Università degli studi di palermo

Ingegneria informatica e delle TLC

Geometria e Algebra 1

Concetti di Algebra 1

Author:
Gaetano Di Grazia
author
author

Contacts:
education.digrazia@gmail.com
email@sample.it
email@sample.it

Author:
Gaetano Di Grazia et al.

13 luglio 2020

Premessa

Ho scritto il presente testo per sostenere l'esame di Geometria e Algebra 1 (12 CFU) presso l'università degli studi di Palermo.
Considerando il fatto che questo può (sarà sicuramente) essere errato in qualche sua parte lo metto a disposizione del web anche, e soprattutto, per correzioni, modifiche e miglioramenti che possano arricchire questo lavoro.
Lo scopo del testo, ovvero delle parti vuote, è quello di dimostrare i teoremi in vista dell'esame e risolvere passo passo gli esercizi.

Indice

1 Insiemistica

Un insieme è semplicemente una collezione di oggetti ed è un concetto *primitivo*.
Georg Cantor, fondatore della teoria degli insiemi, lo definisce così: "*Un insieme è una collezione di oggetti determinati e distinti della nostra percezione o del nostro pensiero concepiti come un tutto unico.*
Tali oggetti si dicono gli elementi dell'insieme"

1.1 Inclusione

Un insieme B si dice sottoinsieme di un insieme A se ogni suo elemento appartiene ad A, ossia

$$B \subseteq A \Rightarrow \forall b \in B, b \in A$$

Possiamo inoltre distinguere i sottoinsiemi in due categorie, i sottoinsiemi *propri* e *impropri*.
Dicesi sottoinsieme improprio l'insieme vuoto $\emptyset$ e l'insieme A stesso. Dicesi, invece, sottoinsieme *proprio* se

$$B \subset A \Leftrightarrow \forall b \in B, b \in A \; ed \; \exists a \in A : a \notin B$$

1.2 Insiemi uguali

Due insiemi si dicono uguali se

$$A \subseteq B \; e \; B \subseteq A$$

1.3 Operazioni tra insiemi

1.3.1 Unione

$$A \cup B = \{x | x \in A \; o \; x \in B\}$$

1.3.2 Intersezione

$$A \cap B = \{x | x \in A \; e \; x \in B\}$$

1.3.3 Differenza

La differenza tra due insiemi restituisce come risultato un insieme i cui elementi sono quelli del primo insieme che non appartengono al secondo insieme, ossia

$$A - B = \{x \in A : x \notin B\}$$

si noti che, per come è definita, la differenza non è commutativa.

1.3.4 Complemento

Stabilito un insieme universo $\mathfrak{A}$, ossia un insieme generico contenente gli elementi di nostro interesse, si definisce *complemento* di un insieme A rispetto al dato universo U l'insieme di tutti gli elementi di $\mathfrak{A}$ che non appartengono ad A

$$C_A = \{x \in \mathfrak{A} : x \notin A\}$$

Si noti che si il complementare si ottiene a partire dalla differenza di due insiemi in cui uno è incluso nell'altro.

1.3.5 Proprietà delle operazioni tra insiemi

1. IDEMPOTENZA:
   $A \cup A = A, \quad A \cap A = A$;
2. ASSOCIATIVA:
   $(A \cup B) \cup C = A \cup (B \cup C)$;
   $(A \cap B) \cap C = A \cap (B \cap C)$;
3. COMMUTATIVA:
   $A \cup B = B \cup A \quad A \cap B = B \cap A$;
4. DISTRIBUTIVA:
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;

1.4 Prodotto cartesiano

Siano A e B due insiemi diversi dall'insieme vuoto (A,B $\neq \emptyset$).
Il prodotto cartesiano $A \times B$ è

$$A \times B = \{(a, b) | a \in A \wedge b \in B\}$$

In un prodotto cartesiano si ha che la coppia ordinata (a_1, b_1) è uguale a un'altra coppia ordinata (a_2, b_2) se e solo se a_1 è uguale ad a_2 e b_1 è uguale a b_2.

$$(a_1, b_1) = (a_2, b_2) \Leftrightarrow a_1 = a_2 \wedge b_1 = b_2$$

Il prodotto cartesiano può anche essere applicato su due insiemi coincidenti

$$A^2 = A \times A = \{(a_1, a_2) | a_1 \in A \wedge a_2 \in A\}$$

Il prodotto ottenuto può essere nuovamente "moltiplicato" per A, anche più volte, ossia

$$A^n = A^{n-1} \times A = A \times A \times ... \times A = \{(a_1, a_2, ..., a_n) | a_i \in A\}$$

La $(a_1, a_2, ..., a_n)$ viene detta $n-$pla.

2 Relazioni o corrispondenze

Dati due insiemi A e B si definisce corrispondenza o relazione R da A in B una legge che associa elementi di A ad elementi di B.
Si noti che in una *relazione* da A in B ad un elemento del dominio può essere associato più di un elemento o nessun elemento del codominio.

2.1 Relazioni su un insieme

Definizione 2.1. *Dato un insieme A, si definisce relazione* ***binaria*** *o semplicemente relazione su A una corrispondenza da A in se stesso.*

Si noti che una relazione su A individua un sottoinsieme del prodotto cartesiano $A \times A$

2.2 Proprietà delle relazioni

Definizione 2.2 (Proprietà riflessiva)**.** *Una relazione R definita su un insieme A è riflessiva se ogni elemento di A è in relazione con se stesso.*

$$\forall x \in A, xRx$$

Definizione 2.3 (Proprietà simmetrica)**.** *Una relazione R definita su un insieme A è simmetrica se, comunque presi x e y in A, se x è in relazione con y allora y è in relazione con x.*

$$\forall x, y \in A, xRy \Rightarrow yRx$$

Definizione 2.4 (Proprietà antisimmetrica)**.** *Una relazione R definita su un insieme A è antisimmetrica se, comunque presi x e y in A con $x \neq y$, se x è in relazione con y allora y non è in relazione con x, ossia*

$$\forall x, y \in A,\ x \neq y, xRy \Rightarrow y \not Rx$$

o, equivalentemente, se x è in relazione con y e y è un relazione con x, allora x=y

$$\forall x, y \in A, xRy \wedge yRx \Rightarrow x = y$$

Definizione 2.5 (Proprietà transitiva)**.** *Una relazione R definita su un insieme A è transitiva se, comunque presi tre elementi in A x, y e z , se x è in relazione con y e y è in relazione con z, allora x è in relazione con z.*

$$\forall x, y, z \in A, xRy \wedge yRz \Rightarrow xRz$$

2.3 Relazioni d'equivalenza

Definizione 2.6. *Una relazione R su un insieme A per la quale valgono le proprietà riflessiva, simmetrica e transitiva è detta relazione d'equivalenza.*

Esercizio 2.7. *Si verifichi che la seguente relazione sia d'equivalenza*

$$xRy \Leftrightarrow x = y, x, y \in A$$

Esercizio 2.8. *Si verifichi che la seguente relazione sia d'equivalenza*

$$aRb \Leftrightarrow a - b = 2n, n \in \mathbf{Z}, a, b \in A$$

Esercizio 2.9. *Sia* $A = \mathbf{Z}$.
Data la seguente relazione

$$aRb \Leftrightarrow ab \geq 0, a, b \in A$$

si stabilisca se questa è, o meno, di equivalenza.

Esercizio 2.10. *Sia* $A = \mathbf{Z}^{\star}$.
Data la seguente relazione

$$aRb \Leftrightarrow ab > 0, a, b \in A$$

si stabilisca se questa è, o meno, di equivalenza.

2.3.1 Classe di equivalenza

Definizione 2.11. *Sia dato un insieme* A *e sia* R *una relazione di equivalenza definita in* A.

Sia $a \in A$, si chiama ***classe di equivalenza di a*** *il sottoinsieme di A formato da tutti gli elementi b di A che sono in relazione con a, ossia*

$$\left[a\right] = \{b \in A | aRb\} = \{b \in A | bRa\}$$

È importante notare che $\left[a\right] \neq \emptyset$, poiché almeno $a \in \left[a\right]$, la classe di equivalenza si indica con $\left[a\right]$ oppure con $\overline{a}$.
Nel simbolo della classe d'equivalenza la a che figura tra parentesi è detta rappresentante della classe e può essere un qualsiasi elemento di quella stessa classe.

Esercizio 2.12. *Sia $A = \mathbf{Z}$.*
Considerata la relazione R definita nel modo seguente

$$aRb \Leftrightarrow a - b = 2n, n \in \mathbf{Z}, a, b \in A$$

Si determini $\left[3\right]$.

Esercizio 2.13. *Sia $A = \mathbf{Z}$.*
Considerata la relazione R definita nel modo seguente

$$aRb \Leftrightarrow ab > 0, a, b \in A$$

Si determini $\left[-5\right]$, $\left[-2\right]$.

Le classi di equivalenza godono delle seguenti proprietà:

- $\left[a\right] = \left[b\right] \Leftrightarrow aRb$;
  (segue dimostrazione)

- $a \not R b \Rightarrow \big[a\big] \cap \big[b\big] = \emptyset$.
  (segue dimostrazione per assurdo)

Proposizione 2.14. *Due classi d'equivalenza o coincidono o sono disgiunte (segue dimostrazione).*

2.4 Insieme quoziente

Sia dato un insieme A e sia R=$\sim$ una relazione di equivalenza definita in A.
Si definisce insieme quoziente di A modulo $\sim$ l'insieme di tutte le classi di equivalenza

$$A/\sim = \{\big[a\big]_\sim | a \in A\}$$

2.4.1 Partizione di un insieme

Sia A_i una famiglia di sottoinsiemi di A, essa costituisce una partizione di A se l'unione di tutti gli A_i d come risultato A stesso e se l'intersezione tra due sottoinsiemi di A_i e A_j

è l'insieme vuoto $\forall i \neq j$.

Proposizione 2.15. *Le classi di equivalenza di A costituiscono una partizione di A.*
(segue dimostrazione)

Esempio 2.16. *Sia A un generico insieme.*
Consideriamo la relazione $\sim$ definita nel modo seguente:

$$x \sim y \Leftrightarrow x = y, x, y \in A$$

Sia $a \in A$, allora $\big[a\big] = \{a\}$.
Dunque l'insieme quoziente è

$$A/\sim = \{\big[a\big] | a \in A\} = \{\{a\} | a \in A\}$$

Esercizio 2.17. *Sia $A = \mathbf{Z}$.*
Considerata la relazione $\sim$ definita nel modo seguente

$$a \sim b \Leftrightarrow a - b = 2n, n \in \mathbf{Z}, a, b \in A$$

Si determini $\mathbf{Z}/\sim$

Esercizio 2.18. *Sia $A = \mathbf{Z}$.*
Considerata la relazione $\sim$ definita nel modo seguente

$$a \sim b \Leftrightarrow ab > 0 a, b \in A$$

Si determini $\mathbf{Z}/\sim$

2.5 Esercizi

Esercizio 2.19. *Delle seguenti relazioni su* $\mathbf{N}$ *verificare quali tra le proprietà riflessiva, simmetrica, anti-simmetrica e transitiva sono valide:*

1. $x\mathfrak{R}y \Leftrightarrow x|y$;

2. $x\mathfrak{R}y \Leftrightarrow$ *hanno lo stesso numero di cifre;*

3. $x\mathfrak{R}y \Leftrightarrow x - y = 3n$ *per qualche naturale* n;

4. $x\mathfrak{R}y \Leftrightarrow$ *hanno un divisore comune diverso da* 1;

Esercizio 2.20. *Sia $|n|$ il valore assoluto di $n \in \mathbf{Z}$ con*

$$\begin{cases} n \ \ se \ \ n \geq 0 \\ -n \ \ se \ \ n < 0 \end{cases}$$

In $\mathbf{Z}$ si definisca la relazione, indicata con $\sim$ tale che

$$m \sim n \Leftrightarrow$$

Dimostrare che è una relazione d'equivalenza e determinare $\frac{\mathbf{Z}}{\sim}$

Esercizio 2.21. *Sia $A = \mathbf{Z}$.*
Considerata la relazione $\sim$ definita nel modo seguente

$$a \sim b \Leftrightarrow a - b = 3k \forall a, b \in \mathbf{Z}, \forall k \in \mathbf{Z}$$

Dimostrare che è una relazione d'equivalenza e determinare le classi di equivalenza.

Esercizio 2.22. *Sia $A = \mathbf{Z}$.*
Considerata la relazione $\sim$ definita nel modo seguente

$$a \sim b \Leftrightarrow (a + b - 1)(a - b) = 0 \forall a, b \in \mathbf{Z}$$

Dimostrare che è una relazione d'equivalenza e determinare le classi di equivalenza.

Esercizio 2.23. *Sia* $A = \mathbf{Z}$.
Considerata la relazione $\sim$ *definita nel modo seguente*

$$a \sim b \Leftrightarrow a^2 - a = b^2 - b \forall a, b \in \mathbf{Z}$$

Dimostrare che è una relazione d'equivalenza e determinare le classi di equivalenza.

3 Funzioni

3.1 Funzione

Una funzione da A a B è una legge, o relazione, che ad ogni elemento di A associa uno ed un solo elemento di B.

- $f : A \to B$
- $a \to b = f(a)$
- $\forall a \in A \, \exists! b \in B | f(a) = b$

Possiamo quindi utilizzare, un criterio per stabilire se una legge sia o meno una applicazione, ossia

Criterio 3.1. *Per verificare che una legge* $f : A \to B$ *sia una funzione bisogna verificare che*

- $\forall x \in A, \exists f(x) \in B$;
- $\forall x \in A, \exists! f(x)$

$$x = y \Rightarrow f(x) = f(y)$$

Esercizio 3.2. *Si consideri la corrispondenza* $f : \mathbf{Z} \to \mathbf{Z}$ *definita da*

$$f(x) = 2x, \forall x \in \mathbf{Z}$$

si dica se è o meno una funzione.

Esercizio 3.3. *Si consideri la corrispondenza* $f : \mathbf{Q} \to \mathbf{Q}$ *definita da*

$$f(\frac{a}{b}) = 5\frac{a}{b}, \forall \frac{a}{b} \in \mathbf{Q}$$

si dica se è o meno una funzione.

Esercizio 3.4. *Si consideri la corrispondenza* $f : \mathbf{R} \to \mathbf{R}$ *definita da*

$$f(x) = \frac{5}{2-x}, \forall x \in \mathbf{R}$$

si dica se è o meno una funzione.

Esercizio 3.5. *Si consideri la corrispondenza* $f : \mathbf{Q} \to \mathbf{Q}$ *definita da*

$$f(\frac{a}{b}) = 2b, \forall \frac{a}{b} \in \mathbf{Q}$$

si dica se è o meno una funzione.

3.1.1 Funzione iniettiva

Una funzione $f : A \to B$ si dice iniettiva se elementi distinti di A hanno immagini distinte

$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

(segue dimostrazione numerica)

Esercizio 3.6. *Si consideri l'applicazione* $f : \mathbf{Z} \to \mathbf{Z}$ *definita da*

$$f(x) = 3x + 1, \forall \frac{a}{b} \in \mathbf{Q}$$

si dica se è o meno iniettiva.

Esercizio 3.7. *Si consideri l'applicazione* $f : \mathbf{Z} \to \mathbf{Z}$ *definita da*

$$f(x) = x^2, \forall x \in \mathbf{QZ}$$

si dica se è o meno iniettiva.

3.1.2 Insieme immagine

$$Im\, f = \{f(a) | a \in A\} \subseteq B$$

3.1.3 Funzione suriettiva

Una funzione $f : A \to B$ è detta suriettiva se comunque prendo b appartenente a B esiste una a appartenente ad A tale che $f(a)$ sia uguale a b

$$\forall b \in B\, \exists a \in A | f(a) = b$$

(segue dimostrazione)

Si noti, inoltre, che una funzione $f : A \to B$ è suriettiva se il suo insieme immagine è uguale al codominio, ossia

$$Im\, f = B$$

ciò ci suggerisce che ogni funzione è suriettiva se pensata, ossia "ristretta", a valori nel suo codominio.
Possiamo quindi utilizzare, un criterio per stabilire se una legge sia o meno una applicazione, ossia

Criterio 3.8. *$f : A \to B$ è suriettiva se, $\forall b \in B \exists x \in A$ tale che l'equazione*

$$f(x) = b$$

ha soluzione.

Esercizio 3.9. *Si consideri l'applicazione $f : \mathbf{Z} \to \mathbf{Z}$ definita da*

$$f(x) = x + 6, \forall x \in \mathbf{Z}$$

si dica se è o meno suriettiva.

Esercizio 3.10. *Si consideri l'applicazione* $f : \mathbf{Z} \to \mathbf{Z}$ *definita da*

$$f(x) = 3x + 1, \forall x \in \mathbf{Z}$$

si dica se è o meno suriettiva.

3.1.4 Funzione biettiva

Una funzione $f : A \to B$ si dice biettiva o biunivoca se è sia iniettiva che suriettiva, ossia

$$\forall b \in B \, \exists! a \in A | f(a) = b$$

3.2 Cardinalità

Si dice cardinalità di un insieme A il numero di elementi dell'insieme stesso

$$|A| = n$$

Esercizio 3.11. *Quando una funzione può essere biiettiva in base alla cardinalità degli insiemi? Perché?*

3.3 Funzione composta

Siano $f : A \to B$ e $g : B \to C$ due funzioni.
Si dice funzione composta, e si indica con $g \circ f : A \to C$ una funzione che applica prima la funzione f e poi la funzione g.

$$c = (g \circ f)(a) = g\big[f(a)\big]$$

3.3.1 Proprietà delle funzioni composte

Siano $f : A \to B$ e $g : B \to C$ due funzioni, allora

- se f e g sono iniettive, la funzione composta $g \circ f : A \to C$ è a sua volta iniettiva (segue dimostrazione);

- se f e g sono suriettive la funzione composta $g \circ f : A \to C$ è a sua volta suriettiva (segue dimostrazione);

- se f e g sono biettive la funzione composta $g \circ f : A \to C$ è a sua volta biiettiva

3.4 Funzione identità

Si dice funzione identità una funzione $f : A \to A$ che associa ad ogni elemento di A l'elemento stesso

$$f : A \to A \Rightarrow f(a) = a$$

(segue dimostrazione)

Si noti che la funzione identità si comporta da *elemento neutro*.

3.5 Funzione inversa

Sia $f : A \to B$ una funzione.
La sua funzione inversa $f^{-1} : B \to A$ è tale che le funzioni composte $f^{-1} \circ f : A \to A$ e $f \circ f^{-1} : B \to B$ sono funzioni identità.
Una funzione $f : A \to B$ è invertibile se e solo se è biiettiva e vale il viceversa, ovvero ogni funzione biiettiva è invertibile

$$\forall f : A \to B \text{ biiettiva } \exists! f^{-1} : B \to A | f \circ f^{-1} = \text{ fun. identità } \wedge f^{-1} \circ f = \text{ fun. identità}$$

3.6 Numero di funzioni

Siano A e B due insiemi di cardinalità rispettivamente k e n.
Il numero di tutte le possibili funzioni $f : A \to B$ è uguale a n^k

$$\text{⁂} = f : A \to B = n^k, \ |A| = k \wedge |B| = n$$

Siano A e B due insiemi con la stessa cardinalità e sia $f : A \to B$ una funzione:

- se f è suriettiva è anche iniettiva;
- se f è iniettiva è anche suriettiva.

Esercizio 3.12. *Siano dati gli insiemi* $A = \{1; 2\}$ *e* $B = \{b_1; b_2; b_3\}$ *quante possibili funzioni si possono avere? Le si scrivano.*

3.7 Funzione identica

Sia A un insieme.
Si dice funzione identica $id\,A$ una funzione che associa ad ogni elemento di A un altro elemento di A.

- $id\,A : A \to A$
- $x \to y \qquad x, y \in A$

3.8 Numero di funzioni identiche biiettive

Sia A un insieme.
Il numero di tutte le possibili funzioni identiche biiettive ricavabili da A è dato dal fattoriale della cardinalità di A

$$n = k!,\ |A| = k$$

Esercizio 3.13. *Sia dato l'insieme* $A = \{1; 2; 3\}$ *quante possibili funzioni identiche si possono avere? Le si scrivano.*

3.9 Operazioni su insiemi

Un'operazione su insiemi è un'applicazione e si indica con $*$.

$$* = A \times A \to A$$
$$(a_1, a_2) \to a_1 * a_2$$

Una operazione su A può essere

3.9.1 Associativa

$$(a * b) * c = a * (b * c),\ \forall a, b, c \in A$$

3.9.2 Commutativa

$$a * b = b * a,\ \forall a, b \in A$$

3.9.3 Elemento neutro

Si dice elemento neutro rispetto a una determinata operazione quell'elemento che se operato assieme ad un altro non cambia il valore di quest'ultimo.

$$\exists e \in A : a * e = e * a = a\, \forall a \in A$$

3.9.4 Elemento simmetrico

Si dice elemento simmetrico rispetto ad una determinata operazione, quell'elemento che se operato assieme ad un altro restituisce l'elemento neutro dell'operazione.

$$a * a' = a' * a = e$$

3.9.5 Chiusura

Diremo che un insieme A è chiuso rispetto all'operazione $*$, denotato con $(A, *)$, se

$$\forall a, b \in A \Rightarrow a * b = c : c \in A$$

3.10 Leggi

3.10.1 Legge di cancellazione

$$a \star c = a \star b \Rightarrow c = b$$

3.10.2 Legge di annullamento del prodotto

$$a \cdot b = 0 \Leftrightarrow a = 0 \vee b = 0$$

Tale legge è definita in A se e solo se A è sottoinsieme di **N** o degli insiemi superiori a **N**.

3.11 Monoide

Un monoide è una struttura algebrica (o insieme) M munito di una singola operazione binaria $*$ che ad ogni coppia di elementi a, b di M associa l'elemento $a * b$, rispettando i seguenti assiomi:

- **chiusura**: $\forall a, b \in M \Rightarrow a * b \in M$.
  L'insieme è chiuso rispetto al prodotto e viene detto **magma**;
- **associatività**: dati $a, b, c \in M \Rightarrow (ab)c = a(bc)$.
  Un magma che rispetta anche la proprietà associativa è detto **semigruppo**;
- **neutro**: $\exists e \in M : ae = ea = a \; \forall a \in M$.

3.12 Assioma del buon ordinamento

Sia S un sottoinsieme dell'insieme **N** dei numeri naturali diverso dall'insieme vuoto, allora S ammette un valore minimo

$$S \subseteq \mathbb{N}, \; S \neq \emptyset$$

3.13 Principio di induzione (I forma)

Sia $\mathcal{P}$ una determinata proprietà riguardante i numeri naturali o un loro sottoinsieme. Se $\mathcal{P}$ applicata al valore minimo dell'insieme considerato è valida, e supponendo che sia vera $\mathcal{P}$ applicata a $n - 1$ è possibile da ciò dimostrare che $\mathcal{P}$ applicata ad n è vera. Allora $\mathcal{P}$ sarà vera per qualunque $n \in \mathbb{N}$. (segue dimostrazione per assurdo)

3.14 Insieme delle parti

Sia A un insieme.

Si dice insieme delle parti di A e si indica con $\mathbb{P}(A)$, l'insieme di tutti i possibili sottoinsiemi di A.
Se, allora, A ha cardinalità n, $\mathbb{P}(A)$ avrà cardinalità 2^n

$$|A| = n \Rightarrow |\mathbb{P}(A)| = 2^n$$

Domanda 3.1. *Sia $A = 1; 2; 3$ qual è la cardinalità dell'insieme delle parti? Si scrivano i possibili sottoinsiemi.*

Esercizio 3.14. *Si dimostri la proprietà enunciata sopra.*

(Suggerimento: si sfrutti l'induzione)

3.15 Validità della divisione in N

$$\forall a, b \in \mathbb{N},\ b \neq 0\ \exists q, r \in \mathbb{N} : a = b \cdot q + r\ 0 \leq r < b$$

(segue dimostrazione per induzione su a)

3.16 Principio di induzione (II forma)

Sia $\mathcal{P}(n)$ una determinata proprietà riguardante $n \in \mathbb{N}$, $(n \geq n_0)$, allora

- se $\mathcal{P}(n)$ è vera;
- supposta vera $\mathcal{P}(k)$ per ogni $0 \leq k < n$, allora $\mathcal{P}(n)$ è vera $\forall n \in \mathbb{N}$

Questa seconda forma è più "forte" della prima in quanto prende come elemento iniziale il più piccolo elemento dell'insieme per il quale ha senso la proprietà in oggetto. (segue dimostrazione)

3.17 Esercizi

Esercizio 3.15. *Dimostrare, mediante il principio di induzione, il teorema seguente:* ***La somma dei primi n numeri dispari è*** n^2

Esercizio 3.16. *Dimostrare, mediante il principio di induzione, il teorema seguente:* ***La somma dei primi n numeri dispari è*** n^2

Esercizio 3.17. *Dimostrare, mediante il principio di induzione, il teorema seguente:* ***Per ogni*** $n > 1$***, la somma dei quadrati dei primi n numeri è data da:***

$$1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$$

Esercizio 3.18. *Dimostrare, mediante il principio di induzione, il teorema seguente:* ***Per ogni*** $n > 1$***, la somma dei cubi dei primi n numeri è data da:***

$$1^3 + 2^3 + 3^3 + ... + n^3 = \left[\frac{n \cdot (n+1)}{2}\right]^2$$

Esercizio 3.19. *Dimostrare, mediante il principio di induzione, che* $\forall x \neq 1, \forall h \in \mathbf{N}$*, vale la proposizione seguente*

$$1^3 + 2^3 + 3^3 + ... + n^3 = \left[\frac{n \cdot (n+1)}{2}\right]^2$$

4 Strutture algebriche

4.1 Proprietà

Date due operazioni $*, \circ$ e un insieme A

- commutativa: $a * b = b * a$;
- associativa: $(a * b) * c = a * (b * c)$;
- distributiva: $a * (b \circ c) = (a * b) \circ (a * c)$;
- neutro: $\exists e \in A : \forall \in A,\ a * e = a$;
- inverso: $\forall a \in A,\ \exists b \in A : a * b = e$.
  $\forall a, b, c \in A$

4.2 Schema

+, •	associativa	neutro	inverso	commutativa	distributiva	
Gruppoide						1 OP.
Semigruppo	+					
Semigruppo abeliano	+			+		
Monoide	+	+				
Monoide abeliano	+	+		+		
Gruppo	+	+	+			
Gruppo abeliano	+	+	+	+		
Anelloide	+	+	+	+	+	2 OP.
Semianello	+, •	+		+	+	
Semianello unitario	+, •	+, •		+	+	
Anello	+, •	+	+	+	+	
Anello unitario	+, •	+, •	+	+	+	
Anello unitario commutativo	+, •	+, •	+	+, •	+	
Corpo	+, •	+, •	+, •-{0}	+	+	
Campo	+, •	+, •	+, •-{0}	+, •	+	

5 Numeri interi

Per la somma l'insieme dei numeri interi gode delle seguenti proprietà:

1. **commutativa**
$$\forall a, b \in \mathbb{Z} \Rightarrow a + b = b + a$$
2. **associativa**
$$\forall z_1, z_2, z_3 \in \mathbb{Z} \rightarrow (z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$
3. **elemento neutro**
$$\forall z \in \mathbb{Z},\ \exists 0 \in \mathbb{Z} : z + 0 = 0 + z = z$$
4. **elemento simmetrico**
$$\forall z \in \mathbb{Z}\ \exists!(-z) \in \mathbb{Z} : z + (-z) = (-z) + z = 0$$

Quando valgono le proprietà 2, 3 e 4 si dice che l'insieme ha una struttura di **gruppo**.
Alla luce di ciò, visto che vale anche la proprietà 1, l'insieme $\mathbb{Z}$ si dice che assume una struttura di gruppo commutativo o abeliano rispetto alla **somma**, $(\mathbb{Z}, +)$.
Per il prodotto, l'insieme dei numeri interi gode delle seguenti proprietà

1. **commutativa**
$$\forall a, b \in \mathbb{Z} \Rightarrow a \cdot b = b \cdot a$$
2. **associativa**
$$\forall z_1, z_2, z_3 \in \mathbb{Z} \rightarrow (z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$
3. **elemento neutro**
$$\forall z \in \mathbb{Z},\ \exists 1 \in \mathbb{Z} : z + 1 = 1 + z = z$$

4. **distributiva (rispetto alla somma)**

$$\forall a, bc, \in \mathbb{Z} \Rightarrow (a+b) \cdot c = a \cdot c + b \cdot c$$

È importante notare che per $(\mathbb{Z}, \cdot)$ non può esistere l'elemento simmetrico in quanto apparterrebbe ai numeri razionali $\mathbb{Q}$.
Alla luce di quanto detto sulle proprietà che valgono in $\mathbb{Z}$, possiamo dire che $(\mathbb{Z}, +, \cdot)$ è un anello con unità commutativa.

5.1 Validità della divisione

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

(segue dimostrazione sull'esistenza di q ed r).

(segue dimostrazione dell'unicità di q ed r).

5.2 Divisori

Definizione 5.1 (Divisore)**.** *Dati due numeri interi a e b, si dice che b divide a (o a è multiplo di b o b è divisore di a) e si scrive*

$$b|a$$

se esiste $c \in \mathbf{Z} : a = bc$.

Possiamo inoltre osservare le seguenti:

- $a|0$;

- $0|a \Rightarrow a = 0$;

- $b|a$, con $b \neq 0 \Leftrightarrow$ il resto della divisione di a per b è 0;

- $\forall a \in \mathbf{Z}, \pm 1, \pm a$ sono divisori di a, infatti $a = a \cdot 1 = (-a) \cdot (-1)$;

Sfruttando l'ultima osservazione, possiamo dare la seguente

Definizione 5.2 (Divisori impropri)**.** *Sia $a \in \mathbf{Z}$.*
*Allora $\pm 1, \pm a$ sono detti divisori **impropri** di a.*
Di conseguenza, un divisore b di a tale che $b \neq \pm 1, \pm a$ è detto divisore proprio di a.

In merito ai divisori, possiamo adesso enunciare le seguenti

Proprietà 5.3 (Transitiva)**.**

$$\forall b_1, b_2, b_3 \in \mathbf{Z}, b_1|b_2 \wedge b_2|b_3 \Rightarrow b_1|b_3$$

(segue dimostrazione)

Proprietà 5.4.

$$\forall b_1, b_2 \in \mathbf{Z}, b_1|b_2 \wedge b_2|b_1 \Rightarrow b_1 = \pm b_2$$

(segue dimostrazione)

Proprietà 5.5 (Compatibilità con somma e differenza)**.**

$$\forall b_1, b_2, b_3 \in \mathbf{Z}, b_1|b_2 \wedge b_1|b_3 \Rightarrow b_1|(b_2 \pm b_3)$$

(segue dimostrazione)

Diamo la seguente

Definizione 5.6 (Interi associati)**.** *Dati due interi $a, b \in \mathbf{Z}$.*
Allora, a, b si diranno associati se $a|b$ e $b|a$ ossia se si dividono a vicenda; si scrive

$$a \sim b$$

Osservazione 5.7.

$$a \sim b \Leftrightarrow a = \pm b$$

Osservazione 5.8. *In $\mathbf{Z}$ consideriamo la seguente relazione R: $a, b \in \mathbf{Z}$, $aRb \Leftrightarrow a \sim b$.*
Si verifica facilmente che R è una relazione d'equivalenza.

5.2.1 Numero primo

Un numero p si dice primo se ha come divisori soltanto ± 1 e $\pm p$.
In altri termini se possiede soltanto divisori impropri.

5.3 Massimo Comun Divisore

Definizione 5.9 (Massimo comun divisore)**.** *Dati due numeri interi $a, b \in \mathbb{Z}$ si definisce massimo comun divisore di a e b un intero d che soddisfa le seguenti proprietà:*

- *d è un divisore comune di a e di b*

$$d|a \wedge d|b$$

Domanda 5.1. *Come si traduce questa espressione in relazione alle proprietà dei divisori?*

- *ogni altro divisore d_0 comune di a e di b è divisore di d*

$$d_0|a, d_0|b \Rightarrow d_0|d$$

Osservazione 5.10. *Se d e d' sono due massimi comun divisori di a e dib allora sono necessariamente associati, ossia sono l'uno l'opposto dell'altro*

$$d = \pm d'$$

Domanda 5.2. *Come si spiega l'osservazione precedente?*

Osservazione 5.11. *Si noti che si definisce* ***il*** *massimo comun divisore di a e di b quello tra i due che è maggiore o uguale a zero.*

Domanda 5.3. *Quali conclusioni possiamo trarre dalla risposta alla domanda 5.2 e dall'osservazione 5.11?*

Teorema 5.12 (Esistenza del Massimo Comun Divisore)**.** *Dati due numeri interi $a, b \in \mathbf{Z}$ esiste sempre il loro massimo comun divisore, $d = (a, b)$ e si può scrivere nella forma*

$$d = ax + by$$

per opportuni $x, y \in \mathbf{Z}$

(segue dimostrazione)

Osservazione 5.13. *La scrittura*

$$d = ax + by$$

è detta Identità di Bézout.
Si noti che tale espressione non è unica, infatti

$$1 = 3 \cdot +(-4) \cdot 5 = (-2) \cdot 7 + 3 \cdot 5$$

Ciò che quindi ci chiediamo è, dati due numeri interi $a, b \in \mathbf{Z}$

1. Come determiniamo il MCD, d=(a,b)?
2. Come determiniamo una identità di Bézout d = ax + by?

Possiamo rispondere ad entrambe le domande mediante *l'algoritmo Euclideo delle divisioni successive.*
Questo si basa sul seguente risultato:

Proposizione 5.14. *Siano $a, b \in \mathbf{Z}, b \neq 0$.*
Sia $a = bq + r$, con $0 \leq r < |b|$, allora:

$$(a, b) = (b, r)$$

(segue dimostrazione)

5.3.1 Algoritmo Euclideo delle divisioni successive

L'algoritmo Euclideo consiste in una successione finita di divisioni euclidee in modo che il divisore e il resto, se non nullo, diventino rispettivamente il dividendo e il divisore della divisione successiva; il processo si arresta non appena si trova un resto non nullo.
Siano $a, b \in \mathbf{Z}$.
Se $b = 0$ si ha $(a, 0) = |a| = a \cdot (\pm 1) + 0 \cdot y$.
Analogamente, se $a = 0$ si ha $(0, b) = |b| = 0 \cdot x + b \cdot (\pm 1)$. Inoltre $(a, b) = (\pm a, \pm b)$ e $(a, b) = (b, a)$.
Per cui possiamo supporre $a \geq b > 0$.
In altre parole, in metodo è il seguente

$$a = b\,q_1 + r_1 \quad 0 \leq r_1 < b$$

$$b = r_1\,q_2 + r_2 \quad 0 \leq r_2 < r_1$$

$$\vdots$$

$$r_{k-2} = r_{k-1}\,q_k + r_k \quad 0 \leq r_k < r_{k-1}$$

$$r_{k-1} = r_k\, q_{k+1} + r_2 \quad 0 \leq r_k < r_{k-1}$$

r_k, ovvero l'ultimo resto non nullo è il massimo comun divisore di a e b.
$r_k | r_{k-1} \Rightarrow r_k | r_{k-1} \cdot q_k + r_k \Rightarrow r_k | r_{k-2} \Rightarrow r_k | r_{k-3} \Rightarrow \ldots \Rightarrow r_k | a \Rightarrow r_k | b$.
Poiché r_k è il massimo comun divisore se
$d' | a \wedge d' | b \Rightarrow d' | r_k$

Esempio 5.15 ((72, 22) = ?). $72 = 22 \cdot 3 + 6$

$$22 = 6 \cdot 3 + 4$$

$$6 = 4 \cdot 1 + 2$$

$$4 = 2 \cdot 2 + 0$$

Dunque $(72, 22) = 2$.
Come detto, però, possiamo, attraverso il metodo euclideo delle divisioni successive, determinare una identità di Bézout.
Per il teorema sull'esistenza del Massimo Comun Divisore si ha che esistono due interi x, y *tali che*

$$2 = 72 \cdot x + 22 \cdot y$$

determiniamo x *e* y.
Visto che

$$72 = 22 \cdot 3 + 6$$

$$22 = 6 \cdot 3 + 4$$

$$6 = 4 \cdot 1 + 2$$

$$4 = 2 \cdot 2 + 0$$

Allora

$$\left.\begin{matrix} 2 = 6 - 4 \cdot (1) \\ 4 = 22 - 6 \cdot (3) \end{matrix}\right\} = 2 = 6 - (22 - 6 \cdot 3) \cdot (1) = 6 + 6 \cdot 3 - 22 = 6(1+3) - 22 = 6 \cdot 4 - 22$$

$2 = 6 - 4 = 6 - 22 + 6 \cdot 3 = 6 \cdot 4 - 22 = (72 - 22 \cdot 3) \cdot 4 - 22 = 72 \cdot 4 - 22 \cdot 12 - 22 = 72 \cdot 4 - 22 \cdot 13$
in definitiva, allora

$$2 = 72 \cdot 4 + 22 \cdot (-13)$$

5.3.2 Coprimi

Due numeri interi a e b si dicono coprimi se il loro massimo comun divisore è 1, ossia (a, b) = 1.
Diamo, inoltre, il seguente

Criterio 5.16. *Dati* $a, b \in \mathbf{Z}$*, allora,* a *e* b *sono coprimi se e soltanto se 1 si può scrivere come loro combinazione lineare a coefficienti interi*

$$(a, b) = 1 \Leftrightarrow 1 = a \cdot x + b \cdot y, \quad x, y \in \mathbf{Z}$$

(segue dimostrazione dal t. es. mcd)

Conseguenza 5.17. *1. due interi consecutivi sono coprimi*

$$(a, a+1) = 1, \forall a \in \mathbf{Z}$$

2. dividendo due interi per il loro massimo comun divisore si ottengono interi coprimi

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$$

Esercizio 5.18. *Si dimostrino entrambe le conseguenze precedenti.*

Proposizione 5.19. *Siano $a, p \in \mathbf{Z}$, p primo.*
Se $p \not| a| \Rightarrow (p, a) = 1$

Esercizio 5.20. *Si dimostri la proposizione.*

Proposizione 5.21. *Se un intero divide un prodotto di interi ed è coprimo con uno dei due fattori, allora divide l'altro, ossia:*

$$\forall a, b, c \in \mathbf{Z}, a|bc, (a, b) = 1 \Rightarrow a|c$$

Esercizio 5.22. *Si dimostri la proposizione.*

Proposizione 5.23. *Siano $a, b, m \in \mathbf{Z}$ e $(a, b) = 1$, allora*

$$a|m, b|m, (a, b) = 1 \Rightarrow ab|m$$

Esercizio 5.24. *Si dimostri la proposizione.*

5.4 Minimo comune multiplo

Definizione 5.25.

Dati due numeri interi $a, b \in \mathbf{Z}$ si definisce minimo comune multiplo di a e di b, e si denota con $\big[a, b\big]$, l'intero positivo m che soddisfa le seguenti proprietà:

- m è un multiplo comune di a e di b:

$$a|m \wedge b|m$$

- ogni altro multiplo m_0 comune di a e di b è multiplo di m:

$$a|m_0 \wedge b|m_0 \Rightarrow m|m_0$$

Osservazione 5.26. *Come per il massimo comun divisore si dimostra che se m ed m' sono due minimi comuni multipli di a e di b allora sono associati, ossia $m = \pm m'$.*

Teorema 5.27. *Dati $a, b \in \mathbf{Z}$, allora $\exists \big[a, b\big]$ e*

$$(a, b)\big[a, b\big] = |ab|$$

Esempio 5.28.

$$\big[72, 22\big] = \frac{|72 \cdot 22|}{(72, 22)} = \frac{72 \cdot 22}{2} = 72 \cdot 11 = 792$$

Esercizio 5.29. *Si dimostri la proposizione.*

5.5 Teorema fondamentale dell'aritmetica

L'importanza della classe dei numeri primi consiste nel fatto che ogni numero naturale maggiore di 1 può essere espresso come prodotto di primi.
Questa affermazione, a prima vista così ovvia, è nota come teorema fondamentale dell'aritmetica, diamo allora il seguente:

Teorema 5.30 (Teorema fondamentale dell'aritmetica)**.** *Ogni naturale $n > 1$ si può scrivere come prodotto di primi*

$$n = p_1 p_2 \dots p_k$$

con p_i primo $\forall i = 1, ..., k$. Inoltre, tale fattorizzazione è ***unica*** *a meno dell'ordine dei fattori, ossia se esistono due fattorizzazioni*

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_k$$

con p_i e q_j primi, allora $k = h$ e riordinando opportunamente i fattori si ha:
$p_1 = q_1, p_2 = q_2 \dots p_k = q_k$

Esercizio 5.31. *Si dimostri l'esistenza di tale fattorizzazione (insieme non vuoto).*

Esercizio 5.32. *Si dimostri l'unicità di tale fattorizzazione (induzione).*

Teorema 5.33 (Esistenza di infiniti numeri primi)**.** *Esistono infiniti numeri primi*

Esercizio 5.34. *Si dimostri il teorema per assurdo.*

Teorema 5.35 ($\sqrt{p}$ non è razionale)**.** *Sia $p > 1$ un numero primo. Allora $\sqrt{p}$ non è un numero razionale.*

Esercizio 5.36. *Si dimostri il teorema per assurdo.*

5.6 Esercizi

Esercizio 5.37. *Calcolare il massimo comun divisore tra* 1547 *e* 560*. Si scriva, inoltre, l'identità di Bézout.*

Esercizio 5.38. *Calcolare il massimo comun divisore tra* -44880 *e* 5292*. Si scriva, inoltre, l'identità di Bézout.*

6 Congruenze

6.1 Congruenze in Z

Definizione 6.1. *Sia n un intero fissato.*
Si dice che $a, b \in \mathbf{Z}$ sono congruenti modulo n e si scrive

$$a \equiv b(mod n)$$

se n divide $a - b$, in altri termini, se esiste un intero $k \in \mathbf{Z}$ tale che $kn = a - b$.

Si noti che ciò definisce una relazione binaria su Z, detta, appunto, congruenza modulo n.

Proposizione 6.2 (La congruenza modulo n è una relazione di equivalenza)**.**

Esercizio 6.3. *Si dimostri la proposizione precedente.*

Definizione 6.4 (Classe di resto)**.** *Per ogni $a \in \mathbf{Z}$, la classe di equivalenza di a rispetto alla congruenza modulo n si chiama classe di congruenza di a modulo n (o **classe di resto** di a modulo n) e si indica con $\left[a\right]_n$.*
Inoltre, l'insieme quoziente di $\mathbf{Z}$ rispetto alla congruenza modulo n si denota con il simbolo $\mathbf{Z}_n$.

Esempio 6.5.

Consideriamo ora la congruenza modulo 2 e siano $a, b \in \mathbf{Z}$. Allora

$$a \equiv_2 b \Leftrightarrow a - b \text{ è pari}$$

ciò avviene se a, b sono entrambi pari o entrambi dispari.
Quindi le classi di congruenza modulo 2 sono esattamente 2: una è l'insieme dei numeri pari, l'altra l'insieme dei numeri dispari.
La prima è la classe di congruenza di 0, l'altra la classe di congruenza di 1; quindi, in definitiva, si ha che

$$\mathbf{Z}_2 = \{\left[0\right]_2, \left[1\right]_2\}$$

Possiamo allora, in generale, enunciare la seguente

Proposizione 6.6 (Cardinalità di $\mathbf{Z}_n$)**.** *Per ogni intero positivo n, $\mathbf{Z}_n$ ha n elementi e, precisamente,*

$$\mathbf{Z}_n = \{\left[0\right]_n, \left[1\right]_n, ..., \left[n-1\right]_n\}$$

Si noti che gli elementi $0, 1, ..., n-1$ si dicono i *rappresentanti canonici* della congruenza modulo n.
Se $a_0, a_1, ..., a_{n-1} \in \mathbf{Z}$ sono tali che $\mathbf{Z_n} = \{\left[a_0\right]_n, \left[a_1\right]_n, ..., \left[a_{n-1}\right]_n\}$ è un sistema completo di rappresentanti per la congruenza modulo n.

Esempio 6.7.

Si consideri $\mathbf{Z}_3 = \{\left[0\right]_3, \left[1\right]_3, \left[2\right]_3\}$.
Allora un sistema completo di rappresentanti per la congruenza modulo 3 è $\{3, 4, 5\}$, o anche $\{330, 3001, 12362\}$

Esercizio 6.8. *Si dimostri la proposizione precedente.*

Proposizione 6.9 (Compatibilità della congruenza rispetto alla somma e al prodotto)**.** *Siano $a, a', b, b' \in \mathbf{Z}$ tali che $a \equiv_n a'$ e $b \equiv_n b'$, allora*

1. $a + b \equiv_n a' + b'$;
2. $ab \equiv_n a'b'$.

Esercizio 6.10. *Si dimostri la proposizione precedente.*

Osservazione 6.11.

Si noti che le proprietà 1 e 2 della proposizione precedente si possono riassumere dicendo che la congruenza modulo n è **compatibile** rispetto alla somma e al prodotto.
Queste proprietà consentono di dotare l'insieme $\mathbf{Z}_n$ di una struttura di anello, definiamo su di esso, allora, le seguenti operazioni

- **Somma:** $\forall a, b \in \mathbf{Z}$, $\left[a\right]_n + \left[b\right]_n = \left[a + b\right]_n$;
- **Prodotto:** $\forall a, b \in \mathbf{Z}$, $\left[a\right]_n \cdot \left[b\right]_n = \left[a \cdot b\right]_n$.

Queste definizioni sono ben poste, ossia la classe di congruenza a secondo membro non dipende dalla scelta dei rappresentanti a e b nelle classi di congruenza a primo membro: infatti, in base alla proposizione 6.6 $\left[a\right]_n = \left[a'\right]_n$ e $\left[b\right]_n = \left[b'\right]_n$, allora

$\left[a\right]_n + \left[b\right]_n = \left[a+b\right]_n$;

- $\left[a\right]_n \cdot \left[b\right]_n = \left[a \cdot b\right]_n$.

A parole, la definizione significa che per sommare due classi si sceglie il rappresentante di ciascuna classe, si somma (in base all'usuale somma di numeri interi) e si calcola la classe del risultato.
Si noti che il simbolo a destra dell'uguaglianza rappresenta l'usuale somma di numeri interi, quello a sinistra rappresenta la nuova operazione fra classi che si vuole definire.

6.1.1 Esercizi

Esercizio 6.12. *Si risolva la congruenza* $27 \equiv_5 2$ *e si indichi la classe di resto.*

Esercizio 6.13. *Si risolva la congruenza* $37 \equiv_8 13$ *e si indichi la classe di resto.*

Esercizio 6.14. *Si risolva la congruenza* $143 \equiv_{12} 23$ *e si indichi la classe di resto.*

Esercizio 6.15. *Si calcoli* $\left[124\right]_4$

Esercizio 6.16. *Si calcoli* $\left[25\right]_3$

Esercizio 6.17. *Si calcoli* $\left[37\right]_5$

Esercizio 6.18. *Si calcoli* $\left[210\right]_6$

Esercizio 6.19. *Si calcoli* $\left[27\right]_3$

Esercizio 6.20. *Si calcoli* $\left[315\right]_{10}$

6.2 Equazioni Diofantee

Come visto precedentemente (qui), possiamo enunciare il seguente

Lemma 6.21. *Siano* $d, a, b \in \mathbf{Z}$.
Se $d|a$ *e* $d|b \Rightarrow d|ax + by \; \forall x, y \in \mathbf{Z}$

Esercizio 6.22. *Si dimostri il lemma precedente.*

Conseguenza 6.23. *Se* $d = (a, b) \Rightarrow d|ax + by \; \forall x, y \in \mathbf{Z}$.

Definizione 6.24. *Siano* $a, b, c \in \mathbf{Z}$.
Una equazione nella forma $ax + by = c$ *nelle variabili* x, y *si dice equazione diofantea.*

Uno dei problemi che potremmo ritrovarci a risolvere, ad esempio, è $4x + 5y = 1$ che ammette soluzioni intere $x = -1, y = 1$ ma anche $x = 4, y = -3$.
In generale, allora, possiamo dare la seguente

Proposizione 6.25. *Condizione necessaria e sufficiente affinché l'equazione diofantea* $ax + by = c, \; a, b, c \in \mathbf{Z}$ *ammetta soluzione è che* $MCD(a, b) = d|c$, *ossia*

$$\exists \; sol \; ax + by = c \Leftrightarrow MCD(a, b) = d|c \Leftrightarrow c = d \cdot t$$

Esempio 6.26.

Ad esempio, l'equazione $3x + 7y = 2$ ammette soluzione, poiché $(3, 7) = 1$ e $1|2$.
Osserviamo che, allora, $1 = 3(-2) + 7(1)$ da cui, moltiplicando per 2 entrambi i membri si ha

$$2 = 3(-4) + 7(2)$$

Si noti però, che come detto la soluzione $(-4, 2)$ è **una** soluzione e quindi non è unica, infatti anche $(10, -4)$ è soluzione.

Esercizio 6.27. *Si dimostri la proposizione precedente.*

Osservazione 6.28 (Algoritmo per la risoluzione)**.** *La dimostrazione della proposizione precedente, ci offre un metodo per determinare una soluzione dell'equazione* $ax + by = c$. *Infatti, basta esprimere il* $MCD(a, b) = d$ *come* $d = a \cdot \alpha + b \cdot \beta$ *e allora, poiché* $d|c \Rightarrow c = d \cdot h = (a\alpha + b\beta)h = a(\alpha h) + b(\beta h)$ *quindi la soluzione è la coppia*

$$x = \alpha h,\ y = \beta h$$

Proposizione 6.29. *Sia* (x, y) *una soluzione intera dell'equazione* $ax + by = c$, *allora tutte le soluzioni sono del tipo* (x', y') *dove*

$$x' = x - \frac{b}{d}t,\ y' = y - \frac{a}{d}t\ \forall t \in \mathbf{Z}$$

dove $d = MCD(a, b)$.

6.2.1 Esercizi

Esercizio 6.30. *Determinare una soluzione, se esiste, dell'equazione* $153x + 45y = 18$

Esercizio 6.31. *Determinare una soluzione, se esiste, dell'equazione* $7x + 13y = -5$

6.3 Equazioni congruenziali

Definizione 6.32. *Sia* n *un intero positivo.*
Si dice congruenza lineare (modulo n*) il problema di trovare tutti i numeri interi* x *che soddisfano una relazione di congruenza della forma*

$$ax \equiv_n b,\ a, b \in \mathbf{Z}, a \neq 0$$

Proposizione 6.33 (Risolubilità di congruenze lineari)**.** *Sia n un intero positivo e siano $a, b \in \mathbf{Z}$, dove $a \neq 0$.*
Sia, inoltre, $d = MCD(a, n)$, allora la congruenza lineare

$$ax \equiv_n b$$

ammette soluzione se e solo se $d|b$.
In tal caso, detta x_0 una soluzione particolare, le soluzioni sono tutti e soli i numeri interi

$$x_k = x_0 + \frac{n}{d}k$$

Esercizio 6.34. *Si dimostri la proposizione precedente.*

Osservazione 6.35. *Supponiamo, allora, che la congruenza lineare*

$$ax \equiv_n b$$

abbia soluzione, ossia che $d|b$. Allora, questa sarà equivalente alla congruenza lineare

$$\frac{a}{d}x \equiv_{\frac{n}{d}} \frac{b}{d}$$

ove $\frac{a}{d}$ e $\frac{n}{d}$ sono coprimi.

Seppure, allora, l'introduzione delle equazioni diofantee tra le congruenze lineari e le equazioni congruenziali possa sembrare anacronistica, ciò non è vero.
Infatti, il problema della ricerca di una congruenza lineare in una indeterminata è equivalente a quello della ricerca delle soluzioni di una equazione diofantea in due indeterminate.
Poiché x' è una soluzione di $aX \equiv_n b$ se, e soltanto se, esiste $y' \in \mathbf{Z}$ tale che $ax' - b = ny'$, ovvero se, e soltanto se, (x', y') è soluzione dell'equazione diofantea

$$ax - ny = b$$

Una soluzione, allora, può essere esplicitamente trovata riducendo il problema alla risoluzione dell'equazione diofantea nelle indeterminate x ed y, ovvero calcolando i coefficienti della relazione di Bézout che esprime $d := MCD(a, n)$, ricorrendo all'algoritmo euclideo delle divisioni successive.

6.3.1 Esercizi

Esercizio 6.36. *Si risolva l'equazione congruenziale* $15x \equiv_{21} 12$.

Esercizio 6.37. *Si risolva l'equazione congruenziale* $7x \equiv_5 3$.

Esercizio 6.38. *Si risolva l'equazione congruenziale* $5x \equiv_{11} 5$.

Esercizio 6.39. *Si risolva l'equazione congruenziale* $7x \equiv_{10} 4$.

Esercizio 6.40. *Si risolva l'equazione congruenziale* $21x \equiv_5 6$.

Esercizio 6.41. *Si risolva l'equazione congruenziale* $13x \equiv_{12} 11$.

Esercizio 6.42. *Si risolva l'equazione congruenziale* $259x \equiv_{11} 16$.

Esercizio 6.43. *Si risolva l'equazione congruenziale* $7x \equiv_{256} 16$.

Esercizio 6.44. *Si risolva l'equazione congruenziale* $73x \equiv_{35} -101$.

6.4 Teorema cinese del resto

Teorema 6.45. *Condizione sufficiente affinché il sistema di congruenze*

$$\begin{cases} x \equiv_{n_1} a_1 \\ x \equiv_{n_2} a_2 \\ \vdots \\ x \equiv_{n_s} a_s \end{cases}$$

ammetta soluzioni è che i moduli siano a due a due coprimi, ovvero che $\forall i \neq j \Rightarrow (n_i, n_j) = 1$.

Osservazione 6.46. *Si noti che se* x_0 *è una soluzione,* ***tutte*** *le soluzioni di tale sistema saranno date da:*

$$x = x_0 + h(n_1 \cdot n_2 \dots n_s),\ h \in \mathbf{Z}$$

Esercizio 6.47. *Si dimostri l'esistenza della soluzione.*

Esercizio 6.48. *Si dimostri l'unicità della soluzione.*

6.4.1 Esercizi

Esercizio 6.49. *Determinare se esiste la soluzione del seguente sistema lineare*

$$\begin{cases} x \equiv_4 2 \\ x \equiv_6 7 \end{cases}$$

6.5 Sistemi di congruenze

Consideriamo adesso un sistema di congruenze generico del tipo

$$(1) \quad \begin{cases} a_1 x \equiv_{n_1} b_1 \\ a_2 x \equiv_{n_2} b_2 \\ \vdots \\ a_s x \equiv_{n_s} b_s \end{cases}$$

in cui supporremo $(n_i, n_j) = 1$, per $i \neq j$.
Allora, una soluzione di tale sistema è un intero che soddisfa contemporaneamente tutte le congruenze del sistema, segue dunque che il sistema sarà compatibile
$\Leftrightarrow (a_i, n_i) | b_i \ \forall i = 1, ..., s$.
La risoluzione del sistema (1) equivale a risolvere un sistema del tipo

$$\begin{cases} x \equiv_{n_1'} c_1 \\ x \equiv_{n_2'} c_2 \\ \vdots \\ x \equiv_{n_s'} c_s \end{cases}$$

con $(n_i', n_j') = 1$.
Infatti, se (1) ammette soluzione allora $d_i = MCD(a_i, n_i) | b_i, \ \forall i = 1, ..., s$.
Dividendo la $i-$esima congruenza per $d_i = MCD(a_i, n_i')$ si ottiene un sistema equivalente

$$\begin{cases} a_1' x \equiv_{n_1'} b_1' \\ a_2' x \equiv_{n_2'} b_2' \\ \vdots \\ a_s' x \equiv_{n_s'} b_s' \end{cases}$$

dove $a'_k = \frac{a_k}{d_k}, b'_k = \frac{b_k}{d_k}, n'_k = \frac{n_k}{d_k}$.
Poiché $(a'_k, n'_k) = \left(\frac{a_k}{d_k}, \right) = 1 \Rightarrow$ ogni congruenza ammette soluzione unica $c_i (mod\ n'_i)$ quindi

$$\begin{cases} x \equiv_{n'_1} c_1 \\ x \equiv_{n'_2} c_2 \\ \vdots \\ x \equiv_{n'_k} c_k \end{cases}$$

6.5.1 Esercizi

Esercizio 6.50. *Scrivere un sistema di tre equazioni congruenziali che non ammetta soluzioni (intere) sebbene le sue singole equazioni (separatamente) ne ammettano.*

Esercizio 6.51. *Determinare se esiste la soluzione del seguente sistema lineare*

$$\begin{cases} 3x \equiv_5 3 \\ 5x \equiv_7 3 \end{cases}$$

Esercizio 6.52. *Determinare se esiste la soluzione del seguente sistema lineare*

$$\begin{cases} 7x \equiv_4 5 \\ 21x \equiv_5 2 \end{cases}$$

Esercizio 6.53. *Calcolare tutte le soluzioni del sistema di equazioni congruenziali seguente:*

$$\begin{cases} 21x \equiv_4 -93 \\ -11x \equiv_7 \\ 6178x \equiv_3 983 \\ 71x \equiv_5 52 \end{cases}$$

Esercizio 6.54. *Calcolare tutte le soluzioni del sistema di equazioni congruenziali seguente:*

$$\begin{cases} 79x \equiv_8 91 \\ -81x \equiv_7 -129 \\ 39x \equiv_{15} 132 \end{cases}$$

Esercizio 6.55. *Calcolare tutte le soluzioni del sistema di equazioni congruenziali seguente:*

$$\begin{cases} 17x \equiv_5 -105 \\ -55x \equiv_3 11 \\ 23x \equiv_7 36 \end{cases}$$

Esercizio 6.56. *Verificare che il seguente sistema di equazioni congruenziali*

$$\begin{cases} 3x \equiv_{10} 7 \\ 3x \equiv_5 2 \end{cases}$$

ha esattamente dieci soluzioni x tali che $0 \leq x \leq 100$

6.6 Calcolo combinatorio

6.6.1 Fattoriale

Sia n un numero naturale, il fattoriale $n!$ è dato da

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$$

6.6.2 Applicazioni biiettive di un insieme

Sia A un insieme di cardinalità $|A| = n$.
Il numero di applicazioni biiettive da A in A è uguale a $n!$.

6.6.3 Permutazione

Una permutazione è un'applicazione biunivoca di un insieme in sé stesso.

6.6.4 Coefficiente binomiale

Sia A un insieme di cardinalità $|A| = n$.
Tramite il coefficiente binomiale $\binom{n}{k}$ si può trovare il numero di tutti i possibili sottoinsiemi di A di cardinalità k fissata e si esprime nel seguente modo

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

(segue dimostrazione)

Il coefficiente binomiale gode della seguenti proprietà:

- $$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{1 \cdot n!} = 1$$
- $$\binom{n}{n} = \frac{n!}{n!(n-n)!} = 1$$
- $$\binom{n}{1} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1)!}{(n-1)!} = n$$
- $$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

6.6.5 Binomio di Newton

Il binomio di Newton permette di calcolare una qualsiasi potenza di binomio tramite la formula

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k$$

(segue dimostrazione, similitudine con triangolo di tartaglia)

6.7 Teoremi di Eulero e Fermat

Lemma 6.57 (Congruenza di potenza di binomio)**.** *Sia p un numero primo. Per ogni $x, y \in \mathbf{Z}$: $(x+y)^p = x^p + y^p \ (mod\ p)$.*

Esercizio 6.58. *Si dimostri il lemma precedente.*

Teorema 6.59 (Piccolo teorema di Fermat)**.** *Sia p un numero primo, allora, per ogni $a \in \mathbf{Z}$,*

$$a^p \equiv a \ (mod\, p)$$

Esercizio 6.60. *Si dimostri il teorema precedente.*

Corollario 6.60.1. *Siano $a, p \in \mathbf{Z}$ con $(a, p) = 1$, se p è primo, allora*

$$a^{p-1} \equiv_p 1$$

Esercizio 6.61. *Si dimostri il corollario precedente.*

Diamo ora la seguente

Definizione 6.62 (Funzione di Eulero)**.** *Per ogni $n \geq 1$, si chiama funzione di Eulero l'applicazione (o funzione)*

$$\varphi : \mathbf{N} \to \mathbf{N} : \varphi(1) = 1$$

e per ogni $n > 1, \varphi(n)$ è il numero di interi positivi minori di n e primi con n e $\varphi(1) = 1$.

Esempio 6.63.

- $\varphi(2) = 1$;
- $\varphi(3) = 2$ perché $1, 2$ sono gli interi positivi minori di 3 e primi con 3;
- $\varphi(20) = 8$ perché gli interi positivi minori di 20 e primi con 20 sono: $1, 3, 7, 911, 13, 17, 19$.

Se però volessimo calcolare $\varphi(1320)$ ci troveremmo in difficoltà in quanto non è semplice trovare il numero dei naturali minori di 1320 e primi con 1320.
Per calcolare la funzione di Eulero di un dato numero intero n ci vengono in aiuto alcune proprietà della funzione di Eulero.
La proprietà fondamentale della funzione di Eulero è di essere moltiplicativa.

Lemma 6.64. *Siano $m, n \in \mathbf{N}$ tali che $(m, n) = 1$, allora $\varphi(m \cdot n) = \varphi(m)\varphi(n)$*

Lemma 6.65. *Siano $p \in \mathbf{N}$ un numero primo.*
Allora:

1. *$\varphi(p) = p - 1$;*
2. *$\forall k \in \mathbf{N}, \varphi(p^k) = p^k - p^{k-1}$;*

Esercizio 6.66. *Si dimostri il punto 2.*

Quindi, dai lemmi precedenti si ha la seguente

Proposizione 6.67. *Se $n = p_1^{k_1} \dots p_r^{k_r}$ è la fattorizzazione di n come prodotto di potenze di numeri distinti, allora*

$$\varphi(n) = \varphi(p_1^{k_1} \dots p_r^{k_r}) = \varphi(p_1^{k_1}) \dots \varphi(p_r^{k_r}) = p_1^{k_1} - p_1^{k_1 - 1} \dots p_r^{k_r} - p_r^{k_r - 1}$$

Esempio 6.68.

$$\varphi(234) = \varphi(2 \cdot 3^2 \cdot 13) = \varphi(2) \cdot \varphi(3^2) \cdot \varphi(13) = 1 \cdot (3^2 - 39) \cdot 12 = 1 \cdot 6 \cdot 12 = 72$$

Possiamo quindi enunciare il seguente teorema che non è possibile dimostrare con le conoscenze acquisite fino a questo momento ma verrà dimostrato in seguito ad alcuni risultati sui gruppi.

Teorema 6.69 (Teorema di Eulero)**.** *Sia $n \geq 2$ e sia $a \geq 2$ tale che $(a, n) = 1$, allora*

$$a^{\varphi(n)} \equiv_n 1$$

Corollario 6.69.1. *Se $n = p$ è un primo, si ottiene allora*

$$a^{p-1} \equiv_p 1$$

Osservazione 6.70. *Ogni numero intero, nella rappresentazione decimale, si rappresenta nella forma*

$$a_n a_{n-1} a_{n-2} \dots a_1 a_0$$

con $0 \leq a_i \leq 9$.
Tale numero deve intendersi come

$$a_n a_{n-1} a_{n-2} \dots a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$$

Criterio 6.71 (Ultime cifre di un numero $a \in \mathbf{Z}$)**.** *In generale volendo conoscere le ultime n cifre di un numero $a \in \mathbf{Z}$ basta risolvere la congruenza $a \equiv x \,(mod\ 10^n)$*

6.7.1 Esercizi

Esercizio 6.72. *Si calcolino le ultime due cifre di* $n = 81^{82}$.

6.7.2 Esercizi

Esercizio 6.73. *Si calcolino le ultime tre cifre di* $n = 7^{827}$.

6.7.3 Esercizi

Esercizio 6.74. *Si calcolino le ultime due cifre di* $n = 47913^{6403}$.

6.8 Criteri di divisibilità

Si consideri un numero $z \in \mathbb{Z}$ di cifre $a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0$, è possibile rappresentare quest'ultimo come

$$z = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_{n-2} \cdot 10^{n-2} + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$$

6.8.1 Divisibilità per 2

Un numero è divisibile per 2 se la sua ultima cifra è divisibile per 2. (segue dimostrazione)

6.8.2 Divisibilità per 5

Un numero è divisibile per 5 se la sua ultima cifra è divisibile per 5. (segue dimostrazione analoga a quella della divisibilità per 2)

6.8.3 Divisibilità per 3

Un numero è divisibile per 3 se la somma delle sue cifre è divisibile per 3. (segue dimostrazione)

6.8.4 Divisibilità per 11

Un numero è divisibile per 11 se la somma delle sue cifre pari meno la somma delle sue cifre dispari è divisibile per 11.

$$11|a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n$$

(segue dimostrazione)

7 Teoria dei Gruppi

Definizione 7.1 (Operazione binaria)**.** *Sia X un insieme non vuoto, si dice allora operazione (binaria) su X ogni applicazione*

$$f : X \times X \to X$$

Diamo allora la seguente

Definizione 7.2 (Gruppo)**.** *Si dice **gruppo** ogni coppia ordinata $(G, *)$, ove G è un insieme non vuoto, e $*$ è un'operazione, definita in G, verificante le seguenti condizioni:*

1. *per ogni $x, y, z \in G, x * (y * z) = (x * y) * z$, ovvero è **associativa**;*
2. *esiste $e \in G : \forall x \in G, x * e = e * x = x$, ovvero esiste un elemento neutro;*
3. *$\frac{\forall x \in G \exists \overline{x} \in G : x * \overline{x} =}{x * x = e}$ (ogni elemento ammette un simmetrico);*
   *Inoltre, il gruppo si dice abeliano (o **commutativo**) se*
4. *$\forall x, y \in G, x * y = y * x$, ovvero $*$ è commutativa.*

A partire dal teorema di Lagrange possiamo dare il seguente

Corollario 7.2.1. *Se g è un elemento del gruppo finito G, allora l'ordine di g divide quello di G, in particolare*

$$g^{|G|} = e$$

ma ancora più interessante dal punto di vista pratico è il seguente

Corollario 7.2.2. *Un gruppo di ordine primo è ciclico e i suoi unici sottogruppi sono quelli banali.*

——————————————————- **OLD** ——————————————————

8 Teoria dei gruppi: gruppi e cicli

8.1 Schema riassuntivo

8.2 Gruppo

Sia G un insieme e sia $*$ una generica operazione.
Si dice che G è un gruppo rispetto a quest'operazione se:

- $\star$ è associativa per tutte le g appartenenti a G

$$\forall g_1, g_2, g_3 \in G,\ g_1 \star (g_2 \star g_3) = (g_1 \star g_2) \star g_3$$

- esiste l'elemento neutro

$$\forall g \in G \exists e \in G : e \star g = g \star e = g$$

- esiste l'elemento simmetrico

$$\forall g \in G \exists g' \in G : g \star g' = g' \star g = e$$

8.3 Gruppo commutativo

Un gruppo si dice commutativo o abeliano se in esso vale anche la proprietà commutativa, ossia

$$\forall g_1, g_2 \in G, g_1 \star g_2 = g_2 \star g_1$$

Si noti che in un gruppo:

- l'elemento neutro è unico;
  (segue dimostrazione

  per assurdo)

- ogni elemento ha un solo elemento simmetrico.
  (segue dimostrazione

per assurdo)

Gli insiemi dei numeri interi, razionali, reali e complessi $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$ sono gruppi abeliani rispetto all'operazione **somma**, con 0 come elemento neutro e $-g$ come elemento simmetrico.
Gli insiemi dei numeri interi, razionali, reali e complessi $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$ sono gruppi abeliani rispetto all'operazione **prodotto**, con 1 come elemento neutro e g^{-1} come elemento simmetrico.
Consideriamo un insieme G che è un gruppo rispetto al prodotto, allora valgono le seguenti proprietà:

- $\forall a, b \in G\ (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$;
  (segue dimostrazione)

- $\forall a, b, c \in G$ se $a \cdot b = a \cdot c \Rightarrow b = c$;
  (segue dimostrazione)

Il gruppo delle permutazione è un esempio di gruppo non commutativo.
Consideriamo un insieme A di cardinalità $|A| = n$ e consideriamo l'insieme S_A delle sue permutazioni.

$$S_A : \{f : A \to A : f \text{ è biunivoca}\}$$

Dalle nozioni precedentemente viste sappiamo quindi che $|S_A| = n!$.
Verifichiamo che il gruppo S_A rispetto all'operazione di composizione tra applicazioni sia effettivamente tale

1. $(g \circ f) \circ h = g \circ (f \circ h) \Rightarrow$ vale la proprietà associativa;
2. esiste l'elemento neutro, ovvero l'applicazione identità, $f : A \to A, a \to a$;
3. esiste l'elemento simmetrico

   $$\forall f \in S_A \exists f^{-1} \in S_A : f \circ f^{-1} = f^{-1} \circ f =$$

   funzione identità

Si ha quindi che S_A è effettivamente un gruppo rispetto all'operazione di composizione tra applicazioni ma non gode della proprietà commutativa, infatti si ha che:

$$f \circ g \neq g \circ f$$

allora $(S_A, \circ$ **non** è un gruppo commutativo.

8.4 Ciclo

Consideriamo una permutazione che agisce su n elementi, si ha un ciclo di lunghezza k se la permutazione agisce su k elementi lasciando invariati gli altri $n - k$.

8.5 Cicli disgiunti

Due cicli si dicono disgiunti se agiscono su elementi differenti in una stessa permutazione.
Ogni permutazione si può scrivere come prodotto di cicli disgiunti.

8.6 Ciclo inverso

Sia $(a_1, a_2, ..., a_k)$ un ciclo, si ha che il suo inverso è $(a_1, a_2, ..., a_k)^{-1} = (a_1, a_2, ..., a_k)$

8.7 Trasposizione

Una trasposizione è un qualsiasi ciclo di lunghezza 2.
Ogni ciclo si può scrivere come prodotto di trasposizioni.
In particolare un ciclo di lunghezza k si può scrivere come prodotto di $k - 1$ trasposizioni.

8.8 Ciclo pari

Un ciclo di lunghezza k si dice pari se $k - 1$ è pari.

8.9 Ciclo dispari

Un ciclo di lunghezza k si dice dispari se $k - 1$ è dispari.

8.10 Sottogruppo

Sia G un determinato gruppo rispetto ad una operazione.
L'insieme H, sottoinsieme di G, è un sottogruppo di G rispetto alla stessa operazione se valgono:

- $x \cdot y \in H \quad \forall x, y \in H$
- $1_G \in H$
- $\exists x^{-1} \in H \forall x \in H$

Inoltre, possiamo dire che H è un sottogruppo di G se e solo se

$$\forall x, y \in H \Rightarrow x^{-1} \cdot y \in H \wedge x \cdot y^{-1} \in H$$

(segue dimostrazione)

8.11 Sottogruppi banali

Sia G un gruppo rispetto al prodotto, sono suoi sottogruppi banali quelli generati dagli insiemi $\{1\}$ e G.
Considerati i gruppi $(\mathbb{C}, +)$ e $(\mathbb{C}^\star, \cdot)$ si hanno i seguenti sottogruppi

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +);$$

$$(\mathbb{Q}^\star, +) \leq (\mathbb{R}^\star, +) \leq (\mathbb{C}^\star, +);$$

Si noti che il simbolo di sottogruppo è "$\leq$".
Consideriamo l'insieme $< n >$ del tipo

$$< n >= \{n \cdot t : t \in \mathbb{Z}\}$$

Tutti i sottogruppi di $(\mathbb{Z}, +)$ sono del tipo $(< n >, +)$ e sono chiamati sottogruppi generati da n.
(segue dimostrazione)

8.12 Ordine

Consideriamo un generico gruppo $(G, \cdot)$ e un suo elemento a, l'ordine (o periodo) di a, in simboli $O(a)$, è il più piccolo intero positivo, se esiste, tale che

$$a^n = 1_G$$

Se n esiste, diremo che a è un elemento di periodo n, altrimenti a si dice aperiodico.
Nel caso in cui si tratti di un gruppo $(G, +)$ deve valere

$$n \cdot a = 1_G$$

Consideriamo il gruppo $(G, \cdot)$ e un suo elemento a di periodo n, allora valgono le seguenti proprietà:

- $a^k = 1_G \Leftrightarrow n|k$;
  (segue dimostrazione)

- $a^h = a^k \Leftrightarrow h \equiv_n k$

Si noti, infine che il periodo di un ciclo che agisce su k elementi è k e il periodo di un prodotto tra cicli disgiunti è uguale al minimo comune multiplo dei periodi dei singoli cicli.

8.13 Gruppo ciclico moltiplicativo generato da a

Siano

- $(G^\star, \cdot)$ un gruppo;
- a un elemento di $G^\star$;
- $< a >$ un sottogruppo ciclico di $(G^\star, \cdot)$ generato da a tale che $< a >= \{a^i : i \in \mathbb{Z}\}$

allora si ha che $(G^\star, \cdot)$ è un gruppo ciclico se

$$\exists a : G =< a >$$

8.14 Gruppo ciclico moltiplicativo generato da a

Siano

- $(G, +)$ un gruppo;
- a un elemento di G;
- $< a >$ un sottogruppo ciclico di $(G, +)$ generato da a tale che $< a >= \{z \cdot a : z \in \mathbb{Z}\}$

allora si ha che $(G, +)$ è un gruppo ciclico se

$$\exists a : G =< a >$$

Si noti che, sia G un gruppo e sia a un suo elemento tale che $G =< a >$, se a è aperiodico allora si ha che $|G| = \infty$.
Inoltre, si ha che

$$a^k = a^l \Leftrightarrow k = l$$

(segue dimostrazione)

Siano G un gruppo e H un suo sottogruppo rispetto a una determinata operazione, siano a e b due elementi di G, si definiscono la congruenza modulo H a destra e a sinistra tali che

- $a \equiv_D b mod H \Leftrightarrow a \cdot b^{-1} \in H$
- $a \equiv_S b mod H \Leftrightarrow a^{-1} \cdot b \in H$

Entrambe le congruenze sono relazioni d'equivalenza.
(segue dimostrazione)

8.15 Teorema sulla cardinalità di un sottogruppo

Siano G un gruppo e H un suo sottogruppo rispetto a una determinata operazione. Allora si ha che

$$\forall a \in G \Rightarrow |Ha| = |H|$$

(segue dimostrazione)

8.15.1 Corollario

Sia G un gruppo e sia H uno dei suoi sottogruppi rispetto alla congruenza modulo H a destra

$|Ha| = |aH| = |H|$;

$\big[a\big] = Ha$;

$Ha = Hb \Leftrightarrow a \equiv_D b \; mod \; H \Leftrightarrow a \cdot b^{-1} \in H$

Allora G è dato dall'unione di tutti gli Ha

8.16 Indice di H in t

Siano G un gruppo e H un suo sottogruppo rispetto alla congruenza modulo H a destra o a sinistra, l'indice di H in G indica il numero di tutte le classi di equivalenza distinte.

8.17 Teorema di Lagrange

Siano G un gruppo e H un suo sottogruppo rispetto alla congruenza modulo H a destra o a sinistra, allora si ha che

$|G| = |H|\big[G : H\big]$

$G = UHa$

$|G| = \sum_{a \in G} |Ha| = |Ha| \cdot \big[G : H\big] = |H| \cdot \big[G : H\big]$

Sia G un gruppo finito e sia a un elemento di G, si ha

$$O(a)||G|$$

Inoltre, vale

$$a^(G) = 1$$

Infine se si ha che l'ordine di G è finito ed è un numero primo, allora G è ciclico (segue dimostrazione)

9 Matrici

9.1 Matrice

Una matrice $m \times n$ a coefficienti reali è una tabella di m righe ed n colonne di elementi reali.
Se si ha $m = n$ allora la matrice è detta quadrata di ordine n.
$M_A(\mathbb{R})$ è l'insieme delle quadrate.
$(M_2(\mathbb{R}, +)$ è un gruppo commutativo. Consideriamo due matrici quadrate di ordine 2, allora valgono le seguenti operazioni:

- somma:
- moltiplicazione per un fattore α;
- prodotto righe per colonne

Per verificare che l'insieme delle matrici quadrate reali di ordine n sia un gruppo rispetto al prodotto righe per colonne dobbiamo verificare che

1. valga la proprietà associativa;
2. esista l'elemento neutro;
3. esista l'elemento simmetrico.

Se, per esempio, consideriamo l'insieme delle matrici quadrate reali di ordine 2, possiamo verificare che valgono le proprietà 1 e 2 tuttavia non sempre esiste l'elemento simmetrico poiché, banalmente, non tutte le matrici sono regolari (ovvero non tutte sono invertibili).
(segue dimostrazione)

9.2 Determinante

Sia A una matrice reale quadrata di ordine 2, il determinante di A, $det\,A$, è dato dalla differenza tra il prodotto degli elementi della prima diagonale meno quello degli elementi della seconda diagonale.

$$detA = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$$

Una qualsiasi matrice quadrata è invertibile se e solo se il suo determinante è non nullo. In particolare, avendo una matrice A del tipo

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Si avrà che la matrice inversa, A^{-1} è data da

$$A^{-1} = \frac{1}{detA} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

9.3 Gruppo lineare di ordine 2

Si definisce il gruppo lineare di ordine 2 come l'insieme di tutte le matrici reali quadrate di ordine 2 tali che il loro determinante non è nullo.

$$\mathrm{GL}_2(\mathbb{R}) = \{A \in \mathrm{M}_2(\mathbb{R}) : detA \neq 0\}$$

Si noti che il gruppo lineare di ordine 2 è un gruppo rispetto all'operazione di prodotto righe per colonne $(GL_2(\mathbb{R}), \cdot)$, ma non è un gruppo abeliano o commutativo.

9.4 Teorema di Binet

Siano A e B due matrici, il determinante della matrice $A \times B$ è uguale al prodotto tra i determinanti delle due singole matrici, ossia

$$det(A \times B) = detA \times detB$$

Inoltre, per quanto riguarda i determinanti vale anche la seguente proprietà:

$$det(A^{-1} = \frac{1}{detA}$$

9.5 Sottogruppo normale

Siano G un gruppo ed N un suo sottogruppo, si dice che N è sottogruppo normale di G, $N \leqslant \mathrm{G}$, se per ogni g appartenente a G vale

$$N\,g = g\,N$$

ossia

$$n\,g = g\,n_1 \;\forall n, n_1 \in N$$

Se G è un gruppo abeliano, allora tutti i suoi sottogruppi saranno normali.
Per trovare se un determinato N, sottogruppo di G, è un gruppo normale, si deve considerare che N è sottogruppo normale di G se e solo se per ogni g appartenente a G e per ogni $g^{-1} \cdot n \cdot g \in N$
(segue dimostrazione)

9.6 Insieme quoziente

Sia G un gruppo rispetto a un'operazione e sia N un suo sottogruppo normale, si definisce l'insieme quoziente $\frac{G}{N}$ come

$$\frac{G}{N} = \{N \cdot g : g \in G\} = \{g \cdot N : g \in G\}$$

Per l'insieme quoziente vale la seguente proprietà:

$$\left.\begin{cases} Ng_1 = Ng_1' \\ Ng_2 = Ng_2' \end{cases}\right\} \Rightarrow Ng_1\, Ng_2 = Ng_1'\, Ng_2' \Rightarrow Ng_1g_2 = Ng_1'g_2'$$

(segue dimostrazione)

Inoltre, l'insieme quoziente è un gruppo rispetto al prodotto, in particolare si ha che

$$Ng_1 \cdot Ng_2 = Ng_1 \cdot g_2$$

(segue dimostrazione p.: associativa, neutro, simmetrico)

Rispetto alla somma l'insieme quoziente si definisce come

$$\frac{G}{N} = \{g + N : g \in G\}$$

Si noti che considerando l'insieme quoziente di $\mathbb{Z}$ rispetto ai gruppi ciclici generati da n e rispetto all'operazione di somma, vi è una netta somiglianza con le classi di resto modulo n.
$(\mathbb{Z}, +) \quad < n >= \{n\,k : k \in \mathbb{Z}\ n \in \mathbb{N}\}$

$$\frac{Z}{< n >} = \{a+ < n >: a \in \mathbb{Z}\}$$

$a = q\,n + r\ 0 \leq r < n$

$a+ < n >= n\,q + r+ < n >= r+ < n >$

Si hanno quindi le classi

$$\{0+ < n >; 1+ < n >; ...; n-1+ < n >\} = \{\overline{0}; \overline{1}, ..., \overline{n-1}\}$$

9.7 Insieme delle unità di Zn

Sia $\mathbb{Z}_n$ l'insieme delle classi reste modulo n, si definisce l'insieme delle unità di $\mathbb{Z}_n$, come l'insieme di tutte le classi di resto modulo n tali che siano invertibili.
L'insieme delle unità di $\mathbb{Z}_n$ è un gruppo rispetto al prodotto.
(segue dimostrazione p. associativa, neutro, simmetrico)

9.8 Generatori di un gruppo ciclico

Sia $G =< g >$ un gruppo rispetto alla moltiplicazione, allora si ha che:

- se G è infinito, i generatori di G sono g e g^{-1};

- se G è finito di cardinalità n, i suoi generatori sono tutti i g^k tali che $MCD(k, n) = 1$, ovvero k ed n sono coprimi.

(segue dimostrazione)

Diciamo inoltre che:

Proprietà 9.1. *Ogni sottogruppo di un gruppo ciclico è a sua volta ciclico*

(segue dimostrazione)

Proprietà 9.2. *Sia G un insieme di cardinalità n generato da ¡g¿.*

Se k è una divisore di n allora esiste ed è unico un sottogruppo di G di ordine k

(segue dimostrazione)

9.9 Omomorfismo tra gruppi

Siano G e G' due gruppi rispetto ad una determinata operazione.
Un omomorfismo tra G e G' è una funzione o applicazione $f : G \to G'$ tale che per ogni g_1 e g_2 appartenenti a G sia

$$f(g_1 \cdot g_2) = f(g_1)\, f(g_2)$$

Da notare che nel primo caso tra g_1 e g_2 si applica l'operazione del gruppo G, mentre nel secondo caso tra $f(g_1)$ e $f(g_2)$ si applica l'operazione del gruppo G'.
Sia $f : G \to G'$ un omomorfismo, allora valgono le seguenti **proprietà:**

- $f(1_G) = 1_{G'}$;
  (segue dimostrazione)

- $f(g^{-1}) = \big[f(g)\big]^{-1}$;
  (segue dimostrazione)

- $f(g^n) = \big[f(g)\big]^n$;
  (segue dimostrazione)

9.10 Nucleo

Sia $f : G \to G'$ un omomorfismo.

Il nucleo di f è

$$ker f = \{g \in G : f(g) = 1_{G'}\}$$

Il nucleo è un sottogruppo di G e sicuramente non è vuoto perché sappiamo già che 1^G vi appartiene.

9.11 Immagine

Sia $f : G \to G'$ un omomorfismo.
L'immagine di f è

$$Im\, f = \{f(g) \forall g \in G\} = \{g' \in G' : g' = f(g) \;\; g \in G\}$$

L'immagine è un sottogruppo di G'

9.12 Teorema sul nucleo e immagine

Sia $f : G \to G'$ un omomorfismo, allora si ha che:

- $Ker\, f$ è un sottogruppo normale di G;
- $Im\, f$ è un sottogruppo di G'

(segue dimostrazione di entrambe)

Proprietà 9.3. *Sia $f : G \to G'$ un omomorfismo e sia $Ker\, f$ il suo nucleo, allora si ha che f è iniettivo se e solo se $Ker\, f = \{1_G\}$*

(segue dimostrazione)

9.13 Omomorfismo canonico

Siano G un gruppo ed N un suo sottogruppo normale rispetto a una determinata operazione.
Sia $\frac{G}{N}$ il gruppo dell'insieme quoziente rispetto alla stessa operazione.
Allora $\pi : G \to \frac{G}{N}$ è un omomorfismo canonico che associa ad ogni g di G, ossia

$$\pi(g) = gN$$

(segue dimostrazione)

9.14 I teorema di omomorfismo tra gruppi

Sia $f : G \to G'$ un omomorfismo e sia $Ker\, f$ il suo nucleo.
Allora esiste ed è unico un isomorfismo $f : Ker\, f \to Im\, f$ tale che

$$f : G \to Im\, f = \mathcal{F} : \frac{G}{Ker\, f} \to Im\, f \circ \pi : G \to \frac{G}{Ker\, f}$$

con $Im\, f \subseteq G'$.
(segue dimostrazione)

9.15 Isomorfismo

Dicesi isomorfismo un omomorfismo $f : G \to G'$ biunivoco e si dice che G è isomorfo a G', in simboli

$$G \cong G'$$

9.15.1 Corollario

Poiché $f : \frac{G}{Ker\, f} \to Im\, f$ è un isomorfismo, se $f : G \to G'$ è suriettivo allora si ha che $G' = Im\, f$ e quindi $f : \frac{G}{Ker\, f} \to G'$ è un isomorfismo.

9.16 Isomorfismo rispetto Z

Sia G un gruppo ciclico (moltiplicativo) tale che $G =< g >$, allora si ha che

- se $|G| = \infty$ allora G è isomorfo a $\mathbb{Z}$;
- se $|G| = m$ allora G è isomorfo a $\mathbb{Z}_n$.

(segue dimostrazione)

10 Anelli

10.1 Anello

Sia A un insieme, si dice che A è un anello rispetto a due operazioni se si ha che

- A è un gruppo abeliano rispetto alla prima operazione;
- vale la proprietà associativa rispetto alla seconda operazione;
- vale la proprietà distributiva rispetto alle due operazioni.

10.2 Anello con unità

Un insieme A è un anello con unità rispetto a due operazioni se, oltre ad essere un anello, si ha che A contiene l'elemento neutro rispetto alla seconda operazione.

10.3 Anello commutativo

Un insieme A è un anello commutativo rispetto a due operazioni se, oltre ad essere un anello, si ha che in A vale la proprietà commutativa rispetto alla seconda operazione.

10.4 Corpo

Un insieme A è un corpo rispetto a due operazioni se, oltre ad essere un anello, si ha che A, al più escludendo lo 0, è un gruppo rispetto alla seconda operazione.

10.5 Campo

Un insieme A è un campo rispetto a due operazioni se, oltre ad essere un anello, si ha che A, al più escludendo lo 0, è un gruppo abeliano rispetto alla seconda operazione.
In molti casi, se non specificato, si sott'intende che la prima operazione sia la somma, mentre la seconda il prodotto.
In base a quanto detto si ha che:

- $(\mathbb{Z}, +, \cdot)$ è un anello commutativo con unità;
- $(\mathbb{Q}, +, \cdot) \subseteq (\mathbb{R}, +, \cdot) \subseteq (\mathbb{C}, +, \cdot)$, sono campi (o sottocampi).

10.6 Corpo dei quaternioni reali

10.7 Sottoanello

Sia A un anello rispetto a due determinate operazioni e sia S un sottoinsieme di A, allora se S è un anello rispetto alle stesse operazioni di A allora S è un sottoanello di A.
Si noti che S è un sottoanello di A se e solo se valgono:

1. $a \cdot b^{-1} \in S \quad \forall a, b \in S \quad (a - b \in S$ nel caso in cui la prima operazione sia la somma);
2. $a \cdot b \in S \quad \forall a, b \in S$ (si applica la seconda operazione).

La 1, in particolare, ci dice che S rispetto alla prima operazione è sottogruppo di A rispetto alla prima operazione.

10.8 Divisore dello zero

Sia a un elemento di un insieme A diverso da 0, si dice che a è un divisore dello 0 in A se

$$\exists b \neq 0,\, b \in A : a \cdot b = 0$$

Si noti che tutti i campi sono privi di divisori dello zero, la sua presenza quindi basta per affermare che una struttura algebrica non è un campo.
(seque dimostrazione per assurdo)

10.9 Dominio di integrità

Un anello privo di divisori dello 0 si dice dominio di integrità.
Si noti che un campo è sempre un dominio di integrità ma un dominio di integrità non è necessariamente un campo.
Un esempio famoso di ciò è l'anello $(\mathbb{Z}, +, \cdot)$ che è un dominio di integrità ma non è un campo.

10.10 Ideali

10.10.1 Ideale destro

Sia $(A, +, \cdot)$ un anello, si dice che I è un ideale destro di A se si ha che $(I, +)$ è un gruppo abeliano e inoltre vale che

$$x \cdot a \in I \forall a \in A,\ \forall x \in I$$

10.10.2 Ideale sinistro

Sia $(A, +, \cdot)$ un anello, si dice che I è un ideale sinistro di A se si ha che $(I, +)$ è un gruppo abeliano e inoltre vale che

$$a \cdot x \in I \forall a \in A,\ \forall x \in I$$

10.10.3 Ideale bilatero

Se un ideale è contemporaneamente sia destro che sinistro si dice ideale bilatero.
Si noti che un ideale I è sempre un sottoanello ma un sottoanello non è sempre un ideale.
Quinai sia $(A, +, \cdot)$ un anello e sia a un elemento di A, si ha che

$$(a) = \{a \cdot x : x \in A\} \qquad (a) = \{x \cdot a : x \in A\}$$

sono rispettivamente un ideale destro e un ideale sinistro.
(segue dimostrazione)

10.10.4 Ideale bilatero principale

Un ideale bilatero si dice principale se si ha che

$$I = (a) \;\; a \in A$$

10.10.5 Ideale banale

Sia $(A, +, \cdot)$ un anello, si dicono ideale banali di A:

- $(0) = \{0\}$;
- $(1) = \{A\}$.

Proprietà 10.1. *Sia $(A, +, \cdot)$ un anello con unità.*
Se I è un ideale e si ha che l'unità della seconda operazione appartiene ad I, allora $I = A$.

(segue dimostrazione)

Proprietà 10.2. *Se I contiene almeno un elemento invertibile in I, allora si ha che $I = A$.*

(segue dimostrazione)

Proprietà 10.3. *Sia A un anello commutativo con unità, A è un campo se se solo se non possiede ideali non banali.*

(segue dimostrazione)

Proprietà 10.4. *Sia $(A, +, \cdot)$ un anello con unità, allora le seguenti affermazioni sono equivalenti:*

- A è un corpo;
- A è privo di ideali destri non banali;
- A è privo di ideali sinistri non banali.

Esempio
L'insieme delle matrici reali quadrate di ragione 2 non è un corpo rispetto alla somma o al prodotto righe per colonne, infatti possiede ideali destri e sinistri non banali ed è privo di ideali bilateri.

Proprietà 10.5. *Si consideri $(\mathbb{Z}, +, \cdot)$, si ha che ogni ideale di $\mathbb{Z}$ è principale.*

(segue dimostrazione)

Proprietà 10.6. *Sia $(A, +, \cdot)$ un anello e sia I un suo ideale, allora si ha che $(I, +)$ è un sottogruppo di $(A, +)$, quindi si definisce l'insieme*

$$\frac{A}{I} = \{a + I : a \in A\}$$

e si ha che $(\frac{A}{I}, +)$ è un gruppo abeliano, quindi vale

$$(a + I) + (a' + I) = (a + a') + I$$

Possiamo inoltre definire

$$(a + I)(a' + I) = aa' + I$$

(segue dimostrazione)

10.10.6 Anello a ideali principali

Un anello commutativo con unità si dice a ideali principali se ogni suo ideale è principale.

10.10.7 Ideale primo

Sia $(A, +, \cdot)$ un anello commutativo con unità.
Un suo ideale P è primo se per ogni $a \cdot b$ che appartiene a P si ha che o a appartiene a P o b appartiene a P

$$\forall a \cdot b \in P \Rightarrow a \in P \vee b \in P$$

Esempio
Consideriamo $(\mathbb{Z}, +, \cdot)$.
In $\mathbb{Z}$ l'ideale n è primo se n è primo, infatti si ha che se n è primo

$$\forall a \cdot b \in (n) \Rightarrow n|ab \Rightarrow n|a \vee n|b \Rightarrow a \in (n) \vee b \in (n)$$

che vale solo se n è primo.

10.10.8 Ideale massimale

Sia $(A, +, \cdot)$ un anello commutativo con unità, un suo ideale M si dice massimale se per ogni ideale J di A tale che M è contenuto in J e J è contenuto in A, si ha che o $M = J$ o $J = A$.

Esempio

Consideriamo $(\mathbb{Z}, +, \cdot)$.
In $\mathbb{Z}$ tutti gli ideali (n) con n primo sono massimali.
Infatti si ha

$$(n) \subseteq J \subseteq A$$

Consideriamo $J = (n)$, allora

$$n \in (m) \Rightarrow n = m \cdot t \Rightarrow m | n \Rightarrow n = 1 \vee m = n$$

Proprietà 10.7. *Sia $(A, +, \cdot)$ un anello commutativo con unità e sia P un suo ideale. P è un ideale primo se e solo se $\frac{A}{P}$ è un dominio di integrità.*

(segue dimostrazione)

Proprietà 10.8. *Sia $(A, +, \cdot)$ un anello commutativo con unità e sia M un suo ideale. M è un ideale massimale se e solo se $\frac{A}{M}$ è un campo.*

(segue dimostrazione)

10.10.9 Corollario

Sia $(A, +, \cdot)$ un anello commutativo con unità, ogni ideale massimale di A è un ideale primo.
Si noti che non vale necessariamente il contrario.
(segue dimostrazione)

10.11 Omomorfismo anelli

Siano A e A' due anelli rispetto a due determinate operazioni, allora $f : A \to A'$ è un omomorfismo di anelli se valgono

1. $f(a + b) = f(a) + f(b)\ \forall a, b \in A$
2. $f(a \cdot b) = f(a) \cdot f(b)\ \forall a, b \in A$

Il nucleo di $f : A \to A'$ è $Ker\, f = \{a \in A : f(a) = 0_{A'}\}$.
L'immagine di $f : A \to A'$ è $Im\, f = \{f(a) \forall a \in A\}$

Proprietà 10.9. *Sia $f : A \to A'$ un omomorfismo di anelli, $Ker\, f$ è un ideale di A*

(segue dimostrazione)

Proprietà 10.10. *Sia $f : A \to A'$ un omomorfismo di anelli, $Im\, f$ è un sottoanello di A'*

(segue dimostrazione)

10.12 Omomorfismo canonico

Sia $f : A \to A'$ un omomorfismo di anelli.
Poiché $Ker\, f$ è un ideale di A allora $\frac{A}{Ker\, f}$ è un anello, quindi $\pi : A \to \frac{A}{Ker\, f}$ è un omomorfismo canonico di anelli che associa ad ogni a appartenente ad A $a + Ker\, f$.
Inoltre, il nucleo di π, $ker\, \pi$, coincide con il nucleo di f, $Ker\, f$.

10.13 I teorema di omomorfismo di anelli

Sia $f : A \to A'$ un omomorfismo di anelli e sia $\pi : A \to \frac{A}{Ker\, f}$ un omomorfismo canonico.
Allora esiste un isomorfismo di anelli del tipo

$$\mathcal{F} : \frac{A}{Ker\, f} \to Im\, f$$

Inoltre, si ha che

$$f : A \to Im\, f = \mathcal{F} : \frac{A}{Ker\, f} \to Im\, f \circ \pi : A \to \frac{A}{Ker\, f}$$

Si noti anche che per tale motivo $\frac{A}{Ker\, f}$ è isomorfo a $Im\, f$

10.14 Caratteristica di un anello

Sia A un anello con unità, si dice che A ha caratteristica n, se n è il più piccolo intero positivo, se esiste, tale che $n \cdot 1_A = \emptyset$.
Se n non esiste si dice che A ha caratteristica $\emptyset$

10.15 Sottoanello fondamentale

Sia A un anello con unità, si dice che P è un sottoanello fondamentale di A se si ha:

$$P = \{z \cdot 1_A : z \in \mathbb{Z}\}$$

(segue dimostrazione)

Proprietà 10.11. *Se A è un campo, allora P è un dominio di integrità.*

Proprietà 10.12. *Se la caratteristica di A è $\emptyset$ allora P è isomorfo a $\mathbb{Z}$, mentre se la caratteristica di A è n allora P è isomorfo a $\mathbb{Z}_n$.*

(segue dimostrazione

)
Si ha inoltre che f è banalmente un omomorfismo suriettivo.

$$Ker\, f = \{z \in \mathbb{Z} : f(z) = 0\}$$

Si noti che P è isomorfo a $\frac{\mathbb{Z}}{Ker\, f}$ e si ha che $f(z) = z \cdot 1_A$.
Si distinguono i casi:

- se la caratteristica di A è $\emptyset$

$$z = 0 \Rightarrow Ker\, f = (0) \Rightarrow P \cong \frac{\mathbb{Z}}{Ker\, f}) \frac{\mathbb{Z}}{0} = \mathbb{Z}$$

- se la caratteristica di A è n

$$z = n \Rightarrow Ker\, f = (n) \Rightarrow P \cong \frac{\mathbb{Z}}{Ker\, f}) \frac{\mathbb{Z}}{n} = \mathbb{Z}_n$$

10.16 Corollario

Sia K un campo, allora la caratteristica di K è 0 oppure un numero p primo.

10.17 Anello dei polinomi

Sia A un anello commutativo con unità e sia x un'incognita.
L'anello dei polinomi a coefficienti in A si definisce come

$$A\big[x\big] = \{f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n : a_i \in A, n \in \mathbb{N}\}$$

L'anello $(A\big[x\big])$ è commutativo con unità.
Dati due polinomi $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ e
$g(x) = a_0 + a_1 x + a_2 x^2 + ... + a_m x^m$, con $n \geq m$ la somma e il prodotto si definiscono come:

- $f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$;
- $f(x)\, g(x) = \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i\, b_i) x^k$

10.18 Coefficiente direttore

Sia $f(x)$ un polinomio tale che

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

allora a_n si dice coefficiente direttore.

10.19 Grado di un polinomio

Sia $f(x)$ un polinomio tale che

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

allora n si dice grado (deg)di $f(x)$.
Consideriamo due polinomi $f(x)$ e $g(x)$, si ha che

- $deg\big[f(x) + g(x)\big] \leq max\{deg\, f(x); deg\, g(x)\}$
- $deg\big[f(x) \cdot g(x)\big] = deg\, g(x) + deg\, g(x)$ (se A è un dominio di integrità).

Si noti che se A è un dominio di integrità, allora $A\big[x\big]$ è anch'esso un dominio di integrità.

10.20 Divisione tra polinomi

Siano $f(x)$ e $g(x)$ due polinomi appartenenti ad $A\big[x\big]$, allora esistono due polinomi $q(x)$ e $r(x)$ tali che

$$f(x) = g(x)q(x) + r(x) \qquad 0 \leq deg\big[r(x)\big] < deg$$

(segue dimostrazione)

10.21 Massimo comun divisore tra polinomi

Sia $A\big[x\big]$ l'anello dei polinomi e siano $f(x)$ e $g(x)$ due polinomi che vi appartengono, allora esiste il massimo comun divisore tra $f(x)$ $g(x)$ ed è anch'esso un polinomio $d(x)$.

$$f(x), g(x) \in A\big[x\big] \Rightarrow \exists\ MCD(f(x), g(x)) = d(x)$$

10.22 Identità di Bezout per i polinomi

Siano $f(x)$ e $g(x)$ due polinomi appartenenti all'anello dei polinomi $A\big[x\big]$ e sia $d(x)$ il loro massimo comun divisore.
Allora si ha

$$d(x) = \lambda(x)\, f(x) + \beta(x) g(x)$$

10.23 Polinomio divisore

Siano $f(x)$ e $g(x)$ due polinomi appartenenti all'anello dei polinomi $A\big[x\big]$, allora si ha che $g(x)$ è un divisore di $f(x)$ se si ha che

$$f(x) = g(x)q(x)$$

10.24 Polinomio irriducibile

Siano $f(x)$ e $g(x)$ due polinomi appartenenti all'anello dei polinomi $A\big[x\big]$, allora si ha che

$$f(x) = g(x)h(x) \Rightarrow g(x) = a \in A \vee h(x) = b \in A$$

Si noti che tutti i polinomi di grado 1 sono irriducibili.

10.25 Polinomio primo

Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $A\big[x\big]$, $f(x)$ è un polinomio primo se si ha che

$$f(x)|a(x)b(x) \Rightarrow f(x)|a(x) \vee f(x)|b(x)$$

Un polinomio è primo se e solo se è anche irriducibile.

10.26 Teorema per la fattorizzazione di polinomi

Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $A\big[x\big]$, $f(x)$ si fattorizza in prodotto di polinomi indivisibili.
Tale fattorizzazione è unica, se non al più per delle costanti.

10.27 Teorema di Ruffini

Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $K\big[x\big]$ e sia K un campo.
Sia α un elemento di K allora α è una radice di $f(x)$ se e solo se

$$(x - \alpha)|f(x)$$

(segue dimostrazione)

10.28 Molteplicità di una radice

Sia α una radice di un polinomio $f(x)$, si dice che α ha molteplicità m se

$$f(x) = (x - \alpha)^m \cdot q(x) \qquad q(x) \neq 0$$

10.29 Numero di radici di un polinomio

Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $K\big[x\big]$ e sia il gradi di $f(x)$, $deg(f(x)) = n$, allora si ha che $f(x)$ ha in K al più n radici contate con la loro molteplicità.
(segue dimostrazione induzione)

10.30 Teorema fondamentale dell'algebra

Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $\mathbb{C}\big[x\big]$, allora $f(x)$ ha almeno una radice complessa.
Come conseguenza, $f(x)$ ha tutte le radici in $\mathbb{C}$.

- nell'anello dei polinomi $\mathbb{C}\big[x\big]$ gli unici polinomi irriducibili sono quelli con grado $deg(f(x)) = 1$;
- nell'anello dei polinomi $\mathbb{R}\big[x\big]$ gli unici polinomi irriducibili sono quelli con grado $deg(f(x)) = 1$ oppure quelli con grado $deg(f(x)) = 2 : \Delta(f(x)) < 0$

10.31 Polinomio primitivo

Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $\mathbb{Z}\big[x\big]$ esso si dice primitivo se il massimo comun divisore tra i suoi coefficienti è 1.

10.32 Teorema su polinomi irriducibili

Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $\mathbb{Z}\big[x\big]$ e sia $f(x)$ un primitivo.
Allora $f(x)$ è irriducibile in $\mathbb{Z}\big[x\big]$ se e solo se è irriducibile in $\mathbb{Q}\big[x\big]$.
Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $K\big[x\big]$ di grado 2 o 3.
Se $f(x)$ non ha radici in K allora è irriducibile.
Infatti, sia $f(x)$ un polinomio di grado 2 o 3 riducibile, si ha allora

$$f(x) = (ax + b)f'(x) \qquad deg(f'(x)) < deg(f(x)) \Rightarrow x = -\frac{b}{a} \in K$$

Se il polinomio è di grado 4 o maggiore potrebbe essere riducibile pur non avendo radici.

10.33 Criterio di Eisenstein

Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $\mathbb{Z}\big[x\big]$ tale che
$f(x) = a_0 + a_1x + \ldots + a_nx^n$.
Se esiste un primo p tale che $p|a_0$, $p|a_1$,...,$p|a_{n-1}$ ma

$p \not| a_n$

$p^2 \not| a_0$

allora $f(x)$ è irriducibile.
Si noti che se esiste il suddetto primo il polinomio sarà sicuramente irriducibile ma se questo non esiste non necessariamente si avrà che il polinomio è riducibile.

Proprietà 10.13. *Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $\mathbb{Z}\big[x\big]$ tale che $f(x) = a_0 + a_1x + \ldots + a_nx^n$.*
E siano r ed s due interi tra loro coprimi tali che

$$r|a_0 \wedge s|a_n$$

allora si ha che α tale che

$$\alpha = \frac{r}{s} \in \mathbb{Q}$$

è radice del polinomio.

(segue dimostrazione)

Proprietà 10.14. *Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $\mathbb{Z}\big[x\big]$ tale che $f(x) = a_0 + a_1x + \ldots + a_nx^n$ e sia $p : p \not| a_n$, allora si definisce il polinomio $\mathcal{F}(x)$ appartenente all'anello dei polinomi $\mathbb{Z}_p\big[x\big]$.*
Possiamo quindi dire che se $\mathcal{F}$ è irriducibile in $\mathbb{Z}_p$ allora $f(x)$ sarà sicuramente irriducibile in $\mathbb{Z}\big[x\big]$, allo stesso modo se $f(x)$ è riducibile in $\mathbb{Z}\big[x\big]$ allora $\mathcal{F}$ è riducibile in $\mathbb{Z}_p$

(segue dimostrazione

)

10.34 Ideale generato da un polinomio

Sia $f(x)$ un polinomio appartenente all'anello dei polinomi $K\big[x\big]$ con K campo, allora si definisce l'ideale generato da $f(x)$ come

$$(f(x))\{q(x) \cdot f(x) | q(x) \in K\big[x\big]\}$$

Proprietà 10.15. *Sia $f(x)$ un polinomio irriducibile in $K\big[x\big]$, allora l'ideale generato da $f(x)$, $(f(x))$, è un ideale massimale.*

(segue dimostrazione)

10.35 Campo finito

Un campo finito è un campo caratteristico p.

Esempio

Consideriamo il campo $\mathbb{Z}_p$ con p primo e l'anello dei polinomi $\mathbb{Z}_p\big[x\big]$.
Sia $f(x)$ un polinomio irriducibile di grado n appartenente a $\mathbb{Z}_p\big[x\big]$, allora $f(x)$ è un ideale massimale perciò possiamo definire l'anello

$$\frac{\mathbb{Z}_p\big[x\big]}{(f(x))} = \{f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} | a_i \in \mathbb{Z}_p\}$$

con

$$\left|\frac{\mathbb{Z}_p\big[x\big]}{(f(x))}\right| = p^n$$

Sia $\mathbb{F}$ un campo finito, allora valgono le seguenti proprietà:

- Sia P il sotto-anello fondamentale di $\mathbb{F}$, P è isomorfo a $\mathbb{Z}_p$, $P \cong \mathbb{Z}_p$ (p primo);
- la caratteristica di $\mathbb{F}$ è un numero primo p;
- per ogni a elemento di $\mathbb{F}$ si ha che $p \cdot a = 0$
- per ogni a e b appartenenti a $\mathbb{F}$ si ha che $(a+b)^{p^n} = a^{p^n} + b^{p^n}$

10.36 Estensione

Sia $\mathbb{F}$ un campo e sia $\mathbb{E}$ un altro campo che contiene $\mathbb{F}$, $\mathbb{F} \subseteq \mathbb{E}$, allora $\mathbb{E}$ è estensione di $\mathbb{F}$.

10.37 Algebrico

Sia $\mathbb{E}$ un'estensione di un campo $\mathbb{F}$ e sia a un elemento di $\mathbb{E}$ tale che

$$\exists f(x) \in \mathbb{F}\big[x\big]$$

10.38 Estensione algebrica

Sia $\mathbb{E}$ un'estensione di $\mathbb{F}$, si dice che $\mathbb{E}$ è un'estensione algebrica su $\mathbb{F}$ se ogni elemento di $\mathbb{E}$ è algebrico su $\mathbb{F}$.

Esempio

L'insieme dei numeri complessi $\mathbb{C}$ è estensione algebrica su $\mathbb{R}$ ossia l'insieme dei numeri reali.
Sia $\mathbb{K}$ un campo e sia $K\big[x\big]$ un anello commutativo con unità, sia $f(x)$ un polinomio irriducibile in $K\big[x\big]$, sappiamo che l'ideale $(f(x))$ è massimale e che l'insieme $\frac{K\left[x\right]}{(f(x))}$ è un campo

10.39 Campo di spezzamento

Sia E una estensione di F e sia $f(x) \in F\big[x\big]$, si dirà che E è un campo di spezzamento di $f(x)$ su $F\big[x\big]$ se tutte le radici di $f(x)$ sono contenute in E.

Proprietà 10.16. *Sia $f(x) \in F\big[x\big]$ allora esiste sempre un campo di spezzamento*

(segue dimostrazione per induzione II forma)

OSSERVAZIONE
Si osservi che $K[\alpha]$ risulta **spazio vettoriale** di dimensione n su K, in quanto ogni suo elemento risulta combinazione lineare degli elementi della base $B(1, \alpha, \alpha^2, ..., \alpha^{n-1}$ con scalari $a_i \in K$.

11 Svolgimento esercizi

11.1 Generatori di un gruppo ciclico

Sia $G =< g >$ un gruppo rispetto alla moltiplicazione, allora si ha che:

- se G è infinito, i generatori di G sono g e g^{-1};
- se G è finito di cardinalità n, i suoi generatori sono tutti i g^k tali che $MCD(k, n) = 1$, ovvero k ed n sono coprimi.

Esempio

Sia $(G, \cdot)$, con $|G| = 18$, un gruppo ciclico di elementi $G =< g >$, stabilire i suoi generatori.
Come detto, essendo G finito di cardinalità n i generatori di G saranno

$$g^k : (n, k) = 1$$

ossia

$$g^k : (18, k) = 1 \Rightarrow k = 1, 3, 5, 7, 11, 13, 15, 17$$

in definitiva

$$G =< g >=< g^3 >=< g^5 >=< g^7 >=< g^{11} >=< g^{13} >=< g^{15} >=< g^{17} >$$

12 Soluzioni agli esercizi