Lezione 01 - 29/09/2022

Operazione binaria

Un'operazione binaria $*$ su un insieme S è un'applicazione:

$$
\begin{gathered}
*: S \times S \to S \\
(a, b) \mapsto a * b
\end{gathered}
$$

Monoide

Un insieme S dotato di **un'operazione binaria** in cui valgono le proprietà di **associatività** e **esistenza dell'elemento neutro** si dice **MONOIDE**.

- **Proprietà associativa**

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

- **Esistenza elemento neutro**

$$\exists e \in S : e * a = a * e = a\ \forall a \in S$$

Es.:

- $(\mathbb{N}, +)$, con elemento neutro $e = 0$
- $(\mathbb{N}, \cdot)$, con elemento neutro $e = 1$

Più in generale ogni insieme X nella lista

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

rispetto a $+$ o rispetto a $\cdot$ è un monoide.

Lemma - L'elemento neutro è unico

In un monoide S l'elemento neutro è unico

Dimostrazione: Siano e_1, e_2 due elementi neutri

$$e * a \overset{(1)}{=} a * e \overset{(2)}{=} a$$
$$e_1 \overset{(1)}{=} e_1 * e_2 \overset{(2)}{=} e_2$$

Dove, nella seconda equazione:

- Nel primo passaggio vengono posti: $a = e_1$ e $e = e_2$
- Nel secondo passaggio vengono posti: $a = e_2$ e $e = e_1$

Monoide commutativo

Un monoide si dice **commutativo** se

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

Es.:

X insieme, $F_X = \{f : X \to X\}$ e $f * g = f \circ g$ si ha che

$$(f \circ g) = f(g(x))$$

F_X è un **monoide** perché la composizione di funzioni è associativa. L'elemento neutro è:

$$\mathrm{Id}_x(x) = x, \forall x \in X$$

Infatti:

$$f \circ \mathrm{Id}_x = \mathrm{Id}_x \circ f = f$$

Es.:

$$(f \circ \mathrm{Id}_x)(x) = f(\mathrm{Id}_x(x)) = f(x)$$
$$(\mathrm{Id}_x \circ f)(x) = \mathrm{Id}_x(f(x)) = f(x)$$

Gruppo e gruppo abeliano

Un **monoide** $(G, *)$ si dice **GRUPPO** se

$$\forall g \in G \; \exists g' \in G : g * g' = g' * g = e$$

Ovvero g' è l'**elemento inverso** di g.

Se G è **commutativo**, diciamo anche che è un **GRUPPO ABELIANO**.
Es.:

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$

Esempio: Sia $F_x \supset S_x = \{f : X \to X, \text{ f biiettiva}\}$

Biiettiva siginifica che: $\exists g : X \to X \text{ t.c. } f \circ g = g \circ f = \text{Id}_X$

$$f^{-1}(B) = \{x \in X | f(x) = B\}$$

Prendiamo:

- f biunivoca
- $B = \{y\}$

Si ha che $f^{-1}(y)$ ha un solo elemento.

Notazione - gruppo simmetrico

S_n è un gruppo simmetrico su $X = \{1, 2, ..., n\}$, dove X indica le permutazioni su $\{1, 2, ..., n\}$

Lemma - Inverso unico

In un gruppo G l'inverso di ogni elemento è unico

Dimostrazione: supponiamo che g_1, g_2 siano entrambi inversi di g, per ipotesi

$$g * g_1 = g_1 * g = e$$
$$g * g_2 = g_2 * g = e$$

Si avrà la seguente cosa:

$$g_1 = g_2 * e = g_1 * (g * g_2) \overset{assoc.}{=} (g_1 * g) * g_2 = e * g_2 = g_2$$

Anello, anello commutativo con unità e campo

Un anello con unità R è un insieme dotato di due operazioni binarie $+$ e $\cdot$ tali che:

1. $(R, +)$ è un **gruppo abeliano**,
2. $(R, \cdot)$ è un **monoide**

Valgono le proprietà distributive:

$$(a+b)c = ac + bc, \forall a, b, c \in R$$
$$a(b+c) = ab + ac, \forall a, b, c \in R$$

Se $(R, \cdot)$ è un **monoide commutativo**, diciamo che R è un **anello commutativo con unità**.
Es.:

- $(\mathbb{Z}, +, \cdot)$

Se $(R \setminus \{0\}, \cdot)$ è un **gruppo abeliano**, diciamo che R è un **campo**.
Es.:

- $(\mathbb{Q}, +, \cdot)$
- $(\mathbb{R}, +, \cdot)$

In un anello $0 \cdot a = 0, \forall a \in R$, infatti:

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

Lezione 02 - 30/09/2022

Relazione

Sia X insieme, $X \times X = \{(a,b)|a,b \in X\}$

Esempio:

$$X = \{1,2\}$$
$$X \times X = \{(1,1),(1,2),(2,1),(2,2)\}$$

Definizione

Una relazione su X è un sottoinsieme R di $X \times X$. Diremo che $x \in X$ è in relazione con $g \in X$ se $(x,g) \in R$

Esempio:

$$X = \{1,2,3\}$$
$$R = \{(1,2),(1,3),(3,3)\}$$

- 1 è in relazione con 2
- 2 non è in relazione con 1

Notazione

Se R è una relazione e x è in relazione con y, scriveremo $x \sim y$.

Definizione - Relazione di equivalenza

Una relazione R su X si dice di **equivalenza** se valgono le 3 seguenti proprietà:

1. **Riflessiva**: $x \sim x, \forall x \in X$
2. **Simmetrica**: $x \sim y \Rightarrow y \sim x$
3. **Transitiva**: $x \sim y, y \sim z \Rightarrow x \sim z$

Esempi:

- R è la relazione di eguaglianza
- X = rette nel piano, R = relazione di parallelismo
- Congruenza modulo n, $n \in \mathbb{N}$

Osservazione

$\mathbb{Z}$ non è una campo in quanto non si può fare la divisione, ma si può comunque fare la divisione con resto. Verrà dimostrato che dati

$$a, b \in \mathbb{Z}, b \neq 0 \; \exists! q, r \in \mathbb{Z} \text{ t.c.}$$
$$a = bq + r, \; 0 \leq r < |b|$$

Esempio: $17 = 4 * 4 + 1$

Fissato n, si pone

$$a \equiv_n b$$
$$\text{oppure}$$
$$a \equiv b \mod n$$

se a, b hanno lo stesso resto nella divisione per n. Quindi $a \equiv_n b$ se

$$a = q_1 n + r$$
$$b = q_2 n + r$$

e varrà la seguente regola

$$b - a = q_2 n + r - (q_1 n + r) = (q_2 - q_1)n$$

ovvero che $b - a$ è un multiplo di n, quindi

$$b \equiv_n a \Leftrightarrow \text{b-a è multiplo di n}$$

Verifichiamo che $\equiv_n$ è una **relazione di equivalenza**

- **Riflessiva**: $a \equiv_n a,\ a - a = 0 = 0 \cdot n$ ✓
- **Simmetrica**: $a \equiv_n b \Rightarrow b \equiv_n a$
  - Ipotesi: $b - a = kn$
  - Tesi: $\exists h : a - b = hn$, cioè $a - b = (-k)n$, quindi $h = -k$ ✓
- **Transitiva**: $a \equiv_n b, b \equiv_n c \Rightarrow a \equiv_n c$
  - Ipotesi:
    1. $b - a = hn$
    2. $c - b = kn$
  - Tesi: $\exists s : c - a = sn$. Sommando 1. con 2. si ottiene

$$c - a = c - b + b - a = hn + kn = (h + k)n \checkmark$$

Classi di equivalenza

Se R è un'equivalenza su X, poniamo per $x \in X$

$$[x] = \{y \in X | y \sim x\}$$

e la chiamiamo **classe di equivalenza di x.**

Osservazione

$$x \sim y \Leftrightarrow [x] = [y]$$

Dimostrazione:

- $\Rightarrow$

  Supponiamo $x \sim y$ e facciamo vedere che $[x] = [y]$, ovvero $[x] \subseteq [y]$ e $[y] \subseteq [x]$.

  1. $z \in [x]$

$$z \sim x, \overbrace{x \sim y}^{\text{ipotesi}} \overset{\text{TRA.}}{\Rightarrow} z \sim y \Rightarrow z \in [y]$$

  2. $t \in [y]$

$$t \sim y, \overbrace{x \sim y}^{\text{ipotesi}} \overset{SIM.}{\Rightarrow} y \sim x \overset{TRA.}{\Rightarrow} t \sim x \Rightarrow t \in [x]$$

- $\Leftarrow$

  Supponiamo $[x] = [y]$, allora $x \in [y]$, quindi $x \sim y$.

Costruzione dell'insieme quoziente

Siano X inseme e $\sim$ relazione di equivalenza

$$X/ \sim = \{[x] | x \in X\}$$

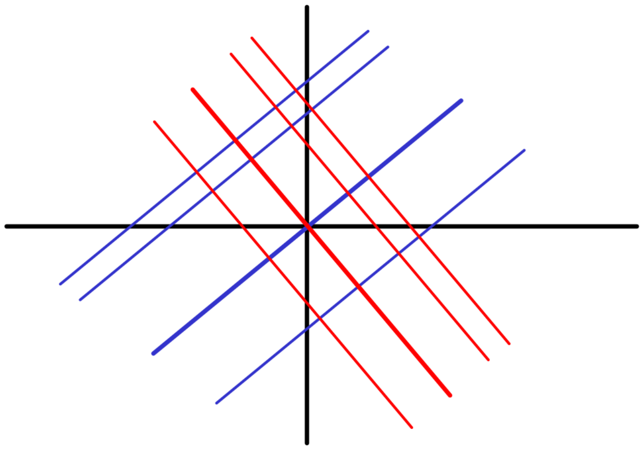
e si chiama **insieme quoziente di x modulo $\sim$.**

Esempi:

- $[x] = [y] \Leftrightarrow x = y$

  $X/_= = X$

- $X/_\sim = \text{direzioni nel piano} \leftrightarrow \text{rette che passano per l'origine}$



  Vengono scelte come rappresentanti solo quelle che passano per l'origine.

- $a \equiv_n b \Leftrightarrow a, b \text{ hanno lo stesso resto nella divisione per } n \leftrightarrow$
  $\text{un insieme di rappresentanti è dato dai resti della divisione per } n$

$$\mathbb{Z}/ \equiv_n = \{[0], [1], ..., [n-1]\}$$

  Esempi:

- $\mathbb{Z}/\equiv_2 = \{[0],[1]\}$ che stanno ad indicare rispettivamente i **numeri pari** e i **numeri dispari**.
- $\mathbb{Z}/\equiv_3 = \{[0],[1],[2]\}$

> Di solito si scrive $\mathbb{Z}_n$ per indicare $\mathbb{Z}/\equiv_n$.

Definizione di anello su Zn

Si vuole definire una struttura di anello su $\mathbb{Z}_n$:

- $+ \ \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

  $([a],[b]) \mapsto [a+b]$
- $\cdot \ \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

  $([a],[b]) \mapsto [ab]$

Esempio: $n = 4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$
$[2]$	$[2]$	$[0]$	$[2]$
$[3]$	$[3]$	$[2]$	$[1]$

> ⚠️ Negli anelli si toglie lo 0 per l'operazione $\cdot$

> ⚠️ 2 non ha inversi quindi non è un campo. In quanto non ha inversi si dice che 2 è un **divisore dello 0**.

Spiegazione: a differenza di 2, tutti gli altri hanno inverso:

- $[1] \cdot [1] = [1]$
- $[3] \cdot [3] = [1]$

Mentre per $[2]$ non c'è nessuna classe $[b]$ tale che $[2] \cdot [b] = [1]$.

Problema teorico

Quando si definisce una funzione su un insieme quoziente, bisogna assicurarsi che la definizione sia **ben posta**, ovvero non dipenda dal **rappresentante scelto**.

Esempio: $\mathbb{Z}_{21}$

$$[18] + [8] = [26] = [5]$$

Ma in $\mathbb{Z}_{21}$ si ha anche $[18] = [-3]$ e $[8] = [50]$, quindi analogamente

$$[-3] + [50] = [47] = [5]$$

I risultati sono gli stessi, ma andrebbe dimostrato!

Verifichiamo che la $+$ in $\mathbb{Z}_n$ non dipenda dai rappresentanti. Bisogna vedere che:

$$[a] = [a'], [b] = [b'] \Rightarrow [a + b] = [a' + b']$$

Ipotesi:

1. $a' - a = kn$, ovvero è un multiplo di n
2. $b' - b = hn$

Verifichiamo che $(a' + b') - (a + b)$ è un multiplo di n:

$$a' + b' - a - b = \underbrace{(a' - a)}_{1.} + \underbrace{(b' - b)}_{2.} = kn + hn = (k + h)n \checkmark$$

Facciamo la stessa cosa per il prodotto:

$$[a] = [a'], [b] = [b'] \Rightarrow [ab] = [a'b']$$

Ipotesi:

1. $a' - a = hn$
2. $b' - b = kn$

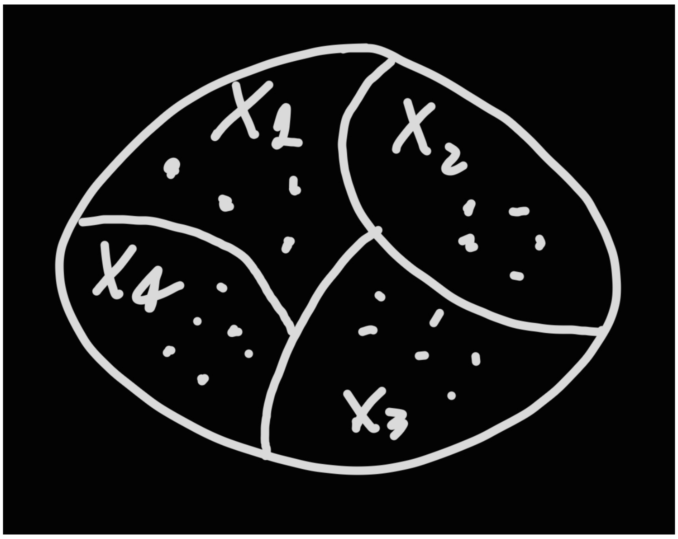
$$
a'b' - ab = (a + hn)(b + kn) - ab = ab + hnb + akn + hkn^2 - ab = \\
= (hb + ak + hkn)n \checkmark
$$

Entrambe le operazioni son **ben poste**.

Partizione

Sia X un insieme. Una famiglia $\{X_\alpha\}_{\alpha \in I}$ sottoinsiemi non vuoti di X si dice **partizione** di X se:

1. $X = \bigcup_{\alpha \in I} X_\alpha$
2. $X_\alpha \cap X_\beta = \emptyset \text{ se } \alpha \neq \beta$



$$
X = X_1 \cup X_2 \cup X_3 \cup X_4 \\
X_i \cap X_j = \emptyset \text{ se } i \neq j
$$

Proposizione

Esiste una corrispondenza biunivoca tra paritzioni di X e relazioni di equivalenza su X.

<u>Dimostrazione</u>: sia $\sim$ una relazione di equivalenza. Poniamo

$$
X_\alpha = \{x \in X | x \sim \alpha\} \alpha \in X
$$

Dico che $\{X_\alpha\}_{\alpha \in X}$ è una partizione di X.

Dato $\alpha \in X$, allora $\alpha \in X_\alpha$ poichè $\alpha \sim \alpha$ per la **relazione riflessiva**. Quindi $X = \bigcup X_\alpha$.

Devo ora vedere che se X_α e X_β si intersecano, allora $\alpha = \beta$:
Sia $z \in X_\alpha \cap X_\beta$

$$\begin{aligned} & z \in X_\alpha, z \sim \alpha \overset{SIM.}{\Longrightarrow} \alpha \sim z \\ & z \in X_\beta, z \sim \beta \\ & \overset{TRA.}{\Longrightarrow} \alpha \sim \beta \Rightarrow X_\alpha = X_\beta \end{aligned}$$

<u>Viceversa</u>: sia $X = \bigcup_{\alpha \in I} X_\alpha$ una partizione. Definisco la relazione

$$x \sim y \Leftrightarrow \exists \delta \in I : x, y \in X_\delta$$

Verifico che $\sim$ è di **equivalenza**:

- **Riflessiva**: $x \sim x$, devo vedere che esiste

$$\alpha \in I \text{ t.c. } x \in X_\alpha$$

  Ma questo segue dall'ipotesi che $X = \bigcup_{\alpha \in I} X_\alpha$.

- **Simmetrica**:

$$\begin{aligned} & x \sim y \Rightarrow \exists \alpha \in I \text{ t.c. } x, y \in X_\alpha \\ & \Rightarrow y \sim x \text{ (poichè entrambe appartengono a } X_\alpha) \end{aligned}$$

- **Transitiva**:

$$x \sim y, y \sim z \Rightarrow x \sim z$$

  Ipotesi:

$$\begin{aligned} & \exists \alpha_1 \in I : x, y \in X_{\alpha_1} \\ & \exists \alpha_2 \in I : x, y \in X_{\alpha_2} \end{aligned}$$

  quindi $y \in X_{\alpha_1} \cap X_{\alpha_2} \Rightarrow \alpha_1 = \alpha_2$ e di conseguenza $x, z \in X_{\alpha_1} \Rightarrow x \sim z$.

  Si verifica facilmente che le corrispondenze costruite sono una l'inversa dell'altra.

Lezione 04 - 07/10/2022

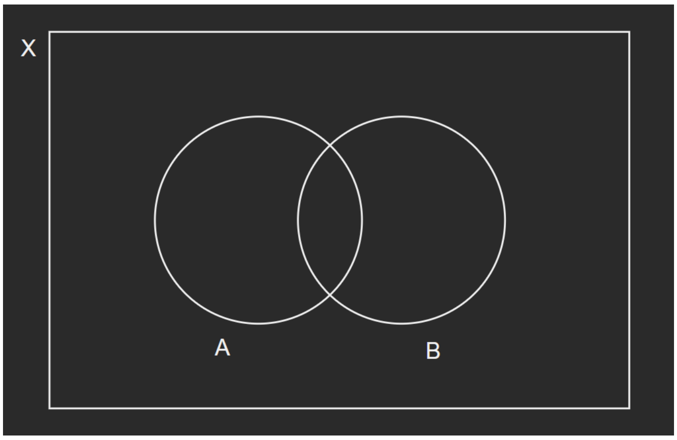
Relazione d’ordine (parziale)

Definizione: una relazione d’ordine $\leq$ su X è un sottoinsieme **non vuoto** di $X \times X$ che verifica le seguenti proprietà:

- **Riflessiva**: $x \leq x, \ \forall x \in X$
- **Antiriflessiva**: $x \leq y, \ y \leq x \Rightarrow x = y$
- **Transitiva**: $x \leq y, \ y \leq z \Rightarrow x \leq z$

Esempi:

1. Usuale $\leq$ su $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
   Nota: In questo caso, dati due elementi x, y risulta
   $$x \leq y \text{ oppure } y \leq x$$
   Una relazione d’ordine con questa proprietà si dice **totale**.
2. Sia X insieme, $\mathcal{P}(X)$ l’insieme delle parti di X e $A, B \in \mathcal{P}(X)$
   $$A \leq B \text{ se } A \subseteq B$$
   Guardando il seguente diagramam di Venn



Si ha che $A \nsubseteq B$ e $B \nsubseteq A$, quindi **non è una relazione d'ordine**.

3. Sia $X = \mathbb{N}$ e la relazione $\leq = |\ \text{"divide"}$

$$a \mid b \Leftrightarrow b \text{ è un multiplo di } a, \text{cioè } \exists c \in \mathbb{N} \text{ t.c. } b = ac$$

Esempi: $2 \nmid 5, 2 \mid 6$

- **Riflessiva**:

$$a \mid a,\ a = 1a \checkmark$$

- **Antisimmetrica**:

$$\begin{aligned} a &\mid b, b \mid a \\ b &= ca \\ a &= db \\ (b \neq 0)\ 1 &= cd \Rightarrow c = d = 1,\ \text{quindi } a = b \checkmark \end{aligned}$$

> ⚠️ In $\mathbb{Z}$, $cd = 1 \nRightarrow c = 1 = d$, in quanto potrebbe anche essere che $c = d = -1$, quindi la divisibilità non è una **relazione d'ordine** su $\mathbb{Z}$.

- **Transitiva**: $a \mid b, b \mid c \Rightarrow a \mid c$

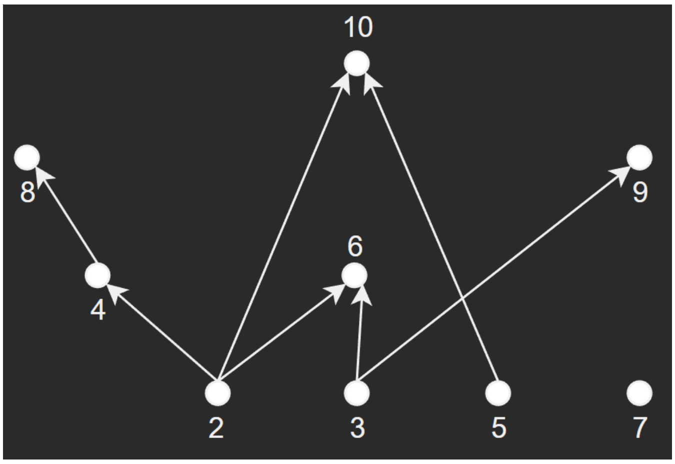
$$\begin{aligned} a \mid b &\Rightarrow b = ka \\ b \mid c &\Rightarrow c = hb \\ c = hb = hka &= (hk)a \Rightarrow a \mid c \checkmark \end{aligned}$$

Grafo di Hasse

Un insieme X dotato di una **relazione d'ordine parziale** è usualmente chiamato **POSET** (Partially - Ordered - Set). Spesso quando X è un insieme finito, un POSET viene rappresentato tramite il suo **grafo di Hasse**:

- **Vertici**: elementi di X
- **Lati orientati**: x → y se $x \leq y$ e $x \leq t \leq y \Rightarrow x = t \text{ oppure } y = t$, ovvero **non ci sono altri nodi di mezzo**.

<u>Esempio</u>: $X = \{2, 3, ..., 10\}$, con la relazione $\leq = |$



Costruzione di Z a partire da N

Siano $X = \mathbb{N} \times \mathbb{N}$ e ρ è la seguente relazione

$$(n, m)\rho(n', m') \iff n + m' = m + n'$$

Verifichiamo che si una relazione d'equivalenza:

- **Riflessiva**: $(n, m)\rho(n, m)$ vera in quanto $n + m = m + n$✓
- **Simmetrica**:

$$(n, m)\rho(n', m') \text{ ipotesi } n + m' = m + n'$$
$$(n', m')\rho(n, m) \text{ tesi } n' + m = m' + n \text{ ✓}$$

- **Transitiva**:

$$(n, m)\rho(n'm') \text{ e} \tag{1}$$
$$(n', m')\rho(n", m") \tag{2}$$
$$\text{tesi } (n, m)\rho(n", m") \tag{3}$$

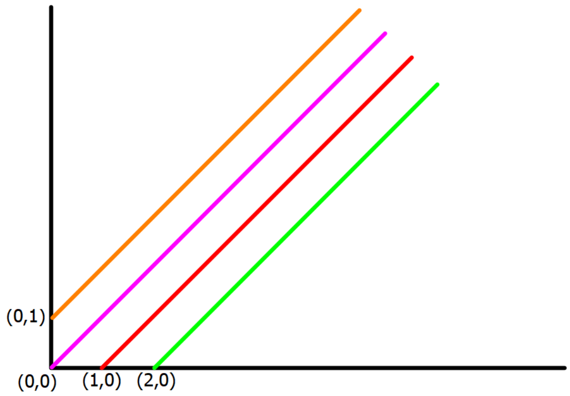
Da (1), (2) e (3) seguono le seguenti cose:

1. $n + m' = m + n'$
2. $n' + m" = m' + n"$
3. $n + m" = m + n"$

Dimostriamo che $n + m" = m + n"$

$$\begin{aligned} n + m" &= \underbrace{n + m'}_{1.} - m' + m" = \\ &= m + n' - m' + m" = \\ &= m - m' + \underbrace{n' + m"}_{2.} = \\ &= m - m' + m' + n" = \\ &= m + n" \end{aligned}$$

Definizione: $\mathbb{Z} = \mathbb{N} \times \mathbb{N}_{/\rho}$



Esempi:

$$\begin{aligned} [(1, 0)] &= \{(n, m) : (n, m) \sim (1, 0)\} \\ &= \{(n, m) : m + 1 = n\} \end{aligned}$$

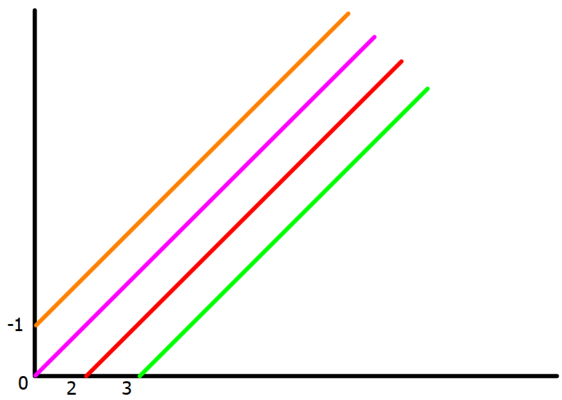
$$
\begin{aligned}
[(0,0)] &= \{(n,m) : (n,m) \sim (0,0)\} \\
&= \{(n,m) : (n,m)\}
\end{aligned}
$$

Poniamo

$$
\begin{aligned}
\mathbb{Z}_+ &= \{[(n,0)] : n \neq 0\} \\
\mathbb{Z}_- &= \{[(0,n)] : n \neq 0\} \\
0 &= [(0,0)]
\end{aligned}
$$

e

$$
\begin{aligned}
\mathbb{Z} &= \mathbb{Z}_+ \cup \mathbb{Z}_- \cup \{0\} \\
n &= [(n,0)] \\
-n &= [(0,n)] \\
0 &= [(0,0)]
\end{aligned}
$$



Definiamo le operazioni su $\mathbb{Z}$:

- Operazione $+$:

$$[(n,m)] + [(n',m')] = [(n+n', m+m')]$$

<u>Osservazione</u>:

$$
\begin{aligned}
2+3 &= [(2,0)] + [(3,0)] = [(5,0)] = 5 \\
2+(-2) &= [(2,0)] + [(0,2)] = [(2,2)] = [(0,0)] = 0 \\
2+(-3) &= [(2,0)] + [(0,3)] = [(2,3)] = [(0,1)] = -1
\end{aligned}
$$

- Operazione $\cdot$:

$$[(n,m)][(n',m')] = [(nn'+mm', n'm+m'n)]$$

<u>Osservazione</u>:

$$n \cdot m = [(n,0][(m,0)] = [(nm,0)] = nm,\ n,m > 0$$
$$n \cdot 0 = [(n,0)][(n,n)] = [(n^2,n^2)] = [(0,0)] = 0$$

Verifica che la definizione dell'addizione è ben posta, cioè che non dipende dal rappresentante scelto:

$$[(m,n)] + [(m',n')] = [(m+n', n+m')]$$
$$[(m,n)] = [(a,b)],\ [(m',n')] = [(a',b')]$$
$$\Rightarrow [(m+m', n+n')] = [(a+a', b+b')]$$

Ipotesi:

1. $m+b = n+a$
2. $m'+b' = n'+a'$

Tesi:

3. $m + m\text{'} = b+b',\ n+n' = a+a'$

Sommando membro a membro 1. e 2. si ottiene 3.

Proposizione

$(\mathbb{Z}, +, \cdot)$ è un **annello commutativo con unità**.

Lemma

Sia A un anello commutativo con unità:

1. $a \cdot 0 = 0 \cdot a = 0,\ \forall a$
2. $(-a)b = -ab$
3. $(-a)(-b) = ab$

<u>Dimostrazione</u>:

1. $0 + a \cdot 0 = a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$

$$\begin{aligned} (0 + a \cdot 0) + (-a \cdot 0) &= (a \cdot 0 + a \cdot 0) + (-a \cdot 0) \\ \text{(assoc.) } 0 + (a \cdot 0 + (-a \cdot 0)) &= a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) \\ 0 + 0 &= a \cdot 0 + 0 \\ 0 &= a \cdot 0 \end{aligned}$$

2. $0 \stackrel{1.}{=} 0 \cdot b = (a + b(-a)b = ab + (-a)b$

   Che è quello che si vuole: $(-a)b$ è l'elemento che devo sommare ad ab per ottenere 0. $-ab = (a)b$

3. $(-a)(-b) \stackrel{2.}{=} -(a(-b)) \stackrel{2.}{=} -(-ab) = ab$

Proposizione

Se $a, b \in \mathbb{Z}, ab = 0$ se e solo se $b = 0$ oppure $a = 0$

Dimostrazione: Si usa il fatto che gli interi hanno un segno

$$\mathbb{Z} = \mathbb{Z}_+ \cup \mathbb{Z}_- \cup \{0\}$$

Se $a, b > 0$ per la definizione di prodotto $ab > 0$

Se $a, b < 0$ per il lemma:

$$ab = \overset{>0}{(-a)}\overset{>0}{(-b)} > 0$$

Se $a > 0, b < 0$ allora $-b > 0$ e per il lemma

$$0 < a(-b) = -ab \Rightarrow ab > 0$$

Costruzione di Q a partire da Z

Siano $X = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ e ρ una relazione di equivalenza su X definita nel seguente modo:

$$(m, n)\rho(m', n') \Leftrightarrow mn' = nm'$$

Idea:

$$\frac{n}{m} = \frac{n'}{m'}$$

Bisogna dimostrare che:

1. ρ è una relazione di equivalenza
2. $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}_{/\rho}$
3. $\mathbb{Q}$ è un campo, quindi vanno definite le operazioni

$$[(m,n)] + [(m',n')] = [(mn' + nm', nn')]$$

questo perché

$$\frac{n}{m} + \frac{n'}{m'} = \frac{nm' + n'm}{mm'}$$

Poi

$$\begin{aligned} [(m,n)][(m',n')] &= [(mm', nn')] \\ -[(m,n)] &= [(-n,m)] \\ [(m,n)]^{-1} &= [(n,m)] \\ 0 &= [(0,1)] \\ 1 &= [(1,1)] \end{aligned}$$

Lezione 05 - 10/10/2022

Esercizio operazioni ben poste

$$\begin{aligned} \mathbb{R} \quad & x \sim_1 y \text{ se } [x] = [y] \\ & x \sim_2 y \text{ se } \{x\} = \{y\} \end{aligned}$$

Dove con:

- $[x] = \text{parte intera } \leq x$
- $\{x\} = \text{parte frazionaria } x - [x]$

$\sim_1$ e $\sim_2$ sono relazioni di equivalenza in quanto sono definite in **termini di uguaglianza**.

Chiamiamo:

- $\bar{x} = x \mod \sim_1 \quad (\bar{x} = \{y \in \mathbb{R} : y \sim_1 x\})$
- $\tilde{x} = x \mod \sim_2$

Definiamo

$$\begin{aligned} \bar{x} +_1 \bar{y} = \overline{x+y} \\ \tilde{x} +_2 \tilde{y} = \widetilde{x+y} \end{aligned}$$

Sono ben poste?

$+_1$ **non è ben posta**. Vengano presi $\overline{0.2} = \overline{0.8}$

$$\begin{aligned} \overline{0.2} + \overline{0.2} = \overline{0.2 + 0.2} = \overline{0.4} = 0 \\ \overline{0.8} + \overline{0.8} = \overline{0.8 + 0.8} = 1.6 \end{aligned}$$

Ma $0 \neq 1.6$ anche se abbiamo posto $\overline{0.2} = \overline{0.8}$. Questo significa che l'operazione **dipende** dai rappresentanti che vengono scelti.

$+_2$ invece è **ben posta**. Per dimostrarlo si osserva che

$$x \sim_2 y \Leftrightarrow x - y \in \mathbb{Z} \quad \text{(differiscono per un intero)}$$

È facile vedere che $+_2$ è ben posta:

$$\widetilde{x} = \widetilde{x_1}, \tilde{y} = \widetilde{y_1} \text{ allora } \widetilde{x+y} = \widetilde{x_1 + y_1}$$

<u>Ipotesi</u>:

$$\begin{gathered} x - x_1 = n, y - y_1 = m \\ x + y - (x_1 + y_1) = x - x_1 + y - y_1 = n + m \in \mathbb{Z} \end{gathered}$$

Definizioni: divisore dello zero, dominio di integrità, elemento invertibile, elementi associati, elemento irriducibile, elemento primo

Sia A un **anello commutativo con unità**:

1. Un elemento $a \in A, a \neq 0$ si dice **divisore dello zero** se esiste $b \in A, b \neq 0 : ab = 0$
2. Un **dominio di intregrità** è un anello commutativo con unità **privo** di divisori dello 0
3. Se $a, b \in A$ diciamo che $a \mid b$ se $\exists c \in A : b = ac$
4. Un elemento $a \in A : a \mid 1$ si dice **invertibile**
5. Due elementi $a, b \in A : a \mid b \wedge b \mid a$ si dicono **associati**
6. Un elemento $a \in A, a \neq 0, a$ non invertibile si dice **irriducibile** se

$$a = bc \Rightarrow b \text{ invertibile o } c \text{ invertibile}$$

7. Un elmento $a \in A, a \neq 0, a$ non invertibile si dice **primo** se

$$a \mid bc \Leftrightarrow a \mid b \text{ oppure } a \mid c$$

Commenti ed esempi

- In $\mathbb{Z}_6, \overline{2} \cdot \overline{3} = \overline{0}$

  Per lo stesso motivo, se $n = ab \text{ con } a, b \neq 1$ allora $\mathbb{Z}_n$ non è un domino di integrità
- È stato già dimostrato che $\mathbb{Z}$ è un dominio di integrità
- Dire che $a \mid 1$ significa dire che $\exists b \in A : ab = 1$
- È immediato osservare che in $\mathbb{Z}$ gli unici elementi invertibili sono ± 1 perchè la relazione in $\mathbb{Z}$

  $$ab = 1$$

  è possibile solo quando $a = b = 1$ oppure $a = b = -1$

Proposizione

In un dominio di integrità

$$a \text{ primo} \Rightarrow a \text{ riducibile}$$

Dimostrazione: Supponiamo a primo e facciamo vedere che se $a = bc$ allora b è invertibile o c è invertibile.

Se $a = bc$, in particolare $a \mid bc$, quindi per ipotesi $a \mid b$ oppure $a \mid c$.

Se $a \mid b$ significa che $b = ad$, quindi $a = bc$ diventa

$$a = adc$$
$$a(1 - dc) = 0$$

Poichè $a \neq 0$ per l'ipotesi, $1 - dc = 0$ ovvero $dc = 1$ ovvero c è **invertibile**.

Se $a \mid c$ si procede allo stesso modo: $c = af$, allora

$$a = bc$$
$$a = baf$$
$$a(1-bf) = 0$$
$$\Rightarrow bf = 1 \Leftrightarrow b \text{ è invertibile}$$

MCD e algoritmo euclideo in Z

Definizione: $a, b \in \mathbb{Z}$. Un numero $d \in \mathbb{Z}$ si dice un MCD(Massimo Comun Divisore) tra a e b se:

1. $d \mid a, \quad d \mid b$
2. $d' \mid a, \quad d' \mid b \Rightarrow d' \mid d$ (d è il più grande)

Nomenclatura: due interi a, b tali che $\mathrm{MCD}(a, b) = 1$ si dicono **coprimi**, ovvero non hanno divisori comuni.

Proposizione

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

Esempi:

$$\begin{aligned} 29, 7 &\rightsquigarrow 29 = 7 \cdot 4 + 1 \\ -29, 7 &\rightsquigarrow -29 = 7 \cdot (-5) + 6 \\ 29, -7 &\rightsquigarrow 29 = (-7) \cdot (-4) + 1 \\ -29, -7 &\rightsquigarrow -29 = (-7) \cdot 5 + 6 \\ 6, 7 &\rightsquigarrow 6 = 7 \cdot 0 + 6 \end{aligned}$$

Dimostrazione: Ricordiamo che dati a, b dobbiamo trovare q, r tali che

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

Vanno dimostrate **esistenza** e **unicità** di questi due elementi

- **Esistenza**:

  Sia $a > 0$. Procediamo per induzione su a.

  Se $a = 0$, poniamo $q = 0$ e $r = 0$ (base)

  Se $|b| > a$, posso porre $q = 0$ e $r = a$

  Quindi posso supporre $|b| \leq a$, cioè $a - |b| \geq 0$ e $a > a - |b|$, per induzione esistono q' e r' tali che

$$\begin{aligned} &a - |b| = q'b + r', \quad 0 \leq r' < |b| \\ &a = |b| + q'b + r' \end{aligned}$$

Se $b > 0$

$$a = \underbrace{b(1+q')}_{=q} + \underbrace{r'}_{=r} \quad 0 \le r < |b|$$

Se $b < 0$

$$\begin{aligned} a &= -b + q'b + r' \\ &= \underbrace{b(q'-1)}_{=q} + \underbrace{r'}_{=r} \quad 0 \le r < |b| \end{aligned}$$

Se $a < 0,\ -a > 0$ posso quindi usare la prima parte con $-a$. Per i dettagli, vedere sul libro di testo.

- **Unicità**

$$a = \overbrace{bq + r}^{(1)} = \overbrace{bq' + r'}^{(2)} \quad \begin{aligned} 0 &\le r < |b| \\ 0 &\le r' < |b| \end{aligned}$$

Possiamo assumere $r' \ge r$. Sottraiamo (1) da (2)

$$\begin{aligned} &0 \le r' - r = b(q - q') \\ &|b||q - q'| = |r' - r| = r' - r \le r' < |b| \end{aligned}$$

Siccome $b \neq 0$, da $|b||q - q'| < |b|$ segue che $|q - q'| < 1 \Rightarrow q = q'$.
Ma se $q = q'$

$$bq + r = bq' + r' = bq + r'$$

Quindi bq ha come resti sia r che r', che deve significare che $r = r'$.

Teorema - Identità di Bezout

Dati $a, b \in \mathbb{Z}$ non entrambi 0, esiste $d = \mathrm{MCD}(a,b)$. Inoltre esistono interi $s, t \in \mathbb{Z}$ tali che:

$$d = sa + tb$$

tale espressione viene chiamata **identità di Bezout** e ne esistono infinite.

Dimostrazione: ricordiamo che il principio di induzione è equivalente al principio del minimo: ogni sottoinsieme $S \neq \emptyset, S \subseteq \mathbb{N}$, ha minimo.

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

- $S \neq \emptyset$: supponiamo $a \neq 0$. Se $a > 0, a \in S$. Se $a < 0, -a \in S$. Per costruzione $S \subseteq \mathbb{N}$.

  Per il principio del minimo esiste $d = \min S$. Dico che $d = \mathrm{MCD}(a, b)$. Dimostro che $d \mid a$ facendo la divisione con resto di a per d e mostrando che il resto è 0.

  $$\begin{gathered} a = qd + r, \quad 0 \leq r < d \\ 0 \leq r = a - qd \overset{*}{=} a - q(x_0 a + y_0 b) = \\ = (1 - x_0 q)a - q y_0 b \leq d \end{gathered}$$

  $*$: $d = x_0 a + y_0 b$ in quanto $d \in S$ siccome abbiamo detto che $d = \min S$ e gli elementi di S sono della forma $xa + yb$.

  Se $r \neq 0$, ho dimostrato che $r \in S$, $r < d = \min S$ (contraddizione, in quanto risulta che r è minore di d).

  Questo significa che $r = 0$ e quindi abbiamo dimostrato che $d \mid a$ e similmente $d \mid b$. Inoltre è chiaro che se $d' \mid a$ e $d' \mid b$ allora $d' \mid d$.

  Infatti se $a = hd', b = kd'$ allora

  $$d = x_0 a + y_0 b = x_0 h d' + y_0 k d' = (x_0 h + y_0 k) d'$$

  e qunque $d' \mid d$.

Lezione 06 - 13/10/2022

Algoritmo euclideo

Notazione: Si chiama $(a, b) = \text{MCD}$ positivo di a, b.

Nel seguito vediamo come:

1. Calcolare algoritmicamente (a, b)
2. Trovare un’identità di bezout per (a, b)

Esempio:

- $(3522, 321)$

$$\begin{aligned} 3522 &= 321 \cdot 10 + 312 \\ 321 &= 312 \cdot 1 + 9 \\ 312 &= 9 \cdot 34 + 6 \\ 9 &= 6 \cdot 1 + \underline{3} \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

  Dove l’ultimo resto non nullo nella catena di divisioni è il risultato, in questo caso $(3522, 321) = 3$.

  Vediamo l’dentità di bezout: cerchiamo un’espressione del tipo $3 = x \cdot 321 + y \cdot 3522$

$$\begin{aligned}3 &= 9-6\\ &= 9-(312-9\cdot 34)\\ &= 9\cdot 35-312\\ &= (321-312)\cdot 35-312\\ &= 321\cdot 35-312\cdot 36\\ &= 321\cdot 35-(3522-321\cdot 10)\cdot 36\\ &= -3522\cdot 36+321\cdot 35+321\cdot 360\\ &= -3522\cdot 36+321\cdot 395\end{aligned}$$

quindi abbiamo che $3 = -3522 \cdot 36 + 321 \cdot 395$.

- $(57, 23)$

$$\begin{aligned}57 &= 23\cdot 2+11\\ 23 &= 11\cdot 2+\underline{1}\\ 11 &= 1\cdot 11+0\end{aligned}$$

Quindi $(57, 23) = 1$ (sono coprimi)

Vediamo l'identità di bezout: cerchiamo un'espressione del tipo $1 = x \cdot 23 + y \cdot 57$

$$\begin{aligned}1 &= 23-11\cdot 2\\ &= 23-(57-23\cdot 2)\cdot 2\\ &= 23-57\cdot 2+23\cdot 4\\ &= 23\cdot 5-57\cdot 2\end{aligned}$$

quindi abbiamo che $1 = 23 \cdot 5 - 57 \cdot 2$.

Proposizione - Soluzioni di ax+by=c

L'equazione $(1) ax + by = c,\ a, b, c \in \mathbb{Z}$ possiede una soluzione intera

$$(x, y) \in \mathbb{Z} \text{ sse } (a, b) \mid c$$

Esempi:

- $2x + 2y = 5$ non ha soluzione intere perche $(2, 2) \nmid 5$

- $2x + 2y = 4$ ha soluzioni intere, ad esempio $x = y = 1$

<u>Dimostrazione</u>: supponiamo che l'equazione (1) abbia soluzione $(\bar{x}, \bar{y})$. Allora vale

$$a\bar{x} + b\bar{y} = c$$

Sia $d = (a, b)$ con $d \mid a$ e $d \mid b$, quindi $d \mid a\bar{x}, d \mid b\bar{y}$, quindi $d \mid a\bar{x} + b\bar{y} = c$ come vogliamo.

Viceversa, supponiamo che $d \mid c$. Scriviamo l'**identità di bezout** per d:

$$d = \alpha a + \beta b$$

Poichè $d \mid c, c = hd$

$$c = hd = \underbrace{h\alpha}_{x} a + \underbrace{h\beta}_{y} b$$

Proposizione - In Z ogni irriducibile è primo

In $\mathbb{Z}$ ogni **irriducibile** è **primo**.

<u>Dimostrazione</u>: Supponiamo p **irriducibile** e $p \mid ab$. Dobbiamo far vedere che se $p \nmid a$ allora $p \mid b$.

Siccome $p \mid ab,\ ab = ph \Rightarrow (a, p) = 1$.

Dunque esistono $s, t \in \mathbb{Z}$ t.c. $as + tp = 1$. Moltiplico questa relazione per b

$$b = bas + btp = \overbrace{abs}^{p|} + \overbrace{pbt}^{p|} \Rightarrow p \mid b$$

Teorema fondamentale dell'aritmetica

Sia $n > 1$ un intero. Allora n è prodotto di un numero finito di potenze di primi:

$$n = p_1^{h_1} ... p_s^{h_s} \quad h_i > 0,\ p_i \neq p_j,\ i \neq j$$

Inoltre tale fattorizzazione è unica nel senso che se

$$n = q_1^{k_1} ... q_t^{k_t} \quad k_i > 0,\ q_i \neq q_j, i \neq j, q_i \text{ primi}$$

allora $s = t$ a meno di **rioridinamenti** $p_i = q_i$ **e** $h_i = k_i$**.**

Dimostrazione:

- **Esistenza**: per induzione su n, con base ovvia $n = 2$.

  Supponiamo di avere dimostrato l'esistenza della fattorizzazione per ogni intero $k,\ 2 \leq k < n$ e dimostriamola per n.

  Se n è **primo** non c'è **nulla da dimostrare**.

  Altrimenti **non è irriducibile**, quindi può scriversi come

$$\begin{aligned} n = n_1 n_2, \quad & 2 \leq n_1 < n \\ & 2 \leq n_2 < n \end{aligned}$$

  Per induzione n_1, n_2 hanno fattorizzazione e quindi anche n ce l'ha

$$n_1 = p_1^{a_1} ... p_s^{a_s} \ , \quad n_2 = q_1^{b_1} ... q_s^{b_s}$$
$$n = p_1^{a_1} ... p_s^{a_s} q_1^{b_1} ... q_s^{b_s} = t_1^{c_1} ... t_n^{c_n} \text{ con i } t_i \ \underline{\text{primi}}$$

  Esempio:

$$\begin{aligned} n_1 &= 2^3 \cdot 3^4 \cdot 5 \\ n_2 &= 2^3 \cdot 3 \cdot 5 \cdot 7 \\ n_1 n_2 &= 2^6 \cdot 3^5 \cdot 5^2 \cdot 7 \end{aligned}$$

- **Unicità**: Si consideri $n = p_1^{h_1} ... p_s^{h_s} \ (*)$

  Procediamo per induzione su $m = h_1 + ... + h_s$

  - Caso base: $m = 1$; la $(*)$ ci dice che n è primo. **Supponiamo** che ci sia **un'altra fattorizzazione in primi**. Sia p

$$\begin{aligned} p = n = q_1^{k_1} ... q_t^{k_t} \\ \implies p \mid q_1^{k_1} ... q_t^{k_t} \end{aligned}$$

    Poichè p è primo, p **divide uno dei** q_i

$$p \mid q_i$$

    ma q_i è primo, quindi $p = q_i$. Allora

$$p = q_1^{k_1} ... p^{k_i} ... q_t^{k_t}$$

implica

$$1 = q_1^{k_1} ... p^{k_i - 1} ... q_t^{k_t}$$
$$\implies k_1 = ... = k_{i-1} = k_{i+1} = ... = k_t = 0 \quad k_i = 1$$

Quindi la seconda fattorizzazione è proprio $n = q_i = p$.

- Caso $m > 1$: **supponiamo** che n abbia **due fattorizzazioni.**

$$(**) n = p_1^{h_1} ... p_s^{h_s} = q_1^{k_1} ... q_t^{k_t}$$

con $h_1 + ... + h_s = m_i$ come prima

$$p_1 \mid q_1^{k_1} ... q_t^{k_t}$$

quindi come prima $p_1 \mid q_i$ e quindi $p_1 = q$.

Allora $(**)$ diventa

$$p_1^{h_1} ... p_s^{h_s} = q_1^{k_1} ... p_1^{k_i} ... q_t^{k_t}$$
$$p_1^{h_1 - 1} ... p_s^{h_s} = q_1^{k_1} ... p_1^{k_i - 1} ... q_t^{k_t}$$

Al primo membro la somma degli esponenti è $m - 1$. Per induzione ho l'unicità della fattorizzazione, quindi $h_i - 1 = k_i - 1$ e gli altri fattori coincidono a meno di riordinamento. Quindi la **fattorizzazione di n è unica**.

> ⚠️ Si noti come nel corso della dimostrazione si sia utilizzata pesantemente l'equivalenza in $\mathbb{Z}$ tra l'essere **primo** e l'essere **irriducibile**.

Proposizione - I numeri primi sono infiniti

Dimostrazione: supponiamo il viceversa, ovvero che $p_1 ... p_N$ sia la lista **finita** di tutti i numeri primi. Sia

$$M = p_1 \cdot ... \cdot p_N + 1$$

Osserviamo che M da resto 1 quando è diviso per ogni numero primo, quindi M **non è divisibile** per nessun primo, **contro il teorema fondamentale dell'aritmetica**■

Congruenze e sistemi di congruenze

Vogliamo risolvere equazioni del tipo

$$ax = b \text{ in } \mathbb{Z}_n$$

ovvero **congruenze** del tipo

$$ax \equiv b \mod n$$

e anche sistemi del tipo

$$\begin{cases} a_1x \equiv b_1 \mod n_1 \\ a_2x \equiv b_2 \mod n_2 \\ ... \\ a_kx \equiv b_k \mod n_k \end{cases}$$

Proprietà fondamentali delle congruenze

Ricordiamo che $a \equiv b \mod n$ se $n \mid b - a$

$$\begin{aligned} a &= xn + r \\ b &= yn + r \\ b - a &= (x-y)n \Rightarrow n \mid b - a \end{aligned}$$

viceversa se $n \mid b - a,\ b - a = hn$, se

$$\begin{aligned} a &= xn + r_1 \\ b &= yn + r_2 \\ b - a &= (x-y)n + r_1 - r_2 \\ &= hn \Rightarrow r_1 = r_2 \end{aligned}$$

> ⚠️ Il fatto che $r_1 = r_2$ segue dal fatto che n divide $a - b$, quindi il resto deve essere 0. Questo accade solo se $r_1 = r_2$.

Sia $a \equiv_n b$; allora

1. $a + c \equiv_n b + c$
2. $ac \equiv_n bc$
3. $a^i \equiv_n b^i,\ i \geq 0$
4. $ac \equiv_n bc,\ (c, n) = 1 \Rightarrow a \equiv_n b$

$$\begin{aligned} n \mid bc - ac = (b-a)c \\ (c,n) = 1 \Rightarrow \exists s,t : cs + tn = 1 \\ b - a = (b-a)cs + (b-a)tn \\ = ns + (b-a)tn \\ = n(s + (b-a)t) \end{aligned}$$

   Dunque $n \mid b - a$, ovvero $a \equiv_n b$.

5. $ac \equiv bc \mod n \Rightarrow a \equiv b \mod \dfrac{n}{(n,c)}$

> ⚠️ Nota: **non** è vero che $ac \equiv_n bc \Rightarrow a \equiv_n b$, ovvero non è vero che si può dividere per c. Esempio:
>
> $$\begin{aligned} 3 \cdot 5 \equiv 3 \cdot 8 \mod 9 \\ 15 \equiv 24 \mod 9 \\ 6 \equiv 6 \mod 9 \checkmark \end{aligned}$$
>
> Ma $5 \not\equiv 8 \mod 9$.

Lemma

Sia p primo e $x, y \in \mathbb{Z}$,

$$(x+y)^p = x^p + y^p \mod p$$

Dimostrazione:

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

Ma $p \mid \binom{p}{k}$ se $k \neq 0, p$, quindi nella somma restano solo il primo e l'ultimo termine $\bmod p$

$$(x+y)^p = \underbrace{\binom{p}{0}}_{=1} x^0 + y^{p-0} + \underbrace{\binom{p}{p}}_{=1} x^p y^{p-k} = x^p + y^p$$

Teorema - Piccolo teorema di Fermat

Sia $a \in \mathbb{Z}$, p un **numero primo**, allora

$$a^p \equiv a \mod p$$

Dimostrazione: Se $a \geq 0$, **procediamo per induzione** su a

- $a = 0$

  Non c'è niente da dimostrare

- $a > 0$

  Assumiamo $a^p \equiv a \mod p$ sia vero e dimostriamo che $(a+1)^p \equiv a+1 \mod p$.

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

- $a < 0$

  $$0 = 0^p = (a + (-a))^p \equiv a^p + (-a)^p \equiv a^p - a \Rightarrow a^p \equiv a \mod p$$

  Nota: dato che $-a > 0$, per quanto provato nel punto precedente si ha che $(-a)^p \equiv -a$.

Corollario

Se $(a, p) = 1$, allora $a^{p-1} \equiv 1 \mod p (*)$.

Dimostrazione: Se $(a,p)=1$, posso semplificare a nella relazione $a^p \equiv a \mod p$, ottenendo $(*)$

Lezione 07 - 14/10/2022

Ripasso - Elementi invertibili

Ricordiamo che se A è un **anello commutativo con unità**, un elemento $a \in A$ si dice **invertibile** se

$$\exists b \in A : ab = 1$$

Esempio: In $\mathbb{Z}$ gli elementi invertibili sono ± 1.
Osserviamo inoltre che gli elementi invertibili di A **formano un gruppo rispetto al prodotto**. Infatti basta verificare che il prodotto di elementi invertibili è invertibile: Se a, b sono invertibili, esistono

$$c, d \in A : ac = 1 \quad bd = 1$$

ma allora

$$(ab)(cd) = acbd = 1 \cdot 1 = 1$$

Osservazione: $\{\pm 1\}$ è un gruppo rispetto al prodotto. La tabella moltiplicativa è:

	1	-1
1	1	-1
-1	-1	1

Proposizione

$\bar{a} \in \mathbb{Z}_n$ è invertibile se e solo se $(a, n) = 1$

Corollario

$\{\bar{a} \in \mathbb{Z}_n : 0 < a < n,\ (a, n) = 1\}$ è un gruppo (che spesso viene denotato con $\mathbb{U}_n$)

Dimostrazione: supponiamo che $(a, n) = 1$. Scriviamo l'**identità di bezout**:

$$ab + ns = 1$$

prendiamo le classi resto $\bmod n$

$$\begin{gathered}\overline{ab + ns} = \overline{1} \\ \overline{a}\overline{b} + \underbrace{\overline{ns}}_{=\overline{0}} = \overline{1} \\ \overline{a}\overline{b} = \overline{1}\end{gathered}$$

Dunque $\overline{a}$ è invertibile e $\overline{b}$ è l'**inverso**.
Viceversa, se $\overline{a}$ è **invertibile**, esiste $\overline{b} \in \mathbb{Z}_n$ con $\overline{a}\overline{b} = \overline{1}$, cioè

$$\begin{aligned}&ab \equiv 1 \mod n \\ &ab - 1 = kn \\ &\underbrace{ab - kn = 1}_{\text{identità di bezout}} \Rightarrow (a, n) = 1\end{aligned}$$

Esempi esercizi:

1. Trovare gli **elementi invertibili** in $\mathbb{Z}_{42}$

$$\begin{gathered}42 = 2 \cdot 3 \cdot 7 \\ \{\overline{1}, \overline{5}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{37}, \overline{41}\}\end{gathered}$$

   Procedimento:

   - Si prende il modulo
   - Si fattorizza
   - Si prendono i fattori che non hanno multipli in comune

2. Trovare l'inverso di $\overline{31}$ in $\mathbb{Z}_{42}$

$$\begin{aligned} 42 &= 31 + 11 \\ 31 &= 11 \cdot 2 + 9 \\ 11 &= 9 \cdot 1 + 2 \\ 9 &= 2 \cdot 4 + 1 \end{aligned}$$

Scriviamo ora l'identità di bezout

$$\begin{aligned} 1 &= 9 - 2 \cdot 4 \\ &= 9 - (11 - 9) \cdot 4 \\ &= 9 \cdot 5 - 11 \cdot 4 \\ &= (31 - 11 \cdot 2)5 - 11 \cdot 4 \\ &= 31 \cdot 5 - 11 \cdot 14 \\ &= 31 \cdot 5 - (42 - 31) \cdot 14 \\ &= 31 \cdot 19 - 42 \cdot 14 \end{aligned}$$

Quindi l'inverso di $\overline{31}$ è $\overline{19}$ in $\mathbb{Z}_{42}$ in quanto $\overline{31} \cdot \overline{19} = \overline{1}$.

Spoiler - la cardinalità di Un

Definizione: funzione ϕ di Eulero

$$\phi(n) = |\{a \in \mathbb{N}, 1 \leq a <, (a, n) = 1\}|$$

Teorema: $\phi(n)$ si calcola a partire dalla fattorizzazione di n usando le due segenti regole:

1. Se p **primo**, $\phi(p^n) = p^n - p^{n-1}$
2. Se $(r, s) = 1$, $\phi(rs) = \phi(r) \cdot \phi(s)$

Esempio:

- Calcolo di $\phi(42)$

$$\begin{aligned} \phi(42) = \phi(2 \cdot 3 \cdot 7) &\overset{(2)}{=} \phi(2)\phi(3)\phi(7) \\ &\overset{(1)}{=} (2-1)(3-1)(7-1) = 1 \cdot 2 \cdot 6 = 12 \end{aligned}$$

- Calcolo di $\phi(100)$

$$\phi(100) = \phi(2^2 \cdot 2^5) = \phi(2^2)\phi(2^5)$$
$$= (2^2 - 2)(5^2 - 2) = (4-2)(25-5) = 40$$

Congruenze lineari

Una **congruenza lineare** è un'equazione della forma

$$ax \equiv b \mod n$$

con $a, b \in \mathbb{Z},\ n \in \mathbb{N}$.

> ⚠️ Può essere pensata come l'equazione $\bar{a}\bar{x} = \bar{b}$ in $\mathbb{Z}_n$

Proposizione

Una congruenza $ax \equiv b \mod n$ ha soluzione se e solo se $(a, n) \mid b$.

Dimostrazione:

$$ax \equiv b \mod n \iff ax - b = kn \iff ax - kn = b$$

ovvero, la congruenza $ax \equiv b \mod n$ ha soluzione se e solo se l'**equazione diofantea** $ax - kn = b$ **ha soluzione**, che accade se e solo se $(a, n) \mid b$.

Proposizione

Sia $ax \equiv b \mod n$ una **congruenza lineare** con $(a, n) \mid b$. Se x_0 è una soluzione, **tutte le soluzioni** sono del tipo

$$x_0 + h \cdot \underbrace{\frac{n}{(a,n)}}_{\text{è un intero}}, \quad h \in \mathbb{Z}$$

tra queste le soluzioni con $0 \leq h < (a, n)$ sono **a due a due non congruenti** e **ogni altra soluzione è congruente a una di esse**.

Esempio: $2x \equiv 4 \mod 8$ con $d = (a, n) = 2$.

Le soluzioni fondamentali sono: $x_0,\ x_0 + 4$. Ad esempio:

- $x_0 = 2$

- $x_0 = 4$

Proviamo che $x_0 + h \cdot \frac{n}{d}$ (abbiamo posto $d = (a, n)$) è una soluzione:

$$\begin{aligned} a(x_0 + h \cdot \frac{n}{d}) &= ax_0 + ah \cdot \frac{n}{d} \\ &\equiv b + \underbrace{\text{m.c.m}(a, n) \cdot h}_{\text{è un multiplo di n}} \\ &\equiv b \mod n \end{aligned}$$

Proviamo ora che **ogni soluzione è di questo tipo**: siano x_0, x_0' due soluzioni, allora

$$\begin{aligned} &ax_0 = b + hn, \ ax_0' = b + kn \\ &a(x_0 - x_0') = (h-k)n \\ &\frac{a}{d}(x_0 - x_0') = (h-k)\frac{a}{d} \end{aligned}$$

$$(\frac{a}{d}, \frac{n}{d}) = 1 \quad \begin{aligned} &\frac{n}{d} \mid x_0 - x_0' \\ &x_0 - x_0' = h \cdot \frac{n}{d} \\ &x_0 = x_0' + h \cdot \frac{n}{d} \end{aligned}$$

Resta da vedere che le soluzioni $x_0 + h \cdot \frac{n}{d} \quad 0 \leq h < d$

1. Sono **a due a due non congruenti**
2. Che **ogni altra soluzione è congruente a una di loro**

<u>Dimostrazione per 1.</u>: Supponiamo per assurdo che

$$x_0 + h_1 \cdot \frac{n}{d} \equiv x_0 + h_2 \cdot \frac{n}{d} \mod n, \quad 0 \leq h_1 < h_2 < d \ (1)$$

allora

$$h_1 \cdot \frac{n}{d} \equiv h_2 \cdot \frac{n}{d} \mod n$$

dunque

$$h_1 \equiv h_2 \mod \frac{n}{n/d}$$

e qundi $h_1 \equiv h_2 \mod d$ che è **assurdo** per (1).

ℹ️ Si ricorda che per la proprietà 5 delle congruenze

$$ac \equiv bc \mod n$$
$$a \equiv b \mod \frac{n}{(n,c)}$$

Dimostrazione per 2: prendiamo una soluzione $x_0 + h \cdot \frac{n}{d}$ e dividiamo h per d:

$$h = dq + r \quad 0 \leq r < d$$
$$x_0 + h \cdot \frac{n}{d} = x_0 + (dq + r)\frac{n}{d} = x_0 + nq + r\frac{n}{d} \equiv x_0 + r\frac{n}{d} \mod n$$

Corollario

Se $(a, n) = 1$, la congruenza $ax \equiv b \mod n$ **ammette soluzione unica** $\mod n$.

Esempio:

$$5x \equiv 16 \mod 7$$
$$\overline{5}\overline{x} = \overline{16} = \overline{2} \text{ in } \mathbb{Z}_7$$

L'inverso di $\overline{5}$ in $\mathbb{Z}_7$ è $\overline{3}$

$$\overline{3} \cdot \overline{5}\overline{x} = \overline{3} \cdot \overline{2}$$
$$\overline{x} = \overline{6}$$
$$x = 6 + 7k, \; k \in \mathbb{Z}$$

⚠️ Devo trovare l'inverso di $\overline{5}$ per isolare la $\overline{x}$.

Sistemi di congurenze lineari

Vogliamo ora risolvere sistemi di congruenze lineari del tipo

$$\begin{cases} a_1 x \equiv b_1 \mod n_1 \\ a_2 x \equiv b_2 \mod n_2 \\ ... \\ a_s x \equiv b_s \mod n_s \end{cases}$$

Supponiamo dapprima $(n_i, n_j) = 1,\ i \neq j$.

Supponiamo inoltre $d_i = (a_i, n_i) \mid b_i$.

Se divido per d_i ciascuna equazione, ottengo un sistema del tipo:

$$\begin{cases} a'_1 x \equiv b'_1 \mod n'_1 \\ a'_2 x \equiv b'_2 \mod n'_2 \\ ... \\ a'_s x \equiv b'_s \mod n'_s \end{cases}$$

con $a_i = \dfrac{a_i}{d_i}$, $b_i = \dfrac{b_i}{d_i}$ e $n_i = \dfrac{n_i}{d_i}$.

Ma allora $(a'_i, n'_i) = 1$ quindi a'_i è invertibile in $\mathbb{Z}_n$ e quindi il sistema può riscriversi nella forma

$$\begin{cases} x \equiv c_1 \mod n'_1 \\ ... \\ x \equiv c_s \mod n'_s \end{cases}$$

con $c_i = a_i'^{-1},\ (n'_i, n'_j) = 1,\ i \neq j$.

<u>Esempio</u>:

$$\begin{cases} 1025x \equiv 5312065 \mod 8 \\ 36x \equiv 322 \mod 5 \\ 4x \equiv 7 \mod 3 \end{cases}$$

si trasforma in

$$\begin{cases} x \equiv 1 \mod 8 \\ x \equiv 2 \mod 5 \\ x \equiv 1 \mod 3 \end{cases}$$

soluzione

$$\begin{aligned} x &= 1 + 8n \\ 1 + 8n &\equiv 2 \quad \mod 5 \\ 8n &\equiv 1 \quad \mod 5 \\ 3n &\equiv 1 \quad \mod 5 \\ n &\equiv 2 \quad \mod 5 \end{aligned}$$

$$\begin{aligned} n &= 2 + 5m \\ x &= 1 + 8n = 1 + 8(2 + 5m) = \\ &= 17 + 40m \end{aligned}$$

$$\begin{aligned} 17 + 40m &\equiv 1 \quad \mod 3 \\ 2 + m &\equiv 1 \quad \mod 3 \\ m &\equiv -1 \quad \mod 3 \\ m &\equiv 2 \quad \mod 3 \\ m &= 2 + 3s \end{aligned}$$

$$\begin{aligned} x &= 17 + 40m = 17 + 40(2 + 3s) = \\ &= 97 + 120s \end{aligned}$$

Lezione 09 - 20/10/2022

Teorema cinese del resto

Il sistema di congruenze

$$\begin{cases} x \equiv c_1 \mod r_1 \\ x \equiv c_2 \mod r_2 \\ ... \\ x \equiv c_s \mod r_s \end{cases}$$

con $(r_i, r_j) = 1,\ i \neq j$, **ha soluzione unica** $\mod r_1 \cdot r_2 \cdot ... \cdot r_s$**.**

Dimostrazione: poniamo $R = r_1 \cdot r_2 \cdot ... \cdot r_s,\ R_k = \dfrac{R}{r_k}$.

Ovviamente si ha che $(R_k, r_k) = 1$, quindi la congruenza

$$R_k x \equiv c_k \mod r_k$$

ammette un'unica soluzione $\bar{x}_k \mod r_k$. Pongo

$$\bar{x} = R_1\bar{x}_1 + R_2\bar{x}_2 + ... + R_s\bar{x}_s$$

e dico che $\bar{x}$ risolve il sistema di congruenze. Infatti la **k-esima equazione** è

$$\begin{aligned} x &\equiv c_k \mod r_k \\ \bar{x} &= R_1\bar{x}_1 + R_2\bar{x}_2 + ... + R_s\bar{x}_s \\ &\equiv R_k\bar{x}_k \equiv c_k \mod r_k \end{aligned}$$

Per provare l'unicità $\mod r_1 \cdot ... \cdot r_s$, supponiamo che $\bar{y}$ sia un'altra soluzione:

$$\bar{x} \equiv c_k \equiv \bar{y} \mod r_k,\ \forall k$$

quindi

$$\begin{aligned} \bar{x} - \bar{y} &\equiv 0 \mod r_k,\ \forall k \\ \text{ovvero } \bar{x} - \bar{y} &\equiv 0 \mod r_1 \cdot ... \cdot r_s \end{aligned}$$

ovvero $\bar{x} \equiv \bar{y} \mod r_1 \cdot ... \cdot r_s$.

Esempio:

$$\begin{cases} x \equiv 1 \mod 8 \\ x \equiv 2 \mod 5 \\ x \equiv 1 \mod 3 \end{cases}$$

si ha che:

- $R = 5 \cdot 8 \cdot 3 = 120$
- $R_1 = 15$
- $R_2 = 24$
- $R_3 = 40$

che forma il seguente sistema

$$\begin{cases} R_1 x \equiv c_1 \mod r_1 \\ R_2 x \equiv c_2 \mod r_2 \\ R_3 x \equiv c_3 \mod r_3 \end{cases}$$

ovvero

$$\begin{cases} 15x \equiv 1 \mod 8 \\ 24x \equiv 2 \mod 5 \\ 40x \equiv 1 \mod 3 \end{cases}$$

ricaviamo ora le $\overline{x}_k$

$$\begin{array}{lllll} 15x \equiv 1 \mod 8 & \rightarrow & -x \equiv 1 \mod 8 & \rightarrow & x \equiv -1 \equiv 7 \mod 8 & \overline{x}_1 = 7 \\ 24x \equiv 2 \mod 5 & \rightarrow & -x \equiv 2 \mod 5 & \rightarrow & x \equiv -2 \equiv 3 \mod 5 & \overline{x}_2 = 3 \\ 40x \equiv 1 \mod 3 & \rightarrow & x \equiv 1 \mod 3 & & & \overline{x}_3 = 1 \end{array}$$

quindi

$$\begin{aligned} \overline{x} &= R_1\overline{x}_1 + R_2\overline{x}_2 + R_3\overline{x}_3 \mod 120 \\ &= 15 \cdot 7 + 24 \cdot 3 + 40 \cdot 1 = 105 + 72 + 40 \\ &= 217 \equiv 97 \mod 120 \end{aligned}$$

e quindi tutte le soluzioni sono del tipo $x = 97 + 120k$.

Proposizione

Siano r, s interi ≥ 2, $(r, s) = 1$. Allora la corrispondenza

$$f : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$$

data da

$$f(x \bmod rs) = (x \bmod r, x \bmod s)$$

è **biunivoca** e **rispetta le operazioni**.

⚠️ Più avanti diremo che f è un **isomorfismo di anelli**.

Esempio:

$$\begin{aligned}
\mathbb{Z}_6 \to& \mathbb{Z}_3 \times \mathbb{Z}_2 \\
\bar{0} \mapsto& (\bar{0}, \bar{0}) \\
\bar{1} \mapsto& (\bar{1}, \bar{1}) \\
\bar{2} \mapsto& (\bar{2}, \bar{0}) \\
\bar{3} \mapsto& (\bar{0}, \bar{1}) \\
\bar{4} \mapsto& (\bar{1}, \bar{0}) \\
\bar{5} \mapsto& (\bar{2}, \bar{1})
\end{aligned}$$

Dove quello che si trova prima di '$\mapsto$' è inteso in $\bmod 6$, mentre quello che si trova nelle parentesi è inteso rispettivamente alle posizioni nella coppia $\bmod 3$ e $\bmod 2$.

Esempio:

$$\bar{3} + \bar{5} = \bar{8} = \bar{2}$$
$$(\bar{0}, \bar{1}) * (\bar{2}, \bar{1}) = (\bar{2}, \bar{0})$$

Dimostrazione di f biunivoca: Poichè $|\mathbb{Z}_{rs}| = |\mathbb{Z}_r| \times |\mathbb{Z}_s| = rs$, basta vedere che f è **suriettiva**.

Dire che f è suriettiva significa dire che dato $\bar{a} \in \mathbb{Z}_r$, $\bar{b} \in \mathbb{Z}_s$, esiste $x \in \mathbb{Z}_{rs}$ tale che

$$\begin{cases} x \equiv a \mod r \\ x \equiv b \mod s \end{cases} \tag{1}$$

ma questo è garantito dal **teorema cinese dei resti**: il sistema (1) ha soluzione **unica** $\mod rs$.

Esempio:

$$\begin{cases} 2x \equiv 8 \mod 9 \\ 2x \equiv 6 \mod 15 \end{cases}$$
$$\begin{cases} x \equiv 40 \mod 9 \\ x \equiv 48 \mod 15 \end{cases}$$
$$\begin{cases} x \equiv 4 \mod 9 \\ x \equiv 3 \mod 15 \rightarrow \begin{cases} x \equiv 3 \mod 5 \\ x \equiv 3 \mod 3 \ (*) \end{cases} \end{cases}$$

Sia ha che $x \equiv 0 \mod 3 \Rightarrow 0, 3, 6$ e $(*)$ si può riscrivere come $x = 3k$. Il sistema però non è risolubile.

Teorema di Eulero-Fermat

Ricordiamo prima la **funzione di Eulero**:

$$\phi(n) = |\{x \in \mathbb{N} : 1 \leq x < n,\ (x, n) = 1)\}|$$
$$\phi(rs) = \phi(r)\phi(s) \quad \text{se } (r, s) = 1$$
$$\phi(p^k) = p^k - p^{k-1}$$

e ricordiamo il **piccolo teorema di Fermat**:

$$a^p \equiv a \mod p$$
$$\text{se } (a, p) = 1 \quad a^p \equiv 1 \mod p$$

Teorema: **Teorema di Eulero-Fermat**

Sia $(a, n) = 1$

$$a^{\phi(n)} = 1 \mod n$$

⚠️ Se p è **primo**, $\phi(p) = p - 1$, quindi il **piccolo teorema di Fermat** è un caso speciale di **teorema di Eulero-Fermat**

Dimostrazione: per prima cosa proviamo che se p è **primo** e $p \nmid a$ allora

$$a^{\phi(p^k)} \equiv 1 \mod p^k$$

Procediamo per **induzione su k**:

- $k = 1$, si ottiene il **piccolo teorema di Fermat**
- Supponiamo la tesi vera per k e dimostriamola per $k+1$

$$\begin{aligned} &a^{\phi(p^k)} \equiv 1 \mod p^k, \text{ ovvero} \\ &a^{\phi(p^k)} = 1 + hp^k \\ &\phi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p \cdot \phi(p^k) \end{aligned}$$

dunque

$$\begin{aligned} a^{\phi(p^{k+1})} &= a^{p\phi(p^k)} = (1 + hp^k)^p = \\ &= 1 + \binom{p}{1} hp^k + \binom{p}{2}(hp^k)^2 + ... + \binom{p}{p-1}(hp^k)^{p-1} + (hp^k)^p \equiv 1 \end{aligned}$$

dove tutti gli $hp^k \equiv 0 \mod p^{k+1}$.

In generale, $n = p_1^{h_1}...p_s^{h_s}$

$$\phi(n) = \phi(p_1^{h_1})...\phi(p_s^{h_s}) \; (*)$$

Da quanto già visto risulta

$$a^{\phi(p_i^{h_i})} \equiv 1 \mod p_i^{h_i} \; (\blacksquare)$$

Inoltre da $(*)$ si ha che $\phi(p_i^{h_i}) \mid \phi(n)$.

Elevando ambo i membri per $(\blacksquare)$ alla $\dfrac{\phi(n)}{\phi(p_i^{h_i})}$ otteniamo

$$a^{\phi(n)} \equiv 1 \mod p_i^{h_i}$$

Ma allora $a^{\phi(n)} \equiv 1 \mod \underbrace{p_1^{h_1}...p_s^{h_s}}_{=n}$.

Lezione 12 - 27/10/2022

Definzione - Spazio vettoriale

Uno spazio vettoriale su $\mathbb{K}$ (campo) è un **insieme non vuoto** V dotato di un'**operazione binaria** $+$ rispetto alla quale V è un **gruppo abeliano** e di un'applicazione

$$\begin{gathered} \mathbb{K} \times V \to V \\ (\alpha,\ v) \mapsto \alpha v \end{gathered}$$

tale che

$$\begin{array}{cl} (\alpha+\beta)v = \alpha v + \beta v & \forall \alpha, \beta \in \mathbb{K},\ \forall v \in V \\ (\alpha\beta)v = \alpha(\beta v) & \forall \alpha, \beta \in \mathbb{K},\ \forall v \in V \\ \alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2 & \forall \alpha \in \mathbb{K},\ \forall v_1, v_2 \in V \\ 1v = v & \forall v \in V \end{array}$$

Nomenclatura

- Gli elementi di V si chiamano **vettori**
- Gli elementi di $\mathbb{K}$ si chiamano **scalari**

Esempi

1. Sia $\mathbb{K}$ un campo e $V = \mathbb{K}^n = \{(x_1, ..., x_n) : x_i \in \mathbb{K}\}$
   Prendiamo come esempio $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$

   $$\begin{aligned} &(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n) \\ &\alpha(x_1, ..., x_n) = (\alpha x_1, ..., \alpha x_n) \end{aligned}$$

   Esempio pratico

   $$\begin{aligned} &4(2,1,6) + 5(-1,2,\frac{1}{4}) + \frac{3}{2}(0,1,3) = \\ =&(8,4,24) + (-5,10,\frac{5}{4}) + (0,-\frac{3}{2},-\frac{9}{2}) = (3,\frac{25}{2},\frac{83}{4}) \end{aligned}$$

2. Definzione: Una matrice a m righe e n colonne a **coefficienti nel campo** $\mathbb{K}$ è una tabella di elementi di $\mathbb{K}$ del tipo

$$\begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ \vdots & & a_{ij} & \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix}$$

Chiamiamo $M_{mn}(\mathbb{K})$ tale insieme.
Diciamo che una matrice è **quadrata** se $m = n$

Notazione:

Se $A \in M_{mn}(\mathbb{K})$ denoto con

- $(A)_{ij}$ l'elemento di posto (i, j)
- A^i l'i-esima colonna
- A_j la j-esima riga

Esempio

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 5 & 6 \end{pmatrix}$$
$$(A)_{11} = 1 \quad (A)_{12} = 2 \quad (A)_{13} = 3$$
$$(A)_{21} = 4 \quad (A)_{22} = 5 \quad (A)_{23} = 6$$
$$A^1 = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \quad A^2 = \begin{pmatrix} 2 \\ 5 \end{pmatrix} \quad A^3 = \begin{pmatrix} 3 \\ 6 \end{pmatrix}$$
$$A_1 = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \quad A_1 = \begin{pmatrix} 4 & 5 & 6 \end{pmatrix}$$

$M_{mn}(\mathbb{K})$ è uno **spazio vettoriale** rispetto a

$$\begin{aligned} (A+B)_{ij} = (A)_{ij} + (B)_{ij} \qquad & 1 \le i \le m \\ & 1 \le j \le n \\ \alpha \in \mathbb{K} \quad (\alpha A)_{ij} = \alpha (A)_{ij} \qquad & 1 \le i \le m \\ & 1 \le j \le n \end{aligned}$$

N.B.:

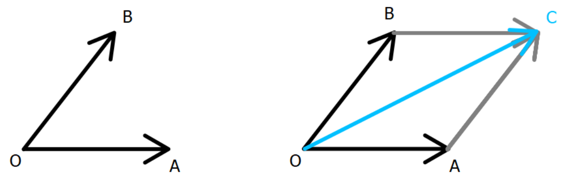
- se $m = n = 1,\ M_{11}(\mathbb{K}) = \mathbb{K}$, dunque ogni campo è uno **spazio vettoriale su se stesso**;
- se $m = 1,\ M_{1n}(\mathbb{K}) = \mathbb{K}^n$, chiamati **vettori riga**;
- se $n = 1,\ M_{m1}(\mathbb{K}) \leftrightarrow \mathbb{K}^m$, chiamati **vettori colonna**.

3. **Vettori geometrici**

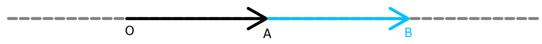
   Consideriamo lo spazio **bidimensionale della geometria euclidea** e fissiamo un punto o. Chiamiamo **vettore** un segmento orientato $\overrightarrow{AB}$. Definiamo una struttura di **spazio vettoriale su** $\mathbb{R}$ sull'insieme ν_0 dei vettori applicati in o.

   $$\nu_0 = \{\overrightarrow{OA} : a \in \mathbb{E}^3\}$$

   - $\overrightarrow{OA} + \overrightarrow{OB} = \overrightarrow{OC}$

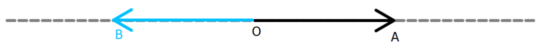


- $0 \cdot \overrightarrow{OA} = \overrightarrow{OO}$
  $\alpha \cdot \overrightarrow{OO} = \overrightarrow{OO}$
  - Se $\alpha > 0$



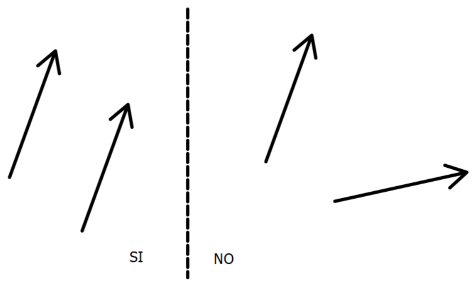
$$\overrightarrow{OB} = \alpha \cdot \overrightarrow{OA}$$

  - Se $\alpha < 0$



$$\overrightarrow{OB} = \alpha \cdot \overrightarrow{OA}$$

Si definiscono poi i **vettori liberi** come lo spazio di vettori applicati modulo la **relazione di equivalenza** che identifica due vettori applicati se esiste una **traslazione** che manda uno all'altro



le operazioni di ν_0 passano al quoziente.

Prodotto righe per colonne tra matrici

Per comodità scrivo M_{mn} invece di $M_{mn}(\mathbb{K})$.

$$M_{ms} \times M_{sn} \to M_{mn}$$
$$(AB)_{ij} = \sum_{k=1}^{s} (A)_{ik} \cdot (B)_{kj}, \quad 1 \leq i \leq m,\ 1 \leq j \leq n$$

Esempio:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 0 & 1 & 4 & -1 \\ 2 & 3 & 0 & 4 \\ 3 & 6 & -1 & -1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1\cdot 0 + 2\cdot 2 + 3\cdot 3 & 1\cdot 1 + 2\cdot 3 + 3\cdot 6 & 1\cdot 4 + 2\cdot 0 + 3\cdot(-1) & 1\cdot(-1) + 2\cdot 4 + 3\cdot(-1) \\ 4\cdot 0 + 5\cdot 2 + 6\cdot 3 & 4\cdot 1 + 5\cdot 3 + 6\cdot 6 & 4\cdot 4 + 5\cdot 0 + 6\cdot(-1) & 4\cdot(-1) + 5\cdot 4 + 6\cdot(-1) \end{pmatrix} =$$

$$= \begin{pmatrix} 13 & 25 & 1 & 4 \\ 28 & 55 & 10 & 10 \end{pmatrix}$$

Proposizone

Se $A \in M_{ms},\ B \in M_{st},\ C \in M_{tn}$

$$(AB)C = A(BC)$$

Osservazione

Nel caso delle matrici quadrate M_n, il prodotto righe per colonne è un'operazione binaria associativa per la proprietà precedente che, per elemento neutro ha la **matrice identità**

$$I_n = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & ... & 1 & 0 \\ 0 & ... & 0 & 1 \end{pmatrix}$$

$(I_n)_{ij} = \delta_{ij}$ dove δ_{ij} è detta la **delta di Krnoecker** ed è definita come segue

$$\delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

ovvero vale 1 solamente nella **diagonale** e tutto il resto è 0.

Proposizione

$M_n(\mathbb{K})$ è un **anello con unità**.
N.B.: se $n \geq 2$, $M_n(\mathbb{K})$ **non è commutativo**

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} -2 & 8 \\ -3 & 18 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 8 \\ 8 & 10 \end{pmatrix}$$

Esempi di gruppi

1. $(\mathbb{Z}, +),\ (\mathbb{Z}_n, +)$
2. $(\nu, +),\ \nu$ spazio vettoriale $(\nu = \mathbb{R},\ \mathbb{Q})$
3. S_n
4. $\mathbb{U}_n$ elementi invertibili in $\mathbb{Z}_n$
5. $(\mathbb{K} \setminus \{0\}, \cdot)$

Domanda

Abbiamo visto che M_n sono **un anello**; possiamo chiederci se $M_n \setminus \{0\}$ è un **gruppo** rispetto il **prodotto righe per colonne**. Questo è vero se per ogni $A \in M_n,\ A \neq 0\ \exists B \in M_n$ tale che

$$AB = BA = I_n \quad (*)$$

Questo in generale è **falso**. Dimostreremo che esiste una funzione detta **determinante**

$$\det : M_n(\mathbb{K}) \to \mathbb{K}$$

tale che

$$A \text{ è invertibile } \iff \det A \neq 0$$

cioè vale $(*)$. Quindi $\{A \in M_n(\mathbb{K}) : \det A \neq 0\}$ è un gruppo **infinito** (se $\mathbb{K}$ è infinito) **non abeliano** se $n \geq 2$.

<u>Esempio</u>:

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

Definizione - Sottogruppo

Sia G un **gruppo**. Diciamo che $\emptyset \neq H \subseteq G$ è un **sottogruppo** di G (notazione: $H \leq G$) se H è un **gruppo rispetto all'operazione indotta da** G**.**

$$\begin{tikzcd} G \times G \arrow[r] & G \\ H \times H \arrow[u, phantom, "\rotatebox{90}{$\subseteq$}"] \arrow[ur] \arrow[r] & H \arrow[u, phantom, "\rotatebox{90}{$\subset$}"] \end{tikzcd}$$

<u>Osservazione</u>: $H \leq G$ se e solo se

1. $\forall h_1, h_2 \in H \qquad h_1 \cdot h_2 \in H$
2. $e \in H$
3. $\forall h \in H,\ h^{-1} \in H$

Proposizione

$$H \leq G \iff ab^{-1} \in H, \quad \forall a, b \in H\ (*)$$

con questa scrittura sono state compattate le tre proprietà sopra.

<u>Nota</u>: in notazione additiva:

$$ab^{-1} \in H \text{ diventa } a - b \in H$$

<u>Dimostrazione</u>: Supponiamo che valgano *1. 2.* e *3.* e vediamo che vale $(*)$.

Dati $a, b \in H$, per la proprietà *3.* si ha $b^{-1} \in H$ e per la *1.* $ab^{-1} \in H$, quindi vale $(*)$.

Supponiamo che valga $(*)$, dobbiamo dimostrare *1. 2.* e *3.*

Prendiamo in $(*)$ $a = b$

$$ab^{-1} = aa^{-1} = e \in H$$

quindi vale *2.* Prendiamo in $(*)$ $a = e,\ b = h$. Abbiamo

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

quindi vale *3.* Infine prendiamo in $(*)$ $a = h_1,\ b = h_2^{-1}$

$$ab^{-1} = h_1(h_2^{-1})^{-1} = h_1 \cdot h_2 \in H$$

quindi vale *1.*

Esempio: **il centro di un gruppo**. Sia G un gruppo. Definiamo

$$Z(G) = \{x \in G : xy = yx\ \forall y \in G\}$$

osserviamo che G è **abeliano** se e solo se $Z(G) = G$ (tutti gli elmenti in G commutano). In generale si ha $Z(G) \leq G$.

Verifichiamolo usando la proposizione precedente: $x, y \in Z(G) \Rightarrow xy^{-1} \in Z(G)$

- **Ipotesi**:

$$\begin{aligned} xg = gx \quad \forall g \in G\ (2) \\ yg = gy \quad \forall g \in G \end{aligned}$$

- **Tesi**: $xy^{-1}g = gxy^{-1} \quad \forall g \in G$

  $yg = gy$ può essere riscritta come

$$\begin{aligned} y^{-1}ygy^{-1} &= y^{-1}gyy^{-1} \quad \text{moltiplico } y^{-1} \text{ a sx e dx} \\ gy^{-1} &= y^{-1}g\ (1) \end{aligned}$$

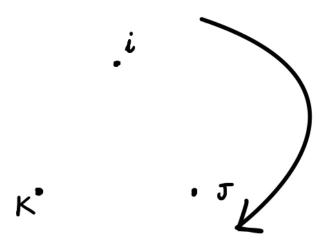
  Da cui si ricava

$$xy^{-1}g = x(y^{-1}g) \overset{(1)}{=} x(gy^{-1}) = (xg)y^{-1} \overset{(2)}{=} (gx)y^{-1} = gxy^{-1}$$

Esempio: Q **:** unità dei **quaternioni**

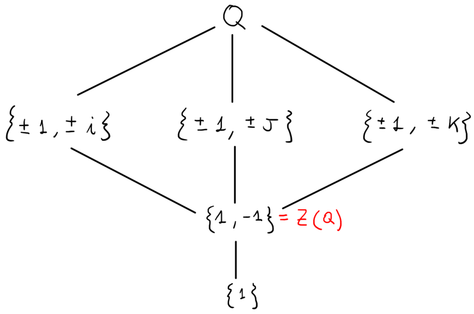
$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

Le regole moltiplicative seguono dal seguente disegno:



- $i^2 = j^2 = k^2 = -1$
- $ij = k \quad jk = i \quad ki = j$
- $ji = -k \quad kj = -i \quad ik = -j$

I **sottogruppi generati** sono i seguenti:



Sottogruppi di Z

Proposizione: i sottogruppi di $\mathbb{Z}$ sono tutti e soli del tipo $n\mathbb{Z},\ n \in \mathbb{N}$.

Dimostrazione: vediamo prima di tutto che $n\mathbb{Z}$ è un sottogruppo. Per la proposizione dobbiamo vedere che se $x, y \in n\mathbb{Z}$, allora $x - y \in n\mathbb{Z}$ (ricordiamo che $\mathbb{Z}$ non + un gruppo rispetto alla moltiplicazione, quindi usiamo la notazione additiva).

Ma $x, y \in n\mathbb{Z}$ significa $x = na,\ y = nb$, per cui

$$x - y = na - nb = n(a - b) \in n\mathbb{Z}$$

Viceversa, sia $H \leq \mathbb{Z}$; se $H = \{0\}$ allora $H = n\mathbb{Z}$ con $n = 0$. Quindi possiamo supporre che esista $h \in H, n \neq 0$; poiché $H \leq \mathbb{Z}$, se $h \in H$, anche $-h \in H$, quindi posso supporre $h > 0$. Sia

$$\emptyset \neq H' = \{h \in H : h > 0\}$$

Quindi esiste $\overline{h} = \min H'$.

Dico che $H = \overline{h}\mathbb{Z}$. È chiaro che $\overline{h}\mathbb{Z} \subseteq H$, perchè $\overline{h} \in H$ e quindi tutti i multipli di $\overline{h}$ appartengono ad H ($H \leq \mathbb{Z}$).

Viceversa, prendo $x \in H$ e scrivo

$$x = q\overline{h} + r \qquad 0 \leq r < h$$

quindi $r = x - q\overline{h}$ e sappiamo che $x \in H$ per ipotesi. Dunque $r \in H$, ma $\overline{h}$ è il **minimo intero positivo** che appartiene ad H, quindi $r = 0$ e quindi

$$x = q\overline{h} \in \overline{h}\mathbb{Z}$$

come volevamo.

Omomorfismo

Siano $G_1,\ G_2$ gruppi. Un **omomorfismo** tra G_1 e G_2 è un'applicazione

$$f : G_1 \to G_2$$

tale che $f(gg') = f(g)f(g'),\ \forall g, g' \in G_1$.

Un **isomorfismo**

$$f : G_1 \to G_2$$

è un **omomorfismo biunivoco**.

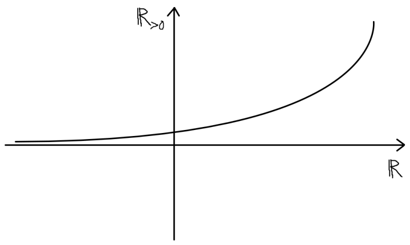
Esempio:

$$f : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$$
$$x \mapsto e^x$$

è un **isomorfismo** in quanto

$$f(x + y) = f(x)f(y)$$
$$e^{x+y} = e^x e^y$$

La **biunivocità** segue dal grafico dell'esponenziale



Lezione 13 - 28/10/2022

Notazione - definizione

Sia G un **gruppo** e $g \in G$. Definiamo le **potenze** come segue

$$g^i = \begin{cases} g^{i-1} \cdot g & \text{se } i > 0 \\ e & \text{se } i = 0 \\ (g^{-1})^{-i-1} \cdot g^{-1} & \text{se } i < 0 \end{cases}$$

Nota: è una definizione induttiva

Osservazione: in notazione additiva si ha

$$\begin{gathered} g^i \to ig \\ g^{-i} \to -ig \end{gathered}$$

> ⚠️ Fare la **potenza** di un elemento x di un gruppo G equivale ad **iterare** a partire da x o da x^{-1} l'operazione del gruppo.

Proposizione

Se H, K sono **sottogruppi** di un gruppo G, anche $H \cap K$ lo è.
Dimostrazione: Per ipotesi

$$\begin{gathered} h_1 h_2^{-1} \in H \quad \forall h_1, h_2 \in H \ (1) \\ k_1 k_2^{-1} \in K \quad \forall k_1, k_2 \in K \ (2) \end{gathered}$$

Siano ora $x,\ y$ elementi qualsiasi di $H \cap K$. Devo dimostrare che

$$xy^{-1} \in H \cap K$$

ma se $x, y \in H \cap K$, in particolare $x, y \in H$ quindi per (1) $xy^{-1} \in H$ e $x, y \in K$, quindi per (2) $xy^{-1} \in K$. Dunque $xy^{-1} \in H \cap K$.

Osservazione: L'enunciato vale per una qualsiasi **famiglia di sottogruppi** di G

$$\alpha \in A \quad H_\alpha \leq G \Longleftrightarrow \bigcap_{\alpha \in A} H_\alpha \leq G$$

Definizione - Sottogruppo generato

Sia G un **gruppo** e $X \leq G$. Si definisce **sottogruppo generato da** X l'insieme

$$< X >= \bigcap_{X \subseteq H \leq G} H$$

Caso speciale (importante): $X = \{g\}$ allora

$$< g >= \{g^i : i \in \mathbb{Z}\}$$

e prende il nome di **sottogruppo ciclico generato da** g**.**

Proposizione

Sia $X = \{x_1, x_2, ...\} \leq G$. Allora

$$< x >= \{t_1 \cdot ... \cdot t_r : r \in \mathbb{N},\ t_i \in X \text{ oppure } t_i^{-1} \in X\}$$

Idea: per generare un gruppo a partire dagli elementi di X devo prendere **tutti i possibili prodotti di elementi di** X **e dei loro inversi**.

Esempio: in $\mathbb{Z}$

$$< 2, 3 >= \{2s + 3t : s, t \in \mathbb{Z}\} = \mathbb{Z}$$

Definizione - Gruppo ciclico

Un **gruppo** G si dice **ciclico** se $\exists g \in G : G =< g >$.

Esempi:

1. $(\mathbb{Z}, +)$ è **ciclico**, generato da 1

$$n = n \cdot 1$$

Nota: anche -1 genera $\mathbb{Z}$ e **nessun altro intero** lo genera.

2. $(\mathbb{Z}_n, +)$ è ciclico, generato da $\bar{1}$

$$\bar{n} = n \cdot \bar{1}$$

Dimostreremo che $\mathbb{Z}_n$ ha $\phi(n)$ generatori.

Esempio:

- $\mathbb{Z}_6$ ha $\phi(6) = \phi(3)\phi(2) = 2$ generatori
- $\mathbb{Z}_8$ ha $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$ generatori. Verifica:

$$\begin{aligned}
&< \bar{0} > = \{\bar{0}\} \\
&< \bar{1} > = \mathbb{Z}_8 \\
&< \bar{2} > = \{\bar{2}, \bar{4}, \bar{6}, \bar{0}\} \\
&< \bar{3} > = \{\underbrace{\bar{3}, \bar{6}}_{+3}, \bar{1}, \bar{4}, \bar{7}, \bar{2}, \bar{5}, \bar{0}\} = \mathbb{Z}_8 \\
&< \bar{4} > = \{\bar{4}, \bar{0}\} \\
&< \bar{5} > = \{\underbrace{\bar{5}, \bar{2}}_{+5}, \bar{7}, \bar{4}, \bar{1}, \bar{6}, \bar{4}, \bar{0}\} = \mathbb{Z}_8 \\
&< \bar{6} > = \{\bar{6}, \bar{4}, \bar{2}, \bar{0}\} \\
&< \bar{7} > = \{\bar{7}, \bar{6}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}, \bar{0}\} = \mathbb{Z}_8
\end{aligned}$$

3. $(\mathbb{R} \setminus \{0\}, \cdot) \geq \{\pm 1\} \cong \mathbb{Z}_2$ ($\cong$ è il simbolo che indica un **isomorfismo**). Sia

$$\begin{aligned}
\phi : \{\pm 1\} &\to \mathbb{Z}_2 \\
1 &\mapsto \bar{0} \\
-1 &\mapsto \bar{1}
\end{aligned}$$

Si ha che

$$
\begin{gathered}
\phi(1 \cdot 1) = \phi(1) + \phi(1) = \bar{0} + \bar{0} \\
\phi(1 \cdot (-1)) = \phi(1) + \phi(-1) = \bar{0} + \bar{1} = \bar{1} \\
\phi((-1) \cdot (-1)) = \phi(-1) + \phi(-1) = \bar{1} + \bar{1} = \bar{0}
\end{gathered}
$$

Definzione - Ordine

L'**ordine** di $g \in G$, denotato con $o(g)$, è il **minimo intero positivo**, se esiste, tale che

$$
g^n = e
$$

se tale n **non esiste**, si pone $o(g) = +\infty$.

Osservazione: in altri termini

$$
o(g) = | < g > |
$$

in particolare G è **ciclico se e solo se esiste** $g \in G$, con $o(g) = |G|$

Osservazione: se G è **ciclico**, allora è **abeliano**. Infatti, se $G =< g >,\ x, y \in G$

$$
\begin{gathered}
x = g^i,\ y = g^j \\
xy = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = yx
\end{gathered}
$$

Il viceversa **non è vero**.

Esempio: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}$

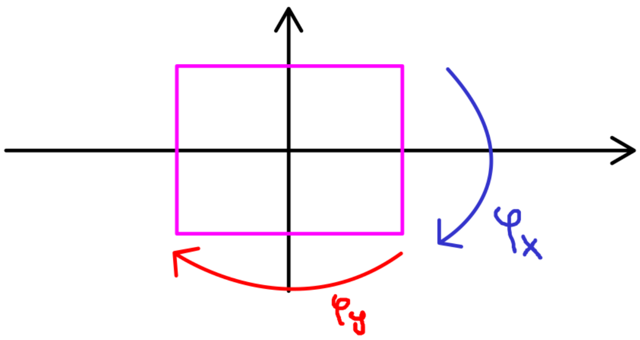
$$
\begin{gathered}
< (\bar{0}, \bar{0}) > = \{(\bar{0}, \bar{0})\} \\
< (\bar{1}, \bar{0}) > = \{(\bar{1}, \bar{0}), (\bar{0}, \bar{0})\} \\
< (\bar{0}, \bar{1}) > = \{(\bar{0}, \bar{1}), (\bar{0}, \bar{0})\} \\
< (\bar{1}, \bar{1}) > = \{(\bar{1}, \bar{1}), (\bar{0}, \bar{0})\}
\end{gathered}
$$

Quindi tutti gli elmento diversi da $e = \{(\bar{0}, \bar{0})\}$ hanno ordine 2, quindi nessuno di essi ha ordine 4 e quindi il **gruppo non è ciclico**.

Il gruppo è chiaramente **abeliano**, ma **non è ciclico**.

Nota

Il gruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$ è **isomorfo** al cosiddetto **gruppo di Klein**, delle **simmetrie di un rettangolo** con non è un quadrato:



$$
\begin{gathered}
V = \{Id, \phi_x, \phi_y, \phi_o\} \\
\phi_x(x, y) = (x, -y) \\
\phi_y(x, y) = (-x, y) \\
\phi_o(x, y) = (-x, -y)
\end{gathered}
$$

<u>Osservazione</u>: abbiamo due gruppi di ordine 4 **non isomorfi** $\mathbb{Z}_4$ e V: il primo è **ciclico** mentre il secondo **non è ciclico**.

Proposizione

Sia G un **gruppo** e $g \in G$. Se $o(g) = +\infty$, allora $g^h \neq g^k$ per $h \neq k$. Se invece $o(g) = n$ allora

$$< g >= \{e, g, ..., g^{n-1}\}$$

e $g^h = g^k$ sse $h \equiv k \mod n$.

<u>Dimostrazione</u>: Supponiamo $o(g) = +\infty$ e $g^h = g^k$. Allora

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

Se $o(g) = n$, per definizione $e, g, ..., g^{n-1}$ sono **elementi distinti del sottogruppo** $< g >$ (se fosse $g^i = g^j, \ 1 \leq i \leq j < n$ avremmo $g^{i-j} = e$ con $i - j < n$ contro la definzione di $o(g)$).

Dunque basta vedere che ogni potenza di g è nella lista $\{e, g, ..., g^{n-1}\}$.

Consideriamo $g^s, \ s \in \mathbb{Z}$; $s = qn + r \quad 0 \leq r < n$

$$g^s = g^{qn+r} = g^{qn} g^r = (g^n)^q g^r = e^q g^r = eg^r = g^r \quad 0 \leq r \leq n-1$$

Supponiamo ora $g^h = g^k$

$$g^{h-k} = e \qquad h-k = q'n + r' \quad 0 \leq r' \leq n-1$$
$$g^{h-k} = g^{q'n+r'} = g^{r'} \Rightarrow r' = 0$$

ovvero $h - k = q'n$ ovvero $h \equiv k \mod n$.

Viceversa, $h \equiv k \mod n,\ h = k + tn$

$$g^h = g^{k+tn} = g^k g^{tn} = g^k (g^n)^t = g^k e^t = g^k e = g^k$$

Lezione 14 - 03/11/2022

Reminescenze gruppo ciclico

Ricordiamo che un gruppo G si dice ciclico se $\exists g \in G : G =< g >$.

Esempi:

1. $\mathbb{Z} =< 1 >$
2. $\mathbb{Z}_n =< \bar{1} >$
3. $\mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico

Osservazione: G ciclico $\Rightarrow G$ abeliano, ma non è vero il viceversa (come nell'esempio 3.).

Proposizione 1

Ogni sottogruppo di un gruppo ciclico G è **ciclico**.

Dimostrazione: sia $G =< g >$ e $H \leq G$.

Se $H = \{e\}$, allora $H =< e >$ quindi è **ciclico**.

Supponiamo $H \neq \{e\}$, quindi esiste $g^i \in H, i \neq 0$. Siccome $H \leq G$, se $g^i \in H$ anche $g^{-i} \in H$. Pertanto $\{i \in \mathbb{N} : g^i \in H\} \neq \emptyset$ e quindi **ammette minimo**, chiamiamolo m.

Dico che $H =< g^m >$. Poichè $g^m \in H$, $g^{km} \in H \ \forall k \in \mathbb{Z}$ (perché $H \leq G$), quindi $< g^m > \subseteq H$. Devo dimostrare l'inclusione contraria.

Sia $g^t \in H$

$$\begin{gathered} t = qm + r, \quad 0 \leq r < m \\ g^t = g^{qm+r} = g^{qm} g^r \\ g^r = g^t g^{-qm} \in H \end{gathered}$$

Per la **minimalità di** m segue che $r = 0$. Dunque $t = qm$ e quindi $g^t \in < g^m >$, che è quanto volevamo.

Proposizione 2

Sia $G =< g >$ un **gruppo ciclico finto** di ordine n. Allora

a. $H \leq G, \ |H| \mid n$ (la cardinalità di H divide n)

b. Se $k \mid |G|$, esiste **un unico** $H \leq G, \ |H| = k$

Dimostrazione a.: Sia $H \leq G$; per la $\text{prop } 1.\ H =< g^m >$;

$$(g^m)^n = (g^n)^m = e^m = e$$

quindi $o(g^m) \mid n$, dove $g^m = |H|$ e $n = |G|$ (in generle se $g^k = e \Rightarrow o(g) \mid k$).

Dimostrazione b.: Sia $k \mid n$; allora $| < g^{\frac{n}{k}} > | = k$.

Facciamo vedere che $< g^{\frac{n}{k}} >$ è l'**unico** sottogruppo di ordine k. Sia H un altro tale sottogruppo; $H =< g^h >$ dove h è il **minimo intero positivo** tale che $g^h \in H$

$$|H| = k = | < g^h > | = \frac{n}{h}$$

dunque $h = \frac{n}{k}$ e $H =< g^{\frac{n}{k}} >$.

Proposizione: Se $g \in G$ ha ordine finito n, allora

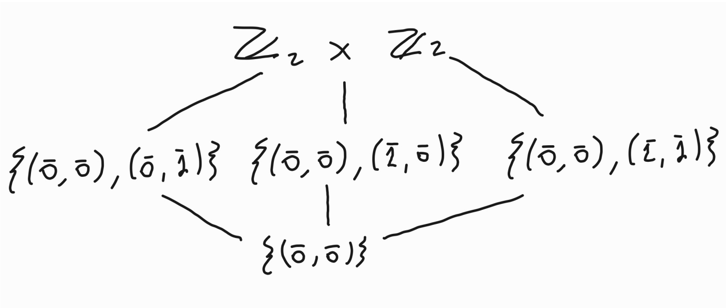
$$o(g^k) = \frac{n}{(n, k)}$$

Corollario delle prop 1. e 2.: Il **reticolo dei sottogruppi** di un gruppo cicliclo di ordine n è **isomorfo al reticolo dei divisori di** n.

Esempio: POSET dei sottogruppi di un gruppo:

$$H_1, H_2 \leq G \qquad H_1 \preccurlyeq H_2 \Leftrightarrow H_1 \subseteq H_2$$

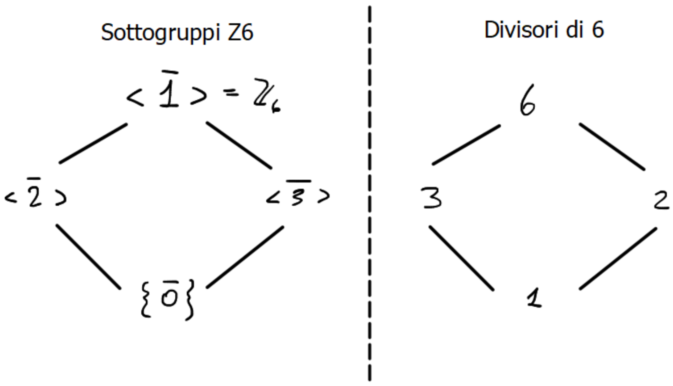
- $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}$



$\mathbb{Z}_6 =< \bar{1} >$

Abbiamo visto che il sottogruppo di ordine k è generato da $g^{\frac{n}{k}}$

n	k		
6	6	$\bar{1}$	
	3	$\bar{2}$	$< \bar{2} >= \{\bar{2}, \bar{4}, \bar{0}\}$
	2	$\bar{3}$	$< \bar{3} >= \{\bar{3}, \bar{0}\}$
	1	$\bar{0}$	



Proposizione 3

Sia $G =< g >$ un **gruppo ciclico** di ordine n. Allora $< g^i >$ genera G se e solo se $(i, n) = 1$.

<u>Dimostrazione</u>: g^i genera G se e solo se $o(g^i) = n$

$$n = o(g^i) = \frac{n}{(n,i)} \iff (n, i) = 1$$

Gruppo simmetrico

$$S_n = \{f : \{1, ..., n\} \to \{1, ..., n\} | f \text{ è biunivoca}\}$$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Per scrivere le permutazioni in modo più conveniente, introduciamo, fissata $\sigma \in S_n$, una **relazione di equivalenza** su $\{1, ..., n\}$

$$i \equiv_\sigma j \iff \exists k \in \mathbb{Z} : i = \sigma^k(j)$$

Esempio:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 3 & 2 & 5 & 4 & 7 & 9 & 8 & 6 & 1 \end{pmatrix}$$

$$\begin{aligned} &1 \equiv_\sigma 10 \\ &2 \equiv_\sigma 3 \\ &4 \equiv_\sigma 5 \\ &6 \equiv_\sigma 7 \equiv_\sigma 9 \\ &8 \equiv_\sigma 8 \end{aligned}$$

quindi si ha che

$$\sigma = (1, 10)(2, 3)(4, 5)(6, 7, 9)$$

Tale rappresentazione viene chiamata **rappresentazione in cicli disgiunti.**

⚠️ Gli elementi in σ che restano fissati, come in questo caso l'8, non vengono riportati nella rappresentazione in cicli disgiunti.

Verifichiamo ora che $\equiv_\sigma$ è di equivlenza:

- **Riflessiva**: $i \equiv_\sigma i$ ovvio perché $i = \sigma^0(i)$
- **Simmetrica**: $i \equiv_\sigma j \Rightarrow j \equiv_\sigma i$. Vera in quanto $\exists k : i \in \sigma^k(j)$ e $j = \sigma^{-k}(i)$.
- **Transitiva**: $i \equiv_\sigma j,\ j \equiv_\sigma k \Rightarrow i \equiv_\sigma k$.

$$\begin{gathered} \exists t : i = \sigma^t(j) \\ \exists s : j = \sigma^s(k) \\ i = \sigma^t(j) = \sigma^t(\sigma^s(k)) = \sigma^{t+s}(k) \end{gathered}$$

  quindi $i \equiv_\sigma k$.

Definizione

Data $\sigma \in S_n$, un **ciclo** di σ è l'insieme ordinato

$$(x, \sigma(x), \sigma^2(x), ..., \sigma^{m-1}(x))$$

due cicli si dicono **disgiunti** se lo sono come insiemi.

Osservazione: possiamo interpretare un ciclo come la permutazione

$$x \mapsto \sigma(x), \sigma(x) \mapsto \sigma^2(x), ..., \sigma^{m-1}(x) \mapsto x$$

Esempio:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 3 & 2 & 7 & 1 & 4 \end{pmatrix} = (1,8,3,6,7)(2,5)$$

Esempio: trasformazione di cicli non disgiunti in cicli disgiunti

$$(1,2,3,4)(2,6,4,8)(8,7,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 3 & 8 & 5 & 1 & 4 & 7 \end{pmatrix} = (1,2,6)(4,8,7)$$

Procediemento:

- Inizio dall'1 e lo faccio scorrere attraverso i vari cicli (non disgiunti) da **destra verso sinistra** e vedo dove va a finire:
  1. Nel ciclo $(8,7,3)$ l'1 non viene mappato da nessuna parte;
  2. Nel ciclo $(2,6,4,8)$ l'1 non viene mappato da nessuna parte;
  3. Nel ciclo $(1,2,3,4)$ l'1 viene mappato in 2, i cicli sono finiti e quindi nella permutazione avremo $\sigma(1) = 2$.
- Passo al 2 e faccio lo stesso procedimento:
  1. Nel ciclo $(8,7,3)$ il 2 non viene mappato da nessuna parte;
  2. Nel ciclo $(2,6,4,8)$ il 2 viene mappato in 6, quindi ora nel prossimo ciclo dovrò controllare il 6 dove verrà mappato;
  3. Nel ciclo $(1,2,3,4)$ il 6 non viene mappato da nessuna parte, i cicli sono finiti e quindi avremo $\sigma(2) = 6$.
- Passo al 3:
  1. Nel ciclo $(8,7,3)$ il 3 viene mappato in 8;
  2. Nel cilclo $(2,6,4,8)$ l'8 viene mappato in 2;

3. Nel ciclo $(1,2,3,4)$ il 2 viene mappato in 3, quindi $\sigma(3)=3$.

- …

Infine vengono scritti i cicli disgiunti partendo dalla permutazione ottenuta.

Proposizione - Permutazione prodotto di cicli

Ogni permutazione è **prodotto dei suoi cicli**.

Dimostrazione: sia $\sigma \in S_n$ e siano $\gamma_1, ..., \gamma_k$ i suoi cicli. Poiché $\equiv_\sigma$ è una **relazione di equivalenza**, pensando i cilci come **insiemi** si ha

$$\bigcup_{i=1}^{k} \gamma i = \{1, ..., n\} \quad \gamma_i \cap \gamma_j = \emptyset,\ i \neq j$$

Dobbiamo far vedere che se penso $\gamma_1, ..., \gamma_k$ come **permutazioni** allora $\sigma = \gamma_1, ..., \gamma_k$, ovvero

$$\sigma(x) = (\gamma_1, ..., \gamma_k)(x)\ \forall x \in \{1, ..., n\}$$

Ora, ogni $x \in \{1, ..., n\}$ compare in **uno solo** dei cicli $\gamma_1, ..., \gamma_k$. Sia questo ciclo $\gamma_i = (x, \sigma(x), ..., \sigma^{m-1}(x))$. Per ogni $j \neq i$ e per ogni $y = \sigma^h(x)$ (ovvero per ogni y che compare nella scrittura di γ_i) risulta

$$\gamma_i(y) = y$$

dunque, $\forall x \in \{1, ..., n\}$

$$(\gamma_1, ..., \gamma_k)(x) = (\gamma_1, ..., \gamma_i)(x) = \gamma_1 ..., \gamma_{i-1}(\sigma(x)) = \sigma(x)$$

quindi $\sigma = \gamma_1, \gamma_2, ..., \gamma_k$.

Proposizione - Ordine di una permutazione

Se $\sigma = \gamma_1 ... \gamma_k$ è la **decomposizione in cicli disgiunti** di σ e γ_i ha lunghezza m_i, allora

$$o(\sigma) = \mathrm{m.c.m}\{m_1, ..., m_k\}$$

Dimostrazione: Ovvio dalla **definizione di ordine** e dal fatto che i cicli disgiunti **commutano**. Sia m_i l'ordine dell'i-esimo ciclo e $S = \mathrm{m.c.m}(m_1, ..., m_k)$ si ha che

$$\sigma^S = (\gamma_1, ..., \gamma_k)^S = \gamma_1^S ... \gamma_k^S$$

Esempi:

1. Calcolare l'ordine di

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix}$$

   Riportiamo σ in notazione in cicli disgiunti:

$$\sigma = (1,2,3)(4,5,6,8)$$

   quindi $o(\sigma) = \text{m.c.m}(3,4) = 12$.

2. Calcolare l'ordine di

$$\sigma = (1,2,3)(2,3,4)(3,4,5)$$

   Attenzione: non è 3 in quanto i cicli **non sono disgiunti**! Riportiamo σ in notazione in cilci disgiunti:

$$\sigma = (1,2)(4,5)$$

   quindi $o(\sigma) = \text{m.c.m}(2,2) = 2$.

Notazione

I cicli di lunghezza m vengono chiamati m-cicli. I cicli di lunghezza 2 vengono chiamati **trasposizioni**.

Porposizione- Ciclo prodotto di trasposizioni

Ogni **ciclo** è **prodotto di trasposizioni**. In particolare, S_n è generato dalle trasposizioni.

Dimostrazione: ogni ciclo si può scrivere come prodotto di trasposizioni, ad esempio

$$(1,2,...,n) = (1,n)(1,n-1)(1,n-2)...(1,3)(1,2)$$

Ora **ogni permutazione è prodotto di cicli** e **ogni ciclo è prodotto di trasposizioni**, quindi **ogni permutazione è prodotto di trasposizioni**.

Osservazione: La scrittura come prodotto di trasposizioni non è unica

$$(1,3) = (1,2)(2,3)(1,2) = (2,3)(1,2)(2,3)$$

Teorema

Se $\sigma = \tau_1...\tau_k = \tau'_1...\tau'_h$ con τ_i, τ'_j trasposizioni, allora $h \equiv k \mod z$.

Definizione - Parità delle permutazioni

Diciamo che σ è **pari** se si scrive come **prodotto di un numero pari di trasposizioni**, **dispari** altrimenti.

Esercizio: determinare ordine e parità della seguente permutazione

$$\sigma = (1,4,7,8)(2,9,7,6)(4,3,1,7)(2,9,5)$$

riportiamola in notazione in cicli disgiunti

$$\sigma = (1,6,2,8)(3,4)(5,9) \quad (*)$$

da cui deduciamo che $o(\sigma) = \text{m.c.m}(4,2,2) = 4$. Ora riportiamo i cicli disgiunti in prodotti di trasposizioni:

$$\sigma = (1,8)(1,2)(1,6)(3,4)(5,9)$$

da cui deduciamo che è **dispari**.

Definizione - Partizione di un numero naturale

Una **partizione** di $n \in \mathbb{N}$ è una sequenza di interi $\lambda_1 \geq ... \geq \lambda_k \geq 1$ tali che

$$\sum_{i=1}^{k} \lambda_i = n$$

Chiamiamo con $p(n)$ il **numero di partizioni** di n. Si ha che

$$\begin{array}{llllllll}
p(1) = 1 & & & & & & & \\
p(2) = 2 & 2 & 11 & & & & & \\
p(3) = 3 & 3 & 21 & 111 & & & & \\
p(4) = 5 & 4 & 31 & 22 & 211 & 1111 & & \\
p(5) = 7 & 5 & 41 & 32 & 311 & 221 & 2111 & 11111
\end{array}$$

Definizione - Struttura ciclica di una permutazione

Osserviamo che una permutazione di S_n individua, tramite la **decomposizione in cicli disgiunti**, una partizione di n che è detta **struttura ciclica** della permutazione.

La **struttura ciclica** della σ precedente $(*)$ è: 4221.

Esempio: $p(5) = 7$

		ordine	parità
5	$(1,2,3,4,5)$	5	p
41	$(1,2,3,4)$	4	d
32	$(1,2,3)(4,5)$	6	d
311	$(1,2,3)$	3	p
221	$(1,2)(3,4)$	2	p
2111	$(1,2)$	2	d
11111	id	1	p

Relazione coniugio

Ricordiamo che in un gruppo qualsiasi due elementi g_1, g_2 si dicono **coniugati** se esiste $g_3 \in G$:

$$g_1 = g_3 g_2 g_3^{-1}$$

Teorema

$\sigma, \tau \in S_n$ sono **coniugate** se e solo se hanno la **stessa struttura ciclica**.

Idea della dimostrazione: $\tau\sigma\tau^{-1}$ si ottiene dalla decomposizione in cicli disgiunti di σ sostituendo ad a la cifra $\tau(a)$.

$$\sigma = (a,b,c,d)(e,f)(g,h)$$
$$\tau\sigma\tau^{-1} = (\tau(a),\tau(b),\tau(c),\tau(d))(\tau(e),\tau(f))(\tau(g),\tau(h))$$

Esempio:

$$\sigma = (1,2,3,4)(5,6)(7,8)$$
$$\sigma' = (2,4,6,8)(7,1)(3,5)$$

> ⚠️ Notare che σ e σ' hanno la **stessa struttura ciclica**: 422

una permutazione τ che **conigua** σ in σ' è

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 7 & 1 & 3 & 5 \end{pmatrix}$$

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

$$\begin{aligned} \tau\sigma\tau^{1} &= (1,7)(2,4,6,8)(3,5) = \\ &= (2,4,6,8)(7,1)(3,5) = \sigma' \end{aligned}$$

⚠️ Ricordiamo che per risolvere questo tipo di esercizio si procede applicando le permutazioni da **destra verso sinistra**, quindi prima applico τ^{-1} e vedo dove viene mappato ogni elemento che man mano viene scelto, poi applico σ ed infine τ.
Ricordiamo inoltre che τ^{-1} vuol dire **leggere la permutazione al contrario**, quindi ogni elemento all'interno di un ciclo viene mappato in quello che si trova alla sua sinistra e non destra.

Lezione 15 - 04/11/2022

Osservazione - Il sottogruppo alterno

La mappa $\epsilon : S_n \to \{\pm 1\}$ definita come

$$\epsilon(\sigma) = \begin{cases} 1 & \sigma \text{ è pari} \\ -1 & \sigma \text{ è dispari} \end{cases}$$

è un **omomorfismo** di gruppi; questo è equivalente a dire che il **prodotto** di due permutaizioni pari **è pari** così come il prodotto di una permutazione pari ed una dispari e il prodotto di una permutazione dispari ed una pari **è dispari**. A sua volta questo segue dalle definizioni.

Esempio:

$$\sigma = \tau_1 ... \tau_6 \qquad \sigma' = \tau_1' ... \tau_8' \qquad \tau_i, \tau_j' \text{ trasposizioni}$$
$$\sigma\tau = \underbrace{\tau_1 ... \tau_6 \tau_1' ... \tau_8'}_{14 \text{ trasposizioni}}$$

In particolare

$$A_n = \{\sigma \in S_n : \sigma \text{ è pari}\}$$

è un sottogruppo di S_n e prende il nome di **sottogruppo alterno**.

Lemma - Cardinalità del sottogruppo alterno

$|A_n| = \frac{n!}{2}$ (ovvero sono metà pari e metà dispari)

Dimostrazione: basta costruire una **corrispondenza biunivoca**

$$\Phi : A_n \to \{\sigma \in S_n | \sigma \text{ è dispari}\}$$

Questo conclude perché se $a = |A_n|$

$$n! = a + |\{\sigma \in S_n : \sigma \text{ è dispari}\}| = 2a \Longrightarrow a = \frac{n!}{2}$$

Sia τ una permutazione **dispari fissata**

$$\Phi(\sigma) = \sigma\tau$$

$\Phi(\sigma)$ è dispri, perchè σ è pari, quindi Φ è effettivamente un'applicazione

$$A_n \to \{\sigma \in S_n : \sigma \text{ è dispari}\}$$

- Φ è **iniettiva**:

$$\begin{aligned} \Phi(\sigma) &= \Phi(\sigma') \\ \sigma\tau &= \sigma'\tau \\ \sigma\tau\tau^{-1} &= \sigma'\tau\tau^{-1} \\ \sigma &= \sigma' \end{aligned}$$

- Φ è **suriettiva**: $\alpha \in S_n$ dispari, $\alpha\tau^{-1} \in A_n$ e

$$\Phi(\alpha\tau^{-1}) = \alpha\tau^{-1}\tau = \alpha$$

Esercizio sulla relazione coniugio

Siano $\sigma = (1,5)(2,3,4)$ e $\tau = (1,4,3)(2,6,7,5)$

$$\tau\sigma\tau^{-1} = (\tau(1), \tau(1))(\tau(2), \tau(3), \tau(4)) = (4,2)(6,1,3)$$

derivata nel seguente modo

$$\begin{aligned}\tau\sigma\tau^{-1} : &1 \to 3 \to 4 \to 3\\ &2 \to 5 \to 1 \to 4\\ &3 \to 4 \to 2 \to 6\\ &4 \to 1 \to 5 \to 2\\ &5 \to 7 \to 7 \to 5\\ &6 \to 2 \to 3 \to 1\\ &7 \to 6 \to 6 \to 7\end{aligned}$$

Calcolare τ tale che $\tau\sigma\tau^{-1} = \mu$ dove

$$\sigma = (1,2,3)(4,7,8)$$
$$\tau = (3,4,9)(5,2,1)$$

$$\begin{aligned}\tau\sigma\tau^{-1} &= (\tau(1),\tau(2),\tau(3))(\tau(4),\tau(7),\tau(8)) =\\ &= \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 3 & 4 & 9 & 5 & 6 & 7 & 2 & 1 & 8\end{pmatrix}\end{aligned}$$

> ℹ️ In quanto in σ non sono presenti $5, 6$ e 9, in $\tau\sigma\tau^{-1}$ possono essere messi uno dei valori rimanenti a caso.

Lemma - Gli r-cicli di Sn

In S_n gli r-cicli sono

$$\frac{1}{r} \cdot \frac{n!}{(n-r)!}$$

<u>Dimostrazione</u>: Il **primo numero** del ciclo lo posso scegliere in n modi, **il secondo** in $n-1$, il terzo in $n-2$ …. l'r**-esimo** in $n-r+1$ modi. In totale

$$n(n-1)...(n-r+1) = \frac{n!}{(n-r)!}$$

Però ognuno dei cicli ottenuti in questo modo viene **contato r volte** (ci sono ripetizioni):

$$(1,2,...,r) = (2,3,...,r,1) = (3,4,...,r,1,2)....$$

Ad esempio in S_n ci sono $\binom{n}{2}$ trasposizioni.

Classi laterali e teorema di Lagrange

Sia G un gruppo e $H \leq G$; definiamo **due relazioni di equivalenza** ρ_d, ρ_s su G:

$$a\rho_d b \iff ab^{-1} \in H$$
$$a\rho_s b \iff b^{-1}a \in H$$

1. ρ_d, ρ_s sono relazioni di equivalenza
   - **Riflessiva**: $a\rho_d a \qquad aa^{-1} \in H \qquad e \in H$
   - **Simmetrica**: $a\rho_d b \Rightarrow b\rho_d a$

   $$ab^{-1} \in H \qquad (ab^{-1})^{-1} \in H$$
   $$(ab^{-1})^{-1} = ba^{-1} \Leftrightarrow b\rho_d a$$

   - **Transitiva**: $a\rho_d b,\ b\rho_d c \Rightarrow a\rho_d c$. Si ha che $ab^{-1} \in H$ e $bc^{-1} \in H$ e si ha che $H \leq G$.

   $$(ab^{-1})(bc^{-1}) \in H$$
   $$(ab^{-1})(bc^{-1}) = abb^{-1}c^{-1} = ac^{-1} \Leftrightarrow a\rho_d c$$

2. $\rho_d = \rho_s$ se G è **abeliano**.
3. Esempio: $G = \mathbb{Z}$ e $H = n\mathbb{Z}$. Sia $\rho = \rho_d = \rho_s$

   $$a\rho b \Leftrightarrow ab^{-1} \in H \to a - b \in n\mathbb{Z}$$

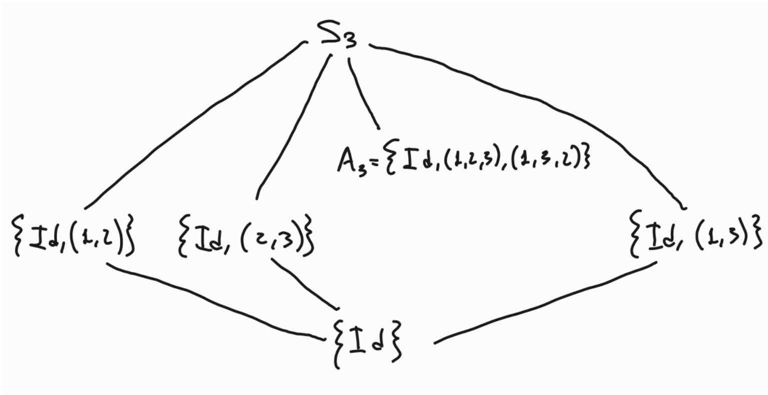
   che implica che ρ è precisamente la **congruenza mod n**.
4. Struttura delle **classi di equivalenza**
   - Classe **laterale destra** di $a \bmod H$

   $$\begin{aligned}\{b \in G : b\rho_d a\} &= \{b \in G : ba^{-1} \in H\} \\ &= \{b \in G : ba^{-1} = h \text{ per qualche } h \in H\} \\ &= \{b \in G : b = ha \text{ per qualche } h \in H\} \\ &= Ha \leftarrow \text{classe laterale destra di } a \bmod H\end{aligned}$$

   - Classe **laterale sinistra** di $a \bmod H$

$$
\begin{aligned}
\{b \in G : b\rho_s a\} &= \{b \in G : a^{-1}b \in H\} \\
&= \{b \in G : a^{-1}b = h \text{ per qualche } h \in H\} \\
&= \{b \in G : b = ah \text{ per qualche } h \in H\} \\
&= aH \leftarrow \text{classe laterale sinistra di } a \bmod H
\end{aligned}
$$

<u>Esempio</u>: $S_3 = \{Id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$



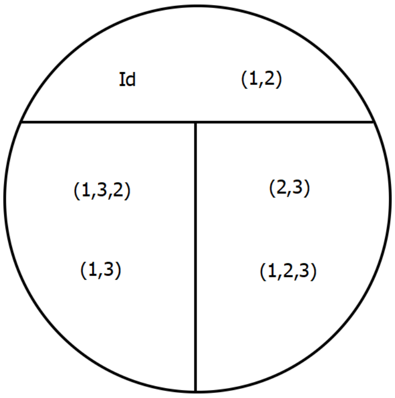
Poniamo $H = \{Id, (1,2)\}$ e troviamo le **classi laterali destre** e **sinistre** di $S_3 \bmod H$:

$$
\begin{aligned}
HId &= H \\
H(1,2) &= \{Id \cdot (1,2), (1,2)(1,2)\} = \{(1,2), Id\} = H \\
H(2,3) &= \{Id \cdot (2,3), (1,2)(2,3)\} = \{(2,3), (1,2,3)\} \\
H(1,3) &= \{Id \cdot (1,3), (1,2)(1,3)\} = \{(1,3), (1,3,2)\} \\
H(1,2,3) &= \{Id \cdot (1,2,3), (1,2)(1,2,3)\} = \{(1,2,3), (2,3)\} \\
H(1,3,2) &= \{Id \cdot (1,3,2), (1,2)(1,3,2)\} = \{(1,3,2), (1,3)\}
\end{aligned}
$$

Quindi si ha che

- $H = H(1,2)$
- $H(2,3) = H(1,2,3)$
- $H(1,3) = H(1,3,2)$

Che formano la seguente **partizione** di S_3:



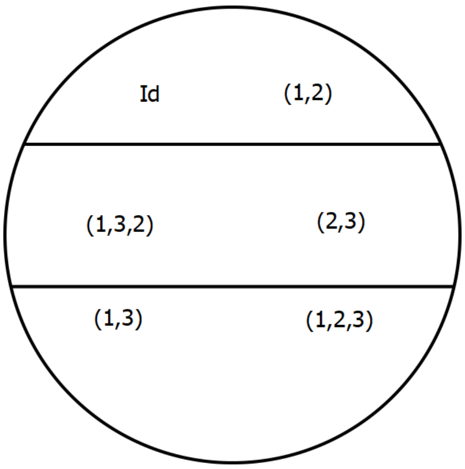
Passiamo ora alle **classi laterali sinistre**:

$$
\begin{aligned}
IdH &= H \\
(1,2)H &= \{(1,2)\cdot Id, (1,2)(1,2)\} = H \\
(2,3)H &= \{(2,3)\cdot Id, (2,3)(1,2)\} = \{(2,3),(1,3,2)\} \\
(1,3)H &= \{(1,3)\cdot Id, (1,3)(1,2)\} = \{(1,3),(1,2,3)\} \\
(1,2,3)H &= \{(1,2,3)\cdot Id, (1,2,3)(1,2)\} = \{(1,2,3),(1,3)\} \\
(1,3,2)H &= \{(1,3,2)\cdot Id, (1,3,2)(1,2)\} = \{(1,3,2),(2,3)\}
\end{aligned}
$$

Quindi si ha che

- $(1,2)H = H$
- $(2,3)H = (1,3,2)H$
- $(1,3)H = (1,2,3)H$

Che formano la seguente **partizione** di S_3:



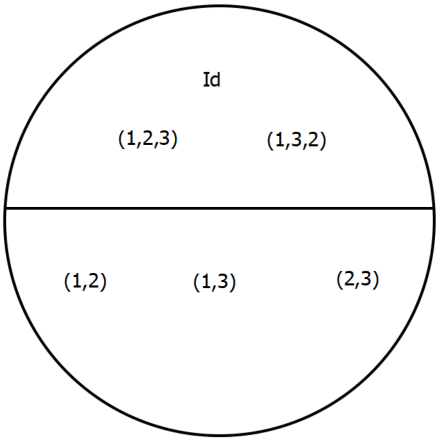
Sia ora $H = \{Id, (1,2,3), (1,3,2)\}$. Poichè H è un sottogruppo

$$H = H(1,2,3) = H(1,3,2) = (1,2,3)H = (1,3,2)H$$

Calcoliamo ora le **classi laterali destre**:

$$\begin{aligned} H(1,2) &= \{(1,2), (1,2,3)(1,2), (1,3,2)(1,2)\} \\ &= \{(1,2), (1,3), (2,3)\} = (1,2)H \\ H(2,3) &= \{(2,3), (1,2,3)(2,3), (1,3,2)(2,3)\} \\ &= \{(2,3), (1,2), (1,3)\} = (2,3)H \\ H(1,3) &= \{(1,3), (1,2,3)(1,3), (1,3,2)(1,3)\} \\ &= \{(1,3), (2,3), (1,2)\} = (1,2)H \end{aligned}$$

Che forma la seguente **partizione**



Teorema - Cardinalità classi laterali destre e sinistre

Tutte le **classi laterali destre e sinistre** hanno **la stessa cardinalità**, che è quella di H.

<u>Dimostrazione</u>: dati $a, b \in G$ costruiamo una **corrispondenza**

$$\begin{gathered} \alpha : Ha \to Hb \\ \alpha(ha) = hb \end{gathered}$$

α è **biunivoca**

- **Iniettività**:

$$
\begin{aligned}
\alpha(ha) &= \alpha(h'a) \\
hb &= h'b \\
hbb^{-1} &= h'bb^{-1} \\
h &= h'
\end{aligned}
$$

- **Suriettività**: dato che $hb \in Hb$, risulta per definizione

$$hb = \alpha(ha)$$

Ora se prendo $b = e$ ottengo una corrispondenza biunivoca

$$\alpha : Ha \to He = H$$

Posso procedere allo stesso modo con i **laterali sinistri**:

$$
\begin{gathered}
\beta : aH \to bH \\
\beta(ah) = bh
\end{gathered}
$$

è una biezione, che da luogo ad una biezione $aH \leftrightarrow H$ quando prendo $b = e$. Quindi

$$
\begin{array}{ccccc}
aH & \leftrightarrow & H & \leftrightarrow & Ha \\
\beta \updownarrow & & & & \updownarrow \alpha \\
bH & & & & Hb
\end{array}
$$

Teorema - Teorema di Lagrange

Se G è un **gruppo finito** e $H \leq G$, detto $[G : H]$ il **numero di laterali** di H in G, risulta

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

> ℹ️ $[G : H]$ si legge **indice di H in G**.

Corollario

Se $H \leq G$, G **finito** allora $|H| \mid |G|$

Dimostrazione: Abbiamo visto che tutte le classi laterali hanno la **stessa cardinalità** $|H|$. Poiché le classi laterali **formano una partizione** di G, l'ordine di G è quello di H moltiplicato per il numero di classi laterali denotato con $[G : H]$.

Lezione 17 - 10/11/2022

Numeri complessi

Introduciamo ora i **numeri complessi**. Nell'insieme $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ delle coppie ordinate di numeri reali, definiamo le seguenti operazioni:

- $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ ed equivale proprio alla somma in $\mathbb{R}^2$

$$(a, b) + (c, d) = (a + c, b + d)$$

- $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$

$$(a, b)(c, d) = (ac - bd, ad + bc)$$

Esempio:

$$(a, 0)(c, 0) = (ac, 0) \leftarrow \text{"copula"}$$
$$(0, 1)(0, 1) = (-1, 0)$$

Proposizione - C è un campo

$\mathbb{C}$ è un campo.

Dimostrazione: è chiaro che $(\mathbb{C}, +)$ è un **gruppo abeliano** il cui elemento neutro è $(0, 0)$.
Dobbiamo vedere poi che $(\mathbb{C} \setminus \{0\}, \cdot)$ è un **gruppo abeliano**. Dico che:

1. $(1,0)$ è l'elemento neutro
2. se $(a,b) \neq (0,0)$ allora $(a,b)^{-1}$ è

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right)$$

Verifiche:

- $(1,0)$ elemento neutro

$$(a,b)(1,0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a,b)$$

- Inverso di (a,b)

$$\begin{aligned}(a,b)(a,b)^{-1} &= (a,b)\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right) = \\ &= \left(a \cdot \frac{a}{a^2+b^2} - b \cdot \frac{-b}{a^2+b^2}, a \cdot \frac{-b}{a^2+b^2} + b \cdot \frac{a}{a^2+b^2} \right) = \\ &= \left(\frac{a^2+b^2}{a^2+b^2}, 0 \right) = (1,0)\end{aligned}$$

Forma algebrica

$$(a,b) = (a,0) + (0,b) = \underbrace{(a,0)}_{a} + \underbrace{(0,a)}_{i}\underbrace{(b,0)}_{b}$$

Abbiamo la seguente corrispondenza:

$$(a,b) \leftrightarrow a + ib$$

che prende il nome di **forma algebrica del numero complesso**. Inoltre, i viene chiamata **unità immaginaria**.

Si vede subito che le operazioni introdotte prima corrispondono, quando si usa la **forma algebrica**, a operare con le **usuali regole di calcolo** in $\mathbb{R}$ insieme a:

$$ib = bi \tag{1}$$
$$i^2 = -1 \tag{2}$$

<u>Esempio</u>:

$$(5+4i)(7-3i) = 35 + 28i - 15i - 4 \cdot 3i^2 = 47 + 13i$$

<u>Nota</u>:

$$\frac{1}{a+ib} \cdot \frac{a-ib}{a-ib} = \underbrace{\frac{a-ib}{a^2+a^2}}_{(*)} = \frac{a}{a^2+b^2} + i \cdot \frac{-b}{a^2+b^2}$$

La scrittura $(*)$ non ha senso **come numero complesso**, mentre quella alla sua destra dopo l'uguale ha senso.

Definizoni - Coniugato e modulo

Sia $z = a + ib$. Il **coniugato** di z è

$$\bar{z} = a - ib$$

mentre il suo **modulo** è

$$|z| = \sqrt{z\bar{z}} = \sqrt{a^2+b^2} \in \mathbb{R}$$

infatti

$$\sqrt{z\bar{z}} = \sqrt{(a+ib)(a-ib)} = \sqrt{a^2-(ib)^2} = \sqrt{a^2+b^2} \in \mathbb{R}$$

<u>Nota</u>: $z^{-1} = \dfrac{\bar{z}}{|z|^2}$

Proprietà

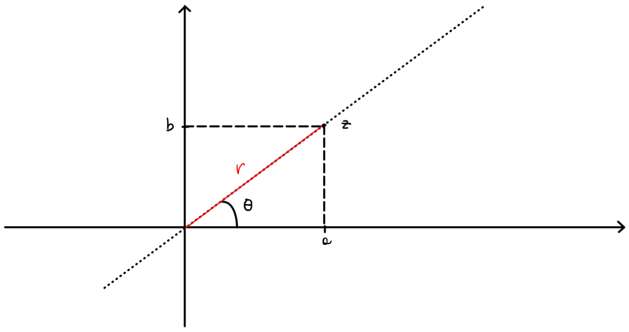
- $\overline{\overline{z}} = z$
- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$
- $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$
- $z\overline{z} = a^2 + b^2 \geq 0;\ z\overline{z} = 0 \Leftrightarrow z = 0$

  Il numero reale $z\overline{z}$ prende il nome di **norma del numero complesso** z
- $|z_1 z_2| = |z_1||z_2|$
- $|z_1 + z_2| \leq |z_1| + |z_2|$ (ovvero vale la **disugualianza triangolare**)

Forma trigonometrica

Si ha la corrispondenza

$$\begin{array}{ccc} \mathbb{C} & \longleftrightarrow & \mathbb{R}^2 \\ z = a + ib & & (a, b) \end{array}$$



dove:

$$a = r\cos\theta$$
$$b = r\sin\theta$$
$$z = r \cdot (\cos\theta + i\sin\theta)$$
$$r = |z| = \sqrt{a^2 + b^2}$$

ℹ️ L'angolo θ prende il nome di **argomento del numero complesso** z.

N.B.: Se $z' = r'(\cos\theta' + i\sin\theta')$

$$zz' = rr'(\cos(\theta + \theta') + i\sin(\theta + \theta'))$$

che ci dice che il **prodotto** di due numeri complessi scritti sotto forma trigonometrica è il numero complesso che ha come argomento la **somma degli argomenti** e come modulo il **prodotto dei moduli** (ricordiamo che r è il modulo).

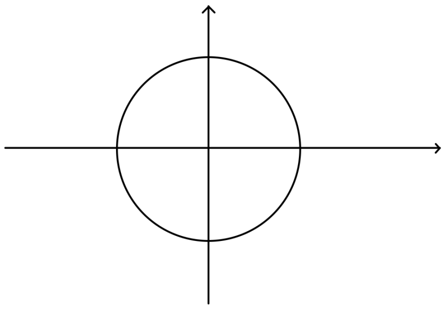
In particolare, la forma trigonometrica di un numero complesso si presta molto bene al **calcolo delle potenze**, perché per ogni intero $n \geq 0$ si ha la seguente formula di **de Moivre**:

$$z^n = r^n(\cos n\theta + i\sin n\theta)$$

Osservazioni varie:

$$S^1 = \{z \in \mathbb{C} : |z| = 1\}$$

rappresenta la circonferenza unitaria:



$$z \in S^1$$
$$z = \cos\theta + i \sin\theta$$

S^1 è un **gruppo** rispetto alla **moltiplicazione**.

Radici n-esime di un numero complesso

Dato $\alpha \in \mathbb{C}$, vogliamo trovare le soluzioni complesse di

$$z^n = \alpha$$

Vedremo che avremo sempre, se $\alpha \neq 0$, n radici n-esime distinte.

Osserviamo che quest'affermazione è falsa in $\mathbb{R}$:

- $\alpha = -1$ con n pari non ha nessuna soluzione
- $\alpha = 1$, $n = 3$ ha una sola soluzione

$$x^3 = 1 \quad x^3 - 1 = 0 \quad (x-1)\underbrace{(x^2 + x + 1)}_{>0} = 0 \Leftrightarrow x = 1$$

Proposizione

Se $\alpha = r(\cos\theta + i\sin\theta),\ \alpha \neq 0,\ n > 0$ le **radici n-esime** di α sono:

$$z_k = \sqrt[n]{r} \cdot \left(\cos\frac{\theta + 2k\pi}{n} + i \sin\frac{\theta + 2k\pi}{n}\right)$$

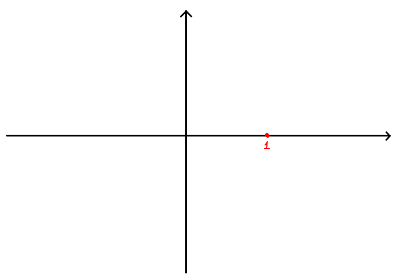
con $k \in \{0, ..., n-1\}$

Vedremo negli esercizi che

$$C_n = \{z \in \mathbb{C} : \overbrace{z^n = 1}^{\text{radici n-esime dell'unità}}\}$$

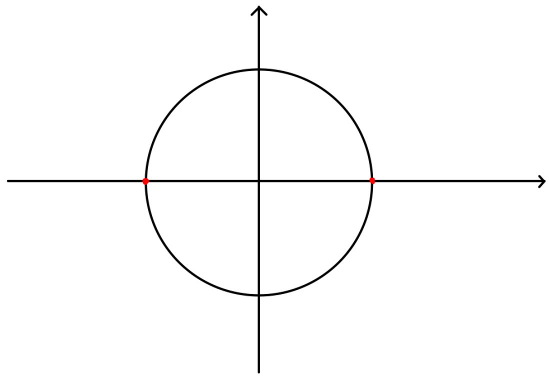
è un **sottogruppo** di $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ **isomorfo** a $\mathbb{Z}_n$.

Se $\alpha = 1$, allora $r = 1$ e $\theta = 0$

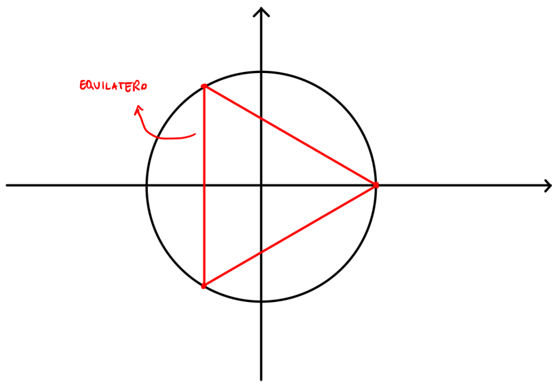


$$z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

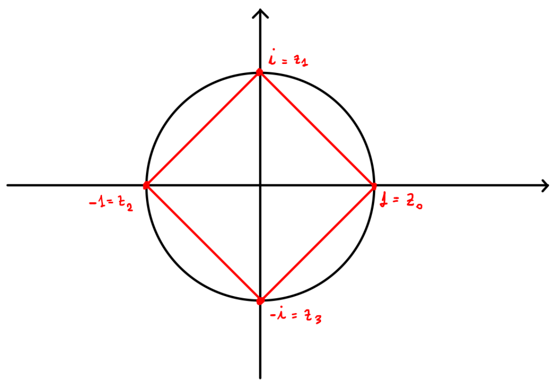
- $n = 2$



- $n = 3$



- $n = 4$



Corollari

Ricoridiamo il **teorema di Lagrange:**

Se G è un **gruppo finito** e $H \leq G$, allora $|H| \mid |G|$. Precisamente

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

Corollario 1

Se $G = p$, p **primo**, allora G è **ciclico**.

Sia $g \in G,\ g \neq e$. Allora $| < g > |$ divide $|G| = p$. Poiché p è **primo**

$$| < g > | = o(g) = p$$

quindi G è ciclico.

Corollario 2

Se G è un **gruppo finito**

$$o(g) \mid |G| \ \forall g \in G$$

Infatti, $o(g) = | < g > |$, che divide $|G|$

Corollario 3

Se $|G| = n$, allora $g^n = e \ \forall g \in G$. Infatti, dato $g \in G$ $|G| = k \cdot o(g)$ quindi

$$g^{|G|} = g^{k \cdot o(g)} = \left(g^{o(g)}\right)^k = e^k = e$$

<u>Esempio</u>: $G = \mathbb{U}_{16}$, $|G| = \phi(2^4) = 8$

$$3^{|G|} = 3^8 = 6561 \equiv 1 \mod 16$$

<u>Osservazione</u>: nuova dimostrazione del **teorema di Eulero-Fermat**:

$$(a, n) = 1 \quad a^{\phi(n)} \equiv 1 \mod n$$

Infatti $U(n)$ ha carindalità $\phi(n)$ e quindi la relazioni precedente è il **corollario 3** in questo caso.

Isomorfismo

$\Phi : G \to G$' è un **omomorfismo** se

$$\Phi(g_1 g_2) = \Phi(g_1)\Phi(g_2) \qquad \forall g_1, g_2 \in G$$

Φ è un **isomorfismo** se è **biunivoca.**

Proprietà che si conservano per isomorfismo

- Abelianità

- Cardinalità
- Ordine dei sottogruppi e degli elementi

Esempi: $(\mathbb{Z}, +)$ e $(\mathbb{Q} \setminus 0, \cdot)$ **non sono isomorfi**.

In $(\mathbb{Z}, +)$ tutti gli elementi **non nulli** hanno **ordine infinito**, mentre in $(\mathbb{Q} \setminus \{0\}, \cdot)$ gli elementi 1 e -1 hanno **ordine** 2.

Più formalmente, se esistesse

$$f : \mathbb{Q} \setminus \{0\} \to \mathbb{Z} \text{ isomorfismo}$$

$f(-1)$ dovrebbe avere ordine 2, ma **nessun elemento non nullo** di $\mathbb{Z}$ ha **ordine finito**.

Classificazione dei gruppi di ordine ≤ 7 a meno di isomorfismo

1. $\{e\}$
2. $\mathbb{Z}_2$
3. $\mathbb{Z}_3$
4. $\mathbb{Z}_4, \ V = \mathbb{Z}_2 \times \mathbb{Z}_2 \ (*)$
5. $\mathbb{Z}_5$
6. $\mathbb{Z}_6, \ S_3$ (la vedremo in futuro)
7. $\mathbb{Z}_7$

Classificazione dei gruppi di ordine 4 (*)

Se **esiste un elemento di ordine** 4, allora il gruppo è **ciclico**. Altrimenti tutti gli elementi non identici hanno ordine 2.

$$G = \{Id, a, b, c\} \quad a^2 = b^2 = c^2 = e$$
$$ab = \begin{array}{ccccccc} e & \rightsquigarrow & ab = e & \Rightarrow & a = b^{-1} = b & \text{No} \\ a & \rightsquigarrow & ab = a & \Rightarrow & b = e & \text{No} \\ b & \rightsquigarrow & ab = b & \Rightarrow & a = e & \text{No} \\ c & \rightsquigarrow & ab = c & & & \text{Sì} \end{array}$$

Con $ab = c$ si ha

$$\begin{aligned} ab = c = ba \\ bc = a = cb \\ ac = b = ca \end{aligned}$$

Ker e Im

Sia $\Phi : G \to G'$ un **omomorfismo**. Definiamo

$$\begin{aligned} \mathrm{Ker}\Phi &= \{g \in G : \Phi(g) = e'\} \\ \mathrm{Im}\Phi &= \{g \in G' : \exists g \in G : \Phi(g) = g'\} \end{aligned}$$

Proprietà

1. $\Phi(e) = e'$

$$e'\Phi(g) = \Phi(g) = \Phi(eg) = \Phi(e)\Phi(g) = e'\Phi(g)\Phi(g)^{-1} = \Phi(e)\Phi(g)\Phi(g)^{-1} = e' = \Phi(e)$$

2. $\Phi(g^{-1}) = \Phi(g)^{-1}$

$$\Phi(g)\Phi(g^{-1}) = \Phi(gg^{-1}) = \Phi(e) = e' \rightsquigarrow \Phi(g^{-1}) = \Phi(g)^{-1}$$

<u>Esercizio</u>: $\mathrm{Ker}\Phi \leq G,\ \mathrm{Im}\Phi \leq G'$

- $\mathrm{Ker}\Phi \leq G$: devo mostrare che

$$a, b \in \mathrm{Ker}\Phi \Rightarrow ab^{-1} \in \mathrm{Ker}\phi$$

  - **Ipotesi**: $\Phi(a) = \Phi(b) = e'$
  - **Tesi**: $\Phi(ab^{-1}) = e'$

$$\Phi(ab^{-1}) = \Phi(a)\Phi(b^{-1}) = \Phi(a)\Phi(b)^{-1} = e'e'^{-1} = e'$$

- $\mathrm{Im}\Phi \leq G'$: devo mostrare che

$$a', b' \in \mathrm{Im}\Phi \Rightarrow a'b'^{-1} \in \mathrm{Im}\Phi$$

  - **Ipotesi**: $a' = \Phi(a),\ b' = \Phi(b)$
  - **Tesi**: $\exists c \in G : \Phi(c) = a'b'^{-1}$

$$a'b'^{-1} = \Phi(a)\Phi(b)^{-1} = \Phi(a')\Phi(b'^{-1}) = \Phi(\underbrace{ab^{-1}}_{c})$$

Proposizione

Sia $\Phi : G \to G'$ un **isomorfismo**. Allora Φ è **iniettiva** se e solo se $\mathrm{Ker}\Phi = \{e\}$.

<u>Dimostrazione</u>: **Supponiamo Φ iniettiva** e consideriamo $g \in \mathrm{Ker}\Phi$.
Vogliamo dimostrare che $g = e$. Abbiamo

$$\Phi(g) = e' = \Phi(e)$$

Poichè Φ **è iniettiva**, $g = e$.

Viceversa, supponiamo che $\mathrm{Ker} = \{e\}$ e proviamo che Φ è inieittiva, ovvero

$$
\begin{aligned}
\Phi(g_1) &= \Phi(g_2) \Rightarrow g_1 = g_2 \\
\Phi(g_1)\Phi(g_2)^{-1} &= \Phi(g_2)\Phi(g_2)^{-1} \quad \text{molt. a dx per } \Phi(g_2)^{-1} \\
\Phi(g_1)\Phi(g_2^{-1}) &= e' \\
\Phi(g_1 g_2^{-1}) &= e' \\
g_1 g_2^{-1} \in \mathrm{Ker}\Phi &= \{e\} \\
g_1 g_2^{-1} &= e \\
g_1 g_2^{-1} g_2 &= e g_2 \quad \text{molt. a dx per } g_2 \\
g_1 &= g_2
\end{aligned}
$$

Definizione - Sottogruppo normale

$N \leq G$ si dice **normale** in G ($N \trianglelefteq G$) se

$$xN = Nx \quad \forall x \in G$$

ovvero se i **laterali destri e sinistri coincidono**, ovvero

$$
\begin{aligned}
\forall n_1 \in \mathbb{N}\ \exists n_2 \in \mathbb{N} : x n_1 = n_2 x \\
\forall n_2 \in \mathbb{N}\ \exists n_1 \in \mathbb{N} : x n_2 = n_1 x
\end{aligned}
$$

Esempi:

1. In un **gruppo abeliano**, ogni sottogruppo è normale
2. In S_3 abbiamo verificato direttamente che
   - $\{\mathrm{Id}, (1,2,3), (1,3,2)\} \trianglelefteq S_3$ in quanto:

$$
\begin{aligned}
H = H(1,2,3) = H(1,3,2) &= (1,2,3)H = (1,3,2)H \\
H(1,2) &= (1,2)H \\
H(2,3) &= (2,3)H \\
H(1,3) &= (1,3)H
\end{aligned}
$$

   - $\{\mathrm{Id}, (1,2)\} \not\trianglelefteq S_3$ in quanto ad esempio:

$$H(2,3) = \{(2,3)(1,2,3)\} \neq \{(2,3)(1,3,2)\} = (2,3)H$$

Ricordiamo che $x, y \in G$ si dicono **coniugati** se

$$\exists g \in G : y = gxg^{-1}$$

Notazione: Se $H \leq G$

$$H^x = xHx^{-1} = \{xhx^{-1} : h \in H\}$$

Proposizione

Sia $N \leq G$. Sono equivalenti

1. $N \trianglelefteq G$
2. $N^x = N \; \forall x \in G$
3. $xnx^{-1} \in N, \; \forall x \in G, \forall n \in N$
4. N è un **unione di classi di coniugio**.

Dimostrazione: bisogna vedere che $1. \Rightarrow 2. \Rightarrow 3. \Rightarrow 4. \Rightarrow 1.$

- $1. \Rightarrow 2.$

$$\begin{aligned} xN &= Nx \; \forall x \\ xNx^{-1} &= Nxx^{-1} = N \\ N^x &= N \end{aligned}$$

- $2. \Rightarrow 3.$

  Ovvio. Sappiamo che $xNx^{-1} = N$; in particolare, dato $n_1 \in N \; \exists n_2 \in N$ tale che

$$xn_1x^{-1} = n_2 \in N$$

- $3. \Rightarrow 4.$

  Basta vedere che per ogni elemento $n \in N$ la sua classe di coniugio è contenuta in N. Ma questa è proprio l'ipotesi.

- $4. \Rightarrow 1.$

  Dimostrata nella prossima lezione.

Lezione 18 - 11/11/2022

Ultima dimostrazione della lezione precedente

Ricordiamo: $N \leq G$ è **normale** se

$$xN = Nx \; \forall x \in G$$

Dimostrazione:

- $4. \Rightarrow 1.$

  Ricordiamo che la classe di coniugio di $z \in G$ è

  $$\mathrm{cl}(z) = \{xzx^{-1} : x \in G\}$$

  Per ipotesi sappiamo che

  $$N = \dot{\bigcup_{n \in I \subset N}} \mathrm{cl}(n)$$

  Devo dimostrare che $xN = Nx$, ovvero che:

  - dato $n_1 \in N, \; \exists n_2 : xn_1 = n_2 x$ e
  - dato $n_1' \in N \; \exists n_2' \in N : n_1' x = x n_2'$

  Ora $n_1 \in \mathrm{cl(n)}$ per qualche $n \in I$, dunque

  $$yn_1y^{-1} = n \rightsquigarrow n_1 = y^{-1}ny$$
  $$xn_1x^{-1} = xy^{-1}nyx^{-1} = xy^{-1}n(xy^{-1})^{-1} \in \mathrm{cl}(n)$$

  e quindi $xn_1x^{-1} \in N$ ovvero $xn_1x^{-1} = n_2$ per qualche $n_2 \in N$, ovvero $xn_1 = n_2x$.
  Ripetendo allo stesso modo l'argomento per n_1' otteniamo che $n_1'x = xn_2'$

Perchè abbiamo introdotto i sottogruppi normali

Se $N \trianglelefteq G$, l'insieme delle classi laterali (destre o sinistre), denotato con G/N, si può dotare della **struttura di gruppo**.

Teorema - G/N è un gruppo

G/N (G modulo N) con l'**operazione binaria**

$$NxNy = Nxy$$

è un **gruppo**. Se G è finito

$$|G/N| = |G|/|N|$$

Dimostrazione: verifichiamo anzitutto che l'operazione è **ben posta**, ovvero

$$Nx = Nx',\ Ny = Ny' \Rightarrow Nxy = Nx'y'$$

questo **segue** dal fatto che $N \trianglelefteq G$. Infatti

$$Nxy = NxNy = Nx'Ny' = NNx'y' = Nx'y'$$

Mostriamo ora che ha le proprietà del gruppo:

- **Associatività**:

$$(NxNy)Nz = NxyNz = N(xy)z = Nx(yz) = NxNyz = Nx(NyNz)$$

- **Elemento neutro**:

$$NxNe = Nxe = Nx, \quad NeNx = Nex = Nx$$

- **Inverso**: $(Nx)^{-1} = Nx^{-1}$

$$\begin{gathered} NxNx^{-1} = Nxx^{-1} = Ne = N \\ Nx^{-1}Nx = Nx^{-1}x = Ne = N \end{gathered}$$

Proiezione al quoziente

Se $N \trianglelefteq G$ c'è un **omomorfismo suriettivo**

$$\begin{gathered} \pi : G \to G/N \\ \pi(x) = Nx \end{gathered}$$

È chiaro che π è **suriettiva**; è un omomorfismo

$$\pi(xy) = Nxy = NxNy = \pi(x)\pi(y)$$

Inoltre $\mathrm{Ker}\ \pi = N$. Infatti

$$\begin{aligned} \mathrm{Ker}\ \pi = \{g \in G : \pi(g) = Ne\} &= \\ = \{g \in G : Ng = N\} &= N \end{aligned}$$

Omomorfismo

Siano $(G_1, *_1),\ (G_2, *_2)$ gruppi, $f : G_1 \to G_2$ è un **omomorfismo** se

$$f(g *_1 g') = f(g) *_2 f(g')$$

<u>Esempio</u>: $f : \mathbb{Z}_4 \to \mathbb{Z}_8,\ f(\overline{x}) = 4\overline{x}$. Si ha

- $f(\overline{0}) = \overline{0}$
- $f(\overline{1}) = \overline{4}$
- $f(\overline{2}) = \overline{0}$
- $f(\overline{3}) = \overline{4}$

$$\forall \overline{x}, \overline{y} \in \mathbb{Z}_4 \quad f(\overline{x} + \overline{y}) = f(\overline{x}) + f(\overline{y}) \quad \begin{aligned} &\text{e Ker} f = \{\overline{0}, \overline{2}\} \\ &\text{Im} f = \{\overline{0}, \overline{4}\} \end{aligned}$$

<u>Esempio</u>:

$$f : S_n \to \mathbb{Z}_2 \qquad f(w) = \begin{cases} \overline{0} & \text{se } w \text{ pari} \\ \overline{1} & \text{se } w \text{ dispari} \end{cases}$$

Per le **proprietà dei segni delle permutazioni** f è un omomorfismo

$$\text{Ker} f = \{w \in S_n : f(w) = \overline{0}\} = \{w \in S_n : w \text{ è pari}\} = A_n$$

Lemma

Se $f : G \to G'$ è un **isomorfismo**,

$$\text{Ker} f \trianglelefteq G$$

<u>Dimostrazione</u>: Il modo **più comodo per dimostrarlo è usando la condizione** $3.$ (negli esercizi va fatto proprio così) dell'ultima proposizione della lezione precedente.
Devo quindi far vedere che se $g \in \text{Ker} f$ e $x \in G$, allora $xgx^{-1} \in \text{Ker} f$;

- **Ipotesi**: $f(g) = e'$
- **Tesi**: $f(gxg^{-1}) = e'$

$$f(xgx^{-1}) = f(x)\overbrace{f(g)}^{=e}f(x^{-1}) = f(x)\overbrace{f(g)}^{=e}f(x)^{-1} = f(x)f(x)^{-1} = e'$$

Teorema - Teorema fondamentale di omomorfismo tra gruppi

Siano G, G' **gruppi** e $f : G \to G'$ un **omomorfismo**. Allora esiste un **unico isomorfismo**

$$\overline{f} : G/\mathrm{Ker} f \to \mathrm{Im} f$$

tale che $f = \overline{f} \circ \pi$, dove $\pi : G \to G/\mathrm{Ker} f$ è la **proiezione canonica**

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & \mathrm{Im} f \subset G' \\ G/\mathrm{Ker} f \arrow[ur, dashed, "\overline{f}"'] & \end{tikzcd}$$

Dimostrazione: poniamo $N = \mathrm{Ker} f$. Definiamo $\overline{f} : G/N \to \mathrm{Im} f$ come

$$\overline{f}(Nx) = f(x)$$

Devo vedere che:

1. $\overline{f}$ è **ben posta**
2. $\overline{f}$ è **iniettiva**
3. $\overline{f}$ è **suriettiva**
4. $\overline{f}$ è un **omomorfismo**

Verifiche:

1. significa che

$$\begin{aligned}
&Nx = Ny \Rightarrow \overline{f}(Nx) = \overline{f}(Ny) \\
&Nx = Ny \Rightarrow f(x) = f(y) \\
&xy^{-1} \in N \\
&xy^{-1} \in \mathrm{Ker} f \\
&f(xy^{-1}) = e' \qquad f(x)f(y^{-1}) = e' \\
&f(x)f(y)^{-1} = e' \quad f(x) = f(y)
\end{aligned}$$

2. $\overline{f}(Nx) = \overline{f}(Ny) \Rightarrow Nx = Ny$ cioè $f(x) = f(y) \Rightarrow Nx = Ny$

   Basta seguire al **contrario** le implicazioni di 1.

$$f(x) = f(y) \Rightarrow f(x)f(y^{-1}) = e' \Rightarrow f(xy^{-1}) = e' \Rightarrow xy^{-1} \in \mathrm{Ker} f = N \Rightarrow Nx = Ny$$

3. Dato $y \in \mathrm{Im} f,\ \exists x \in G : y = f(x) = \overline{f}(Nx)$
4. $\overline{f}(NxNy) = \overline{f}(Nxy) = f(xy) = f(x)f(y) = \overline{f}(Nx)\overline{f}(Ny)$

Applicazione

Proposizione

Sia G un **gruppo ciclico**, se G è **infinito** allora $G \cong \mathbb{Z}$, se G è **finito** $G \cong \mathbb{Z}_n$ per qualche n.

Dimostrazione: Sia $G =< g >$. Consideriamo

$$f : \mathbb{Z} \to G,\ f(k) = g^k$$

f è chiaramente **suriettiva** ed è un **omomorfismo**:

$$f(k+h) = g^{k+h} = g^k g^h = f(k)f(h)$$

Se G è **infinito** sappiamo che $g^h \neq g^k$ per $h \neq k$, dunque f è **iniettiva**, quindi un **isomorfismo** $\mathbb{Z} \cong G$.

Se $G =< g >$ è **ciclico** di ordine n, allora $\mathrm{Ker} f = n\mathbb{Z}$ e per il **teorema di omomorfismo**

$$G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$