

Definizioni Algebra

Aggiornato lez. 24 (metto le notazioni sulle matrici?)

Anno accademico 2021/2022

Contents

| | | |
|----------|--|----------|
| 1 | Capitolo 1 | 6 |
| 1.1 | Corrispondenza | 6 |
| 1.2 | Relazione in se | 6 |
| 1.3 | Relazione/Corrispondenza inversa | 6 |
| 1.4 | Relazione di equivalenza | 6 |
| 1.5 | Relazione banale (di uguaglianza) | 6 |
| 1.6 | Relazione caotica | 6 |
| 1.7 | Classe di equivalenza | 6 |
| 1.8 | Insieme quoziente | 7 |
| 1.9 | Partizione insiemistica | 7 |
| 1.10 | Funzione/Applicazione | 7 |
| 1.11 | Iniettiva | 7 |
| 1.12 | Suriettiva | 8 |
| 1.13 | Biunivoca (biiettiva) | 8 |
| 1.14 | Funzione caratteristica | 8 |
| 1.15 | Operazione binaria | 8 |
| 1.16 | Assiomi di Peano | 8 |
| 1.17 | Principio del buon ordinamento di \mathbb{N} | 9 |
| 1.18 | Teor: Divisione con resto su \mathbb{N} | 9 |
| 2 | Calcolo combinatorio | 9 |
| 2.1 | Notazione funzionale | 9 |
| 2.2 | Fattoriale crescente | 9 |
| 2.3 | Fattoriale decrescente | 9 |
| 2.4 | Pigeonhole principle (principio dei cassetti) | 9 |
| 2.5 | Permutazione | 9 |
| 2.6 | Coefficiente binomiale | 9 |
| 2.7 | Formula | 10 |
| 2.8 | Relazione ricorsiva | 10 |
| 2.9 | Simmetria | 10 |
| 2.10 | Relazione d'ordine | 10 |
| 2.11 | POSET (Partial order set) | 10 |

| | | |
|----------|---|-----------|
| 3 | I numeri | 11 |
| 3.1 | Costruzione di \mathbb{Z} (interi) | 11 |
| 3.2 | Definizione di \mathbb{Z} | 11 |
| 3.3 | Classi su \mathbb{Z} | 11 |
| 3.4 | Sottoinsiemi di \mathbb{Z} | 11 |
| 3.5 | Somma su \mathbb{Z} | 11 |
| 3.6 | Prodotto su \mathbb{Z} : | 11 |
| 3.7 | Proprietà operazioni su \mathbb{Z} | 11 |
| 3.8 | Divisibilità | 12 |
| 3.9 | Multiplo | 12 |
| 3.10 | Associati | 12 |
| 3.11 | Unità | 12 |
| 3.12 | Irriducibile | 12 |
| 3.13 | Primo | 12 |
| 3.13.1 | Proposizione: in \mathbb{Z} , a è primo $\Rightarrow a$ irriducibile | 12 |
| 3.13.2 | Proposizione: in \mathbb{Z} a irriducibile \Rightarrow a primo | 13 |
| 3.14 | Massimo comune divisore | 13 |
| 3.14.1 | Teor: Esistenza del MCD tra due numeri | 13 |
| 3.14.2 | Prop: se $c a$ e $c b$ allora c divide ogni combinazione lineare di a e b | 14 |
| 3.15 | Proposizione | 14 |
| 3.15.1 | Lemma $MCD(m, m+1)=1$ | 14 |
| 3.16 | Algoritmo di Euclide | 14 |
| 3.16.1 | Lemma1: L'algoritmo termina | 14 |
| 3.16.2 | Lemma2: Se $a = bq + r$ $MCD(a, b) = MCD(b, r)$ | 14 |
| 3.16.3 | Corollario: $MCD(a, b) = MCD(r_n, 0) = r_n$ | 15 |
| 3.16.4 | Lemma3 | 15 |
| 3.17 | Coprimi | 15 |
| 3.17.1 | Osservazione1 | 15 |
| 3.17.2 | Osservazione 2 | 15 |
| 3.17.3 | Proposizione 1 | 15 |
| 3.17.4 | Proposizione 2 | 15 |
| 3.18 | Equazione diofantea | 15 |
| 3.18.1 | Teor: Soluzione equazione diofantea | 15 |
| 3.19 | Teorema fondamentale dell'aritmetica | 16 |
| 3.19.1 | Osservazione 1 | 16 |
| 3.19.2 | Osservazione 2 | 16 |
| 3.19.3 | Dimostrazione esistenza | 16 |
| 3.20 | Dimostrazione unicità | 16 |
| 3.21 | Teor. Euclide - Esistenza infiniti primi | 17 |
| 4 | Congruenze | 18 |
| 4.1 | Congruenza modulo n | 18 |
| 4.2 | Proposizione | 18 |
| 4.3 | Quoziente | 18 |
| 4.4 | Proposizione | 18 |

| | | |
|----------|---|-----------|
| 4.5 | Osservazione | 19 |
| 4.6 | Proposizione somma | 19 |
| 4.7 | Dimostrazione prodotto | 19 |
| 4.8 | Proposizione | 19 |
| 4.9 | Classi resto invertibili | 20 |
| 4.10 | Teorema Uguaglianza sbagliata | 20 |
| 4.10.1 | Grande teorema di Fermat | 21 |
| 4.10.2 | Piccolo teorema di Fermat | 21 |
| 4.11 | Teorema Eulero-Fermat | 21 |
| 4.12 | Corollario | 22 |
| 5 | Strutture algebriche | 23 |
| 5.1 | Gruppo | 23 |
| 5.2 | Gruppo commutativo (abeliano) | 23 |
| 5.3 | Anello | 23 |
| 5.3.1 | Anello commutativo | 23 |
| 5.3.2 | Anello unitario | 23 |
| 5.3.3 | Divisore dello zero | 23 |
| 5.3.4 | Dominio di integrità | 24 |
| 5.3.5 | Legge di annullamento del prodotto | 24 |
| 5.4 | Campo | 24 |
| 5.5 | Semigrupp | 24 |
| 5.5.1 | Monoide | 24 |
| 5.6 | Elenco gruppi | 24 |
| 5.7 | Gruppo simmetrico | 25 |
| 5.7.1 | Permutazione | 25 |
| 5.7.2 | S_n | 25 |
| 5.7.3 | Proposizione | 25 |
| 5.7.4 | Proposizione | 25 |
| 5.7.5 | 3 ^a notazione: Permutazione come prodotto di cicli disgiunti | 25 |
| 5.7.6 | Orbita | 25 |
| 5.7.7 | Proposizione | 26 |
| 5.7.8 | Permutazione ciclica | 26 |
| 5.7.9 | Teorema prodotto di scambi | 26 |
| 5.7.10 | Teorema parità | 26 |
| 5.7.11 | Pari, dispari | 26 |
| 5.7.12 | Gruppo alterno | 26 |
| 5.7.13 | Segno | 26 |
| 5.8 | Classi coniugate in S_n | 27 |
| 5.8.1 | Definizione | 27 |
| 5.8.2 | Proposizione | 27 |
| 5.9 | Definizione multinsieme | 27 |
| 5.10 | Gruppi finiti | 27 |
| 5.10.1 | Proprietà 1 | 27 |
| 5.10.2 | Proprietà 2 | 27 |
| 5.11 | Sottogruppi | 28 |

| | | |
|----------|---|-----------|
| 5.11.1 | Definizione | 28 |
| 5.11.2 | Criteri di verifica | 28 |
| 5.11.3 | Notazione | 28 |
| 5.11.4 | Proposizione | 28 |
| 5.12 | Proposizione: intersezione di sottogruppi | 29 |
| 5.13 | Proposizione 1 | 29 |
| 5.14 | Proposizione 2 | 29 |
| 6 | Sottogruppo generato | 29 |
| 6.1 | Definizione | 29 |
| 6.2 | Notazione | 30 |
| 6.3 | Proposizione | 30 |
| 6.4 | $\langle X \rangle$ è il più piccolo sottogruppo che contiene X | 30 |
| 6.5 | Definizione: ordine (periodo) | 30 |
| 6.6 | Definizione: gruppo ciclico | 30 |
| 6.7 | Proposizione | 30 |
| 6.8 | Proposizione | 31 |
| 6.9 | Proposizione: sottogruppi di un gruppo ciclico | 31 |
| 6.10 | Osservazione | 32 |
| 6.11 | Proposizione | 32 |
| 6.12 | Proposizione | 32 |
| 6.13 | Teorema di Lagrange | 32 |
| 6.13.1 | Corollario 1 | 33 |
| 6.13.2 | Corollario 2 | 33 |
| 6.14 | Definizione: indice di un sottogruppo | 33 |
| 7 | Classi laterali di un sottogruppo | 33 |
| 7.1 | Definizione: congruenza destra modulo | 33 |
| 7.2 | Proposizione | 33 |
| 7.3 | Insieme quoziente | 34 |
| 7.4 | Proposizione | 34 |
| 7.5 | Definizione: congruenza sinistra modulo | 34 |
| 8 | Omomorfismi | 35 |
| 8.1 | Isomorfismo | 35 |
| 8.2 | Omomorfismo | 35 |
| 8.3 | Epimorfismo | 35 |
| 8.4 | Monomorfismo | 35 |
| 8.5 | Isomorfismo 2 | 35 |
| 8.6 | Proposizione | 35 |
| 8.7 | Kernel/Nucleo | 35 |
| 8.8 | Proposizione | 36 |
| 8.9 | Omomorfismo di anelli | 36 |
| 8.10 | Proposizione | 37 |
| 8.11 | Proposizione | 37 |

| | | |
|-----------|---|-----------|
| 9 | Polinomi a coefficienti reali in 1 indeterminata | 38 |
| 9.1 | Descrizione | 38 |
| 9.2 | Somma di polinomi | 38 |
| 9.3 | Rappresentazione come successioni | 38 |
| 9.3.1 | Somma di polinomi | 38 |
| 9.4 | Teorema: $(\mathbb{R}[x], +)$ è un gruppo (commutativo) | 38 |
| 9.5 | Prodotto di polinomi | 39 |
| 9.6 | Teorema $(\mathbb{R}, +, \cdot)$ è un anello | 39 |
| 9.7 | Grado del prodotto | 39 |
| 9.8 | Fatti importanti | 39 |
| 10 | Spazi Vettoriali | 40 |
| 10.1 | Definizione spazio vettoriale | 40 |
| 10.2 | Scalare | 40 |

1 Capitolo 1

Relazione e corrispondenza sono interscambiabili.

1.1 Corrispondenza

Una corrispondenza ρ di X in Y è una terna (ρ, X, Y) dove $\rho \subseteq X \times Y$.

1.2 Relazione in se

Una Relazione di X in se, è una corrispondenza ρ di X in X . Se $(x, y) \in \rho$ si scrive anche $x\rho y$ (notazione infissa), cioè x è in relazione ρ con y .

1.3 Relazione/Corrispondenza inversa

Una corrispondenza ρ di X in Y è la relazione di Y in X denotata con ρ^{-1} data dalla seguente:

$$y\rho^{-1}x \Leftrightarrow x\rho y$$

1.4 Relazione di equivalenza

una relazione su A (cioè un sottoinsieme ρ di $A \times A$) si dice di equivalenza se verifica le tre seguenti proprietà:

Riflessiva: $\forall a \in A, a\rho a$.

Simmetrica: $\forall a, b \text{ in } A, a\rho b \Rightarrow b\rho a$

Transitiva: $\forall a, b, c \in A \text{ se } (a\rho b \wedge b\rho c) \Rightarrow a\rho c$

1.5 Relazione banale (di uguaglianza)

Su A $x, y \in A$ $x\rho y \Leftrightarrow x = y$

1.6 Relazione caotica

Su A $x\rho y \forall x, y \in A$

1.7 Classe di equivalenza

Data la relazione ρ in A , si definisce classe di equivalenza modulo ρ di un elemento $a \in A$ l'insieme di tutti gli elementi che sono equivalenti ad a ; si denota con $[a]_\rho$.

$$[x]_\rho := \{y \in A : y\rho x\}$$

1.8 Insieme quoziente

Data la relazione di equivalenza ρ su A , si definisce insieme quoziente l'insieme delle classi di equivalenza di ρ dato $x \in A$ si denota con A/ρ .

$$A/\rho = \{[x]_\rho : x \in A\}$$

Nota: Relazione di equivalenza e partizioni insiemistiche sono sostanzialmente la stessa cosa.

1.9 Partizione insiemistica

Una partizione insiemistica di A è una famiglia di sottoinsiemi di A non vuoti, tali che ad ogni elemento di A corrisponde un solo sottoinsieme.

$$H = \{A_i : i \in I\}$$

con

$$A_i \subseteq A \quad \forall i \in I$$

con

$$i \neq j, \quad i, j \in I \Leftrightarrow A_i \cap A_j = \emptyset$$

che equivale a dire:

$$\cup_{i \in I} A_i = A$$

cioè la famiglia H ricopre A .

1.10 Funzione/Applicazione

$f : S \rightarrow T$ è un'applicazione di S in T se (f, S, T) è una corrispondenza di S in T , ovvero $f \subseteq S \times T$ che soddisfa la seguente proprietà:

$\forall x \in S \exists ! y$ in T denotato con $y = f(x)$, f è una legge univoca (ben definita).

L'elemento $f(x)$ si chiama **immagine dell'elemento**.

L'immagine di f è un sottoinsieme del codominio T definito da:

$$Im(f) := \{y \in T : \exists x \in S, y = f(x)\}$$

Controimmagine di y è il sottoinsieme di S del dominio definito da:

$$f^{-1}(y) := \{x \in S : f(x) = y\} \subseteq S$$

1.11 Iniettiva

f è iniettiva $\Leftrightarrow \forall x, x' \in S : [f(x) = f(x') \Rightarrow x = x']$.

Definizione alternativa: f è iniettiva $\Leftrightarrow \forall x, x' \in S : [f(x) \neq f(x') \Rightarrow x \neq x']$.

f è iniettiva $\Leftrightarrow \forall y \in T \quad |f^{-1}| \leq 1$, ovvero per ogni elemento y in T esiste al più un'immagine.

1.12 Suriettiva

f è suriettiva se $\Rightarrow \forall y \in T \exists x \in S : f(x) = y$

Definizione alternativa: f è suriettiva $\Leftrightarrow f(S) = Im(S) = T$.

f è suriettiva $\Leftrightarrow \forall y \in T |f^{-1}(y)| \geq 1$, ovvero per ogni elemento y in T esiste almeno un'immagine.

1.13 Biunivoca (biiettiva)

se f è sia iniettiva che suriettiva.

f è biiettiva $\Leftrightarrow \forall y \in T |f^{-1}(y)| = 1$, ovvero per ogni elemento y in T esiste una sola immagine.

1.14 Funzione caratteristica

E' la funzione che vale 1 se $x \in S$, 0 se $x \notin S$.

1.15 Operazione binaria

Un'operazione binaria su S , è un'applicazione $m : S \times S \rightarrow S$; notazione funzionale $(s, s') \mapsto m(s, s')$; notazione infissa $sm s'$ o $s * s$.

1.16 Assiomi di Peano

per la costruzione dei naturali \mathbb{N}

1. I numeri formano una classe
2. Lo "zero" è un numero
3. Se a è un numero allora il successore a' è un numero
4. Se $a \neq b$ sono due numeri allora $a' \neq b'$
5. Lo "zero" non è successore di nessun numero ($\nexists a$ numero tale che $zero = a'$)
6. Assioma di induzione:
Se S è una classe di numeri tale che:
 - $zero \in S$
 - Se $a \in S$ allora $a' \in S$

allora ogni naturale è in S .

I naturali sono la più piccola classe che

- Contiene lo zero
- Chiusa rispetto a contenere i successori

1.17 Principio del buon ordinamento di \mathbb{N}

Se $S \subseteq \mathbb{N}, S \neq \emptyset$, allora esiste un minimo in S , cioè esiste $m \in S$ tale che se $h \in \mathbb{N}, h < m$ allora $h \notin S$.

1.18 Teor: Divisione con resto su \mathbb{N}

Siano $a, b \in \mathbb{N}, b \neq 0$; allora esistono $q, r \in \mathbb{N}$ tali che

- $a = bq + r$
- $0 \leq r < b$

$\forall a, b \in \mathbb{Z}, b \neq 0; \exists$ unici $q, r \in \mathbb{Z}$ con $a = bq + r \wedge 0 \leq r < b$ TODO: Dimostrazione

2 Calcolo combinatorio

2.1 Notazione funzionale

Insieme delle applicazioni da A verso B

$$B^A = \{f : A \rightarrow B\}$$

2.2 Fattoriale crescente

$$n^{(m)} := n * (n + 1) * \dots * (n + m - 1)$$

2.3 Fattoriale decrescente

$$n_{(m)} := n * (n - 1) * \dots * (n - m + 1)$$

2.4 Pigeonhole principle (principio dei cassetti)

Se ho n oggetti e m cassetti, se $n > m$ e devo disporre tutti gli oggetti nei cassetti allora esiste un cassetto che contiene almeno due oggetti.

2.5 Permutazione

Sia A un insieme. Una biiezione $f : A \rightarrow A$ si chiama anche *permutazione* di A.

2.6 Coefficiente binomiale

Prima interpretazione combinatoria: $\binom{n}{i}$ è il coefficiente di $x^i y^{n-i}$ nello sviluppo $(x + y)^n = \sum_{z_i \in \{x, y\}} z_1 \dots z_n$, ovvero il numero di stringhe binarie (su x, y)

- lunghe n
- con i occorrenze di x

- con $n-i$ occorrenze di y
- $(x + y)^n = \sum_{i=0}^n \binom{n}{i} x^i y^{n-i}$

Seconda interpretazione combinatoria: numero di sottoinsiemi di cardinalità i su un insieme $[n]$ di cardinalità n .

2.7 Formula

$$\binom{n}{i} = \frac{n(n-1) * \dots * (n-i+1)}{i!} = \frac{n!}{i!(n-i)!}$$

2.8 Relazione ricorsiva

$$\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$$

Dimostrazioni algebrica e combinatoria.

2.9 Simmetria

$$\binom{n}{i} = \binom{n}{n-i}$$

Il coefficiente binomiale è simmetrico rispetto al centro della riga n -esima $\lfloor \frac{n}{2} \rfloor$ del triangolo rappresentante tutti i coefficienti del coefficiente binomiale.

Dimostrazioni algebrica e combinatoria.

2.10 Relazione d'ordine

Una relazione ρ su X è una relazione d'ordine (o un ordine, o un ordinamento) se valgono per ρ le proprietà:

- (R) $\forall x, x\rho x$
- (AS) $\forall x, y (x\rho y \wedge y\rho x) \Rightarrow x = y$
- (T) $\forall x, y, z (x\rho y \wedge y\rho z) \Rightarrow x\rho z$

2.11 POSET (Partial order set)

Un insieme munito di una relazione d'ordine si dice parzialmente ordinato.

3 I numeri

3.1 Costruzione di \mathbb{Z} (interi)

Partendo da \mathbb{N} : prendiamo su $\mathbb{N} \times \mathbb{N}$ la relazione ρ definita sulle coppie $(n, m) \in \mathbb{N} \times \mathbb{N}$ tale che $(n, m)\rho(n', m') \Leftrightarrow n + m' = m + n'$

3.2 Definizione di \mathbb{Z}

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \rho$$

3.3 Classi su \mathbb{Z}

$\overline{(0, 0)}$ zero
 $\overline{(m, 0)}, m > 0$ positivi
 $\overline{(0, n)}, n > 0$ negativi

3.4 Sottoinsiemi di \mathbb{Z}

$$\mathbb{Z} = \mathbb{Z}^{>0} \cup \{0, 0\} \cup \mathbb{Z}^{<0}$$

3.5 Somma su \mathbb{Z}

$$\overline{(n, m)} + \overline{(n', m')} = \overline{(n + n', m + m')}$$

3.6 Prodotto su \mathbb{Z} :

$$\overline{(n, m)} \cdot \overline{(n', m')} = \overline{(nn' + mm', nm' + mn')}$$

3.7 Proprietà operazioni su \mathbb{Z}

$\forall a, b, c \in \mathbb{Z}$ (a, b, c coppie $\overline{(n, m)}$) valgono le seguenti:

1. Associatività: $(a + b) + c = a + (b + c)$
2. Commutatività: $a + b = b + a$
3. Esiste uno *zero* per la somma, cioè un elemento $0 : a + 0 = 0 + a = a$
4. $\forall a \in \mathbb{Z}$ esiste un elemento detto *opposto*, denotato con $-a$, cioè un elemento tale che: $a + (-a) = (-a) + a = 0$.
 $a = \overline{(n, m)}$
 $-a = \overline{(m, n)}$
5. Associatività prodotto: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
6. Commutatività prodotto: $a \cdot b = b \cdot a$

7. Esiste un *elemento neutro* per il prodotto, "1", cioè un numero in \mathbb{Z} tale che:

$$a \cdot 1 = 1 \cdot a = a$$

$$\overline{(n, m)} \cdot \overline{(1, 0)} = \overline{(n, m)}$$

8. Distributività del prodotto sulla somma:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

3.8 Divisibilità

Dati $a, b \in \mathbb{Z}$ si dice che a divide b , e si indica $a|b$, se e solo se $\exists c \in \mathbb{Z}$ tale che $b = a \cdot c$ (ovvero $a|b \Leftrightarrow \exists c \in \mathbb{Z} : b = a \cdot c$).

La divisibilità è una relazione sugli interi:

3.9 Multiplo

Se $a|b$ diremo che b è un multiplo di a .

3.10 Associati

a, b sono associate se $a|b$ e $b|a$

Oss1: in \mathbb{N}^* sono associati $\Leftrightarrow a = b$.

Oss2: in generale, in $\mathbb{Z} \Leftrightarrow a = b$ oppure $a = -b$.

3.11 Unità

In \mathbb{Z} sono $+1$ e -1 .

3.12 Irriducibile

Un elemento $a \in \mathbb{Z}$, $a \neq 0$ è irriducibile se $a = b \cdot c \Rightarrow b$ oppure c sono unità.

3.13 Primo

Un elemento $a \in \mathbb{Z}$ si dice primo se:

$$a|b \cdot c \Rightarrow a|b \text{ oppure } b|c$$

3.13.1 Proposizione: in \mathbb{Z} , a è primo $\Rightarrow a$ irriducibile

Sia $a = b \cdot c$: usando l'ipotesi che a è primo allora $a|b$ oppure $a|c$.

Se $a|b \Rightarrow \exists h : b = a \cdot h \Rightarrow a = a \cdot h \cdot c \Rightarrow h \cdot c = 1 \Rightarrow c = \pm 1$

Allora $a = b \cdot (+1)$ oppure $a = b \cdot (-1)$, a è irriducibile.

3.13.2 Proposizione: in \mathbb{Z} a irriducibile \Rightarrow a primo

Ipotesi: a irriducibile

Tesi: a primo Supponiamo che $a|bc \Leftrightarrow \exists h \in \mathbb{Z} : bc = ah$,

voglio mostrare che $a|b$ oppure $a|c$ ovvero che se $a \nmid b$ allora $a|c$.

Ora a irriducibile, i suoi divisori sono $a, -a, 1, -1$. $a \nmid b$ allora anche $-a \nmid b \Rightarrow$ i divisori comuni tra a e b sono $1, -1 \rightarrow MCD(a, b) = 1$.

$$\exists(\text{id. Bézout}) \exists h, k \in \mathbb{Z}$$

$$1 = ah + bk$$

moltiplicando per c

$$c = cah + cbk = a(ck + k) \quad [cb = a]$$

quindi $a|c$.

3.14 Massimo comune divisore

Dati a, b non entrambi nulli, un elemento $d \in \mathbb{Z}$ si chiama massimo comune divisore tra a e b un numero tale che:

- $d|a \wedge d|b$
- Se $c|a \wedge c|b$, allora $c|d$: d è il massimo tra i divisori comuni.

Chiamiamo massimo comune divisore l'unico positivo che soddisfa le due proprietà.

3.14.1 Teor: Esistenza del MCD tra due numeri

$\forall a, b \in \mathbb{Z}$ non entrambi nulli, esiste un numero $d \in \mathbb{N}^*$ tale che $d = MCD(a, b)$

Il massimo comune divisore si esprime come una combinazione lineare tra a e b , ovvero esistono $s, t \in \mathbb{Z}$ tali che $d = s \cdot a + t \cdot b$ (*identità di Bézout*).

Dimostrazione:

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

1. $S \subseteq \mathbb{N}$
2. $S \neq \emptyset$

a e b sono non entrambi nulli, quindi almeno uno dei due è $\neq 0$. Sia esso a .

Se $a > 0$ allora $1 \cdot a + 0 \cdot b = a > 0$ Se $a < 0$ allora $(-1) \cdot a + 0 \cdot b = a > 0$

Dimostrazione che $d|a$ e $d|b$:

Dividiamo a per d (divisione col resto): $\exists q, r$ con $a = dq + r$, $0 \leq r < d$

Se $r = 0$ allora $d|a$

Se $r \neq 0$ allora $0 < r < d$

$r = a - dq$; dato che $d \in S \Rightarrow d = x_0a + y_0b$ allora

$$r = a - q(x_0a + y_0b) = a - qx_0a - qy_0b = a(1 - qx_0) - (qy_0)b$$

Quindi $r \in S$ perchè è una combinazione lineare > 0 ma $r < d$, però d è il minimo di $S \Rightarrow$ Assurdo.

Dimostrazione se $d'|a$ e $d'|b$ allora $d'|d$:

Poichè $d'|a$ e $d'|b$ si ha che

$$\exists h : a = d' \cdot h, \exists k : b = d' \cdot k$$

Ora

$$\begin{aligned} d &= x_0 a + y_0 b \\ &= x_0 (d' h) + y_0 (d' k) = \\ &= d' (x_0 h + y_0 k) \Rightarrow d' | d \end{aligned}$$

3.14.2 Prop: se $c|a$ e $c|b$ allora c divide ogni combinazione lineare di a e b

$$\begin{aligned} a &= ch \\ b &= ck \\ \Rightarrow xa + yb &= xch + yck \\ &= c(xh + yk) \Rightarrow \in \mathbb{Z} \\ &\Rightarrow c|xa + yb \end{aligned}$$

3.15 Proposizione

$$1 = at + bs \Rightarrow MCD(a, b) = 1$$

3.15.1 Lemma $MCD(m, m+1)=1$

Sia $m \in \mathbb{N}$, $m \geq 1$ allora $MCD(m, m+1) = 1$.

Dimostrazione:

$$m + 1 - m = 1 \Rightarrow 1(m + 1) + (-1)m = 1$$

Potendo scrivere 1 come combinazione lineare di m e $m+1$, m e $m+1$ sono primi tra loro.

3.16 Algoritmo di Euclide

3.16.1 Lemma1: L'algoritmo termina

La successione dei resti è un numero $0 \leq \dots < r_2 < r_1 < b$.

3.16.2 Lemma2: Se $a = bq + r$ $MCD(a, b) = MCD(b, r)$

TODO: scrivere dimostrazione

3.16.3 Corollario: $MCD(a, b) = MCD(r_n, 0) = r_n 1$

Per il lemma 2 $MCD(a, b) = MCD(b, r_1) = MCD(r_1, r_2) = \dots = MCD(r_{n-1}, r_n) = MCD(r_n, 0)$

3.16.4 Lemma3

Se $x \in \mathbb{N}^*$ allora $MCD(x, 0) = x$

3.17 Coprimi

a, b non entrambi nulli, a e b si dicono coprimi (o *primi fra loro*) se $MCD(a, b) = 1$.

3.17.1 Osservazione1

Se a e b sono primi fra loro, allora

$$\exists x, y \in \mathbb{Z} : 1 = xa + yb$$

3.17.2 Osservazione 2

Se

$$d = MCD(a, b) \Rightarrow \exists x, y : d = ax + by$$

3.17.3 Proposizione 1

Se $\exists x_0, y_0$ con $1 = ax + by$ allora a, b sono primi tra loro.

3.17.4 Proposizione 2

Se a e b sono coprimi e dividono un terzo numero c , allora $ab|c$.

3.18 Equazione diofantea

Equazione con una o più incognite sugli interi di cui si cercano le soluzioni intere. Sono del tipo:

$$ax + by = c$$

3.18.1 Teor: Soluzione equazione diofantea

L'equazione diofante lineare in x e y $ax + by = c$ $a, b, c \in \mathbb{Z}$ possiede soluzioni intere $(x, y) \in \mathbb{Z}^2 \Leftrightarrow d = MCD(a, b) | c$

(Dim \Rightarrow) La condizione $MCD(a, b) | c$ è necessaria.

Ipotesi: esiste una soluzione di $x^2 + y^2 = z^2$

Tesi: $d | \text{termine noto}$, $d = MCD(a, b) : d | a$ e $d | b \Rightarrow d |$ ogni combinazione lineare di a, b .

Se x_0, y_0 sono una soluzione, allora $ax_0 + by_0 = c \Rightarrow d | c = ax_0 + by_0$

(Dim \Leftarrow) La condizione è sufficiente.

Ipotesi $MCD(a, b) = ah + bk$, per opportuni $h, k \in \mathbb{Z}$

3.19 Teorema fondamentale dell'aritmetica

$\forall n > 1, n \in \mathbb{N}, \exists p_1, \dots, p_j \in \mathbb{N}$ (irriducibili) $\exists h_1, \dots, h_j \geq 1$ tali che:

- $n = p_1^{h_1} \dots p_j^{h_j}$ p_1, \dots, p_j distinti
- la fattorizzazione di $n = p_1^{h_1} \dots p_j^{h_j}$ p_1, \dots, p_j è unica a meno di riordinare i fattori

3.19.1 Osservazione 1

j può essere 1, cioè potrebbe esserci un solo irriducibile nella fattorizzazione di n , anche h possono essere 1. Se n è irriducibile $\Rightarrow n = n$ è la fattorizzazione in irriducibili di n .

3.19.2 Osservazione 2

1 non è considerato irriducibile perché si perderebbe l'unicità della scrittura in irriducibili.

3.19.3 Dimostrazione esistenza

Con principio di induzione in forma forte.

Base: $n=2$, 2 è irriducibile.

Per **oss1** $2 = 2^1$ è la fattorizzazione in primi in irriducibili di 2

Ipotesi induttiva: ogni $2 \leq a < n$ ($2 \leq a \leq n-1$) è fattorizzabile in irriducibili: $\exists \alpha_1 \dots \alpha_t \alpha_i \leq 1$ e q_1, \dots, q_t irriducibili con $a = q_1^{\alpha_1} \dots q_t^{\alpha_t}$

Passo induttivo: provare che n sia prodotto di irriducibili

Primo caso: n irriducibile \rightarrow fatto, per *oss.1*

Secondo caso: n riducibile: $\exists b, c \in \mathbb{Z}, 1 \neq b, c \neq n$ (divisori propri) con $n = bc \Rightarrow 2 \leq b, c < n$.

Allora per b e c vale l'ipotesi induttiva e quindi

$$b = q_1^{\alpha_1} \dots q_t^{\alpha_t} \quad c = x_1^{\beta_1} \dots x_s^{\beta_s}$$

$$n = bc = q_1^{\alpha_1} \dots q_t^{\alpha_t} x_1^{\beta_1} \dots x_s^{\beta_s}$$

3.20 Dimostrazione unicità

Per induzione su m , con m è la lunghezza minima di una fattorizzazione per n .

m : minimo numero di irriducibili di una fattorizzazione di n

Base: $m = 1 \Rightarrow n = n$ è primo.

Se per assurdo $n = q_1 \dots q_s$, $s \geq 2$ allora $n|q_1$ o $n|q_2 \dots q_s$.

Prendiamo $n|q_1$, anche q_1 è primo $\Rightarrow n = q_1$; semplificando da entrambe le parti $\Rightarrow 1 = q_2 \dots q_s$ che porterebbe ad un assurdo perché $1 \neq 1$.

Quindi $n = q_1$ ed è l'unica fattorizzazione.

Ipotesi induttiva: se il minimo numero di primi in una fattorizzazione di n è $m - 1$, allora la fattorizzazione è unica a meno dell'ordine.

Passo induttivo: m è il minimo di una fattorizzazione di n .

3.21 Teor. Euclide - Esistenza infiniti primi

L'insieme $P = \{p \in \mathbb{N} : p \text{ è primo}\}$ è infinito.

Dimostrazione: Supponiamo che P sia finito, cioè $P = \{p_1, \dots, p_n\}$.

Sia $m = p_1 \dots p_n$ il prodotto di tutti i primi.

Considero $m + 1$: per il teorema fondamentale dell'aritmetica $m + 1 = p_1^{k_1} \dots p_n^{k_n}$, $k_1, \dots, k_n \geq 0$ almeno uno degli esponenti $\neq 0$.

Per il lemma su MCD di un numero ed il suo successivo m e $m+1$ sono coprimi.

Sia j tale che $k_j > 0$, cioè $p_j^{k_j} | m + 1$; vale anche $p_j | m$ allora $p_j | \text{MCD}(m, m+1) = 1$ che è un assurdo.

4 Congruenze

4.1 Congruenza modulo n

La congruenza modulo n (n fissato) è una relazione di equivalenza definita su \mathbb{Z} .

$$x \equiv y \pmod{n} \Leftrightarrow x - y \text{ multiplo di } n \Leftrightarrow n | x - y$$

4.2 Proposizione

La congruenza \pmod{n} è una relazione di equivalenza.

Dimostrazione:

(R)

$$\forall x \in \mathbb{Z} : x \equiv x \pmod{n} \Leftrightarrow n | (x - x)$$

Vera perché $0 = 0 \cdot n$.

(S)

$$\forall x, y \in \mathbb{Z} : x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$$

So che $n | x - y \Leftrightarrow x - y = nh$ per qualche $h \in \mathbb{Z}$.

Moltiplicando per -1: $y - x = -nh = n(-h)$ quindi $n | y - x \Rightarrow y \equiv x \pmod{n}$

(T)

$$x \equiv y \pmod{n} \wedge y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$$

$$(x - y) = nh_1 \wedge (y - z) = nh_2$$

$$(x - z) = (x - y) - (y - z) = nh_1 - nh_2 = n(h_1 - h_2) \text{ quindi } n | x - z \Rightarrow x \equiv z \pmod{n}$$

4.3 Quoziente

Il quoziente della congruenza \pmod{n} si denota come $\mathbb{Z}_{/\equiv \pmod{n}} = \{[x]_n : x \in \mathbb{Z}\}$.

Il quoziente \mathbb{Z}_n si chiama anche **interi modulo n**.

4.4 Proposizione

Dati $x, y \in \mathbb{Z}$ si ha: $x \equiv y \pmod{n} \Leftrightarrow$ il resto delle divisioni di x e di y per n è lo stesso.

Dimostrazione \Rightarrow (se $x \equiv_n y$ hanno lo stesso resto $x - y = nh$ (per qualche h)

$$x = nh + y$$

Dividendo y per n : $\exists! q, r \in \mathbb{Z} : y = nq + r, 0 \leq r < n$.

Scambiando in x : $x = nh + nq + r = n(h + q) + r$, x ed y hanno quindi lo stesso resto.

4.5 Osservazione

Sia $x = nq + r$, $0 \leq r < n$ la divisione con resto di x per n .
Allora

$$[x]_n = [r]_n \Leftrightarrow x \equiv r \pmod{n} \Leftrightarrow x - r = nq$$

Quindi

$$n \mid x - r$$

4.6 Proposizione somma

La somma classi resto in \mathbb{Z}_n , definita da: $\overline{x} + \overline{y} := \overline{x + y}$, è ben posta, ovvero non dipende dalla scelta dei rappresentanti.

Dimostrazione Siano $x' \in \overline{x}$, cioè $\overline{x'} = \overline{x}$ e $y' \in \overline{y}$ cioè $\overline{y'} = \overline{y}$, allora

$$x' \equiv x \pmod{n} \Leftrightarrow x' = x + kn$$

$$y' \equiv y \pmod{n} \Leftrightarrow y' = y + hn$$

Da verificare: $\overline{x' + y'} = \overline{x + y} \Leftrightarrow x' + y' = x + y + tn$

Quindi:

$$\begin{aligned} x' + y' &= x + kn + y + hn \\ &= x + y + kn + hn \\ &= x + y + (k + h)n \quad [(k + h) = t] \end{aligned}$$

4.7 Dimostrazione prodotto

$$\begin{aligned} x' \cdot y' &= (x + kn)(y + hn) \\ &= xy + xhn + kny + khn^2 \\ &= xy + n(xh + ky + khn), \quad [(xh + ky + khn) = t] \end{aligned}$$

4.8 Proposizione

$a \in \mathbb{Z}$, \overline{a} invertibile in $\mathbb{Z}_n \Leftrightarrow MCD(a, n) = 1$

Dim \Rightarrow

Ipotesi: $\overline{a} \in \mathbb{Z}$ invertibile

Tesi: $(a, n) = 1$

Esiste $b \in \mathbb{Z} : \overline{a} \cdot \overline{b} = 1$

$$\Leftrightarrow ab \equiv 1 \pmod{n}$$

$$\Leftrightarrow n \mid 1 - ab$$

$$\Leftrightarrow 1 - ab = nk$$

$$\Leftrightarrow 1 = ab + nk$$

$$\Rightarrow MCD(a, n) = 1$$

Dim \Leftarrow

Ipotesi: $MCD(a, n) = 1$

Tesi: \bar{a} è invertibile

Se $MCD(a, n) = 1$ allora esistono $h, k \in \mathbb{Z}$:

$$1 = ah + nk \in \mathbb{Z}$$

$$\bar{1} = \overline{ah + nk}$$

$$\bar{1} = \bar{a}\bar{h} + \bar{n}\bar{k} \in \mathbb{Z}$$

$$\bar{n}\bar{k} = \bar{0}\bar{k}$$

$$\bar{1} = \bar{a}\bar{h} \Rightarrow \bar{h} = (\bar{a})^{-1}$$

4.9 Classi resto invertibili

$$\cup(\mathbb{Z}_n) := \{a \in \mathbb{Z}_n : \bar{a} \text{ invertibile}\} \subseteq \mathbb{Z}_n$$

$$\cup(\mathbb{Z}_n) = \{\bar{a} : MCD(a, n) = 1\}$$

4.10 Teorema Uguaglianza sbagliata

Se p è primo allora $\forall x, y \in \mathbb{Z}$ vale:

$$(x + y)^p \equiv x^p + y^p \pmod{p}$$

$$(\bar{x} + \bar{y})^p = \bar{x}^p + \bar{y}^p \pmod{p}$$

Dimostrazione: $(x + y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i}$

$$\binom{p}{0} = 1 = \binom{p}{p}$$

$$\binom{p}{0} x^0 y^p = 1 y^p$$

$$\binom{p}{p} x^p y^0 = 1 x^p$$

Considerare con $0 < i < p$ il coefficiente binomiale è:

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i(i-1)\dots 2 \cdot 1} \in \mathbb{N}$$

$$p \left(\frac{(p-1)\dots(p-i+1)}{i!} \right) \Rightarrow p \mid \binom{p}{i} \forall i = 2, \dots, p-1$$

$$\Rightarrow \binom{p}{i} \equiv 0 \pmod{p}$$

4.10.1 Grande teorema di Fermat

$x^n + y^n = z^n, n \geq 3$ non ha soluzioni intere.

4.10.2 Piccolo teorema di Fermat

$\forall a \in \mathbb{Z}, \forall p(\text{mod})$ primo si ha che: $a^p \equiv a(\text{mod } p)$ in \mathbb{Z}_p , p primo vale $\bar{a}^p = \bar{a}$.

Dimostrazione per $a \in \mathbb{N}$

Per induzione su a

Base:

$$\begin{aligned} a &= 0 \\ 0^p &\stackrel{?}{\equiv} 0(\text{mod } p) \\ 0^p = 0 \in \mathbb{Z} &\Rightarrow 0^p \equiv (\text{mod } p) \end{aligned}$$

Ipotesi induttiva: supponiamo vera per a l'affermazione $a^p \equiv a(\text{mod } p)$

Passo induttivo: verifichiamo per $(a+1)$.

$$(a+1)^p \equiv a^p + 1^p \equiv a + 1$$

$a^p \rightarrow a$ e $1^p \rightarrow 1$ per ipotesi induttiva.

Se $a < 0$ è ancora vero?

Se $a < 0$ allora $-a > 0$, cioè $(-a)^p \equiv -a(\text{mod } p)$. Ora:

$$\begin{aligned} 0 &= a - a \\ 0^p &= (a - a)^p \\ 0^p &\equiv (a - a)^p \equiv a^p + (-a)^p \\ &\equiv a^p - a \equiv 0 \cdot (\text{mod } p) \Leftrightarrow a^p \equiv a(\text{mod } p) \end{aligned}$$

4.11 Teorema Eulero-Fermat

Se $(a, p) = 1$ cioè se $\bar{a} \neq \bar{0}$ in \mathbb{Z}_p allora

$$a^{p-1} \equiv 1(\text{mod } p)$$

Dimostrazione: se $(a, p) = 1$ allora esiste l'inverso moltiplicativo di \bar{a} in \mathbb{Z}_p .

So che

$$\begin{aligned} a^p &\equiv a(\text{mod } p) \\ (\bar{a}^p) &\equiv \bar{a}(\text{mod } p) \\ \Rightarrow \text{moltiplicando per l'inverso} &\Rightarrow \bar{a}^{p-1} = \bar{1} \text{ in } \mathbb{Z}_p \\ \Leftrightarrow a^{p-1} &\equiv 1(\text{mod } p) \end{aligned}$$

4.12 Corollario

Se $(a, p) = 1$ e se p primo allora \bar{a}^{p-2} è l'inverso moltiplicativo di \bar{a} in \mathbb{Z}_p

Dimostrazione: l'inverso di \bar{a} è \bar{x} con $\bar{a} \cdot \bar{x} = \bar{2}$, ma

$$\bar{a} \cdot \bar{a}^{p-2} = \bar{a}^{p-1} = \bar{1}$$

per il *teorema di Eulero-Fermat*.

5 Strutture algebriche

5.1 Gruppo

Un insieme S non vuoto, munito di una operazione

$$m : S \times S \rightarrow S$$

$$(a, b) \mapsto m(a, b) = a * b \text{ (notazione infissa)}$$

che verifica i punti 1, 3, 4 si chiama *gruppo* $(S, *)$.

L'operazione su S è dunque:

- associativa
- con elemento neutro e : $\forall x, x * e = e * x = x$
- per ogni elemento x esiste un inverso rispetto al prodotto $*$ cioè un elemento y tale che $x * y = y * x = e$, che si denota x^{-1}

5.2 Gruppo commutativo (abeliano)

Se il gruppo $(S, *)$ soddisfa anche la proprietà 2 (quindi associatività, elemento neutro, opposto, +commutatività).

5.3 Anello

Un anello è una terna $(A, +, \cdot)$ con:

- A insieme non vuoto
- $+$ due operazioni binarie, associative
- $(A, +)$ è un gruppo abeliano
- Distributività: $\forall a, b, c \in A, a \cdot (b + c) = a \cdot b + a \cdot c$

5.3.1 Anello commutativo

Se un anello $(A, +, \cdot)$ il prodotto è commutativo, cioè se $\forall a, b \in A, a \cdot b = b \cdot a$.

5.3.2 Anello unitario

Se esiste un elemento di A , che si denota con 1_A , tale che $a \cdot 1_A = 1_A \cdot a = a$.

5.3.3 Divisore dello zero

Un elemento $a \in A, a \neq 0_A$ di un anello si dice divisore dello zero se esiste $b \in A, b \neq 0$ con $a \cdot b = 0_A$.

5.3.4 Dominio di integrità

Se $(A, +, \cdot)$ è privo di divisori dello zero.

5.3.5 Legge di annullamento del prodotto

Se in un dominio di integrità $a \cdot b = 0_A$ allora $a = 0_A$ oppure $b = 0_A$.

5.4 Campo

Un campo è una terna $(K, +, \cdot)$ con K insieme non vuoto e 2 operazioni.

- $(K, +, \cdot)$ anello commutativo unitario
- Detto 0_k l'elemento neutro della somma e denotato con $K^* = K \setminus \{0_k\}$, deve valere che $\forall x \in K^* : x \cdot x^{-1} = 1_k$

Quindi campo \Leftrightarrow anello commutativo unitario con in più $K \setminus \{0_k\} = (K^*, \cdot)$ gruppo.

5.5 Semigrupp

Sia X un insieme non vuoto.

$*$:

$$X * X \rightarrow Z$$

$$(a.b) \mapsto a * b$$

una operazione binaria associativa: $\forall a, b, c \in X : a + (b + c) = (a + b) + c$

Un insieme X , munito di una operazione associativa si chiama **semigrupp**.

5.5.1 Monoide

Se $(X, +)$ è un semigrupp ed inoltre esiste un elemento 1_X tale che $a + 1_X = 1_X + a = a$ (1_X elemento neutro dell'operazione $+$), allora $(X, +)$ si chiama **monoide**.

5.6 Elenco gruppi

- (A^*, \cdot) è un monoide non commutativo.
- $(\mathbb{N}, +)$ (commutativo) monoide (0 el. neutro) ma non è un gruppo.
- $(\mathbb{Z}, +)$ gruppo commutativo (0 el. neutro).
- $(\mathbb{Q}, +)$ gruppo commutativo (0 el. neutro); $\frac{p}{a} \rightarrow \text{opposto} - \frac{p}{a}$.
- (\mathbb{N}^*, \cdot) monoide, non è un gruppo.
- (\mathbb{Z}^*, \cdot) monoide, non è un gruppo.
- (\mathbb{Q}, \cdot) non è un gruppo, 0 non ha inverso.
- (\mathbb{Q}^*, \cdot) gruppo.
- $(\mathbb{R}, +)$ gruppo.
- (\mathbb{R}^*, \cdot) monoide, gruppo.

$(\mathbb{Z}_n, +)$ gruppo finito commutativo; el. neutro $\bar{0}$.
 (\mathbb{Z}_n, \cdot) monoide, semigrupp (non è un gruppo $\bar{0}$ non è invertibile).
 $(\cup(\mathbb{Z}_n), \cdot)$ gruppo, el. neutro $\bar{1} = \{\bar{a} : (a, n) = 1\}$ (el. invertibili).

5.7 Gruppo simmetrico

5.7.1 Permutazione

$f : [n] \rightarrow [n]$ si chiama permutazione di n elementi se f è biiettiva.

5.7.2 S_n

$$\begin{aligned}
 S_n &:= \{\sigma : [n] \rightarrow [n] : \sigma \text{ e' biiettiva}\} \\
 &= \{\sigma : \sigma \text{ e' una biiezione}\}
 \end{aligned}$$

5.7.3 Proposizione

$$|S_n| = n!$$

5.7.4 Proposizione

(S_n, \cdot) l'insieme delle permutazioni di n elementi con il prodotto di composizione funzionale è un gruppo di cardinalità $n!$ non commutativo.

Dimostrazione

- S_n non vuoto, $n \geq 1$
- Esiste un elemento neutro rispetto al prodotto \cdot , la permutazione identica:
 $\sigma \circ id = id \circ \sigma = \sigma$.
- Prodotto associativo $\forall \sigma, \tau, \rho \in S_n$ $(\sigma \circ \tau) \circ \rho(i) = \sigma \circ (\tau \circ \rho)(i) = \sigma(\tau(\rho(i)))$
- $\forall \sigma \in S_n$ esiste un elemento σ^{-1} tale che $\sigma \circ \sigma^{-1} = id$.

5.7.5 3^a notazione: Permutazione come prodotto di cicli disgiunti

S_n : Definire una relazione di equivalenza su $[n]$ associata a $\sigma \in S_n$.

$$x, y \in [n]$$

$$x \equiv_{\sigma} y \Leftrightarrow \exists i : y = \sigma^i(x)$$

Si osservi che $\sigma \in S_n$, allora la potenza i -esima di σ , con $i \in \mathbb{N}$ è la permutazione $\sigma^i = \sigma \circ \dots \circ \sigma$ per i volte.

5.7.6 Orbita

L'orbita di $x \in [n]$ è la classe di equivalenza di x nella relazione \equiv_{σ} .

$$O_{\sigma}(x) = \{y \in [n] \mid \exists i \text{ con } y = \sigma^i(x)\}$$

5.7.7 Proposizione

Se τ_1 e τ_2 hanno cicli disgiunti $\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$

5.7.8 Permutazione ciclica

Chiamo ciclica una permutazione di S_n in cui nella rappresentazione in cicli disgiunti ha al più un solo ciclo di lunghezza > 1

5.7.9 Teorema prodotto di scambi

Ogni permutazione si può scrivere come prodotto di scambi

Dimostrazione 1: Se la permutazione ha un solo ciclo $\sigma = (a_1, a_2, \dots, a_k) =$ un k -ciclo $= (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_3)(a_1, a_2) = (a_1, a_2, a_3, \dots, a_k)$

Dimostrazione 2: Se ho un σ qualunque, allora

$$\sigma = C_1 \cdot C_2 \cdot \dots \cdot C_k$$

dove C_i è un ciclo (nella decomposizione in cicli disgiunti)

$$C_1 = (a_1, \dots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_2)$$

$$C_2 = (b_1, \dots, b_j) = (b_1, b_j)(b_1, b_{j-1}) \dots (b_1, b_2)$$

...

$$\sigma = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_2) (b_1, b_j)(b_1, b_{j-1}) \dots (b_1, b_2)$$

5.7.10 Teorema parità

Il numero di scambi usati in diverse fattorizzazioni di una permutazione ha sempre la stessa parità.

5.7.11 Pari, dispari

Una permutazione è pari se il numero di scambi (in una sua fattorizzazione in scambi) è pari, dispari altrimenti.

5.7.12 Gruppo alterno

Le permutazioni pari si chiamano *gruppo alterno*.

5.7.13 Segno

Data σ in S_n , il segno di σ è $\varepsilon(\sigma) = (-1)^{\text{parità di } (\sigma)}$

5.8 Classi coniugate in S_n

5.8.1 Definizione

Dato G gruppo rispetto ad un'operazione \cdot , un elemento x' si dice coniugato con $x \Leftrightarrow$

$$\exists y \in G \text{ con } : x' = yxy^{-1}$$

In S_n σ, σ' sono coniugate \Leftrightarrow

$$\exists \tau \in S_n : \sigma' = \tau \sigma \tau^{-1}$$

(si dice che σ è coniugato a σ' tramite τ)

5.8.2 Proposizione

Due permutazioni $\sigma, \sigma' \in S_n$ sono coniugate \Leftrightarrow hanno la stessa struttura ciclica.

5.9 Definizione multinsieme

Una partizione λ di un intero n è un multinsieme di naturali ≥ 1 la cui somma da n .

5.10 Gruppi finiti

5.10.1 Proprietà 1

Dato (G, \cdot) gruppo e $x, y \in G$ allora $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ (l'inverso del prodotto è il prodotto degli inversi in ordine inverso).

Dimostrazione: $(xy)^{-1} = ? e_G$ (el. neutro del gruppo).

Ora

$$\begin{aligned} (x \cdot y)^{-1} \cdot (y^{-1} \cdot x^{-1}) &= \\ x \cdot (y \cdot y^{-1}) \cdot x^{-1} &= \\ x \cdot e_G \cdot x^{-1} &= \\ x \cdot x^{-1} &= \\ e_G \end{aligned}$$

5.10.2 Proprietà 2

In un gruppo vale sempre la cancellazione:

$$ax = bx \Leftrightarrow a = b$$

Dimostrazione: $\exists x^{-1}$: Se $ax = bx$ e moltiplico per x^{-1}

$$axx^{-1} = bxx^{-1}$$

$$a \cdot e = b \cdot e$$

$$a = b$$

Conseguenza: Su una riga (qualunque) della tavola moltiplicativa del gruppo ci sono una e una sola volta tutti gli elementi del gruppo.

5.11 Sottogruppi

5.11.1 Definizione

Un sottogruppo S di (G, \cdot) è:

- Un sottoinsieme non vuoto di $S \subseteq G$
- S , con la stessa operazione di G è un gruppo

5.11.2 Criteri di verifica

Per verificare che S sia un sottogruppo di G ;

- Associatività: "gratis" : $S \subseteq G$ e il prodotto in G è associativo.

1. $\forall a, b \in S : a \cdot b \in S$ ovvero $S \times S \rightarrow S$
2. $e_G \in S$
3. $\forall a \in S \subseteq G, a^{-1} \in S$

5.11.3 Notazione

$$(S, \cdot) \leq (G, \cdot)$$

altrimenti

$$S \not\leq G$$

5.11.4 Proposizione

S non vuoto e $S \subseteq (G, \cdot)$ è un sottogruppo di G se e solo se

$$\forall a, b \in S : a \cdot b^{-1} \in S \quad (*)$$

Dimostrazione

Ipotesi: $\forall a, b : a \cdot b^{-1} \in S$

Tesi: valgono 1, 2, 3 dei criteri di verifica.

Dimostrazione 2:

$S \neq \emptyset : \exists a_0 \in S$ applico $(*)$ ad a_0, a_0 :

$$a_0 \cdot a_0^{-1} = e_G \in S$$

è quindi l'elemento neutro.

Dimostrazione 3:

$\forall a \in S : a^{-1} \in S$? Per 2. $e_G \in S, a \in S$, applico (*)

$$e_G \cdot a^{-1} = a^{-1} \in S$$

Dimostrazione 1:

Dati $a, b \in S, a \cdot b \in S$? Per la 3 $b^{-1} \in S$.

Dati a, b^{-1} per (*)

$$a \cdot (b^{-1})^{-1} = a \cdot b \in S$$

5.12 Proposizione: intersezione di sottogruppi

Sia (G, \cdot) un gruppo e $H \leq G, K \leq G$ due sottogruppi. Allora:

$$H \cap K \leq G$$

L'intersezione di sottogruppi di G è un sottogruppo di G

Dimostrazione:

1. $1_G \in H \cap K$?

Poiché H e K sono sottogruppi $1_G \in H, K$ e quindi $1_G \in H \cap K$

2. Siano $x, y \in H \cap K$: verifico che $x \cdot y \in H \cap K$.

$x \in H$ e $x \in K$; $y \in H$ e $y \in K$ allora:

$$xy \in H; xy \in K \Rightarrow xy \in H \cap K$$

3. Se $x \in H \cap K \Rightarrow x^{-1} \in H \cap K$?

La dimostrazione è simile a quella del punto precedente

5.13 Proposizione 1

$$H_1, H_2, \dots, H_t \leq G \Rightarrow H_1 \cap H_2 \cap \dots \cap H_t \leq G$$

5.14 Proposizione 2

Siano $S, T \leq G$:

$$S \cup T \leq G \Leftrightarrow S \cup T = T \vee S \cup T = S$$

6 Sottogruppo generato

6.1 Definizione

Siano G un gruppo e $X \subseteq G$, si definisce sotto gruppo generato di X il più piccolo sottogruppo di G che contenga X

6.2 Notazione

$$\langle X \rangle := \bigcap_{X \subseteq H \leq G} H$$

6.3 Proposizione

Se $X = \{x, x_2, \dots\} \subseteq G \neq 0$ allora:

$$\langle X \rangle = \{t_1, t_2, \dots, t_r : t_i \in X \text{ oppure } t_i^{-1} \in X\}$$

L'insieme che contiene i prodotti finiti di elementi di X oppure i cui inversi sono in X .

Dimostrazione:

1. $\langle X \rangle$ contiene X , $r = 1, t_i \in X$
2. $\langle X \rangle \leq G$
 - contiene 1_G : sia $\bar{x} \in X$ qualunque $\Rightarrow \bar{x} \in \langle X \rangle, \bar{x}^{-1} \in \langle X \rangle$ e $\bar{x} \cdot \bar{x}^{-1} = 1_G \in \langle X \rangle$
 - $\langle X \rangle$ è chiuso rispetto al prodotto di G
 - Se $t_1, t_2, \dots, t_r \in \langle X \rangle$, e t_1

TODO:CONTROLLARE APPUNTI

6.4 $\langle X \rangle$ è il più piccolo sottogruppo che contiene X

Da dimostrare in proprio, lo ha dato come esercizio

6.5 Defizione: ordine (periodo)

Se un elemento di G ha periodo finito, allora si chiama *ordine* (o periodo) di g il più piccolo positivo tale che $g^m = 1_G$

6.6 Definizione: gruppo ciclico

Un gruppo G si dice ciclico se esiste $g_0 \in G$ tale che $G = \langle g_0 \rangle$ (*gruppo che viene generato da un solo elemento*).

6.7 Proposizione

Il sottogruppo generato da un elemento (in un gruppo ciclico) è commutativo.

Dimostrazione:

$$\begin{aligned}\langle g \rangle &= \{g^h : h \in \mathbb{Z}\} \\ x &= g^h, y = g^k \quad h, k \in \mathbb{Z} \\ x \cdot y &= g^h g^k = g^{h+k} = g^k g^h = y \cdot x\end{aligned}$$

6.8 Proposizione

Sia G gruppo:

1. Se $g \in G$ ha periodo infinito ($\nexists h > 0 : g^h = e$) allora $\exists h, k \in \mathbb{Z}, h \neq k, g^h \neq g^k$: il gruppo ciclico generato da $G, \langle g \rangle \cong \mathbb{Z}$.
2. g ha periodo finito.
Se $n = \text{periodo di } g = o(g) = \text{ord}_G(g)$ ovvero $n = \min\{k > 0 : g^k = e\}$ allora $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$ dove queste potenze sono tutte distinte.

Dimostrazione pt.1: Dimostro che se:

$$g^h = g^k \Rightarrow h = k$$

infatti moltiplico per g^{-k} ed ho:

$$g^{h-k} = g^{k-k} \Rightarrow g^{h-k} = g^0 = e$$

ma g è aperiodico

$$\Rightarrow h - k = 0 \Rightarrow h = k$$

Dimostrazione pt.2: so che $\langle g \rangle = \{g^h : h \in \mathbb{Z}\}$ devo dimostrare che ogni elemento g^h sta già in $\{e, g, g^2, \dots, g^{n-1}\}$.

Divido h per n :

$$h = nq + r, \quad 0 \leq r < n$$

$$\Rightarrow g^h = g^{nq+r} = g^{nq} g^r = (g^n)^q g^r = e^q g^r = e g^r = g^r$$

ed r è un numero $0 \leq r < n$ e quindi è una potenza dell'insieme.

6.9 Proposizione: sottogruppi di un gruppo ciclico

0. Sottogruppi di $(\mathbb{Z}, +)$: sono tutti e soli della forma

$$H = m\mathbb{Z} = \{mh : h \in \mathbb{Z} = \langle m \rangle\}, \quad m \in \mathbb{N}$$

Non dimostrato.

1. I sottogruppi di $\langle g \rangle$ con $g \in (G, \cdot)$, g aperiodico, sono tutti e soli della forma:

$$H = \langle g^m \rangle$$

per qualche $m \in \mathbb{Z}$.

Non dimostrato.

2. I sottogruppi di un gruppo ciclico generato da un elemento di ordine n ($g^n = e$, n più piccolo positivo con $g^n = e$) sono anch'essi ciclici e generati da $\langle g^h \rangle$, $h|n$.

6.10 Osservazione

I sottogruppi di un gruppo ciclico finito verificano la seguente condizione:

$$H \leq \langle g \rangle \Rightarrow |H| \mid o(g) = |\langle g \rangle|$$

L'ordine di un sottogruppo $H \leq \langle g \rangle$ divide l'ordine dell'elemento g , che è anche l'ordine del gruppo.

6.11 Proposizione

In S_n , sia $\sigma(C_1)(C_2)\dots(C_k)$ la fattorizzazione di σ come prodotto dei suoi cicli disgiunti. Allora se m_i =lunghezza di C_i

$$\text{ordine}(\sigma) = \text{mcm}(m_1, m_2, \dots, m_k)$$

6.12 Proposizione

$G = C_n = \langle g \rangle$ gruppo ciclico generato da un elemento di ordine $n = \{id, g, g^2, \dots, g^n\}$.
Tutti e soli i generatori di C_n sono le potenze di g con esponente coprimo con n .

Generatori: $g^t, (t, n) = 1$

6.13 Teorema di Lagrange

Se G è un gruppo finito, allora l'ordine di un sottogruppo divide l'ordine del gruppo:

$$H \leq G \Rightarrow |H| \mid |G| = o(H) \mid o(G)$$

Oss: non vale sempre il viceversa.

Se $d \mid o(G) \Rightarrow \exists H \leq G, o(H) = d$

Dimostrazione: Siano $n = o(G)$ e $m = o(H)$, i il numero di calssi laterali destre modulo H .

Ci_d = indice del sottogruppo H nel gruppo G .

$i = |G/\sim_d|$ = numero di classi laterali. Esistono a_1, a_2, \dots, a_i rappresentanti distinti delle classi laterali.

$$\begin{aligned} G &= Ha_1 \dot{\cup} Ha_2 \dot{\cup} \dots \dot{\cup} Ha_i \Rightarrow |G| = o(G) = \\ &= \sum_{j=1}^i |Ha_j| = \sum_{j=1}^i |H| = i \cdot |H| = i \cdot m \end{aligned}$$

cioè ho $n = i \cdot m$. $\text{ord}(G)$ = numero classi laterali destre $\cdot \text{ord}(H)$.

Da questa relazione deduco che:

1. $\text{ord}(H) \mid \text{ord}(G)$
2. $i \mid o(G)$

Oss: ripeto tutto per le classi laterali sinistre $i_s \cdot m = n$.

6.13.1 Corollario 1

Se $|G| = p$ primo, allora gli unici sottogruppi di G sono $H = \{e\}$ oppure $H = G$ (non ci sono sottogruppi intermedi).

6.13.2 Corollario 2

Se $|G| = \text{primo}$, allora G è ciclico (in particolare è abeliano).

Dimostrazione: Se $|G| = p$ primo > 1 .

Sia $x_0 \in G, x_0 \neq e$. Sia $H = \langle x_0 \rangle \neq \{e\}$ ($H = \{e, x_0, x_0^2, \dots\}$), per il *corollario 1*:

$$H = G \Rightarrow G = \langle x_0 \rangle$$

6.14 Definizione: indice di un sottogruppo

L'indice di un sottogruppo H in un gruppo G è:

$$i = i_s = i_d$$

e si denota:

$$i = [G : H]$$

7 Classi laterali di un sottogruppo

7.1 Definizione: congruenza destra modulo

Sia (G, \cdot) un gruppo, sia $H \leq G$ sottogruppo.

Definiamo congruenza destra modulo H la relazione così definita:

$$\forall a, b \in G : a \sim_d b \Leftrightarrow a \cdot b^{-1} \in H$$

7.2 Proposizione

$\sim_d \pmod{H}$ è una relazione di equivalenza.

Dimostrazione:

- (R) $a \sim_d a$?

$$a \cdot a^{-1} = e \in H$$

- (S) $a \sim_d b \Rightarrow b \sim_d a$?

$$ab^{-1} \in H$$

H sottogruppo:

$$(ab^{-1})^{-1} \in H$$

$$\Rightarrow (b^{-1})^{-1} \cdot a^{-1} = b^{-1} \cdot a \Rightarrow b \sim_d a$$

- (T) $a \sim_d b$ e $b \sim_d c \Rightarrow a \sim_d c$?

$$ab^{-1} \in H \text{ e } bc^{-1} \in H$$

$$(ab^{-1})(bc^{-1}) \in H$$

H è chiuso rispetto al prodotto

$$(ab^{-1})(bc^{-1}) = ac^{-1} \Rightarrow a \sim_d c$$

7.3 Insieme quoziente

Dato $a \in G$: $[a]_{\sim_d} = H \cdot a$ dove $Ha = \{ha : h \in H\}$, $H = \{e, h_1, h_2, \dots\}$, $Ha = \{e \cdot a, h_1 \cdot a, \dots\}$.

Dimostrazione: devo provare 1. $Ha \subseteq [a]_{\sim_d}$ e 2. $[a]_{\sim_d} \subseteq Ha$.

1.

$$b \in Ha$$

$$\Leftrightarrow \exists h : b = ha$$

moltiplicando per a^{-1}

$$\Leftrightarrow h = ba^{-1}$$

$$\Leftrightarrow ba^{-1} \in H$$

$$\Leftrightarrow b \sim_d a \Leftrightarrow b \in [a]_{\sim_d}$$

è la stessa di sopra ma partendo dalla fine verso l'inizio.

7.4 Proposizione

Tutte le classi laterali destre hanno la stessa cardinalità.

Dimostrazione: dimostro che $|Ha| = |H| \forall a \in A$ ($|Ha| = [a]_{\sim_d}$, per transitività $|Ha| = |Hb|$).

Sia

$$\varphi : H \rightarrow Ha$$

$$h \rightarrow ha$$

- Surriettiva: ogni elemento di Ha è del tipo ha per qualche $h \in H$.
- Iniettiva: $\varphi(a) = \varphi(h') \Rightarrow ha = h'a \Rightarrow$ per la cancellatività nel gruppo $\Rightarrow h = h'$

7.5 Definizione: congruenza sinistra modulo

$$\forall a, b \in G, \quad a \sim_s b \Leftrightarrow b^{-1}a \in H$$

La classe laterale sinistra : $[a]_{\sim_s} = aH = \{ah : h \in H\}$

8 Omomorfismi

8.1 Isomorfismo

Dati $(G, *)$ e (H, \cdot) due gruppi, un isomorfismo di G in H è

- $\varphi : G \rightarrow H$ una biiezione.
- φ rispetta le operazioni di gruppo, cioè:

$$\forall a, b \in G : \varphi(a * b) = \varphi(a) \cdot \varphi(b), \quad \varphi(a) \text{ e } \varphi(b) \in H$$

Si dice che G è isomorfo ad H e si scrive $G \cong H$.

8.2 Omomorfismo

Se $\varphi : G \rightarrow H$ conserva le operazioni di G e H , φ si chiama omomorfismo, ovvero un omomorfismo è un'applicazione tale che:

$$\forall a, b \in G : \varphi(a * b) = \varphi(a) \cdot \varphi(b)$$

8.3 Epimorfismo

Se φ è suriettiva, φ si chiama epimorfismo.

8.4 Monomorfismo

Se φ è iniettiva, si chiama monomorfismo.

8.5 Isomorfismo 2

Se φ è biunivoca, allora φ si chiama isomorfismo.

8.6 Proposizione

L'isomorfismo tra gruppi è una relazione di equivalenza.

8.7 Kernel/Nucleo

Se l'applicazione φ è un omomorfismo, allora viene definito *nucleo* di $\varphi \subseteq G$

$$Ker(\varphi) : \{x \in G : \varphi(x) = e'\}$$

dove:

e = l'elemento neutro di G

e' = l'elemento neutro di G'

8.8 Proposizione

Dato $\varphi : G \rightarrow G'$ omomorfismo, allora:

1. $\varphi(e) = e'$
2. $\varphi(g^{-1}) = (\varphi(g))^{-1}$
3. $\text{Ker}(\varphi) \leq G$
4. $\text{Im}\varphi \leq G'$

Dimostrazione 1: Per dimostrare che $\varphi(e)$ è l'elemento neutro di e' devo mostrare che $\forall y \in G'$: $\varphi(e) \cdot y = y$; moltiplicando per y^{-1} (la cancellazione in G') si ottiene:

$$\begin{aligned}\varphi(e)\varphi\varphi^{-1} &= \varphi\varphi^{-1} \\ \Rightarrow \varphi(e) &= e'\end{aligned}$$

Dimostrazione 2: lasciata per esercizio

Dimostrazione 3: $\text{Ker}\varphi \leq G$?

- contiene e : è il punto 1: infatti $\varphi(e) = e'$
- è chiuso rispetto al prodotto: siano $a, b \in \text{Ker}\varphi$ e verifichiamo che $a * b \in \text{Ker}\varphi$:

$$\begin{aligned}a \in \text{Ker}\varphi &\Rightarrow \varphi(a) = e' \\ b \in \text{Ker}\varphi &\Rightarrow \varphi(b) = e' \\ a * b : \varphi(a * b) &= \varphi(a)\varphi(b) = e' \cdot e' = e' \\ &\Rightarrow a * b \in \text{Ker}\varphi\end{aligned}$$

- è chiuso rispetto agli inversi: sia $a \in \text{Ker}\varphi$ (cioè $\varphi(a) = e'$) devo provare che $a^{-1} \in \text{Ker}\varphi$:

$$\varphi(a^{-1}) = (\varphi(a))^{-1} = (e')^{-1} = e'$$

quindi $a^{-1} \in \text{Ker}\varphi$

Dimostrazione 4 TODO: Ricontrollare appunti

8.9 Omomorfismo di anelli

Se $(A, +, \cdot)$ è $(A', +, \cdot)$ sono anelli $0_A, 0_{A'}$ i corrispettivi elementi neutri, un omomorfismo di anelli è un'applicazione:

$$\varphi : A \rightarrow A'$$

tale che:

- $\varphi(x_1 + x_2) = \varphi(x_1) + \varphi(x_2) \quad \forall x_1, x_2 \in A$
- $\varphi(x_1 \cdot x_2) = \varphi(x_1) \cdot \varphi(x_2)$

$$\text{Ker}\varphi = \{x \in A : \varphi(x) = 0'_A\} \subseteq A \text{ sottoanello}$$

TODO: *qui c'è un insieme che non ho capito

8.10 Proposizione

$\varphi : (G, *) \rightarrow (G', \cdot)$ omomorfismo di gruppi, allora:

$$\varphi \text{ iniettiva} \Leftrightarrow \text{Ker}\varphi = \{e\}$$

$$\varphi \text{ iniettiva} \Leftrightarrow |\varphi^{-1}(y)| \leq 1 \quad \forall y$$

$$\varphi \text{ iniettiva} + \text{omomorfismo} \Leftrightarrow \varphi^{-1}(e^{-1}) = e$$

Dimostrazione: $\text{Ker} = \text{Ker}\varphi \leq G'$

Consideriamo la congruenza modulo il segno (?) k

$$a \sim_d b \Leftrightarrow ab^{-1} \in K (= \text{Ker}\varphi) \Leftrightarrow \varphi(a * b^{-1}) = e'$$

φ è un morfismo:

$$\Leftrightarrow \varphi(a)\varphi(b^{-1}) = e$$

$$\Leftrightarrow \varphi(a)(\varphi(b))^{-1} = e'$$

moltiplicando per $\varphi(b)$

$$\Leftrightarrow \varphi(a) = \varphi(b)$$

$$\Leftrightarrow \varphi \text{ iniettiva}$$

8.11 Proposizione

$G, G' \quad \varphi : G \rightarrow G'$ omomorfismo, allora:

1. Se G finito, allora l'ordine $\text{Im}\varphi$ divide l'ordine di G (ed anche di G' , se G' è finito).
2. Se G è ciclico, allora $\text{Im}\varphi$ è un sottogruppo ciclico di G'
3. Se $g \in G$ ha periodo finito, allora il periodo di $\varphi(g)$ divide l'ordine di g

9 Polinomi a coefficienti reali in 1 indeterminata

9.1 Descrizione

$$\mathbb{R}[x] := \{p(x) = a_0 + a_1x + a_2x^2 + \dots + a_kx^k : a_i \in \mathbb{R}, i = 0, \dots, k, k \in \mathbb{N}\}$$

9.2 Somma di polinomi

Dati

$$p(x) = a_0 + a_1x + a_2x^2 + \dots + a_kx^k$$

$$q(x) = b_0 + b_1x + b_2x^2 + \dots + b_kx^k$$

con $k \leq h$

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_k + b_k)x^k + b_{k+1}x^{k+1} + \dots + b_hx^h$$

9.3 Rappresentazione come successioni

Con esempio:

$$p(x) = 1 + 3x - 4x^3 \leftrightarrow (1, 3, 0, -4, 0, 0, \dots)$$

9.3.1 Somma di polinomi

$$p(x) = (a_0, a_1, a_2, \dots)$$

$$q(x) = (b_0, b_1, b_2, \dots)$$

$$p(x) + q(x) = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots)$$

a_i, b_i sono i coefficienti di x^i nel polinomio che rappresentano.

9.4 Teorema: $(\mathbb{R}[x], +)$ è un gruppo (commutativo)

Dimostrazione:

- $\mathbb{R}[x]$ è non vuoto
- La somma è associativa

$$(\underline{a} + \underline{b}) + \underline{c} = (\dots(a_n + b_n) + c_n \dots) = (\dots a_n + (b_n + c_n) \dots) = \underline{a} + (\underline{b} + \underline{c})$$

- $0 \in \mathbb{R}$ è l'elemento neutro di $\mathbb{R}[x]$

$$0 = 0 + 0x + 0x^2 + \dots \rightarrow (0, 0, 0, \dots)$$

- Ogni polinomio ha il suo opposto: se

$$p(x) = a_0 + a_1x + \dots + a_kx^k$$

allora l'opposto di $p(x)$ è

$$-p(x) = -a_0 - a_1x - \dots - a_kx^k$$

9.5 Prodotto di polinomi

$$p(x) = a_0 + a_1x + \dots + a_kx^k \leftrightarrow (a_0, a_1, \dots)$$

$$q(x) = b_0 + b_1x + \dots + b_kx^k \leftrightarrow (b_0, b_1, \dots)$$

$$p(x) \cdot q(x) = c_0 + c_1x + \dots + c_r x^r \leftrightarrow (c_0, c_1, \dots)$$

$$\begin{aligned} c_0 + c_1x + \dots + c_r x^r &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \\ &\quad + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + \dots \end{aligned}$$

La successione dei coefficienti di $p(x) \cdot q(x)$ è data da:

$$c_n = \sum_{i=0}^n a_i b_{n-i} = \sum_{i+j=n} a_i b_j$$

9.6 Teorema $(\mathbb{R}, +, \cdot)$ è un anello

$(\mathbb{R}, +, \cdot)$ è un anello commutativo, unitario con unità del prodotto uguale a 1 ed è un dominio di integrità. *non dimostrato*

9.7 Grado del prodotto

Se il grado di $p(x) = k$ ed il grado di $q(x) = h$ il grado del prodotto $p(x)q(x) = k + h$

9.8 Fatti importanti

- in $\mathbb{R}[x]$ si può fare la "divisione col resto":

$$\forall a(x), b(x) \in \mathbb{R}, b(x) \neq 0$$

$$\exists! q(x), r(x) \in \mathbb{R} :$$

1. $a(x) = b(x) \cdot q(x) + r(x)$
2. il grado di $r(x) < \text{grado } b(x)$

- Conseguenza della divisione col resto:

$$MCD(m(x), n(x))$$

$$m(x) = n(x) \cdot q_1(x) + r_1(x)$$

$$n(x) = r_1(x) \cdot q_2(x) + r_2(x)$$

...

Termina quando il resto è un polinomio di grado 0.

10 Spazi Vettoriali

10.1 Definizione spazio vettoriale

Uno spazio vettoriale V su un campo K è

- Un insieme nn vuoto V , in cui sono definite due operazioni, di cui una interna ed una esterna.

Interna: somma $+$:

$$\begin{aligned} V \times V &\rightarrow V \\ (v, w) &\mapsto v + w \end{aligned}$$

Esterna: prodotto \cdot per uno scalare:

$$\begin{aligned} K \times V &\rightarrow V \\ (c, v) &\mapsto c \cdot v \end{aligned}$$

- $(V, +)$ è un gruppo commutativo
- $K \times V \rightarrow V$ e $(c, v) \mapsto c \cdot v$ tale che:

– distributività per vettori:

$$\begin{aligned} \forall c \in K, \forall v, w \in V \\ c(v + w) &= cv + vw \\ (v + w)c &= vc + wc \end{aligned}$$

– associatività per gli scalari:

$$\begin{aligned} \forall c, d \in K, \forall v \in V \\ c(dv) &= (cd)v \end{aligned}$$

- distributività per gli scalari:

$$\begin{aligned} \forall c, d \in K, v \in V \\ (c + d)v &= cv + dv \end{aligned}$$

- $1 \cdot v = v$

10.2 Scalare

E' un elemento del campo.