Lezione 01

27 settembre 2021

$\mathbb{N} = \{0, 1, 2, \dots\}$ numeri naturali

$x+1=0 \qquad x=-1$ non ha sol in $\mathbb{N}$

$\mathbb{Z} = \{\dots -3, -2, -1, 0, 1, 2, \dots\} = \mathbb{N} \cup -\mathbb{N}$ interi

$ax+b=0 \qquad a \neq 0 \qquad x=-\frac{b}{a}$ se $a \nmid b$ $-\frac{b}{a} \notin \mathbb{Z}$

$2x+3=0$ non ha sol in $\mathbb{Z}$.

$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z} \; n \neq 0 \right\}$ (con l'identificazione di frazioni equivalenti)

↳ razionali

$a_0 = 0 \; ; \; a_1 = 0,1 \; ; \quad a_2 = 0,101 \; ; \; a_3 = 0,101001$

$a_n = a_{n-1} + 10^{-\square} = 0,101001\dots1\underbrace{0\dots0}_{n-1}1$

$\lim_n a_n \notin \mathbb{Q}$ (i numeri razionali sono i numeri decimali con sviluppo finito o periodico)

$\supset$

$\subset$ ola dimostrazione

$\mathbb{R}$ = numeri decimali

$\mathbb{C} = \{a+ib \mid a, b \in \mathbb{R}\} \qquad i^2 = -1$

Su $\mathbb{R}$ ($\mathbb{Q}, \mathbb{Z}, \mathbb{N}$) c'è un ordinamento $<$

OPERAZIONI: un'operazione su X è una funzione $\varphi \; X \times X \longrightarrow X$

Studio di $\mathbb{N}$

Def della Peano

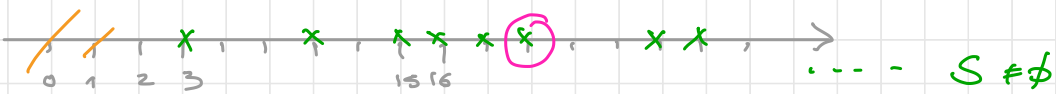
1. $\exists$ un elemento iniziale 0
2. Ogni elemento ammette un successore

$$\forall n \quad \exists\, n+1$$

Assioma del buon ordinamento (Principio del minimo)

Ogni sottoinsieme non vuoto di $\mathbb{N}$ ammette un elem. minimo

$$\forall\, S \subset \mathbb{N},\ S \neq \emptyset \quad \exists\, m_0 \in S \text{ tale che } m_0 \leq s\ \forall s \in S$$



So che $S \neq \emptyset$ $\exists\, m \in S$

$0 \in S$? — si: 0 è il minimo; no: vado avanti

$1 \in S$? — si: 1 è il min; no: vado avanti

con al più $m+1$ tentativi trovo il minimo

Oss: Il principio del minimo vale anche per gli ed degli insiemi del tipo

$$\{ n \in \mathbb{Z} \mid n \geq n_0 \} \qquad n_0 \in \mathbb{Z}$$

- Per gli insiemi del tipo

$$\{ n \in \mathbb{Z} \mid n \leq n_0 \} \qquad n_0 \in \mathbb{Z}$$

vale un analogo principio del max.

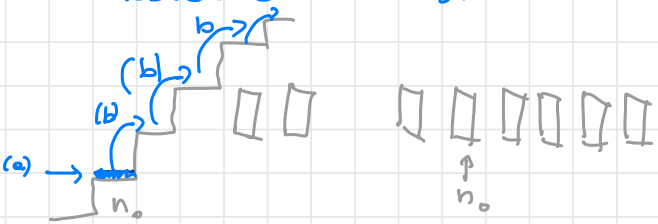
Principio di induzione (I forma)

Sia $P(n)$ una proprietà definita $\forall n \geq n_0$ $(n_0 \in \mathbb{Z})$

Supponiamo che (IPOTESI):
- (a) $P(n_0)$ sia vera — Passo base
- (b) $\forall n \geq n_0$ se $P(n)$ è vera allora $P(n+1)$ è vera — Passo induttivo

Allora $P(n)$ è vera $\forall n \geq n_0$ ← TESI

- Si usa per dimostrare certi enunciati $\forall n \geq n_0$
- Si verificano le ipotesi (a) e (b) e il Principio assicura la Tesi



- (b) se una Tessera cade fa cadere la successiva

(a) una Tessera cade

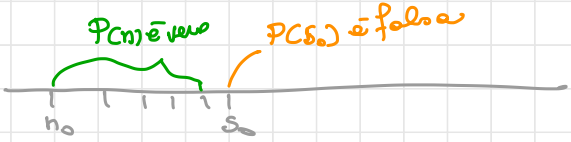
Dim (via Principio del minimo)

$S = \{ n \geq n_0 \mid P(n) \text{ è falsa} \}$ la tesi è $S = \emptyset$

Per assurdo: se fosse $S \neq \emptyset$ per il Principio del minimo

$\exists\, s_0 \in S$ s_0 minimo di S $s_0 \leq n$ $\forall n \in S$

$s_0 > n_0$ perché $P(n_0)$ è vera e $P(s_0)$ è falsa



$s_0 - 1 \geq n_0$ $\quad P(s_0 - 1)$ è vera

$\Downarrow$ (b) dato che $s_0 - 1 \geq n_0$

$P(s_0)$ è vera $\Rightarrow$ assurdo!

$\Rightarrow \quad S = \phi \Rightarrow P(n)$ è vera $\forall n \geq n_0$ $\square$

Esempio:

$$1 + 2 + \dots + n = \frac{n(n+1)}{2} \qquad \forall n \geq 0$$

$$\begin{cases} 1 + 2 + \dots + n = x \\ n + n-1 + \dots + 1 = x \end{cases}$$

$$(n+1) + (n+1) + \dots + (n+1) = n(n+1) = 2x \qquad x = \frac{n(n+1)}{2}$$

Posso dimostrarlo anche per induzione

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \qquad \forall n \geq 0$$

$P(n)$

Devo verificare PB e PI.

PB $\quad n_0 = 0 \quad P(0)$ è vera $\quad 0 = \frac{0(0+1)}{2}$ ✓

PI $\quad n \geq 0$ assumo $P(n)$ vera e devo dimostrare che $P(n+1)$ è vera

$$\underbrace{0 + 1 + \dots + n}_{P(n)} + (n+1) = \frac{(n+1)(n+1+1)}{2}$$

$P(n)$ $\quad \| \quad n(n+1)/2$

$$\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$ ✓

Ho verificato (a) (b) quindi per il Principio $\Rightarrow P(n)$ è vera $\forall n \geq 0$

Principio di induzione (II forma – forte)

Sia $P(n)$ una proprietà definita $\forall n \geq n_0$ $(n_0 \in \mathbb{Z})$

Supponiamo che
- (a) $P(n_0)$ sia vera — Passo base
- (b') $\forall m > n_0$ se $P(k)$ è vera $\forall n_0 \leq k < m$ $\Rightarrow P(m)$ è vera — Passo induttivo

(Ipotesi)

Allora $P(n)$ è vera $\forall n \geq n_0$ ← Tesi

(b') è un'ipotesi più debole di (b) quindi dato che la Tesi è la stessa l'induzione II è a priori più forte (in realtà è equivalente)

Teorema fondamentale dell'aritmetica (Teo fattorizzazione unica)

Ogni $n \in \mathbb{Z}$ $n \neq 0, \pm 1$, a meno del segno, si fattorizza in modo "unico" come prodotto di numeri primi.

(unico = a meno dell'ordine dei fattori)

Dim dell'esistenza:

Per induzione II $P(n) = \{n$ si fattorizza in primi$\}$

Dato che non ci interessa il segno considero $n \geq 2$

(per $n \leq -2$ fattorizzo $m = -n \geq 2$ e metto $-$ davanti)

Tesi: $P(n)$ è vera $\forall n \geq 2$

PB $n = 2$ $P(2)$ è vera 2 si fattorizza in primi ✓
2 è primo

PI: Assumo $P(k)$ vera $\forall\ 2 \leq k < m$ e devo dimostrare che $P(m)$ è vera cioè che m ammette una fattorizzazione in primi

m / primo ✓
\ non primo $= h\,k$ $1 < h, k < m$

$2 \leq h, k < m$

⇓

$P(h)$ e $P(k)$ sono vere.

$h = p_1 \cdots p_r$ $r \geq 1, p_i$ primo $\forall\ 1 \leq i \leq r$

$k = q_1 \cdots q_s$ $s \geq 1$ q_j primo $\forall\ 1 \leq j \leq s$

$m = hk = p_1 \cdots p_r\, q_1 \cdots q_s$ ← si fattorizza in primi

Valgono (a) $n=2$ e (b') $\Rightarrow$ $P(n)$ è vera $\forall n \geq 2$ Ind II

Dim per Induzione I:

$Q(n) = \{ P(k) \text{ è vera} \quad \forall\, n_0 \le k \le n \}$

$n_0 = 2$

PB: $Q(2) = P(2)$ vera

PI $Q(n)$ vera $= P(2), \dots, P(n)$ sono vere

Voglio vedere che $Q(n+1)$ è vera cioè

$P(2), \dots, P(n), P(n+1)$ sono vere

($P(2), \dots, P(n)$: lo so dato che assumo $Q(n)$; $P(n+1)$: m)

$m = n+1$ / primo

$\forall\, h\, k \quad 2 \le h, k < m$

e dato che $P(h)$ e $P(k)$ sono vere

(Sono parte dell'ipotesi $Q(n)$ è vera)

$\Rightarrow$ m si fattorizza (stesso discorso di prima)

Esercizio: Dimostrare l'esistenza della fatt usando il p del minimo. (vedi lezioni anno scorso)

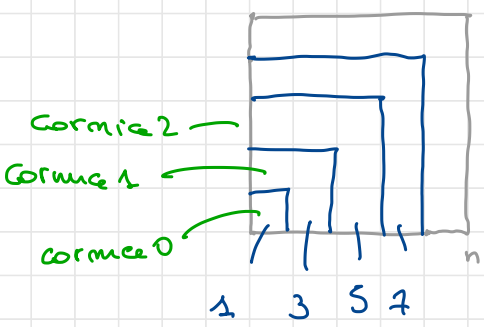
$$\sum_{i=0}^{n-1} (2i+1) = n^2 \qquad \forall n \geq 1$$

PB $n=1$ $\quad \sum_{i=0}^{1-1} (2i+1) = 1 = 1^2$ ✓

PI $\quad \sum_{i=0}^{n+1-1} (2i+1) = (n+1)^2$

$$\sum_{i=0}^{n-1} (2i+1) + 2n+1 = n^2 + 2n + 1 = (n+1)^2$$

(= per IP IND)



È un quadrato di area n^2 se un quadratino ha lato e sono n^2 quadratini

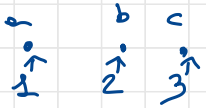
la cornice i-esima ha $2i+1$ quadratini $\forall i = 0, \dots, n-1$

$$\sum_{i=0}^{n-1} (2i+1) = n^2$$

CALCOLO COMBINATORIO

Contare = mettere in corrispondenza biunivoca con un segmento di $\mathbb{N}$.

$\mathbb{N}_r = \{1, 2, \dots, r\}$

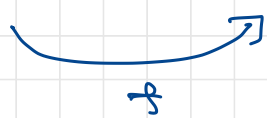


$\# X = n$ $\qquad X \longleftrightarrow \mathbb{N}_n$ corrisp biunivoca (1 a 1)

Due insiemi hanno la stessa cardinalità se possono essere messi in corrispondenza biunivoca.

$g \circ f$ è una corrisp biunivoca tra X e Y

Viceversa $\quad X \overset{h}{\longleftrightarrow} Y \overset{g}{\longleftrightarrow} \mathbb{N}_n \qquad f = g \circ h$



Principio dei cassetti (Pigeonhole principle)

Se metto n oggetti in k cassetti e $k < n$, c'è almeno un cassetto che contiene almeno 2 oggetti

$1 \le k < n$ nessuna funzione $\mathbb{N}_n \longrightarrow \mathbb{N}_k$ è iniettiva

Dim: Per induzione su n $\quad P(n) = \{ \forall k < n \ \forall f \ \mathbb{N}_n \to \mathbb{N}_k, f \text{ non è iniettiva} \}$

PB: $n = 2$ $\qquad \mathbb{N}_2 = \{1, 2\} \longrightarrow \mathbb{N}_1 = \{1\}$

In questo caso l'unica funzione $\quad 1 \mapsto 1 \quad 2 \mapsto 1$ è evidentemente non è iniettiva

PI: Assumiamo $P(n)$ vera e dimostriamo $P(n+1)$

Per assurdo supponiamo che $\exists\ h \quad 1 \le h < n+1$ e

$$\varphi : \{1, \dots, n, n+1\} \longrightarrow \{1, \dots h\} \quad \text{iniettiva}$$

$\varphi(n+1) = x \qquad \varphi^{-1}(x) = n+1$ perché φ è iniettiva.

$$\varphi^* = \varphi_{|\{1,\dots,n\}} : \{1,\dots,n\} \longrightarrow \{1,\dots,h\} \setminus \{x\}$$

è ancora una funzione iniettiva

$$\varphi^* \ \{1,\dots,n\} \longrightarrow \{h-1 \text{ el } \} \quad \text{iniettiva}$$

$1 \le h < n+1$ d'altra parte $h > 1 \qquad 1 < h < n+1$

$\Rightarrow 1 \le h-1 < n$ Abbiamo trovato un assurdo. □

$\# X = n \qquad X = \{x_1, \dots, x_n\}$

$\# Y = m \qquad Y = \{y_1, \dots, y_m\}$

PRODOTTO CARTESIANO

$$X \times Y = \{ (x, y) \mid x \in X,\ y \in Y \} \leftarrow \text{coppie ordinate}$$

$$\# X \times Y = |X \times Y| = n \cdot m$$

scelte per $x \in X$ — # scelte per $y \in Y$

$\# X = 2 \qquad X = \{x_1, x_2\} \qquad \# Y = 3 \qquad Y = \{y_1, y_2, y_3\}$

	x_1	x_2
y_1	x_1, y_1	(x_2, y_2)
y_2		
y_3		

Esempio: Numero di Targhe possibili

$L = \{\text{Lettere}\} \to 26$

$N = \{\text{Numeri}\} \to 10 \quad \{0, \dots, 9\} = \mathbb{N}$

$$L \times L \times N \times N \times N \times L \times L$$

$$26^4 \cdot 10^3$$

FUNZIONI $X \to Y$

$$F(X \to Y) = \{ f : X \to Y \}$$

$x_1 \to$ m possibilità (un qualsiasi el di Y)

$x_2 \to$ m "

$\vdots$

$x_n \to$ m possibilità

$$\#F(X \to Y) = m^n = \#Y^{\#X}$$

$$F(X \to Y) = Y^X$$

notazione

$Y \times \dots \times Y$ $|X|$ volte

$\{(y_{i_1}, y_{i_2}, \dots, y_{i_n}) \mid y_{i_j} \in Y\}$

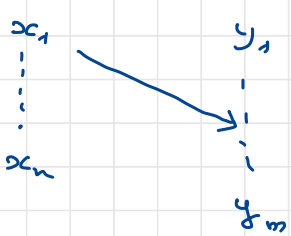
La n-upla $(y_{i_1}, \dots, y_{i_n}) \longleftrightarrow f(x_j) = y_{i_j}$.
(coordinata)

FUNZIONI INIETTIVE

$$I(X \to Y) = \{ f : X \to Y \mid f \text{ è iniettiva} \}.$$

$$\# I(X \to Y) = \begin{cases} 0 & \text{se } m < n \\ m(m-1)\dots(m-n+1) & m \geq n \end{cases}$$

Il caso $m < n$ segue dal principio dei cassetti.



Per $f(x_1)$ ho m scelte
per $f(x_2)$ $m-1$ scelte
$f(x_n)$ $m-n+1$ scelte

Oss: $I(X \to X) = S(X)$ permutazioni di X

$|X| < +\infty$ $\quad f: X \to X$ è iniettiva $\iff$ è suriettiva $\iff$ è biiettiva

Esempio L'ipotesi che X sia finito è necessaria

$$f: \mathbb{N} \to \mathbb{N}, \quad n \mapsto 2n$$ è iniettiva ma non suriettiva.

E le funzioni suriettive $X \to Y$ quante sono?

$m > n$ $\quad 0$
$m = n$ $\quad n!$

Esercizio $\#X = n \quad \#Y = n-1$

Insieme delle parti di X

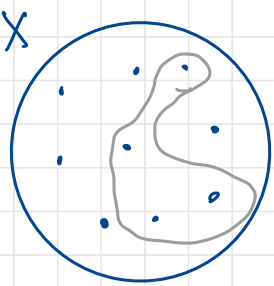
$$\mathcal{P}(X) \doteq \{ A \mid A \subseteq X \}$$

$X = \{1,2,3\}$

$$\mathcal{P}(X) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{2,3\}, \{1,3\}, \{1,2\}, \{1,2,3\} \}$$

$$\mathcal{P}(\{1,2,3\}) = 8 = 2^3$$

$$\boxed{\#\mathcal{P}(X) = 2^{\#X}}$$



Per fare un sotto insieme scelgo gli el da mettere.

$\forall x \in X$ ho 2 possibilità metterlo o non metterlo. $\longrightarrow 2^n$ costruzioni $\neq$

Formalmente:

$$F: \mathcal{P}(X) \longleftrightarrow \{ f \mid X \longrightarrow \{0,1\} \}$$

$$A \longmapsto \varphi_A \qquad \varphi_A(x) = \begin{cases} 0 & \text{se } x \notin A \\ 1 & \text{se } x \in A \end{cases}$$

F è ben definita: $\forall A \in \mathcal{P}(X)$

$$F(A) = \varphi_A \in \{ X \longrightarrow \{0,1\} \}$$

F iniettiva: $\forall A, B \in \mathcal{P}(X) \quad A \neq B \Rightarrow F(A) \neq F(B)$

$$\varphi_A \neq \varphi_B$$

$\Rightarrow A \neq B \quad \exists x \in A \setminus B$ oppure $B \setminus A \Rightarrow \varphi_A(x) \neq \varphi_B(x)$

$A \not\subseteq B$ oppure $B \not\subseteq A$

F è surgettiva: $\forall \varphi \in \{X \to \{0,1\}\}\ \exists A \in \mathcal{P}(X)$

Tale che $F(A) = \varphi_A \equiv \varphi$

$A = \varphi^{-1}(1)$ $\quad x \in A \iff \varphi(x) = 1$

$\varphi_A \equiv \varphi$

$\varphi_A(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases}$

$\varphi(x) = \begin{cases} 1 & x \in A \text{ per def di } A \\ 0 & \text{altrimenti} \end{cases}$

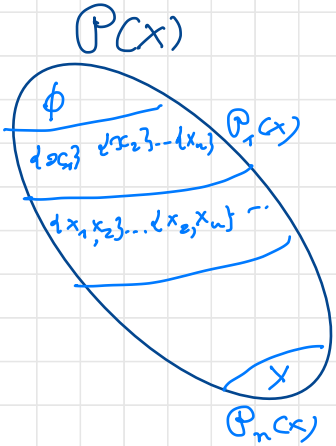
Lezione 03 — 4 ottobre '21

$\mathcal{P}(X) = \{ A \mid A \subseteq X \}$ $\qquad X$

$\# X = n$

$\mathcal{P}_r(X) = \{ A \in \mathcal{P}(X) \mid |A| = r \}$

$\# \mathcal{P}_n(X) \doteq \binom{n}{r}$ ← coeff binomiale di n su r



So che:

- $\binom{n}{r} \in \mathbb{N} \quad \forall n, r$
- $\binom{n}{0} = 1 \quad \forall n$
- $\binom{n}{1} = n \quad \forall n$
- $\binom{n}{n} = 1 \quad \forall n$
- $\binom{n}{r} = 0 \quad r > n$

$\mathcal{P}_r(X) \ni A \qquad A = \{ x_{i_1}, \dots, x_{i_r} \}$ $\qquad x_{i_j} \in X$ ha tutti diversi

$x_{i_j} \neq x_{i_h} \quad \forall j \neq h$

So contare $(x_{i_1}, \dots, x_{i_r})$ ← r-uple (ordinate)

ogni r-upla individua univocamente una funzione iniettiva $\mathbb{N}_r \to X$ perché x_{i_j} sono due a due distinti

Osservo $I(\mathbb{N}_r \to X)$ = r-uple ordinate di r elementi a 2 a 2 distinti

$$= \binom{n}{r} r!$$

$$\Rightarrow \boxed{\#\mathcal{P}_r(X) = \frac{\#\text{ } r\text{-uple ordinate di } r \text{ elementi distinti}}{r!} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \binom{n}{r}}$$

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \frac{n!}{r!(n-r)!} \Rightarrow \begin{cases} \text{se } r=0 \Rightarrow 1 \quad (0!=1) \\ r>n \quad \binom{n}{r}=0 \text{ lo sapevo a priori} \end{cases}$$

Osservazione:

$$\mathcal{P}(X) = \bigcup_{r=0}^{n} \mathcal{P}_r(X)$$

$$\Rightarrow \#\mathcal{P}(X) = \sum_{r=0}^{n} \#\mathcal{P}_r(X)$$

$$\boxed{2^n = \sum_{r=0}^{n} \binom{n}{r}}$$

Proprietà 1) $\binom{n}{r} = \binom{n}{n-r}$ $\forall n \ \forall r$

2) $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$ $\forall n, r$

La verifica algebrica di queste formule è ovvia

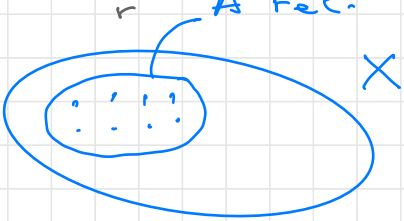
Dato che si tratta di uguaglianze tra cardinalità di insiemi cerco di capire il perché delle uguaglianze su argomenti di cardinalità.

1) $$\binom{n}{r} = \frac{n!}{r!\,(n-r)!} = \frac{n!}{(n-r)!\,(n-(n-r))!} = \binom{n}{n-r}$$

($n-(n-r)$ = r)

$$\#\mathcal{P}_r(X) = \#\mathcal{P}_{n-r}(X)$$

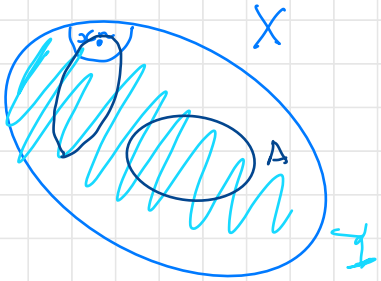
$$A \longleftrightarrow X \setminus A$$



2) $$\#\mathcal{P}_r(X) = \#\mathcal{P}_r(Y) + \#\mathcal{P}_{r-1}(Y)$$

$Y = X - \{x_n\}$

$\#Y = n-1$



$$\mathcal{P}_r(X) \hookrightarrow \mathcal{P}_r(Y) \cup \mathcal{P}_{r-1}(Y)$$

ψ

A

$$\begin{cases} x_n \in A \Rightarrow A - \{x_n\} \subset \mathcal{P}_{r-1}(Y) \\ x_n \notin A \Rightarrow A \subset \mathcal{P}_r(Y) \end{cases}$$

$$F : \mathcal{P}_r(Y) \cup \mathcal{P}_{r-1}(Y) \longrightarrow \mathcal{P}_r(X)$$

$$A \subseteq \mathcal{P}_r(Y) \longmapsto A$$

$$B \subseteq \mathcal{P}_{r-1}(Y) \longmapsto A = B \cup \{x_n\}$$

Verificare che F è una corrisp. biunivoca.

TRIANGOLO DI PASCAL-TARTAGLIA

la riga $n+1$-esima contiene $\binom{n}{0}\ \binom{n}{1}\ \cdots\ \binom{n}{n}$

$\binom{0}{0}$

$\binom{1}{0}\ \binom{1}{1}$

$\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2}$

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1 ← $\Sigma = 2^5$

Esercizio

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$$

La divisione euclidea

$\mathbb{Z}$ abbiamo il v. a $|\cdot| \quad \mathbb{Z} \to \mathbb{N}$, $z \mapsto |z|$

$|ab| = |a||b|$

$|a+b| \le |a|+|b|$

Dividere a per b : "approssimare" a con un multiplo di b.

$a=37 \quad b=3 \qquad 37 = 3 \cdot 12 + 1$ ← resto

$a=38 \qquad 38 = 3 \cdot 12 + 2$ ← per convenzione si sceglie quello con resto positivo

$3 \cdot 13 - 1$

Teorema di divisione euclidea (divisione con resto)

$\forall a, b \in \mathbb{Z}$ $b \neq 0$ esistono e sono unici $q, r \in \mathbb{Z}$ tali che

1) $a = qb + r$

2) $0 \leq r < |b|$

Dim: Esistenza: caso $b > 0$ $|b| = b$

$$X = \{ r \in \mathbb{Z} \mid r = a - kb \quad k \in \mathbb{Z} \} \cap \mathbb{N}$$

$X \subseteq \mathbb{N}$ $X \neq \phi$ $r = a + |a| b \geq 0$

$\uparrow$ X

Per il principio del minimo $\exists r_0 \in X$ minimo.

$r_0 = a - qb$ $q \in \mathbb{Z}$ $a = qb + r_0$ $r_0 \geq 0$

Se per assurdo fosse $r_0 > |b| = b$

$0 \leq r_0 - b = a - qb - b = a - b(q+1) \Rightarrow r_0 - b \in X$

ma questo è assurdo perché $r_0 - b < r_0$ e r_0 era il minimo in X.

Caso $b < 0$ $|b| = -b$

Sappiamo che $\exists q, r \in \mathbb{Z}$ t.c. che $a = q|b| + r$ $0 \leq r < |b|$

$= (-q) b + r$

$-q, r \in \mathbb{Z}$ $0 \leq r < |b|$

Unicità $\quad a = b q_1 + r_1 \qquad 0 \le r_1 < |b|$

$\qquad = b q_2 + r_2 \qquad 0 \le r_2 < |b|$

$r_1 \ge r_2$ (o viceversa) $\quad |b| > r_1 \ge r_1 - r_2 = |q_1 - q_2| |b|$

$\hookrightarrow \ge 0$

Se $\begin{cases} q_1 = q_2 \Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2 \to \text{ok} \\ q_1 \neq q_2 \quad \underline{|b| > |q_1 - q_2| |b| \ge |b|} \text{ assurdo} \end{cases}$

$\hookrightarrow q_1 - q_2 \neq 0 \quad |q_1 - q_2| \ge 1$

▨

Def: $a, b \in \mathbb{Z}$, $b \neq 0$. Si dice che b DIVIDE a $\quad b \mid a$

se $\exists\, q \in \mathbb{Z}$ tale che $\quad a = qb$

cioè se il resto della divisione di a per b è 0

In questo caso si dice che a è un MULTIPLO di b

Oss: La divisibilità è una RELAZIONE tra le coppie di el di $\mathbb{Z}$

$\mathbb{Z} \times \mathbb{Z} \qquad (a, b) \qquad a \mid b$

(Una relazione R su A è un sottoinsieme X di $A \times A$

$(a_1, a_2) \in X \iff a_1 R a_2$

$A = \mathbb{Z} \qquad R = \text{divisibilità} \qquad X = \{(a,b) \in \mathbb{Z}^2 \mid a \mid b\}$

Proprietà $\quad$ RIFLESSIVA $\quad \forall x \in A \quad x R x$

SIMMETRICA $\quad \forall x, y \in A \quad x R y \Rightarrow y R x$

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

TRANSITIVA $\forall x, y, z \in A$

$xRy \wedge yRz \Rightarrow xRz$

Es $\geq$ su $\mathbb{R}$

$\geq$ riflessiva ✓

$\geq$ ~~simmetrica~~ $x \geq y \quad y \geq x$ NO

antisimmetrica $x \geq y \wedge y \geq x \Rightarrow y = x$ ✓

Transitiva ✓

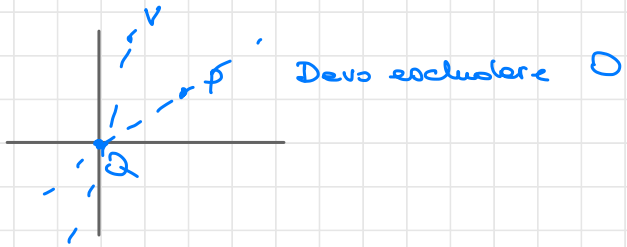
Definizioni: $\mathcal{R}$ relazione su A si dice REL DI EQUIVALENZA se è simmetrica, riflessiva e transitiva.

Es: $A = \mathbb{R}^2 \setminus \{0\}$ $\mathcal{R}$ = stare sulla retta per 0.

rifl: $P \mathcal{R} P$ ✓

sim $P \mathcal{R} Q \Rightarrow Q \mathcal{R} P$ ✓

Trans $P \mathcal{R} Q \quad Q \mathcal{R} V \Rightarrow P \mathcal{R} V$ ✓



La divisibilità è una relazione su $\mathbb{Z}$

Riflessiva $a|a \quad \forall a \in \mathbb{Z}$

non è simmetrica $1|2$ ma $2 \nmid 1$

antisimmetrica $a|b \wedge b|a \Rightarrow a = \pm b$

Transitiva $a|b \wedge b|c$

$$b = aq \qquad c = bp \qquad q, p \in \mathbb{Z}$$

$$\Rightarrow c = (aq)p = a(\underbrace{qp}_{\in \mathbb{Z}}) \Rightarrow a|c$$

Def R rel su A è una **relazione d'ordine** se è riflessiva, antisimm e transitiva.

Una relazione d'ordine è di **ordine totale** se vale anche

$$\forall x, y \in A \quad xRy \text{ oppure } yRx$$

Oss La relazione di divisibilità è è una relazione d'ordine su $\mathbb{N}$, ma non è un ordinamento totale

$$2 \nmid 3 \text{ e } 3 \nmid 2.$$

$\geq$ è una relazione d'ordine totale.

Def: $a, b \in \mathbb{Z}$ non entrambi nulli. Si dice che $d \in \mathbb{Z}$ è un **massimo comune divisore** tra a e b se

i) $d|a \wedge d|b$ (d è un divisore comune)

ii) $x|a \wedge x|b \Rightarrow x|d$ (d è il più grande dei divisori comuni)

Def $a, b \in \mathbb{Z}$ non entrambi nulli. $m \in \mathbb{Z}$ è un **m.c.m** tra a e b se

i) $a|m \wedge b|m$ m è multiplo comune ad a e b

ii) $a|x \wedge b|x \Rightarrow m|x$ m è il piccolo multiplo comune.

Notazioni: $(a,b) = mcd(a,b) = gcd(a,b)$

$[a,b] = mcm(a,b) = lcm(a,b)$

Teorema: $a, b \in \mathbb{Z}$ non entrambi nulli
Il mcd tra a e b esiste ed è unico
(a meno del segno).

Dim: UNICITÀ: Siano d e d' mcd tra a e b

i) $d \mid a \wedge d \mid b$ i') $d' \mid a \wedge d' \mid b$

ii) $x \mid a \wedge x \mid b \Rightarrow x \mid d$ ii') $x \mid a \wedge x \mid b \Rightarrow x \mid d'$

(ii) (ii') $d \mid a \wedge d \mid b \overset{(ii')}{\Longrightarrow} d \mid d'$
(i)
$x = d$

Per simmetria $d' \mid d \Rightarrow d \mid d' \wedge d' \mid d$

$d' = du \quad d = vd' \quad u, v \in \mathbb{Z}$

$\Rightarrow d' = d'uv \quad \Rightarrow uv = 1$
$\Rightarrow u = \pm 1, \quad v = \pm 1$

$d' = \pm d$

Lezione 04 — 11 ottobre '21

Per l'esistenza del MCD si può (a,b)

$$X = \{ax+by \mid x,y \in \mathbb{Z}\}$$

$$Y = X \cap \mathbb{N} \setminus \{0\} \quad Y \subseteq \mathbb{N}$$

$Y \neq \emptyset$ a segno(a) + b segno b $= |a|+|b| > 0$

Sia d il minimo di Y. Allora $d = (a,b)$

$$d = ax_0 + by_0 \qquad x_0, y_0 \in \mathbb{Z}$$

Esercizio: fare la verifiche di (i) e (ii)

ALGORITMO DI EUCLIDE : $a,b \in \mathbb{Z}$ non entrambi 0

$$\{a,b\} \longrightarrow \{d, x_0, y_0\}$$

$d, x_0, y_0 \in \mathbb{Z}$ $\quad d = (a,b)$ e $\boxed{d = ax_0 + by_0}$ IDENTITÀ DI BÉZOUT

$b \neq 0$

$N = n+1$ passi

$$\begin{cases} a = qb + r_0 & 0 \le r_1 < |b| \\ r_0 = q_1 r_1 + r_2 & 0 \le r_2 < r_1 \\ \vdots \\ r_{n-2} = q_{n-1} r_{n-1} + r_n & 0 \le r_n < r_{n-1} \\ r_{n-1} = q_n r_n + 0 \end{cases}$$

Allora $(a,b) = r_n$ e "risalendo nei passaggi dell'AE trovo x_0, y_0.

$(240, 35)$ (a, b)

$240 = 6 \cdot 35 + 30$ (r_0, r_1) $\quad 0 \le r_1 < r_0$

30

* $35 = 1 \cdot 30 + 5 \quad 0 \le 5 < 30$ (r_2, r_1)

$30 = 6 \cdot 5 + 0$

$\Rightarrow \quad 5 = (240, 35)$

$5 = 240\, x_0 + 35\, y_0$

* $5 = 35 - 1 \cdot 30 =$

$= 35 - 1\,(240 - 6 \cdot 35) =$

$= 240(-1) + 35\,(1 + 6) =$

$= 240(-1) + 35 \cdot 7$ (x_0, y_0)

Esempio $(324, 39) = 3 \qquad 3 = 324(-3) + 39 \cdot 25$

$324 = 8 \cdot 39 + 12 \qquad 3 = 39 - 3\,(324 - 8 \cdot 39)$

$39 = 3 \cdot 12 + 3 \quad \rightarrow 3 = 39 - 3 \cdot 12$

$12 = 4 \cdot 3 + 0$

Dim:

1) L'algoritmo Termina: $\{r_i\}_{i \ge 0}$ la successione dei resti

$\forall\, k \qquad 0 \le r_k < r_{k-1} < r_{k-2} \cdots < r_0$

Devo dire che $r_m = 0$ dopo un certo punto in poi

e questo è vero perché non esistono successioni strettamente decrescenti di numeri naturali positivi:

2] L'algoritmo è corretto $r_n = (a,b)$ Trovo x_0, y_0

Lemma: $a, b \in \mathbb{Z}$ non entrambi 0, $\forall k \in \mathbb{Z}$

$$(a,b) = (a, b-ka)$$

Dimo: $d = (a,b)$ $\delta = (a, b-ka)$

i) $d|a$, $d|b$
ii) $x|a$ e $x|b \Rightarrow x|d$

$a = d\,a_1$ ($a_1 \in \mathbb{Z}$) $b = d\,b_1$ ($b_1 \in \mathbb{Z}$) $\Rightarrow d \mid b-ka = d(\underbrace{b_1 - ka_1}_{\in \mathbb{Z}})$

$\Rightarrow d|a$, $d|b-ka \Rightarrow d|\delta$ (per cii) per δ)

Per simmetria posso concludere che $\delta|d$

$d = (a,b)$ $\delta = (a, \underbrace{b-ka}_{\beta})$

$(a, \beta + ka)$ Da quanto ho mostrato sopra so anche che $\delta = (a,\beta) \mid d = (a, \beta+ka)$

$\Rightarrow \delta|d$ e $d|\delta$. Dato che sono entrambi positivi $\delta = d$. □

Dimostro l'alg per induzione sul numero di passi N necessari.

$P(N)$ = Se l'alg termina al N passi, allora funziona.

PB: $N = 1$ $\quad a = q b + 0$ $\quad r_0$

$(a, b) = b$ ✓ $\quad a x_0 + b y_0 = b$

$x_0 = 0$

$y_0 = 1$

Passo induttivo:

Se l'AE richiede $N-1$ passi allora funziona ← ip induttiva

$a = q_0 b + r_1$ ← $\quad b, r_0$

$r_0 = q_1 r_1 + r_2$ ← è l'AE per (b, r_1) e richiede $N-1$ passi

$\Rightarrow r_n = (b, r_1)$ ← ip ind

$r_n = b h_0 + r_1 k_0$

$h_0, k_0 \in \mathbb{Z}$

$r_{n-2} = q_{n-1} r_{n-1} + r_n$

$r_{n-1} = q_n r_n + 0$

$r_n = (b, r_1) = (b, a - q_0 b) = (a, b)$

↑ Lemma

$r_n = b h_0 + r_1 k_0 = b h_0 + k_0 (a - q_0 b) =$

$= k_0 a + b (h_0 - q_0 k_0)$

$x_0 \quad , \quad y_0 \quad \in \mathbb{Z}$

Equazioni diofantee: equazioni con coeff interi di cui si cercano le sol intere

$x^n + y^n = z^n$ ← si fissa n . . . .

$(*)$ $ax+by=c$ $\quad a,b,c \in \mathbb{Z}$

cerco le sol intere.

Se $c = d = (a,b)$ so che ammette sol e so calcolarle con l'AE.

Proposizione. L'eq $(*)$ ha soluzione $\iff d=(a,b) \mid c$

In Tal caso so calcolare una soluzione (con l'AE).

Dim:

$(\Rightarrow)$ $\exists\, x_1, y_1 \in \mathbb{Z}$ tiche $ax_1 + by_1 = c$

$d = (a,b) \Rightarrow a = d\,a_1 \quad a_1 \in \mathbb{Z}$
$b = d\,b_1 \quad b_1 \in \mathbb{Z}$

$$d(\underbrace{a_1 x_1 + b_1 y_1}_{\in \mathbb{Z}}) = c \Rightarrow d \mid c$$

$(\Leftarrow)$ $c = d\gamma \quad \gamma \in \mathbb{Z}$

$ax + by = d\gamma$ ← cerco una sol.

Con l'AE posso calcolare $x_0, y_0 \in \mathbb{Z}$ tali che

$$ax_0 + by_0 = d$$

$$\Rightarrow \quad a(\underbrace{x_0\gamma}_{x_1}) + b(\underbrace{y_0\gamma}_{y_1}) = d\gamma = c \qquad x_1, y_1 \in \mathbb{Z}$$

D

Corollario 1: $(a,b)=1 \iff \exists\, x_1, y_1 \in \mathbb{Z}$ t.c.h.e

$$ax_1+by_1=1$$

Dim: ($\Rightarrow$) è sempre vera per ogni valore di (a,b)

($\Leftarrow$) $ax+by=1$ ha sol. $\Rightarrow (a,b)\mid 1$ (Prop)

$\Rightarrow (a,b)=1$ □

Corollario 2 $(a,b)=d$ e $a=da_1$, $b=db_1$

$\Rightarrow (a_1,b_1)=1$

Dim: $(a,b)=d \Rightarrow \exists x_0, y_0 \in \mathbb{Z}$ tali che

$$ax_0+by_0=d \Rightarrow da_1x_0+db_1y_0=d$$

$$\Rightarrow a_1x_0+b_1y_0=1 \underset{\text{cor1}}{\Rightarrow} (a_1,b_1)=1$$ □

Lemma 1: $c \mid ab$ $(c,a)=1 \Rightarrow c \mid b$

Dim: $\exists x_1, y_1 \in \mathbb{Z}$ t.c.h.e $cx_1+ay_1=1$

$$\Rightarrow cbx_1+\underbrace{aby_1}_{=cm}=b \qquad c(\underbrace{bx_1+my_1}_{\in\mathbb{Z}})=b$$

$(c \mid ab)$ $\Downarrow$

$c \mid b$ □

Ricerca delle sol di $ax+by=c$

1) $d \mid c$? no $\rightarrow$ l'eq non ha soluzioni

sì $\rightarrow$ $c=dk$ $k \in \mathbb{Z}$

Caso $c=0$ eq omogenea $ax+by=0$ ⊛

$d=(a,b)$ $\quad a=da_1$ $\quad (a_1,b_1)=1$

$b=db_1$

⊛ $\quad a_1x+b_1y=0$

$a_1x=-b_1y \Rightarrow a_1 \mid b_1y \quad (a_1,b_1) \Rightarrow a_1 \mid y$

$\Rightarrow y=a_1t \quad t\in\mathbb{Z}$

$a_1x=-b_1a_1t \Rightarrow x=-b_1t$

$$\begin{cases} x=-b_1t \\ y=a_1t \end{cases} \quad t\in\mathbb{Z}$$

Queste sono tutte e sole le sol dell'eq omogenea

Caso generale $ax+by=dk$

$AE \rightarrow x_0,y_0 \longrightarrow (x_1,y_1)=(\underset{\| x_1}{x_0k}, \underset{\| y_1}{y_0k})$ ← una sol particolare

$\Rightarrow$ l'insieme delle soluzioni di $ax+by=dk$ è

$$\begin{cases} x=x_1-b_1t \\ y=y_1+a_1t \end{cases}$$

$t\in\mathbb{Z}$.

Per verificarlo sostituisco x e y nell'eq e vedo che la soddisfa

$$a(x_1 - b_1 t) + b(y_1 + a_1 t) =$$

$$= ax_1 + by_1 + a(-b_1 t) + b(a_1 t) = dk$$

Viceversa se ho due sol dell'eq

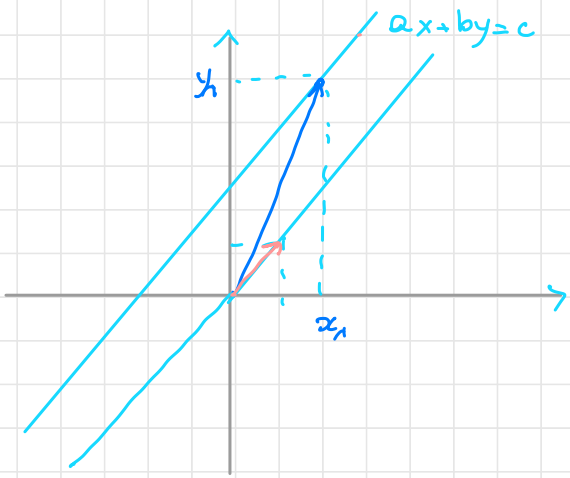
(x_1, y_1) e (x_2, y_2)

$$a x_1 + b y_1 = dk$$

$$a x_2 + b y_2 = dk$$

$$a(x_2 - x_1) + b(y_2 - y_1) = 0 \qquad \Rightarrow \begin{cases} x_2 = x_1 - b_1 t \\ y_2 = y_1 + a_1 t \end{cases}$$

$x_2 - x_1 = -b_1 t$ $\quad$ $y_2 - y_1 = a_1 t$



$\exists$ punti con entrambe le coord intere $(a, b, c \in$

Esempio : $55x + 99y = 22$

$(55, 99) =$

$99 = 1 \cdot 55 + 44$

$55 = 1 \cdot 44 + 11 \quad \rightarrow \quad 11 = (55, 99)$

$44 = 4 \cdot 11 + 0 \qquad 11 \mid 22$

$\rightarrow \quad 5x + 9y = 2$

$5 \cdot \underbrace{4}_{x_1} + 9 \cdot \underbrace{(-2)}_{y_1} = 2$

$$\begin{cases} x = 4 - b_1 t = & b_1 = 9 \\ y = -2 + a_1 t & a_1 = 5 \end{cases}$$

Def 1: $p \in \mathbb{Z}$ $p > 1$ si dice IRRIDUCIBILE se

$p = xy \quad x, y \in \mathbb{Z} \Rightarrow x = \pm 1 \ \vee \ y = \pm 1$

Def 2: $p \in \mathbb{Z}$ $p > 1$ si dice PRIMO se $\forall a, b$ t.c.

$p \mid ab \Rightarrow p \mid a \ \vee \ p \mid b$

Oss: Se p primo $p \mid a_1 \cdots a_n \Rightarrow \exists i$ t.c. $p \mid a_i$

(Es: si fa per induzione su n. Il caso $n=2$ è la def.)

Lemma 2: $p \in \mathbb{Z}$. p è irriducibile $\Leftrightarrow$ p è primo.

Dim: ($\Leftarrow$) (vale anche più in generale, non solo su $\mathbb{Z}$).

$p = xy \Rightarrow p \mid xy \Rightarrow p \mid x \ \vee \ p \mid y$

(p è primo)

per simmetria posso supporre $p|x \Rightarrow x = pu \quad u \in \mathbb{Z}$

$p = puy \Rightarrow 1 = uy \Rightarrow y = \pm 1$

($\Rightarrow$) (vale negli anelli a fattorizzazione unica ma non in generale).

Sia p irriducibile e supponiamo $p|ab \quad a,b \in \mathbb{Z}$

Se $p|a \rightarrow$ OK

$p \nmid a \Rightarrow (a,p) = 1 \Rightarrow p|b$

p è irriducibile — Lemma 1: $p|ab$, $(p,a)=1$

$\Rightarrow p$ è primo $\square$

Lemma 3 $a|m$, $b|m$ e $(a,b)=1 \Rightarrow ab|m$

Oss: In generale sappiamo che se $a|m$ e $b|m$

$\Rightarrow [a,b] | m$ (viene dalla def di mcm)

Dim: $m = ax$ $\quad b|ax$ $\quad (b,a)=1 \overset{L1}{\Rightarrow} b|c$

$\Rightarrow x = bc \Rightarrow m = ax = abc \Rightarrow ab|m$ $\blacksquare$

Proposizione $[a,b] = \dfrac{|a||b|}{(a,b)}$

Dim: $m = \dfrac{|a||b|}{(a,b)}$ e verifico per m le due proprietà del mcm

$m = ab_1 = a_1 b$ ....

Lezione 05 — 13 ottobre '21

Teorema fondamentale dell'aritmetica (T. di fatt. unica)

Ogni intero >1 si scrive in modo "unico" come prodotto di numeri primi

Dim: Esistenza: Per induzione II.

$n=2$ ok è primo

Supponiamo che ogni numero k, $2 \le k < n$ si fattorizza come prodotto di primi e dimostriamo che anche n si fattorizza.

n { è primo ✓

non è primo $\Rightarrow$ non è irriducibile $\Rightarrow$ è riducibile

$= mk$ $\quad 2 \le m, k < n$

Per m e k vale l'ip induttiva $\Rightarrow$

$m = p_1 \cdots p_r$ $\quad p_i$ primi $\quad r \ge 1$

$k = q_1 \cdots q_t$ $\quad q_j$ primi $\quad t \ge 1$

$\Rightarrow n = mk = p_1 \cdots p_r q_1 \cdots q_t$ cioè n è prodotto di primi

UNICITÀ Per induzione sulla lunghezza delle fattorizzazioni

$P(\ell) = \{ \forall n \in \mathbb{N} \mid n$ ammette una fattorizzazione di lunghezza $\ell \Rightarrow$ la fatt di n è unica $\}$

$P(1)$ n ha una fatt di lungh $1 \iff n$ è primo

$\iff n$ è irriducibile $\Rightarrow$ la f di n è unica.

P.I. Supponiamo che $P(h)$ sia vera per $h < \ell$

e dimostriamo che $P(\ell)$ è vero.

$n = p_1 \cdots p_\ell = q_1 \cdots q_s$ * p_i, q_j primi $\ell \geq 1$, $s \geq 1$

Tesi $\ell = s$ a meno di riordinare $p_i = q_i$

* $p_\ell \mid q_1 \cdots q_s$ poiché p_ℓ è primo $\Rightarrow p_\ell \mid q_j$

per qualche j. Ad esempio $p_\ell \mid q_s$

q_s è primo e quindi irriducibile $\Rightarrow q_s = p_\ell u$

$\Rightarrow$ ~~$p_\ell = \pm 1$~~ $\vee$ $u = \pm 1$ $\Rightarrow q_s = p_\ell$

↑ p_ℓ è primo!

$p_1 \cdots \cancel{p_\ell} = q_1 \cdots \cancel{q_s}$

$m = p_1 \cdots p_{\ell-1} = q_1 \cdots q_{s-1}$

m ha lungh $< \ell$ e quindi m ammette una sola fattorizzazione. $\Rightarrow$ $\ell - 1 = s - 1 \Rightarrow \ell = s$

$p_i = q_i$ a meno di riordinare

ma $r_c = r_e = r_s$ $\Rightarrow$ Tesi. ☒

Congruenze.

Def $a, b, n \in \mathbb{Z}$ $n \geq 2$ si dice che a è congruo a b modulo n

$$a \equiv b \pmod{n}$$

se

$$n \mid b-a$$

Proposizione 1: La relazione di congruenza è di equivalenza.

Dim: . riflessiva $a \equiv a \ (n)$ $\forall a \in \mathbb{Z}$ $n \mid a-a=0$ ok ✓

. simmetrica $a \equiv b \ (n) \Rightarrow b \equiv a \ (n)$

$\Downarrow$

$n \mid b-a \Rightarrow n \mid a-b \Rightarrow b \equiv a \ (n)$

. Transitiva $a \equiv b \ (n) \wedge b \equiv c \ (n) \Rightarrow a \equiv c \ (n)$

$\Uparrow$

$n \mid a-b \Rightarrow a-b = nk \quad k \in \mathbb{Z} \Rightarrow$
$n \mid b-c \Rightarrow b-c = nh \quad h \in \mathbb{Z}$

$$a-c = (a-b)+(b-c) = nk + nh = n(\underbrace{k+h}_{\in \mathbb{Z}})$$

$\Rightarrow n \mid a-c \Rightarrow a \equiv c \ (n)$ ☒

Proposizione 2: $a, b \in \mathbb{Z}$ $n \geq 2$. Sono fatti equivalenti.

1) $n \mid a-b$
2) $\exists k_0 \in \mathbb{Z}$ t.c. $a = b + nk_0$
3) $\{a + nk\}_{k \in \mathbb{Z}} = \{b + nh\}_{h \in \mathbb{Z}}$
4) a e b hanno lo stesso resto nella divisione per n

Dim: $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (1)$

$1) \Rightarrow (2)$ $\quad n \mid a-b \Rightarrow a-b = nk_0 \Rightarrow (2)$

$(2) \Rightarrow 3)$ $\quad \{a+nk\}_{k\in\mathbb{Z}} = \{b+nk_0+nk\}_{k\in\mathbb{Z}} = \{b+n(k_0+k)\}_{k\in\mathbb{Z}}$

$(\mathbb{Z} \to \mathbb{Z},\ k \to k_0+k$ è biiettiva$)$ $\quad$ (k_0+k varia in $\mathbb{Z}$ al variare di k in $\mathbb{Z}$, chiamo h)

$= \{b+nh\}_{h\in\mathbb{Z}}$

$(3) \Rightarrow (4)$ $\quad a = qn+r \quad 0 \le r < n$

$r = a-qn \in \{a+nk\}_{k\in\mathbb{Z}} = \{b+nh\}_{h\in\mathbb{Z}}$

$\exists\, h_0 \in \mathbb{Z}$

$r = a-qn = b+nh_0$

$b = n(-h_0)+r \quad 0 \le r < n$

$\Downarrow$

r è il resto della div di b per n

$\Rightarrow (4)$

$(4) \Rightarrow (1)$ $\quad a = q_1 n + r \quad 0 \le r < n$

$b = q_2 n + r$

$b-a = n(q_2-q_1) + r - r \Rightarrow n \mid b-a$ ▨

Proposizione 3 (proprietà delle congruenze)

1) $a \equiv b \ (n) \quad c \equiv d \ (n) \Rightarrow a+c \equiv b+d \ (n)$, $\ ac \equiv bd \ (n)$

2) $a \equiv b \ (n) \quad a \equiv b \ (m) \Rightarrow a \equiv b \ ([m,n])$

3) $a \equiv b \ (n) \Rightarrow (a,n) = (b,n)$

4) $a \equiv b \ (n)$ $d \mid n \Rightarrow a \equiv b \ (d)$

5) $a \equiv b \ (n) \Rightarrow \forall h \in \mathbb{Z} \quad ah \equiv bh \ (n)$

(6) $ra \equiv rb \ (n)$ $r \neq 0 \Rightarrow a \equiv b \left(\frac{n}{(n,r)}\right)$

In particolare se $(n,r)=1$ si ha che r si può "cancellare" $a \equiv b \ (n)$

Dim

(1) $a \equiv b \ (n)$ $a = b + kn$ $c \equiv d \ (n)$, $c = d + hn$

$ac = (b+kn)(d+hn) = bd + n(\dots) \equiv bd \ (n)$

(2) $a \equiv b \ (n)$ $a \equiv b \ (m)$

$n \mid b-a \ \wedge \ m \mid b-a \Rightarrow [m,n] \mid b-a$ (↑ Lemmi...)

$\Rightarrow a \equiv b \ ([m,n])$

(3) $a \equiv b \ (n)$ $a = qn + r$, $b = q_1 n + r$ $0 \leq r < n$

$(a,n) = (qn+r, n) = (r,n) = (r+q_1 n, n) = (b,n)$

(4) ovvio

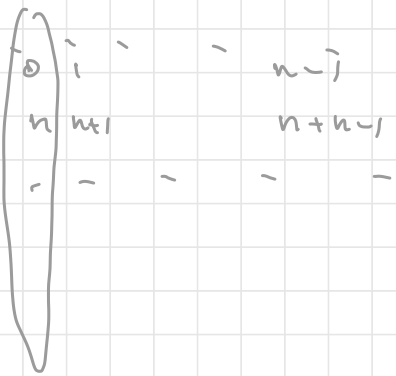
(5) viene da (4)

(6) $ra \equiv rb \ (n)$ $n \mid r(b-a)$ $d = (n,r) \Rightarrow \left(\frac{n}{d}, \frac{r}{d}\right) = 1$

$\frac{n}{d} \mid \frac{r}{d}(b-a) \Rightarrow \frac{n}{d} \mid b-a \Rightarrow b \equiv a \left(\frac{n}{(n,r)}\right)$ ▨

Oss: Ogni intero modulo n è congruo al suo resto nella div per n cioè a uno tra

$0, 1, \dots, n-1$



Esercizio: Un intero è divisibile per 3 $\iff$ la somma delle sue cifre è div per 3.

$n = a_k \dots a_1 a_0$ ← notazione posizionale $0 \le a_i < 9$

$n = a_k 10^k + \dots + a_1 10 + a_0 \equiv a_k (1)^k + \dots + a_1 (1) + a_0 \ (3)$

$\downarrow$

$10 \equiv 1 \ (3)$

$\equiv a_k + \dots + a_1 + a_0$

$n \equiv 0 \ (3) \iff a_k + \dots + a_1 + a_0 \equiv 0 \ (3)$

Idem per il criterio di div. per 9 $(10 \equiv 1 \ (9))$

$10 \equiv -1 \ (11) \rightarrow$ criterio di div per 11 (scriverlo!)

Equazioni e sistemi con le congruenze.

$$aX \equiv b \quad (n)$$

Prop: l'eq $ax \equiv b \ (n)$ ha soluzione $\Leftrightarrow (a,n) \mid b$

In tal caso la sol è del tipo $x \equiv x_0 \ \left(\frac{n}{(a,n)}\right)$

Quindi le soluzioni modulo n sono d e sono

$$x \equiv x_0 + i \ \frac{n}{(a,n)} \quad (n) \qquad i = 0, 1, \dots, (a,n)-1$$

Dim $ax \equiv b \ (n)$

$ax = b + kn$ per un certo $k \in \mathbb{Z}$

$\bigstar$ $\underline{ax - nk = b}$ ← eq diofantea lineare

a, n e b sono noti x, k incognite

$\bigstar$ $\underline{\text{ha soluzione} \Leftrightarrow d=(a,n) \mid b}$ e le soluzioni sono

$$\begin{cases} x = x_0 + \frac{n}{d} t \\ k = y_0 + \frac{a}{d} t \\ t \in \mathbb{Z} \end{cases} \Leftrightarrow x \equiv x_0 \ \left(\frac{n}{d}\right)$$

$x_0 \quad x_0 + \frac{n}{d}1 \quad x_0 + \frac{n}{d}2 \quad \dots \quad x_0 + \frac{n}{d}(d-1)$

$\| \quad$

$x_0 + \frac{n}{d} d \ (n)$

$t \in \mathbb{Z} \qquad t = dq + r \quad 0 \le r < d$

$x \equiv x_0 + \frac{n}{d}(dq + r) =$ (corretto dopo la lezione)

$= x_0 + nq + \frac{n}{d} r \equiv x_0 + \frac{n}{d} r \ (n)$ ∎

Sistemi di eq. lineari (*) $\begin{cases} x \equiv a \ (n) \\ x \equiv b \ (m) \end{cases}$ $\begin{cases} x = a + kn \\ x = b + hm \end{cases}$

$kn - hm = b - a$ eq risolvente del sistema.

So che l'eq risolvente ha soluzione

$\iff (n, m) \mid b-a$ e in tal caso le sol sono

$$\begin{cases} k = k_0 + \dfrac{m}{(n,m)} t \\ h = h_0 + \dfrac{n}{(n,m)} t \end{cases}$$

$$x = a + kn = a + \left(k_0 + \frac{m}{(n,m)} t\right) n \qquad t \in \mathbb{Z}$$

$$= a + k_0 n + \boxed{\frac{mn}{(m,n)}} t$$

" $[m,n]$

$$x \equiv a + k_0 n \ ([m,n])$$

Il sistema * ha soluzione $\iff (m,n) \mid b-a$ e in tal caso la sol è unica modulo $[m,n]$.

Teorema cinese del resto (CRT, TCR)

$m_1, \dots, m_r \in \mathbb{Z}$ $m_i \geq 2$ $(m_i, m_j) = 1 \ \forall i \neq j$

Allora il sistema

$$\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ \\ x \equiv a_n \ (m_n) \end{cases}$$

ammette un unica sol modulo $m_1 \cdots m_r$

Lemma 1) $(a, mn) = 1 \iff (a,m)=1 \wedge (a,n)=1$

2) $(m,n)=1 \Rightarrow (a,mn) = (a,m)(a,n)$

Dim: 1) $\Leftarrow$) $\exists\, x_0 y_0$ tali che $ax_0 + m(ny_0) = 1$

$\Downarrow$

$(a,m) = 1$

$\Leftarrow$ $\exists\, h_0 k_0 \in \mathbb{Z}$ $\quad a h_0 + m k_0 = 1$

$\exists\, \lambda_0 \mu_0 \in \mathbb{Z}$ $\quad a\lambda_0 + n\mu_0 = 1$

$$a(\underbrace{\text{----}}_{\in\mathbb{Z}}) + mn\,\underbrace{k_0\mu_0}_{\in\mathbb{Z}} = 1$$

$\Rightarrow (a, mn) = 1$

(2) ovvio con la caratterizzazione del mcd con la fattorizzazione.

Alternativamente: Sia $d = (a,m)$ e $\delta = (a,n)$ $\Delta = (a, mn)$

$(m,n)=1 \Rightarrow (d,\delta) = 1$

Chiaramente $d, \delta \mid \Delta \Rightarrow d\delta \mid \Delta$ *

D'altra parte $d = ax_0 + my_0$ $\quad x_0, y_0, w_0, z_0 \in \mathbb{Z}$.

$\delta = aw_0 + nz_0$

$\Rightarrow d\delta = a(\underbrace{\text{---}}_{\in\mathbb{Z}}) + mn\,\underbrace{y_0 z_0}_{\in\mathbb{Z}} \Rightarrow \Delta \mid d\delta$ ** $\Rightarrow \Delta = d\delta$. ▨

DIM AGGIUNTA!

Dim TCR $n = 2$ già vista. $(m_1, m_2) = 1 \mid a_1 - a_2$

e la sol è unica modulo $[m_1, m_2] = m_1 m_2$

In generale $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \\ x \equiv a_n \pmod{m_n} \end{cases}$ $\Rightarrow$ Per l'ipotesi induttiva questo sotto sistema ha soluzione $x \equiv x_0 \pmod{m_2 \cdots m_n}$

$$\begin{cases} x \equiv a_1 \quad (m_1) \\ x \equiv x_0 \quad (m_2 \cdots m_n) \end{cases}$$

$(m_2 \cdots m_n)$ — n

Lemma (2) $\Rightarrow$

$$(m_1, m_2 \cdots m_n) = \prod_{i=2}^{n} (m_1, m_i) = 1$$

$\uparrow$

$$(m_i, m_j) = 1 \qquad 2 \le i \ne j \le n$$

$\Rightarrow$ Il sistema ha un'unica soluzione modulo

$$m_1 \cdot m_2 \cdots m_n$$

□

Esempio

$$\begin{cases} x \equiv 2 \ (3) \\ x \equiv 72 \ (5) \\ x \equiv -4 \ (7) \end{cases} \xrightarrow{TCR}$$ Ammette un'unica sol modulo $3 \cdot 5 \cdot 7$

$$\begin{cases} x \equiv 2 \quad (15) \\ x \equiv 3 \quad (7) \end{cases} \qquad \begin{aligned} x &= 2 + 15t \quad * \\ x &= 3 + 7s \end{aligned}$$

$$15t - 7s = 1$$

$$15(1) - 7(2) = 1$$

$$t = 1 + 7\lambda \qquad \lambda \in \mathbb{Z}$$

$$x = 2 + 15(1 + 7\lambda) = 2 + 15 + 105\lambda \qquad \lambda \in \mathbb{Z}$$

$$x \equiv 17 \quad (105)$$

Lezione 06 — 20 ottobre '21

X insieme $\mathcal{R}$ relazione binaria su X

$(x, y \in \mathcal{R} \quad x \mathcal{R} y)$ - $\mathcal{R}$ si dice relazione di equivalenza

se
- riflessiva $\forall x \in X \quad x \mathcal{R} x$
- simmetrica $\forall x, y \in X \quad x \mathcal{R} y \iff y \mathcal{R} x$
- transitiva $\forall x, y, z \in X \quad x \mathcal{R} y \; y \mathcal{R} z \Rightarrow x \mathcal{R} z$.

Oss $\equiv_n$ è una relazione di equiv su $\mathbb{Z}$

Def $\mathcal{R}$ rel. di eq. su X - Si dice classe di equivalenza di $x \in X$ modulo $\mathcal{R}$

$$[x]_{\mathcal{R}} = \{ y \in X \mid x \mathcal{R} y \}$$

$[x]_{\mathcal{R}} \subset X$

$\forall y \in [x]_{\mathcal{R}}$ lo chiamo RAPPRESENTANTE di $[x]$

Esempio $\mathbb{Z} \quad \equiv_{12}$ (classe di congruenza) $\quad [3]_{12} = \{ a \in \mathbb{Z} \mid a \equiv 3 \ (12) \} =$

$$= \{ 3 + 12k \mid k \in \mathbb{Z} \}$$

$3, 15, -9$ sono rappresentanti $[3]_{12}$

Oss: Come rappresentanti delle classi modulo n posso prendere i possibili resti della divisione per n

$$[0]_n, [1]_n, \dots, [n-1]_n$$

$a = qn + r \qquad [a]_n = [r]_n$

$0, 1, \dots, n-1$ sono i rappresentanti canonici.

modulo 12 $\quad [0], [1], \dots, [11]$

$[24], [-11], \dots [-1)$

Prop: R rel di eq su X

1) $[x] = [y] \iff xRy$

2) Due classi di equivalenza sono disgiunte o coincidono. Quindi le classi di equivalenza danno una partizione di X

Dim: (1) ($\Leftarrow$) $xRy \Rightarrow y \in [x]$

$z \in [y] \quad yRz \quad xRy \Rightarrow xRz \Rightarrow z \in [x]$ (Trans.)

$\Rightarrow [y] \subseteq [x]$

Per simmetria ho anche $[x] \subseteq [y] \Rightarrow =$

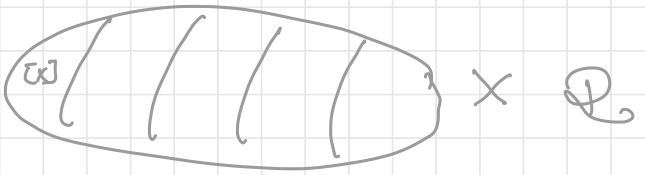
($\Rightarrow$) $[x] = [y] \Rightarrow y \in [x] \Rightarrow xRy$

② $[x] \cap [y] \neq \emptyset \qquad z \in [x] \cap [y]$

$$x R z \ \wedge \ y \underset{\text{simm.}}{R} z \ \Rightarrow \ x R y \ \underset{(1)}{\Rightarrow} \ [x] = [y]$$

$$X = \bigcup_{x \in X} [x] = \bigcup_{x \in \mathcal{U}} [x]$$

$\mathcal{U}$ = insieme di rappresentanti delle classe



Oss: $\mathbb{Z} = \bigcup_{i=0}^{n-1} [i]_n$

$n = 2 \qquad \mathbb{Z} = [0]_2 \cup [1]_2$

$[0]_2$ numeri pari — $[1]_2$ numeri dispari

Def X, R classi equiv., $\{ [x] \mid x \in \Lambda \} = X/R$ insieme quoziente

Esempio: $\mathbb{Z} \ \equiv_n$

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

$\mathbb{Z}/_{\equiv_n}$ insieme quoziente $\qquad \left| \mathbb{Z}/_{n\mathbb{Z}} \right| = n$

Esempio: $\mathbb{Z}/12\mathbb{Z} = \{[0], [1], [2], \dots, [11]\} =$

$= \{[12], [-11], [2], \dots, [-2], [-1]\}$

$\mathbb{Z}/n\mathbb{Z}$ = insieme delle classi di congruenza modulo n (di resto)

- $+$ $[a]_n + [b]_n := [a+b]_n$ somma (è la somma in $\mathbb{Z}$)
- $\cdot$ $[a] \cdot [b] := [a \cdot b]_n$ prodotto

$+, \cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

⚠ Le operazioni sono ben definite?

Ho definito $+$ $\cdot$ in termini di rappresentanti delle classi. Devo verificare che cambiando i rappresentanti il risultato non cambia.

$c \in [a]$, $d \in [b]$

$[a]_n + [b]_n = [a+b]_n$)) ?

$[c]_n + [d]_n = [c+d]_n$

$a \equiv c \pmod n$, $b \equiv d \pmod n$ $\Longrightarrow$ $a+b \equiv c+d \pmod n$, $a \cdot b \equiv c \cdot d \pmod n$

Proprietà delle congruenze.

Proprietà di $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

$+$ (gruppo abeliano)
- è associativa
- $\exists$ l'elemento neutro $[0]_n$
- $\exists$ l'inverso di ogni classe ($[-a]_n$ è l'inverso (opposto) di $[a]_n$)
- è commutativa

→ $(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo abeliano (= commutativo)

$\cdot$
- associativo
- $\exists$ l'elemento neutro $[1]_n$
- commutativo

Non tutte le classi sono invertibili:

$$[a]_n[x]_n = [1]_n \iff ax \equiv 1 \ (n)$$

$[a]$ è inv. modulo $n \iff$ la congruenza $ax \equiv 1 \ (n)$ ha soluzione $\iff (a,n) \mid 1 \iff (a,n) = 1$

$\mathbb{Z}/6\mathbb{Z}$ $[0]$ $[2]$, $[4]$ $[3]$ non sono invertibili

p. distributiva • $\forall [a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$

$$[a]([b]+[c]) = [a][b] + [a][c]$$

Def $(A, +, \cdot)$ $(A+)$ gruppo abeliano
- associativa
vale la distributiva → ANELLO

Se un anello ammette l'el neutro risp. al $\cdot$

$\rightarrow$ Anello con identità

Prop: $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$ è un anello commutativo con id

Oss $(\mathbb{Z}, +, \cdot)$ è un anello comm con 1

$(2\mathbb{Z}, +, \cdot)$ è un anello comm

Per noi anello è sempre comm con 1.

Oss: Per verificare le proprietà di $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$

si scrivono e si usano le analoghe proprietà su $\mathbb{Z}$

$+$ è comm. $\forall [a], [b] \in \mathbb{Z}/_{n\mathbb{Z}}$

- $[a]_n + [b]_n = [b]_n + [a]_n$

$$[a]+[b] = [a+b] = [b+a] = [b]+[a]$$

$=$ def $+$; $=$ $+$ è comm in $\mathbb{Z}$; $=$ def $+$

$\rightarrow$ Verificare le altre proprietà

Def $[a] \in \mathbb{Z}/_{n\mathbb{Z}}$ si dice INVERTIBILE se è invertibile rispetto a $\cdot$, cioè se $\exists\, [x] \in \mathbb{Z}/_{n\mathbb{Z}}$ t.c.

$[a][x] = [1]$

Questo è eq. alla risolubilità di

$$ax \equiv 1 \ (n)$$

Conclusione: $[a]$ è inv. in $\mathbb{Z}/n\mathbb{Z} \iff (a, n) = 1$

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{ [a] \in \mathbb{Z}/n\mathbb{Z} \mid [a] \text{ è invertibile} \}$$

Es: $(\mathbb{Z}/12\mathbb{Z})^\times = \{[1], [5], [7], [11]\}$

Proposizione

- $\left((\mathbb{Z}/n\mathbb{Z})^\times, \cdot\right)$ è un gruppo abeliano
- Se p è primo $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}$

  $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ è un campo ($\leftarrow$ x la def. v. Manfredini)

Dim: • Si tratta di vedere che $\cdot$ è un'op su $(\mathbb{Z}/n\mathbb{Z})^\times$

cioè che $\forall [a], [b] \in (\mathbb{Z}/n\mathbb{Z})^\times \Rightarrow [a]\cdot[b] \ (= [ab]) \in (\mathbb{Z}/n\mathbb{Z})^\times$

$\exists [u], [v] \in (\mathbb{Z}/n\mathbb{Z})^\times$ $\quad [a][u] = [au] = [1]$

$[b][v] = [bv] = [1]$

$\Rightarrow [u][v] = [uv]$ è l'inverso di $[a][b]$

$[a][b][u][v] = [abuv] = [(au)(bv)] = [1 \cdot 1] = [1]$

associatività, $[1] \in \mathbb{Z}/n\mathbb{Z}^\times$, $\exists$ inverso, comm.

(associatività: vera su $(\mathbb{Z}/n\mathbb{Z}, \cdot)$; $[1] \in \mathbb{Z}/n\mathbb{Z}^\times$: ovvio; $\exists$ inverso: per def $\mathbb{Z}/n\mathbb{Z}^\times$; comm.: vera per $(\mathbb{Z}/n\mathbb{Z}, \cdot)$)

• • $\mathbb{Z}/p\mathbb{Z}^\times = \{[a] \in \mathbb{Z}/p\mathbb{Z} \mid (a,p) = 1\}$

Tolgo da $\mathbb{Z}/p\mathbb{Z}$ le classi $[a]$ $p \mid a$

cioè solo la classe $[0]$ $(= [p\lambda]\ \forall \lambda)$

Teorema cinese (II forma)

$m, n \geq 2$ $\quad \varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$[a]_{mn} \longmapsto ([a]_m, [a]_n)$

φ è bigettiva $\iff (m,n) = 1$

Dim:

φ è ben definita $\quad [a]_{mn} = [b]_{mn} \Rightarrow \varphi[a]_{mn} = \varphi[b]_{mn}$

$([a]_m, [a]_n) = ([b]_m, [b]_n)$

Occorre cioè vedere che $a \equiv b \pmod{mn} \Rightarrow \begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$

($\Leftarrow$) $(m,n) = 1$

φ è su: $\forall ([a]_m, [b]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$\exists [x] \in \mathbb{Z}/mn\mathbb{Z}$ t.c.

$$\varphi(\underbrace{[x]}_{mn}) = ([a]_m, [b]_n)$$

$$([x]_m, [x]_n) = ([a]_m, [b]_n)$$

($\Leftarrow$) $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ φ è surj $\Leftarrow$ il sistema ammette sol.

Poiché $(m,n) = 1 \underset{CRT}{\Rightarrow}$ il sistema ammette sol.

Poiché la sol del sistema è unica mod l prodotto φ è anche iniettiva

($\Rightarrow$) $(m,n) = d > 1$ $([0]_m, [1]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

questo non appartiene all'immagine in quanto il sistema $\begin{cases} x \equiv 0 \pmod{m} \\ x \equiv 1 \pmod{n} \end{cases}$ non ha soluzione

perché $(m,n) = d \nmid 0 - 1 = -1$ □

Esempio $\mathbb{Z}/_{12\mathbb{Z}} \hookrightarrow \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$

$$[x] \longmapsto ([1], [2])$$

$$\begin{cases} x \equiv 1 \quad (4) \\ x \equiv 2 \quad (3) \end{cases} \qquad x \equiv 5 \quad (12)$$

$$[x] \longrightarrow ([2], [0])$$

$$\begin{cases} x \equiv 2 \quad (4) \\ x \equiv 0 \quad (3) \end{cases} \qquad x \equiv 6 \quad (12)$$

$$\begin{array}{lll} \overline{0} \longrightarrow (\overline{0}, \overline{0}) & & \overline{6} \longrightarrow (\overline{2}, \overline{0}) \\ \overline{1} \longrightarrow (\overline{1}, \overline{1}) & & \overline{7} \longrightarrow (\overline{3}, \overline{1}) \\ \overline{2} \longrightarrow (\overline{2}, \overline{2}) & & \overline{8} \longrightarrow (\overline{0}, \overline{2}) \\ \overline{3} \longrightarrow (\overline{3}, \overline{0}) & & \overline{9} \longrightarrow (\overline{1}, \overline{0}) \\ \overline{4} \longrightarrow (\overline{0}, \overline{1}) & & \overline{10} \longrightarrow (\overline{2}, \overline{1}) \\ \overline{5} \longrightarrow (\overline{1}, \overline{2}) & & \overline{11} \longrightarrow (\overline{3}, \overline{2}) \end{array}$$

Corollario Se $(m,n) = 1 \Rightarrow \mathbb{Z}/_{mn\mathbb{Z}}^{\times} \xleftrightarrow{\varphi^{\times}} \mathbb{Z}/_{m\mathbb{Z}}^{\times} \times \mathbb{Z}/_{n\mathbb{Z}}^{\times}$

$$[x]_{mn} \longrightarrow ([x]_m, [x]_n)$$

è bigettiva.

Def: Per prima cosa occorre vedere che

$\varphi^{\times}$ è ben definita cioè che $\varphi^{\times}([x]_{mn}) \in \mathbb{Z}/_{m\mathbb{Z}}^{\times} \times \mathbb{Z}/_{n\mathbb{Z}}^{\times}$

$[x]_{mn} \in \mathbb{Z}/_{mn}^{\times} \Rightarrow [x]_m \in \mathbb{Z}/_{m\mathbb{Z}}^{\times}$ $[x]_n \in \mathbb{Z}/_{n\mathbb{Z}}^{\times}$

$\Updownarrow$ ↗ ola la buona def. $\Updownarrow$

$(x, mn) = 1 \Rightarrow (x, m) = 1$ $(x, n) = 1$

$\Leftarrow$ ↳ Lemma

↗ ola la suriettività

Oss: Se $(m,n) = 1 \Rightarrow \left|\mathbb{Z}/_{mn\mathbb{Z}}^{\times}\right| = \left|\mathbb{Z}/_{m\mathbb{Z}}^{\times}\right| \left|\mathbb{Z}/_{n\mathbb{Z}}^{\times}\right|$

Funzione ϕ di Eulero

$$\phi \quad \mathbb{N}_{>0} \longrightarrow \mathbb{N}_{>0}$$
$$n \longmapsto \phi(n) := \#\mathbb{Z}/_{n\mathbb{Z}}^{\times} = \#\{x \mid 0 \le x < n \quad (x,n) = 1\}$$

Abbiamo visto che

$\underline{(m,n) = 1} \Rightarrow \phi(mn) = \phi(m)\,\phi(n)$ ← ϕ è moltiplicativa

$n = p_1^{e_1} \cdots p_r^{e_r}$ $p_i \neq p_j$ primi $e_i \ge 1$

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{e_i})$$

Dobbiamo calcolare $\phi(p^e)$ p primo $e \ge 1$

$\phi(p) = p - 1$ $\{x \mid 0 \le x < p \ (x,p) = 1\} = \{1, \dots, p-1\}$

$\phi(p^e) = \#\{x \mid 0 \le x < p^e, \ (x, p^e) = 1\} =$

$$= p^e - \#\{x \mid 0 \le x < p^e \quad (x, p^e) \neq 1\}$$

$(x, p^e) \neq 1 \iff p \mid x \iff x = py$

$0 \le py < p^e \qquad 0 \le y < p^{e-1}$

$\Rightarrow$ sono p^{e-1} valori di y e quindi di x,

$$\Rightarrow \phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$$

$$\phi(p_1^{e_1} \cdots p_r^{e_r}) = \prod_{i=1}^{n} p_i^{e_i - 1}(p_i - 1)$$

Es $\phi(12) = \phi(2^2)\,\phi(3)$

$= 2(2-1)(3-1) = 4$

$\phi(84) = \phi(4)\,\phi(3)\,\phi(7)$

$4 \cdot 6 = 24.$

Oss: $\forall n > 2$ $\phi(n)$ è pari

Teorema di Eulero

$m \geq 2 \quad x \in \mathbb{Z} \quad (x, m) = 1 \Rightarrow x^{\phi(m)} \equiv 1 \pmod{m}$

Oss: $m = p$ primo $p \nmid x \Rightarrow x^{p-1} \equiv 1 \pmod{p}$

Lezione 07 — 25 ottobre '21

Teorema di Eulero

$m \geq 2 \quad x \in \mathbb{Z} \quad (x,m)=1 \Rightarrow x^{\varphi(m)} \equiv 1 \pmod{m}$

Dim: $(x,m)=1 \Rightarrow \bar{x} \in (\mathbb{Z}/m\mathbb{Z})^\times$

$$q_{\bar{x}} : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$$
$$\bar{a} \longmapsto \bar{x}\bar{a}$$

$\bar{x}\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ perché abbiamo visto che è chiuso rispetto al prodotto

$q_{\bar{x}}$ è iniettiva: infatti

$q_{\bar{x}}(\bar{a}) = q_{\bar{x}}(\bar{b}) \Leftrightarrow \bar{x}\bar{a} = \bar{x}\bar{b} \Leftrightarrow \bar{a}=\bar{b} \Rightarrow q_{\bar{x}}$ iniettiva

moltiplico entrambi i membri per $\bar{x}^{-1}$

$\Rightarrow q_{\bar{x}}$ è biiettiva perché dominio e codominio hanno la stessa cardinalità finita.

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{a}_1, \dots, \bar{a}_{\varphi(m)}\}$$

$$q_{\bar{x}}\left((\mathbb{Z}/m\mathbb{Z})^\times\right) = \{\bar{x}\bar{a}_1, \dots, \bar{x}\bar{a}_{\varphi(m)}\} = (\mathbb{Z}/m\mathbb{Z})^\times$$

$$\Rightarrow \prod_{i=1}^{\varphi(m)} \bar{a}_i = \prod_{i=1}^{\varphi(m)} \bar{x}\bar{a}_i = \bar{x}^{\varphi(m)} \prod_{i=1}^{\varphi(m)} \bar{a}_i$$

Osservo che $\prod_{i=1}^{\varphi(m)} \bar{a}_i = \bar{b} \in (\mathbb{Z}/m\mathbb{Z})^\times$ quindi è invertibile.

$\bar{b} = \bar{x}^{\phi(m)}\bar{b} \Rightarrow \bar{x}^{\phi(m)} = \bar{1} \Rightarrow x^{\phi(m)} \equiv 1 \pmod m$

Corollario (Piccolo Teorema di Fermat)

p primo - $\forall x \in \mathbb{Z}$ $\quad x^p \equiv x \pmod p$

Dim. • $(x,p) = 1$ per Eulero $x^{p-1} \equiv 1 \pmod p$ ($\phi(p)$)

$\Rightarrow x^p \equiv x \pmod p$

• $(x,p) \neq 1 \Rightarrow p \mid x \quad x \equiv 0 \pmod p \Rightarrow x^p \equiv x \pmod p$

perché entrambi i membri sono 0.

Congruenze esponenziali: $a^x \equiv b \pmod m$

Esempio $3^x \equiv 1 \pmod{13}$

- ammette soluzioni? sì per Eulero $(3,13) = 1 \Rightarrow 3^{\phi(13)} \equiv 1 \pmod{13}$
- determinare TUTTE le soluzioni

$3^0 = 1$ $\quad 3^3 = 1$ $\quad 3^6 \equiv 1$

$3^1 = 3$ $\quad 3^4 = 3$ $\quad \dots$

$3^2 = 9$ $\quad 3^5 = 9$ $\quad \dots$

$3^x \equiv 1 \pmod{13} \iff x \equiv 0 \pmod 3$

($\Leftarrow$) $x \equiv 0 \pmod 3$ $\quad x = 3k$ $\quad 3^{3k} \equiv (3^3)^k \equiv 1^k \equiv 1 \pmod{13}$

($\Rightarrow$) $3^x \equiv 1 \pmod{13}$ $\quad x = 3q + r$ $\quad 0 \leq r < 3$

$3^x \equiv 3^{3q+r} = (3^3)^q 3^r \equiv 1^q 3^r \equiv 3^r \equiv 1 \pmod{13}$

$\Rightarrow \quad r=0 \quad \Rightarrow \quad 3 \mid x \Rightarrow \quad x \equiv 0 \quad (3)$

$(a,m)=1 \qquad a^x \equiv 1 \quad (m) \iff \quad x \equiv 0 \quad (\vartheta(a))$

dove $\quad \vartheta(a) = \min \{ k>0 \mid a^k \equiv 1 \ (m) \}$

↳ ordine (moltiplicativo) di a modulo m

$(\Leftarrow) \quad x \equiv 0 \quad (\vartheta(a)) \quad \Rightarrow x = q\,\vartheta(a)$

$$a^x \equiv \left(a^{\vartheta(a)}\right)^q \equiv (1^q) \equiv 1 \qquad (m)$$

$(\Rightarrow) \quad a^x \equiv 1 \quad (m) \qquad x = q\,\vartheta(a) + r \qquad 0 \le r < \vartheta(a)$

$$a^x = \left(a^{\vartheta(a)}\right)^q a^r \equiv 1^q a^r \equiv a^r \equiv 1 \quad (m)$$

$a^{\vartheta(a)} \equiv 1 \ (m)$

Per la minimalità di $\vartheta(a) \Rightarrow r=0 \Rightarrow x \equiv 0 \quad (\vartheta(a))$

Conseguenza $\quad \forall (a,m)=1 \qquad \vartheta(a) \mid \phi(m)$

Esempio: $\quad 2^x \equiv 1 \quad (105) \qquad (2,105)=1$

$105 = 3 \cdot 5 \cdot 7$

$x \equiv 0 \quad (\vartheta(2)) \qquad \vartheta(2) \bmod 105.$

Basta determinare $\vartheta(2)$.

- So che $\vartheta(2) \mid \phi(105) = \phi(3)\phi(5)\phi(7) = 2 \cdot 4 \cdot 6 = 2^4 \cdot 3$

  Voglio scoprire i conti

- Oss $\quad d \mid m \quad$ di è un divisore proprio $(d \neq m)$

  $\iff$ d divide un divisore max di m

  cioè $\frac{m}{p}$ perché qualche primo di m

- Posso usare TCR. $2^x \equiv 1 \pmod{105} \iff \begin{cases} 2^x \equiv 1 \pmod 3 \\ 2^x \equiv 1 \pmod 5 \\ 2^x \equiv 1 \pmod 7 \end{cases}$

$\vartheta(2)$ modulo 3

$\begin{cases} x \equiv 0 \pmod 2 \leftarrow \text{inutile} \\ x \equiv 0 \pmod 4 \\ x \equiv 0 \pmod 3 \end{cases}$ ammette sol unica mod $12 \neq [4,3]=1$

$x \equiv 0 \pmod{12}$ risolve, quindi è l'unica soluzione

$$x \equiv 0 \pmod{12}$$

$(a,m)=1 \qquad a^x \equiv b \pmod m \iff b \equiv a^{x_0} \pmod m \qquad x \equiv x_0 \pmod{\vartheta(a)}$

$b \equiv a^{x_0} \pmod m$ per qualche x_0

$b \not\equiv a^x \pmod m$ per ogni x ← il sistema non ha sol.

$a^x \equiv a^{x_0} \pmod m$

$a^{x-x_0} \equiv 1 \pmod m$ che ha sol $x - x_0 \equiv 0 \pmod{\vartheta(a)}$

$x \equiv x_0 \pmod{\vartheta(a)}$

Esempio $3^x \equiv 61 \pmod{91}$

$91 = 7 \cdot 13$.

$\begin{cases} 3^x \equiv 61 \equiv -2 \pmod 7 \\ 3^x \equiv 61 \equiv 9 = 3^2 \pmod{13} \end{cases}$

mod 7

$3^0 = 1 \quad 3^6 = 1$

$3^1 = 3$

$3^2 = 2$

$3^3 = -1$

$3^4 = -3$

$3^5 = -2 \leftarrow x_0 = 5$

$\vartheta_7(3) = 6$ ($|\phi(7)$ ok)

$-2 = 3^5 \Rightarrow x \equiv 5 \pmod 6$

mod 13

$x_1 = 2$

$3^0 = 1$

$3^1 = 3$

$3^2 = 9$

$3^3 = 1$

$\vartheta_{13}(3) = 3$

$x \equiv 2 \pmod 3$

$\begin{cases} x \equiv 5 \quad (6) \\ x \equiv 2 \quad (3) \end{cases}$ ha sol $\Leftrightarrow (6,3) = 3 \mid 5-2=3$

In questo caso la sol è unica modulo $[6,3] = 6$

$\Rightarrow x \equiv 5 \ (6)$

Idempotenti di $\mathbb{Z}/m\mathbb{Z}$ $\quad x^2 \equiv x \quad (m)$

Esempio $x^2 \equiv x \quad (6) \qquad x(x-1) \equiv 0 \quad (6)$

Prova

$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
✓	✓	✗	✓	✓	✗

$\begin{cases} x(x-1) \equiv 0 \quad (2) \\ x(x-1) \equiv 0 \quad (3) \end{cases}$ 2 e 3 sono primi $\Rightarrow$ vale la legge di annullamento del prodotto

$\Rightarrow$ mod 2 $\quad x \equiv 0 \ \vee \ x \equiv 1 \quad (2)$ ← Tutte

mod 3 $\quad x \equiv 0 \ \vee \ x \equiv 1 \quad (3)$

$x \equiv 0 \ (3)$ $\qquad$ $x \equiv 1 \ (3)$

$x \equiv 0 \ (6) \quad x \equiv 3 \ (6) \qquad x \equiv 1 \ (6) \quad x \equiv 4 \ (6)$

$m = p$ primo $\rightarrow$ 2 soluzioni $x \equiv 0 \ (p) \ \vee \ x \equiv 1 \ (p)$

↳ vale l'annullamento prodotto $x(x-1) \equiv 0 \ (p)$

$m = p^e \qquad x(x-1) \equiv 0 \quad (p^e)$

Poiché x e $x-1$ sono coprimi $p \mid x \Rightarrow p \nmid x-1$

e viceversa. $p^e \mid x(x-1) \Rightarrow p^e \mid x \ \vee \ p^e \mid x-1$

$\Rightarrow \quad x \equiv 0 \ (p^e) \ \vee \ x \equiv 1 \ (p^e)$

$m = p_1^{e_1} \cdots p_r^{e_r} \qquad x^2 \equiv x \ (m) \iff \begin{cases} x^2 \equiv x & (p_1^{e_1}) \\ x^2 \equiv x & (p_2^{e_2}) \\ \vdots & \\ x^2 \equiv x & (p_r^{e_r}) \end{cases}$

Per quanto già visto si ha

$$\begin{cases} x \equiv 0, 1 & (p_1^{e_1}) \\ \vdots & \\ x \equiv 0, 1 & (p_r^{e_r}) \end{cases}$$

Quante sono le sol del sistema?

ho 2^r sistemi, Tutti nella forma TCR → ognuno ha sol unica → 2^r soluzioni DISTINTE

in quanto 2 sistemi differiscono almeno in una equazione.

Esercizi

1) Contare le soluzioni della congruenza $x^2 \equiv 1 \ (m)$

2) $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ si dice NILPOTENTE se $\exists n \in \mathbb{N}$ t.c.

$$\bar{a}^n = \bar{0}$$

Caratterizzare i nilpotenti di $\mathbb{Z}/m\mathbb{Z}$.

Crittografia: il metodo RSA

Cifrare un messaggio → "Trasformarlo" in modo che chi intercetta la trasmissione non possa comprenderlo

Il destinatario deve avere la chiave per decifrarlo

Def Un **crittosistema** $(\mathcal{M}, \mathcal{C}, f, f^{-1})$

$\mathcal{M} = \{$ messaggi in chiaro $\}$

$\mathcal{C} = \{$ messaggi cifrati $\}$

$f : \mathcal{M} \longrightarrow \mathcal{C}$ funzione iniettiva funzione di cifratura

$m \longmapsto f(m) = c$ = messaggio cifrato

f^{-1} funzione di decifratura

→ Cifrario di Giulio Cesare: Si fanno corrispondere le lettere ai numeri in ordine A→1, B→2, ... Z→26

$\mathcal{M} = \{$lettere$\}$ $\mathcal{C} = \mathbb{N}$

oppure come usare Traslazione.

Evoluzioni Si numerano le lettere dopo averle permutate → a numero uguale corrisponde lettera uguale

⚠ Sono fragili: si possono facilmente con analisi delle frequenze delle lettere.

→ Trasformazioni di blocchi di k lettere

ad esempio agendo sui blocchi con una matrice kxk

con $\det = \pm 1$ (assicura l'invertibilità in $\mathbb{Z}$)

→ Crittosistemi a chiave pubblica

Sono crittosistemi per i quali la funzione di cifratura f è nota a tutti (pubblica) ma quella di decifratura è nota solo a chi detiene il crittosistema

> È necessario che la conoscenza di f non consenta di calcolare f^{-1} in tempi rapidi.

Rivest Shamir Adleman 1977

A → detentore del codice

1) Sceglie due primi GRANDI p, q
2) $n = pq$
3) Calcola $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$
4) Sceglie e tale che $(e, \phi(n)) = 1$
5) Calcola $d \in \mathbb{Z}/n\mathbb{Z}^{\times}$ t.c. $de \equiv 1 \ (\phi(n))$
6) Rende noti n, e CHIAVE PUBBLICA
7) Tiene segreti p, q, d CHIAVE PRIVATA

La funzione di cifratura è

$$f(x) = x^e \pmod n$$

Tutti possono cifrare messaggi perché f è pubblica

((e, n) sono noti)

A riceve il messaggio cifrato x^e e applica la funzione di decifratura $f^{-1}(y) = y^d$

$$f^{-1}(x^e) = x^{ed} \equiv x \quad (n)$$

Infatti $x \in \mathcal{U} = \mathbb{Z}/n\mathbb{Z}$ $\quad n = pq$

- $\text{se } (x,n) = 1 \quad x^{\phi(n)} \equiv 1 \quad (n) \qquad ed \equiv 1 \quad (\phi(n))$

$$\Rightarrow ed = k\phi(n) + 1 \qquad x^{ed} = \left(x^{\phi(n)}\right)^k x \equiv x \quad (n)$$

In generale $x^{ed} \equiv x \quad (n) \iff \begin{cases} x^{ed} \equiv x & (p) \ \checkmark \\ x^{ed} \equiv x & (q) \ \checkmark \end{cases}$

- se $(x,n) = p \qquad p \mid x \qquad x^{ed} \equiv x \ (p)$ (entrambi $\equiv 0$)

$(x,q) = 1$ come sopra $\quad x^{ed} \equiv x \ (q)$

- se $x \mid n \qquad x^{ed} \equiv 0 \ (n) \quad x \equiv 0 \ (n) \quad x^{ed} \equiv x \quad (n)$

- Conoscendo solo e e n è difficile calcolare d

A sa calcolarlo perché conoscendo $n = pq$ sa calcolare $\phi(n)$. LA SICUREZZA DEL SISTEMA DIPENDE DALLA DIFFICOLTÀ DI FATTORIZZARE n.

Ogni crittosistema di questo tipo "scade" perché fattorizzare n è una questione di tempo

Esempio $p=11$ $q=17$ $n=187$ $\phi(n)=10\cdot 16=160$

$e=7$ $d=23$

$7d \equiv 1 \ (160)$ $\begin{cases} 7d \equiv 1 \ (2^5) \\ 7d \equiv 1 \ (5) \end{cases}$ $2d \equiv 1 \ (5)$ $d \equiv 3 \ (5)$

$7d - 32t = 1$ $d=-9$ $t=-2$ $\begin{cases} d \equiv -9 \ (2^5) \\ d \equiv (3) \ (5) \end{cases}$ $d \equiv 23 \ (160)$

B vuole far arrivare ad A il messaggio $\mathbf{m=42}$

B calcola

$$f(m) = m^7 = 42^7 \equiv 15 \ (187)$$

$15 = c$

B invia ad A $c=15$

A riceve $c=15$ e applica f^{-1}

$$f^{-1}(15) \equiv 15^{23} \ (187)$$

$$\begin{cases} m \equiv 15^{23} \ (11) \\ m \equiv 15^{23} \ (17) \end{cases}$$

$15^{23} \equiv 4^{23} \equiv (4^{10})^2 (4)^3 \equiv 5 \cdot 4 \equiv -2 \ (11)$ ($4^{10} \equiv 1$)

$15^{23} \equiv (-2)^{23} \equiv (-2)^{16}(-2)^7 \equiv -2^9 \cdot 2^5 = 2^3 \equiv 8 \ (17)$

$$\begin{cases} m \equiv -2 \ (11) \\ m \equiv 8 \ (17) \end{cases}$$

$-2+11s = 8+17t$

$11s - 17t = 10$

$s = 4+17\lambda$

$t = 2+11\lambda$ $\Rightarrow$

$m = -2+11(4+17\lambda)$

$\equiv 42 \ (187)$

Gruppi

Def 1: G insieme $\neq \emptyset$ $\quad * : G \times G \longrightarrow G$ operazione

$(G, *)$ si dice GRUPPO se

1) $*$ è associativo $\quad \forall a,b,c \in G \quad a*(b*c) = (a*b)*c$
2) $\exists$ l'elemento neutro $\exists\, e \in G$ tale che
$\forall a \in G \quad e*a = a*e = a$
3) $\exists$ inverso di ogni elemento
$\forall a \in G \; \exists\, a'$ tale che
$a * a' = a' * a = e$

Def 2: Un gruppo si dice ABELIANO se $*$ è commutativo

Oss: Per verificare che $(G,*)$ è un gruppo occorre molto spesso anche che $* : G \times G \longrightarrow G$ cioè che G è chiuso rispetto all'operazione $*$

$$\left(\forall\, g_1, g_2 \in G \Rightarrow g_1 * g_2 \in G \right)$$

Esempi

1) K campo $(K, +, \cdot) \Rightarrow (K, +)$ è un gruppo abeliano, $(K \setminus \{0\}, \cdot)$ è un gruppo abeliano (K^*)

$\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ sono gruppi ab. rispetto a +

$\mathbb{R}^*, \mathbb{Q}^*, \mathbb{C}^*, (\mathbb{Z}/p\mathbb{Z})^*$ " " " " .

2) $(\mathbb{Z}, +)$ è un gruppo

$(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo

$\mathbb{Z}^\times = \{\pm 1\} \leftarrow (\mathbb{Z}^\times, \cdot)$ è un gruppo

$(\mathbb{Z}/n\mathbb{Z}^\times, \cdot)$ è un gruppo (visto le volte scorse)

3) $C_n = \{z \in \mathbb{C}^\times \mid z^n = 1\}$ $(C_n, \cdot)$ è un gruppo

$1 \in C_n$ $\quad 1^n = 1$ ↳ GRUPPO DELLE RADICI n-esime di 1

chiusura: $z, w \in C_n \Rightarrow z \cdot w \in C_n$

$z, w \in \mathbb{C}^\times \quad z^n = 1 \quad w^n = 1 \Rightarrow zw \in \mathbb{C}^\times$

$(zw)^n = \underbrace{(zw)\dots(zw)}_{n \text{ volte}} = z^n w^n = 1 \cdot 1 = 1$

↓ commutano

associatività: lo è in $\mathbb{C}^\times$

$1 \in C_n$ già detto

inverso $\quad z \in C_n \Rightarrow z \in \mathbb{C}^\times \quad z^n = 1$

$\Rightarrow z^{-1} \in \mathbb{C}^\times \quad (z^{-1})^n = z^{-n} = (z^n)^{-1} = 1^{-1} = 1$

commutativo ✓

$|C_n| = n$ ← dalla Teoria dei numeri complessi

$w_0 \in \mathbb{C}^\times$

$X = \{z \in \mathbb{C}^\times \mid z^n = w_0\}$ $(X, \cdot)$

So che $|X| = n$ $\quad w_0 \neq 0$

X è un gruppo $\iff w_0 = 1$

4) X insieme $\quad S(X) = \{ f : X \to X \text{ bigettive} \}$ PERMUTAZIONI DI X

$(S(X), \circ)$ è un gruppo.

$X \neq \emptyset \Rightarrow S(X) \ni id_X : X \to X$, $x \mapsto x$ è l'el neutro (verificato)

$\forall f, g \in S(X) \Rightarrow f \circ g \in S(X)$

$X \xrightarrow{g} X \xrightarrow{f} X$, $f \circ g$ ✓

- associatività $\forall f, g, h \in S(X) \quad f \circ (g \circ h) = (f \circ g) \circ h$

Devo vedere $f \circ (g \circ h)(x) = (f \circ g)(h(x))$

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

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

$\forall f \in S(X) \quad f^{-1} \in S(X)$. ok.

Se $|X| = n \quad S(X) \cong S_n \quad |S_n| = n!$

$S(\{1, \dots, n\})$

In generale $S(X)$ non è abeliano (non è ab se $|X| \geq 3$)

$1, 2, 3 \in X$

σ $1 \to 2$
$2 \to 3$
$3 \to 1$
$x \to x$ $\quad \forall x \neq 1,2,3$

t $1 \to 2$
$2 \to 1$
$x \to x$ $\quad \forall x \neq 1,2$

$\sigma \circ t \neq t \circ \sigma$ infatti $\sigma \circ t(1) = \sigma(2) = 3$
$t \circ \sigma(1) = t(2) = 1$

S_3 è un gruppo non abeliano con 6 elementi

$\sigma = (1\ 2\ 3)$ $\quad t = (1,2)$ $\quad 3 \to 3$ $\quad id =$

$\sigma^2 =$ $1 \to 3$
$2 \to 1$ $\quad (1\ 3\ 2)$
$3 \to 2$

$\sigma \circ t =$ $1 \to 2 \to 3$ $\quad (1,3)$
$2 \to 1 \to 2$
$3 \to 3 \to 1$

$t \circ \sigma$ $1 \to 2 \to 1$ $\quad (2,3)$
$2 \to 3 \to 3$
$3 \to 1 \to 2$

$S_3 = \{ id, \sigma, \tau, \sigma^2, \sigma\tau, t\sigma, \sigma^2\sigma \}$

$\sigma^2 \circ t =$ $1 \to 2 \to 1$
$2 \to 1 \to 3$ $\quad (2,3)$
$3 \to 3 \to 2$

$\sigma^3 =$ $1 \to 2 \to 3 \to 1$ $\quad \sigma^3 = id \quad t^2 = id$
$2 \to 3 \to 1 \to 2$
$3 \to 1 \to 2 \to 3$

Proposizione Sia $(G, \cdot)$ un gruppo. Allora

1) L'elemento neutro di G è unico
2) $\forall g \in G$ l'inverso di g è unico
3) $\forall g \in G \quad (g^{-1})^{-1} = g$
4) $\forall g, h \in G \quad (gh)^{-1} = h^{-1} g^{-1}$
5) Valgono le leggi di cancellazione

$$\forall a, b, c \in G \quad ab = ac \Rightarrow b = c$$

$$ba = ca \Rightarrow b = c$$

Dim: 1) $e, e_1 \in G$ elementi neutri

$$e_1 = e \cdot e_1 = e$$

(e_1 è il neutro; e è il neutro; e_1 è il neutro)

2) Siano a e b inversi di $x \in G$

$$b = e \cdot b = (ax)b = axb = a(xb) = a \cdot e = a$$

(e è inv di x; associativo; associativo; b è inverso di x)

3) $g \in G \quad (g^{-1})^{-1} = g$ ← per mostrarlo basta far vedere che g ha le proprietà dell'inverso di g^{-1}

$g \cdot g^{-1} = g^{-1} g = e$ ← questo è vero perché g^{-1} è l'inverso di g

4) Verifico che $h^{-1}g^{-1}$ è l'inverso di gh

$$(gh)(h^{-1}g^{-1}) = (h^{-1}g^{-1})(gh) = e$$ DA VERIFICARE

$$g(hh^{-1})g^{-1} = g\, e\, g^{-1} = gg^{-1} = e$$

$$= h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e$$

5) $$ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$$

$$\Rightarrow \underbrace{(a^{-1}a)}_{e} b = \underbrace{(a^{-1}a)}_{e} c \Rightarrow b = c$$

■

Def $(G,*)$ gruppo. $H \subseteq G$ $H \neq \emptyset$

H si dice sottogruppo di G $(H \leq G)$ se $(H, *_H)$ è un gruppo

$$(*_H : H \times H \to H)$$

Cioè se H è un gruppo con l'op indotta da G

Esempi: G, G, $\{e\}$ sono sottogruppi di G.

Proposizione $(G,\cdot)$ gruppo $H \subseteq G$, $H \neq \emptyset$.

$H \leq G \iff$ 1) H è chiuso rispetto a $\cdot$ $(\forall h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H)$

2) $\forall h \in H \Rightarrow h^{-1} \in H$

(IN non è un sgr di $\mathbb{Z}$. + (1) vale ma (2) no)

Dim: ($\Rightarrow$) ovvio

($\Leftarrow$) (1) dice che $\cdot$ è un'op su H

- è associativa - vera perché lo è in G
- $e \in H$ perché $H \neq \emptyset \Rightarrow \exists h \in H$

$\Rightarrow h^{-1} \in H \Rightarrow e = h h^{-1} \in H$ (2) (1)

- $\exists$ inverso: è la (2). □

Esempi

1) $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$

2) $C_n < \mathbb{C}^\times$

3) $\mathbb{Z}/n\mathbb{Z}^\times \not\leq \mathbb{Z}/n\mathbb{Z}$ perché sono gruppi rispetto a operazioni $\neq$.
non è un sottogruppo

4) $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ = insieme dei multipli di n

$\Rightarrow n\mathbb{Z} \leq \mathbb{Z} \quad \forall n$

$n = 0 \quad 0\mathbb{Z} = \{0\} < \mathbb{Z}$

$n\mathbb{Z} \neq \emptyset$, $0 \in n\mathbb{Z} \quad 0 = n \cdot 0$

chiuso rispetto a + $nk, nh \in n\mathbb{Z} \Rightarrow nk + nh = n(k+h) \in n\mathbb{Z}$
$\in \mathbb{Z}$

$\exists$ opposto $\quad x \in n\mathbb{Z} \quad x = nk \quad k \in \mathbb{Z}$

$-x = n(-k) \quad -k \in \mathbb{Z} \Rightarrow -x = n(k) \in n\mathbb{Z}.$

Oss: $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n$ (verificarlo)

$n\mathbb{Z} = m\mathbb{Z} \iff n \mid m \wedge m \mid n \iff n = \pm m$

Proposizione: G gruppo $H, K \leq G$.

- $H \cap K \leq G$
- $H \cup K$ è un sgr di $G \iff H \subseteq K \vee K \subseteq H$

Verificare per esercizio

Def: G gruppo. $Z(G) = \{ g \in G \mid gx = xg \ \forall x \in G \}$

↳ CENTRO di G

Prop: 1) $Z(G) \leq G$

2) $Z(G) = G \iff G$ è abeliano

Dim: . $Z(G) \ni e$ perché $ex = xe (= x) \ \forall x \in G$

. chiuso rispetto all'op.

➡ $g_1, g_2 \in Z(G) \Rightarrow g_1 g_2 \in Z(G)$

$(g_1 x = x g_1, \ g_2 x = x g_2 \quad \forall x \in G)$

$g_1 g_2 \in G$ perché $g_1, g_2 \in G$ e G è gruppo.

$(g_1 g_2)x = g_1(g_2 x) = g_1(x g_2) = (g_1 x) g_2 = (x g_1) g_2 = x(g_1 g_2)$

ass $\quad g_2 \in Z(G)$ $\quad$ ass.

$\forall x \in G \Rightarrow g_1 g_2 \in Z(G)$

- $\forall g \in Z(G) \Rightarrow g^{-1} \in Z(G)$

$g^{-1} \in G \qquad g^{-1} x = x g^{-1} \quad \forall x \in G$ ←

So che $\quad gx = xg \quad \forall x \in G$ (perché $g \in Z(G)$)

moltiplico a sx per g^{-1}

$g^{-1} g x = g^{-1} x g$

$x = g^{-1} x g$

moltiplico a dx per g^{-1}

$x g^{-1} = g^{-1} x g g^{-1} = g^{-1} x \quad \forall x \in G$

(in e)

- G è abeliano $\iff Z(G) = G$

$\Leftarrow$

Basta osservare che $Z(G)$ è abeliano; infatti

se $g, h \in Z(G) \qquad gh = hg$

Richiamo la costruzione di $n\mathbb{Z}$ in un gruppo generico

$n\mathbb{Z} = \{kn\}_{k \in \mathbb{Z}}$

$x \in G \qquad \{x^k\}_{k \in \mathbb{Z}}$

Pongo $\langle x \rangle \doteq \{x^k\}_{k \in \mathbb{Z}}$ SOTTOGRUPPO GENERATO DA x

($x^0 = e$ $\quad h > 0 \quad x^h = \underbrace{x \cdot \ldots \cdot x}_{h \text{ volte}}$ $\quad h < 0 \quad n = -m \quad m > 0$

$x^n = (x^m)^{-1} = (x^{-1})^m$

Valgo le usuali proprietà delle potenze)

Proposizione G gruppo $x \in G$

1. $\langle x \rangle$ è un sgr di G
2. $\langle x \rangle$ è abeliano.

Dim 1) è ovvio $x \in \langle x \rangle \Rightarrow \langle x \rangle \neq \emptyset$

$x^m, x^n \in \langle x \rangle = \{x^k\}_{k \in \mathbb{Z}}$ $\quad x^h x^m = x^{h+m} \in \langle x \rangle$

x^{-n} è l'inverso di x^n

2) $\langle x \rangle$ è abeliano perché

$\forall\, x^n, x^m \in \langle x \rangle \qquad x^h \cdot x^m = x^{h+m} = x^{m+n} = x^m \cdot x^h$

$\forall\, n, m$ $\qquad \square$

Esempio S_3 $\qquad \langle \sigma \rangle = \{id, \sigma, \sigma^2\}$ $\quad \langle \tau \rangle = \{id, \tau\}$

Lezione 09 — 3 novembre '21

G gruppo $\quad x \in G \quad \langle x \rangle = \{x^k\}_{k \in \mathbb{Z}}$

- $\langle x \rangle$ è un sottogruppo di G

Oss: Se G è un gruppo finito $\langle x \rangle$ è finito.

($x \in G \Rightarrow x^k \in G \quad \forall k \in \mathbb{Z}$.

Anche se G è infinito $\langle x \rangle$ potrebbe essere finito. - Risposta banale $G = \mathbb{Z} \quad x = 0$

$\langle 0 \rangle = \{k0\} = \{0\}$

Provo a fare di meglio $\quad n \in \mathbb{Z} \quad \langle n \rangle = \{kn\}_{k \in \mathbb{Z}} = n\mathbb{Z}$

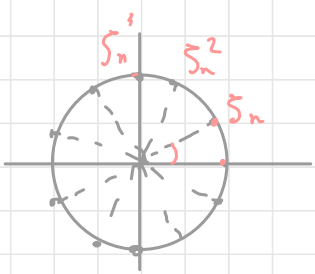
non finisce $\quad (\langle n \rangle) = +\infty$.

- $G = \mathbb{C}^\times \quad x = \zeta_n$ = radice n-esima di $1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$

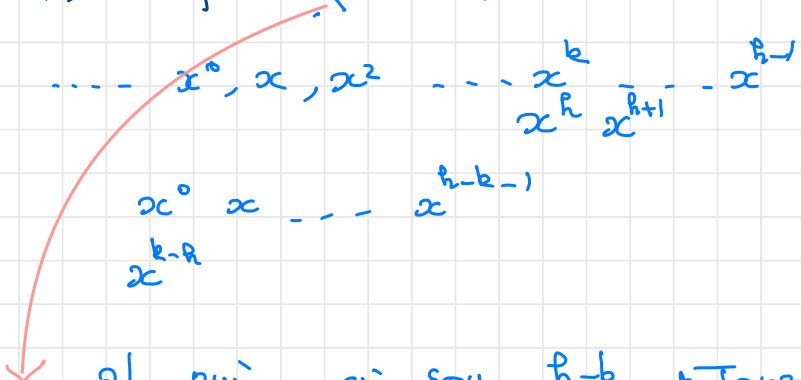
$$\langle \zeta_n \rangle = \{\zeta_n^k\}_{k \in \mathbb{Z}} = \{\dots\}$$

↑ sono tutte radici n-esime di 1 $\Rightarrow$ sono al più n.

(Scriverle e vedere che sono esattamente n cioè che $\langle \zeta_n \rangle$ è il gruppo delle radici n-esime di 1.



$\langle x \rangle$ è finito $\iff \exists\, h>k \quad x^h = x^k \iff x^{h-k} = e$



al più ci sono $h-k$ potenze di x distinte perché $x^h = x^k$ $\Rightarrow$ le potenze di x si ripetono ciclicamente.

$\langle x \rangle$
- le potenze di x sono tutte distinte $\Rightarrow |\langle x \rangle| = +\infty$
- $\exists\, h,k$ tali che $x^h = x^k \Rightarrow |\langle x \rangle|$ è finito

perché le potenze di x si ripetono ciclicamente.

Def $x \in G$ $\quad \mathrm{ord}_G(x) = \min \{ k>0 \mid x^k = e \}$

se $\{ k>0 \mid x^k = e \} = \emptyset$ poniamo $\mathrm{ord}_G(x) = +\infty$

$\mathrm{ord}_{\mathbb{K}^*} \zeta_n = n$ $\qquad \mathrm{ord}_{\mathbb{Z}} 7 = +\infty$

Proposizione: $x \in G$ $\quad \mathrm{ord}(x) = d < +\infty$

Allora $\langle x \rangle = \{ e, x, x^2, \dots, x^{d-1} \}$

- $|\langle x \rangle| = d$ l'ordine del gruppo $\langle x \rangle$ è uguale all'ordine di x
- $x^n = e \iff d \mid n$ ($d = \mathrm{ord}(x)$)

Oss $x^{100000} \equiv 1 \quad (7)$

$x \in \mathbb{Z}/7\mathbb{Z}^* \qquad x^{\phi(7)} \equiv 1 \ (7) \Rightarrow \text{ord}\, x \mid \phi(7) = 6$

$x^{100\cdot000} \equiv 1 \ (7) \qquad \text{ord}\, x \mid 100\cdot000$

$\Rightarrow \text{ord}\, x \mid (6, 100\cdot000) = 2$

$x^{100\cdot000} \equiv 1 \quad (7) \iff x^2 \equiv 1 \quad (7) \iff x \equiv \pm 1 \ (7)$

Dim:

$\#\{e, x, \dots, x^{d-1}\} = d \qquad x^a = x^b \quad d > a > b$

$x^{a-b} = e \quad 0 < a-b < d$

→ non è possibile perché $d = \min\{k > 0 \mid x^k = e\}$

perciò le potenze $e = x^0, x^1, \dots, x^{d-1}$ sono distinte

$\{e, x, \dots, x^{d-1}\} \subseteq \langle x \rangle \Rightarrow |\langle x \rangle| \geq d$

dico che $=$

$\langle x \rangle \ni x^n \qquad n = qd + r \qquad 0 \leq r < d \qquad n \in \mathbb{Z}$

$x^{qd+r} = (x^d)^q x^r = x^r \Rightarrow x^n = x^r \in \{0, x, \dots, x^{d-1}\}$

$x^d = e$

→ $\langle x \rangle \subseteq \{e, x, \dots, x^{d-1}\} \Rightarrow$ sono $= \Rightarrow |\langle x \rangle| = d$

- $x^n = e \iff d \mid n$

$\Leftarrow$ $d \mid n \Rightarrow n = qd$ $\quad x^n = (x^d)^q = e$

$\Rightarrow$ $\quad n = qd + r \quad 0 \le r < d$

$e = x^n = x^r \quad r < d$ e $\{x^0 = e, x, \dots, x^{d-1}\}$ sono distinti.

$\Rightarrow \quad r = 0$ $\quad \square$

Oss: Se $\operatorname{ord} x = +\infty \Rightarrow |\langle x \rangle| = +\infty$

Def: Un gruppo G si dice CICLICO se

$\exists\, x \in G$ tale che $G = \langle x \rangle$

x si chiama generatore di G.

Esempi

1) $\mathbb{Z}$ è ciclico $\quad \mathbb{Z} = \langle 1 \rangle = \{k \cdot 1\}_{k \in \mathbb{Z}} = \{k\}_{k \in \mathbb{Z}}$.

$(\mathbb{Z} = \langle -1 \rangle)$ ± 1 sono gli unici generatori di $\mathbb{Z}$.

2) $\mathbb{R}$ non è ciclico ....

3) $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle = \{k [1]_n\}_{k \in \mathbb{Z}} = \{[k]_n\}_{k \in \mathbb{Z}}$

4) $(\mathbb{Z}/8\mathbb{Z})^\times$ non è ciclico. $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$(\mathbb{Z}/8\mathbb{Z})^\times$ è ciclico $\Leftrightarrow$ contiene un el di ordine 4.

$x^2 \equiv 1 \quad (8) \quad \forall x$ dispari

$\Rightarrow \bar{1}$ ha ordine 1

Se $\bar{x} \neq \bar{1}$ $\bar{x}$ ha ordine 2

non ci sono el di ordine 4

5) p, q primi distinti dispari $\Rightarrow \left(\mathbb{Z}/_{pq}\right)^*$ non è ciclico

ha ordine $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$

Mostro che $\forall x \in \mathbb{Z} \quad x^{\frac{(p-1)(q-1)}{2}} \equiv 1 \quad (pq)$

Esercizio: $\mathbb{Z}/_{11\mathbb{Z}}^{\times}$ è ciclico.

Devo dire che $\exists x$ $\text{ord}\, x = \phi(11) = 10$

So che $x^{\phi(11)} \equiv 1 \quad (11)$ per il T di Eulero,

$\text{ord}\, x = d$? $\quad d \mid \phi(11) = 10$

$2^2 \equiv 4 \quad (11)$

$2^5 \equiv -1 \quad (11)$

$\Rightarrow \text{ord}\, \bar{2} = 10 \Rightarrow \mathbb{Z}/_{11\mathbb{Z}}^{\times} = \langle \bar{2} \rangle$

Teorema: Ogni sgr di un gruppo ciclico è ciclico.

Dim: $G = \langle g \rangle \quad H \leq G$

$H = \begin{cases} H = \{e\} = \langle e \rangle & \checkmark \\ H \neq \{e\} \quad \exists h \in H \ h \neq e, \ h = g^k \ k \in \mathbb{Z} \end{cases}$

$g^k, g^{-k} \in H$ quindi posso prendere $k > 0$

$S = \{ m > 0 \mid g^m \in H \}$ $\quad \phi \neq S \subset \mathbb{N}$

Sia $m_0 = \min S$ $\quad g^{m_0} \in H$

Dico che $H = \langle g^{m_0} \rangle$

$\supset$ ovvio

$\subset$ con la div per m_0

Concludere la dimo

Sottogruppi di $\mathbb{Z}$.

I sottogruppi di $\mathbb{Z}$ sono tutti del tipo $n\mathbb{Z}$ $n \in \mathbb{Z}$

Inoltre $n\mathbb{Z} = m\mathbb{Z} \iff m = \pm n$

- $\mathbb{Z}$ è ciclico $\quad \mathbb{Z} = \langle 1 \rangle$
- $H \leq \mathbb{Z}$ $\quad H$ è ciclico $\quad H = \langle n \rangle = n\mathbb{Z}$ $\quad n \in \mathbb{Z}$

$\langle n \rangle = \langle m \rangle$ (= $n\mathbb{Z} = m\mathbb{Z}$) $\iff n\mathbb{Z} \subset m\mathbb{Z} \wedge m\mathbb{Z} \subset n\mathbb{Z}$.

$n\mathbb{Z} \subset m\mathbb{Z} \iff m \mid n$

($\Rightarrow$) $n \in m\mathbb{Z} \Rightarrow n = mk$ per $k \in \mathbb{Z} \Rightarrow m \mid n$

($\Leftarrow$) $m \mid n \Rightarrow n = mk$ $k \in \mathbb{Z} \Rightarrow n \in m\mathbb{Z}$

se $x \in n\mathbb{Z}$ $\quad x = nz = m \underbrace{kz}_{\in \mathbb{Z}} \in m\mathbb{Z}$

Es: $m\mathbb{Z} \cap n\mathbb{Z}$.

Il gruppo $\mathbb{Z}/n\mathbb{Z}$

È ciclico $\quad \mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle \qquad \text{ord}\, \bar{1} = n$

$\bar{a} \in \mathbb{Z}/n\mathbb{Z} \qquad \text{ord}_{\mathbb{Z}/n\mathbb{Z}}\, \bar{a} = \min\{k > 0 \mid k\bar{a} = \bar{0}\}$

Per trovarlo devo trovare la minima sol positiva della congruenza $\quad xa \equiv 0 \quad (n)$

$ax \equiv 0 \quad (n)$

$(a,n) = d \qquad a = a_1 d \qquad n = n_1 d$

$\Downarrow$

$(a_1, n_1) = 1$

$d a_1 x \equiv 0 \quad (d n_1)$

$\Updownarrow$

$x \equiv 0 \quad (n_1)$

$(a_1, n_1) = 1$

La minima sol positiva della congruenza è

$$x = n_1 = \frac{n}{(a,n)}$$

$$\boxed{\text{ord}_{\mathbb{Z}/n\mathbb{Z}}\, \bar{a} = \frac{n}{(a,n)}}$$

in particolare $\text{ord}\, \bar{a} \mid n$

Esempio $\mathbb{Z}/20\mathbb{Z}$ ha ordine $20 = 2^2 \cdot 5$

$1, 2, 4, 5, 10, 20$

$\text{ord}\,\bar{a} = \frac{n}{(a,n)} = \frac{20}{(a,20)}$

$\text{ord}\,\bar{a} = 1 \iff (a,n) = n \iff \bar{a} = \bar{0}$ (1) $= \phi(1)$

$\text{ord}\,\bar{a} = 2 \iff (a,20) = 10 \iff a = 10k \quad k \equiv 1\ (2)$
$\bar{a} = \bar{10}$ (1) $= \phi(2)$

$\text{ord}\,\bar{a} = 4 \iff (a,20) = 5$
$\bar{a} = \bar{5}, \bar{15}$ (2) $= \phi(4)$

$\text{ord}\,\bar{a} = 5 \iff (a,20) = 4 \quad \bar{a} = \bar{4}, \bar{8}, \bar{12}, \bar{16}$ (4) $= \phi(5)$

$\text{ord}\,\bar{a} = 10 \iff (a,20) = 2 \quad \bar{a} = \bar{2}, \bar{6}, 14, 18$ $4 = \phi(10)$

$\text{ord}\,\bar{a} = 20 \iff (a,20) = 1 \quad \bar{a} = \bar{1}, \bar{3}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{17}, \bar{19}$

$\bar{a}$ è un generatore di $\mathbb{Z}/20\mathbb{Z}$ ↖ sono $\phi(20) = \phi(4)\phi(5) = 8$

Conseguenze

1) $\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z} \quad \text{ord}\,\bar{a} \mid n$

2) $\bar{a}$ genera $\mathbb{Z}/n\mathbb{Z} \iff (a,n) = 1$, quindi $\mathbb{Z}/n\mathbb{Z}$ ha $\phi(n)$ generatori

3) $\forall d \mid n$ in $\mathbb{Z}/n\mathbb{Z}$ ci sono ESATTAMENTE $\phi(d)$ elementi di ordine d.

Dimostriamo 3. $\text{ord}\,\bar{a} = \frac{n}{(a,n)} = d \iff$

$(a, n) = \frac{n}{d} \quad \Rightarrow \quad a = \frac{n}{d} k \qquad (k, d) = 1$

(perché $a = \frac{n}{d} k \qquad (a, n) = \frac{n}{d}(k, d) = \frac{n}{d}$)

$0 \le a < n$

$0 \le \frac{n}{d} k < n \qquad 0 \le k < d \qquad (k, d) = 1$

sono $\phi(d)$

Corollario $\sum_{d \mid n} \phi(d) = n$

Dim: $n = |\mathbb{Z}/n\mathbb{Z}|$

$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d \mid n} X_d \qquad X_d = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{ord}\, \bar{a} = d\}$

$n = \sum_{d \mid n} |X_d|$ nel (3) abbiamo detto che $|X_d| = \phi(d)$

$n = \sum_{d \mid n} \phi(d)$

Sottogruppi di $\mathbb{Z}/n\mathbb{Z}$

Dal Teorema so che sono ciclici → sono del Tipo

$H = \langle \bar{a} \rangle \longrightarrow |H| = \text{ord}\, \bar{a} \longrightarrow$ ci sono sgr di

ordine $d \iff d \mid n$

$\mathbb{Z}/n\mathbb{Z}$ ha un unico sgr di ordine d $\forall d \mid n$

$H \leq \mathbb{Z}/n\mathbb{Z}$ $\quad H = \langle \bar{a} \rangle$ $\quad |H| = \text{ord}\,\bar{a} = d \mid n$.

$H_d = \{\bar{0}, \frac{\overline{n}}{d}, \frac{\overline{n}}{d}2, \dots, \frac{\overline{n}}{d}(d-1)\} = \langle \frac{\overline{n}}{d} \rangle$

$\subseteq$ chiaro

+ hanno la stessa card.

H_d contiene tutti gli el di ordine d $\left(\frac{\overline{n}}{d}k \quad (k,d)=1\right)$

$\Rightarrow$ ogni sgr di ordine d coincide con H_d

□

Lezione 10 — 8 novembre

Def $(G, *)$ $(G', *')$

$f: G \to G'$ è un omomorfismo di gruppi

$\forall x, y \in G \quad f(x * y) = f(x) *' f(y)$

Esempi

1) G, G' gruppi $\quad f: G \to G'$, $x \mapsto e'$

f è un omo. $f(x * y) = f(z) = e'$ ($z \in G$)

$f(x) *' f(y) = e' *' e' = e'$

2) $\mathrm{id}: G \to G$, $x \mapsto x$ omo

3) $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

$a \mapsto \overline{a}$ è un omo

$\pi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \pi(a) + \pi(b)$

Se $m \mid n$ $\quad \pi_{n,m} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ è omo

$[a]_n \mapsto [a]_m$

- è ben definita ←
- $\pi_{n,m}([a]_n + [b]_n) = \pi_{n,m}([a]_n) + \pi_{n,m}([b]_n)$

$\forall [a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z}$

$[a]_4 \longrightarrow [a]_3$ NO

$[1]_4 = [5]_4$

$\downarrow \quad \downarrow$

$[1]_3 \neq [2]_3$ non è ben definita.

4) $\varphi\ (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \cdot)$

$x \longmapsto e^x$ omo

$\varphi(x+y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$. $\forall x, y \in \mathbb{R}$.

Proprietà degli omomorfismi

$f: G \longrightarrow G'$ omo di gruppi

1) $f(e) = e'$

2) $f(x^{-1}) = f(x)^{-1}$ $\forall x \in G$

3) $\forall H \leq G \quad f(H) \leq G'$

In particolare $f(G) \leq G'$

4) $\forall K \leq G'$ $f^{-1}(K) \leq G$. In particolare

$\ker f = f^{-1}(e') = \{ x \in G \mid f(x) = e' \} \leq G$

5) f è iniettivo $\iff \ker f = \{e\}$

6) Se f è bigettivo $\Rightarrow f^{-1}$ è un omomorfismo

Dim ① $f(e) = f(ee) = f(e)f(e) \Rightarrow e' = f(e)$

$ee=e$ — f omo — cancellazione

④ $K \leq G'$ $f^{-1}(K) = \{ x \in G \mid f(x) \in K \}$

. $e \in f^{-1}(K)$ perché $f(e) = e' \in K$ perché K sgr di G'

. $\forall x, y \in f^{-1}(K) \Rightarrow xy \in f^{-1}(K)$

$xy \in G$ perché prodotto di el di G

$f(xy) \in K$

$f(x)f(y) \in K$ perché prodotto di 2 el di K e $K \leq G'$

$\Uparrow$ K $x \in f^{-1}(K)$ perché $y \in f^{-1}(K)$

. $x \in f^{-1}(K) \Rightarrow x^{-1} \in f^{-1}(K)$

$x^{-1} \in G$ ovvio

$f(x^{-1}) = f(x)^{-1} \in K$ vero in quanto $f(x) \in K$ ($\Leftarrow x \in f^{-1}(K)$) + K sgr

(2)

5) f è iniettivo $\iff \ker f = \{e\}$

($\Rightarrow$) $f(x) = e' \iff x = e$

$$\ker f = \{x \in G \mid f(x) = e'\} = \{e\}$$

($\Leftarrow$) $f(x) = f(y) \Rightarrow f(x) f(y^{-1}) = e'$

$$f(x y^{-1}) = e'$$

$\Rightarrow x y^{-1} = e \Rightarrow x = y$

Proposizione: $f\ G \to G'$ omo.

1. $\forall x \in G \quad \text{ord}\, f(x) \mid \text{ord}\, x$ (convenzione $n \mid \infty\ \forall n$)
2. f è iniettivo $\iff \text{ord}\, f(x) = \text{ord}\, x \quad \forall x \in G$

Dim: 1. $+\infty > d = \text{ord}\, x = \min\{k > 0 \mid x^k = e\} \quad x \in G$

$x^d = e$

$f(x)^d = f(x^d) = f(e) = e'$

$\Rightarrow \text{ord}\, f(x) \mid d$

Se $\text{ord}\, x = +\infty$ non c'è niente da dim.

2. ($\Leftarrow$) $x \in \ker f$ devo dimostrare che $x = e$

$f(x) = e' \Rightarrow \text{ord}\, f(x) = 1 \Rightarrow \text{ord}\, x = 1 \Rightarrow x = e$

($\Rightarrow$) Se $\operatorname{ord} f(x) = +\infty$ $\overset{1.}{\Rightarrow}$ $\operatorname{ord} f(x) = +\infty \mid \operatorname{ord} x \Rightarrow \operatorname{ord} x = +\infty$.

Sia $\operatorname{ord} f(x) = n \Rightarrow f(x)^n = e'$

$\Rightarrow f(x^n) = f(x)^n = e'$

poiché f è iniettivo $\Rightarrow x^n = e \Rightarrow \operatorname{ord} x \mid n = \operatorname{ord} f(x)$

Da 1. ho che $\operatorname{ord} f(x) \mid \operatorname{ord} x \Rightarrow \operatorname{ord} x = \operatorname{ord} f(x)$

Def $f: G \to G'$ omo biiettivo $\to$ **ISOMORFISMO**.

Oss: Gruppi isomorfi sono "indistinguibili" dalle proprietà di gruppo.

- hanno la stessa cardinalità
- hanno elementi degli stessi ordini

$f: G \xrightarrow{\sim} G' \qquad \operatorname{ord} x = \operatorname{ord} f(x)$

- gruppi isomorfi hanno "gli stessi" sottogruppi

$$\{H \leq G\} \longleftrightarrow \{K \leq G'\}$$

$$H \xrightarrow{\varphi} f(H)$$

$$f^{-1}(K) \xleftarrow{\psi} K$$

$\varphi \circ \psi (K) = K \qquad f \circ f^{-1}(K) = K$

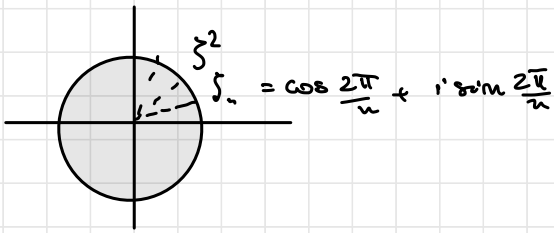
$\psi \circ \varphi (H) = H \qquad f^{-1} \circ f(H) = \ker f \cdot H = \ker_G(H) = H$

Esempio $C_n = \{ z \in \mathbb{C}^\times \mid z^n = 1 \}$

$C_n < \mathbb{C}^\times$

$|C_n| = n$

$C_n = \langle \zeta_n \rangle$



$C_n \cong \mathbb{Z}/n\mathbb{Z}$

$\zeta^a \longleftarrow \bar{a}$ è un isomorfismo.

Teorema

G ciclico $\Rightarrow$ $\cdot\ |G| = +\infty \quad G \cong \mathbb{Z}$

$\cdot\ |G| = n \quad G \cong \mathbb{Z}/n\mathbb{Z}$

Dim. $G = \langle g \rangle$ $\leftarrow$ G è ciclico

$|G| = +\infty \qquad \langle g \rangle = \{ g^k \}_{k \in \mathbb{Z}} \qquad g^m \neq g^k \ \ \forall m \neq k$

$(g^{m-k} = e)$

$\varphi : \mathbb{Z} \longrightarrow G$

$k \longmapsto g^k$

dico che φ è iso.

φ omo: $\varphi(k+h) = \varphi(k) \cdot \varphi(h) \qquad \forall h, k \in \mathbb{Z}.$

$$\varphi(k+h) = g^{k+h} = g^k g^h = \varphi(k)\cdot\varphi(h)$$

φ è iniettivo: $\varphi(m) \neq \varphi(k) \quad \forall\, m \neq k$

φ è su: ovvio $\operatorname{Im} f = \{g^k\}_{k\in\mathbb{Z}} = \langle g\rangle = G$

$|G| = n \qquad \varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$

$\bar{a} \longmapsto g^a$

φ è ben definita: $\bar{a} = \bar{b} \Rightarrow g^a = g^b$

$\bar{a} = \bar{b} \iff a \equiv b \ (n) \iff b = a + hn \quad h \in \mathbb{Z}$

$g^b = g^{a+hn} = g^a (g^n)^h = g^a$

($g^n = e$ perché $|G| = n$, quindi $\operatorname{ord} g = n$)

φ è omo $\qquad \varphi(\bar{a} + \bar{b}) = g^{a+b} = g^a g^b = \varphi(\bar{a})\varphi(\bar{b})$

φ è su $\qquad \operatorname{Im}\varphi = \{g^0, g^1, \dots, g^{n-1}\} = \langle g\rangle = G$

($\operatorname{ord} g = n$)

Poiché $|\mathbb{Z}/n\mathbb{Z}| = |G| = n < +\infty \Rightarrow \varphi$ è biettivo

e quindi è un iso $\qquad \square$

Conseguenza: Sappiamo tutto sui gruppi ciclici.

$G = \langle g\rangle$ infinito. Tutti i suoi elementi $\neq e$ hanno

ordine ∞

- $H \leq G \Rightarrow H = \langle g^n \rangle$ per qualche n

$\left(\{n\mathbb{Z}\}_{n \in \mathbb{N}} \longleftrightarrow \{H \leq G\} \right)$ $\quad \varphi(n\mathbb{Z}) = \langle g^n \rangle$

$\varphi(nk) = g^{nk}$

$G = \langle g \rangle$ $|G| = n$. ha $\phi(d)$ el di ordine d

$\forall d \mid n$ (non ci sono el di ordine h se $h \nmid n$)

- Ha un unico sgr di ordine d $\forall d \mid n$

E se $H \leq G \Rightarrow |H| \mid |G|$

($d \mid n$ in $\mathbb{Z}/n\mathbb{Z}$ il sgr di ordine d

$H_d = \langle \frac{n}{d} \rangle = \{k \frac{n}{d}\}_{k=0,\dots,d-1} \xrightarrow{\varphi} \langle g^{n/d} \rangle$

Esempio $\mathbb{Z}/n\mathbb{Z} \cong C_n = \langle e^{i\frac{2\pi}{n}} \rangle$

- $n = 100$ chi è il sgr di ordine 20 di C_{100}?

è quello generato da $\left(e^{\frac{2\pi i}{100}}\right)^{\frac{100}{20}} = \langle e^{\frac{10\pi}{100} i} \rangle$

- Chi sono gli el di ordine n di C_n?

So che sono $\phi(n)$ e sono le immagini degli el di ordine n di $\mathbb{Z}/n\mathbb{Z}$

$\{ \bar{a} \mid (a,n)=1 \} \xrightarrow{\varphi} \{ g^a \mid (a,n)=1 \}$

$\uparrow$

el di ordine n di $\mathbb{Z}/n\mathbb{Z}$

$e^{\frac{2\pi k i}{n}} \qquad (k,n)=1$

Oss ovvia: Ogni gruppo ciclico è abeliano

Il viceversa è falso $\mathbb{Z}/8\mathbb{Z}^*$

PRODOTTO DIRETTO DI GRUPPI

$(G_1, *_1)$ $(G_2, *_2)$ gruppi

$G_1 \times G_2 = \{ (x,y) \mid x \in G_1 \ y \in G_2 \}$ ← prodotto cartesiano

Definiamo su $G_1 \times G_2$ un'operazione componente per componente

$$(a,b) * (c,d) = (a *_1 c, b *_2 d)$$

Proposizione 1. $(G_1 \times G_2, *)$ è un gruppo (prodotto diretto)

2. $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$

3. $\text{ord}(x,y) = [\text{ord}_{G_1}(x), \text{ord}_{G_2}(y)]$

Dim 1. Esercizio

2. $Z(G) = \{ x \in G \mid xg = gx \ \forall g \in G \}$

$(x,y) \in Z(G_1 \times G_2) \quad \forall (g_1, g_2) \in G_1 \times G_2$

$(x,y) * (g_1,g_2) = (g_1,g_2) * (x,y)$

$(x *_1 g_1,\ y *_2 g_2) = (g_1 *_1 x,\ g_2 *_2 y)$

$\Leftrightarrow \quad x *_1 g_1 = g_1 *_1 x \qquad \forall g_1 \in G_1$

$y *_2 g_2 = g_2 *_2 y \qquad \forall g_2 \in G_2$

$\Leftrightarrow \quad x \in Z(G_1) \ \wedge \ y \in Z(G_2)$

3. $m = \operatorname{ord}_{G_1}(x) \qquad n = \operatorname{ord}_{G_2}(y) \qquad d = \operatorname{ord}_{G}(x,y)$

Tesi $d = [x,y]$

$(x,y)^{[m,n]} = (x^{[m,n]}, y^{[m,n]}) = (e_1, e_2)$

$m \mid [m,n]$

$n \mid [m,n]$

$\Rightarrow o(x,y) = \operatorname{ord}(x,y) \mid [m,n]$

D'altra parte $(x,y)^d = (e_1, e_2)$

$(x,y)^d = (x^d, y^d) = (e_1, e_2) \Leftrightarrow x^d = e_1 \Leftrightarrow \operatorname{ord} x \mid d$

$y^d = e_2 \Leftrightarrow \operatorname{ord} y \mid d$

$\Rightarrow [\operatorname{ord} x, \operatorname{ord} y] = [m,n] \mid d$

Esempio $\mathbb{Z}/_3 \times \mathbb{Z}/_2 = \{(0,0), (0,1), (1,0) (1,1) (2,0), (2,1)\}$

$(2,0) + (2,1) = (4,1) = (1,1)$

$\text{ord}(0,0) = 1$
$\text{ord}(0,1) = 2$
$(1\,0) \to 3$
$(1,1) \to 6$
$(2,0) \to 3$
$(2,1) \to 6$

$\mathbb{Z}/_3 \times \mathbb{Z}/_2$ è un gruppo di ordine 6 che ha el di ordine 6 $\to$ è ciclico!

$\mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \cong \mathbb{Z}/_{6\mathbb{Z}}$

② $\mathbb{Z}/_2 \times \mathbb{Z}/_2 = \{(0,0), (01), (1,0) (1,1)\}$

$1 \quad 2 \quad 2 \quad 2$

è un gruppo abeliano non ciclico.

$\mathbb{Z}/_2 \times \mathbb{Z}/_2 \cong \mathbb{Z}/_{8\mathbb{Z}}^{\times}$ ← esercizio.

③ $\mathbb{Z}/_3 \times \mathbb{Z}/_3$

Teorema cinese del resto (III forma)

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z} \iff (m,n) = 1$$

Dim: $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ $\quad |G| = mn$

Dimostrare $G \cong \mathbb{Z}/mn\mathbb{Z}$ è equivalente a mostrare che è ciclico. E questo è vero $\iff \exists\, g \in G$ ord $g = |G| = mn$.

$g = (\bar{x}, \bar{y})$ $\quad \bar{x} \in \mathbb{Z}/m\mathbb{Z}$ $\quad \bar{y} \in \mathbb{Z}/n\mathbb{Z}$.

$$\text{ord}(\bar{x}, \bar{y}) = \text{mcm}\left(\text{ord}_m \bar{x}, \text{ord}_n \bar{y}\right)$$

$$\text{ord}\, x = \frac{m}{(m,x)} \qquad \text{ord}\, \bar{y} = \frac{n}{(n,y)}$$

$$\text{ord}\, g = \text{ord}(\bar{x}, \bar{y}) = \left[\frac{m}{(m,x)}, \frac{n}{(n,y)}\right] \leq [m,n] = \frac{mn}{(m,n)}$$

$[m,n] < mn$

Se $(m,n) > 1 \Rightarrow$ G non è ciclico perché non ha elementi di ordine mn.

Se $(m,n) = 1$ $\quad g = (\bar{1}, \bar{1})$ ha ordine $[\text{ord}_m \bar{1}, \text{ord}_n \bar{1}]$

$[m,n] = mn$

∎

Teorema cinese del resto

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z} \iff (m,n)=1$$

$\mathbb{Z}/mn\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z} \supseteq$ anello

$\Leftarrow$ $\text{ord}(\bar{1},\bar{1}) = [m,n] = mn$

$(\Rightarrow)$ ....

Sapevamo che la mappa

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$[a]_{mn} \longmapsto ([a]_m, [a]_n)$$

se $(m,n)=1$ è biiettiva.

Si verifica che φ è anche un omo, cioè

$$\varphi([a+b]_{mn}) = \varphi([a]_{mn}) + \varphi([b]_{mn})$$

$\forall\, [a], [b] \in \mathbb{Z}/mn\mathbb{Z}$.

Corollario $(m,n)=1 \Rightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/mn\mathbb{Z})^*$

Dim

Abbiamo già visto che $\varphi^* : (\mathbb{Z}/mn\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$

$[a] \longmapsto ([a]_m, [a]_n)$

è biiettiva, basta

puoi verificare che è un omo

$$\varphi^*([a\cdot b]_{mn}) = \varphi^*([a]_{mn}) \cdot \varphi^*([b]_{mn})$$

→ verifica semplice (esercizio).

Oss. p, q primi distinti $p \neq q \Rightarrow \mathbb{Z}/pq^*$ non è ciclico.

$$\mathbb{Z}/pq\mathbb{Z}^* \cong \mathbb{Z}/p\mathbb{Z}^* \times \mathbb{Z}/q\mathbb{Z}^*$$

Per dire che NON è ciclico basta dire che ha una proprietà dei ciclici. Qui vedo che ha almeno 3 el di ordine 2, mentre un gruppo ciclico ha $\phi(2)$ el di ordine 2 $\times$ $2 \mid |G| - 1$

altrimenti

$$\left|\mathbb{Z}/pq^*\right| = (p-1)(q-1) \text{ pari}$$

$(-\bar{1}, \bar{1})$, $(\bar{1}, -\bar{1})$, $(-1, -1)$ hanno tutti ordine 2.

G gruppo $H \leq G$. Definisco una relazione su G ponendo $x \sim_H y$ se $y^{-1}x \in H$ RELAZIONE SX MODULO H

$\sim_H$ è una rel di equivalenza.

- $x \sim_H x \iff x^{-1}x = e \in H$ ✓
- $x \sim_H y \Rightarrow y \sim_H x$ $\quad y^{-1}x \in H \Rightarrow x^{-1}y = (y^{-1}x)^{-1} \in H \Rightarrow y \sim_H x$
- $x \sim_H y \quad y \sim_H z \Rightarrow x \sim_H z$

$y^{-1}x \in H \quad z^{-1}y \in H \Rightarrow (z^{-1}y)(y^{-1}x) \in H$

$z^{-1}x \in H \Rightarrow x \sim_H z$

Ne segue che la rel di equiv. (congruenza) mod H definisce delle classi di equivalenza che danno una partizione di G.

$$[x]_H = \{y \in G \mid y \sim x\} = \{y \in G \mid x^{-1}y \in H\} =$$

$$= \{y \in G \mid y \in xH\} = xH$$

" $\{xh \mid h \in H\}$

classe laterale sx di H

Esempio $G = \mathbb{Z}$ $\quad H = n\mathbb{Z}$

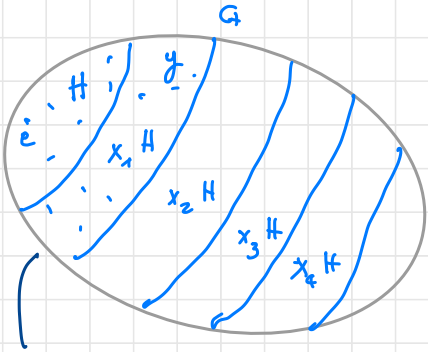
$x \sim_H y$ $\quad y^{-1}x \in H$ in notazione additiva

$x \equiv_H y$ $\quad -y + x \in H = n\mathbb{Z} \iff n \mid x - y$

$\iff x \equiv y \pmod n$

$H \leq G$ $\quad G = \bigcup_{x \in R} xH$ $\quad R$ = insieme di rappr. per le class.

$= \bigcup_{x \in R} xH$ $\quad \leftarrow$ G è unione disgiunta delle sue classi laterali modulo H.



$x_1 H = yH$ perché $y \in x_1 H$ $\quad y \in yH$ $\quad y = y \cdot e \in H$

$\Rightarrow y \in x_1 H \cap yH \Rightarrow$ non sono disgiunte quindi

$$x_1 H = yH$$

Teorema di Lagrange

Sia G un gruppo finito e sia $H \leq G$

$\Rightarrow |H| \mid |G|$

(L'ordine di un sgr divide l'ordine del gruppo)

Dim $\quad |G| = n$

Allora $\quad n = |G| = \left| \bigcup_{x \in R} xH \right| = \sum_{x \in R} |xH|$

Osserviamo che $\quad |xH| = |H| \quad \forall x \in G$

$\varphi : H \longrightarrow xH$ è bigettiva.
$h \longmapsto xh$

Tutte le classi laterali di H hanno la stessa cardinalità

La suppettività è ovvia $xH = \{xh\}_{h \in H}$

Iniettività $xh_1 = xh_2 \Rightarrow h_1 = h_2$ (cancellazione)

$$|G| = \sum_{x \in R} |xH| = \sum_{x \in R} |H| = |H| \cdot |R|$$

$\Rightarrow |H| \mid |G|$ ☒

Oss: Per i gruppi anche vale anche il viceversa

$\forall d \mid |G| \quad \exists!$ sgr di G di ordine d.

Esempio. $\mathbb{Z}/n\mathbb{Z}$ $\bar{0}, \bar{1}, \dots, \overline{n-1}$ $R = \{0, \dots, n-1\}$

$|\mathbb{Z}| = \infty$ $|n\mathbb{Z}| = \infty$ il Teorema di Lagrange non dice niente.

. $\mathbb{Z}/n\mathbb{Z}$ $H = \langle \bar{k} \rangle$ $|H| \mid n$ $|H| = \frac{n}{(n,k)}$ (ord $\bar{k}$)

Corollario 1: G gruppo finito

1) $\forall x \in G$ ord $(x) \mid |G|$

2) $\forall x \in G$ $x^{|G|} = e$

Dim 1) ord $x = |\langle x \rangle|$. Per L. ord $x = |\langle x \rangle| \mid |G|$

2) è chiaro perché $|G|$ è un multiplo dell'ordine di x.

Corollario 2 (Teorema di Eulero)

$m \geq 2 \quad a \in \mathbb{Z} \quad (a,m)=1 \Rightarrow a^{\phi(m)} \equiv 1 \pmod m$

Dim: Lo ottengo applicando il T di L (Cl) al gruppo

$G = \mathbb{Z}/m\mathbb{Z}^{\times}$ $\quad \forall\, \bar{a} \in \mathbb{Z}/m\mathbb{Z}^{\times} \ (\Leftrightarrow (a,m)=1)$

$|G| = \phi(m)$ si ha $\bar{a}^{\phi(m)} = \bar{1}$

$a^{\phi(m)} \equiv 1 \pmod m$

Corollario 3

Ogni gruppo di ordine p primo è ciclico e quindi isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

Dim. Sia $|G| = p$ primo $\Rightarrow p \geq 2 \quad \exists x \in G \ x \neq e$

$\operatorname{ord} x \mid p$ ma $\operatorname{ord} x \neq 1$ perché $x \neq e$

$\Rightarrow \operatorname{ord} x = p \Rightarrow \langle x \rangle = G$

Essendo G ciclico di ordine $p \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$ per quanto già dimostrato $\square$

In modo analogo si possono definire una rel di eq modulo $H \leq G$ e le classi laterali dx.

$x, y \in G \quad x \underset{H}{\sim} y \Leftrightarrow xy^{-1} \in H \quad (x \in Hy)$

$\underset{H}{\sim}$ è di equivalenza $[x] = \{ y \mid y \underset{H}{\sim} x \} =$

$= \{ y \mid yx^{-1} \in H \}$

$\{ y \mid y \in Hx \} = Hx$

classe laterale dx di H

Esempio $G = \mathbb{Z}$ $H = n\mathbb{Z}$

classi laterali sx $x + n\mathbb{Z} = \{ x + nz \}_{z \in \mathbb{Z}}$

classe laterale dx $n\mathbb{Z} + x = \{ nz + x \}_{z \in \mathbb{Z}}$

Dato che $\mathbb{Z}$ è abeliano $x + n\mathbb{Z} = n\mathbb{Z} + x$

↑ classe lat sx ↑ classe lat dx.

Oss: Se G è abeliano $xH = Hx \quad \forall x \in G$

Esempio $G = S_3 = \{ id, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau \}$

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

$\tau = (1\,2)$ $3 \to 3$

$\sigma^2 = (1\,3\,2)$

$\sigma\tau = (1\,3)$

$\sigma^2\tau = (2\,3)$

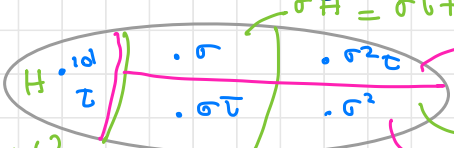
$\sigma \neq \sigma^2$ perché $\sigma \neq id$

$\sigma \neq \tau$ perché lo vedo

$\sigma \neq \sigma\tau$ perché $id \neq \tau$

$\tau \neq \sigma\tau$ " $id \neq \sigma$

$H = \langle \tau \rangle = \{ id, \tau \}$



e $H = \tau H = \{ \tau, id \}$

$\sigma H = \{\sigma \cdot id, \sigma \cdot \tau\} = \{\sigma, \sigma\tau\}$

Calcolo ora le classi laterali dx di H

H, $H\sigma = \{id \cdot \sigma, \tau \cdot \sigma\} = \{\sigma, t\sigma\} = \{\sigma, \sigma^2\tau\}$

$\tau\sigma = (1,2) \circ (1\,2\,3)$

$= (2,3)$

$= \sigma^2\tau$

$1 \xrightarrow{\sigma} 2 \xrightarrow{\tau} 1$

$2 \longrightarrow 3 \longrightarrow 3$

$3 \longrightarrow 1 \longrightarrow 2$

$\sigma H \neq H\sigma$

$G = S_3$ $\quad K = \langle \sigma \rangle = \{id, \sigma, \sigma^2\}$

$\tau K = \{\tau, \tau\sigma, \tau\sigma^2\} = K\tau$

($\tau\sigma = \sigma^2\tau$, $\tau\sigma^2 = \sigma\tau$)

Le classi laterali sx sono K τK

e quelle dx K $K\tau = \tau K$

→ Le classi laterali di un sgr possono coincidere anche con un gruppo non abeliano

Def $H \leq G$ si dice SOTTOGRUPPO NORMALE $H \trianglelefteq G$

se $\forall g \in G$ $\quad gH = Hg$

Osservazioni:

1) Se G è abeliano tutti i suoi sgr sono normali

2) In S_3 $\langle \sigma \rangle$ è normale, mentre $\langle \tau \rangle$ non è normale.

3) $H \trianglelefteq G \iff gH = Hg \ \forall g \in G \iff gHg^{-1} = H \ \forall g \in G$

In realtà si ha $H \trianglelefteq G \iff gHg^{-1} \subseteq H \ \forall g \in G$

$\Rightarrow$ è ovvio

$\Leftarrow$ $gHg^{-1} \subseteq H$ + $g^{-1}H(g^{-1})^{-1} \subseteq H$

$g^{-1}Hg \subseteq H$

$\Updownarrow$

$gg^{-1}Hgg^{-1} \subseteq gHg^{-1}$

quindi abbiamo

$gHg^{-1} \subseteq H$ e $H \subseteq gHg^{-1} \Rightarrow gHg^{-1} = H$

ATTENZIONE $gH = Hg$ è più debole che dire

$gh = hg \quad \forall h \in H$

Vuol dire che $\forall h \in H \quad gh \in Hg$

$\forall h \in H \ \exists h' \in H$ t.c. $gh = h'g$

$K = \langle \sigma \rangle < S_3$ $\quad t\langle \sigma \rangle = \{t, t\cdot\sigma, t\sigma^2\}$

$\langle \sigma \rangle t = \{t, \sigma t, \sigma^2 t\}$

Esercizio G gruppo

1) $\{e\}, Z(G), G \trianglelefteq G$

Def: G gruppo H sgr di G

$[G:H]$ = # classi laterali sx di H in G

↑ indice di H in G

Esercizio: 1) # cl lat sx di H in G = # classi lat dx di H in G

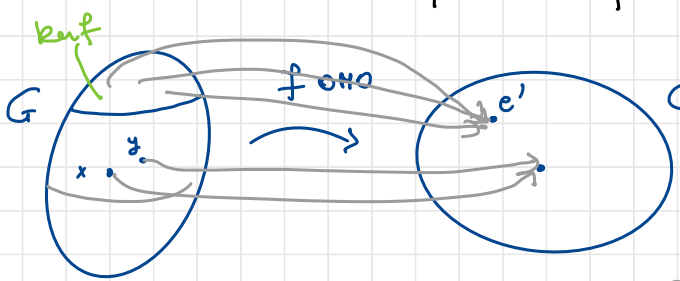
2) Ogni sgr di indice 2 è normale

Proposizione: $f: G \longrightarrow G'$ omomorfismo

Allora 1) $\ker f \trianglelefteq G$

2) $\forall x, y \in G \quad f(x) = f(y) \iff x \ker f = y \ker f$

3) Sia $x \in G \quad z = f(x) \Rightarrow f^{-1}(z) = x \ker f$



$x = yt$
$t \in \ker f$

$x \ker f$

$f(xt) = f(x) f(t) = f(x) e' = f(x)$

Dim: 1) $g \ker f g^{-1} \subseteq \ker f \quad \forall g \in G$

$t \in \ker f \qquad gtg^{-1} \in \ker f \quad \forall g \in G$

$\Rightarrow \quad f(gtg^{-1}) = e'$

$f(g)\, f(t)\, f(g^{-1}) = f(g)\, f(g)^{-1} = e'$

($f(t) = e'$)

2) $f(x) = f(y) \iff f(y)^{-1} f(x) = f^{-1}(y) f(y) = e'$

$\iff f(y^{-1}x) = e' \iff y^{-1}x \in \ker f \iff x \in y \ker f$

$\Rightarrow x \ker f = y \ker f$

3) $z = f(x) \qquad f^{-1}(z) = \{ y \in G \mid f(y) = z \} =$

$= \{ y \in G \mid f(y) = f(x) \} = x \ker f$

(↓ punto (2).)

□

Lezione 12 — 22 novembre 2021

G gruppo $\quad N \trianglelefteq G \quad (gN = Ng \ \forall g \in G)$

$G/N = \{ gN \mid g \in G \}$ insieme quoziente

↖ l'esistenza esiste anche se N non è normale in G

(Es: $G = \mathbb{Z} \quad N = n\mathbb{Z} \quad \mathbb{Z}/n\mathbb{Z} = \{ \overline{0} \}$

Se $N \trianglelefteq G$ posso considerare su G/N una struttura di gruppo indotta da G.

$$g_1 N \cdot g_2 N \overset{\text{def}}{=\!=} g_1 g_2 N$$

$g_1 N \cdot g_2 N$: prodotto che voglio definire in G/N

$g_1 g_2 N$: prodotto in G

L'operazione è ben definita: devo verificare che se

$x_1 N = g_1 N \quad x_2 N = g_2 N \Rightarrow x_1 x_2 N = g_1 g_2 N$

$x_i = g_i \cdot n_i \qquad \forall i = 1, 2$

$$x_1 x_2 = (g_1 n_1)(g_2 n_2) = g_1 (n_1 g_2) n_2 = g_1 g_2 h n_2 \in g_1 g_2 N$$

$N \trianglelefteq G$

$n_1 g_2 \in gN$

$n_1 g_2 = g n \quad n \in N$

$$\Rightarrow x_1 x_2 N = g_1 g_2 N$$

Teorema G/N con l'op $g_1N \cdot g_2N = g_1g_2N$ è un gruppo (si dice gruppo quoziente)

Oss: $\mathbb{Z}/n\mathbb{Z}$ è il gruppo quoziente di $\mathbb{Z}$ rispetto al sgr $n\mathbb{Z}$.

Prop: $N \trianglelefteq G$. La mappa $\pi_N : G \longrightarrow G/N$, $x \longmapsto xN$ è un omo di gruppi, suriettivo, $\ker \pi_N = N$.

Dim $\pi_N \quad x \longmapsto xN \quad \forall x \in G$

$\pi_N(xy) = xyN = xN \cdot yN = \pi_N(x)\pi_N(y) \quad \forall x,y \in G$

$\Rightarrow \pi_N$ è omo.

π_N sur: ovvio

$$\ker \pi_N = \{x \in G \mid \pi_N(x) = xN = N\} = N$$

($eN = N$; $xN = N$ def di π; N identità di G/N)

($n \in N \quad \pi_N(n) = nN = N \Rightarrow N \subset \ker \pi_N$

$x \in \ker \pi_N \quad \pi_N(x) = xN = N \Rightarrow x \in N$)

Corollario: I sottogruppi normali di G sono tutti e soli i nuclei degli omo definiti su G.

Dim: $N \trianglelefteq G \Rightarrow N = \ker \pi_N$

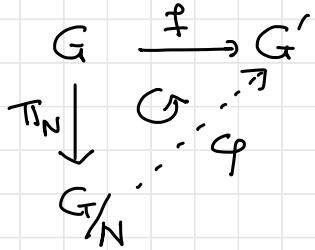
Viceversa se $f : G \to G'$ omo $\Rightarrow \ker f \trianglelefteq G$. □

1° Teorema di omomorfismo

$f: G \longrightarrow G'$ omo di gruppi, $N \trianglelefteq G$, $N \subseteq \ker f$

Allora $\exists!$ omo $\varphi: G/N \to G'$ che fa commutare il seguente diagramma:

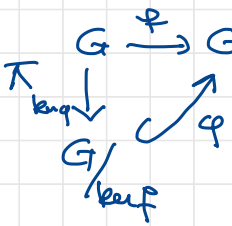
$$f = \varphi \circ \pi_N$$



Inoltre $\operatorname{Im}\varphi = \operatorname{Im} f$

$$\ker \varphi = \ker f / N$$

Caso particolare $N = \ker f$ il Teorema dice che

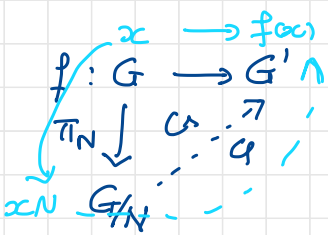


φ è iniettivo $\quad G/\ker f \cong \operatorname{Im} f = \operatorname{Im}\varphi$

$\Rightarrow$ Ogni omo definito su G si può fattorizzare in un omomorf. suriettivo e uno iniettivo

$$f = \varphi \circ \pi_{\ker f}$$

Dim



$f = \varphi \circ \pi_N$ ← devo def un omo φ che verifica questa equazione.

$\forall g \in G \quad f(x) = \varphi(\pi_N(x)) = \varphi(xN)$

$\Rightarrow$ se φ esiste è unico perché deve valer

$$\varphi(xN) = f(x)$$

Quindi quella è l'unica def possibile: FUNZIONA?

Buona def: $xN = yN$

$\varphi(xN) = f(x)$ $\qquad$ $\varphi(yN) = f(y)$

Devo vedere che $f(x) = f(y)$

Per la Prop della volta scorsa $f(x) = f(y) \Leftrightarrow$

$x \ker f = y \ker f \iff x \in y \ker f$

So che $xN = yN \Rightarrow x \in yN \subseteq y \ker f$

$\downarrow$

$N \subseteq \ker f$.

φ è omo:

$$\varphi(xN \cdot yN) = \varphi(xN)\varphi(yN)$$

$\varphi(xyN)$ $\qquad$ $f(x)f(y)$

$f(xy)$ $\qquad$ $\nwarrow$ f è omo

$\operatorname{Im}\varphi = \{ \varphi(xN) \mid xN \in G/N \} =$

$= \{ \varphi(xN) \mid x \in G \} = \{ f(x) \mid x \in G \} = \operatorname{Im} f.$

($\varphi(xN) = f(x)$)

$$\ker \varphi = \{ xN \mid \varphi(xN) = e' \} =$$

$$= \{ xN \mid f(x) = e' \} = \{ xN \mid x \in \ker f \}$$

$$= \ker f / N$$

xN con rappresentante $x \in \ker f$ □

2° Teorema di omomorfismo

G gruppo $H, K \trianglelefteq G$ $\quad H \subseteq K$

$$\frac{G/H}{K/H} \cong G/K$$

Dim Applico il Teo di omo a

$$\pi_K : G \longrightarrow G/K \qquad x \longrightarrow xK$$

$H \trianglelefteq G$
$H \subset \ker \pi_K = K$

$\pi_H : G \to G/H$, $\quad x \to xH$

$\varphi : G/H \to G/K$

$\operatorname{Im}\varphi = \operatorname{Im}\pi_K = G/K$
cioè
φ è suriettiva

$$\ker \varphi = \frac{\ker \pi_K}{H} = K/H$$

Riapplico il Teo di omo

alla mappa φ

$\ker\varphi = K/H$

φ è ben

$\varphi : G/H \to G/K$, $\quad \bar{x} = xH \to xK$

$\pi : G/H \to G/H/\ker\varphi$, $\quad \bar{x} \to \ker\varphi$

$\varphi' : G/H/\ker\varphi \to G/K$

150

$$\frac{G/H}{K/H} = G/H/\ker\varphi$$

Esempio $\mathbb{Z}$ $m\mathbb{Z} \subseteq n\mathbb{Z}$ $(n \mid m)$

$$\frac{\mathbb{Z}/m\mathbb{Z}}{n\mathbb{Z}/m\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$$

Oss: Il quoziente di un gruppo ciclico è ciclico

Dim diretta: $G = \langle g \rangle$ $N \triangleleft G$ (tutti i sgr sono normali perché ciclico $\Rightarrow$ abeliano)

$$G/N = \langle gN \rangle$$
$$\supseteq$$
$$\subseteq \quad xN \in G/N \quad x \in G = \langle g \rangle \Rightarrow x = g^k \quad k \in \mathbb{Z}$$
$$\Rightarrow xN = g^k N = (gN)^k \in \langle gN \rangle$$

3° Teorema di omomorfismo

$H, K \triangleleft G$ $\quad \dfrac{H}{H \cap K} \cong \dfrac{HK}{K}$

Dim Cerco un omo surg da $H \to HK/K$

$f: H \to HK/K$, $h \mapsto hK$ — è un sgr di G perché $HK = KH$ condizione garantita dalla normalità

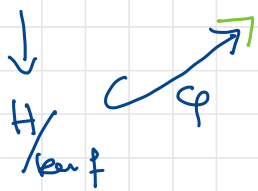
Esercizio $H, K < G$

$HK < G \iff HK = KH$

In particolare questo è vero se almeno uno tra H e K è normale in G.

Applico a f il 1° T di omo con $N = \ker f$

$f : H \to HK/K$ f è omo (facile)



$\mathrm{Im}\,\varphi = \mathrm{Im} f = \{hk \mid h \in H\} = HK/K$

$\ker \varphi = \{e\} \Rightarrow \frac{H}{\ker f} \cong \frac{HK}{K}$

$\subseteq$

$\supseteq$ $hkK \in HK/K$

$H \quad K$

$hK \in \varphi(h)$

$\ker f = \{h \in H \mid f(h) = hK = K\}$

$= \{h \in H \mid h \in K\} = H \cap K$

Quindi $\frac{H}{H \cap K} \cong HK/K$ ☒

Teorema di corrispondenza tra sottogruppi

G gruppo $N \trianglelefteq G$ $\pi_N : G \to G/N$

La proiezione π_N induce una corrispondenza biunivoca tra i sottogruppi di G/N e i sottogruppi di G che contengono N.

Questa corrispondenza conserva la normalità e l'indice di sgr-

$$Y = \{ H < G/N \} \qquad X = \{ H < G \mid N \subseteq H \}$$

$$X \longleftrightarrow Y$$

$$H \xmapsto{\alpha} \pi_N(H) = H/N$$

$$\{ \pi_N(h) \mid h \in H \} = \{ hN \mid h \in H \} = H/N$$

$$\pi_N^{-1}(\mathcal{H}) \xleftarrow{\beta} \mathcal{H}$$

Dim:

La corrisp. biunivoca è data da α che ha β come inverso.

α è ben definita $\quad H < G \quad N \subset H \Rightarrow \pi_N(H) = H/N \in Y$

β è ben definita $\quad \mathcal{H} < G/N \quad \pi_N^{-1}(\mathcal{H}) < G$

$N \in \mathcal{H}$ ↑ identità di G/N

$$\pi_N^{-1}(N) = \ker \pi_N \subset \pi_N^{-1}(\mathcal{H})$$

$$\Rightarrow N \subseteq \pi_N^{-1}(\mathcal{H})$$

$$\Rightarrow \pi_N^{-1}(\mathcal{H}) \in X$$

$$\alpha \circ \beta = id_Y \leftarrow \alpha \circ \beta(\mathcal{H}) = \pi_N \circ \pi_N^{-1}(\mathcal{H}) = \mathcal{H}$$

(π è surj)

$$\beta \circ \alpha = id_X \leftarrow \pi_N^{-1}(\pi_N(H)) = \pi_N^{-1}(H/N) =$$

$$= \{ h \in G \mid \pi_N(h) = hN \in H/N \} = \{ h \in G \mid h \in H \} = H$$

$H \in X \quad H \trianglelefteq G \iff \pi_N(H) = H/N \trianglelefteq G/N$

Fatto generale: * $H \trianglelefteq G \quad f: G \to G'$ è suriettiva

$\Rightarrow f(H) \trianglelefteq G'$

* $H \trianglelefteq G' \Rightarrow f^{-1}(H) \trianglelefteq G$

π_N è suriettiva e quindi

$H \in X \quad H \trianglelefteq G \Rightarrow \pi_N(H) \trianglelefteq G/N$

$H \trianglelefteq G/N \Rightarrow \pi_N^{-1}(H) \trianglelefteq G$

Indice di sottogruppo. $H \in X$

$[G : H] = [G/N : H/N]$ — le classi sono del tipo $\bar{g} \in G/N$, $\bar{g} = gN$, $\bar{g}H = gN \cdot H/N$

$\bar{g} = gN$, $H = \pi_N(H)$

$xH = yH \iff (xN)\,H/N = yN \cdot H/N$

Esempio $G = \mathbb{Z} \quad N = n\mathbb{Z} \quad G/N = \mathbb{Z}/n\mathbb{Z}$

$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

In questo caso $X = \{m\mathbb{Z} \mid m\mathbb{Z} \supset n\mathbb{Z}\} = \{m\mathbb{Z} \mid m \mid n\}$

Questo mi dice che i sgr di $\mathbb{Z}/n\mathbb{Z}$ sono

esattamente tanti quanti i divisori di n e sono $\Pi(m\mathbb{Z}) = m\mathbb{Z}/n\mathbb{Z}$

Il teorema ci dice anche che si conserva l'indice, cioè che

$$m = [\mathbb{Z} : m\mathbb{Z}] = \left[\mathbb{Z}/n\mathbb{Z} : m\mathbb{Z}/n\mathbb{Z}\right]$$

In questo caso particolare lo sapevamo già perché avevamo già calcolato i sgr di $\mathbb{Z}/n\mathbb{Z}$

$$m\mathbb{Z}/n\mathbb{Z} = \langle \bar{m} \rangle \leftarrow \text{punto che ordine}$$

$$\text{ord}\,\bar{m} = \frac{\text{ord}\,\bar{1}}{(m, \text{ord}\,\bar{1})} = \frac{n}{(m,n)} = \frac{n}{m}$$

Oss: Se $N \trianglelefteq G$ $\quad |G/N| = [G : N]$

Lezione 13 — 24 novembre '21

Anelli

Def $(A, +, \cdot)$ si dice anello se

1) $(A,+)$ è un gruppo abeliano
2) $\cdot$ è associativo
3) Valgono le leggi distributive $a(b+c) = a\cdot b + a\cdot c$ $\forall a,b,c \in A$

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

Def $(A,+,\cdot)$ si dice COMMUTATIVO se il prodotto è commutativo

$(A,+,\cdot)$ è un anello con identità se $\exists$ l'el. neutro per il prodotto $1 \in A$ $\quad 1\cdot a = a\cdot 1 = a \quad \forall a \in A$

Esempi: . $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/m\mathbb{Z}$ sono anelli commutativi con identità

. $(m\mathbb{Z}, +, \cdot)$ è un anello commutativo senza identità

. $M_{n\times n}(\mathbb{R})$ è un anello non commutativo con identità $(\forall n > 1)$

Def $(A,+,\cdot)$ anello con identità

$A^* = \{x \in A \mid x \text{ è invertibile}\}$

$x \in A$ è invertibile in A se $\exists y \in A$ tale che

$$xy = yx = 1 \qquad (y = x^{-1})$$

Esempio $\mathbb{Z}^\times = \{\pm 1\}$ $\quad \mathbb{Z}/m\mathbb{Z}^\times = \{\bar{a} \mid (a, m) = 1\}$

$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

Def $x \in A$ si dice DIVISORE DI ZERO se

$\exists y \in A$ $y \neq 0$ t.c. $xy = yx = 0$

Esempio in $\mathbb{Z}$ l'unico divisore di zero è 0

$\mathbb{Z}/6\mathbb{Z}$ $\quad \bar{2}$ è un div di zero

$\bar{2} \cdot \bar{3} = \bar{0}$

$\neq 0$

Def: $(A, +, \cdot)$ commutativo con 1 si dice DOMINIO D'INTEGRITÀ se l'unico divisore di zero di A è lo 0 $\quad D(A) = \{0\}$

$\hookrightarrow$ {divisori di zero di A}.

Def $(A, +, \cdot)$ comm con 1 si dice CAMPO se

$K^\times = K \setminus \{0\}$

($(K, +)$ è gr abeliano e $(K \setminus \{0\}, \cdot)$ è gr abeliano)

Proposizione: A anello (comm) con 1 _ Allora

1) $\forall a \in A \quad a \cdot 0 = 0$

2) $(A^\times, \cdot)$ è un gruppo (abeliano se A è commutativo)

3) $D(A) = \{\text{div. di zero di } A\} \quad D(A) \cap A^\times = \emptyset$

4) Se A è un dominio di integrità $\Rightarrow$ valgono la legge di annullamento del prodotto e la cancellazione per la moltiplicazione per el $\neq 0$

Dim: 1) $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a0 \Rightarrow a0 = 0$

↑ l. di cancellazione somma

2) $1 \in A^\times$

- $x, y \in A^\times \Rightarrow xy \in A^\times$
- $x \in A^\times \Rightarrow x^{-1} \in A^\times$ ovvio

$\exists\, x^{-1}, y^{-1} \in A \quad xx^{-1} = x^{-1}x = 1$

$yy^{-1} = y^{-1}y = 1$

$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1x^{-1} = xx^{-1} = 1$

↓ assoc.

$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}1y = y^{-1}y = 1$

3) $D \cap A^\times = \emptyset$ Per assurdo suppongo che esista

$x \in D \cap A^\times$

$x \in D \quad \exists y \in A \quad y \neq 0$ t.c. che $xy = yx = 0$

$x \in A^\times \quad \exists v \in A$ t.c. che $xv = vx = 1$

$$\left.\begin{array}{l} (yx)v = 0 \cdot v = 0 \\ \| \\ y(xv) = y\,1 = y \end{array}\right\} \text{assurdo perché } y \neq 0$$

4) A dominio $a \cdot b = 0$

se $a = 0$ ok

se $a \neq 0$ / $b = 0$ ok

\ $b \neq 0$ assurdo

perché $\Rightarrow a$ div. di $0 \neq 0$

mentre A è dominio

$\Rightarrow$ in A vale la legge di annullamento del prodotto

Cancellazione $ab = ac \quad a(b-c) = 0$

se $a \neq 0$ per la l. di ann. del prodotto

ottengo $b - c = 0 \Rightarrow b = c$

Corollario 1: Ogni campo è un dominio d'integrità

Dim: $K^\times = K \setminus \{0\} \quad D \cap K^\times = \emptyset \Rightarrow D \subset \{0\}$

$\Rightarrow D = \{0\} \Rightarrow K$ dominio

Corollario 2: Ogni dominio d'integrità finito è un campo

Dim: $A \quad |A| < +\infty$ dominio d'integrità

$\forall x \in A \quad x \neq 0$

$$\varphi_x : A \longrightarrow A \qquad \text{mappa}$$
$$a \longmapsto ax$$

è iniettiva ($\varphi_x(a) = \varphi_x(b) \iff ax = bx$

$\Rightarrow a = b$)

Poiché $x \neq 0$

Poiché $|A| < +\infty$ φ_x è anche suriettiva.

$\Rightarrow 1 \in \mathrm{Im}\,\varphi_x \quad \exists\, a \in A$ t.c.c. $\varphi_x(a) = ax = 1$

$\Rightarrow x$ è invertibile in $A \quad \forall x \neq 0$

$\Rightarrow A$ è un campo. □

Oss: • Se A non è finito il cor2 non vale: $\mathbb{Z}$

• $\mathbb{Z}/m\mathbb{Z} \qquad \mathbb{Z}/m\mathbb{Z}^* = \{\bar{a} \mid (a,m)=1\}$

$$D = \{\bar{a} \mid (a,m) \neq 1\}$$

$(a,m) = d > 1 \qquad \bar{a}\,\frac{m}{d} = \bar{0} \quad$ e $\frac{m}{d} \neq 0$

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}^* \cup D$$

Corollario 3: A anello finito $\Rightarrow A = A^* \cup D$

Dim: Con la dim del cor2 applicata così

$A^\times \cup D \subseteq A$ ovvio

$\supseteq$ $a \in A$ se $a \in D$ ✓

se $a \notin D$ φ_a è iniettiva, quindi

suriettiva $\Rightarrow$ $a \in A^\times$ (con la def del Cor 2).

—— o ——

Def A, B anelli con identità

$\varphi : A \to B$ è un omo di anelli se

1) $\varphi(1_A) = 1_B$

2) $\varphi(x +_A y) = \varphi(x) +_B \varphi(y) \quad \forall x, y \in D$

3) $\varphi(x \cdot_A y) = \varphi(x) \cdot_B \varphi(y) \quad \forall x, y \in A$

—— o ——

POLINOMI

A anello comm con 1 x indeterminata

$$A[x] = \{ a_0 + a_1 x + \dots + a_n x^n \mid n \in \mathbb{N} \quad a_i \in A \}$$

↳ anello dei pol in x con coeff. in A

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad g(x) = \sum_{i=0}^{m} b_i x^i$$

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

(somma in A)

dove ho completato i polinomi con degli zeri.

$(m < n \qquad b_{m+1} = \dots = b_n = 0)$

$$f(x) \cdot g(x) = \sum_{i=0}^{n+m} \left(\sum_{j+k=i} a_j b_k \right) x^i$$

$$f(x)\,g(x) = a_0 b_0 + (a_0 b_1 + b_1 a_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \dots$$

Teorema $(A[x], +, \cdot)$ è un anello comm con 1

Def $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x] \setminus \{0\}$

$$\deg f(x) = \partial f(x) := \max\{ i \mid a_i \neq 0 \}$$

Non definiamo il grado del polinomio 0

Oss: $\mathbb{Z}/6\mathbb{Z}[x]$ $\qquad 2x \qquad 3x^2$

$2x$: grado = 1 $\qquad$ $3x^2$: grado 2

$$2x \cdot 3x^2 = 6x^3 = 0$$

Proprietà del grado

1) $\deg(f+g) \leq \max\{\deg f, \deg g\}$

2) Se A è un dominio d'integrità

$$\deg(f \cdot g) = \deg f + \deg g$$

Dim (1) $\qquad f(x) + g(x) = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i$

$$\deg f+g \leq \max\{\deg f, \deg g\}$$

(2) $\deg f = n \qquad \deg g = m$

$f(x) = a_n x^n + \dots \qquad g(x) = b_m x^m + \dots$

$a_n \neq 0 \qquad b_m \neq 0$

$f(x)\,g(x) = a_n b_m x^{n+m} + \dots + a_0 b_0$

$\downarrow$

$\neq 0$ poiché $a_n \neq 0$ e $b_m \neq 0$

poiché A dominio

$\Rightarrow \deg(fg) = n+m = \deg f + \deg g.$

Corollario 1 A dominio $\Rightarrow$ A[x] dominio

Dim: $f, g \in A[x] \setminus \{0\} \qquad \deg f = n \geq 0 \qquad \deg g = m \geq 0$

$f(x)\,g(x) = \underset{\neq 0}{a_n b_m} x^{n+m} + \dots$

$\deg(fg) = m+n \geq 0 \qquad fg \neq 0$

Corollario 2 A dominio $\Rightarrow (A[x])^* = A^*$

Dim $f \in A[x]^* \quad \exists\, g \in A[x] \quad f \cdot g = 1$

$\deg(\underset{\| }{f} g) = \deg(1) = 0$

$\deg f + \deg g = 0 \longrightarrow \deg f = \deg g = 0$

$\Rightarrow f \in A^*$

Oss in $\mathbb{Z}/4\mathbb{Z}[x]$ $(2x+1)^2 = 4x^2+4x+1 = 1$

Polinomi di $K[x]$ (K campo)

$K[x] \longleftrightarrow \mathbb{Z}$

deg $\longleftrightarrow$ $|\cdot|$

Teorema di divisione euclidea

Siano $f, g \in K[x]$ $f \neq 0$

Allora esistono e sono unici $q, r \in K[x]$ tali che

$$g = qf + r \qquad r = 0 \ \vee \ \deg r < \deg f$$

Teorema di Ruffini

$f \in K[x]$ $a \in K$

$$f(a) = 0 \iff x - a \mid f(x)$$

Dim: $f(x) = (x-a)\,q(x) + r(x)$ $r = 0 \ \vee \ \deg r < \deg(x-a) = 1$

Valuto in a

$f(a) = (a-a)\,q(a) + r \iff r = f(a)$

$f(a) = 0 \iff r = 0 \iff (x-a) \mid f(x)$ ☐

$f, g \in K[x]$ non entrambi nulli si

può parlare di MCD e si può calcolare con l'algoritmo di Euclide.

$\{f, g\} \xrightarrow{AE} d(x) = mcd(f(x), g(x))$

$d(x) = a(x) f(x) + b(x) g(x)$

UNICITÀ $d(x)$, $d_1(x)$ MCD tra f e g

$d(x) \mid d_1(x) \Rightarrow d_1(x) = c(x) d(x)$

$d_1(x) \mid d(x) \Rightarrow d_1(x) = c(x) \gamma(x) d_1(x)$

$c(x) \gamma(x) = 1 \Rightarrow c = cost$

→ ho unicità a meno di costanti moltiplicative $\neq 0$

Fattorizzazione di polinomi

Def $f \in K[x]$ non costante si dice IRRIDUCIBILE se $\forall k(x)$

$f(x) = g(x) h(x)$ $g, h \in K[x] \Rightarrow$ $g = cost$ oppure $h = cost$ (invertibile / inv.)

Def $f \in K[x]$ non costante si dice PRIMO $\forall k[x]$

$f \mid gh$ con $g, h \in K[x]$ si ha $f \mid g \vee f \mid h$

Prop: $f \in K[x]$ è irriducibile $\iff$ è primo

(Stesse dim che in $\mathbb{Z}$)

Teorema di fattorizzazione unica

Ogni polinomio di $K[x]$ non costante si fattorizza in modo "unico" come prodotto di polinomi irriducibili

"unico" a meno dell'ordine dei fatt e di molt per el. invertibili

$$x^2 = \frac{1}{2}x \cdot 2x$$

Corollario: $f \in K[x]$ $f \neq 0 \Rightarrow f$ ha al più $\deg f$ radici in K contate con molteplicità

Dim

$$f(x) = (x-\alpha_1)^{e_1} \cdots (x-\alpha_r)^{e_r} g(x)$$

$\uparrow$ prodotto dei fattori di grado ≥ 1

$$\deg f = e_1 + \cdots + e_r + \deg g$$

$$\deg g \geq 0 \Rightarrow e_1 + \cdots + e_r \leq \deg f.$$

□

Dim del Teo di div euclidea $g = fq + r$

$\rightarrow$ $g = 0$ $q = 0$ $f = 0$ $r = 0$

Se $g \neq 0$ uso l'induzione su $n = \deg g$.

$n = 0$ g = costante se $\deg f = 0$ $g = f \frac{g}{f}$

se $\deg f > 0$ $\quad g = 0 f + g \quad \deg g < \deg f$.

$\deg g = n \qquad \deg f = m \qquad$ se $m > n$

$g = 0 f + g$ ✓

se $\deg f = m \leq \deg g = n \qquad g = \sum b_i x^i$.

$f = \sum a_i x^i$.

$g_1(x) = g(x) - \frac{b_n}{a_m} x^{n-m} f(x)$

$g_1(x) = q_1(x) f(x) + r(x)$ per ip induttiva

$g(x) = g_1(x) + \frac{b_n}{a_m} x^{n-m} f(x) =$

$= f(x) \left(q_1(x) + \frac{b_n}{a_m} x^{n-m} \right) + r(x)$

Unicità come su $\mathbb{Z}$.

Lezione 14 — 29 novembre '21

Fattorizzare polinomi. Dove? in $K[x]$ dato che in questo caso vale la FU K = campo

In quale campo? x^2+1 è irriducibile in $\mathbb{R}[x]$ ma in $\mathbb{C}[x]$ $(x^2+1)=(x+i)(x-i)$

$\mathbb{C}[x]$

Teorema fondamentale dell'algebra

Ogni polinomio non costante di $\mathbb{C}[x]$ ammette almeno una radice in $\mathbb{C}$.

Conseguenze:

1) $p(x) \in \mathbb{C}[x]$ è irriducibile $\iff$ $\deg p(x) = 1$.

($\Leftarrow$) I polinomi di grado 1 sono irrid in $K[x]$ $\forall K$ campo

$p(x) = f(x)\,g(x)$ (↓ $p(x)$: 1; ↓ $f(x)$: $n \le 1$; ↓ $g(x)$: $m \le 1$)

$m+n=1$, $n=1$ $m=0$ $\Rightarrow g \in K^*$

($\Rightarrow$) Se $\deg p = d > 1$ Per il TF dell'A $\exists\, a \in \mathbb{C}$ a radice di $p(x)$ $\Rightarrow$ $x-a \mid p(x)$ $\Rightarrow$ $p(x) = (x-a)\,q(x)$

$\mathbb{C}[x]^* = \mathbb{C}^*$ $x-a$ non è invertibile

$\deg q(x) = \deg p(x) - \deg(x-\alpha) = n-1 > 0$

$\Rightarrow q(x) \notin \mathbb{C}[x]^* = \mathbb{C}^*$ $\Rightarrow$ l'eq $p(x) = (x-\alpha)q(x)$ mostra che $p(x)$ non è irriducibile $\Rightarrow$ assurdo

quindi $\deg p(x) = 1$.

2) Ogni polinomio non costante di $\mathbb{C}[x]$ si fattorizza come prodotto di polinomi di grado 1.

- in $\mathbb{C}[x]$ vale il Teorema di FU quindi ogni polinomio è prodotto di p.p. irriducibili
- Per (1) i polinomi irriducibili di $\mathbb{C}[x]$ hanno grado 1.

3) Ogni polinomio di $\mathbb{C}[x]$ ha tante radici (contate con molt.) quanto il suo grado

$$p(x) = a(x-\alpha_1)^{e_1} \cdots (x-\alpha_r)^{e_r}$$

$$\deg p = e_1 + \cdots + e_r$$

Conclusione: In $\mathbb{C}[x]$ abbiamo risultati Teorici "bellissimi" ma determinare le radici è in generale difficile

Esempio $x^n - a \in \mathbb{C}[x]$ in questi casi le radici sono note perché sono le radici n-esime

di a

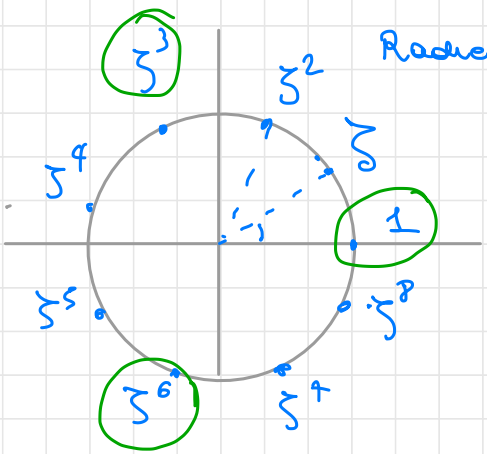
$$a = \rho e^{i\theta} \qquad a \neq 0$$

$$\sqrt[n]{a} = \left\{ \sqrt[n]{\rho} \left(\cos \frac{\theta + 2k\pi}{n} + i \sin \frac{\theta + 2k\pi}{n} \right) \;\middle|\; k = 0, \dots, n-1 \right\}$$

Esercizio fattorizzare $x^6 + x^3 + 1$ in $\mathbb{C}[x]$

$$x^6 + x^3 + 1 = \frac{x^9 - 1}{x^3 - 1} = \frac{(x-\alpha_1) \cdots (x-\alpha_9)}{(x-\beta_1)(x-\beta_2)(x-\beta_3)}$$

$\beta_1 = \alpha_1 \quad \beta_2 = \alpha_3 \quad \beta_3 = \alpha_6$



Radici none di 1 $\quad \{ \zeta \in \mathbb{C} \mid \zeta^9 = 1 \}$

$$= \langle \zeta \rangle$$

Radici cubiche di 1

$$x^6 + x^3 + 1 = \frac{\prod_{i=0}^{8} (x - \zeta^i)}{\prod_{k=0}^{2} (x - \zeta^{3k})} =$$

$$= (x-\zeta)(x-\zeta^2)(x-\zeta^4)(x-\zeta^5)(x-\zeta^7)(x-\zeta^8)$$

$\mathbb{R}[x]$ $\quad f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{R}[x], \; a_n \neq 0 \quad \deg f = n.$

$f(x) \in \mathbb{C}[x]$ in $\mathbb{C}[x]$ si spezza in pol di grado 1.

$\mathbb{R} = \{ z \in \mathbb{C} \mid z = \bar{z} \}$

$$\overline{f(x)} = \sum_{i=0}^{n} \overline{a_i}\, x^i = \sum_{i=0}^{n} a_i \cdot x^i = f(x)$$

$$f(x) = a_n (x-\alpha_1) \cdots (x-\alpha_n) \qquad \text{in } \mathbb{C}[x]$$

$$\| \leftarrow f(x) \in \mathbb{R}[x] \qquad \alpha_i \in \mathbb{C}$$

$$\overline{f(x)} = \overline{a_n}\, \overline{(x-\alpha_1)} \cdots \overline{(x-\alpha_n)} =$$

$$= a_n (x-\overline{\alpha_1}) \cdots (x-\overline{\alpha_n})$$

Per il Th di FU i fattori di $\overline{f(x)}$ sono quelli di $f(x)$ dato che $\overline{f(x)} = f(x)$

$\forall i \quad \exists\, j_i$ t.c.h. $(x-\overline{\alpha_i}) = (x-\alpha_{j_i})$

- $j_i = i$: $\overline{\alpha_i} = \alpha_i \iff \alpha_i \in \mathbb{R}$
- $j_i \neq i$: $(x-\alpha_i) \mid f(x)$ in $\mathbb{C}[x]$, $(x-\overline{\alpha_i}) \mid f(x)$ $\Rightarrow (x-\alpha_i)(x-\overline{\alpha_i}) \mid f(x)$ in $\mathbb{C}[x]$

($x-\alpha_i$ e $x-\overline{\alpha_i}$ sono irriducibili in $\mathbb{C}[x]$ distinti)

$$(x-\alpha_i)(x-\overline{\alpha_i}) = x^2 - 2\mathrm{Re}\,\alpha_i\, x + |\alpha_i|^2 \in \mathbb{R}[x]$$

$f(x) \in \mathbb{R}[x]$ $\quad f(x) = \underbrace{(x-\alpha_1)(x-\overline{\alpha_1})}_{\mathbb{R}[x]}\, q(x) \Rightarrow q(x) \in \mathbb{R}[x]$

Il quoziente della divisione appartiene al campo di definizione dei due polinomi

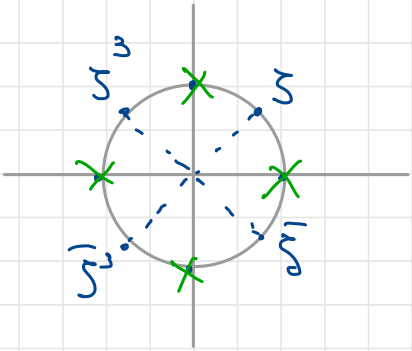
$$f(x) = \underbrace{(x-\alpha_1)\cdots(x-\alpha_r)}_{\alpha_1,\dots,\alpha_r \in \mathbb{R}} \underbrace{\left[(x-\alpha_{t+1})(x-\overline{\alpha_{t+1}})\right]}_{\in \mathbb{R}[x]} \cdots \underbrace{\left[(x-\alpha_s)(x-\overline{\alpha_s})\right]}_{\in \mathbb{R}[x]}$$

Conclusione

- I polinomi irriducibili di $\mathbb{R}[x]$ sono quelli
  - di grado 1
  - di grado 2 con $\Delta < 0$

- Ogni polinomio di $\mathbb{R}[x]$ si fattorizza in un polinomio di grado 1 e di grado 2 con $\Delta < 0$

In particolare x^4+1 NON È IRRIDUCIBILE su $\mathbb{R}$



$$x^4+1 = x^4+1+2x^2-2x^2 =$$
$$= (x^2+1)^2 - 2x^2 =$$
$$= (x^2+1-\sqrt{2}x)(x^2+1+\sqrt{2}x)$$

$$x^4+1 = \frac{x^8-1}{x^4-1}$$

Non avere radici non significa essere irriducibile

(questo vale solo per polinomi di grado 2 e 3)

$\mathbb{Q}[x]$

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$$

Moltiplicando per il MCM dei denom. degli a-

ottengo $df(x) \in \mathbb{Z}[x]$

$$\frac{5}{4}x^2 + \frac{10}{3} \overset{\cdot 12}{\rightsquigarrow} 15x^2 + 40 = 5(3x^2+8)$$

$$\frac{5}{12}(3x^2+8) = \frac{5}{4}x^2 + \frac{10}{3}$$

$f \in \mathbb{Q}[x]$ $\exists\, \gamma \in \mathbb{Q}^*$ t.c.b. $\gamma f(x) \in \mathbb{Z}[x]$

e MCD tra i coeff di $\gamma f(x)$ è 1.

$$f(x) \longrightarrow \underbrace{\gamma f(x)}_{f_1(x)} = \sum_{i=0}^{n} b_i x^i \qquad b_i \in \mathbb{Z}$$

$c(f_1) = (b_0, \dots, b_n) = 1$ ← contenuto di $f \in \mathbb{Z}[x]$ è il mcd dei coeff

$f \in \mathbb{Z}[x]$ si dice PRIMITIVO se $c(f) = 1$

Lemma di Gauß

$f \in \mathbb{Z}[x]$ PRIMITIVO

f è riducibile in $\mathbb{Z}[x] \iff$ è riducibile in $\mathbb{Q}[x]$

$$(x^3 - x) = \frac{1}{2} \cdot x \left(\frac{2}{7}x + \frac{2}{7}\right)(7x - 7) =$$

$$= 2x(x+1)(x-1)$$

Metodi

1) Ricerca delle radici razionali $f(x) \in \mathbb{Z}[x]$

$f\left(\frac{\alpha}{\beta}\right) = 0 \quad \alpha, \beta \in \mathbb{Z}. \quad (\alpha, \beta) = 1$

$f(x) = a_n x^n + \dots + a_0 \qquad a_i \in \mathbb{Z}$

$f\left(\frac{\alpha}{\beta}\right) = a_n \left(\frac{\alpha}{\beta}\right)^n + \dots + a_1 \left(\frac{\alpha}{\beta}\right) + a_0 = 0$

$a_n \alpha^n + \dots + a_1 \alpha \beta^{n-1} = - a_0 \beta^n$

$\alpha (a_n \alpha^{n-1} + \dots + a_1 \beta^{n-1}) = - a_0 \beta^n \qquad \text{in } \mathbb{Z}$

$\Rightarrow \alpha \mid a_0 \beta^n \quad \text{ma} \quad (\alpha, \beta) = 1 \Rightarrow \alpha \mid a_0$

$- a_n \alpha^n = a_{n-1} \alpha^{n-1} \beta + \dots + a_0 \beta^n$

$= \beta (a_{n-1} \alpha^{n-1} + \dots + a_0 \beta^{n-1})$

$\Rightarrow \beta \mid a_n \alpha^n \quad \text{ma} \quad (\beta, \alpha) = 1 \Rightarrow \beta \mid a_n$

Quindi se $f(x) \in \mathbb{Z}[x]$ $\frac{\alpha}{\beta}$ è radice in $\mathbb{Q}$ di f

$(\alpha, \beta) = 1 \Rightarrow \frac{\alpha}{\beta} \in \left\{ \frac{\varepsilon}{\delta} \;\middle|\; \varepsilon \mid a_0 \wedge \delta \mid a_n \right\} = R$

→ So determinare tutte le radici razionali di f perché appartengono ad un insieme finito R.

(Le radici di f devono $\in R$ e quindi le determino testando gli el. di R che sono in numero finito).

2) Riducendo modulo un primo.

p primo $\qquad \pi_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x]$

$$f(x) = \sum_{i=0}^{n} a_i x^i \longrightarrow \sum_{i=0}^{n} \overline{a}_i x^i = \overline{f}(x)$$

π_p è un omo di anelli

$\left(\pi_p(1) = \overline{1} \qquad \pi_p(f(x)+g(x)) = \pi_p(f(x)) + \pi_p(g(x)) \right)$

$\Rightarrow$ Se $p \nmid a_n \quad \Rightarrow \deg \pi_p(f(x)) = \deg f(x)$

Proposizione: Se $p \nmid a_n$ e $\pi_p(f(x))$ è riducibile in $\mathbb{Z}/p\mathbb{Z}[x]$ e $f(x)$ è primitivo $\Rightarrow f(x)$ è riducibile in $\mathbb{Z}[x]$ e quindi per il L. di G. anche in $\mathbb{Q}[x]$

Esempio x^2+x+1 è riducibile in $\mathbb{Z}/2\mathbb{Z}[x]$

- ha grado 2 quindi è riducibile $\Leftrightarrow$ non ha radici

$\Rightarrow$ Tutti i polinomi del tipo

$$a_2 x^2 + a_1 x + a_0 \qquad \text{con } a_2, a_1, a_0 \in \mathbb{Z}$$

dispari e senza fattori comuni

sono IRRIDUCIBILI in $\mathbb{Z}[x]$ e quindi in $\mathbb{Q}(x)$ per il L. di G (è primitivo)

Dim: Dimostriamo che se $f(x) \in \mathbb{Z}[x]$ primitivo è RIDUCIBILE e $p \nmid a_n \Rightarrow \pi_p(f(x))$ è riducibile

$f(x) = g(x) h(x) \qquad n > m \geq 1$

$n \quad m \quad n-m$

$\pi(f(x)) = \pi(g(x))\,\pi(h(x))$ ← $\pi(f(x))$ è riducibile.

$n \quad m' \leq m \quad d' \leq n-m$ gradi.

ma $n = m' + d' \leq m + n - m \Rightarrow m = m'$, $d' = n-m$ □

Il viceversa non vale. Ad esempio il polinomio

$$x^4 + 1$$

è IRRIDUCIBILE in $\mathbb{Z}[x]$ $(\mathbb{Q}[x])$ ←

è RIDUCIBILE mod p $\forall p$ primo.

3) Criterio di Eisenstein

Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ primitivo e sia p primo.

Supponiamo che (1) $p \nmid a_n$

(2) $p \mid a_i \quad \forall i = 0, \dots, n-1$

(3) $p^2 \nmid a_0$

$\Rightarrow f(x)$ è riducibile in $\mathbb{Z}[x]$ e per L ed G anche in $\mathbb{Q}[x]$

Dim Per assurdo supponiamo che $f(x) = g(x)\,h(x)$

$\deg g = m \geq 1 \qquad \deg h = n-m \geq 1$

$$\pi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x]$$

$$f(x) = \sum_{i=0}^{n} a_i x^i \longmapsto \overline{f}(x) = \overline{a}_n x^n \neq 0$$

$(\overline{a}_i = 0 \ \forall i = 0, \dots, n-1)$

$$\pi(f(x)) = \pi(g(x)) \cdot \pi(h(x))$$

$$g(x) = \sum_{i=0}^{m} b_i x^i \qquad h(x) = \sum_{i=0}^{n-m} c_i x^i$$

$$\pi(g) = \overline{b}_m x^m + \dots + \overline{b}_0 \qquad \pi(h) = \overline{c}_{n-m} x^{n-m} + \dots + \overline{c}_0$$

$$\overline{a}_n x^n = \pi(g) \cdot \pi(h) \quad \text{in } \mathbb{Z}/p\mathbb{Z}[x]$$

↑ vale la FU.

$\Rightarrow \pi(g)$ e $\pi(f)$ sono fattori

$$\overline{a}_n x^n \Rightarrow \pi(g) = \overline{b}_m x^m \quad \text{e} \quad \pi(h) = \overline{c}_{n-m} x^{n-m}$$

$$\Rightarrow \overline{b}_0 = \overline{c}_0 = 0$$

$a_0 = b_0 c_0 \Rightarrow p^2 \mid a_0$ e questo è assurdo.

Corollario: $\forall n$ esistono infiniti polinomi irriducibili di grado n in $\mathbb{Q}[x]$ ($\mathbb{Z}[x]$)

Dim $x^n - p$ p primo $n \geq 1$.

↳ è p-Eisenstein.

Lezione 15 — 1° dicembre '21

$K[x]$ ← anello

A anello (con con 1) $I \subseteq A$ si dice IDEALE se

- $I \trianglelefteq (A, +)$
- I assorbe la moltiplicazione di A

$$\forall a \in A \quad \forall x \in I \quad ax \in I$$

A/I ← è un gruppo quoziente

$$(a+I) + (b+I) = a+b+I$$

Posso definire

$$(a+I) \cdot (b+I) = ab+I$$

La proprietà di assorbimento di I un ideale di verificare che l'operazione è ben definita e

$(A/I, +, \cdot)$ è un anello commutativo ← se A è con $1+I$ è l'id ← $1 \in A$

$A = \mathbb{Z}$ $\quad I = n\mathbb{Z}$ ← ideale di A

$$\forall m \in \mathbb{Z} \quad mI \subseteq I \qquad m \cdot n\mathbb{Z} \subset n\mathbb{Z}$$

$A = K[x]$ $\quad f(x) \in K[x]$ $\quad$ Analogue con $A = \mathbb{Z}$ $n \in \mathbb{Z}$ $n\mathbb{Z} = (n)$

$$(f(x)) \doteq f(x)\,K[x] = \{ f(x)\,a(x) \mid a(x) \in K[x] \}$$

↳ ideale generato da $f(x)$
che è un ideale si verifica in modo ovvio.

↳ ⚠ non è il sgr generato da $f(x)$

$$\langle f(x) \rangle = \{ n f(x) \}_{n \in \mathbb{Z}}$$

Teorema $\left(\frac{K[x]}{(f(x))}, +, \cdot \right)$ è un anello comm con identità

Un insieme di rappr per gli el di $K[x]/(f(x))$

è dato dai resti delle divisione per $f(x)$, cioè

dai polinomi $r(x)$ $\deg r(x) < \deg f$ più il pol 0

In particolare $K[x]/(f(x))$ è un K-sp. vettoriale:

dim $\frac{K[x]}{(f(x))}_K = \deg f$, base $\overline{1}, \overline{x}, \dots, \overline{x}^{\deg f - 1}$

Dim: $1 + (f(x))$ ← identità $\quad 0 + (f(x))$

Ogni classe $a(x) + (f(x))$ è rappresentata dal

resto della div di $a(x)$ per $f(x)$

$$a(x) = q(x) f(x) + r(x) \qquad \begin{cases} r(x) = 0 \\ \partial r(x) < \partial f(x) \end{cases}$$

$$a(x) + (f(x)) = r(x) + \underbrace{q(x) f(x)}_{\in (f(x))} + (f(x)) = r(x) + (f(x))$$

Dico che $r_1(x) + (f(x)) = r_2(x) + (f(x))$ $\partial r_i < \partial f$ oppure $r_i = 0$

$\iff r_1(x) - r_2(x) \in (f(x))$

$\partial(r_1(x) - r_2(x)) < \partial f(x) \Rightarrow r_1(x) = r_2(x)$

$$\frac{K[x]}{(f(x))} = \left\{ \sum_{i=0}^{n-1} a_i \cdot \overline{x^i} \;\middle|\; a_i \in K \right\} \qquad n = \deg f$$

$$\Rightarrow \frac{K[x]}{(f(x))} = \langle \bar{1}, \bar{x}, \dots, \bar{x}^{n-1} \rangle_K \leftarrow \{x^i\}_{i=0}^{n-1} \text{ genera su } K$$

$\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}$ sono linearmente indip perché'

$\sum_{i=0}^{n-1} a_i \bar{x}^i = \bar{0} \iff a_i = 0 \ \forall i$

$\square$

↓ è un resto

Ci ricordiamo $\mathbb{Z}/n\mathbb{Z}$

- invertibili $\bar{a}$ t.c. $(a,n)=1$
- div di zero $\bar{a}$ $(a,n)=d>1$
- nilpotenti ....

Proposizione $\overline{a(x)} \in K[x]/(f(x))$

1) $\overline{a(x)}$ è invertibile $\iff (a(x), f(x)) = 1$

2) $\overline{a(x)}$ è div di zero $\iff (a(x), f(x)) \neq 1$

In particolare ogni el è o div di zero o invertibile.

Dim $(a(x), f(x)) = 1 \iff \exists\ \lambda(x), \mu(x) \in K[x]$

tale che $a(x)\lambda(x) + f(x)\mu(x) = 1$

$\iff a(x)\lambda(x) \in 1 + (f(x))$

$\overline{a(x)}\ \overline{\lambda(x)} = \overline{1} \iff \overline{a(x)}$ è invertibile

② $(a(x), f(x)) = d(x)$ $\deg d \geq 1$ $\quad (a, n) = d$

$a\frac{n}{d} \equiv 0 \pmod n$

$a\frac{n}{d} = 0$

$0 \neq \frac{n}{d}$

$a(x) = a_1(x)\, d(x)$

$f(x) = f_1(x)\, d(x)$

$\overline{a(x)} \cdot \overline{f_1(x)} = \overline{a_1(x)}\ \overline{d(x)\, f_1(x)} = \overline{0}$

$\overline{f(x)} = \overline{0}$

e $\overline{f_1(x)} \neq \overline{0}$

$\Rightarrow \overline{a(x)}$ è div. di zero

Viceversa se $\exists\ \overline{b(x)} \neq \overline{0}$ t.c. $\overline{a(x)}\,\overline{b(x)} = \overline{0}$

$\Rightarrow \overline{a(x)}$ non è inv. $\Rightarrow (a(x), f(x)) \neq 1$ □

Corollario $K[x]/(f(x))$ è un campo $\iff f(x)$ è irriducibile

Dim $K[x]/(f(x))$ è un campo $\iff \forall\ \overline{a(x)} \neq \overline{0}$ è invertibile $\iff \forall\ \overline{a(x)} \neq \overline{0}$

ossia $(a(x), f(x)) = 1 \iff \forall\ r(x) \in K[x]$

con $\deg r(x) < \deg f$ mi ha $(r(x), f(x)) = 1$

$\Rightarrow$ $f(x)$ è irriducibile $\square$

Esempi $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ← notazione

Conosciamo 2 gruppi con 4 elem $\mathbb{Z}/4\mathbb{Z}$ ← non sono campi

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$K[x]/(f(x))$ sp. vett di dim $n = \deg f$ su K.

↑ quello con prodotto diretto (comp. per comp)
$(1,0)(0,1) = (0,0)$

$K = \mathbb{F}_2$ $f(x)$ irriducibile di grado n

$\Rightarrow$ $\dfrac{\mathbb{F}_2[x]}{(f(x))}$ è un campo con 2^n el perché è $\cong \mathbb{F}_2^n$

$f(x) = x^2+x+1$ ↑ irriducibile $\quad \mathbb{F}_4 = \dfrac{\mathbb{F}_2[x]}{(f(x))}$ è un campo di card 4.

$\bar{0}, \bar{1}, \bar{x}, \overline{x+1}$ $\quad \overline{x^2+x+1} = \bar{0}$ $\quad \bar{x}^2 = -(\bar{x}+1)$

chi è l'inverso $\bar{x}\,\bar{x} = \bar{x}^2 = \overline{x+1}$

$\bar{x}(\overline{x+1}) = \overline{x^2+x} = \bar{1}$

$g(x) = x^3+x+1$ $\quad \dfrac{\mathbb{F}_2[x]}{(g(x))}$ ho un campo con 2^3 el.

ESTENSIONI DI CAMPI

$K \subseteq F$ campi F è un'estensione di K F/K

Esempi: $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{F}_4/\mathbb{F}_2$

Def $\alpha \in F$ si dice ALGEBRICO SU K

se $\exists f(x) \in K[x]$, $f(x) \neq 0$ tale che $f(\alpha) = 0$

$\alpha \in F$ si dice TRASCENDENTE SU K se non è algebrico su K.

$f(x) \in K[x] \setminus \{0\}$ $f(x) = \sum_{i=0}^{n} a_i x^i$

$f(\alpha) = a_n \alpha^n + \dots + a_1 \alpha + a_0$

$= 0$ $\{1, \alpha, \dots, \alpha^n\}$ sono linearmente dip. $/K$ — α alg su K

$\neq 0$ $\forall f \neq 0$ Tutte le potenze di α sono l. indip $/K$ $\{\alpha^i\}_{i \geq 0}$ — α Trascendente su K

Esempi: $\sqrt{5}$ è alg su $\mathbb{Q}$

$f(x) = x^2 - 5 \in \mathbb{Q}[x]$ $f(x) \neq 0$ $f(\sqrt{5}) = 0$

π è trascendente su $\mathbb{Q}$ .....

ma è alg su $\mathbb{R}$ $x - \pi \in \mathbb{R}[x]$ e si annulla in π

Def F/K è un'estensione algebrica se

$\forall a \in F$ a è algebrico su K.

Es: $\mathbb{R}$ non è algebrica su $\mathbb{Q}$ ($\pi \in \mathbb{R}$ non è alg su $\mathbb{Q}$)

F/K $a \in F$ $K[a] = \{ f(a) \mid f(x) \in K[x] \}$

$$\varphi_a : K[x] \longrightarrow F \qquad f(x) \longmapsto f(a)$$

omomorfismo di valutazione

↑ verifica facile

$\operatorname{Im} \varphi_a = K[a]$ ← anello

$$\begin{array}{ccc} K[x] & \xrightarrow{\varphi_a} & K[a] \subset F \\ \pi \downarrow & \circlearrowright & \nearrow \bar{\varphi} \\ K[x]/\ker\varphi_a & & \end{array}$$

$\bar{\varphi}$ ← isomorfismo di gruppi

$\bar{\varphi}$ è un isomorfismo di anelli in quanto

$$\bar{\varphi}(\bar{1}) = 1$$

$$\bar{\varphi}(\overline{a(x)}\,\overline{b(x)}) = \bar{\varphi}(\pi(a(x))\,\pi(b(x))) =$$

$$\bar{\varphi}(\pi(a(x)b(x))) = \varphi_a(a(x)b(x)) =$$

$$= a(a)b(a) = \bar{\varphi}(\overline{a(x)}) \cdot \bar{\varphi}(\overline{b(x)})$$

$K[\alpha] \cong K[x]/\ker \varphi_\alpha$ come anelli

$\ker \varphi_\alpha = \{ f(x) \in K[x] \mid f(\alpha) = 0 \}$

α è trascendente/K $\iff$ $\ker \varphi_\alpha = \{0\}$ $\iff$ φ_α è iniettiva

$\iff$ $K[\alpha] \cong K[x]$

α è algebrico $\iff$ $\ker \varphi_\alpha \neq \{0\}$ $\iff$ φ_α NON è iniettiva

Sia $\mu_\alpha(x) \in \ker \varphi_\alpha$ monico, di grado minimo tra i pol di $\ker \varphi_\alpha$

$\Downarrow$

$\mu_\alpha(\alpha) = 0$

($S = \{ \deg f(x) \mid f(x) \in \ker \varphi_\alpha \setminus \{0\} \} \neq \emptyset$ se α è alg.

$S \subset \mathbb{N}$ $\Rightarrow$ S ammette minimo)

Proposizione: 1) μ_α è irriducibile in $K[x]$

2) $\ker \varphi_\alpha = (\mu_\alpha(x))$

3) $\mu_\alpha(x)$ è l'unico pol monico irriducibile che si annulla in α

che $\in \ker \varphi_\alpha$

Dim: $\mu_\alpha(x) \in \ker \varphi_\alpha$

$\Rightarrow \mu_\alpha(\alpha) = 0$ se fosse $\mu_\alpha(x) = a(x) b(x)$ ($a(x), b(x) \in K[x]$)

$\Rightarrow 0 = \mu_\alpha(\alpha) = a(\alpha) b(\alpha)$ in $K[\alpha]$ CF

$\Rightarrow$ per la legge di annullamento del prodotto $\begin{cases} a(\alpha)=0 \\ b(\alpha)=0 \end{cases}$

μ_α ha grado minimo tra i polinomi di $K[x]$ che si annullano in α

$\deg a(x) \geq \deg \mu_\alpha(x) \Rightarrow$ b costante e $\deg a(x) = \deg \mu_\alpha(x)$

$\Rightarrow \mu_\alpha(x)$ è irriducibile in $K[x]$

(2) $\mu_\alpha(x) \in \ker \varphi_\alpha \Rightarrow (\mu_\alpha(x)) \subset \ker \varphi_\alpha$

$a(x)\mu_\alpha(x) \xrightarrow{\varphi_\alpha} a(\alpha)\mu_\alpha(\alpha) = 0$

$\Downarrow$

$a(x)\mu_\alpha(x) \in \ker \varphi_\alpha$

$p(x) \in \ker \varphi_\alpha \quad p(x) \in K[x] \wedge p(\alpha)=0$

$p(x) = q(x)\mu_\alpha(x) + r(x) \qquad r(x) \in K[x]$

$\Downarrow \qquad r(x)=0$

$\begin{cases} \deg r(x) < \deg \mu_\alpha \end{cases}$

$0 = p(\alpha) = q(\alpha)\underbrace{\mu_\alpha(\alpha)}_{=0} + r(\alpha)$

$r(\alpha)=0 \Rightarrow r=0$ perché $\mu_\alpha(x)$ aveva grado minimo tra i polinomi di $\ker \varphi_\alpha$

$\Downarrow$

$r(x) \in \ker \varphi_\alpha$

$\Rightarrow p(x) = q(x)\mu_\alpha(x) \in (\mu_\alpha(x))$

(3) $\ker \varphi_\alpha = (\mu_\alpha(x))$

$\supseteq$ $f(x)$ = monico, irriducibile, $f(\alpha)=0$

Devo vedere $f(x) = \mu_\alpha(x)$

$f(x) \in \ker \varphi_\alpha = (\mu_\alpha(x)) \Rightarrow f(x) = a(x)\,\mu_\alpha(x)$

Se $f(x)$ è irred uno dei due fattori è invertibile $\rightarrow$ $\mu_\alpha(x)$ non è inv perché $\deg \mu_\alpha \geq 1$

$\Rightarrow$ $a(x) = a = \text{cost}$ $\qquad f(x) = a\,\mu_\alpha(x) \Rightarrow a = 1$

($f(x)$: monico; $\mu_\alpha(x)$: monico)

$\Rightarrow f(x) = \mu_\alpha(x)$ $\square$

Def F/K $\alpha \in F$ algebrico su K.

Si dice POLINOMIO MINIMO di α/K l'unico polinomio monico, irriducibile di $K[x]$ che si annulla in α.

Esempio $\alpha = \sqrt{5} \rightarrow \sqrt{5}$ è alg su $\mathbb{Q}$ $x^2 - 5 \in \mathbb{Q}[x]$

Dico $\mu_{\sqrt{5}}(x) = x^2 - 5$

- è monico
- è irred su $\mathbb{Q}[x]$
- $\mu_{\sqrt{5}}(\sqrt{5}) = 5 - 5 = 0$

$\Rightarrow \mathbb{Q}[\sqrt{5}] \cong \mathbb{Q}[x]/(\mu_\alpha(x))$ $\leftarrow$ è un CAMPO

$\alpha \in F$ alg su K $\quad \mu_\alpha(x) \in K[x]$ pol min di α/K

$$K[\alpha] \cong \frac{K[x]}{(\mu_\alpha(x))} \Rightarrow K[\alpha] \text{ è un campo}$$

↑ è riducibile

Esempio. $\mathbb{Q}[\sqrt{5}]$ $\quad 1+\sqrt{5}$ che ha come inverso

$$\frac{1}{1+\sqrt{5}} = \frac{1-\sqrt{5}}{1-5} = -\frac{1}{4} + \frac{\sqrt{5}}{4}$$

• $\mathbb{Q}[\sqrt[3]{2}]$ $\quad \mu_\alpha(x) = x^3 - 2 \in \mathbb{Q}[x]$

↑ campo !

$$\mathbb{Q}[\sqrt[3]{2}] \cong \frac{\mathbb{Q}[x]}{(x^3-2)}$$

$1, \sqrt[3]{2}, \sqrt[3]{4}$ $\quad \leftarrow \quad \bar{1}, \bar{x}, \bar{x}^2$

$a1 + b\sqrt[3]{2} + c\sqrt[3]{4} \qquad a,b,c \in \mathbb{Q}$

$1 + 2\sqrt[3]{2} - \sqrt[3]{4}$ cerco l'inverso

$$(1 + 2\sqrt[3]{2} - \sqrt[3]{4})(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 1$$

$a + 2a\sqrt[3]{2} - a\sqrt[3]{4} +$
$-2b + b\sqrt[3]{2} + 2b\sqrt[3]{4}$
$2c - 4 \cdot 2 \cdot c\sqrt[3]{2} + c\sqrt[3]{4}$

$$a - 2b + 2c + (2a + b - 8c)\sqrt[3]{2} + (a + 2b + c)\sqrt[3]{4} = 1$$

$$\begin{cases} a-2b+c=1 \\ 2a+b-8c=0 \\ a+2b+c=0 \end{cases} \rightsquigarrow$$ Trovo un'unica sol.

In generale se α è alg su K $K[\alpha]$ è un campo

$\dim_K K[\alpha] = \deg \mu_\alpha$ base $1, \alpha, \dots, \alpha^{\deg \mu_\alpha - 1}$

($K[\alpha] \cong \frac{K[x]}{(\mu_\alpha(x))}$)

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f(x), g(x) \in K[x] \;\; g(\alpha) \neq 0 \right\}$$

Se α è alg/K $K[\alpha] = K(\alpha)$

($K[\alpha] \ni g(\alpha) \neq 0$ $\frac{1}{g(\alpha)} \in K[\alpha]$

$\forall f(\alpha) \in K[\alpha]$ $f(\alpha)\frac{1}{g(\alpha)} \in K[\alpha]$).

Def F/K campi GRADO di F/K

$$[F:K] \doteq \dim_K F$$

Abbiamo visto $\alpha \in F$ alg su K

$$[K[\alpha]:K] = \dim_K K[\alpha] = \deg \mu_\alpha(x).$$

Lezione 16 — 6 dicembre '21

$K \subset F$ $\quad \alpha \in F$ si dice alg/k se $\exists f(x) \in K[x]$

$f(x) \neq 0$ e $f(\alpha) = 0$

$$\sum_{i=0}^{n} a_i \alpha^i = 0 \qquad a_i \in k$$

$\Rightarrow \{1, \alpha, \dots, \alpha^n\}$ sono l.dip su k.

$$k[\alpha] \cong k[x] / \ker \varphi_\alpha \cong k[x] / (\mu_\alpha(x))$$

$1, \alpha, \dots, \alpha^{n-1}$ base — campo

$\ker \varphi_\alpha \neq 0 \iff \alpha$ è alg su k

$\leftarrow$ campo $\Uparrow$ ($\mu_\alpha(x)$ è irred su k)

$\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}$

e in tal caso $\ker \varphi_\alpha = (\mu_\alpha(x))$

$\hookrightarrow$ pol minimo di α/k

$\mu_\alpha(x)$ è l'unico pol di $k[x]$ t.c.

- monico
- irred
- $\mu_\alpha(\alpha) = 0$

$$[F : k] \doteq \dim_k F$$

$$[k[\alpha] : k] = \deg \mu_\alpha(x)$$

$\hookrightarrow$ pol minimo di α/k

$F = k[\alpha]$ estensione semplice

Proposizione: F/K estensione di campi

$[F:K] < +\infty$ — Allora F è algebrico su K

(cioè $\forall \alpha \in F$ α è alg su K)

Dim: Sia $[F:K]=n$ e sia $\alpha \in F$

$\{1, \alpha, \dots, \alpha^n\}$ è un insieme di $n+1$ el di F

Poiché $[F:K]=n \Rightarrow 1, \alpha, \dots, \alpha^n$ sono l. dip su K.

$\Rightarrow \exists\, a_0, \dots, a_n \in K$ NON TUTTI NULLI t.c.

$$a_0 \cdot 1 + a_1 \alpha + \dots + a_n \alpha^n = 0$$

$\Rightarrow f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ non è nullo e si annulla in α $(f(\alpha)=0) \Rightarrow \alpha$ è alg su K.

(Ogni estensione finita è algebrica)

Il viceversa è falso

Teorema dei gradi nelle Torri di estensioni

$K \subseteq F \subseteq L$ e sia $[F:K]=n$ $[L:F]=m$

$\Rightarrow [L:K]=nm$

L — m — F — n — K (nm)

Dim $[F:K]=n$ sia $v_1, \dots, v_n$ K-base di F

$[L:F]=m$ $w_1, \dots, w_m$ una F-base di L

Dico che $\{v_i w_j\}_{\substack{j=1,\dots,m \\ i=1,\dots,n}}$ è una K-base di L

questo garantisce in particolare $[L:K] = nm$

generano: $\alpha \in L$ $\quad \alpha = \sum_{j=1}^{m} \lambda_j w_j$ perché $L = \langle w_1, \dots, w_m \rangle_F$

$\lambda_j \in F$

D'altra parte $\forall j$ $\quad \lambda_j = \sum_{i=1}^{n} a_{ji} v_i \qquad a_{ji} \in K$

Sostituendo $\quad \alpha = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ji} v_i \right) w_j =$

$$= \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ji} v_i w_j$$

$\{v_i w_j\}_{\substack{j=1,\dots,m \\ i=1,\dots,n}}$ genera L su K.

indipendenza lineare: $\quad \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ji} v_i w_j = 0 \qquad a_{ji} \in K$

$$\left(\sum_{i=1}^{n} a_{1i} v_i \right) w_1 + \left(\sum_{i=1}^{n} a_{2i} v_i \right) w_2 + \dots + \left(\sum_{i=1}^{n} a_{mi} v_i \right) w_m = 0$$

$\in F$ $\qquad F$ $\qquad F$

è una comb dei w_j con coeff in F

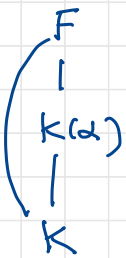
$\{w_j\}$ sono l. indip su F $\Rightarrow$ Tutti i coeff sono 0

$$\sum_{i=1}^{n} a_{1i} v_i = \quad = \sum_{i=1}^{n} a_{mi} v_i = 0$$

$\{v_1, \dots, v_n\}$ sono l. indip su $K \Rightarrow a_{ji} = 0 \ \forall i, \forall j$

Corollario F/K $\alpha \in F$

$\Rightarrow [K(\alpha) : K] \mid [F : K]$



Def F/K $\alpha_1, \dots, \alpha_n \in F$ algebrici su K

$$K[\alpha_1, \dots, \alpha_n] = \{ p(\alpha_1, \dots, \alpha_n) \mid p \in K[x_1, \dots, x_n] \}$$

Proposizione: $\alpha_1, \dots, \alpha_n \in F$ alg su K

1) $K[\alpha_1, \dots, \alpha_n]$ è un campo

2) $K[\alpha_1, \dots, \alpha_n]$ è il più piccolo sottocampo di F che contiene K e $\alpha_1, \dots, \alpha_n$

Dim (1) Per induzione su n.
$n = 1$ è il caso visto $K[\alpha] = K(\alpha)$

Per ip ind $F_0 = K[\alpha_1, \dots, \alpha_{n-1}]$ è un campo

$$K[\alpha_1, \dots, \alpha_n] = K[\alpha_1, \dots, \alpha_{n-1}][\alpha_n] = F_0[\alpha_n]$$

campo — il caso $n=1$ anche che è un campo

(2) $K[\alpha_1, \dots, \alpha_n] = \bigcap_{\substack{K \subseteq M \subseteq F \\ \alpha_1, \dots, \alpha_n \in M}} M$

è il più piccolo sottocampo di F che contiene $\alpha_1, \dots, \alpha_n$

- è campo perché $\cap$ di campi
- contiene K e $\alpha_1, \dots \alpha_n$ perché tutti i termini dell'$\cap$ li contengono

sì che è un sottocampo di F che contiene $\alpha_1, \dots \alpha_n$ perché è uno dei termini dell'$\cap$. $\supseteq$

Dall'altra parte $\forall M$ $K, \alpha_1, \dots, \alpha_n \subset M$

Poiché M è campo tutte le espressioni del tipo

$p(\alpha_1, \dots, \alpha_n)$ con $p \in K[x_1, \dots x_n]$ sono in M

$\Rightarrow K[\alpha_1, \dots, \alpha_n] \subset M$ $\forall M$ dell'intersezione

$$K[\alpha_1, \dots \alpha_n] \subset \bigcap_{\dots} M$$

□

Oss $[K[\alpha, \beta] : K] =$

$K[\alpha][\beta] \quad — \quad K(\alpha) \quad — \quad K$

deg polinomio di p su $K(\alpha)$ — deg $\mu_{\alpha/K}$

Esercizio Calcolare il pol minimo di $\sqrt[4]{2}$ su

$\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$

$\mathbb{R}$ $\quad \sqrt[4]{2} \in \mathbb{R}$ $\quad \mu_{\alpha|\mathbb{R}}(x) = x - \sqrt[4]{2}$

$\mathbb{Q}$ $\quad x - \sqrt[4]{2}$ $\quad x^2 = \sqrt{2}$ $\quad x^4 = 2$

$x^4 - 2 \in \mathbb{Q}[x]$ $\quad x^4 - 2 \in \ker \mu_{\sqrt[4]{2}/\mathbb{Q}} = (\mu_{\sqrt[4]{2}/\mathbb{Q}}(x))$

$= f(x)\, h(x)$

D'altra parte $x^4 - 2$ è irrid in $\mathbb{Z}[x]$ per il criterio di Eisenstein con $p = 2$ e quindi anche in $\mathbb{Q}[x]$ per il Lemma di Gauss. $\Rightarrow x^4 - 2 = \mu_{\sqrt[4]{2}/\mathbb{Q}}(x)$

Se $K \supseteq \mathbb{Q}$ il pol minimo di α/K è un fattore di $\mu_{\alpha/\mathbb{Q}}$

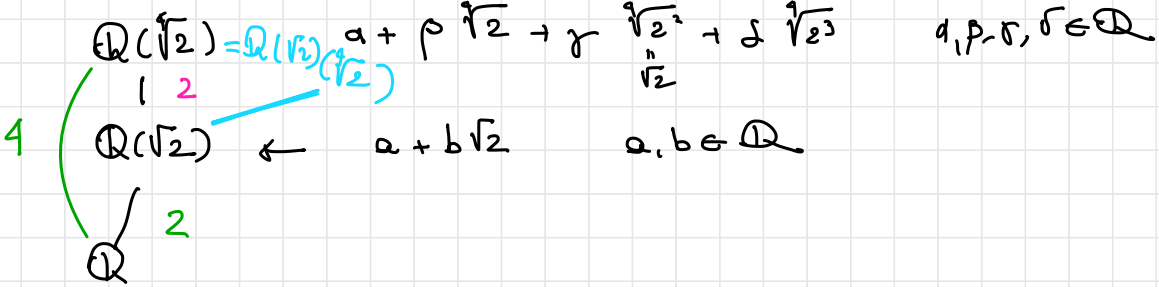
$\mu_{\alpha|\mathbb{Q}} \in K[x]$ e quindi $(\mu_{\alpha/K}) \ni \mu_{\alpha|\mathbb{Q}}$

$\Rightarrow \mu_{\alpha|\mathbb{Q}}(x) = \mu_{\alpha/K}(x) \cdot h(x)$

$\mathbb{Q}(\sqrt{2})$ $\quad \mu_{\sqrt[4]{2}/\mathbb{Q}(\sqrt{2})}(x) \mid \mu_{\sqrt[4]{2}/\mathbb{Q}}(x) = x^4 - 2$

$x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ e si annulla in $\sqrt[4]{2}$

quindi $x^4 - 2$ non è irriducibile in $\mathbb{Q}(\sqrt{2})$



Ho trovato $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$ che annulla $\sqrt[4]{2}$

So che $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})]$ è 2

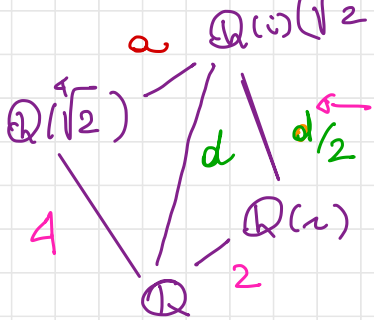
$\Rightarrow$ $x^2 - \sqrt{2}$ è il pol minimo di $\sqrt[4]{2}$ / $\mathbb{Q}(\sqrt{2})$

$\mathbb{Q}(i)$ è $x^2 + 1 = \mu_{i/\mathbb{Q}}(x)$

$i \in \mathbb{Q} \Rightarrow [\mathbb{Q}(i) : \mathbb{Q}] > 1$

$x^2 + 1 \in \mathbb{Q}[x] \Rightarrow \mu_{i/\mathbb{Q}}(x) \mid x^2 + 1 \Rightarrow \mu_{i/\mathbb{Q}}(x) = x^2 + 1$

$[\mathbb{Q}(i) : \mathbb{Q}] = 2$



$4 \mid d$

$2 \mid d$

$\Rightarrow [4,2] = 4 \mid d$

D'altra parte $\mu_{\sqrt[4]{2}/\mathbb{Q}(i)}(x) \mid x^4 - 2$ (ha grado $d/2$)

$\Rightarrow d/2 \leq 4$

$\Rightarrow 4 \mid d \quad d \leq 8 \Rightarrow d = \begin{cases} 4 \\ 8 \end{cases}$

$d = 4a$

$d = 8 \iff a = 2$

$d = 4 \iff a = 1$

$$\left[\mathbb{Q}(\sqrt[4]{2})(i) : \mathbb{Q}(\sqrt[4]{2}) \right] = a$$

Dico che $a = 2$ in quanto $\mathbb{Q}(\sqrt[4]{2})(i) \neq \mathbb{Q}(\sqrt[4]{2})$ perché $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ ma $i \notin \mathbb{R} \Rightarrow$ $i \notin \mathbb{Q}(\sqrt[4]{2}) \Rightarrow a \neq 1 \Rightarrow a = 2$

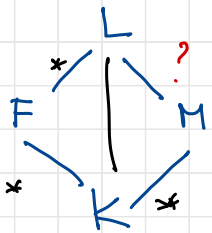
$\Rightarrow d = 8 \Rightarrow d/2 = 4$

$\Rightarrow \deg \mu_{\sqrt[4]{2}/\mathbb{Q}(i)} = 4$

$\Rightarrow \mu_{\sqrt[4]{2}/\mathbb{Q}(i)}(x) = x^4 - 2$

Riassumendo: • $K \subset L \subset F$ $\quad d \in F$ algebrico su K

$\mu_{d/K} \quad \mu_{d/L} \quad \mu_{d/L} \mid \mu_{d/K}$



Def L campo si dice **algebricamente chiuso** se ogni polinomio non costante di $L[x]$ ammette almeno una radice in L

Oss: 1) Il Teorema fond dell'algebra assicura che $\mathbb{C}$ è alg chiuso

2) L è alg chiuso $\iff$ ogni pol non cost di L si fattorizza in $L[x]$ come prodotto di pol di grado 1 $\iff$ i pol irred di $L[x]$ sono solo quelli di grado 1.

Def: $\overline{K}/K$ si dice che $\overline{K}$ è una chiusura algebrica di K se

1) $\overline{K}$ è alg chiuso

2) $\overline{K}$ è algebrico su K.

Esempi $\mathbb{C}$ è alg chiuso.

① $\mathbb{C}$ è una chiusura alg di $\mathbb{R}$.

$$\frac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{R}[i]$$

↑ ha come base su $\mathbb{R}$ $1, i$ cioè gli el di questo campo sono $a+ib$ $a,b \in \mathbb{R}$

$\Rightarrow \mathbb{C} = \mathbb{R}[i]$

$[\mathbb{C} : \mathbb{R}] = 2 \Rightarrow \mathbb{C}$ è alg su $\mathbb{R}$ perché questi sti finito è algebrico.

(α alg su $K \Rightarrow [K(\alpha) : K] = \deg_{\alpha|K} < +\infty$

$\Rightarrow K(\alpha)$ è algebrico su K)

$\Rightarrow \mathbb{C}$ 1) è alg chiuso
2) algebrico su $\mathbb{R}$ $\Longrightarrow$ $\mathbb{C}$ è una chiusura alg di $\mathbb{R}$.

(2) $\mathbb{C}$ non è una chiusura alg di $\mathbb{Q}$ perché non è algebrico su $\mathbb{Q}$.

Teorema (di esistenza e unicità della chiusura algebrica)

Ogni campo ammette una chiusura algebrica e questa è unica a meno di isomorfismo su K

($\overline{K}$ e Ω chiusure alg di K

$\Rightarrow \exists\ \varphi\ \overline{K} \to \Omega$ isomorfismo di anelli tale che $\varphi_{|K} = id$

Def K campo, $\overline{K}$ chiusura alg di K.

Sia $f \in K[x]$ non costante, e siano $\alpha_1, \dots, \alpha_n \in \overline{K}$ le sue radici

Si dice CAMPO DI SPEZZAMENTO DI f SU K il campo

$$K(\alpha_1, \dots, \alpha_n)$$

Oss Il campo di spezz di f su K è il più piccolo sottocampo di una data chiusura algebrica $\overline{K}$ che contiene tutte le radici di f.

Esempio $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ $\quad \sqrt[3]{2}, \ \zeta_3\sqrt[3]{2}, \ \zeta_3^2\sqrt[3]{2}$

$1, \zeta_3, \zeta_3^2$ sono le radici anche di 1

Il c. di s. di $f(x)$ su $\mathbb{Q}$

$$F = \mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\right)$$

- $F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

  $\supset \sqrt[3]{2} \in F$ perché si ottiene $\zeta_3 = \zeta_3\sqrt[3]{2} / \sqrt[3]{2} \in F$

  $\subset \sqrt[3]{2}$ e $\sqrt[3]{2}\,\zeta_3 \in F \dots \zeta_3^2\sqrt[3]{2} \in F$

- $[F : \mathbb{Q}] = 6$ ← FARE !

Caratteristica di un campo

F $\qquad \varphi : \mathbb{Z} \longrightarrow F$

$1 \longmapsto 1_F$

$n \longmapsto \underbrace{1_F + \dots + 1_F}_{n \text{ volte}}$

φ è omo di anelli

1° Teo di omo

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & F \\ \downarrow & \nearrow_{\bar{\varphi}} & \\ \mathbb{Z}/\ker\varphi & & \end{array}$$

$\ker\varphi = n\mathbb{Z}$ $\qquad n \neq 1$ perché $1_F \neq 0_F$

Dico che $n = 0$ oppure $n = \text{primo}$

Devo escludere $n = kh$ $\qquad 1 < k, h < n$

Infatti $\varphi(n) = 0 = \varphi(k)\,\varphi(h) = 0$

↳ in un campo vale la legge di annullamento del prodotto $\Rightarrow \varphi(k) = 0 \ \vee \ \varphi(h) = 0$ assurdo $k, h < n$

$\Rightarrow \ker \varphi = \begin{cases} \{0\} \\ p\mathbb{Z} \end{cases}$ per p primo

$\mathbb{Z}/\ker\varphi \simeq \begin{cases} \mathbb{Z} \\ \mathbb{Z}/p\mathbb{Z} \end{cases}$

Def $\operatorname{char} K = \begin{cases} 0 & \text{se } \ker\varphi = \{0\} \\ p & \text{se } \ker\varphi = p\mathbb{Z} \end{cases}$

Se $\operatorname{char} K = p \Rightarrow \mathbb{Z}/p\mathbb{Z} \hookrightarrow K$

$\operatorname{char} K = 0 \quad \mathbb{Z} \hookrightarrow K$ e poiché

K è un campo $\quad \mathbb{Q} \hookrightarrow K$

I campi di caratt 0 sono quelli che contengono $\mathbb{Q}$ quelli di caratt p contengono $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

Campi finiti

Un campo finito è un campo di cardinalità finita

Es $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ è un campo finito

$\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\zeta_4)$

Oss 1: Se F è un campo finito $|F| < +\infty$

$\Rightarrow$ $\mathrm{char} F = p$ per un certo primo p.

$$\mathrm{char} F = \begin{cases} 0 \Rightarrow \mathbb{Q} \subset F \Rightarrow |F| = +\infty \\ p \end{cases}$$

$\mathrm{char} F = p \Rightarrow \mathbb{F}_p \subset F$

Oss 2: Se $f(x) \in \mathbb{F}_p[x]$ irriducibile $\deg f = n$

$\Rightarrow$ $F = \mathbb{F}_p[x]/(f(x))$ è un campo

ha caratt p

ed ha card p^n

($[F : \mathbb{F}_p] = \deg f = n$ $1, \bar{x}, \dots, \bar{x}^{n-1}$ è $\mathbb{F}_p$ base di F

$a_0 + a_1 \bar{x} + \dots + a_{n-1} \bar{x}^{n-1}$ questi al al

variare di $a_i \in \mathbb{F}_p$ descrivono Tutti gli el di F

una e una sola volta → p scelto $\forall a_i$

$\Rightarrow p^n = |F|$

F come sp. vett è iso a $\mathbb{F}_p^n$

↑ attenzione $\mathbb{F}_p^n (= (\mathbb{Z}/p\mathbb{Z})^n)$ non è un campo

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

L'iso non è di anelli ma solo di sp. vett

Esempio: $\mathbb{F}_p(x)$ ha caratt p ma è un campo infinito

Esempi

$\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4 = \dfrac{\mathbb{F}_2[x]}{(x^2+x+1)}$, $\mathbb{F}_5$, $\exists\, \mathbb{F}_6$?

Lemma del binomio ingenuo

Sia K campo di caratt p. Allora $\forall x, y$ indeterminate e $\forall n$ $(x+y)^{p^n} = x^{p^n} + y^{p^n}$

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

$p \mid \binom{p}{i}$ $\forall i = 1, \dots, p-1$

$\binom{p}{i} = \dfrac{p!}{i!\,(p-i)!}$ ($p \mid p!$ ma $p \nmid i!\,(p-i)!$)

Nei campi di caratt p $\quad p = 0$

pseudo $\quad (x+y)^p = x^p + y^p$

Per induzione si dimostra $\forall n$.

$$(x+y)^{p^n} = \left((x+y)^{p^{n-1}}\right)^p \overset{\text{ip ind}}{=} \left(x^{p^{n-1}} + y^{p^{n-1}}\right)^p \overset{n=1}{=} x^{p^n} + y^{p^n}$$

□

Proposizione

F campo finito $\Rightarrow$ $|F| = p^n$ dove p è un primo e $n \geq 1$

Dim: F campo finito $\Rightarrow$ $\mathrm{char}\, F = p \Rightarrow F \supset \mathbb{F}_p$

$[F : \mathbb{F}_p] = n$

$\hookrightarrow [F : \mathbb{F}_p] < +\infty$ perché F ha solo un # finito di elementi

$\Rightarrow F \cong (\mathbb{F}_p)^n$ (come sp. vett)

($v_1, \dots, v_n$ base gli el di F $\quad \sum a_i v_i$ è unica e la loro scrittura

$F \longrightarrow (\mathbb{F}_p)^n$

$\sum a_i v_i \longrightarrow (a_1, \dots, a_n)$)

$\Rightarrow |F| = p^n$

□

Teorema:

$\forall\, p$ primo $\forall n \geq 1$ esiste un unico campo con p^n elementi in ogni fissata chiusura alg di $\mathbb{F}_p$.

Dim $\overline{\mathbb{F}_p}$ chiusura alg di $\mathbb{F}_p$.

Se $\exists\, F \subset \overline{\mathbb{F}_p}$ con p^n elem.

$$\mathbb{F}_p \subset F \subset \overline{\mathbb{F}_p}$$

$$|F^\times| = p^n - 1$$

Gli el $\neq 0$ di questo campo devono soddisfare il pol.

$$x^{p^n-1} - 1$$

(cioè $\forall\, \alpha \in F^\times \quad \alpha^{p^n-1} = 1$)

$$F \subset \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0\}$$

↳ α è radice di $x(x^{p^n-1} - 1) = x^{p^n} - x$

$f(x) = x^{p^n} - x$ ha grado p^n e quindi in $\overline{\mathbb{F}_p}$ ha esattamente p^n radici contate con molteplicità

Ha radici multiple? NO perché $f'(x) = p^n x^{p^n-1} - 1 = -1$

$(f(x), -1) = 1$

$$\Rightarrow \#\{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0\} = p^n$$

L'unica possibilità per avere un campo con p^n elem e che $\{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0\}$ sia un campo

Se non lo è $\Rightarrow$ $\overline{\mathbb{F}_p}$ non contiene campi con p^n el e quindi non esistono

Se è un campo $\Rightarrow \overline{\mathbb{F}_p}$ contiene un UNICO campo con p^n el.

$$F = \{ \alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0 \}$$

Verifico che F è un campo

$0, 1 \in F \qquad 0^{p^n} = 0 \qquad 1^{p^n} = 1$

$\alpha, \beta \in F \qquad \alpha \pm \beta \in F$

$\alpha^{p^n} = \alpha \qquad \beta^{p^n} = \beta \qquad \alpha\beta \in F$

$\beta^{-1} \in F \qquad (\beta^{-1})^{p^n} = \beta^{-p^n} = (\beta^{p^n})^{-1} = \beta^{-1}$

$\Rightarrow \beta^{-1} \in F$ ✓

$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ ✓

$(\alpha \pm \beta)^{p^n} \overset{\uparrow}{=} \alpha^{p^n} + (\pm\beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$ ✓ □

Notazione: Indicheremo con $\mathbb{F}_{p^n}$ l'unico sottocampo di $\overline{\mathbb{F}_p}$ con p^n el.

$$\mathbb{F}_{p^n} = \{ \alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0 \}$$

In particolare $\mathbb{F}_{p^n}$ è il c. di s. su $\mathbb{F}_p$ del pol $x^{p^n} - x$ (e anche di $x^{p^n-1} - 1$)

Che $\mathbb{F}_{p^n} = \dfrac{\mathbb{F}_p[x]}{(f(x))}$ per un certo $f(x) \in \mathbb{F}_p[x]$ riducibile di grado n?

Sì ma non possiamo ancora dirlo.

Teorema

Ogni sottogruppo moltiplicativo **finito** di un campo è ciclico.

Oss: Se K è un campo, il Teorema parla dei sottogruppi $G < K^\times$ $|G| < +\infty$

Abbiamo già visto con i cgr fusi di $\mathbb{C}^\times$

$G < \mathbb{C}^\times$ $|G| = n$ $\Rightarrow G = \{\zeta \in \mathbb{C}^* \mid \zeta^n = 1\}$

Oss: $\mathbb{Z}/2 \times \mathbb{Z}/2$ 1 el di ordine 1 $(\bar{0}\,\bar{0})$
3 el di ordine 2
0 el di ordine 4

Dim: K campo $G < K^\times$ $|G| = n < +\infty$

Voglio dimostrare che G è CICLICO.

Osservo che $\forall d$ il polinomio $X^d - 1 = f_d(x)$ ha al più d radici in K e quindi ha al più d radici in G $(\subset K)$

Se

$$G_d = \{ g \in G \mid g^d = 1 \} \Rightarrow |G_d| \leq d$$

$$k_d = \#\{ g \in G \mid \operatorname{ord} g = d \}$$

$d \nmid n \qquad k_d = 0$

$d \mid n \qquad k_d \begin{cases} = 0 \\ > 0 \end{cases} \rightarrow \exists\, g \in G \quad \operatorname{ord} g = d$

$\langle g \rangle < G$ di ordine $d \Rightarrow \langle g \rangle \subset G_d$

($\langle g \rangle$: ha ordine d; G_d: ha ordine $\leq d$)

$\Rightarrow$ Se G contiene un el di ordine d, g

$\Rightarrow$ ha un unico sgr di ordine d

G_d che è anche ciclico $\langle g \rangle$.

$\rightarrow k_d = \phi(d)$

$$n = |G| = \sum_{d \mid n} k_d \leq \sum_{d \mid n} \phi(d) = n$$

$=$

$\Rightarrow \forall\, d \mid n \quad k_d = \phi(d)$, in particolare $k_n = \phi(n) \geq 1$

G è ciclico $\square$

Corollario 1 $\quad \mathbb{F}_{p^n}^{\times}$ è ciclico $\quad \forall\, p, \forall\, n$.

Corollario 2 $\forall p, \forall n$ $\mathbb{F}_{p^n}$ è un'estensione semplice di $\mathbb{F}_p$, cioè $\exists \alpha \in \mathbb{F}_{p^n}$ t.c. $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$

Dim $\mathbb{F}_{p^n}^{\times} = \langle \alpha \rangle \Rightarrow \mathbb{F}_p[\alpha] = \mathbb{F}_{p^n}$

$\subset$ perché $\alpha, \mathbb{F}_p \subset \mathbb{F}_{p^n}$

$\supset$ $\forall \beta \in \mathbb{F}_{p^n}$ $\beta = 0$ oppure $\beta \in \langle \alpha \rangle$

$\Rightarrow \beta \in \mathbb{F}_p[\alpha]$

Oss: Abbiamo visto che ogni generatore del gruppo moltiplicativo ($\mathbb{F}_p^{\times} = \langle \alpha \rangle$) è un generatore dell'estensione $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$

Il viceversa è falso cioè se $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$ non è detto che α generi il gruppo moltiplicativo.

Cerchi esempio

Corollario $\forall p$ e $\forall n$ $\exists f \in \mathbb{F}_p[x]$ irriducibile di grado n (ce ne posso contare)

Dim $\forall p, \forall n$ $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha] \cong \dfrac{\mathbb{F}_p[x]}{(\mu_\alpha(x))}$

$\mu_\alpha(x)$ è irriducibile di grado n. Perciò $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ □

Oss: $f(x)$ irred. di grado n $\{\alpha_1, \dots, \alpha_n\} \subset \overline{\mathbb{F}_p}$

$\mathbb{F}_p[\alpha_1] \cong \mathbb{F}_p[x]/(f(x))$

$\mathbb{F}_p[\alpha_2] \cong \mathbb{F}_p[x]/(f(x)) \Rightarrow [\mathbb{F}_p[\alpha_n] : \mathbb{F}_p] = n$

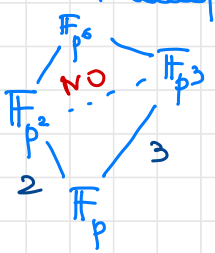
$\mathbb{F}_p[\alpha_n] \cong \mathbb{F}_p[x]/(f(x))$ ↑ ha p^n elem.

$\mathbb{F}_p[\alpha_i] \subset \overline{\mathbb{F}_p} \quad \forall i \Rightarrow \mathbb{F}_p[\alpha_1] = \dots = \mathbb{F}_p[\alpha_n]$

→ Il c. di spezzamento di $f(x)$

$\mathbb{F}_p[\alpha_1, \dots, \alpha_n] = \mathbb{F}_p[\alpha_i] = \mathbb{F}_{p^n}$ ↓ $\forall i$

Sottocampi di $\mathbb{F}_{p^n}$



$[\mathbb{F}_{p^3} : \mathbb{F}_p] 3 \qquad [\mathbb{F}_{p^2} : \mathbb{F}_p] = 2 \qquad 2 \nmid 3$

$\mathbb{F}_{p^2} \not\subset \mathbb{F}_{p^3}$

Proposizione

$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$

Dim: ($\Rightarrow$) $\mathbb{F}_p \subset \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ passo ai gradi

$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] [\mathbb{F}_{p^m} : \mathbb{F}_p] \Rightarrow n = mh$

↑ TORRI (h, m) $\Rightarrow m \mid n$

($\Leftarrow$) $m \mid n$ $\quad n = mh$

Vogliamo mostrare che $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ o analogamente che $\mathbb{F}_{p^m}^{\times} \subset \mathbb{F}_{p^n}^{\times}$

Ghi el di $\mathbb{F}_{p^m}^{\times} = \{ \alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^m - 1} = 1 \}$

e quelli di $\mathbb{F}_{p^n}^{*} = \{ \alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n - 1} = 1 \}$

$\alpha \in \mathbb{F}_{p^m}^{\times} \qquad \alpha^{p^m - 1} = 1$ *

Osservo $\quad p^m \equiv 1 \quad (p^m - 1)$

$n = mh \quad p^n \equiv p^{mh} \equiv 1^h = 1 \quad (p^m - 1)$

$\Rightarrow \quad p^n \equiv 1 \quad (p^m - 1) \quad \Rightarrow \quad p^n - 1 = \lambda (p^m - 1)$

* elevo alla λ e ottengo

$$\alpha^{(p^m - 1)\lambda} = 1^{\lambda} = 1$$

$$\alpha^{p^n - 1} = 1 \quad \Rightarrow \alpha \in \mathbb{F}_{p^n}^{\times}$$

$\square$

Campi di spezzamento su $\mathbb{F}_p$.

Teorema: Sue $f(x) \in \mathbb{F}_p[x]$ e sue $f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r}$

la sua fatt. su $\mathbb{F}_p$ - Possiamo $\deg f_i(x) = d_i$

$\Rightarrow$ Il c. di sp. di f su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$

dove $d = \text{mcm}\{d_1, \dots, d_r\}$

Dim: Sia $\mathbb{F}_{p^m}$ il c. di sp di $f(x)$ su $\mathbb{F}_p$

(è di questo tipo dato che è un est finito di $\mathbb{F}_p$

$\mathbb{F}_p(\gamma_1 \dots \gamma_n)$)

Devo dim che $m = d$

Sia γ_i una qualsiasi radice di $f_i(x)$

Dato che f_i è irriol il suo campo di sp è

$\mathbb{F}_p(\gamma_i) = \mathbb{F}_{p^{d_i}}$

$\mathbb{F}_{p^m}$ è per def la più piccola est di $\mathbb{F}_p$ che

contiene TUTTE le radici di f

$\Rightarrow \mathbb{F}_{p^m}$ è la più piccola est di $\mathbb{F}_p$ che

contiene $\mathbb{F}_{p^{d_i}}$ $\forall i$

Cioè m è il minimo intero T.C.

$d_i \mid m \quad \forall i \Rightarrow m = d = \text{mcm}\{d_i\}$

□

Osservazioni sulle fatt dei polinomi di $\mathbb{F}_p[x]$.

Sappiamo il criterio delle derivate.

Cordiamo: f irriducibile ha radici multiple

$$\iff f'(x)=0$$

(f irrid non ha fattori propri.

f ha radici multiple $(f,f') \neq 1$

1 $\quad f \quad \Rightarrow f \mid f'$

non perché ha fattori multipli

$\Rightarrow$ non $\quad \deg f > \deg f' \Rightarrow f'=0$

In campi di caratt $=0$ non succede mai

$\rightarrow$ i polinomi irriducibili hanno sempre radici distinte (sono separabili)

E in char p? Può succedere

Esempio: $\mathbb{K}=\mathbb{F}_p(x) \quad \mathbb{K}[t]$

$f(t)=t^p-x \qquad f'(t)=pt^{p-1}=0$

$f(t)$ è irriducibile

$\alpha \in \overline{\mathbb{K}} \quad f(\alpha)=0 \quad \alpha^p=x \quad f(t)=t^p-\alpha^p =$

$= (t-\alpha)^p$

Nei campi finiti non succede che un polinomio irriducibile abbia radici multiple.

Teorema: $f \in \mathbb{F}_p[x]$ e $f'(x) = 0 \Rightarrow f(x) = g(x)^p$ con $g(x) \in \mathbb{F}_p[x]$

Campi di spezzamento su $\mathbb{F}_p$ $x^n - 1$

$f_n(x) = x^n - 1 \in \mathbb{F}_p[x]$ $\quad n = p^a m \quad (m,p) = 1$

$$f_n(x) = x^{mp^a} - 1 = (x^m - 1)^{p^a} = f_m(x)^{p^a}$$

c. di sp di $f_n(x)$ = c. di sp. di $f_m(x)$ $p \nmid m$.

$$G_d = \{ \alpha \in \overline{\mathbb{F}}_p \mid \alpha^{p^l} - 1 = 0 \}$$

Lemma: $G_n = G_m$ è ciclico di ordine m.

Dim $G_n = G_m$ $\quad f_n(x) = f_m(x)^{p^a}$

$G_n < \overline{\mathbb{F}}_p^*$ ed è finito quindi ciclico

$|G_m| = m$ $\quad f_m(x)$ ha m radici distinte

$f_m'(x) = mx^{m-1} \neq 0 \quad p \nmid m$

$(f, f') = 1$

$f = x^m - 1$ ↑ $f' = m x^{m-1}$

□

C. di sp di $f_m(x) = x^m - 1$

$\mathbb{F}_p[G_m] = \mathbb{F}_{p^k}$ si tratta di trovare k.

Lemma 2 $G_m \subset \mathbb{F}_{p^k} \iff m \mid p^k - 1$

Dim: ($\Rightarrow$) $G_m \subset \mathbb{F}_{p^k} \iff G_m < \mathbb{F}_{p^k}^\times \Rightarrow m = |G_m| \mid p^k - 1$ (dove $|\mathbb{F}_{p^k}^\times| = p^k - 1$)

($\Leftarrow$) $m \mid p^k - 1 \Rightarrow p^k - 1 = h m$

$\alpha \in G_m \iff \alpha^m = 1 \Rightarrow \alpha^{p^k - 1} = \alpha^{mh} = 1^h = 1$

$\Rightarrow \alpha \in \mathbb{F}_{p^k}^\times$

□

Teorema $n = p^a m$ $(m, p) = 1$

Il c. di sp di $x^n - 1$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^k}$ con

$k = \operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times} p$

Dim: c. di sp $x^n - 1$ = c. di s $x^m - 1$

$\mathbb{F}_p[G_m] = \mathbb{F}_{p^k}$

So che $G_m \subset \mathbb{F}_{p^d} \iff m \mid p^d - 1$

k è il minimo numero per il quale si ha

$$G_m \subset \mathbb{F}_{p^k}$$

$$k = \min\{d \mid m \mid p^d - 1\} = \min\{d \mid p^d \equiv 1 \ (m)\}$$

$$= \operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^*} p$$

□

Esempio: $f_7(x) = x^7 - 1$ e.d.sp su $\mathbb{F}_3$ → su $\mathbb{F}_{11}$

$\mathbb{F}_3$ cerco $\operatorname{ord}_{(\mathbb{Z}/7\mathbb{Z})^*} 3$

$3^d \equiv 1 \ (7)$

$d \equiv 0 \ (6)$

↳ 6

$$x^7 - 1 = (x-1)(x^6 + x^5 + \dots + x + 1)$$

6 = m.c.m dei gradi dei fattori irriducibili di $x^7 - 1$

⇒ $x^6 + x^5 + \dots + x + 1$ o è irriducibile

$3 + 2 + 1$

Ma $3 + 2 + 1$ non è possibile perché

in $\mathbb{F}_3$ non ha radici perché $d^7 \equiv 1 \ (3)$

$d \equiv 1 \ (3)$

$\mathbb{F}_{11}$ $\operatorname{ord}_{(\mathbb{Z}/7\mathbb{Z})^*} 11 = 3$

$x^7 - 1 = (x-1)(x^6 + \dots + x + 1)$ → $3+1+1+1$, $3+3$

perché il grado del c.d. sp è 3

Escludo $3+1+1+1$ perché l'unico radice è -1

e non ha radici multiple.

$x^8 - 1$ su $\overline{\mathbb{F}_p}$

$p = 2 \qquad x^8 - 1 = (x-1)^8$

$p \neq 2 \qquad p^k \equiv 1 \quad (8) \qquad k = 1, \; k = 2$

$\Rightarrow$ i fattori irred di $x^8 - 1$ su $\overline{\mathbb{F}_p}$ hanno grado 1 o 2

$$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$$

x^4+1 è sempre riducibile su $\overline{\mathbb{F}_p}$ $\forall p$

Il polinomio x^4+1 è irriducibile su $\mathbb{Q}$

ma è rid mod p $\forall p$.