

Aritmetica

A.A. 2022-2023

SIMONE SACCANI



numeri di Fibonacci

I numeri di Fibonacci sono definiti:
$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_n = F_{n-1} + F_{n-2} \quad \forall n \geq 2 \end{cases}$$

vorrei una formula "compatta", ossia vorrei dire chi è F_n senza dover calcolare F_{n-1} e F_{n-2}

Faccio un tentativo: provo a cercare un $\alpha \in \mathbb{R}$ t.c. $F_n = \alpha^n$

α dovrebbe soddisfare $\alpha^n = \alpha^{n-1} + \alpha^{n-2}$

$\alpha = 0$ lo escludo. Allora posso dividere per α^{n-2} : $\alpha^2 = \alpha + 1 \rightarrow \alpha^2 - \alpha - 1 = 0$

Dunque se un simile α esistesse, dovrebbe essere una radice del polinomio $x^2 - x - 1$

Ma queste radici le conosco: $\alpha = \frac{1+\sqrt{5}}{2}$ $\beta = \frac{1-\sqrt{5}}{2}$

Verifico subito che $F_n \neq \left(\frac{1+\sqrt{5}}{2}\right)^n$ e $F_n \neq \left(\frac{1-\sqrt{5}}{2}\right)^n$ già per n piccoli

Nota però che $\alpha^n + \beta^n$ è una successione che soddisfa la regola ricorsiva di Fibonacci:

$$\alpha^n + \beta^n = (\alpha^{n-1} + \beta^{n-1}) + (\alpha^{n-2} + \beta^{n-2})$$

Tento allora $F_n = \alpha^n + \beta^n$

Quali a e b potrebbero andare bene?

$$\begin{cases} F_0 = a\alpha^0 + b\beta^0 \\ F_1 = a\alpha^1 + b\beta^1 \end{cases} \rightarrow \begin{cases} 0 = a + b \\ 1 = a\left(\frac{1+\sqrt{5}}{2}\right) + b\left(\frac{1-\sqrt{5}}{2}\right) \end{cases}$$

Si risolve il sistema e si trova che c'è una sola soluzione: $a = \frac{1}{\sqrt{5}}$ $b = -\frac{1}{\sqrt{5}}$

Dunque:

Teorema Dato $n \in \mathbb{N}$, vale la seguente formula per i numeri di Fibonacci:

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

Metodo per le ricorrenze lineari a coefficienti costanti

Il metodo si generalizza e si può tentare per tutte le successioni lineari a coefficienti costanti:

$$a_n = r_1 a_{n-1} + r_2 a_{n-2} + r_3 a_{n-3} + \dots + r_i a_{n-i} \quad \text{con } r_1, r_2, r_3, \dots, r_i \in \mathbb{C}$$

esempio

$$\begin{cases} a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3} & n \geq 4 \\ a_1 = 4 \\ a_2 = 22 \\ a_3 = 82 \end{cases}$$

Provo: $a_n = \alpha^n$

α dovrebbe soddisfare $\alpha^n = 6\alpha^{n-1} - 11\alpha^{n-2} + 6\alpha^{n-3}$

Dato che $\alpha = 0$ di sicuro non va bene

Divido per α^{n-3} : $\alpha^3 = 6\alpha^2 - 11\alpha + 6$

Ossia α deve essere una radice di $x^3 - 6x^2 + 11x - 6$

Le radici sono 1, 2, 3

Osservo che $a_n = 1^n$ non va bene; $a_n = 2^n$ non va bene; $a_n = 3^n$ non va bene.

Tento allora $a_n = a \cdot 1^n + b \cdot 2^n + c \cdot 3^n$ con a, b, c da determinare

Tento in questo modo perché so che $a_n = a \cdot 1^n + b \cdot 2^n + c \cdot 3^n$

soddisfa la stessa relazione ricorsiva di a_n

Per trovare a, b, c imposto il sistema:

$$\begin{cases} a \cdot 1^1 + b \cdot 2^1 + c \cdot 3^1 = a_1 = 4 \\ a \cdot 1^2 + b \cdot 2^2 + c \cdot 3^2 = a_2 = 22 \\ a \cdot 1^3 + b \cdot 2^3 + c \cdot 3^3 = a_3 = 82 \end{cases}$$

Risolvere il sistema e trovo un'unica soluzione: $\begin{cases} a = -2 \\ b = -3 \\ c = 4 \end{cases}$

Dunque la successione $C_n = (-2) \cdot 1^n + (-3) \cdot 2^n + 4 \cdot 3^n$ soddisfa la stessa regola ricorsiva di a_n e inoltre $a_1 = C_1$, $a_2 = C_2$, $a_3 = C_3$.

"Dunque" $\forall n \geq 1$ vale $a_n = C_n$

ATTENZIONE

Se il polinomio associato ha una radice con molteplicità maggiore di uno, la successione è costruita con α^n e la sua "derivata", $n\alpha^{n-1}$, dove α è la radice.

esempio

$$b_0 = 5 \quad b_1 = 7 \quad b_n = 4b_{n-1} - 4b_{n-2}$$

$$x^2 - 4x + 4 = 0 \rightarrow (x-2)^2 = 0 \rightarrow x=2$$

$$\Rightarrow b_n = a2^n + bn2^{n-1}$$

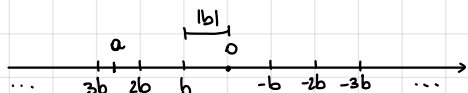
$$\begin{cases} 5 = a2^0 + b \cdot 0 \cdot 2^{-1} \\ 7 = a \cdot 2^1 + b \cdot 1 \cdot 2^0 \end{cases} \Leftrightarrow \begin{cases} a = 5 \\ b = -3 \end{cases}$$

$$\Rightarrow b_n = 5 \cdot 2^n - 3n \cdot 2^{n-1}$$

Divisione euclidea

$$a, b \in \mathbb{Z}, b \neq 0$$

Esistono unici $q, r \in \mathbb{Z}$ tali che $a = qb + r$ con $0 \leq r < |b|$



DEF. $a, b \in \mathbb{Z}$, a divide b se esiste $c \in \mathbb{Z}$ tale che $b = ac$

Se $(a, b) \neq (0, 0)$, il Massimo Comun Divisore di a e b è denotato $\text{MCD}(a, b) \geq 1$

$$a, b \in \mathbb{Z}, b \neq 0$$

Siano $q_1, r_1 \in \mathbb{Z}$ tali che $a = q_1 b + r_1$ con $0 \leq r_1 < |b|$

Se $r_1 = 0$ ci fermiamo. Altrimenti siano $q_2, r_2 \in \mathbb{Z}$ tali che $b = q_2 r_1 + r_2$ con $0 \leq r_2 < |r_1|$

Se $r_2 = 0$ ci fermiamo. Altrimenti siano $q_3, r_3 \in \mathbb{Z}$ tali che $r_1 = q_3 r_2 + r_3$ con $0 \leq r_3 < |r_2|$

Se $r_3 = 0$ ci fermiamo. Altrimenti...

Si costruisce così la successione: $r_1 = a$ $r_0 = b$ $r_{i-2} = q_i r_{i-1} + r_i$ con $0 \leq r_i < |r_{i-1}|$ per $i = 1, 2, 3, \dots$

Poiché $0 \leq r_i < |r_{i-1}|$, la successione si ferma.

Sia k il minimo tale che $r_{k+1} = 0$

proposizione $|r_k| = \text{MCD}(a, b)$

$$r_{k-1} = q_{k+1} r_k + r_{k+1} = 0 \quad \text{Quindi } r_k \text{ divide } r_{k-1}$$

$$r_{k-2} = q_k r_{k-1} + r_k \quad \text{Quindi } r_k \text{ divide } r_{k-2}$$

$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} \quad \text{Quindi } r_k \text{ divide } r_{k-3} \dots$$

Si conclude che $|r_k|$ divide a e b

$$r_1 = q_1 r_0 + r_1 \rightarrow r_1 = r_1 - q_1 r_0 \quad \text{Se divide } r_1 \text{ e } r_0, \text{ deve dividere } r_1$$

$$r_0 = q_2 r_1 + r_2 \rightarrow r_2 = r_0 - q_2 r_1 \quad \text{Quindi } d \text{ divide } r_2$$

... Si conclude che d divide $|r_k|$

claim Se d divide a e b , allora d divide $qa - b$

DIM Esiste c_1 tale che $a = dc_1$

Esiste c_2 tale che $b = dc_2$

$$qa - b = qdc_1 - dc_2 = d(\underbrace{qc_1 - c_2}_{c_3})$$

esempio

$$a = 124 \quad b = -17$$

$$a = q_1 b + r_1 \text{ tali che } 0 \leq r_1 < |b| = 17$$

$$124 = (-7)(-17) + 5 \quad q_1 = -7 \quad r_1 = 5$$

$$b = q_2 r_1 + r_2 \text{ tali che } 0 \leq r_2 < |r_1| = 5$$

$$-17 = (-4) \cdot 5 + 3 \quad q_2 = -4 \quad r_2 = 3$$

$$r_1 = q_3 r_2 + r_3 \text{ tali che } 0 \leq r_3 < |r_2| = 3$$

$$5 = 1 \cdot 3 + 2 \quad q_3 = 1 \quad r_3 = 2$$

$$r_2 = q_4 r_3 + r_4 \text{ tali che } 0 \leq r_4 < |r_3| = 2$$

$$3 = 1 \cdot 2 + 1 \quad q_4 = 1 \quad r_4 = 1$$

$$r_3 = q_5 r_4 + r_5 \text{ tali che } 0 \leq r_5 < |r_4| = 1$$

$$2 = 2 \cdot 1 + 0 \quad q_5 = 2 \quad r_5 = 0$$

$$\rightarrow \text{MCD}(124, -17) = |r_4| = 1$$

Teorema di Bezout

Siano $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$
 Allora esistono $y, z \in \mathbb{Z}$ tali che
 $ya + zb = \text{MCD}(a, b)$

esempio

$$1 = 3 - 1 \cdot 2$$

$$2 = 5 - 1 \cdot 3$$

$$1 = 3 - 1(5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5$$

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

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

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

$$5 = 12 \cdot 4 - (-7)(-17)$$

$$1 = 2(-1 \cdot 7) + 7(12 \cdot 4 - (-7)(-17)) =$$

$$= 7 \cdot 12 \cdot 4 + 51(-1 \cdot 7)$$

$$r_4 = r_2 - q_4 r_3$$

$$r_3 = r_1 - q_3 r_2$$

$$r_4 = r_2 - q_4(r_1 - q_3 r_2) = (1 + q_3 q_4) r_2 - q_4 r_1$$

$$r_2 = r_0 - q_2 r_1$$

$$r_4 = (1 + q_3 q_4)(r_0 - q_2 r_1) - q_4 r_1 = (1 + q_3 q_4) r_0 + (-q_2 - q_2 q_3 q_4 - q_4) r_1$$

$$r_1 = r_{-1} - q_1 r_0$$

$$r_4 = (1 + q_3 q_4) r_0 + (-q_2 - q_2 q_3 q_4 - q_4)(r_{-1} - q_1 r_0) =$$

$$= (1 + q_3 q_4 - q_1(-q_2 - q_2 q_3 q_4 - q_4)) r_0 + (-q_2 - q_2 q_3 q_4 - q_4) r_{-1}$$

DIMOSTRAZIONE

Prendiamo $a > b \geq 1$ e sia lo sviluppo dell'algoritmo di Euclide:

$$(n+1 \text{ passi}) \quad \text{MCD}(a, b) \left\{ \begin{array}{l} a = q_1 b + r_1 \\ b = q_2 r_1 + r_2 \\ \dots \\ r_{n-2} = q_n r_{n-1} + r_n \\ r_{n-1} = q_{n+1} r_n + 0 \end{array} \right\} \text{MCD}(b, r_1) \quad (n \text{ passi})$$

Sia $P(n)$: "se a e b sono due numeri per cui l'algoritmo di Euclide richiede n passi, allora vale Bezout."

BASE $a = q_1 b$ $\text{MCD}(a, b) = b = 0 \cdot a + 1 \cdot b$

PASSO INDUTTIVO Prendo $P(n)$ VERA e cerco di dimostrare $P(n+1)$

$$\text{MCD}(b, r_1) = \lambda b + \mu r_1 \quad \lambda, \mu \in \mathbb{Z}$$

Osservo che un divisore comune di a e b deve dividere $r_1 = a - q_1 b$

$$\text{e in particolare } \text{MCD}(a, b) = \text{MCD}(a, b, r_1) = \text{MCD}(b, r_1) = \lambda b + \mu r_1$$

Dalla prima equazione dell'algoritmo di Euclide ricavo $r_1 = a - q_1 b$

$$\text{Sostituendo } \text{MCD}(a, b) = \lambda b + \mu(a - q_1 b) = \mu a + (\lambda - q_1 \mu) b$$

$$\text{Perciò } \exists y, z \in \mathbb{Z} \text{ t.c. } \text{MCD}(a, b) = ya + zb$$

Quindi $P(n)$ è vera $\forall n \geq 1$.

□

$P(n)$ $n \in \mathbb{N}$ predicato

esempio $P(n)$: " $2^n > n^2 + 3n + 1$."

$Q(n)$: "quando piove n gatti" NO

Principio di induzione

Supponiamo di avere un predicato $P(n)$, $n \in \mathbb{N}$.

Se, dato un numero $n_0 \in \mathbb{N}$, vale che

① $P(n_0)$ è VERA (base dell'induzione)

② $\forall n \geq n_0 \quad P(n) \Rightarrow P(n+1)$ (passo induttivo)

Allora vale che $P(n)$ è vera $\forall n \geq n_0$

DIMOSTRAZIONE successione $a_n = c_n$ (pg. 1)

Sia $P(n)$: " $a_n = c_n$ "

BASE $P(1)$ è VERA

PASSO INDUTTIVO Sia $n \geq 1$. Prendo per VERA $P(n)$ e cerco di dimostrare $P(n+1)$: $a_n = c_n \Rightarrow a_{n+1} = c_{n+1}$

$$a_2 = c_2, a_3 = c_3$$

$$a_4 = 6a_3 - 11a_2 + 6a_1$$

$$c_4 = 6c_3 - 11c_2 + 6c_1$$

$$a_{n+1} = 6a_n - 11a_{n-1} + 6a_{n-2}$$

$$c_{n+1} = 6c_n - 11c_{n-1} + 6c_{n-2}$$

Ho fallito ma...

$Q(n)$: " $\forall k$ t.c. $1 \leq k \leq n$ vale che $a_k = c_k$ "

BASE $Q(1)$ VERA $Q(1)$: $a_1 = c_1$

PASSO INDUTTIVO $Q(1) \Rightarrow Q(2)$, $Q(2) \Rightarrow Q(3)$ le verifico direttamente.

Sia ora $n \geq 3$. Prendo per vera $Q(n)$ e cerco di dimostrare $Q(n+1)$

$$a_{n+1} = 6a_n - 11a_{n-1} + 6a_{n-2}$$

$$c_{n+1} = 6c_n - 11c_{n-1} + 6c_{n-2}$$

Per ipotesi induttiva, so che $a_n = c_n$, $a_{n-1} = c_{n-1}$, $a_{n-2} = c_{n-2}$.

Allora deduco che $a_{n+1} = c_{n+1}$

Dunque la $Q(n+1)$ è vera.

Il principio di induzione ora dice che $Q(n)$ è vera per ogni $n \geq 1$ \square

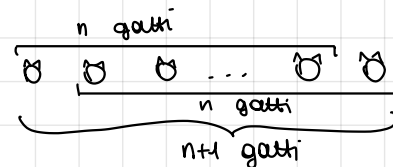
ATTENZIONE

La verifica del passo base è importantissima.

esempio $P(n)$: "Dati n gatti, sono tutti dello stesso colore."

BASE $P(1)$ vera

PASSO INDUTTIVO Prendo per vera $P(n)$



Problema: $P(2)$ FALSA

$P(1) \Rightarrow P(2)$? è FALSA e non compresa nell'argomento

Principio di induzione forte

Dato $P(n)$ predicato.

Se, per un $n_0 \in \mathbb{N}$, vale che:

① $P(n_0)$ è vera

② $\forall n \geq n_0, [P(n_0) \wedge P(n_0+1) \wedge P(n_0+2) \wedge \dots \wedge P(n)] \Rightarrow P(n+1)$

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

È equivalente all'induzione semplice.

Assioma del buon ordinamento Ogni sottoinsieme non vuoto di \mathbb{N} ha un minimo.
(principio del minimo)

È equivalente ai principi di induzione.

esercizio Dato un numero intero $a \geq 2$, dimostrare che a si fattorizza come prodotto di uno o più fattori primi.

DIMOSTRAZIONE

Per induzione forte

$P(n)$: "sia $n \geq 2$, allora n si fattorizza come prodotto di uno o più fattori primi."

BASE $P(2)$ VERA

Sia $n \geq 2$, prendo per vere $P(2), P(3), \dots, P(n)$ e cerco di dimostrare $P(n+1)$

$n+1 = \begin{cases} \text{primo} & \text{☺} \\ \text{altrimenti} & n+1 = ab \text{ con } 1 < a < n+1, 1 < b < n+1 \end{cases}$

So dalla $P(a)$ che a si scrive come prodotto di primi.

So dalla $P(b)$ che b si scrive come prodotto di primi.

Allora $n+1 = \underbrace{\text{prodotto dei primi che danno } a} \cdot \underbrace{\text{prodotto dei primi che danno } b}$

DIMOSTRAZIONE ALTERNATIVA

Principio del minimo

Sia $S = \{n \geq 2 \mid P(n) \text{ è FALSA}\}$

Se S non fosse vuoto, per il principio del minimo, $\exists m \in S$ minimo

$m = \begin{cases} \text{primo? NO} \\ \text{non primo? } m = ab \text{ con } 1 < a < m, 1 < b < m \end{cases}$

a, b dunque $\notin S$, essendo minori del suo minimo.

Allora $P(a)$ e $P(b)$ sono VERE

Come sopra, dalle scritture di a e b come prodotto di primi, ricavo che m si scrive come prodotto di primi

ASSURDO perché $m \in S$ e $P(m)$ FALSA

□

teorema Siano a, b, c interi.
se $a \mid bc$ e $\text{MCD}(a, b) = 1$, allora $a \mid c$.

DIMOSTRAZIONE

Per Bezout, so che esistono λ, μ tali che $\lambda a + \mu b = 1$

Moltiplico per c : $\lambda ac + \mu bc = c$

Noto che $a \mid ac$ e $a \mid bc$ per ipotesi

Allora a divide il membro di sinistra.

Dunque $a \mid c$. □

proposizione Dati $a, b \in \mathbb{Z}$ non entrambi nulli, vale:

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

DIMOSTRAZIONE

Per Bezout esistono λ, μ tali che $\lambda a + \mu b = \text{MCD}(a, b)$

Divido per $\text{MCD}(a, b)$:

$$\lambda \cdot \frac{a}{\text{MCD}(a,b)} + \mu \cdot \frac{b}{\text{MCD}(a,b)} = 1$$

Si vede immediatamente che se d è divisore comune di $\frac{a}{\text{MCD}(a,b)}$ e $\frac{b}{\text{MCD}(a,b)}$ allora d deve dividere 1 □

CONGRUENZE

Def. Sia m intero positivo

Diremo che a è congruo a b modulo m

$$a \equiv b (m)$$

se il resto della divisione euclidea di a per m è uguale al resto della divisione euclidea di b per m .

esempio

$$17 \equiv 5 (12)$$

$$17 = 1 \cdot 12 + 5 \quad 5 = 0 \cdot 12 + 5$$

$$-31 \equiv 17 (12)$$

$$-31 = 12(-3) + 5$$

proposizione

$$a \equiv b (m) \text{ se e solo se } m \mid a - b$$

DIMOSTRAZIONE

Infatti:

$$\Rightarrow \text{supponiamo } a \equiv b (m) : a = mq_1 + r \text{ e } b = mq_2 + r$$

$$\text{Allora } a - b = mq_1 + r - mq_2 - r = m(q_1 - q_2)$$

$$\text{Dunque } m \mid a - b$$

$$\Leftarrow \text{Se } m \mid a - b, \text{ allora } a - b = ms \rightarrow a = b + ms$$

Se la divisione euclidea di b per m è:

$$b = qm + r$$

Ho che

$$a = b + ms = (qm + r) + ms = m(q + s) + r$$

ed è questa la divisione euclidea di a per m .

$$\text{Quindi } a \equiv b (m)$$

□

esempio

$$-3 \stackrel{?}{\equiv} 12 (15) \text{ Vero}$$

teorema

$$\text{Se } a \equiv a' (m) \text{ e } b \equiv b' (m)$$

$$\text{Allora } ab \equiv a'b' (m) \text{ e } a + b \equiv a' + b' (m)$$

DIMOSTRAZIONE

$$a \equiv a' (m) \rightarrow m \mid a - a' \rightarrow a - a' = ms, \text{ con } s \in \mathbb{Z}$$

$$b \equiv b' (m) \rightarrow m \mid b - b' \rightarrow b - b' = mr, \text{ con } r \in \mathbb{Z}$$

$$ab - a'b' = (a' + ms)(b' + mr) - a'b' = \cancel{a'b'} + a'mr + b'ms + m^2rs - \cancel{a'b'} = m(a'r + b's + mrs)$$

$$\text{Da cui: } m \mid ab - a'b' \rightarrow ab \equiv a'b' (m)$$

$$a + b - a' - b' = \cancel{a'} + ms + \cancel{b'} + mr - \cancel{a'} - \cancel{b'} = m(s + r)$$

$$\text{Da cui: } m \mid a + b - (a' + b') \rightarrow a + b \equiv a' + b' (m) \quad \square$$

esempio

$$17 \cdot (-31) \equiv ? (12)$$

$$17 \equiv 5 (12) \text{ e } -31 \equiv 5 (12)$$

$$\text{Per cui } 17 \cdot (-31) \equiv 5 \cdot 5 \equiv 1 (12)$$

esempio

$$\text{Calcolare } 3^{17} \equiv ? (11)$$

$$3 \equiv 3 (11)$$

$$3^2 \equiv -2 (11)$$

$$3^4 \equiv 4 (11)$$

$$3^8 \equiv 16 \equiv 5 (11)$$

$$3^{16} \equiv 3 (11)$$

$$3^{17} \equiv 3 \cdot 3 \equiv 9 \equiv -2 (11)$$

critéri di divisibilità

• DIVISIBILITÀ per 3

"un numero è congruo modulo 3 alla somma delle sue cifre"

esempio $12483 = 1 \cdot 10^4 + 2 \cdot 10^3 + 4 \cdot 10^2 + 8 \cdot 10 + 3 \equiv 1 + 2 + 4 + 8 + 3 \equiv 0 \pmod{3}$

Nota $10 \equiv 1 \pmod{3}$

esempio $17822 \equiv 1 + 7 + 8 + 2 + 2 = 20 \equiv 2 \pmod{3}$

• DIVISIBILITÀ PER 11

esempio $12483 = 1 \cdot 10^4 + 2 \cdot 10^3 + 4 \cdot 10^2 + 8 \cdot 10 + 3$

Nota $10 \equiv -1 \pmod{11}$

$12483 \equiv 1(-1)^4 + 2(-1)^3 + 4(-1)^2 + 8(-1) + 3 \equiv 1 - 2 + 4 - 8 + 3 \equiv -2 \equiv 9 \pmod{11}$

esempio 12483782 è un quadrato?

NO infatti

$12483782 \equiv 2 \pmod{3}$

Ma osservo che nessun quadrato $\equiv 2 \pmod{3}$

Infatti $a^2 \equiv \begin{cases} 0 \\ 1 \end{cases} \pmod{3}$

Perché se $a \equiv 0 \pmod{3}$ allora $a^2 \equiv 0 \pmod{3}$

se $a \equiv 1 \pmod{3}$ allora $a^2 \equiv 1 \pmod{3}$

se $a \equiv 2 \pmod{3}$ allora $a^2 \equiv 1 \pmod{3}$

(esaurisce tutti i casi possibili)

DEF. Diremo che b è un **inverso** di a modulo m se

$ab \equiv 1 \pmod{m}$

esempio (-31) è un inverso di 17 modulo 12

$(-31) \cdot 17 \equiv 5 \cdot 5 \equiv 1 \pmod{12}$

Teorema Un intero a ha un inverso modulo m
se e solo se $\text{MCD}(a, m) = 1$

DIMOSTRAZIONE

\Leftarrow : Per Bezout, esistono λ, μ tali che

$$\lambda a + \mu m = 1$$

$$\lambda a + \mu \cdot 0 \equiv 1 \pmod{m} \rightarrow \lambda a \equiv 1 \pmod{m}$$

Ponendo $b = \lambda$, ho finito.

\Rightarrow : Supponiamo che esista b inverso di a modulo m , ossia

$$ab \equiv 1 \pmod{m}$$

Questo equivale a dire che

$$m \mid ab - 1$$

ossia

$$ab - 1 = km \quad \text{per un certo intero } k$$

$$ab - km = 1$$

Da cui col consueto argomento, si ricava

$$\text{MCD}(a, m) = 1$$

□

TeoremaDato $m \in \mathbb{N} \setminus \{0\}$ $\forall a \in \mathbb{Z} \setminus \{0\}, \forall b_1, b_2 \in \mathbb{Z}$

Vale

$$ab_1 \equiv ab_2 \pmod{m} \quad \text{se e solo se} \quad b_1 \equiv b_2 \pmod{\frac{m}{\text{MCD}(a,m)}}$$

DIMOSTRAZIONE \Rightarrow : Supponiamo che $ab_1 \equiv ab_2 \pmod{m}$ Allora $m \mid ab_1 - ab_2$ ossia esiste q intero tale che

$$mq = ab_1 - ab_2$$

Divido per $\text{MCD}(a, m)$

$$\frac{m}{\text{MCD}(a, m)} \cdot q = \frac{a}{\text{MCD}(a, m)} (b_1 - b_2)$$

primi fra loro

 $\frac{m}{\text{MCD}(a, m)}$ divide $\frac{a}{\text{MCD}(a, m)} (b_1 - b_2)$, ma è primo con $\frac{a}{\text{MCD}(a, m)}$, allora

$$\frac{m}{\text{MCD}(a, m)} \mid b_1 - b_2$$

ossia

$$b_1 \equiv b_2 \pmod{\frac{m}{\text{MCD}(a, m)}}$$

 \Leftarrow : Supponiamo che $b_1 \equiv b_2 \pmod{\frac{m}{\text{MCD}(a, m)}}$

Allora

$$\frac{m}{\text{MCD}(a, m)} \cdot k = b_1 - b_2$$

da cui

$$mk = \text{MCD}(a, m) (b_1 - b_2)$$

ossia

$$m \mid \text{MCD}(a, m) (b_1 - b_2)$$

da cui

$$m \mid \text{MCD}(a, m) (b_1 - b_2) \cdot \frac{a}{\text{MCD}(a, m)}$$

cioè

$$m \mid (b_1 - b_2) \cdot a$$

ossia

$$ab_1 \equiv ab_2 \pmod{m} \quad \square$$

esempio

$$6 \equiv 42 \pmod{12}$$

$$1 \equiv 7 \pmod{12} \quad \text{FALSO}$$

$$1 \equiv 7 \pmod{2}$$

esempio

$$22 \equiv 154 \pmod{12}$$

$$2 \equiv 14 \pmod{12}$$

MORALE: in una congruenza, si può moltiplicare entrambi i membri per un numero primo col modulo ottenendo una congruenza equivalente
Lo stesso con "dividere" (se si può dividere)

Equazioni di primo grado con le congruenze

$$ax \equiv b \pmod{m}$$

con $a, b \in \mathbb{Z}$, m intero positivo

Teorema L'equazione $ax \equiv b \pmod{m}$ ha soluzione se e solo se $\text{MCD}(a, m) \mid b$

DIMOSTRAZIONE

\Rightarrow Sia $\bar{x} \in \mathbb{Z}$ una soluzione: $a\bar{x} \equiv b \pmod{m}$

$m \mid a\bar{x} - b$, ossia $a\bar{x} - b = km$, k intero

$$a\bar{x} - km = b$$

Da cui $\text{MCD}(a, m) \mid b$

\Leftarrow Supponiamo $\text{MCD}(a, m) \mid b$

Considero $ax \equiv b \pmod{m}$

Uso la regola della divisione per osservare l'equazione sopra è equivalente a

$$\frac{a}{\text{MCD}(a, m)} x \equiv \frac{b}{\text{MCD}(a, m)} \pmod{\left(\frac{m}{\text{MCD}(a, m)}\right)} \quad (*)$$

Osservo che $\frac{a}{\text{MCD}(a, m)}$ è primo con $\frac{m}{\text{MCD}(a, m)}$.

Allora è invertibile modulo $\frac{m}{\text{MCD}(a, m)}$. Sia c un inverso.

$$\text{Considero } c \frac{a}{\text{MCD}(a, m)} x \equiv c \frac{b}{\text{MCD}(a, m)} \pmod{\left(\frac{m}{\text{MCD}(a, m)}\right)} \quad (**)$$

Nota: (*) e (**) sono equivalenti perché ho moltiplicato per c , che è primo con il modulo (c infatti è invertibile modulo $\frac{m}{\text{MCD}(a, m)}$)

In conclusione, l'equazione iniziale è equivalente a:

$$x \equiv c \cdot \frac{b}{\text{MCD}(a, m)} \pmod{\left(\frac{m}{\text{MCD}(a, m)}\right)}$$

□

esempio

$$70x \equiv 222 \pmod{24}$$

$$35x \equiv 111 \pmod{12}$$

$$-x \equiv -9 \pmod{12}$$

$$x \equiv 9 \pmod{12}$$

$$S = \{ 9 + 12k \mid k \in \mathbb{Z} \}$$

esempio

$$168x \equiv 3080 \pmod{455}$$

$$168x \equiv 350 \pmod{455}$$

$$84x \equiv 175 \pmod{455} \quad (5 \cdot 7 \cdot 13)$$

$$12x \equiv 25 \pmod{65}$$

$$\text{MCD}(12, 65) = 1$$

Faccio invece

$$12x \equiv 25 + 65 \pmod{65}$$

$$12x \equiv 90 \pmod{65}$$

$$6x \equiv 45 \pmod{65}$$

$$\text{Noto che } 6 \cdot 11 = 66 \equiv 1 \pmod{65}$$

Allora moltiplico per 11

$$11 \cdot 6x \equiv 45 \cdot 11 \pmod{65}$$

$$x \equiv 495 \pmod{65}$$

$$x \equiv 40 \pmod{65}$$

Se usassi Euclide e Bezout

$$1 = 12\lambda + 65\mu$$

$$1 \equiv 12\lambda \pmod{65}$$

esempio

equazione diofantea di primo grado in due variabili

$$3192x + 117y = 288 \quad (*)$$

Trovare tutte le coppie $(\bar{x}, \bar{y}) \in \mathbb{Z} \times \mathbb{Z}$ che la rendono vera

oss. Noto che se (\bar{x}, \bar{y}) è soluzione, allora

$$3192\bar{x} + 117\bar{y} = 288$$

$$117\bar{y} = 288 - 3192\bar{x}$$

$$\text{Quindi } 117 \mid 288 - 3192\bar{x}$$

$$3192\bar{x} \equiv 288 \quad (117) \quad (**)$$

Quindi se (\bar{x}, \bar{y}) risolve la (*), allora \bar{x} risolve la (**) e viceversa,
se \bar{x} risolve la (**), allora esiste unica una coppia (\bar{x}, \bar{y}) che risolve (*)

Studio dunque

$$3192x \equiv 288 \quad (117)$$

$$1064x \equiv 96 \quad (39)$$

$$11x \equiv 18 \quad (39)$$

$$\text{MCD}(11, 39) = 1$$

Moltiplico per 7

$$77x \equiv 126 \quad (39)$$

$$-x \equiv 9 \quad (39)$$

$$x \equiv -9 \quad (39)$$

$$\text{ossia } x \equiv 30 \quad (39)$$

Le soluzioni sono $30 + 39k$ al variare di $k \in \mathbb{Z}$

$$117y + 3192(30 + 39k) = 288$$

$$117y = 288 - 30 \cdot 3192 - 3192 \cdot 39k$$

$$y = -816 - 1064k$$

Quindi tutte e sole le soluzioni della diofantea iniziale sono le coppie

$$(30 + 39k, -816 - 1064k) \text{ al variare di } k \in \mathbb{Z}$$

Per esempio per $k=0$ $(30, -816)$

$$\text{per } k=1 \quad (-9, 248) \rightarrow (-9 + 39q, 248 - 1064q) \text{ al variare di } q \in \mathbb{Z}$$

oss. $ax \equiv b \pmod{m}$ ha le stesse soluzioni di

$$\frac{a}{k}x \equiv \frac{b}{k} \pmod{\frac{m}{\text{MCD}(a, m)}} \quad \text{se } k|a \text{ e } k|b$$

Teorema cinese del resto

Teorema cinese del resto

Dato il sistema di congruenze

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

i cui moduli sono due a due coprimi ($\text{MCD}(m_i, m_j) = 1, i \neq j$).

tal sistema ammette sempre soluzione;

esiste un'unica soluzione x_0 con $0 \leq x_0 < m_1 m_2 \dots m_k$,

e tutte le soluzioni sono:

$$x_0 + s \cdot m_1 m_2 \dots m_k \quad \text{con } s \in \mathbb{Z}$$

DIMOSTRAZIONE

Per induzione su n , numero di equazioni del sistema.

BASE $n=2$

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases} \quad a + km_1 \quad \text{con } k \in \mathbb{Z} \quad \text{sono le soluzioni della prima eq.}$$

$$\rightarrow a + km_1 \equiv b \pmod{m_2} \quad \text{cerchiamo } k: m_1 k \equiv b - a \pmod{m_2}$$

C'è soluzione se e solo se $\text{MCD}(m_1, m_2) \mid b - a$

Siano x_0 e x_1 due soluzioni del sistema

$$\begin{cases} x_0 \equiv a \pmod{m_1} \\ x_0 \equiv b \pmod{m_2} \end{cases} \quad \begin{cases} x_1 \equiv a \pmod{m_1} \\ x_1 \equiv b \pmod{m_2} \end{cases} \Rightarrow \begin{cases} x_0 - x_1 \equiv 0 \pmod{m_1} \\ x_0 - x_1 \equiv 0 \pmod{m_2} \end{cases}$$

$x_0 - x_1$ è un multiplo di $\text{mcm}(m_1, m_2)$

Se x_0 è soluzione del sistema, allora $x_0 + s \cdot \text{mcm}(m_1, m_2)$ con $s \in \mathbb{Z}$ è ancora soluzione.

$$\begin{cases} x_0 \equiv a \pmod{m_1} \\ x_0 \equiv b \pmod{m_2} \end{cases} \rightarrow \begin{aligned} x_0 &= a + k_1 m_1 \quad \text{per un } k_1 \in \mathbb{Z} \\ x_0 &= b + k_2 m_2 \quad \text{per un } k_2 \in \mathbb{Z} \end{aligned}$$

$$x_0 + s \cdot \text{mcm}(m_1, m_2) = a + k_1 m_1 + s \cdot \text{mcm}(m_1, m_2) \quad \text{dove } \text{mcm}(m_1, m_2) = m_1 \cdot \overline{m_1}$$

$$a + m_1 k_1 + s \overline{m_1} \cdot m_1 = a + m_1 (k_1 + s \overline{m_1})$$

$$\text{Quindi } x_0 + s \cdot \text{mcm}(m_1, m_2) \equiv a \pmod{m_1}$$

$$\text{Se } \text{MCD}(m_1, m_2) = 1, \text{ le soluzioni sono } x_0 + s \cdot m_1 m_2$$

PASSO INDUTTIVO

Supponiamo che il sistema $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_{n-1} \pmod{m_{n-1}} \end{cases}$ abbia soluzione $x_0 + s \cdot m_1 m_2 \dots m_{n-1}$, $s \in \mathbb{Z}$

Consideriamo il sistema $\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_{n-1} \pmod{m_{n-1}} \\ x \equiv a_n \pmod{m_n} \end{cases}$

Il sistema ammette soluzione se e solo se: $x_0 + s \cdot m_1 m_2 \dots m_{n-1} \equiv a_n \pmod{m_n}$

Da cui $s \cdot m_1 m_2 \dots m_{n-1} \equiv a_n - x_0 \pmod{m_n}$. Per $\text{MCD}(m_n, m_1 m_2 \dots m_{n-1}) = 1 \mid a_n - x_0$, quindi ammette sempre soluzione.

Siano x_1 e x_2 due soluzioni del sistema:

$$\begin{cases} x_1 \equiv a_1 \pmod{m_1} \\ \vdots \\ x_1 \equiv a_n \pmod{m_n} \end{cases} \quad \begin{cases} x_2 \equiv a_1 \pmod{m_1} \\ \vdots \\ x_2 \equiv a_n \pmod{m_n} \end{cases} \Rightarrow \begin{cases} x_1 - x_2 \equiv 0 \pmod{m_1} \\ \vdots \\ x_1 - x_2 \equiv 0 \pmod{m_n} \end{cases}$$

Quindi tutte le soluzioni differiscono per un multiplo di m_1, m_2, \dots, m_n

Ossia le soluzioni sono $x_1 + s \cdot m_1 m_2 \dots m_n$, $s \in \mathbb{Z}$

□

esempio

$$\begin{cases} 14x \equiv 4570 \pmod{30} & \text{MCD}(14, 30) = 2 \mid 4570 \\ 45x \equiv 231 \pmod{8} & \text{MCD}(8, 45) = 1 \mid 231 \end{cases}$$
$$\begin{aligned} 14x &\equiv 10 \pmod{30} & 5x &\equiv -1 \pmod{8} \\ 7x &\equiv 5 \pmod{15} & -x &\equiv -3 \pmod{8} \\ -x &\equiv 10 \pmod{15} & x &\equiv 3 \pmod{8} \\ x &\equiv 5 \pmod{15} \end{aligned}$$
$$\rightarrow \begin{cases} x \equiv 5 \pmod{15} \\ x \equiv 3 \pmod{8} \end{cases} \quad \begin{aligned} \text{MCD}(15, 8) &= 1 \mid 5-3 \\ x &= 5 + k \cdot 15 \\ x_0 &= 35 + s \cdot 120 \quad s \in \mathbb{Z} \end{aligned}$$

Def. $n, k \in \mathbb{Z}, n \geq k \geq 0$

$\binom{n}{k}$:= numero di sottoinsiemi di $\{1, 2, \dots, n\}$ di cardinalità k

teorema

Formula di Newton: per $n \in \mathbb{N}$ e x variabile, si ha

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k$$

proposizione

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k \cdot (k-1) \cdot \dots \cdot 2 \cdot 1} = \frac{n!}{k! (n-k)!} \quad \binom{n}{k} = \binom{n}{n-k}$$

p primo $\binom{p}{i}$

$$\binom{p}{i} \cdot i! (p-i)! = p!$$

$$1 \leq i \leq p-1, \quad 1 \leq p-i \leq p-1 \quad \Rightarrow p \mid \binom{p}{i} \quad \text{se } i \neq 0, i \neq p$$

esempio

$$p=5 \quad \binom{5}{0}=1, \binom{5}{1}=5, \binom{5}{2}=10, \binom{5}{3}=10, \binom{5}{4}=5, \binom{5}{5}=1$$

**PICCOLO
teorema di
Fermat**

Se p è un primo e $a \in \mathbb{Z}$ non è multiplo di p , allora:

$$a^{p-1} \equiv 1 \pmod{p}$$

DIMOSTRAZIONE

$$a^p \equiv a \pmod{p}$$

Supponiamo $n^p \equiv n \pmod{p}$

Vogliamo dimostrare $(n+1)^p \equiv n+1 \pmod{p}$

$$\text{Nota che } (a+b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i} \equiv a^p + b^p \pmod{p} \quad (\text{per il lemma})$$

$$\Rightarrow (n+1)^p \equiv n^p + 1^p \equiv n + 1 \pmod{p}$$

Per induzione $n^p \equiv n \pmod{p}$ quindi $(n+1)^p \equiv n+1 \pmod{p}$

Il passo base è $n=1$: $1^{p-1} \equiv 1 \pmod{p}$ Vero \square

esempio

$$15^{1443} \equiv ? \pmod{7}$$

$$1443 = 9 \cdot 6 + 3 \quad 0 \leq r < 6$$

Per Fermat: $15^6 \equiv 1 \pmod{7}$

$$15^{1443} = 15^{9 \cdot 6 + 3} = (15^6)^9 \cdot 15^3 \equiv 15^3 \pmod{7}$$

$$1443 \equiv 3 \pmod{6}$$

$$15^3 \equiv ? \pmod{7}$$

Def. Chiamiamo ordine di un elemento $[a]_m \neq [0]_m$ in \mathbb{Z}_m il più piccolo intero positivo b tale che $[a]^b = 1$. Scriveremo $b = o([a])$

esempio in \mathbb{Z}_7 cerco $o([2])$
 $[2]^1 = [2]$ $[2]^2 = [4]$ $[2]^3 = [8] = [1] \rightarrow o([2]) = 3$

cerco $o([3])$

$$[3]^1 = [3] \quad [3]^2 = [2] \quad [3]^3 = [6] = [-1] \quad [3]^6 = [1] \rightarrow o([3]) = 6$$

proposizione Se $[a] \neq [0]$ in \mathbb{Z}_p e se $[a]^c = 1$, allora $o([a]) \mid c$

DIMOSTRAZIONE

Infatti $c = o([a]) \cdot q + r$ con $0 \leq r < o([a])$

$$[a]^c = [1]$$

$$[a]^{o([a]) \cdot q + r} = [1]$$

$$([a]^{o([a])})^q [a]^r = [1]$$

$$\text{Da cui } [a]^r = 1$$

Deve essere $r=0$, altrimenti si contraddice la minimalità dell'ordine

Teorema di Wilson

Sia p primo, allora

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv -1 \pmod{p}$$

$$\text{oppure } [1] \cdot [2] \cdot \dots \cdot [p-1] = [-1] \text{ in } \mathbb{Z}_p$$

DIMOSTRAZIONE

Si nota che, a parte $[1]$ e $[-1]$, per ogni fattore $[a]$ compare anche il suo inverso $[b]$, che è distinto da $[a]$.

Sia infatti $[c]$ tale che l'inverso di $[c]$ sia sempre $[c]$.

$$\text{Vale allora } [c][c] = 1$$

$$[c]^2 = 1$$

$$c^2 - 1 \equiv 0 \pmod{p} \quad (c+1)(c-1) \equiv 0 \pmod{p} \rightarrow p \mid (c+1)(c-1)$$

Se $\text{MCD}(p, c-1) = 1$ allora $p \mid c+1$ ossia $c \equiv -1 \pmod{p}$

Se $\text{MCD}(p, c-1) = p$ allora $p \mid c-1$ ossia $c-1 \equiv 0 \pmod{p}$ $c \equiv 1 \pmod{p}$

Dunque nel prodotto $[1][2] \dots [p-1]$ i fattori si semplificano a due a due eccetto $[1]$ e $[p-1] = [-1]$ □

esempio In \mathbb{Z}_{11} : $[1] \cdot \cancel{[2]} \cdot \cancel{[3]} \cdot \cancel{[4]} \cdot \cancel{[5]} \cdot \cancel{[6]} \cdot \cancel{[7]} \cdot \cancel{[8]} \cdot \cancel{[9]} \cdot [10] = [1] \cdot [10] = [1] \cdot [-1] = [-1]$

RSA

p e q due primi distinti (Alice e Bob)

B conosce p e q , e costruisce $e \in \mathbb{N}$ tale che sia invertibile $\text{mod}((p-1)(q-1))$

e poi si calcola $d \in \mathbb{N}$ tale che $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$

B dà ad A $n = pq$ e e

A prende il suo messaggio $m \in \mathbb{N}$, $0 < m < pq$

A calcola $m^e \text{ mod } pq$, diciamo c : A manda c a B

B decripta il messaggio di A calcolando $c^d \text{ mod } (pq)$: in questo modo ritrova m !

proposizione p e q primi distinti, e e d tali che $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$, $0 < m < pq$.
Allora $(m^e)^d \equiv m \pmod{pq}$

DIMOSTRAZIONE

$x \equiv m \pmod{pq}$ è equivalente (per il teorema cinese del resto) a

$$\begin{cases} x \equiv m \pmod{p} \\ x \equiv m \pmod{q} \end{cases}$$

$$(m^e)^d \equiv m \pmod{p} \quad (m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} = m + (m^{p-1})^{k(q-1)} \equiv m \cdot 1^{k(q-1)} = m \pmod{p}$$

esempio

$$p=7, q=13, e=5 \rightarrow pq=91 \quad (p-1)(q-1)=72$$

A ci manda $c=44$

$$2 \cdot 72 = 144 = 145 - 1 = 29 \cdot 5 - 1 \rightarrow d=29$$

$$44^{29} \equiv ? \pmod{91}$$

$$91 \cdot 11 = 1001 \equiv 0 \pmod{91} \quad 2^{10} = 1024 \equiv 23 \pmod{91} \quad 4 \cdot 23 = 92 \equiv 1 \pmod{91}$$

$$2^{12} \equiv 1 \pmod{91} \quad 2^5 \cdot 2^5 = 2^{10} \equiv 23 \pmod{91} \quad 11^2 = 121 \equiv 30 \pmod{91} \quad 11^4 \equiv 30^2 \equiv 900 \equiv -10 \pmod{91}$$

$$(11^4)^3 \equiv (-10)^3 \equiv -1000 \equiv 1 \pmod{91} \quad (2 \cdot 2 \cdot 11)^{29} \equiv 23 \cdot 11^5 \equiv 23 \cdot 11 \cdot (-10) \equiv 71 \cdot (-10) \equiv 18 \pmod{91}$$

$$\Rightarrow 44^{29} \equiv 18 \pmod{91}$$

classi di resto

Fissiamo $n \in \mathbb{N}, n \geq 2$

$a \in \mathbb{Z}$, $[a]_n := \{a + km, k \in \mathbb{Z}\}$ classi di resto modulo m

esempio

$$n=4$$

$$[0]_4, [1]_4, [2]_4, [3]_4, [1]_4 = [5]_4$$

In generale: $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$ (oppure $\mathbb{Z}/n\mathbb{Z}$)

Definiamo su \mathbb{Z}_n due operazioni:

la somma: $[a]_n + [b]_n := [a+b]_n \quad +: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$

il prodotto: $[a]_n \cdot [b]_n := [a \cdot b]_n \quad \cdot: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$

esempio Verificare che le definizioni sono ben poste

Proprietà

- Esiste il "neutro" della somma, ossia $[0]_n + [b]_n = [b]_n = [b]_n + [0]_n$
- Esiste l' "opposto" rispetto alla somma di ogni elemento: $[a]_n + [-a]_n = [0]_n = [-a]_n + [a]_n$
- La somma è associativa: $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$
- La somma è commutativa: $[a]_n + [b]_n = [b]_n + [a]_n$
- Esiste il "neutro" del prodotto: $[1]_n \cdot [a]_n = [a]_n = [a]_n \cdot [1]_n$
- Il prodotto è associativo: $([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$
- Distributività: $[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$, $([a]_n + [b]_n) \cdot [c]_n = [a]_n \cdot [c]_n + [b]_n \cdot [c]_n$
- Il prodotto è commutativo: $[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$

TEORIA DEI GRUPPI

DEF. Un gruppo G è un insieme non vuoto con una operazione, che indicheremo con \cdot , tale che:

- 1) $\forall a, b, c \in G$ vale $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (proprietà associativa)
- 2) $\exists e$ tale che $\forall a \in G$ vale $a \cdot e = e \cdot a = a$ (esistenza dell'elemento neutro, detto identità)
- 3) $\forall a \in G \exists b \in G$ tale che $a \cdot b = b \cdot a = e$ (esistenza dell'inverso)

DEF. Un gruppo si dice **commutativo** o **abeliano** se l'operazione è commutativa, ossia:

- 4) $\forall a, b \in G \quad a \cdot b = b \cdot a$

Teorema Dato G gruppo, vale:

- 1) c'è un solo elemento neutro e
- 2) $\forall a \in G$ esiste un solo inverso, che chiameremo a^{-1}
- 3) $\forall a \in G$ vale che $(a^{-1})^{-1} = a$
- 4) $\forall a, b \in G$ vale che $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
- 5) $a, b, c \in G$: l'equazione $a \cdot x \cdot b = c$ ha un'unica soluzione $x = a^{-1} \cdot c \cdot b^{-1}$ in G

DIMOSTRAZIONE

- 1) Siano e, e' elementi neutri

$$e = e \cdot e' = e' \quad \text{perché } e' \text{ è elemento neutro} \quad \text{perché } e \text{ è l'elemento neutro}$$

- 2) Siano h e k due inversi di a

$$h = h \cdot e = h \cdot (a \cdot k) = (h \cdot a) \cdot k = e \cdot k = k$$

- 3) Osserviamo che $(g^{-1})^{-1} (g^{-1}) = e = (g^{-1}) (g^{-1})^{-1}$ per def di $(g^{-1})^{-1}$

$$\text{D'altra parte } g \cdot g^{-1} = e = g^{-1} \cdot g \quad \text{per def di } g^{-1}$$

In conclusione g e $(g^{-1})^{-1}$ sono entrambi inversi di g^{-1} .

Per il punto 2) $g = (g^{-1})^{-1}$

- 4) Considero $e = (a \cdot b) \cdot (a \cdot b)^{-1}$.

Moltiplico per $(b^{-1} \cdot a^{-1})$ e applico la proprietà associativa:

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

$$\text{Da cui } (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

- 5) Sia \bar{x} una soluzione: $a \bar{x} b = c$

Allora, moltiplicando a sinistra per a^{-1} e a destra per b^{-1} :

$$\bar{x} = (a^{-1} \cdot a) \bar{x} (b \cdot b^{-1}) = a^{-1} c b^{-1}. \quad \text{Quindi l'unica soluzione è } x = a^{-1} c b^{-1} \quad \square$$

DEF. Dato G gruppo, diremo che

un sottoinsieme $H \subseteq G$ è un **sottogruppo di G** se:

- 1) $e \in H$
- 2) $\forall a, b \in H$ vale $a \cdot b \in H$
- 3) $\forall a \in H$ vale $a^{-1} \in H$

Si scriverà **$H < G$**

esempio $\{e\} < G, \quad G < G$

Def. Dato un gruppo G , si definisce **centro di G** il sottoinsieme formato dagli elementi che commutano con tutti gli elementi del gruppo:

$$Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$$

Vale $Z(G) < G$

Nota: Se G è commutativo, $Z(G) = G$

esempio

$(\mathbb{Z}_m, +)$ è un gruppo

$\mathbb{Z}_m^* = \{[a]_m \mid [a]_m \text{ è invertibile}\}$ è un gruppo con l'operazione moltiplicazione

$$\mathbb{Z}_4^* = \{[1]_4, [3]_4\} \quad \mathbb{Z}_5^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$$

$$\mathbb{Z}_6^* = \{[1]_6, [5]_6\} \quad \mathbb{Z}_8^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$$

Def. Dato un elemento $a \in G$, chiamo

$$(a) = \{a^i \mid i \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$$

$(a^{-1})^2 \uparrow$ \uparrow inverso di a

Con queste convenzioni, vale la confortante regola $a^i \cdot a^j = a^{i+j} \ \forall i, j \in \mathbb{Z}$

oss: $(a) < G$

Def. Se, per qualche $a \in G$, vale $G = (a)$, diremo che G è un **gruppo ciclico** e si dice che a genera G .

esempio

$(\mathbb{Z}_m, +)$ è un gruppo ciclico

$$\mathbb{Z}_m = ([1]_m)$$

esempio

$(\mathbb{Z}, +)$ è un gruppo ciclico

$$\mathbb{Z} = (1) = (-1)$$

Invece (2) è sottogruppo di \mathbb{Z} : $(2) \neq \mathbb{Z}$

Def. Dato un numero intero n , una **permutazione** dei numeri $1, 2, \dots, n$ è una funzione f bigettiva dall'insieme $\{1, 2, \dots, n\}$ in se stesso.

Chiamiamo S_n l'insieme di tali permutazioni.

Nota: $|S_n| = n!$

(S_n, \circ) è un gruppo

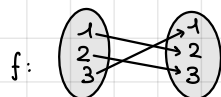
Def. Chiamiamo S_n il **gruppo simmetrico** su n elementi.

esempio

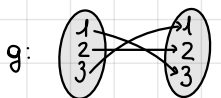
$$S_3 = \{f : \{1, 2, 3\} \rightarrow \{1, 2, 3\} \mid f \text{ è bigettiva}\}$$

(S_3, \circ) è un gruppo $|S_3| = 6$

Rappresento così i suoi elementi



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



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

Faccio un calcolo $g = (1, 3)(2)$ $h = (1, 2)(3)$

$$g \circ h = (1, 2, 3) \quad h \circ g = (1, 3, 2) \quad g \circ h \neq h \circ g \rightarrow S_3 \text{ non è commutativo}$$

Elenco dei 6 elementi di S_3 :

$$S_3 = \{(1)(2)(3), (1, 2)(3), (1, 3)(2), (2, 3)(1), (1, 2, 3), (1, 3, 2)\}$$

$$S_3 = \{e, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$$

$$\text{Sia } H = \{e, (1, 2)\} \quad \text{Notiamo che } H < S_3$$

Laterali sinistri

Def. Sia G un gruppo, sia $H < G$

Chiameremo **laterale sinistro di H** o H -laterale sinistro, un sottoinsieme del tipo:

$$gH = \{gh \mid h \in H\} \quad \text{dove } g \in G$$

L'insieme i cui elementi sono gli H laterali sinistri si indica con G/H

e la sua cardinalità $|G/H|$ si chiama indice di H in G .

esempio

Sia $G = S_3$. Sia $H = \{e, (1,2)\}$

I laterali sinistri di H sono:

$$eH = \{e \cdot e, e(1,2)\} = \{e, (1,2)\} = H$$

$$(1,2)H = \{(1,2)e, (1,2)(1,2)\} = \{(1,2), e\} = H$$

$$(1,3)H = \{(1,3)e, (1,3)(1,2)\} = \{(1,3), (1,2,3)\} \quad \text{non è sottogruppo di } G$$

$$(1,2,3)H = \{(1,2,3)e, (1,2,3)(1,2)\} = \{(1,2,3), (1,3)\}$$

$$(2,3)H = \{(2,3)e, (2,3)(1,2)\} = \{(2,3), (1,3,2)\} \quad \text{non è sottogruppo di } G$$

$$(1,3,2)H = \{(1,3,2)e, (1,3,2)(1,2)\} = \{(1,3,2), (2,3)\}$$

Notiamo che i laterali di H in S_3 sono 3, a due a due disgiunti, e forniscono una partizione di S_3

esempio

Sia $G = (\mathbb{Z}, +)$

$$H = (5)$$

$$0+H = \{x \in \mathbb{Z} \mid x \equiv 0 (5)\} = [0]_5$$

$$1+H = \{x \in \mathbb{Z} \mid x \equiv 1 (5)\} = [1]_5$$

$$2+H = [2]_5$$

$$3+H = [3]_5$$

$$4+H = [4]_5$$

$$5+H = [5]_5 = [0]_5 = 0+H$$

teorema

Sia G gruppo e $H < G$.

Ogni elemento $w \in G$ è contenuto in uno ed un solo laterale sinistro di H , che coincide con wH

DIMOSTRAZIONE

Nota subito che $w \in wH = \{w \cdot e, wh_1, \dots\}$

Supponiamo adesso che $w \in pH$, con $p \in G$.

Dobbiamo mostrare che $pH = wH$

Infatti $w \in pH$ significa $\exists h_1 \in H$ t.c. $w = ph_1$

Ora scrivo $pH = \{ph \mid h \in H\} = \{ph_1h \mid h \in H\}$, cioè $H = h_1H$

$$h_1H = \{h_1h \mid h \in H\} \subseteq H$$

$$H \subseteq h_1H$$

Preso $\bar{h} \in H$ noto che $h_1^{-1}\bar{h} \in H$, allora $h_1h_1^{-1}\bar{h} \in h_1H$

Ma $h_1h_1^{-1}\bar{h} = e\bar{h} = \bar{h}$, dunque $\bar{h} \in h_1H$

Dunque $pH = ph_1H = wH$

□

corollario

I laterali sinistri di H danno una partizione di G .

corollario Dati gH e bH laterali, allora $bH = gH$ se e solo se $b \in gH$ (o equivalentemente $g \in bH$).

DIMOSTRAZIONE

\Rightarrow : $bH = gH$. Per definizione di laterale, e poiché $e \in H$, si ha: $b \in bH$ e $g \in gH$.
Ma poiché $bH = gH$: $b \in gH$ e $g \in bH$.
 \Leftarrow : $b \in gH$ e $g \in bH$. Ma per definizione di classe laterale, $b \in bH$ e $g \in gH$.
Per il teorema, $bH = gH$. \square

corollario Dati gH e bH laterali, allora $bH = gH$ se e solo se $g^{-1}b \in H$ (o equivalentemente $b^{-1}g \in H$).

DIMOSTRAZIONE

\Rightarrow : $bH = gH$. Per il corollario precedente $b \in gH$ e $g \in bH$.
Poiché esiste l'inverso: $g^{-1}b \in g^{-1}gH = H$ e $b^{-1}g \in b^{-1}bH = H$.
 \Leftarrow : $g^{-1}b \in H$ e $b^{-1}g \in H$. Moltiplicando per gli inversi: $b = gg^{-1}b \in gH$ e $g = bb^{-1}g \in bH$.
Per il corollario precedente, questa condizione è equivalente a $bH = gH$. \square

teorema di Lagrange Se G è gruppo finito e $H < G$ allora $|H|$ divide $|G|$.

DIMOSTRAZIONE

I laterali sinistri di H danno una partizione di G .

Basta dimostrare che

$$\forall g \in G, |gH| = |H|$$

Costruisco la funzione $f: H \rightarrow gH$
$$h \mapsto gh$$

e mostro che f è bigettiva

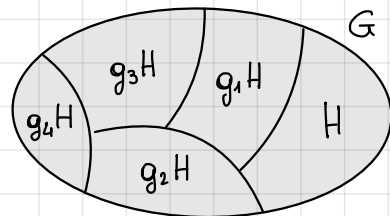
f è surgettiva per definizione di gH

f è iniettiva perché

$$\text{Siano } h_1, h_2 \text{ tali che } f(h_1) = f(h_2) \rightarrow gh_1 = gh_2$$

Moltiplico entrambi i membri per g^{-1} :

$$g^{-1}gh_1 = g^{-1}gh_2 \rightarrow h_1 = h_2 \quad \square$$



def. Sia G gruppo

Chiamo **ordine** di $g \in G$, il più piccolo intero positivo t tale che $g^t = e$

Si scrive **$o(g) = t$**

Se tale t non esiste, allora g ha ordine infinito: $o(g) = +\infty$

Conoscevamo già questa definizione per \mathbb{Z}_p^*

corollario In un gruppo finito G , ogni elemento x ha ordine finito tale che $o(x) \mid |G|$

DIMOSTRAZIONE

Noto che, dato $g \in G$, con G gruppo finito,

esiste sicuramente un numero intero positivo s tale che $g^s = e$

$$g, g^2, g^3, g^4, \dots$$

Dovrà succedere che per $i < j$

$$g^i = g^j$$

Moltiplico per g^{-i} :

$$e = g^{j-i} \quad \text{con } j-i > 0$$

Sia ora $\{e, x, x^2, \dots, x^{o(x)-1}\}$

Tutti gli elementi sono distinti: se fosse $x^i = x^j$ con $1 \leq i < j \leq o(x)$, allora sarebbe $x^{j-i} = e$, ma non può essere poiché $j-i < o(x)$.

Noto che $\{e, x, x^2, \dots, x^{o(x)-1}\} = \langle x \rangle$

Dunque $|\langle x \rangle| = o(x)$ che divide $|G|$ per Lagrange. \square

corollario Sia G gruppo finito e sia $g \in G$. Allora vale $|(g)| = o(g)$ e divide $|G|$.

corollario Se x è un elemento di un gruppo finito G , vale:
 $x^{|G|} = e$

DIMOSTRAZIONE

Dato che $o(x) \mid |G|$, scrivo $|G| = o(x) \cdot k$ con k intero positivo.

Allora $x^{|G|} = x^{o(x) \cdot k} = (x^{o(x)})^k = e^k = e$ \square

Consideriamo adesso $\mathbb{Z}_{10}^* = \{[1], [3], [7], [9]\}$ è un gruppo

Dunque ogni elemento elevato alla quarta dà 1

$$3^4 \equiv 1 \pmod{10}$$

\mathbb{Z}_{20}^* ha 8 elementi

Allora $7^8 \equiv 1 \pmod{20}$, $9^8 \equiv 1 \pmod{20}$

Funzione di Eulero

Def. Dato n intero positivo, definisco

la funzione $\varphi: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$, che si chiama **φ di Eulero**.

$\varphi(1) = 1$ e **$\varphi(n)$** := il numero degli interi positivi k con $1 \leq k < n$ e $\text{MCD}(k, n) = 1$.

Dunque $|\mathbb{Z}_m^*| = \varphi(m)$

Teorema

Dato m intero positivo, dato a primo con m , vale
 $a^{\varphi(m)} \equiv 1 \pmod{m}$

DIMOSTRAZIONE

Se $m=1$ è banale

Sia $m \geq 2$. Visto che a e m sono coprimi $[a]_m \in \mathbb{Z}_m^*$

Per il corollario vale $[a]_m^{\varphi(m)} = [1]_m$

che equivale a:

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad \square$$

OSS: Se $m=p$, si ritrova l'enunciato del piccolo th. di Fermat, visto che $\varphi(p) = p-1$

Teorema

φ è una funzione aritmetica moltiplicativa, ossia vale che
 se $\text{MCD}(b,c)=1$ allora $\varphi(bc) = \varphi(b) \varphi(c)$

DIMOSTRAZIONE

OSS: Dato $m > 0$, se $s \equiv t \pmod{m}$, allora s è primo con t se e solo se t è primo con m

Infatti: $s = km + r$ $t = \ell m + r$

Se un primo p divide t e m , allora divide r , allora divide m ed r , dunque s

Calcoliamo $\varphi(bc)$

Sia u un intero positivo $< bc$ e primo con bc .

Vale che

$$\begin{cases} u \equiv \lambda \pmod{b} & \text{con } 1 \leq \lambda < b \\ u \equiv \mu \pmod{c} & 1 \leq \mu < c \end{cases}$$

Per l'osservazione precedente, $\text{MCD}(\lambda, b) = 1$ e $\text{MCD}(\mu, c) = 1$

Viceversa, dati λ e μ con $1 \leq \lambda < b$, $1 \leq \mu < c$ e $\text{MCD}(\lambda, b) = 1$, $\text{MCD}(\mu, c) = 1$

per il teorema cinese, esiste unica soluzione mod (bc) di $\begin{cases} x \equiv \lambda \pmod{b} \\ x \equiv \mu \pmod{c} \end{cases}$

Chiamiamola u e osserviamo che $\text{MCD}(u, bc) = 1$

Sempre applicando l'osservazione iniziale: sia p primo che divide u e bc , allora diciamo che p divide u e b , allora $u \equiv \lambda \pmod{b}$ è assurdo \square

Teorema

Dato m intero positivo

Se $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ fattorizzazione in primi, allora

$$\varphi(m) = (p_1^{a_1} - p_1^{a_1-1}) (p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1})$$

DIMOSTRAZIONE

Per il teorema precedente

$$\varphi(m) = \varphi(p_1^{a_1}) \cdot \varphi(p_2^{a_2}) \cdot \dots \cdot \varphi(p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1-1}) \dots (p_k^{a_k} - p_k^{a_k-1})$$

Perché se p è primo, $\varphi(p^k) = p^k - p^{k-1}$ \square

esempio

$$\varphi(8) = 2^3 - 2^2 = 4 \quad |\mathbb{Z}_8^*| = 4$$

$$\varphi(5) = 5^1 - 5^0 = 4 \quad |\mathbb{Z}_5^*| = 4$$

$$\varphi(900) = \varphi(5^2) \varphi(2^2) \varphi(3^2) = 20 \cdot 2 \cdot 6 = 240 \quad \text{dunque } |\mathbb{Z}_{900}^*| = 240$$

omomorfismi di gruppi

DEF. Dati due gruppi G_1 e G_2 , una funzione $f: G_1 \rightarrow G_2$ si dice **omomorfismo** se
 $\forall g, h \in G_1 \quad f(gh) = f(g)f(h)$

esempio $T: V \rightarrow W$ sp. vett. $\Rightarrow T$ si dice applicazione lineare
 $\forall v_1, v_2 \in V \quad T(v_1 + v_2) = T(v_1) + T(v_2) \quad \forall v \in V, \forall \lambda \in K \quad T(\lambda v) = \lambda T(v)$
 T è omomorfismo di gruppi rispetto alla somma

proposizione Sia $f: G_1 \rightarrow G_2$ omomorfismo, allora vale

$$\begin{aligned} f(e_{G_1}) &= e_{G_2} \\ f(g^{-1}) &= (f(g))^{-1} \quad \forall g \in G_1 \end{aligned}$$

DIMOSTRAZIONE

$$f(e_{G_1}) = f(e_{G_1} e_{G_1}) = f(e_{G_1}) \cdot f(e_{G_1})$$

perché f omo

$$f(e_{G_1}) = f(e_{G_1}) \cdot f(e_{G_1})$$

Moltiplico entrambi i membri a sinistra $f(e_{G_1})^{-1}$ e ottengo

$$e_{G_2} = f(e_{G_1})$$

$$f(g) \cdot f(g^{-1}) = f(g \cdot g^{-1}) = f(e_{G_1}) = e_{G_2}$$

Quindi $f(g^{-1})$ è inverso di $f(g)$ ed è unico: $f(g^{-1}) = f(g)^{-1}$ \square

esempio $g: \mathbb{Z}_{20} \rightarrow \mathbb{Z}_{10}$
 $[a]_{20} \mapsto [a]_{10} \quad g \text{ è ben definita}$
 $g \text{ è omomorfismo: } g([a]_{20} + [b]_{20}) = g([a+b]_{20}) = [a+b]_{10} = [a]_{10} + [b]_{10} = g([a]_{20}) + g([b]_{20})$

DEF. Dati due gruppi G_1 e G_2 , se un omomorfismo $f: G_1 \rightarrow G_2$ è biiettivo, allora è un **isomorfismo**. Se esiste un isomorfismo fra due gruppi G_1 e G_2 , si dicono **isomorfi**:

$$G_1 \cong G_2 \quad \text{o} \quad G_1 \stackrel{\cong}{\cong} G_2 \quad \text{o} \quad G_1 \xrightarrow{\cong} G_2$$

Dato un gruppo G , un isomorfismo $f: G \rightarrow G$ si dice **automorfismo**.

$\text{Aut}(G)$ è l'insieme degli automorfismi di un gruppo G .

esempio la funzione $\exp: \mathbb{R} \rightarrow \mathbb{R}^{\times}$ definita da $\exp(a) = e^a \quad \forall a \in \mathbb{R}$
è un isomorfismo tra $(\mathbb{R}, +)$ e $(\mathbb{R}^{\times}, \cdot)$

proposizione $(\text{Aut } G, \circ)$ è un gruppo

DIMOSTRAZIONE

(1) Siano $f, g, h \in \text{Aut } G$

$$\text{Si ha } (f \circ g) \circ h = f(g \circ h) = f(g(h)) \quad \text{e} \quad f \circ (g \circ h) = f(g(h)) = f(g(h))$$

$$\text{Perciò: } (f \circ g) \circ h = f \circ (g \circ h)$$

(2) $\text{id}(g) = g$ è biettiva, quindi $\text{id} \in G$

$$f \circ \text{id} = \text{id} \circ f = f \quad \forall f$$

(3) f è biettiva, quindi esiste f^{-1} tale che $f(g) \circ f(g)^{-1} = e$

DEF. Sia G un gruppo e sia $g \in G$. Consideriamo la funzione $C_g: G \rightarrow G$ definita da
 $C_g(h) = ghg^{-1} \quad \forall h \in G$

Tale funzione si chiama **coniugio** rispetto all'elemento g

proposizione Sia G un gruppo e sia $g \in G$.
Il coniugio C_g è un automorfismo di G .

DIMOSTRAZIONE

C_g è biettiva, infatti possiede un'inversa, che è $C_{g^{-1}}$.

Inoltre C_g è un omomorfismo; infatti, $\forall h, k \in G$, si ha:

$$C_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = C_g(h)C_g(k) \quad \square$$

esempio in S_3 $g = (1,2,3)$ $x = (1,2)$ g^{-1} : basta rovesciare l'ordine
Calcolo $C_g(x) = g \cdot x \cdot g^{-1}$, ossia $(1,2,3)(1,2)(3,2,1) = (1)(2,3)$

def. Dato $f: G_1 \rightarrow G_2$ omomorfismo
Chiamo $\text{Ker } f = \{g \in G_1 \mid f(g) = e_{G_2}\}$

proposizione $\text{Ker } f < G_1$

DIMOSTRAZIONE

- $f(e_{G_1}) = e_{G_2}$ dunque $e_{G_1} \in \text{Ker } f$
- se $g_1, g_2 \in \text{Ker } f$: $f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2) = e_{G_2} \cdot e_{G_2} = e_{G_2}$ dunque $g_1 \cdot g_2 \in \text{Ker } f$
- se $g \in \text{Ker } f$, allora devo dimostrare $g^{-1} \in \text{Ker } f$
 $e_{G_2} = f(e_{G_1}) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1}) = e_{G_2} \cdot f(g^{-1}) = f(g^{-1})$
Confrontando, ottengo $f(g^{-1}) = e_{G_2}$, cioè $g^{-1} \in \text{Ker } f \quad \square$

def. Dato $f: G_1 \rightarrow G_2$ omomorfismo
Chiamo $\text{Im } f = \{f(g) \mid g \in G_1\}$

proposizione $\text{Im } f < G_2$

DIMOSTRAZIONE

- $e_{G_2} = f(e_{G_1})$ dunque $e_{G_2} \in \text{Im } f$
- $f(g_1), f(g_2) \in \text{Im } f$: $f(g_1) \cdot f(g_2) = f(g_1 \cdot g_2)$ dove $g_1 \cdot g_2 \in G_1 \Rightarrow f(g_1) \cdot f(g_2) \in \text{Im } f$
- $f(g) \in \text{Im } f$, dunque $g \in G$ e $g^{-1} \in G$ (per def. di gruppo).
Ma allora $f(g^{-1}) = f(g)^{-1} \in \text{Im } f \quad \square$

teorema Dato $f: G_1 \rightarrow G_2$ omomorfismo
Vale che f è iniettiva $\Leftrightarrow \text{Ker } f = \{e_{G_1}\}$

DIMOSTRAZIONE

\Rightarrow : Se in $\text{Ker } f$ esistesse $u \neq e_{G_1}$, si avrebbe:

$f(u) = e_{G_2} = f(e_{G_1})$, che contraddice l'iniettività.

\Leftarrow : Supponiamo per assurdo che f non sia iniettiva.

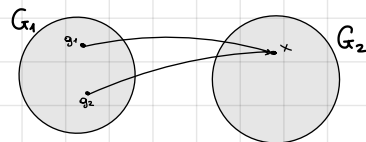
Allora $\exists g, h \in G_1, g \neq h$, tali che $f(g) = f(h)$

Moltiplicando per $f(h)^{-1}$:

$$e_{G_2} = f(h)^{-1} \cdot f(h) = f(h)^{-1} \cdot f(g) = f(h^{-1}) \cdot f(g) = f(h^{-1} \cdot g)$$

Per ciò $h^{-1}g \in \text{Ker } f = \{e_{G_1}\}$, da cui $h^{-1}g = e_{G_1}$.

Moltiplicando a sinistra per h : $g = h$, assurdo. \square



gruppi ciclici

Def. G è un gruppo ciclico se esiste g t.c. $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$

Sia G un gruppo ciclico

(1) Chi sono i generatori di G ? Quanti sono?

(2) Chi sono i sottogruppi di G ? Quanti sono?

proposizione Sia G un gruppo ciclico
Sia H un sottogruppo non banale di G .
Allora H è ciclico

DIMOSTRAZIONE

Sia $g \in G$ un generatore di G , ossia $G = \langle g \rangle$

Sia k il minimo intero positivo tale che $g^k \in H$

Sia $g^a \in H$, $a \in \mathbb{Z}$

Siano $q, r \in \mathbb{Z}$ tali che $a = qk + r$ con $0 \leq r < k$

$$g^a = g^{qk+r} = (g^k)^q \cdot g^r$$

Quindi $(g^k)^{-q} \cdot g^a = g^r \in H$

Per la minimalità di k , questo implica $r=0$

Quindi $g^a = (g^k)^q$

Dunque $H = \langle g^k \rangle$ □

corollario Sia G un gruppo ciclico infinito, e sia g un generatore di G , ossia $G = \langle g \rangle$.
Allora i sottogruppi di G sono tutti e soli i gruppi ciclici $\langle g^n \rangle$
con $n \in \mathbb{N}, n \geq 1$. In particolare i generatori di G sono g e g^{-1} ,
e $\langle g^{n_1} \rangle \subseteq \langle g^{n_2} \rangle$ se e solo se $n_2 \mid n_1$.

DIMOSTRAZIONE

$\Rightarrow H < G$: per la prop precedente, $H = \langle h \rangle$ con $h \in G$, quindi $h = g^n \Rightarrow H = \langle g^n \rangle$

$\Leftarrow \langle g^n \rangle = \{\dots, g^{2n}, g^n, e, g^n, g^{2n}, \dots\} \subseteq G$

1) $e = g^0 \in \langle g^n \rangle$

2) $g^\lambda, g^\mu \in \langle g^n \rangle \Rightarrow g^\lambda \cdot g^\mu = g^{\lambda+\mu} = g^{(\lambda+\mu)n} \in \langle g^n \rangle$

3) $g^{kn} \in \langle g^n \rangle$: $\exists g^{-kn} \in \langle g^n \rangle$: $g^{kn} \cdot g^{-kn} = g^0 = e \Rightarrow H < G$

Se $n=1$: $\langle g \rangle = \{\dots, g^2, g^1, e, g, g^2, \dots\} = \langle g^{-1} \rangle = G$

$\langle g^{n_1} \rangle \subseteq \langle g^{n_2} \rangle \Leftrightarrow g^{n_1} \in \langle g^{n_2} \rangle \Leftrightarrow \exists \ell \in \mathbb{Z} : n_1 = \ell n_2 \Leftrightarrow n_2 \mid n_1$ □

proposizione Sia G un gruppo ciclico finito di ordine $|G|=n$,
e sia g un generatore di G , ossia $G = \langle g \rangle$
Allora per ogni $k \in \mathbb{Z}$, $\langle g^k \rangle = \langle g^{\text{MCD}(k,n)} \rangle$

DIMOSTRAZIONE

Sia $d := \text{MCD}(k, n)$

Sia $k = q \cdot d$, $q \in \mathbb{Z}$

Per Bézout, esistono $x, y \in \mathbb{Z}$, tali che $d = xk + yn$

$$\langle g^k \rangle = \langle (g^d)^q \rangle \subseteq \langle g^d \rangle = \langle (g^k)^x (g^n)^y \rangle = \langle (g^k)^x e^y \rangle = \langle (g^k)^x \rangle \subseteq \langle g^k \rangle$$

$$\Rightarrow \langle g^k \rangle = \langle g^d \rangle$$
 □

corollario Sia G un gruppo ciclico finito di ordine $|G|=n \geq 2$ e sia d un divisore positivo di n . Allora:

- (1) ci sono $\varphi(d)$ elementi di G di ordine d e sono esattamente i generatori del sottogruppo $(g^{\frac{n}{d}})$.
- (2) in particolare c'è un unico sottogruppo di G di ordine d , ossia $(g^{\frac{n}{d}})$. Infine, per d_1 e d_2 , divisori positivi di n , $(g^{d_1}) \subseteq (g^{d_2})$ se e solo se $d_2 \mid d_1$.

DIMOSTRAZIONE

Per la proposizione precedente, ogni elemento g^k con $1 \leq k \leq n$ e $\text{MCD}(k, n) = d$ è generatore di $(g^{\frac{n}{d}})$.

Per $d=1$: ci sono $\varphi(n)$ elementi di G di ordine n , ossia generatori di $G = (g)$.

Questo fatto applicato al gruppo ciclico $(g^{\frac{n}{d}})$, che ha ordine d , ci dice che ci sono $\varphi(d)$ generatori di $(g^{\frac{n}{d}})$, che per la proposizione sono gli elementi di G di ordine d . Le altre osservazioni sono ora evidenti. \square

Una conseguenza immediata di questo corollario è: $\sum_{d \mid n} \varphi(d) = n$

esempio $(\mathbb{Z}_{12}, +)$

- $([0]) = \{[0]\}$
- $([1]) = \mathbb{Z}_{12}$
- $([2]) = \{[2], [4], [6], [8], [10], [0]\}$
- $([3]) = \{[3], [6], [9], [0]\}$
- $([4]) = \{[4], [8], [0]\}$
- $([5]) = \{[5], [10], [3], [8], [1], [6], [11], [4], [9], [2], [7], [0]\} = \mathbb{Z}_{12}$
- $([6]) = \{[6], [0]\}$
- $([7]) = \mathbb{Z}_{12}$
- $([8]) = \{[8], [4], [0]\}$
- $([9]) = \{[9], [6], [3], [0]\}$
- $([10]) = \{[10], [8], [6], [4], [2], [0]\}$
- $([11]) = \mathbb{Z}_{12}$

proposizione Sia G un gruppo di ordine n finito tale che per ogni divisore positivo d di n , G ha al più un sottogruppo di ordine d . Allora G è ciclico.

DIMOSTRAZIONE

d divisore positivo di n

$G_d := \{g \in G \mid g \text{ ha ordine } d\}$

Quindi $|G_d| \leq \varphi(d)$

$n = |G| = \sum_{d \mid n} |G_d| \leq \sum_{d \mid n} \varphi(d) = n$

Quindi $|G_n| = \varphi(n) \geq 1$, quindi G è ciclico \square

esempio $S_4 \supseteq \{\text{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ Gruppo di Klein

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

Non è ciclico, perché ogni elemento ha ordine al più 2, non 4

Il gruppo simmetrico

$$S_n = \{ \sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \text{ biiezione} \}$$

Notazione. • prodotto di cicli disgiunti

esempio $\sigma = (1, 5)(2, 4, 6) \in S_6$

Nota: un ciclo di lunghezza 1 è un punto fisso; un ciclo di lunghezza 2 è una trasposizione

• doppio array $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

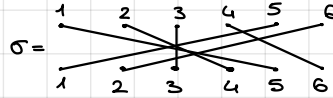
esempio $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix}$

• one-line notation $\sigma = \sigma(1) \sigma(2) \sigma(3) \dots \sigma(n)$

esempio $\sigma = 543612$

• treccia

esempio



Def. Sia $\sigma \in S_n$

Un' inversione di σ è una coppia (i, j) con $1 \leq i < j \leq n$ e $\sigma(i) > \sigma(j)$

inv(σ) = numero di inversioni di σ (che varia da 0 a $\binom{n}{2}$)

proposizione

Consideriamo S_n

(1) $\text{inv}(\text{id}) = 0$

(2) $\text{inv}(\sigma) = \text{inv}(\sigma^{-1})$

(3) $1 \leq i < j \leq n \quad \text{inv}((i, j)) = 2(j - i - 1) + 1$

(4) $\sigma, \tau \in S_n \quad (-1)^{\text{inv}(\sigma) + \text{inv}(\tau)} = (-1)^{\text{inv}(\sigma \circ \tau)}$

DIMOSTRAZIONE

La (1) e la (3) si calcolano direttamente, ad esempio con le trecce.

Per la (2) osserviamo che la treccia di σ^{-1} si ottiene da quella di σ riflettendo la figura rispetto a una retta orizzontale, quindi le inversioni non cambiano.

Per la (4), osserviamo che la composizione di trecce si ottiene mettendo le trecce una dopo l'altra.

Poi osserviamo che (i, j) con $1 \leq i < j \leq n$ è un'inversione di $\tau \circ \sigma$ se e solo se i fili che partono da i e da j si intersecano solo nella prima metà del diagramma o solo nella seconda.

Questo dimostra la proprietà (4). □

Oss Ogni permutazione si può scrivere in infiniti modi come prodotto di trasposizioni

Sia $\sigma = (a_1, a_2, \dots, a_{k_1})(b_1, b_2, \dots, b_{k_2}) \dots$

$(a_1, a_2, \dots, a_{k_1}) = (a_1, a_2)(a_2, a_3) \dots (a_{k_1-1}, a_{k_1}) = (a_1, a_{k_1})(a_1, a_{k_1-1}) \dots (a_1, a_2)$

proposizione

Sia $\sigma \in S_n$

$\sigma = \tau_1 \tau_2 \dots \tau_r = \tau'_1 \tau'_2 \dots \tau'_s$ con τ_i e τ'_j trasposizioni per ogni i e j

Allora $r \equiv s \pmod{2}$

DIMOSTRAZIONE

$(-1)^{\text{inv}(\sigma)} = (-1)^{\text{inv}(\tau_1 \tau_2 \dots \tau_r)} = (-1)^{\text{inv}(\tau'_1 \tau'_2 \dots \tau'_s)}$

Quindi $(-1)^{\text{inv}(\sigma)} = (-1)^{\text{inv}(\tau_1 \tau_2 \dots \tau_r)} = (-1)^{\text{inv}(\tau_1) + \text{inv}(\tau_2) + \dots + \text{inv}(\tau_r)} = (-1)^r$

Analogamente $(-1)^{\text{inv}(\sigma)} = (-1)^s$

Da cui $(-1)^r = (-1)^s$, cioè hanno la stessa parità □

proposizione Se $\sigma \in S_n$ è dato in cicli disgiunti
 come $\sigma = p_1 p_2 \dots p_r$ con p_i di lunghezza k_i
 Allora $(-1)^{\text{inv}(\sigma)} = (-1)^{\sum_{i=1}^r (k_i - 1)}$

DIMOSTRAZIONE

Per la proposizione, abbiamo: $(-1)^{\text{inv}(\sigma)} = (-1)^{\text{inv}(p_1 p_2 \dots p_r)} = (-1)^{\text{inv}(p_1) + \text{inv}(p_2) + \dots + \text{inv}(p_r)}$

Bisogna quindi mostrare che $(-1)^{\text{inv}(p_i)} = (-1)^{k_i - 1}$

Ma p_i si scrive come prodotto di $k_i - 1$ trasposizioni, da cui segue la tesi. \square

def. Il segno di una permutazione $\sigma \in S_n$ è

$$\text{sgn}(\sigma) := (-1)^{\text{inv}(\sigma)}$$

Una permutazione $\sigma \in S_n$ è detta **pari** se $\text{sgn}(\sigma) = 1$, mentre è detta **dispari** se $\text{sgn}(\sigma) = -1$

esempio S_3 : $\text{id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)$
 $\text{sgn}(\sigma)$: $1, -1, -1, -1, 1, 1$

OSS $C_2 = \{+1, -1\}$ con il prodotto è un gruppo ciclico di ordine 2

$\text{sgn} : S_n \rightarrow C_2$ è un **omomorfismo**

Infatti: $\text{sgn}(\sigma \circ \tau) = \text{sgn}(\sigma) \text{sgn}(\tau)$

$$(-1)^{\text{inv}(\sigma \circ \tau)} = (-1)^{\text{inv}(\sigma)} \cdot (-1)^{\text{inv}(\tau)} = (-1)^{\text{inv}(\sigma) + \text{inv}(\tau)}$$

Si definisce $A_n := \ker \text{sgn}$ (gruppo alterno)

Risulta $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$

(infatti esiste la biezione $A_n \leftrightarrow (1,2)A_n, \dots$)

Data una permutazione $\sigma \in S_n$, $\sigma = (a_1, a_2, \dots, a_{k_1})(b_1, b_2, \dots, b_{k_2}) \dots$

il suo ordine è $o(\sigma) = \text{lcm}(k_1, k_2, \dots)$

Siano $\sigma, \tau \in S_n$, e consideriamo la scomposizione in cicli disgiunti di σ :

$$\sigma = (a_1, a_2, \dots, a_{k_1})(b_1, b_2, \dots, b_{k_2}) \dots$$

Allora vale:

$$\tau \sigma \tau^{-1} = (\tau(a_1), \tau(a_2), \dots, \tau(a_{k_1}))(\tau(b_1), \tau(b_2), \dots, \tau(b_{k_2})) \dots$$

Questo definisce la classe di coniugio di $\sigma \in S_n$:

$$C(\sigma) = \{ \tau \sigma \tau^{-1} \mid \tau \in S_n \}$$

che contiene tutte e sole le permutazioni di S_n i cui cicli hanno la stessa lunghezza di σ .

Quanti elementi ci sono in $C(\sigma)$?

Sia $\lambda(\sigma)$ la tupla $(\lambda_1, \lambda_2, \dots, \lambda_k)$ delle lunghezze dei cicli di σ , con $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k > 0$.

Sia $\alpha_i = \alpha_i(\sigma)$ il numero dei cicli di lunghezza i . $\alpha_i = |\{j \mid \lambda_j = i\}|$

Dunque: $C(\sigma) = \{ \tau \in S_n \mid \lambda(\tau) = \lambda(\sigma) \}$

proposizione $|C(\sigma)| = \frac{n!}{1^{\alpha_1} \cdot 2^{\alpha_2} \cdot \dots \cdot n^{\alpha_n} \cdot \alpha_1! \cdot \alpha_2! \cdot \dots \cdot \alpha_n!}$

sottogruppi normali e quozienti

Def. Dato G gruppo e $H < G$

Diremo che H è **sottogruppo normale** di G se

$$\forall g \in G, \forall h \in H \text{ vale } C_g(H) \subseteq H \quad (\text{o } gHg^{-1} \subseteq H \text{ o } ghg^{-1} \in H)$$

e si scrive $H \triangleleft G$

Oss Dato che $gHg^{-1} \subseteq H$ deve valere $\forall g \in G$

Osservo che allora

$$gHg^{-1} \subseteq H \text{ e } g^{-1}Hg \subseteq H, \text{ da cui } g g^{-1} H g g^{-1} \subseteq g H g^{-1} \text{ ossia } H \subseteq g H g^{-1}$$

Dunque $H \triangleleft G$ se e solo se $gHg^{-1} = H \quad \forall g \in G$

Oss Se G è abeliano, ogni sottogruppo H è normale

proposizione Dati due gruppi G_1, G_2 e un omomorfismo $f: G_1 \rightarrow G_2$, vale che $\text{Ker } f$ è un sottogruppo normale di G_1 ($\text{Ker } f \triangleleft G_1$).

DIMOSTRAZIONE

Siano $h \in \text{Ker } f$ e $g \in G_1$:

$$f(ghg^{-1}) = f(g) f(h) f(g^{-1}) = f(g) e_{G_2} f(g^{-1}) = e_{G_2} \Rightarrow C_g(\text{Ker } f) \subseteq \text{Ker } f$$

Questo vale $\forall g \in G_1$. Prendendo g^{-1} .

$$C_{g^{-1}}(\text{Ker } f) \subseteq \text{Ker } f$$

Applicando C_g :

$$C_g(C_{g^{-1}}(\text{Ker } f)) \subseteq C_g(\text{Ker } f) \Rightarrow \text{Ker } f \subseteq C_g(\text{Ker } f) \Rightarrow \text{Ker } f = C_g(\text{Ker } f) \Rightarrow \text{Ker } f \triangleleft G_1 \quad \square$$

Se $\text{Ker } f \triangleleft G_1$, allora è possibile definire un prodotto su G/H affinché sia un gruppo.

Dati due sottoinsiemi A, B , il loro prodotto "naturale" è:

$$AB = \{ab \mid a \in A, b \in B\}$$

Consideriamo due classi laterali g_1H e g_2H

$$g_1H g_2H = g_1 g_2 H$$

Dobbiamo verificare se questa def "naturale" è ben data, ossia consideriamo

$$g_1'H = g_1H \text{ e } g_2'H = g_2H \text{ vorremmo che } \underset{g_1'g_2'H}{g_1'H \cdot g_2'H} = \underset{g_1g_2H}{g_1H \cdot g_2H}$$

Notiamo che $g_1' \in g_1H$, lo scrivo come $g_1' = g_1h_1$

Analogamente $g_2' = g_2h_2$

$$\text{Dunque } g_1'g_2'H = g_1h_1g_2h_2H = g_1g_2g_2^{-1}h_1g_2h_2H$$

Vogliamo verificare se è uguale a g_1g_2H

Cio' accade se e solo se $(g_2^{-1}h_1g_2)h_2 \in H$

$$\text{ossia } (g_2^{-1}h_1g_2)h_2 = h \in H$$

$$\text{ossia } (g_2^{-1}h_1g_2) = hh_2^{-1} \in H$$

In conclusione, il prodotto indicato sopra su G/H è ben definito se e solo se

$$\forall g \in G, \forall h \in H \text{ vale } ghg^{-1} \in H, \text{ ossia } H \triangleleft G$$

Def. Dato un gruppo G e un suo sottogruppo normale H , chiameremo

G/H , munito del prodotto definito sopra, il gruppo quoziente di G su H .

esempio

$$G = \mathbb{Z} \quad H = (m) \text{ per } m \text{ intero}$$

$$\text{se } m=1 \quad \mathbb{Z}/(1) \cong \mathbb{Z}/\mathbb{Z} \text{ è un gruppo con un solo elemento, } \{0\}$$

$$\text{se } m=0 \quad \mathbb{Z}/(0) \cong \mathbb{Z}$$

esempio

$$G = S_4$$

$$K = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

$$\text{Noto che } K < S_4, \text{ infatti: } a^2 = b^2 = c^2 = e, \quad ab = c, \quad ac = b, \quad cb = a$$

$$\text{Noto anche che } ba = c$$

$$K \text{ è gruppo abeliano ed è } K \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = \{([a]_2, [b]_2)\} \quad (\text{da verificare})$$

$$e \rightarrow ([0], [0])$$

$$a \rightarrow ([1], [0])$$

$$b \rightarrow ([0], [1])$$

$$c \rightarrow ([1], [1])$$

K si chiama sottogruppo di Klein

$$\text{oss} \quad \text{Per quanto visto alle scorse lezioni} \quad g(\cdot, \cdot)(\cdot, \cdot)g^{-1} = (*, *) \quad (*, *)$$

$$\text{Dunque } gKg^{-1} = K \text{ ossia } K \triangleleft S_4$$

Quindi possiamo dare una struttura di gruppo a S_4/K , che è un gruppo con 6 elementi

$$\alpha = (1,2,3)K \quad \alpha^2 = ((1,2,3)K)^2 = (1,2,3)^2 K = (3,2,1)K \quad \alpha^3 = (1,2,3)^3 K = eK$$

$$\beta = (1,2)K \quad \beta^2 = (1,2)^2 K = eK$$

$$\gamma = (1,2,3,4)K \quad \gamma^2 = (1,2,3,4)^2 K = (1,3)(2,4)K = eK$$

MORALE: nessun elemento in S_4/K ha ordine 6

$$\text{Di sicuro dunque } S_4/K \not\cong \mathbb{Z}_6$$

Primo teorema di omomorfismo

Dati G_1 e G_2 gruppi, e un omomorfismo $f: G_1 \rightarrow G_2$

Vale che

$$G_1/\text{Ker } f \cong \text{Im } f$$

DIMOSTRAZIONE

$$\text{Costruisco } \bar{f}: G_1/\text{Ker } f \rightarrow \text{Im } f, \quad g_1 \text{Ker } f \mapsto f(g_1), \text{ ossia } \bar{f}(g_1 \text{Ker } f) = f(g_1)$$

\bar{f} è ben definita; infatti un altro rappresentante di $g_1 \text{Ker } f$ sarebbe $g_1 k \text{Ker } f$, con $k \in \text{Ker } f$.

$$\text{Allora } \bar{f}(g_1 k \text{Ker } f) = f(g_1 k) = f(g_1) f(k) = f(g_1)$$

\bar{f} è un omomorfismo, infatti:

$$\bar{f}(g_1 \text{Ker } f \cdot g_2 \text{Ker } f) = \bar{f}(g_1 g_2 \text{Ker } f) = f(g_1 g_2) = f(g_1) f(g_2)$$

$$\text{Inoltre: } \bar{f}(g_1 \text{Ker } f) \bar{f}(g_2 \text{Ker } f) = f(g_1) f(g_2) \Rightarrow \bar{f} \text{ omomorfismo}$$

Bisogna dimostrare che \bar{f} è biiettivo

$$\text{Per l'injectività: } \bar{f}(g \text{Ker } f) = f(g) = e_{G_2} \Rightarrow g \in \text{Ker } f \text{ e quindi } g \text{Ker } f = e \text{Ker } f$$

$$\Rightarrow \text{Ker } \bar{f} = \{e \text{Ker } f\} \Rightarrow \bar{f} \text{ injectiva}$$

$$\text{Per la surgettività: } \forall y \in \text{Im } f \quad \exists g \in G_1 : f(g) = y$$

$$\bar{f}(g \text{Ker } f) = f(g) = y \Rightarrow \bar{f} \text{ surgettiva.} \quad \square$$

corollario Dati due gruppi G_1, G_2 e un omomorfismo surgettivo $f: G_1 \rightarrow G_2$, vale che:

$$G_1/\text{Ker } f \cong G_2$$

corollario Dati due gruppi G_1, G_2 e un omomorfismo injectivo $f: G_1 \rightarrow G_2$, vale che:

$$G_1 \cong \text{Im } f$$

corollario

Sia $H \triangleleft G$

Considero la funzione

$$\pi: G \longrightarrow G/H$$

definita così: $g \mapsto gH$

Allora π è omomorfismo (proiezione al quoziente G/H)
e $\text{Ker } \pi = H$

Def. Sia G un gruppo e sia $X \subseteq G$ un sottoinsieme di G . Definiamo

$$\langle X \rangle := \{ y_1 y_2 \dots y_k \mid k \in \mathbb{N}, y_i \in X \cup X^{-1} \forall i \} \subseteq G$$

$$\langle \emptyset \rangle = \{e\}$$

esempio $\langle \{g\} \rangle = \langle g \rangle$

$$\langle G \rangle = \langle G \rangle$$

Oss $\langle X \rangle$ è un sottogruppo di G

$\langle X \rangle$ è il sottogruppo generato da X

Se $G = \langle X \rangle$, si dice che X genera G

Oss Siano G un gruppo e $\{H_i\}_{i \in I}$ una famiglia di sottogruppi di G

Allora $\bigcap_{i \in I} H_i$ è un sottogruppo di G .

Def. Siano G_1 e G_2 gruppi.

Il prodotto cartesiano (diretto) di G_1 e G_2 è il gruppo $G_1 \times G_2$ con l'operazione:

$$(g_1, g_2) \cdot (\tilde{g}_1, \tilde{g}_2) := (g_1 \tilde{g}_1, g_2 \tilde{g}_2)$$

gruppo diedrale

$D_n = \{ \text{simmetrie del } n\text{-agono regolare} \}$

p : rotazione di $\frac{2\pi}{n}$ in senso orario intorno all'origine

r : riflessione intorno all'asse $x=0$

$$D_n = \{ \text{id}, p, p^2, \dots, p^{n-1}, r, rp, rp^2, \dots, rp^{n-1} \}$$

$$\text{dove } p^{-1}r = rp \quad rpr = p^{-1}$$

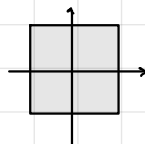
$$|D_n| = 2n \text{ elementi}$$

esempio

$$n=4$$

$$p_1 = (1, 2, 3, 4) \in S_4$$

$$r_1 = (1, 4)(2, 3) \in S_4$$



esercizio $\langle \{p, r\} \rangle \subseteq S_4$ è isomorfo a D_4

esercizio Mostrare che S_3 è isomorfo a D_3

TEORIA DEGLI ANELLI

Def. Un anello con unità R è un insieme munito di due operazioni, $+$ e \cdot , tali che:

- $(R, +)$ è un gruppo commutativo
- $\forall a, b, c \in R \quad (ab)c = a(bc)$
- esiste un elemento $1 \in R$ tale che $\forall a \in R \quad a \cdot 1 = 1 \cdot a = a$
- $\forall a, b, c \in R$ vale $(a+b) \cdot c = a \cdot c + b \cdot c$
 $a \cdot (b+c) = a \cdot b + a \cdot c$

Def. Un anello in cui la moltiplicazione è commutativa si chiama anello commutativo.

Def. Sia R un anello commutativo
Diremo che $a \in R$ è un divisore di 0 se
 $\exists b \in R, b \neq 0$, tale che $ab = 0$

Def. Un anello commutativo R in cui $0 \neq 1$ e in cui l'unico divisore di 0 è 0, si chiama dominio o dominio di integrità.

NOTA: tra gli anelli con unità, ammettiamo l'anello banale $\{0\}$ (stupid ring)

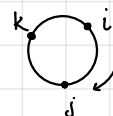
Def. Un elemento u di un anello R si dice invertibile se esiste $v \in R$ tale che
 $uv = vu = 1$
Denoteremo con R^* l'insieme degli elementi invertibili di R

esempio $\mathbb{Z}_{20}^*, \mathbb{Z}^* = \{1, -1\}$
esercizio In generale (R^*, \cdot) è un gruppo.

Def. Due elementi a, b di un anello commutativo R si dicono associati se
esiste $p \in R^*$ tale che $a = bp$

Def. Un anello R in cui $0 \neq 1$ e in cui ogni elemento $\neq 0$ ammette un inverso si chiama corpo (division ring)
Un corpo commutativo si chiama campo.

esempio $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$
è spazio vettoriale su \mathbb{R} di dim 4 con base $1, i, j, k$
La moltiplicazione si basa sulle seguenti regole:
 $i^2 = j^2 = k^2 = -1$
 $ij = k \quad jk = i \quad ki = j$ da cui $ji = -k \quad kj = -i \quad ik = -j$



In \mathbb{C} , l'inverso di $a + ib$ è $\frac{a - ib}{a^2 + b^2}$

In \mathbb{H} , l'inverso di $a + ib + jc + kd$ è $\frac{a - ib - jc - kd}{a^2 + b^2 + c^2 + d^2}$
Dentro \mathbb{H} , vive felice

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ gruppo con la moltiplicazione

esercizio Calcolare $\mathbb{Z}(Q_8)$ e trovare tutti i sottogruppi

Teorema Se p è un numero primo, \mathbb{Z}_p è un campo

DIMOSTRAZIONE

Se prendiamo una classe $[a]_p \neq [0]_p$ in \mathbb{Z}_p , vale $\text{MCD}(a, p) = 1$

Allora la soluzione $ax \equiv 1 \pmod{p}$ ha soluzione: $\exists b \in \mathbb{Z}$ t.c. $ab \equiv 1 \pmod{p}$

Quindi in \mathbb{Z}_p vale $[a]_p [b]_p = [ab]_p = [1]_p$

Dunque $[a]_p$ è invertibile in \mathbb{Z}_p e $[b]_p$ è il suo inverso \square

Lemma Sia A un anello.

Allora $\forall a, b \in A$ vale:

- 1) $a \cdot 0 = 0 \cdot a = 0$
- 2) l'opposto di a è unico e vale $-(-a) = a$
- 3) $a(-b) = (-a)b = -(ab)$
In particolare $(-1)a = a(-1) = -a$
- 4) $(-a)(-b) = ab$
In particolare $(-1)(-1) = 1$

DIMOSTRAZIONE

1) $a \cdot 0 = a \cdot (0+0) \stackrel{\text{distr.}}{=} a \cdot 0 + a \cdot 0$

Dunque $a \cdot 0 = a \cdot 0 + a \cdot 0$

Sommando l'opposto di $a \cdot 0$: $0 = a \cdot 0$

2) già vista per i gruppi

3) Dimostro che $a(-b) = -(a \cdot b)$

Basta dimostrare $a \cdot b + a(-b) = 0$, perché l'opposto è unico.

Uso la distributiva $a(b + (-b)) = a \cdot 0 \stackrel{1)}{=} 0$

4) $(-a)(-b) \stackrel{3)}{=} -(a \cdot (-b)) \stackrel{3)}{=} -(-(a \cdot b)) \stackrel{2)}{=} ab$ \square

Approfondiamo il concetto di dominio

esempio \mathbb{Z}_{10} non è un dominio perché $[5]_{10} [2]_{10} = [0]_{10}$

$\mathbb{R}[x]$ è un dominio

Un campo \mathbb{K} è un dominio.

Infatti se fosse $a \neq 0, b \neq 0$ e $ab = 0$

avrei $a^{-1}ab = a^{-1}0 \rightarrow b = 0$ ASSURDO

Proposizione Se D è un dominio, vale la "legge di cancellazione", ossia se $a \in D$ e $a \neq 0$ allora $ab = ac \Rightarrow b = c$

DIMOSTRAZIONE

$ab = ac$ equivale $ab - ac = 0 \rightarrow a(b - c) = 0$

Dato che $a \neq 0$ e D è dominio, deve essere $b - c = 0$, ossia $b = c$ \square

esempio In \mathbb{Z}_{12} vale $[3][4] = [3][8]$ ma $[4] \neq [8]$

Infatti \mathbb{Z}_{12} non è un dominio

esempio \mathbb{Z} è dominio

$\mathbb{Z}[x]$ è dominio

Def. Un sottoanello T di un anello R è un sottoinsieme tale che:

- $1 \in T$
- T è sottogruppo rispetto alla $+$
- $\forall a, b \in T$ vale $ab \in T$

Def. Sia R un anello.

Un sottoinsieme S è un sottoanello se è lui stesso un anello con le operazioni ereditate da R .

esempio $\mathbb{R}[x, y] \supseteq \mathbb{R}[x]$

Omomorfismi di anelli

Def. Dati R ed S anelli.

Una funzione $\phi: R \rightarrow S$ si dice omomorfismo se

- $\forall a, b \in R \quad \phi(a+b) = \phi(a) + \phi(b)$
- $\forall a, b \in R \quad \phi(ab) = \phi(a)\phi(b)$
- $\phi(1_R) = 1_S$

Oss La funzione $f: \mathbb{Z}_{12} \rightarrow \{0\}$

tale che $f([a]) = 0 \quad \forall [a] \in \mathbb{Z}_{12}$ è un omomorfismo di anelli, dato che $\{0\}$ è l'anello banale in cui $0=1$.

Def. Dato $\phi: R \rightarrow S$ omomorfismo

Chiamiamo $\text{Ker } \phi$, nucleo di ϕ , l'insieme

$$\text{Ker } \phi = \{r \in R \mid \phi(r) = 0_S\}$$

esempio $f: \mathbb{Z} \rightarrow \mathbb{Z}_2$

$$m \mapsto [m]_2$$

si verifica subito che f è un omomorfismo di anelli

$$\text{Ker } f = \{\text{i numeri pari}\}$$

Già da questo esempio si vede che $\text{Ker } f$ non è un sottoanello

In effetti il nucleo di un omomorfismo di anelli non contiene 1 ,

a meno che non si sia nella seguente situazione

$g: R \rightarrow \{0\}$ allora $\text{Ker } g = R$ e solo in questo caso il Ker è un anello.

Oss Noto che $f: R \rightarrow S$ omomorfismo di anelli

$\text{Ker } f$ ha la seguente proprietà:

sia $n \in \text{Ker } f$, sia $r \in R$

allora $nr \in \text{Ker } f$ e anche $rn \in \text{Ker } f$

Infatti $f(nr) = f(n)f(r) = f(n) \cdot 0 = 0$ e analogamente $f(rn) = 0$

Def. Un ideale I di un anello R è un sottogruppo additivo tale che

$\forall r \in R, \forall h \in I$ vale $rh \in I$ e anche $hr \in I$

Se $I \neq R$, si dice che I è un ideale proprio

esempio $\{0\} \subset R$ è un ideale

esempio $\{\text{numeri pari}\} \subset \mathbb{Z}$ è un ideale

esempio $\text{Ker } f \subset R$ è un ideale, con f omomorfismo

esercizio Se I e J ideali, allora $I+J$ ideale

Anche $I \cap J$ è ideale

DEF.

Dati I, J ideali

Definisco $IJ = \{ \text{tutti gli elementi che si possono scrivere come somma di un numero finito di elementi } ab \text{ con } a \in I, b \in J \}$

esercizio IJ è ideale

$$r(a_1b_1 + \dots + a_sb_s) = ra_1b_1 + \dots + ra_sb_s = \underbrace{(ra_1)}_I b_1 + \dots + \underbrace{(ra_s)}_I b_s \in IJ$$

esempio Sia $R = \mathbb{Z}$, $I = (6)$, $J = (4)$

$$I \cap J = (12)$$

$$IJ = \{a_1b_1 + \dots + a_sb_s \mid s \geq 1, a_i \text{ è multiplo di } 6, b_j \text{ è multiplo di } 4\} = (24)$$

OSS Vale sempre $IJ \subset I \cap J$ ma non è detto che siano uguali

NOTAZIONE Sia A anello commutativo

Indico con (a) l'insieme $(a) = \{a \cdot r \mid r \in A\}$ che è l'ideale generato da a

Dati $a, b \in A$

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

In \mathbb{Z} le notazioni coincidono

$$\mathbb{Z} \text{ anello: } (6) = \{6m \mid m \in \mathbb{Z}\} \text{ coincide con } (\mathbb{Z}, +) \text{ gruppo: } (6)$$

esempio $\mathbb{Z} \times \mathbb{Z}$ è anello

$$(a, b)(a', b') := (aa', bb')$$

$$0 \text{ è } (0, 0) \quad 1 \text{ è } (1, 1)$$

Notiamo che $(0, 1)(1, 0) = (0, 0) \Rightarrow \mathbb{Z} \times \mathbb{Z}$ non è un dominio

esempio $A = \mathbb{R}[x]$ $a = x^2 + x + 1$

$(x^2 + x + 1)$ è l'ideale generato da $x^2 + x + 1$

$$(x^2 + x + 1) = \{(x^2 + x + 1)f(x) \mid f(x) \in \mathbb{R}[x]\}$$

Anelli quoziente

Sia A anello e I ideale

Considero l'insieme A/I delle classi di resto

$$A/I = \{a + I \mid a \in A\}$$

Come sappiamo $a_1 + I = a_2 + I$ se e solo se $a_1 - a_2 \in I$ se e solo se $a_1 \in a_2 + I$ / $a_2 \in a_1 + I$

Ho in A/I la somma

$$(b_1 + I) + (b_2 + I) := (b_1 + b_2) + I$$

In realtà ho anche un prodotto

$$(b_1 + I)(b_2 + I) := (b_1 b_2) + I$$

Va verificato che è ben definito

$$\text{Siano } b'_1 + I = b_1 + I \quad b'_2 + I = b_2 + I$$

$$\text{allora } b'_1 = b_1 + p_1 \text{ con } p_1 \in I \text{ e } b'_2 = b_2 + p_2 \text{ con } p_2 \in I$$

Devo verificare che $(b'_1 + I)(b'_2 + I) = b'_1 b'_2 + I$ è uguale a $b_1 b_2 + I$

$$\text{Scrivo } b'_1 b'_2 = (b_1 + p_1)(b_2 + p_2) = b_1 b_2 + \underbrace{b_1 p_2 + p_1 b_2 + p_1 p_2}_I$$

$$\text{Dunque } b'_1 b'_2 + I = b_1 b_2 + I$$

Con queste operazioni, si verifica che A/I è un anello con unità

Primo teorema di omomorfismo

Siano R, S due anelli e

sia $\phi: R \rightarrow S$ un omomorfismo di anelli. Allora:

$$R / \text{Ker } \phi \cong \text{Im } \phi$$

Polinomi

Sia K un campo. Consideriamo l'insieme $K[x]$ dei polinomi nella variabile x .

Un polinomio è una espressione del tipo

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \text{con } a_j \in K$$

Se $a_n \neq 0$, dico che $\deg(f(x)) = n$. $\deg(0) = -\infty$ (oppure non definito)

esempio

$$\mathbb{R}[x]$$

$$\deg(7x+2) = 1$$

$$\deg(9) = 0$$

$\deg(0)$ talvolta si preferisce non attribuire un grado

DIVISIONE EUCLIDEA

Sia $f(x) \in K[x]$, sia $g(x) \in K[x]$ con $g(x) \neq 0$

allora $\exists q(x), r(x)$ tali che

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

$$\text{e } r(x) < \deg(r(x)) < \deg(g(x))$$

esercizio

Dimostrarlo per induzione

esempio

$$\begin{array}{r|l} x^4 - x^3 + 6x^2 + x - 7 & x^3 + 6x + 7 \\ \ominus x^4 & x - 1 \\ \hline & -x^3 - 6x - 7 \\ \ominus & -x^3 - 6x - 7 \\ \hline & 0 \end{array}$$

$$x^4 - x^3 + 6x^2 + x - 7 = (x^3 + 6x + 7)(x - 1) + 0$$

$$\begin{array}{r|l} x^3 + 6x + 7 & x^2 + 3x + 2 \\ x^3 + 3x^2 + 2x & x - 3 \\ \hline & -3x^2 + 4x + 7 \\ & -3x^2 - 9x - 6 \\ \hline & 13x + 13 \end{array}$$
$$x^3 + 6x + 7 = (x^2 + 3x + 2)(x - 3) + (13x + 13)$$

$q(x) \qquad r(x)$

Abbiamo anche in $K[x]$ un concetto di MCD

Def.

Dati $f(x), g(x) \in K[x]$, non entrambi 0,

un MCD di $f(x)$ e $g(x)$ è un polinomio $d(x) \in K[x]$ tale che

• $d(x) \mid f(x)$ e $d(x) \mid g(x)$

• se $c(x) \in K[x]$ soddisfa $c(x) \mid f(x)$ e $c(x) \mid g(x)$ allora $\deg c(x) \leq \deg d(x)$

Il MCD è unico se si considera il polinomio monico

esempio

$$f(x) = (x-1)(x+1) \quad g(x) = (x-1) \quad \text{in } \mathbb{Q}[x]$$

Qui $(x-1)$ è un MCD, ma anche $117(x-1)$ è MCD

esempio $x^3 + 6x + 7 = (x^2 + 3x + 2)(x - 3) + (13x + 13)$
 $(x^2 + 3x + 2) = (13x + 13) q_1(x) + r_1(x) = (13x + 13) \left(\frac{1}{13}x + \frac{2}{13}\right) + 0$

Vale, come in \mathbb{Z} , che si possono trovare i MCD con l'algoritmo di Euclide

$$f(x) = g(x) q_0(x) + r_0(x)$$

$$g(x) = r_0(x) q_1(x) + r_1(x)$$

$$r_0(x) = r_1(x) q_2(x) + r_2(x)$$

...

$$r_{n-2}(x) = r_{n-1}(x) q_n(x) + r_n(x)$$

$$r_{n-1}(x) = r_n(x) q_{n+1}(x) + 0$$

si conclude che $r_n(x)$ è un MCD

Ripetendo i passaggi di Bezout visti per \mathbb{Z} , riesco a scrivere

$$r(x) = \lambda(x) f(x) + \mu(x) g(x) \quad \text{per certi } \lambda(x), \mu(x) \in K[x]$$

Da qui si osserva facilmente che:

1) ogni altro divisore di $f(x)$ e $g(x)$ divide $r_n(x)$

2) dunque se $d(x)$ è un altro MCD, vale

$$r_n(x) = k d(x) \quad \text{dove } k \in K^*$$

Perciò anche per i polinomi vale il teorema di Bézout:

teorema di Bézout Siano $a(x), b(x) \in K[x]$. Allora $\exists \lambda(x), \mu(x) \in K[x]$ t.c.
 $\lambda(x) a(x) + \mu(x) b(x) = \text{MCD}(a(x), b(x))$

Alcune proprietà di \mathbb{Z} si ritrovano dunque in $K[x]$

proposizione Se in $K[x]$ $a(x) \mid b(x) c(x)$ ma un $\text{MCD}(a(x), b(x)) = 1$
 allora $a(x) \mid c(x)$

DIMOSTRAZIONE

Per Bézout $\lambda(x) a(x) + \mu(x) b(x) = 1$

$$\underbrace{\lambda(x) a(x) c(x)}_{a(x) \mid} + \underbrace{\mu(x) b(x) c(x)}_{a(x) \mid} = c(x)$$

Quindi $a(x) \mid c(x)$

□

RADICI DI UN POLINOMIO

Def. Sia K campo, $f(x) \in K[x]$

$r \in K$ è una **radice** di $f(x)$ se $f(r) = 0$

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad a_i \in K$$

$$f(r) = a_n r^n + a_{n-1} r^{n-1} + \dots + a_1 r + a_0$$

Lemma Sia K campo, $f(x) \in K[x]$

Sia $r \in K$ una radice di $f(x)$.

Allora $(x-r)$ divide $f(x)$ in $K[x]$.

Equivalentemente, esiste $g(x) \in K[x]$ tale che $f(x) = (x-r) g(x)$
 con $\deg g(x) = \deg(f(x)) - 1$

DIMOSTRAZIONE

$$f(x) = g(x) (x-r) + h(x) \quad \text{con } \deg h(x) < \deg(x-r) = 1$$

$$f(r) = g(r) (r-r) + h(r) = h(r) = 0$$

□

□

Teorema Fondamentale dell'algebra (Gauss)

Ogni polinomio $f(x) \in \mathbb{C}[x]$ di grado positivo ha una radice $r \in \mathbb{C}$

$$f(x) \in \mathbb{C}[x], \quad f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \quad a_i \in \mathbb{C}, \quad a_n \neq 0$$

Sia $z \in \mathbb{C}$ una radice di $f(x)$

$$0 = f(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$$

$$0 = \overline{a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0} = \overline{a_n} \bar{z}^n + \overline{a_{n-1}} \bar{z}^{n-1} + \dots + \overline{a_1} \bar{z} + \overline{a_0} = \bar{f}(\bar{z})$$

$$\bar{f}(x) = \overline{a_n} x^n + \overline{a_{n-1}} x^{n-1} + \dots + \overline{a_1} x + \overline{a_0}$$

Sia ora $f(x) \in \mathbb{R}[x]$ di grado positivo

Se $z \in \mathbb{C}$ una radice di $f(x)$

allora anche \bar{z} è una radice di $f(x)$

Supponiamo che $z \notin \mathbb{R}$, $z = \alpha + \beta i$ con $\beta \neq 0$

$$f(x) = (x-z)(x-\bar{z})q(x)$$

$$\text{OSS } (x-z)(x-\bar{z}) = x^2 - (z+\bar{z})x + z\bar{z} = x^2 - 2\operatorname{Re}(z)x + |z|^2 \in \mathbb{R}[x]$$

$\exists q(x), r(x) \in \mathbb{R}[x]$ tali che

$$f(x) = q(x)(x-z)(x-\bar{z}) + r(x)$$

$$\text{con } \deg r(x) < \deg (x-z)(x-\bar{z}) = 2$$

Se $\deg(r(x)) = 1$, allora $r(x) = ax + b$. Valutando in z_0 si ha:

$$0 = f(z_0) = q(z_0)(z_0 - z)(z_0 - \bar{z}) + r(z_0) = r(z_0) = az_0 + b \quad \text{ASSURDO perché } \operatorname{Im}(az_0 + b) = a \operatorname{Im}(z_0) \neq 0$$

Quindi $\deg(r(x)) \leq 0$, ossia $r(x)$ è costante.

$$0 = f(z) = q(z)(z-z)(z-\bar{z}) + r(z) \quad \Rightarrow \quad r(x) = 0$$

corollario Ogni polinomio $f(x) \in \mathbb{R}[x]$ di grado positivo fattorizza in un prodotto di fattori di grado minore o uguale a 2.

QUOZIENTE $\mathbb{K}[x]/(f(x))$

$$\cdot f(x) = 0 \quad (0) = 0 \quad \mathbb{K}[x]/(0) = \mathbb{K}[x]$$

$$\cdot f(x) = a \in \mathbb{K}, a \neq 0, \quad (a) = \mathbb{K}[x] \quad \mathbb{K}[x]/(a) = \{0\}$$

$$\cdot \deg f(x) > 0$$

esempio $\mathbb{R}[x] \ni f(x) = x^2 + 1$

$$\mathbb{R}[x]/(x^2+1)$$

$$3x^4 - 5x^3 + x - \sqrt{3} + (x^2+1)$$

$$3(-1)^2 - 5x^3 + x - \sqrt{3} + (x^2+1)$$

$$(3(x^4 - 1) = 3(x^2+1)(x^2-1) \in (x^2+1))$$

$$= 3 - 5(-1)x + x - \sqrt{3} + (x^2+1) =$$

$$= 6x + 3 - \sqrt{3} + (x^2+1)$$

$$\mathbb{K}[x]/(f(x)) \quad \deg f(x) = n > 0$$

ha n dimensioni su \mathbb{K}

$$\text{base : } \{x^0 + (f(x)), x^1 + (f(x)), x^2 + (f(x)), \dots, x^{n-1} + (f(x))\}$$

esercizio

\mathbb{K} campo, R anello, $R \ni \mathbb{K}$ sottanello

Verificare che R è spazio vettoriale su \mathbb{K}

esempio $A = K[x]$ e sia $f(x) \in K[x]$ prendiamo $K = \mathbb{Z}_2$ e $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$

Posso costruire l'anello quoziente

$$K[x]/(f(x)) = \mathbb{Z}_2[x]/(x^2+x+1)$$

Quanti elementi ha?

Un elemento è di questo tipo $g(x) + (x^2+x+1)$

$$g(x) = (x^2+x+1)q(x) + r(x)$$

$$\text{Allora } g(x) + (x^2+x+1) = r(x) + (x^2+x+1)$$

Dunque per rappresentare le classi bastano i resti delle divisioni per x^2+x+1

$0+I, 1+I, x+I, x+1+I$ sono i 4 elementi di $\mathbb{Z}_2/(x^2+x+1)$

$$(x+I)(x+1+I) = x(x+1)+I = x^2+x+I = 1+I$$

Dunque $\mathbb{Z}_2[x]/(x^2+x+1)$ è un campo con 4 elementi, che chiameremo \mathbb{F}_4 .

$$g(x) \in K[x] \quad \overline{g(x)} := g(x) + (f(x))$$

$$f(\bar{x}) = 0 \quad f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$f(\bar{x}) = a_n \bar{x}^n + a_{n-1} \bar{x}^{n-1} + \dots + a_1 \bar{x} + a_0 = \overline{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0}$$

MORFISMI DI VALUTAZIONE

Def. Sia A un anello commutativo e sia R un anello che contiene A come sottoanello.

Allora, $\forall r \in R$, la mappa

$$\varphi_r: A[x] \rightarrow R \quad \varphi_r(f(x)) := f(r) \quad \forall f(x) \in A[x]$$

è un omomorfismo, chiamato morfismo di valutazione in r .

esempio Consideriamo:

$$\varphi_i: \mathbb{R}[x] \rightarrow \mathbb{C} \quad f(x) \mapsto f(i) \quad x \mapsto i$$

Si dimostra che $\text{Ker } \varphi_i = (x^2+1)$ e $\text{Im } \varphi_i = \mathbb{C}$

Per il primo teorema di omomorfismo:

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$$

Teorema Sia I ideale in $K[x]$.

Esiste in I un $f(x)$ tale che

$$I = (f(x))$$

DIMOSTRAZIONE

Se $I = (0)$, non ho nulla da dimostrare.

Sia dunque $I \neq (0)$

Considero l'insieme $\{\deg g(x) \mid g(x) \in I, g(x) \neq 0\} \subseteq \mathbb{N}$

È un sottoinsieme non vuoto di \mathbb{N} . Sia m il minimo.

Sia $f(x) \in I$ tale che $\deg f(x) = m$

Dimostriamo che $I = (f(x))$

Prendiamo un $h(x) \in I$

Facciamo la divisione euclidea: $h(x) = f(x)q(x) + r(x)$

$$\text{dove } r(x) = \begin{cases} 0 \\ \deg r(x) < \deg f(x) \end{cases}$$

Se $\deg r(x) < \deg f(x)$: $r(x) = h(x) - \underbrace{f(x)}_I \underbrace{q(x)}_I$

perché $f(x) \in I$ e assorbimento

dunque $r(x) \in I$

ASSURDO perché $\deg r(x) < \deg f(x) = m$

□

DEF. Un ideale I di un anello commutativo A si dice principale se è generato da un solo elemento, ossia se esiste $a \in A$ tale che $I = (a)$

DEF. Un dominio d'integrità si dice dominio a ideali principali (PID) se tutti i suoi ideali sono principali.

esempio $\mathbb{R}[x, y]$. L'ideale $I = (x, y)$ non è monogenerato

$$I = (x, y) = \{xh(x, y) + yq(x, y) \mid h(x, y), q(x, y) \in \mathbb{R}[x, y]\}$$

se fosse vero $(x, y) = (f(x, y))$

$$f(x, y) \mid x \text{ e } f(x, y) \mid y$$

Donque $f(x) = c$, con c costante

Ma allora $(f(x, y)) = (c) = (1) = \mathbb{K}[x, y]$ ASSURDO

esempio $\mathbb{Z}[x]$ con $I = (2, x)$

I non è monogenerato $2 \nmid x$ (esercizio)

DEF. Sia $f(x) \in \mathbb{K}[x]$ un polinomio $\neq 0$ e non costante, ossia $\deg f(x) \geq 1$

Diremo che $f(x)$ è irriducibile se

$$f(x) = a(x)b(x) \Rightarrow a(x) \text{ o } b(x) \text{ è invertibile}$$

proposizione Sia $f(x) \in \mathbb{K}[x]$ polinomio irriducibile.

Allora $\mathbb{K}[x]/(f(x))$ è un campo

DIMOSTRAZIONE

Sia $I = (f(x))$

Sia $a(x) + I$ un elemento di $\mathbb{K}[x]/I$ diverso da $0 + I$

Dobbiamo mostrare che esiste l'inverso.

Uso Bézout:

Noto che $\text{MCD}(a(x), f(x)) = 1$

Per Bézout esistono $\lambda(x)$ e $\mu(x)$ tali che

$$a(x)\lambda(x) + f(x)\mu(x) = 1$$

Allora affermo che $\lambda(x) + I$ è l'inverso cercato.

Infatti:

$$(a(x) + I)(\lambda(x) + I) = a(x)\lambda(x) + I = 1 + I$$

$$\text{perché } a(x)\lambda(x) - 1 = f(x)\mu(x) \in I$$

□

esempio $x^2 + x + 1 \in \mathbb{Z}_2[x]$ è irriducibile

$\mathbb{Z}_2[x]/(x^2 + x + 1)$ è un campo

oss Se $f(x)$ non è irriducibile, allora

$\mathbb{K}[x]/(f(x))$ non è un campo.

Infatti esistono divisori di 0:

se $f(x) = a(x)b(x)$ con $\deg a(x) \geq 1$, $\deg b(x) \geq 1$

allora $(a(x) + I)(b(x) + I) = 0 + I$

Inoltre $\mathbb{K}[x]/(a) \cong \mathbb{K}[x]$ e $\mathbb{K}[x]/(b) \cong \{0\}$

Si potrebbero studiare "congruenze" modulo polinomi

$$a(x)p(x) \equiv b(x) \pmod{m(x)}$$

Trovare $p(x)$ tale che $(a(x) + I)(p(x) + I) = b(x) + I$ in $\mathbb{K}[x]/I$ dove $I = (m(x))$

Vale anche il Teorema cinese del resto.

Anelli euclidei

Def. Un dominio D si dice **anello euclideo** se esiste una **funzione grado**:

$$g: D \setminus \{0\} \rightarrow \mathbb{N}$$

tale che

- 1) $\forall a, b \in D$, entrambi non 0, vale $g(a) \leq g(ab)$
- 2) $\forall a, b \in D$, con $b \neq 0$, esistono $q, r \in D$ tali che
 $a = bq + r$ dove $r = 0$ o $g(r) < g(b)$

Lemma In un anello euclideo D siano $a, b \neq 0$
Se $b|a$ e $a \nmid b$, allora $g(b) < g(a)$

DIMOSTRAZIONE

Sia $a = bc$

Ora faccio la divisione euclidea: $b = aq + r$

Dato che $a \nmid b$, $r \neq 0$ e allora $g(r) < g(a)$

D'altra parte $r = b - aq = b - bcq = b(1 - cq)$

Allora, per la 1), $g(r) \geq g(b)$

Dunque $g(a) > g(r) \geq g(b)$

Nota: $1 - cq \neq 0$, altrimenti c invertibile e da $a = bc$
ricavo $ac^{-1} = b$ ma per ipotesi $b \nmid a$ **Assurdo** \square

Lemma In un anello euclideo D vale che $g(1) \leq g(b) \forall b \in D$
e inoltre $g(b) = g(1)$ se e solo se b è invertibile.

DIMOSTRAZIONE

Per il primo punto: dalla proprietà 1) della funzione grado, $g(1) \leq g(1 \cdot b) = g(b) \forall b \in D$

Per il secondo punto:

$\Rightarrow: g(b) = g(1)$ Sia $a \in D$: $a = bq + r$ con $r = 0$ oppure $g(r) < g(b)$, ma $g(b)$ è il minimo grado possibile, quindi $r = 0$. Da cui $a = bq$, quindi $a \in (b) \forall a \in D \Rightarrow D = (b)$
quindi b è invertibile.

$\Leftarrow: b \in D^*$ quindi $D = (b)$.

Perciò $\forall a \in D \exists r \in D: a = rb$, da cui $g(a) \geq g(b)$, quindi g è il valore minimo del grado.

Quindi $g(b) = g(1)$ \square

Def. L'insieme $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ è chiamato **anello degli interi di Gauss**.

$\mathbb{Z}[i]$ è un sottoanello di \mathbb{C}

Per questo $\mathbb{Z}[i]$ è un dominio

oss Sia R sottoanello di K campo.

Allora R è un dominio.

Infatti se avessi in R $a \neq 0, b \neq 0$ tali che $ab = 0$

questo varrebbe anche in K , ma so che in K l'unico divisore di 0 è 0.

Proposizione $\mathbb{Z}[i]$ è euclideo

DIMOSTRAZIONE

Definisco un grado

$$g: \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}$$

$$a+bi \mapsto a^2+b^2 = |a+bi|^2$$

La proprietà 1) è facile

Siano $z, w \in \mathbb{Z}[i]$, entrambi $\neq 0$

Allora $g(zw) \geq g(z)$

perché $g(zw)$ in questo caso è $g(z)g(w)$

in $\mathbb{Z}[i]$ il grado ha valore minimo 1.

Siano adesso $z, w \in \mathbb{Z}[i]$ con $w \neq 0$

I vertici di questi quadrati sono gli elementi $aw+biw$ al variare di $a, b \in \mathbb{Z}$

Prendo il vertice più vicino a z (se sono più di uno, ne scelgo uno)

Tale vertice è multiplo di w , diciamo

$$w_0 w \text{ con } w_0 \in \mathbb{Z}[i]$$

$$|z - w_0 w| \leq \frac{|w|}{\sqrt{2}}$$

Elevando al quadrato

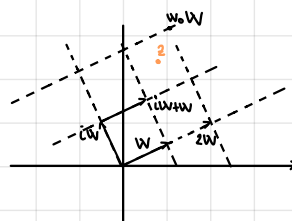
$$g(z - w_0 w) \leq \frac{g(w)}{2}$$

Dunque posso scrivere

$$z = w w_0 + \underset{r}{(z - w_0 w)}$$

$$\text{con } g(r) \leq \frac{g(w)}{2} < g(w)$$

□



Fattorizzazione negli anelli euclidei

DEF. Sia D anello euclideo

Un elemento $p \in D$ ma $p \notin D^*$, $p \neq 0$, si dice **irriducibile** se

$$p = \alpha\beta \implies \alpha \in D^* \text{ oppure } \beta \in D^*$$

Teorema Sia D un anello euclideo. Allora D è un dominio a ideali principali.

DIMOSTRAZIONE

Vedi teorema precedente.

DEF. Sia D un anello euclideo e siano $a, b \in D$ elementi non entrambi nulli.

Sia d un generatore dell'ideale (a, b) . Diremo che d è un **massimo comun divisore** di a e b .

Negli anelli euclidei si può fare l'algoritmo di Euclide per trovare il MCD fra due elementi a, b non entrambi nulli.

NOTA $\text{MCD}(a, b)$ è un elemento $d \in D$ tale che

$$\bullet d|a \text{ e } d|b$$

$$\bullet \text{ se } c|a \text{ e } c|b, \text{ allora } c|d$$

Non è unico, ma due massimi comuni divisori di a e b differiscono solo per moltiplicazione per invertibile, ossia sono associati.

Teorema di Bézout

Sia D un anello euclideo

Dati $a, b \in D$ non entrambi nulli, sia $\text{MCD}(a, b)$ un massimo comun divisore di a e b .

Allora esistono $\lambda, \mu \in D$ tali che:

$$\lambda a + \mu b = \text{MCD}(a, b)$$

esercizio

dimostrare che se c è un altro massimo comune divisore di a e b , allora $\text{MCD}(a, b)$ e c sono associati

Gli elementi irriducibili in D hanno allora anche la seguente proprietà, che li caratterizza (primalità)

Teorema

Sia $p \in D$ irriducibile. Se $p|ab$ e $p \nmid a$, allora vale che $p|b$

DIMOSTRAZIONE

$\text{MCD}(a, p) = 1$ a meno di associati.

Per Bézout: $1 = \lambda a + \mu p$

Moltiplico per b : $b = \lambda ab + \mu pb$

Nota che $p|\lambda ab$, $p|\mu pb$, dunque $p|b$. \square

Teorema di esistenza e unicità della fattorizzazione

In un anello euclideo D ogni elemento $d \in D \setminus (D \setminus \{0\})$ ammette una fattorizzazione come prodotto di irriducibili e tale fattorizzazione è unica (a meno di associati)

DIMOSTRAZIONE

Il fatto che una fattorizzazione esista si dimostra per induzione forte sul grado o con il principio del minimo in maniera analoga a \mathbb{Z} :

$$d \begin{cases} \text{è irriducibile} \\ \text{d} = ab \text{ con } \deg a < \deg d \text{ e } \deg b < \deg d \end{cases}$$

Supponiamo di avere due fattorizzazioni.

$$d = p_1 \cdots p_r \quad \text{e} \quad d = q_1 \cdots q_s \quad (\text{anche con ripetizioni}) \quad \text{con } p_i, q_j \text{ irriducibili}$$

Sia $r \leq s$ e procedo per induzione su r .

PASSO BASE $r=1$: $d = p_1$ e $d = q_1 \cdots q_s$

Deve essere $s=1$ altrimenti assurdo.

PASSO INDUTTIVO

Suppongo l'enunciato vero fino a $r-1$ e considero:

$$d = p_1 \cdots p_r \quad d = q_1 \cdots q_s$$

Osservo che $p_1|d$, allora $p_1|q_1(q_2 \cdots q_s)$

Se $p_1|q_1$ vuol dire che p_1 e q_1 sono associati

Allora divido d per p_1 : $d' = p_2 \cdots p_r$, $d' = k q_2 \cdots q_s$ con k invertibile e concludo per ipotesi induttiva.

Se invece $p_1 \nmid q_1$, allora per il teorema precedente $p_1|q_2 \cdots q_s$

Ora se $p_1|q_2$, allora p_1 e q_2 sono associati; divido per p_1 e concludo per ipotesi induttiva.

Se $p_1 \nmid q_2$, allora per il teorema precedente $p_1|q_3 \cdots q_s$

e in un numero finito di passi si trova comunque un q_i associato a p_1

A questo punto si divide d per p_1 e si concluda per ipotesi induttiva. \square

esempio ~~caso~~caso

$$A = \{f(x) \in \mathbb{R}[x] \mid f(0) \in \mathbb{Q}\}$$

A è un sottoanello di $\mathbb{R}[x]$

$$2x^2 \in A$$

$$2x^2 = \begin{cases} (\sqrt{2}x)(\sqrt{2}x) \\ (2x)(x) \end{cases}$$

Osservo che x e $\sqrt{2}x$ sono irriducibili in A.

Se $x = \alpha(x)\beta(x)$ allora per ragioni di grado o $\alpha(x) = \text{cost}$ o $\beta(x) = \text{cost}$
e allora o $\alpha(x)$ invertibile o $\beta(x)$ invertibile

Se $\sqrt{2}x = p(x)g(x)$, per ragioni di grado diciamo senza perdita di generalità:

$$p(x) = ax+b \quad g(x) = k \quad \text{con } a \neq 0 \text{ e } k \neq 0 \text{ e } p(x), g(x) \in A$$

$$\text{Da cui } \sqrt{2}x = (ax+b)k = akx + bk \quad \text{da cui } b=0$$

Dunque $p(x) = ax$ e $g(x) = k$ costante $\neq 0$

Dato che $g(x) = k \in A$, allora $k \in \mathbb{Q}$ e dunque è invertibile in A.

$$\text{Quindi } 2x^2 = \begin{cases} (\sqrt{2}x)(\sqrt{2}x) \\ (2x)(x) \end{cases}$$

sono due fattorizzazioni irriducibili ma x e $\sqrt{2}x$ non sono associati

(quindi in A la fattorizzazione non è unica)

Se fosse $\sqrt{2}x = x \cdot \text{invertibile}$

→ gli invertibili in A sono le costanti razionali

$$\sqrt{2}x = x \cdot r \quad \text{con } r \in \mathbb{Q}$$

quindi $r = \sqrt{2} \in \mathbb{Q}$ assurdo

NOTA 1 Dunque A non è euclideo

NOTA 2 Si nota che $x \mid (\sqrt{2}x)(\sqrt{2}x) = 2x^2$ ma $x \nmid \sqrt{2}x$ in A

NOTA 3 Come mai $\sqrt{2} \notin \mathbb{Q}$?

$$\text{Se fosse } \sqrt{2} = \frac{a}{b} \quad \text{con } a, b \in \mathbb{Z}, b \neq 0$$

$$\sqrt{2}b = a$$

$$2b^2 = a^2 \text{ e questo è assurdo:}$$

a sx l'esponente di 2 è dispari, a dx è pari.

Contraddice l'unicità della fattorizzazione

La Fattorizzazione in $\mathbb{Z}[i]$

esempio $5 \in \mathbb{Z}[i]$

$$5 = (2+i)(2-i) \quad 2 = (1+i)(1-i)$$

Lemma Sia $p \in \mathbb{Z}$ un numero primo dispari che non è irriducibile in $\mathbb{Z}[i]$

Allora p si può scrivere come somma di due quadrati di interi.

DIMOSTRAZIONE

p non è irriducibile, allora $p = (a+bi)(c+di)$

con $a+bi$ e $c+di$ non invertibili

$$\text{In particolare } |a+bi|^2 = a^2+b^2 > 1 \quad \text{e} \quad |c+di|^2 = c^2+d^2 > 1$$

$$\text{Nota che } p = \overline{p} = \overline{(a+bi)(c+di)} = (a-bi)(c-di)$$

Moltiplicando

$$p^2 = \underbrace{(a^2+b^2)}_1 \underbrace{(c^2+d^2)}_1$$

Per l'unicità della fattorizzazione in \mathbb{Z} , deve essere $p = a^2+b^2$ e $p = c^2+d^2$ □

Lemma Sia $p \in \mathbb{Z}$ un primo della forma $4n+1$. Allora la congruenza $x^2 \equiv -1 \pmod{p}$ ammette soluzione in \mathbb{Z} .

DIMOSTRAZIONE

Sia $x = 1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2}$. Poiché $p-1 = 4n$, $x = (-1)(-2) \dots (-\frac{p-1}{2})$

$$\begin{aligned} \text{Perciò } x^2 &= 1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2} \cdot (-1)(-2)(-3) \dots (-\frac{p-1}{2}) \equiv \\ &\equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2} \cdot \frac{p-1}{2} \cdot \dots \cdot (p-1) \equiv (p-1)! \equiv -1 \pmod{p} \end{aligned}$$

\uparrow
 th. Wilson

□

esempio 3 non riesco a scriverlo come somma di due quadrati

$$5 = 2^2 + 1^2$$

7 non riesco

11 non riesco

$$13 = 3^2 + 2^2$$

$$17 = 4^2 + 1^2$$

teorema Sia $p \in \mathbb{Z}$ numero primo con $p \equiv 1 \pmod{4}$. Allora p non è irriducibile in $\mathbb{Z}[i]$ e dunque esistono $a, b \in \mathbb{Z}$ tali che $a^2 + b^2 = p$.

DIMOSTRAZIONE

Visto il lemma, basta dimostrare che p non è irriducibile in $\mathbb{Z}[i]$

Sceglio un $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \pmod{p}$ (esiste, già dimostrato)

Dunque $p \mid x^2 + 1$, ossia $p \mid (x+i)(x-i)$

Se p fosse irriducibile, siccome $\mathbb{Z}[i]$ è euclideo, deve valere $p \mid x+i$ o $p \mid x-i$

Entrambe sono assurde: $p(a+bi) = x+i \rightarrow pa + pbi = x+i$ con $a, b \in \mathbb{Z}$
da cui $pb = 1$

proposizione Se $p \in \mathbb{Z}$ è un primo $p \equiv 3 \pmod{4}$ non si può esprimere come somma di due quadrati

DIMOSTRAZIONE

$$p = a^2 + b^2$$

Avrei mod 4:

$$3 \equiv a^2 + b^2 \pmod{4} \quad \text{ASSURDO} \quad \text{perché } a^2 \equiv \begin{matrix} 0 \\ 1 \end{matrix} \pmod{4} \quad \square$$

corollario
teorema di Natale di Fermat I numeri primi p che si possono scrivere come somma di due quadrati sono solo 2 e $p \equiv 1 \pmod{4}$.

Teorema Tutti e soli gli irriducibili in $\mathbb{Z}[i]$ sono (a meno di associati):

- i primi p di \mathbb{Z} t.c. $p \equiv 3 \pmod{4}$
- gli $z \in \mathbb{Z}[i]$ t.c. $|z|^2$ sia un numero primo.

DIMOSTRAZIONE

\Leftarrow : se p è primo di \mathbb{Z} , $p \equiv 3 \pmod{4}$

abbiamo già visto che è irriducibile in $\mathbb{Z}[i]$ (non si può scrivere come somma di due quadrati)

Sia z t.c. $|z|^2 = p$ con p primo

Supponiamo che $z = w_1 w_2$ con $w_1, w_2 \in \mathbb{Z}[i]$

$$|z|^2 = |w_1|^2 |w_2|^2$$

$$p = |w_1|^2 |w_2|^2$$

Allora deve essere o $|w_1|^2 = 1$ o $|w_2|^2 = 1$ e dunque

o w_1 è invertibile o w_2 è invertibile

Quindi z è irriducibile.

\Rightarrow : Sia $z \in \mathbb{Z}[i]$ irriducibile

$z \mid z \cdot \bar{z} = q_1 \cdots q_s$ fattorizzazione in \mathbb{Z} con q_i primi (con eventuali ripetizioni)

Dato che $\mathbb{Z}[i]$ è euclideo e z è irriducibile, sappiamo che z deve dividere uno dei q_i

Scriviamo $zw = q_i$ con $w \in \mathbb{Z}[i]$

- se w è invertibile, z è associato a q_i , che è primo.

Dunque q_i è irriducibile e allora dato che q_i è un primo di \mathbb{Z} ,

sappiamo che $q_i \equiv 3 \pmod{4}$

- se w non è invertibile, allora $|w|^2 > 1$

$$\text{Da } zw = q_i, \quad |z|^2 |w|^2 = q_i^2$$

perché z è irriducibile e pertanto non invertibile

Poiché q_i è primo, deve valere

$$|z|^2 = q_i \quad \text{e} \quad |w|^2 = q_i$$

□

esempio

$$|1+2i|^2 = 5$$

$$|2+3i|^2 = 13$$

$$|1+i|^2 = 2$$

esercizio

Sia $p \in \mathbb{Z}$, $p \equiv 1 \pmod{4}$

La scrittura $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$ è unica?

Supponiamo di avere $p = a^2 + b^2$ e $p = c^2 + d^2$

Allora $p = (a+bi)(a-bi)$ e $p = (c+di)(c-di)$

Siccome $|c+di|^2 = c^2 + d^2 = p$, sappiamo che $c+di$ è irriducibile, e analogamente anche $c-di$, $a+bi$, $a-bi$.

Quindi, dato che in $\mathbb{Z}[i]$ la fattorizzazione è unica, vale

$$a+bi = \begin{cases} c+di \\ c-di \end{cases} \quad \text{a meno di associati}$$

Dato che gli invertibili sono $1, -1, i, -i$, abbiamo 2 casi:

$$a^2 = c^2 \quad \text{e} \quad b^2 = d^2 \quad \text{oppure} \quad a^2 = d^2 \quad \text{e} \quad b^2 = c^2$$

esercizio Dire se $\mathbb{Z}[i]/(3)$ è un campo e calcolare quanti elementi ha.

Considero la classe $a+bi+(3)$

se $a+bi=3q+r$, allora $a+bi+(3)=r+(3)$

Ora un resto r di una divisione per 3 ha grado

$$|r|^2 < |3|^2 = 9$$

$$0+(3) \quad i+(3) \quad 2+i+(3)$$

$$1+(3) \quad 2i+(3) \quad 1+2i+(3)$$

$$2+(3) \quad 1+i+(3) \quad 2+2i+(3)$$

NOTA potendo sommare multipli di 3 alla parte reale e alla parte immaginaria, ho potuto scegliere dei rappresentanti con coordinate non negative

Dunque $\mathbb{Z}[i]/(3)$ ha 9 elementi

Notiamo che 3 è irriducibile in $\mathbb{Z}[i]$

Prendiamo ora uno dei 9 resti, per esempio $1+2i$

$$\text{MCD}(1+2i, 3) = 1 \quad \text{a meno di associati}$$

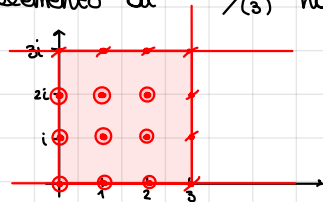
3 è irrid. e $\nexists \mid 1+2i$ perché $|3|^2 > |1+2i|^2$

Per Bézout esistono $\lambda, \mu \in \mathbb{Z}[i]$ t.c.

$$(1+2i)\lambda + 3\mu = 1$$

allora $\lambda+(3)$ è l'inverso di $1+2i+(3)$

Ogni elemento di $\mathbb{Z}[i]/(3)$ ha un inverso moltiplicativo, dunque $\mathbb{Z}[i]/(3)$ è un campo



$$(3) = \{3(a+bi) \mid a, b \in \mathbb{Z}\}$$

esercizio

Dimostrare che $\mathbb{Z}[i]/(a+bi)$ ha a^2+b^2 elementi
e che è un campo se e solo se $a+bi$ è irriducibile

complementi: dominio con fattorizzazione non unica

Consideriamo gli anelli $\mathbb{Z}[\sqrt{n}]$ e $\mathbb{Z}[i\sqrt{n}]$

Se n è un quadrato, $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}$. Consideriamo n 'squarefree'.

Questi anelli in generale non sono euclidei.

Si può comunque definire una "seminorma",

$$\begin{aligned} \ell: \mathbb{Z}[\sqrt{n}] &\longrightarrow \mathbb{Z} \\ a+b\sqrt{n} &\longmapsto a^2-nb^2 \end{aligned}$$

Lemma L'applicazione ℓ è moltiplicativa.

DIMOSTRAZIONE

Siano $a+b\sqrt{n}, c+d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$:

$$(a+b\sqrt{n})(c+d\sqrt{n}) = ac+bdn + (ad+bc)\sqrt{n}$$

$$\begin{aligned} \text{Perciò } \ell((a+b\sqrt{n})(c+d\sqrt{n})) &= (ac+bdn)^2 - n(ad+bc)^2 = a^2c^2 + 2abcdn + b^2d^2n^2 - a^2d^2n - 2abcdn - b^2c^2n = \\ &= c^2(a^2-nb^2) - nd^2(a^2-nb^2) = (a^2-nb^2)(c^2-nd^2) = \ell(a+b\sqrt{n})\ell(c+d\sqrt{n}) \end{aligned}$$

□

Lemma Un elemento $z \in \mathbb{Z}[\sqrt{n}]$ è invertibile se e solo se $\ell(z) \in \{-1, 1\}$.

DIMOSTRAZIONE

\Rightarrow : z è invertibile, quindi $zw=1$ per un certo $w \in \mathbb{Z}[\sqrt{n}]$

$$\text{Quindi } \ell(zw) = \ell(z)\ell(w) = \ell(1) = 1 \Rightarrow \ell(z) \in \{-1, 1\}.$$

\Leftarrow : $\ell(z) \in \{-1, 1\}$, quindi $|a^2-nb^2|=1$, da cui

$$(a+b\sqrt{n})(a-b\sqrt{n}) = 1 \text{ oppure } (a+b\sqrt{n})(-a+b\sqrt{n}) = 1 \Rightarrow z \text{ è invertibile} \quad \square$$

Lemma L'anello $\mathbb{Z}[\sqrt{10}]$ non è un dominio a fattorizzazione unica.

DIMOSTRAZIONE

Osserviamo ad esempio:

$$(4+\sqrt{10})(4-\sqrt{10}) = 6 = 2 \cdot 3$$

2, 3 sono irriducibili: infatti, se fosse $2 = (a+b\sqrt{10})(c+d\sqrt{10})$

$$\text{allora } \ell(a+b\sqrt{10})\ell(c+d\sqrt{10}) = \ell(2) = 4 \Rightarrow \text{le norme sono } \pm 2$$

$$\text{ma } a^2-10b^2 = \pm 2 \text{ non ha soluzioni intere ASSURDO}$$

Analogamente $a^2-10b^2 = \pm 3$ non ha soluzioni intere.

$4 \pm \sqrt{10}$ risultano irriducibili: infatti hanno norma 6, quindi i loro fattori dovrebbero avere norma 2 o 3, ma si è dimostrato che non esistono tali elementi. □

Sia K campo, sia $f(x) \in K[x]$ con $\deg f(x) \geq 1$

Consideriamo $K[x]/(f(x))$

Se $f(x)$ è riducibile, $f(x) = g(x)h(x)$ con $\deg(g(x)) \geq 1$ e $\deg(h(x)) \geq 1$

allora $\bar{g}(x)$ e $\bar{h}(x)$ sono divisori dello 0.

Def. Siano A_1 e A_2 due anelli.

Il loro prodotto diretto $A_1 \times A_2$ ha le seguenti operazioni di somma e prodotto:

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \quad (a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2) \quad \forall (a_1, a_2), (b_1, b_2) \in A_1 \times A_2$$

Analogia:

Sia $n \in \mathbb{Z}$, $n \geq 2$ tale che $n = ab$, con $a, b \in \mathbb{Z}$, $a > 1$, $b > 1$

Consideriamo il quoziente $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$

Risulta che $f: \mathbb{Z}/(n) \rightarrow \mathbb{Z}/(a) \times \mathbb{Z}/(b)$ definita da $f([c]_n) = ([c]_a, [c]_b)$

è un omomorfismo di anelli (esercizio). Per il teorema cinese è un isomorfismo

Quindi $\mathbb{Z}/(n) \cong \mathbb{Z}/(a) \times \mathbb{Z}/(b)$

Sia quindi $\text{MCD}(g(x), h(x)) = 1$. Risulta che:

$$\varphi: K[x]/(f(x)) \rightarrow K[x]/(g(x)) \times K[x]/(h(x))$$

è un isomorfismo di anelli

Irriducibilità

esempio Descriviamo i polinomi irriducibili di grado piccolo in $\mathbb{Z}_2[x]$

$$x, x+1, x^2+x+1, x^3+x^2+1, x^3+x+1, x^4+x^3+x^2+x+1, x^4+x^3+1, x^4+x+1$$

esercizio 1) Dato $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ con $a_n \neq 0 \neq a_0$ e sia $\frac{p}{q}$ una radice di $f(x)$ con $p, q \in \mathbb{Z}$, $\text{MCD}(p, q) = 1$. Allora $q | a_n$ e $p | a_0$

2) Descrivere un algoritmo che decide se un dato polinomio in $\mathbb{Q}[x]$ ha una radice razionale, e in caso affermativo ne calcola una.

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + \dots + a_1 \frac{p}{q} + a_0 \rightarrow 0 = a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n$$

esercizio Siano A_1 e A_2 due anelli, e sia $\varphi: A_1 \rightarrow A_2$ un omomorfismo

Sia $f(x) = a_n x^n + \dots + a_1 x + a_0 \in A_1[x]$

Allora $\bar{\varphi}: A_1[x] \rightarrow A_2[x]$ definito da $\bar{\varphi}(f(x)) = \varphi(a_n) x^n + \dots + \varphi(a_1) x + \varphi(a_0) \in A_2[x]$ è un omomorfismo di anelli

Def. Un polinomio $f(x) \in \mathbb{Z}[x]$ è **primitivo** se il MCD dei suoi coefficienti è uguale a 1.
(in pratica è primitivo se non ha fattori irriducibili di grado zero)

Proposizione

Sia p un primo, sia $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_p = \mathbb{Z}/(p)$ la proiezione al quoziente e sia $\hat{\varphi}: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ l'omomorfismo descritto sopra.

Sia $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ primitivo con $n \geq 1$, e $p \nmid a_n$.

Se $\hat{\varphi}(f(x))$ è irriducibile in $\mathbb{Z}_p[x]$, allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$.

DIMOSTRAZIONE

Supponiamo che f sia riducibile: $f(x) = g(x)h(x)$ con $\deg g(x) \geq 1$, $\deg h(x) \geq 1$ perché f è primitivo

Si ha $\hat{\varphi}(f(x)) = \hat{\varphi}(g(x)) \hat{\varphi}(h(x))$ e $\deg \hat{\varphi}(f(x)) = \deg f(x)$ perché $[a_n]_p \neq [0]_p$

Donque dev'essere $\deg \hat{\varphi}(g(x)) = \deg(g(x)) \geq 1$ e $\deg \hat{\varphi}(h(x)) = \deg(h(x)) \geq 1$

Quindi $\hat{\varphi}(f(x))$ è riducibile.

□

esempio $x^3 + 5x + 1 \in \mathbb{Z}[x]$
 \downarrow
 $x^3 + x + 1 \in \mathbb{Z}_2[x]$

Teorema criterio di Eisenstein

Sia $p \in \mathbb{N}$ un primo, e sia $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ primitivo tale che:

(i) $p \nmid a_n$

(ii) $p \mid a_i$ con $i = 0, \dots, n-1$

(iii) $p^2 \nmid a_0$

Allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$

DIMOSTRAZIONE

Supponiamo che $f(x) = g(x)h(x)$ con $g(x), h(x) \in \mathbb{Z}[x]$, $\deg(g(x)) \geq 1$, $\deg(h(x)) \geq 1$ perché f è primitivo.

Applichiamo $\hat{\phi}$.

$$[a_n]_p x^n = \hat{\phi}(f(x)) = \hat{\phi}(g(x)) \hat{\phi}(h(x)) \quad \text{dove per ipotesi } [a_n]_p \neq [0]_p$$

Osserviamo che in $\mathbb{Z}_p[x]$, il prodotto di due polinomi è un monomio solo se sono entrambi monomi.

Siccome $\deg \hat{\phi}(f(x)) = \deg f(x) = n$, varrà $\deg \hat{\phi}(g(x)) = \deg g(x) \geq 1$ e $\deg \hat{\phi}(h(x)) = \deg h(x) \geq 1$

quindi $\hat{\phi}(g(x)) = [b_r]_p x^r$ e $\hat{\phi}(h(x)) = [c_{n-r}]_p x^{n-r}$

Perciò i termini b_0 e c_0 sono divisi da p .

Allora $p^2 \mid a_0 = b_0 c_0$ ASSURDO

Quindi $f(x)$ non può essere riducibile in $\mathbb{Z}[x]$ \square

Lemma di GAUSS

Se $f(x), g(x) \in \mathbb{Z}[x]$ sono primitivi, allora $f(x) \cdot g(x)$ è primitivo.

DIMOSTRAZIONE

$$f(x) = \sum_{i=0}^n a_i x^i \quad g(x) = \sum_{j=0}^k b_j x^j$$

Se $f(x) \cdot g(x)$ non è primitivo, sia p un primo che divide tutti i coefficienti di $f(x) \cdot g(x)$

Siano a_r e b_s i coefficienti dei termini di grado più alto che non sono divisi da p

Il coefficiente di x^{r+s} in $f(x)g(x)$ è

$$\sum_{i+j=r+s} a_i b_j = a_r b_s + a_{r+1} b_{s-1} + \dots + a_{r-1} b_{s+1} + \dots$$

da cui p divide a_r o b_s ASSURDO $\leftarrow \square$

corollario

Se $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

Allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ se e solo se

$f(x)$ è primitivo e irriducibile in $\mathbb{Q}[x]$

DIMOSTRAZIONE

\Leftarrow : implicazione banale

\Rightarrow : Sia $f(x)$ primitivo e irriducibile in $\mathbb{Z}[x]$

Supponiamo che $f(x) = g(x)h(x)$ con $g(x), h(x) \in \mathbb{Q}[x]$

$\exists \alpha, \beta \in \mathbb{Q}$ tali che $\alpha \beta f(x) = (\alpha g(x))(\beta h(x))$

Per Gauss $\alpha \beta f(x)$ è primitivo

$f(x)$ primitivo $\Rightarrow \alpha \beta \in \mathbb{Z}$ (non ci sono coefficienti da semplificare)

$\alpha \beta f(x)$ primitivo $\Rightarrow \alpha \beta = \pm 1$

$\Rightarrow f(x)$ è riducibile in $\mathbb{Z}[x]$ $\leftarrow \square$

TEORIA DEI CAMPI

Sia K campo. Sia $f(x) \in K[x]$ irriducibile

Allora come sappiamo $L = K[x]/(f(x))$ è un campo che contiene K

e $\alpha = x + (f(x))$ è una radice di f in L

esempio $x^3 - 2 \in \mathbb{Q}[x]$ è irriducibile (per Eisenstein con $p=2$)

$$L = \mathbb{Q}[x]/(x^3 - 2)$$

Def. Dato L campo e A sottoanello di L ,
si dice che A è un sottocampo di L se
 $\forall a \in A, a \neq 0$, l'inverso di a appartiene ad A .

Def. Dati due campi $K \subseteq L$
diremo che L è un' estensione di K .

Oss L è uno spazio vettoriale su K

Def. Dati due campi $K \subseteq L$ e un elemento $\alpha \in L$, indicheremo con
 $K(\alpha)$ il minimo sottocampo (rispetto all'inclusione) di L che contiene K e α .

Si dice che $K(\alpha)$ è una estensione semplice di K

Oss $K(\alpha)$ è l'intersezione di tutti i sottocampi che contengono K e α .

Dati $K \subseteq L$ e $\alpha \in L$ considero

$$\begin{aligned} \psi: K[x] &\longrightarrow L \\ f(x) &\longmapsto f(\alpha) \end{aligned}$$

Come noto, ψ è un omomorfismo di anelli.

Considero

$$\text{Ker } \psi \begin{cases} = (0) \\ \neq (0) \end{cases}$$

Se $\text{Ker } \psi = (0)$ vuol dire che α non è radice di nessun polinomio $f(x) \in K[x]$ eccetto il polinomio 0.

Def. Se $\alpha \in L$ non è radice di nessun polinomio a coefficienti in K ,
si dice che α è trascendente su K .

esempio π, e sono trascendenti su \mathbb{Q}

In questo caso per il primo teorema di omomorfismo di anelli, vale che

$$K[x]/(0) \cong \text{Im } \psi \quad \text{ossia } K[x] \cong K[\alpha] = \text{Im } \psi$$

in particolare $K[\alpha]$ non è un campo, quindi $K[\alpha] \neq K(\alpha)$

Sia invece $\text{Ker } \psi \neq (0)$

Dato che $\text{Ker } \psi$ è ideale di $K[x]$ e $K[x]$ è euclideo, allora $\text{Ker } \psi$ è principale: $\text{Ker } \psi = (g(x))$

Def. Dati due campi $K \subseteq L$ si dice che un elemento $\alpha \in L$ è algebrico su K se esiste
un polinomio non nullo in $K[x]$ di cui α è radice, ossia se il nucleo $\text{Ker } \psi$ della valutazione definita
sopra è diverso da zero. Un generatore $f(x)$ di $\text{Ker } \psi$ si chiama polinomio minimo di α su K .

Oss Un polinomio minimo di α su K divide ogni altro polinomio di $K[x]$ che ha α come radice.

Il polinomio minimo diventa unico se lo si considera monico

Quindi $\text{Ker } \psi = (g(x))$

Osserviamo che $g(x)$ è irriducibile in $\mathbb{K}[x]$

Infatti se fosse $g(x) = g_1(x)g_2(x)$ con $1 \leq \deg g_1(x) < \deg g(x)$ $1 \leq \deg g_2(x) < \deg g(x)$

Quando valutato in α

$$g(\alpha) = g_1(\alpha)g_2(\alpha) = 0 = g_1(\alpha)g_2(\alpha) \text{ in } \mathbb{L}$$

Allora $0 = g_1(\alpha) = 0$ o $g_2(\alpha) = 0$, ossia $g_1(x) \in \text{Ker } \psi$ oppure $g_2(x) \in \text{Ker } \psi$

ASSURDO poiché $g(x)$ ha grado maggiore

Per il primo teorema di omomorfismo di anelli

$$\mathbb{K}[x] / (g(x)) \cong \mathbb{K}[\alpha]$$

Sappiamo che è un campo perché $g(x)$ è irriducibile in $\mathbb{K}[x]$

Allora $\mathbb{K}[\alpha] \subseteq \mathbb{K}(\alpha)$ ma $\mathbb{K}[\alpha]$ è un campo.

Deve allora valere $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$

esempio $\mathbb{K} = \mathbb{Q}$ $\mathbb{L} = \mathbb{R}$ $\alpha = \sqrt[3]{2}$ $\mathbb{Q}[x] / (x^3-2) \cong \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$

x^3-2 è polinomio minimo di $\sqrt[3]{2}$

Infatti $\sqrt[3]{2}$ è radice di x^3-2 e x^3-2 è irriducibile, deve essere lui un generatore di $\text{Ker } \psi$

$$\frac{1}{1+\sqrt[3]{2}} \in \mathbb{Q}(\sqrt[3]{2})$$

Considero $1+x+(x^3-2)$ in $\mathbb{K}[x] / (x^3-2)$

Il suo inverso è $\frac{1}{3}(x^2-x+1) + (x^3-2)$

$$\text{cioè } (1+x) \frac{1}{3}(x^2-x+1) = 1 + N(x)(x^3-2)$$

Lo valuto in $\sqrt[3]{2}$

$$(1+\sqrt[3]{2}) \frac{1}{3}((\sqrt[3]{2})^2 - \sqrt[3]{2} + 1) = 1 + 0$$

Quindi $\frac{1}{3}((\sqrt[3]{2})^2 - \sqrt[3]{2} + 1)$ è l'inverso di $(1+\sqrt[3]{2})$ e appartiene a $\mathbb{Q}(\sqrt[3]{2})$

Prendo adesso un'altra radice di x^3-2

$$\text{Chiamo } \omega = \cos \frac{2}{3}\pi + i \sin \frac{2}{3}\pi$$

Anche $\beta = \sqrt[3]{2}\omega$ è una radice di x^3-2

Ripeto lo stesso argomento di prima

$$\mathbb{Q}[x] / (x^3-2) \cong \mathbb{Q}[\sqrt[3]{2}\omega]$$

$$\psi: \mathbb{Q}[x] \rightarrow \mathbb{C}$$

$$f(x) \mapsto f(\beta)$$

Prima avevamo trovato $\mathbb{Q}[x] / (x^3-2) \cong \mathbb{Q}[\sqrt[3]{2}]$

Vale dunque $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}\omega) \cong \mathbb{Q}(\sqrt[3]{2}\omega^2)$ ma non coincidono

$$\mathbb{Q}(\sqrt[3]{2}\omega) \neq \mathbb{Q}(\sqrt[3]{2}\omega^2)$$

Se fossero uguali $\mathbb{Q}(\sqrt[3]{2}\omega) = \mathbb{Q}(\sqrt[3]{2}\omega^2) = \mathbb{K}_1$

$$\frac{\sqrt[3]{2}\omega^2}{\sqrt[3]{2}\omega} = \omega \in \mathbb{K}_1$$

$$\frac{\sqrt[3]{2}\omega}{\omega} = \sqrt[3]{2} \in \mathbb{K}_1$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subsetneq \mathbb{K}_1$$

sp. vett.
di dim 3 su \mathbb{Q}

quindi devono coincidere \nmid ASSURDO per ragioni dimensionali

Teorema Dati $K \subseteq L$ campi.
 Sia $f(x)$ un polinomio irriducibile in $K[x]$ che
 ha due radici distinte α, β in L .
 Allora esiste un isomorfismo θ :
 $\theta: K[\alpha] \longrightarrow K[\beta]$
 tale che $\theta(\alpha) = \beta$ e $\theta|_K = \text{identità}$

DIMOSTRAZIONE

$$K[\alpha] \cong K[x] / (f(x)) \cong K[\beta]$$

$$\alpha \longleftrightarrow x + (f(x)) \longleftrightarrow \beta \quad \square$$

Teorema Sia $f(x) \in K[x]$ con K campo.
 Sia $\deg f(x) = n \geq 1$.
 Allora f ha al più n radici in K (contate con molteplicità)

DIMOSTRAZIONE

Come sappiamo, se $\alpha \in K$ è radice di f , allora $(x - \alpha) \mid f(x)$
 ossia $f(x) = (x - \alpha)g(x)$ con $\deg g(x) = n - 1$

Cerco adesso le radici di $g(x)$ e proseguo.

$$f(x) = (x - \alpha)(x - \beta) \cdots h(x) \quad \text{con } h(x) \text{ che non ha radici in } K \quad \text{Qui mi fermo.}$$

Se $f(x)$ avesse anche un'altra radice α' , avrei $f(x) = (x - \alpha') \cdots h'(x)$
 e questo è ASSURDO perché contraddice l'unicità della
 fattorizzazione in $K[x]$, anello euclideo.

Infatti $x - \alpha'$ è irriducibile. \square

esempio $x^2 - 2x$ ha 4 radici in $\mathbb{Z}_8[x]$

Teorema Sia K un campo e sia $f(x) \in K[x]$ un polinomio di grado $n \geq 0$.
 Allora esistono un campo E tale che $K \subseteq E$ ed elementi e_1, \dots, e_n (eventualmente con ripetizioni)
 di E tali che $f(x)$ si fattorizza nel seguente modo in $E[x]$ (λ è una costante):

$$f(x) = \lambda (x - e_1)(x - e_2) \cdots (x - e_n)$$

DIMOSTRAZIONE

Per induzione su $n = \deg f(x)$. La base $n = 0$ è un'immediata verifica.

Sopponiamo $n = \deg f(x) \geq 1$ e sia $f_1(x)$ un fattore irriducibile di $f(x)$.

Costruiamo $F = K[x] / (f_1(x))$: in tale campo esiste $\bar{\alpha}$ radice di $f(x)$. Poniamo $e_1 = \bar{\alpha}$.

In $F[x]$ quindi si ha: $f(x) = (x - e_1)g(x)$ con $\deg g(x) = n - 1$

Per ipotesi induttiva, esiste un campo E che estende F ed elementi e_2, \dots, e_n in E tale che:

$$g(x) = \lambda (x - e_2) \cdots (x - e_n)$$

Osserveremo che E estende K in quanto $K \subseteq F \subseteq E$ e in $E[x]$:

$$f(x) = \lambda (x - e_1)(x - e_2) \cdots (x - e_n) \quad \square$$

Estensioni di campi

F, K campi $F \subseteq K$

K è spazio vettoriale su F

$\alpha \in K$, $F(\alpha) :=$ il più piccolo sottocampo di K che contiene sia F sia α

$$F \subseteq F(\alpha) \subseteq K$$

$F(\alpha)$ è spazio vettoriale su F

$$\dim_F F(\alpha)$$

Se $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \dots$ sono tutti lin. ind. su F , allora $\dim_F F(\alpha) = \infty$

Altrimenti esistono $f_0, f_1, \dots, f_m \in F$ t.c. $f_0 + f_1 \alpha + f_2 \alpha^2 + \dots + f_m \alpha^m = 0$ e f_0, \dots, f_m non tutti zero

Possiamo assumere $f_m \neq 0, m \geq 1$

Allora $g(x) := f_m x^m + \dots + f_1 x + f_0 \in F[x]$ è tale che $g(\alpha) = 0$

Quindi α è algebrico su F

$$\varphi_\alpha: F(x) \longrightarrow K \quad \varphi_\alpha(f(x)) := f(\alpha)$$

$$x \longmapsto \alpha$$

Se α è algebrico su F , esiste $g(x) \in F[x]$ t.c. $g(\alpha) = 0 \Rightarrow g(x) \in \text{Ker } \varphi_\alpha$

Quindi $\text{Ker } \varphi_\alpha \neq \{0\}$. Quindi esiste $f(x) \in F[x]$ t.c. $\text{Ker } \varphi_\alpha = (f(x))$

Per il teorema di omomorfismo

$$F[x] / (f(x)) \cong \text{Im } \varphi_\alpha \subseteq K$$

Ma $f(x)$ è irriducibile, quindi $\text{Im } \varphi_\alpha$ è un sottocampo di K che contiene F e α

Necessariamente $\text{Im } \varphi_\alpha = F[\alpha] \subseteq F(\alpha) \Rightarrow F[\alpha] = F(\alpha) = \text{Im } \varphi_\alpha$

DEF. Dati due campi $F \subseteq K$, il **grado di K su F** è la dimensione di K come spazio vettoriale su F e si indica con il simbolo $[K:F]$.

Se la dimensione è infinita, si scrive $[K:F] = \infty$.

Se il grado è finito, si dice che K è una **estensione finita** di F , altrimenti si dice che è una **estensione infinita**.

NOTAZIONE $[K:F] = \dim_F K$

proposizione F, K, L campi, $F \subseteq K \subseteq L$

Supponiamo che $[L:K] = m \in \mathbb{N}$, $[K:F] = n \in \mathbb{N}$

Allora $[L:F] = [L:K][K:F] = mn$

DIMOSTRAZIONE

Sia $\{w_1, \dots, w_n\}$ una base di K su F .

Sia $\{v_1, \dots, v_m\}$ una base di L su K .

Consideriamo $\{v_i w_j \mid 1 \leq i \leq m, 1 \leq j \leq n\} \subseteq L$

Sia $\alpha \in L$, allora esistono $k_1, k_2, \dots, k_m \in K$ t.c. $\alpha = k_1 v_1 + k_2 v_2 + \dots + k_m v_m$

Esistono f_{ij} con $1 \leq i \leq m$ e $1 \leq j \leq n$ t.c. $k_i = \sum_{j=1}^n f_{ij} w_j$

Quindi $\alpha = \sum_{i=1}^m \sum_{j=1}^n f_{ij} v_i w_j$ quindi i $v_i w_j$ generano.

Sono lin. ind. poiché: $\sum_{i=1}^m \sum_{j=1}^n f_{ij} v_i w_j = 0 \Leftrightarrow \sum_{i=1}^m (f_{i1} w_1 + \dots + f_{in} w_n) v_i = 0$

Poiché i v_i sono lin. ind., equivale a: $f_{i1} w_1 + \dots + f_{in} w_n = 0$

Ma i w_j sono lin. ind., quindi: $f_{ij} = 0$ \square

esempio $\mathbb{Q}(\sqrt[3]{7}) \supseteq \mathbb{Q}$

$x^3 - 7$ è irriducibile per Eisenstein ($p=7$)

Quindi $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$

corollario Se L è una estensione finita di F e $F \subseteq K \subseteq L$, allora K è una estensione finita di F e L è una estensione finita di K .
Inoltre $[L:F] = [L:K] \cdot [K:F]$

DIMOSTRAZIONE

Consideriamo L come sp. vett. su F . ha dim finita e K è ssp, quindi K ha dim finita su F .

Una base di L su F è anche un insieme finito di generatori di L su K , quindi L ha dim finita su K .

Si conclude applicando il teorema precedente. \square

teorema F, K campi, $F \subseteq K$
 $\alpha \in K$ è algebrico se e solo se $\dim_F F(\alpha)$ è finita.

DIMOSTRAZIONE

\Leftarrow : se $[F(\alpha):F] = m \in \mathbb{N}$, allora $\{1, \alpha, \alpha^2, \dots, \alpha^m\}$ è lin. dip, poiché composto da $m+1$ elementi.

Allora esistono $p_0, p_1, \dots, p_m \in F$ non tutti nulli tali che:

$$p_0 + p_1 \alpha + \dots + p_m \alpha^m = 0$$

dunque α è algebrico su F poiché è soluzione del polinomio $p_m x^m + \dots + p_1 x + p_0 \in F[x]$

\Rightarrow : se α è algebrico su F , sappiamo che $F(\alpha) = F[\alpha] \cong F[x]/(f(x))$ dove $f(x)$ è il polinomio minimo

Per quanto noto, $[F(\alpha):F]$ è finito ed uguale a $\deg f$. \square

def. Dati due campi $F \subseteq K$, un elemento $\alpha \in K$ si dice **algebrico di grado n su F** se $[F(\alpha):F] = n$, ovvero se il suo polinomio minimo su F ha grado n .

proposizione F, K campi, $F \subseteq K$
Siano $\alpha, \beta \in K$ algebrici su F , rispettivamente di grado m e n
Allora $\alpha \pm \beta, \alpha \cdot \beta$ e α/β (se $\beta \neq 0$) sono algebrici su F di grado $\leq mn$.

DIMOSTRAZIONE

$$[F(\alpha):F] = m \in \mathbb{N}, \quad F(\alpha) \subseteq K$$

β è algebrico su $F(\alpha)$. sia f il suo polinomio irriducibile su F ($\deg f = n$)
 f potrebbe non essere irriducibile in $F(\alpha)[x]$: in tal caso il polinomio minimo è uno dei fattori irriducibili di f in $F(\alpha)[x]$. Dunque il grado di β su $F(\alpha)$ è $\leq n$. Quindi:

$$[F(\alpha)(\beta):F] = [F(\alpha)(\beta):F(\alpha)] [F(\alpha):F] \leq nm$$

$F(\alpha)(\beta) = F(\alpha, \beta)$ è il più piccolo sottocampo di K che contiene F, α, β , quindi contiene $\alpha \pm \beta, \alpha \cdot \beta, \alpha/\beta$ (se $\beta \neq 0$), che risultano algebrici di grado $\leq nm$.

Ad esempio: $F(\alpha + \beta) \subseteq F(\alpha, \beta)$, dunque $[F(\alpha + \beta):F] \leq nm$.

Per il teorema precedente $\alpha + \beta$ è algebrico su F di grado $\leq nm$. \square

corollario F, K campo, $F \subseteq K$
Allora gli elementi algebrici di K su F formano un sottocampo di K che contiene F .

esempio $\mathbb{Q} \subseteq \mathbb{C}$ $\bar{\mathbb{Q}} = \{z \in \mathbb{C} \text{ algebrici su } \mathbb{Q}\}$
 $\mathbb{Q} \subsetneq \bar{\mathbb{Q}} \subsetneq \mathbb{C}$

DEF. Siano F, K campi, $F \subseteq K$
L'estensione $F \subseteq K$ è **algebraica** se ogni elemento $\alpha \in K$ è algebrico su F .

OSS Un'estensione finita $F \subseteq K$ è algebraica. Infatti dato $\alpha \in K$, si può considerare $F \subseteq F(\alpha) \subseteq K$: risulta $F \subseteq F(\alpha)$ finita quindi α è algebrico.

proposizione Siano $F \subseteq K \subseteq L$ campi, con $F \subseteq K$ estensione algebraica e $K \subseteq L$ estensione algebraica.
Allora $F \subseteq L$ è algebraica.

DIMOSTRAZIONE

$\alpha \in L$. Per ipotesi, α è algebrico su K ,
quindi esiste $g(x) = k_n x^n + k_{n-1} x^{n-1} + \dots + k_1 x + k_0$, con $k_i \in K$ e $g(\alpha) = 0$.
Ora, K è algebrico su F quindi $[F(k_0) : F]$ è finito.
Anche $[F(k_0, k_1) : F]$ è finito, poiché k_1 è algebrico su F , e quindi anche su $F(k_0)$.
Iterando, si ha $[F(k_0, k_1, \dots, k_m) : F]$ è finito.
Poi $[F(\alpha, k_0, \dots, k_m) : F(k_0, \dots, k_m)]$ è finito, poiché α è algebrico su $F(k_0, \dots, k_m)$.
Per il teorema delle torri di estensioni: $[F(\alpha, k_0, \dots, k_m) : F]$ è finito e $F(\alpha) \subseteq F(\alpha, k_0, \dots, k_m)$
 $\Rightarrow \alpha$ è algebrico su F . \square

DEF. Si dice che un numero complesso z è un **numero algebrico** se z è algebrico su \mathbb{Q} .

OSS I numeri algebrici formano un sottocampo $\mathcal{A} \subseteq \mathbb{C}$ con $[\mathcal{A} : \mathbb{Q}] = \infty$.

campi di spezzamento

DEF. Sia F un campo e sia $f(x) \in F[x]$ un polinomio non nullo.

Una estensione finita E di F si dice un **campo di spezzamento** di $f(x)$ su F se:

- in $E[x]$ $f(x)$ si fattorizza come prodotto di polinomi di grado 1
- $\forall K$ campo tale che $F \subseteq K \subsetneq E$, $f(x)$ non si fattorizza in $K[x]$ come prodotto di polinomi di primo grado

OSS Dato $f(x) \in K[x]$ un campo di spezzamento esiste.

ALGORITMO sia $f(x) = f_1^{m_1}(x) \dots f_k^{m_k}(x)$ con f_i irriducibili in $K[x]$

Se $\deg f_1 = \deg f_2 = \dots = \deg f_k = 1$

allora f ha tutte le radici in K e K è il campo di spezzamento di $f(x)$ su K .

Supponiamo invece $\deg f_1 > 1$

Crea $K_1 = K[x]/(f_1(x))$ campo. In K_1 , $f_1(x)$ ha una radice $\alpha = \bar{x}$.

Fattorizzo ora $f(x)$ in $K_1[x]$ e itero il processo.

proposizione Sia K campo, sia $f(x) \in K[x]$ polinomio non nullo di grado n .
Allora, se E è un campo di spezzamento di $f(x)$ su K , vale
 $[E : K] \leq n!$

$$E = K(\alpha_1, \dots, \alpha_n)$$

esempio Sia $f(x)$ di grado 10 irriducibile

$K_1 = K[x]/(f(x))$ ha grado 10

$f(x) = (x - \alpha) \tilde{f}(x)$ Supponiamo \tilde{f} irriducibile

Allora $K_2 = K_1[x]/(\tilde{f}(x))$ ha grado 9

$$\underbrace{K \subseteq K_1}_{10} \subseteq \underbrace{K_2}_{9} \dots$$

esempio $x^4 - 2$ in $\mathbb{Q}[x]$

Un campo di spezzamento in \mathbb{C} è $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i, \sqrt[4]{2}i, \sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$$

$x^4 - 2$ è pol. min.

$$\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}[x]/(x^4 - 2) \quad x^2 + 1 \text{ è pol. min di } i \text{ su } \mathbb{Q}(\sqrt[4]{2})$$

$$\text{Dunque } [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8 < 4! = 24$$

esempio $x^3 - 2 \in \mathbb{Q}[x]$

$$\mathbb{Q}(\sqrt[3]{2}, \omega)$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$$

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

ω è radice

irriducibile in $\mathbb{Q}(\sqrt[3]{2})[x]$ perché non ha radici in $\mathbb{Q}(\sqrt[3]{2})$ e ha grado 2

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6 = 3!$$

teorema Sia \mathbb{F} un campo e siano \mathbb{E} e \mathbb{E}' campi di spezzamento di $f(x) \in \mathbb{F}[x]$ non nullo.

(vedi Algebra I)

Allora esiste ϕ' isomorfismo: $\mathbb{E} \rightarrow \mathbb{E}'$

tale che $\phi'|_{\mathbb{F}} = \text{id}$

campi finiti

Sia \mathbb{K} campo.

Considero $\phi: \mathbb{Z} \rightarrow \mathbb{K}$ omomorfismo di anelli ($1 \mapsto 1$)

Notiamo che $\text{Ker } \phi$ è un ideale di \mathbb{Z} e dunque $\text{Ker } \phi = (d)$

Si distinguono due casi

• $d = 0$ allora ϕ è iniettivo

cioè \mathbb{K} contiene $\text{Im } \phi$ che è una "copia" di \mathbb{Z}

Dato che \mathbb{K} è un campo, \mathbb{K} allora contiene una "copia" di \mathbb{Q}

In particolare \mathbb{K} è infinito

Si dice in questo caso $d = 0$ che \mathbb{K} ha caratteristica 0.

• $d \neq 0$, $\text{Ker } \phi = (d)$

Se d non è primo, si avrebbero in \mathbb{K} dei divisori di zero non banali ASSURDO

Si deduce che deve essere $d = p$ primo

Per il I teorema di omomorfismo: $\mathbb{Z}/(p) \cong \text{Im } \phi \subseteq \mathbb{K}$

Dunque \mathbb{K} contiene una copia di \mathbb{Z}_p e si dice che \mathbb{K} ha caratteristica p.

In \mathbb{K} vale:

$$\underbrace{1+1+\dots+1}_{p \text{ volte}} = \phi(1) + \dots + \phi(1) = \phi(1+\dots+1) = \phi(p) = 0$$

Notiamo che \mathbb{K} è uno spazio vettoriale su \mathbb{Z}_p

Sia $v \in \mathbb{K}$. Vale che

$$\underbrace{v+\dots+v}_{p \text{ volte}} = \underbrace{(1+\dots+1)}_{p \text{ volte}} v = 0v = 0$$

NOTA Esistono campi di caratteristica p infiniti

$\mathbb{Z}_2(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{Z}_2[x], g(x) \neq 0 \right\}$ campo delle funzioni razionali a coefficienti in \mathbb{Z}_2

$\mathbb{Z}_2(x)$ ha caratteristica 2 e infiniti elementi

OMOMORFISMO DI FROBENIUS

DEF. Sia \mathbb{K} un campo di caratteristica p .

$$\text{Sia } \mathcal{F} : \mathbb{K} \rightarrow \mathbb{K}$$

$$a \mapsto a^p$$

\mathcal{F} si chiama **omomorfismo di Frobenius**

Si osserva facilmente che \mathcal{F} è un omomorfismo di anelli

$$1 \mapsto 1^p = 1$$

$$ab \mapsto (ab)^p = a^p b^p$$

$$(a+b) \mapsto (a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{p-1} a b^{p-1} + b^p = a^p + b^p$$

OSS Se ho un omomorfismo di campi $f: \mathbb{K}_1 \rightarrow \mathbb{K}_2$

f è iniettivo. Infatti $\text{Ker } f$ è ideale di \mathbb{K}_1

e allora $\text{Ker } f = \begin{cases} (0) \\ \mathbb{K}_1 \end{cases}$ si esclude perché $f(1) = 1$

NOTA Anche $\mathcal{F}^s = \underbrace{\mathcal{F} \circ \mathcal{F} \circ \dots \circ \mathcal{F}}_{s \text{ volte}}$ è omomorfismo iniettivo

teorema Sia \mathbb{E} campo qualunque
e sia $\psi: \mathbb{E} \rightarrow \mathbb{E}$ omomorfismo
Allora $\text{Fix } \psi = \{r \in \mathbb{E} \mid \psi(r) = r\}$ è un sottocampo di \mathbb{E} .

DIMOSTRAZIONE

$\psi(0) = 0, \psi(1) = 1$ quindi $0, 1 \in \text{Fix } \psi$

$r, s \in \text{Fix } \psi$, allora

$$\psi(r+s) = \psi(r) + \psi(s) = r+s \text{ dunque } r+s \in \text{Fix } \psi$$

$$\psi(rs) = \psi(r)\psi(s) = rs \text{ dunque } rs \in \text{Fix } \psi$$

Quindi $\text{Fix } \psi$ è un sottocampo di \mathbb{E} .

Sia $r \in \text{Fix } \psi, r \neq 0$: $\psi(r^{-1}) = \psi(r)^{-1} = r^{-1}$ dunque $r^{-1} \in \text{Fix } \psi$

Quindi $\text{Fix } \psi$ è un sottocampo di \mathbb{E} . \square

cardinalità dei campi finiti

Sia adesso \mathbb{L} un campo finito

Allora ha caratteristica p per un certo primo p

Inoltre $[\mathbb{L} : \mathbb{Z}_p] = n$ finito

Infatti \mathbb{L} è uno spazio vettoriale su \mathbb{Z}_p di dimensione n .

Sia v_1, \dots, v_n una base. Allora ogni elemento di \mathbb{L} si scrive in modo unico come

$$\alpha_1 v_1 + \dots + \alpha_n v_n \quad \text{con gli } \alpha_i \in \mathbb{Z}_p$$

Dunque $|\mathbb{L}| = p^n$

proposizione La cardinalità di un campo finito è un intero della forma p^n ,
per un certo primo p e un certo intero positivo n .

Consideriamo $\mathbb{L}^* = \mathbb{L} \setminus \{0\}$ è un sottogruppo moltiplicativo

Per Lagrange, se $y \in \mathbb{L}^*$ $y^{|\mathbb{L}^*|} = 1$ quindi $y^{|\mathbb{L}|+1} = y$ o $y^{p^n} = y$

Ossia tutti gli elementi di \mathbb{L} sono radici di $x^{p^n} - x$

Dunque \mathbb{L} è un campo di spezzamento di $x^{p^n} - x$

teorema Dato p primo e n intero, $n \geq 1$
esiste un campo \mathbb{L} con p^n elementi

DIMOSTRAZIONE

Considero R un campo di spezzamento di $x^{p^n} - x$ su \mathbb{Z}_p (sappiamo che esiste)

Considero $f: R \rightarrow R: r \mapsto r^p$

Considero $f^n: R \rightarrow R: r \mapsto r^{p^n}$

Considero Fix_{f^n} sottocampo di R

Gli elementi di Fix_{f^n} sono gli r tali che $f^n(r) = r$, cioè $r^{p^n} = r$,
ossia le radici di $x^{p^n} - x$

Tali radici sono distinte* dunque $|\text{Fix}_{f^n}| = p^n$ ed è il campo cercato.

NOTA Poiché $\text{Fix}_{f^n} \subseteq R$ ed entrambi sono campi di spezzamento di $x^{p^n} - x$, devono coincidere \square

**criterio
della derivata**

Sia $f(x) \in \mathbb{F}[x]$, \mathbb{F} campo qualunque

Allora $f(x)$ ha una radice multipla (in una estensione di \mathbb{F})

se e solo se $f(x)$ e $f'(x)$ hanno un fattore in comune di grado ≥ 1

DIMOSTRAZIONE

OSS se $f(x)$ e $g(x)$ hanno in comune un fattore non banale in $\mathbb{K}[x]$, con $\mathbb{F} \subseteq \mathbb{K}$, allora

cio' è vero anche in $\mathbb{F}[x]$. Infatti se fossero coprimi in $\mathbb{F}[x]$, esisterebbero $a(x), b(x) \in \mathbb{F}[x]$ t.c.

$a(x)f(x) + b(x)g(x) = 1$, ma questa relazione varrebbe anche in $\mathbb{K}[x]$ ASSURDO

Supponiamo allora che le radici di $f(x)$ siano in \mathbb{F} (altrimenti basta considerare $\mathbb{F} \subseteq \mathbb{K}$)

\Rightarrow Se $f(x)$ ha una radice multipla $\alpha: f(x) = (x - \alpha)^m q(x)$ con $m > 1$

Ora $((x - \alpha)^m)' = m(x - \alpha)^{m-1}$, quindi $f'(x) = (x - \alpha)^m q'(x) + m(x - \alpha)^{m-1} q(x) = (x - \alpha) r(x)$ poiché $m > 1$

$\Rightarrow f(x)$ e $f'(x)$ hanno in comune il fattore $(x - \alpha)$

\Leftarrow se $f(x)$ non ha radici multiple: $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ con $\alpha_i \neq \alpha_j$ per $i \neq j$

allora $f'(x) = \sum_{i=1}^n (x - \alpha_1) \cdots \widehat{(x - \alpha_i)} \cdots (x - \alpha_n)$ (dove \wedge indica il termine omissso)

Nessuna radice di $f(x)$ è radice di $f'(x)$, poiché $f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0$ poiché $\alpha_i \neq \alpha_j$

Ma se $f(x)$ e $f'(x)$ hanno in comune un fattore non banale, hanno anche una radice in comune

$\Rightarrow f(x)$ e $f'(x)$ non hanno in comune fattori non banali \square

teorema Sia \mathbb{K} un campo, sia G un sottogruppo moltiplicativo finito di \mathbb{K}^* con $|G| = n$
Allora G è ciclico.

DIMOSTRAZIONE

Ricordiamo la formula $n = \sum_{d|n} \varphi(d)$

Definisco $\forall d|n$ il sottinsieme di $G: X_d = \{a \in G \mid o(a) = d\}$

Vale $\sum_{d|n} |X_d| = n$

Quindi $n = \sum_{d|n} |X_d| = \sum_{d|n} \varphi(d)$

Se G non fosse ciclico, allora $|X_n| = 0$

Deve allora esistere $d|n$, $d < n$, tale che $1 \leq \varphi(d) < |X_d|$

Prendo $g \in X_d$. Vale che $o(g) = d$ e in particolare tutti gli elementi

di $\langle g \rangle$ sono radici di $x^d - 1$

Notiamo che in $\langle g \rangle$ ci sono esattamente $\varphi(d)$ elementi di ordine d e quindi $|\langle g \rangle \cap X_d| = \varphi(d)$

Poiché $|X_d| > \varphi(d)$, esiste in X_d un elemento $h \notin \langle g \rangle$

Ma allora h è una radice di $x^d - 1$

Dunque avrei $d+1$ radici di $x^d - 1$ ASSURDO \square

teorema Sia $f(x)$ irriducibile in $\mathbb{Z}_p[x]$ di grado n . Allora

$$K = \mathbb{Z}_p[x]/(f(x))$$

 è campo di spezzamento di $f(x)$ su \mathbb{Z}_p

DIMOSTRAZIONE

In K , $f(x)$ ha una radice, ossia $x + (f(x)) = \bar{x}$, che chiameremo α

Notiamo che α è anche radice di $x^{p^n} - x$ poiché ogni elemento di \mathbb{F}_{p^n} è radice di tale polinomio

Allora $f(x) \mid x^{p^n} - x$ poiché $f(x)$ è irriducibile

Allora tutte le radici di $f(x)$ sono radici di $x^{p^n} - x$ e

dunque stanno tutte in K

Quindi K contiene un campo di spezzamento \mathbb{J} di $f(x)$

$$\mathbb{Z}_p \subseteq \mathbb{J} \subseteq K \text{ e } \alpha \in \mathbb{J}$$

Donque $[\mathbb{J} : \mathbb{Z}_p] \geq [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$ poiché $\mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/(f(x))$

Donque $\mathbb{J} = K$ \square

corollario $\forall p$ primo, $\forall n$ intero positivo, esiste in $\mathbb{Z}_p[x]$
 un polinomio irriducibile di grado n

DIMOSTRAZIONE

Prendo un K tale che $[K : \mathbb{Z}_p] = n$, ossia un campo con p^n elementi

Ricordo che K^* è ciclico (sottogruppo moltiplicativo di un campo)

Sia β un generatore di K^*

Considero $\mathbb{Z}_p \subseteq \mathbb{Z}_p(\beta) \subseteq K$
 \uparrow
 $=$ poiché $(\beta) = K^*$

Sia $g(x)$ il polinomio minimo di β . Allora

$$\mathbb{Z}_p(\beta) \cong \mathbb{Z}_p[x]/(g(x))$$

Poiché $[K : \mathbb{Z}_p] = n$, vale $\deg g(x) = n$ \square

teorema Dato p primo e n intero positivo, vale che
 $x^{p^n} - x$ è il prodotto di tutti i polinomi monici
 irriducibili di $\mathbb{Z}_p[x]$ di grado d con $d \mid n$

DIMOSTRAZIONE

Prima fa abbiamo notato che se $f(x) \in \mathbb{Z}_p[x]$ è irriducibile di grado d
 allora divide $x^{p^d} - x$

Ora, sia $d \mid n$. Mostro che $f(x) \mid x^{p^n} - x$

Sia α radice di $f(x)$: $\alpha^{p^d} - \alpha = 0$ ossia $\alpha^{p^d} = \alpha$

$(\alpha^{p^d})^{p^d} = (\alpha)^{p^d} = \alpha$ ossia $\alpha^{p^{2d}} = \alpha$ e così via : $\alpha^{p^{kd}} = \alpha$

fino a trovare $\alpha^{p^n} = \alpha$

Allora α è radice di $f(x)$ e di $x^{p^n} - x$ e dunque $f(x) \mid x^{p^n} - x$ \square

Polinomi Simmetrici

Sia \mathbb{F} un campo. Consideriamo l'anello $\mathbb{F}[x_1, x_2, \dots, x_n]$ dei polinomi nelle variabili x_1, x_2, \dots, x_n .

Dati $\sigma \in S_n$ e $f = f(x_1, x_2, \dots, x_n) \in \mathbb{F}[x_1, x_2, \dots, x_n]$, si pone:

$$\sigma \cdot f = \sigma f(x_1, x_2, \dots, x_n) := f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

DEF. Si definiscono **polinomi simmetrici** i polinomi invarianti per permutazioni delle variabili:

$$\text{Sym}[X_n] = \text{Sym}_{\mathbb{F}}[X_n] := \{f \in \mathbb{F}[x_1, x_2, \dots, x_n] \mid \sigma \cdot f = f \quad \forall \sigma \in S_n\}$$

DEF. Il **polinomio elementare simmetrico** di grado $d \in \mathbb{N}$ nelle variabili x_1, x_2, \dots, x_n è definito come

$$e_0(x_1, x_2, \dots, x_n) := 1 \quad \text{se } d=0$$

$$e_d(x_1, x_2, \dots, x_n) := \sum_{1 \leq i_1 < i_2 < \dots < i_d \leq n} x_{i_1} x_{i_2} \dots x_{i_d} \quad \text{se } 1 \leq d \leq n$$

Teorema Fondamentale dei polinomi simmetrici

C'è un isomorfismo di anelli:

$$\text{Sym}[X_n] \cong \mathbb{F}[e_1, e_2, \dots, e_n]$$

dove $e_i := e_i(x_1, x_2, \dots, x_n)$ per $i=1, 2, \dots, n$

DIMOSTRAZIONE

Sia $f \in \text{Sym}[X_n]$. si vuole trovare algebricamente g t.c. $f = g(e_1, e_2, \dots, e_n)$

cancellando il leading term di f sottraendo un opportuno monomio nelle e_i .

Dato un monomio $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ scriviamo $\alpha := (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}^n$ e

poniamo $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ e $|\alpha| := \sum_{i=1}^n \alpha_i$

Ora ordiniamo i monomi monici di $\mathbb{F}[x_1, x_2, \dots, x_n]$ con il degree lexicographic order

dato da $x_1 > x_2 > \dots > x_n$, ossia dati $\alpha, \beta \in \mathbb{N}^n$ poniamo $x^\alpha < x^\beta$ se $|\alpha| < |\beta|$

oppure se $|\alpha| = |\beta|$ e $\alpha < \beta$ nell'ordine lessicografico di \mathbb{N}^n

Il leading term di un polinomio è il suo termine non nullo con il monomio monico più grande

Proprietà: (1) $\forall x^\alpha, x^\beta$ o $x^\alpha \leq x^\beta$ o $x^\alpha \geq x^\beta$ (l'ordine è totale)

(2) $x^\alpha < x^\beta$ se e solo se $x^\alpha x^\gamma < x^\beta x^\gamma \quad \forall \alpha, \beta, \gamma \in \mathbb{N}^n$

(3) per ogni x^α c'è un numero finito di x^β con $x^\beta < x^\alpha$

Dalle proprietà si deduce facilmente che il leading term del prodotto

di due polinomi è il prodotto dei leading terms

Siccome f è simmetrico, il suo leading term $c x^\alpha$, con $0 \neq c \in \mathbb{F}$ e $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$, deve essere

tale che $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$. Infatti, se $\alpha_i < \alpha_{i+1}$, permutando x_i e x_{i+1} fissiamo f , ma quindi f ha un termine $x^{\alpha'}$, dove α' è ottenuto da α scambiando α_i e α_{i+1} . Ma $\alpha' > \alpha$, che contraddice la massimalità di α

Ora dato il leading term $c x^\alpha$, consideriamo $e_1^{\beta_1} e_2^{\beta_2} \dots e_n^{\beta_n}$ dove $\beta_i = \alpha_i - \alpha_{i+1}$ per $i=1, \dots, n-1$ e $\beta_n = \alpha_n$

Il suo leading term è $x_1^{\beta_1 + \beta_2 + \dots + \beta_n} x_2^{\beta_2 + \dots + \beta_n} \dots x_n^{\beta_n} = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$

dunque $f(x) - c e_1^{\beta_1} e_2^{\beta_2} \dots e_n^{\beta_n}$ è un polinomio simmetrico con monomio del leading term strettamente più piccolo del leading term di f

Iterando questa procedura (per inclusione sulla grandezza del monomio del leading term di f) arriviamo in un numero finito di passi a zero.

Questo mostra che ogni polinomio simmetrico è un polinomio negli e_i a coefficienti in \mathbb{F} .

d'unicità segue dal fatto che i $e_1^{\beta_1} e_2^{\beta_2} \dots e_n^{\beta_n}$ sono linearmente indipendenti, poiché i loro leading terms sono tutti distinti. \square

Teorema Fondamentale dell'algebra

Ogni polinomio di grado positivo a coefficienti complessi ha una radice complessa.

Lemma Se ogni polinomio di grado positivo a coefficienti reali ha una radice complessa, allora ogni polinomio di grado positivo a coefficienti complessi ha una radice complessa.

DIMOSTRAZIONE

Sia $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$ e definiamo

$\bar{f}(x) = \bar{a}_n x^n + \dots + \bar{a}_1 x + \bar{a}_0 \in \mathbb{C}[x]$ dove \bar{a}_i è il coniugato complesso di a_i .

Ora $g(x) := f(x)\bar{f}(x) \in \mathbb{R}[x]$ poiché $\bar{g}(x) = \overline{f(x)\bar{f}(x)} = \bar{f}(x)f(x) = f(x)\bar{f}(x) = g(x)$

Dunque se g ha una radice $z \in \mathbb{C}$, allora $g(z) = f(z)\bar{f}(z) = 0$

$\Rightarrow f(z) = 0$ oppure $\bar{f}(z) = 0$, da cui $0 = \overline{\bar{f}(z)} = \overline{f(\bar{z})}$

$\Rightarrow f$ ha una radice complessa. \square

teorema Ogni polinomio di grado positivo a coefficienti reali ha una radice complessa.

DIMOSTRAZIONE (d'Alembert)

Sia $f(x) \in \mathbb{R}[x]$ di grado positivo $n = m2^k$, con $m, k \in \mathbb{N}$, m dispari, supponiamo monico

Dimostriamo per induzione su k .

Per $k=0$, f ha grado dispari. In questo caso f ha una radice reale: i limiti

$\lim_{y \rightarrow +\infty} f(y) = +\infty$ e $\lim_{y \rightarrow -\infty} f(y) = -\infty$ hanno segno opposto, dunque f interseca l'asse x (continuità di \mathbb{R}).

Sia ora $k \geq 1$. Sia K una estensione di \mathbb{C} in cui f si fattorizza come prodotto di fattori lineari.

Sia $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = \prod_{i=1}^n (x - r_i)$ con $r_i \in K$ non necessariamente distinti

Vogliamo mostrare che almeno un $r_i \in \mathbb{C}$

Per ogni $t \in \mathbb{R}$ sia $f_t(x) := \prod_{1 \leq i < j \leq n} (x - r_i - r_j - tr_i r_j)$

Osserviamo che i coefficienti di $f_t(x)$ sono polinomi negli r_i a coefficienti reali, dunque

i coefficienti di $f_t(x)$ sono in K . Ma questo polinomio negli r_i , dunque i coefficienti di $f_t(x)$

sono polinomi simmetrici nelle r_i a coefficienti reali.

Per il teorema fond. dei polinomi simmetrici, questi coefficienti si esprimono come polinomi

nelle $e_i(r_1, r_2, \dots, r_n)$ a coefficienti reali, e gli e_i sono a meno del segno a_{n-i} , reale

$\Rightarrow f_t(x)$ ha coefficienti reali

Ora il grado di $f_t(x)$ è $\binom{n}{2} = \frac{n(n-1)}{2} = m(n-1)2^{k-1}$ (bisogna scegliere i, j da $\{1, \dots, n\}$) e $n-1$ è dispari \Rightarrow per ipotesi induttiva $f_t(x)$ ha una radice complessa

Dunque per una certa coppia (i, j) con $1 \leq i < j \leq n$, $r_i + r_j + tr_i r_j \in \mathbb{C}$

Questo è vero $\forall t \in \mathbb{R}$, ma (i, j) dipende da t . Ma i reali sono infiniti, dunque esiste

(i, j) per cui esistono $t_1, t_2 \in \mathbb{R}$ t.c. $r_i + r_j + t_1 r_i r_j, r_i + r_j + t_2 r_i r_j \in \mathbb{C}$

$\Rightarrow (t_1 - t_2)r_i r_j \in \mathbb{C} \Rightarrow r_i r_j \in \mathbb{C} \Rightarrow r_i + r_j \in \mathbb{C}$

Ma allora $x^2 - (r_i + r_j)x + r_i r_j = (x - r_i)(x - r_j) \in \mathbb{C}[x]$

In questo caso le radici sono complesse $\Rightarrow r_i, r_j \in \mathbb{C}$ \square

Esercizio compito 21.I.2019

- 1) Trovare il polinomio minimo su \mathbb{Q} di $\sqrt[3]{7} + \sqrt{2}$
- 2) Sia $\zeta_5 \in \mathbb{C}$ radice quinta di 1, $\zeta_5 \neq 1$, $\zeta_5 = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$
Trovare il polinomio minimo di ζ_5 su \mathbb{Q} e su $\mathbb{Q}(\sqrt{5})$

RISOLUZIONE

1) $\alpha = \sqrt[3]{7} + \sqrt{2} \quad \alpha - \sqrt{2} = \sqrt[3]{7} \quad (\alpha - \sqrt{2})^3 = 7$

$$\alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} = 7$$

$$\alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} - 7 = 0 \quad x^3 - 3\sqrt{2}x^2 + 6x - 2\sqrt{2} - 7 \notin \mathbb{Q}[x]$$

$$\sqrt{2}(3\alpha^2 + 2) = \alpha^3 + 6\alpha - 7$$

$$\sqrt{2} = \frac{\alpha^3 + 6\alpha - 7}{3\alpha^2 + 2} \in \mathbb{Q}(\alpha)$$

$$2(3\alpha^2 + 2)^2 = (\alpha^3 + 6\alpha - 7)^2$$

$$\text{Facendo i calcoli, trovo } \alpha^6 - 6\alpha^4 - 14\alpha^3 + 12\alpha^2 - 84\alpha + 41 = 0$$

Dunque $x^6 - 6x^4 - 14x^3 + 12x^2 - 84x + 41$ è un polinomio di cui α è radice. È irriducibile?

Calcolo il grado $[\mathbb{Q}(\alpha) : \mathbb{Q}]$

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ \uparrow \quad \downarrow \\ \mathbb{Q}(\sqrt{2}) \quad \mathbb{Q}(\sqrt[3]{7}) \\ \uparrow \quad \downarrow \quad \uparrow \quad \downarrow \\ \mathbb{Q} \quad \mathbb{Q} \quad \mathbb{Q} \quad \mathbb{Q} \end{array}$$

$x^2 - 2$ (irr. Eisenstein) $x^3 - 7$ (irr. Eisenstein)

$$\sqrt[3]{7} \in \mathbb{Q}(\alpha) \text{ perché } \sqrt[3]{7} = \alpha - \sqrt{2}$$

$\mathbb{Q}(\alpha) \quad \mathbb{Q}(\alpha)$

Per il teo. torri:

$$2 \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] \text{ e } 3 \mid [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

$$\text{Quindi } 6 \mid [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

Inoltre, poiché α è radice di un polinomio di grado 6, il polinomio minimo di α ha grado ≤ 6 .

$$\text{Dunque } [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 6$$

$$\text{Deduco quindi } [\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$$

Allora adesso sappiamo che $x^6 - 6x^4 - 14x^3 + 12x^2 - 84x + 41$ è il polinomio minimo cercato
($\mathbb{Q}(\alpha) \cong \mathbb{Q}[x] / (p.m.)$)

2) ζ_5 è radice di $x^5 - 1$

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$$

ζ_5 è radice di questo

Dimostreremo che $x^4 + x^3 + x^2 + x + 1$ è irriducibile utilizzando Eisenstein⁺

oss Sia K campo e $f(x) \in K[x]$

Vale che $f(x)$ è irriducibile se e solo $f(ax+b)$, con $a \in K^*$, è irriducibile

Infatti, se fosse $f(x) = g(x)h(x)$ allora $f(x+1) = g(x+1)h(x+1)$

$$\text{Dunque considero } x^4 + x^3 + x^2 + x + 1 = \frac{x^5 - 1}{x - 1}$$

e sostituisco $x \rightarrow x+1$

$$(x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1 = \frac{(x+1)^5 - 1}{x} = \frac{x^5 + \binom{5}{1}x^4 + \binom{5}{2}x^3 + \binom{5}{3}x^2 + \binom{5}{4}x + 1 - 1}{x} =$$

$$= x^4 + \binom{5}{1}x^3 + \binom{5}{2}x^2 + \binom{5}{3}x + \binom{5}{4}$$

Applico Eisenstein con $p=5$

NOTA: per ogni p primo, vale, con la stessa dimostrazione, che $x^{p-1} + x^{p-2} + \dots + x + 1$ è irriducibile su \mathbb{Q}