mathbb{Z}_m$

La relazione di congruenza è compatibile rispetto a somma e prodotto

$$a \equiv b \pmod m \wedge c \equiv d \pmod m \Rightarrow \begin{cases} a+c \equiv b+d \pmod m \\ a \cdot c \equiv b \cdot d \pmod m \end{cases}$$

$(\mathbb{Z}_m, +, \cdot)$ è un anello commutativo

1) $(\mathbb{Z}_m, +)$ gruppo Abeliano
neutro: $[0]$ opposto $[-a]$

2) $(\mathbb{Z}_m, \cdot)$ semigruppo commutativo unitario
neutro: $[1]$

3) $\cdot$ è distributivo rispetto a $+$

INVERTIBILITÀ di una classe in $\mathbb{Z}_m$

Sia $m \in \mathbb{N}^*$ e $[a] \in \mathbb{Z}_m \setminus \{[0]\}$

$[a]$ invertibile $\Leftrightarrow$ $MCD(>0)(a,m) = 1$

Dim TODO

Esempio (notazione $\bar{a}$ alias $[a]$)

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ tutti i possibili resti di una divisione per 6

$U(\mathbb{Z}_6) = \{\cancel{\bar{0}}, \bar{1}, \cancel{\bar{2}}, \cancel{\bar{3}}, \cancel{\bar{4}}, \bar{5}\}$ elementi invertibili di $\mathbb{Z}_6$

$MCD(0,6) = 6$ $\quad MCD \neq 1$

Teorema:

Sia $m \in \mathbb{N}^*$ e sia $a \in \mathbb{Z}_m \setminus \{[0]\}$

$[a]$ è divisore dello zero $\Leftrightarrow$ $MCD(a,m) > 1$

Dim TODO

corollario: $[a]$ invertibile $\Leftrightarrow$ $[a]$ non è divisore dello zero

Teorema

Sia $m \in \mathbb{N}^*$ $(m > 1)$. le seguenti proposizioni sono equivalenti

1) m è primo
2) $\mathbb{Z}_m$ è un campo
3) $\mathbb{Z}_m$ è un dominio di integrità

$\rightarrow$ anello commutativo privo di divisori dello zero

$(\mathbb{Z}_m\ +, \cdot)$ $\quad a \cdot b = b \cdot a \ \ \forall a,b \in \mathbb{Z}_m$

$a \cdot b = 0 \Rightarrow a = 0 \lor b = 0$