Appunti di Logica e Algebra 2

Pietro Pizzoccheri

2024

Indice

1 Introduzione

1.1 Insiemi

Un insieme è una collezione di oggetti, detti elementi dell'insieme.

$$\mathbb{N} := \{0, 1, 2, 3, ...\} \quad \text{insieme dei numeri naturali}$$

$$\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\} \quad \text{insieme degli interi}$$

$$\mathbb{Q} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\} \quad \text{insieme dei numeri razionali}$$

$$\mathbb{R} := \text{insieme dei numeri reali}$$

$$\mathbb{C} := \text{insieme dei numeri complessi}$$

1.1.1 Operazioni tra insiemi

$$\subseteq \quad \text{inclusione tra insiemi}$$

$$\subsetneq \quad \text{inclusione propria tra insiemi}$$

$$X \subseteq Y \quad \text{si legge "}X \text{ è sottoinsieme di } Y\text{" o "}X \text{ è incluso in } Y\text{"}$$

Se X è un insieme finito, indico con $|X|$ il numero di elementi di X, detto anche la **cardinalità di** X.

$$\varnothing : \text{Insieme vuoto e } |\varnothing| = 0$$

Siano X e Y due insiemi. L'insieme $X \times Y := \{(x, y) : x \in X, y \in Y\}$ lo chiamiamo **prodotto cartesiano** di X e Y.

Sia $A \in \mathcal{P}(x)$, dove $\mathcal{P}(X) := \{A : A \subseteq X\}$ è detto **Insieme delle parti di** X. L'insieme $A^c := X \setminus A$ è detto **complementare** di A

1.2 Funzioni

Siano X e Y due insiemi. **Una funzione** f **da** X **a** Y è un sottoinsieme $F \subseteq X \times Y$ tale che:

- $(x, y_1) \in F$, $(x, y_2) \in F \implies y_1 = y_2$, $\forall x \in X$, $y_1, y_2 \in Y$.
- $x \in X \implies \exists y \in Y$ tale che $(x, y) \in F$

Una funzione $F \subseteq X \times Y$ la indichiamo con $f : X \to Y$. E scriviamo $f(x) = y$ se $(x, y) \in F$.

Definizione: *La funzione $Id_x : X \to X$ tale che $Id_x(x) = x, \forall x \in X$ la chiamiamo* ***funzione identità su*** *X*

Definizione: *Una funzione $f : X \to Y$ è* ***iniettiva*** *se $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2$*

Definizione: *Una funzione $f : X \to Y$ è **suriettiva** se $Im(f) = Y$, dove $Im(f) = \{y \in Y : \exists x \in X \text{ tale che } f(x) = y\}$ è detta **immagine di** f*

Definizione: *Una funzione $f : X \to Y$ è **biunivoca** se è sia iniettiva che suriettiva.*

1.2.1 Composizione di funzioni

Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni. La **composizione di f e g** è la funzione $g \circ f : X \to Z$ tale che $(g \circ f)(x) = g(f(x))$, $\forall x \in X$.

Definizione: *una funzione $f : X \to Y$ è detta **invertibile** se esiste una funzione $g : Y \to X$ tale che*

- $g \circ f = Id_X$
- $f \circ g = Id_Y$

*la funzione g è detta **funzione inversa di** f e la indichiamo con f^{-1}.*

Una funzione $f : X \to Y$ è invertibile se e solo se è biunivoca.

1.2.2 Operazioni su insiemi

Definizione: *Una funzione $f : X \times X \to X$ è detta **operazione su** X. Invece di $f(x, y)$ scriveremo $x \cdot y$.*

Definizione: *Un'operazione $\cdot$ su X è detta **associativa** se $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\forall x, y, z \in X$.*

Definizione: *Un'operazione $\cdot$ su X è detta **commutativa** se $x \cdot y = y \cdot x$, $\forall x, y \in X$.*

Esempio:

- $\mathcal{P}(X)$con l'operazione di unione $\cup$ è associativa e commutativa, così come lo è con l'intersezione $\cap$.
- $A \backslash B := A \cup B^C$ **(differenza insiemistica)** è un'operazione su $\mathcal{P}(X)$.
  non è associativa: sia $A \neq \varnothing$. Allora $A \backslash (A \backslash A) = A \neq (A \backslash A) \backslash A = \varnothing$
  non è commutativa: $A \backslash \varnothing = A \neq \varnothing \backslash A = \varnothing$, se $A \neq \varnothing$
- $A \Delta B := (A \backslash B) \cup (B \backslash A)$ **(differenza simmetrica)** è un'operazione su $\mathcal{P}(X)$.
  è commutativa e anche associativa, facilmente verificabile coi diagrammi di Venn.
- Sia $F(X) := \{f : X \to X\}$.
  La composizione" $\circ$" è un'operazione su $F(X)$.
  è associativa, ma non è commutativa.
- $a \circ b = \frac{a+b}{2}$ è un'operazione commutativa su $\mathbb{Q}$, ma non associativa.

Definizione: *Sia $\cdot$ un'operazione su X. Un elemento $e \in X$ tale che $e \cdot x = x \cdot e = x$, $\forall x \in X$ è detto **elemento neutro** o **identità**.*

L'identità è unica; se $e, e' \in X$ sono due identità, allora $e = e \cdot e' = e'$.

1.3 Monoidi e Gruppi

Definizione: *Un insieme X con un'operazione associativa e un'identità è detto* ***monoide****.*

Esempio:

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con l'addizione e identità 0 sono monoidi.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con la moltiplicazione e identità 1 sono monoidi.
- $\mathcal{P}(X)$ con $\cup$ e come identità l'insieme X è un monoide.
- $\mathcal{P}(X)$ con $\cap$ e come identità l'insieme vuoto è un monoide.
- $F(X) := \{f : X \to X\}$ con la composizione" $\circ$ "e come identità la funzione identità (Id_X) è un monoide.

Definizione: *Sia Xun monoide. Un elemento $x \in X$ è detto* ***invertibile*** *se esiste $y \in X$ tale che $x \cdot y = y \cdot x = e$, dove e è l'identità di X. L'elemento y è detto* ***inverso*** *di x.*

Se $x \in X$ è invertibile, il suo inverso è unico e lo indichiamo con x^{-1}.
L'identità del monoide è invertibile e il suo inverso è l'identità stessa.

Esempio:

- L'insieme degli elementi invertibili di $(\mathbb{N}, +)$ è $\{0\}$.
- Linsieme degli elementi invertibili di $(\mathbb{Z}, +)$ è $\mathbb{Z}$, di $(\mathbb{Q}, +)$ è $\mathbb{Q}$, di $(\mathbb{R}, +)$ è $\mathbb{R}$, di $(\mathbb{C}, +)$ è $\mathbb{C}$.
- L'insieme degli elementi invertibili di $(\mathbb{N}, \cdot)$ è $\{1\}$, di $(\mathbb{Z}, \cdot)$ è $\{1, -1\}$, di $(\mathbb{Q}, \cdot)$ è $\mathbb{Q} \setminus \{0\}$, di $(\mathbb{R}, \cdot)$ è $\mathbb{R} \setminus \{0\}$, di $(\mathbb{C}, \cdot)$ è $\mathbb{C} \setminus \{0\}$.
- L'insieme degli elementi invertibili di $F(X) = \{f : X \to X\}$ è l'insieme delle funzioni invertibili.

Definizione: *Un monoide X è detto* ***gruppo*** *se ogni suo elemento è invertibile. Se l'operazione è commutativa, il gruppo è detto* ***gruppo abeliano****.*

Esempio:

- $(\mathcal{P}(x), \Delta)$ è un gruppo abeliano. L'identità è l'insieme vuoto e l'inverso di $A \in \mathcal{P}(x)$ è A stesso. $(A^2 = \varnothing, \forall A \subseteq X)$
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sono gruppi abeliani
- $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}\backslash\{0\}, \cdot)$ sono gruppi abeliani
- sia $X = \{1, 2, ..., n\}$ l'insieme delle funzioni invertibili $f : X \to X$ è il **Gruppo delle permutazioni di n elementi (o gruppo simmetrico)**.Lo indichiamo con $S?n$. $|S_n| = m!$. Non è abeliano se $n \geq 3$.

Definizione: *Sia X un monoide con identità e. Un sottoinsieme $Y \subseteq X$ tale che $e \in Y$ e Y è chiuso rispetto all'operazione di X è detto* ***sottomonide di*** *X.Analogamente definiamo la nozione di* ***sottogruppo di*** *X. il gruppo $\{e\}$ è detto* ***sottogruppo banale di*** *X.*

Esempio:

- Con l'addizione, $\{0\}$ èun sottomonoide di $\mathbb{N}$. $\{0\}$ è anche sottogruppo banale.
- Con la moltiplicazione abbiamo la catena di sottomonoidi $\{1\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq insiemeR \subseteq \mathbb{C}$ e di sottogruppi $\{1\} \subseteq \mathbb{Q}\backslash\{0\} \subseteq \mathbb{R}\backslash\{0\} \subseteq \mathbb{C}\backslash\{0\}$
- con l'addizione abbiamo la caten di sottogruppi $\{0\} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Definizione: *Sia X un monoide e $S \subseteq X$ un sottoinsieme. L'insieme $\langle S \rangle := \{x_1 \cdot x_2 \cdot ... \cdot x_n : n \in \mathbb{N}, x_1, x_2, ..., x_n \in S\}$ è detto **sottomonoide generato da** S (intersezione di utti i sottomonoidi di X che contengono S). Se X è un gruppo, $\langle S \rangle$ è detto **sottogruppo generato da** S.*

Esempio:

- $S = \{1\} \subseteq (\mathbb{N}, +)$. Allora $\langle S \rangle = \{0, 1, 2, ...\} = \mathbb{N}$
- sia $S := \{p \in \mathbb{N} : p \text{ è primo}\} \cup \{0\} \subseteq (\mathbb{N}, \cdot)$. allora $\langle S \rangle = \mathbb{N}$
- $S = \{0, 1\} \subseteq (\mathbb{N}, .)$. Allora $\langle S \rangle = \{0, 1\}$
- sia $S = \{1\} \subseteq (\mathbb{Z}, +)$. il sottogruppo generato da S è $\langle S \rangle = \mathbb{Z}$
- uno spazio ettoriale V è un gruppo abeliano se consideriamo l'operazione di addizione fra vettori. Prendiamo $V = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Sia $v = (1, 1) \in \mathbb{R}^2$. Il sottogruppo $\langle \{v\} \rangle = \{(n, n) : n \in \mathbb{Z}\}$ è un sottogruppo proprio del sottospazio generato da $\{v\}$. Sia $v_1 = (1, 0)$ ed $v_2 = (0, 1)$, allora il sottogruppo $\langle \{v_1, v_2\} \rangle$ è $\mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{R} \times \mathbb{R}$

Definizione: *Siano M_1, M_2 con identità e_1, e_2 rispettivamente. Si definisce prodotto diretto di M_1 e M_2 l'insieme $M_1 \times M_2$ con l'operazione $(m_1, m_2) \cdot (m_1', m_2') = (m_1 \cdot m_1', m_2 \cdot m_2')$ e identità (e_1, e_2). Analogamente si definisce prodotto diretto di gruppi $G_1 e G_2$.*

L'inverso di una coppia $(a, b) \in G_1 \times G_2$ è (a^{-1}, b^{-1}).

1.4 Morfismi

Definizione: *Siano $M_1 e M_2$ monoidi con identità $e_1 e e_2$. Una funzione $f : M_1 \to M_2$ è un **morfismo di monoidi se:***

- $f(e_1) = e_2$
- $f(xy) = f(x)f(y)$

Definizione: *Siano $G_1 e G_2$ gruppi con identità $e_1 e e_2$. Una funzione $f : G_1 \to G_2$ è un **morfismo di gruppi se:***

- $f(e_1) = e_2$
- $f(xy) = f(x)f(y)$

Definizione: *Il **nucleo** di un morfismo di monoidi $f : M_1 \to M_2$ è il sottomonoide di M_1 definito come: $Ker(f) := \{x \in M_1 : f(x) = e_2\}$*

Definizione: *Il nucleo di un morfismo di gruppi $f : G_1 \to G_2$ è il sottogruppo di G_1 definito come: $Ker(f) := \{x \in G_1 : f(x) = e_2\}$.* ***Il nucleo è un sottogruppo di*** *G_1. e $Im(f)$* ***è un sottogruppo di*** *G_2.*

Definizione: *Un* ***isomorfismo di monoidi (e di gruppi)*** *èun morfismo biunivoco, tale che la funzione inversa sia un morfismo.*

Proposizione: *Sia $f : M_1 \to M_2$ un morfismo di monoidi. Se f è biunivoco, allora è un isomorfismo. Questo vale anche per i gruppi.*

Dimostrazione: *Dobbiamo far vedere che la funzione inversa $f^{-1} : M_2 \to M_2$ è un morfismo di monoidi. Poiché $f(e_1) = e_2$, allora $f^{-1}(e_2) = e_2$. Siano $x_2, y_2 \in M_2$, allora esistono $x_1, y_1 \in M_1$ tali che $f(x_1) = x_2, f(y_1) = y_2$. Quindi $f^{-1}(f(x_1)f(y_1)) = f^{-1}(f(x_1y_1)) = x_1y_1 = f^{-1}(x_2)f^{-1}(y_2)$*

Esempio:

- Siano $M_1 = (\mathcal{P}(X), \cup)$ e $M_2 = (\mathcal{P}(X), \cup)$, dove X è un insieme. Sia $f : M_1 \to M_2$ definita ponendo $f(A) = A^C, \forall A \subseteq X$. la funzione f è biunivoca. Inlotre, dalle formule di De Morgan segue che $f(A \cap B) = (A \cap B)^C = A^C \cup B^C = f(A) \cup f(B)$. Quindi f è un isomorfismo di monoidi, poiché $f(X) = X^C = \varnothing$, essendo X l'identità di M_1 e $\varnothing$ l'identità di M_2.

- Sia $\mathbb{Z}_2 := \{0, 1\}$ con l'operazione definita come: $0+0 = 0, 0+1 = 1+0 = 1, 1+1 = 0$. Sia $X := \{1, 2, ..., n\}, n \in \mathbb{N}$. La funzione $f : \mathcal{P}(X) \to \mathbb{Z}_2 \times ... \times \mathbb{Z}_2$ (n volte) definita da: $f(A) = (a_1, a_2, ..., a_n)$, dove $a_i = 1$ se $i \in A$ e $a_i = 0$ se $i \notin A$.
  è un isomorfismo del gruppo $(\mathcal{P}(X), \Delta)$ con il gruppo $\mathcal{P}(X) \to \mathbb{Z}_2 \times ... \times \mathbb{Z}_2 = (\mathbb{Z}_2)^n$

Vediamo ora come ogni monoide finito è isomorfo a un monoide di matrici quadrate, dove l'operazione è il prodotto righe per colonne.
Sia $M = \{x_1, ..., x_n\}$ un monoide, $|M| = n \in \mathbb{N}$, con identità $e = x_1$. Pero ogni $x \in M$ definiamo una matrice $A(x) \in Mat_{n\times n}(\mathbb{Z})$ nel seguente modo: $A(x)_{ij} = 1$ se $x_i \cdot x = x_j$ e $A(x)_{ij} = 0$ altrimenti. La funzione $F : M \to Mat_{n\times n}(\mathbb{Z})$ $(x \mapsto A(x))$ è iniettiva.
Infatti, se $A(x) = a(y)$, allora $A(x)_{i1} = A(y)_{i1}$, $\forall i \in \{1, ..., n\}$.
Quindi se $A(x)_{i1} = A(y)_{i1} = 1$, allora $xx_1 = xe = x = yx_1 = y$.
Risulta inoltre facile vedere che $A(xy) = A(x)A(y)$ (prodotto righe per colonne), ossia che F è un morfismo di monoidi ($Mat_{n\times n}(\mathbb{Z})$ è un monoide con l'operazione di prodotto righe per colonne, la cui identità è la matrice I_n).
Quindi $F : M \to Im(F)$ è un isomorfismo di monoidi.

Esempio: Sia $M = (\mathbb{Z}_2, \cdot)$ il monoide definito da:

$\cdot$	0	1
0	0	0
1	0	1

costruiamo un sottomonoide di $Mat_{4\times4}(\mathbb{Z})$ isomorfo a $M\times M = \{(0,0),(0,1),(1,0),(1,1)\}$.

$$(0,0) \mapsto \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, (0,1) \mapsto \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, (1,0) \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, (1,1) \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

$\cdot$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$
$(1,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$
$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$

Si può verificare direttamnete che le matrici hanno la stessa tabella moltiplicativa. (fine esempio)

Abbiamo quindi visto che un monoide finito di cardinalità n è isomorfo a un monoide di matrici $n \times n$ le cui colonne hanno un unico "1" e altrove sono "0".
Ognuna di queste matrici può essere vista come una funzione da $X = \{1, ..., n\} in X$:

$$A_{ij} = 1 \Leftrightarrow f(j) = i$$

$$A_{ij} = 0 \Leftrightarrow f(j) \neq i$$

Il prodotto righe per colonne corrisponde alla composizione di funzioni.
Quindi un monoide finito di cardinalità n è isomorfo a un sottomonide del monoide delle funzioni f da $\{1, ..., n\}$ in $\{1, ..., n\}$ con l'operazione di composizione.

Notiamo che un elemento $x \in M$ di un monoide finito M è invertibile se e solo se la matrice associata è invertibile (una matrice $A \in Mat_{n\times n}(\mathbb{Z})$ è invertibile se e solo se il suo determinante è invertibile su $\mathbb{Z}$, ossia se e solo se $det(a) \in \{-1, 1\}$).

Da ciò segue che un gruppo finito G di cardinalità $|G| = n$, è isomorfo a un gruppo di matrici le cui componenti sono"0" e "1" e che hanno un unico "1" in ogni riga e ogni colonna (matrici di permutazioni).
Il gruppo G è inoltre isomorfo a un sottogruppo del gruppo delle funzioni biunivoche da $\{1, ..., n\}$ in $\{1, ..., n\}$, che abbiamo chiamato **gruppo simmetrico** S_n.
Gli elementi di S_n in notazione a una linea sono indicati nel modo seguente: sia $\sigma \in S_n$ una funzione biunivoca da $\{1, ..., n\}$ in $\{1, ..., n\}$, allora σ è indicata come $\sigma(1)\sigma(2)...\sigma(n)$.

Teorema (Teorema di Cayley)**:** *Ogni sottogruppo finito di cardinalità $n \in \mathbb{N}\backslash\{0\}$ è isomorfo a un sottogruppo di S_n*

Esempio:

- $S_2 = \{12, 21\}$
  $S_3 = \{123, 132, 213, 231, 312, 321\}$

- vediamo il gruppo $(\mathbb{Z}_2, +)$ come gruppo di matrici e come gruppo di permutazioni.
  $(\mathbb{Z}_2, +) \simeq \{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\} \simeq \{12, 21\} = S_2$ $(\simeq isomorfismodigruppi)$

1.5 Relazioni

Definizione: *Sia X un insieme. Un sottoinsieme $R \subseteq X \times X$ è detto* ***relazione su*** X.

Definizione: *Una relazione $R \subseteq X \times X$ è detta* ***relazione di equivalenza*** *se soddisfa le seguenti proprietà:*

- ***riflessità***: $(x, x) \in R$, $\forall x \in X$
- ***simmetria***: $(x, y) \in R \implies (y, x) \in R$, $\forall x, y \in X$
- ***transitività***: $(x, y) \in R$ e $(y, z) \in R \implies (x, z) \in R$, $\forall x, y, z \in X$

Se R è una relazione di equivalenza su X e $(x, y) \in R$, scriviamo $x \sim y$, che si legge "x è equivalente a y".

Definizione: *Sia X un insieme e $R \subseteq X \times X$ una relazione di equivalenza su X. L'insieme $[x]_R := \{y \in X : x \sim y\}$ è detto* ***classe di equivalenza di*** x ***rispetto a*** R.

Definizione: *L'insieme ${}^{X}/_{\sim} := \{[x] : x \in X\}$ è detto* ***insieme quoziente***.

Definizione: *La funzione $\pi : X \to {}^{X}/_{\sim}$, $x \mapsto [x]$ è detta* ***proiezione canonica***.

Definizione: *Siano $x, y \in X$. Allora se $x \sim y$ abbiamo che $[x] = [y]$. Se $x \nsim y$ abbiamo che $[x] \cap [y] = \varnothing$. Quindi $X = \biguplus_{[x] \in X/\sim} [x]$, ossia ${}^{X}/_{\sim}$ è una partizione di X.*

Esempio:

- L'uguaglianza " = " è una relazione di equivalenza su ogni insieme X.
- Sia $X = \{1, 2, ..., n\}$. Definiamo si $\mathcal{P}(X)$ la seguente relazione: $A \sim B \Leftrightarrow |A| = |B|, \forall A, B \subseteq X$. Questa è una relazione di equivalenza e ${}^{\mathcal{P}(X)}/_{\sim} \equiv \{0, 1, ..., n\}$. Se $A \subseteq X$ è tale che $|A| = k \leq n$ allora $|[A]| = \binom{n}{k} := \frac{n!}{k!(n-k)!}$
- Sia G un gruppo e $H \subseteq G$ un sottogruppo. La relazione $\sim$ su G definita da $g_1 \sim g_2 \Leftrightarrow g_1 = g_2 h$ per qualche $h \in H$ è una relazione di equivalenza.
  - $g \sim g : g \cdot e$, $\forall g \in G, e \in H$
  - $g_1 \sim g_2 \to g_2 \sim g_1 : g_1 = g_2 h \to g_1 h^{-1} = g_2$ $(h^{-1} \in H)$
  - $g_1 \sim g_2, g_2 \sim g_3 \to g_1 \sim g_3 : g_1 = g_2 h, g_2 = g_3 h' \to g_1 = g_3 h h' = g_3 h'', \forall g_1, g_2, g_3 \in G$

  In questo caso l'insieme quoziente lo indichiamo con ${}^{G}/_{H}$.

Definizione: *Il numero $\binom{n}{k}$ è chiamato* ***coefficiente binomiale***, *questo perché $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^n y^{n-k}, \forall x, y \in \mathbb{C}$*

1.5.1 Insieme quoziente per gruppi abeliani

Se G è un gruppo abeliano, possiamo definire la seguente operazione "+" su G/H: $[g_1] + [g_2] := [g_1 + g_2]$, vediamo che è ben definita: se $g_1' = g_1 + h_1$ e $g_2' = g_2 + h_2$, allora $[g_1'] = [g_1]$, $[g_2'] = [g_2]$ e $g_1' + g_2' = g_1 + h_1 + g_2 + h_2 = g_1 + g_2 + h$, dove $h = h_1 + h_2 \in H$. Quindi $[g_1' + g_2'] = [g_1 + g_2]$. L'operazione è ovviamente associativa e commutativa, perché lo è quella su G. Inoltre $[g] + [0] = [g]$, $\forall [g] \in G/H$ dove con "0" abbiamo indicato l'identità di G. Quindi la classe $[0]$ dell'identità di $(G/H, +)$. Infine $[g] + [-g] = [g - g] = [0]$, dove con $-g$ abbiamo indicato l'inverso di g in G. Quindi $-[g] = [-g], \forall [g] \in G/H$, ossia $(G/H, +)$ è un gruppo abeliano.

Esempio: